creative commons
COMMONS DEED

저작자표시 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.
- 이차적 저작물을 작성할 수 있습니다.
- 이 저작물을 영리 목적으로 이용할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

공학석사 학위논문

비상분리기능의 안전요구사항 분석 및 검증

Analysis and Verification of Safety Requirements for Emergency Disconnect Function

2015 년 2 월

서울대학교 대학원

조선해양공학과

남 현 준

비상분리기능의 안전요구사항 분석 및 검증

지도 교수 양 영 순

이 논문을 공학석사 학위논문으로 제출함
2015 년 2 월

서울대학교 대학원
조선해양공학과
남 현 준

남현준의 공학석사 학위논문을 인준함
2015 년 2 월

위 원 장 성 우 제 (인)

부위원장 양 영 순 (인)

위 원 임 영 섭 (인)

초 록

1998년 국제전기기술위원회는 안전계장시스템을 통해 구현되는 안전기능을 대상으로 생애주기 동안의 관리를 위한 지침을 제시하였다. 이후 각종 산업에서는 사용되고 있는 안전기능 중 안전계장시스템을 통해 구현되는 기능에 대해 국제전기기술위원회에서 제시한 지침을 적용하였으며, 노르웨이의 석유 협회인 OLF도 이러한 경향에 따라 석유산업에 해당 지침을 적용하였다. 하지만 석유산업에 사용되고 있는 안전기능 중 대다수는 위험 경고 및 작업자를 필요로 하는 조정시스템을 통해 구현되기 때문에 제시된 지침의 대상에 부합하지 않았다. 따라서 OLF는 수동작동기능 개념을 도입하여 조정시스템을 통해 구현되는 안전기능을 안전계장시스템을 통해 구현되는 기능으로 간주하였으나, 이는 실제 제어루프 중 일부만을 다루는 한계를 가지고 있다. 따라서 본 논문에서는 안전기능을 구현하기 위한 조정시스템의 설계 및 검증을 위해 국제전기기술위원회에서 제시한 지침을 기반으로 하되, 실제 제어루프를 고려할 수 있는 방안을 제시하였다. 또한 제시한 접근 방안을 해양시추산업에 사용되는 비상분리기능에 적용하였다. 즉, 비상분리기능에 요구되는 사항을 분석하고 이를 비상분리시스템에 할당하여, 비상분리시스템이 할당된 요구사항을 만족시킬 수 있는지 검증하였다. 비상분리기능에 요구되는 사항은 안전무결성 요구사항과 안전기능 요구사항으로 분류하여 각각에 대해 분석 및 검증을 수행하였다. 안전무결성 요구사항을 분석하기 위해 SINTEF에서 제시한 Environmental Risk Acceptance Criteria을 기준으로 삼았고, PFH 2.71E-07/hour 이하의 안전무결성이 요구되는 것을 확인하였다. 해당 요구사항을 만족시키기 위해 구조적 강건성을 고려하여 비상분리시스템의 Redundancy를 결정하였고, Simplified Method, IEC Formulas, 그리고 PDS Method를 통해 안전무결성 요구사항 만족여부를 검증하였다. 수행 결과 PFH 1.89E-07/hour, 1.92E-07/hour, 1.83E-07/hour로 요구되는 안전무결성 수준을 만족시키는 것을 확인하였다. 최종적으로 검증의 타당성 검토를 위해 Petri Net with Monte-Carlo Simulation을 통해 분석을 수행하였고, 수행 결과 PFH: 1.89E-07/hour로 검증이 타당하였음을 확인하였다. 안전기능 요구사항으로 비상분리기능이 작동하는데 소요되는 시간으로 정의되는 반응시간에 대한 조건이 존재하며, API에서 요구한 최소 반응시간인

90초를 기준으로 삼았다. API SPECIFICATION 16D에 따라 제어시스템을 구성하는 주요 장비 제원을 결정하였고, 제조업체를 통해 구매하는 장비의 제원은 카탈로그를 통해 파악하여 비상분리시스템을 구성하였다. 반응시간 검증을 위해 SimulationX를 통해 모델링 및 시뮬레이션을 수행하였고, 수행 결과 비상분리기능 수행에 소요되는 시간은 53초로 요구되는 최소 반응시간 내에 기능이 수행되는 것을 확인하였다. 조정시스템으로 구현되는 안전기능에 대해 실제 제어루프를 고려할 수 있는 접근 방안을 제시하였고, 비상분리기능에 적용하여 실질적인 적용 방안도 함께 제시하였다. 제시한 접근 방안은 대다수의 안전기능이 조정시스템으로 구현되는 석유산업에 폭넓게 적용될 수 있을 것으로 기대되며, 다른 산업에도 적용되어 안전성을 향상시키는데 도움이 될 수 있을 것이라 생각된다.

주요어: 비상분리기능, 안전요구사항, 안전무결성, 반응시간, Petri Net SimulationX
학 번: 2013-21067

목 차

제 1 장 서 론 1
제 1 절 연구 배경 1
제 2 절 연구 내용 4

제 2 장 비상분리기능 정의 5

제 3 장 안전무결성 요구사항 분석 및 검증 20
제 1 절 안전무결성 요구사항 분석 23
제 2 절 안전무결성 요구사항을 고려한 시스템 구성 26
제 3 절 안전무결성 요구사항 검증 32
제 4 절 안전무결성 요구사항 검증의 타당성 검토 46

제 4 장 안전기능 요구사항 분석 및 검증 56
제 1 절 안전기능 요구사항 분석 56
제 2 절 안전기능 요구사항을 고려한 시스템 구성 58
제 3 절 안전기능 요구사항 검증 70

제 5 장 결 론 78

참고문헌 80

부록 83

Abstract 94

표 목차

Table 3-1 SIL Table (IEC, 1999) 23
Table 3-2 Failure Classification..... 34

그림 목차

Figure 1-1 Layers of Defense against a Possible Accident (American Institute of Chemical Engineers, 2001) 1
Figure 1-2 Overall Safety Lifecycle (IEC, 1998) 2
Figure 1-3 Analysis and Verification Procedure for Overall Safety Requirements (Based on IEC, 1998, ISO, 2006).. 4
Figure 2-1 Description of Riser Stack-up and Utilization Ratios for Quasi-static Drift (Josefsson, 2014) 5
Figure 2-2 Typical Drive-off/Drift-off Behavior (Chen, 2007) 6
Figure 2-3 Three Main Barrier Functions with Respect to the Safety of DP Drilling Operation (Chen, 2007)..... 7
Figure 2-4 Description of Emergency Disconnect Function (Based on Chen, 2007, ABEL ENGINEERING Web Site) 8
Figure 2-5 Emergency Disconnect Sequence..... 9
Figure 2-6 Description of Emergency Disconnect System (Based on API, 2012) 10
Figure 2-7 Blind Shear Ram Preventer(Transocean, 2011) 11
Figure 2-8 Shearing Process by Blind Shear Ram Preventer (National Commission, 2011) 12
Figure 2-9 Blind Shear Ram Preventer Closing (Januarilham, 2012) 12
Figure 2-10 Choke & Kill Valve(Magnum, 2012) 13
Figure 2-11 LMRP Connector(drill-equip.com) 14
Figure 2-12 Choke & Kill Stab Connector(Radoil.com).... 15
Figure 2-13 Multiplexed Electro-Hydraulic Control System(Bai, 2012) 16
Figure 2-14 SCADA System for Emergency Disconnect. 17
Figure 2-15 Control Logic for Measuring Drilling Rig's Position..... 18

Figure 2-16 Control Logic for Initiating Emergency Disconnect Function 19
Figure 3-1 Reliability Block Diagram of BOP Control System (Eikeskog, 2012) 20
Figure 3-2 Control Loop for Operator Intervention System(Left) and Control Loop for Manual Initiator Function Concept(Right) 21
Figure 3-3 Subsystems and Required Percentage of Safety Integrity 22
Figure 3-4 Environmental Risk Acceptance Criteria Related to Released Volumes of Oil to Sea(SINTEF, 2011) 24
Figure 3-5 Risk Reduction Scheme for Hydrocarbon Release to Sea Initiated by Loss of Position 25
Figure 3-6 Required Safety Integrity for Subsystems (Based on Pepperl-Fuchs, 2001) 26
Figure 3-7 Architectural Constraints on Type A Safety Related Subsystems(IEC, 1999) 27
Figure 3-8 Architectural Constraints on Type B Safety Related Subsystems(IEC, 1999) 27
Figure 3-9 Functional Block Diagram for Emergency Disconnect System 28
Figure 3-10 Safety Integrity Requirements of Emergency Disconnect System from DGPS to Indicator 29
Figure 3-11 Reliability Data for Emergency Disconnect System from DGPS to Indicator Data from PDS Handbook and IEC 60947-5-4) 29
Figure 3-12 Block Diagram of Emergency Disconnect System from DGPS to Indicator 30
Figure 3-13 Safety Integrity Requirements of Emergency Disconnect System from Push Button to Solenoid Valve. 31
Figure 3-14 Reliability Data for Emergency Disconnect System from DGPS to Indicator (Data from PDS Handbook and ISO 13849-1) 31
Figure 3-15 Block Diagram of Emergency Disconnect System from Push Button to Solenoid Valve 31
Figure 3-16 Block Diagram for Emergency Disconnect System 32
Figure 3-17 State Variable and Time to Failure of an Item (Rausand, 2014) 33

Figure 3-18 Probability Distribution Function and Probability Density Function (Rausand, 2014) 33
Figure 3-19 PFD of an Item with Imperfect Proof Test(Rausand, 2014) 35
Figure 3-20 Number of Item Failure N(t) Plotted against Time t (Rausand, 2014)..... 35
Figure 3-21 Relationship between ROCOF and PFH in time interval (t_1, t_2)(Rausand, 2014) 37
Figure 3-22 PDS Formulas for Average PFH (Rausand, 2014) 41
Figure 3-23 Configuration Factors for Selected koon Architectures(Rausand, 2014) 41
Figure 3-24 PFH Calculation Formulas 42
Figure 3-25 Reliability Block Diagram for Emergency Disconnect System..... 42
Figure 3-26 Input Data Set for Safety Integrity Verification of Emergency Disconnect System 43
Figure 3-27 Safety Integrity Analysis Results..... 44
Figure 3-28 Reliability Block Diagram for Re-arranged Emergency Disconnect System..... 44
Figure 3-29 Safety Integrity Analysis Results for Re-arranged Emergency Disconnect System..... 45
Figure 3-30 Petri Net Model for Repairable 1oo2 Voted Group (Rausand, 2014)..... 47
Figure 3-31 Reachability Graphs of Petri Net Model for 1oo2 Voted Group(Rausand, 2014)..... 47
Figure 3-32 Analytical Methods for Petri Net Models(IEC, 2012)..... 48
Figure 3-33 Petri Net Model for 2oo3 Voted Group(Rausand, 2013)..... 48
Figure 3-34 Simple Petri Net Model(Rausand, 2013) 49
Figure 3-35 Petri Net Model with Inhibitor Arc(Rausand, 2014)..... 50
Figure 3-36 Symbols Used for Transition(Rausand, 2014) 51
Figure 3-37 Reliability Block Diagram Driven Petri Net(Signoret, 2012)..... 53
Figure 3-38 Petri Net Model for 1oo2 Valve Group(Signoret, 2012)..... 53
Figure 3-39 Petri Net Model for Each Component of

Emergency Disconnect System..... 54
Figure 4-1 Description of Watch Circle and Drive-off Analysis of Vessel in Beaufort Sea (Imperial Oil, 2009). 57
Figure 4-2 Conventional Blind Shear Ram Preventer (Hydril) 59
Figure 4-3 MCS Gate Valve for Choke & Kill valve(Cameron) 59
Figure 4-4 DWHC Collet Connector for LMRP Connector(Cameron) 60
Figure 4-5 Choke & Kill Stab Connector(Radoil) 61
Figure 4-6 Specification of Emergency Disconnect System 61
Figure 4-7 Forces on the Hydraulic Actuator 62
Figure 4-8 Pressures on Blind Shear Ram Actuator..... 63
Figure 4-9 Distortion Energy Theory for Drill Pipe Shearing 64
Figure 4-10 Drill Pipe Shearing Pressure Calculation Method (Agito AS, 2010) 64
Figure 4-11 Accumulator Conditions..... 65
Figure 4-12 Accumulator Calculation Method Overview(API, 2004) 67
Figure 4-13 Method B for Calculating Accumulator Specifications (API, 2004) 67
Figure 4-14 Subsea Accumulator Specification..... 68
Figure 4-15 HPU Module and Model of Subsea Accumulator Charging System 69
Figure 4-16 Simulation Result of Hydraulic Transmission from HPU to Subsea Accumulator 69
Figure 4-17 Specification of Emergency Disconnect System Model..... 70
Figure 4-18 Schematic Diagram of Subsea Electro-Hydraulic Control for Emergency Disconnect System (Pipe & Hose Specification from Agito AS, 2010)..... 71
Figure 4-19 Forces on Blind Shear Ram Preventer..... 72
Figure 4-20 Blind Shear Ram Preventer Model 72
Figure 4-21 Choke & Kill Valve Model 73
Figure 4-22 Concept of LMRP Connector Actuator Modeling 74
Figure 4-23 LMRP Connector Model..... 74

Figure 4 -24 Choke & kill Stab Connector 7 5
Figure 4 -25 Emergency Disconnect System Model..... 7 6
Figure 4 -26 Response Time by Hydraulic Control System. 7 7

제 1 장 서 론

제 1 절 연구 배경

모든 산업은 본연적으로 특정 수준의 위험성을 가지고 있기 때문에 사고를 예방하고, 그 피해 정도를 경감시키기 위해 다양한 안전기능을 필요로 한다. 이러한 안전기능은 Fig. 1-1와 같이 기본공정제어시스템, 위험 상황 경고 및 작업자를 필요로 하는 조정시스템(이하 조정시스템), 그리고 안전계장시스템 등의 독립적인 안전관련시스템을 통해 구현된다.

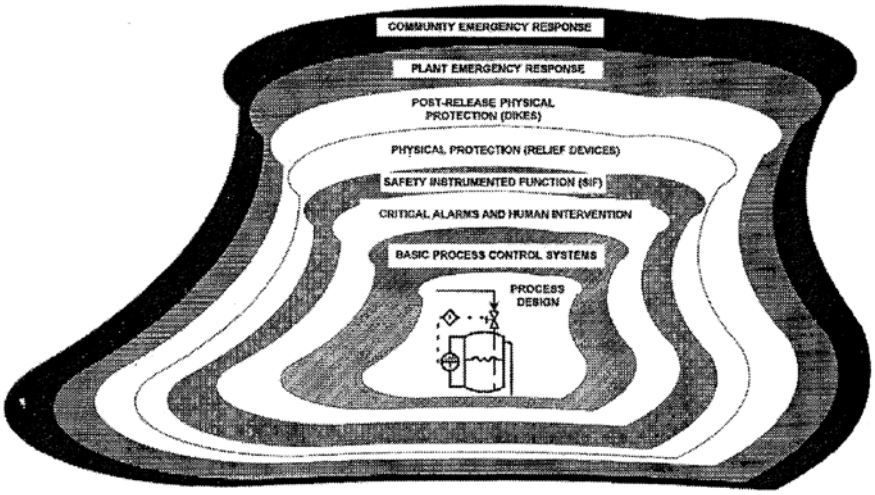

Figure 1-1 Layers of Defense against a Possible Accident
(American Institute of Chemical Engineers, 2001)

1998년 국제전기기술위원회(이하 IEC)는 '안전기능이 안전관련시스템을 통해 정상적으로 구현되고 있는 상태에서 제어되고 있는 장치(Equipment Under Control)의 안전'으로 정의되는 기능적 안전(Functional Safety) 개념을 도입하여, 기능적 안전을 보장하기 위해 생애주기 동안 안전관련시스템을 관리할 수 있는 지침을 제시하였다(Fig. 1-2). 해당 지침은 전기·전자 제어시스템으로 구성된 안전관련시스템으로 구현되는 안전기능만을 대상으로 하였기 때문에 안전계장시스템으로 구현되는 안전기능에 초점을 맞춰 지침이 확립되었다. 이후 해당 지침은 화학공정산업(IEC 61511), 원자핵산업(IEC 61513), 자동차산업(ISO 26262), 의료산업(IEC

60601), 그리고 철도산업(IEC 62425, 62269)에 적용되었다.

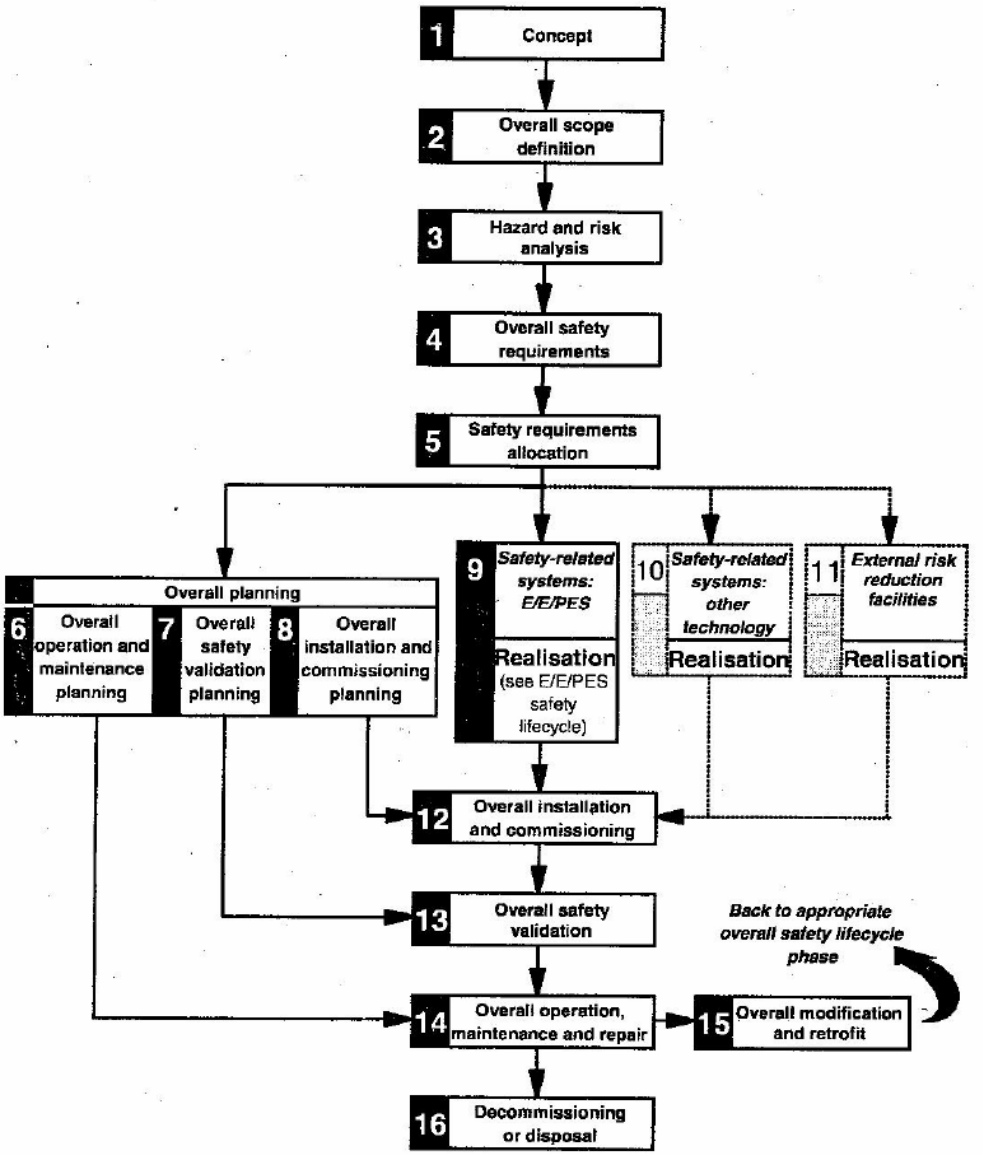

Figure 1-2 Overall Safety Lifecycle (IEC, 1998)

이러한 경향에 따라 2004년 노르웨이의 석유협회인 OLF는 석유산업에 IEC에서 제시한 지침을 적용하였다. 하지만 석유산업에서 사용되는 대다수의 안전기능은 조정시스템에 의해 구현되기 때문에 안전계장시스템을 대상으로 확립된 지침을 적용하기에 어려움이 있었다. 이에 OLF는 수동작동기능(Manual Initiator Function)이라는 새로운 개념을 도입하여 석유산업에 사용되는 조정시스템을 안전계장시스템으로 간주하였다. 이후 석유산업에 사용되는 안전관련시스템에 대해서 OLF의

지침에 따라 대다수의 연구가 수행되었다. 하지만 작업자에 대한 의존도가 높은 해저폭발방지기와 같은 조정시스템에 대해서는 안전계장시스템으로 간주하는 것에 어려움이 있으며(Eikeskog, 2012), 석유산업에서는 전기·전자 제어시스템이 아닌 유압 제어시스템이 큰 비중을 차지하고 있기 때문에, IEC에서 제시한 지침을 그대로 적용하는데 한계가 있다.

본 논문은 해양시추산업에 사용되는 비상분리기능을 연구 대상으로 삼아, 라이저(Riser)와 유정헤드(Wellhead)의 기능적 안전을 보장하기 위해 해당 기능에 요구되는 사항을 분석하고, 이를 만족시킬 수 있도록 비상분리시스템을 구성하여 구성된 시스템이 해당 기능을 구현하여 제어되고 있는 장치의 안전을 성공적으로 보장할 수 있는지 검증하였다. 마콘도 유전 사고 이후 새롭게 개정된 API STANDARD 53(2012)에서는 동적 위치제어시스템을 사용하는 시추리그에 대해서 비상분리기능을 의무적으로 구비할 것을 권고하고 있으며, 2003년 West Engineering Services에서 북해에 사용중인 시추리그에 대해 조사한 바에 따르면 당시에도 동적 위치제어시스템을 사용하는 시추리그 모두에 비상분리기능이 구비되어 있음을 확인할 수 있었다. 또한 비상분리기능은 북극해의 유전 개발에 필요한 핵심 안전기능으로 주목받고 있음을(Hamilton, 2011) 확인할 수 있었다. 이러한 현상들은 해양시추산업에서 사용되는 안전기능으로서 비상분리기능의 중요성을 방증하고 있다. 하지만 EQE International(2000)사에서 비상분리시스템에 대해 리스크 평가를 수행한 사례를 제외하고는 다른 연구 사례를 찾아볼 수 없어 학문적인 접근이 더욱 필요한 상태이며, 이러한 관점에서 비상분리기능을 연구 대상으로 삼는 것이 의미를 가진다고 할 수 있다.

석유산업에 사용되는 안전관련시스템과 관련된 대다수의 연구가 OLF의 지침에 따라 수행되고 있다. 본 논문에서는 OLF와 같이 IEC에서 제시한 지침을 차용하여 조정시스템에 적용하였다. 하지만 조정시스템을 안전계장시스템으로 간주하기 위해 OLF에서 도입한 수동작동기능 개념이 실제 조정시스템의 제어루프를 고려하지 못하여 보수적이지 못한 결과를 도출할 수 있다는 점에 착안하여, 실제 제어루프를 고려한 접근 방안을 제시하였다. 제시한 접근 방안에 따라 비상분리기능을 대상으로 연구를 수행하여 실질적인 적용 방안을 함께 제시하였다.

제 2 절 연구 내용

IEC는 제어되고 있는 장치에 대해 위험도 분석을 수행하여 필요한 안전기능을 정의, 해당 기능에 대해 요구사항을 분석하여 이를 만족시키기 위해 시스템을 구성하고 검증할 것을 권고하고 있다. 하지만 본 논문에서는 제어되고 있는 장치에 해당하는 라이저와 유정헤드에 대한 위험도 분석을 수행하지 않고, 안전기능 중 비상분리기능을 대상으로 삼아 연구를 수행하였다. Fig. 1-3의 절차에 따라 연구를 수행하였다.

Figure 1-3 Analysis and Verification Procedure for Overall Safety Requirements (Based on IEC, 1998, ISO, 2006)

비상분리기능의 정의와 구성을 분석하고, 이를 구현하기 위해 필요한 비상분리시스템의 구성을 함께 분석하여 제 2장에 정리하였다. 안전요구사항은 안전무결성 요구사항과 안전기능 요구사항으로 분류되는데, 전자는 위험상황을 인지하고 안전기능을 성공적으로 수행할 수 있는 능력과 관계가 있으며 후자는 제어되고 있는 장치의 안전을 보장하기 위한 본연의 목적과 관계가 있다. 비상분리기능을 대상으로 안전무결성 요구사항과 안전기능 요구사항을 분석하고, 요구사항을 비상분리시스템에 할당하였다. 이후 비상분리시스템에 할당된 안전무결성 요구사항과 안전기능 요구사항의 만족 여부를 검증하였고, 이 과정을 제 3장과 제 4장에 각각 정리하였다. 제 5장에서는 본론의 내용을 정리하고, 연구 결과가 가지는 의의를 기술하였다.

제 2 장 비상분리기능 정의

시추리그가 규정된 위치를 벗어나면 라이저와 유정헤드에 하중이 걸려 취약한 부분이 파괴된다(Fig. 2-1[①]). 시추작업이 많이 진행되지 않은 상황에서 라이저 또는 유정헤드가 파괴될 경우에는 단순히 이수(Mud)가 손실되는 사고로 이어지겠지만, 저류층까지 시추가 진행된 상황에서는 저류층 유체, 즉 탄화수소가 바다로 유출되는 최악의 사고로 이어질 수 있다. 만약 사고 이후 대처가 적절히 이루어질 경우에는 해당 유정의 개발을 재개할 수도 있지만, 그렇지 못할 경우에는 해당 유정을 폐쇄하고 다른 위치에서 새로운 유정을 개발해야 하는 상황이 발생할 수도 있기 때문에 이러한 사고는 유정 개발 계획에 막대한 차질을 일으킨다.

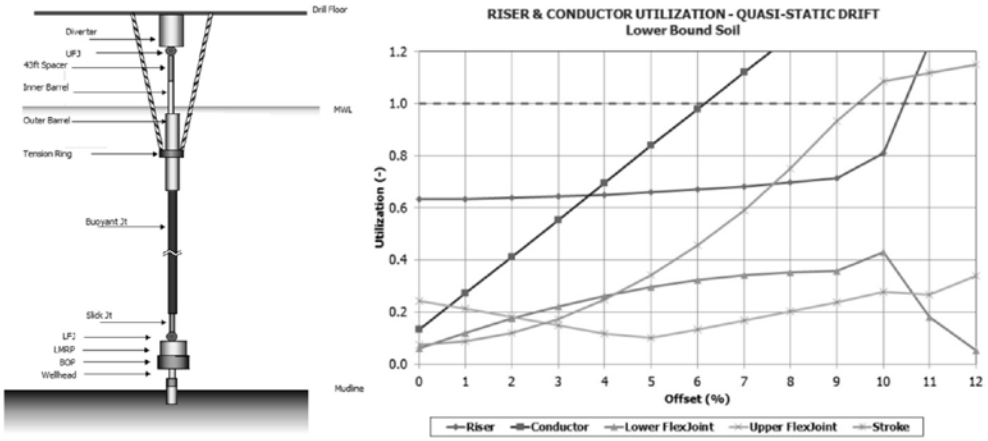

Figure 2-1 Description of Riser Stack-up and Utilization Ratios for Quasi-static Drift (Josefsson, 2014)

① Fig. 2-1은 일반적인 라이저시스템의 구성과 시추리그의 Offset(규정된 위치에서 벗어난 거리를 수심으로 나눠 백분율로 나타낸 값)에 따라 각 구성 요소에 작용하는 하중을 나타낸다. Josefsson(2014)은 시추리그에 Drift-off가 발생하는 특정 상황에 대해서 구조해석을 수행하였다. 각 구성 요소마다 고장 유형을 정의하고, 유형별로 고장이 발생할 때의 하중을 계산하여 기준으로 삼았다. 이후 시추리그의 Offset에 따라 각 구성 요소에 발생하는 하중을 기준으로 나눠 Utilization Ratio를 계산하였다. 해당 시나리오에서는 시추리그의 Offset이 6.14 %일 때 Conductor Casing에 고장이 발생하여 파괴된다. Conductor Casing의 기능은 위에 설치되는 해저장비들의 하중을 견디는 것으로, 만약 파괴될 경우 설치된 장비들이 유실될 수 있다. 즉, Conductor Casing의 파괴는 해저폭발방지기(Subsea BOP) 유실 사고로 연결되어 유정제어수단을 잃는 상황이 발생할 수 있다.

시추리그가 규정된 위치를 벗어나는 원인은 'Drive-off' 와 'Drift-off' 의 두 가지 유형으로 존재한다. Drive-off는 Thruster의 잘못된 작동으로 시추리그가 목표 지점에서 멀어지는 현상을 의미하고, Thruster 제어 당시 목표 지점을 잘못 설정하거나 Thruster 중 일부가 오작동을 일으키는 경우 발생한다. Drift-off는 해류에 시추리그가 떠밀려 목표 지점에서 멀어지는 현상을 의미하고, 정전으로 Thruster 기능을 손실하거나 갑작스런 기상조건의 변화가 있을 경우 발생한다. 두 사건이 발생하였을 때 시추리그의 일반적인 움직임은 Fig. 2-2와 같이 나타나며, Drive-off가 발생하면 시추리그가 Thruster의 힘으로 이동하기 때문에 같은 시간 내에 많은 거리를 이동하게 된다. Drive-off가 발생할 경우에는 목표 지점을 수정하거나 Thruster의 작동을 멈추는 등 여러 가지 대처 방안이 존재하지만, Drift-off가 발생할 경우에는 대처할 수 있는 방안이 상대적으로 적다.

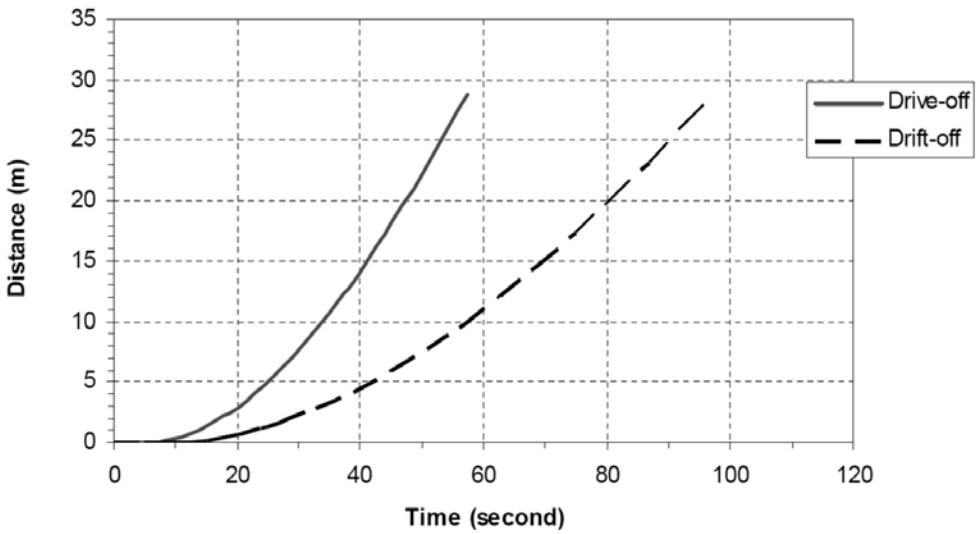

Figure 2-2 Typical Drive-off/Drift-off Behavior (Chen, 2007)

앞서 살펴본 두 원인에 의해 시추리그가 규정된 위치를 벗어날 경우 일반적으로 세 가지 방호기능(Barrier Function)이 사용된다(Fig. 2-3). 시추리그가 규정된 위치를 벗어나는 사건은 그 정도에 따라 Loss of Position, Critical Loss of Position, 그리고 Loss of Well Integrity로 분류된다. 또한 시추리그가 규정된 위치를 벗어나는 정도는 시추리그가

Watch Circle[②]로 명명된 여러 단계의 한계선(Green Zone or Advisory Limit, Yellow Limit, Red Limit, 그리고 Physical Limit)을 벗어나는지 여부로 판단한다. 시추리그가 Green Zone(Advisory Limit)을 벗어날 경우에는 Loss of Position을 방지하기 위해 동적 위치제어시스템을 통해 위치제어기능이 구현되며, Yellow Limit을 벗어날 경우에는 Critical Loss of Position을 방지하기 위해 마찬가지로 동적 위치제어시스템을 통해 위치제어기능이 구현되지만 앞의 경우와 달리 시추작업을 중단하고 비상상황에 대비한다. 최종적으로 시추리그가 Red Limit을 벗어날 경우에는 Loss of Well Integrity를 방지하기 위해 비상분리시스템을 통해 비상분리기능을 수행한다. 시추리그가 Physical Limit을 벗어날 경우에는 라이저와 유정헤드의 취약부가 파괴되어 유정의 무결성을 잃는다. 방호기능을 구현하기 위한 안전관련시스템으로 동적 위치제어시스템과 비상분리시스템이 필요하고, Fig. 1-1에 따라 분류할 경우 동적 위치제어시스템은 기본공정제어시스템에 해당하고 비상분리시스템은 조정시스템으로 분류할 수 있다.

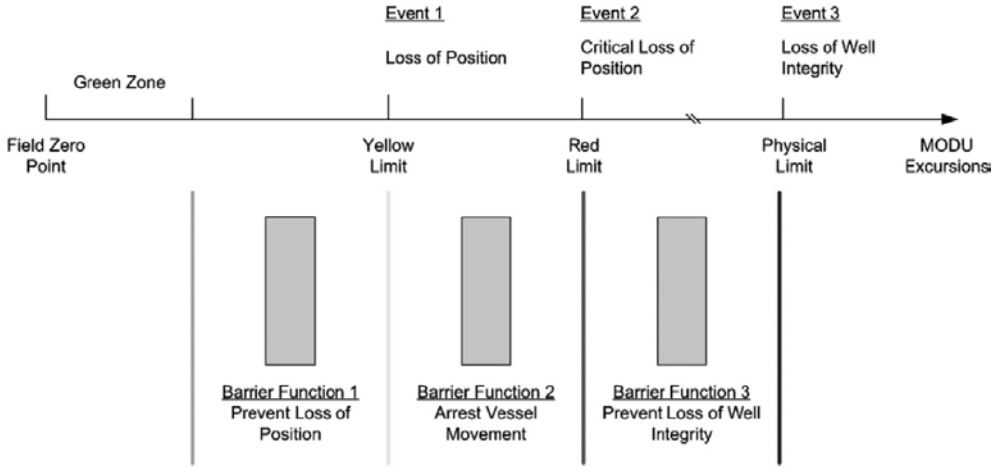

Figure 2-3 Three Main Barrier Functions with Respect to the Safety of DP Drilling Operation (Chen, 2007)

본 논문에서는 최종단계의 방호기능에 해당하는 비상분리기능을 연구 대상으로 삼았다. 비상분리기능은 부유식 시추리그가 Red Limit을 벗어날 경우 유정을 폐쇄하고, Lower Marine Riser Package(이하

② Watch Circle은 시추를 수행하는 석유회사마다 조금씩 다르다. 수심에 따라 Yellow Limit과 Red Limit의 기준이 존재하며, Physical Limit은 라이저와 유정헤드의 구조해석을 통해 결정된다.

LMRP)를 분리하는 기능으로 정의된다(API, 2004). Fig. 2-3의 방호기능3, 즉 Prevent Loss of Well Integrity에 해당하는 기능으로 시추리그가 Red Limit을 벗어나면 작업자에게 경고를 주고, 이를 확인한 작업자가 버튼을 눌러 기능이 작동된다. 기능이 작동되면 Fig. 2-4의 오른쪽 그림과 같이 유정을 폐쇄하고, LMRP를 Lower Blowout Preventer(이하 BOP) Stack에서부터 분리한다. 유정이 폐쇄되지 않은 상태에서 LMRP가 분리될 경우에는 저류층 유체(Reservoir Fluid)가 바다로 유출되기 때문에 LMRP가 분리되기 전에 반드시 유정이 폐쇄되어야 한다. 간혹 자동전단기능(Auto-shear Function)[③]을 갖춘 시추리그에 한해 LMRP분리가 먼저 이뤄질 수 있지만, 일반적으로 유정폐쇄가 먼저 이뤄진 후에 LMRP분리가 이뤄진다.

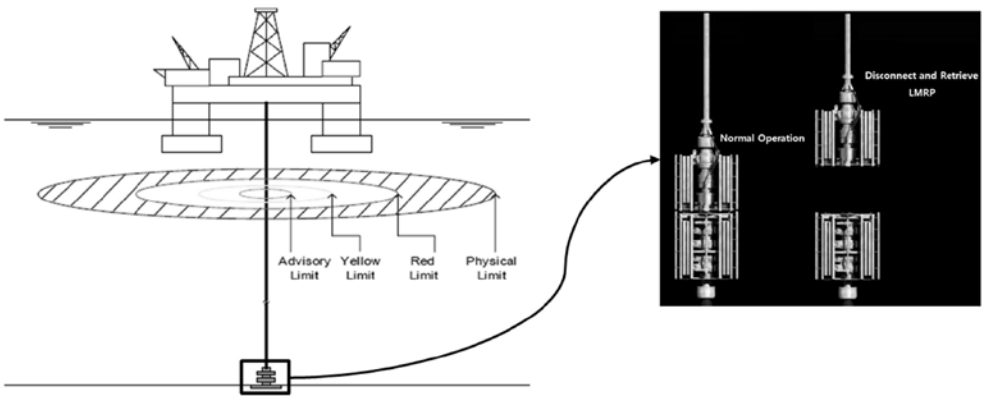

Figure 2-4 Description of Emergency Disconnect Function
(Based on Chen, 2007, ABEL ENGINEERING Web Site)

비상분리기능의 구성과 절차는 시추리그마다 다르지만, 유정폐쇄를 위해 블라인드 전단 램 방지기(Blind Shear Ram Preventer)를 닫는 기능과 LMRP분리를 위해 LMRP연결부(LMRP Connector)를 분리하는 기능을 반드시 포함한다(API, 2004). 일반적으로는 유정폐쇄를 위해 블라인드 전단 램 방지기를 닫는 기능과 초크 & 킬 밸브(Choke & Kill

[③] 자동전단기능은 계획되지 않은 LMPR분리가 발생하였을 경우 자동으로 유정을 폐쇄하는 기능으로 정의된다(West Engineering, 2003). LMRP가 분리되면 기계적으로 자동전단기능이 작동되며, Lower BOP Stack에 위치한 축압기로부터 유압을 제공받아 유정을 폐쇄한다. 일반적으로 사용되는 기능은 아니며, 2003년 West Engineering Services에서 북해에 사용중인 시추리그에 대해 조사한 바에 따르면 당시 20대의 시추리그 중 단 3대만이 자동전단기능을 수행할 수 있는 시스템을 구비하고 있는 것을 확인할 수 있다.

Valve)를 닫는 기능을 포함하며, LMRP분리를 위해 LMPR연결부를 분리하는 기능과 초크 & 킬 파이프 연결부(Choke & Kill Stab Connector)를 분리하는 기능을 포함한다(West Engineering, 2003). 본 논문에서는 비상분리기능의 일반적인 구성을 따르고, Bureau of Safety and Environmental Enforcement(이하 BSEE)의 내부자료(BP-HZN-MBI00010443)를 참고하여 Fig. 2-5와 같이 비상분리기능의 절차를 구성하였다. BSEE의 내부자료는 TSF Horizon호에서 사용한 비상분리기능의 절차를 포함하고 있으며, 블라인드 전단 램 방지기를 닫는 일반적인 비상분리 절차를 참고하였다.

Start EDS **Command to Pods:** Unlock all functions that were locked by BOP Workstations (CCU)
Command to Pods: Close blind shear ram preventer Close upper inner choke Close upper outer choke Close lower inner choke Close lower outer choke Close upper inner kill Close upper outer kill Close lower inner kill Close lower outer kill
Command to Pods: Vent upper inner choke Vent upper outer choke Vent lower inner choke Vent lower outer choke Vent upper inner kill Vent upper outer kill Vent lower inner kill Vent lower outer kill
Command to Pods: Unlatch choke/kill connector primary Unlatch choke/kill connector secondary
Command to Pods: Vent blind shear ram preventer
Command to Pods: Unlatch LMRP connector primary Unlatch LMRP connector secondary
EDS is complete

Figure 2-5 Emergency Disconnect Sequence

비상분리기능을 구현하기 위해 필요한 시스템은 비상분리시스템(Emergency Disconnect Sequenced System or Emergency Quick Disconnect System, EDS or EQD)으로 명명된다. 비상분리기능의 구성에 따라 시스템의 구성이 달라지기 때문에 앞서 결정한 비상분리기능의 구성에 따라 비상분리시스템을 구성하였다. 비상분리시스템은 해저폭발방지기의 장비 일부와 제어시스템을 공유한다. 따라서 비상분리기능에 구현을 위해 사용되는 해저폭발방지기의 장비 일부와 제어시스템에 대해 분석하고 정리하였다.

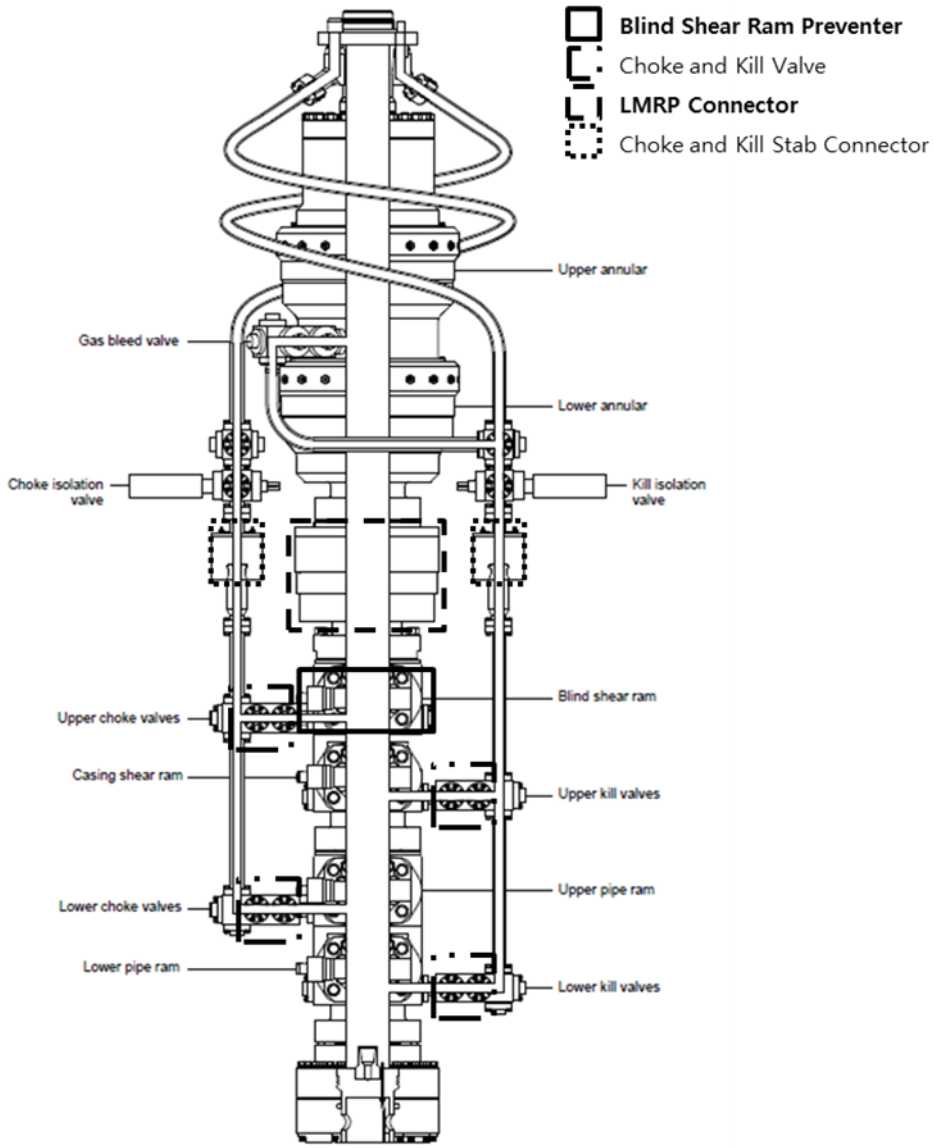

Figure 2-6 Description of Emergency Disconnect System (Based on API, 2012)

먼저 비상분리기능에 필요한 해저폭발방지기의 장비에 대해 살펴보도록 하겠다. 앞서 비상분리기능을 유정폐쇄기능과 LMRP분리기능으로 분류하였고, 유정폐쇄기능은 블라인드 전단 램 방지기를 닫는 기능과 초크 & 킬 밸브를 닫는 기능으로, LMRP분리기능은 LMPR연결부를 분리하는 기능과 초크 & 킬 파이프 연결부를 분리하는 기능으로 구성하였다. 따라서 비상분리기능의 구현을 위해 블라인드 전단 램 방지기, 초크 & 킬 밸브, LMRP연결부, 그리고 초크 & 킬 파이프 연결부를 필요로 한다(Fig. 2-6).

블라인드 전단 램 방지기는 블라인드 램 방지기와 전단 램 방지기의 기능이 복합된 방지기로 시추파이프를 자르고 유정을 폐쇄하기 위해 사용된다. Fig. 2-7은 Transocean사에서 제작한 블라인드 전단 램 방지기에 해당한다. 시추파이프를 자르기 위해 양쪽에 날(Blade)이 위치하는데, 초기에는 양쪽 날 모두 V자 모양을 하고 있었으나 최근에는 Fig. 2-7과 같이 한쪽 날은 일자모양 그리고 다른 한쪽 날은 V자 모양을 하고 있는 경우가 많다. 날을 날카롭게 하여 시추파이프를 자르는 것이 아니라 아래쪽에 위치한 일자모양의 날이 시추파이프를 받쳐주고, 위쪽에 위치한 V자모양의 날이 파이프를 눌러 전단력(Shear Force)으로 시추파이프를 끊어뜨린다(Fig. 2-8). Fig. 2-9와 같이 유압유(Hydraulic Oil)가 셔틀 밸브를 지나(①) Closing Port에 유입되어(②) 피스톤을 가운데로 밀어 블라인드 램 방지기가 시추파이프를 자르고 유정을 폐쇄한다(③). 이후 Wedge Lock 혹은 Multiple Position Lock(이하 MPL)과 같은 장치를 통해 피스톤 위치를 고정시켜 유정을 폐쇄한 상태로 유지한다(④). BSEE에서는 해저폭발방지기의 구성 조건으로 최소 한 개 이상의 블라인드 전단 램 방지기를 구비할 것을 요구하고 있다.

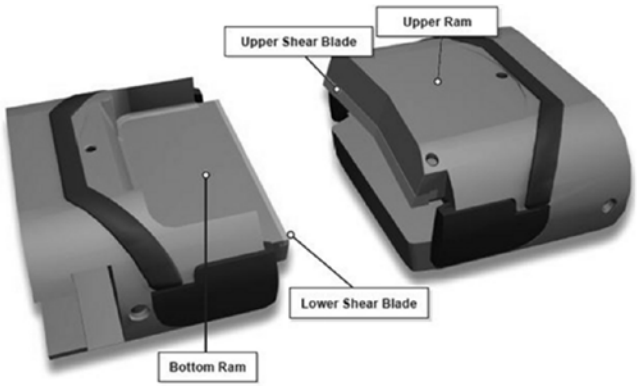

Figure 2-7 Blind Shear Ram Preventer(Transocean, 2011)

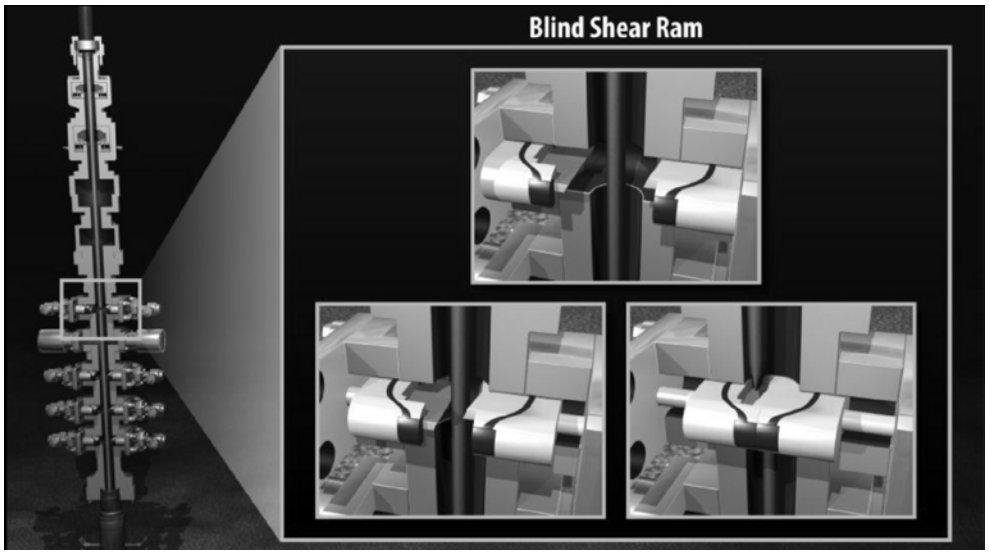

Figure 2-8 Shearing Process by Blind Shear Ram Preventer
(National Commission, 2011)

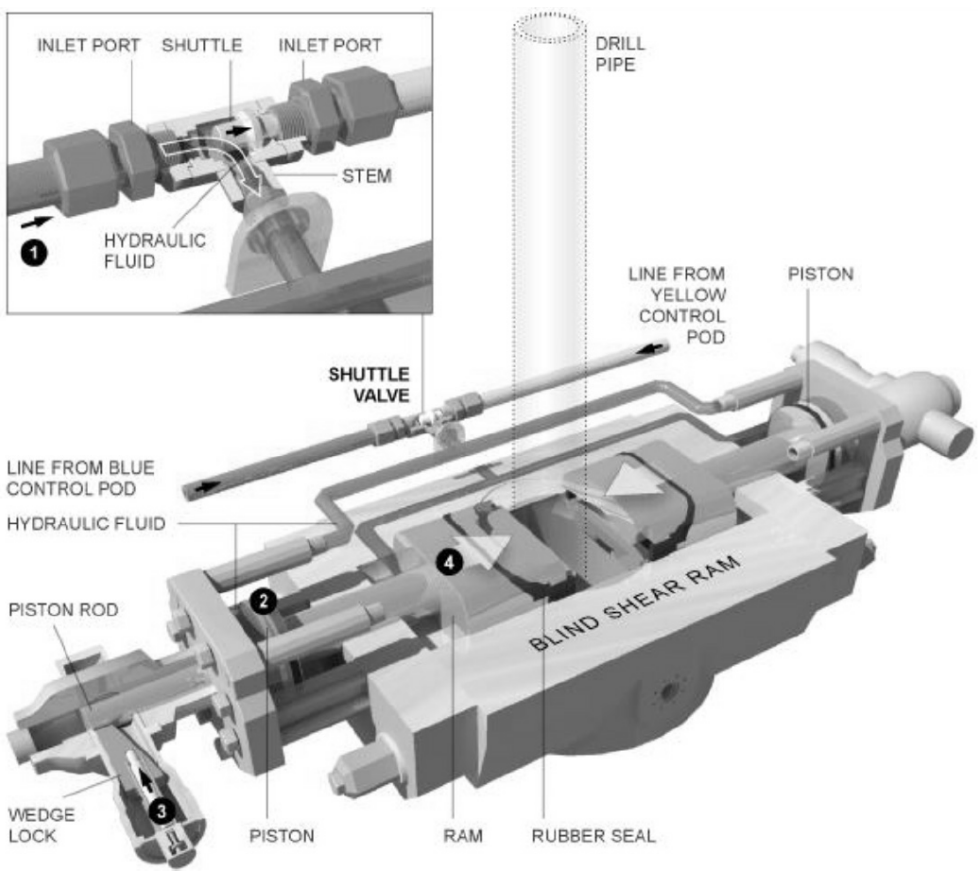

Figure 2-9 Blind Shear Ram Preventer Closing (Januarilham, 2012)

초크 & 킬 밸브는 초크 & 킬 라인(Choke & Kill Line)으로 저류층 유체 혹은 이수를 우회시키기 위해 사용된다. 초크 라인은 시추작업 중 압력의 균형을 잃어 저류층 유체가 유정 내부로 침투하는 현상인 킥(Kick)이 발생하였을 때 저류층 유체를 따로 우회시켜 빼내기 위한 우회로(Bypass)에 해당하고, 킬 라인은 압력의 균형을 맞추기 위해 무거운 이수를 보내기 위한 우회로에 해당한다. 두 라인의 기능은 다르지만 우회로는 초크 라인과 킬 라인의 구분 없이 존재하며, 어떤 기능으로 사용되는지에 따라 그때마다 이름을 붙여 부른다. 일반적으로 초크 & 킬 밸브로는 게이트 밸브(Gate Valve)가 사용되며, 스프링을 통해 고장이 발생할 경우 자동으로 닫힐 수 있는 Fail-close기능이 구비되어있다(Fig. 2-10). 유압유가 Closing 또는 Opening Port에 유입되어 피스톤을 밀어 밸브를 닫거나 개방한다. 일반적으로 안쪽 밸브(Inner Valve)와 바깥쪽 밸브(Outer Valve) 두 개씩 한 쌍으로 사용하며, 주로 4쌍의 초크 & 킬 밸브를 사용한다.

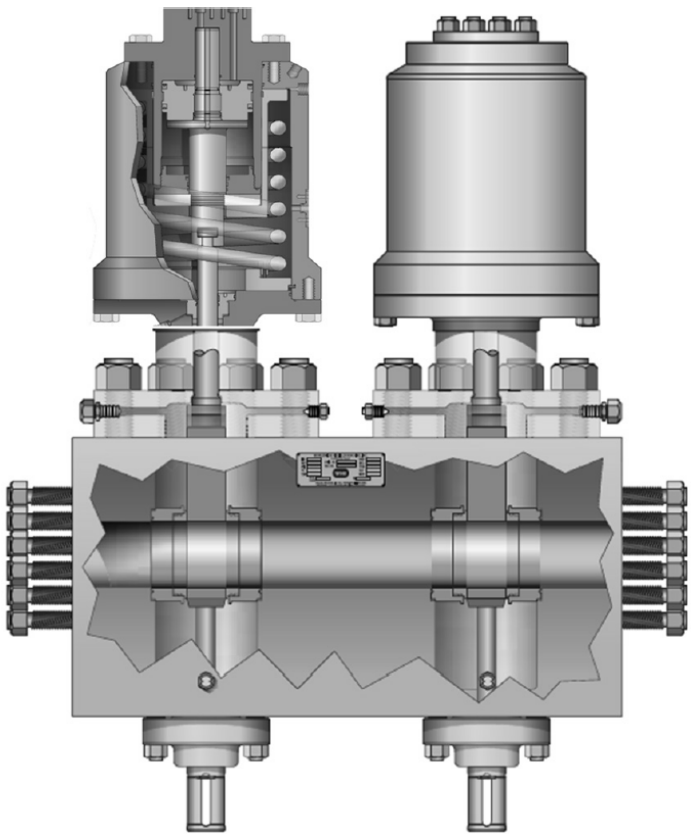

Figure 2-10 Choke & Kill Valve(Magnum, 2012)

LMRP연결부는 LMRP를 Lower BOP Stack에서 분리하기 위해 사용된다. LMRP는 플랫폼의 명령을 전달하여 장비를 제어하기 위한 여러 장비들의 모임으로 Riser Adapter, Flex Joint, Rigid Conduit Manifold, Control Pod, 그리고 Annular Preventer로 구성되어 있다. Lower BOP Stack은 유정헤드 바로 위에 위치하여 실질적인 기능을 수행하기 위한 여러 장비들의 모임으로 각종 램 방지기로 구성되어 있다. LMRP연결부를 통해 LMRP를 Lower BOP Stack으로부터 분리할 경우, Lower BOP Stack은 유정헤드 위에 남아 음파제어(Acoustic Control) 또는 ROV(Remotely Operated Vehicle)를 통한 제어로 유정을 제어할 수 있다. 일반적으로는 Primary Port를 통해 유압유가 유입되어 결속 또는 분리기능을 수행하지만 비상상황에는 Secondary Port를 통해 더 높은 압력의 유압유를 사용하여 빠른 시간 내에 분리될 수 있도록 한다(Fig. 2-11). 하지만 본 논문은 Secondary Port의 사용에 대해서는 고려하지 않았다.

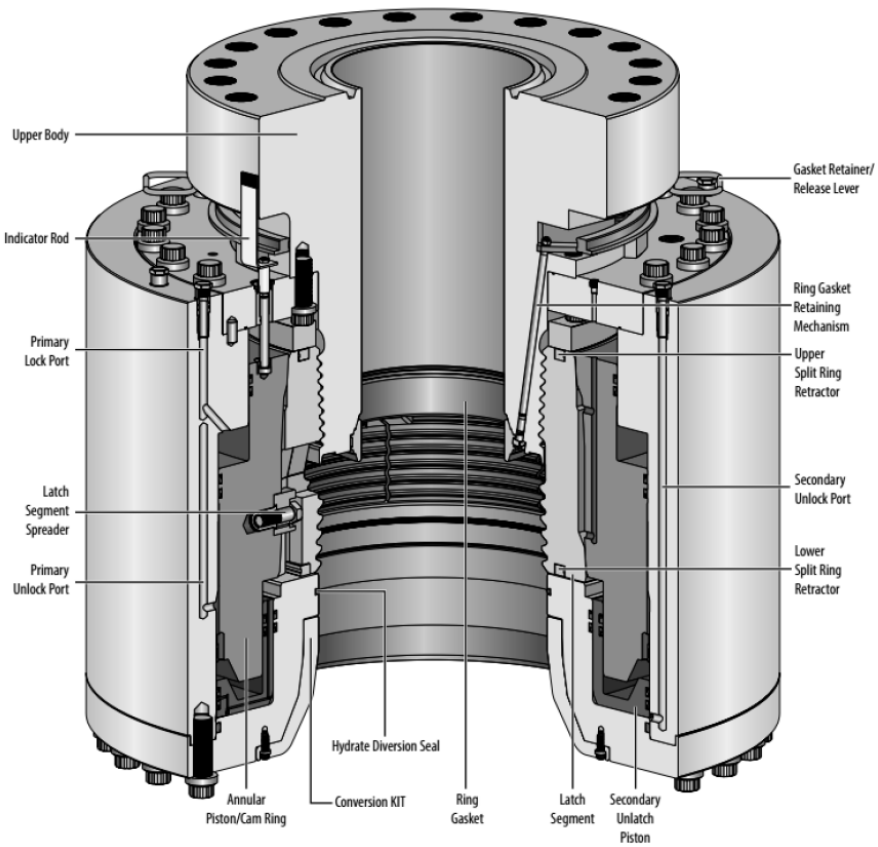

Figure 2-11 LMRP Connector(drill-equip.com)

초크 & 킬 파이프 연결부는 초크 & 킬 라인을 분리하기 위해 사용된다. LMRP분리 당시 초크 & 킬 라인이 연결되어 있을 경우, 초크 & 킬 밸브 부근에 하중이 걸려 밸브 앞의 라인이 파괴될 수 있는 위험이 있다. 따라서 LMRP분리 이전에 반드시 초크 & 킬 파이프 연결부가 분리되어야 하며, 당연히 초크 & 킬 밸브를 닫은 후에 분리가 이루어져야 한다. Actuating Cylinder에 유압유가 유입되어 연결부를 결속하거나 분리한다(Fig. 2-12).

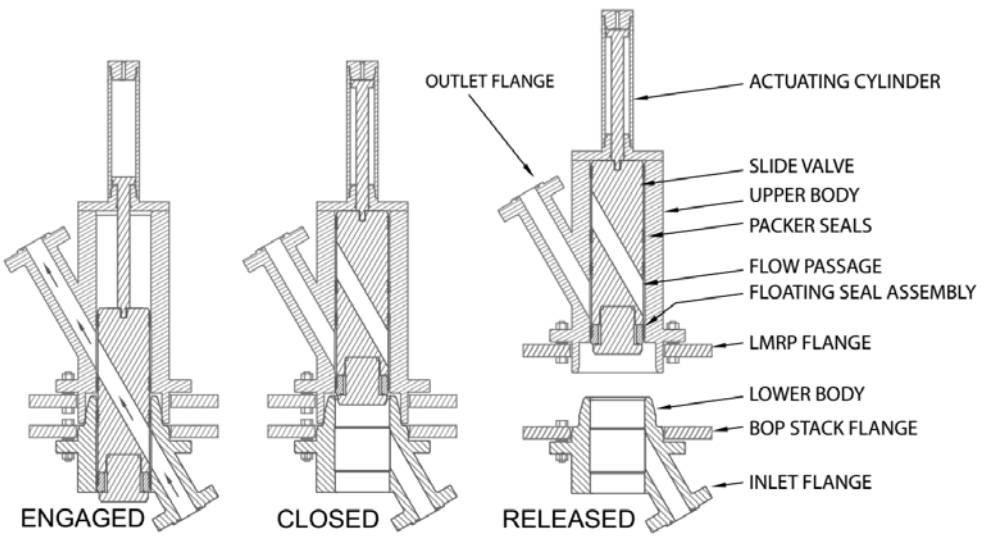

Figure 2-12 Choke & Kill Stab Connector(Radoil.com)

다음으로 비상분리기능 구현을 위해 필요한 해저폭발방지기의 제어시스템에 대해서 살펴보도록 하겠다. 앞서 비상분리기능에 필요한 장비들에 대해서 살펴보았는데, 해당 장비들의 작동하기 위해서는 제어시스템이 필요하다. 특히 Fig. 2-5와 같이 절차에 따라 순차적으로 여러 기능이 구현되어야 하는 비상분리기능의 경우 전자 장치를 이용한 제어가 필요하기 때문에 다중화된 전자식 유압 제어시스템(Multiplexed Electro-Hydraulic Control System, 이하 MUX제어시스템) 또는 전자식 제어시스템(All Electric Control System)을 필요로 한다. 하지만 전자식 제어시스템의 경우 아직 개발단계에 있어 상용화되지 않았기 때문에 MUX제어시스템을 통해 비상분리기능이 구현된다.

일반적인 해저폭발방지기의 MUX제어시스템 구성은 Fig. 2-13와 같다. 작업자가 버튼을 눌러 특정 기능을 작동시키라는 명령을 내리면 Master Control Station에서 Umbilical을 통해 Subsea Electronics

Module(이하 SEM)에 전기 신호를 전달한다. SEM은 전기신호를 해석하여 신호에 따라 해당 기능을 구현하기 위해 필요한 장비의 구동부(Actuator)에 유압유가 유입될 수 있도록 솔레노이드 밸브를 열어 기능을 작동시킨다. 이때, SEM과 솔레노이드 밸브는 기본적으로 플랫폼에 위치한 Electrical Power Unit을 통해 전력을 공급받아 작동하지만 비상시에는 Uninterruptible Power Supply를 통해 전력을 공급받아 작동한다. 유압유는 LMRP 또는 Lower BOP Stack에 위치한 축압기를 통해 공급을 받고, 축압기는 플랫폼에 위치한 Hydraulic Power Unit(이하 HPU)으로부터 유압유를 공급받는다. 즉, 장비가 구동될 당시에는 축압기에 저장된 유압유를 사용하고, 장비가 구동되지 않을 때 플랫폼의 HPU에서부터 유압유 공급받아 축압기를 충전한다. Fig. 2-13에는 각종 센서가 해저에 위치하여 계측값을 SEM에 전달하고, SEM이 MCS로 전기신호를 보내 작업자가 그 값을 확인하는 것으로 시스템이 구성되어 있다. 계측값이 기준값에서부터 많이 벗어날 경우 MCS에서 경고등을 작동시켜 작업자가 위험 상황을 인지하고 대처할 수 있도록 한다.

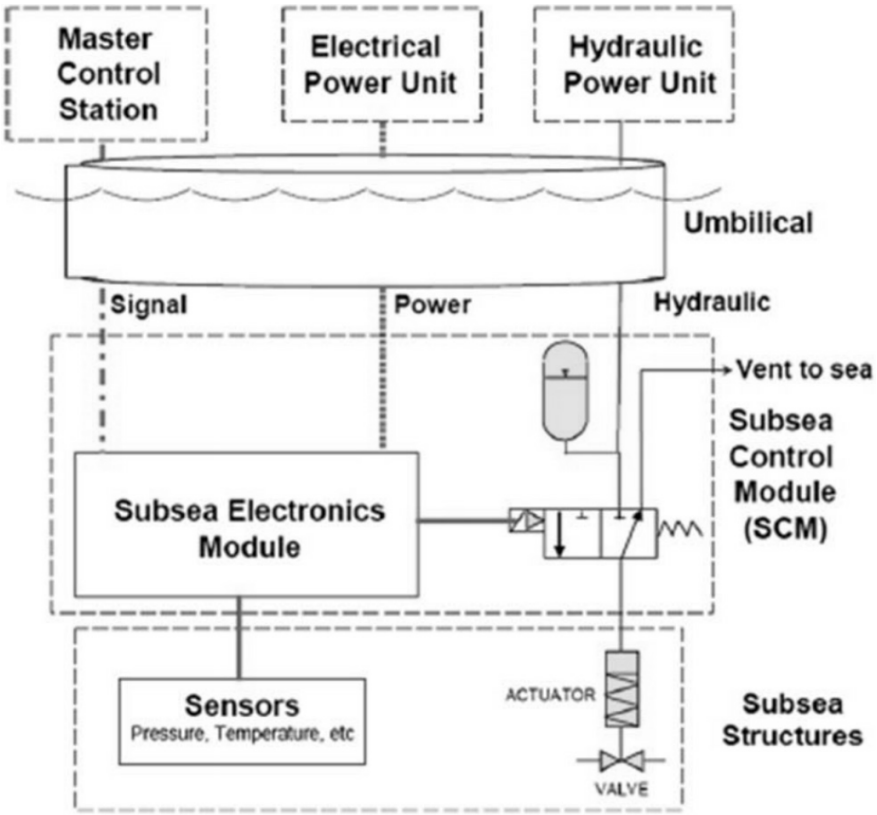

Figure 2-13 Multiplexed Electro-Hydraulic Control System(Bai, 2012)

비상분리기능을 구현하기 위한 MUX제어시스템의 신호 전달 및 처리 체계에 대해 보다 자세히 살펴보면, 비상분리시스템은 조정시스템으로서 대표적인 감독관 수준의 제어시스템(Supervisory Control and Data Acquisition System, 이하 SCADA시스템)에 해당한다. 작업자는 MCS의 Programmable Logic Controller(이하 PLC)에서 수행되는 감독관 수준의 제어(Supervisory Level Control)에 관여하고, SEM과 같이 멀리 떨어진 곳에 위치한 PLC에서 국부적인 제어(Local Level Control)를 담당한다. MUX제어시스템의 신호 전달 및 처리 체계는 Fig. 2-14과 같다. 작업자와 기계와의 인터페이스(Human Machine Interface, 이하 HMI)는 작업자가 시스템의 상태를 확인하고 버튼을 눌러 특정 기능을 작동시킬 수 있는 패널에 해당한다. 시추리그에는 Driller's Panel과 Toolpusher's Panel 두 HMI Station이 존재한다.

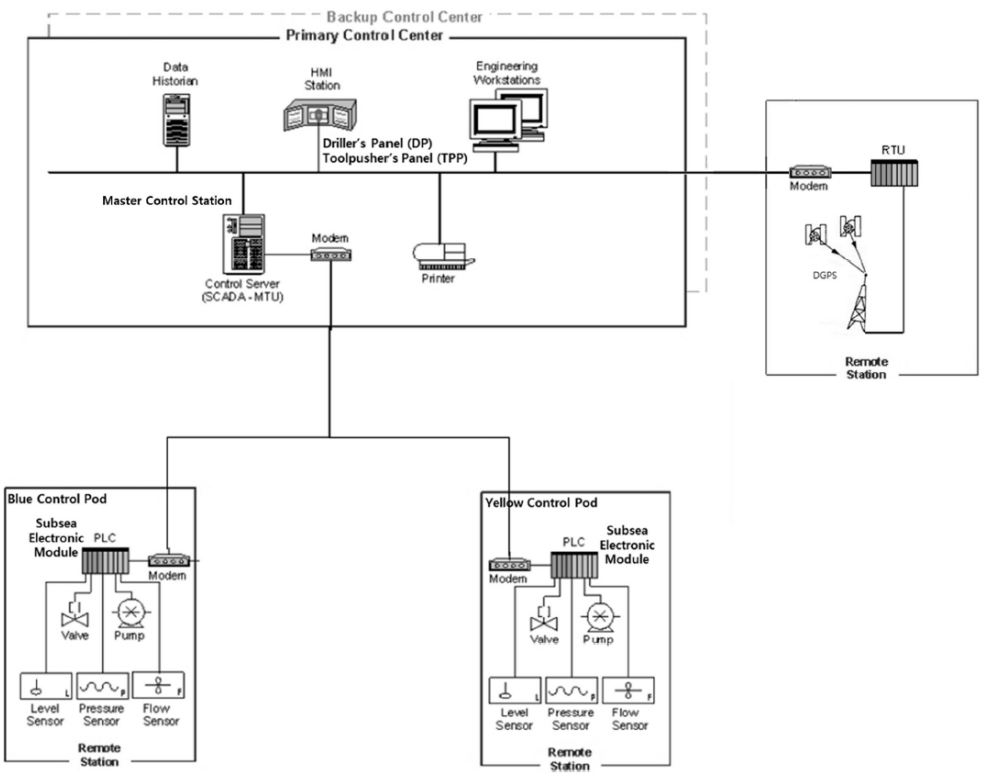

Figure 2-14 SCADA System for Emergency Disconnect

Differential Global Positioning System(이하 DGPS)를 통해 시추리그의 위치를 계측하여 Remote Terminal Unit(RTU)의 PLC에

프로그램화되어 있는 Voting Logic에 따라 계측값을 도출한다. 일반적으로 계측하는 장비의 수가 여러 대이기 때문에 여러 대의 계측 장비에서 계측한 값 중에 대표값을 찾기 위한 Voting Logic을 필요로 한다. Voting Logic으로 결정된 계측값을 바탕으로 비상상황을 판단하고 경우에 따라 경고등을 작동시킨다. 비상분리기능의 경우 DGPS의 계측값을 Watch Circle의 여러 한계선과 비교하여 특정 한계선을 넘어가게 되면 HMI Station에 경고등을 작동시킨다. 비상분리기능에 대해 각 PLC에 프로그램화되어 있는 제어논리를 Fig. 2-15에 나타내었다.

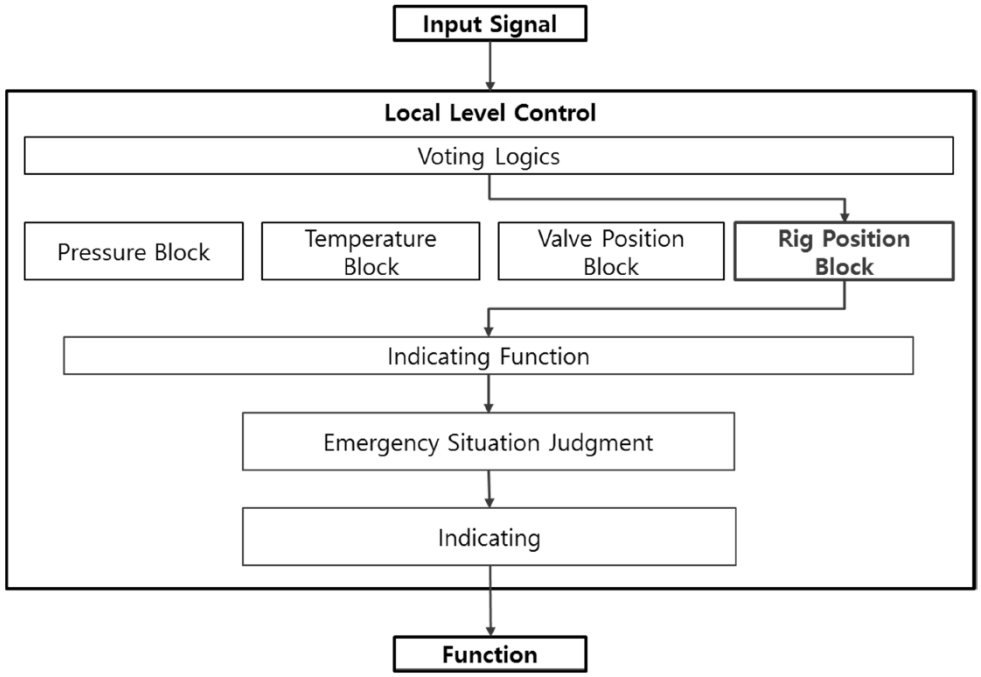

Figure 2-15 Control Logic for Measuring Drilling Rig's Position

HMI Station에 경고등이 울리면 작업자는 버튼을 눌러 필요한 기능을 작동시킨다. MCS의 PLC에 프로그램화되어 있는 제어논리에 따라 작업자가 누른 버튼에 해당하는 기능을 작동시키는 전기신호를 출력한다. 전기신호는 SEM의 PLC에 전달되어 절차에 따라 세부적인 기능을 수행하기 위해 필요한 장비들을 작동시킨다. 비상분리기능의 경우 작업자가 버튼을 누르면 비상분리기능을 수행하라는 전기신호가 전달되어 SEM의 PLC에서 블라인드 전단 램 방지기 닫기, 초크 & 킬 밸브 닫기, LMRP분리, 그리고 초크 & 킬 파이프 분리의 기능을

수행하기 위해 필요한 장치들을 순차적으로 작동시킨다. 비상분리기능에 대해 각 PLC에 프로그램화되어 있는 제어논리를 Fig. 2-16에 나타내었다.

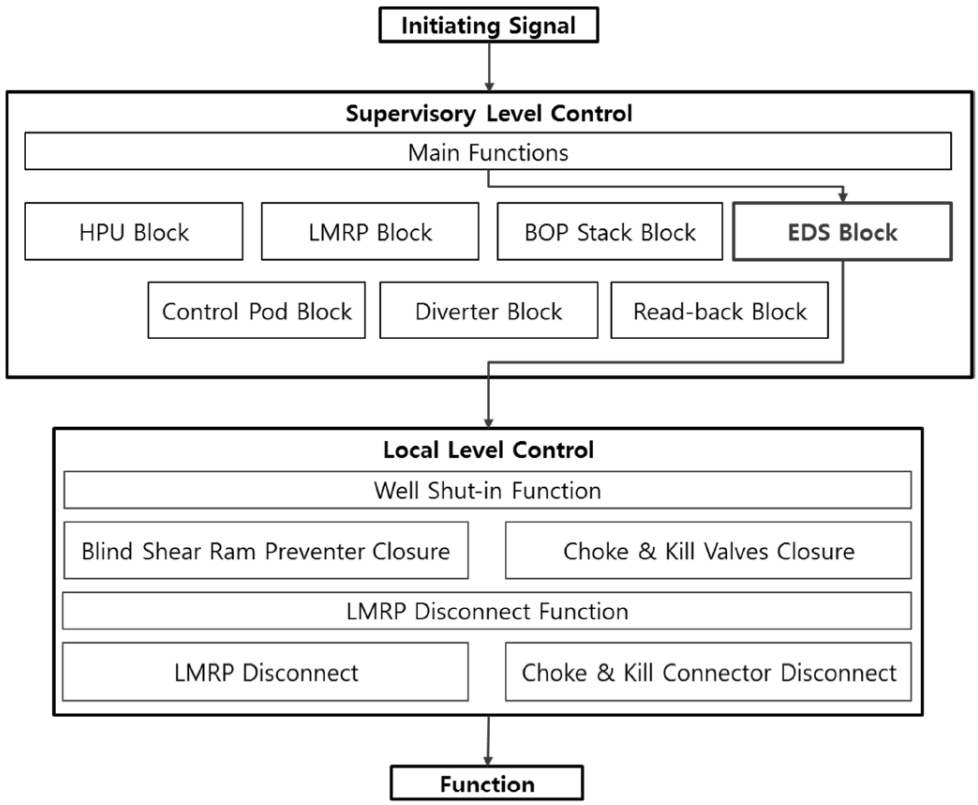

Figure 2-16 Control Logic for Initiating Emergency Disconnect Function

이상으로 비상분리기능을 정의하고 기능을 구현하기 위해 필요한 비상분리시스템에 대해서 살펴보았다. 비상분리기능은 라이저와 유정헤드의 안전을 보장하기 위한 최종 단계의 방호기능에 해당한다. 본 논문에서는 비상분리기능의 유정폐쇄기능은 블라인드 전단 램 방지기를 닫는 기능과 초크 & 킬 밸브를 닫는 기능으로, LMRP분리기능은 LMPR연결부를 분리하는 기능과 초크 & 킬 파이프 연결부를 분리하는 기능으로 구성하였다. 이후 정의된 비상분리기능의 구현을 위해 필요한 장비들과 제어시스템에 대해서 살펴보았다. 비상분리시스템은 작업자를 필요로 하는 조정시스템으로서 SCADA시스템에 해당한다. 따라서 SCADA시스템으로서의 구성과 제어논리에 대해 살펴보았다.

제 3 장 안전무결성 요구사항 분석 및 검증

2004년 노르웨이의 석유협회인 OLF는 석유산업에서 사용하는 안전관련시스템의 관리를 위해 IEC에서 제시한 지침을 적용하였다. 하지만 석유산업에서 사용되는 대다수의 안전기능은 조정시스템에 의해 구현되기 때문에 안전계장시스템을 대상으로 확립된 IEC의 지침을 적용하기에 어려움이 있었다. 안전계장시스템은 위험 상황을 감지하고 그에 필요한 안전기능을 Logic Solver가 자동으로 작동시키는 반면, 조정시스템은 위험 상황을 감지하면 경고등을 켜서 작업자가 이를 인지하게 하고, 작업자가 버튼을 눌러 필요한 안전기능을 작동시키는 명령을 내려 기능이 구현된다. 이에 OLF는 작업자를 배제시키기 위해 조정시스템으로 구현되는 안전기능을 버튼이 눌러져 안전기능이 구현되는 기능을 수동작동기능으로 정의하였다. 수동작동기능 개념을 통해 조정시스템으로 구현되는 안전기능을 안전계장시스템에 의해 구현되는 것으로 간주할 수 있었고, 이에 IEC의 지침을 적용하였다. 하지만 안전기능은 특정 위험 사건에 대해 인지하여 제어되고 있는 장치를 안전한 상태로 되돌리고 유지하는 기능으로 정의(IEC, 1998)되기 때문에 수동작동기능만을 단독으로 안전기능으로 정의할 수 없다.

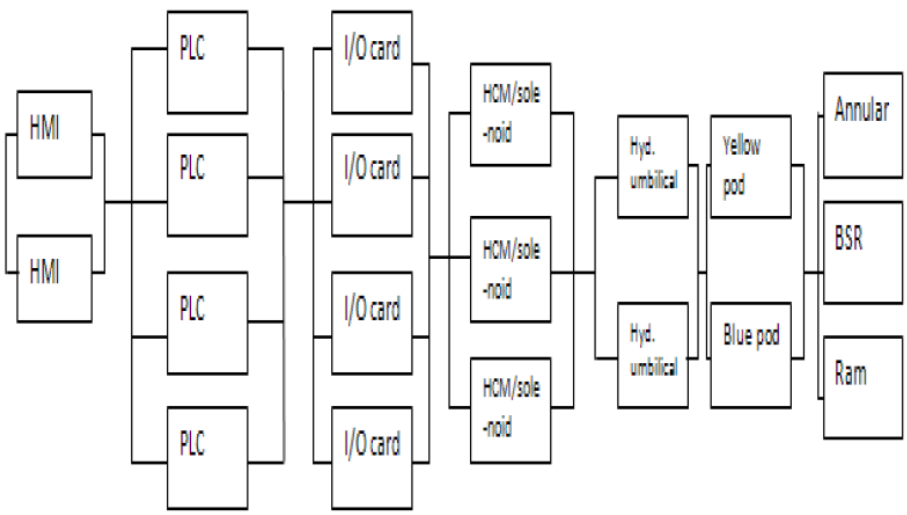

Figure 3-1 Reliability Block Diagram of BOP Control System (Eikeskog, 2012)

Eikeskog(2012)는 해저폭발방지기의 기능을 안전계장시스템으로 구현되는 기능으로 정의하는 OLF의 접근 방안에 대해 의문을 제시하면서도 수동작동기능 개념을 적용하여 연구를 수행하였다. Fig. 3-1은 해저폭발방지기 제어시스템의 신뢰성블록선도로, 작업자가 버튼을 누를 수 있는 HMI에서부터 기능을 수행하기 위해 필요한 장비까지만을 대상으로 하는 것을 확인할 수 있다. 앞서 언급한 바와 같이 안전기능은 위험 상황을 인지하고 필요한 기능을 작동시켜 시스템을 안전한 상태로 유지시키기 위한 기능으로 정의되기 때문에 Fig. 3-2의 왼쪽 그림과 같이 센서로 현재 상황을 파악하고 작업자에게 위험상황을 알려 작업자가 기능을 작동시키는 명령을 내려 기능이 구현되는 것까지가 안전기능의 제어루프에 해당한다. 이에 반해 OLF의 수동작동기능 개념은 Fig. 3-2의 오른쪽 그림과 같이 작업자가 기능을 작동시키는 것만을 고려하기 때문에 실제 제어루프의 일부만을 다룰 수 밖에 없어 보수적이지 못한 결과를 도출할 수 있다. 실제로 Eikeskog의 연구 결과 해저폭발방지기 제어시스템의 안전무결성 수준이 Safety Integrity Level(이하 SIL) 2에 해당하여 요구되는 수준인 SIL 2를 만족시켰으나, 센서부터 위험 상황을 알리기 위한 장비까지 고려한다면 SIL 2를 보장할 수 없다.

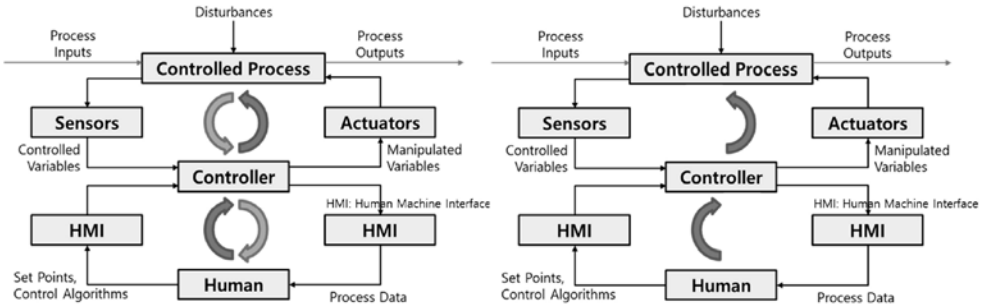

Figure 3-2 Control Loop for Operator Intervention System(Left) and Control Loop for Manual Initiator Function Concept(Right)

본 논문은 기존 OLF의 접근 방안의 이러한 문제점에 착안하여, 위험상황을 인지하고 기능을 수행하기까지의 실제 제어루프를 고려하였다. 다만 작업자에 대해서는 고려하기 어렵기 때문에 작업자에 대한 고려는 배제하였다. 안전계장시스템에서는 위험상황을 인지하는 서브시스템을 Input Subsystem으로, 위험상황을 판단하여 기능을 작동시키는 서브시스템을 Logic Solver Subsystem으로, 그리고 기능을

구동하는 서브시스템을 Output Subsystem으로 명명하고 일반적으로 각각에 대해 전체 안전무결성의 35%-15%-50%를 할당한다(Hoekstra, 2005). 아직 조정시스템, 특히 SCADA시스템에 대해서는 데이터베이스가 구축이 되지 않아 이러한 비율을 찾기가 어렵기 때문에 우선적으로 본 논문에서는 안전계장시스템의 비율을 차용하였고, 해당 비율에 따라 각 서브시스템에 요구되는 안전무결성 수준을 파악하였다. 이를 통해 위험상황을 인지하고 경고등을 작동시키는 경고기능과 위험상황을 판단하고 기능을 작동시키는 작업자의 기능, 그리고 기능을 구동시키는 수동작동기능 각각에 요구되는 안전무결성 수준을 파악할 수 있었다. 작업자의 기능에 대해서는 많은 연구가 수행되고 있다. 가령 작업자가 경고등 표시를 착각할 확률, 의도와 달리 다른 버튼을 누를 확률, 판단 실수를 할 확률 등 데이터베이스를 구축하고자 하는 노력이 이루어지고 있지만 작업자의 능력에 따라 그리고 그날 그날의 컨디션에 따라 변화의 폭이 크기 때문에 이러한 방식으로 작업자에 대해 고려하는 것은 매우 어려운 문제에 해당한다. 35%-15%-50%의 비율로 작업자의 기능에 요구되는 안전무결성 수준을 파악할 수 있고 작업자에 대한 데이터베이스를 통해 검증을 수행할 수 있을 것이라고도 생각이 되지만, 요구되는 수준에 따라 작업자의 능력 또는 경력, 작업자의 수 등을 결정하는 것이 보다 현실적인 방안이 될 수 있을 것이라 생각한다. 본 논문에서는 요구되는 안전무결성의 15%에 해당하는 작업자의 기능에 대한 고려를 배제하였으며, 이후 더 이상 작업자의 기능과 관련된 내용은 없음을 것임을 밝히는 바이다.

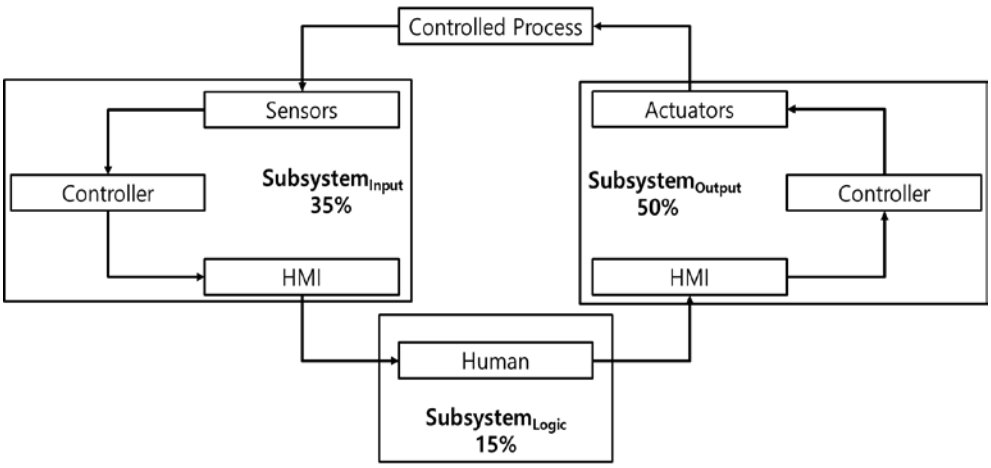

Figure 3-3 Subsystems and Required Percentage of Safety Integrity

제 1 절 안전무결성 요구사항 분석

안전무결성은 안전관련시스템이 주어진 시간 및 조건 하에 요구되는 안전기능을 성공적으로 수행할 수 있는 능력으로 정의되지만(IEC, 1998), 실제로는 안전기능 수행에 실패할 확률로 결정된다. 즉, 특정 안전기능이 90%의 확률로 성공적으로 기능을 수행할 수 있음을 보여주는 것이 아니라 10%의 확률로 기능 수행에 실패한다는 것을 보여준다. 실패 확률은 안전기능의 요구 빈도에 따라 Probability of Failure per Hour(이하 PFH) 또는 Probability of Failure on Demand(이하 PFD)로 나타낸다. 특정 안전기능의 요구 빈도가 지속적이거나 1년에 1번 이상일 경우 이러한 기능은 지속적 혹은 높은 요구 빈도의 기능(Continuous Demand Mode/ High Demand Mode Function)으로 분류되고, PFH로 실패 확률을 나타낸다. 이는 단위시간 동안 기능 수행에 실패할 확률을 의미하며 단위는 [1/hour]에 해당한다. 요구 빈도가 1년에 1번 보다 미만일 경우 이러한 기능은 낮은 요구 빈도의 기능(Low Demand Mode)로 분류되고, PFD로 실패 확률을 나타낸다. 이는 요구가 있을 때 기능 수행에 실패할 확률을 의미하며 단위는 없다. 하지만 요구가 있을 때의 확률을 의미한다는 뜻으로 [1/demand]로 단위를 표시하는 경우도 있다. 일반적으로 PFH와 PFD 모두 매우 작은 숫자에 해당한다. 따라서 PFH 또는 PFD로 특정 수치를 제시하더라도 너무 작은 값이기에 그 수치에 대한 감이 없는 경우가 많다. 따라서 IEC(1999)에서는 실패 확률을 수준 1부터 4까지로 분류하는 안전무결성레벨(SIL)을 제시하였고(Table 3-1), 대다수의 경우 SIL을 통해 안전무결성 수준을 나타낸다.

Table 3-1 SIL Table (IEC, 1999)

SIL	PFH [1/hour]	PFD
1	$10^{-6} \leq PFH \leq 10^{-5}$	$10^{-2} \leq PFD \leq 10^{-1}$
2	$10^{-7} \leq PFH \leq 10^{-6}$	$10^{-3} \leq PFD \leq 10^{-2}$
3	$10^{-8} \leq PFH \leq 10^{-7}$	$10^{-4} \leq PFD \leq 10^{-3}$
4	$10^{-9} \leq PFH \leq 10^{-8}$	$10^{-5} \leq PFD \leq 10^{-4}$

비상분리기능은 IMO기준으로 동적 위치제어시스템의 등급이 3인 시추리그에 대해 1년에 1번 이상 요구되어 높은 요구 빈도의 안전기능에 해당한다(OLF, 2004). 따라서 기능 수행에 실패할 확률은 PFH로 계산한다. OLF는 비상분리기능에 대해 허용 가능한 위험도 수준을 파악하여 요구되는 안전무결성을 직접 계산해볼 것을 권고하면서도 최소 SIL 2 이상의 안전무결성을 요구하였고, 해당 요구사항은 구체적인 계산의 결과가 아닌 그 동안의 데이터베이스를 바탕으로 추측한 것이라고 것을 밝혔다. 본 논문에서는 근거가 함께 제시되지 않은 OLF의 요구사항에 따르지 않고, 허용 가능한 위험도 수준을 파악하여 비상분리기능에 요구되는 안전무결성 수준을 직접 계산하였다. 허용 가능한 위험도 수준은 특정 수치로 일정하게 정해져 있는 것이 아니라 국가마다 기준이 다르기 때문에 정하는 것이 어렵다. 본 논문은 SINTEF에서 탄화수소 누출과 관련하여 제시한 허용 가능 위험도 수준을 기준으로 삼았다. 라이저와 유정헤드의 파괴에 따른 탄화수소 유출은 Significant Harm에 해당한다고 가정하였다. 앞서 언급한 바와 같이 저류층까지 시추가 진행된 경우에만 탄화수소 유출이 발생하기 때문에 중간 정도의 수준이라고 판단하였다. 이때 허용 가능한 사고 빈도는 10^{-3}으로 1,000년에 한 번 정도 라이저와 유정헤드가 파괴가 발생할 수 있는 수준을 기준으로 삼았다.

Consequence class	Released volume of oil to sea	Acceptable annual frequency
Minor harm	< 10 m^3	10^{-1}
Moderate harm	10–100 m^3	10^{-2}
Significant harm	100–1000 m^3	10^{-3}
Serious harm	1000–10 000 m^3	10^{-4}
Major/Catastrophic harm	> 10 000 m^3	10^{-5}

Figure 3-4 Environmental Risk Acceptance Criteria Related to Released Volumes of Oil to Sea(SINTEF, 2011)

제 2절에서 살펴본 것과 같이 라이저와 유정헤드의 파괴로 인한 탄화수소 유출의 Initiating Event는 Loss of Position에 해당한다. Loss of Position은 시추리그가 Yellow Limit을 벗어나는 사건으로 정의되며 해당 사건은 1년에 평균 1.25번 발생한다(Bakken, 2001). Yellow Limit을 벗어날 경우에는 Critical Loss of Position을 방지하기

위해 시추작업을 중단하고 동적 위치제어시스템을 통해 위치제어기능을 수행한다. 즉, 동적 위치제어시스템을 통해 탄화수소 유출을 방지하여 위험도를 저감시킨다. 동적 위치제어시스템의 고장확률은 3.27E-05/hour에 해당하여(Ebrahimi, 2010), Loss of Position이 발생하였을 때 동적 위치제어시스템이 기능을 수행하지 못하는 빈도를 계산하면 1년에 0.36번에 해당한다. 이를 허용 가능한 위험도 수준으로 저감시키기 위해 비상분리기능을 필요로 하고, 허용 가능한 위험도 수준과 앞서 계산한 Loss of Position이 발생하였을 때 동적 위치제어시스템이 기능을 수행하지 못하는 빈도를 비교하여 비상분리시스템에 요구되는 안전무결성을 계산하였다. 계산식과 계산 결과를 수식 (3-1)과 (3-2)에 나타냈다. 계산 결과에 따르면, 비상분리시스템에 요구되는 고장확률은 3.19E-07/hour로, SIL 2 수준에 해당하였다. 해당 결과는 OLF에서 요구한 SIL 2와 동일하다는 것을 보여주지만, 구체적인 수치를 제시할 수 있어 비상분리기능의 안전무결성에 대해 정량적으로 접근이 가능하다. Loss of Position으로 인한 탄화수소 유출과 관련하여 위험도 저감 방안과 저감 방안을 통해 허용 가능한 위험도 수준을 달성하는 전략을 Fig. 3-5에 정리하였다. 이후 검증을 통해 비상분리시스템이 기능 수행에 실패할 확률을 계산하여, 비상분리시스템으로 위험도가 저감되어 허용 가능한 위험도를 달성할 수 있는지를 확인하였다.

$$(1.25 \times 1) \times (3.27 \times 10^{-5} \times 8{,}760) \times (PFH_{EDS} \times 8{,}760) = 1 \times 10^{-3} \times 1 \quad (3-1)$$

$$\therefore PFH_{EDS} = 3.19 \times 10^{-7}/hour \quad (3-2)$$

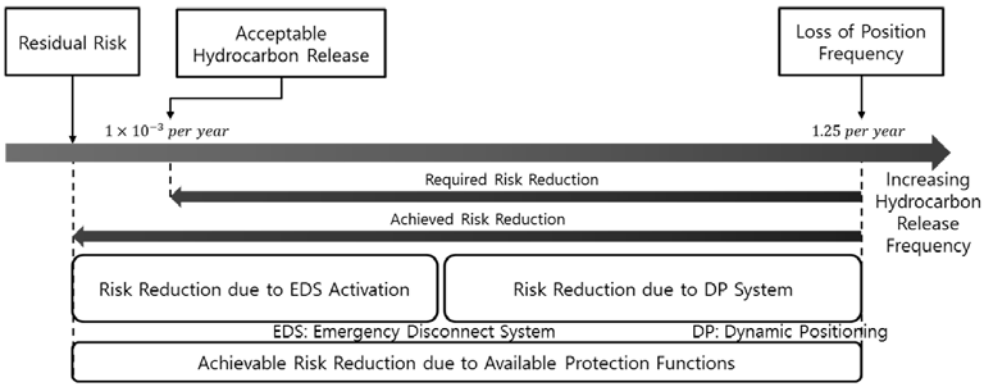

Figure 3-5 Risk Reduction Scheme for Hydrocarbon Release to Sea Initiated by Loss of Position

비상분리기능에 요구되는 안전무결성은 PFH 3.19E-07/hour에 해당한다. 이는 비상분리시스템에 할당되어 비상분리시스템이 기능 수행에 실패할 확률에 해당한다. 비상분리시스템을 세 서브시스템으로 나눠 각 서브시스템에 35%-15%-50%의 비율로 안전무결성 요구사항을 할당하고, 작업자에 해당하는 15%, 즉 PFH 4.79E-08/hour를 배제하였다. 작업자를 배제한 비상분리시스템에는 PFH 2.71E-07/hour의 안전무결성 요구사항이 할당되어 Input Subsystem은 PFH 1.12E-07/hour 그리고 Output Subsystem은 PFH 1.60E-07/hour의 안전무결성 요구사항이 할당되었다(Fig. 3-6).

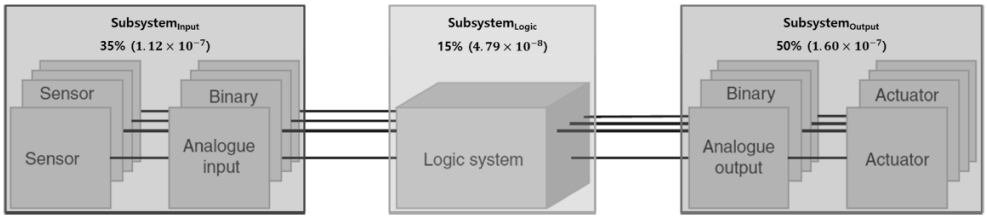

Figure 3-6 Required Safety Integrity for Subsystems
(Based on Pepperl-Fuchs, 2001)

제 2 절 안전무결성 요구사항을 고려한 시스템 구성

IEC(1999)는 안전관련시스템의 구조적 강건성(Structural Robustness)를 고려하여 시스템을 구성하는 방안을 제시하였다. 강건성은 시스템의 구성 요소 중 일부에 고장이 발생하더라도 기능을 수행할 수 있는 능력으로 정의되는데, 이는 시스템의 구성에 의해 결정되기 때문에 구조적 강건성으로 명명하였다. 즉, 구조적 강건성을 고려한다는 것은 시스템의 구성 요소 중 일부에 고장이 발생하더라도 기능 수행에 문제가 발생하지 않도록 시스템을 구성하는 것을 의미한다. IEC에서는 이와 관련하여 Hardware Fault Tolerance(이하 HFT)라는 개념을 도입하였다. HFT는 기능 수행에 문제가 발생하지 않는 범위에서 고장이 발생하여도 괜찮은 구성 요소의 수로 정의된다. 예를 들어 엔진을 3대 가지고 있는 선박이 엔진 2대만으로 운영이 가능하다고 한다면 HFT는 1에 해당하여, 한 개의 엔진에 고장이 발생하더라도 기능 수행에 문제가 없다. HFT라는 개념을 도입함으로써 구조적 강건성은 HFT를 결정하는 문제로 생각할 수 있게 되었고, IEC(1999)에서는 서브시스템의 안전무결성 요구사항에 따라 최소

HFT를 결정할 수 있는 표를 제시하였다(Fig. 3-7과 Fig. 3-8). HFT를 결정하기 위해서는 서브시스템의 유형, Safe Failure Fraction(이하 SFF), 그리고 SIL을 필요로 한다. 서브시스템의 유형은 A와 B로 크게 두 가지로 분류된다. 비교적 단순한 구조를 가지고 있어 서브시스템의 고장 상태 및 고장 원인에 대해 명확히 규명되어 있는 경우에는 A로 분류되고, 구조가 복잡하여 고장 상태와 고장 원인이 명확하게 규명되지 않은 경우에는 B로 분류된다. 일반적으로 Input과 Output Subsystem은 A유형으로 분류되고 Logic Subsystem은 B유형으로 분류된다. SFF는 고장률 중 제어되고 있는 장치의 안전에 큰 영향이 없는 고장률의 비로 정의된다. SFF는 수식 (3-3)으로 계산할 수 있으며, 데이터베이스에 각 부품마다의 고장률이 존재하기 때문에 각 부품마다 SFF 값을 가지고 있다. SIL은 해당 부품에 요구되는 안전무결성레벨에 해당한다. 만약 A유형의 서브시스템에 해당하고, SFF가 75%일 때 SIL 3가 요구된다면 해당 부품의 Fig. 3-7에 따라 최소 HFT를 1로 결정할 수 있다. 최소 HFT이기 때문에 HFT를 1 이상으로 시스템을 구성할 수 있다. 본 논문에서는 각 서브시스템에 대해 IEC에서 제시한 방법에 따라 최소 HFT를 결정하여 구조적 강건성을 보장할 수 있게 시스템을 구성하였다.

$$SFF = \frac{(\lambda_S + \lambda_{DD})}{(\lambda_S + \lambda_D)} \times 100 \qquad (3-3)$$

Safe failure fraction (SFF)	Hardware fault tolerance (HFT)		
	0	1	2
< 60 %	SIL1	SIL2	SIL3
60 % ... 90 %	SIL2	SIL3	SIL4
90 % ... 99 %	SIL3	SIL4	SIL4
> 99 %	SIL3	SIL4	SIL4

Figure 3-7 Architectural Constraints on Type A Safety Related Subsystems(IEC, 1999)

Safe failure fraction (SFF)	Hardware fault tolerance (HFT)		
	0	1	2
< 60 %	not allowed	SIL1	SIL2
60 % ... 90 %	SIL1	SIL2	SIL3
90 % ... 99 %	SIL2	SIL3	SIL4
> 99 %	SIL3	SIL4	SIL4

Figure 3-8 Architectural Constraints on Type B Safety Related Subsystems(IEC, 1999)

구조적 강건성을 고려하여 시스템을 구성하기 이전에 비상분리시스템의 기능블록선도를 작성하였다. 기능블록선도는 한 개의 부품이 수행하는 기능을 한 개의 블록을 단위로 하여, 시스템이 기능 수행을 위해 어떠한 부품을 필요로 하는지 분석하기 위해 작성되었다. 비상분리시스템의 기능블록선도는 Fig. 3-9와 같다. DGPS를 통해 위치정보를 받아오면 Analog Input으로 아날로그 데이터를 디지털 데이터로 변환하여 PLC로 전달한다. PLC에서는 Fig. 2-15의 제어논리에 따라 계측값 중 대표값을 결정하고, 일반적인 상황인지 비상상황인지에 대해 판단하여 비상상황에 해당하면 경고등을 작동시키라는 명령을 내린다. 디지털 데이터로 명령이 출력되어 Indicator를 작동시킨다. 이후 작업자가 상황을 판단하여 필요한 기능을 작동시키기 위해 버튼을 누른다. Analog Input으로 아날로그 데이터를 디지털 데이터로 변환하여 Supervisory Level PLC로 전달한다. Supervisory Level PLC와 SEM Fig. 2-16의 제어논리에 따라 비상분리기능과 관련된 장비의 작동을 위해 솔레노이드 밸브를 작동시킨다.

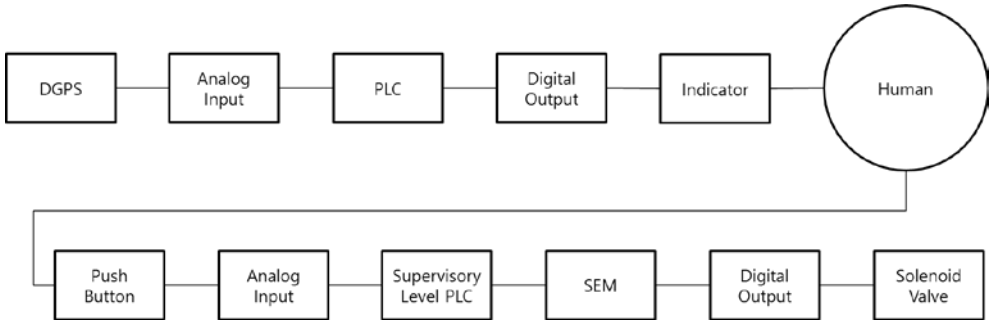

Figure 3-9 Functional Block Diagram for Emergency Disconnect System

먼저 Input Subsystem에 해당하는 DGPS-Analog Input-PLC-Digital Output-Indicator에 대해 구조적 강건성을 고려하여 Redundancy를 결정하였다. Input Subsystem을 또 다시 Input Subsystem, Output Subsystem, 그리고 Output Subsystem으로 분류하고 안전무결성의 35%-15%-50% 비율로 각각에 할당하여 각 서브시스템에 요구되는 안전무결성을 파악할 수 있었다(Fig. 3-10). 이후 PDS Handbook을 통해 Analog Input, PLC, Digital Output의 SFF를 파악하였고, IEC 60947-5-4를 통해 Indicator의 SFF를

파악할 수 있었다. 하지만 DGPS에 대해서는 관련 정보를 찾아볼 수 없었기 때문에 고장률을 가정하여 SFF를 계산할 수 있었다. 이후 Fig. 3-7과 Fig. 3-8을 통해 각 구성 요소마다 최소 HFT를 결정하였고 이를 바탕으로 k-out-of-n(이후 koon) [④] 을 결정하였다. 각 구성 요소의 정보, 최소 HFT, 그리고 koon을 결정하여 Fig. 3-11에 정리하였다. 그 결과 DGPS-Analog Input은 최소 HFT가 0으로 여분의 장비를 필요로 하지 않는 것을 확인하였고, PLC는 최소 HFT가 1로 여분의 장비 한 개를 필요로 하는 것을 확인하였다. 그리고 Digital Output-Indicator는 최소 HFT가 0으로 여분의 장비를 필요로 하지 않는 것을 확인하였다. 이에 따라 각각의 koon을 1oo1, 1oo2, 그리고 1oo1으로 결정하였다. PLC는 1oo2로 구성되어야 하므로 2개로 구성되어야 하며, 그 중 한 개만 정상적으로 기능을 수행하면 Logic Subsystem의 기능이 수행되는 것을 의미한다. 이에 DGPS-Analog Input-PLC-Digital Output-Indicator의 블록선도가 Fig. 3-12와 같이 작성된다.

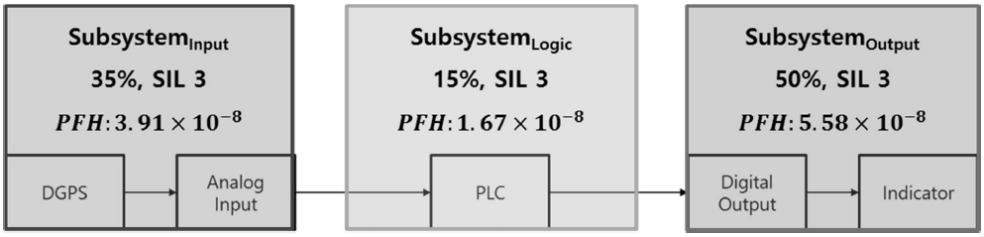

Figure 3-10 Safety Integrity Requirements of Emergency Disconnect System from DGPS to Indicator

	Component	Type	λ_D ($\times 10^{-6}$)	λ_{DU} ($\times 10^{-6}$)	λ_S ($\times 10^{-6}$)	SFF	HFT	koon
Subsystem Input	DGPS	A	10.00	1.000	10.00	95%	0	1oo1
	Analog Input	A	1.600	0.160	1.600			
Subsystem Logic	PLC	B	4.800	0.480	4.800	95%	1	1oo2
Subsystem Output	Digital Output	A	1.600	0.160	0.160	94%	0	1oo1
	Indicator	A	0.100	0.050	0.025			

Figure 3-11 Reliability Data for Emergency Disconnect System from DGPS to Indicator Data from PDS Handbook and IEC 60947-5-4)

[④] k-out-of-n System 또는 k-out-of-n Voted System이라고 불린다. 이는 일반적으로 n개의 구성 요소 중 k개만 기능을 수행하면 시스템의 기능이 수행되는 구조를 의미한다. 보다 명확하게 표현하기 위해서는 koon:G라고 표현하며, koon:F의 경우는 n개의 구성 요소 중 k개가 기능 수행에 실패하면 시스템이 기능 수행에 실패하는 구조를 의미한다.

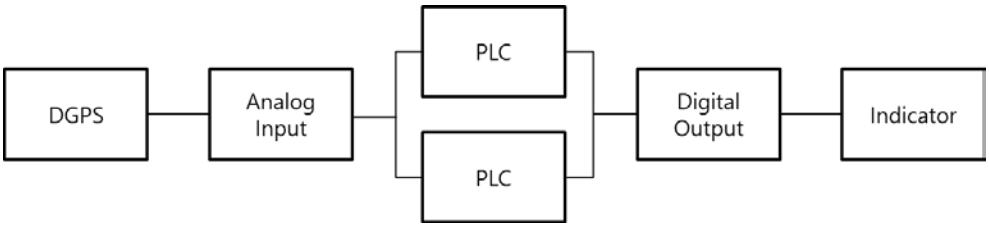

Figure 3-12 Block Diagram of Emergency Disconnect System from DGPS to Indicator

이후 Output Subsystem에 해당하는 Push Button-Analog Input-Supervisory Level PLC—SEM-Digital Output-Solenoid Valve에 대해 구조적 강건성을 고려하여 Redundancy를 결정하였다. Output Subsystem을 또 다시 Input Subsystem, Output Subsystem, 그리고 Output Subsystem으로 분류하고 안전무결성의 35%-15%-50% 비율로 각각에 할당하여 각 서브시스템에 요구되는 안전무결성을 파악할 수 있었다(Fig. 3-13). 이후 PDS Handbook을 통해 Analog Input, Supervisory Level PLC, SEM, Digital Output, Solenoid Valve의 SFF를 파악하였고, ISO 13849-1을 통해 Push Button의 SFF를 파악할 수 있었다. 이후 Fig. 3-7과 Fig. 3-8을 통해 각 구성 요소마다 최소 HFT를 결정하였고 이를 바탕으로 koon을 결정하였다. 각 구성 요소의 정보, 최소 HFT, 그리고 koon을 결정하여 Fig. 3-14에 정리하였다. 그 결과 Push Button-Analog Input은 최소 HFT가 1으로 1oo2로 여분의 장비 한 개를 필요로 하는 것을 확인하였고, Supervisory Level PLC-SEM은 최소 HFT가 각각 1과 2에 해당하여 2oo3와 1oo3로 여분의 장비를 각각 한 개와 두 개를 필요로 하는 것을 확인하였다. 그리고 Digital Output-Solenoid Valve는 최소 HFT가 0으로 여분의 장비를 필요로 하지 않는 것을 확인하였다. 이에 Push Button-Analog Input-Supervisory Level PLC—SEM-Digital Output-Solenoid Valve의 블록선도가 Fig. 3-15와 같이 작성된다. 블록선도의 경우 koon을 표현하는데 어려움이 있다. 따라서 블록선도 아래에 koon을 기재하는 경우도 있지만 Fig. 3-12와 Fig. 3-15에서는 koon을 따로 기재하지 않았고, 총 개수만을 블록선도에 표현하였다. HFT에 따라 koon을 결정할 때에는 기본적으로 k값을 1로 두었다.

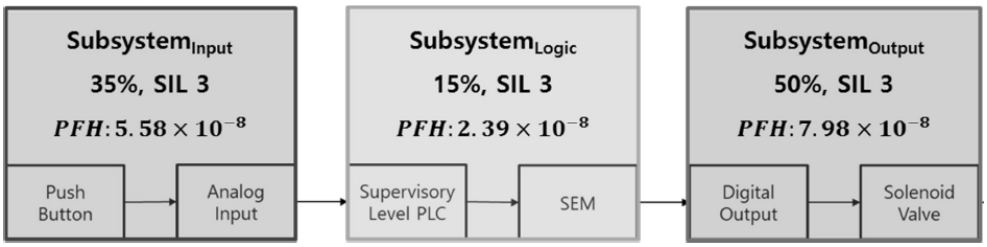

Figure 3-13 Safety Integrity Requirements of Emergency Disconnect System from Push Button to Solenoid Valve

	Component	Type	λ_D ($\times 10^{-6}$)	λ_{DU} ($\times 10^{-6}$)	λ_S ($\times 10^{-6}$)	SFF	HFT	koon
Subsystem$_{Input}$	Push Button	A	0.500	0.400	0.300	86%	1	1oo2
	Analog Input	A	1.600	0.160	1.600			
Subsystem$_{Logic}$	PLC	B	4.800	0.480	4.800	95%	1	2oo3
	SEM	B	4.000	1.200	3.500	84%	2	1oo3
Subsystem$_{Output}$	Digital Output	A	1.600	0.160	1.600	91%	0	1oo1
	Solenoid Valve	A	0.160	0.160	0.240			

Figure 3-14 Reliability Data for Emergency Disconnect System from DGPS to Indicator (Data from PDS Handbook and ISO 13849-1)

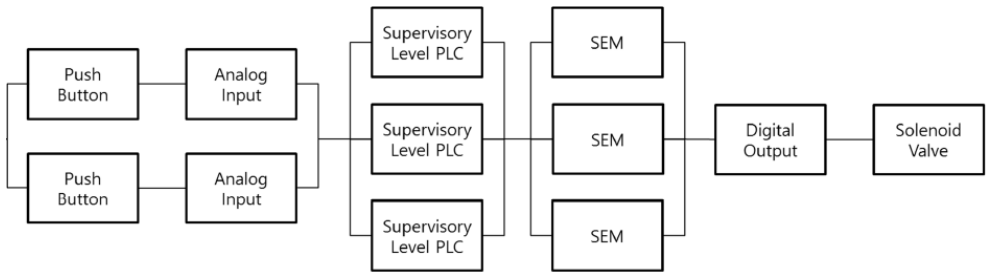

Figure 3-15 Block Diagram of Emergency Disconnect System from Push Button to Solenoid Valve

이상으로 비상분리기능에 요구되는 안전무결성을 만족시키기 위해 구조적 강건성을 고려하여 비상분리시스템을 구성하였다. 먼저 비상분리시스템이 기능 수행을 위해 어떠한 부품을 필요로 하는지 파악하기 위해 Fig. 3-9와 같이 기능블록선도를 구성하였고, Fig. 3-7과 Fig. 3-8에 따라 각 부품의 HFT를 결정하여 시스템을 구성하였다. 이를 통해 구성된 비상분리시스템의 블록선도를 작성할 수 있었고, Fig. 3-16이 비상분리시스템의 블록선도에 해당한다.

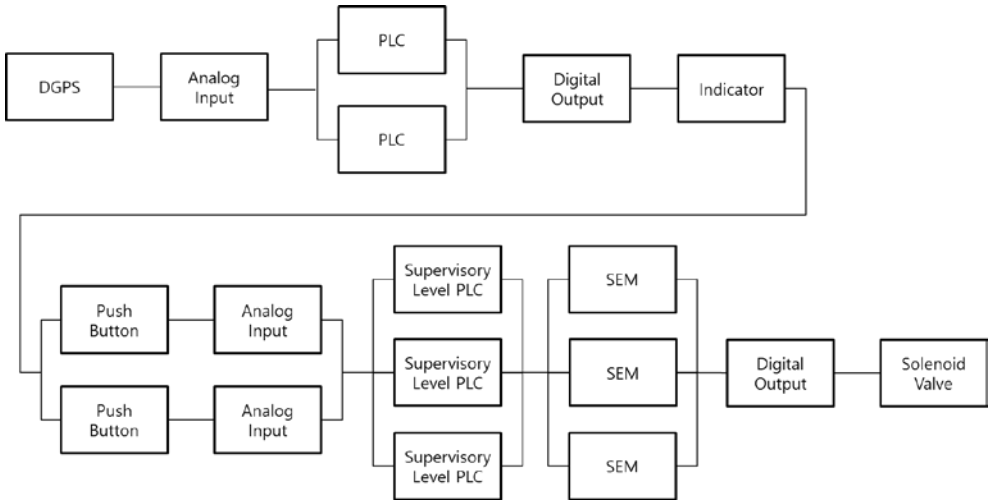

Figure 3-16 Block Diagram for Emergency Disconnect System

제 3 절 안전무결성 검증

제 1절에서는 비상분리기능의 안전무결성 요구사항을 분석하였고 제 2절에서는 안전무결성 요구사항을 비상분리시스템에 할당하여, 비상분리시스템이 요구사항을 만족시킬 수 있도록 시스템을 구성하였다. 본 절에서는 비상분리시스템이 구현하는 비상분리기능이 안전무결성 요구사항을 만족시킬 수 있는지 여부에 대해 검증을 수행하였다. 제 1절에서 언급한 바와 같이 비상분리기능의 안전무결성은 비상분리시스템이 기능 수행에 실패할 확률, 즉 비상분리시스템의 고장 확률로 계산할 수 있다. 비상분리시스템의 고장 확률 계산을 위해 Simplified Formulas, IEC Formulas, 그리고 PDS Method 세 가지 해석 방법을 사용하였다. 해석에서 사용한 가정은 다음과 같고, 각각에 대해 간단하게 살펴보았다.

① 고장 발생 시간(Time to Failure, T)은 지수분포에 따름
② 안전한 고장과 자가진단으로 감지되는 고장은 고려하지 않음
③ Proof Test로 발견된 고장은 수리되어 100% 복구됨

고장 발생 시간은 지수분포에 따른다고 가정하였다. 고장 발생 시간은 시스템이 작업을 시작 후부터 고장이 발생할 때까지의 시간에

해당한다(Fig. 3-17[5]). 고장이 발생할 확률분포함수는 F(t)로 나타내며, 이는 해당 시스템이 (0, t] 사이에 고장이 발생할 확률에 해당한다. 시간 t가 고장 발생 시간보다 크거나 같으면 고장이 발생하기 때문에 수식 (3-4)와 같이 고장 발생의 확률분포함수를 정의할 수 있다. 고장 발생의 확률밀도함수는 f(t)로 나타내며, 이는 수식 (3-5)와 같이 정의된다. 시간에 따라 확률분포함수와 확률밀도함수의 값이 바뀌고, 이를 Fig. 3-18에 나타내었다.

$$F(t) = \Pr(T \le t) \; for \; t > 0 \tag{3-4}$$

$$f(t) = \frac{d}{dt}F(t) = \lim_{\Delta t \to 0} \frac{\Pr(t < T \le t + \Delta t)}{\Delta t} \tag{3-5}$$

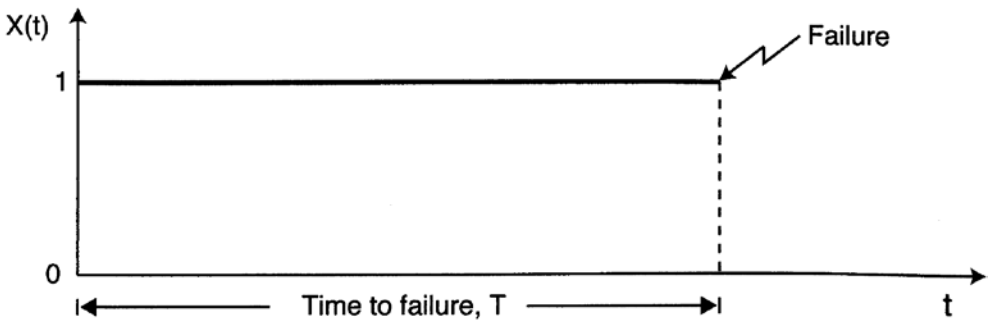

Figure 3-17 State Variable and Time to Failure of an Item (Rausand, 2014)

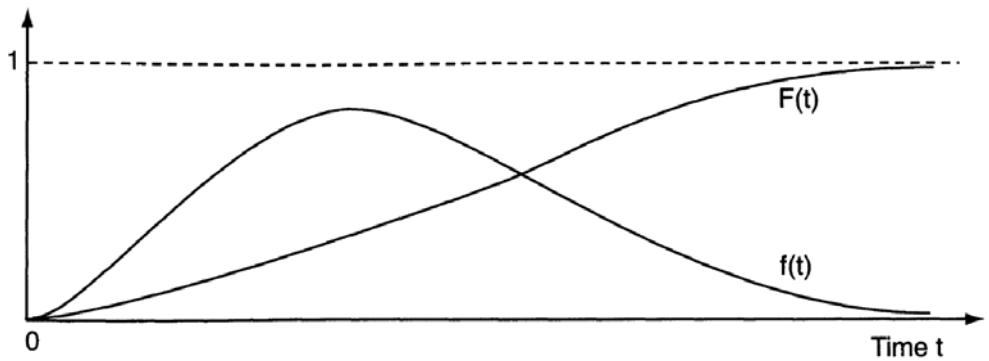

Figure 3-18 Probability Distribution Function and Probability Density Function (Rausand, 2014)

[5] Fig. 3-17의 상태 변수 X(t)는 1과 0의 값으로 Item의 상태를 나타낸다. 1은 정상적인 상태를 의미하고 0은 고장이 발생한 상태를 의미한다. Fig. 3-17을 보면 고장 발생 시간 전까지는 Item이 정상적인 상태에 있다가 고장 발생 시간이 지나 고장이 발생하면 고장이 발생한 상태로 전이되는 것을 확인할 수 있다.

안전한 고장과 자가진단으로 감지되는 고장은 고려하지 않는다고 가정하였다. 고장은 안전한 고장(Safe Failure)과 위험한 고장(Dangerous Failure) 그리고 자가 진단으로 감지되는 고장(Detected Failure)과 감지되지 않는 고장(Undetected Failure)의 기준에 따라 크게 네 가지로 분류할 수 있다(Table 3-1). 안전한 고장과 위험한 고장의 기준은 안전관련시스템의 고장이 제어되고 있는 장치의 고장으로 연결되는지에 의해 구분된다. 안전관련시스템의 고장이 제어되고 있는 장치의 고장으로 연결되지 않으면 안전한 고장으로 분류되고 안전관련시스템의 고장이 제어되고 있는 장치의 고장으로 연결되면 위험한 고장으로 분류된다. 이는 안전기능의 요구 유무와 관련되는 것으로, 안전기능이 요구되지 않는 상태에서 안전관련시스템에 고장이 발생하면 제어되고 있는 장치의 안전과 무관하여 안전한 고장으로 분류될 수 있다. 자가 진단으로 감지되는 고장과 감지되지 않는 고장은 명칭 그대로 자가 진단 시 감지 가능 여부로 분류한다. 자가 진단은 매 초 단위로 실시하기 때문에 감지 가능한 고장이 발생할 경우 즉시 발견하여 수리를 할 수 있다. 안전한 고장과 감지 가능한 고장은 고려하지 않는다고 가정하여, 해당 사고로 인해 기능을 수행하지 못하는 경우를 배제되었다. 즉, 본 논문에서는 자가 진단으로 감지되지 않는 위험한 고장만을 다루었다.

Table 3-2 Failure Classification

	Safe Failure	Dangerous Failure
Detected Failure	Safe Detected(SD)	Dangerous Detected(DD)
Undetected Failure	Safe Undetected(SU)	Dangerous Undetected(DU)

마지막으로 Proof Test로 발견된 고장은 수리되어 100% 복구된다고 가정하였다. Proof Test는 특정 주기에 따라 Item의 고장 여부를 검사하는 것으로 모든 고장은 Proof Test로 감지 가능하다고 가정하였고, 감지된 고장은 수리되어 100% 복구된다고 가정하였다. 하지만 현실에서는 수리를 통해 다시 100%의 성능을 복구되는 경우는 흔치 않고 Fig. 3-19와 같이 시간이 지날수록 고장확률이 더 높아진다. Proof Test의 주기는 τ로 나타내며, 본 논문에서는 West Engineering(2009)를 참고하여 160시간마다 Proof Test를 수행하는 것으로 가정하였다. 그리고 고장이 발생하였을 때, 평균 수리

시간(Mean Repair Time or Mean Down Time, MRT or MDT)은 10시간으로 가정하였다. 단, Proof Test에 소요되는 시간은 고려하지 않았다.

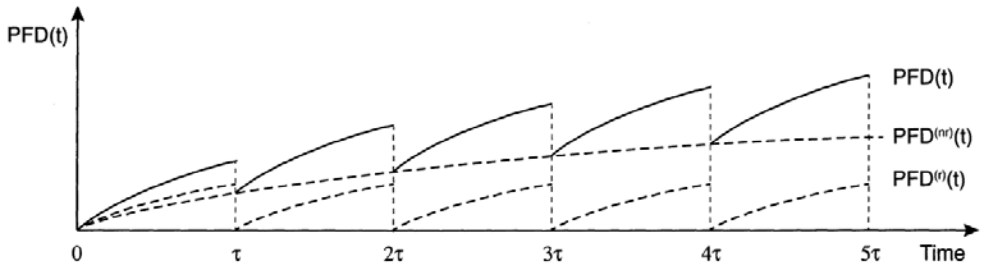

Figure 3-19 PFD of an Item with Imperfect Proof Test(Rausand, 2014)

PFH는 Rate of Occurrence of Failures(이하 ROCOF)의 개념과 유사하지만 위험 고장에 대해서 ROCOF를 계산한다(Rausand, 2014). 따라서 먼저 ROCOF에 대해서 살펴보도록 한다. ROCOF는 고장 발생 빈도로 정의된다. 시간에 따른 고장 횟수를 Plot하면 Fig. 3-20과 같이 나타낼 수 있으며, 이 때 ROCOF는 평균 고장 횟수에 대한 미분계수에 해당한다. 이를 수식으로 나타내면 수식 (3-6)과 (3-7)로 나타낼 수 있다. △t가 매우 작다고 하면 ROCOF는 수식 (3-8)과 같이 나타낼 수 있다. 일반적으로 안전기능 구현의 실패는 짧은 구간 △t동안 많아야 1번이다. 즉, (t, t+△t)동안의 고장 횟수의 차이 N(t+△t)-N(t)는 0 또는 1에 해당한다. 따라서 평균값의 정의에 따라 N(t+△t)-N(t)의 평균값은 (t, t+△t)동안의 고장이 발생할 확률과 동일하다고 할 수 있다. 따라서 ROCOF는 수식 (3-9)와 같이 나타낼 수 있다.

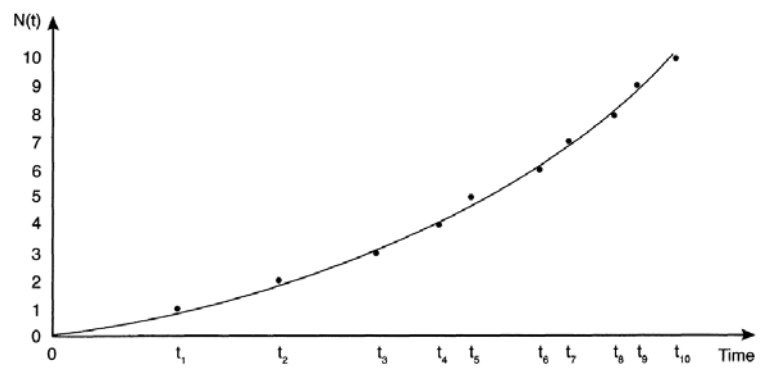

Figure 3-20 Number of Item Failure N(t) Plotted against Time t (Rausand, 2014)

$$\omega(t) = \frac{d}{dt}E[N(t)] \tag{3-6}$$

$$\omega(t) = \lim_{\Delta t \to 0} \frac{E[N(t+\Delta t) - N(t)]}{\Delta t} \tag{3-7}$$

$$\omega(t) \approx \lim_{\Delta t \to 0} \frac{E[N(t+\Delta t)] - E[N(t)]}{\Delta t} = \frac{Mean\ Number\ of\ Failures\ in\ (t, t+\Delta t)}{\Delta t} \tag{3-8}$$

$$\omega(t) \approx \lim_{\Delta t \to 0} \frac{Pr[Failures\ in\ (t, t+\Delta t)]}{\Delta t} \tag{3-9}$$

구간 (0, τ)에서 ROCOF의 평균값은 다음과 같이 계산할 수 있다. 먼저 수식 (3-10)과 같이 고장 횟수의 평균값을 계산하여, 수식 (3-11)의 구간 (0, τ)에서 ROCOF 평균값 계산식에 대입한다. 이를 통해 ROCOF를 평균 고장 횟수와 연관시킬 수 있으며, 둘의 상관관계는 수식 (3-13)으로 나타난다. 평균 고장 횟수는 평균의 정의에 따라 수식 (3-13)과 같이 계산할 수 있는데, 검사 주기 동안 고장 횟수는 0번 또는 1번에 해당하기 때문에 수식 (3-14)와 같이 계산된다. 고장 횟수의 평균은 고장이 한 번 발생할 확률에 해당하며, 수식 (3-4)로 정의된 고장 발생의 확률분포함수 F(τ)와 동일하다. 따라서 ROCOF의 평균값을 고장 발생의 확률분포함수로 계산할 수 있으며, 수식 (3-15)와 같이 표현이 가능하다. ROCOF의 평균값은 수식 (3-16)과 같이 수식 (3-5)로 정의된 고장 발생 확률밀도함수 f(t)의 평균값으로도 표현된다.

$$E[N(t)] = \int_0^{\tau} \omega(t)dt \tag{3-10}$$

$$\bar{\omega}(0,\tau) = \frac{1}{\tau}\int_0^{\tau} \omega(t)dt \tag{3-11}$$

$$\bar{\omega}(0,\tau) = \frac{E[N(\tau)]}{\tau} \tag{3-12}$$

$$E[N(\tau)] = 0 \cdot \Pr[N(\tau)=0] + 1 \cdot \Pr[N(\tau)=1] + 2 \cdot \Pr[N(\tau)=2] + \cdots \tag{3-13}$$

$$E[N(\tau)] \approx \Pr[N(\tau)=1] = F(\tau) \tag{3-14}$$

$$\bar{\omega}(0,\tau) = \frac{E[N(\tau)]}{\tau} \approx \frac{F(\tau)}{\tau} \tag{3-15}$$

$$\bar{\omega}(0,\tau) \approx \frac{F(\tau)}{\tau} = \frac{1}{\tau}\int_0^{\tau} f(t)dt = \bar{f}(0,\tau) \tag{3-16}$$

제어되고 있는 장치가 안전기능을 요구할 때, 안전관련시스템에 고장이 발생하면 해당 고장을 위험 고장이라 정의한다. PFH는 위험 고장에 대해서 ROCOF의 평균값을 계산하는 것과 동일하다. 시간t에 대해 ROCOF값을 Plot하면 Fig. 3-21과 같이 나타낼 수 있으며, 이 때 PFH는 구간(t_1, t_2)의 평균값에 해당한다. PFH는 수식 (3-17)과 (3-18)과 같이 계산이 가능하다. 지속적 혹은 높은 요구 빈도의 안전기능에 대해서는 기능에 대한 요구가 항시 이루어지고 있다고 가정한다. 따라서 요구 빈도에 대해 고려할 필요 없이 고장이 발생하면 모두 위험 고장에 해당한다.

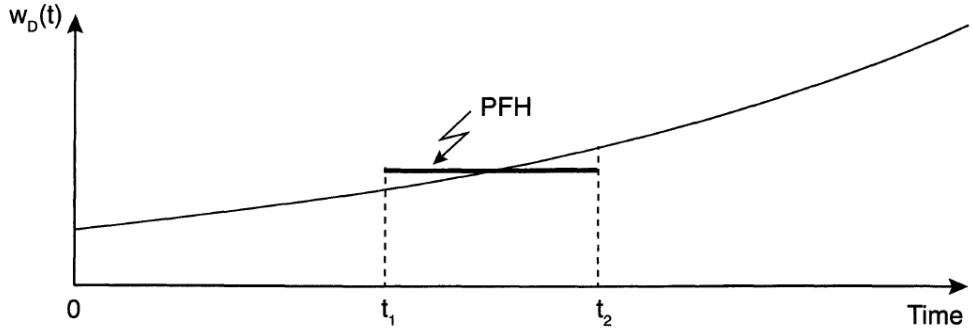

Figure 3-21 Relationship between ROCOF and PFH in time interval (t_1, t_2)(Rausand, 2014)

$$PFH(t_1,t_2) = \omega_D(t_1,t_2) = \frac{1}{t_2 - t_1}\int_{t_1}^{t_2} \omega_D(t)dt \quad (3-17)$$

$$PFH_{avg}(0,\tau) = \bar{\omega}_D(0,\tau) = \frac{Mean\ Number\ of\ Dangerous\ Failures\ in\ (0,\tau)}{\tau} \quad (3-18)$$

PFH를 계산할 때, 공통원인고장(Common Cause Failure)을 고려하기 위해서 β 요소 모델(β Factor Model)을 사용하였다. 공통원인고장은 두 개 이상의 장비로 구성된 시스템에서는 매우 중요한 문제에 해당한다. 이에 공통원인고장을 고려하기 위해 많은 연구가 수행되었지만 가장 보편적으로 사용되는 방법이 β 요소 모델에 해당한다. 하나의 원인으로 인해 둘 이상의 구성 요소에 고장이 동시에 발생하는 경우를 공통원인고장으로 정의하고 있다. β 요소 모델은 부품의 고장률을 개별원인고장률과 공통원인고장률로 나눴고, β는 두

고장률의 비로 정의 된다. PFH를 계산하기 위해 세 가지 방법론을 사용하였는데, 각각에서 공통원인고장을 어떻게 고려할 것인지에 대해 각각 기술하였다.

PFH를 계산하기 위해 제시된 근사식으로는 Simplified Formulas, IEC Formulas, 그리고 PDS Method가 있다. Simplified Formulas는 2004년 Rausand & Hoyland에 의해 소개된 방법이고, IEC Formulas는 2000년 IEC에 의해 소개된 방법이다. 마지막으로 PDS Method는 2013년 SINTEF에 의해 소개된 방법이다. 각 방법론 마다 추가적인 가정을 필요로 하는 경우도 있지만 앞서 가정한 사항에 따라 검증을 수행하였다. PFH를 계산하기 위해 제시된 세 가지 방법론에 대해서 살펴보도록 하겠다.

먼저 Simplified Formulas는 명칭처럼 가장 간단한 방법에 해당한다. 해당 방법론은 고장이 발생한 부품에 대해 수리하는데 소요되는 시간을 고려하지 않는다. 따라서 다른 두 방법론과 다르게 MRT에 대한 고려가 없다. 먼저 Redundancy가 없는 1oo1에 대한 PFH 계산식을 살펴보도록 하겠다. 감지되지 않는 위험한 고장만을 다루는 것으로 가정을 하였고, 고장 발생 시간은 지수분포에 따른다고 하였기 때문에 Proof Test의 주기 τ 동안 고장이 발생할 확률은 수식 (3-19)와 같다. 이를 통해 수식 (3-20)과 같이 Proof Test의 주기 τ 동안 평균 고장 횟수를 계산하여 수식 (3-21)과 같이 PFH를 계산한다. 이 때, $\lambda \cdot \tau$ 가 0.1보다 작거나 같을 경우에 한해 수식 (3-22)와 같이 가정할 수 있으며 결국 PFH는 수식 (3-23)으로 계산할 수 있다.

$$p(\tau) = \Pr(T_{DU} \le \tau) = 1 - e^{-\lambda_{DU}\tau} \quad (3-19)$$

$$E[N(0,\tau)] = 0 \cdot \Pr[N(0,\tau) = 0] + 1 \cdot \Pr[N(0,\tau) = 1] = p(\tau) \quad (3-20)$$

$$PFH^{1oo1} = \frac{E[N(0,\tau)]}{\tau} = \frac{p(\tau)}{\tau} = \frac{1}{\tau}(1 - e^{-\lambda_{DU}\tau}) \quad (3-21)$$

$$1 - e^{-\lambda_{DU}\tau} \approx \lambda_{DU} \quad (3-22)$$

$$PFH^{1oo1} = \lambda_{DU} \quad (3-23)$$

Redundancy가 존재하는 koon에 대한 PFH 계산식을 살펴보도록 하겠다. 구간 (0, τ)에서 고장이 발생한 부품의 개수를 M(τ)라고 할

때, 고장 확률은 수식 (3-24)와 같이 계산할 수 있다. koon의 경우 위험 고장은 고장이 발생한 부품의 개수 M(τ)가 n-k+1개 이상일 때에 해당한다. 즉, 위험 고장이 발생할 확률은 수식 (3-25)와 같이 계산할 수 있으며, 이를 통해 평균 고장 횟수를 수식 (3-26)과 같이 계산할 수 있다. 이 때, PFH는 정의에 따라 수식 (3-27)과 같이 계산할 수 있으며 수식 (3-28)과 (3-29)의 가정에 따라 최종적으로 PFH는 수식 (3-30)으로 계산할 수 있다.

$$\Pr[M(\tau)=j]=\binom{n}{j}(1-e^{-\lambda_{DU}\tau})^{j}(e^{-\lambda_{DU}\tau})^{n-j} \tag{3-24}$$

$$\Pr[Dangerous\ Failures\ in\ (0,\tau)]=\Pr[M(\tau)\geq n-k+1]=\sum_{j=n-k+1}^{n}\Pr[M(\tau)=j] \tag{3-25}$$

$$E[N(\tau)]=0\cdot\Pr[N(0,\tau)=0]+1\cdot\Pr[N(0,\tau)=1]=\Pr[M(\tau)\geq n-k+1 \tag{3-26}$$

$$PFH^{koon}=\frac{E[N(\tau)]}{\tau}=\frac{1}{\tau}\sum_{j=n-k+1}^{n}\binom{n}{j}(1-e^{-\lambda_{DU}\tau})^{j}(e^{-\lambda_{DU}\tau})^{n-j} \tag{3-27}$$

$$1-e^{-\lambda_{DU}\tau}\approx\lambda_{DU} \tag{3-28}$$

$$PFH^{1oo1}=\lambda_{DU} \tag{3-29}$$

$$PFH^{koon}\approx\frac{\Pr[M(\tau)=n-k+1]}{\tau}=\binom{n}{n-k+1}(\lambda_{DU})^{n-k+1}\tau^{n-k} \tag{3-30}$$

공통원인고장은 β 요소 모델을 통해 고려한다. PFH를 개별원인고장에 인한 것과 공통원인고장에 인한 것으로 나눠 수식 (3-31)과 같이 계산한다. 이 때 개별원인고장에 인한 PFH는 기존의 PFH 계산식에 각 구성 요소의 개별원인고장률을 대입한다. β는 정의에 따라 수식 (3-32)와 같이 나타내지고, 이에 개별원인고장률은 수식 (3-33)으로 나타내진다. 공통원인고장에 인한 PFH는 수식 (3-34)에 따라 계산되는데, 이는 공통원인고장률과 같은 값을 가진다.

$$PFH=PFH_i+PFH_C \tag{3-31}$$

$$\beta=\frac{\lambda^C}{\lambda} \tag{3-32}$$

$$\lambda^i=(1-\beta)\cdot\lambda \tag{3-33}$$

$$PFH_C=\beta\cdot\lambda \tag{3-34}$$

IEC Formulas는 Channel[⑥]-Equivalent Mean Downtime[⑦]과 Group-Equivalent Mean Downtime을 제시하고 이를 PFH 계산에 사용한다. 감지되지 않는 위험 고장만을 고려하기 때문에 감지되는 위험 고장에 의한 수리시간에 해당하는 Mean Time To Repair(이하 MTTR)을 0으로 가정하였다. MTTR이 0일 때 Channel-Equivalent Mean Downtime과 Group-Equivalent Mean Downtime은 수식 (3-35)과 (3-36)로 표현된다. 1oo1에 대한 PFH 계산식은 Simplified Formulas와 동일하여 수식 (3-37)으로 표현된다. 1oo2에 대한 PFH 계산식은 수식 (3-38)로 표현되고, 이는 감지되지 않는 위험 개별원인고장으로 인해 두 구성 요소 각각에 고장이 발생하는 확률과 공통원인고장으로 두 구성 요소에 동시에 고장이 발생하는 확률의 합을 의미한다. 마찬가지로 2oo3에 대한 PFH 계산식은 (3-39)로 표현되며, 1oo3에 대한 PFH 계산식은 (3-40)로 표현된다. Simplified Formulas와 같이 koon에 대하여 일반화된 식이 아닌 1oo2와 같이 위험 고장이 발생하는 경우를 따져 PFH를 계산한다. 본 논문에서는 1oo2, 2oo3, 그리고 1oo3의 계산식만이 필요하기 때문에 이를 수식으로 기술하였고, 다른 koon 구성에 대해 PFH를 계산하는 식은 IEC 61508-6(2000)에 상세히 기술되어있다.

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{2} + MRT\right) \quad (3-35)$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{n-k+2} + MRT\right) \quad (3-36)$$

$$PFH^{1oo1} = \lambda_{DU} \quad (3-37)$$

$$PFH^{1oo2} = 2 \cdot \lambda_D^i\left(1 - e^{-(1-\beta)\lambda_{DU} t_{CE}}\right) + \beta \cdot \lambda_{DU} = 2 \cdot [(1-\beta) \cdot \lambda_{DU}]^2 \cdot t_{CE} + \beta \cdot \lambda_{DU} \quad (3-38)$$

$$PFH^{2oo3} = 6 \cdot [(1-\beta) \cdot \lambda_{DU}]^2 \cdot t_{CE} + \beta \cdot \lambda_{DU} \quad (3-39)$$

$$PFH^{1oo3} = 6 \cdot [(1-\beta) \cdot \lambda_{DU}]^2 \cdot t_{CE} \cdot t_{GE} + \beta \cdot \lambda_{DU} \quad (3-40)$$

---

⑥ 일반적으로 가장 낮은 단계의 구성 요소, 부품을 Element라고 명명하고, 한 개 이상의 Element가 모여 하나의 기능을 수행하는 경우 해당 모임을 Channel이라 명명한다. 같은 기능을 수행하는 Channel이 여러 개 존재하여 koon을 구성하면 해당 모임을 (Voted) Group이라고 명명한다.

⑦ Mean Downtime은 Channel 혹은 Group에 고장이 발생하여 기능을 수행하지 못하는 시간을 의미한다. 반의어는 Uptime으로 정상적으로 기능을 수행할 수 있는 시간을 의미한다.

PDS Method는 개별원인고장으로 인한 PFH 계산을 위해 Simplified Formulas를 사용하지만, 수식 (3-33)의 개별원인고장률을 사용하지 않고 감지되지 않는 위험 고장률을 그대로 사용한다. 또한 공통원인고장으로 인한 PFH 계산을 위해 Configuration Factor를 도입하였다. Simplified Formulas와 IEC Formulas는 공통원인고장으로 인한 PFH가 koon와 관계없이 동일한 값을 가졌지만, PDS Method에 따르면 koon에 따라 계수 C_{koon}이 달라 공통원인고장으로 인한 PFH가 달라진다. 이는 koon이 다르면 시스템의 구성뿐만 아니라 선택논리가 달라지기 때문에 koon에 따라 공통원인고장률이 달라져야 한다는 생각이 반영된 결과라고 할 수 있다. Fig. 3-22는 PDS Method를 통해 PFH를 계산하는 식에 해당하며, Fig. 3-33은 C_{koon}에 해당한다.

	PFH formulas in the PDS method		
Voting	Contribution from Independent failures		Contribution from CCFs
1oo1	λ_{DU}		NA
noon	$n\lambda_{DU}$		NA
1oo2	$\lambda_{DU}^2\tau$	+	$\beta\lambda_{DU}$
1oo3	$\lambda_{DU}^3\tau^2$	+	$C_{1oo3}\beta\lambda_{DU}$
2oo3	$3\lambda_{DU}^3\tau^2$	+	$C_{2oo3}\beta\lambda_{DU}$
koon	$\binom{n}{n-k+1}\lambda_{DU}^{n-k+1}\tau^{n-k}$	+	$C_{koon}\beta\lambda_{DU}$

Figure 3-22 PDS Formulas for Average PFH (Rausand, 2014)

k/n	$n=2$	$n=3$	$n=4$	$n=5$	$n=6$
$k=1$	1.00	0.50	0.30	0.20	0.15
$k=2$	–	2.00	1.10	0.80	0.60
$k=3$	–	–	2.80	1.60	1.20
$k=4$	–	–	–	3.60	1.90
$k=5$	–	–	–	–	4.50

Figure 3-23 Configuration Factors for Selected koon Architectures(Rausand, 2014)

본 논문에는 1oo1, 1oo2, 2oo3, 그리고 1oo3만 사용되며, 각 방법론에 따라 식을 Fig. 3-24에 정리하였다.

k out of n	Simplified Formula	IEC Formula	PDS Method
1oo1	λ_{DU}	λ_{DU}	λ_{DU}
1oo2	$((1-\beta)*\lambda_{DU}))^2*\tau+\beta*\lambda_{DU}$	$2*\left((1-\beta)*\lambda_{DU}\right)^2*\left(\frac{\tau}{2}+MRT\right)+\beta*\lambda_{DU}$	$(\lambda_{DU})^2*\tau+\beta*\lambda_{DU}$
2oo3	$3*((1-\beta)*\lambda_{DU}))^2*\tau+\beta*\lambda_{DU}$	$6*\left((1-\beta)*\lambda_{DU}\right)^2*\frac{\lambda_D}{\lambda_{DU}}*\left(\frac{\tau}{2}+MRT\right)+\beta*\lambda_{DU}$	$3*(\beta*\lambda_{DU})^2*\tau+2*\beta*\lambda_{DU}$
1oo3	$((1-\beta)*\lambda_{DU}))^3*\tau^2+\beta*\lambda_{DU}$	$6*\left((1-\beta)*\lambda_{DU}\right)^2*(\frac{\lambda_D}{\lambda_{DU}})^2*\left(\frac{\tau}{2}+MRT\right)*\left(\frac{\tau}{3}+MRT\right)+\beta*\lambda_{DU}$	$(\lambda_{DU})^3*\tau^2+0.5*\beta*\lambda_{DU}$

Figure 3-24 PFH Calculation Formulas

Fig. 3-24의 식을 사용하여 검증을 수행하기 위해 비상분리시스템의 신뢰성블록선도(Reliability Block Diagram)를 작성하였다. 신뢰성블록선도는 특정 기능을 수행하기 위해 여러 구성 요소들로 구성된 시스템의 상태를 표현하기 위한 논리도로 정의된다. 신뢰성블록선도 작성 후 구조 함수(Structure Function)를 구성하여 안전무결성 해석을 수행하기도 하지만, 본 논문에서는 기능 수행을 위한 시스템의 구성을 가시화하기 위해 신뢰성블록선도를 작성하였다(Fig. 3-25).

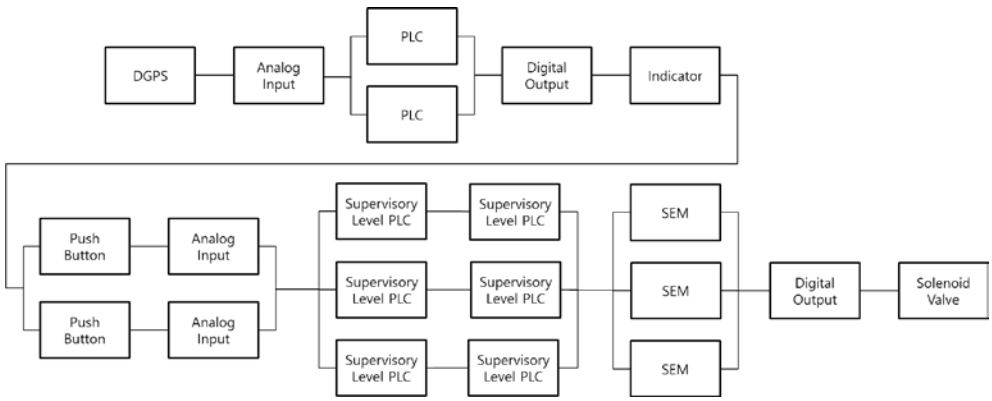

Figure 3-25 Reliability Block Diagram for Emergency Disconnect System

세 가지 방법론에 따라 검증을 수행하기 위해 필요한 입력값을 정리하였다. 세 방법론을 적용하기 위해 필요한 입력값은 각 구성 요소의 고장률(감지되지 않는 위험 고장률 λ_{DU}과 위험 고장률 λ_D), β요소, Proof Test 주기 τ, 그리고 평균 수리 시간 MRT이다. 비상분리시스템의 구성 요소인 DGPS, Analog Input, PLC, Digital

Output, Indicator, Push Button, SEM, 그리고 Solenoid Valve의 입력값을 정리하여 Fig. 3-26으로 나타냈다. 고장률의 출처를 함께 기재하였다. 수치 옆에 *표시는 데이터를 찾지 못해 가정한 값이다. β를 찾을 수 없는 경우에는 모두 3%로 가정하였다.

Component	λ_D ($\times 10^{-6}$)	λ_{DU} ($\times 10^{-6}$)	β	τ	MRT	Ref.
DGPS	10.00*	1.000*	0.03*	160	10	Assumption
Analog Input	1.600	0.160	0.05	160	10	PDS Handbook
PLC	4.800	0.480	0.05	160	10	PDS Handbook
Digital Output	1.600	0.160	0.05	160	10	PDS Handbook
Indicator	0.100	0.050*	0.03*	160	10	IEC 60947-5-4
Push Button	0.500	0.400	0.03*	160	10	PDS Handbook
SEM	4.000	1.200	0.05	160	10	PDS Handbook
Solenoid Valve	0.160	0.160	0.03*	160	10	ISO 13849-1

Figure 3-26 Input Data Set for Safety Integrity Verification of Emergency Disconnect System

Fig. 3-25의 신뢰성블록선도에 대해 Simplified Formulas, IEC Formulas, 그리고 PDS Method를 통해 안전무결성 검증을 수행한 결과를 Fig. 3-27과 같이 정리하였다. 검증 결과 구성한 비상분리시스템은 비상분리기능에 요구되는 안전무결성을 만족시키지 못해 성공적으로 기능을 구현할 수 없음을 확인하였다. 이러한 결과는 Fig. 3-27의 수치 중 *표시가 되어 있는 구성 요소에 의해 도출된 것으로 확인되었다. *표시가 되어 있는 구성 요소의 고장 확률은 단독으로도 요구되는 안전무결성 수준을 만족시키지 못하는 것을 확인할 수 있다. 특이점은 모두 1oo1의 구성을 따르고 있다는 점이다. 1oo1의 PFH는 각 구성 요소의 감지되지 않는 위험 고장률에 해당한다. 구조적 강건성을 고려할 때는 SFF를 고려하였기 때문에 1oo1으로 충분하다는 결과가 도출될 수 있으나 감지되지 않는 위험 고장률의 크기 자체가 일정수준보다 커지면 이러한 현상이 발생할 수 있음을 짐작할 수 있다. 따라서 요구되는 안전무결성을 만족시키기 위해 *표시가 된 구성 요소에 대해서는 HFT를 하나씩 늘리는 방안을 고려하였다. 즉, 해당 구성 요소에 대해 HFT를 1로 늘리고 모두 1oo2로 구성을 변경하였다. 변경된 구성에 대해서도 신뢰성블록선도를 작성하였고, 이를 Fig. 3-28로 나타내었다. 이후 Fig. 3-28의 신뢰성블록선도에 대해 세 가지 방법론을 통해 안전무결성 검증을 수행한 결과를 Fig. 3-29와 같이 정리하였다.

	Koon	Component	Simplified	IEC	PDS
$Subsystem_{Input}$	1oo1	DGPS Analog Input	1.16E-06*	1.16E-06*	1.16E-06*
$Subsystem_{Logic}$	1oo2	PLC	2.40E-08	2.40E-08	2.40E-08
$Subsystem_{Output}$	1oo1	Digital Output Indicator	2.10E-07*	2.10E-07*	2.10E-07*
Sum			**1.39E-06**	**1.39E-06**	**1.39E-06**
Required Safety Integrity				**1.12E-07**	
$Subsystem_{Input}$	1oo2	Push Button Analog Input	2.00E-08	2.00E-08	2.00E-08
$Subsystem_{Logic}$	2oo3	PLC	8.40E-08	8.80E-08	7.80E-08
	1oo3	SEM			
$Subsystem_{Output}$	1oo1	Digital Output Solenoid Valve	3.20E-07*	3.20E-07*	3.20E-07*
Sum			**4.24E-07**	**4.28E-07**	**4.18E-07**
Required Safety Integrity				**1.60E-07**	
Total			**1.82E-06**	**1.82E-06**	**1.81E-06**
Required Safety Integrity				**2.71E-07**	

Figure 3-27 Safety Integrity Analysis Results

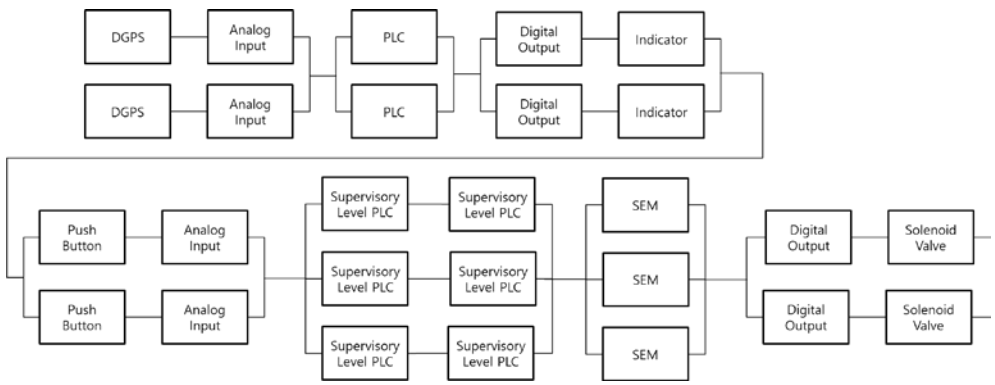

Figure 3-28 Reliability Block Diagram for Re-arranged Emergency Disconnect System

DGPS, Analog Input, Digital Output, Indicator, 그리고 Solenoid Valve의 HFT를 하나씩 늘려 Fig. 3-28과 같이 비상분리시스템을 구성할 경우 Fig. 3-29에서 확인할 수 있듯이 비상분리시스템이 비상분리기능에 요구되는 사항을 만족시킬 수 있는 것을 확인할 수 있다. 비상분리기능에 요구되는 안전무결성은 작업자를 배제하였을 때, PFH 2.71E-07/hour에 해당한다. 해당 요구사항을 비상분리시스템에 할당하여 시스템이 안전무결성 요구사항을 만족시킬 수 있는지 검증하기

위해 Simplified Formulas, IEC Formulas, 그리고 PDS Method를 사용하였고, 그 결과 PFH 1.89E-07/hour, PFH 1.92E-07/hour, 그리고 PFH 1.83E-07/hour로 요구사항인 PFH 2.71E-07/hour보다 작아 요구사항을 만족시키는 것을 검증하였다. 이는 구성한 비상분리시스템이 성공적으로 비상분리기능을 수행하여 라이저와 유정헤드의 안전을 보장할 수 있음을 의미한다.

	Koon	Component	Simplified	IEC	PDS
$Subsystem_{Input}$	1oo2*	DGPS	3.82E-08	3.80E-08	3.82E-08
		Analog Input			
$Subsystem_{Logic}$	1oo2	PLC	2.40E-08	2.40E-08	2.40E-08
$Subsystem_{Output}$	1oo2*	Digital Output	9.50E-09	9.50E-09	9.50E-09
		Indicator			
Sum			**7.17E-08**	**7.15E-08**	**7.17E-08**
Required Safety Integrity				**1.12E-07**	
$Subsystem_{Input}$	1oo2	Push Button	2.00E-08	2.00E-08	2.00E-08
		Analog Input			
$Subsystem_{Logic}$	2oo3	PLC	8.40E-08	8.80E-08	7.80E-08
	1oo3	SEM			
$Subsystem_{Output}$	1oo2*	Digital Output	1.28E-08	1.28E-08	1.28E-08
		Solenoid Valve			
Sum			**1.17E-07**	**1.21E-07**	**1.11E-07**
Required Safety Integrity				**1.60E-07**	
Total			**1.89E-07**	**1.92E-07**	**1.83E-07**
Required Safety Integrity				**2.71E-07**	

Figure 3-29 Safety Integrity Analysis Results for Re-arranged Emergency Disconnect System

Simplified Formulas와 PDS Method는 1oo2에 대해서는 계산 결과가 거의 유사한 결과를 보인다. 1oo2에 대해 계산식을 비교하면, 개별원인고장에 대해 고려하는 항은 다르지만 공통원인고장에 대해 고려하는 항은 동일하다. 그런데 두 방법에 따라 계산된 PFH가 유사한 값을 가진다는 것은 PFH가 공통원인고장에 의해 결정된다고 생각할 수 있다. 2oo3와 1oo3에 대해서는 차이를 보이는데, 이는 공통원인고장에 대해 고려하는 항이 달라졌기 때문이다. PLC만을 비교해보면 Simplified Formulas와 PDS Method로 계산한 결과가 PFH 2.40E-08/hour와 4.80E-08/hour에 해당하고, 2배 차이가 나는 것을 확인할 수 있다. 2oo3의 계산식을 비교해보면 PDS Method의 공통원인고장을 고려하는 항에 Configuration Factor 2가 곱해져 있는 것을 확인할 수 있다. 이를

통해 PFH를 결정하는 주요 요소가 공통원인고장이라는 것을 알 수 있었다. Simplified Formulas와 IEC Formulas를 비교하면 DGPS와 Analog Input의 PFH는 Simplified Formulas가 더 크게 계산되었지만, PLC와 SEM의 PFH는 IEC가 더 크게 계산되었음을 확인할 수 있다. IEC Formulas는 위험 고장률과 MRT를 추가적으로 고려하기 때문에 두 변수에 의해 결과가 달라졌을 것으로 예상된다.

제 4 절 안전무결성 검증의 타당성 검토

앞서 비상분리시스템에 할당된 안전무결성 요구사항 만족 여부를 검증하였고, 본 절에서는 검증의 타당성에 대해서 검토한다. 타당성 검토는 검증에 사용된 해석 방법 외에 다른 해석 방법으로 검증을 수행하고, 모형이나 시제품을 통해 고장 확률을 확인해보는 방법을 통해 이루어진다. 현실적으로 모형이나 시제품을 만들어 실험을 할 수 있는 여건이 되지 않았기 때문에 다른 해석 방법을 통해 다시 검증을 수행하는 것으로 검증의 타당성을 검토하였다. 타당성 검토를 위해 근사식을 사용하지 않고 시간에 따른 시스템의 상태전이를 분석하였다. 이를 위해 2012년 IEC에서 권고한 Petri Net을 사용하였다.

Petri Net은 컴퓨터 공학에서 동시성(Concurrency)을 구현하기 위해 도입되어 지난 30년 동안 안전관련시스템의 고장 확률 계산을 위해 사용되었다. Petri Net은 기본적으로 시스템의 상태전이를 모사하기 위한 도구에 해당하며, Reachability Graphs(이하 RG)를 통해 정성적/정량적인 해석이 가능하다. RG는 시스템을 구성하는 모든 구성요소의 상태를 0과 1로 표현하여 벡터형태로 표현하는 Reachability Set의 모든 경우를 고려하여, 시간에 따라 Reachability Set이 어떻게 바뀌는지 그래프로 표현한 것이다. 하나의 구성 요소가 1oo2로 구성된 시스템의 상태전이를 모사한 결과는 Fig. 3-30과 같으며, 이를 해석하기 위해 RG를 작성하여 Fig. 3-31로 나타냈다. RG를 작성하는 것 자체가 정성적인 해석에 해당하여, 시스템과 그 구성 요소들의 상태에 대해 모든 경우의 수를 보여줄 수 있다. 반면 정량적인 해석을 위해서는 시간의 진행에 따라 시스템과 그 구성 요소들의 상태가 어떻게 변하는지를 고려할 수 있는 Timed RG를 구성해야 한다. 이를 통해 Markov Chain 또는 Monte-Carlo Simulation 기법을 사용하여 해석을 수행한다. IEC 62551(2012)에서는 시스템의 크기와 상태전이에 소요되는 시간의 분포 종류에 크게 제한 받지 않는 Monte-Carlo

Simulation 기법을 사용할 것을 권고하고 있다(Fig. 3-32).

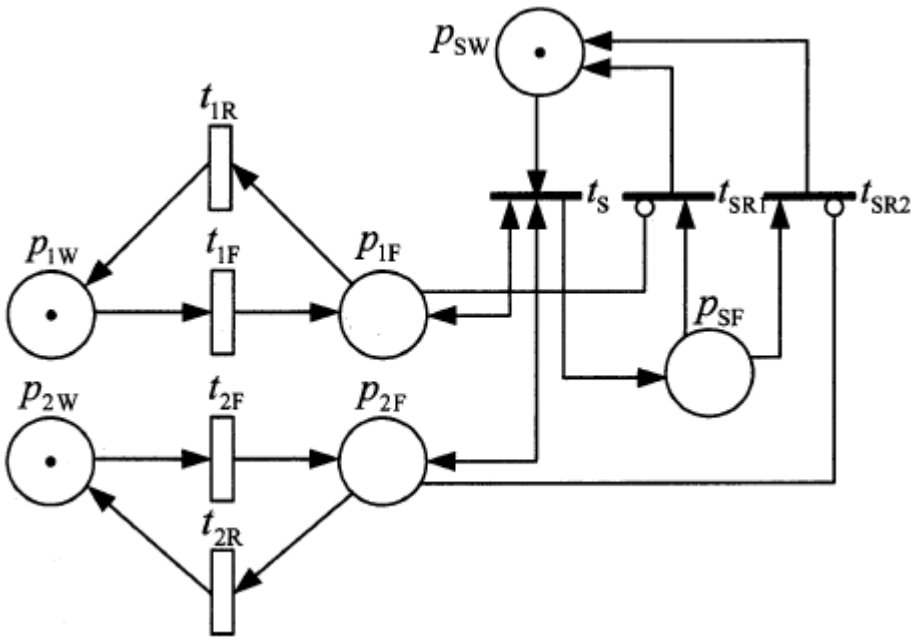

Figure 3-30 Petri Net Model for Repairable 1oo2 Voted Group (Rausand, 2014)

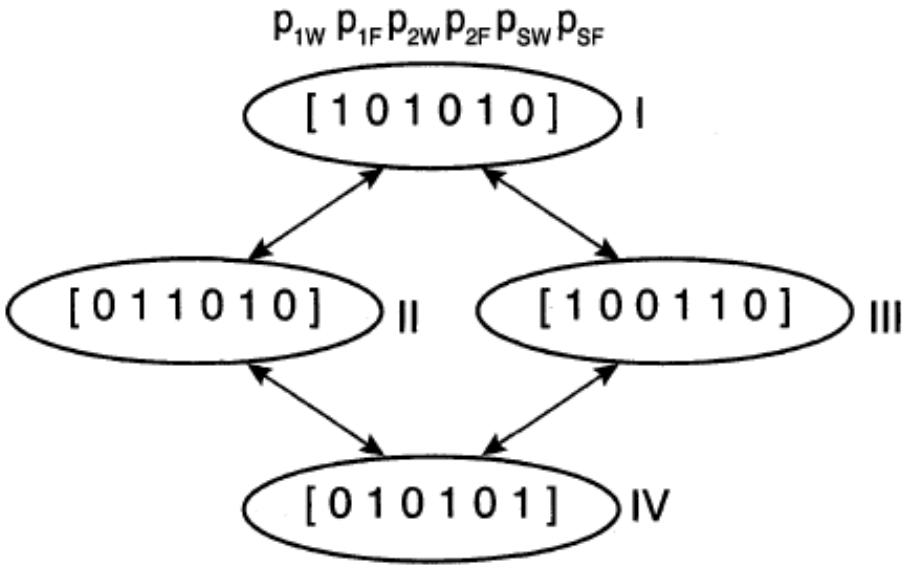

Figure 3-31 Reachability Graphs of Petri Net Model for 1oo2 Voted Group(Rausand, 2014)

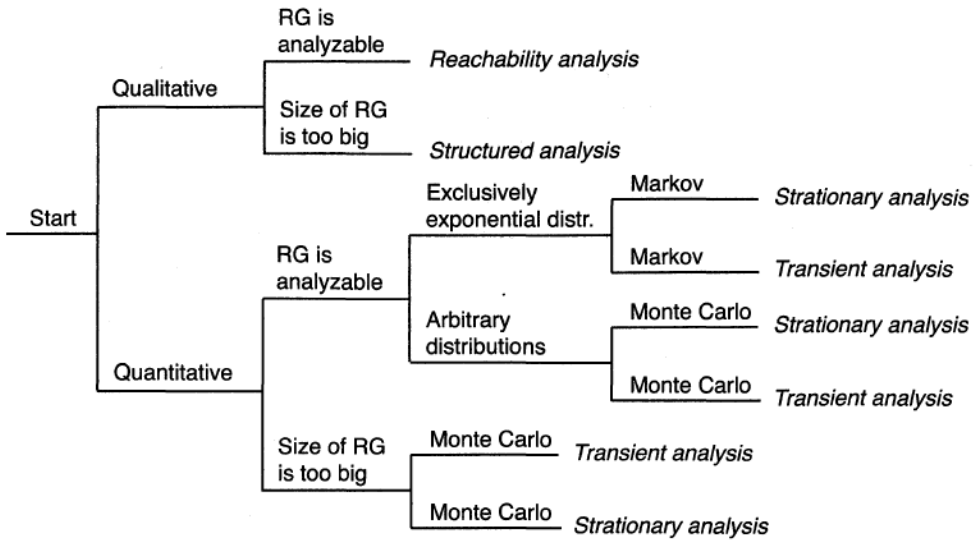

Figure 3-32 Analytical Methods for Petri Net Models(IEC, 2012)

Petri Net은 전기·전자 제어시스템의 제어논리를 모사하는데 용이하고, 시간의 흐름에 따라 시스템의 상태전이를 직관적으로 모사할 수 있는 장점을 가지고 있지만 시스템의 크기가 커질수록 Petri Net이 지나치게 복잡해지는 단점을 가지고 있다. 2oo3만 해도 시스템의 Petri Net 모형이 Fig. 3-33과 같이 매우 복잡해진다. 따라서 보다 간단하게 시스템의 상태전이를 모사하고 해석할 수 있는 방안이 많이 제시되고 있으며, 본 논문에서는 Signoret(2012)에 의해 개념적으로 제안된 Reliability Block Diagram Driven Petri Net을 사용하였다.

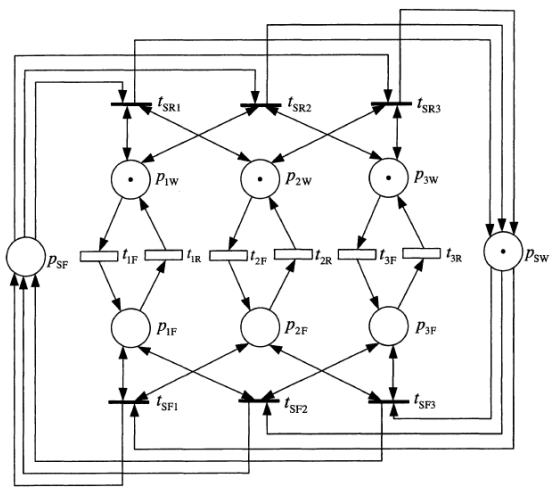

Figure 3-33 Petri Net Model for 2oo3 Voted Group(Rausand, 2013)

Reliability Block Diagram Driven Petri Net으로 비상분리시스템의 안전무결성 해석을 수행하기에 앞서, Petri Net에 대해서 간단하게 살펴본다. Petri Net모형은 상태를 나타내는 Place(p_i)와 상태전이를 야기하는 사건에 해당하는 Transition(t_i)로 구성된다. Fig. 3-34는 가장 간단한 Petri Net모형에 해당한다. 모형을 이해하기 위해서는 Fig. 3-34에 네모로 표시한 것과 같이 하나의 상태와 하나의 사건을 단위로 보는 것이 좋다. Fig. 3-34에 점으로 표시된 것은 토큰(Token)으로 불리는 동적 요소로 특정 Place에 위치하여 해당 시스템의 상태를 알려준다. p_1에 토큰이 위치하면, 해당 시스템은 p_1으로 정의된 상태에 있음 의미한다. 먼저 p_1과 t_1을 단위로 살펴보면, 사건 t_1이 발생할 경우 토큰이 사건 t_1으로 인해 p_1에서 벗어나는 것을 확인할 수 있다. 이후 t_1과 p_2를 단위로 살펴보면, 사건 t_1이 발생할 경우 토큰이 사건 t_1으로 인해 p_2로 들어오는 것을 확인할 수 있다. 사실상 Fig. 3-34의 경우는 간단한 모형에 해당하기 때문에 Petri Net모형에 익숙하지 않은 사람도 단위로 나눌 필요 없이 직관적으로 이해할 수 있다. 하지만 Petri Net모형이 복잡해져 Place와 Transition의 수가 늘어나면 하나의 상태와 하나의 사건을 단위로 하여 분석하지 않으면 모형을 잘못 이해하는 경우가 생길 수 있다.

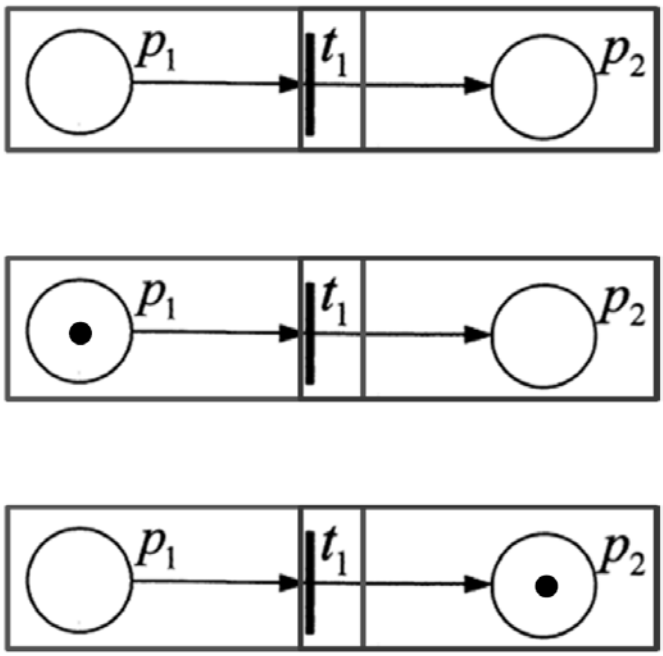

Figure 3-34 Simple Petri Net Model(Rausand, 2013)

상태와 사건을 연결하는 아크(Arc)는 크게 두 종류가 존재한다. 하나는 일반적인 화살표로 상태전이가 발생하는 것을 의미하고, 다른 하나는 선 끝에 원이 붙어있는 형태[⑧]로 상태전이가 발생하는 것을 방지하는 것을 의미한다. 이를 Inhibitor Arc라고 부른다. Fig. 3-35를 예를 들어 설명을 하자면, p_2와 t_1을 단위로 살펴보면 둘은 Inhibitor Arc로 연결되어 p_2에 토큰이 존재할 경우 사건 t_1은 절대로 발생하지 않는다. 따라서 p_1에 토큰이 존재하여도 사건 t_1이 발생하지 못해 상태전이가 일어나지 않는다. p_2의 토큰이 사라질 경우에만 사건 t_1으로 인한 상태전이가 가능해진다. Multiplicity(또는 Weight)는 사건이 발생하기 위해 필요한 토큰의 수로 정의되어, 일반적으로 Arc 중간에 표시된다. Arc 중간에 아무 표시가 없을 경우에는 하나의 토큰을 필요로 하지만 특정 숫자가 적혀있는 경우에는 이전 상태에 그 숫자만큼의 토큰이 존재해야만 사건이 발생된다.

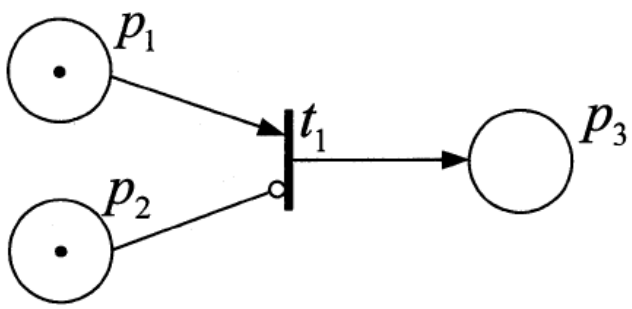

Figure 3-35 Petri Net Model with Inhibitor Arc(Rausand, 2014)

만약 상태전이에 시간이 소요되는 경우(Timed Transition)에 해당 Petri Net을 Timed Petri Net이라 명명한다. 상태전이에 소요되는 시간이 결정론적으로 주어진 경우와 확률론적으로 주어진 경우 모두 표현이 가능하다. 상태전이에 소요되는 시간이 모두 결정론적으로 주어진 경우에는 별 다른 명칭이 없지만, 상태전이에 소요되는 시간이 모두 확률론적으로 주어진 경우에는 해당 Petri Net을 Stochastic Petri Net이라 한다. 하지만 결정론적으로 주어진 경우와 확률론적으로 주어진 경우가 혼재되어 있는 경우가 일반적이며 이러한 경우에는 해당

[⑧] Inhibitor Arc는 선 끝에 원이 붙어 있는 형태가 가장 많이 사용되지만 아직 관련 기준이 제시되지 않아 Petri Net Model마다 모양이 다를 수 있다. 이에 IEC(2012)에서는 Inhibitor Arc를 점선으로 나타낼 것을 기준으로 삼았으나, 아직까지는 선 끝에 원이 붙어 있는 형태를 많이 사용하고 있다.

Petri Net을 Generalized Stochastic Petri Net이라 한다. 상태전이에 소요되는 시간 또는 시간의 확률 분포는 Transition 근처에 표시하는데, Transition의 기호 또한 달라진다. 사용되는 Transition 기호를 정리하여 Fig. 3-36으로 나타냈다. Petri Net을 안전무결성 해석(신뢰성 해석)에 사용할 경우, 상태전이에 소요되는 시간은 주로 지수분포를 사용한다. 이 때 지수분포의 계수 λ는 각 구성 요소의 고장률에 해당한다.

	Type of transition			
	Deterministic		*Stochastic*	
	Delay is zero	Delay is *d*	Exponentially or geometrically distributed	Arbitrarily distributed
Parameter		*d*	λ	ϕ Arbitrary distribution
Symbol				

Figure 3-36 Symbols Used for Transition(Rausand, 2014)

본 논문에서는 사용하는 Reliability Block Diagram Driven Petri Net은 신뢰성블록선도와 Petri Net을 결합한 개념이다. 신뢰성블록선도를 이용해 고장 확률을 계산하는 과정은 시간에 따른 시스템의 거동을 살펴볼 수 없는 단점을 가지고 있으나 Functional Block, 즉 기능 단위로 구성 요소를 나눠 세부 기능을 수행하기 위한 부품을 파악하고 부품의 고장 확률로 시스템 전체의 고장 확률을 계산할 수 있다. 반면 Petri Net은 시간에 따른 시스템의 동적 거동을 해석할 수 있지만 시스템 전체에 대해 해석을 수행하기 위해서는 Petri Net Model 자체가 너무 복잡해져 해석에 어려움을 가진다는 단점을 가지고 있다. 따라서 이 두 방법론은 서로 상호보완적인 역할을 할 수 있으며, 이에 Signoret(2012)은 두 방법론을 통합한 Reliability Block Diagram Driven Petri Net의 개념을 제안하게 되었다. 기본적인 개념은 신뢰성블록선도가 기능 단위로 구성 요소를 나누기 때문에 각 기능 단위마다 Petri Net Model을 만들어 해석을 수행하고, 이를 통해 각 기능 단위마다의 고장 확률을 계산하면 신뢰성블록선도를 통해 시스템

전체의 고장 확률을 계산하는 것이다. Signoret(2012)은 안전계장시스템에 대해 해당 방법론을 적용시켜 Petri Net Model을 만들었다(Fig. 3-37). Fig. 3-37을 살펴보면 (1)부터 (D)까지는 센서가 2oo3로 구성되어있고, (D)부터 (E)까지는 Logic Solver가 1oo1으로 구성되어 있으며 (E)부터 (S)까지는 밸브가 1oo2로 구성되어 있다. 센서에 대해서만 간단히 살펴보면 세 개의 센서 각각에 대해서 Petri Net Model을 만들었다. 센서의 Petri Net Model은 네 개의 상태와 5개의 사건으로 구성되어 있다. 먼저 상태에 대해 알아보면, W는 정상적으로 작동하여 기능을 수행할 수 있는 상태, U는 고장이 발생하여 기능을 수행하지 못하는 상태, D는 Proof Test를 통해 고장을 감지한 상태, 그리고 마지막으로 R은 수리되고 있는 상태에 해당한다. 토큰이 W에서 U로 이동하기 위해서는 두 사건 중 하나가 발생해야 한다. 하나는 공통원인고장이고 다른 하나는 개별원인고장이다. 공통원인고장은 외부 Petri Net Model로 표현되어 메시지를 통해 조건문으로 작동한다. ?Ccf는 Ccf=1이면 사건이 발생한다는 것을 의미하고, 외부 Petri Net Model을 살펴보면 공통원인고장의 발생 시간이 지수분포를 따른다고 되어 있으며, 고장이 발생하면 !Ccf라는 메시지를 통해 Ccf가 0에서 1로 바뀐다. 이후 조건문에 의해 센서의 상태가 W에서 U로 전이된다. 개별원인고장의 발생 시간은 지수분포를 따른다고 되어 있으며, 고장이 발생하면 센서의 상태가 W에서 U로 전이된다. 상태가 W에서 U로 전이될 때, !-S1이라는 메시지가 있어 S1이 1에서 0으로 바뀐다. 토큰이 W에서 U로 이동하기 위해서는 하나의 사건을 필요로 하며, 이는 고장을 감지하는 사건에 해당한다. 여기에서는 고장이 발생하면 바로 고장이 감지되어 상태가 W에서 D로 곧장 바뀌게 되는 것으로 되어 있다. 하지만 일반적으로 Proof Test 주기에 따라 검사를 수행할 때 고장이 감지되기 때문에 이에 대한 고려가 필요하다. 따라서 공통원인고장과 마찬가지로 외부 Petri Net Model을 통해 조건문을 통해 사건이 발생하는 것으로 모델링할 수 있다. 토큰이 D에서 R로 이동하기 위해서는 하나의 사건을 필요로 하며, 이는 수리를 시작하는 사건에 해당한다. 수리 시작은 수리작업을 수행하는 팀이 현재 작업이 가능한지의 조건문을 통해 사건이 발생한다. ??nbR>0이라는 메시지를 통해 현재 작업이 가능한 팀이 존재하는지 파악하여 만약 존재할 경우 바로 수리가 시작되며, !!nbR=nbR-1이라는 메시지를 통해 수리작업을 수행하는 하나의 팀이 작업에 투입되어 작업 가능한 팀의 수가 하나 줄어드는

것을 모델링하였다. 이후 토큰이 R에서 W로 이동하기 위해서는 수리 완료라는 사건을 필요로 하고, MRT만큼의 시간이 소요되면 수리 완료 사건이 발생하여 센서의 상태가 기능 수행이 가능한 상태로 전이된다. Logic Solver와 밸브의 Petri Net Model도 센서와 크게 다르지 않게 구성되어 있기 때문에 설명을 생략하도록 한다. 1oo2로 구성된 밸브에 대해서 기존 Petri Net Model을 Fig. 3-38로 나타내어 Reliability Block Diagram Driven Petri Net으로 보다 간단히 모델링이 가능하다는 것을 보여주었다.

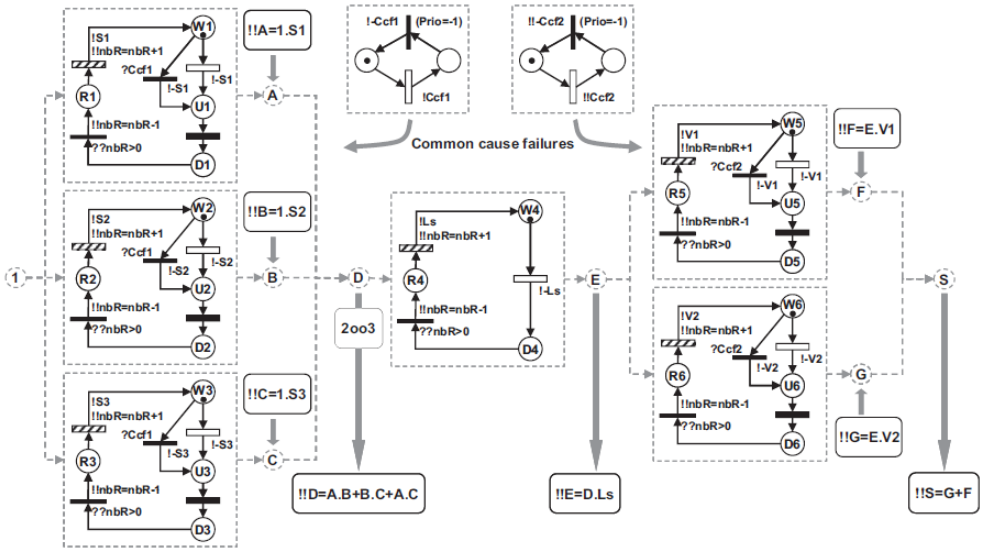

Figure 3-37 Reliability Block Diagram Driven Petri Net(Signoret, 2012)

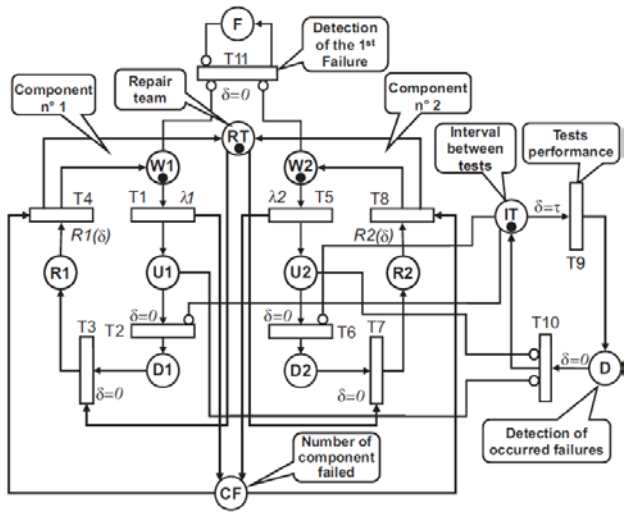

Figure 3-38 Petri Net Model for 1oo2 Valve Group(Signoret, 2012)

이제 비상분리시스템에 대해 Reliability Block Diagram Driven Petri Net을 모델링하였다. Signoret(2012)이 제시한 개념을 바탕으로 모델링을 수행하였고, IEC의 권고에 따라 Monte-Carlo Simulation을 통해 해석을 수행하였다. 비상분리시스템의 신뢰성블록선도는 Fig. 3-28로 제시하였고, 각 구성 요소에 대해 Fig. 3-39와 같이 Petri Net Model을 만들었다.

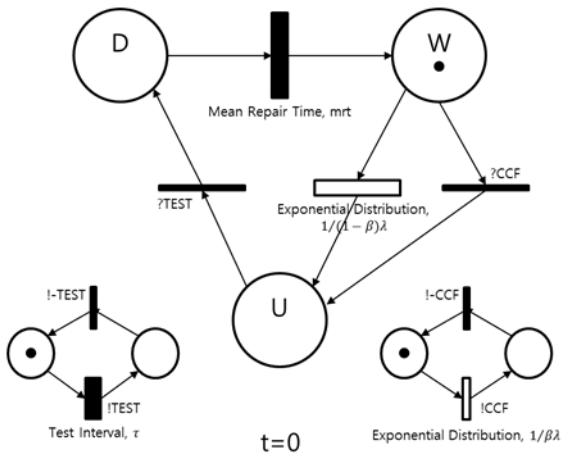

Figure 3-39 Petri Net Model for Each Component of Emergency Disconnect System

상태는 3개로 구성되어 있으며, W는 정상적으로 기능을 수행할 수 있는 상태, U는 기능을 수행할 수 없는 상태, 그리고 D는 고장이 감지된 상태에 해당한다. Signoret(2012)이 안전계장시스템을 모델링 한 것과는 다르게 외부 Petri Net Model을 통해 Proof Test주기를 고려하였으나, 수리작업을 수행하는 팀에 대한 고려는 배제하였다. Proof Test 주기를 고려하기 위한 외부 Petri Net Model에 대해서 간단하게 설명하자면, 외부 Petri Net Model은 Proof Test주기(τ)만큼의 시간이 지나면 감지 완료 사건이 발생하여 !TEST를 통해 TEST의 값이 0에서 1로 바뀐다. 이후 ?TEST라는 메시지로 TEST값이 1이 바뀌는 것을 확인하면 고장을 감지하는 사건이 발생하여, 구성 요소의 상태가 고장이 감지된 상태로 전이된다. 공통원인고장과 개별원인고장은 β요소 모델을 통해 모델링되었으며, Simplified Formulas와 IEC Formulas와 같이 β의 정의에 따라 고장 발생 시간에 대한 지수분포의 계수를 결정하였다.

해석은 Monte-Carlo Simulation을 통해 수행하였다. 다만 해석을 수행하는 과정에서 Signoret(2012)이 제안한 개념과 상이한 부분이 발생하였다. Signoret의 모델링 방법은 (1)부터 (S)까지의 모든 구성 요소에 대해 순차적으로 해석이 수행되어야 하기 때문에 해석에 많은 시간이 소요된다. 하지만 실제 시스템의 고장은 하나의 작은 기능을 수행하기 위해 koon으로 구성된 Group이 기능을 수행하지 못할 경우 발생하고, 따라서 순차적으로 (1)부터 (S)까지 진행될 필요 없이 Group이 기능을 수행하지 못하는 경우를 찾아 시스템의 고장을 발견할 수 있도록 해석을 수행하였다. 해석은 Matlab®을 수행하였고, Petri Net Model과 Monte-Carlo Simulation을 수행하는 과정이 Main코드에 포함되어 있으며 외부 Petri Net은 Function으로 구성하였다. Matlab® 코드는 부록에 수록하였다. Monte-Carlo Simulation 수행 횟수는 10^6번으로 하였을 때 값이 수렴하는 것을 확인하였고 그 결과 비상분리시스템의 고장 확률은 PFH 1.89E-07/hour에 해당하는 것을 확인하였다. 이는 앞서 근사식을 통해 검증을 수행한 결과와 거의 동일하며, 비상분리기능에 요구되는 PFH 2.71E-07/hour를 만족시키는 값에 해당한다. 구성한 비상분리시스템이 비상분리기능에 요구되는 안전무결성 수준을 만족시키는 것을 다시 검증하여 이전에 수행하였던 검증이 타당함을 보여주었다.

제 4 장 안전기능 요구사항 분석 및 검증

안전기능 요구사항은 제어되고 있는 장치의 안전을 보장하기 위한 안전기능 본연의 목적과 관계가 있기 때문에 안전기능마다 요구사항이 다르다. 에어백의 기능에 대한 안전기능 요구사항을 생각해보면 에어백의 기능을 사고가 발생하였을 때 사망사고를 방지하는 것으로 정의할 경우, 사고 발생 후 에어백이 작동하는데 소요되는 시간과 에어백의 높이 등 사망사고 방지와 직접적으로 관련된 사항이 안전기능 요구사항에 해당한다고 할 수 있다. OLF는 석유산업에 사용되는 안전관련시스템의 관리를 위해 IEC가 제시한 지침을 적용하는 방안을 제시하였지만, 안전기능 요구사항에 대해서는 따로 언급을 하고 있지 않다. 따라서 OLF의 접근 방안에 따라 안전무결성 요구사항과 관련된 연구들이 많이 수행되었지만 이와 함께 안전기능 요구사항을 다루는 경우를 찾아볼 수 없었다. 실제로 안전기능 요구사항과 관련된 연구는 역학적 지식을 기초로 하는 해석 및 검증이 주를 이루어, 안전기능 요구사항이라는 개념을 사용하지 않는다. 하지만 IEC의 지침에 따르면 안전무결성 요구사항과 안전기능 요구사항이 함께 고려되어야 하며, 이 안전무결성/안전기능 요구사항을 정리하여 하나의 시방서로 제출되어야 한다. 앞서 비상분리기능의 안전무결성 요구사항에 대해서 이미 살펴보았기 때문에 본 장에서는 비상분리기능의 안전기능 요구사항에 대해 분석하고, 이를 비상분리시스템에 할당하여 시스템을 구성하고, 해당 시스템이 비상분리기능의 안전기능 요구사항을 만족시킬 수 있는지 검증하였다. 이로써 비상분리기능에 대해 안전무결성/안전기능 요구사항의 분석 및 검증을 함께 살펴볼 수 있었다. 안전기능 요구사항의 검증에 대한 타당성 검토는 따로 수행되지 않았다.

제 1 절 안전기능 요구사항 분석

비상분리기능에 대해서는 반응시간(Response Time)이 가장 주요한 안전기능 요구사항에 해당한다. Drive-off 또는 Drift-off가 발생하면 Fig. 2-2와 같이 시간이 지남에 따라 시추리그가 규정된 위치에서부터 빠르게 벗어난다. 이에 시추리그가 Red Limit을 벗어나는 것을 확인한 작업자가 비상분리기능을 작동시키더라도 시추리그가

빠르게 움직여 기능이 완료되기 전에 Physical Limit에 도달하면 라이저와 유정헤드가 파괴되어 탄화수소 유출 사고가 발생할 수 있다. 즉, 작업자의 명령이 전달되어 원하는 장비를 통해 기능을 수행하는데 소요되는 시간으로 정의되는 반응시간 ⑨ 이 비상분리기능에서 가장 중요한 변수에 해당하는 것을 알 수 있다.

보퍼트 해(Beaufort Sea)에 사용될 시추리그에 대해 비상분리기능에 요구되는 반응시간을 직접 분석한 연구 사례가 존재한다. Imperial Oil사(2009)는 특정 환경 상황에서 Drive-off로 인한 시추리그의 움직임에 대해 해석을 수행하였다. 그리고 라이저 시스템을 구성하여 시추리그의 움직임에 따라 라이저 시스템의 각 구성 요소에 작용하는 하중을 분석하여 라이저 혹은 유정헤드가 파괴는 각도를 계산하였다. 이후 시추리그의 움직임에 따라 라이저 시스템의 각도가 어떻게 달라지는지 분석하여 모든 정보를 시간을 축으로 하는 하나의 그래프에 나타냈다(Fig. 4-1). Imperial Oil사(2009)는 해당 그래프를 통해 비상분리기능에 요구되는 반응시간을 분석하였고, 최소 반응시간으로 45초를 제시하였다.

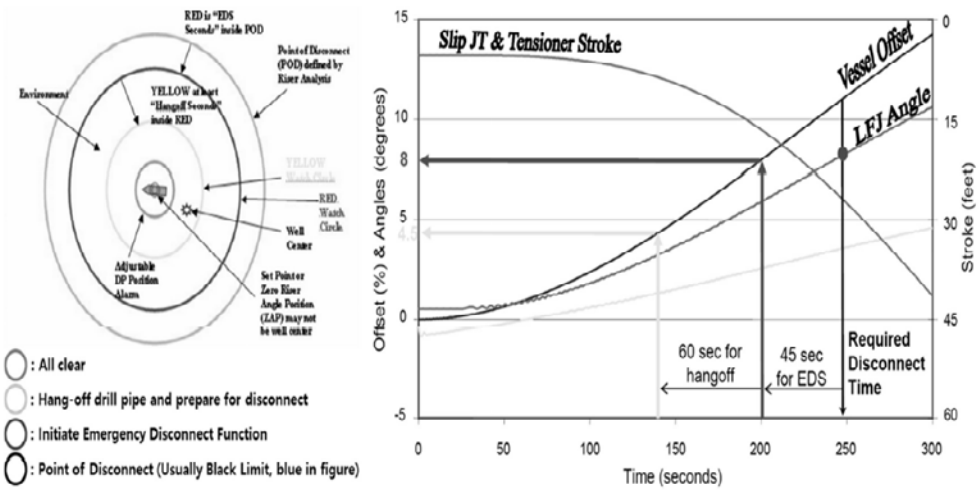

Figure 4-1 Description of Watch Circle and Drive-off Analysis of Vessel in Beaufort Sea (Imperial Oil, 2009)

⑨ ISO(2006)는 반응 시간을 플랫폼에 있는 작업자가 내린 명령이 해저에 위치한 장비까지 전달되는 시간에 해당하는 Signal Time과 전달된 명령에 따라 장비가 기능을 수행하는데 소요된 시간에 해당하는 shift time의 합으로 표현하였다. 즉, 반응 시간이란 작업자가 내린 명령이 실제로 이행되는 데 소요되는 시간이라 할 수 있다.

본 논문에서는 Drive-off 또는 Drift-off로 인한 시추리그의 거동을 분석하고, 라이저시스템에 대한 구조 해석을 수행하여 비상분리시스템의 최소 반응시간을 결정하는 것 대신 산업에서 주로 사용되는 기준을 따랐다. 시추산업에서는 미국석유협회인 API의 규정을 따르는 것이 가장 일반적이기 때문에 새롭게 개정된 API STANDARD 53(2012)를 참고하였다. API(2012)는 비상분리시스템의 최소 반응시간으로 90초를 제시하였다. 조금 더 세부적으로는 블라인드 전단 램 방지기로 유정을 폐쇄하는데 45초 그리고 LMRP 연결부로 LMRP를 분리하는데 45초를 최소 반응시간으로 제시하였다. 즉, 본 논문에서는 최소 반응시간 90초를 비상분리기능의 안전기능 요구사항으로 삼았다.

제 2 절 안전기능 요구사항을 고려한 시스템 구성

요구되는 최소 반응시간 90초 이내에 비상분리기능을 구현하기 위해 시스템을 구성하였는데, 주로 제 2장에서 살펴본 일반적인 비상분리시스템의 구성에 따르고 각 구성 요소의 제원을 결정하였다. 각 구성 요소의 제원을 결정하기 위해 시추리그의 환경 조건 및 운영 조건을 다음과 같이 가정하였다. 시추리그의 환경 조건으로 수심은 10,000 ft로, 그리고 지표면과 해저면의 온도를 각각 20 ℃와 1 ℃로 가정하였다. 유정헤드의 구경은 18 3/4 inch로, 그리고 비상분리시스템의 정격운전압력과 동작압력은 각각 15,000 psi와 5,000 psi로 가정하였다.

먼저 비상분리기능을 위해 필요한 장비에 해당하는 블라인드 전단 램 방지기, 초크 & 킬 밸브, LMRP연결부, 그리고 초크 & 킬 파이프 연결부의 제원을 해당 환경 조건과 운영 조건을 고려하여 결정하였다. 일반적으로 해당 장비는 제조업체에서부터 구매하기 때문에 제조업체의 카탈로그를 참조하였고, 유정헤드의 구경과 정격운전압력에 맞는 제품을 선별하여 제원을 파악하였다.

블라인드 전단 램 방지기는 Hydril사의 Conventional Ram BOP로 선정하였다. 블라인드 전단 램 방지기를 작동시키기 위한 유압유의 압력은 3,000 psi와 5,000 psi 중 선택이 가능하고, 열고 닫는 기능을 위해 Opening Port와 Closing Port에 유입되는 유압유의 부피는 각각 33.4 US gallon과 38.8 US gallon에 해당한다. Hydril사의 Conventional Ram BOP의 모습은 Fig. 4-2로 나타냈다. 피스톤 위치를 유지하기 위해 사용되는 MPL에 대해서는 따로 고려하지 않았다.

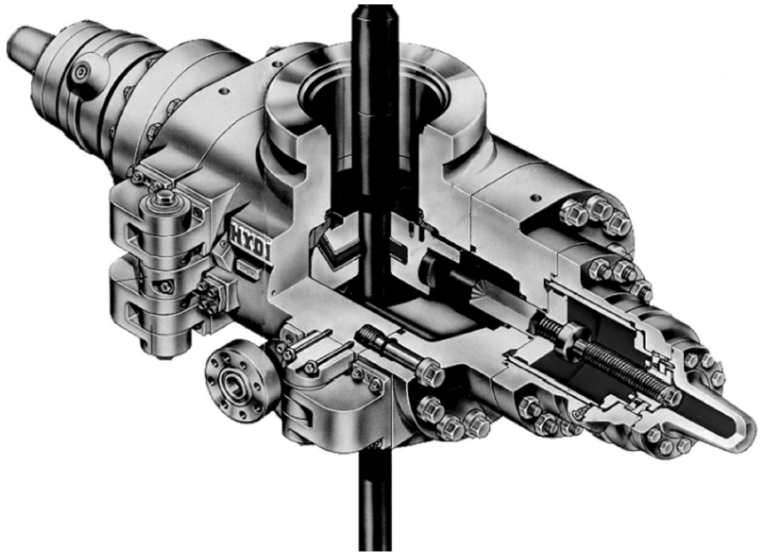

Figure 4-2 Conventional Blind Shear Ram Preventer (Hydril)

초크 & 킬 밸브는 Cameron사의 MCS Gate Valve로 선정하였다. 초크 & 킬 밸브를 작동시키기 위한 유압유의 압력은 1,500 psi와 3,000 psi 중 선택이 가능하고, 열고 닫는 기능을 위해 Opening Port와 Closing Port에 유입되는 유압유의 부피는 동일하게 0.75 US gallon 에 해당한다. Cameron사의 MCS Gate Valve의 모습은 Fig. 4-3으로 나타냈다. Fail-close기능을 구현하기 위해 스프링이 구비되어 있지만, 스프링에 대한 제원은 찾아볼 수 없었다.

Figure 4-3 MCS Gate Valve for Choke & Kill valve(Cameron)

LMRP연결부는 Cameron사의 DWHC Collet Connector로 선정하였다. LMRP연결부를 작동시키기 위한 유압유의 압력은 3,000 psi와 5,000 psi 중 선택이 가능하고, 결속하고 분리하는 기능을 위해 Unlatch Port와 Latch Port에 유입되는 유압유의 부피는 각각 12.1 US gallon과 15.1 US gallon에 해당한다. Cameron사의 LMRP연결부의 모습은 Fig. 4-4로 나타냈다. 비상시 더 높은 압력의 유압유를 사용하여 빠르게 결속하고 분리하기 위해 Secondary Port가 구비되어 있지만, 이에 대해서는 따로 고려하지 않았다.

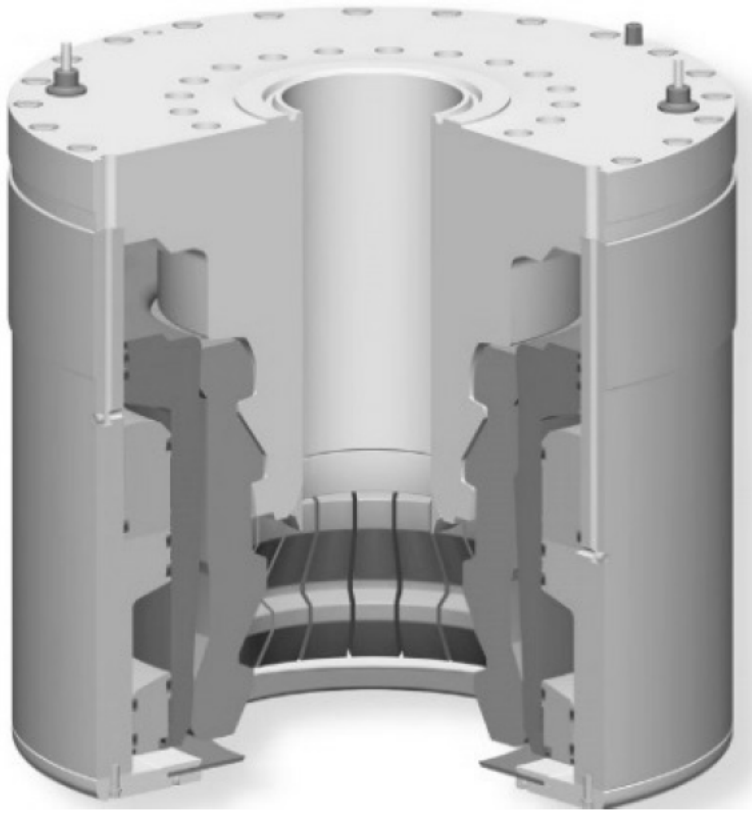

Figure 4-4 DWHC Collet Connector for LMRP Connector(Cameron)

초크 & 킬 파이프 연결부는 Radoil사의 Choke & Kill Connector로 선정하였다. 초크 & 킬 파이프 연결부를 작동시키기 위한 유압유의 압력은 1,500 psi와 3,000 psi 중 선택이 가능하고, 결속하고 분리하는 기능을 위해 Latch Port와 Unlatch Port에 유입되는 유압유의 부피는 동일하게 1 US gallon에 해당한다. Radoil사의 초크 & 킬 파이프 연결부의 모습은 Fig. 4-5로 나타냈다.

Figure 4-5 Choke & Kill Stab Connector(Radoil)

비상분리기능을 위해 필요한 장비에 해당하는 블라인드 전단 램 방지기, 초크 & 킬 밸브, LMRP연결부, 그리고 초크 & 킬 파이프 연결부의 제원을 환경 조건과 운영 조건을 고려하여 결정하였고, 이를 정리하여 Fig. 4-6과 같이 나타냈다. Fig. 4-6에는 Closing Ratio와 유압유 압력(Pressure to Close against RWP in Fig. 4-6)이 함께 기재되어 있다. 하지만 일반적으로 제조회사의 카탈로그에서 Closing Ratio가 기재되어 있는 경우는 드물기 때문에 그런 경우 API(2004)에서 권고한 바와 같이 Closing Ratio를 10으로 가정하였다.

Equipment	Bore Size (inch)	Rated Working Pressure (psi)	Operating Pressure (psi)	Opening (Unlatch) Volume (US gallon)	Closing (Latch) Volume (US gallon)	Closing Ratio (-)	Pressure to Close against RWP (psi)
Blind Shear Ram Preventer	18 3/4	15,000	3,000 & 5,000	33.4	38.8	7.27	2,459
Choke & Kill Valve	18 3/4	15,000	3,000 & 5,000	6(0.75×8)	6(0.75×8)	10	1,500
LMRP Connector	3 1/16	15,000	1,500 & 3,000	12.1	15.1	10	1,500
Choke & Kill Stab Connector	4 1/2	10,000	1,500 & 3,000	2(1×2)	2(1×2)	10	1,000
Total				115.4			

Figure 4-6 Specification of Emergency Disconnect System

Closing Ratio는 수식 피스톤 면적과 축 면적의 비로 정의되어 수식 (4-1)과 같이 계산된다. Closing Ratio는 정격운전압력에 대한 유압유의 압력을 결정하기 위해 필요한 값으로 수식 (4-2)와 같이 힘의 평형을 계산하는 과정에서 그 개념이 도입되었다. Closing Ratio를 통해 수식 (4-3)으로 유압유의 압력을 결정할 수 있다. 정격운전압력은 장비 내부 압력과 장비 외부 압력의 차로 정의되어 장비가 견딜 수 있는 최대 차압으로 정의된다. 따라서 Fig. 4-7과 같이 특정 장비의 구동부를 살펴보면 축의 왼쪽에는 정격운전압력이 작용하며, 축의 오른쪽에 위치한 피스톤에는 유압유의 압력으로 인한 힘이 작용한다.

$$Closing\ Ratio = \frac{Piston\ Area}{Piston\ Shaft\ Area} \tag{4-1}$$

$$Piston\ Area \times Hyraulic\ Pressure = Piston\ Shaft\ Area \times Rated\ Working\ Pressure \tag{4-2}$$

$$Hydraulic\ Pressure = Rated\ Working\ Pressure \div Closing\ Ratio \tag{4-3}$$

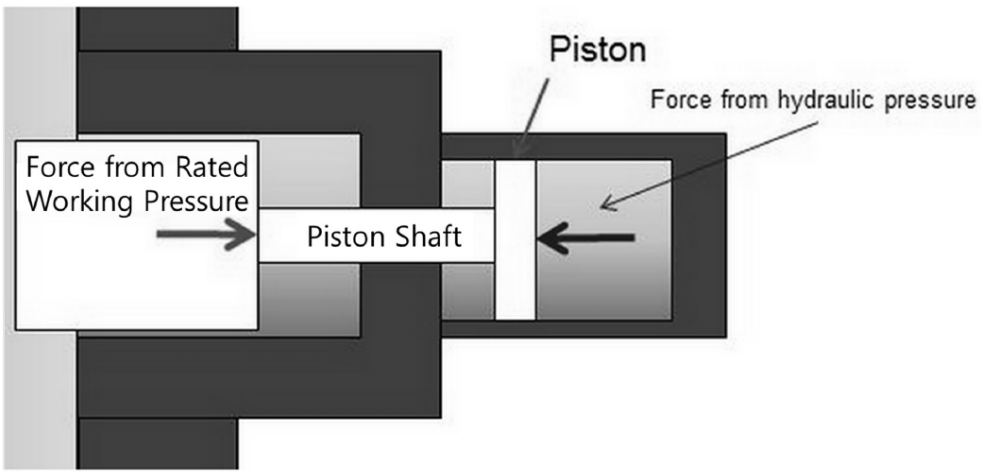

Figure 4-7 Forces on the Hydraulic Actuator

Fig. 4-6에서 초크 & 킬 밸브, LMRP연결부, 그리고 초크 & 킬 파이프 연결부의 유압유 압력은 수식(4-3)으로 계산되었지만, 블라인드 전단 램 방지기의 유압유 압력은 다르게 계산되었음을 확인할 수 있다. Fig. 4-8은 블라인드 전단 램 방지기에 작용하는 압력을 보여준다. Fig. 4-7과는 달리 해수의 압력을 고려하는 것을 확인할 수 있다. 하지만

Fig. 4-8의 3번이 유압유 압력에 정수압까지 고려하였기 때문에, 유압유의 정수압과 큰 차이가 없는 해수의 압력은 Fig. 4-7과 같이 생략이 가능하다. 또한 일반적으로 Housing이 되어 있는 경우에는 Fig. 4-8의 4번과 같이 해수의 압력이 작용하지 않아 생략이 가능하다. 다만 블라인드 전단 램 방지기의 유압유 압력 계산을 위해서는 Fig. 4-8의 1번과 같이 시추파이프를 전단하는데 필요한 압력을 추가적으로 고려해야 한다. 시추파이프를 전단하는데 필요한 압력을 계산하기 위해 Koutsolelos(2012)의 연구와 같이 구조해석을 바탕으로 한 학문적인 연구가 활발하게 이뤄지고 있지만, 실제 산업에서는 다양한 실험을 바탕으로 한 제조업체의 경험식이 사용된다. 따라서 블라인드 전단 램 방지기 제조업체로 유명한 Cameron, Varco Shaffer, 그리고 Hydril의 경험식을 조사하였다. Cameron사의 경우 Distortion Energy Theory를 기반으로 하는 경험식을 사용하는 것을 확인하였지만, Varco Shaffer와 Hydril은 어떤 식을 사용하는지 확인할 수 없었다. 이에 본 논문에서는 Hydril의 블라인드 전단 램 방지기를 사용하지만 계산식으로는 부득이하게 Cameron사의 경험식을 사용하였다. Cameron사에서 사용하는 경험식은 Fig. 4-9로 나타내지는 Distortion Energy Theory를 기반으로 한다. Cameron사의 경험식은 Fig. 4-10와 같다. 해당 식은 S-135 재질의 시추파이프를 전단하는데 필요한 압력을 계산하기 위한 것으로, 피스톤의 행정 길이에 따라 Fig. 4-10의 오른쪽 그래프와 같이 압력이 작용하는 것을 확인할 수 있다.

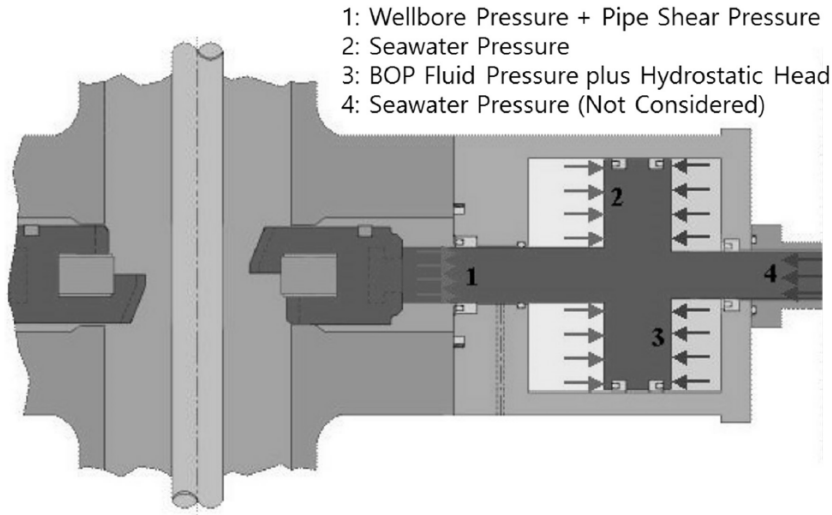

Figure 4-8 Pressures on Blind Shear Ram Actuator

Fig. 4-10으로 나타난 Cameron의 경험식에 따라 시추파이프 전단에 필요한 압력을 계산하기 위해 계산에 필요한 변수를 결정하였다. C_1은 379.6 inch^2, C_2는 52.2 inch^2, C_3는 0.23, P_W는 5,000 psi, Yield Stress는 135,000 psi, Outer Diameter(이하 OD)는 5.5 inch, 그리고 Inner Diameter(이하 ID)는 4.778 inch로 결정하였다. C_1과 C_2는 제조업체의 카탈로그에도 나와있지 않아 Fig. 4-10의 오른쪽 그래프와 같이 피스톤의 행정 길이를 11.8 inch로 하여 Closing Port와 Opening Port의 부피를 통해 C_1과 C_2를 결정하였다. C_3는 Cameron사에서 실험을 통해 제시한 수치에 해당하며, S-135 재질의 시추파이프를 사용하기 때문에 Yield Stress를 135,000 psi로 결정하였다. 유정의 압력은 5,000 psi로 가정하였고, 시추파이프의 OD와 ID는 일반적으로 시추 산업에서 사용되는 시추파이프의 제원으로 결정하였다. Fig. 4-10의 계산식에 각 변수의 값을 대입하여 시추파이프를 전단하는데 필요한 압력을 계산하였다. 계산 결과 시추파이프의 전단을 위해 2,459 psi의 압력이 필요하다는 것을 확인할 수 있었다.

$$F = 0.577 \times S_Y \times Are = 0.577 \times S_U \times Area$$

S_Y: drill pipe material yield strength

S_U: drill pipe material ultimate strength

$Area$: cross-sectional area of the drill pipe

Figure 4-9 Distortion Energy Theory for Drill Pipe Shearing

$$P_{Shear} = \frac{\left((C_3 * \sigma_{yield})(pipe_{OD}^2 - pipe_{ID}^2) * 2.92\right) + P_W * C_2}{C_1}$$

P_{shear}=calculated required operator pressure to shear (psi)
C_1=piston rod closing area (in^2)
C_2=piston rod opening area (in^2)
C_3=empirical constant obtained from laboratory testing
P_w=wellbore pressure at time of shear (only kick pressure, psi)
σ_{yield}=yield strength of the tubular material (psi)
$pipe_{OD}$=pipe/tube outside diameter ($inches$)
$pipe_{ID}$=pipe/tube inside diameter ($inches$)

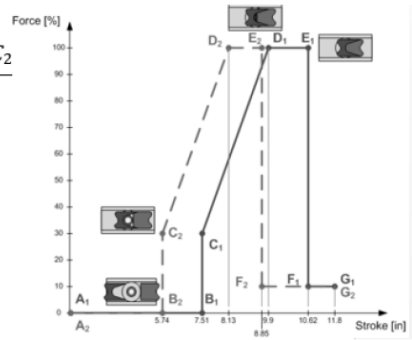

Figure 4-10 Drill Pipe Shearing Pressure Calculation Method (Agito AS, 2010)

비상분리기능을 수행하기 위해 필요한 MUX제어시스템은 Fig. 2-13의 기본 구성을 바탕으로 하고 주요 장비의 제원은 API

SPECIFICATION 16D(2004)에 따라 결정하였다. 앞서 제 2장에서 MUX제어시스템으로 장비를 구동하는 원리에 대해서 간단하게 소개한 바 있지만 다시 간단하게 살펴보도록 하겠다. MUX제어시스템은 작업자의 명령을 전기신호로 전달하여 해저의 솔레노이드 밸브를 작동시키고, 솔레노이드 밸브가 열리면서 축압기에 저장된 유압유가 장비에 유입되어 명령을 수행한다. 명령을 완수하고 난 이후에는 플랫폼으로부터 유압유를 공급받아 축압기를 채우고 다음 명령을 수행할 준비를 한다. 이처럼 해저에 위치한 축압기로 모든 기능이 수행되기 때문에 MUX제어시스템에서는 축압기의 제원을 결정하는 것이 가장 중요하다.

축압기는 일반적으로 LMRP와 Lower BOP Stack 두 곳에 위치한다. 위치에 따라 그 역할이 다른데, LMRP에 위치한 축압기는 유압밸브를 작동시키거나 환형(Annular) 방지기를 작동시키는데 사용되며 Lower BOP Stack에 위치한 축압기는 Lower BOP Stack에 있는 장비들을 작동시키는데 사용된다. 본 장에서는 Lower BOP Stack에 위치한 장비들을 작동시키는데 소요되는 시간을 검증하는 것이기 때문에 Lower BOP Stack에 위치한 축압기의 제원을 결정하였다.

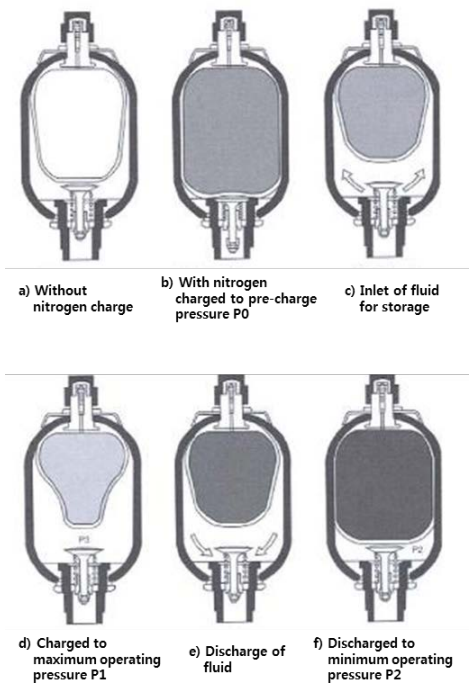

Figure 4-11 Accumulator Conditions

축압기는 용기에 높은 압력의 가스를 미리 채워서 고압 상태를 유지하여 충전된 유압유의 압력을 유지시킨다. 피스톤형, 다이아프램형, 그리고 블래더형 등 다양한 축압기가 존재하지만 MUX제어시스템에서는 일반적으로 블래더형 축압기가 사용된다. 축압기의 제원을 결정한다는 것은 축압기의 네 상태에 대해 정의하는 것이다. 유압유가 충전되기 전 고압의 가스만 존재하는 Pre-Charged, 유압유가 충전된 Charged, 유압유의 압력이 최소 동작 압력에 해당하는 Minimum Operating Pressure, 그리고 유압유가 완전히 빠져나간 Fully Discharge가 축압기의 네 상태에 해당한다(Fig. 4-11).

축압기의 제원을 결정하기 위해 API(2004)에서 제시한 방법론을 사용하였다. 이때, 수심이 10,000 ft일 때 정수압은 4,450 psi에 해당하기 때문에 Fig. 4-6의 유압유 압력과 정수압을 고려하면 축압기에 유입되는 유압유의 압력은 5,015 psi보다 큰 값에 해당한다. 따라서 해저 축압기의 제원은 API(2004)에서 제시한 방법론 중 Method B를 통해 결정된다(Fig. 4-12 & 4-13). Method B는 충전을 위해 사용하는 가스를 Real Gas로 가정하고, 가스의 팽창과 수축 과정을 Isothermal Process로 가정하는 방법론에 해당한다. 먼저 기능 수행을 위해 필요로 하는 유압유의 부피를 파악하여, Method B에 따라 Volume Efficiency를 계산하고 이를 통해 축압기의 제원을 결정하였다. Volume Efficiency를 계산할 때는 각 상태의 밀도를 필요로 하는데, 해당 값은 NIST 웹북(http://webbook.nist.gov/chemistry/fluid/)에서 Isothermal Process를 지정하여 Normal B.P. convention으로 해저면의 온도와 최소 동작 압력(Minimum Operating Pressure)[10]에서의 정보를 얻었다. 기능 수행을 위해 필요로 하는 유압유의 부피(Functional Volume Required, 이하 FVR)는 규정마다 다르지만, API(2004)에서는 비상분리기능을 위해 필요한 모든 장비를 결속하고(열고) 분리하는데(닫는데) 필요한 유압유의 부피로 정의하였다. Fig. 4-6에서 기능 수행에 필요한 장비의 제원을 참고하였고, 이후 모델링의 편의상 각 장비를 결속하고(열고) 분리하는데(닫는데) 필요한 유압유의 부피를 큰 값으로 동일하다고 가정하였으며, 따라서 FVR은 123.8 US gallon에 해당하였다.

[10] 축압기에서 내보내는 유압유의 최소 압력에 해당하는 값으로 각 장비를 작동시키기 위해 필요한 유압유의 압력 중 가장 높은 값에 정수압을 합한 값으로 선정하였다. 따라서 블라인드 전단 램 방지기를 작동시키기 위해 필요한 압력에 정수압을 합한 해당하는 6,924 psi가 최소 동작 압력에 해당한다.

Maximum gas pressure, psia	Surface systems			Subsea systems	
	Surface accumulators	Rapid discharge systems, such as dedicated shear system	Surface accumulator (including credit for any stack-mounted accumulators) for subsea systems	Main hydraulic supply supplement stack-mounted accumulator	Rapid discharge systems (e.g., autoshear, deadman) dedicated shear systems, and some acoustic and special-purpose accumulators
Functional volume requirements	5.1.4: Close one annular and all rams and open one side outlet line 5.1.5.1: twice pilot function volume needed to close all BOPs in the BOP stack 5.5.3: operate all of the divert mode functions	Volume and pressure requirement specified by purchaser. Usually 100% of function and required pressure times method design factor for volume.	5.2.3.1: Close and open one annular and four rams 5.2.3.2: pilot function volume needed to close and open one annular and four ram BOPs in the BOP stack 5.5.3: operate all of the divert mode functions	Volume and pressure requirement specified by purchaser. May be required in order to meet closing times if flow supply from surface is inadequate without added subsea supply.	5.8.2.2, 5.9.1: Volume and pressure requirement specified by purchaser. Usually 100% of function and required pressure times method design factor for volume.
< 5015 psia	Method A	Method C	Method A	Method A	Method C
> 5015 psia	Method B	Method C	Method B	Method B	Method C

Method A	Method B	Method C
ideal gas, isothermal	real gas, NIST data, isothermal	real gas, NIST data, adiabatic
1.5 volume design factor for volume-limited condition, F_v	1.4 volume design factor for volume-limited condition, F_v	1.1 volume design factor for both volume and pressure-limited conditions, F_v and F_p
1.0 volume design factor for pressure-limited condition, F_p	1.0 volume design factor for pressure-limited condition, F_p	

Figure 4-12 Accumulator Calculation Method Overview(API, 2004)

$$\boldsymbol{FVR = \min(BV_{surf} * VE_{v,surf} + BV_{sm} * VE_{v,sm}, BV_{surf} * VE_{p,surf} + BV_{sm} * VE_{p,sm})}$$

$$FVR = Functional\ Volume\ Required\ (given)$$

$$BV = Bottle\ Volume\ (find)$$

$$VE = Volumetric\ Efficiency\ (see\ below\ Table)$$

✓ Volumetric Efficiency

$$\boldsymbol{VE_p = (^{\rho_0}/_{\rho_2} - {}^{\rho_0}/_{\rho_1})/1.0}$$

$$\boldsymbol{VE_v = (1.0 - {}^{\rho_0}/_{\rho_1})/1.4}$$

✓ Optimum pre-charge density

$$\boldsymbol{\rho_0 = 1.0/(^{1.4}/_{\rho_2} - {}^{0.4}/_{\rho_1})}$$

Figure 4-13 Method B for Calculating Accumulator Specifications (API, 2004)

Method B를 통해 결정된 축압기의 제원을 Fig. 4-14으로 나타냈다. 앞서 언급한 바와 같이 네 상태에서의 충전 가스의 압력과 부피, 그리고 유압유의 부피가 결정되었다. 축압기 용기의 부피는 13.8 US gallon에 해당하여 FVR 123.8 US gallon을 확보하기 위해서는 70개의 축압기 용기가 필요하다. 즉, 70개의 축압기가 Lower BOP Stack에 위치하여 완전히 충전되었을 경우에 비상분리기능을 수행하기 위해 125.4 US gallon의 유압유를 공급할 수 있도록 Fig. 4-14와 같이 제원을 결정하였다.

Water Depth (ft)	Condition	Temperature (℃)	Gas Pressure (psi)	Gas Volume (gallon)	Hydraulic Fluid Volume (gallon)	Usable Volume (gallon)
10,000	Pre-Charged	1	6271.9	966.0	0.0	70 ea. of bottles
	Charged	1	9331.6	790.5	175.5	125.4
	Minimum Operating Pressure	1	6909.0	915.9	50.14	
	Fully Discharged	1	6271.9	386.4	0.0	>123.8

Figure 4-14 Subsea Accumulator Specification

만약 축압기 안의 유압유를 완전히 사용한 경우에는 제 2장에서 설명한 것과 같이 HPU로 유압유를 공급하여 축압기를 충전한다. API(2004)에 따르면 HPU는 두 대의 펌프(Primary Pump와 Secondary Pump)와 축압기, 그리고 패널로 구성되어 15분 이내에 해저에 위치한 축압기를 완전히 충전할 수 있어야 한다. 펌프는 해저로 제공되는 유압유의 압력이 작동 압력 5,000 psi보다 떨어질 때 작동을 시작하는데, Primary Pump는 작동 압력의 90%에 해당하는 4,500 psi에 작동을 시작하고 Secondary Pump는 작동 압력의 85%에 해당하는 4,250 psi에 작동을 시작한다. 그리고 Primary Pump는 작동 압력의 97%에 해당하는 4,850 psi에 도달하였을 때 작동을 멈추며, Secondary Pump는 작동 압력의 95%에 해당하는 4,750 psi에 작동을 멈춰 공급되는 유압유의 압력이 5,000 psi에 공급할 수 있도록 한다. 두 대의 펌프는 모두 25 US gallon/min의 유속으로 유압유를 공급하여 15분 이내에 해저에 위치한 축압기를 완전히 충전할 수 있도록 하였다. HPU 내부에 위치하는 축압기는 40 US gallon의 부피에 해당하는 축압기 용기 11개로 구성하였다. 이는 수심을 0으로 설정하였을 때, 비상분리기능을 위해 필요한 모든 장비를 결속하고(열고) 분리하는데(닫는데) 필요한 유압유의 부피를 FVR로 하여 API Method A로 결정하였다. 구성한 HPU가 해저에 위치한 축압기를 15분 이내에 완전히 충전시킬 수 있는지 SimulationX를 통해 살펴보았다. HPU는

ITI Subsea에서 제공하는 HPU모듈을 사용하여 모델링을 수행하였으며, 해저 축압기는 수직 블래더형 축압기 모듈을 사용하여, 그리고 HPU로부터 해저에 위치한 축압기까지 유압유를 전달하는 Rigid Conduit Line은 외경 3.5 inch와 내경 2.63 inch에 해당하는 파이프로 모델링하였다(Fig. 4-15). 모델링 이후 시뮬레이션을 수행하였고, 그 결과 15분 동안 HPU로 충전 가능한 유압유의 양은 128.7 US gallon에 해당하였고, 15분 이내에 기능 수행에 필요한 125.4 US gallon의 유압유를 충전할 수 있는 것을 확인하였다(Fig. 4-16). Fig. 4-16에 표시된 점선은 125.4 US gallon의 충전이 완료되는 시점에 해당한다.

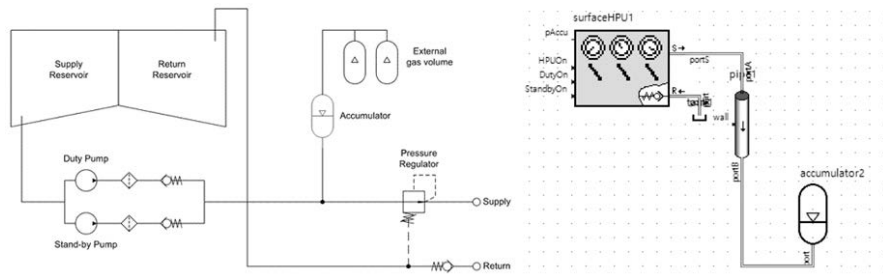

Figure 4-15 HPU Module and Model of Subsea Accumulator Charging System

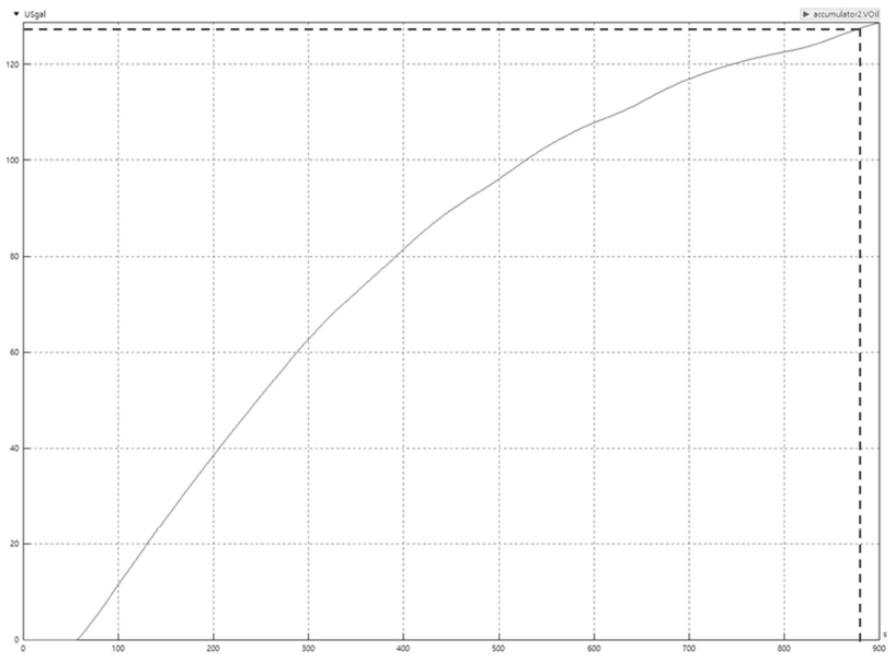

Figure 4-16 Simulation Result of Hydraulic Transmission from HPU to Subsea Accumulator

제 3 절 안전기능 요구사항 검증

제 2절에서 구성한 비상분리시스템이 비상분리기능의 안전기능 요구사항에 해당하는 최소 반응시간인 90초 이내에 기능을 수행할 수 있는지에 대해서 검증을 수행하였다. 검증은 유압제어시스템의 시간에 따른 거동을 분석할 수 있는 SimulationX를 통해 모델링 및 시뮬레이션을 수행한 결과를 바탕으로 이루어졌다. 모델링 및 시뮬레이션을 수행하기에 앞서 비상분리기능을 수행하기 위해 필요한 장비의 제원을 Fig. 4-17에 정리하였다. 모델링 및 시뮬레이션의 편의상 Fig. 4-6에서 각 장비를 결속하고(열고) 분리하는데(닫는데) 필요한 유압유의 부피를 큰 값으로 동일하다고 가정하였다.

EDS Equipment	Bore Size (inch)	Rated Working Pressure (psi)	Closing Volume (gallon)	Opening Volume (gallon)	Closing Ratio (-)	Pressure to Close Against RWP (psi)
LMRP Connector	18 3/4	15,000	15.1	15.1	-	1,500
Blind Shear Ram BOP	18 3/4	15,000	38.8	38.8	**7.27**	2,459
C & K Valve	3 1/16	15,000	0.75 (8 ea.)	0.75 (8 ea.)	-	1,500
C & K Connector	4 1/2	10,000	1.0 (2 ea.)	1.0 (2 ea.)	-	1,000
Total	-	-	61.9	61.9	-	2,459
			123.8			

Figure 4-17 Specification of Emergency Disconnect System Model

비상분리시스템의 MUX제어시스템의 구성을 위해 API(2004)에 따라 주요 장비의 제원을 결정하였고, Fig. 4-18과 같이 개요도로 정리하였다. 유압유가 이동하는 파이프라인의 제원은 Macondo 유전에 사용된 Deepwater Horizon BOP의 제원을 참고하였다(Agito AS, 2010). Fig. 4-18에는 HPU 내부에 위치한 파이프라인과 HPU부터 해저 축압기까지 연결하는 파이프라인의 제원이 기재되어 있지만, 해저에 위치한 축압기로 장비들이 작동하는 부분에 대해 모델링을 수행하였기 때문에 기재된 제원을 모델링에 반영하지 않았다. 해저에 위치한 축압기부터 각 장비의 구동부까지 연결하는 외경 3 inch와 1 inch의 Hose Line은 모델링에 반영되었다. 해저 축압기는 완전히 충전된 상태로 모델링되었다.

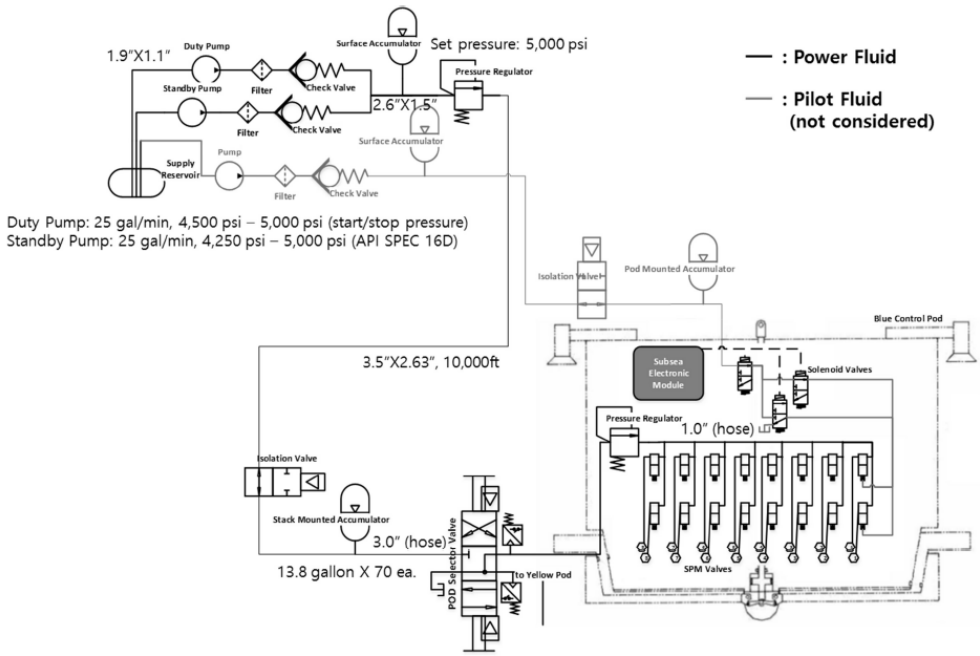

Figure 4-18 Schematic Diagram of Subsea Electro-Hydraulic Control for Emergency Disconnect System (Pipe & Hose Specification from Agito AS, 2010)

SimulationX를 통해 비상분리기능에 필요한 장비와 MUX제어시스템의 모델링을 수행하였다. 먼저 블라인드 램 방지기, 초크 & 킬 밸브, LMRP연결부, 그리고 초크 & 킬 파이프 연결부에 대해 모델링을 수행하였다. 블라인드 전단 램 방지기는 SimulationX내에 모듈이 따로 존재하지 않기 때문에 양로드형 실린더로 모델링하였다. Hydril사의 카탈로그에 기재된 폐쇄 용적과 개방 용적을 바탕으로 피스톤 행정 길이를 11.8 inch, 피스톤 직경을 23.45 inch로 가정하였다. 하나의 램 블록을 Mass로 모델링하였고 무게는 170 kg에 해당한다. 블라인드 전단 램 방지기에는 Fig. 4-19와 같이 파이프 전단력과 유압과 이수로 인한 감쇠력이 작용한다. 파이프 전단력은 외력으로 모델링하였고, 파이프를 전단하기 위해 필요한 압력과 압력이 작용하는 면적의 곱으로 전단력을 계산하였고, Fig. 4-10과 같이 피스톤의 행정 길이에 따라 전단력이 바뀌도록 모델링하였다. 유압과 이수로 인한 감쇠력은 Damper로 모델링하였고, 관련 정보를 구하기 어려워 SimulationX에서 Default로 사용하는 값을 그대로 사용하였다. 블라인드 램 방지기는 Fig. 4-20과 같이 모델링하였다. 피스톤 위치를 고정하는 MPL은 고려하지 않았다.

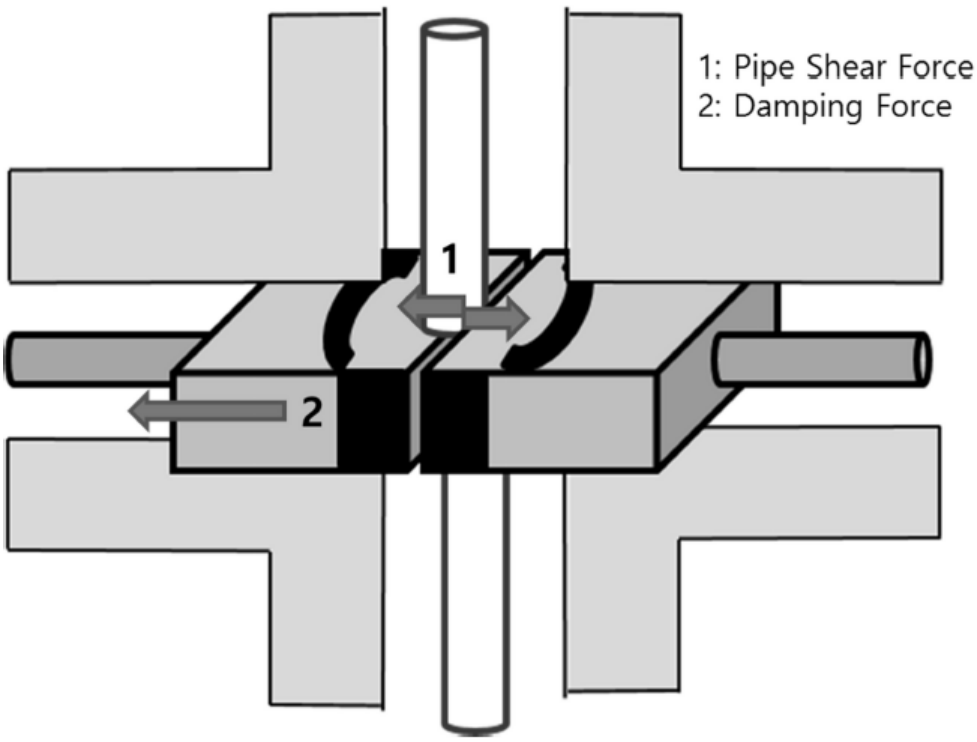

Figure 4-19 Forces on Blind Shear Ram Preventer

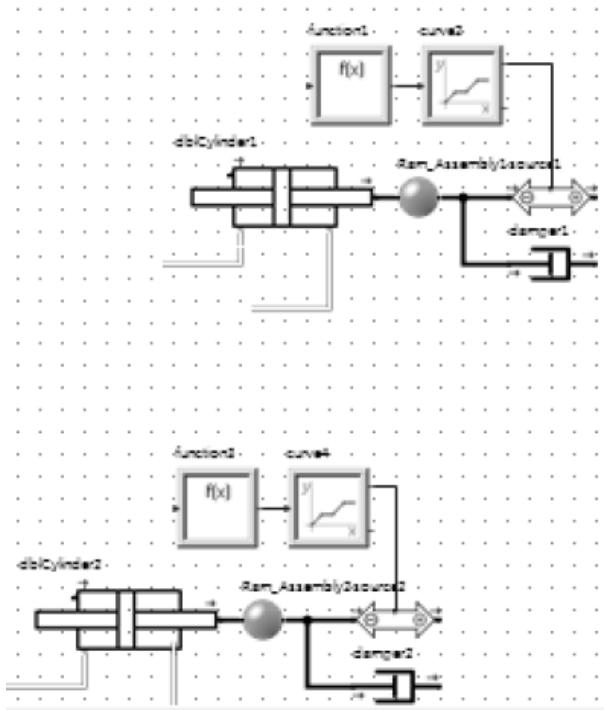

Figure 4-20 Blind Shear Ram Preventer Model

초크 & 킬 밸브는 SimulationX내에 존재하는 게이트 밸브로 모델링하였다. Cameron사의 카탈로그에 기재된 폐쇄 용적과 개방 용적을 바탕으로 피스톤 행정 길이를 7.992 inch, 피스톤 직경을 5.538 inch로 가정하였다. 스프링을 통해 Fail-close기능을 구현하였는데, 이때 스프링의 강도는 1100N/mm로 가정하였다. 초크 & 킬 밸브는 Fig. 4-21과 같이 모델링하였다. 두 개를 한 쌍으로 총 네 쌍의 초크 & 킬 밸브가 존재한다.

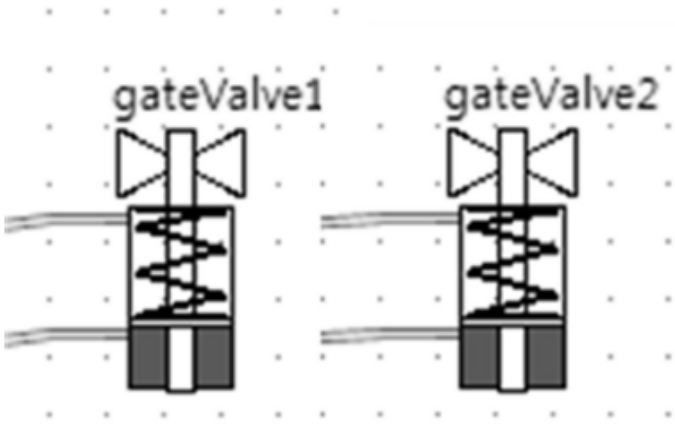

Figure 4-21 Choke & Kill Valve Model

LMRP연결부는 SimulationX내에 모듈이 따로 존재하지 않기 때문에 양로드형 실린더로 모델링하였다. Cameron사의 카탈로그에 기재된 폐쇄 용적과 개방 용적을 바탕으로 피스톤 행정 길이를 23.86 inch, 피스톤 직경을 14.38 inch로 가정하였다. LMRP연결부의 구동부는 실제로 Fig. 4-22의 왼쪽 그림에 나타난 것과 같이 환형으로 생겼다. 하지만 SimulationX에는 환형으로 생긴 구동부 모듈을 제공하지 않기 때문에 Fig. 4-22의 오른쪽 그림과 같이 양로드형 실린더로 모델링하였다. LMRP연결부를 결속하고 분리하기 위해 필요한 힘은 외력으로 모델링하였고 정격 운전 압력에 대해 필요한 유압유의 압력에 면적을 곱한 값으로 일정하게 존재한다. 감쇠력은 Damper로 모델링하였고, 관련 정보를 구하기 어려워 SimulationX에서 Default로 사용하는 값을 그대로 사용하였다. LMRP연결부는 Fig. 4-23과 같이 모델링하였다.

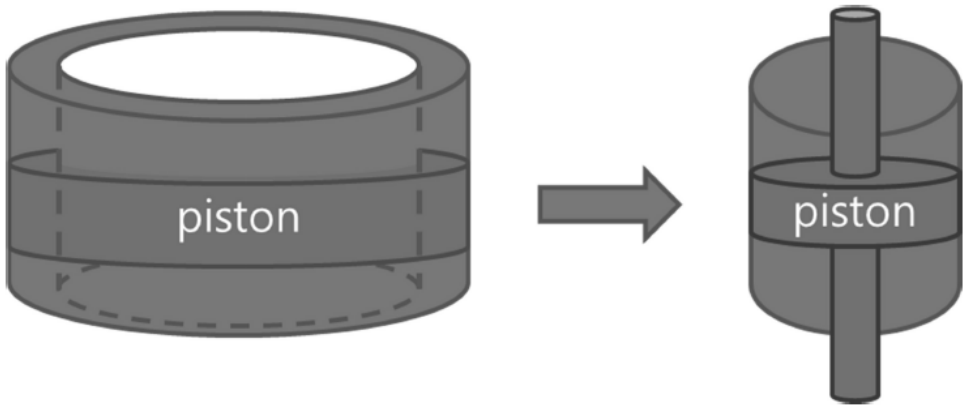

Figure 4-22 Concept of LMRP Connector Actuator Modeling

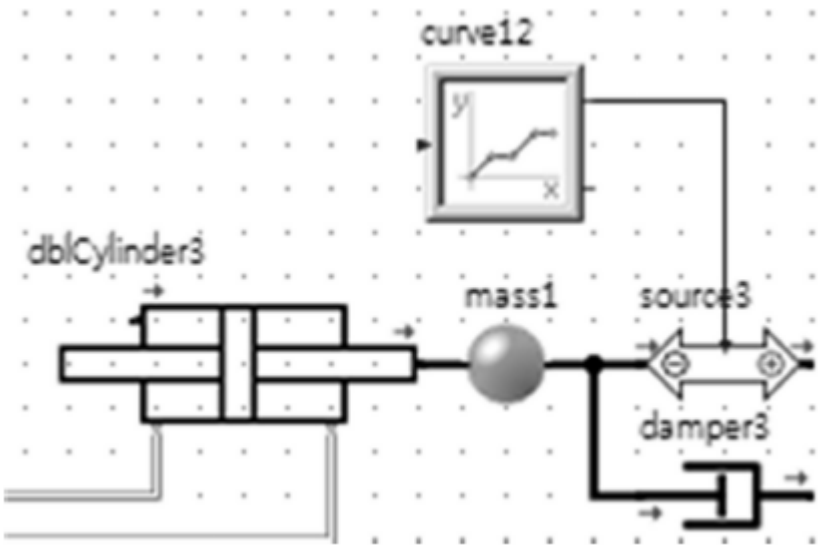

Figure 4-23 LMRP Connector Model

초크 & 킬 파이프 연결부는 SimulationX내에 모듈이 따로 존재하지 않기 때문에 양로드형 실린더로 모델링하였다. Radoil사의 카탈로그에 기재된 폐쇄 용적과 개방 용적을 바탕으로 피스톤 행정 길이를 27.43 inch, 피스톤 직경을 3.451 inch로 가정하였다. 초크 & 킬 파이프 연결부를 닫기 위해 필요한 힘은 외력으로 모델링하였고 정격 운전 압력에 대해 필요한 유압유의 압력에 면적을 곱한 값으로 일정하게 존재한다. 감쇠력은 Damper로 모델링하였고, 관련 정보를 구하기 어려워 SimulationX에서 Default로 사용하는 값을 그대로 사용하였다. Choke & Kill Stab Connector는 두 개가 한 쌍으로 존재하며 Fig. 4-23과 같이 모델링하였다.

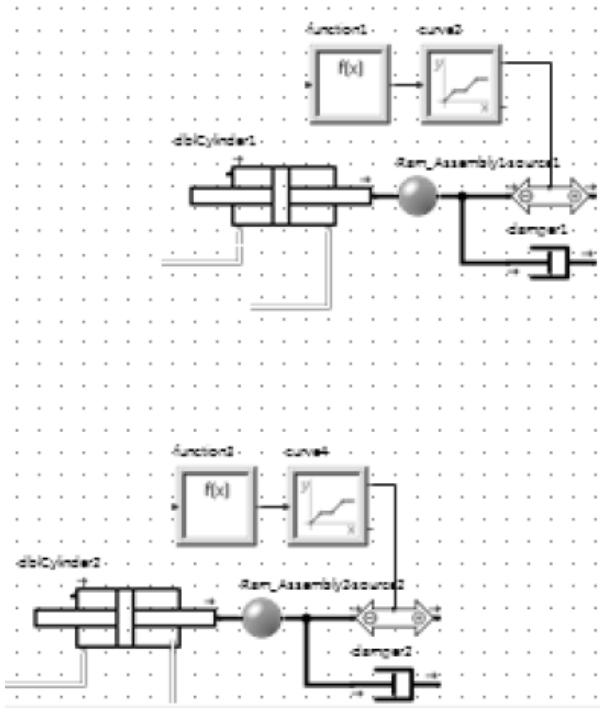

Figure 4-24 Choke & kill Stab Connector

MUX제어시스템의 경우 해저에 위치한 축압기로부터 기능 수행에 필요한 유압유를 공급받기 때문에 축압기에서부터 각 장비의 구동부까지 유압유를 공급하는 시스템을 모델링하였다. 축압기는 Fig. 4-14에서 완전히 충전되었을 때의 제원으로 모델링하였으며, 축압기로부터 각 장비의 구동부까지는 모두 외경이 1 inch에 해당하는 Hose로 모델링하였다. 모델링 결과는 Fig. 4-25로 나타내었다.

모델링을 마친 후 시뮬레이션을 통해 비상분리시스템의 반응시간을 분석하였다. SimulationX는 유압제어시스템의 모델링 및 시뮬레이션을 위한 것으로 작업자의 명령이 해저에 위치한 PLC에 전달되어 솔레노이드 밸브를 작동시키기 위한 전기·전자 제어시스템에 대해 고려하지 못하였다. Marine Technology Society(2012)에서 플랫폼에서부터 해저의 비상분리시스템까지 명령을 전달하는데 소요되는 시간을 알 수 없는 경우 10초로 가정하는 것을 권고하고 있기 때문에 전기·전자 제어시스템에 의해 소요되는 시간은 10초로 가정하였다. 즉, 10초부터 시뮬레이션이 시작될 때, 비상분리시스템의 반응시간을 계산

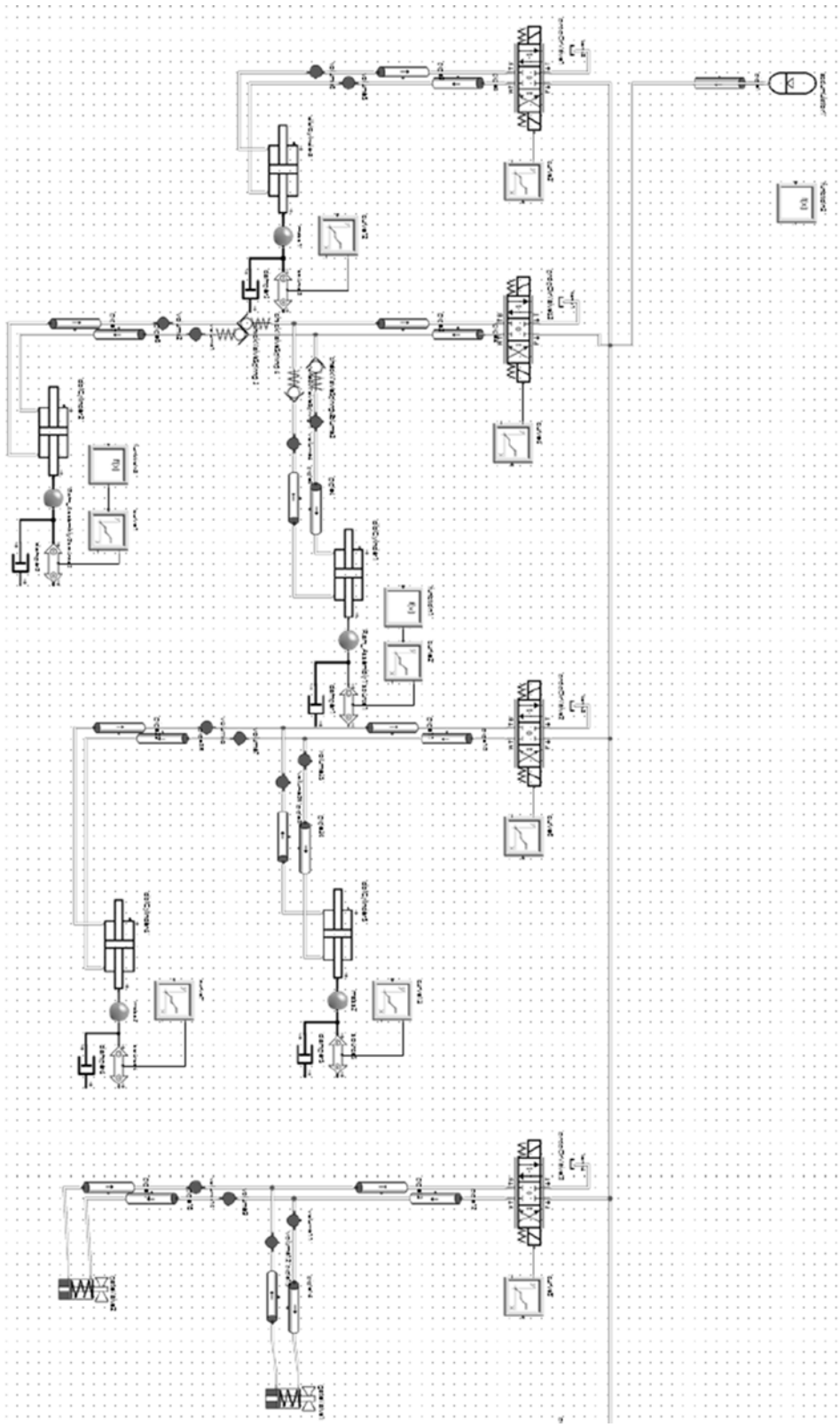

Figure 4-25 Emergency Disconnect System Model

였다. Fig. 2-5의 비상분리기능 절차에 따라 기능이 수행될 때, 유압제어시스템에 의한 반응시간은 43.16초로 계산되었다(Fig. 4-26). 전기·전자 제어시스템에 의해 소요되는 시간은 10초로 가정한다면 비상분리기능을 수행하는데 소요되는 시간은 총 53.16초에 해당하며 이는 안전기능 요구사항에 해당하는 최소 반응시간 90초보다 작은 값에 해당한다. 즉, SimulationX를 통해 비상분리시스템의 모델링 및 시뮬레이션을 수행한 결과 기능을 수행하는데 53.16초가 소요되어 안전기능 요구사항을 만족하는 것을 검증할 수 있었다. 안전기능 요구사항의 검증에 대한 타당성 검토는 따로 수행하지 않았다. 타당성 검토를 위해서는 시제품이나 모형에 대해 실험결과를 제출해야 하지만 본 논문에서는 따로 실험을 수행하지 않았다.

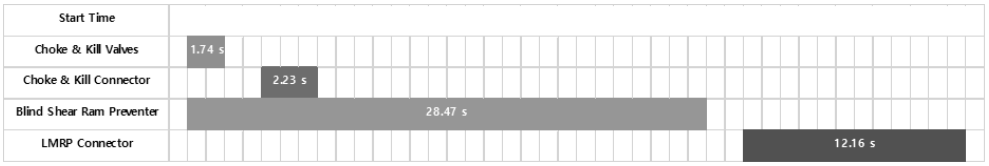

Figure 4-26 Response Time by Hydraulic Control System

제 5 장 결 론

안전계장시스템으로 구현되는 안전기능을 대상으로 하여 생애주기 동안 관리하기 위한 IEC의 지침을 조정시스템으로 구현되는 안전기능에 적용하기 위한 방안을 제시하였다. 그리고 이를 해양시추산업에서 사용되는 비상분리기능에 적용하여 라이저 또는 유정헤드의 기능적 안전을 보장하기 위해 비상분리기능에 요구되는 사항을 분석하고, 요구사항을 기능을 구현하기 위해 필요한 비상분리시스템에 할당하여 시스템이 할당된 요구사항을 만족시킬 수 있는지 검증하였다. 이때 비상분리기능의 안전요구사항은 안전무결성 요구사항과 안전기능 요구사항으로 분류하여 각각에 대해 제시한 방안에 따라 분석 및 검증을 수행하였다.

안전무결성 요구사항을 분석하기 위해 SINTEF에서 제시한 Environmental Risk Acceptance Criteria을 기준으로 삼아 요구되는 안전무결성 수준을 정량적으로 분석하였고, 비상분리시스템의 고장으로 인한 사고의 정보를 찾을 수 없어 중간 수준을 기준으로 삼았다. 이후 요구되는 안전무결성 수준을 만족시키기 위해 구조적 강건성을 고려하여 시스템을 구성하였고, 보편적으로 사용되는 세 가지 근사식을 통해 검증을 수행하여 구성한 비상분리시스템이 요구사항을 만족시키는 것을 확인하였다. 이 과정에서 조정시스템으로 구현되는 안전기능의 특성을 고려하여 위험상황을 감지하는 것부터 작업자의 명령으로 기능이 수행되기까지의 제어루프를 고려하여 연구를 수행하였다. 최종적으로는 개념적으로 제안된 Reliability Block Diagram Driven Petri Net을 사용하여 검증 결과의 타당성을 검토하였다. 이 과정에서 정보의 부족으로 인해 부득이하게 가정을 한 부분이 존재한다. 허용 가능한 위험도 수준과 몇몇 구성 요소의 β 값과 고장률이 그에 해당하는 것으로, 만약 관련 정보를 얻을 수 있었다면 보다 신뢰할 수 있는 결과를 도출할 수 있었을 것이라 생각한다.

비상분리기능을 수행하는데 소요되는 시간으로 정의되는 반응시간이 안전기능 요구사항에 해당한다. 이에 반응시간과 관련된 요구사항을 분석하였고, API(2012)에서 제시한 최소 반응시간을 안전기능 요구사항으로 삼았다. 이후 심해 시추 환경과 운영 조건을 가정하여 해당 환경과 조건에서 비상분리기능을 구현하기 위한 시스템을

구성하였다. 이후 SimulationX를 사용하여 모델링 및 시뮬레이션을 수행하였고, 그 결과 요구되는 최소 반응시간 이내에 비상분리기능을 수행할 수 있음을 검증하였다. 시추 장비와 관련 계산식에 대한 정보를 찾기가 어려워 가정 사항이 많았다. 마찬가지로 만약 관련 정보를 얻을 수 있었다면 보다 신뢰할 수 있는 결과를 도출할 수 있었을 것이라 생각한다. OLF의 지침에서 안전기능 요구사항에 대해 따로 언급이 없어 대다수의 연구가 안전무결성 요구사항에 대해서만 이뤄지는 상황에서 안전무결성 요구사항과 안전기능 요구사항을 함께 고려했다는 점에서 의미를 가질 수 있다고 생각한다.

본 논문은 조정시스템으로 구현되는 안전기능의 안전요구사항을 분석하고 검증하기 위해 안전계장시스템에 대해 확립되어있는 IEC의 지침을 적용할 수 있는 방안을 제시하였다. 뿐만 아니라 제시한 접근 방안을 비상분리기능에 적용하여 실질적인 적용 사례도 함께 제시하였다. 제시한 접근 방안은 대다수의 안전기능이 조정시스템으로 구현되는 석유산업에 폭넓게 적용될 수 있을 것으로 기대되며, 다른 산업에도 적용되어 안전성을 향상시키는데 도움이 될 수 있을 것이라 생각된다.

참고 문헌

Agito AS. (2010). “Hydraulic Analysis Deepwater Horizon BOP Control System ULTRADEEP”. BP Incident Investigation Report Appendix Z.

American Institute of Chemical Engineers. (2001). Layer of Protection Analysis.

American Petroleum Institute. (2004). Specification for Control Systems for Drilling Well Control Equipment and Control Systems for Diverter Equipment. API Specification 16D 2nd Edition.

American Petroleum Institute. (2010). Blowout Prevention Equipment Systems for Drilling Wells. API Standard 53 4th Edition.

Bai Yong. Bai. Chiang. (2012). Subsea Engineering Handbook. Elsevier.

Bakken Bjorn Inge. (2001). “Risk Associated with Drive-Off/Drift-Off when Drilling on DP”. Dynamic Positioning Committee.

Chen Haibo. (2008). Safety of DP Drilling Operations in the South China Sea.

EBrahimi Ali. (2010). Effect analysis of Reliability, Availability, Maintainability and Safety(RAMS) Parameters in design and operation of Dynamic Positioning(DP) systems in floating offshore structures. Master Thesis in KTH Royal Institute of Technology.

Eikekog Karl Henry. (2010). Master in Risk Management – Offshore Safety. Master Thesis of University of Stavanger.

EQE INTERNATIONAL. (2000). Risk Assessment of the Deepwater Horizon Blowout Preventer(BOP) Control System.

Hoekstra, B. (2005). Safety integrity – not only a matter of reliable hardware. Business Briefing: Exploration and Production: The Oil and Gas Review, 114-117.

http://webbook.nist.gov/chemistry/fluid/

http://drill-equip.com

http://radoil.com

Imperial Oil. (2009). Overview of Dynamic Positioning.

International Electrotechnical Commission. (1998). FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS. Part 1. General Requirements.

International Electrotechnical Commission. (1999). FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS. Part 2. Requirements for electrical/electronic/programmable electronic safety-related systems

International Electrotechnical Commission. (2002). LOW VOLTAGE SWITCHGEAR AND CONTROLGEAR. Part 5-4: Control circuit devices and switching elements - Method of assessing the performance of low energy contacts Special tests.

International Organization for Standardization. (2000). Petroleum and natural gas industries — Design and operation of subsea production systems — Part 6: Subsea production control systems.

International Organization for Standardization. (2008). Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design.

Januailham Yahya. (2012). Analysis of Component Criticality in the Blowout Preventer. Master Thesis in University of Stavanger.

Jossefsson. (2014). Improved DP System Failure Simulation for Drilling Riser Emergency Disconnect

Koutsolelos Evangelos. (2012). Numerical Analysis of a Shear Ram and Experimental Determination of Fracture Parameters. Master Thesis in Massachusetts Institute of Technology.

Marine Technology Society. (2012). DP Operation Guidance. Dynamic Positioning Committee.

National Commission. (2011). Macondo the Gulf Oil Disaster.

OLF. (2004). Application of IEC 61508 and IEC 61511 In thre Norwegian Petroleum Industry.

Pepperl-Fuchs. (2001). Manual Safety Integrity Level.

Rausand Marvin. (2014). Reliability of Safety-Critical Systems Theory and Applications. Wiley.

Signoret Jean-Pierre. (2012). “Make your Petri nets

understandable: Reliability block diagrams driven Petri nets". Reliability Engineering and Safety System.

SINTEF. (2010). Reliability Prediction Method for Safety Instrumented Systems. PDS Method Handbook 2010 Edition.

SINTEF. (2011). Barriers to prevent and limit acute releases to Sea. Environmental risk acceptance criteria and requirements to safety systems.

Transocean. (2011). Macondo Well incident. Transocean Investigation Report Volume 1.

West Engineering Services. (2003). Evaluation of Secondary Intervention Methods in Well Control.

WEST Engineering Services, (2009). Blow-out prevention equipment reliability joint industry project (Phase I –Subsea). Final report.

부 록

Reliability Block Diagram Driven Petri Net의 Matlab®코드를 수록하였다.

```
t=0;     %Global Time
t_end=175200;    %시스템의 수명
ts=10;    %time step

tau=160;

n_comp=24;    %component의 수
n_group=11;  %group의 수
t_base_if=zeros(1, n_comp); %개별 고장의 기준 시각
t_base_ccf=zeros(1, n_comp);     %공통 고장의 기준 시각

t_f=zeros(1, n_comp);    %component의 고장 발생 시각 저장

t_if=zeros(1, n_comp);  %개별 고장이 발생하는 시각
t_ccf=zeros(1, n_comp);     %공통 고장이 발생하는 시각
t_ccf_g=zeros(1, n_group);  %grooup별 공통 고장이 발생하는 시각

R=zeros(3, n_comp); %각 component의 reachability set
for i=1:1:n_comp
    R(1, i)=1;  %처음에는 모두 정상 상태
end

test=zeros(1, n_comp);
ccf=zeros(1, n_comp);

%Input Data
lambda=[1.00E-06       1.00E-06       1.60E-07       1.60E-07
4.80E-07     4.80E-07     1.60E-07     1.60E-07     5.00E-08
5.00E-08     4.00E-07     4.00E-07     1.60E-07     1.60E-07
```

```
4.80E-07    4.80E-07    4.80E-07    1.20E-06    1.20E-06
1.20E-06    1.60E-07    1.60E-07    1.60E-07    1.60E-
07];
beta=[0.03   0.03    0.05    0.05    0.05    0.05    0.05
0.05    0.03    0.03    0.03    0.03    0.05    0.05    0.05
0.05    0.05    0.05    0.05    0.05    0.05    0.05    0.03
0.03];
mrt=10*ones(1, 24);

n_f=0;  %시스템 고장횟수
pfh=0;
a=0;

%Monte-Carlo Simulationr
s=1E6;

for p=1:1:s
    %Monte-Carlo Simulation 시작
    %공통 고장이 발생하는 시각 계산
    t_ccf_g(1,   1)=t_base_ccf(1,   1)+random('exp',   1/(beta(1,
1)*lambda(1, 1)));
    t_ccf_g(1,   2)=t_base_ccf(1,   3)+random('exp',   1/(beta(1,
3)*lambda(1, 3)));
    t_ccf_g(1,   3)=t_base_ccf(1,   5)+random('exp',   1/(beta(1,
5)*lambda(1, 5)));
    t_ccf_g(1,   4)=t_base_ccf(1,   7)+random('exp',   1/(beta(1,
7)*lambda(1, 7)));
    t_ccf_g(1,   5)=t_base_ccf(1,   9)+random('exp',   1/(beta(1,
9)*lambda(1, 9)));
    t_ccf_g(1,   6)=t_base_ccf(1,   11)+random('exp',   1/(beta(1,
11)*lambda(1, 11)));
    t_ccf_g(1,   7)=t_base_ccf(1,   13)+random('exp',   1/(beta(1,
13)*lambda(1, 13)));
    t_ccf_g(1,   8)=t_base_ccf(1,   15)+random('exp',   1/(beta(1,
15)*lambda(1, 15)));
```

```
    t_ccf_g(1,  9)=t_base_ccf(1,  18)+random('exp',  1/(beta(1,
18)*lambda(1, 18)));
    t_ccf_g(1,  10)=t_base_ccf(1,  21)+random('exp',  1/(beta(1,
21)*lambda(1, 21)));
    t_ccf_g(1,  11)=t_base_ccf(1,  23)+random('exp',  1/(beta(1,
23)*lambda(1, 23)));

    t_ccf(1, 1)=t_ccf_g(1, 1);
    t_ccf(1, 2)=t_ccf_g(1, 1);
    t_ccf(1, 3)=t_ccf_g(1, 2);
    t_ccf(1, 4)=t_ccf_g(1, 2);
    t_ccf(1, 5)=t_ccf_g(1, 3);
    t_ccf(1, 6)=t_ccf_g(1, 3);
    t_ccf(1, 7)=t_ccf_g(1, 4);
    t_ccf(1, 8)=t_ccf_g(1, 4);
    t_ccf(1, 9)=t_ccf_g(1, 5);
    t_ccf(1, 10)=t_ccf_g(1, 5);
    t_ccf(1, 11)=t_ccf_g(1, 6);
    t_ccf(1, 12)=t_ccf_g(1, 6);
    t_ccf(1, 13)=t_ccf_g(1, 7);
    t_ccf(1, 14)=t_ccf_g(1, 7);
    t_ccf(1, 15)=t_ccf_g(1, 8);
    t_ccf(1, 16)=t_ccf_g(1, 8);
    t_ccf(1, 17)=t_ccf_g(1, 8);
    t_ccf(1, 18)=t_ccf_g(1, 9);
    t_ccf(1, 19)=t_ccf_g(1, 9);
    t_ccf(1, 20)=t_ccf_g(1, 9);
    t_ccf(1, 21)=t_ccf_g(1, 10);
    t_ccf(1, 22)=t_ccf_g(1, 10);
    t_ccf(1, 23)=t_ccf_g(1, 11);
    t_ccf(1, 24)=t_ccf_g(1, 11);

    %개별 고장이 발생하는 시각 계산
    for i=1:1:n_comp
        t_if(1,  i)=t_base_if(1,  i)+random('exp',  1/((1-beta(1,
```

```
i))*lambda(1, i)));
        t_f(1, i)=min(t_if(1, i), t_ccf(1, i));
    end
    if min(t_f)<t_end
        t=fix(min(t_f)/tau)*tau;
    else
        t=t_end;
    end
        while t<t_end
            for i=1:1:n_comp
                test(1, i)=Function_TEST(t, tau);
                ccf(1, i)=Function_CCF(t, t_ccf(1, i));
                [R(1, i), R(2, i), R(3, i)] = Comp_Reachability( t,
t_if(1, i), ccf(1, i), test(1, i), mrt(1, i) );

                if R(3, i)==1 && ccf(1, i)==0
                    t_base_if(1, i)=t+mrt(1, i);
                    t_if(1, i)=t_base_if(1, i)+random('exp', 1/((1-
beta(1, i))*lambda(1, i)));
                    t_f(1, i)=min(t_if(1, i), t_ccf(1, i));
                    a=1;
                end

            end

            if R(3, 1)==1 && ccf(1, 1)==ccf(1, 2) && ccf(1,
1)==1
                t_base_ccf(1, 1)=t+mrt(1, 1);
                t_base_ccf(1, 2)=t+mrt(1, 2);

                t_ccf_g(1, 1)=t_base_ccf(1, 1)+random('exp',
1/(beta(1, 1)*lambda(1, 1)));
                t_ccf(1, 1)=t_ccf_g(1, 1);
                t_ccf(1, 2)=t_ccf_g(1, 1);
                t_f(1, 1)=min(t_if(1, 1), t_ccf(1, 1));
```

```
            t_f(1, 2)=min(t_if(1, 2), t_ccf(1, 2));

            if min(t_f)<t_end
                t=fix(min(t_f)/tau)*tau-ts;
            else
                t=t_end;
            end
        end

        if R(3, 3)==1 && ccf(1, 3)==ccf(1, 4) && ccf(1,
3)==1
            t_base_ccf(1, 3)=t+mrt(1, 3);
            t_base_ccf(1, 4)=t+mrt(1, 4);

            t_ccf_g(1,    2)=t_base_ccf(1,    3)+random('exp',
1/(beta(1, 3)*lambda(1, 3)));
            t_ccf(1, 3)=t_ccf_g(1, 2);
            t_ccf(1, 4)=t_ccf_g(1, 2);
            t_f(1, 3)=min(t_if(1, 3), t_ccf(1, 3));
            t_f(1, 4)=min(t_if(1, 4), t_ccf(1, 4));

            if min(t_f)<t_end
                t=fix(min(t_f)/tau)*tau-ts;
            else
                t=t_end;
            end
        end

        if R(3, 5)==1 && ccf(1, 5)==ccf(1, 6) && ccf(1,
5)==1
            t_base_ccf(1, 5)=t+mrt(1, 5);
            t_base_ccf(1, 6)=t+mrt(1, 5);

            t_ccf_g(1,    3)=t_base_ccf(1,    5)+random('exp',
1/(beta(1, 5)*lambda(1, 5)));
```

```
            t_ccf(1, 5)=t_ccf_g(1, 3);
            t_ccf(1, 6)=t_ccf_g(1, 3);
            t_f(1, 5)=min(t_if(1, 5), t_ccf(1, 5));
            t_f(1, 6)=min(t_if(1, 6), t_ccf(1, 6));

            if min(t_f)<t_end
                t=fix(min(t_f)/tau)*tau-ts;
            else
                t=t_end;
            end
        end

        if R(3, 7)==1 && ccf(1, 7)==ccf(1, 8) && ccf(1,
7)==1
            t_base_ccf(1, 7)=t+mrt(1, 7);
            t_base_ccf(1, 8)=t+mrt(1, 8);

            t_ccf_g(1,    4)=t_base_ccf(1,    7)+random('exp',
1/(beta(1, 7)*lambda(1, 7)));
            t_ccf(1, 7)=t_ccf_g(1, 4);
            t_ccf(1, 8)=t_ccf_g(1, 4);
            t_f(1, 7)=min(t_if(1, 7), t_ccf(1, 7));
            t_f(1, 8)=min(t_if(1, 8), t_ccf(1, 8));

            if min(t_f)<t_end
                t=fix(min(t_f)/tau)*tau-ts;
            else
                t=t_end;
            end
        end

        if R(3, 9)==1 && ccf(1, 9)==ccf(1, 10) && ccf(1,
9)==1
            t_base_ccf(1, 9)=t+mrt(1, 9);
            t_base_ccf(1, 10)=t+mrt(1, 10);
```

```
                t_ccf_g(1,     5)=t_base_ccf(1,     9)+random('exp',
1/(beta(1, 9)*lambda(1, 9)));
                t_ccf(1, 9)=t_ccf_g(1, 5);
                t_ccf(1, 10)=t_ccf_g(1, 5);
                t_f(1, 9)=min(t_if(1, 9), t_ccf(1, 9));
                t_f(1, 10)=min(t_if(1, 10), t_ccf(1, 10));

                if min(t_f)<t_end
                    t=fix(min(t_f)/tau)*tau-ts;
                else
                    t=t_end;
                end
            end

            if R(3, 11)==1 && ccf(1, 11)==ccf(1, 12) && ccf(1,
11)==1
                t_base_ccf(1, 11)=t+mrt(1, 11);
                t_base_ccf(1, 12)=t+mrt(1, 12);

                t_ccf_g(1,    6)=t_base_ccf(1,    11)+random('exp',
1/(beta(1, 11)*lambda(1, 11)));
                t_ccf(1, 11)=t_ccf_g(1, 6);
                t_ccf(1, 12)=t_ccf_g(1, 6);
                t_f(1, 11)=min(t_if(1, 11), t_ccf(1, 11));
                t_f(1, 12)=min(t_if(1, 12), t_ccf(1, 12));

                if min(t_f)<t_end
                    t=fix(min(t_f)/tau)*tau-ts;
                else
                    t=t_end;
                end
            end

            if R(3, 13)==1 && ccf(1, 13)==ccf(1, 14) && ccf(1,
```

```
13)==1
                t_base_ccf(1, 13)=t+mrt(1, 13);
                t_base_ccf(1, 14)=t+mrt(1, 14);

                t_ccf_g(1,    7)=t_base_ccf(1,    13)+random('exp',
1/(beta(1, 13)*lambda(1, 13)));
                t_ccf(1, 13)=t_ccf_g(1, 7);
                t_ccf(1, 14)=t_ccf_g(1, 7);
                t_f(1, 13)=min(t_if(1, 13), t_ccf(1, 13));
                t_f(1, 14)=min(t_if(1, 14), t_ccf(1, 14));

                if min(t_f)<t_end
                    t=fix(min(t_f)/tau)*tau-ts;
                else
                    t=t_end;
                end
            end

            if R(3, 15)==1 && ccf(1, 15)==ccf(1, 16) && ccf(1,
16)==ccf(1, 17) && ccf(1, 15)==1
                t_base_ccf(1, 15)=t+mrt(1, 15);
                t_base_ccf(1, 16)=t+mrt(1, 16);
                t_base_ccf(1, 17)=t+mrt(1, 17);

                t_ccf_g(1,    8)=t_base_ccf(1,    15)+random('exp',
1/(beta(1, 15)*lambda(1, 15)));
                t_ccf(1, 15)=t_ccf_g(1, 8);
                t_ccf(1, 16)=t_ccf_g(1, 8);
                t_ccf(1, 17)=t_ccf_g(1, 8);
                t_f(1, 15)=min(t_if(1, 15), t_ccf(1, 15));
                t_f(1, 16)=min(t_if(1, 16), t_ccf(1, 16));
                t_f(1, 17)=min(t_if(1, 17), t_ccf(1, 17));

                if min(t_f)<t_end
                    t=fix(min(t_f)/tau)*tau-ts;
```

```
            else
                t=t_end;
            end
        end

        if R(3, 18)==1 && ccf(1, 18)==ccf(1, 19) && ccf(1,
19)==ccf(1, 20) && ccf(1, 18)==1
            t_base_ccf(1, 18)=t+mrt(1, 18);
            t_base_ccf(1, 19)=t+mrt(1, 19);
            t_base_ccf(1, 20)=t+mrt(1, 20);

            t_ccf_g(1,   9)=t_base_ccf(1,   18)+random('exp',
1/(beta(1, 18)*lambda(1, 18)));
            t_ccf(1, 18)=t_ccf_g(1, 9);
            t_ccf(1, 19)=t_ccf_g(1, 9);
            t_ccf(1, 20)=t_ccf_g(1, 9);
            t_f(1, 18)=min(t_if(1, 18), t_ccf(1, 18));
            t_f(1, 19)=min(t_if(1, 19), t_ccf(1, 19));
            t_f(1, 20)=min(t_if(1, 20), t_ccf(1, 20));

            if min(t_f)<t_end
                t=fix(min(t_f)/tau)*tau-ts;
            else
                t=t_end;
            end
        end

        if R(3, 21)==1 && ccf(1, 21)==ccf(1, 22) && ccf(1,
21)==1
            t_base_ccf(1, 21)=t+mrt(1, 21);
            t_base_ccf(1, 22)=t+mrt(1, 22);

            t_ccf_g(1,   10)=t_base_ccf(1,   21)+random('exp',
1/(beta(1, 21)*lambda(1, 21)));
            t_ccf(1, 21)=t_ccf_g(1, 10);
```

```
            t_ccf(1, 22)=t_ccf_g(1, 10);
            t_f(1, 21)=min(t_if(1, 21), t_ccf(1, 21));
            t_f(1, 22)=min(t_if(1, 22), t_ccf(1, 22));

            if min(t_f)<t_end
                t=fix(min(t_f)/tau)*tau-ts;
            else
                t=t_end;
            end
        end

        if R(3, 23)==1 && ccf(1, 23)==ccf(1, 24) && ccf(1,
23)==1
            t_base_ccf(1, 23)=t+mrt(1, 23);
            t_base_ccf(1, 24)=t+mrt(1, 24);

            t_ccf_g(1,  11)=t_base_ccf(1,  23)+random('exp',
1/(beta(1, 23)*lambda(1, 23)));
            t_ccf(1, 23)=t_ccf_g(1, 11);
            t_ccf(1, 24)=t_ccf_g(1, 11);
            t_f(1, 23)=min(t_if(1, 23), t_ccf(1, 23));
            t_f(1, 24)=min(t_if(1, 24), t_ccf(1, 24));

            if min(t_f)<t_end
                t=fix(min(t_f)/tau)*tau-ts;
            else
                t=t_end;
            end
        end

        if a==1
            if min(t_f)<t_end
                t=fix(min(t_f)/tau)*tau-ts;
            else
                t=t_end;
```

```
                end
                a=0;
            end

            S=(R(3, 1)+R(3, 3))*(R(3, 2)+R(3, 4))+(R(3, 5)*R(3,
6))+(R(3,  7)+R(3,  9))*(R(3,  8)+R(3,  10))+(R(3,  11)+R(3,
13))*(R(3, 12)+R(3, 14))+((R(3, 15)+R(3, 16))*(R(3, 15)+R(3,
17))*(R(3, 16)+R(3, 17)))+(R(3, 18)*R(3, 19)*R(3, 20))+(R(3,
21)+R(3, 23))*(R(3, 22)+R(3, 24));

            if S>0
                n_f=n_f+1;
            end

            t=t+ts;
        end

    t=0;
    for i=1:1:n_comp
        t_base_if(1, i)=0;
        t_base_ccf(1, i)=0;
    end
    R=zeros(3, n_comp); %각 component의 reachability set
    for i=1:1:n_comp
        R(1, i)=1;  %처음에는 모두 정상 상태
    end
    pfh=pfh+n_f/t_end;
    n_f=0;
end
pfh_avg=pfh/s
```

Abstract

Analysis and Verification of Safety Requirements for Emergency Disconnect Function

Hyunjoon Nam
Naval Architecture and Ocean Engineering
The Graduate School
Seoul National University

In 1998, International Electrotechnical Commission suggested a guideline for a management of safety functions realized by safety instrumented systems during life cycles. After that, most of industries used IEC guideline to manage safety functions in their industries. In accordance with this tendency OLF, Norwegian Oil Institute, applied IEC guideline to oil industry. However, as most of safety functions in oil industry were realized by critical alarms and human intervention system, not safety instrumented system, they were not the intended target of IEC guideline. Therefore OLF introduced a concept of manual initiator function to regard a human intervention system as a safety instrumented system. However this concept might have a limitation that it could cover only some parts of control system. So this paper suggested a concept which could consider entire control loop of human intervention system and applied this concept to the emergency disconnect function used in offshore drilling industry. First of all, an analysis was conducted to clarify the safety requirements of emergency disconnect function. After that, emergency disconnect system was organized and safety requirements of emergency disconnect function was allocated to the organized system. Finally, verification was conducted to check

whether the organized emergency disconnect system could satisfy the requirements or not. Safety requirements were divided into safety integrity requirement and safety function requirement. To clarify safety integrity requirement for emergency disconnect function, Environmental Risk Acceptance Criteria which had been suggested by SINTEF was used. As a result, PFH 2.71E-07/hour was required as a safety integrity requirement and it was allocated to the emergency disconnect system. To meet the requirements structural robustness was considered and redundancies of each elements were decided. After that, with Simplified Method, IEC Formulas, and PDS Method verification was conducted. As the results were PFH 1.89E-07/hour, 1.92E-07/hour, and 1.83E-07/hour, it was verified that organized emergency disconnect system could satisfy required safety integrity. Finally, to validate the verification an analysis by Petri Net with Monte-Carlo Simulation was conducted and the result was PFH 1.89E-07/hour. With this result, verification was validated. As a safety functions requirement, there was a required time limit to perform emergency disconnect function after initiation by operators. The time limit was defined as a response time and API suggested 90 s as a minimum response time. With manufacturer's catalog, specification of equipment needed for emergency disconnect function was decided for assumed sea states and operating conditions. Specifications of main components in MUX control system form emergency disconnect system was also decided. After that, to verify the response time of emergency disconnect system modeling and simulation was conducted and the result was 53 s. With this result, it was verified that organized emergency disconnect system could satisfy safety functions requirements. With this paper, a concept to consider entire control loop of safety functions which was realized by a human intervention system was suggested and the application of suggested concept was also suggested. This will be used widely in oil industry where most of safety functions are realized by human intervention systems and also can be applied to other industries. Improvements of the safety in industries can be expected with this

paper.

Keywords : Emergency Disconnect Function, Safety Requirements, Safety Integrity, Response, Petri Net, SimulationX
Student Number : 2013-21067