JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 18, No. 2, pp. 393-401, Apr. 2017

항해장비 소프트웨어 기능안전성 확보를 위한 위험분석 단계 연구

임 상 우[1] · 이 서 정[2*] · 양 회 석[3]
[1]한국해양대학교 대학원 컴퓨터공학과
[2]한국해양대학교 해사IT공학부
[3]㈜나이스컨설팅

Study on Risk Analysis for Software Functional Safety of Marine Navigational Equipment

Sang-Woo Lim[1] · Seojeong Lee[2*] · Hoi-seok Yang[3]

[1]Department of Computer Engineering Graduated school of Korea Maritime and Ocean University, Busan 606-791, South Korea

[2*]Department of Maritime IT, Korea Maritime and Ocean University, Busan 606-791, South Korea
[3]Nice Consulting Co Ltd, Seoul Yeongdeungpo-gu Kyounginro 775, South Korea

[요 약]

각 산업분야에 사용되는 시스템의 소프트웨어 비중이 늘어남에 따라 소프트웨어 안전성과 관련된 사고가 증가하고 있다. 철도, 항공, 의료 등의 주요 산업분야에서는 이를 해결하기 위해 IEC 61508 기반의 안전표준을 작성하여 따르는 것을 권고하고 있다. 항해 장비분야에는 안전표준이 마련되어 있지 않아 기능안전에 대한 확인을 위해 적절한 가이드가 필요하다. 본 논문에서는 정보통신산업진흥원의 기능안전성 공통 개발 가이드를 참고하여 항해 장비의 소프트웨어 기능안전성 확보를 위한 위험분석 단계의 절차와 산출물을 정의하였다. 선박에 탑재하여 수심을 측정하는 음향측심기를 대상으로 사례 연구를 하였다.

[Abstract]

As the importance of software in various industry areas has been increased, the number of accidents related to software safety are growing up. The key industries such as railroads, aviation and medicine, recommend IEC 61508 and international safety standards for their own to achieve functional safety and reduce the issues caused by that. For equipment of ship navigation, there are not any particular standards or guidance which Korean users can introduce as considering software functional safety. This article defines the procedure and outcomes of the risk analysis in order to secure software functional safety in marine navigational equipment and applies them to an echo sounder as a case study.

색인어 : 기능안정성, 위험분석, 소프트웨어 발전과정, 네비게이션 소프트웨어 품질보증

Key word : Functional safety, Risk analysis, Software development process, E-navigation software quality assurance, Eocho sounder

http://dx.doi.org/10.9728/dcs.2017.18.2.393

Received 20 March 2017; **Revised** 19 April 2017
Accepted 25 April 2017

***Corresponding Author; Seojeong Lee**

Tel: +82-051-410-4578
E-mail: sjlee@kmou.ac.kr

Ⅰ. 서 론

해양분야의 사용자들에게 좋은 품질의 소프트웨어와 사용하기 편한 시스템을 제공하기 위해 e-Navigation 소프트웨어 품질 보증을 강조하고 있다. 2015년 6월 MSC(Maritime safety Committee) 95차 회의에서 SQA(Software Quality Assurance)/HCD(Human Centred Design) 통합 가이드라인을 표준 문서로 최종 승인하였다[1]. 이 문서에는 시스템 품질 요소 중의 하나로 기능안전성을 언급하고 있다. 일반적으로 기능안전성 확보하기 위해서는 IEC 61508:2010 (Functional Safety of Electical / Electronic / Programmable Electronic safety – related systems)와 산업분야별 정의된 특정 표준을 따르는 것을 권장하고 있다.

IEC 61508은 모든 종류의 산업에 기능안전성을 적용하기 위한 국제표준으로 소프트웨어의 기능에 위험이 생기거나 사고가 날 염려로부터의 자유를 소프트웨어의 기능안전성으로 정의하고 있다[2]. 다양한 분야에서 IEC 61508을 기반으로 하는 안전 표준을 작성하여 기능안전, 신뢰성, 품질 및 성능에 대한 검증을 요구하고 있다[3][4]. 그림 1은 각 산업분야에서 준수해야 하는 기능안전성 표준을 나타낸다[5]. 하지만 해양분야는 기능 안전 관련 표준이 아직 마련되어 있지 않다.

소프트웨어의 기능안전성을 확보하기 위해서는 소프트웨어의 기능/비기능 요소가 시스템에 미치는 영향을 파악하고 요소로 인해 발생하는 사고의 비중을 분류하고 평가해야 한다. 소프트웨어 위험분석 프로세스는 기존의 개발 생애주기의 요구분석 단계이전에 실시되어 분석된 위험요소들을 시스템에 적절하게 반영해야 한다.

본 논문에서는 항해장비의 소프트웨어 기능안전성 확보를 위해 위험분석을 포함한 소프트웨어 요구분석 프로세스를 제시하며 항해 장비인 음향측심기를 대상으로 프로세스에서 수행하는 활동을 적용하고 도출되는 산출물의 템플릿을 나타낸다.

Ⅱ. 관련 연구

2-1 IEC 61508 (Functional Safety of E/E/PE – related systems)

IEC 61508의 정식명칭은 'E/E/PE 전자 안전 관리 시스템의 기능안전'이다. 모든 종류의 산업에 적용하기 위한 국제표준으로 안전생명주기, 하드웨어, 소프트웨어 등 3가지에 대한 안전성 구현방법 및 검증 방법을 제시하고 있다. Table 1은 IEC 61508의 구성을 나타내며 각 파트에 대한 설명은 다음과 같다.

- Part 0: 기능안전에 대한 일반적인 개념을 정의하고 각 Part의 개요 및 구성에 관하여 명시
- Part 1: 안전 수명주기에 따른 목적, 적용 범위, 입력 및 산출물을 명시함으로써 기능안전을 위한 전체 프레임워크를 정의
- Part 2: 안전제어 시스템에 요구되는 안전 요구사항을 결정하기 위한 다양한 기법의 적용 및 안전무결성 수준의 등급화에 관하여 명시
- Part 3: 안전제어 시스템을 개발하면서 하드웨어가 아닌 소프트웨어에 적용되는 안전기능과 안전무결성수준에 대하여 명시
- Part 4: IEC 61508에서 사용되는 용어 정의 및 설명
- Part 5: 리스크와 안전무결성의 개념에 대한 설명과 함께 두 개념 간의 관계를 명시하고 안전무결성을 결정할 수 있는 다양한 방법론들에 관하여 명시

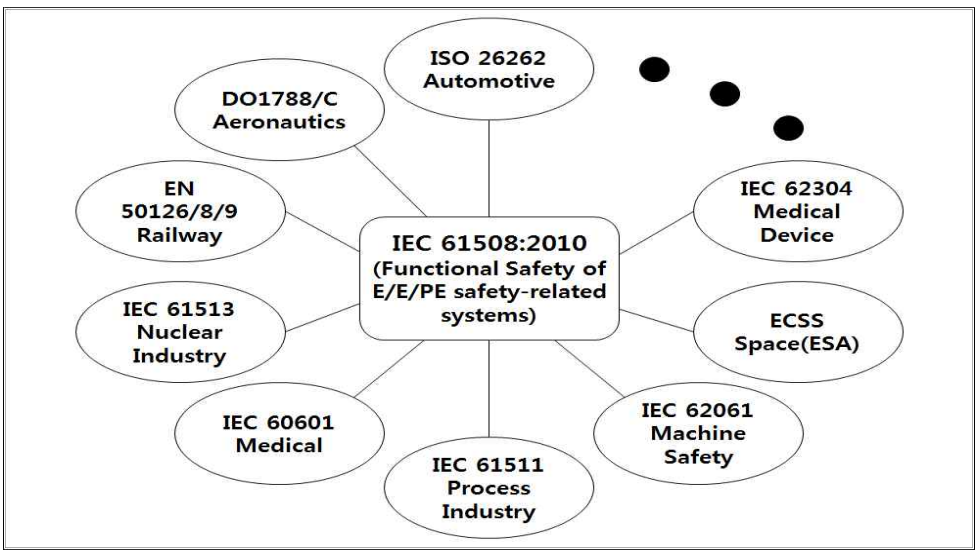

그림 1. E/E/PE 안전관련시스템의 기능안전성
Fig. 1. Functional Safety of E/E/PE safety-related system

표 1. IEC 61508의 구성
Table 1. Configuration of IEC 61508

구분	구성
Part 0	기능안전성과 IEC 61508
Part 1	일반 요구사항
Part 2	E/E/PE 가능한 전자장치 안전 관련 시스템의 요구사항
Part 3	소프트웨어 요구사항
Part 4	정의와 약어
Part 5	안전무결성수준 결정 방법의 예
Part 6	IEC 61508의 Part 2와 Part 3의 적용 지침
Part 7	기법과 수단의 개요

- Part 6: Part 2와 Part 3 적용의 기능적 단계와 두 가지 작동 모드에서의 하드웨어 고장 확률 평가 기법, 진단 범위 및 안전 고장비율 계산 예시 및 소프트웨어 안전무결성에 관하여 명시
- Part 7: Part 2 및 Part 3과 관련된 다양한 안전기법에 관한 설명을 제공함으로써 하드웨어 우발 고장에 대한 제어, 시스템 고장의 회피, 소프트웨어 안전무결성 달성을 위한 기법 및 방법 등을 명시

IEC 61508에서는 하드웨어와 소프트웨어에서 기능안전의 필요성과 필수항목을 제시하고 있지만 기능안전성을 확보할 수 있는 구체적인 방안은 제시하지 않고 있다. 철도, 항공, 의료 등 다양한 분야에서 IEC 61508을 기반으로 하는 안전 표준을 작성하여 소프트웨어 기능안전성을 확보하고 있으나 해양분야에는 아직 표준이 정해지지 않은 상태이다.

2-2 소프트웨어 안전성 공통 개발 가이드

IEC 61508에서는 기능안전성 확보를 위한 방법을 다루었지만 표준문서의 특성상 필요한 산출물만이 제시되어 있을 뿐 실행방법에 대한 명세는 작성되어 있지 않다. 미래창조과학부 산하 NIPA(National IT Industry Promotion Agency: 정보산업진흥원)에서는 기능안전성을 국내의 모든 분야의 소프트웨어에 도입하고자 소프트웨어 안전성 공통 개발 가이드라인을 개발하였다[6]. 소프트웨어 안전성 공통 개발 가이드라인은 현장에서 활용하기 위해 개념 제시 수준을 넘어 실제 실무에 활용할 수 있도록 구체적인 방안을 제시하였다[7]. 안전성 공통 개발 가이드라인에서는 소프트웨어의 신뢰・안전성 분석을 위해 검증된 분석기법을 사용하여 실무에서 활용 가능한 방안과 함께 관련 도구를 제시하고 있다. 위험을 분석하는 기법은 여러 가지가 존재하지만 HAZOP 기법은 귀납적 추론 방식에 기반을 두어 워크시트 작성을 통해 분석을 수행하는 기법으로 위험식별에 더욱 유용한 기법이다[3][8]. HAZOP 기법은 그림 2의 프로세스를 따르며 공정에 관련된 여러 분야의 전문가들이 모여서 설계

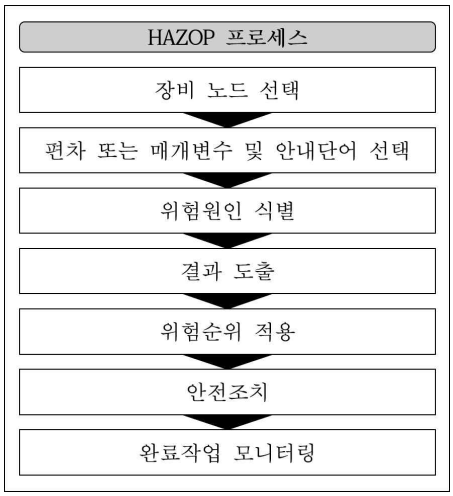

그림 2. HAZOP 프로세스
Fig. 2. Process of HAZOP

된 목적에 어긋나게 된 원인과 결과를 식별하고 위험에 야기되는 문제 가능성의 유무를 공정에 관련된 자료를 토대로 정해진 방법을 통해 파악한다.

2-3 해양분야 위험성 분류기준

HAZOP 기법은 회의를 통해 결과로 나타나기 때문에 명확한 수치로 값이 도출되기 어렵다. 따라서 정확한 결과를 위해서는 정량적인 값을 필수적으로 적용하여야 한다. 보편적으로 분류 단계를 정의하고 기준에 따라 도출된 사항들을 분류한다. 해양분야에서는 해양수산부에서 발간한 '해양 선박사고 위기관리 표준매뉴얼'에 명시된 4가지의 수준을 따르며 표 2는

표 2. 위험경보 수준 (해양 선박 사고)
Table 2. Degree of Hazard alert (Marine vessel accident)

분류	구분	내용
1	관심 (Blue)	징후가 있으나 그 활동수준이 낮으며 가까운 기간 내에 국가위기로 발전할 가능성도 비교적 낮은 상태
2	주의 (Yellow)	징후 활동이 비교적 활발하고 국가위기로 발전할 수 있는 일정 수준의 경향성이 나타나는 상태
3	경계 (Orange)	징후 활동이 매우 활발하고 전개속도, 경향성 등이 현저한 수준으로서 국가위기로의 발전 가능성이 농후한 상태
4	심각 (Red)	징후 활동이 매우 활발하고 전개속도, 경향성 등이 심각한 수준으로서 위기발생이 확실시 되는 상태

4가지의 수준과 각 수준에 따른 설명을 나타낸다[9]. 하지만, 이 분류사항들은 선박의 충돌, 접촉, 침몰, 화재 및 폭발 등으로 대규모의 사상자가 발생하거나 발생이 예상되는 시스템에 적용되는 사항들이기 때문에 소프트웨어의 규모에 맞게 수정이 필요하다.

Ⅲ. 본 론

소프트웨어는 자체만으로는 안전성 문제를 발생시키지 않고 하드웨어와 결합한 시스템에서부터 발생한다. 소프트웨어의 위험분석은 전체 시스템의 설계 맥락에서 수행되어야 하며 소프트웨어의 기능안전성은 하드웨어, 주변 환경, 사람 등을 고려해야 한다. 본 논문에서 제시하는 위험분석 활동은 위험도의 기준을 선정하고 각 위험요소를 위험도에 따라 분류하여 소프트웨어 요구분석에 적용하는 것을 목적으로 한다[10]. 그림 3은 위험분석 활동의 절차를 나타내며 각 절차가 완료된 후 나타나는 결과는 산출물로 도출되어야 한다.

3-1 위험요인 분석

1) 안내단어 정의

안내단어란 공정의 비정상적인 상태를 나타내며 HAZOP 회의를 위해 필요하다. 인터뷰, 브레인스토밍, 프로토타이핑 등을 통해 안내단어를 추출하고 추출된 요구사항들에 대한 제약 사항을 발견, 검토, 명확화하여 확정한다. 요구사항을 정의하기 위해 필수적으로 사용되며 여러 이해관계자들이 함께 선택해야 한다.

2) 위험발생원인 분석

위험발생원인 분석 단계에서는 확정된 요구사항에 영향을 끼칠 수 있는 요소들을 분석한다. 시나리오 분석, 작업 분석, 스토리보드, 벤치마킹, 구조적 분석, 유스케이스 기반 분석 등 다양한 분석 작업이 있으며 분석된 요구사항은 구조화하고 이에 대한 대안을 결정하는 과정까지 포함하여야 한다. 요구사항의 분석이 완료되면 각 안내단어의 원인을 명시하여 리스트를 도출한다.

3-2 위험결과분석 및 기준정의

1) 위험결과 분석

위험결과 분석 단계에서는 요구사항들에 대한 정의와 요소분석 완료 후에 나타날 수 있는 결과를 조사한다. 인적자원, 기계적 결함 등 시나리오가 진행될 때 나타날 수 있는 위험을 명세화한다. 위험요소는 비중이 큰 위험뿐만 아니라 사소한 위험들도 막대한 피해를 줄 수 있으므로 모든 위험요소를 포함하는 것이 중요하다.

2) 위험분류기준 정의

위험분류기준 정의 단계에서는 소프트웨어의 규모에 맞게 위험도를 정의한다. 위험기준은 1~5 또는 상~하 등급으로 정의하며 프로젝트의 HAZOP 회의를 통해 결정된다. 각 안내단어를 대상으로 위험의 발생빈도 및 영향을 근거로 하여 위험기준에 따라 위험도를 결정한다.

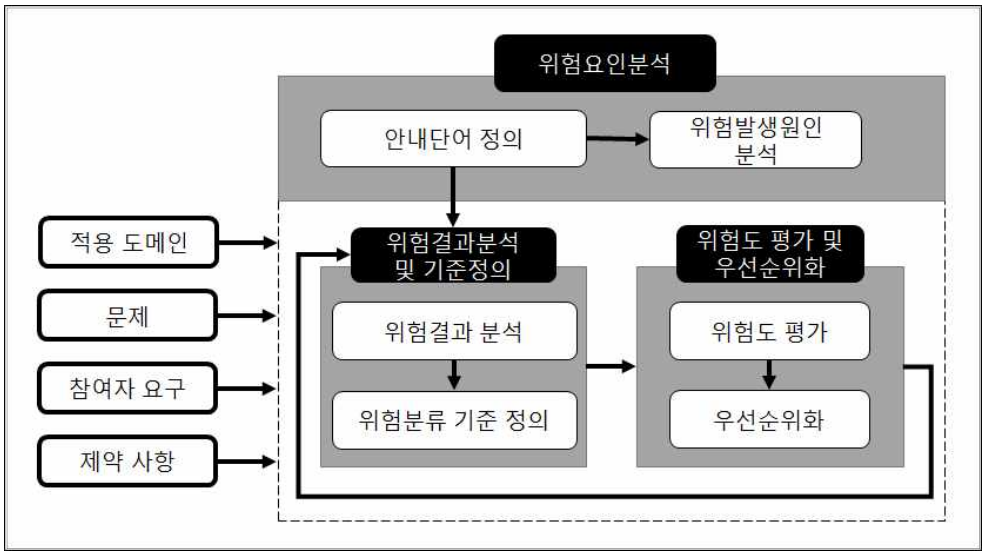

그림 2. HAZOP 프로세스
Fig. 2. Process of HAZOP

3-3 위험도 평가 및 우선순위화

1) 위험도 평가

위험도 평가 단계에서는 프로젝트의 위험도에 따라 분류된 위험요구사항의 위험도를 선정한다. 위험도를 선정함과 동시에 위험이 발생한 후 그에 대응하는 안전조치도 명시하는 것이 효율적이다.

2) 우선순위화

우선순위화 단계에서는 분류된 위험요구사항을 프로젝트의 특성에 맞게 우선순위를 선정한다. 우선순위는 위험도뿐만 아니라 프로젝트의 실행 준서, 장비와의 연결도 등을 종합적으로 고려하여 결정한다.

Ⅳ. 사례 연구: 음향측심기(Echo sounder)

본 논문에서는 선박에 기본적으로 탑재되는 최소한의 장비로 소규모 소프트웨어 기준에 적합한 음향측심기를 대상으로 위험분석을 실시한다. 음향측심기는 메아리처럼 선저에서 소리를 내어 해저에 부딪혀서 되돌아오는 시간으로 수심을 측정하는 장비이다. 음향측심기의 기능안전성을 확보하기 위해서는 잠재적 위험요소를 파악하고 해결방안을 마련할 수 있어야 한다. 표 3은 ISO 9875 (Ships and Marine Techonology)를 기준으로 음향 측심기에 대한 소프트웨어 중심의 기능안전성 분석을 위해 소프트웨어와 관련이 있는 항목을 추출하였다[11]. 전체 항목 17개 중 11개의 항목이 소프트웨어와 관련된 것으로 파악되었다.

표 3. 음향측심기의 성능규격
Table 3. Performance standard of Echo sounder

분류 항목		설 명	구 분
기능	성능 범위	이 장치는 일상 전파와 해저 반사 성능 조건에도 송수파기로 2m ~ 200m의 변환기에서 모든 간격을 측정할 수 있어야 한다.	소프트웨어 하드웨어
	범위 눈금	이 장치는 최소 2개 눈금 범위를 갖는다. 눈금 범위는 얕은 수심 범위인 20m범위와 깊은 수심 범위인 200m범위로 분류된다. 자동 범위 기능은 분류된 범위를 자동적으로 선택한다. 위성 범위가 0부터 초기화되지 않고 사용될 경우에는 그 범위가 사용되고 있음을 보여주어야 한다.	소프트웨어 하드웨어
	주 디스 플레이	주 디스플레이는 직접적인 깊이와 가시적인 측심 기록을 제공하는 적합한 그래픽을 출력한다. 주 디스플레이 기록은 깊은 범위 눈금에서 최소 15분간 측심을 나타내어야 하며 다양한 색상의 디스플레이를 사용할 수 있어야한다.	소프트웨어
	펄스 반복률	펄스 반복률은 깊은 수심 범위에서 매 분당 12펄스, 얕은 수심 범위에서 매 분당 36펄스보다 느려서는 안 된다.	소프트웨어
	횡경사 및 종경사	선박의 횡경사 ±10도 또는 종경사 ±5도일 때, 장치 성능은 이 표준의 요건에 적합하여야 한다.	소프트웨어
자료 보관		서류 기록이나 다른 수단으로 정보(깊이 및 12시간 동안 관련된 시간)를 기록할 수 있어야 한다.	소프트웨어 운용
정확성		1500m/s의 수중 음속을 근거로 할 때, 표시된 깊이의 허용 공차는 다음 중 큰 값으로 한다. - 얕은 수심 범위 눈금에서는 ±0.5m, 깊은 수심 범위 눈금에 서는 ±5m - 표시된 깊이의 ±2.5% 디스플레이 눈금은 얕은 수심 눈금에서 1m당 5.0mm보다 작지 않아야 하고 깊은 수심 눈금에서는 1m당 0.5mm보다 작지 않아야 한다.	소프트웨어
오동작, 경보 및 표시		경보 신호는 가시가청 또는 묵음 기능으로 수심이 초기 설정 값보다 낮을 때 제공되어야 한다. 초기 설정 경보 깊이를 변환기 위치에서 참조하지 않을 경우에는 기준 위치를 표시하여야 한다. 전원의 공급이 실패하거나 감소되는 상태를 표시하는 설비는 배전반이나 그 외 장소 쪽으로 통합할 수 있으며 반드시 이 장치와 일체로 할 필요는 없다.	소프트웨어 하드웨어
인간공학적 기준		범위 눈금 선택 기능은 사용자가 직접 접근할 수 있어야 한다. 다른 기능도 직접 접근할 수 있어야하고, 관련 메뉴에 있는 정해진 제어나 주접근으로 즉시 실행되어야 한다. 수심 정보의 깊이는 사용 범위/눈금의 1/10 미만 간격으로, 시간은 5분을 초과하지 않는 간격으로 표시하여야 한다.	소프트웨어
인터페이스		출력으로부터 구한 깊이 정보를 원격 디지털 디스플레이, 항해 자료 기록기 및 항적 제어 시스템과 같은 다른 장치에 제공할 수 있어야 한다. 이 출력에서는 선박용 골 하부 깊이, 현재 출력되는 깊이 눈금, 병렬(다중, 복수) 설치로 사용하는 송수파기, 적용 가능한 기타 상태 정보를 포함하여야 한다. 이 출력은 디지털 방식, 연속 전달 방식이어야 하며, 관련된 국제 기준(IEC 61162)에 적합한 설비이어야 한다.	소프트웨어
안전 예방 조치		고전압 전기 감광지의 기록 매체를 사용하거나 유동성 기록 기구를 사용하는 경우와 음향 측심기가 동작하는 동안 그 기록으로 접근이 가능한 경우의 차이는 운전자를 위해 안전하게 공급되어야 한다.	소프트웨어

4-1 위험요인 분석

1) 안내단어 정의

음향측심기의 성능규격에서 소프트웨어의 위험이 발생할 수 있는 총 12개의 항목을 대상으로 요구사항을 추출한다. 안내단어는 음향측심기가 작동하지만 기능을 제대로 수행하지 못해서 생기는 위험요소(측정 오류, 범위 오류, 눈금 간격 오류 등)와 음향측심기가 제대로 작동하지 않아 발생하는 위험요소(기록 오류, 오동작, 접근 불가 등)가 나타난다. 본 논문에서 제시하는 안내단어는 한국해양대학교 실습선 한나라 호에 설치되어 있는 음향 측심기의 제조회사인 ㈜삼영이엔씨의 매뉴얼과 실무에 종사하고 있는 항해사들의 설문을 통해 도출하였다.

2) 위험발생원인 분석

확정된 요구사항에 영향을 끼치는 발생원인을 조사한다. 표 4는 분석이 완료된 내용을 작성한 산출물이다.

4-2 위험결과분석 및 기준 정의

1) 위험결과 분석

위험요구사항 수집 단계에서는 요구사항에 의해 나타날 수 있는 위험요구사항을 수집한다. 안내단어로 인해 나타날 수 있는 결과와 위험을 해결하기 위한 안전장치를 명시한 산출물을 도출하였다.

2) 위험분류기준 정의

도출한 위험요구사항을 정의된 기준에 따라 분류한다. 표 6은 2.3절에서 제시한 '해양 선박사고 위기관리 표준매뉴얼'에 명시된 4가지의 수준을 선박에 탑재된 소규모 장비를 대상으로 재정의한 결과이다[5].

표 4. 음향측심기의 안내단어
Table 4. Guideword of Echo sounder

번호	안내단어	발생원인
1	측정 오류	일상 전파와 해저 반사 실패
2	범위 오류	수심 범위가 너무 낮거나 높음
3	눈금간격 오류	범위 눈금 미사용
4	기록 오류	디스플레이 출력 실패
5	다중 정보	너무 많은 정보 수집 및 변환실패
6	자료 손실	서류 및 정보 손실
7	정확성 오류	깊이의 허용 공차의 초과
8	오동작	기기의 동작 오류
9	경보 신호	수심이 초기 설정보다 낮음
10	접근 불가	권한 손실 및 인터페이스 오류

표 5. 음향측심기의 HAZOP 워크시트
Table 5. HAZOP worksheet of Echo sounder

안내단어	원인	결과	안전장치
측정 오류	일상 전파와 해저 반사 실패	수심 측정 불가	송수파기 제어
범위 오류	수심 범위가 너무 낮거나 높음	수심 결과 오류 신뢰성 없는 결과도출	수동범위 제어 시스템
기록 오류	디스플레이 출력 실패	기기 사용 불가	
정확성 오류	깊이의 허용 공차의 초과	신뢰성 없는 결과도출	
다중 정보	너무 많은 정보 수집 및 변환실패	신뢰성 없는 결과도출	변환기
자료 손실	서류 및 정보 손실	항해정보 누락	백업 DB
오동작	기기의 동작 오류	기기 사용 불가	
접근 불가	권한 손실 및 인터페이스 오류	기기 사용 불가	
경보	수심이 초기 설정보다 낮음	좌초 또는 바텀터치	경보 신호

표 6. 위험경보 수준 (항해장비 소프트웨어)
Table 6. Degree of Hazard alert (Maritime equipment software)

분류	구분	내용
1	관심 (Blue)	징후가 있으나 그 활동수준이 낮으며 가까운 기간 내에 소프트웨어 위험으로 발전할 가능성도 비교적 낮은 상태
2	주의 (Yellow)	징후 활동이 비교적 활발하고 소프트웨어 위험으로 발전할 수 있는 일정 수준의 경향성이 나타나는 상태
3	경계 (Orange)	징후 활동이 매우 활발하고 전개속도, 경향성 등이 현저한 수준으로서 소프트웨어 위험으로의 발전 가능성이 농후한 상태
4	심각 (Red)	징후 활동이 매우 활발하고 전개속도, 경향성 등이 심각한 수준으로서 소프트웨어 위험으로 발생이 확실 시 되는 상태

4-3 위험도 평가 및 우선순위화

1) 위험도 평가

표 7은 음향측심기의 안내단어 중 9개의 위험요소를 식별하여 나열한 것이다. 4개는 관심, 3개는 주의, 2개는 경계수준의 위험도를 가지고 있으며 각 위험요소들에 대한 안전조치를 나타낸다.

①트랜듀서 확인: 음향측심기는 선박의 하단부에 부착된 트랜듀서에서 송출하는 음파를 통해 수심을 측정한다. 트랜듀서의 고장은 수심측정의 가장 큰 원인이 될 수 있다.

②수동 설정: 음향측심기는 2m~200m의 변환기에서 모든 간격을 측정할 수 있어야 한다. 이 범위에서 벗어날 경우 수동 설정을 통해 오류를 해결할 수 있어야 한다.

③케이블 설정 및 확인: 소프트웨어를 제공하는 하드웨어의 전원공급을 담당하는 케이블 또는 데이터를 제공하는 커넥터의 연결 상태를 확인한다.

④변환기 설정 변경: 변환기 및 이와 관련된 전달 매체 수신기가 다수일 경우 각 변환기의 상태 또는 설정을 관리할 수 있어야 한다.

⑤데이터 복구: 데이터에 오류가 생겼을 경우 자료를 백업해놓은 시점으로 돌아간다. 각 변환기의 상태 또는 설정을 관리할 수 있어야 한다.

⑥권한 획득 및 리셋: 권한이 손실되었을 경우 제조사와 설계팀에 의뢰하여 권한을 획득하거나 시스템을 초기화한다.

⑦항해 경로 변경: 초기설정이란 선박이 좌초될 위험이 있는 수심으로 설정한다. 만약 수심이 설정 값 보다 낮으면 항해 경로를 변경해야 한다.

2) 우선순위화

분류된 위험요구사항의 위험도를 고려하여 우순순위를 부여한다. 각 요구사항에 부여된 우선순위를 소프트웨어 개발에 적용한다.

Ⅳ. 결 론

본 논문에서는 해양분야에서 기능안전성 확보를 위한 프로세스로 위험분석 단계의 절차와 산출물을 정의하였으며 항해장비인 음향측심기를 대상으로 사례 연구를 실시하였다. 사례연구에서는 소프트웨어의 위험요인을 미리 분석하고 위험도를 측정하여 소프트웨어를 개발할 때 고려해야 하는 잠재적 위험요소를 파악하였다. 개발 초기 단계인 요구사항 단계에서 소프트웨어의 위험도를 파악함으로써 잠재된 위험요소를 예방할 수 있다. 파악한 위험요소를 전체 생애주기에 걸쳐 관리하여 기능안전성을 확보하기 위한 연구가 향후과제로 남을 것이다.

감사의 글

본 연구는 중소기업청 2015년 “구매조건부 신제품개발사업(과제번호 : 1425096815)”과 NIPA 2016년 “소프트웨어신뢰·안전성 확보를 위한 공통 지침 및 가이드 개발과 시범적용 용역사업(과제번호 : 2016-0083-01)”과 2016년 ”기상·환경·선체 정보를 활용한 IEC 61162-450 기반 선박안전운항지원 소프트웨어 플랫폼 및 시스템 개발(과제번호 : S1106- 16-1016)“의 지원으로 수행되었습니다.

표 7. 음향측심기의 안전조치 HAZOP 작업서
Table 7. Safety-conscious HAZOP worksheet of Echo sounder

안내단어	원인	결과	안전장치	위험도	추가안전조치	비고
측정 오류	일상 전파와 해저 반사 실패	수심 측정 불가	송수파기 제어	관심	트랜듀서 확인	
범위 오류	수심 범위가 너무 낮거나 높음	수심 결과 오류 신뢰성 없는 결과도출	수동범위 제어 시스템	관심	수동 설정	
기록 오류	디스플레이 출력 실패	기기 사용 불가	보조 기기 사용	주의	케이블 및 설정 확인	
정확성 오류	깊이의 허용 공차 초과	신뢰성 없는 결과도출	수동 제어 시스템	관심	트랜듀서 확인	
다중 정보	너무 많은 정보의 수집 및 변환 실패	신뢰성 없는 결과도출	변환기	관심	변환기 설정 변경	
자료 손실	서류 및 정보 손실	항해정보 누락	백업 DB	주의	데이터 복구	
오작동	기기의 작동 오류	기기 사용 불가	보조 기기 사용	경계		
접근 불가	권한 손실 및 인터페이스 오류	기기 사용 불가	보조 기기 사용	경계	권한 획득 및 리셋	
경보	수심이 초기설정 보다 낮음	좌초 또는 바텀터치	경보 신호	주의	항해경로 변경	선박 좌초 경보

참고문헌

[1] IMO, “Guideline on software quality assurance and human -centred design for e-navigation”. MSC.1/Circ. 1512, 2015

[2] IEC, “IEC 61508(2010) - Functional safety of electrical /electronic /programmable electronic safety-related systems.”, IEC Publication, 2010

[3] K. H. Kyung and K. Lee, An Ontology-Based Hazard Analysis and Risk Assessment for automotive functional safety, Journal of The Korea Society of Computer and Information, Vol. 20, No. 3, pp. 9-17, March 2015

[4] J. I. Pyo, Study on ISO 26262 Functional Safety Promotion Plan in Automobile Industry, MS. Dong-eui University, Busan, 2012.

[5] S. W. Lim, Risk Analysis and Software Requirement Analysis for Software Functional Safety and a Case Study on Echo Sounder, MS. Korea Maritime & Ocean University, Busan, 2017.

[6] National IT Industry Promotion Agency, “SW safety public development guide”, National IT Industry Promotion Agency, 2016

[7] H. Kim, “A Study on Requirement analysis process for the practical guidance of e-Navigation SQA guideline” *The Journal of Digital Contents Society*, Vol. 16, No. 6, pp. 935-941, June 2016.

[8] M. Kim, M. Park, A Study on the Software Fault Modes and effect Analysis for Software Safety Evaluation, Journal of Korea Multimedia Society, Vol. 15, No. 1, pp. 115-130, January 2012

[9] Ministry of Oceans and Fisheries: “Regulation on the construction and operation of the central accident investigation headquarters of the Ministry of Oceans and Fisheries”, Ministry of Oceans and Fisheries: Ministry of Oceans and Fisheries Order No. 222, 2015.

[10] T. H. Park, T. H. Kim, and H. S. Jin, A Study on the system of Ensuring SW Safety for a SW Oriented Society - Foucs on testing, Evaluation, Certification: Software Policy & Research Institute, 2016.

[11] ISO, “ISO 9875(2010) - Ships and marine technology--Marine echo-sounding equipment.”, ISO Publication, 2000

임상우(Sang-woo Lim)

한국해양대학교 IT공학부 졸업 (2014, 공학사)
동대학교 대학원 컴퓨터공학과 석사과정 졸업(2017, 공학석사)

2017년 3월 현재 (주)지엠티 전임연구원
※관심분야 : 소프트웨어설계, 해양소프트웨어품질, 소프트웨어 품질보증, 소프트웨어기능안전성

이서정(Seojeong Lee)

숙명여자대학교 전산학과 졸업 (1989, 이학사)
동대학교 대학원 전산학과 석사과정 졸업(1991, 이학석사)
동대학교 대학원 전산학과 박사과정 졸업(1998, 이학박사)

1998년~2003년 동덕여자대학교 강의교수
2003년 미국 카네기멜론대학교 소프트웨어전문가 과정이수
2005년~현재 한국해양대학교 해사IT공학부 교수
2009년~현재 해양수산부 국제해사기구 정부대표단 활동
2015년 바다의날 해양수산부 장관표창 수상(해양소프트웨어품질보증 표준개발 공적)
※관심분야 : 소프트웨어설계, 해양소프트웨어품질, 소프트웨어기능안전성

양회석(Hoi-Seok Yang)

서울과학기술대학교 IT정책대학원 공공 정책 석사과정 졸업 (2011년, 정책학석사)

2005년 정보관리기술사 취득
2005년 ~ 2016년 정보화 전략 컨설팅, 품질 및 안전성 컨설팅
2014년~현재 나이스컨설팅 대표
※관심분야 : 소프트웨어 기능안전성, 소프트웨어 공학 및 품질, 비즈니스 ICT 전략, 빅 데이터 전략