하이브리드 추진 선박용 전력 에너지 관리 모듈의 신뢰성 향상을 위한 소프트웨어 정적 분석에 관한 연구

박한수, 김현철, 최주형*
한국조선해양기자재연구원
hspark@komeri.re.kr, lovespins@komeri.re.kr, jhchoi@komeri.re.kr

A study on software static analysis for improving the reliability of power energy management module of hybrid propulsion vessel

Park Han Soo, Kim Hyeun Chul, Choi Joo Hyoung
KOMERI (KOrea Marine Equipment Research Institute)

요 약

본 논문은 하이브리드 추진 선박에서 이산화탄소 배출량을 줄이고, 에너지 효율을 극대화 하기 위해 사용되는 전력 에너지 관리 시스템의 펌웨어에 대해 국제 기능안전 규격인 IEC 61508-3의 소프트웨어 정적 분석 규칙을 적용하여 국제 코딩 규칙 준수에 대한 분석을 실시하였다. IEC 61508-3을 기반으로 정의된 41개의 국제 코딩 규칙을 적용한 결과 총 4개의 규칙을 위배하였고, 381개의 위배 항목이 발견되어, 규칙 준수율은 90.24%로 분석되었다.

Ⅰ. 서 론

IMO 환경규제, 에너지 효율 개선 강제화, 글로벌 선박 패러다임 변화로 친환경 선박의 핵심기술 개발에 대한 필요성이 대두되면서 글로벌 선박 시장 패러다임이 변화되어 친환경 선박 시장이 급격이 확대되고 있는 추세이다. 그 일환으로 하이브리드 추진 방식을 적용한 선박들이 국내에서 개발, 건조되고 있지만 ESS, PCS, 추진 모터 및 엔진 등 전력 기기들을 제어하는 핵심 시스템인 전력 에너지 관리 시스템(PEMS, Power Energy Management System)은 외국 제조사 제품들이 기술 선도하고 있는 실정이다. 본 논문에서는 주요 선진국을 중심으로 개발 중인 하이브리드 추진 선박의 추진시스템 핵심기술을 확보하고 선도하기 위한 목적으로 국내에서 개발 중인 하이브리드 추진 선박을 위한 PEMS의 펌웨어에 대한 안정성과 신뢰성을 향상시키고자 국제 기능안전 표준을 적용하고자 한다.

IEC 61508은 전기/전자/프로그래밍 가능한 전자장치의 기능 안전성에 대해 다루고 있고, 시스템의 안전성을 확보하기 위해 수행해야 하는 활동에 대해 정의하고 있으며, 안전성 확보 활동은 공통적으로 수행해야 하는 활동과 안전 무결성 수준(SIL: Safety Integrity Level)에 따라 세부적으로 수행해야 하는 활동이 정의되어 있다.

본 논문에서는 선박의 추진을 위해 다양한 종류의 연료를 소모하는 하이브리드 추진 선박의 에너지 효율을 위해 사용되는 PEMS에 대해 소프트웨어의 신뢰성을 확보하기 위한 목적으로 전기/전자/프로그래머블 전자(E/E/PE) 안전 관련 시스템의 기능 안전에 대한 국제 표준인 IEC 61508의 Part 3인 소프트웨어 요구사항을 적용하여 PEMS의 펌웨어에 대해 코딩 규칙 검증인 정적 분석을 실시하고자 한다.

Ⅱ. 본론

1. 소스코드 정보

본 논문에서 소개하는 PEMS 모듈은 c언어 기반으로 개발되었으며, 아래 표와 같이 총 22개의 소스코드로 구성되어있다. NMEA 0183 및 NMEA 2000 프로토콜을 기반으로 통신을 담당하는 파트와 전력에 대한 정보를 송수신하고 에너지 효율에 대한 처리를 담당하는 파트, 선박의 상태 및 해상 상황을 반영을 할 수 있도록 다양한 센서 및 알고리즘과 연동 처리하는 Main 파트로 구성되어있다.

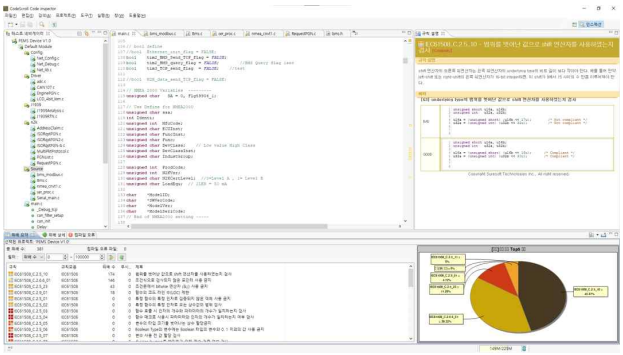
번호	파일명	pLOC	번호	파일명	pLOC
1	ad*.c	337	12	LC*.c	362
2	Ad*.c	763	13	main.c	1,231
3	Bm*.c	480	14	Mu*.c	929
4	bm*.c	572	15	Ne*.c	935
5	CA*.c	536	16	Ne*.c	144
6	En*.c	365	17	Ne*.c	847
7	IS*.c	1,456	18	nm*.c	1,638
8	IS*2.c	1,238	19	PG*.c	466
9	IS*.c	1,772	20	Re*.c	834
10	J1*.c	579	21	se*.c	525
11	J1*.c	962	22	Se*.c	377
총 pLOC			17,348		

※pLOC(physical Line of Code)는 주석과 공백을 포함한 파일의 라인 수

2. 분석 툴 및 적용 규칙

소프트웨어 정적 분석 툴인 Code Inspector를 사용하였다. 정적 분석은 산업계 고유의 코딩 규칙을 적용하여 잠재적인 오류를 제어하는 것이 목적이다. 현재 Code Inspector에서 지원하는 IEC 61508 규격은 총 41개의 규칙으로 본 논문에서는 41개의 규칙 모두를 적용하여 분석하였다.

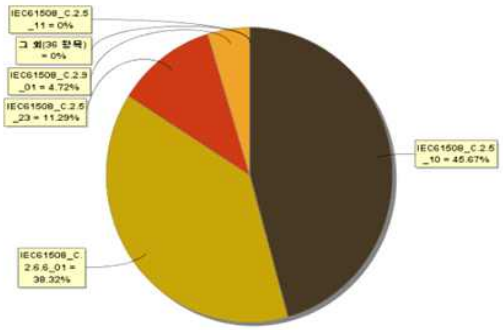
규칙	세부 내용
IEC61508_C.2.5_01	특정 함수의 특정 인자로 검증되지 않은 객체 사용 금지
IEC61508_C.2.5_02	특정 함수의 특정 인자로 오는 상수값의 범위 검사
IEC61508_C.2.5_03	함수호출 시 인자의 수와 파라미터의 개수 일치 검사
IEC61508_C.2.5_04	함수 매크로 사용시 파라미터와 인자의 개수가 일치 검사
IEC61508_C.2.5_05	변수의 타입 크기를 벗어나는 상수 할당금지
IEC61508_C.2.5_06	Boolean변수에는 Boolean 변수와 0, 1 이외의 값 사용 금지
IEC61508_C.2.5_07	변수 사용 전 값 할당 검사
IEC61508_C.2.5_08	division by zero를 방지하기 위한 제수 검증 여부 검사
IEC61508_C.2.5_09	const나 volatile 을 제거하는 명시적 변환 금지
IEC61508_C.2.5_10	범위를 벗어난 값으로 shift 연산자를 사용하였는지 검사
IEC61508_C.2.5_11	문자값 사용 및 저장 외의 용도로 plain char 타입사용금지
IEC61508_C.2.5_12	숫자값의 사용 및 저장외의 용도로 char 타입 사용금지
IEC61508_C.2.5_13	평가순서에 따라 결과가 달라지는 문장사용금지
IEC61508_C.2.5_14	함수 매크로의 파라미터가 괄호로 감싸졌는지 검사
IEC61508_C.2.5_15	매크로 identifier는 사용되기 전에 defined 되었는지 검사
IEC61508_C.2.5_16	지역변수의 주소는 return 문에 사용금지
IEC61508_C.2.5_17	지역변수의 주소가 자신의 scope을 넘어서는 변수에 할당금지
IEC61508_C.2.5_18	함수 prototype에서 포인터 타입의 인자가, 해당객체를 수정하는데 사용되지않으면면 const로 선언되어야 함
IEC61508_C.2.5_19	문장이 있는 모든 switch 절이 break문으로 끝나는지 검사
IEC61508_C.2.5_20	switch문이 하나 이상의 case 문을 가졌는지 검사
IEC61508_C.2.5_21	switch문의 마지막 절이 default절 이어야 한다
IEC61508_C.2.5_22	비교 조건식의 연산 결과가 항상 같게 나오는 표현식 사용금지
IEC61508_C.2.5_23	조건문에서 bitwise 연산자 (&,|) 사용 금지
IEC61508_C.2.5_24	else if 가 있다면 else가 반드시 있는 지 검사
IEC61508_C.2.5_25	switch, while, do-while, for, if가 복합문으로 되어있는지 검사
IEC61508_C.2.5_26	non-void return의 함수에서 명시적 return이 존재하는지 검사
IEC61508_C.2.6.2_01	직,간접적인 재귀호출 금지
IEC61508_C.2.6.2_02	exit 함수 사용 금지
IEC61508_C.2.6.3_01	동적 메모리 할당 금지
IEC61508_C.2.6.4_01	동적 변수 또는 동적 객체 설치에 대한 온라인 확인
IEC61508_C.2.6.6_01	조건식으로 검사되지 않은 포인터 사용 금지
IEC61508_C.2.7_01	함수 복잡도(cyclomatic complexity number) 제한
IEC61508_C.2.7_02	goto 문장 사용 금지
IEC61508_C.2.7_03	for문의 초기화,제어,증감 expression은 모두 loop 제어와 관련 있는지 검사
IEC61508_C.2.7_04	함수의 최대 nesting depth 제한
IEC61508_C.2.8_01	헤더파일에 전역변수 정의 금지
IEC61508_C.2.8_02	헤더파일에 함수 정의 금지
IEC61508_C.2.9_01	함수의 코드 라인 수(LOC) 제한
IEC61508_C.2.9_02	함수가 하나의 exit point 를 가졌는지 검사
IEC61508_C.2.9_03	함수의 파라미터는 함수와 연관된 것만 선언되었는지 검사
IEC61508_C.2.9_04	longjmp 함수, setjmp 매크로 사용 금지



3. 분석 결과

Code Inspector를 이용하여 PEMS 펌웨어에 대해 41개의 국제 코딩 규칙을 적용하여 검증을 한 결과 총 4개의 규칙을 위배 하였고, 381개의 위배 항목이 발생되어, 규칙 준수율은 90.24%로 분석 되었다. (규칙 준수율 = (적용 규칙 수 - 위배 규칙 수) / (전체 규칙 수) * 100)

규칙 위배 중 IEC 61508_C.2.5_10의 규칙이 174건(45.67%)으로 위배율이 가장 높게 분석되었으며, 이 규칙은 범위를 벗어난 값으로 shift 연산자를 사용하였는지를 검사하는 규칙이다. 또한, 분석한 소스 파일 중 nmea_cnv1.c에서 131개의 규칙이 위배 되었으며, 전체 소스 파일 중 34.38%를 차지하여 위배율이 가장 높게 분석되었다.



규칙	규칙 모음	위배 수	위배 수 (무시 제외)	무시된 위배 수
IEC61508_C.2.5_10	IEC61508	174	174	0
IEC61508_C.2.6.6_01	IEC61508	146	146	0
IEC61508_C.2.5_23	IEC61508	43	43	0
IEC61508_C.2.9_01	IEC61508	18	18	0

Ⅲ. 결론

본 논문에서는 하이브리드 추진선박을 위한 PEMS의 펌웨어에 대해 소프트웨의 신뢰성을 확보하기 위한 목적으로 IEC 61508-3 규격을 적용하여 코딩 규칙 검증을 수행하였고, 그 결과 규칙 준수율이 90.24%인 것으로 분석 되었다. 향후 코딩 준수율 향상 시키기 위해 PEMS 펌웨어를 중심으로 개선 방향을 제시하고, 국제 코딩 규칙을 모두 만족시켜 펌웨어의 신뢰성을 향상 시킬 수 있도록 해당 모듈에 적합한 코딩 가이드라인을 개발하고자 한다.

감사의 글

본 연구는 산업부의 “친환경 선박 전주기 핵심기술개발 사업 - 하이브리드 추진선박 에너지 통합모듈 시스템 개발 및 검증(RS-2023-00252794)”의 3차년도 지원에 의하여 이루어진 연구로, 관계부처에 감사드립니다.

참 고 문 헌

[1] IEC, “IEC 61508-3 Functional safety of electrical/electronic/programmable electronic safety-related systems-Part 3: Software requirements“, Edition 2.0, 2010

[2] Suresofttech blog, “IEC 61508-안전 무결성 수준(SIL:Safety Integrity Level)”, 2018, (https://blog.naver.com/suresofttech)

[3] 권기현, “IEC 61508 안전 무결성 수준의 정량적 검증”, JKIIT, Vol.16, No.9, 43-50, September 2018.

[4] 박한수, 이동규, “선박 건조공정 관리 효율화를 위한 작업장 환경 모니터링 디바이스의 국제 코딩 규칙 검증에 관한 연구”, KICS Summer Conference, No.0037, Jun. 2022.