소프트웨어 요구사항 안전성 분석 보고서

수정일자	수정자	버전	추가/수정 항목	내 용
2019-10-17	이용준	0.1		초안작성
2019-11-20	이용준	0.2		
2019-11-23	이용준	1.0		

	고등급(EAL6 이상) 보안마이크로커널 개발				
작성자	이용준	소속	고려대학교	연구 책임자	김승주
작성일	2019-11-23	파일명	2019-SW_REQ-안전성분석서.HWP		
제목	소프트웨어 요구사항 안전성 분석 보고서				

<제목 차례>

<표 차례>

<그림 차례>

	고등급(EAL6 이상) 보안마이크로커널 개발				
작성자	이용준	소속	고려대학교	연구 책임자	김승주
작성일	2019-11-23	파일명	2019-SW_REQ-안전성분석서.HWP		
제목	소프트웨어 요구사항 안전성 분석 보고서				

I. 목적

본 보고서는 고등급 보안 마이크로 커널(CHAOS) 개발을 위해 IEC 61508 표준에 근거하여 안전성 확보를 위한 안전성 분석 활동 내용을 기술하고, 그 결과를 분석하는 것에 그 목적이 있다.

II. 용어 정의 및 약어

- Harm(피해) : 사람들에 대한 물리적 부상 또는 환경/자산에 대한 물리적 피해
- Hazard(위험) : 피해의 잠재적 요인
- Risk(위험성) : 피해 발생의 확률과 피해의 심각도의 합
- Safety(안전) : 수용 불가능한 위험에서 벗어난 상태
- Functional safety(기능 안전) : E/E/PE안전 관련 시스템과 기타 위험성 감소 조치의 올바른 기능에 의한 EUC와 EUC 제어 시스템과 관련된 전체 안전의 일부
- Safety function(안전기능) : 특정 위험한 사건에 대하여 E/E/PE 시스템 또는 기타 위험성 감소 조치에 의해 구현된 기능
- Safety integrity(안전 무결성) : 안전 관련 시스템이 정해진 시간 안에 정해진 모든 조건에 맞는 특정 안전기능을 만족스럽게 수행할 확률
- Software safety integrity(소프트웨어 안전 무결성) : 장애의 위험한 모드에서 시스템적 장애와 관련한 안전 관련 시스템의 안전 무결성
- Safety integrity level, SIL(안전 무결성 등급) : 안전 무결성 값의 범위에 따라 구분된 등급, 4단계가 가장 높고 1단계가 가장 낮음
- Fault(결함) : 요청된 기능을 수행할 때 기능 유닛의 능력이 감소하거나, 손실이 발생하는 비정상적 조건
- Failure(장애) : 요청된 방법 이외의 방법으로 유닛의 기능 또는 동작을 정상적인 제공이 멈추는 경우

Ⅲ. 시스템 개요

시스템 전체의 구조는 아래 그림과 같다. 보안 마이크로커널이 탑재되는 시스템은 하드웨어를 담당하는 Mission Computer과 구동을 제어하는 Flight Computer를 제어하는 역할을 한다.

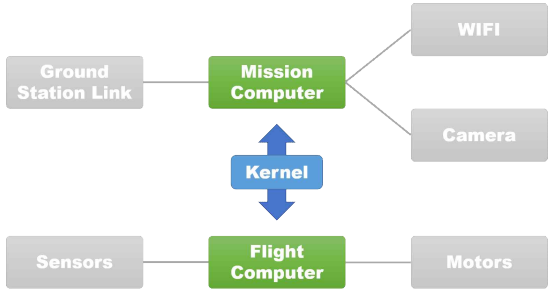

그림 1 상위수준 시스템 구조

보안 마이크로커널 탑재 시스템의 하부 구조는 [그림 2]과 같다. 보안 마이크로커널은 신뢰할 수 있는 커널 도메인에 존재하며, 어플리케이션이 탑재되는 사용자 도메인은 신뢰구간과 비 신뢰구간으로 구별되어 있다. 이러한 구조는 사용자 커널/어플리케이션 간의 영역 침범을 막을 수 있는 구조이다.

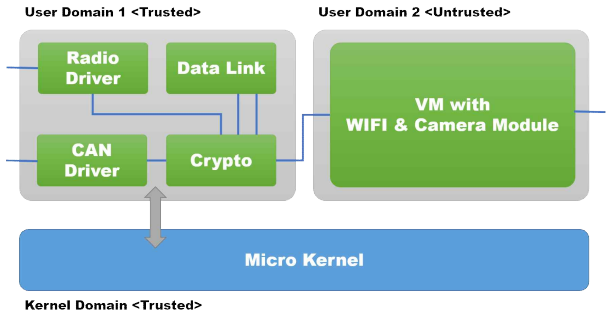

그림 2 하위시스템 및 연계관계

커널 레벨 시스템에는 [그림 3]와 같은 모듈로 구성되어 있다. 세마포어, 뮤텍스, 메시지, 이벤트 등의 모듈은 스케줄러에 의해 동작하며, 이진 세마포어와 메일박스는

	고등급(EAL6 이상) 보안마이크로커널 개발				
작성자	이용준	소속	고려대학교	연구 책임자	김승주
작성일	2019-11-23	파일명	2019-SW_REQ-안전성분석서.HWP		
제목	소프트웨어 요구사항 안전성 분석 보고서				

세마포어에 의해 동작한다.

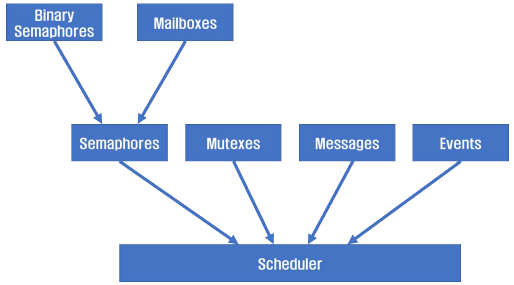

그림 3 CHAOS 커널레벨 시스템 구조

Ⅳ. 안전성 분석기법

가. SW 안전요구사항

SR.1. 안전한 커널은 하드웨어와 커널 자체의 고장 진단을 수행하는 기능이 있어야 함. 고장이 검출되면 적절한 예외처리가 실행되어야 함.

SR.1.1. 커널 고장 진단

SR.1.2. 하드웨어 고장 진단

SR.1.3. 진단 후 적절한 조치 필요

SR.2. 한 컴포넌트의 오작동이 다른 프로세스 또는 커널에 영향을 끼치면 안됨

SR.2.1. 커널 요소 간 분리

SR.2.2. 커널과 어플리케이션 분리

SR.2.3. 어플리케이션 간에 분리

SR.3. 시스템에서 작동하는 작업들의 스케줄링을 예측 할 수 있음

SR.3.1. 공정한 자원 할당

SR.3.2. 우선 순위 반전 문제

SR.3.3. 스케줄 가능성 분석 제공

SR.4. 예측하지 못한 상황이 일어난다면 안전한 상태로 회복. 또한, 다른 구성요소에 손상을 주지 않으며, 신속하게 다시 시작할 수 있음

SR.4.1. 요소간 독립적 재실행

SR.4.2. 안전상태로 회복

SR.4.3. 안전하지 않은 상태 회피

SR.5. 비정상적인 동작을 감지하고 방지함. 비정상적인 동작은 하드웨어 오류가 발생하거나 소프트웨어 실행이 어려운 경우를 말함

SR.5.1. 예외 상황 정의

SR.5.2. 예외 상황 대응

SR.5.3. 예외 상황 감지

나. SW 안전성분석에 사용된 입력자료

SW 요구사항 안전성 분석에 입력으로 사용된 자료는 다음과 같다.

1. CHAOS 소프트웨어 요구사항 명세서 (초안)

2. CHAOS 시스템 구조도 (Architecture Design)

3. 소프트웨어 시스템을 위한 HAZOP (안내어) Guideword

다. SW 요구사항 안전성분석에 사용된 기법

SW 요구사항 안전성 분석에는 PHL, PHA, FMEA, HAZOP 기법을 사용하였다. 각 기법에 간략한 설명은 아래와 같으며, 자세한 설명은 1차년도 안전 무결성 검증 결과물인 '소프트웨어 안전 기능 동향 분석서' 에 기술되어 있다.

표 1 안전성 분석 기법 설명

기법	설명
PHL (Preliminary Hazard List)	예비 위험원 목록 (PHL)은 각 위험 요소 분석의 시작 단계에 생성된다. 분석가가 개념, 운영 및 구현을 기반으로 잘못 될 수 있다고 생각할 수있는 모든 것들을 담은 목록이다. PHL은 관리활동(MA)에 고려 중인 개념과 관련

	된 위험원 목록을 제공한다. 계약자는 MA가 지시한 대로 PHL에 의해 식별된 위험 또는 위험 특성을 조사하여 중요성을 판단해야 한다. 이러한 정보는 관리활동에서 '프로그램의 진행을 계속 가는가?' 과 같은 결정을 내리는 데 중요한 역할을 한다.
PHA (Preliminary Hazard Analysis)	PHA는 시스템 생명주기 중 개념설계 및 목표 설정단계에서 장치의 기능 요구사항을 바탕으로 간소화된 기능별 위험원을 도출한다. 그리고 위험도를 평가하여 안전대책 수립에 의한 위험도 제어의 필요성을 검토하기 위해 수행한다. PHA 수행을 통해 도출된 위험원은 허용할 수 있는 수준으로 위험도를 제어해야 하는 대상이다.
FMEA (Failure Modes and Effects Analysis)	FMEA는 "What If" 분석을 좀 더 체계화한 것이다. 즉, "만약 무슨 일이 벌어진다면 어떻게 될까?"라는 질문을 염두에 두어 하나의 부품, 장비 등이 고장 났을 경우 그것이 전체 제품이나 사용자, 혹은 제품기능에 어떠한 영향을 미치는가, 생각의 범위를 점차 넓혀가면서 상위수준으로 분석하여 가는 것이다.
HAZOP (Hazard and Operability)	시스템, 공정, 운영상의 위험원 식별을 목적으로 하며, 정상적인 상황으로부터 오작동을 식별하고 확인된 오동작으로부터 위험원 발생 유무를 확인한다.

라. SW 요구사항 안전성분석에 사용된 절차

SW 요구사항 안전성 분석은 다음의 절차를 통해 적용하였다.

첫번째로, PHL 작성을 통해 예비위험원을 도출한다. PHA에서는 PHL에 포함된 각 위험원에 대해서 사전분석을 수행한다. 이렇게 식별된 위험원에 대해서 FMEA와 HAZOP을 수행한다. FMEA와 HAZOP의 수행한 결과에 대해 위험원의 심각도와 빈도를 기준으로 분류를 하고 추후 조치를 위해 등급을 결정한다.

표 2 위험원 발생확률

빈도수준	등급	특정 사건
자주 발생 (Frequent)	A	빈번하게 발생할 가능이 있음
빈번히 발생 (Probable)	B	시스템의 생명주기동안 여러번 발생할 수 있음

가끔 발생 (Occasional)	C	시스템의 생명주기동안 가끔 발생할 가능이 있음
거의 발생치 않음 (Remote)	D	가능성은 작지만, 시스템의 생명주기동안 발생할 수 있음
발생 가능성 없음 (Improbable)	E	가능성은 매우 작고, 시스템의 생명주기동안 발생하지 않으리라고 볼 수 있음

표 3 위험원 심각도

내용	범주	정의
파국적 (Catastrophic)	1	사망, 시스템 상실, 또는 심각한 환경 파손
치명적 (Critical)	2	심각한 재해, 심각한 직업병, 상당한 시스템 또는 환경 파손
한계적 (Marginal)	3	사소한 재해, 사소한 직업병, 사소한 시스템 또는 환경 파손
무시가능 (Negligible)	4	사소한 재해나 직업병보다 더 낮음, 사소한 시스템 이나 환경 파손보다 더 낮음

표 4 위험원 수준 결정 매트릭스

구분	위험원 범주			
빈도	파국 (1)	치명 (2)	한계 (3)	무시 (4)
(A) 자주 발생 (Frequent)	1A	2A	3A	4A
(B) 빈번히 발생 (Probable)	1B	2B	3B	4B
(C) 가끔 발생 (Occasional)	1C	2C	3C	4C
(D) 거의 발생치 않음 (Remote)	1D	2D	3D	4D
(E) 발생 가능성 없음 (Improbable)	1E	2E	3E	4E

V. 안전성 분석기법

가. SW 안전요구사항 위험원 분석 내용

	고등급(EAL6 이상) 보안마이크로커널 개발				
작성자	이용준	소속	고려대학교	연구 책임자	김승주
작성일	2019-11-23	파일명	2019-SW_REQ-안전성분석서.HWP		
제목	소프트웨어 요구사항 안전성 분석 보고서				

1) Functional FMEA

표 5 FMEA 분석내용

KRS statement ID	KRS Statement text	Related KRS statements	Description	Potential Failure mode	Potential Root Cause	Detailed Root Cause
Mailbox_Post_Timeout	Post는 수신자의 mailbox에 메시지를 전달해야 한다. 기본 흐름 1. 수신자 mailbox와 msg를 입력으로 받는다. 2. 수신자 mailbox의 상태 조건을 검증한다. 3. 조건이 True이면 메시지를 보낸다. 3.1 조건이 False일때 Timeout 시간까지 대기하며, Timeout 시간이 지나면 종료한다. 4. 메시지를 성공적으로 보냈다면, 대기중인 reader queue를 스케쥴링 해준다. 수신자 mailbox 조건 1. 수신자 mailbox가 존재해야 한다. 2. 수신자의 mailbox는 충분한 buffer가 있어야 한다. 3. 수신자의 mailbox는 writers queue가 있어야 한다.	KRS_Threading KRS_Scheduler KRS_Mutexes KRS_Timers KRS_Queues	Post는 수신자의 mailbox와 msg를 받는다.	Faulty Functionality	Post가 메시지 전달을 실패한다.	Post를 수행해야 하는데 못하는 경우 1. timeout값이 0이 될 수 있음. 2. timeout값이 스케쥴링 불가능할때
				Faulty timing (if applicable to this SRS statement)		
				Faulty sequencing (if the SRS statement pertains to events)		
				Faulty data (if the SRS statement pertains to data)		
				Faulty error handling	Timeout의 Minimum 바운더리를 설정 안함	

2) HAZOP

표 6 HAZOP 분석내용

	아이템	속성	가이드	원인	결과	보호	추천
1	값을 Data Channel 저장소에 보냄	데이터 전송률	증가	데이터 전송률이 매우높음	데이터 항목이 누락되어 시스템이 오래된 데이터를 기반으로 진단할 수 있음		데이터 채널 객체에 데이터 속도 확인 및 경고를 통합하는 것을 고려
2	값을 Data Channel 저장소에 보냄	데이터 전송률	증가	데이터 입력 비율이 매우 높음	데이터 저장소가 가득차서 새로운 값을 입력받을 수 없고, 진단 능력을 상실하게 됨	시스템은 사용 가능한 데이터로 추론을 계속하기 위해 고안	드론의 안전에 대한 각 결함의 영향을 파악하기 위한연구가 필요
3	증거는 진단 규칙변경을 알림	데이터 흐름	없음	변경된 증거로 인해 진단 규칙에 전달되지 않음	진단 규칙이 업데이트되지 않음	만약 증거가 잠재적 위험한 상황과관련된 것이면 전달되지 않음	진단 범위 내에서적용을 체크
4	증거는 진단 규칙변경을 알림	데이터 흐름	기타	잘못된 증거 아이템과관련된 세부사항을 전달	진단 규칙에 따라 위험할 수 있는 잘못된 진단이 나올 수 있음		진단 범위 내에서적용을 체크
5	증거는 진단 규칙변경을 알림	데이터 흐름	기타	통지된 증거와 통지된새로운 매개변수 간의비호환성	진단 규칙에 따라 위험할 수 있는 잘못된 진단이 나올 수 있음		진단 범위 내에서적용을 체크
6	증거는 진단 규칙변경을 알림	데이터 흐름	기타	프로세싱을 위한 증거처리 큐. 파라미터들이더 빠르게 업데이트	증거와 파라미터들 간의 모순		너무 큰 대기 큐를방지하기 위해 데이터 전송률을 천천히 함

3) PHL(예비위험원목록)

	고등급(EAL6 이상) 보안마이크로커널 개발				
작성자	이용준	소속	고려대학교	연구 책임자	김승주
작성일	2019-11-23	파일명	2019-SW_REQ-안전성분석서.HWP		
제목	소프트웨어 요구사항 안전성 분석 보고서				

표 7 PHL 분석내용

	아이템	위험원(Hazard)	결과	코멘트
PHL-01	드론 엔진	운행 중 동작 정지	추락	안전하지 않은 상태
PHL-02	드론 컴퓨터	조작 부주의에 의한 오동작	우발적 파손	안전 분리
PHL-03	드론 베터리	운행 중 전원 부족	추락	안전하지 않은 상태
PHL-04	드론 베터리	BMS 실패	배터리 파손	안전하지 않은 상태
PHL-05	수신기	조종기 연결 실패	제어 불가능	안전하지 않은 상태
PHL-06	드론 네비게이션	항법장치 실패	회항 불가능	안전하지 않은 상태
PHL-07	드론 셀프 테스트	자가진단 실패	불안전한 상태	상태를 알 수 없음

4) PHA(예비위험원분석)

표 8 PHA 분석내용

	위험원(Hazard)	원인	결과	IMRI
PHA-01	운행 중 동작 정지	하드웨어 오류	추락	1D
PHA-02	조작 부주의에 의한 오동작	설계 오류, 소프트웨어 오류	우발적 파손	1D
PHA-03	운행 중 전원 부족	하드웨어 오류 (제조)	추락	1D
PHA-04	BMS 실패	하드웨어 오류 (제조)	배터리 파손	1D
PHA-05	조종기 연결 실패	설계 오류, 소프트웨어 오류	제어 불가능	1D
PHA-06	항법장치 실패	설계 오류, 소프트웨어 오류	회항 불가능	1D
PHA-07	자가진단 실패 (Error)	설계 오류, 소프트웨어 오류	불안전한 상태	1D

나. SW 안전요구사항 위험원 결과 요약

표 9 안전성 분석을 통한 위험원 도출 결과

No	위험원 종류	안전 목표
1	커널에 대한 고장이 발생함	SG.1. 자가진단
2	하드웨어에서 고장이 발생함	

3	모든 고장에 대하여 진단하지 못함	
4	모든 고장에 대하여 적절한 조치를 하지 못함	
5	서로 다른 도메인 사이에서 메모리 조작 및 접근함	SG.2. 도메인 분리
6	한 개의 도메인에서 발생한 고장이 다른 도메인에게 전파됨	
7	어플리케이션에서 커널 메모리 영역을 조작 및 접근함	
8	어플리케이션의 고장이 커널 모듈에 전파됨	
9	한 개의 어플리케이션이 다른 어플리케이션 메모리 영역을 조작 및 접근함	
10	한 개의 어플리케이션의 고장이 다른 어플리케이션에게 전파됨	
11	특정 프로세스가 CPU 자원을 독점함	SG.3. 스케줄 예측 가능
12	특정 프로세스의 작업이 완료될 수 있는지 알 수 없음	
13	특정 프로세스의 작업이 종료되는 시점을 알 수 없음	
14	낮은 우선순위를 갖는 프로세스가 무한 대기 상태에 빠짐	
15	우선순위가 낮은 작업이 우선순위가 높은 작업보다 먼저 실행됨	
16	커널이 제어할 수 없는 상황이 발생함	SG.4. 안전상태 설계
17	비정상 상태가 발생했을 때 안전한 상태로 회복하지 못함	
18	특정 요소의 안전상태 회복이 다른 요소의 고장으로 전이됨	
19	특정 요소의 재시작이 다른 요소의 고장으로 전이됨	
20	안전상태로 회복되는 작업보다 다른 작업의 우선순위가 더 높음	
21	정의되지 않은 예외 상황이 발생함	SG.5. 예외 상황 처리
22	부적절한 예외 상황을 정의함	
23	특정 요소의 안전상태 회복이 다른 요소의 고장으로 전이됨	
24	예외 상황에 대하여 대응하지 못함	
25	예외 상황에 대하여 부적절하게 대응함	
26	예외 상황을 감지하지 못함	

	고등급(EAL6 이상) 보안마이크로커널 개발				
	작성자	이용준	소속	고려대학교	연구 책임자	김승주
	작성일	2019-11-23	파일명	2019-SW_REQ-안전성분석서.HWP	
	제목	소프트웨어 요구사항 안전성 분석 보고서			

- 참고문헌 -

[1] IEC, IEC61508. “61508 functional safety of electrical/electronic/programmable electronic safety-related systems.“ International electrotechnical commission (1998).

[2] ISO, ISO26262. “26262: Road vehicles-Functional safety.“ International Standard ISO/FDIS 26262 (2011).

[3] DoD, U. S. “MIL-STD-882C-System Safety Program Requirements.“ US DoD (1993).

[4] FAA System Safety Handbook. “Federal Aviation Administration.“ (2000).

[5] Hobbs, Chris. “Using an IEC 61508-Certified RTOS Kernel for Safety-Critical Systems.“ (2010).

[6] Redmill, Felix, Morris Chudleigh, and James Catmur. System safety: HAZOP and software HAZOP. Chichester: Wiley, (1999).

[7] Kim, Sung Kyu, and Yong Soo Kim. “An evaluation approach using a HARA and FMEDA for the hardware SIL.“ Journal of Loss Prevention in the Process Industries 26.6 (2013): 1212-1220.

[8] Labovský, Juraj, et al. “Model-based HAZOP study of a real MTBE plant.“ Journal of Loss Prevention in the Process Industries 20.3 (2007): 230-237.

[9] SW 안전성 공통 개발 가이드. “정보통신산업진흥원.“ (2016).

[10] 도성룡, 한혁수. (2016). 사용사례와 HAZOP 기반의 위험원 식별 및 테스트케이스 설계 방안. 정보과학회논문지, 43(6), 662-667.

[11] 도성룡, 김은비, 한동준, 한혁수. (2015). UseCase와 HAZOP 기반의 Hazard 식별 방안. 한국정보과학회 학술발표논문집, (), 464-466.