소프트웨어 안전기능 요구사항 명세서

수정일자	수정자	버전	추가/수정 항목	내 용
2019-09-15	이용준	0.1		초안작성
2019-10-04	이용준	0.2		
2019-11-12	이용준	0.5		
2019-11-23	이용준	1.0		

	고등급(EAL6 이상) 보안마이크로커널 개발				
작성자	이용준	소속	고려대학교	연구 책임자	김승주
작성일	2019-11-23	파일명	2019-SW인전기능요구사항명세서.HWP		
제목	소프트웨어 안전기능 요구사항 명세서				

<제목 차례>

<표 차례>

<그림 차례>

I. 목적

본 명세서는 고등급 보안 마이크로 커널(CHAOS)에 필요한 안전기능 요구사항에 대해서 기술하는 것에 그 목적이 있다. 이것을 통해 개발하는 시스템의 안전기능에 대해서 명확하게 정의하고, 시스템의 제약사항과 상호관계에 대해서 설명한다.

II. 용어 정의 및 약어

- Harm(피해) : 사람들에 대한 물리적 부상 또는 환경/자산에 대한 물리적 피해
- Hazard(위험) : 피해의 잠재적 요인
- Risk(위험성) : 피해발생의 확률과 피해의 심각도의 합
- Safety(안전) : 수용 불가능한 위험으로부터 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(안전 기능) : 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 안전 기능을 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

	고등급(EAL6 이상) 보안마이크로커널 개발					
	작성자	이용준	소속	고려대학교	연구 책임자	김승주
	작성일	2019-11-23	파일명	2019-SW인전기능요구사항명세서.HWP		
	제목	소프트웨어 안전기능 요구사항 명세서				

III. 컨텍스트

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

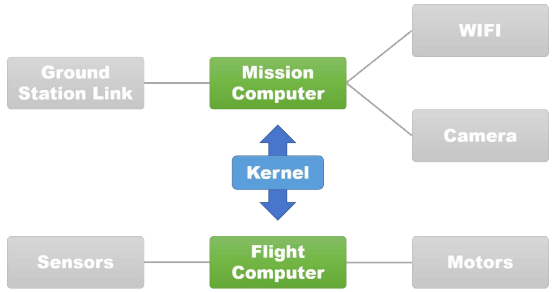


그림 1 상위수준 시스템 구조

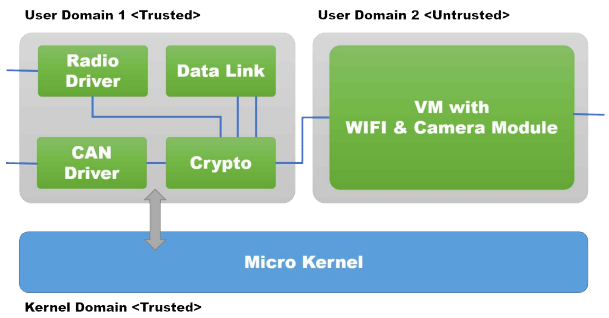


그림 2 하위시스템 및 연계관계

보안 마이크로 커널 탑재 시스템의 하부 구조는 [그림 3]과 같다. 보안 마이크로 커널은 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.

커널 레벨 시스템에는 [그림 4]와 같은 모듈로 구성되어 있다. 세마포어, 뮤텍스,

메시지, 이벤트 등의 모듈은 스케줄러에 의해 동작하며, 이진 세마포어와 메일박스는 세마포어에 의해 동작한다.

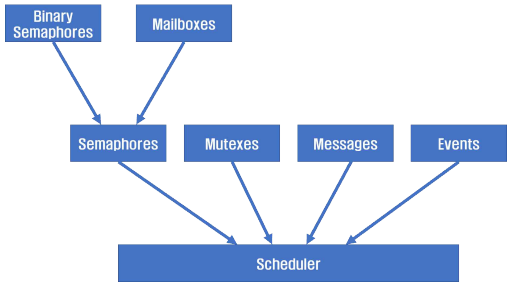


그림 3 CHAOS 커널레벨 시스템 구조

IV. 안전기능 요구사항

3.1 자가진단

3.1.1 세부 기능 명세 도출

안전 목표	자가 진단 기능
1차년도 도출된 안전기능 요구사항	SR.1. 안전한 커널은 하드웨어와 커널 자체의 고장 진단을 수행하는 기능이 있어야 함. 고장이 검출되면 적절한 예외처리가 실행돼야 함.
세부 기능 명 (수행 내용)	SR.1.1. 커널 고장 진단 SR.1.2. 하드웨어 고장 진단 SR.1.3. 진단 후 적절한 조치 필요
세부 기능별 입·출력 인터페이스 (파라미터/반환 값)	인터페이스 명 / 파라미터(입력) / 반환 값 semSignal / X / X semWait / X / X
세부 기능 도출 근거	안전성 분석을 통해 식별된 비정상 활동들에 대한 방지 및 예방하기 위해 세부 기능을 도출함. 비정상 활동 목록은 '소프트웨어 요구사항 안전성 분석 보고서'에 첨부됨.

표 1 자가진단 기능 관련 세부사항 명세

3.1.2 요구사항 준정형 명세

	고등급(EAL6 이상) 보안마이크로커널 개발				
작성자	이용준	소속	고려대학교	연구 책임자	김승주
작성일	2019-11-23	파일명	2019-SW인전기능요구사항명세서.HWP		
제목	소프트웨어 안전기능 요구사항 명세서				

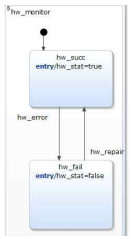
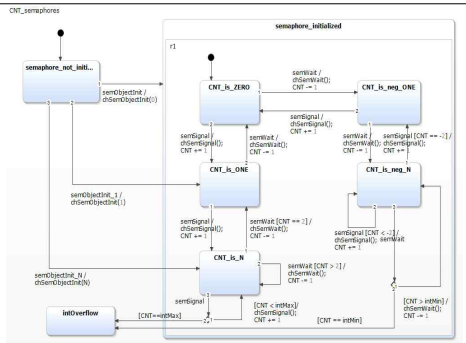
안전 목표	안전기능 세부사항	준정형 명세
자가 진단	하드웨어 고장 진단	
	커널 고장 진단	
	진단 후 적절한 조치 필요	

표 2 자가진단 기능 관련 세부사항 준정형 명세

3.2 도메인 분리

3.2.1 세부 기능 명세 도출

안전 목표	도메인 분리
1차년도 도출된 안전기능 요구사항	SR.2. 한 컴포넌트의 오작동이 다른 프로세스 또는 커널에 영향을 주면 안됨
안전기능	SR.2.1. 커널 요소 간 분리 **SR.2.2. 커널과 어플리케이션 분리** **SR.2.3. 어플리케이션 간에 분리**
입·출력 인터페이스 (파라미터/반환 값)	인터페이스 명 / 파라미터(입력) / 반환 값
세부 기능 도출 근거	안전성 분석을 통해 식별된 비정상 활동들에 대한 방지 및 예방하기 위해 세부 기능을 도출함. 비정상 활동 목록은 '소프트웨어 요구사항 안전성 분석 보고서'에 첨부됨.

표 3 도메인 분리 관련 세부사항 명세

3.2.2 요구사항 준정형 명세

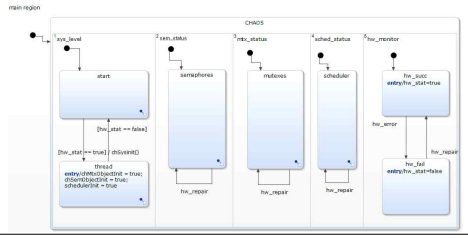
안전 목표	안전기능 세부사항	준정형 명세
도메인 분리	커널 요소간 분리	
	커널과 어플리케이션 분리	-
	어플리케이션 간에 분리	N/A

표 4 도메인 분리 관련 세부사항 준정형 명세

3.3 스케줄링 예측 가능

3.3.1 세부 기능 명세 도출

안전 목표	스케줄링 예측 가능
1차년도 도출된 안전기능 요구사항	SR.3. 시스템에서 작동하는 작업들의 스케줄링을 예측 할 수 있음
안전기능	SR.3.1. 공정한 자원 할당 **SR.3.2. 우선 순위 반전 문제** **SR.3.3. 스케줄 가능성 분석 제공**
입•출력 인터페이스 (파라미터/반환 값)	<table><tr><th>인터페이스 명</th><th>파라미터(입력)</th><th>반환 값</th></tr><tr><td>inheritPriority</td><td>뮤텍스 소유자의 우선순위</td><td>참 / 거짓</td></tr><tr><td>is_schedulable</td><td>thd_id</td><td>참 / 거짓</td></tr></table>
세부 기능 도출 근거	안전성 분석을 통해 식별된 비정상 활동들에 대한 방지 및 예방하기 위해 세부 기능을 도출함. 비정상 활동 목록은 '소프트웨어 요구사항 안전성 분석 보고서'에 첨부됨.

표 5 스케줄링 예측 가능 관련 세부사항 명세

3.3.2 요구사항 준정형 명세

안전 목표	안전기능 세부사항	준정형 명세

	고등급(EAL6 이상) 보안마이크로커널 개발				
작성자	이용준	소속	고려대학교	연구 책임자	김승주
작성일	2019-11-23	파일명	2019-SW인전기능요구사항명세서.HWP		
제목	소프트웨어 안전기능 요구사항 명세서				

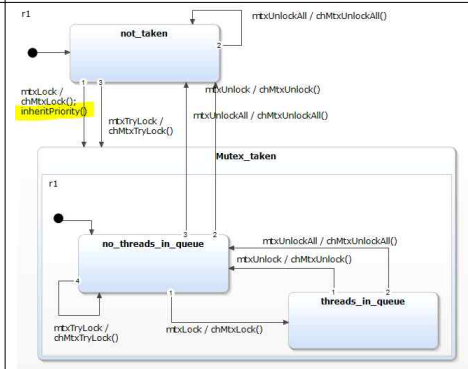
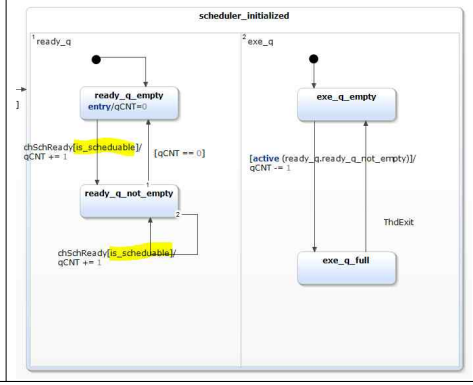
스케줄링 예측 가능	공정한 자원 할당	
	우선 순위 반전 문제	
	스케줄 가능성 분석 제공	

표 6 스케줄링 예측 가능 관련 세부사항 준형정 명세

3.4 안전상태 설계

3.4.1 세부 기능 명세 도출

안전 목표	안전상태 설계
1차년도 도출된 안전기능 요구사항	SR.4. 안전한 커널은 예측하지 못한 상황이 일어난다면 안전한 상태로 회복. 또한, 다른 구성요소에 손상을 주지 않으며, 신속하게 다시 시작할 수 있음
안전기능	SR.4.1. 요소간 독립적 재실행 **SR.4.2. 안전상태로 회복** **SR.4.3. 안전하지 않은 상태 회피**

입•출력 인터페이스 (파라미터/반환 값)	<table><tr><th>인터페이스 명</th><th>파라미터(입력)</th><th>반환 값</th></tr><tr><td>abnormal_resolved</td><td>상대방의 비동기 메시지 상태, 식별자</td><td>참 / 거짓</td></tr><tr><td>!active(client...)</td><td>상대방의 비동기 메시지 상태, 식별자</td><td>참 / 거짓</td></tr></table>
세부 기능 도출 근거	안전성 분석을 통해 식별된 비정상 활동들에 대한 방지 및 예방하기 위해 세부 기능을 도출함. 비정상 활동 목록은 '소프트웨어 요구사항 안전성 분석 보고서'에 첨부됨.

표 7 안전 상태 설계 관련 세부사항 명세

3.4.2 요구사항 준정형 명세

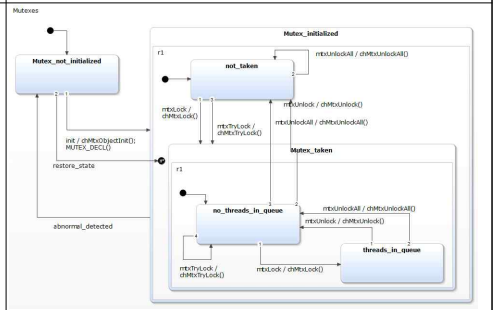
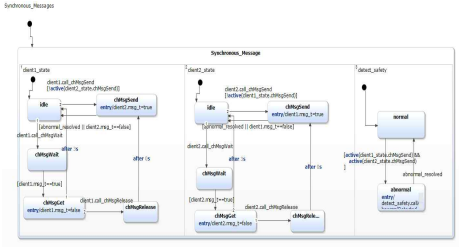
안전 목표	안전기능 세부사항	준정형 명세
안전 상태 설계	요소간 독립적 재실행	-
	안전 상태로 회복	
	안전하지 않은 상태 회피	

표 8 안전 상태 설계 관련 세부사항 준정형 명세

3.5 예외 상황 감지

3.5.1 세부 기능 명세 도출

	고등급(EAL6 이상) 보안마이크로커널 개발				
작성자	이용준	소속	고려대학교	연구 책임자	김승주
작성일	2019-11-23	파일명	2019-SW인전기능요구사항명세서.HWP		
제목	소프트웨어 안전기능 요구사항 명세서				

(보안/안전/기능) 목표	예외 상황 처리
1차년도 도출된 안전기능 요구사항	SR.5. 비정상적인 동작을 감지하고 방지함. 비정상적인 동작은 하드웨어 오류가 발생하거나 소프트웨어 실행이 어려운 경우를 말하며, 이에 안전한 커널은 해당하는 예외처리를 실행
안전기능	SR.5.1. 예외 상황 정의 SR.5.2. 예외 상황 대응 SR.5.3. 예외 상황 감지
입•출력 인터페이스 (파라미터/반환 값)	<table><tr><th>인터페이스 명</th><th>파라미터(입력)</th><th>반환 값</th></tr><tr><td>call_chMBAbnormalAlert</td><td>비정상 행위 식별자, 메일 박스 식별자 리스트</td><td>참 / 거짓</td></tr></table>
세부 기능 도출 근거	안전성 분석을 통해 식별된 비정상 활동들에 대한 방지 및 예방하기 위해 세부 기능을 도출함. 비정상 활동 목록은 '소프트웨어 요구사항 안전성 분석 보고서'에 첨부됨.

표 9 예외 상황 처리 관련 세부사항 명세

3.5.2 요구사항 준정형 명세

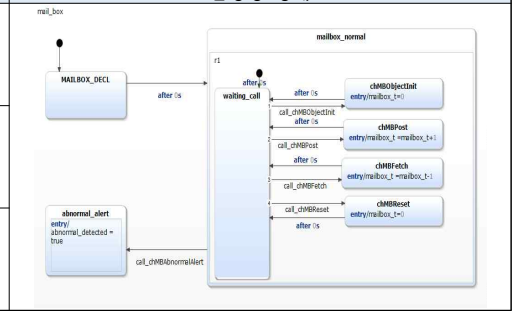
안전 목표	안전기능 세부사항	준정형 명세
예외 상황 처리	예외 상황 정의	
	예외 상황 대응	
	예외 상황 감지	

표 10 예외 상황 처리 관련 세부사항 준정형 명세

- 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.

