SIL4 인증문서 한글 표준양식(템플릿) 적용사례 연구

황경환*, 이길용*, 이기서†

Kyung-Hwan Hwang*, Kil-Yong Lee*, Key-Seo Lee†

Abstract: To achieve the SIL4 Certification of train control system, each signaling manufacturer have to invest much resources(Man power, Time) to prepare various kinds of safety supporting evidence documents in English or English forms, for example, Safety Case documents like Quality Control evidence, Safety Management evidence and Functional Safety management evidence. This paper suggest the man-power and time minimizing method when preparing SIL4 supporting evidence documents by use of standard Korean Forms(Templets) based on system life cycle and EN50126/EN50128/EN50129 standards.

Keywords **:** SIL4 Certification, Safety supporting evidence, Standard Korean Forms(Templets)

초 록 열차제어시스템 SIL4 인증 획득을 위해 각 신호제조사에서는 품질관리증거, 안전성관리증거 및 기능안전성증거자료 등 안전성 입증을 위한 많은 종류의 문서를 주로 영문으로 된 양식 또는 영문을 사용하여 작성하고 있어서 많은 자원(기술인력, 시간 등)을 투입하고 있는 실정이다. 본 논문은 신호제조사에서 SIL4 인증 획득을 위한 안전성 입증자료 작성시에 제품 수명주기 단계별로 EN50126/EN50128/EN50129/ 규격에 준한 한글 표준양식(템플릿)을 적용하여 SIL4 인증 자료 작성을 위한 투입인원 및 기간 단축방안을 제시하고자 함.

주요어 : SIL4 인증, 안전성 입증 자료, 한글 표준양식(템플릿)

1. 서 론

열차제어시스템을 구성하는 하드웨어의 장애나 소프트웨어에 포함되어 있는 설계 오류 또는 운전요원의 인적 오류 등은 시스템의 안전과 관련되어 있는 장치 또는 시스템에 장애를 유발시켜 사람의 사상사고나 시설물 파손 등을 발생시킬 수 있다. 이러한 위험 또는 사고의 발생을 차단하거나 저감하기 위한 방법으로 제 3 자에 의한 안전성 평가와 같은 관리 활동이 요구된다

안전 무결성 수준(Safety Integrity Level, SIL)이란 Safety Function 에 의해 제공되는 위험저감 수준을 나타낸다. 각각의 Safety Function 에 대하여 표준에 따라 안전 무결성 등급이 정의되며(SIL1~SIL4), SIL 등급의 차가 높을수록 안전성 평가시 요구되는 안전 무결성 수준이 높아져서 그만큼 SIL 인증을 위해 준비해야하는 문서가 많아지고 문서 수준이 높아져야 하므로 SIL4 인증 자료 준비를 위해 제조사에서 많은 자원을 투입하고 있다.

* 철도신호사업연구조합 R&D팀
† 교신저자: 광운대학교 로봇학부 교수 (kslee@kw.ac.kr)

2. 본 론

2.1 안전성 평가 절차

안전성 평가에서 시스템 수명주기 단계는 크게 요구사항 단계와 설계/구현 단계로 나눌 수 있으며, 각 단계별 안전성 평가 활동은 다음 Table 1과 같다.

Table 1. 안전성 평가 활동

No	단계	안전성 평가 활동
1	요구사항 단계 (개념 단계)	▪ 안전성 평가 계획 수립 ▪ 기술 및 기능에 대한 안전성 원리 평가 ▪ 요구사항 및 계획 문서 평가 ▪ 안전성 심사 ▪ 상태 평가 보고서
2	설계/구현 단계 (세부 단계)	▪ 세부 기술 평가 ▪ 안전성 관리, 자료 준비, 형상 관리, 시험 등의 심사 ▪ 고장 주입 시험 및 기능 시험 ▪ 최종 평가 보고서

2.2 안전성 승인 조건

EN 50129에 따르면 안전성 승인 조건으로 다음과 같은 사항들을 규정하고 있다.

1) 종합안전성보고서(Safety Case)

종합안전성보고서는 명시된 안전성 요건을 만족한다는 것을 증빙하는 서류이다. 안전에 관련된 시스템이 대상 애플리케이션에 대해 충분히 안전하다는 것을 승인할 목적으로 요구되는 조건은 크게 다음 세 가지 측면에 대한 증거 자료이다.

- 품질 관리 증거
- 안전성 관리 증거
- 기능 및 기술 안전성 증거

안전에 관련된 시스템이 충분히 안전하다는 것으로 승인받기 전에 장치, 하부시스템 및 시스템 수준에서 위 세 가지 측면의 모든 조건들을 만족해야 한다. 이러한 조건을 만족한다는 내용의 증거를 구조화된 안전성 입증 문서에 포함해야 하는데 이를 종합안전성보고서(Safety Case)라고 한다. 종합안전성보고서는 일반제품, 응용분야 또는 특정 응용분야에 대한 안전성 승인을 얻기 위해서 안전성 인증기관에 제출할 전반적인 서류로 이루어진 근거로 Fig. 1과 같이 구성된다.

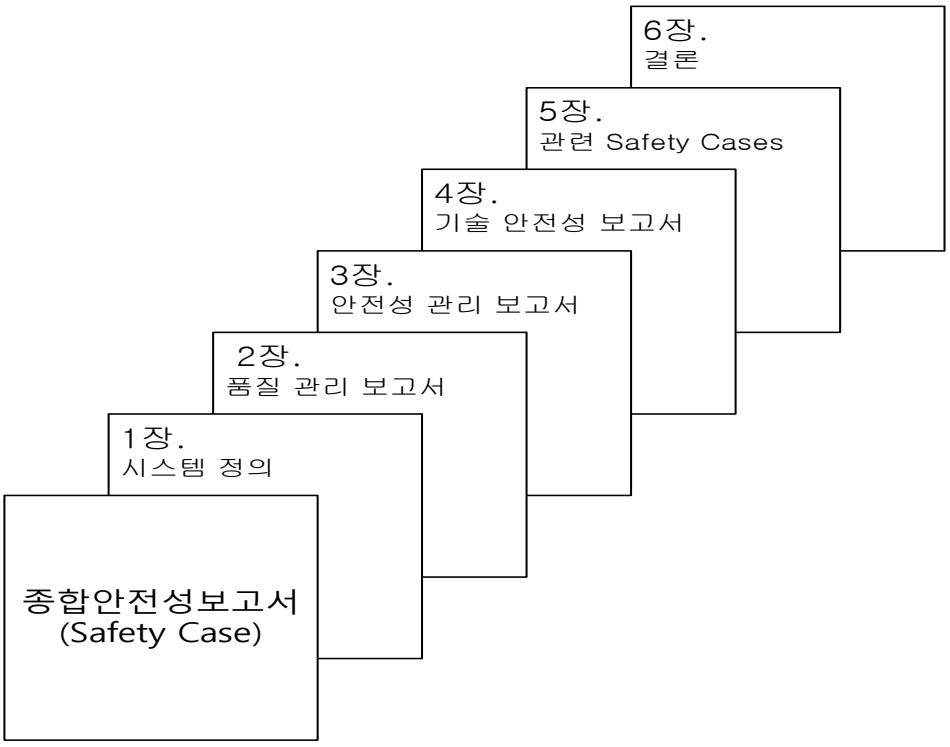


Fig. 1 종합안전성보고서(Safety Case) 구조

2) 품질관리 증거

안전성 승인을 위해 만족해야 할 첫 번째 조건은 시스템/하부시스템/장치의 품질이 수명주기 동안 효과적인 품질관리체계에 의해 관리되고, 지속적으로 관리되어야 한다는 것이다. 이를 입증하는 문서로 이루어진 증거를 품질관리 보고서에 제시해야 한다. 품질관리체계의 목적은 수명주기의 각 단계에서 인적 오류의 발생을 최소화하고, 시스템, 하부시스템 혹은 장치에서 계통 결함으로 인한 위험도를 저감시키기 위한 것이다. 품질관리에 대한 요구사항의 준수는 SIL 1 에서 SIL4 까지 필수이다.

3) 안전성 관리 증거

안전성 승인을 위한 만족해야 할 두 번째 조건은 시스템, 하부시스템 및 장치의 안전성이 효과적인 안전성 관리 절차에 의해 관리되고 지속적으로 관리되어야 한다는 것이다. 이 절차의 목적은 수명주기 동안 안전 관련 인적오류의 발생을 저감시키기 위한 것이고, 안전과 관련된 계통 결함으로 인한 잔여 위험도를 최소화하기 위한 것이다. 이를 입증하는 문서로 이루어진 증거를 안전성관리 보고서에 제시해야 한다. 안전성 관리 절차의 적용은 SIL 1 에서 SIL4 까지 필수이다.

2.3 안전성 평가 대상 산출물

안전성 평가는 시스템, 하드웨어 및 소프트웨어(ASIC 포함)를 대상으로 수행하게 되며 SIL4인증을 위해 각 수명주기 단계별로 요구되는 일반적인 안전성 평가 대상 산출물 목록은 Table 2와 같다.

Table 2. 안전성 평가 대상 산출물

No	항목	ID	수명주기단계	산출물
1	시스템	1.1	계획	Safety plan
				Quality management plan
				System configuration management plan
				System verification and validation plan
		1.2	위험도 분석	Risk analysis report (PHA)
				Hazard Log
		1.3	시스템 요구사항	System requirements specification
				System safety requirements specification
				System requirements verification report
				System validation test plan
				Traceability matrix
		1.4	HW 설계	System architecture specification
				System FMEA
				HW design specification
				Drawing
				HW test plan and report
				RAM prediction
				Detail hardware FMEA
				System reliability modelling: FTA
				HW architecture and design verification report
				Manuals for operation, maintenance, installation
		1.5	시스템 검증	System validation test report
				Environmental Stress and EMC test report
				Internal audit report for quality and safety management
				Generic Application Safety Case
2	소프트웨어	2.1	계획	SW quality assurance plan
				Software quality assurance verification report
				SW configuration management plan
				SW verification & validation plan
		2.2	SW 요구사항	SW requirements specification
				SW requirements test specification
				SW requirements verification report
		2.3	아키텍처 및 설계	SW architecture specification
				SW design specification
				SW Interface Specifications
				SW integration test specification
				SW/HW integration test specification
				SW architecture & design verification report
		2.4	컴포넌트 설계	SW component design specification
				SW component test specification
				SW component design verification report
		2.5	컴포넌트 구현 및 시험	SW source code and supporting documentation
				SW coding guide and Coding standard
				SW component test report
				SW source code verification report
		2.6	통합	SW integration test report
				SW/HW integration test report
				SW integration verification report
		2.7	SW 검증	Overall SW test report
				SW validation report

No	항목	ID	수명주기단계	산출물
				Tools validation report
				Software maintenance plan
				SW Release note
3	ASIC소프트웨어	3.1	계획	ASIC SW quality assurance plan
				ASIC Software quality assurance verification report
				ASIC SW configuration management plan
				ASIC SW verification validation plan
		3.2	SW 요구사항	ASIC SW requirements specification
				ASIC SW requirements test specification
				ASIC SW requirements verification report
		3.3	아키텍처 및 설계	ASIC SW architecture specification
				ASIC SW design specification
				ASIC SW Interface Specifications
				ASIC SW integration test specification
				ASIC SW/HW integration test specification
				ASIC SW architecture & design verification report
		3.4	컴포넌트 설계	ASIC SW component design specification
				ASIC SW coding guide and Coding standard
				ASIC SW component test specification
				ASIC SW component design verification report
		3.5	컴포넌트 구현 및 시험	ASIC SW source code and supporting documentation
				ASIC SW component test report
				ASIC SW source code verification report
		3.6	통합	ASIC SW integration test report
				ASIC SW/HW integration test report
				ASIC SW integration verification report
		3.7	SW 검증	ASIC SW Overall test report
				ASIC SW validation report
				ASIC Tools validation report
				ASIC Software maintenance plan
				ASIC SW Release note

2.4 시스템 개발 수명주기

SIL4 인증시 제작사가 준수해야 할 시스템에 대한 세부 개발 수명주기에 대한 정의는 Fig. 2와 같으며, 기본적인 시스템 수명주기에 하드웨어 개발주기와 소프트웨어 개발 주기를 포함하고 있다. 열차제어시스템을 개발하는 제작사는 이 시스템 개발 수명주기에 따라서 제품을 개발해야 한다. 제작사는 시스템 개발 주기에 따라 Table 2에서 정의한 안전성 평가 대상 과업을 이행하고 산출물을 제출해야 한다.

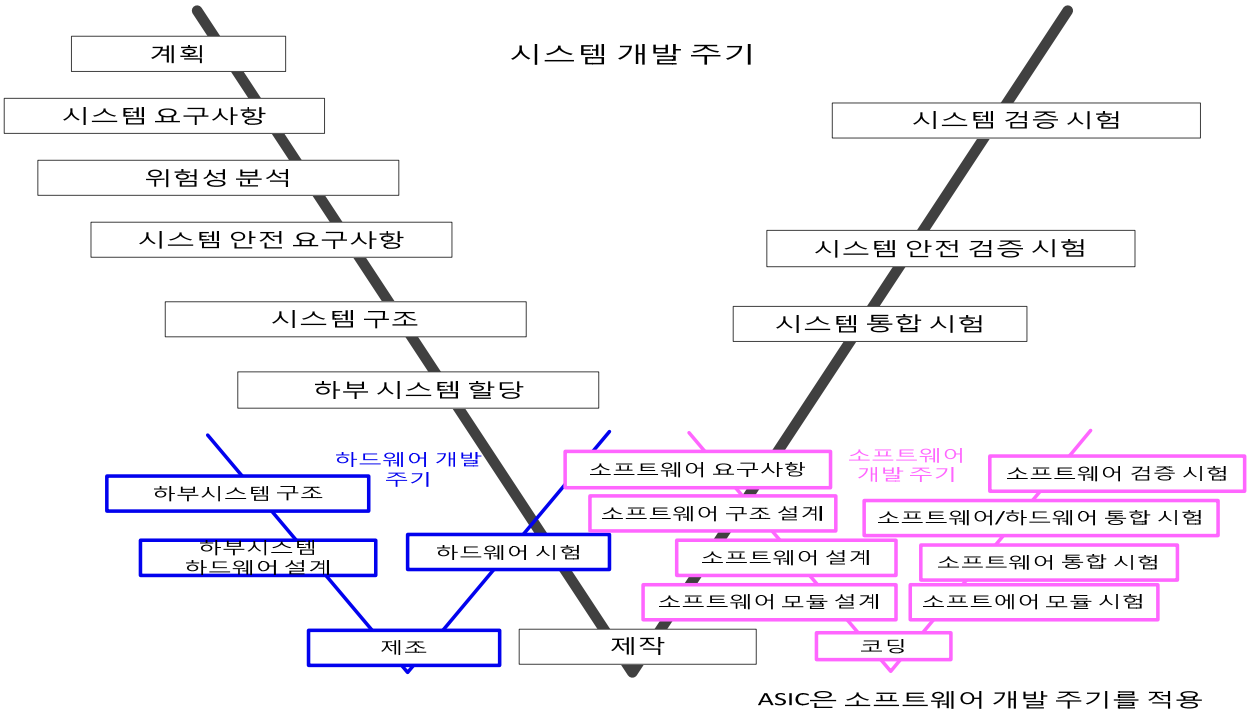


Fig.2 시스템 개발 주기

2.5 한글 표준 문서 양식(템플릿) 목록

철도신호사업연구조합에서는 안전성 활동의 결과를 작성할 수 있는 한글표준문서 양식을 개발하여 국제적 ISA인증기관의 감수를 받았으며 열차제어시스템 SIL4 인증을 준비중인 제작사에 제공예정이다. 철도신호사업연구조합이 제공하게 될 시스템 개발 수명주기 단계 관련 범주별 한글표준문서양식(템플릿) 목록은 Table 3과 같다. 단, 제작사는 철도신호사업연구조합이 제공하는 문서 양식을 이용하되 이에 국한되지 않으며 필요 시 SIL4 인증 대상에 따라 작성내용을 추가 또는 삭제할 수 있다

Table 3. 한글 표준 문서 양식(템플릿) 목록

No	항목	ID	수명주기 단계	문서 양식명
1	시스템	1.1	계획	RSRA-Safety Certification Plan Outline-Template
				RSRA-QAP Checklist
				RSRA-SQAP Checklist
		1.2	위험도 분석	RSRA-HAZOP Form Template
				RSRA-PHA-SHA-SSHA-OSHA Template
		1.3	시스템 요구사항	RSRA-System Safety Requirements Template
				RSRA-Requirements Management Template
		1.4	HW 설계	RSRA-HW DD Template
				RSRA-HW RS Template

No	항목	ID	수명주기 단계	문서 양식명
				RSRA-Interface Control Document-ICD Template
				RSRA-PHW Module Design Specification Template
				RSRA-PHW Module Test Plan Template
				RSRA-PHW Module Test Report Template
				Safety Process and Output Doc Summary EN50129
2	소프트웨어	2.1	계획	RSRA-SW Validation Plan Template
				RSRA-SW Verification Plan Template
				RSRA-SW VALIDATION PLAN Checklist
				RSRA-SW VERIFICATION PLAN Checklist
				RSRA-CENELEC_SW_DEV_Process Summary
		2.2	SW 요구사항	RSRA-SW Requirement Specification Template
				RSRA-SW Requirement Verification Report Template
				RSRA-SW RS Checklist
				RSRA-SW RT_SPEC Checklist
				RSRA-SW Requirements Test Specification Template
				RSRA-SW Requirements Verification Report Template
		2.3	아키텍처 및 설계	RSRA-SW HW Integration Test Plan Template
				RSRA-SW Integration Test Plan Template
				RSRA-SW HW ITP Checklist
				RSRA-SW ITP Checklist
				RSRA-SW Architecture Specification Template
				RSRA-SW Design Specification Template
				RSRA-SW Integration Test Procedure Template
				RSRA-SW ARCH&DESIGN Ver Checklist
				RSRA-SW ARCH_SPEC Checklist
				RSRA-SW DS Checklist
				RSRA-SW Architecture Design and Requirements Verification Report Template
		2.4	컴포넌트 설계	RSRA-SW Module Design Specification Template
				RSRA-SW Module Test Report Template
				RSRA-SW Module Test Specification Template
				RSRA-SW MDS Checklist
				RSRA-SW Module_Ver Checklist
		2.5	컴포넌트 구현 및 시험	RSRA-Coding Standard Checklist
				RSRA-SW CTR Checklist
		2.6	통합	RSRA-SW Integration Test Report Template
				RSRA-SW Integration Test Verification Report Template
		2.7	SW 검증	RSRA-SW Validation Report Checklist

2.6 한글 표준문서양식(템플릿) 예

1) 위험도 분석 템플릿(RSRA-PHA-SHA-SSHA-OSHA Template)

Hazard Analyses
위험원 분석
<<Template>>

Project Name: 프로젝트 명
Doc. Name: 문서 명
Revision: 문서 개정 번호

	Name 이름	Date 날짜	Signature 서명
Author 작성	Name	YYYY-MM-DD	Signature
1st Reviewer 검토 1	Name	YYYY-MM-DD	Signature
2nd Reviewer 검토 2	Name	YYYY-MM-DD	Signature
Approver 승인	Name	YYYY-MM-DD	Signature

Copyright 른구

CONTENTS 목차

Index **page**

1 References 참고 7
1.1 Reference Documents 참고 문서 7
1.2 Acronyms 약어 7
1.3 Definitions 정의 10
2 System Definition – [*System Name*] 시스템 정의 – [*시스템 명칭*] 12
3 Introduction to Hazard Analysis 위험원 분석 소개 13
4 General Considerations 일반적인 고려사항 19
5 Creating Hazard Log 위험원 기록 작성 21
6 Preliminary Hazard Analysis Outline 예비 위험원 분석 개요 23
7 Hazard Categories 위험원 카테고리 23
Hazard Severity Categories 위험원 심각도 카테고리 24
8 Hazard Probability and "Performance" vs "SIL" Level 위험원 가능성 및 "성능" 대 "SIL" 레벨 26
9 Hazard Evaluation Table / Thresholds 위험원 평가 표/한계값 28
10 Preliminary Hazard Analysis – Definitions 예비 위험원 분석 – 정의 31
11 Hazard Analysis: 위험원 분석 32
12 PHA – Environmental Hazards (Sheet 1 of 2): 환경적 위험원 33
13 PHA/OSHA - Installation / Commissioning Hazards (Sheet 1 of 2): 설치/시운전 위험원 33
14 SHA/SSHA: Electrical Hazards (inc. SIHA and SSIHA): 전기적 위험원 34
15 PHA/SHA – Mechanical Hazards (Sheet 1 of 2): 기계적 위험원 34
16 PHA/OSHA – Operational Hazards (Sheet 1 of 4): 운영 위험원 35
17 PHA/OSHA – Maintenance Hazards 유지보수 위험원 36
18 SHA – System Hazard Analysis 시스템 위험원 분석 37

Copyright 른구

2 System Definition – [*System Name*] 시스템 정의 – [*시스템 명칭*]

The [system name] Controller system is a ..... System overview and description.
The [name] system is characterized by the following properties.

[시스템 명칭] 컨트롤러 시스템은 ~~~ 시스템 개요 및 설명
[명칭] 시스템은 다음과 같은 특징이 있다.

Figure 2.1 High Level Block Diagram 상위 레벨 블록 다이어그램

The following System Modes of operation shall also be considered and analyzed.

1) Configuration Mode – The system is configured for various operational parameters, threshold levels and special modes, functions, indicators etc.

2) Test / Diagnostic Mode (if applicable) – In this mode the system runs self-test routines that include interrogating sensors and checking com ports etc.

3) Active Mode – The system shall monitor incoming signals from gas transmitters and other process monitors, displays the measured concentrations, make decisions based on the installed programs, actuate alarms to alert users of safety critical situations, and record events in a datalog. The system shall continuously execute the user logic programs (programmed via ComSafe style software). Typical programmed functions include OR, AND, NOR, NAND, VOTING, timing delays, unlatching/latching conditions, increasing/falling alarms and trouble notification. Up to 5 functions (tasks) can be tied together to perform a system function.

4) Fault Mode – In case of a fault condition the information (fault) shall be displayed on the LCD monitor (unique fault/error ID, "type", device, component, relay in a relay module, etc.), the appropriate fault LED(s) are activated, the trouble signal is sent out, and the appropriate trouble relay(s) (located on the CM) are de-energized. Optionally, the system sends out an email, SMS message, or places a phone call to a pre-defied list of "users".

다음 운영 시스템 모드를 고려하고 분석해야 한다.

1) 구성 모드 – 시스템은 다양한 운영 파라미터, 한계 레벨 및 특별한 모드, 기능, 표시장치 등으로 구성되어 있다.

Copyright 른구

2) 시험/진단 모드 (가능할 경우) – 본 모드에서 시스템은 센서에 신호 전송 및 컴포트 체크 등을 포함하는 자가 시험 루틴을 동작시킨다.

3) 활성화 모드 – 시스템은 가스 송신기 및 기타 프로세스 모니터로부터 수신한 신호 모니터하고 측정된 concentrations 를 표시하고 설치된 프로그램에 기반하여 결정을 내리며 안전 필수(safety critical) 상황을 사용자들에게 알리기 위한 알람을 동작시키고 데이터로그에 사건을 기록한다. 시스템은 사용자 논리 프로그램(Comsafe 스타일 소프트웨어에 의해 프로그램 됨)을 지속적으로 실행해야 한다. 일반적으로 프로그램 된 기능은 OR, AND, NOR, NAND, VOTING, 타이밍 지연, 열림/잠김 조건, 상승/하강 알람 및 문제 발생 공고를 포함한다. 시스템 기능 수행을 위해 기능(업무) 5 개 까지는 하나로 묶을 수 있다.

4) 결함 모드 – 결함 조건인 경우, 정보(결함)는 LCD 모니터에 표시되어야 한다 (고유의 결함/에러 ID, "타입", 장치, 구성품, 릴레이 모듈 내 릴레이 등). 적합한 결함 LED 는 활성화 상태이다. 문제 신호가 송신된다. 적합한 문제 릴레이(CM 에 위치)가 비여자 상태이다. 선택적으로, 시스템은 "사용자"의 사전 정의 목록으로 이메일, SMS 메시지를 송신하거나 전화를 건다.

Figure 2.2 [System Name]

3 Introduction to Hazard Analysis 위험원 분석 소개

The over-arching goal of the program from which the need for this PHA derived, is to perform a Failure Modes and Effects Analysis (FMEA) and Component FMEDA on the [system here] to assure that all risks are identified, analysed, scaled and if, necessarily, mitigated to the level required to achieve the desirable Safety Integrity Level Performance.
모든 위험성이 식별, 분석, 조정 그리고 필요 시 안전 무결성 레벨 성능 성취하기 위해 요구되는 레벨로 경감시켰음을 보장하기 위하여 PHA 의 요구사항으로부터 도출된 프로그램의 주요 목표는 고장유형 및 영향 분석(FMEA) 및 *[시스템 명칭]*의 구성품 FMEDA 를 수행하는 것이다.

Failure Modes and Effects Analysis (FMEA) is methodology for analysing potential reliability problems early in the development cycle where it is easier to take actions to overcome these issues, thereby enhancing reliability through design.

Copyright 른구

2) 소프트웨어 확인 계획서 템플릿(RSRA-Software Verification Plan Template)

Software Verification Plan

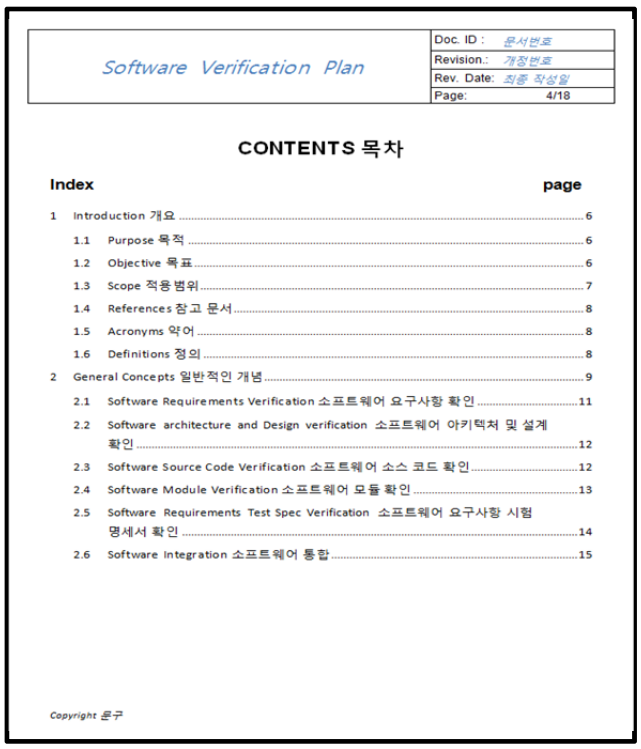
Doc. ID :	문서번호
Revision.:	개정번호
Rev. Date:	최종 작성일
Page:	1/18

Software Verification Plan
소프트웨어 확인 계획서
<<Template>>

Project Name: 프로젝트 명
Doc. Name: 문서 명
Revision: 문서 개정 번호

	Name 이름	Date 날짜	Signature 서명
Author 작성	Name	YYYY-MM-DD	Signature
1st Reviewer 검토 1	Name	YYYY-MM-DD	Signature
2nd Reviewer 검토 2	Name	YYYY-MM-DD	Signature

Copyright 문구



Software Verification Plan

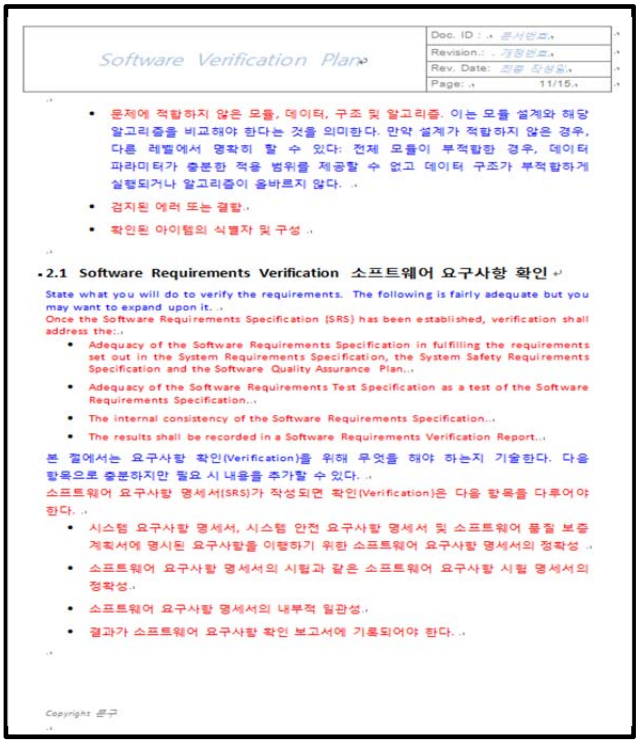
Doc. ID :	문서번호
Revision.:	개정번호
Rev. Date:	최종 작성일
Page:	4/18

CONTENTS 목차

Index **page**

1 Introduction 개요 6
1.1 Purpose 목적 6
1.2 Objective 목표 6
1.3 Scope 적용범위 7
1.4 References 참고 문서 8
1.5 Acronyms 약어 8
1.6 Definitions 정의 8
2 General Concepts 일반적인 개념 9
2.1 Software Requirements Verification 소프트웨어 요구사항 확인 11
2.2 Software architecture and Design verification 소프트웨어 아키텍처 및 설계 확인 12
2.3 Software Source Code Verification 소프트웨어 소스 코드 확인 12
2.4 Software Module Verification 소프트웨어 모듈 확인 13
2.5 Software Requirements Test Spec Verification 소프트웨어 요구사항 시험 명세서 확인 14
2.6 Software Integration 소프트웨어 통합 15

Copyright 문구



- 문제에 적합하지 않은 모듈, 데이터, 구조 및 알고리즘. 이는 모듈 설계와 해당 알고리즘을 비교해야 한다는 것을 의미한다. 만약 설계가 적합하지 않은 경우, 다른 레벨에서 명확히 할 수 있다: 전체 모듈이 부적합한 경우, 데이터 파라미터가 충분한 적용 범위를 제공할 수 없고 데이터 구조가 부적합하게 실행되거나 알고리즘이 올바르지 않다.
- 검지된 에러 또는 결함.
- 확인된 아이템의 식별자 및 구성

2.1 Software Requirements Verification 소프트웨어 요구사항 확인

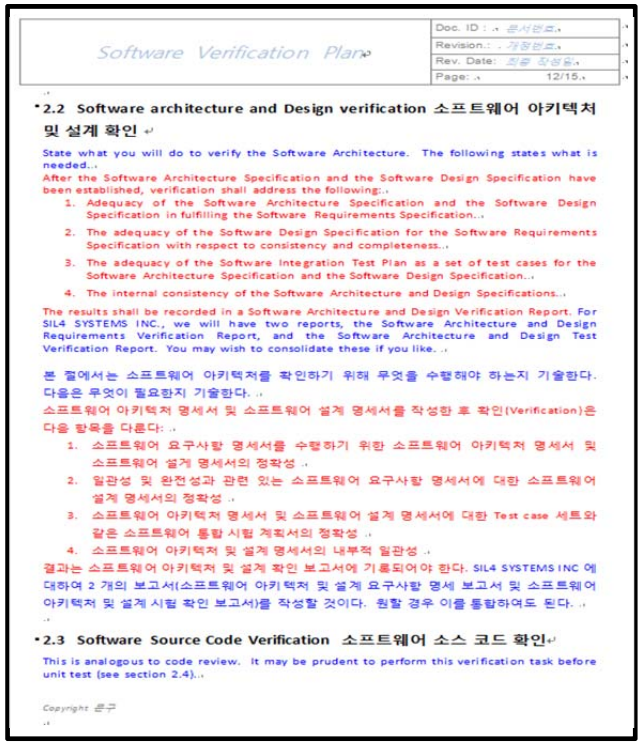
State what you will do to verify the requirements. The following is fairly adequate but you may want to expand upon it.
Once the Software Requirements Specification (SRS) has been established, verification shall address the:

- Adequacy of the Software Requirements Specification in fulfilling the requirements set out in the System Requirements Specification, the System Safety Requirements Specification and the Software Quality Assurance Plan.
- Adequacy of the Software Requirements Test Specification as a test of the Software Requirements Specification.
- The internal consistency of the Software Requirements Specification.
- The results shall be recorded in a Software Requirements Verification Report.

본 절에서는 요구사항 확인(Verification)을 위해 무엇을 해야 하는지 기술한다. 다음 항목으로 충분하지만 필요 시 내용을 추가할 수 있다.
소프트웨어 요구사항 명세서(SRS)가 작성되면 확인(Verification)은 다음 항목을 다루어야 한다.

- 시스템 요구사항 명세서, 시스템 안전 요구사항 명세서 및 소프트웨어 품질 보증 계획서에 명시된 요구사항을 이행하기 위한 소프트웨어 요구사항 명세서의 정확성
- 소프트웨어 요구사항 명세서의 시험과 같은 소프트웨어 요구사항 시험 명세서의 정확성.
- 소프트웨어 요구사항 명세서의 내부적 일관성.
- 결과가 소프트웨어 요구사항 확인 보고서에 기록되어야 한다.

Copyright 문구



2.2 Software architecture and Design verification 소프트웨어 아키텍처 및 설계 확인

State what you will do to verify the Software Architecture. The following states what is needed.
After the Software Architecture Specification and the Software Design Specification have been established, verification shall address the following:

1. Adequacy of the Software Architecture Specification and the Software Design Specification in fulfilling the Software Requirements Specification.
2. The adequacy of the Software Design Specification for the Software Requirements Specification with respect to consistency and completeness.
3. The adequacy of the Software Integration Test Plan as a set of test cases for the Software Architecture Specification and the Software Design Specification.
4. The internal consistency of the Software Architecture and Design Specifications.

The results shall be recorded in a Software Architecture and Design Verification Report. For SIL4 SYSTEMS INC., we will have two reports, the Software Architecture and Design Requirements Verification Report, and the Software Architecture and Design Test Verification Report. You may wish to consolidate these if you like.

본 절에서는 소프트웨어 아키텍처를 확인하기 위해 무엇을 수행해야 하는지 기술한다. 다음은 무엇이 필요한지 기술한다.
소프트웨어 아키텍처 명세서 및 소프트웨어 설계 명세서를 작성한 후 확인(Verification)은 다음 항목을 다룬다:

1. 소프트웨어 요구사항 명세서를 수행하기 위한 소프트웨어 아키텍처 명세서 및 소프트웨어 설계 명세서의 정확성
2. 일관성 및 완전성과 관련 있는 소프트웨어 요구사항 명세서에 대한 소프트웨어 설계 명세서의 정확성
3. 소프트웨어 아키텍처 명세서 및 소프트웨어 설계 명세서에 대한 Test case 세트와 같은 소프트웨어 통합 시험 계획서의 정확성
4. 소프트웨어 아키텍처 및 설계 명세서의 내부적 일관성

결과는 소프트웨어 아키텍처 및 설계 확인 보고서에 기록되어야 한다. SIL4 SYSTEMS INC 에 대하여 2 개의 보고서(소프트웨어 아키텍처 및 설계 요구사항 명세 보고서 및 소프트웨어 아키텍처 및 설계 시험 확인 보고서)를 작성할 것이다. 원할 경우 이를 통합하여도 된다.

2.3 Software Source Code Verification 소프트웨어 소스 코드 확인

This is analogous to code review. It may be prudent to perform this verification task before unit test (see section 2.4).

Copyright 문구

2.7 한글 표준문서양식(템플릿) 적용

열차제어시스템 SIL4 인증을 위한 일반적인 안전성 평가대상 산출물은 2.3장 Table2와 같으며 이러한 산출물 작성 지원을 위한 한글 표준문서양식(템플릿) 목록은 2.5장 Table3과 같다. 국토교통과학 기술진흥원 연구개발과제인 “일반 및 고속철도용 무선통신 및 제어시스템 실용화” 과제의 신호분야 KRTCS(일반•고속철도) SIL4 인증 시 적용예정이며 향후 중소 신호 제조사에서 열차제어시스템(차상신호장치,지상신호장치 등) SIL4 인증 추진 시에도 철도신호사업연구조합을 통해 점차적으로 확대 적용예정이다.

3. 결 론

열차제어시스템 SIL4 인증 시 획득을 위해 준비해야 하는 안전성입증 자료는 ISA 기관 인증을 받기 위해서 현재 대부분 영문으로 작성되고 있어 중소 신호제조사에서는 SIL4 인증을 받고자 하더라도 자원투입에 많은 어려움을 겪고 있는 실정이다.
철도신호사업 연구조합에서는 신호제조사의 SIL4 인증 지원체계를 구축 중에 있으며 이의 일환으로 SIL4 인증문서 한글표준양식(템플릿)을 개발하여 ISA 인증기관의 감수를 받아 완성하였다.

현재 국토교통과학기술진흥원 과제이며 한국철도시설공단이 주관연구기관인 “일반 및 고속철도용 무선통신 및 제어시스템 실용화” 연구과제의 신호분야 KRTCS(일반•고속철도) SIL4 인증 제조사(참여기업)에서 안전성 입증자료 준비에 적용 예정이며 SIL4 인증 획득을 위해 안전성 입증자료 문서준비에 투입해야 하는 기술인력과 시간을 대폭 줄일 수 있다고 예상한다.

감사의 글

본 연구는 국토교통부 일반 및 고속철도용 무선통신 및 제어시스템 실용화 사업의 연구비지원(과제번호15RTRP-B089552-02)에 의해 수행되었습니다.

참고문헌

[1] IEC 61508, “Functional safety of electrical/ electronic/ programmable electronic safety-related systems,” IEC, Geneva, Switzerland, April 2010.

[2] EN 50126:1999, “Railway applications - The specification and demonstration of Reliability, Availability Maintainability and Safety (RAMS)”

[3] EN 50128:2011, “Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems”

[4] EN 50129:2003, “Railway applications - Communications, signalling and processing systems - Safety-related electronic systems for signaling”

[5] 철도신호사업연구조합 (2015) “SIL 인증범위 및 대상선정 정의”

[6] 철도신호사업연구조합 (2015) “안전성평가계획수립 및 지원체계”