"THE Software Engineering"

솔루션링크 아카데미 – 기능안전 과정

2019년 하반기 교육 과정 및 일정

㈜솔루션링크
서울 사무소: 서울 서초구 강남대로27길 7-21 동산빌딩 2층, 전화: 02-576-2202
대전 본사 및 연구소: 대전시 유성구 테크노9로 35, 406 (대전지능로봇산업화센터), 전화: 042-861-4202

SOLUTIONLINK

2019년도 하반기 교육 과정 및 일정

기능안전 교육 과정

No.	교육 과정 명	시 간	장 소	일 정	비 용 (VAT불포함)	비 고
1	A-SPICE(v3.1) 실무적용 관점의 이해	2일	솔루션링크 교육장	'19/6/4(화) ~ 5(수)	34만원	
2	ISO 26262 2nd Edition - 구성 및 개념 이해	2일	솔루션링크 교육장	'19/6/12(수) ~ 13(목)	34만원	
3	자율주행 차량의 안전 확보(SOTIF, ISO/PAS 21448)	1일	솔루션링크 교육장	'19/6/14(금)	20만원	
4	ISO 26262 2nd Edition - 시스템 개발 (안전설계, 안전분석(FMEA/FTA), 테스팅)	3일	솔루션링크 교육장	'19/6/19(수) ~ 21(금)	51만원	
5	ISO 26262 2nd Edition - 하드웨어 개발 (안전설계, FMEDA, 테스팅)	3일	솔루션링크 교육장	'19/6/26(수) ~ 28(금)	51만원	
6	ISO 26262 2nd Edition - 소프트웨어 개발 (안전설계, 안전분석(FTA/FMEA), 테스팅)	3일	솔루션링크 교육장	'19/7/3(수) ~ 5(금)	51만원	
7	ISO26262 2nd Edition - SW 안전 메커니즘 이해 및 구현	2일	솔루션링크 교육장	'19/7/10(수) ~ 11(목)	34만원	
8	ISO26262 2nd Edition - SW 테스팅	1일	솔루션링크 교육장	'19/7/12(금)	20만원	
9	자동차 전장시스템 보안 (Automotive Cybersecurity)	2일	솔루션링크 교육장	'19/7/18(목)~19(금)	34만원	

1. A-SPICE(v3.1) 실무적용 관점의 이해

과정명	A-SPICE(v3.1) 실무적용 관점의 이해	교육시간	2일 (16시간)
추천 교육대상	System/SW 엔지니어, 관리자, 프로세스 담당자	교육형태	이론 100%
과정개요	자동차 개발에 요구되는 프로세스 모델에 대한 이해를 바탕으로, 유럽 OEM이 주로 요구하는 VDA scope에 해당하는 16개 프로세스 영역의 요건 및 실무적용 방안을 습득한다.		
교육목표	* 해외 OEM이 기대하는 프로세스 품질에 대한 이해 * A-SPICE 구성 및 세부 요건에 대한 이해 * 프로세스 역량 수준 및 심사 절차, 기준 이해		
선수지식	없음		

교육내용 요약

일	모듈명	교육 내용
1일차	Overview	• 해외 OEM의 기대 사항 • A-SPICE 개요 • A-SPICE 2.x → 3.x 주요 변경 사항
	Engineering	• SYS.2~3 시스템 분석 설계 • SWE.1~3 소프트웨어 분석 설계 및 구현 • SWE.4~6 소프트웨어 영역 시험 • SYS.4~5 시스템 영역 시험 • Traceability
2일차	Management	• MAN.3 프로젝트 관리 • ACQ.4 협력업체 관리
	Supporting & Process assessment	• SUP.1 품질보증 • SUP.8 형상 관리 • SUP.9 문제 관리 • SUP.10 변경 요청 관리 • Capability level • Process rating& assessment • Wrap up

2. ISO 26262 2nd Edition - 구성 및 개념 이해

과정명	ISO 26262 2nd Edition - 구성 및 개념 이해	교육시간	2일 (14시간)
추천 교육대상	HW/SW 엔지니어, 관리자, 프로세스 담당자	교육형태	이론 100%
과정개요	ISO26262 2nd Edition 기반의 기능 안전 라이프 사이클의 프로세스 구성과 주요 기능 안전 활동 및 산출물에 대해 습득하고, 이를 실무에 적용하기 위한 역량을 배양한다		
교육목표	* ISO26262의 기능안전 라이프사이클 이해 * 기능안전 달성을 위해 수행해야 하는 활동 및 산출물에 대한 전반적 이해		
선수지식	없음		

교육내용 요약

일	모듈명	교육 내용
1일차	ISO26262 개요	• ISO 26262 목적 및 구성 • ISO 26262 주요 개념
	ISO 26262 Part 3, 4	• Hazard Analysis and Risk Assessment (HARA) • Functional safety concept • System development & verification
	ISO 26262 Part 5, 6	• Hardware development & verification • Software development & verification
2일차	ISO 26262 Part 9	• ASIL-oriented and safety-oriented analyses
	ISO 26262 Part 11, 12	• Semiconductors • Motorcycles
	ISO 26262 Part 2, 8	• Management of functional safety • Supporting processes

3. 자율주행 차량의 안전 확보(SOTIF, ISO/PAS 21448)

과정명	자율주행 차량의 안전 확보(SOTIF, ISO/PAS 21448)	교육시간	1일 (8시간)
추천 교육대상	System/HW/SW 엔지니어, 관리자, 프로세스 담당자	교육형태	이론 100%
과정개요	SOTIF (Safety of the Intended Functionality) 시스템의 의도된 기능(intended function)*의 불충분(insufficiency) 또는 사람의 오용(misuse)에 의한 Hazard로 인해 발생되는 리스크를 방지하기 위한 안전 규격인 “ISO/PAS 21448:2019 Road vehicles : Safety of the intended functionality” 전반에 대한 개념을 설명하고 이를 실무에 적용하기 위한 역량을 배양한다. * 시스템 고장(malfunction)에 의해 발생되는 안전 위반(safety violations)을 방지하기 안전 규격은 ISO26262에서 다루고 있음		
교육목표	* SOTIF 필요성 및 기본 개념의 이해 * 개발 프로세스 상에서 SOTIF 주요 활동 습득 * SOTIF를 구현하기 위한 Design, Verification & Validation 단계 별 SOTIF Measure의 이해		
선수지식	없음		

교육내용 요약

일	모듈명	교육 내용
1일차	SOTIF Overviews	• Automated Driving System and SOTIF • SOTIF Introduction, terms & definitions • SOTIF activities in the development process
	SOTIF HARA & Failure Analysis	• Functional and System specification • SOTIF Hazard Identification and Evaluation • Hazardous use case identification
	SOTIF Concept (SOTIF Measures)	• SOTIF Measures (sensor, algorithms, actuator) • Functional restriction for SOTIF risk mitigation • Handing over the authority for improving the controllability • Reduction / mitigation of reasonably foreseeable misuse • Fail operational safety architecture for SOTIF
	SOTIF V&V	• Definition of the Verification and Validation strategy • SOTIF Verification & Validation • Methodology and Criteria for SOTIF release
	SOTIF Activities Examples	• Understanding of SOTIF Activities using AEB example

4. ISO 26262 2nd Edition - 시스템 개발 (안전설계, 안전분석(FMEA/FTA), 테스팅)

과정명	ISO 26262 2nd Edition - 시스템 개발 (안전설계, 안전분석(FMEA/FTA), 테스팅)	교육시간	3일 (21시간)
추천 교육대상	시스템 개발 엔지니어, 시스템 테스트 엔지니어	교육형태	이론 80%, 실습 20%
과정개요	기능안전 요구사항에 대한 이해를 바탕으로 이를 만족하는 시스템 설계 방법을 습득한다. 시스템 수준에서 기능안전 분석 기법인 FMEA와 FTA 수행 방법과 DFA 방법을 습득하고 실습을 통해 적용 능력을 배양한다. ISO26262에서 정의하는 V&V에 대한 수행 요건을 이해하고 시스템 수준의 테스트 기법 적용 방안을 습득한다.		
교육목표	* 시스템 개발 수준에서 요구되는 기능안전 요건의 이해 * 기능안전 요구사항을 만족하는 시스템 설계 방법 습득 * 시스템 수준의 기능안전 분석 기법에 대한 이해 * 기능안전 요구사항을 만족하는 시스템 안전분석 방법 습득 * 실습을 통한 실무 적용 능력 배양 * ISO26262의 V&V 수행 요건에 대한 기본 이해 * ISO26262의 V&V 주요 활동인 테스팅 기법에 대한 이해 * 시스템 수준의 테스트 기법 적용 방안 습득 * 안전 메커니즘 검증 방안 습득		
선수지식	시스템 개발 및 검증 관련 경험 또는 지식, 기능안전에 대한 이해		
교육내용 요약은 다음 장 참고			

4. ISO 26262 2nd Edition - 시스템 개발 (안전설계, 안전분석(FMEA/FTA), 테스팅), 계속

교육내용 요약

	모듈명	교육 내용
1일차	시스템 안전 설계 및 분석 개요	• 기능 안전 시스템의 개발 • 안전분석 개요 및 종류 • ISO 26262 안전분석 요건
	FMEA 및 VDA FMEA	• FMEA 개요 • FMEA 수행 절차 • VDA FMEA
	FMEA 실습	• FMEA 실습
2일차	기능안전 시스템 개발 절차 및 명세	• 기능안전 시스템 개발 절차 • 기능안전 요구사항 명세 • 기능안전 시스템 설계
	시스템 안전설계 방법	• 시스템적 고장 회피 원칙의 적용 • 안전성이 고려된 시스템 아키텍처 설계 • 시스템 아키텍처 엘리먼트 레벨 안전 메커니즘 적용
	시스템 안전설계 사례	• EGAS 컨셉에서 시스템 안전설계 사례 • ASIL에 따른 시스템 안전설계 사례
	시스템 안전설계 실습	• 시스템 안전 아키텍처 설계 실습
3일차	FTA 개념 및 수행 절차	• FTA 개념 • FTA 수행절차
	시스템 FTA	• 시스템 FTA 개요 • 시스템 FTA 수행 절차
	DFA	• DFA 개요 • DFA 수행 절차
	시스템 FTA 실습	• 시스템 FTA 실습

교육내용 요약			
	3일차	시스템 테스트 개요	• 테스트 개요 • 기능안전 시스템 테스트 요건
		시스템 테스트 기법	• 테스트 케이스 설계 방법 • 백-투-백 테스트 • 결함 주입 테스트 • 테스트 환경
		기능안전 시스템 테스트	• 기능안전 테스트 단계 • 안전 메커니즘 검증 방법

5. ISO 26262 2nd Edition - 하드웨어 개발 (안전설계, FMEDA, 테스팅)

과정명	ISO 26262 2nd Edition - 하드웨어 안전 설계 (안전설계, FMEDA, Verification)	교육시간	3일 (21시간)
추천 교육대상	HW 개발 엔지니어, HW 테스트 엔지니어	교육형태	이론 80%, 실습 20%
교육개요	기능안전 요구사항에 대한 이해를 바탕으로 HW 안전 설계 및 구현 방법을 습득한다. HW 수준에서 기능안전 분석 기법인 FMEDA 수행 방법을 습득하고 실습을 통해 실무 적용 역량을 배양한다. ISO26262에서 정의하는 V&V에 대한 수행 요건을 이해하고 HW 수준의 검증(Verification) 기법 적용 방안을 습득한다.		
교육목표	* HW 개발 수준에서 요구되는 기능안전 요건의 이해 * 기능안전 요구사항을 만족하는 HW 설계 방법 습득 * HW 수준의 기능안전 분석 기법인 FMEDA에 대한 이해 * 기능안전 요구사항을 만족하는 정량적인 HW 안전분석 방법 습득 * 실습을 통한 실무 적용 역량 배양 * ISO26262의 V&V 수행 요건에 대한 기본 이해 * ISO26262의 V&V 주요 활동인 검증(Verification) 기법에 대한 이해 * HW 수준의 검증(Verification) 기법 적용 방안 습득 * 안전 메커니즘 검증 방안 습득		
선수지식	HW 개발 관련 경험 또는 지식, 기능안전에 대한 이해		
교육내용 요약은 다음 장 참고			

5. ISO 26262 2nd Edition - 하드웨어 개발 (안전설계, FMEDA, 테스팅), 계속

교육내용 요약

일	모듈명	교육 내용
1일차	기능안전 컨셉	• 기능안전을 고려한 설계 개념 • 기능안전 컨셉 개발
	HW 개발 절차	• 개발 프로세스 • 단계별 수행활동 및 산출물 구성
2일차	HW 기능안전 컨셉 개발	• I/O와 인터페이스를 위한 안전 메커니즘 • 센서를 위한 안전 메커니즘 • 통신 인터페이스에 적용되는 기능안전 컨셉 • 액추에이터를 위한 안전 메커니즘 • 안전 MCU 활용
	ISO26262의 V&V 요구사항	• ISO26262에 정의된 V&V(검증) 요구사항
	하드웨어 검증 기법 적용 방안	• 검증 기법 적용 방안 개요 • 하드웨어 테스트
3일차	FMEDA 개요	• HW 안전 분석 요구사항 및 FMEDA 정의 • 결함의 분류
	FMEDA 수행방안 - 파트 1	• FMEDA 템플릿 및 수행 절차 • 예제 시스템 설명 • FMEDA 준비 • 단일점 결함률 검토
	FMEDA 수행방안 - 파트 2	• 잠재 결함률 검토 • HW 아키텍처 메트릭 계산 • HW 우발고장으로 인한 안전목표 위반 평가 (PMHF)
	FMEDA 실습	• FMEDA 실습

6. ISO 26262 2nd Edition - 소프트웨어 개발 (안전설계, 안전분석(FTA/FMEA), 테스팅) , 계속

과정명	ISO 26262 2nd Edition - 소프트웨어 개발 (안전설계, 안전분석(FTA/FMEA), 테스팅)	교육시간	3일 (21시간)
추천 교육대상	SW 개발 엔지니어	교육형태	이론 80%, 실습 20%
과정개요	ISO26262를 준수하는 SW 아키텍처 및 상세 설계를 예제를 통해서 습득하고, SW 대한 주요 안전 메커니즘을 이해한다. SW 수준에서의 기능 안전 분석 기법인 SW FMEA와 SW FTA 수행 방법과 DFA 방법을 습득하고 실습을 통해 적용 능력을 배양한다.		
교육목표	* SW 개발 수준에서 요구되는 기능안전 요건의 이해 * 기능안전 요구사항을 만족하는 임베디드 소프트웨어 설계 방법 습득 * SW 개발 수준에서 요구되는 기능안전 분석 요건의 이해 * 기능안전 분석 요건을 만족하는 임베디드 소프트웨어 분석 방법(SW FMEA)을 습득 * SW 안전 메커니즘 설계의 이해		
선수지식	SW 개발 관련 경험 또는 지식, 기능안전에 대한 이해		
교육내용 요약은 다음 장 참고			

교육내용 요약

일	모듈명	교육 내용
1일차	SW 설계 개요	• ISO 26262 SW 개발 요건 • A-SPICE SW 개발 요건 • SW 개발 절차 • SW 요구사항 예
	SW 아키텍처 설계	• 데이터 흐름 분석 • SW 아키텍처 설계 원칙 • 초기 구조 식별 • 동적 설계 • 구조평가 및 개선 • SW 아키텍처 설계 문서의 구성 • 실습 (SW 아키텍처 설계)
	SW 상세 설계	• SW 상세 설계 및 구현 원칙 • SW 상세 설계 문서의 구성
2일차	SW 안전분석 및 설계 개요	• ISO 26262 SW개발 요건 (요약) • SW 개발 절차 (ISO 26262 적용) • SW 안전분석 개요
	SW FMEA	• SW Failure Mode • SW FMEA 절차 • 실습 (안전 분석)

교육내용 요약

일	모듈명	교육 내용
2일차	SW 안전설계 메커니즘	• 센서에 적용되는 기능안전 컨셉 • 액츄에이터에 적용되는 기능안전 컨셉 • 제어기에 적용되는 기능안전 컨셉 • 메모리에 적용되는 기능안전 컨셉 • 통신 인터페이스에 적용되는 기능안전 컨셉
	SW FTA 및 의존고장 분석	• 의존고장 분석 개요 • SW DFA 절차
3일차	SW 아키텍처 설계 (안전 메커니즘 적용)	• Failure Mode 별 안전 메커니즘 분류 • 안전 메커니즘 적용 전략 • 실습 (안전 메커니즘 선정) • SW 안전 요구사항 및 안전 설계 예 • 실습 (안전 설계) • SW 아키텍처 설계 문서의 구성 (ISO 26262)
	SW 상세 설계 및 구현 (안전 메커니즘 적용)	• SW 상세 설계 구현 원칙

7. ISO26262 2nd Edition - SW 안전 메커니즘 이해 및 구현

과정명	ISO26262 2nd Edition - SW 안전 메커니즘 이해 및 구현	교육시간	2일 (14시간)
추천 교육대상	SW 엔지니어	교육형태	이론 30%, 실습 70%
과정개요	SW 안전 메커니즘 설계를 이해하고, 예제 시스템 구현 실습을 통해 주요 SW 안전 메커니즘 구현 상세 기법을 습득한다.		
교육목표	* SW 안전 메커니즘 설계의 이해 * 사례를 통한 SW 안전 메커니즘 구현 상세 기법 습득		
선수지식	소프트웨어 분석 및 설계		

교육내용 요약

일	모듈명	교육 내용
1일차	SW 안전 아키텍처 설계	• SW 아키텍처 설계의 안전 체계를 설계하는 과정
	SW 안전 메커니즘 개요	• 전통적인 전장 SW의 아키텍처 • 주요한 SW 안전 메커니즘 목록
	SW 안전 메커니즘 구현 상세	• 메모리 검사를 위한 안전 메커니즘 • 스택 오버플로우 검사를 위한 안전 메커니즘 • 센서의 정합성 확인을 위한 안전 메커니즘의 코드 사례 • 액추에이터 정합성 확인을 위한 안전 메커니즘의 코드 사례 • 감시기(watchdog), 프로그램 흐름 모니터링 등 기능의 수행 전반을 모니터링하는 안전 메커니즘의 코드 사례
	SW 구현 실습 환경 구성	• SW 안전 메커니즘 구현을 위한 실습 환경 구성
2일차	SW 안전 메키니즘 구현 실습	• SW 안전 메커니즘이 종합된 예제 시스템의 설계 실습

실습보드: STMicroelectronics ARM Cortex-M4 STM32F417IG Processor with Crypto Accelerator
개발환경: IAR Embedded Workbench for ARM (EWARM)

8. ISO26262 2nd Edition - SW 테스팅

과정명	ISO26262 2nd Edition - SW 테스팅	교육시간	1일 (8시간)
추천 교육대상	SW 엔지니어 / 테스트 엔지니어	교육형태	이론 100%
과정개요	ISO26262에서 정의하는 SW 테스팅에 대한 수행 요건을 이해하고 단계별 테스트 기법 적용 방안을 습득한다.		
교육목표	* ISO26262의 SW 테스팅 수행 요건에 대한 이해 * SW 테스팅 기법에 대한 이해 및 적용방안 습득 * 안전 메커니즘 검증 방안 습득		
선수지식	소프트웨어 분석 및 설계		

교육내용 요약

일	모듈명	교육 내용
1일차	SW 테스트 개요	• SW V&V 개요 • SW 테스트 기본 • A-SPICE SW 테스트 요건
	SW 테스트 기법	• 블랙박스 테스트 • 화이트박스 테스트
	기능안전 SW 테스트	• 기능안전 SW 테스트 요건 • 기능안전 SW 테스트 기법 • 단계별 테스트 기법 적용
	안전 메커니즘 검증 방법	• 메모리 안전 메커니즘 검증 • 제어기 모니터링 안전 메커니즘 검증 • 센서 및 액츄에이터 안전 메커니즘 검증
	SW 테스트 산출물 구성	• SW 테스트 계획서 • SW 테스트 케이스 • SW 테스트 결과서

9. 자동차 전장시스템 보안 (Automotive Cybersecurity)

과정명	자동차 전장시스템 보안(Automotive Cybersecurity)	교육시간	2일 (14시간)
추천 교육대상	자동차시스템/ SW / HW / 테스트엔지니어	교육형태	이론70%, 실습30%
과정개요	자동차 전장 시스템에서의 보안과 기존IT시스템의 보안과의 차이점을 이해하고, 자동차 전장 시스템 개발에 특화된 다양한 보안 기법을 습득한다.		
교육목표	* 임베디드 시스템 보안에 대한 기본 이해 * 자동차 전장 시스템 보안 분석 및 설계 기법 습득		
선수지식	SW 개발관련경험또는지식, C프로그래밍언어		

교육내용 요약

일	모듈명	교육 내용
1일차	임베디드 보안 개요	• 임베디드 보안과 IT 보안의 차이 소개 • 실습 보드 (STM3241G)의 보안 관련 기능 소개 및 활용 실습 • 임베디드 소프트웨어 및 하드웨어의 주요 취약점 소개 • 암호 (Cryptography) 기법의 개요 및 활용 실습
	임베디드 보안 분석 기법	• 보안을 고려한 소프트웨어 개발 프로세스 • 위협 분석 기법(Threat Analysis)
2일차	임베디드 보안 설계 기법	• 저장 데이터와 전송데이터의 보안 기법 소개 및 활용 실습 • 보안을 고려한 소프트웨어 아키텍처 설계 기법 • 보안을 고려한 하드웨어 인터페이스 설계 기법
	자동차 사이버 보안	• 자동차 전장 시스템의 안전과 보안 이슈 • 자동차 보안 표준 소개(J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems) • 공격 트리를 활용한 자동차 전장 시스템 위협 분석 실습

실습보드: STMicroelectronics ARM Cortex-M4 STM32F417IG Processor with Crypto Accelerator
개발환경: IAR Embedded Workbench for ARM (EWARM)
위협분석도구: SeaMonster-Security Modeling Software