

점검 지원내용

구분	지원내용	
제어 설비	동등분할 시험	
	경계값 분석	
	결정 테이블 테스트	
	상태변경 테스트	
	시큐어코딩 여부 검증	
	CVE, CVSS 등에 기반한 보안 취약점 점검	
	RTOS 디버깅	
	I/O 레스터 관찰	
	메모리값 변동 탐지	
	특정 구간에 대한 처리 성능 측정	
	최신 펌웨어 업데이트 여부 확인	
	모의침투(권한 탈취, 스피어피싱 공격 등)	
	제어 네트워크	Profinet 신뢰성테스트
Profinet 네거티브테스트		비정상적인 통신 전달 정보에 대한 처리상태
Modbus 신뢰성 테스트		프로토콜 정의내 통신에 대한 신뢰성 및 가용성
Modbus 네거티브테스트		비정상적인 통신 전달 정보에 대한 처리상태

스마트공장 보안리빙랩 신청절차

- 
이용 신청서 작성
 ※ KISA 홈페이지 → 하단 알림판 배너 융합보안리빙랩 → 분야별 보안리빙랩 선택
- 
신청서 제출
 ※ e-mail(cslivinglab@kisa.or.kr)
- 
일정 협의
 ※ 신청서 검토 후 e-mail 또는 유선협의
- 
보안리빙랩 방문 후 테스트
 ※ 방문시 방문객 관리대장 작성후 이용
- 
테스트 점검 결과 검토 및 컨설팅

주요 융합보안리빙랩 위치



스마트공장 보안리빙랩 소개

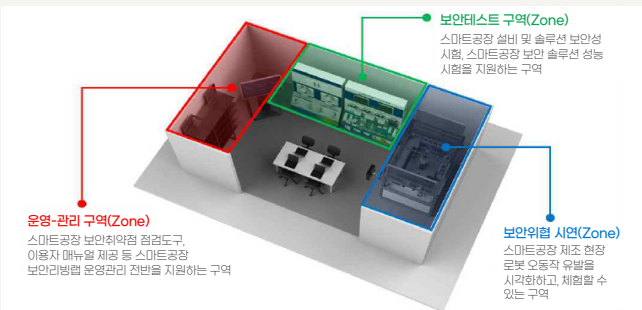
구성 환경

- **보안테스트 구역(Zone)**
음료제조 생산공정(블렌딩 → 캐핑 → 패키징 → 라벨링) 환경에 기반한 제어설비·솔루션 보안취약점 분석 지원
- **보안위협 시연 구역(Zone)**
노르스크 하이드로(랜섬웨어), 대만TSMC(스피어피싱) 해킹 시나리오를 활용한 로봇 오동작, 생산 모터 수치값 오류 유발 시연
- **운영·관리 구역(Zone)**
보안취약점 점검 도구, 이용자 매뉴얼 제공 등



보안테스트 구역 위험시연 구역 운영·관리 구역

구성도



목적

스마트공장 제어설비, 솔루션의 보안성 시험 지원을 통한 스마트공장 보안내재화 촉진 및 국내 스마트공장 보안기업 기술 경쟁력 강화 지원



시험대상

- **제어설비(PLC, HMI)**
생산 공정 환경과 연계한 보안성 및 안정성 테스트

구분	모델명	제조사	요구조건
PLC	XGT 시리즈 등	LS일렉트릭	RAPIDnet→Modbus TCP 가능
	S7-300 시리즈 등	지멘스	Profinet→Modbus TCP 가능
	Q 시리즈 등	미쓰비시	Modbus TCP 가능
	기타 PLC	-	Modbus TCP 가능
HMI	xPanel시리즈 등	CIMON	Modbus TCP 가능
	LS Panel 시리즈 등	LS일렉트릭	Modbus TCP 가능
	미쓰비시 Panel 시리즈 등	미쓰비시	Modbus TCP 가능
	지멘스 Panel 시리즈 등	지멘스	Modbus TCP 가능
	Weintek Panel 시리즈 등	Weintek	Modbus TCP 가능
	기타 HMI	-	Modbus TCP 가능

- **스마트공장 솔루션(MES 등)**
지원언어 : C/C++/JAVA/PYTHON 등
지원컴파일러 : Visual Studio, GCC 등

- **스마트공장 보안제품**
생산 공정 환경과 연계를 통한 보안기능 테스트

구분	모델명	제조사	제약조건
보안 제품	ICS 이상징후 시스템	-	미러링 가능 제품
	일방향 장치	-	정책 적용 제품
	Firewall	-	

이용대상

스마트공장 제어설비·솔루션 기업, 스마트공장 보안 기업 및 교육기관

점검도구

도구명	지원내용
Metasploit	모의침투
Defensics	Modbus, Profinet 피싱
TRACE32	디버깅지원
Coverity	SW 정적분석
Nexpose&Claroty	보안컴플라이언스, 취약점 분석

담당자 연락처

- **전화** 061-820-1214
- **E-Mail** cslivinglab@kisa.or.kr

오시는 길

- 경기도 안산시 단원구 엠티브이12로 17
스마트제조혁신센터 3층

