반도체 기업의
OSS 관리 시스템 구축 사례

2025.02.28

텔레칩스 지식재산권팀

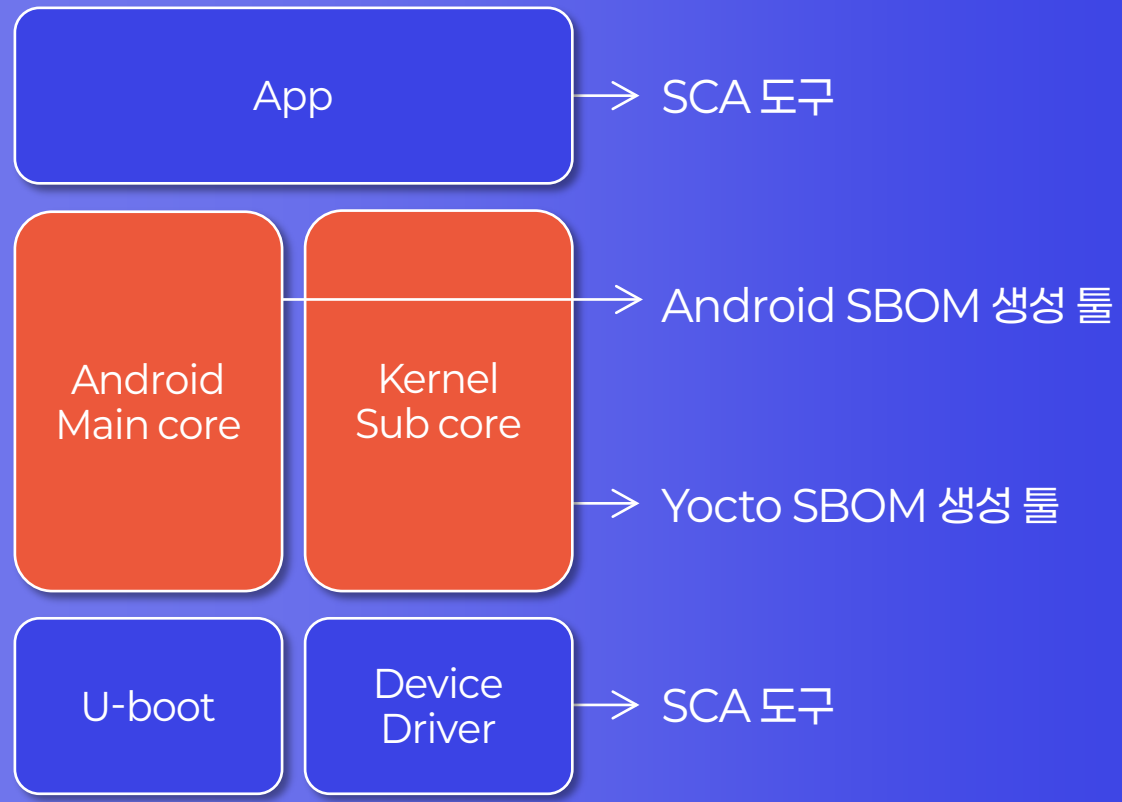
연지영 매니저 (chloe.yeon@telechips.com)

Telechips

1 OSS 관리 시스템 리뉴얼 계기

- 해외 고객들의 SBOM 제출 요구 증대
- 오픈소스 점검 결과 신뢰성 향상 필요
- 고스펙의 SCA 도입 필요성 확대
- SDLC 전반 관리 필요 인식
- 소인원으로 관리 가능한 시스템 필요

초기 SBOM 요구에 대한 대응 안



2 텔레칩스의 소프트웨어 개발 특성

개발 대상

SOC
(System on Chip)

SDK
(Software Development Kit)

BSP
(Board Support Package)

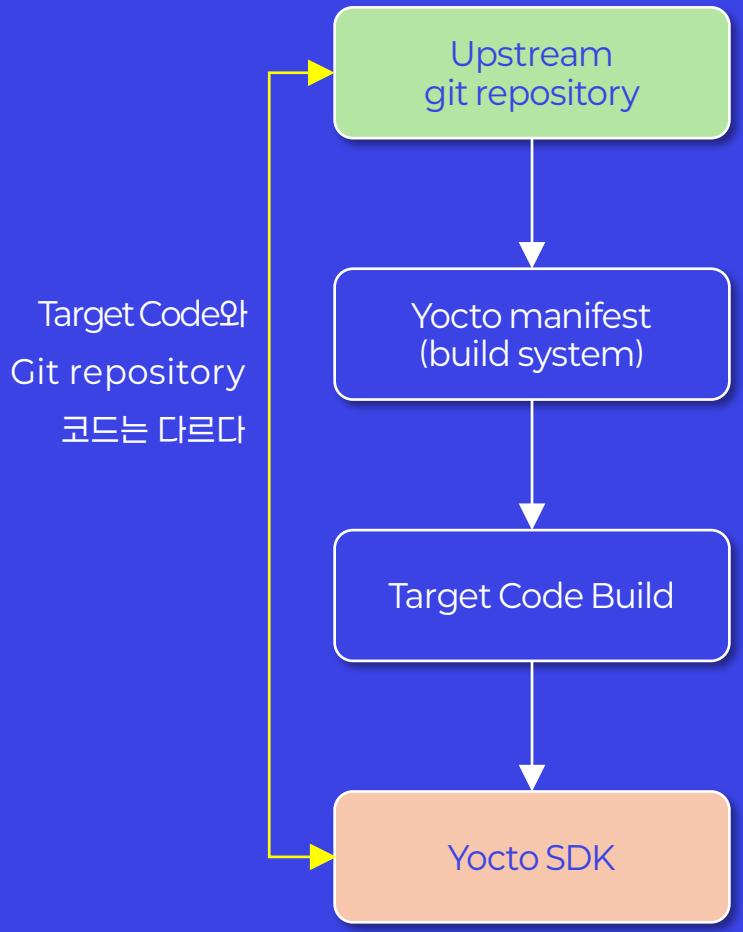
APP
(Application)

SDK(소프트웨어 개발 키트)란

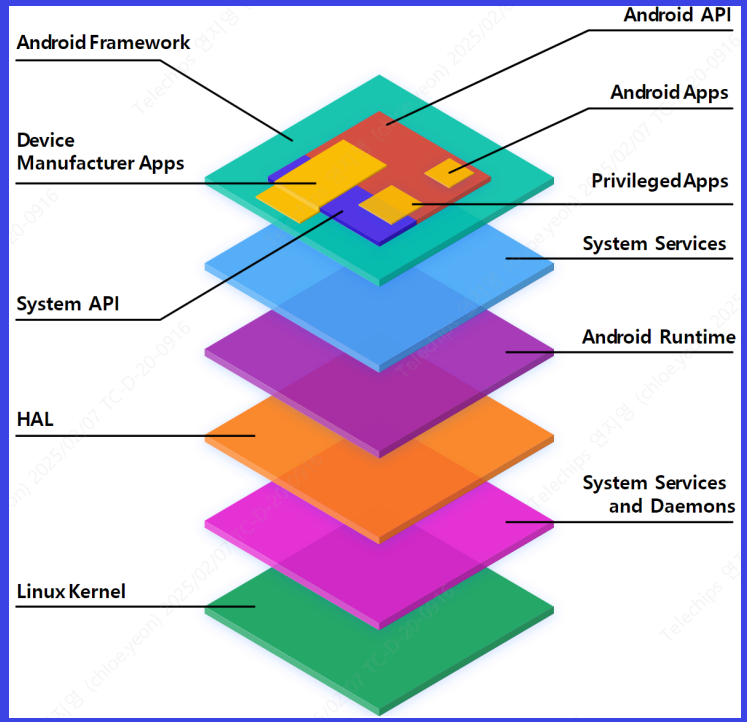
소프트웨어 개발 키트는 일반적으로 소프트웨어 기술자가 사용하여 특정한 소프트웨어 꾸러미, 소프트웨어 프레임워크, 하드웨어 플랫폼, 컴퓨터 시스템, 게임기, 운영 체제 등을 위한 응용 프로그램 등을 만들 수 있게 해주는 개발 도구의 집합이다. - 위키백과

Yocto SDK

Target Code와
Git repository
코드는 다르다



Android SDK



Android SDK Project Size

20GB 이상 ▲

3 OSS 관리 시스템 요구사항

내부 요구사항

- 고스펙의 점검 도구
- CI/CD 통합 연계·반복 점검
- 점검 결과 편차 및 시간 축소
- 이력 및 산출물 등 관리 포털
- 개발 문화 연속성 확보

외부 요구사항

독일 회사

- SBOM SPDX 2.3
- CPE (Common Platform Enumeration)
- pURL (Package URL)
- 식별자 명시

일본 회사

- SPDX Lite
- ISO 5230 / 18974 인증 취득

선정 도구

BlackDuck (SCA) + **FOSSEra (Portal)**

오픈소스 라이선스/보안취약점 점검 엔진

오픈소스 사용 및 관리 효율 / 편의 지원

4 구축 시스템 스펙·기능

BlackDuck (SCA, 오픈소스 점검 툴)		
오픈소스 식별		자동식별 + 수동식별
오픈소스 위험 관리	보안취약점	○
	라이선스	○
오픈소스 점검 연동	CLI/GUI	○
	CI/CD	○
	형상관리	○ (Gihub/Gitlab/Bitbucket/SVN)
오픈소스 DB	DB 규모	870만 개 (프로젝트)+
	업데이트 주기	오픈소스 주2회, 보안취약점 매시간
	자사 코드 DB화	○
	라이선스	2,750+
오픈소스 정보 검색	오픈소스 컴포넌트	○
	라이선스	○
	보안취약점	○
컴플라이언스 지원	점검 결과 보고서	○
	SBOM	○
	고지문	○
신규 보안취약점 모니터링		○
점검 용량		무제한 (1회 점검 10GB ↓)
점검 대상	언어	C, C++, C#, Clojure, Erlang, Golang, Groovy, Java, JavaScript, Kotlin, Node.j, Objective-C, Perl, Python, PHP, R, Ruby, Scala , Swift, .Net 클라우드기술 등
	컨테이너	○
	바이너리	○
	패키지관리자	○
	압축	○
	아카이브	○
	설치기	○
	펌웨어	○
	파일시스템/이미지	○
	SBOM	○

FOSSEra (관리 포털)		
오픈소스 점검 관리	그룹 별 프로젝트 관리	○
오픈소스 리뷰	결과 승인	○
	조치 관리	○
	예외 신청	○
모니터링	신규 오픈소스 보안취약점 알람	○
컴플라이언스	오픈소스 고지문 생성	○ (TXT, HTML)
SBOM	SBOM 생성	○
	제3자 SBOM 검토 및 관리	○
	SBOM 생성 이력 기록	○
공급망 관리	산출물 공급 관리	○
오픈소스 저장소 관리	오픈소스 저장소 검색	○
	취약 오픈소스 격리	○
연계	CI/CD 연계	○
	인사정보(재직여부, 조직정보)	○ (Ldap, SSO, E-mail)
정책 설정	라이선스 정책	○
	보안취약점 정책	○
	프로젝트 별 정책	○
권한	메뉴접근 권한 설정	○
	담당 권한 설정	○
모니터링	메일/메신저/JIRA 알람	○
보안취약점	개선가이드(패치)	○

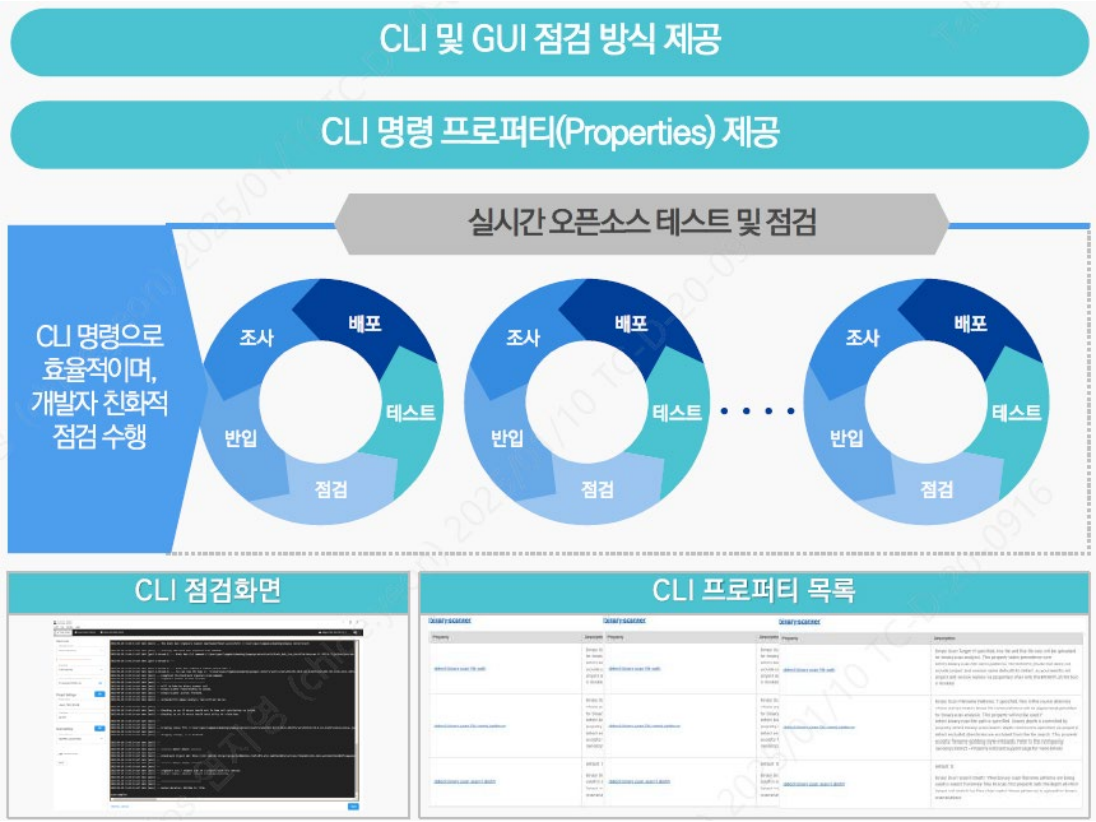
Telechips

4 구축 시스템 스펙·기능 > CI/CD 연동

지원하는 솔루션 (API, Plug-in)

[SDLC별 지원하는 3rd Party 솔루션]

점검 방식 (CLI / GUI)



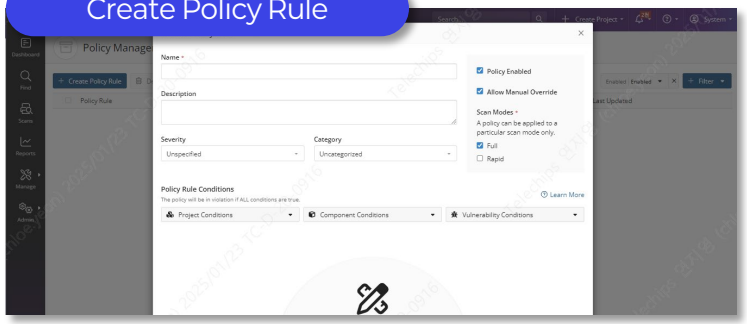
Telechips

4 구축 시스템 스펙·기능 > Management

범례 : 블랙덕 FOSSEra

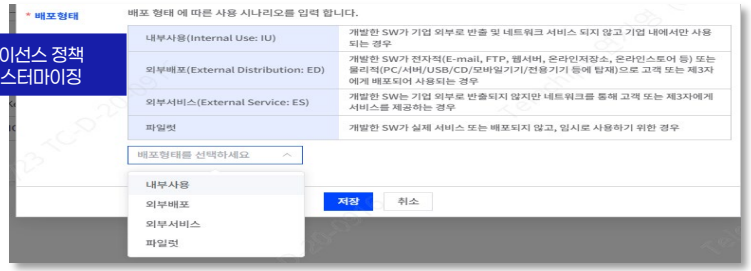
라이선스/보안취약점 등 정책

Create Policy Rule



라이선스, 보안취약점, 컴포넌트, 운영에 대한 관리
수준(Critical, Major, Minor 등) 별 정책을 수립하여 Scan 결과에 적용할 수 있음

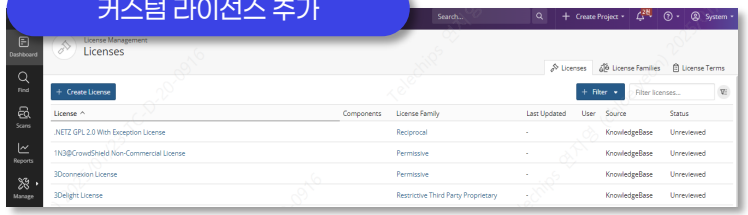
라이선스 정책 커스터마이징



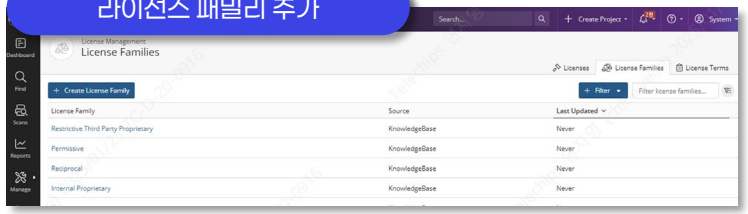
라이선스 별 사용 가능/불가 커스터마이징 할 수 있는 기능 보유

라이선스 상세 정책

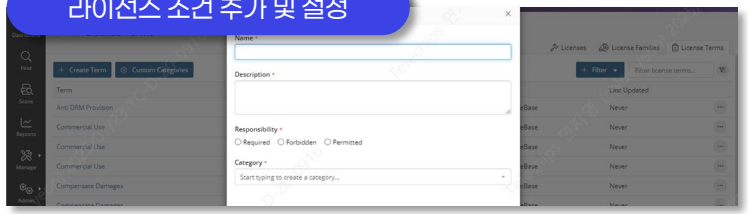
커스텀 라이선스 추가



라이선스 패밀리 추가

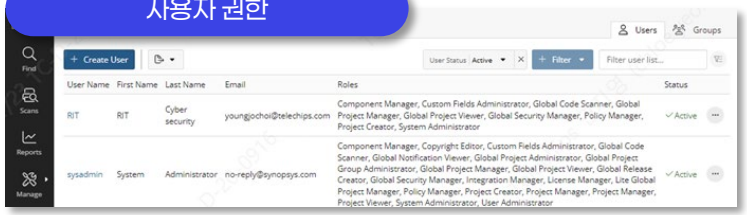


라이선스 조건 추가 및 설정

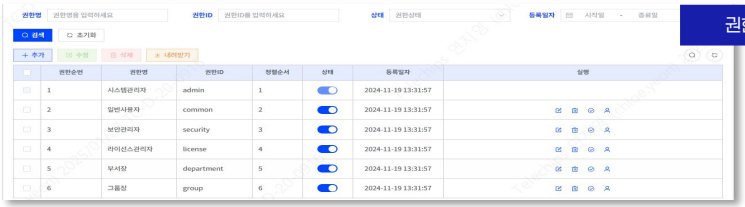


사용자 권한

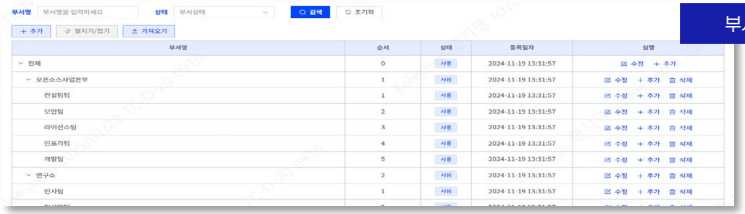
사용자 권한



권한



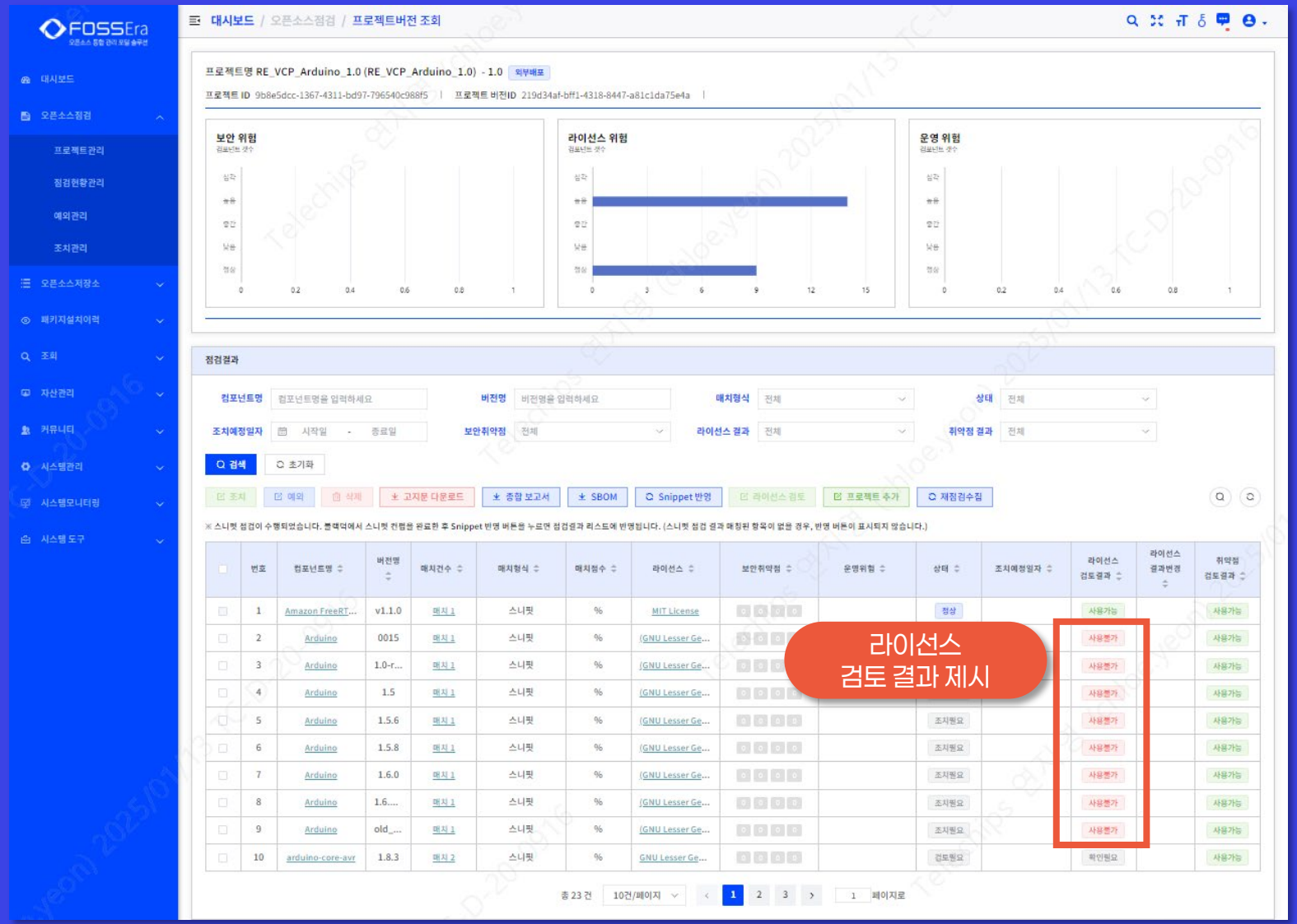
부서

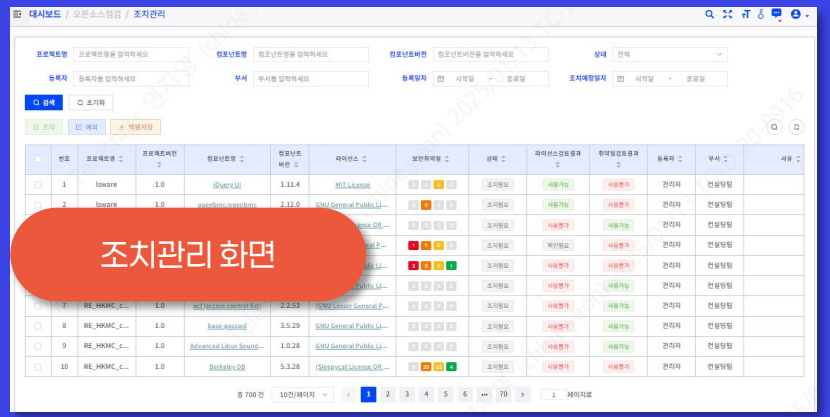


직위

Telechips

4 구축 시스템 스펙·기능 > 점검 결과 관리





Telechips

5 오픈소스 시스템 구축 TF

OSRB 구성원

개발
- Automotive Platform Team (신택현Master, 김윤희M, 김완수M, 승영수M)
- Camera Graphics Team (김요한M)
- Advanced BSP Team (김호연지기M)

사업부
- TOPST BU (모우진 T)

DevOps
- Development & Operations Team (신호찬T, 김진웅M)

개발 프로세스
- R&D Innovation Team (이무원 Master)

지식재산권 (OSS)
- Intellectual Property Rights Team (조록수T, 연지영M)

구축 단계

시스템	프로세스
사내 서버 내 설치	
환경 테스트	
점검 / 운영 프로세스 초안 준비	
모듈 (빌드리스 코드) 스케줄링 점검 테스트	시스템 사용 시나리오 준비
SDK 점검 이슈 분석	프로세스 고도화
Yocto 점검 방안 모색 및 테스트	
AOSP 점검 방안 모색 및 테스트	
운영 테스트	
피드백 반영	
전사 적용	

OSS 점검 방안

가. 건 별 점검

- 개발 완료 건은 필요시 수동 점검 (소스코드 업로드, 저장소 연동 등)

나. 모듈 점검 – 개발단계

- dev branch 스케줄링 점검 > full-request commit 신호로 매일 점검

다. SDK 점검 – 릴리즈 단계

① Yocto (빌드)

- SDK 빌드 시 사용하는 build-autolinux에 OSS 검증 기능 추가 (빌드 시 점검) > bd_scan_yocto_via_sbom 스크립트 활용

시스템 부하, 중복 점검 등 우려되는 사항이 있어, 코드 픽스 단계에서 개별적으로 점검 진행 예정 (빌드마다 점검 X)

② AOSP (빌드리스)

- Blackduck 1회 최대 점검 가능 사이즈 10GB 제한 이슈
- AOSP 중 텔레칩스가 오너쉽을 갖는 코드만 manifest.xml로 구성하여 점검하는 방안 검토 - ing
- Android AOSP Original Code의 SBOM이 필요한 경우 Android SBOM Generator 활용 고려 (예: 중국 고객사)

Telechips

6 점검 범위와 배치

점검 범위

점검 | 비점검

Demo App (GUI 등)

Yocto

Origin Code
고객사가 Upstream에서 다운로드 받는 코드

Modified Code
Telechips가 수정했으며, 고객사에 직접 제공하는 코드

Android

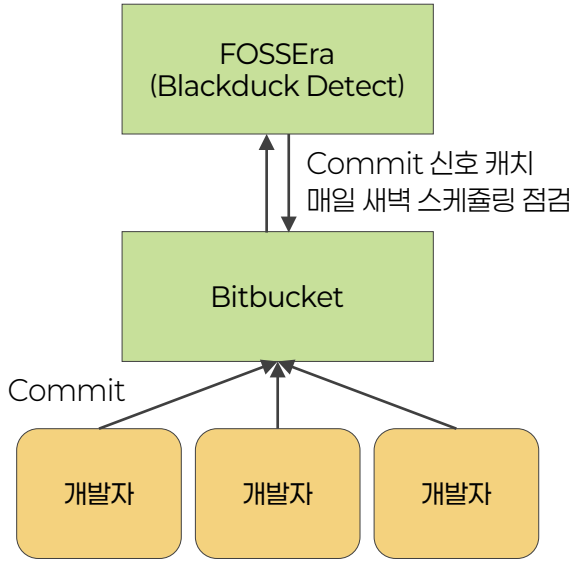
Origin Code
고객사가 google에서 다운로드 받는 코드 (중국의 경우 점검 수행)

Modified Code
Telechips가 수정했으며, 고객사에 직접 제공하는 코드

BSP (Kernel + U-boot)

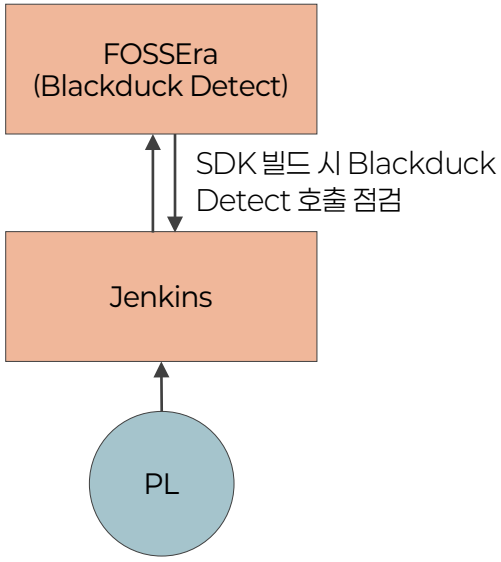
점검 배치

개발 단계 점검



FOSSEra에 Project 생성 / Bitbucket 연동

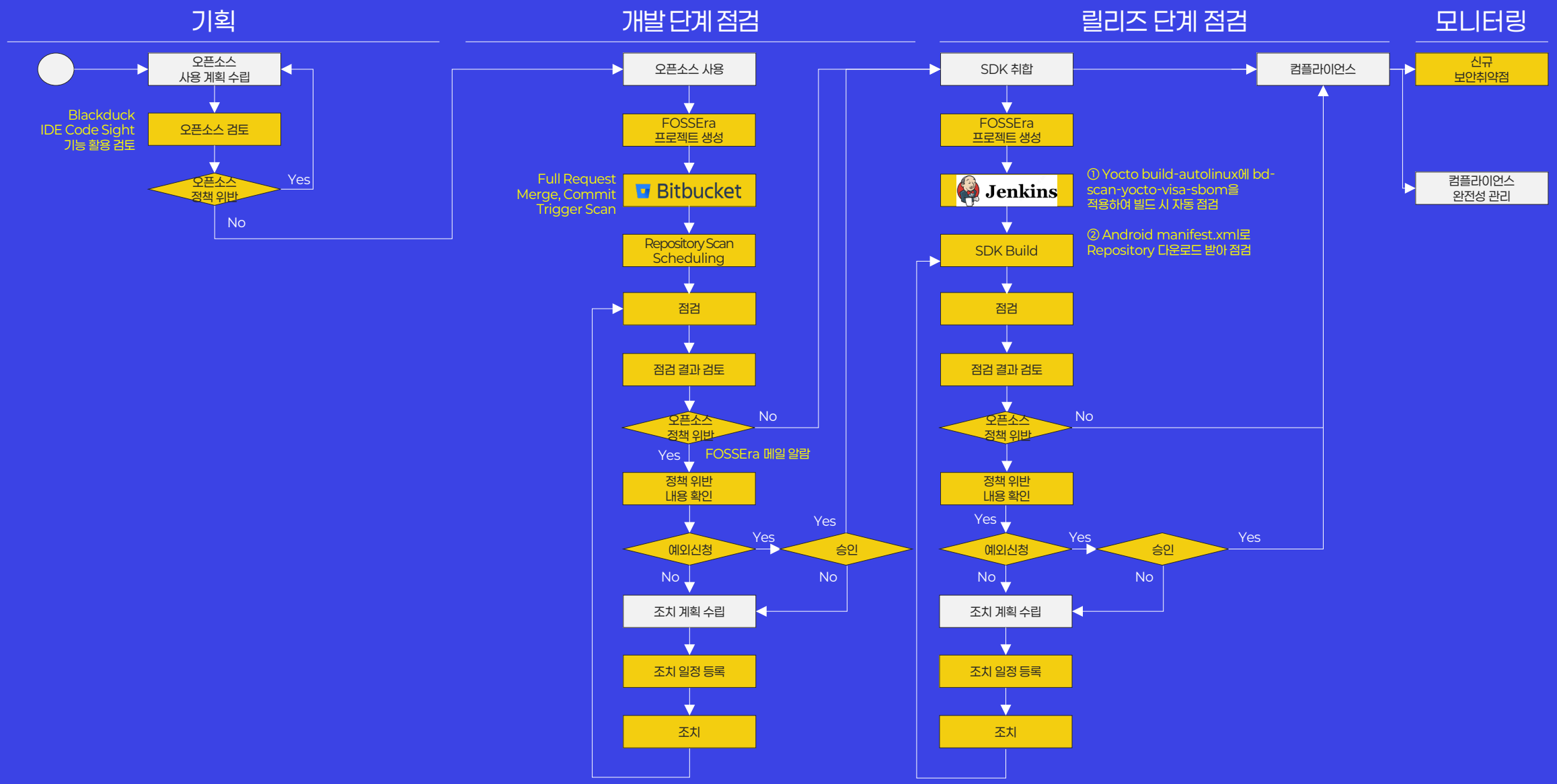
릴리즈 단계 점검



FOSSEra에 Project 생성

Telechips

7 SDLC 점검 프로세스



Telechips

8 최종 목표

Value

안전한 오픈소스 사용

오픈소스 기술 경쟁력 강화

Plan

리나로 프로젝트 참여

리나로(Linaro): ARM 기반의 시스템 온 칩(SoC) 관련 리눅스 프로젝트

TOPST 프로젝트 본격화

TOPST: 다양한 산업군에서 활용할 수 있는 오픈소스보드 > 오픈소스로소스코드공개예정

Yocto Community 시작

TOPST 사업부를 중심으로 Yocto 기술 공유 국내 커뮤니티 시작

- 오픈소스 기여정책·프로세스 구체화
- 기여 독려·보상·지원 방안 마련
- 오픈소스 프로젝트 활성화방안모색
- 외부 기업 / 개발자 참여 독려
- 오픈소스 기여 문화 정착

Goals

2025년 하반기 Open Chain 인증 취득

Taker에서 Giver로 오픈소스 활동 전환

오픈소스 친화적 기업 활동 확대

감사합니다.

Telechips