The supply chain, tool updates and the need for standardized interfaces

Marcel Kurzmann, Robert Bosch GmbH

OpenChain Automotive Workgroup 2024-09

BOSCH

Recap

https://www.openchainproject.org/

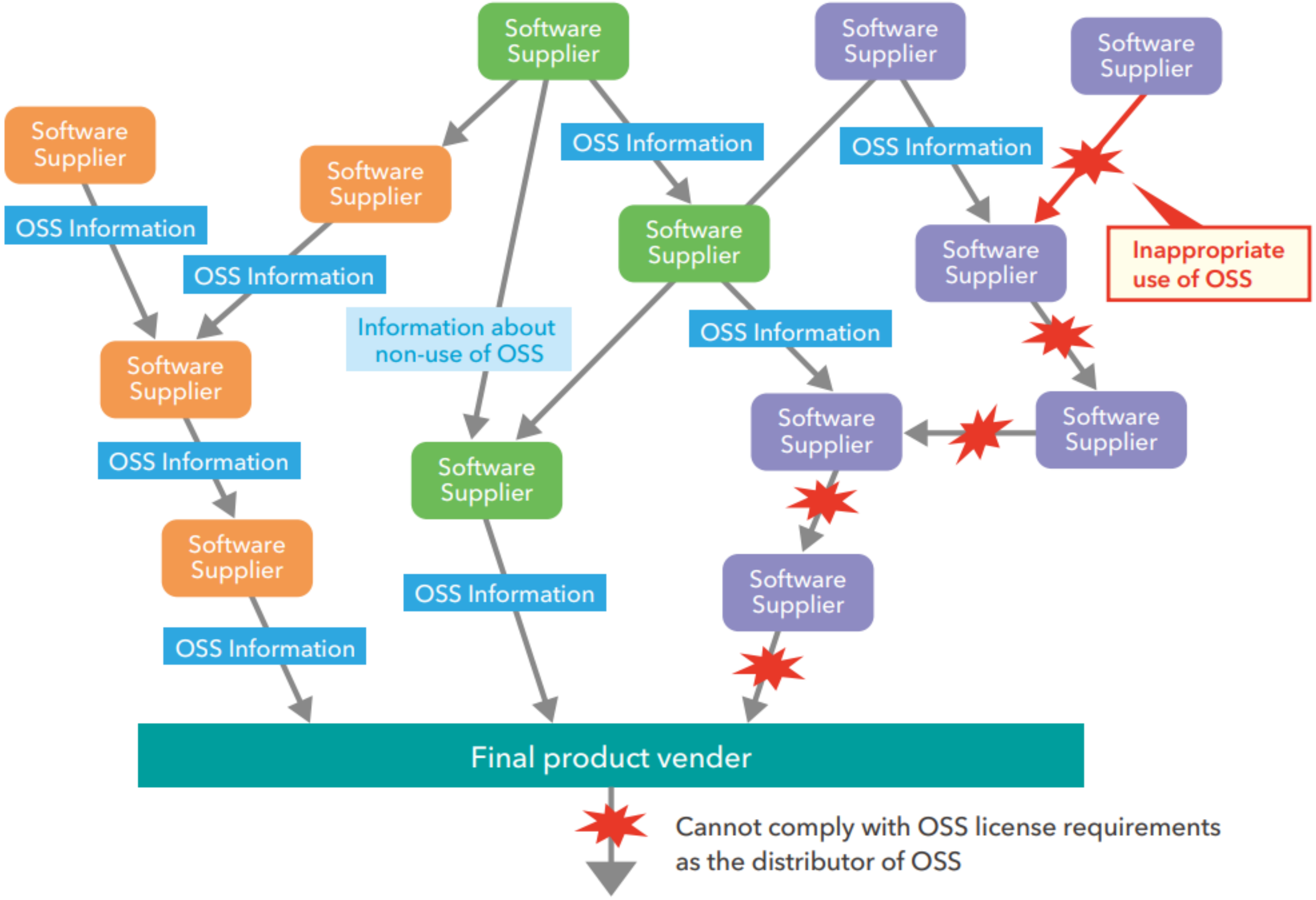
OPENCHAIN

Supply Chain

Recap

Different links in the „chain“

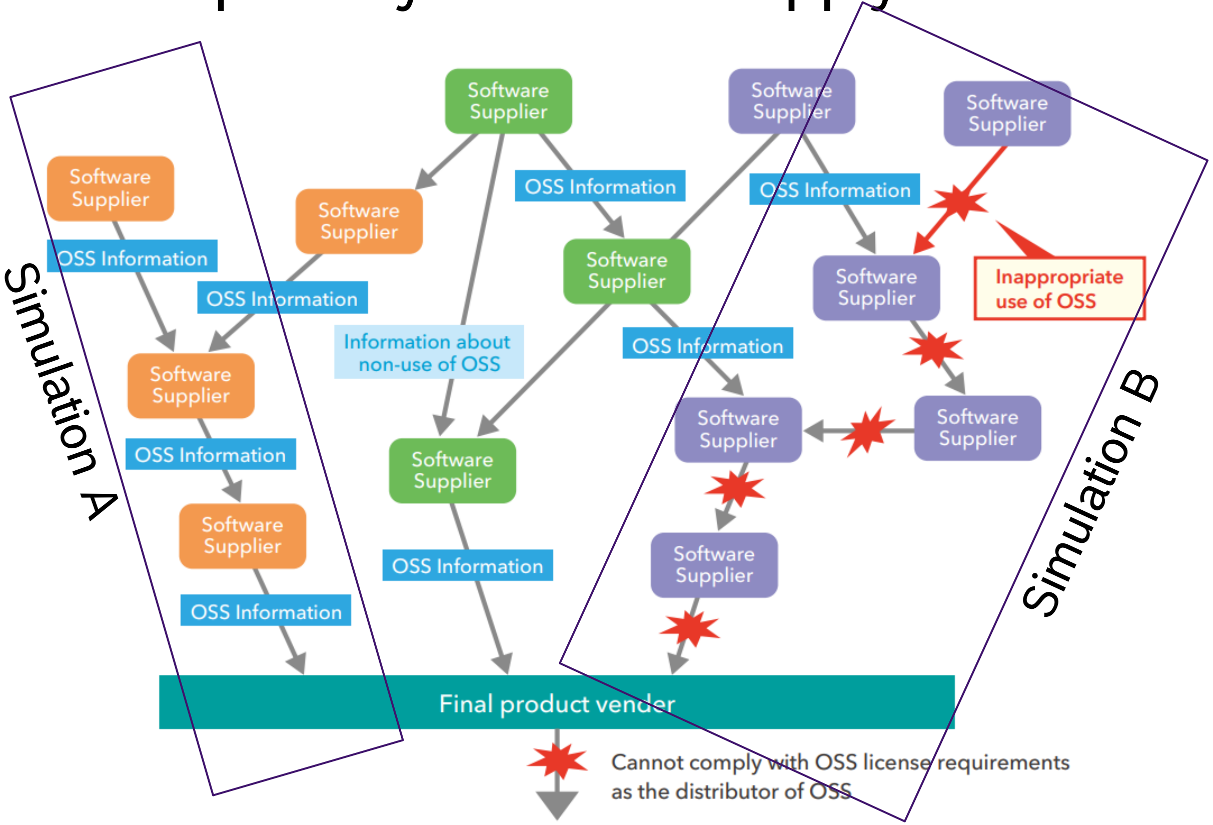
- Different contexts
- Different use cases
- Different problem spaces



Source: https://github.com/OpenChain-Project/Reference-Material/blob/master/Education-For-Suppliers/Supplier-Education-Leaflet/supply-chain-education-leaflet-version-1-2019/OpenChain-2.1-Edition/en/supplier-leaflet-en.pdf

Idea

Establish a publicly available supply chain simulation!



Benefits:

- Use for trainings
- Use for showcases
- Use for testing the tool chain / infrastructure
- Reference for interface discussions
- …

Source: https://github.com/OpenChain-Project/Reference-Material/blob/master/Education-For-Suppliers/Supplier-Education-Leaflet/supply-chain-education-leaflet-version-1-2019/OpenChain-2.1-Edition/en/supplier-leaflet-en.pdf

Recap

https://oss-compliance-tooling.org/

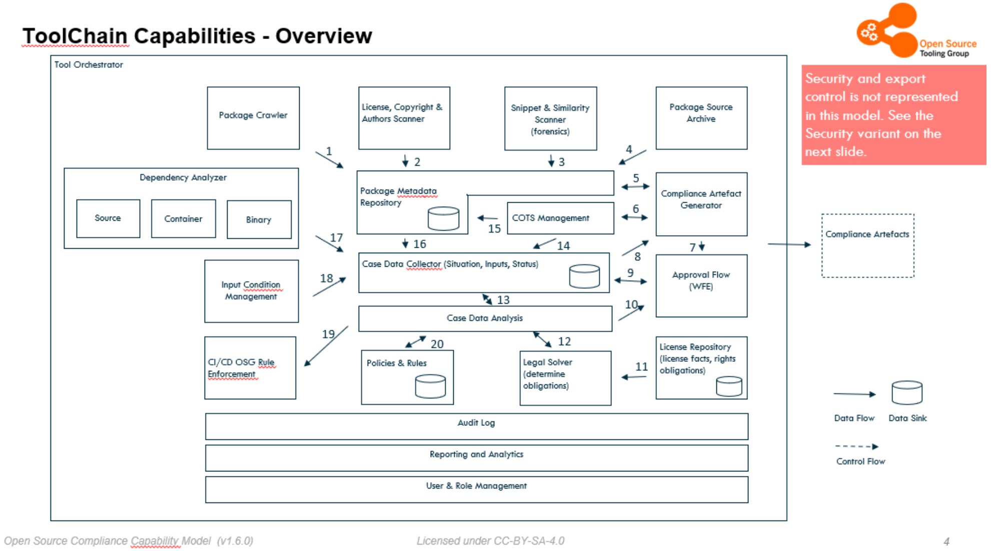
sharing-creates-value

Open Source
Tooling Group

Open Source Tooling Group aka OpenChain Automation Workgroup

Tool Updates

Recap


ToolChain Capabilities - Overview
Open Source Tooling Group
Tool Orchestrator
Package Crawler
License, Copyright & Authors Scanner
Snippet & Similarity Scanner (forensics)
Package Source Archive
Dependency Analyzer
Source
Container
Binary
Package Metadata Repository
COTS Management
Compliance Artefact Generator
Compliance Artefacts
Input Condition Management
Case Data Collector (Situation, Inputs, Status)
Approval Flow (WFE)
Case Data Analysis
CI/CD OSG Rule Enforcement
Policies & Rules
Legal Solver (determine obligations)
License Repository (license facts, rights obligations)
Audit Log
Reporting and Analytics
User & Role Management
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
Data Flow
Data Sink
Control Flow
Open Source Compliance Capability Model (v1.6.0)
Licensed under CC-BY-SA-4.0
4

Security and export control is not represented in this model. See the Security variant on the next slide.

Capability Map

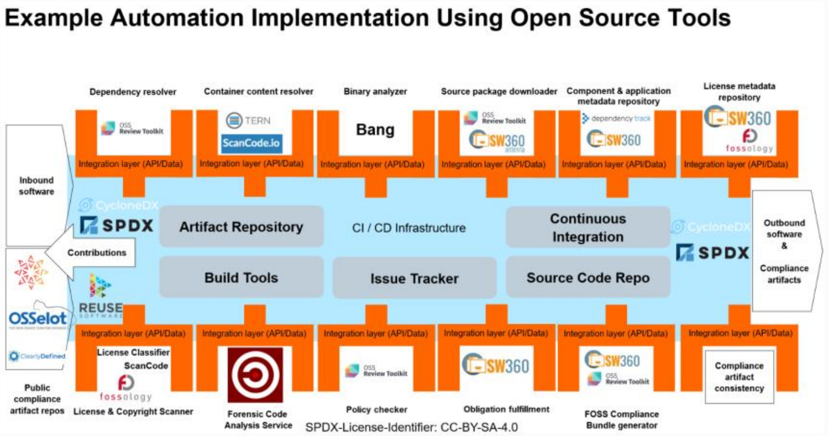
- beyond mere tooling

Source: https://github.com/Open-Source-Compliance/Sharing-creates-value/blob/master/Tooling-Landscape/CapabilityMap/OC_ToolingChain_v1.6.0.pptx

Tool collection

- Potential „solutions“
- Regular exchange (bi-weekly) on tool updates

Focus on Open Source Tooling!


Example Automation Implementation Using Open Source Tools
Dependency resolver
Container content resolver
Binary analyzer
Source package downloader
Component & application metadata repository
License metadata repository
OSS Review Toolkit
TERN
ScanCode.io
Bang
SW360
dependency track
fossology
Integration layer (API/Data)
Inbound software
CycloneDX
SPDX
Artifact Repository
CI / CD Infrastructure
Continuous Integration
Outbound software & Compliance artifacts
Contributions
Build Tools
Issue Tracker
Source Code Repo
REUSE SOFTWARE
OSSelot
ClearlyDefined
Public compliance artifact repos
License Classifier
ScanCode
License & Copyright Scanner
Forensic Code Analysis Service
Policy checker
Obligation fulfillment
FOSS Compliance Bundle generator
Compliance artifact consistency
SPDX-License-Identifier: CC-BY-SA-4.0

Source: https://oss-compliance-tooling.org/Tooling-Landscape/Toolchain-description/

What is the adequate „solution“ for my „problem“?

Background

Goals and needs

- Find match: Map your needs and

  ... find existing solutions

  ... find birds of a feather

Fact sheets

- Share and reuse

Generic architecture model

Standardized representation

- Standardizing while keeping flexibility

Example: Finding clothes online

1st limitation of search range

Women OR Men OR Kids

2nd limitation of search range

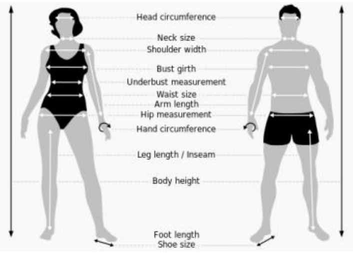
Clothing OR Shoes OR Sportswear OR ...

3rd limitation of search range

Jackets OR T-Shirts OR Pants OR ...

4th limitation of search range

Size ? Determine parameters



„Fact sheet“

Size Chart

XS, S, M, L, XL

Source: https://commons.wikimedia.org/wiki/File:Body_measures_SVG.svg

Get overview of all clothes matching to your parameters https://eclipse-apoapsis.github.io/guidance/

in incubation!

Eclipse Apoapsis
Overview 1/2

- Eclipse Apoapsis Guidance is meant as „landing page“ for navigation (https://github.com/eclipse-apoapsis/guidance)
  - Part A => collecting context information
  - Part B => providing a generic structure for the navigating the „problem spaces“ and map to solutions
    - Standard structure on each level:
      - Problem space
      - Generic architecture
      - Blue prints

- Eclipse Apoapsis ORT-Server (https://github.com/eclipse-apoapsis/ort-server)
  - The ORT server is a standalone application to deploy the OSS Review Toolkit as a service in the cloud

Detailed presentation will be provided in the OCX’24:

Eclipse Apoapsis - Open Source based Software Composition Analysis at scale

Eclipse Apoapsis
Overview 2/2

referring to

- Eclipse Apoasis Guidance => [Part B) Levels]
- **SupplyChain Level**
  - OpenChain Automation Workgroup - SW Dummies
  - ORT Server - public test server
  - OEM SBOM portals
- **Portfolio Level**
  - ORT Server
  - SPDX Operations Profile
  - OWASP DependencyTrack?
- **Product Level**
  - SPDX Operations Profile
- **SW Development Level**

OpenChain Automation Workgroup

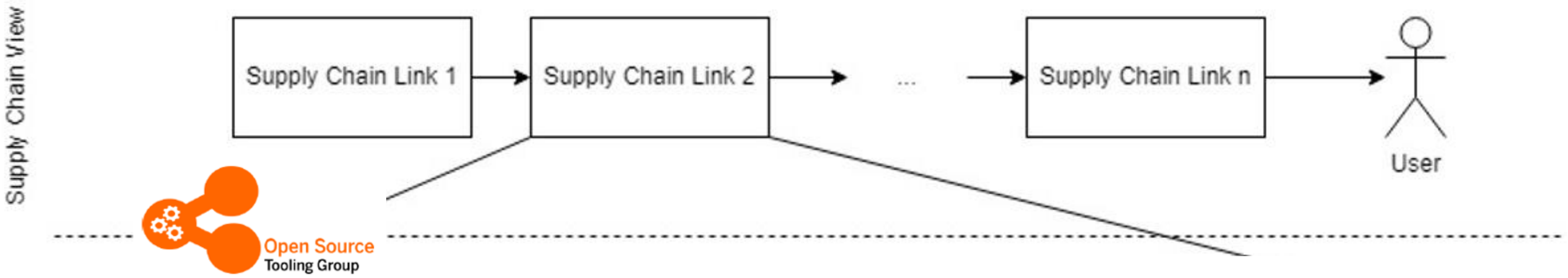
SPDX

OSS Review Toolkit

OpenChain Automation Workgroup => Tools

Coming back to the main idea

Establish a publicly available supply chain simulation - status

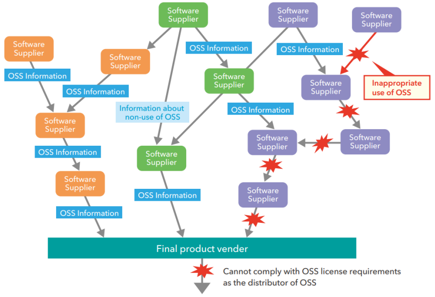


See https://github.com/Open-Source-Compliance/Go-Dummy

1. Dummy-repository simulating upstream
2. Open Source based SCA tooling simulating a SW supplier
3. Open Source Portal/Database simulating an OEM

Detailed presentation will be provided in the OCX’24:

Hello World+ projects to test and benchmark software composition analysis tools



Need for standardized Interfaces
Two-sided

- Standardized interface between the links in the supply chain
  - SPDX, CycloneDX, SWID … => only formats
  - Need for schemes to define the semantics => SEPIA

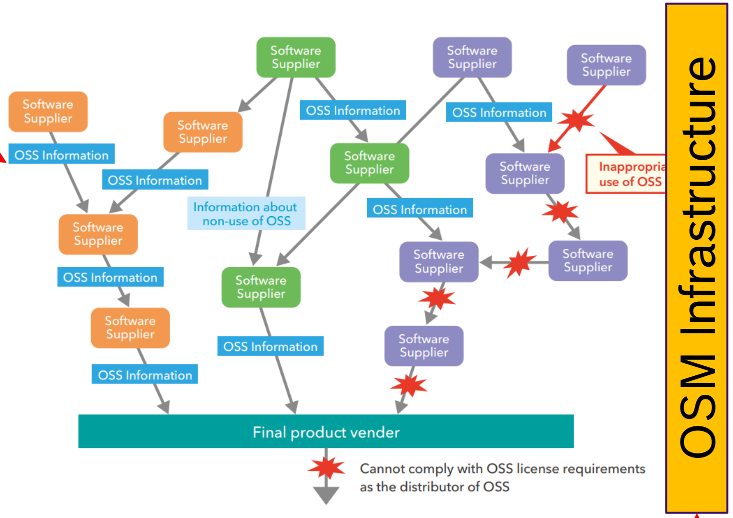
  Detailed presentation will be provided in the Bitkom bfoss24

  SEPIA – SBOM Exchange Procedures, Interfaces and Architecture

- Standardized interface for the tools / infrastructure
  - ORT-Server JVM-API => may integrate further „workers“ from other ven
  - SPDX Version 3 with different profiles => allows „metamodel“ extension
  - SPDX „Operations profile“ to cover also information about the business context

  https://github.com/spdx/spdx-3-model/tree/profile-operations

  SPDX general meeting every first Thursday of a month



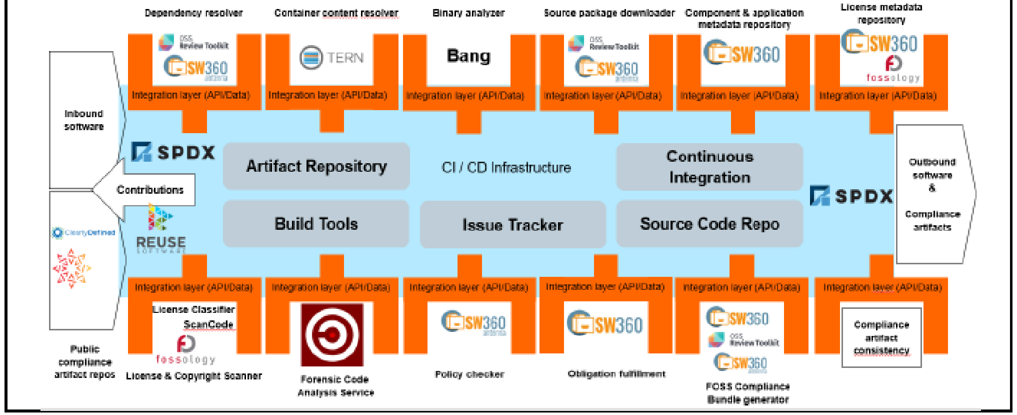
Reference Tooling Work Group

We are building an open source compliance toolchain ecosystem with open source tools as an open source project.
To accomplish this we:

- Use existing independent tooling projects
- Provide reference workflows to allow their adoption
- Provide the concepts and glue to ensure easy interoperability and integration in existing environments
- Provide reference turnkey toolchains that can be used without fees by anybody

World-Wide Collaboration, World-Wide Availability

Example Automation Implementation Using Open Source Tools



Dependency resolver

Container content resolver

Binary analyzer

Source package downloader

Component & application metadata repository

License metadata repository

Integration layer (API/Data)

Inbound software

Contributions

Public compliance artifact repos

Artifact Repository

CI / CD Infrastructure

Continuous Integration

Build Tools

Issue Tracker

Source Code Repo

Outbound software & Compliance artifacts

License Classifier

ScanCode

License & Copyright Scanner

Forensic Code Analysis Service

Policy checker

Obligation fulfillment

FOSS Compliance Bundle generator

Compliance artifact consistency

Join Us in Creating a New Era for Open Source Compliance

Mailing List: oss-based-compliance-tooling@groups.io

Subscription page: https://groups.io/g/oss-based-compliance-tooling

Online meetings: Bi-weekly - Invitations are sent to the mailing list

Website: https://oss-compliance-tooling.org/

And of course we are on GitHub:

https://github.com/Open-Source-Compliance/Sharing-creates-value

Oliver Fendt

THANK YOU!

Open Source
Tooling Group

Join Us in Creating a New Era for Open Source Compliance

Mailing List: oss-based-compliance-tooling@groups.io

Subscription page: https://groups.io/g/oss-based-compliance-tooling

Online meetings: Bi-weekly – see OpenChain Global Calendar
https://www.openchainproject.org/participate

Website: https://oss-compliance-tooling.org /

And of course we are on GitHub:
https://github.com/Open-Source-Compliance/Sharing-creates-value

BOSCH