Bosch – a global network
Four business sectors

Mobility Solutions

Industrial Technology

Energy and Building Technology

Consumer Goods

Researchers and developers across the globe

45,700 associates in research and development

3,000 developers for the Internet of Things

15,000 software engineers

94 research and development locations in 25 countries
Bosch Software Innovations
Spearheading the Internet of Things

Market presence
6.2m connected devices using Bosch IoT Suite

Know-how
800+ IoT experts around the world (Germany, Bulgaria, Singapore, China, Japan, USA)

Experience
250+ IoT international projects in the areas of manufacturing, mobility, energy, home & building, city, agriculture ...

Mobility
Solutions for electromobility, intermodal transportation, and connected vehicles

Industry
Solutions for connected manufacturing

Agriculture
Solutions to support the sustainable intensification of food production

Energy
Solutions for smart and simple energy management

Smart Home & Building
Solutions for connected homes and commercial buildings

Smart City
Connected solutions for urbanites to make life easy and efficient
Ecosystem & Partnerships
Current members of Eclipse IoT Working Group

Source: http://iot.eclipse.org/working-group/
OPEN SOURCE MANAGEMENT
End-to-end compliance

Introduction

- Compliance management is a set of actions that manages OSS components used in products. Companies may have similar processes in place for proprietary components. FOSS components are called "Supplied Software" in the OpenChain specification.

- Such actions often include:
  - Identifying all the FOSS components used in Supplied Software
  - Identifying and tracking all obligations created by those components
  - Confirming that all obligations have been or will be met
  - Small companies may use a simple checklist and enterprises a detailed process.
End-to-end compliance
Example enterprise process

Queued for Process
- Own Proprietary Software
- 3rd Party Software
- FOSS

Identification
Audit
Resolve Issues
Reviews
Approvals
Registration
Notices
Verifications
Distribution
Verifications

Compliance Process
- Review and approve compliance record of FOSS software components
- Compile notices for publication
- Post publication verifications

Outgoing Software
- Written Offer
- Notices & Attributions

Identify FOSS components for review
Scan or audit source code – and – confirm origin and license of source code
Resolve any audit issues in line with company FOSS policies
Record approved software/version in inventory per product and per release
Verify source code packages for distribution – and – verify appropriate notices are provided
Publish source code, notices and provide written offer

Example of Compliance Management End-to-End Process
Open Source Management (OSM) system

Parameters that influence your OSM system setup

- License constraints
  - E.g. only permissive licenses vs. strict copyleft licenses

- Used technologies
  - E.g. JAVA and Maven vs. C-Code on real-time systems

- Development approach
  - E.g. platform development vs. customer specific project development
Open Source Management

Key elements

- Artifact repository
- Source code repository
- Component metadata database
- License database
  - Obligation catalogue
  - Obligation fulfillment guidelines
- Open source code archive

Thesis: those key elements exist (at least virtually) in every OSM system independently from
  - License constraints
  - SW technology
  - Development approach
- Those building blocks are not differentiating (only the managed content and the integration maybe)
Generic Open Source Management system

Key elements

Artifacts Repository
Source Code Repository
Software Build
Software Metadata
Licenses Metadata
Guidance
Obligation Identification
Obligation Fulfillment
Open Source Code Archive
Software Release
FOSS Bundle

What components?
What licenses?
What obligations?
What necessary measures?
License metadata

Services and challenges

Services
- License Provision Service
- License Mapping Service
- License Classification Service
- Application Evaluation Service
- Legal Consulting Service

Challenges
- Standard vs. customized licenses
- Non-standardized license declaration
- Different License Lists
  - OSI Approved, SPDX, TLDRlegal.com, ...
- Context dependency (SaaS, Linking/Embedding, …)
- License incompatibilities
- “Grey areas”
  - Room for interpretation
  - Half-knowledge, wrong interpretations,…
  - License FAQs
  - …

Facilitate by internal services and re-use
Software metadata

Services and challenges

**Services**
- Artifact Scan Service
- Source Code Provision Service
- Source Code Scan Service
- Copyright Provision Service
- Vulnerability Service
- Traceability Service

**Facilitate by information hub**

**Challenges**
- No unique artifact identifiers
- Artifacts with missing source code
- Artifacts with incomplete or fake source code files
- Reference databases of scan tools only updated with delay (leading edge components may be unknown)
- Minified, uglyfied or obfuscated sources
- FOSS components spread over multiple projects/applications
- Different formats and APIs
- ...
FOSS bundle
Services and challenges

FOSS bundle = The totality of the fulfillment of all obligations required for distribution

(Die Gesamtheit der Erfüllung aller zur Distribution erforderlichen Obligationen)

Services

▶ OSS Disclosure Document Service
▶ Copyright Listing Service
▶ Source Code Hosting Service (e.g. written offer)
▶ OSS Source Code Bundle Service
▶ Software Backup Service

Facilitate by automation

Challenges

▶ Time-consuming consolidation of attributions
▶ Different provision channels needing different formats
▶ Various possible obligations exceeding mere provision of attributions
▶ Non-standardized inputs and varying quality of inputs
▶ Integration in an automated build process for continuous delivery
MOTIVATION
Open Chain

Basic OSM-maturity through the supply chain

- Value the work of the open source communities by establishing and maintaining a professional Open Source Management
- Share good practices with suppliers and partners
- Spread the good practices to increase the overall OSM-maturity in the business
- Continuous delivery needs automated processes!

All parts of the supply chain need to keep the source code clean.
OPEN SOURCE PROJECTS FOR OPEN SOURCE MANAGEMENT
Generic Open Source Management system

Key elements

Obligation Fulfillment

Obligation Identification

What components?

What licenses?

What obligations?

What necessary measures?

Software Build

Artifact Repository

Source Code Repository

git

Ant, Gnu, Maven, Gradle,…

sw360

Information Hub

e.g. Protex, iQ

Fossology

Software Metadata

License Metadata

SPDX

Guidance

Obligation Fulfillment

Software Heritage

Open Source Code Archive

Software Release

FOSS Bundle

© Bosch Software Innovations GmbH 2017. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution as well as in the event of applications for industrial property rights.
Tooling vs. employee skills

Trainings and certification

- Automation is the key and tools are important

BUT

- A fool with a tool is still a fool

- Focus on the skills of the developers!
  - Open Chain Curriculum

- Check your OSM-maturity and the maturity of your suppliers
  - Open Chain Specification / Self-Certification
Open Source projects

In the context of Open Source Management

- [https://github.com/Open-Source-Compliance](https://github.com/Open-Source-Compliance)
- [https://www.fossology.org/](https://www.fossology.org/)
- [https://spdx.org/](https://spdx.org/)
- [http://todogroup.org/#](http://todogroup.org/#)
- [https://projects.eclipse.org/projects/technology.sw360](https://projects.eclipse.org/projects/technology.sw360)
- [https://git-scm.com/community](https://git-scm.com/community)
- [https://www.openchainproject.org/](https://www.openchainproject.org/)
- [https://www.softwareheritage.org](https://www.softwareheritage.org)
Open Source Management (OSM)

Further potential for collaboration

- Electronically processable Obligation catalogue => OSADL Open Source License Obligations Checklist [https://www.osadl.org/Single-View.111+M5dfb2364cee.0.html](https://www.osadl.org/Single-View.111+M5dfb2364cee.0.html) => Open Chain
- Creation of the FOSS bundle
- Sharing and reuse of metadata (ideally hosted by the OSS-project itself => SPDX-format)

- Find more tools, gadgets and good practices in Open Chain and TODO-group:
  - [https://github.com/todogroup](https://github.com/todogroup)
  - [https://opensource.google.com/docs/](https://opensource.google.com/docs/)

- Outlook for Contribution Management:
Open Source Management (OSM)
The OSM Community

- Let’s enable a professional Open Source Management for everyone!

- If you need help ask!
THANK YOU

Marcel Kurzmann
Marcel.kurzmann@bosch-si.com
Open Source Officer
Bosch Software Innovations

Dr. Steffen Evers
Steffen.evers@bosch-si.com
Head of Open Source Services
Bosch Software Innovations

Follow us on
Bosch ConnectedWorld Blog