Build systems, traceability and compliance

Arnout Vandecappelle

LPC 2024 – Build System MC

mind

an open source of wisdom

Who is Arnout

Embedded software architect

Focus on Linux OS integration

Mind consultant since 2008

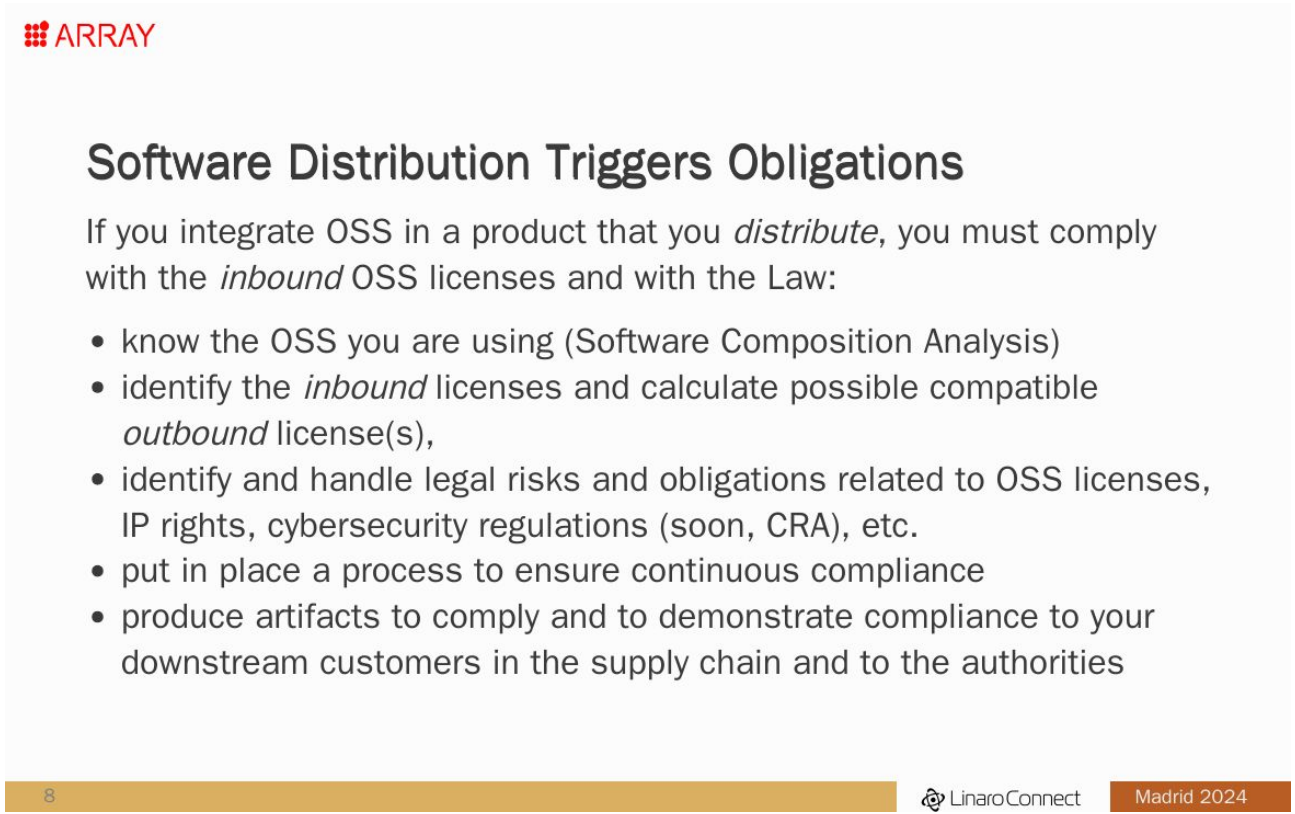
Worked for 40+ customers in multimedia, security, home automation, satellite, telecom, chips, ...

Buildroot maintainer (team of 5)

Agenda

- What is traceability and compliance and why do we need it?
- What can we (build systems) do to improve?

Compliance = knowing what is in the software you distribute



Implementing an Openchain compliant policy and best practice at Linaro, Alberto Pianon and Carlo Piana, Array

More complex if you have a downstream

Current: produce an image → give to end user

Not sufficient if image is re-composed by downstream

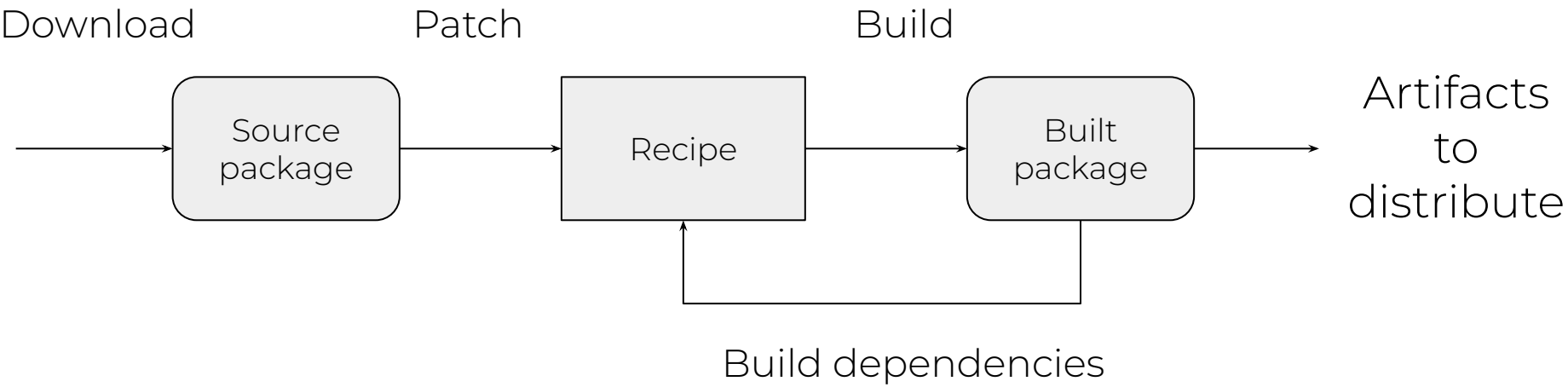
- **A** - Platform image to which downstream adds software
- **B** - Container image composed with others
- **C** - SDK to build appliance
- **D** - ...

Who sees one of the use cases above?

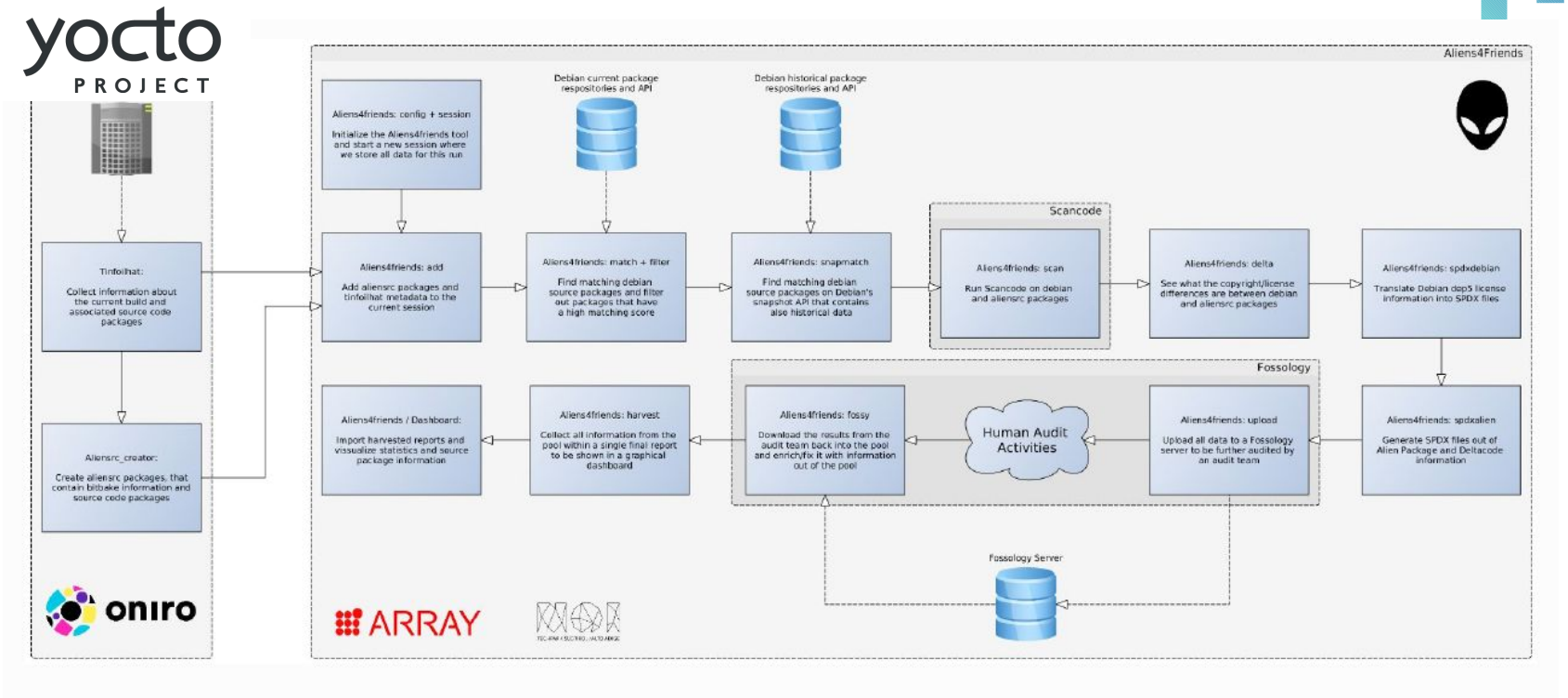
What does this mean concretely?

- Manifest that describes distributed components
- Decomposition
  - E.g. image consists of packages; package consist of files
- Provenance of each component
  - E.g. built from these sources
  - Sources downloaded from that URL at that time
  - Patched with these patches
- License of each component
  - License information is only accurate for source files
  - Concluded license needs some form of review
- Traceability of who concluded this

Build system terminology



Additional workflow on top of yocto for full compliance

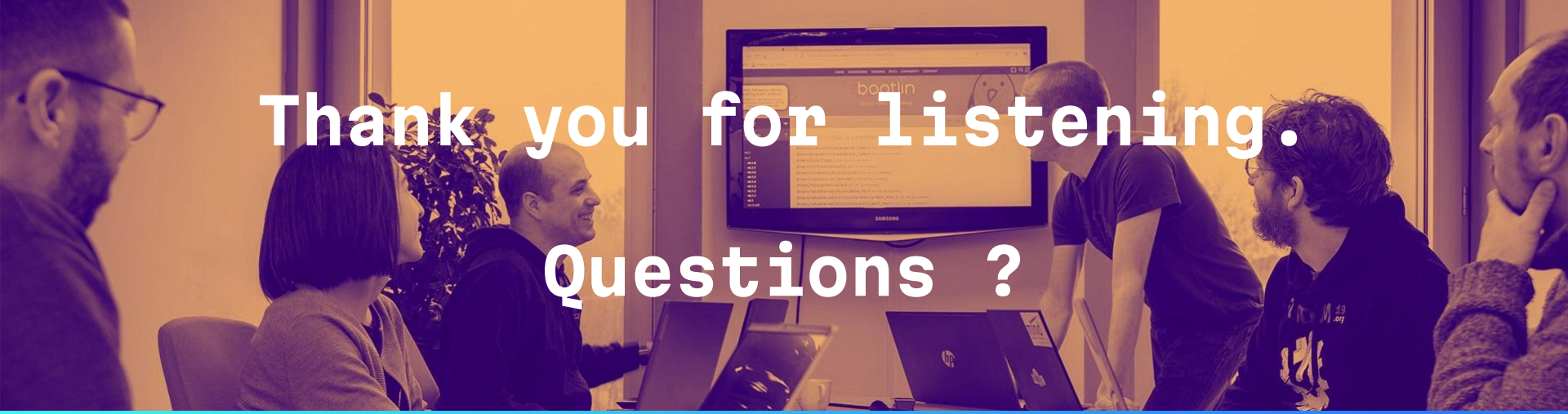


Implementing an Openchain compliant policy and best practice at Linaro, Alberto Pianon and Carlo Piana, Array

What can we do to improve the situation

- Collect per-file info
  - Every source file with its license
  - Every compiled / copied file with its (concluded) license
- Use upstream package's info directly
  - Instead of license info in recipe
  - E.g. cargo-spdx, reuse spdx
- Include per-file info in recipe
  - E.g. in SPDX or DEP5 or REUSE format
- Remove unused sources
  - To make concluded license more believable

What can we do to improve the situation



Thank you for listening.

Questions ?

mind

an open source of wisdom

mind
an open source of wisdom

Division of **Essensium nv**

Arenberg Science Park
Gaston Geenslaan 10
3001 Leuven
Belgium
+32 16 28 65 00

General enquiries
info@mind.be

Employment enquiries
jobs@mind.be