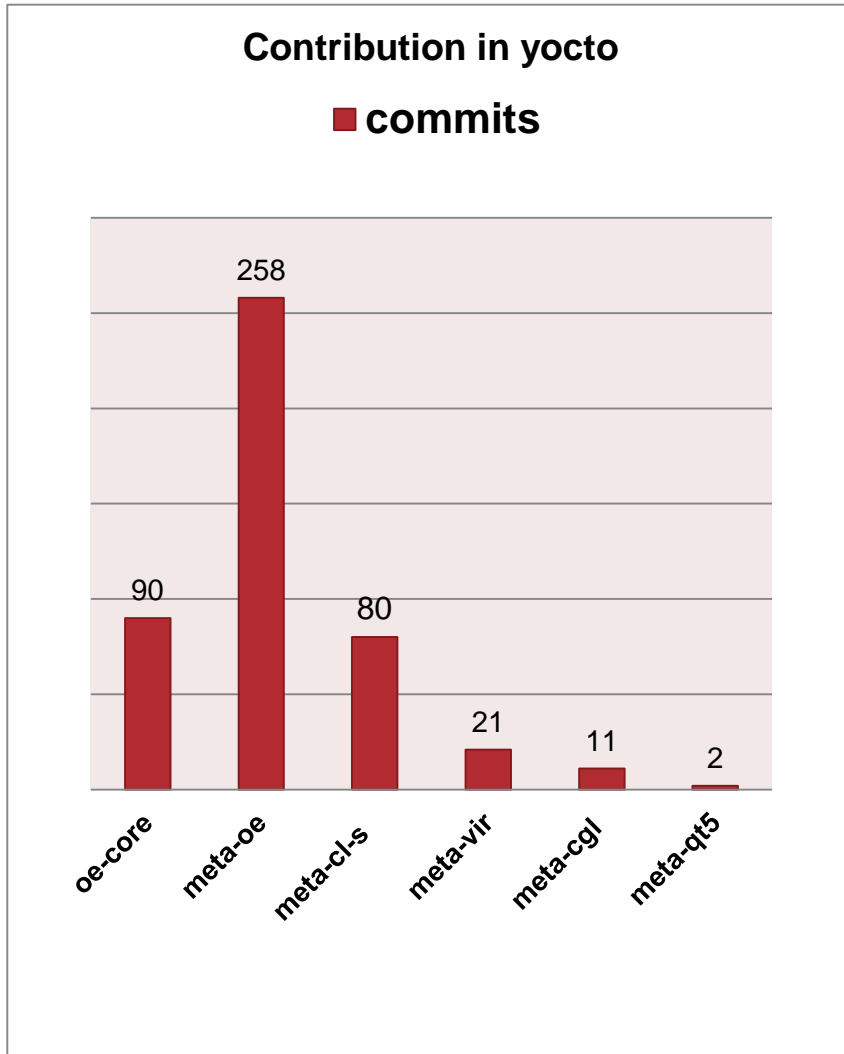


# A Smart Way to Manage OSS Compliance with Yocto+SPDX

Zheng Ruoqin, Fujitsu  
zhengrq.fnst@cn.fujitsu.com  
Lei Maohui, Fujitsu

# Fujitsu's contributions to Yocto community

■ Data comes from yocto (2015 ~)



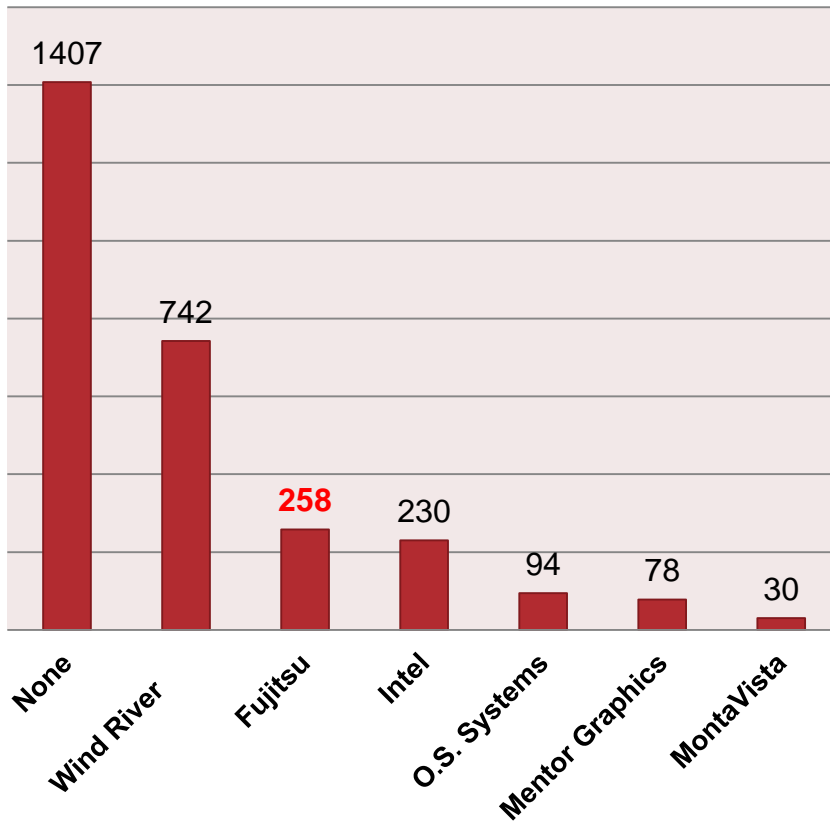
	Layers	Changesets
1	oe-core	90
2	meta-openembedded	258
3	meta-cloud-services	80
4	meta-virtualization	21
5	meta-cgl	11
6	meta-qt5	2

# Fujitsu's contributions to Yocto community

■ Data comes from meta-openembedded.git (2015 ~)

### Top changeset contributors by employer

■ commits



### Developers with the most changesets

	Developer	Changesets
1	Andreas Müller	440 (11.2%)
2	Derek Straka	421 (10.7%)
3	Martin Jansa	312 (7.9%)
4	Khem Raj	300 (7.6%)
5	Jackie Huang	141 (3.1%)
6	Armin Kuster	121 (3.1%)
7	<b>Li xin (Fujitsu)</b>	<b>100 (2.5%)</b>
8	Yi Zhao	86 (2.2%)
9	Roy Li	85 (2.1%)
10	Kai Kang	84 (2.1%)
11	Alexander Kanavin	81 (2.1%)
12	Fabio Berton	62 (1.6%)
13	Andre McCurdy	60 (1.5%)
14	Chen Qi	50 (1.3%)
15	Robert Yang	46 (1.2%)
16	Pascal Bach	44 (1.1%)
17	<b>Bian Naimeng(Fujitsu)</b>	<b>38 (1.0%)</b>

## Introduction of SPDX

- Background of SPDX
- What is SPDX
- Who are working for SPDX
- The status of SPDX specification
- SPDX file

## Yocto+SPDX

- What is Yocto
- Why we use SPDX in Yocto
- Current state about Yocto+SPDX
- What we have done for Yocto+SPDX
- Future work

## Manage SPDX files by smart

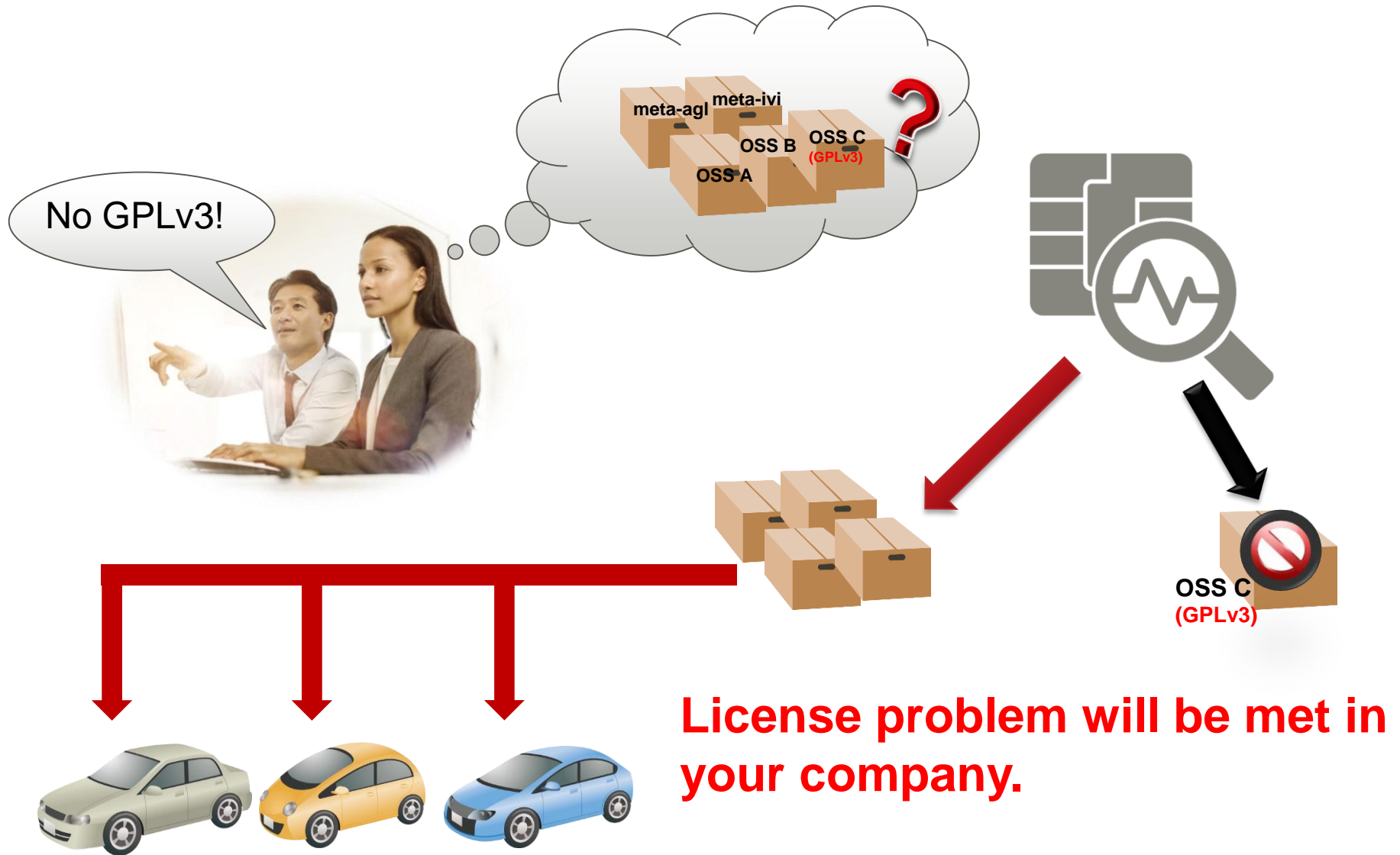
- What is smart
- What we have done
- How to Manage SPDX files by smart
- Future work

# Introduction of SPDX

- Background of SPDX
- What is SPDX
- Who are working for SPDX
- The status of SPDX specification
- SPDX file



# Background of SPDX(1/2)



# Background of SPDX(2/2)



**That Bill of Materials is SPDX which is part of the solution.**

- Obtain details from <https://spdx.org/learn>

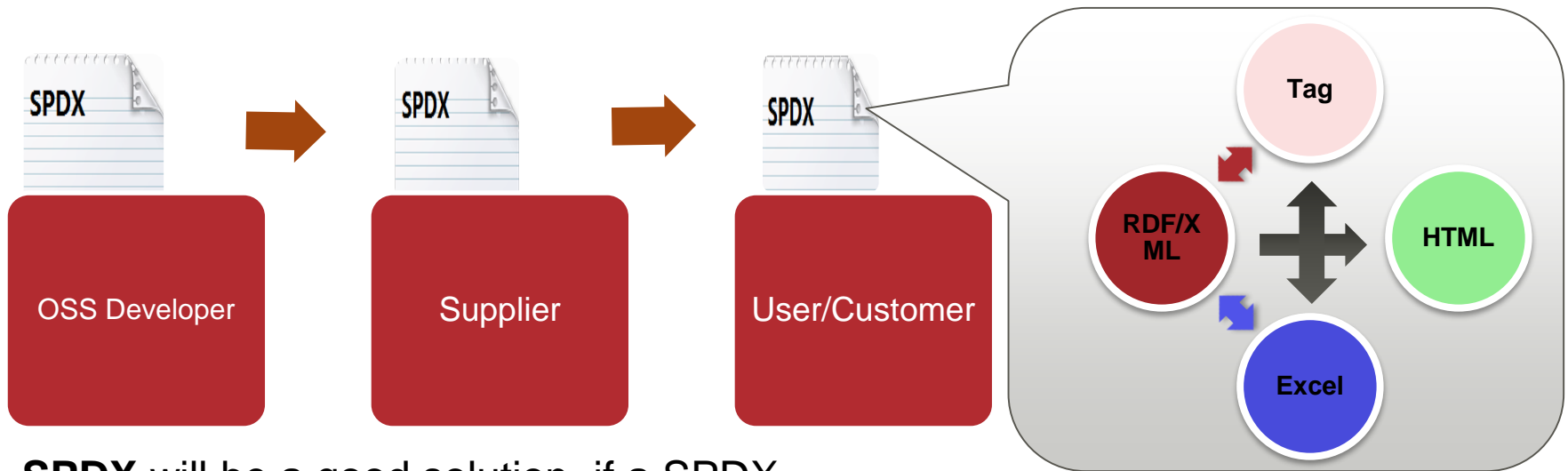


## What is SPDX

- The full name of SPDX is **Software Package Data Exchange**, which is a standard format for communicating the components, licenses and copyrights associated with a software package.

## Vision of SPDX

- achieve license compliance with minimal cost across the supply chain.



**SPDX** will be a good solution, if a SPDX implementation can generate SPDX file including license information automatically.

Obtain details from

- <https://spdx.org/tools>





# Who are working for SPDX

## Technical Team

- **Primary responsibility**
  - Drafts the specification
  - Develops documentation templates, samples and tools.
- **Delivered**
  - SPDX Spec (2.1, 2.0, 1.2, 1.1, 1.0)
  - Tool (fossology)d
  - Spreadsheet Template
- **Recent**
  - SPDX Specification 2.1
  - Tooling

## Legal Team

- **Primary responsibility**
  - Supports and provides recommendations to the SPDX working groups regarding licensing issues.
  - Maintains the [SPDX License List](#)
  - Promotes the SPDX specification to the legal community at-large
- **Delivered**
  - License Expression Syntax
  - License Inclusion Guidelines (Background))
  - Dealing with Public Domain within SPDX Files
- **Recent**
  - Joint Call with Tech Team
  - License List

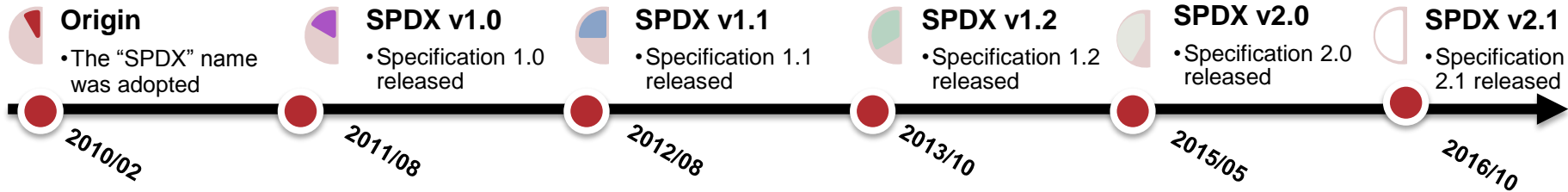
## Outreach Team

- **Primary responsibility**
  - Launch activities for new versions of the SPDX specification.
  - Outreach
  - Participation in events;
  - The SPDX website
- **Delivered**
  - Launch for 1.0 and 1.1
  - Process for Adding to License List (Draft))
  - SPDX Vision & Mission Discussion Document
  - SPDX Vision & Mission Statements (Final Draft))
- **Recent**
  - The SPDX website

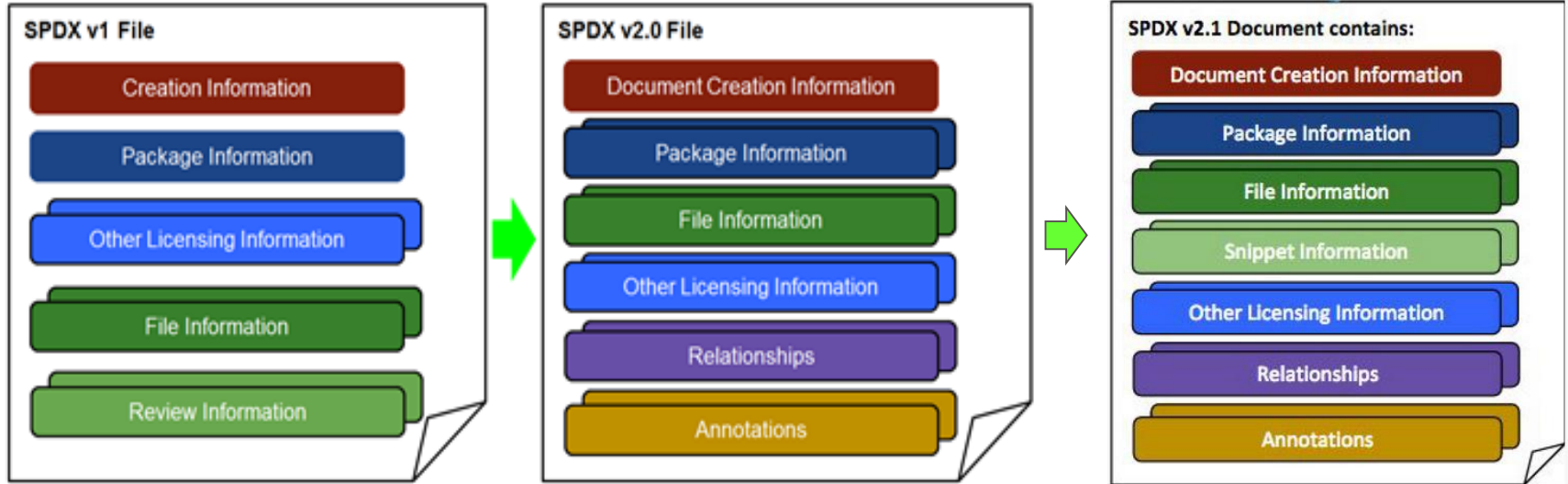
- **Obtain details from**
  - <http://spdx.org/participate>
  - [http://wiki.spdx.org/view/General\\_Meeting/Minutes](http://wiki.spdx.org/view/General_Meeting/Minutes)

# The status of SPDX Specification

## History



## Features in SPDX



## Formats

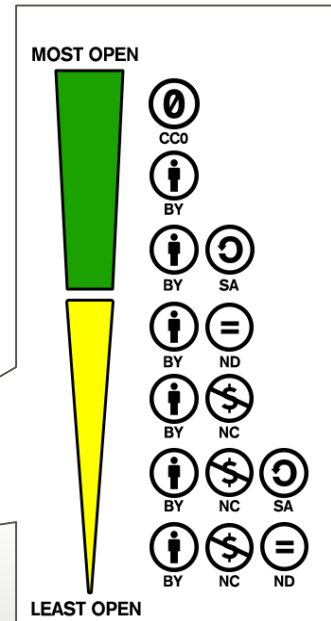
- Tag:value
- RDF/XML

## Important or useful tags

- SPDXVersion
- DataLicense
- Creator
- PackageName
- PackageOriginator
- PackageVersion
- PackageHomePage
- PackageLicenseDeclared

## A sample of SPDX file

```
SPDXVersion: SPDX-2.0
DataLicense: CC0-1.0
PackageName: Foo
PackageOriginator: David A. Wheeler
PackageHomePage: https://github.com/david-a-wheeler/spdx-tutorial/
PackageLicenseDeclared: MIT
```



# Yocto+SPDX

- What is Yocto
- Why we use SPDX in Yocto
- Current state about Yocto+SPDX
- What we have done for Yocto+SPDX
- Future work



# What is Yocto(1/2)

https://www.yoctoproject.org

LINUX FOUNDATION COLLABORATIVE PROJECTS

yocto PROJECT

SEARCH embedded linux Go

ABOUT  
ECOSYSTEM  
DOWNLOADS  
TOOLS + RESOURCES  
DOCUMENTATION

**New to the Project**  
Want to learn more, or just kick the tires? Start here.

START HERE TO LEARN MORE

Introducing the Yocto Project

It's not an embedded Linux distribution – it creates a custom one for you

The Yocto Project is an open source collaboration project that provides templates, tools and methods to help you create custom Linux-based systems for embedded products regardless of the hardware architecture. [Read more](#)

read the **Yocto Project Backgrounder**

learn about Toaster, the Yocto Project Graphical UI

register for developer day at ELC in Berlin

**The Yocto Project is an open source collaboration project that help you create custom Linux-based systems for embedded products**

<https://www.yoctoproject.org/>

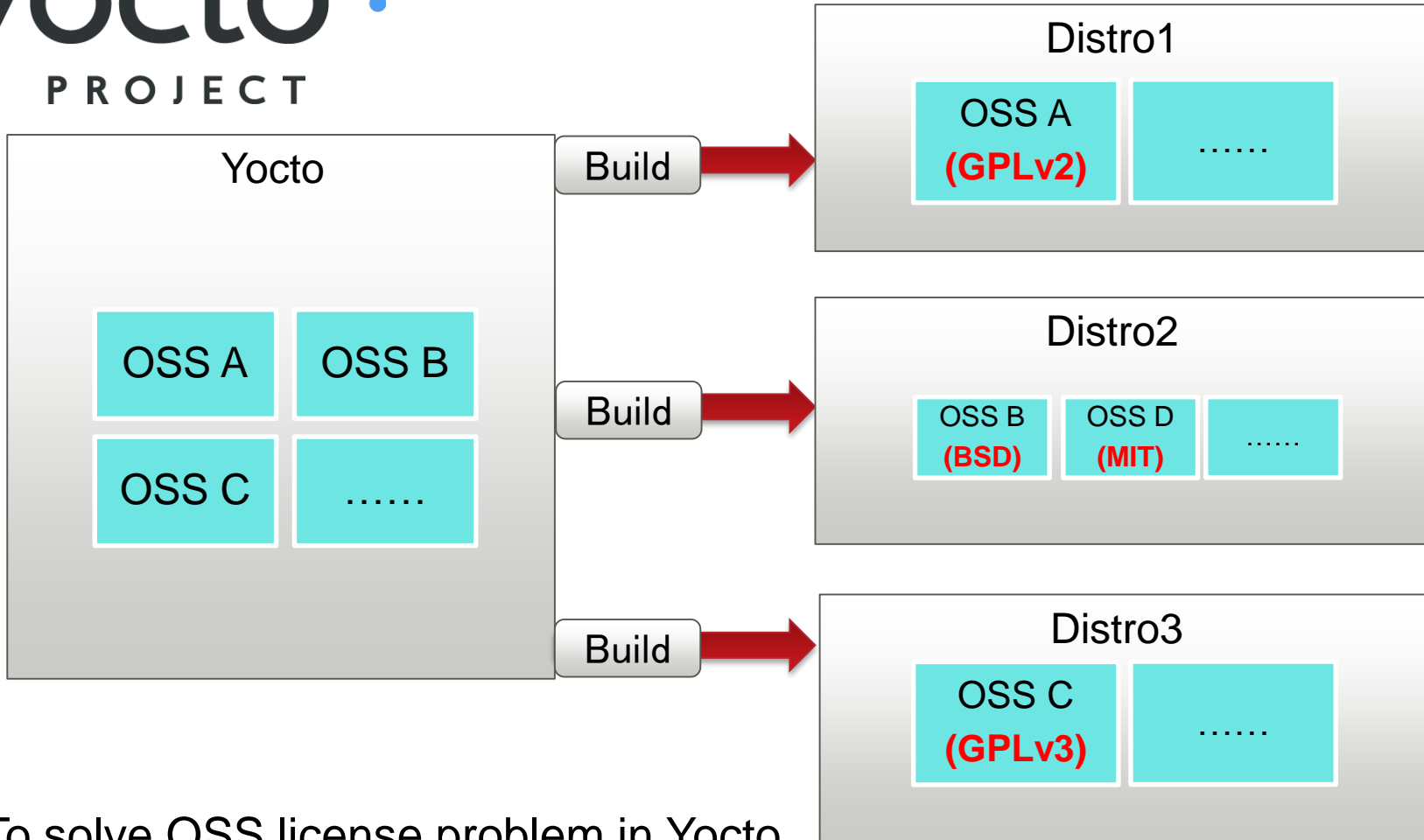
# What is Yocto(2/2)

## Members of Yocto Organization

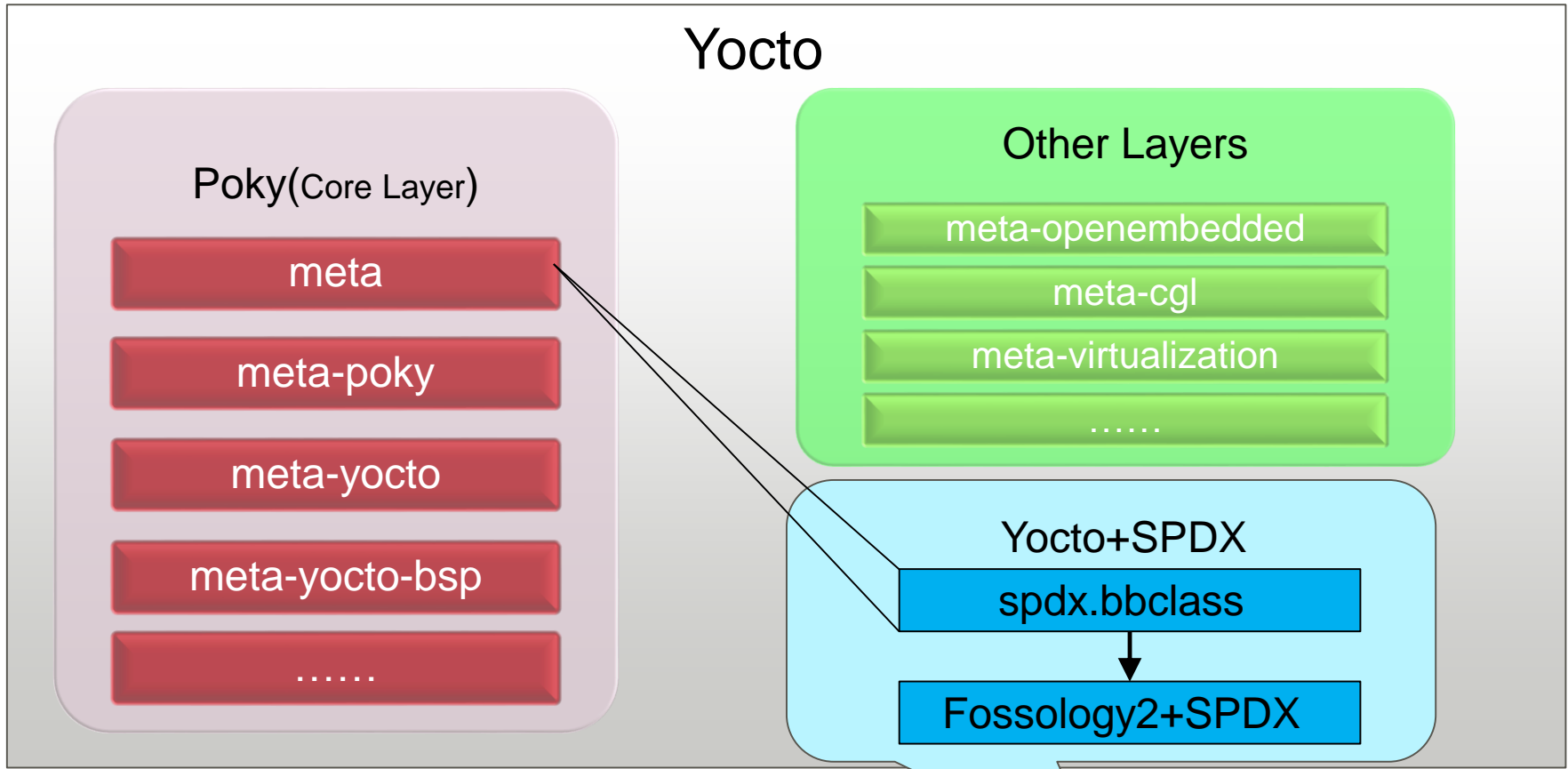


<https://www.yoctoproject.org/>

# Why we use SPDX in Yocto



To solve OSS license problem in Yocto.



## Bitbake taskflow





## History

- Yocto+SPDX was supported from yocto 1.5.

## SPDX Specification

- Yocto+SPDX supports SPDX v1.1 specification.

## SPDX Implementation

- Yocto+SPDX generates spdx files by using fossology2 with fossology-spdx module.
- Environment setup is complex, scanning time is long

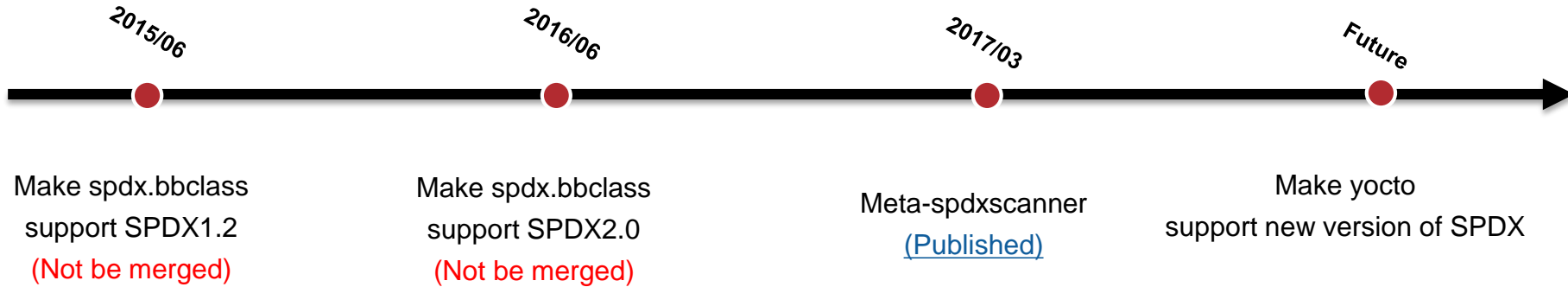
## Activity of Yocto+SPDX

- There are almost no improvements in spdx module.

```
$git log --pretty=format:"%ad %s" meta/classes/spdx.bbclass
Wed Dec 14 21:13:04 2016 +0000 meta: remove True option to getVar calls
Thu Sep 29 15:50:24 2016 -0700 subprocess: remove Popen in favor of check_output
Thu Nov 5 17:48:18 2015 +0200 bbclass: fix spelling mistakes
Thu Nov 13 15:49:52 2014 +0100 spdx.bbclass: improved error handling and code cleanup
Mon Oct 20 16:09:15 2014 +0200 spdx.bbclass: improved stability, fixed SPDX compliance issues. Changes are reflected in licenses
Tue Sep 23 17:48:12 2014 +0800 spdx.bbclass: Add SPDX-specific source tree variable.
Sun Sep 1 08:52:40 2013 +0100 meta: Don't use deprecated bitbake API
Fri Aug 23 14:40:35 2013 -0700 SPDX:real-time license scanning and SPDX output.
```

# What we have done for Yocto+SPDX

Tried to make Yocto support SPDX2.0



- Still use DoSOCSv2
  - Support SPDX 2.0
  - Faster
- Add DoSOCSv2-native into Yocto
  - Easy to build environment

- Introduce a new SPDX create tool - DoSOCSv2
  - Support SPDX 2.0
  - Faster

- Support SPDX 1.2

# Why we choose DoSOCsv2 (1/3)

## What is FOSSology

- FOSSology is an open source license compliance software system and toolkit. As a toolkit you can run license, copyright and export control scans from the command line. As a system, a database and web ui are provided to give you a compliance workflow. License, copyright and export scanners are tools available to help with your compliance activities. ([Website](#))

The screenshot shows the FOSSology web interface. At the top, there is a navigation menu with links for Home, Search, Browse, Upload, Jobs, Organize, Admin, and Help. The 'Upload' link is highlighted with a red box and a white arrow pointing to it. Below the navigation menu, the text 'Show Jobs' is visible, along with the FOSSology logo and version information (3.0.0, commit: [94b5377b]). On the right side, there is a 'logout' link and user information (User: fossy, Group: fossy). Below the navigation menu, there is a 'Close' button. The main content area displays 'SPDX 2 generation scheduled as job #98'. Below this, there is a table with the following data:

cpio-2.11.tar.gz						
Job/Dependency	Status				Average items/sec	ETA
98		spdx2				[Pause] [Cancel]
Job/Dependency	Status				Average items/sec	ETA
97	Completed	spdx2		2016-06-18 09:36 - 2016-06-18 09:36	0.00 items/sec	Scanned [Download SPDX]
Job/Dependency	Status				Average items/sec	ETA
95	Completed	ununpack	540 items	2016-06-18 09:36 - 2016-06-18 09:36	90 items/sec	
96 / 95	Completed	adj2nest	540 items	2016-06-18 09:36 - 2016-06-18 09:36		

A callout box with the text '[Download SPDX]' is positioned over the bottom right corner of the table.

## What is DoSOCSv2

- dosocsv2 is a command-line tool for managing SPDX 2.0 documents and data. ([Website](#))

```
$ dosocs2 oneshot cpio-2.11
dosocs2: cpio-2.11: package_id: 1
dosocs2: running nomos on package 1
cccccpio-2.11: document_id: 1
```

### **SPDXVersion: SPDX-2.0**

```
DataLicense: CC0-1.0
DocumentNamespace: sqlite:///home/leimh/.config/dosocs2/dosocs2.sqlite3/cpio-2.11-fe30375e-3a43-4d1e-9962-eb24f2dbe8bf
DocumentName: cpio-2.11
SPDXID: SPDXRef-DOCUMENT
DocumentComment: <text></text>
```

### ## External Document References

```
## Creation Information
Creator: Tool: dosocs2-0.16.1
Created: 2016-07-09T23:18:52Z
CreatorComment: <text></text>
```

### **LicenseListVersion: 2.2**

### ## Document Annotations

### ## Document Relationships

```
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-package-cpio_2_11-f6eb-4fa85311
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-file-ABOUT-NLS-b502-579bb6d1
```

```
.....
```

# Why we choose DoSOCSv2 (3/3)

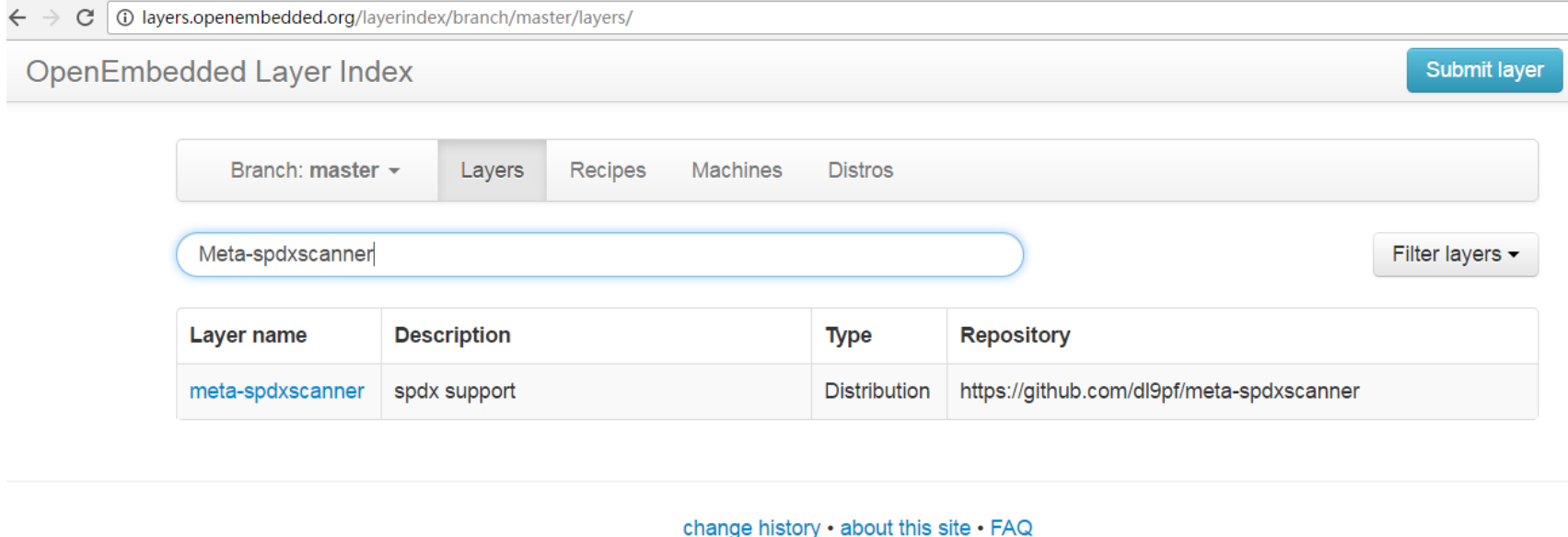
Item		FOSSology3	DoSOCSv2
Last Release		3.1	0.16.1
License		GPLv2	GPLv2
Support SPDX version		<b>2.1</b>	<b>2.0</b>
Scanners		Nomos, Monk, Ninka	Nomos
Supported Platform	Linux	√	√
	Others (Windows/OS X)		
Interface adapt to Yocto		√ (Partial support)	√
Graphical user interface		√	
Project Activity ( <a href="http://www.openhub.net">http://www.openhub.net</a> )		Moderate	Moderate
Scan time		Long	<b>Middle</b>
Scan unpacked sources			√
Build environment complexity		complex	<b>Easy</b>

DoSOCSv2 goes best with Yocto

# A new layer -- meta-spdxscanner (1/3)

## meta-spdxscanner

- Git Repository: <https://github.com/dl9pf/meta-spdxscanner>
- Our contribution to make Yocto+SPDX support SPDX2.0
- Project Activity: Maintained by our team.

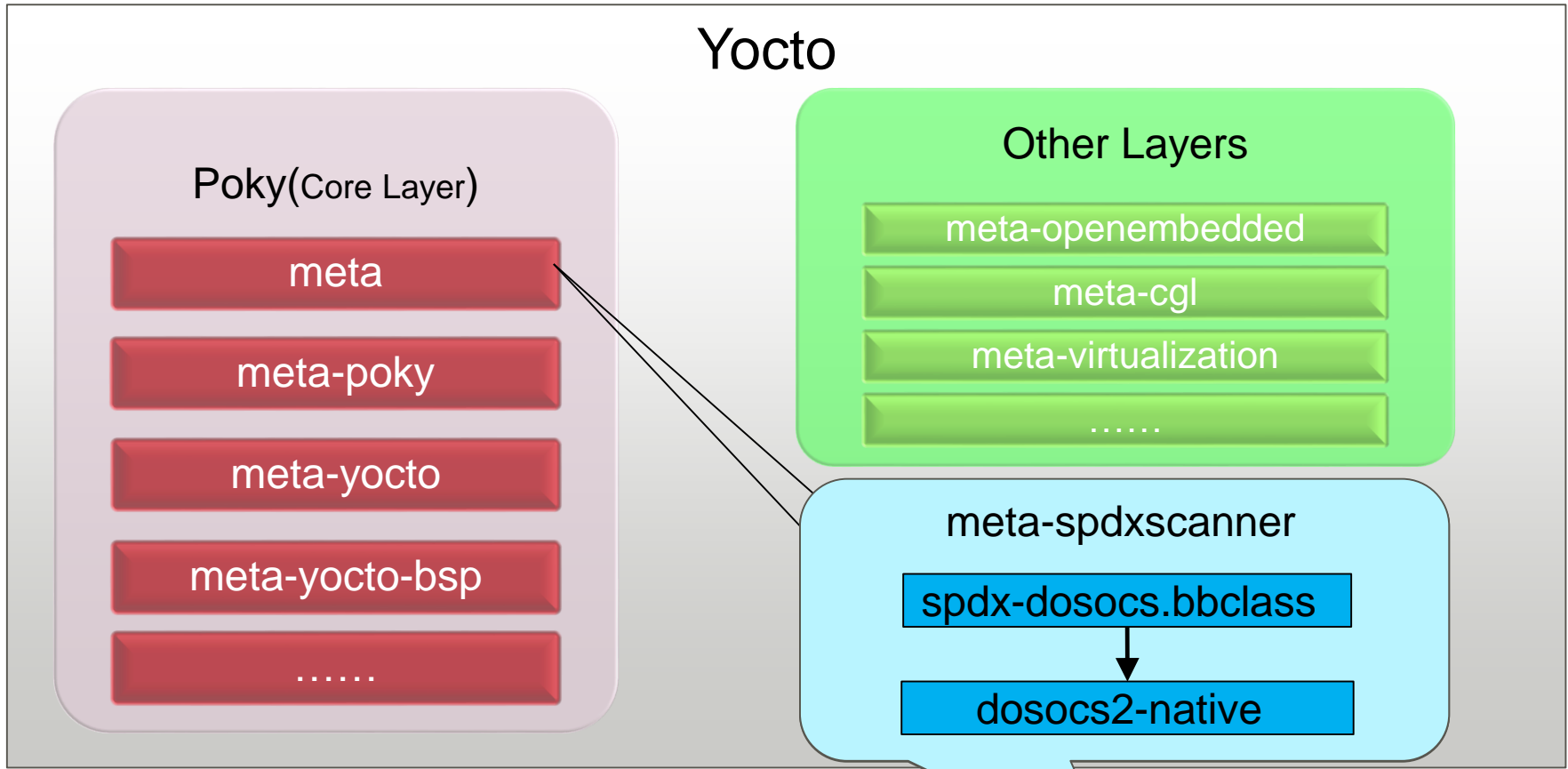


The screenshot shows the OpenEmbedded Layer Index website. The browser address bar displays the URL `layers.openembedded.org/layerindex/branch/master/layers/`. The page title is "OpenEmbedded Layer Index" with a "Submit layer" button on the right. Below the title, there are navigation tabs for "Branch: master", "Layers", "Recipes", "Machines", and "Distros". A search bar contains the text "Meta-spdxscanner" and a "Filter layers" button. Below the search bar is a table with the following data:

Layer name	Description	Type	Repository
<a href="#">meta-spdxscanner</a>	spdx support	Distribution	<a href="https://github.com/dl9pf/meta-spdxscanner">https://github.com/dl9pf/meta-spdxscanner</a>

At the bottom of the page, there are links for "change history", "about this site", and "FAQ".

# A new layer -- meta-spxscanner (2/3)



## Bitbake taskflow



## State of meta-spxscanner

- Already support Yocto 2.1

## How to use meta-spxscanner

```
[zhengrq@localhost build-spx]$ bitbake zlib
Parsing recipes: 100%
#####| .
.....
TARGET_SYS      = "i586-poky-linux"
MACHINE         = "qemux86"
DISTRO          = "poky"
DISTRO_VERSION  = "2.1.2"
TUNE_FEATURES   = "m32 i586"
.....
[zhengrq@localhost build-spx]$ ls
bitbake.lock cache conf spdx sstate-cache tmp
[zhengrq@localhost build-spx]$ ls spdx/
zlib-1.2.8.spdx
```



# Advantage of meta-spdxscanner(1/3)

## Deployment process

spdx.bbclass

Step1. Deploy Fossology-SPDX Server

Deploy Postgresql

Deploy Httpd

Install Fossology

Step2. Deploy Yocto

Git clone

Change local.conf

Inherit spdx

meta-spdxscanner

Step1. Deploy Yocto

Git clone

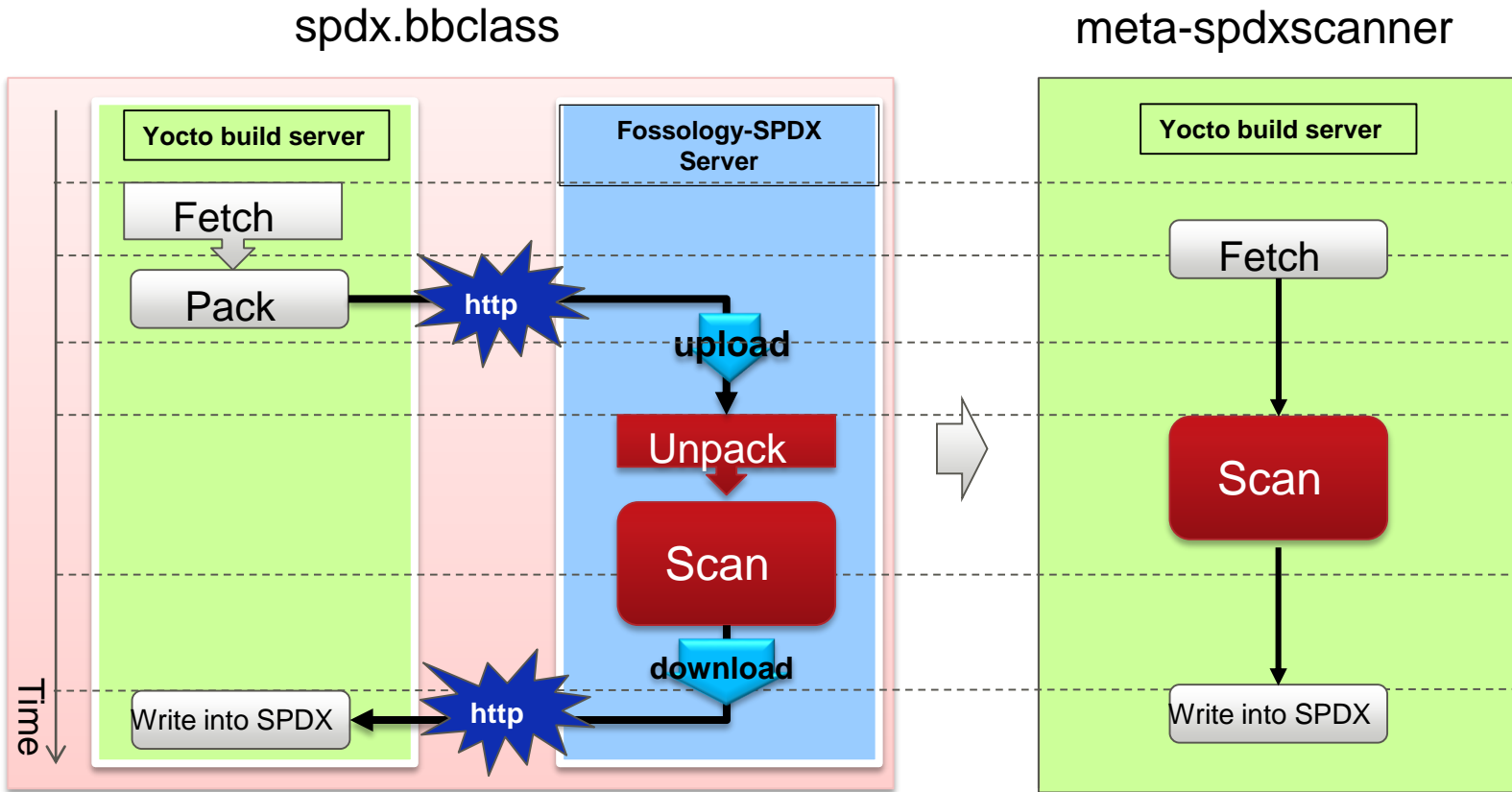
Change local.conf

Inherit spdx-dosocs

Deployment is easier

# Advantage of meta-spdxscanner(2/3)

## Process of scanning

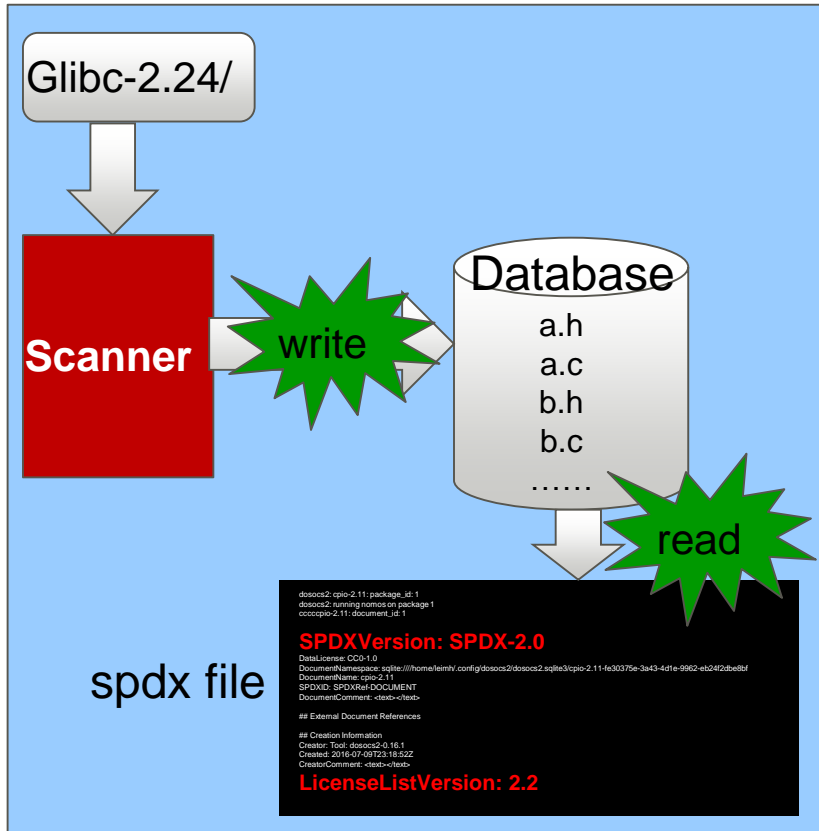


**Scanning process is shorter**

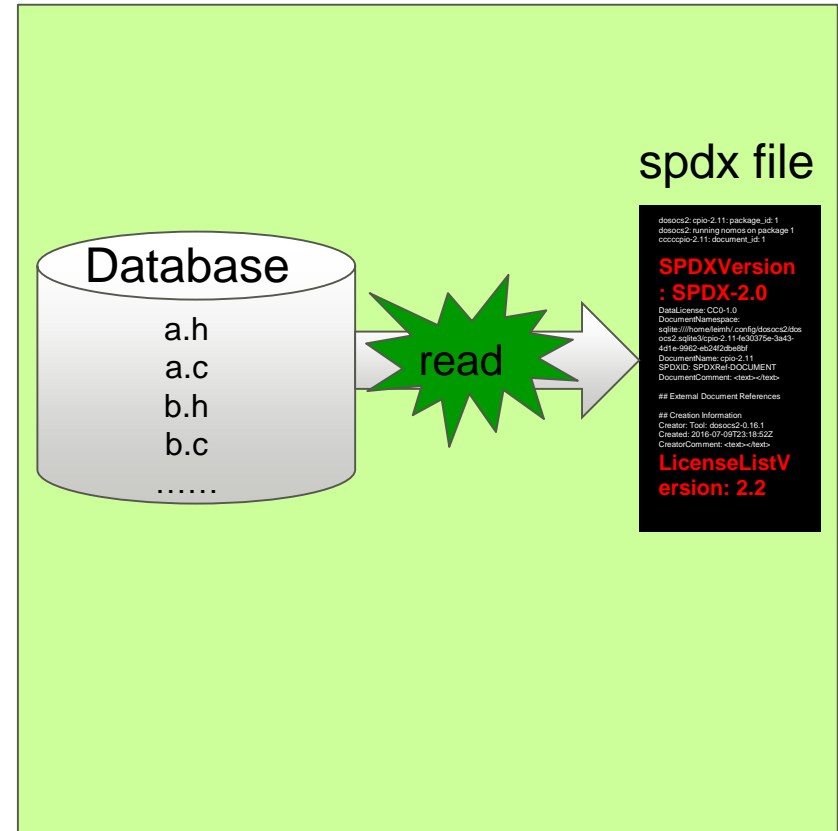
# Advantage of meta-spdxscanner(3/3)

## Process of creating spdx file after first time

First time



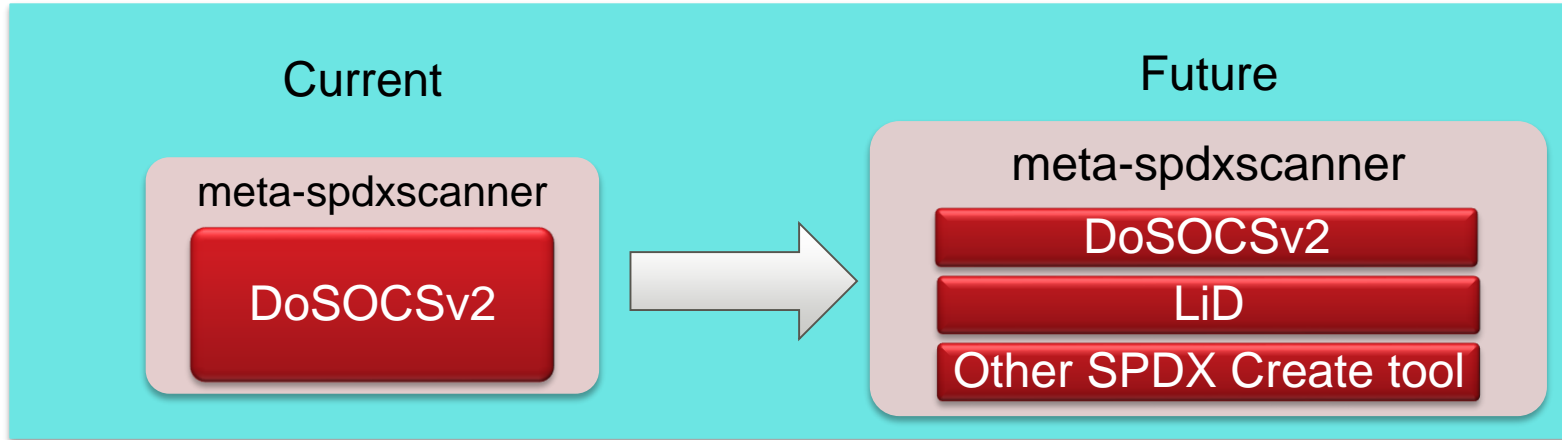
After first time



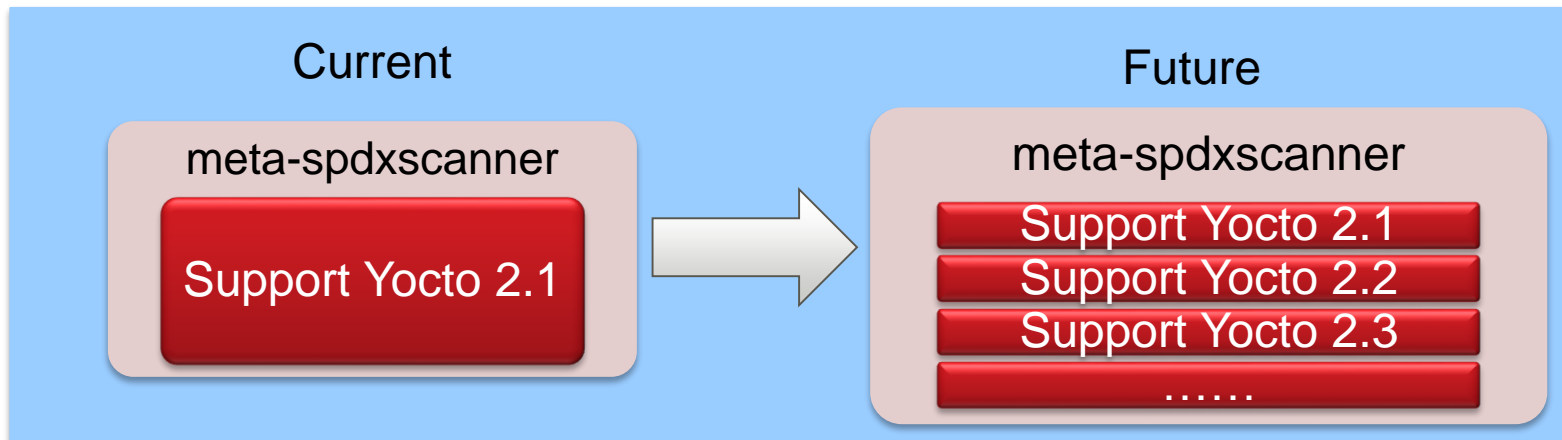
Performance is better

## meta-spdxscanner

- Only support one SPDX create tool, more tools will be included in future



- Only support Yocto 2.1, will match the latest Yocto version



# Manage SPDX files by smart

- What is smart
- What we have done
- How to Manage SPDX files by smart
- The next step

- The Smart Package Manager project has the ambitious objective of creating smart and portable algorithms for solving adequately the problem of managing software upgrades and installation. This tool works in all major distributions and will bring notable advantages over native tools currently in use (APT, APT-RPM, YUM, URPMI, etc).
- Yocto use smart to deploy packages
- Home page: <http://labix.org/smart>



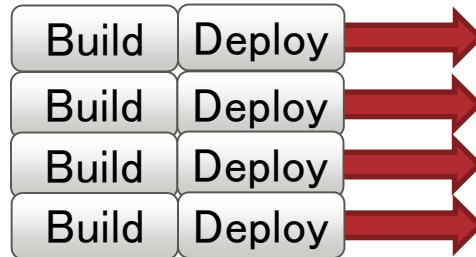
- Original Smart started on May 2004, and version 1.0 was released on Aug 2008. After released 1.5 on Sep 2014, the community became inactive.
- From 2015, our team start to develop smart2
- Git Repository: <https://github.com/ubinux/smart2>
- There are many new features in smart2, including support of SRPM and SPDX files

# What we have done (2/3)

LINUX FOUNDATION COLLABORATIVE PROJECTS



Before using Smart2

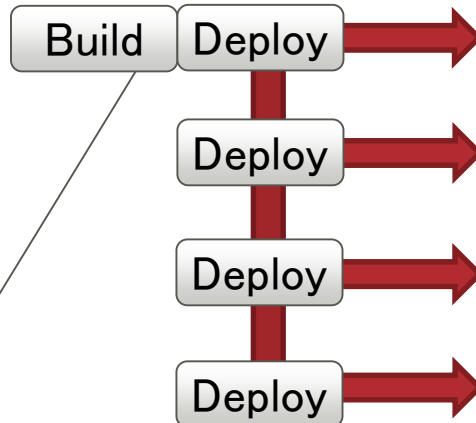


Build and Deploy for Each Targets

LINUX FOUNDATION COLLABORATIVE PROJECTS



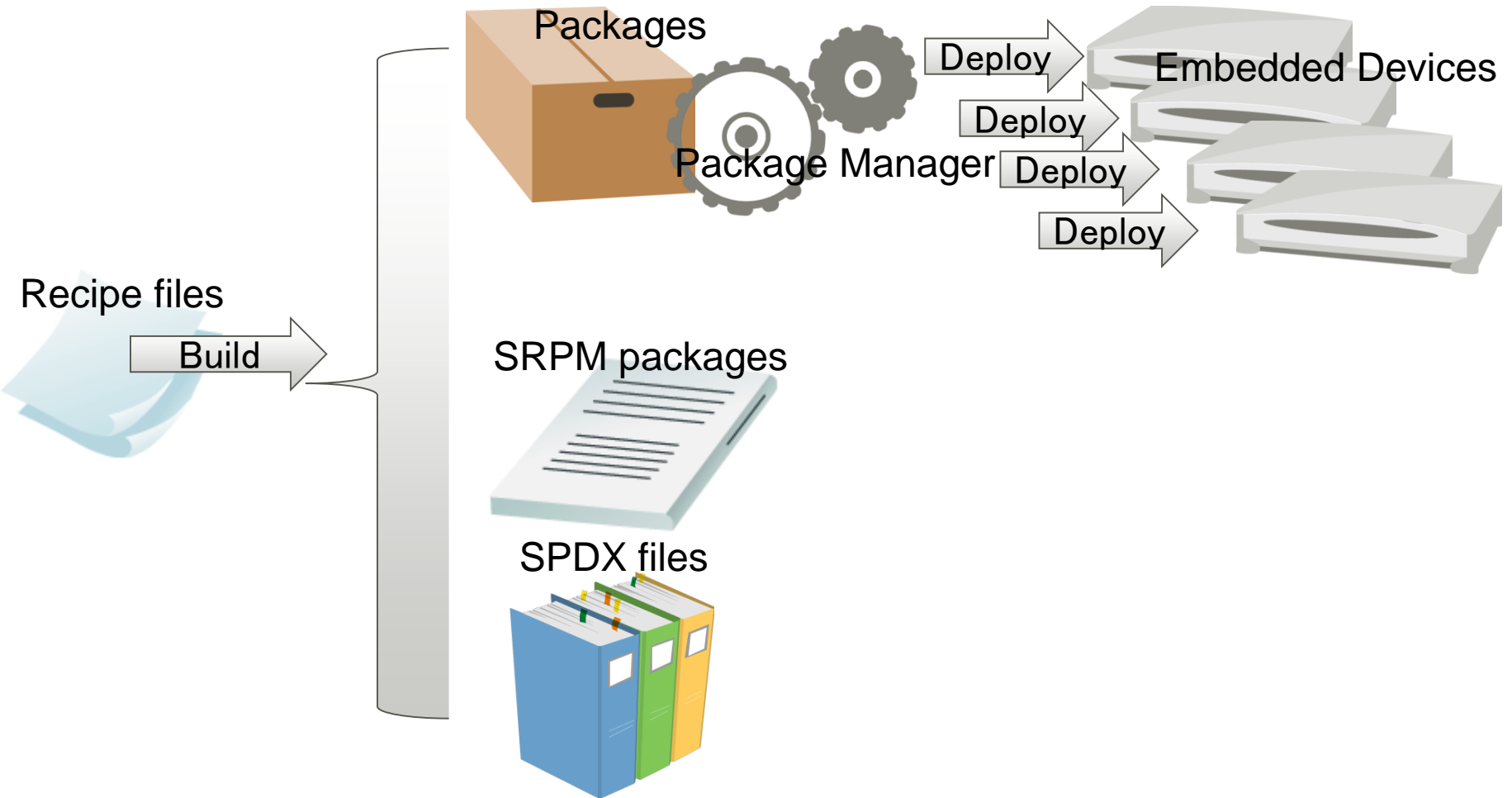
After using Smart2



Build Once, Deploy Anywhere



# What we have done (3/3)



- Accompanied with the package files and SRPM packages, SPDX files are created to manage license information.

## Manage spdx files by smart

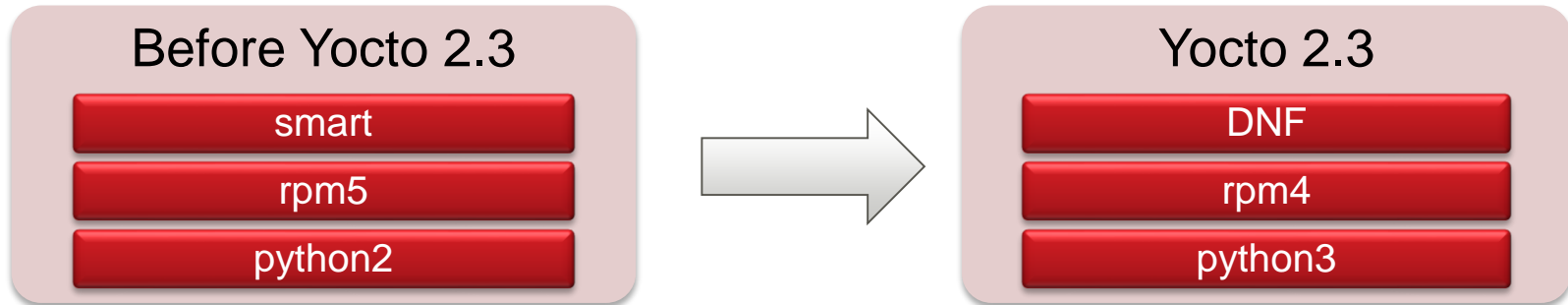
```
leimh@force:~$ ls ./spdx/  
acl-2.2.52.spdx  
acpid-2.0.23.spdx  
adwaita-icon-theme-3.16.2.1.spdx  
alsa-lib-1.0.29.spdx  
alsa-plugins-1.0.29.spdx  
alsa-state-0.2.0.spdx  
alsa-utils-1.0.29.spdx  
anthy-9100h.spdx  
at-3.1.16.spdx  
atk-2.16.0.spdx  
at-spi2-atk-2.16.0.spdx  
at-spi2-core-2.16.0.spdx  
attr-2.4.47.spdx  
audit-2.4.3.spdx  
augeas-1.4.0.spdx  
avahi-0.6.31.spdx
```

## What is DNF

- Dandified Yum (DNF) is the next upcoming major version of Yum.

## Why we use DNF

- Because rpm5 will be replaced by rpm4 from Yocto 2.3 due to the version change of python, Upstream (Yocto) pretends to use DNF from Yocto 2.3 as DNF is more suitable for rpm4.




## Our plan to improve DNF

- Make DNF support SPDX



<https://github.com/rpm-software-management/dnf>

**Any Questions?**



**FUJITSU**

shaping tomorrow with you