SFSCON 2024

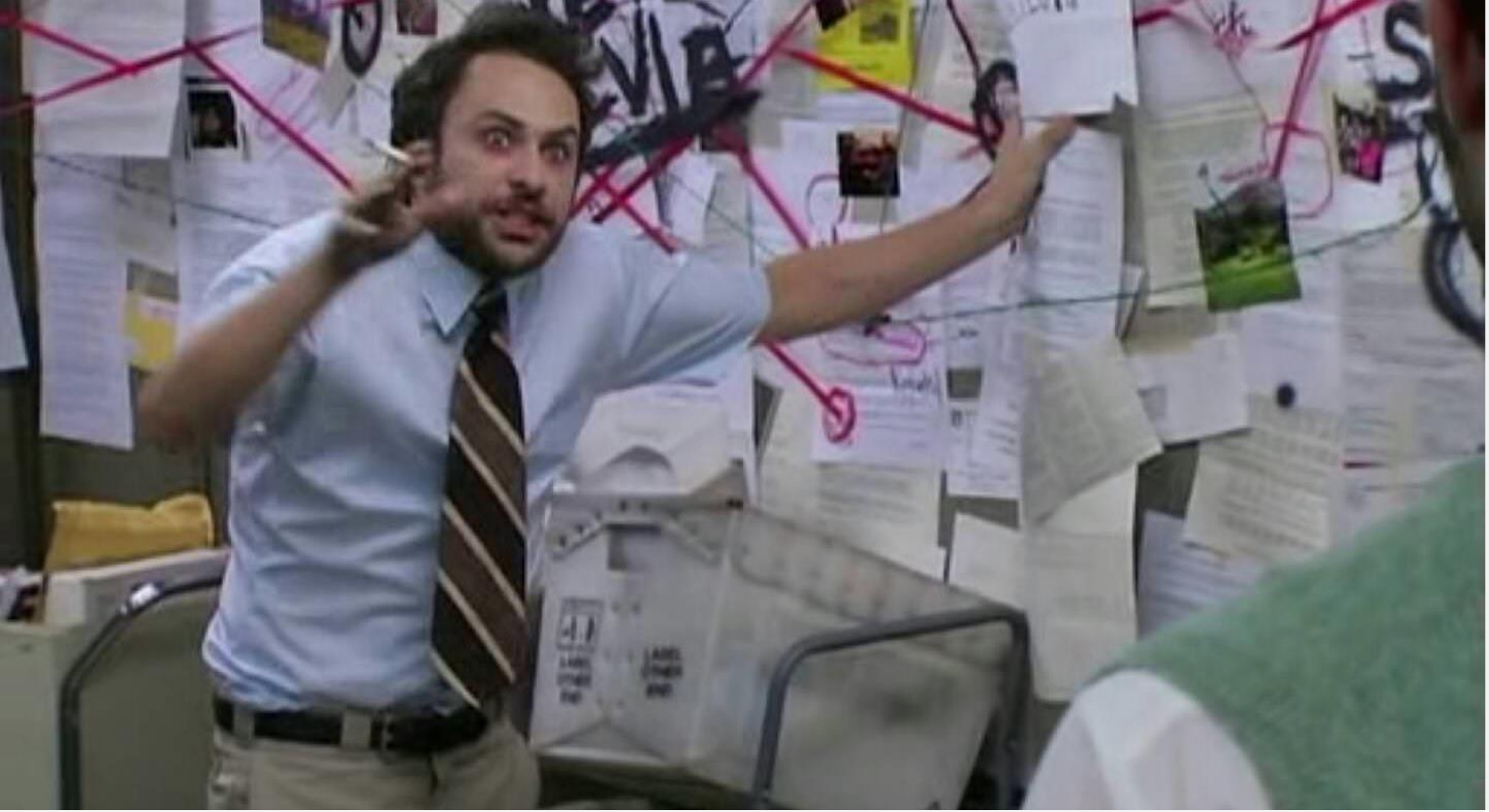
SPDXv3: Advancing Transparency and Security in Software

Alexios Zavras

Alexios Zavras – about me

- Greek, living in Munich
- Intel's Chief Open Source Compliance Officer, working at the Open Source Program Office
- "Open Source" since 1983

- SBOM/SPDX since 2011



SBOM

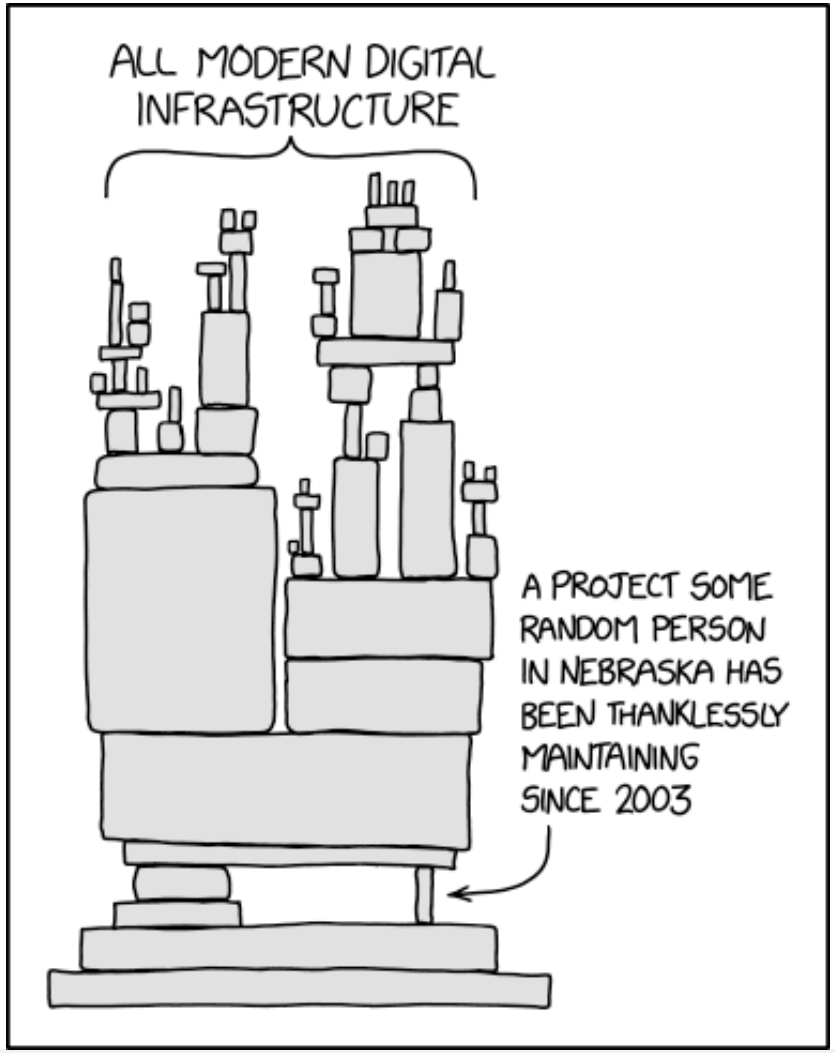
Software Bill Of Materials

Software Bill of Materials (SBOM)

An SBOM is a formal record containing details and supply chain relationships of components used in building software.

- Components include libraries and modules
- Components can be open source or proprietary
- Components can be freely available or paid
- Data can be widely available or access-restricted

Most do not know what software is running



Dependency, by xkcd, CC-BY-NC-2.5

Regulation

- Regulation is ~~coming~~ here!

- US
  - EO 14028 on Improving the Nation's Cybersecurity; May 2021
  - National Cybersecurity Strategy Implementation Plan; July 2023
- EU
  - Cyber Resilience Act (CRA); December 2023
- Germany
- Japan
- …

SPDX

Background and history

SPDX Data

Collecting all information about a ~~software~~ system delivery

- Descriptive
  - Detailed Bill of Materials (aka manifest) of the contents
- Flexible
  - Various formats for automatic processing
- Accurate
  - Focus on capturing facts; allow interpretations

Widespread industry support for SPDX

All logos used with *written permission*

SPDX Governance

- Open
  - open to contributions from anyone interested
  - all team and working group meetings are open
  - team leads nominated by any participant
  - steering committee composed of team leads
- Transparent
  - work is online in the SPDX GitHub organization, including meeting minutes
- Inclusive
  - participants and leads are individuals from diverse backgrounds and industries
  - over 40 organizations contribute directly to the SPDX spec representing most industry segments and geographies

Historical milestones

Executive Order 14028

EU Cyber Resilience Act

2010 SPDX begins

Standardized Single Package Information: Machine and human readable formats

2011 SPDX 1.0

Compliance Use Cases: Additional Project and License Information

2013 SPDX 1.2

Package Relations: 30+ additional use cases supported for complex packaging relationships and distribution scenarios

2015 SPDX 2.0

Security use cases: External references for vulnerabilities and product identification

2020 SPDX 2.2

2021

Free ISO Standard: ISO/IEC 5962 SPDX available

2022 SPDX 2.3

Format Interoperability

CDx SPDX

2023 SPDX 3rc1

Profiles: New areas of use cases:
- Build
- Data
- Security
- AI
- Lite

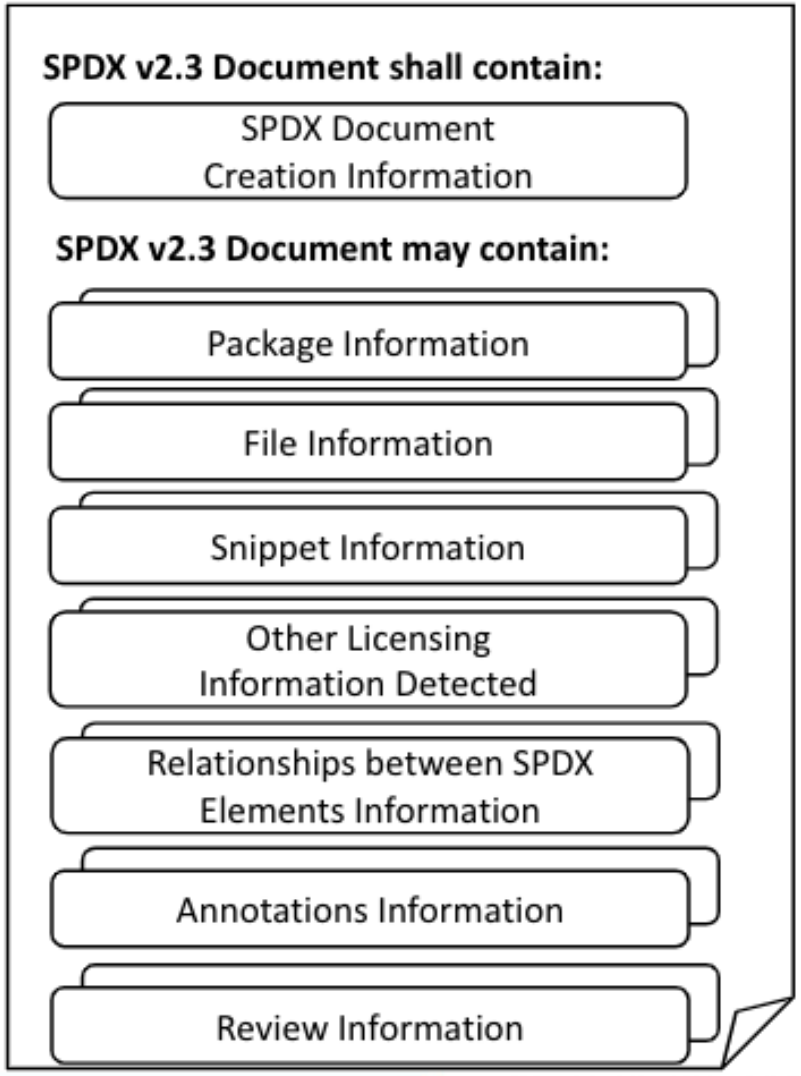
2024+ SPDX 3.x

Profiles: New areas of use cases:
- Services
- Hardware
- Safety
- Operations

SPDXv3

~~Software~~ System Package Data Exchange

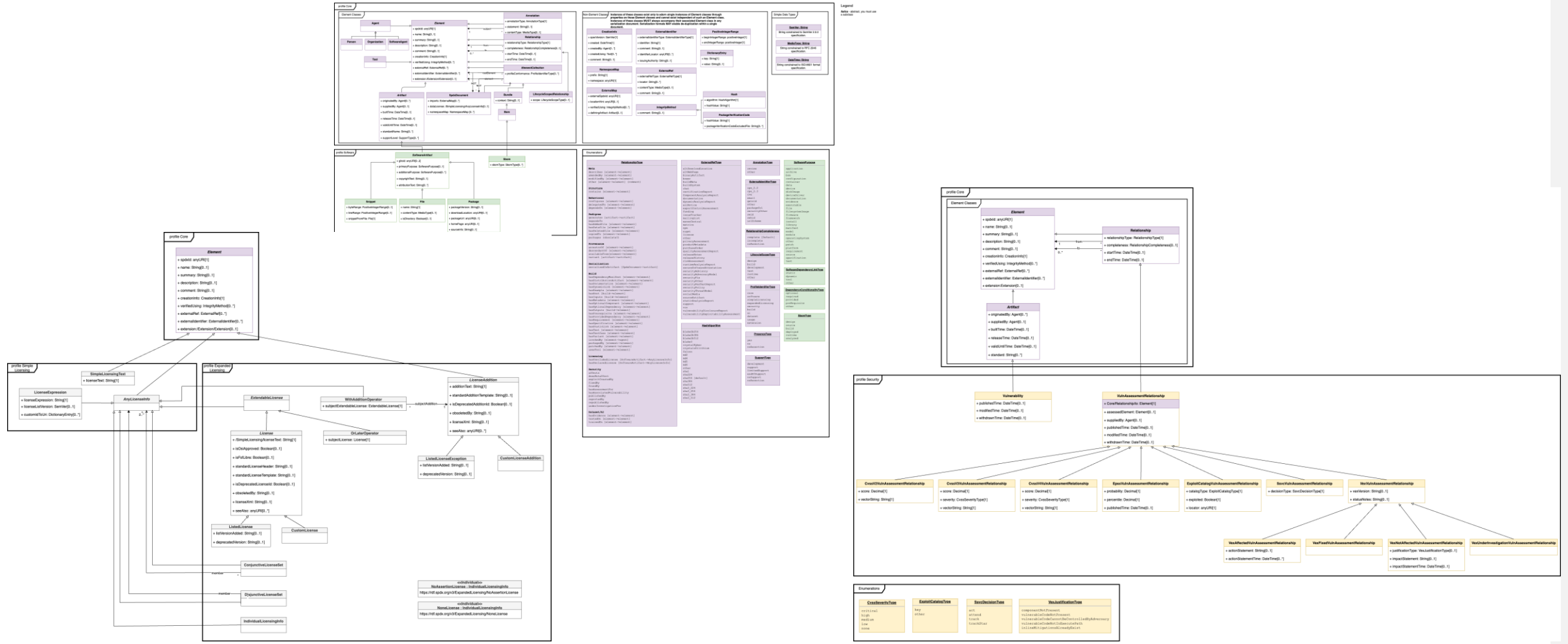
Structure of an SPDXv2 Document



Released: SPDX 3.0

- Major undertaking
- Abstracted information to be more widely useful
- Refactored to CORE and PROFILEs
  - CORE is minimum needed to describe artifacts and relationships
  - PROFILEs for each Area of Interest:
    Licensing, Vulnerabilities, Provenance, …
- Not only for Exchange, but also for storage/processing
- (Finally) Released!
  - On its way to ISO

SPDXv3 is graph-based data



SPDXv3 Profiles

- Core, Software
- Licensing
- Security
- Build
- AI / Dataset

- In progress: Safety, Operations, SaaS, Hardware, ...

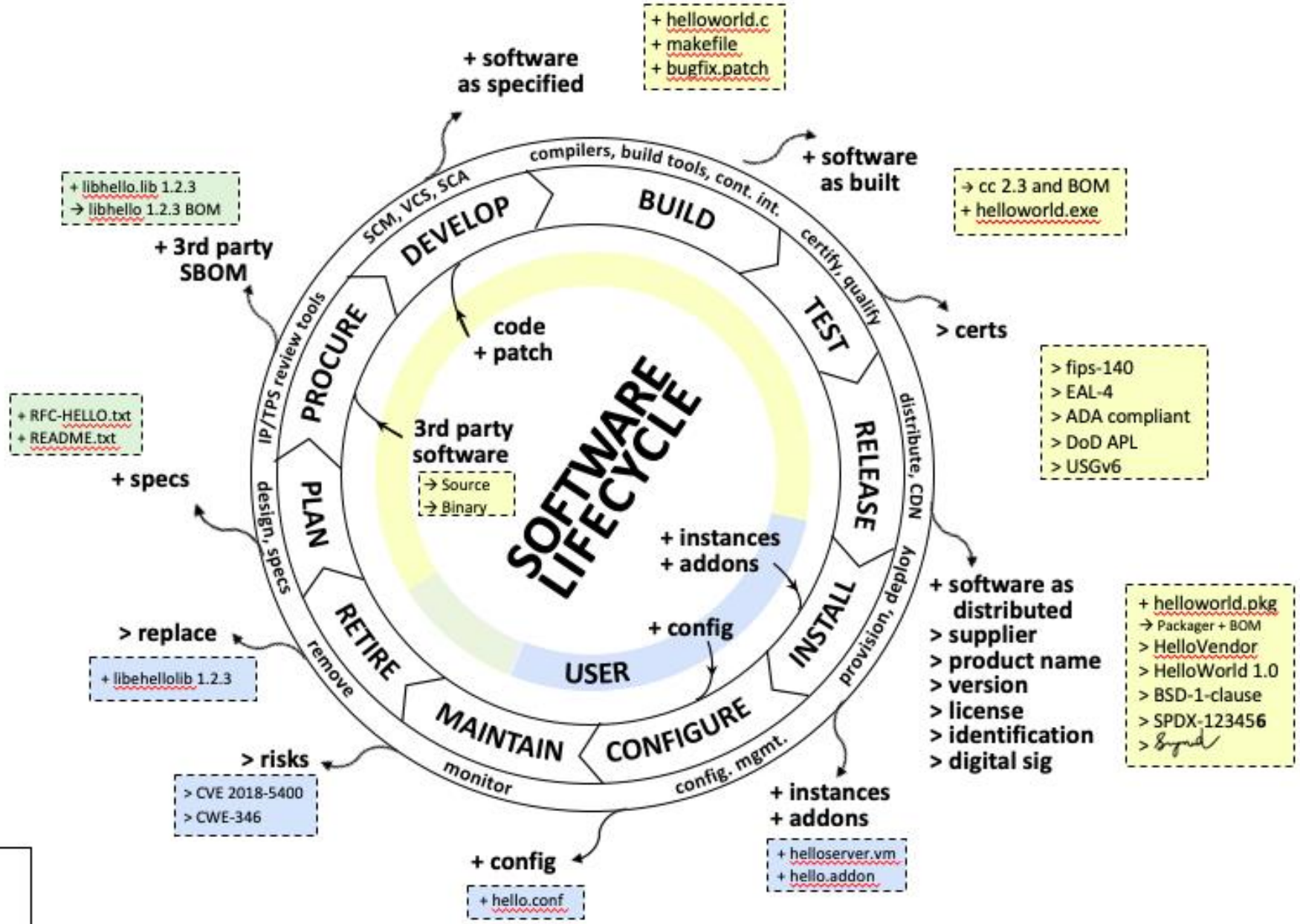
SPDX 3.0 published profiles

SPDX SECURITY	Security information – vulnerability details related to software
SPDX BUILD	Build related information – provenance, reproducible builds
SPDX AI	Information about AI models – model data, security, ethical
SPDX DATA	Information about datasets – used by other components
SPDX LITE	Minimal subset to support industry supply chain workflows
SPDX LICENSING	Information about copyrights and licenses – supports legal compliance
SPDX SOFTWARE	Information specific to software
SPDX CORE	Information used across all profiles

However...

We are not done

Software Lifecycle & Bill of Materials Generation



Types of SBOMs

Design	SBOM of intended, planned software project or product with included components (some of which may not yet exist) for a new software artifact.
Source	SBOM created directly from the development environment, source files, and included dependencies used to build a product artifact.
Build	SBOM generated as part of the process of building the software to create a releasable artifact (e.g., executable or package) from data such as source files, dependencies, built components, build process ephemeral data, and other SBOMs.
Analyzed	SBOM generated through analysis of artifacts (e.g., executables, packages, containers, and virtual machine images) after its build. Such analysis generally requires a variety of heuristics. In some contexts, this may also be referred to as a "third-party" SBOM.
Deployed	SBOM provides an inventory of software that is present on a system. This may be an assembly of other SBOMs that combines analysis of configuration options, and examination of execution behavior in a (potentially simulated) deployment environment.
Runtime	SBOM generated through instrumenting the system running the software, to capture only components present in the system, as well as external call-outs or dynamically loaded components. In some contexts, this may also be referred to as an "Instrumented" or "Dynamic" SBOM.

SPDX: Open for participation!

To everyone

Participate!

Teams

- Technical
- Legal
- Outreach

- Mailing lists
- Meetings
- GitHub

Groups

- AI
- Build
- Data
- Defects
- Functional Safety
- Hardware
- …

All information on https://spdx.dev and https://github.com/spdx


intel

Tools

More work needed!

Tool functional classification taxonomy

Category	Type	Description
Produce	Build	SBOM is automatically created as part of building a software artifact and contains information about the build
	Analyze	Analysis of source or binary files will generate the SBOM by inspection of the artifacts and any associated sources
	Edit	A tool to assist a person manually entering or editing SBOM data
Consume	View	Be able to understand the contents in human readable form (e.g., picture, figures, tables, text, etc.). Use to support decision making & business processes
	Diff	Be able to compare multiple SBOMs and clearly see the differences (e.g., comparing two versions of a piece of software)
	Import	Be able to discover, retrieve, and import an SBOM into your system for further processing and analysis
Transform	Translate	Change from one file type to another file type while preserving the same information
	Merge	Multiple sources of SBOM and other data can be combined together for analysis and audit purposes
	Tool support	Support use in other tools by APIs, object models, libraries, transport, or other reference sources

Tools classifications

- Licensed under:
  - Open Source
  - Proprietary
- SBOM Type
- List keeps expanding…
- Level:
  - Libraries
  - Purpose-specific
  - Complete applications
  - Integrated environments
- Ecosystem