

AI (FMware) BOM - Towards enabling transparency, traceability and compliance

Gopi Krishnan Rajbahadur

SPDX Ambassador, Maintainer and AI and Dataset Profile Co-lead



How to cite this session?

```
@misc{Rajbahadur2024AIwareTutorial,  
author = {Gopi Krishnan Rajbahadur and Kate Stewart},  
title = {AI (FMware) BOM - Towards enabling transparency, traceability and compliance},  
howpublished = {Tutorial presented at the AIware Leadership Bootcamp 2024},  
month = {November},  
year = {2024},  
address = {Toronto, Canada},  
note = {Part of the AIware Leadership Bootcamp series.},  
url =  
{https://aiwarebootcamp.io/slides/2024_aiwarebootcamp_rajbahadur_aifmwarebomtowardsenablingtransparencytraceabilityandcompliance.pdf  
}}
```



Check this paper for more information about this session

```
@article{rajbahadur2024AIBOM,  
  title={Implementing AI Bill of Materials (AI BOM) with SPDX 3.0},  
  author={Karen Bennet and Gopi Krishnan Rajbahadur and Arthit Suriyawongkul and Kate Stewart},  
  journal={https://www.linuxfoundation.org/hubfs/LF%20Research/lfr_spdx_aibom_102524a.pdf},  
  year={2024}  
}
```



International Standards are Essential



“Think of them as a formula that describes **the best way of doing something.**”



“Standards are voluntary guidelines **that provide technical specifications** for certain goods, services and processes.”



“Standards form the fundamental building blocks for product development by **establishing consistent protocols that can be universally understood and adopted.**”



“Technical standards keep us **safe, enable technology to advance, and help businesses succeed.** They quietly make the modern world tick and prevent technological problems that you might not realize could even happen.”

Standards enable



Reliability



Interoperability



Trustworthiness



Safety

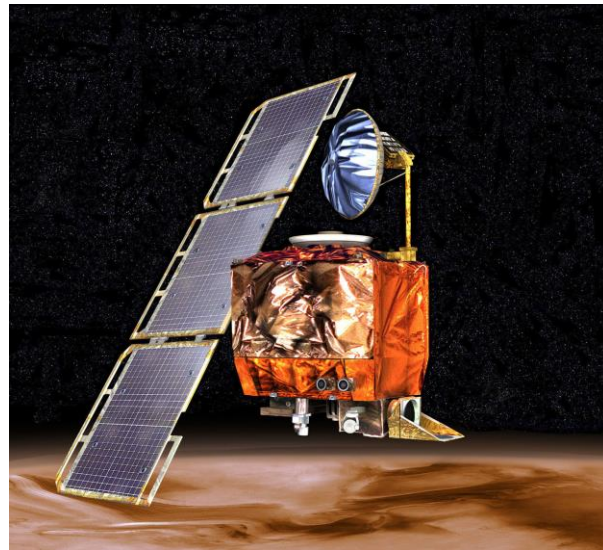


To create standards or not standard

– An example of Mars Climate Orbiter

Mars Climate Orbiter

Mission cost: 551.45 Million



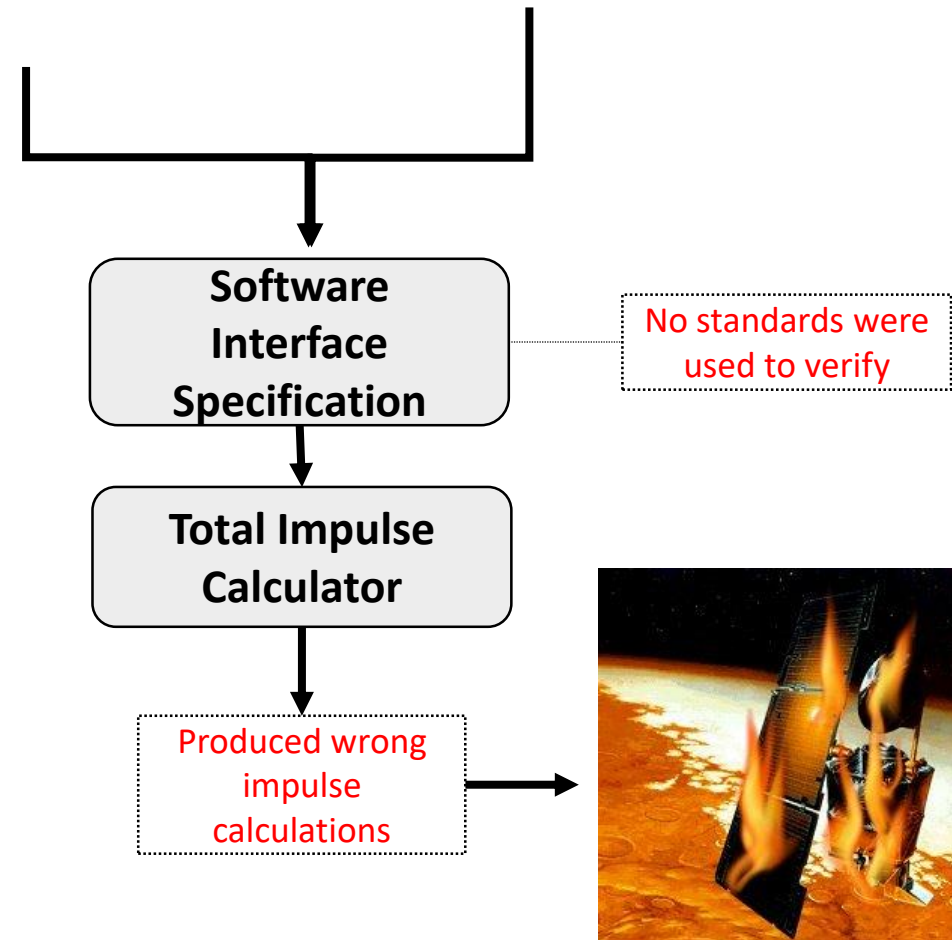
Mars orbiter exploded due to a lack of standardization in the software interface specification highlighting the need for standards



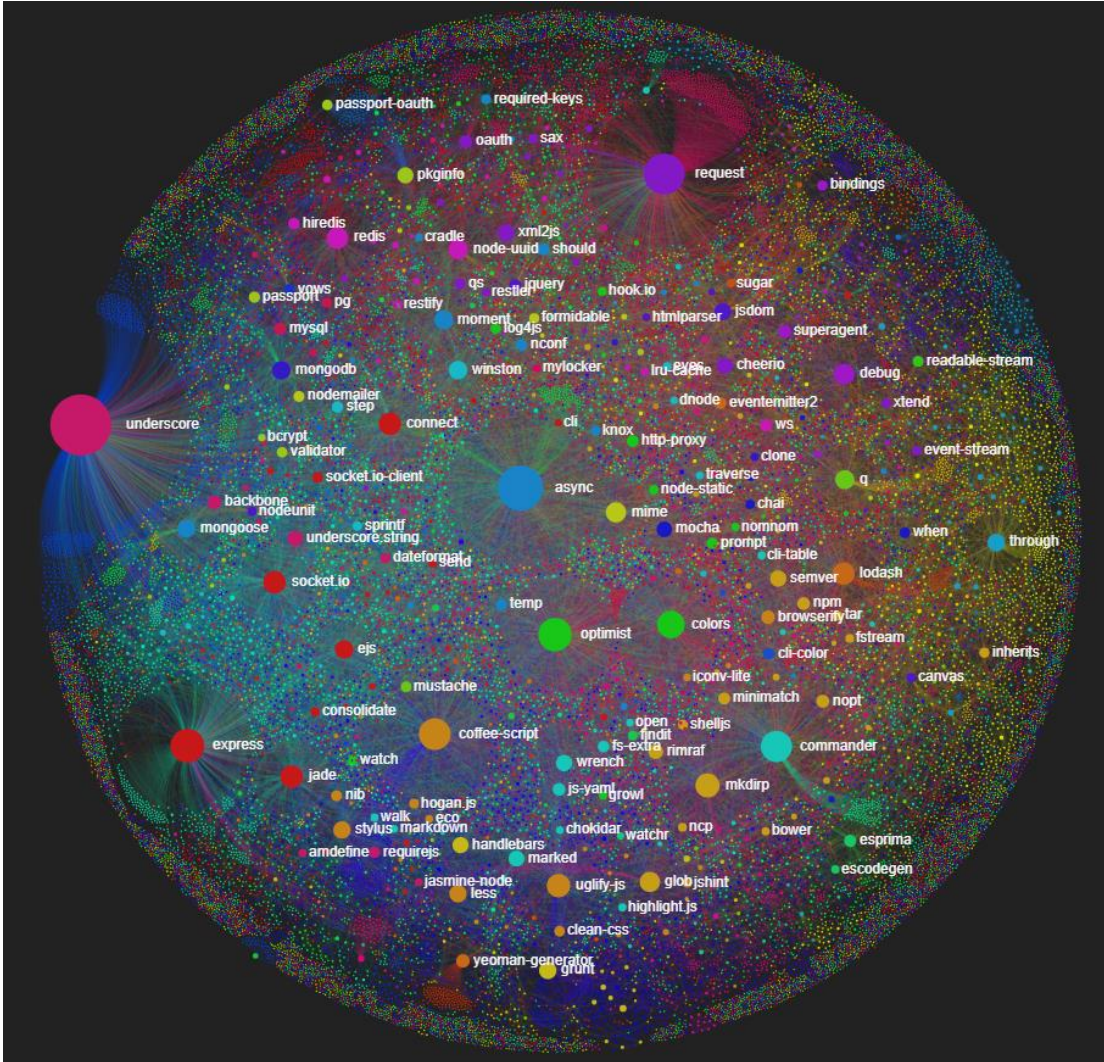
SI Units



US units



Assembly based software development brings many benefits but also many risks!



Today's software is built through the assembly of many components which in turn are built from many other components (aka the software supply chain)

Modern software has many risks that are not related to its self-developed source code due to:

- Problems (e.g., vulnerabilities) in any components would direct or indirectly impact the final software
- Problems in the assembly/packaging/delivery process poses risks as well

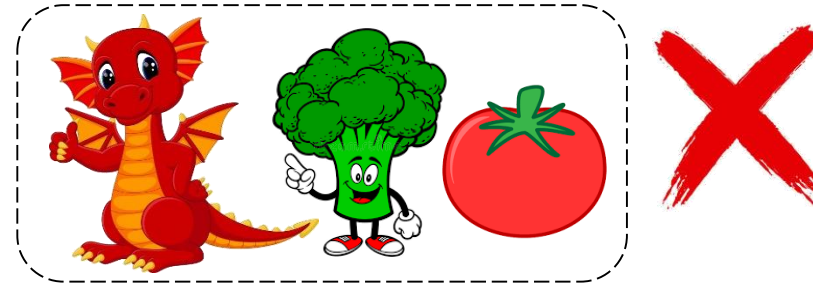
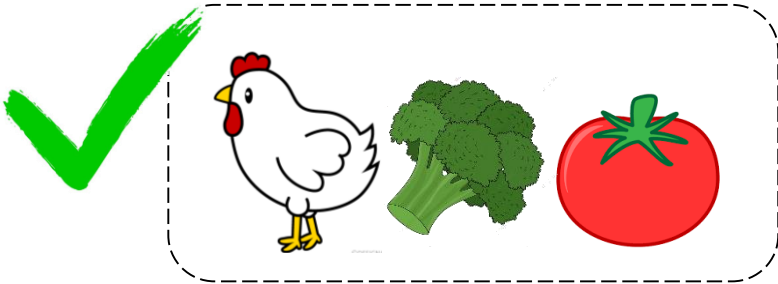


What is Bill of Materials and Why do you need it?

Would you consume this soup?



First logical question, what is in it?



Great news! SBOM (Software Bill of Materials) is now a required part of delivered Software and AIBOM extension can be used to represent even the Alware ingredients



What is AI Bill of Materials (AI BOM)?

AI Nutrition Facts	
Your Product Name	
Description	Describe your product
Privacy Ladder Level ⓘ	1 ▼
Feature is Optional	Yes ▼
Model Type	Generative
Base Model	OpenAI - GPT-4
Trust Ingredients	
Base Model Trained with Customer Data	No ▼
Customer Data is Shared with Model Vendor	No ▼
Training Data Anonymized	N/A ▼
Data Deletion	Yes ▼
Human in the Loop	Yes ▼
Data Retention	30 days
Compliance	
Logging & Auditing	N/A ▼
Guardrails ⓘ	N/A ▼
Input/Output Consistency ⓘ	Yes ▼
Other Resources	
Add any additional resources...	

AI BOM is a detailed recipe for an AI software. It lists all the ingredients (like data, algorithms, and libraries) that go into making an AI system.

Just like a recipe helps you check if you're allergic to any ingredients in a dish, an AI BOM helps companies make sure **their AI software follows safety, transparency and regulatory guidelines.**

AI BOM enables



License
Compliance



Regulatory
Compliance



Vulnerability
Analysis



NTIA Software Bill Of Materials (SBOM) Guidance - Minimum Elements

Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.

SPDX 2.2 +

([ISO/IEC 5962:2021](https://www.iso.org/standard/72431.html))

supports all required minimum elements

(as well the optional that are mentioned in report)

and many more use cases


Checker available at:

<https://github.com/spdx/ntia-conformance-checker>



ISO/IEC 5962:2021

- Able to represent SBOMs from binary images and track back to the source files and snippets.
- Specification is [freely available from ISO site](#).
- Future updates are live tracked at: <https://spdx.github.io/spdx-spec> and work on satisfying safety requirements is being included
- More information at spdx.dev



The screenshot shows the ISO website page for ISO/IEC 5962:2021. The page features the ISO logo, a breadcrumb trail 'ICS > 35 > 35.080', and the title 'ISO/IEC 5962:2021 Information technology – SPDX® Specification V2.2.1'. A light blue box contains the text: 'The electronic version of this International Standard can be downloaded from the ISO/IEC Information Technology Task Force (ITTF) web site.' Below this, there are tabs for 'ABSTRACT' and 'PREVIEW'. The abstract text reads: 'This Software Package Data Exchange® (SPDX®) specification defines a standard data format for communicating the component and metadata information associated with software packages. An SPDX document can be associated with a set of software packages, files or snippets and contains information about the software in the SPDX format described in this specification.' At the bottom, there is a 'GENERAL INFORMATION' section with a status of 'Published' and a publication date of '2021-08'.

ISO

ICS > 35 > 35.080

ISO/IEC 5962:2021

Information technology – SPDX® Specification V2.2.1

The electronic version of this International Standard can be downloaded from the ISO/IEC Information Technology Task Force (ITTF) web site.

ABSTRACT **PREVIEW**

This Software Package Data Exchange® (SPDX®) specification defines a standard data format for communicating the component and metadata information associated with software packages. An SPDX document can be associated with a set of software packages, files or snippets and contains information about the software in the SPDX format described in this specification.

GENERAL INFORMATION

Status : © Published Publication date : 2021-08



SPDX 3.0 Profiles Overview



Information about AI models - ethical, security, and model data



Information about datasets - AI and other data use cases



Security information - vulnerability details related to software



Build related information - provenance and reproducible builds



Minimal subset to support industry supply chain workflows



Information about copyrights and licenses - supports compliance



Information specific to software



Information used across all profiles



SPDX AI Profile



A profile that adds on top of the core-software profile to describe the AI specific elements that will enable transparency and traceability of both components and process that enables the creation of an AI software. It is important to note that, special consideration is given to capture process (in addition to just capturing the components) as process introduces a lot of risks and uncertainties that make up the non-deterministic system that AI is.



SPDX Dataset Profile



A profile that adds on top of the core-software profile to describe the dataset that is used to train or test an AI software. These datasets could also be used for other purposes. Similar, to AI profile, we take special care to ensure that process of forming a dataset is captured. In addition, we also make it a point to capture the provenance and the lineage associated with the dataset. We introduce new fields to do so as provenance and lineage of a dataset has more facets to it compared to traditional software.



What does this mean when we try to document an example AI BOM with the AI & Dataset profiles?

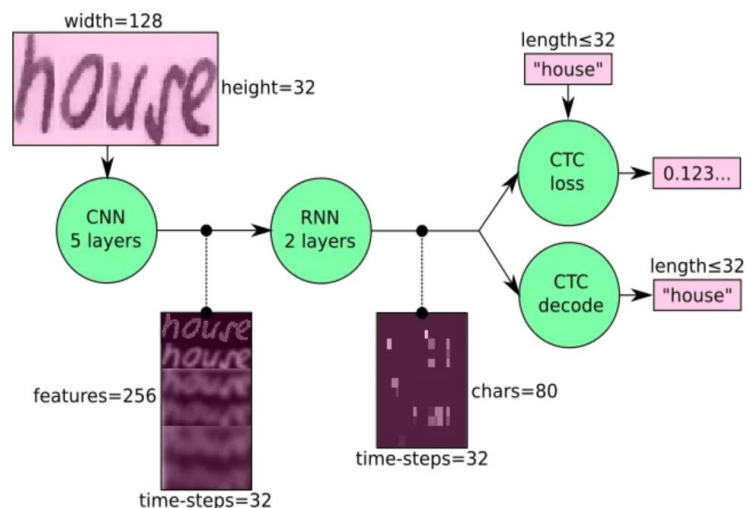


An example AI BOM for SimpleHTR system

The simpleHTR is an Machine Learning project that uses a Deep Neural network to recognize handwritten words

house → "house"

SimpleHTR Architecture



Selection criteria

- Over 1000 stars on GitHub
- Simple machine learning application

Methodology

- Analyzed AI BOM
- Traced upto first-level of dependency



Pain point 1:

Lack of tools to enable creation of AI BOM

- Details are scattered across different sources and even documentation standards like model cards, data cards and factsheets do not capture all the required detail
- Requires costly expertise to gather all the required details for a complete AI BOM including source code analysis, reading academic papers and resolving conflicts.
- For example, the creation of SimpleHTR's analyzed AI BOM took about a 40hrs of time

For real-world AI application, manual AI BOM creation methods cannot be adopted.



Pain point 2:

Required Metadata is Not Readily Available

IAM - line level

Dataset Summary

The IAM Handwriting Database contains forms of handwritten English text which can be used to train and test handwritten text recognizers and to perform writer identification and verification experiments.

Note that all images are resized to a fixed height of 128 pixels.

Languages

All the documents in the dataset are written in English.

Dataset Structure

Data Instances

```
{
  'image': <PIL.JpegImagePlugin.JpegImageFile image mode=RGB size=2467x128 at 0x1A800E8E190,
  'text': 'put down a resolution on the subject'
}
```

Data Fields

- `image`: a `PIL.Image.Image` object containing the image. Note that when accessing the image column (using `dataset[0]["image"]`), the image file is automatically decoded. Decoding of a large number of image files might take a significant amount of time. Thus it is important to first query the sample index before the "image" column, i.e. `dataset[0]["image"]` should always be preferred over `dataset["image"][0]`.
- `text`: the label transcription of the image.

Details missing include

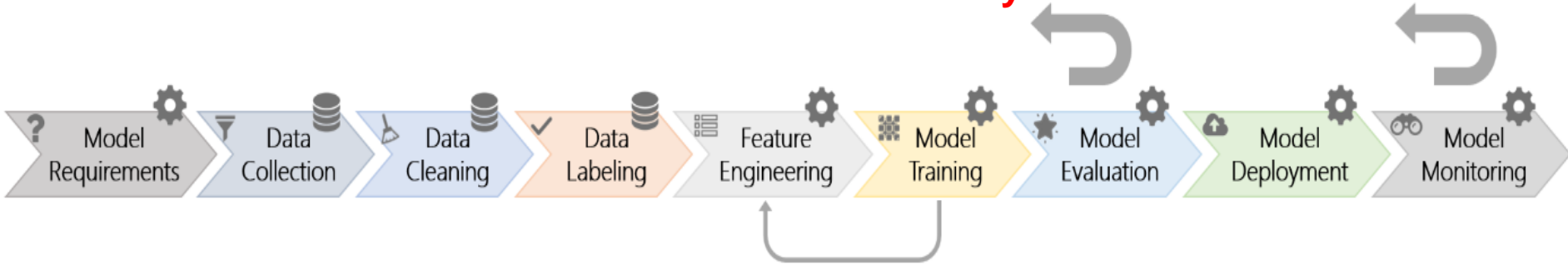
- `datasetSize`
- `Sensor`
- `confidentialityLevel`
- `dataCollectionProcess`
- `dataPreprocessing`
- `hyperparameters`

Requires reading the paper to extract these information which severely hinders adoption

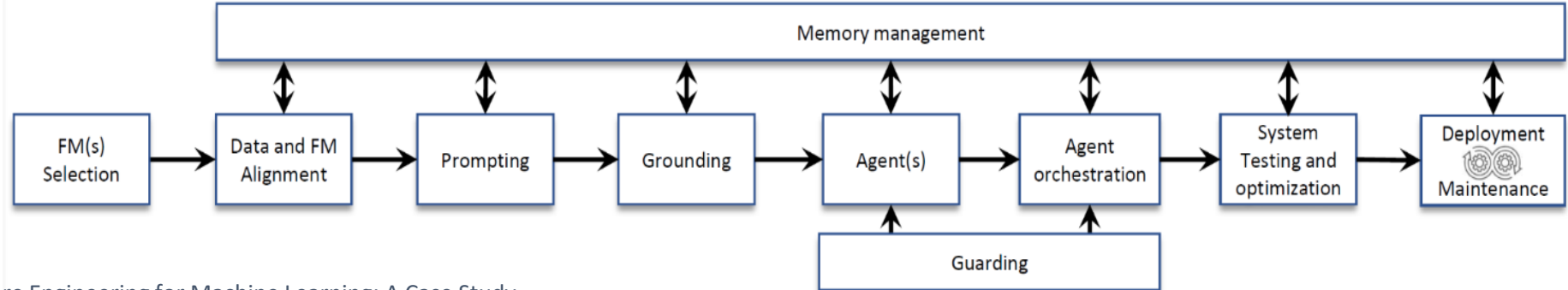


FMware (Foundation Model Powered Software) follows a different lifecycle compared to traditional AI Software

Traditional ML-software Lifecycle



FMware Lifecycle



Challenge 1: Difficulty in Automating AI BOM Generation Due to Disparate Information Sources

The information required to create an AI BOM is typically not found in a unified place like source code repository, it is spread across multiple sources like papers, source code and website

Current Mitigations

- Create a checklist for all possible sources of data
- Have the core-development team sign-off on the AI BOM

Call to Action for Researchers

- Create/enhance metadata standards like SPDX AI and Dataset profile to capture all relevant information
- Develop NLP-based automatic information extraction techniques

Call to Action for AI Engineers

- Meticulously create AI BOMs at the development time using all the fields as opposed to just using the required fields



Challenge 2: High-Level AI Regulations Complicate Translation to System Requirements and Detail Tracking

For example, The EU AI Act mandates "sufficient transparency" and "appropriate human oversight" for high-risk AI systems but lacks clear guidelines on how to achieve these. This vagueness forces developers to interpret broad terms, leading to compliance uncertainty

Current Mitigations

- Leverage legal aid to interpret regulations and verify implementations

Call to Action for Researchers

- Develop frameworks that map regulatory guidelines to system requirements.
- Engage with policymakers to advocate actionable regulatory guidance.

Call to Action for AI Engineers

- Integrate compliance tracking features directly into the AI software development pipeline
- Demonstrate due diligence



Challenge 3: Ambiguous Data Ownership (Synthetic & User Feedback Data) Complicates License Compliance

Data lineage issues complicate compliance when datasets are derived from sources with different licenses. There's also ambiguity around AI-generated synthetic data—it's unclear whether the original dataset's license or the AI model's license applies. Additionally, ownership of user feedback data remains uncertain: does the copyright belong to the user or the platform?

Current Mitigations

- Meticulously track data provenance and lineage
- Create a separate dataset profile for each data source

Call to Action for Researchers

- Develop automated data provenance and lineage identification tools
- Collaborate with regulators to clarify synthetic data copyright

Call to Action for AI Engineers

- Integrate provenance and lineage details in data hosting platforms
- Track and attribute all incoming and outgoing data



Challenge 4: Lack of Detailed Documentation on AI Software Development Hinders Compliance and Safety Assurance

Current AI BOM standards list components but lack fields to capture development details, akin to knowing soup ingredients without insight into the kitchen. The EU AI Act's emphasis on risk management transparency highlights this gap, making compliance and safety harder to ensure without process documentation.

Current Mitigations

- Maintain detailed logs of model training, testing, and deployment processes.
- Use version control systems

Call to Action for Researchers

- Design frameworks for comprehensive documentation of the AI software lifecycle.
- Enhance AI BOM standards to capture process details for compliance and safety

Call to Action for AI Engineers

- Integrate detailed process documentation as a mandatory part of the development cycle.
- Record development activities for compliance.



Challenge 5: Current AI BOM Specification Lack Capacity to Capture FMware Systems Due to Emerging New Artifacts and Stages

FMware systems include a plethora of new artifacts like prompts, adapters and guardrails. In addition, the environment details, the data generation and consumption pipeline are more complex. Finally, the safety and compliance risk for many new stages of FMware are unknown.

Current Mitigations

- Extend existing BOM frameworks manually to include emerging artifacts, even if this approach is ad-hoc & resource-intensive

Call to Action for Researchers

- Work with industry groups to push for the adoption of enhanced AI BOM standards.
- Identify new FMware assets, processes, and lifecycles to enhance AI BOM standards

Call to Action for AI Engineers

- Develop flexible documentation tools that can adapt to new artifacts and stages in FMware systems, aiding in detailed BOM creation.



Implementing AI Bill of Materials (AI BOM) with SPDX 3.0

A Comprehensive Guide to Creating AI and Dataset Bill of Materials.

Authors

Karen Bennet, Gopi Krishnan Rajbahadur,
Arthit Suriyawongkul and Kate Stewart

October 2024



Thank you to all the SPDX Supporters



Summary and Call for Participation - Come Improve Trustworthiness With Us!

Ability to create AI BOMs is pivotal to ensure compliance, transparency, safety and traceability. In short, AI BOMs are critical to ensure the trustworthiness of AI software.

Pain points that prevent us from successfully creating AI BOMs

- Lack of tools to enable creation of AI BOMs
- Required metadata is not readily available
- License compliance quagmire

Challenges that we need to address moving forward

- Automation challenges
- Regulations to requirements tracing challenges
- Ambiguous data ownership challenges
- Process documentation challenges
- FMware challenges

To participate in our working group

