Using SPDX for Functional Safety

FOSDEM 2023
Nicole Pappler
AlektoMetis
Agenda

About me
What is Functional Safety and how can SPDX help
Safety Case and SPDX Relationships
Different SBOMs for Safety and how to use them for your Safety Case
Open points
About me

Professional History:

● Been working in production maintenance, automotive, ECU software development
● All my projects had some safety criticality
● Started to focus on functional safety about 10 years ago

Currently:

● Tech consulting as part of AlektoMetis
● Supporting my customers regarding functional safety, security & compliant use of open source
● Involved in some of the LF projects
  ○ Open Chain (3rd party certification)
  ○ ELISA (Medical Group)
  ○ Zephyr (Functional Safety Manager)
  ○ FuSa for SPDX

What else?

● Not good with remembering names and faces
● GitHub, Discord, etc: @nicpappler
How can we use SPDX for FuSa?
What is Functional Safety?

Definition of Safety

the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment

Definition of Functional Safety

the part of safety that depends on a system or equipment operating correctly in response to its inputs

Detecting potentially dangerous conditions, resulting either in the activation of a protective or corrective device or mechanisms to prevent hazardous events or in providing mitigation measures to reduce the consequences of the hazardous event.
What do I need for Functional Safety?

- Suitable, robust system concept and architecture
- Processes for development, verification, build, deployment and maintenance (according to Safety Standards like IEC 61508)
- Analysis, Reviews and Tests
- Loads of documentation and evidences

- Safety Plan
- Verification Plan
- Requirements
- SW Architecture & Design
- Coding Guidelines
- Test Cases
- Test Reports
- Code
- Calibration Data
How can SPDX support?

**Engineers like to engineer!**

- Creating a fantastic system
- Maintaining the fantastic system
- Applying a process to do so
- Ensuring all documentation and evidences are consistent
How can SPDX support?

**Engineers like to engineer!**

- Creating a fantastic system :-)  
- Maintaining the fantastic system :-)  
- Applying a process to do so :-/  
- Ensuring all documentation and evidences are consistent *no-no-no-no*
How can SPDX support?

Engineers like to engineer!

- Creating a fantastic system :-)  
- Maintaining the fantastic system :-)  
- Applying a process to do so :-/  
- Ensuring all documentation and evidences are consistent no-no-no-no
Using SPDX Relationship Information

Assumption: process to create and maintain all artefacts (requirements, architecture, tests, analysis report) is accepted and applied

Still the biggest pain: Keeping a complete and consistent set of documentation and verifying that the evidences are complete and consistent
Using SPDX Relationship Information

Assumption: process to create and maintain all artefacts (requirements, architecture, tests, analysis report) is accepted and applied

Still the biggest pain: Keeping a complete and consistent set of documentation and verifying that the evidences are complete and consistent

SPDX style solution: Create SPDX Relationships between all documentation artefacts to track all possible system combinations!
Using SPDX Relationship Information

Clause 1: Package Information
Clause 2: File Information
Clause 3: Snippet Information
Clause 4: Other Licensing Information
Detected
Clause 5: Relationship between SPDX
Clause 6: Elements Information
Clause 7: Annotation Information
Clause 8: Review Information
(deprecated)
Annex A: SPDX License List
Annex B: License Matching Guidelines
How do SPDX relationships work for FuSa?
FuSa documentation structure

All FuSa related documentation is part of the Safety Case!

Think of all these documents as part of the release - each document is part of the Bill of Material, as is each screw, each microcontroller and each piece of software!
V-Model style documentation model
SPDX for process and planning

What are plans, process definitions and guidelines?
SPDX for process and planning

What are plans, process definitions and guidelines?

Artefacts, that specify how things are done, other artefacts are structured and created etc.

Examples:

<table>
<thead>
<tr>
<th>Artefact</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Plan</td>
<td>SPECIFICATION of the project structure, the scope, the general development,</td>
</tr>
<tr>
<td></td>
<td>verification, maintenance strategy</td>
</tr>
<tr>
<td>Requirements Management Plan</td>
<td>SPECIFICATION how requirements are created, where they are stored, the</td>
</tr>
<tr>
<td></td>
<td>verification measures applied to requirements</td>
</tr>
<tr>
<td>Coding Guidelines</td>
<td>SPECIFICATION of the ruleset applied when creating code</td>
</tr>
<tr>
<td>Change Management Process</td>
<td>SPECIFICATION of the change workflow, how changes are initiated, the lifecycle</td>
</tr>
<tr>
<td></td>
<td>of changes etc.</td>
</tr>
</tbody>
</table>
SPDX for product documentation

What kind of product documentation do we need to manage?
SPDX for product documentation

What kind of product documentation do we need to manage?

- Requirement type documents like functional requirements and architectural models, test specifications, build information
- Report type documents like test results, analysis results, review results
- Code
SPDX for product documentation

What kind of product documentation do we need to manage?

Specifications, Reports, Tests...

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Requirement Specification</td>
<td>a SPECIFICATION for functional requirements, architectural elements etc.</td>
</tr>
<tr>
<td>Unit Test</td>
<td>the TEST_CASE related to code or a specification artefact</td>
</tr>
<tr>
<td>Unit Test Report</td>
<td>DOCUMENTATION of a unit test EVIDENCE all tests have been performed as planned</td>
</tr>
<tr>
<td>Code</td>
<td>usually is GENERATED from or according to some specification artefact</td>
</tr>
<tr>
<td>Coding Guidelines</td>
<td>SPECIFICATION about the project specific details for the code</td>
</tr>
</tbody>
</table>
SPDX to for assessment lifecycle

The omnipresent question: What will I need for the safety assessment? How can I make my assessor happy?
The omnipresent question: What will I need for the safety assessment? How can I make my assessor happy?

- To begin the proceedings: Planning documents, product architecture/design and a strategy how to implement everything
The omnipresent question: What will I need for the safety assessment? How can I make my assessor happy?

- To begin the proceedings: Planning documents, product architecture/design and a strategy how to implement everything
- A product that has an appropriate concept and architecture for its intended use
- A complete and consistent set of plans, specifications, verification evidences
- A comprehensive statement that your Safety Case is complete
The omnipresent question: What will I need for the safety assessment? How can I make my assessor happy?

<table>
<thead>
<tr>
<th>To start - Functional Safety Management and concept</th>
<th>a list and package of all documents associated with planning, functional (safety) concept and architecture/design</th>
</tr>
</thead>
<tbody>
<tr>
<td>During the assessment phases</td>
<td>packages of documents that represent the current state of development and test</td>
</tr>
<tr>
<td>To finalize the assessment</td>
<td>package of the final documentation, reports and valid product configurations</td>
</tr>
</tbody>
</table>
### SPDX to for assessment lifecycle

The omnipresent question: What will I need for the safety assessment? How can I make my assessor happy?

<table>
<thead>
<tr>
<th>To start - Functional Safety Management and concept</th>
<th>A list and package of all documents associated with planning, functional (safety) concept and architecture/design</th>
</tr>
</thead>
<tbody>
<tr>
<td>During the assessment phases</td>
<td>Packages of documents that represent the current state of development and test</td>
</tr>
<tr>
<td>To finalize the assessment</td>
<td>Package of the final documentation, reports and valid product configurations</td>
</tr>
</tbody>
</table>

Different package information can be used to generate Safety SBOMs to support safety compliance documentation and assessment!
Using SBOMs for Safety Compliance Documentation *

*and for Safety Assessment and Certification Evidence
Safety Deliverables

**Concept Assessment** - all information supporting the soundness of your safety concept, product architecture and implementation strategy

**Final Safety Assessment** - all information related to your concept, development, actual implementation, verification, deployment, maintenance

**Re-Assessments** - all evidences, that the impacts of all applied changes since the last final assessment have been analysed, everything has been implemented and deployed as planned
## Concept Assessment

**Goal:** proof, that your initial approach is generally suitable

**Evidence:** a list and package of all documents associated with planning, functional (safety) concept and architecture/design

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>[Folder icon]</td>
<td>Safety Plan and other plans for implementation and verification strategy</td>
</tr>
<tr>
<td>[Folder icon]</td>
<td>Safety Concept (Safety requirement specification &amp; system/SW architecture)</td>
</tr>
</tbody>
</table>
# Concept Assessment - Design SBOM

**Goal:** proof, that your initial approach is generally suitable

<table>
<thead>
<tr>
<th><strong>Evidence:</strong></th>
<th>a list and package of all documents associated with planning, functional (safety) concept and architecture/design</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Plan and other plans for implementation and verification strategy</td>
<td></td>
</tr>
<tr>
<td>Safety Concept (Safety requirement specification &amp; system/SW architecture)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>SBOM Type:</strong></th>
<th>Generated list of all documents that describe how the final safety related system will be constructed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design S-BOM</td>
<td></td>
</tr>
</tbody>
</table>
Assessment stages

Goal: create traceable deliverables to document the progress of safety development

**Evidence:** a list and package of all documents that has been created for the current development milestone

<table>
<thead>
<tr>
<th>All updated plans</th>
<th>guidelines for implementation (coding guidelines etc.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>requirement &amp; test specifications</td>
<td>verification evidences (test reports)</td>
</tr>
</tbody>
</table>
### Assessment stages - Source SBOM

**Goal:** Create traceable deliverables to document the progress of safety development

**Evidence:** A list and package of all documents that has been created for the current development milestone

<table>
<thead>
<tr>
<th>SBOM Type: Source S-BOM</th>
<th>Generated list of all documents that describe the current state of the system</th>
</tr>
</thead>
<tbody>
<tr>
<td>All updated plans</td>
<td>guidelines for implementation (coding guidelines etc.)</td>
</tr>
<tr>
<td>requirement &amp; test specifications</td>
<td>verification evidences (test reports)</td>
</tr>
</tbody>
</table>

---

*Image Source:* AlektoMetis...we enable digital innovation.
## Assessment stages

**Goal:** create traceable deliverables to document the final release of the release that goes into testing

<table>
<thead>
<tr>
<th><strong>Evidence:</strong> a list and package of all documents that has been created for the current development milestone</th>
</tr>
</thead>
<tbody>
<tr>
<td>final set of plans</td>
</tr>
<tr>
<td>guidelines for implementation (coding guidelines etc.)</td>
</tr>
<tr>
<td>final set of requirement &amp; test specifications</td>
</tr>
<tr>
<td>all verification evidences (test reports)</td>
</tr>
</tbody>
</table>

**SBOM Type:**
## Assessment stages - Build SBOM

**Goal:** create traceable deliverables to document the final release of the release that goes into testing

### Evidence:
- a list and package of all documents that has been created for the current development milestone

<table>
<thead>
<tr>
<th>SBOM Type:</th>
<th>Generated list of all documents that build the final release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build S-BOM</td>
<td>guidelines for implementation (coding guidelines etc.)</td>
</tr>
<tr>
<td></td>
<td>all verification evidences (test reports)</td>
</tr>
<tr>
<td>final set of plans</td>
<td>final set of requirement &amp; test specifications</td>
</tr>
</tbody>
</table>

Final Assessment

Goal: the final artefacts of the Build S-SBOM, plus all valid configuration data

**Evidence:** complete set of documents, information regarding all valid configurations, all deployed combinations of calibration/configuration data

- final set of plans
- final set of requirements
- verification evidences (review and test reports)
- code and/or binaries
- safety analysis evidence
- tool eval & qualification
- configuration data
- calibration data
- evidence of completeness
Final Assessment - Deployed SBOM

Goal: the final artefacts of the Build SBOM, plus all valid configuration data

**Evidence:** complete set of documents, information regarding all valid configurations, all deployed combinations of calibration/configuration data

<table>
<thead>
<tr>
<th>final set of plans</th>
<th>code and/or binaries</th>
<th>configuration data</th>
</tr>
</thead>
<tbody>
<tr>
<td>final set of requirements</td>
<td>safety analysis evidence</td>
<td>calibration data</td>
</tr>
<tr>
<td>verification evidences (review and test reports)</td>
<td>tool eval &amp; qualification</td>
<td>evidence of completeness</td>
</tr>
</tbody>
</table>

**SBOM Type:**

Deployed S-BOM

Generated list of all documents that describe the final state of the system, all configuration data, all calibration data, all verification evidence for the deployed built and applied calibration/configuration data
Closing the evidence loop

**Challenge:** complete list of Safety Case documents, sources and applied configuration and calibration data

- **Configuration Management Plan:** Strategy applied to manage revisions, changes, document types, accountabilities, ... of all work products

- **Configuration Item List:** List of all documents that are under configuration management and planned to be associated with a safety release ⇒ all stuff that must be in the final release
Challenge: complete list of Safety Case documents, sources and applied configuration and calibration data

**Configuration Management Plan**
Strategy applied to manage revisions, changes, document types, accountabilities, ... of all work products

**Configuration Item List:**
List of all documents that are under configuration management and planned to be associated with a safety release ⇒ all stuff that must be in the final release

**Safety Case**
Compilation of all safety evidence required by the Safety Plan
Usually all elements of the Configuration Item List incl. their applicable revision
Challenge: complete list of Safety Case documents, sources and applied configuration and calibration data

Configuration Management Plan
Strategy applied to manage revisions, changes, document types, accountabilities, ... of all work products

Configuration Item List:
List of all documents that are under configuration management and planned to be associated with a safety release ⇒ all stuff that must be in the final release

Safety Case
Compilation of all safety evidence required by the Safety Plan
Usually all elements of the Configuration Item List incl. their applicable revision

Safety S-BOM
Generated Deployed S-BOM
includes a
Closing the evidence loop

**Challenge:** complete list of Safety Case documents, sources and applied configuration and calibration data

- **Configuration Management Plan:** Strategy applied to manage revisions, changes, document types, accountabilities, ... of all work products
- **Configuration Item List:** List of all documents that are under configuration management and planned to be associated with a safety release ⇒ all stuff that must be in the final release
- **Safety Case:** Compilation of all safety evidence required by the Safety Plan. Usually all elements of the Configuration Item List incl. their applicable revision
- **Safety S-BOM:** Generated Deployed S-BOM includes...
Open Topics
Open Topics

- details about the tooling to generate the set of SBOMs used for safety?
- relationships only between artefacts - what are all artefacts in our context?
- complete model for document & evidence types and their relationships
- pilot project for proof of concept
- can we use this approach for cyber security compliance, e.g. according to ISO/SAE 21434?
Getting involved

Functional Safety special interest group

- regular call each Friday 5 pm CET
- [https://lists.spdx.org/g/spdx-fusa](https://lists.spdx.org/g/spdx-fusa)
Feedback, Questions, Comments?