AlektoMetis
...we enable digital innovation.

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 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

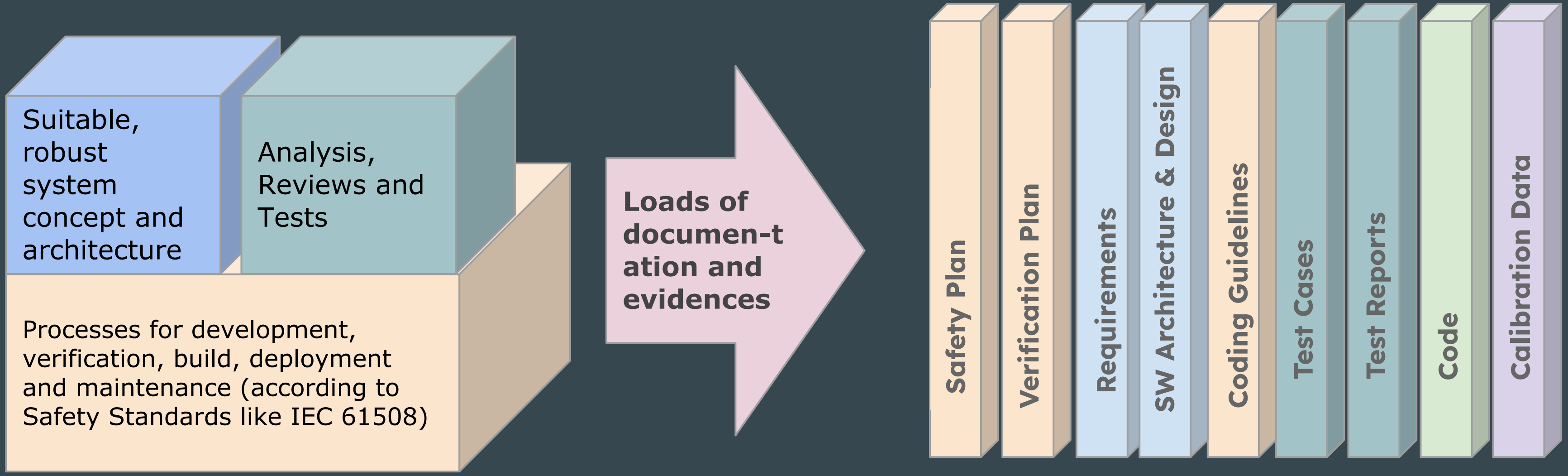
Definition of Functional Safety

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.

AlektoMetis
...we enable digital innovation.

What do I need for Functional Safety?



Suitable, robust system concept and architecture

Analysis, Reviews and Tests

Processes for development, verification, build, deployment and maintenance (according to Safety Standards like IEC 61508)

Loads of documen-tation 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*

AlektoMetis
...we enable digital innovation.

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

AlektoMetis
...we enable digital innovation.

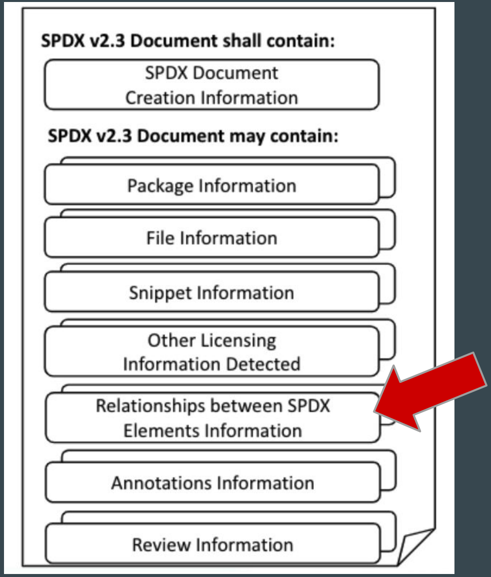
Using SPDX Relationship Information

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



SPDX v2.3 Document shall contain:

SPDX Document Creation Information

SPDX v2.3 Document may contain:

Package Information

File Information

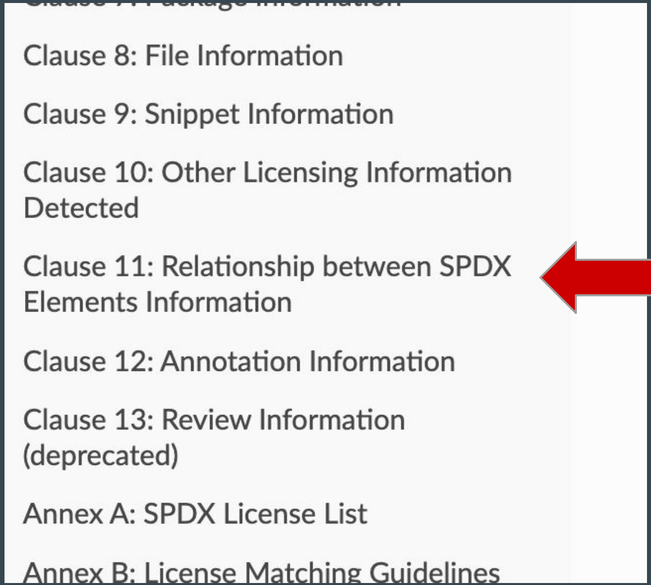
Snippet Information

Other Licensing Information Detected

Relationships between SPDX Elements Information

Annotations Information

Review Information



Clause 7: Package Information

Clause 8: File Information

Clause 9: Snippet Information

Clause 10: Other Licensing Information Detected

Clause 11: Relationship between SPDX Elements Information

Clause 12: Annotation Information

Clause 13: Review Information (deprecated)

Annex A: SPDX License List

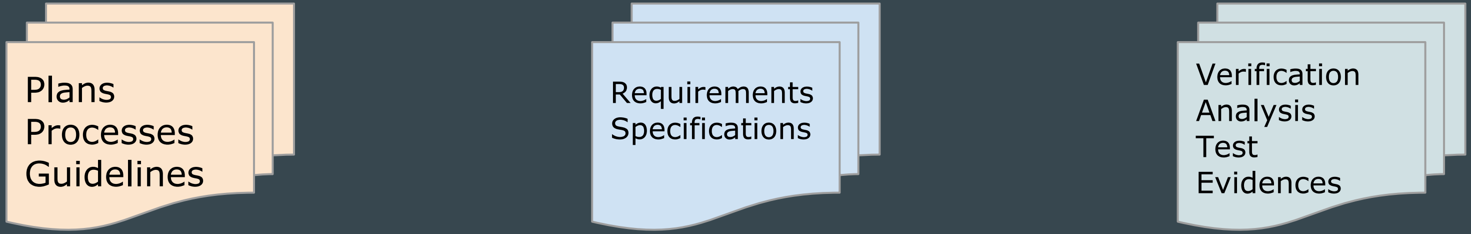
Annex B: License Matching Guidelines

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!

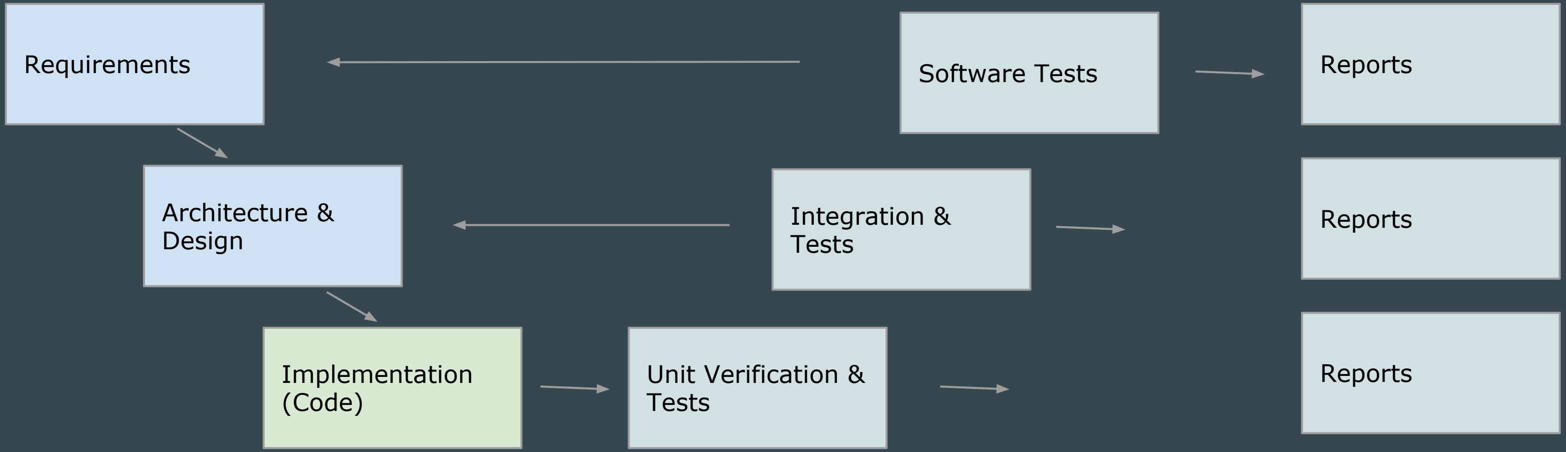


Plans
Processes
Guidelines

Requirements
Specifications

Verification
Analysis
Test
Evidences

V-Model style documentation model



Requirements

Architecture & Design

Implementation (Code)

Unit Verification & Tests

Integration & Tests

Software Tests

Reports

Reports

Reports

Functional Safety Management Plan	Requirements Management Plan	Configuration Management Plan	Documentation Management Plan	Component Qualification / Supply Chain	Validation & Assessment	Tooling Eval & Qualification (Dev, Verification, Build, Deploy…)

SPDX for process and planning

AlektoMetis ...we enable digital innovation.

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:

Safety Plan	SPECIFICATION of the project structure, the scope, the general development, verification, maintenance strategy
Requirements Management Plan	SPECIFICATION how requirements are created, where they are stored, the verification measures applied to requirements
Coding Guidelines	SPECIFICATION of the ruleset applied when creating code
Change Management Process	SPECIFICATION of the change workflow, how changes are initiated, the lifecycle of changes etc.

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...

Safety Requirement Specification	a SPECIFICATION for functional requirements, architectural elements etc.
Unit Test	the TEST_CASE related to code or a specification artefact
Unit Test Report	DOCUMENTATION of a unit test EVIDENCE all tests have been performed as planned
Code	usually is GENERATED from or according to some specification artefact
Coding Guidelines	SPECIFICATION about the project specific details for the code

SPDX to for assessment lifecycle

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

SPDX to for assessment lifecycle

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

SPDX to for assessment lifecycle

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

AlektoMetis
...we enable digital innovation.

SPDX to for assessment lifecycle

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

To start - Functional Safety Management and concept	a list and package of all documents associated with planning, functional (safety) concept and architecture/design
During the assessment phases	packages of documents that represent the current state of development and test
To finalize the assessment	package of the final documentation, reports and valid product configurations

AlektoMetis
...we enable digital innovation.

SPDX to for assessment lifecycle

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

To start - Functional Safety Management and concept	a list and package of all documents associated with planning, functional (safety) concept and architecture/design
During the assessment phases	packages of documents that represent the current state of development and test
To finalize the assessment	package of the final documentation, reports and valid product configurations

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

Safety Plan and other plans for implementation and verification strategy

Safety Concept (Safety requirement specification & system/SW architecture

Concept Assessment - Design SBOM

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

- Safety Plan and other plans for implementation and verification strategy
- Safety Concept (Safety requirement specification & system/SW architecture

SBOM Type: Design S-BOM	Generated list of all documents that describe how the final safety related system will be constructed

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

- All updated plans
- guidelines for implementation (coding guidelines etc.)
- requirement & test specifications
- verification evidences (test reports)

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

- All updated plans
- guidelines for implementation (coding guidelines etc.)
- requirement & test specifications
- verification evidences (test reports)

SBOM Type: Source S-BOM	Generated list of all documents that describe the current state of the system

Assessment stages

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

- final set of plans
- final set of requirement & test specifications
- guidelines for implementation (coding guidelines etc.)
- all verification evidences (test reports)

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

- final set of plans
- guidelines for implementation (coding guidelines etc.)
- final set of requirement & test specifications
- all verification evidences (test reports)

SBOM Type: Build S-BOM	Generated list of all documents that build the final release

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

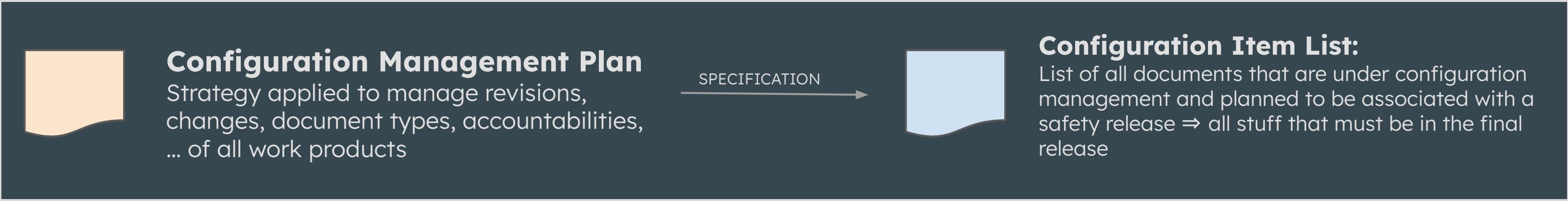
Evidence: complete set of documents, information regarding all valid configurations, all deployed combinations of calibration/configuration data

- 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

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

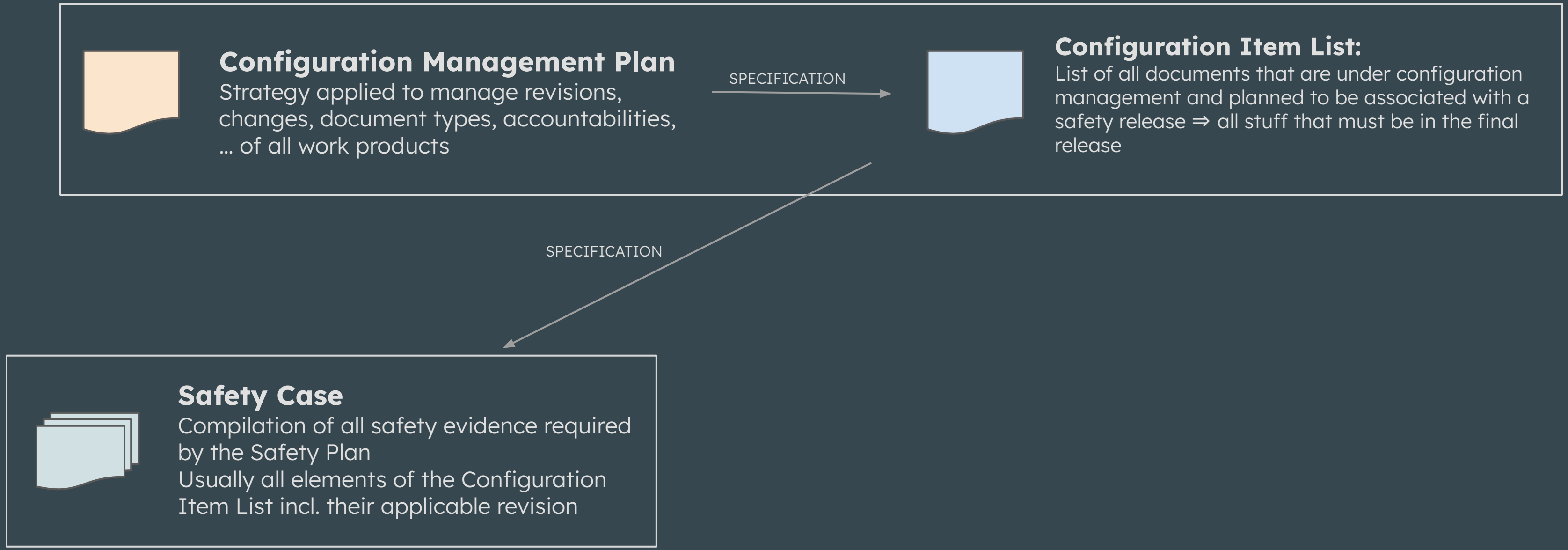


Configuration Management Plan
Strategy applied to manage revisions, changes, document types, accountabilities, … of all work products

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

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

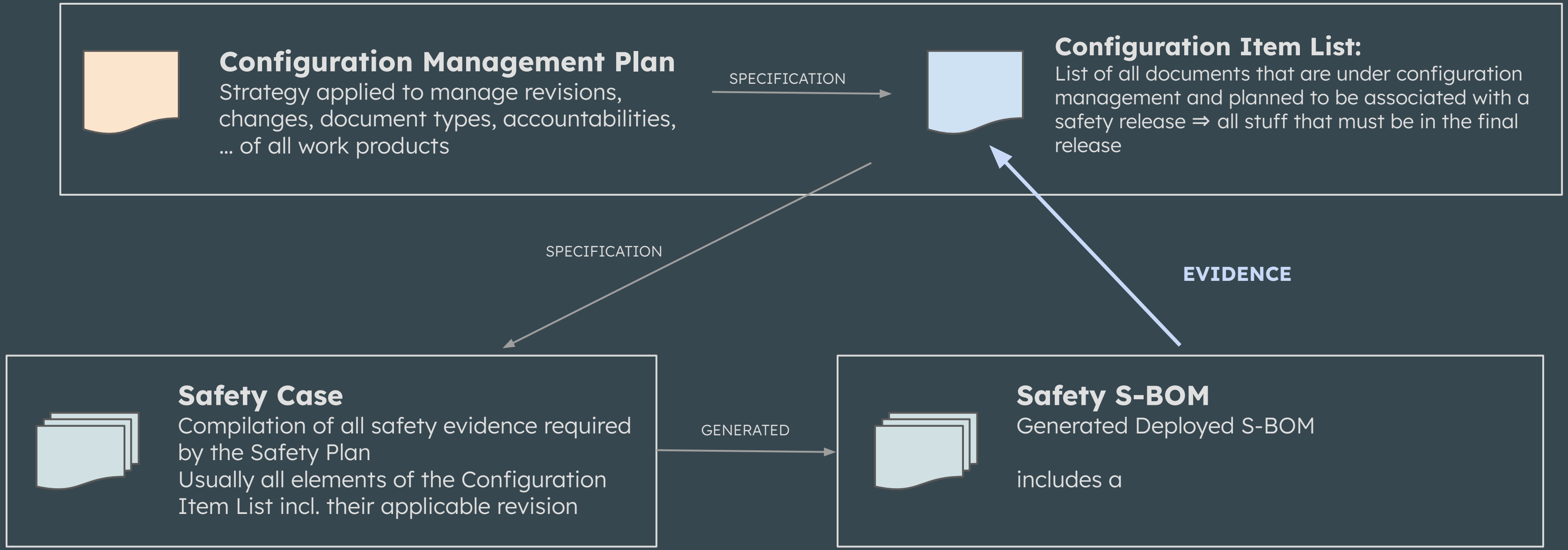
Configuration Item List:
List of all documents that are under configuration management and planned to be associated with a safety release ⇒ all stuff that must be in the final release

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

AlektoMetis
...we enable digital innovation.

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

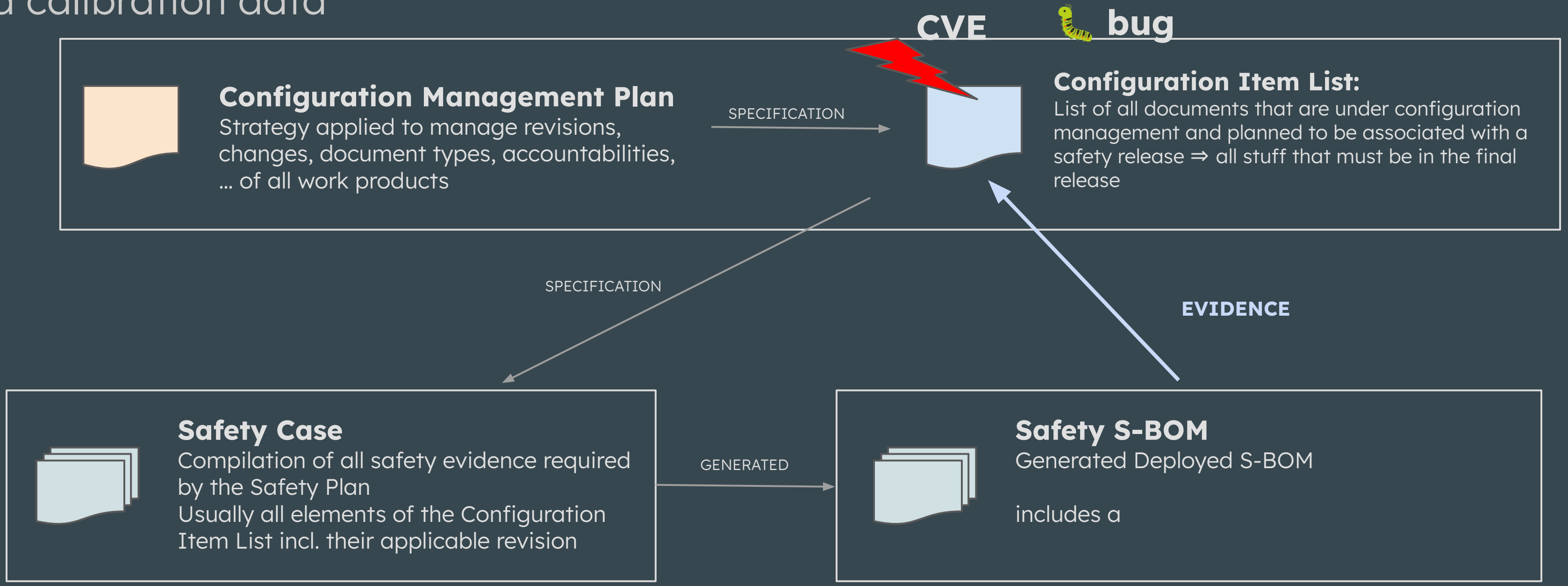
Safety Case
Compilation of all safety evidence required by the Safety Plan
Usually all elements of the Configuration Item List incl. their applicable revision

Safety S-BOM
Generated Deployed S-BOM

includes 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 a

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

Feedback, Questions, Comments?