Safety Processes

Dana Vede & Daniel Krippner

AGENDA

- WHAT & WHY?
- BACKGROUND & MOTIVATION
- CONCLUSIONS
- OTHER RELATED INITIATIVES

SDV
Eclipse Software Defined Vehicle

WHAT and WHY?

Software Defined Vehicle

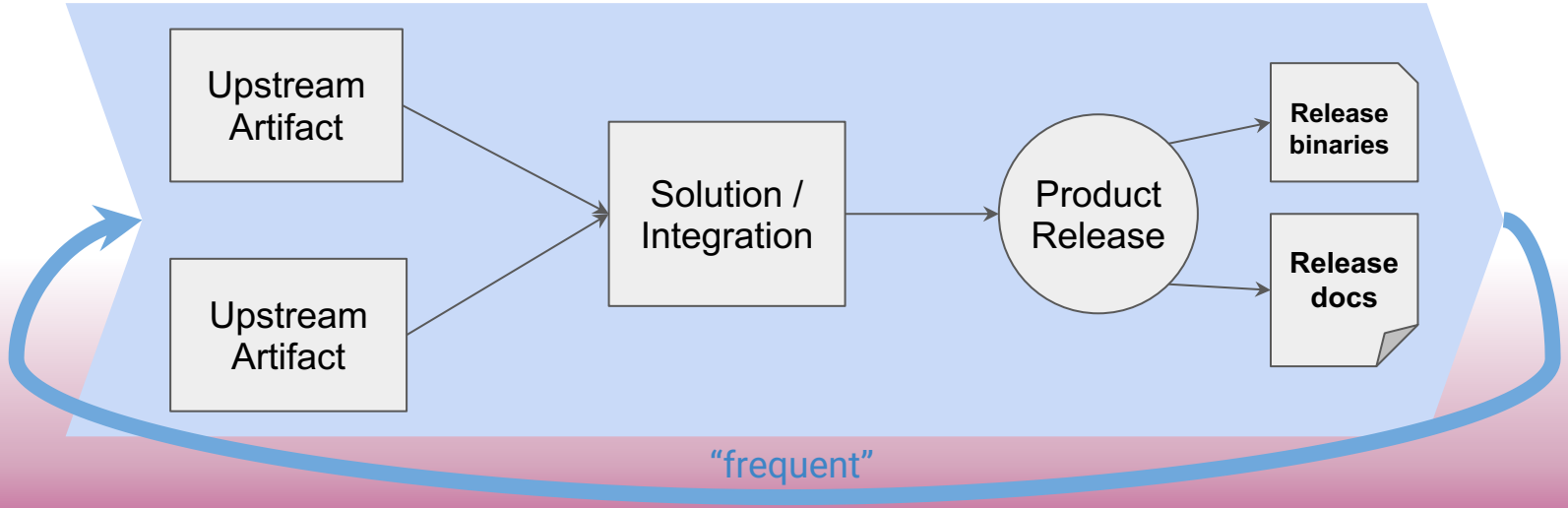
An open technology platform for the software defined vehicle of the future; focused on accelerating innovation of automotive-grade in-car software stacks using open source and open specifications developed by a vibrant community.

"automotive-grade" ?

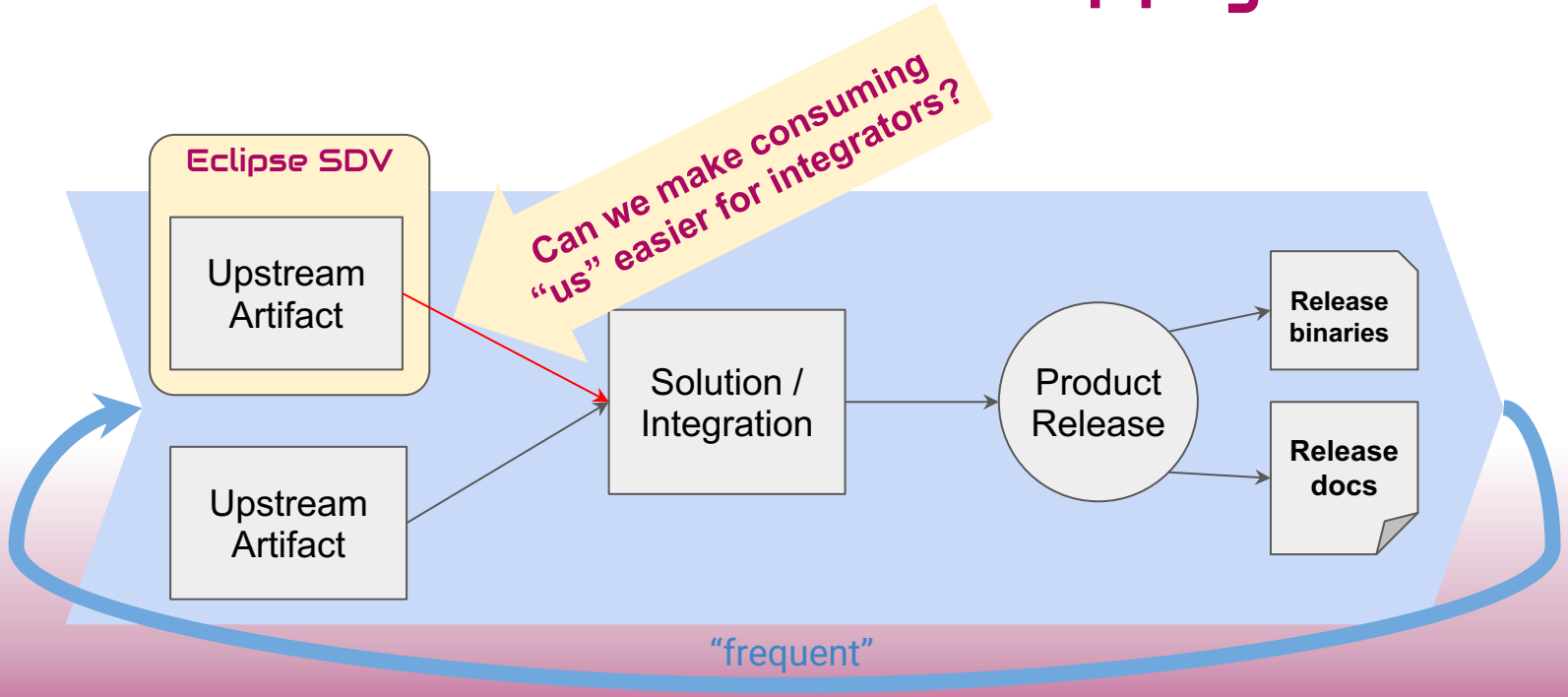
Free stock photos - PxHere - 1055658

SDV Eclipse Software Defined Vehicle

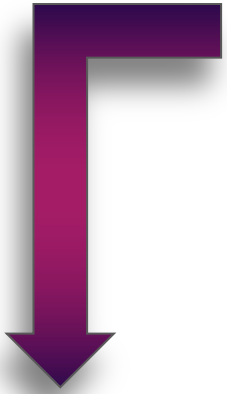
Envisioned Scenario – std. supply chain



Envisioned Scenario – std. supply chain



WHAT and WHY?



Software Defined Vehicle

An open technology platform for the software defined vehicle of the future; focused on accelerating innovation of automotive-grade in-car software stacks using open source and open specifications developed by a vibrant community.

"automotive-grade" ?

- **WHAT:**

  We aim to define an Eclipse SDV process applicable to the SDV projects

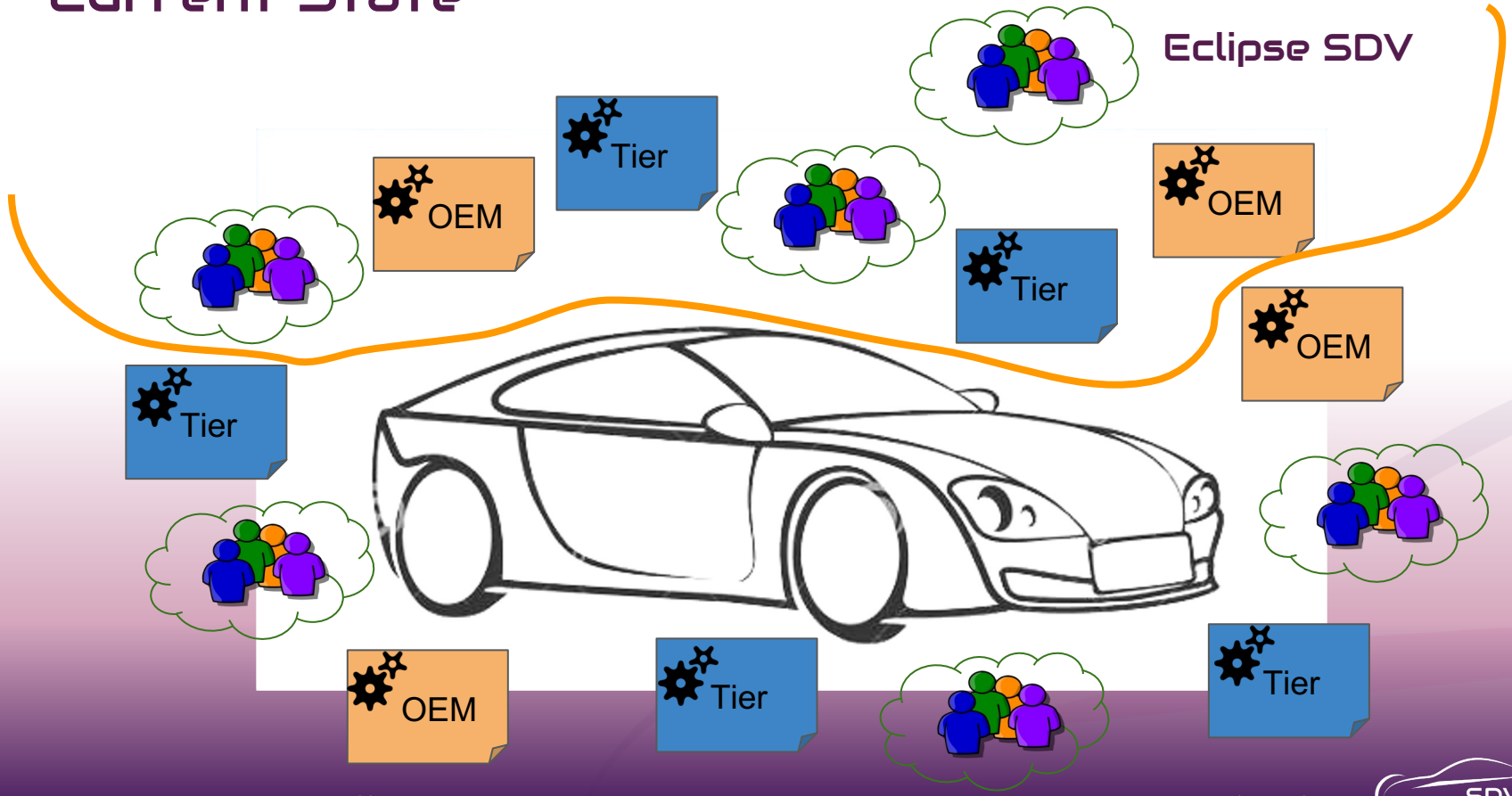
- **WHY:**

  To increase projects' success
  To be part of the automotive industry's innovation

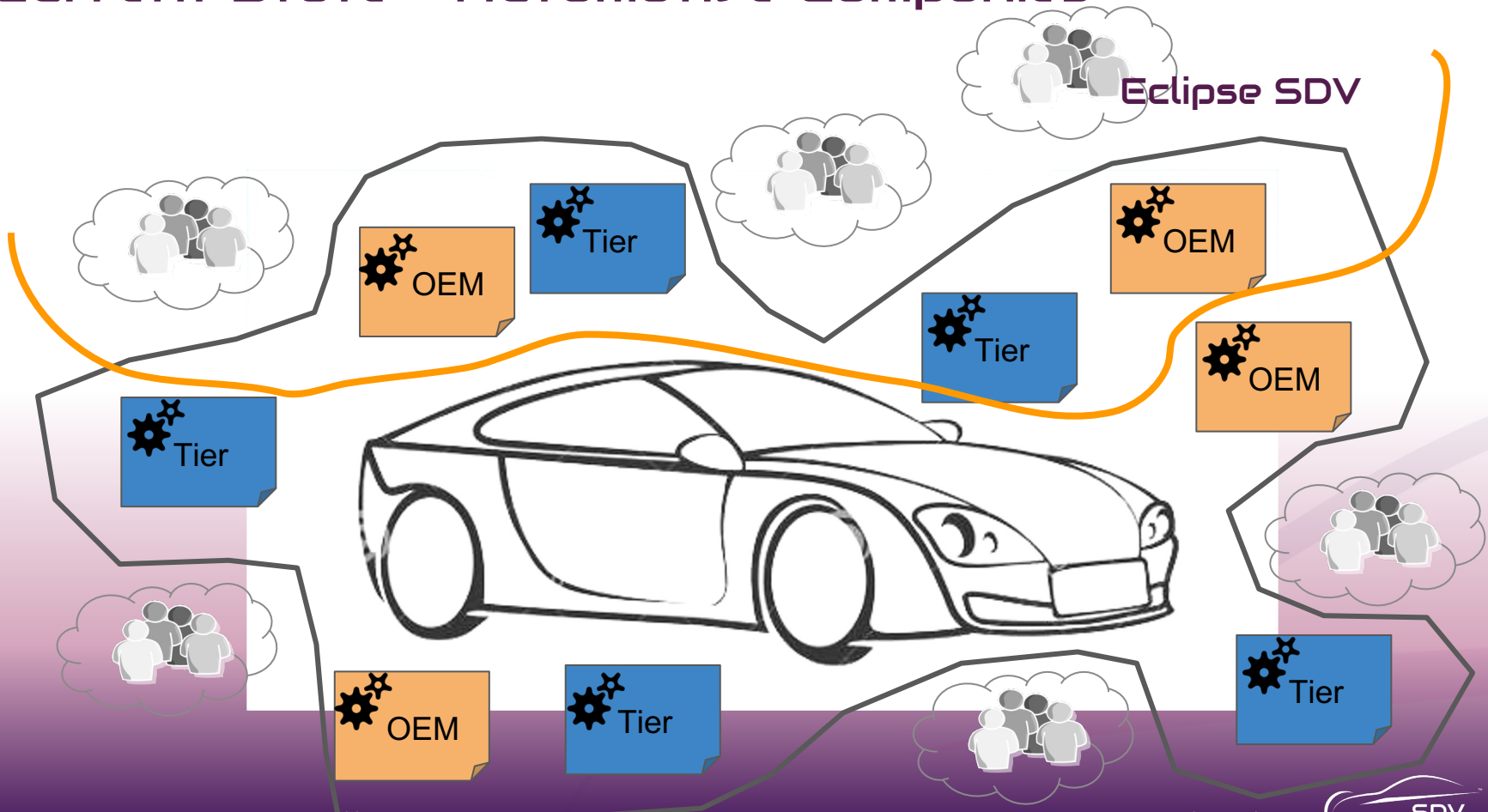
BACKGROUND and MOTIVATION

- What is the current state and what triggers the motivation?
- What would be the desired state and the potential future?

Current State



Current State - Automotive Companies



Definitions

- **Standard** = a level of quality, achievement, etc., that is considered acceptable or desirable / something that is very good and that is used to make judgments about the quality of other things / regularly and widely used, seen, or accepted
- **Compliance** = the management system fully adheres to the requirements of the standard.
- **Certification** = the management system has actually been certified to be in conformance (compliance) with all the requirements of the standard. In essence, certification is proof of a basic compliance claim, similar to a diploma, certificate or stamp.

Current State - Automotive Companies

Automotive-SPICE Standard

- Derived from ISO 15504
- Dedicated for Automotive
- A collection of best practices accompanied by an Evaluation Model.

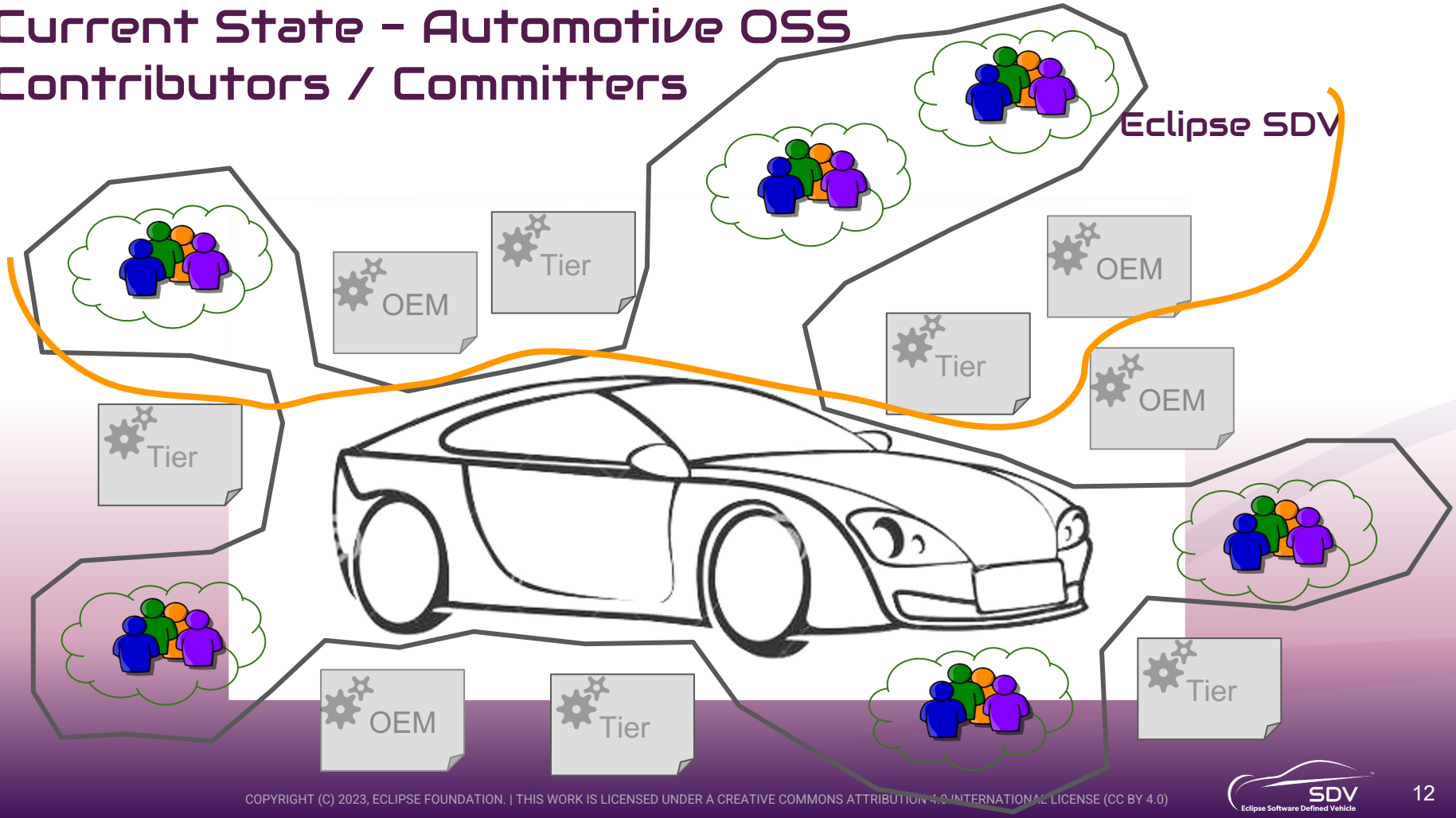
Automotive Functional Safety Standard

- Derived from ISO 61508
- Dedicated for Automotive
- Collection of guidelines to minimize the risk of accidents and unintended failure of automotive systems / subsystems.

Automotive Cyber Security Standard

- Derived from ISO 15408
- Dedicated for Automotive
- A collection of guidelines on protecting the SW running in vehicle, communication between vehicles, smart devices and cloud.

Current State – Automotive OSS Contributors / Committers



Current state – Automotive OSS Contributors / Committers

OSPO*s

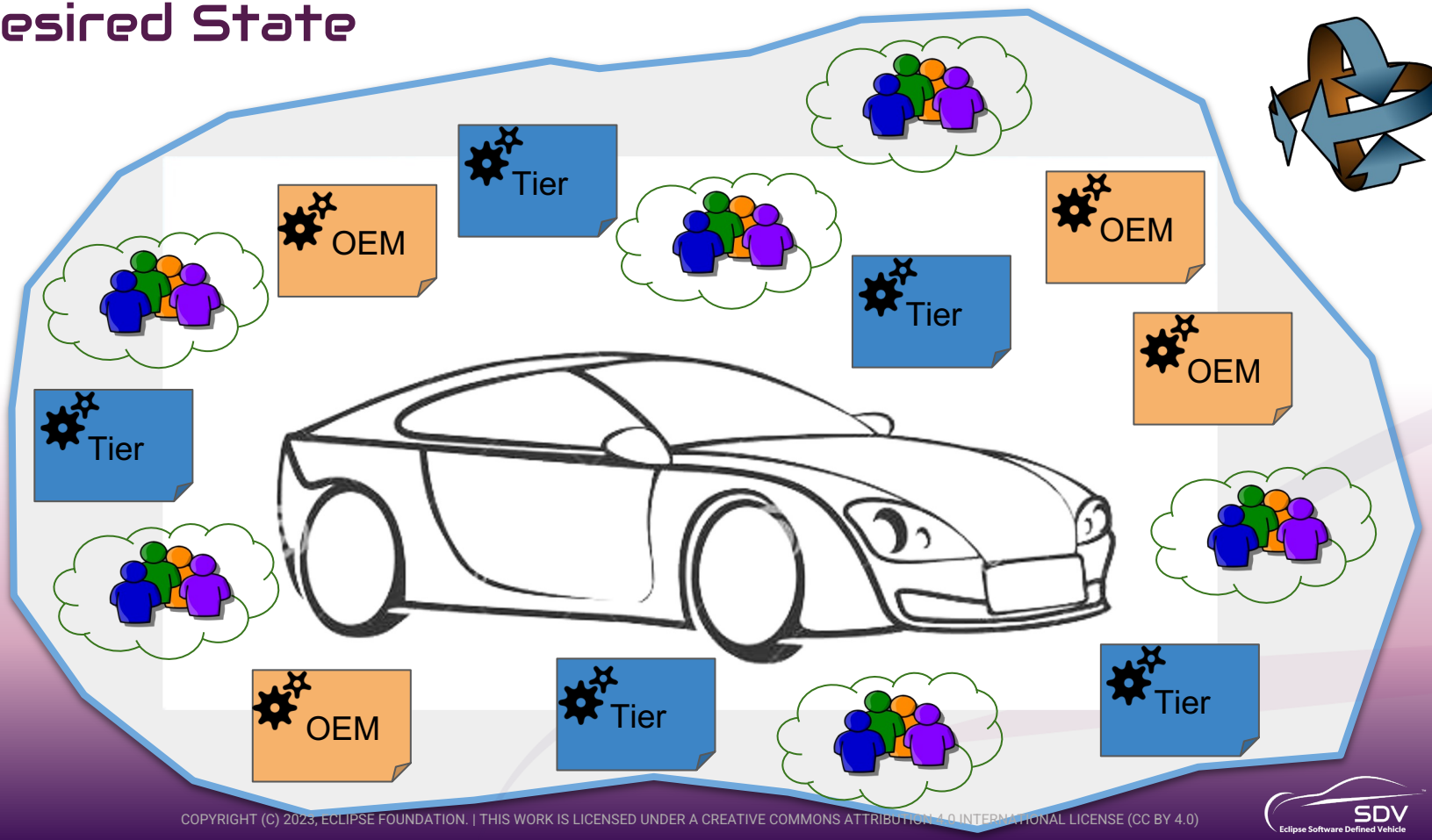
- Define policies on OS projects' governance
- OS/Tech strategy
- Community mgmt support
- Operational enablement
- Are part of Automotive companies

(Open Source Program Office)

Eclipse Foundation

- Defines and provides governance for Eclipse OS Projects
- IP Check
- License Scan
- Cyber Security Auditing

Desired State



Desired state - Automotive Market

OSPOs

- Define policies on OSS projects' governance
- OSS/Tech strategy
- Community mgmt support
- Operational enablement
- Are part of Automotive companies

(Open Source Program Office)

Eclipse Foundation

- Defines and provides governance for Eclipse OS Projects
- IP Check
- License Scan
- Cyber Security Auditing

Eclipse SDV Process

- Defines content-quality objectives for OS SDV projects
- Defines methods for reaching defined quality objectives
- Define project maturity KPIs

CONCLUSIONS

AIM

- ❏ Define and apply a set of best practices that can bring OS Projects closer to being “certification-ready”
  - Code quality
  - Test Types & Levels
  - More detailed documentation
- ❏ Ensure “continuous compliance”
  - Define measurements (KPIs) that can ensure a “continuous compliance” of the defined practices
  - Periodical KPIs measurement and analysis and badges allocation
- ❏ Improve Projects’ adoption and success
  - Win and Display Maturity Badges as part of the business card of the projects

BENEFITS

- ❏ Focus rather on content-quality than on certifications
- ❏ Automotive companies and OS community will speak a more similar language and will be able to better understand each other

OTHER RELATED ACTIVITIES & INITIATIVES

"The mission of the project is to define and maintain a common set of elements, processes and tools that can be incorporated into Linux-based, safety-critical systems amenable to safety certification."

"The scope of the project includes software and documentation development under an OSI-approved license supporting the mission, including documentation, testing, integration and the creation of other artifacts that aid the development, deployment, operation or adoption of the project."

from the technical charter

Photo by Mitchell Luo on Unsplash

ELISA Project insights and overview - FOSDEM 2023 - YouTube

ELISA Working Groups - Fit in an exemplary system

- **Linux Features, Architecture** and **Code Improvements** should integrate into the reference system directly.
- **Tools** and **Engineering process** should serve the reproducible product creation.
- **Medical, Automotive, Aerospace** and future WG use cases strip down the reference system to their use case demands.

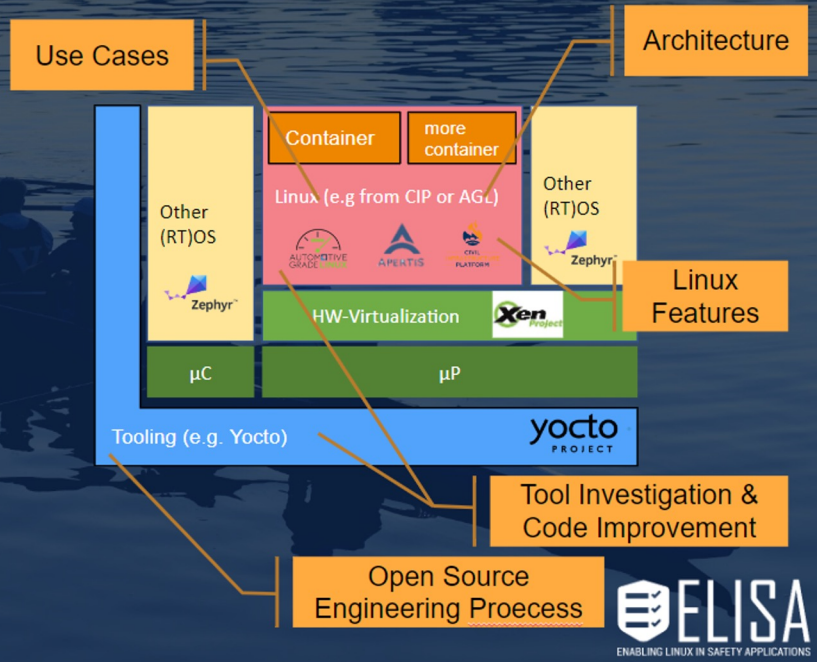


Photo by Mitchell Luo on Unsplash

ELISA Project insights and overview - FOSDEM 2023 - YouTube

zephyrproject-rtos / zephyr Public

Code | Issues 1.5k | Pull requests 469 | Discussions | Actions | Projects 22 | Wiki | Security 41 | Insights

Safety Working Group

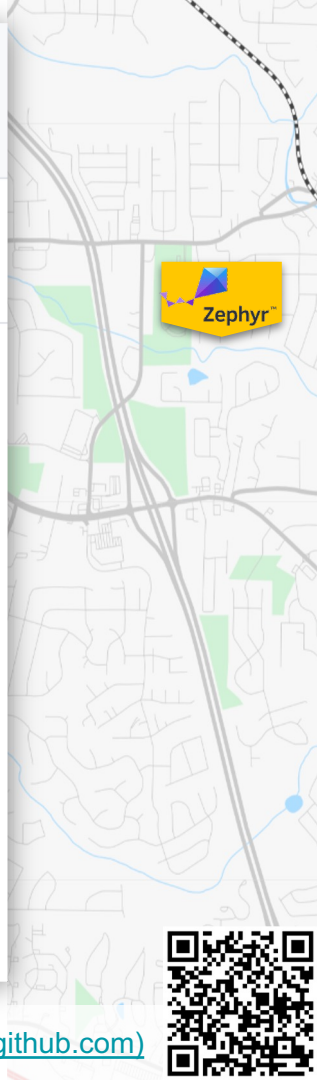
Simon Hein edited this page on Mar 10 · 2 revisions

Introduction

This monthly meeting serves as a discussion forum for anything related to safety in the Zephyr project.

Online meeting

- Kick-off: March 28th, 2023
- Meets every other Tuesday, 7AM-8AM (PT)
- Chairperson: Simon Hein (Baumer)
- Mailing list: safety-wg
- Online conference link and phone: Teams meeting
- Meeting Notes online document



Safety Working Group · zephyrproject-rtos/zephyr Wiki (github.com)

Final Assessment - Deployed SBOM

AlektoMetis ...we enable digital innovation.

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

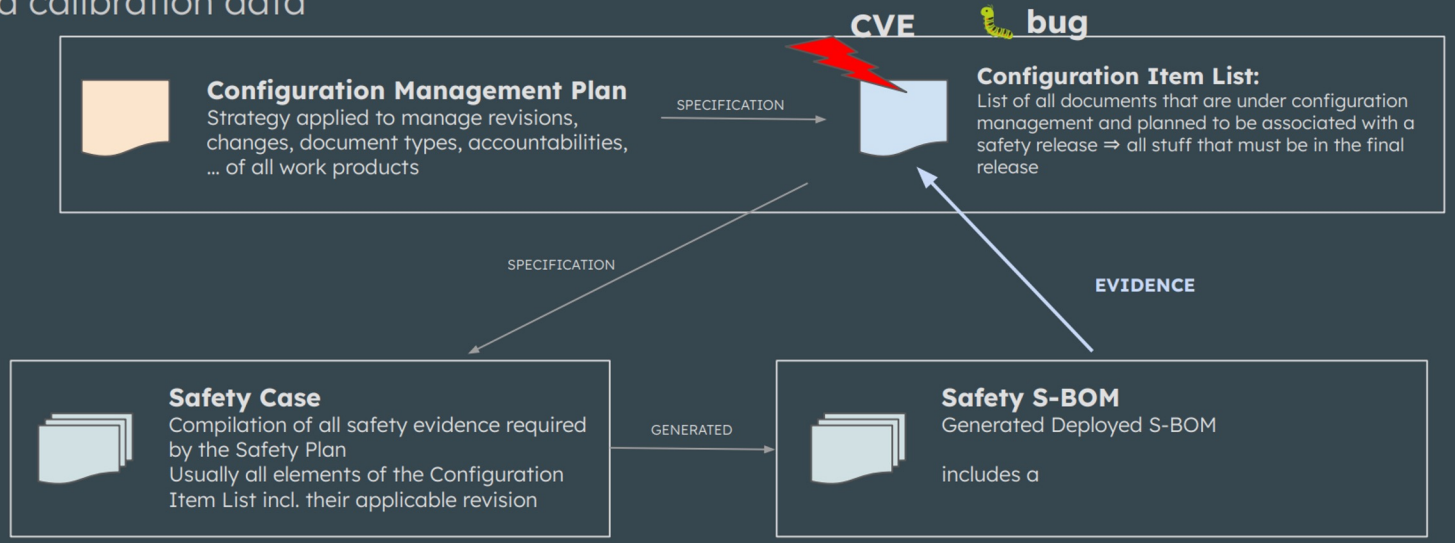
- final set of plans
- final set of requirements
- verification evidences (review and test reports)
- code and/or binaries
- safety analysis evidence
- tool eval & qualification
- configuration data
- calibration data
- evidence of completeness

SBOM Type:	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
Deployed S-BOM	

Closing the evidence loop

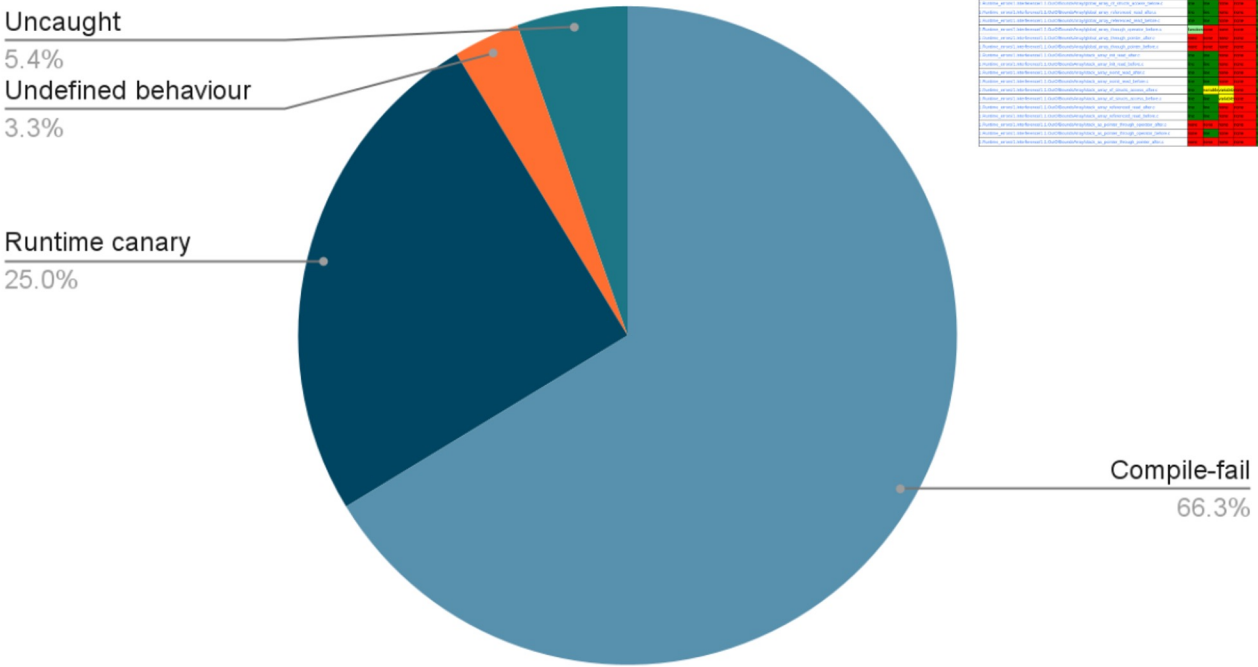
AlektoMetis
...we enable digital innovation.

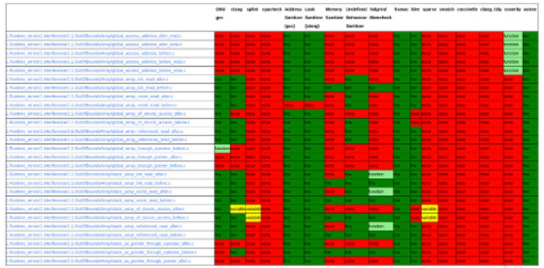
Challenge: complete list of Safety Case documents, sources and applied configuration and calibration data



Comparing ctools checks to stock Rust

Rust conversion of ctools suite





ISO 26262 Part six and Rust

Table 1 - Coding	Table 3 - Design Principles	Table 6 - Design	Table 7 - Unit testing
1a clippy	1a gets-out-of-way	1a needs tooling	1a human
1b unnecessary	1b human	1b semi-built-in	1b human
1c built-in	1c human	1c built-in	1c human
1d semi-built-in	1d semi-built-in	1d clippy	1d human
1e human	1e human	1e built-in	1e human
1f irrelevant	1f human	1f built-in	1f needs-tooling
1g semi-built-in	1g human	1g semi-built-in	1g needs-tooling (some done)
1h semi-built-in	1h system property	1h human	1h clippy but also MIRI
1i built-in	1i system property / semi-built-in	1i semi-built-in	1i clippy but also MIRI
		1j 3rd-party-tooling	1j supported human
			1k supported human
			1l supported human
			1m needs-tooling
			1n irrelevant

THANK YOU!