ELISA
Enabling Linux in Safety Applications

WORKSHOP

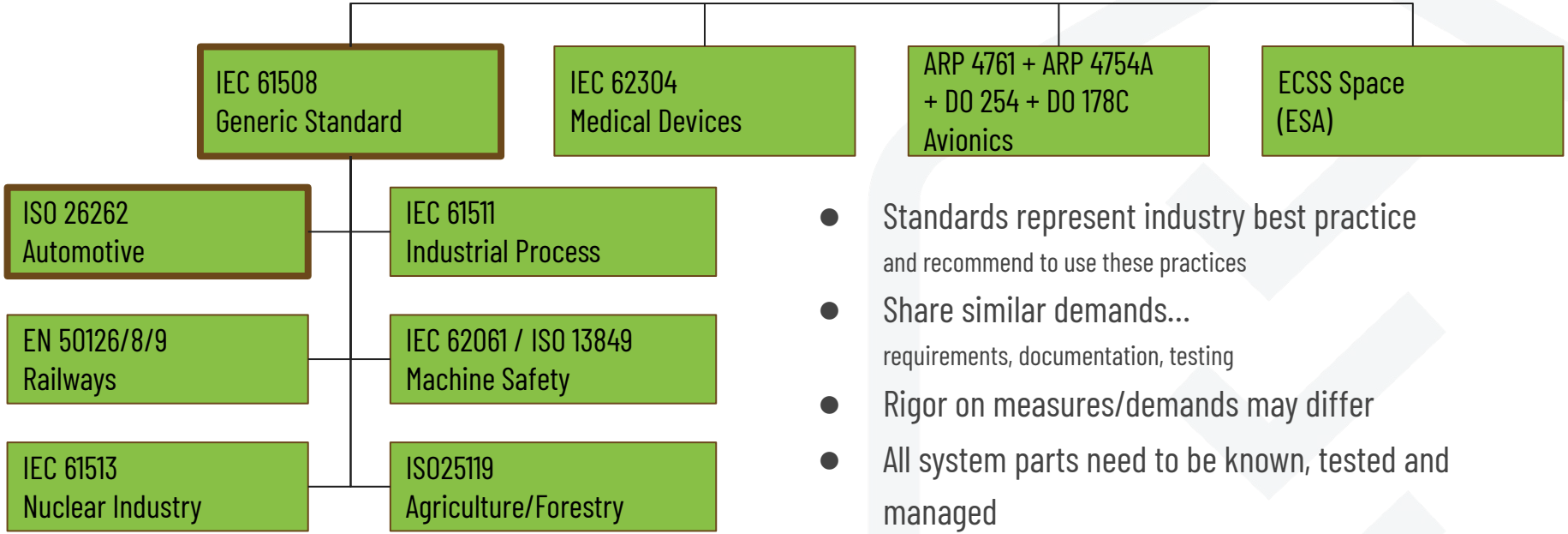
Ask Me Anything about ELISA or Use of OSS in Safety Critical Applications

Philipp Ahmann (ETAS), Gabriele Paoloni (Red Hat)

ELISA WS - Lund, May 7-9, 2025

Intro & Motivation

Samples of safety (integrity) standards



- Standards represent industry best practice
  and recommend to use these practices
- Share similar demands...
  requirements, documentation, testing
- Rigor on measures/demands may differ
- All system parts need to be known, tested and managed
- IEC 61508 and ISO 26262 are mostly referred to in Automotive

ELISA Enabling Linux in Safety Applications WORKSHOP

Route to Safety Certification

- IEC 61508 Route 3S for pre-existing software
- ISO 26262-8 clause 12 approach for simple automotive pre-existing SW
- ISO PAS 8926 as a bridge for complex software
- Challenges increase with increased system complexity (like Linux systems)

Introduction & Motivation

- Safety integrity standards need to adopt to increasing complexity of products
- Safety requires a robust fundament based on processes, technical measures and statistical analysis
- Growing industry interest in open source for safety-certified applications
- Current challenges in integrating open-source solutions with safety standards

(China is already making heavy use of Open Source e.g. in Automotive systems)

The Fundamental Challenge

- Traditional development processes / v-model vs. code centric open source development
- Standard checklist-based approaches vs. nearly not documented collaborative development
- The need for (formal) traceability and documentation in safety-critical systems

Community Challenges For All Projects

- Argument of „OSS development is not organized like commercial software“
- Less influence on maintainers
  (positive & negative – no traditional supplier management)
- Harder to train/direct developers
- Liability of a community?
  (but commercial provider may be liable – insurance)
- Development process: Requirements, traceability, v-model,…
  mapping safety integrity standards

Procedural Requirements for Safety

- Structured documentation of requirements
- Test-to-requirement traceability
- Keeping documentation synchronized with code
- Achieving maintainability over decades
- (And of course all the technical things needed to create a system)

Clash of worlds
(or what is often considered unsafe by safety experts):

- Memory management
- Dynamic memory allocation
- Caches
- Interrupt handling
- non Real time scheduling
- …

Photo by Jukan Tateisi on Unsplash

Project Orientation

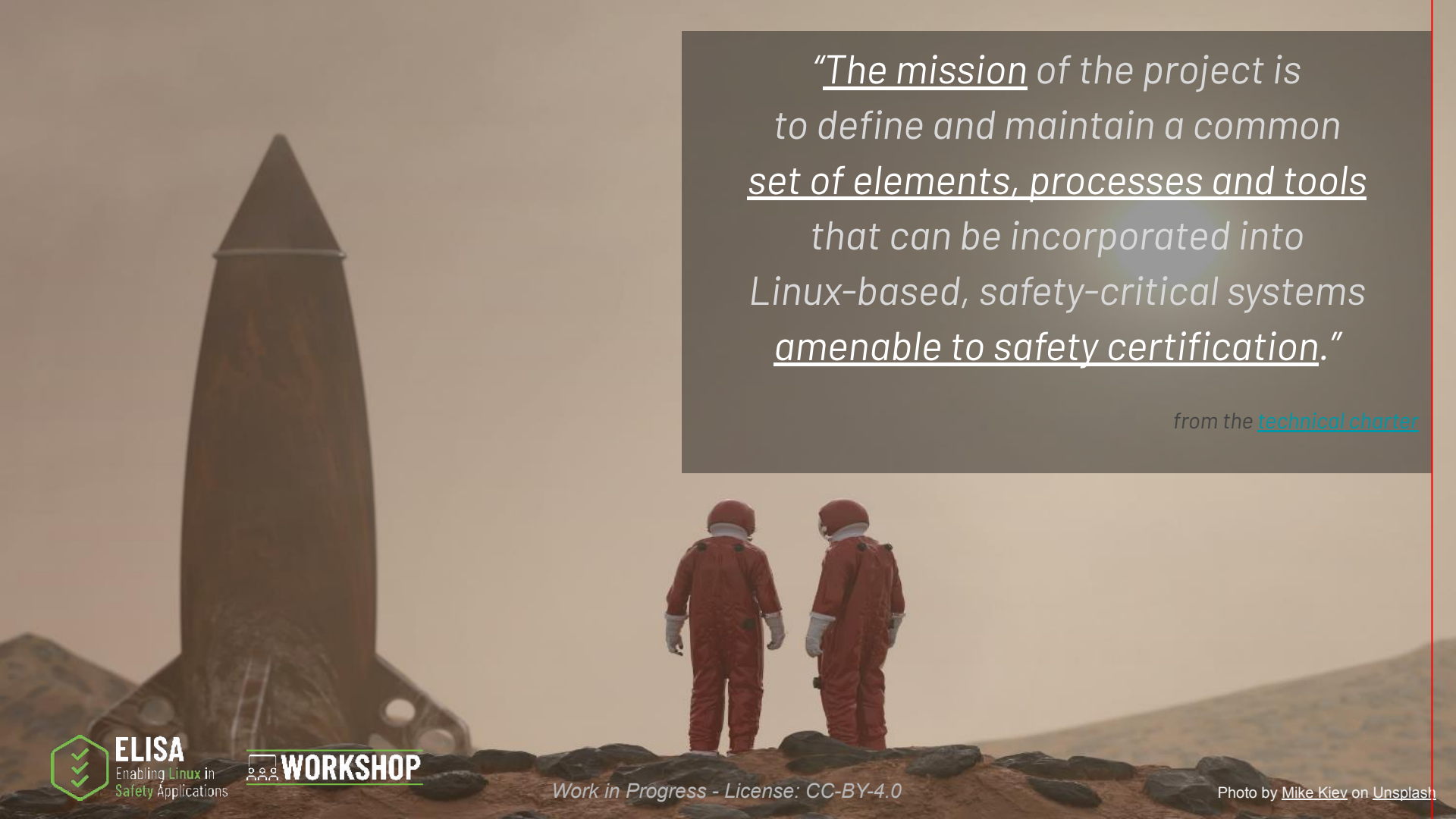
ELISA Project

- Enabling **Safety-critical applications** with **Linux** (beyond Security)
- Increase **dependability & reliability** for whole Linux ecosystem
- **Various use cases**: Aerospace, Automotive, Medical & Industrial
- Supported by major **industrial grade Linux distributors** known for mission critical operation and various industries representatives
- Close community collaboration with **Xen, Zephyr, SPDX, Yocto & AGL** projects
- **Reproducible system** creation from specification to testing
- SW **elements**, engineering **processes**, development **tools**

ELISA : Architecture Processes Features Tools Systems

ELISA Enabling Linux in Safety Applications WORKSHOP

presented in previous session



"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."

from the technical charter

ELISA
Enabling Linux in Safety Applications
WORKSHOP

Photo by Mike Kiev on Unsplash

Linux in Safety Critical Systems

"Assessing whether a system is safe, requires understanding the system sufficiently."

- Understand Linux within that system context and how Linux is used in that system.
- Select Linux components and features that can be evaluated for safety.
- Identify gaps that exist where more work is needed to evaluate safety sufficiently.

presented in previous session

ELISA Enabling Linux in Safety Applications WORKSHOP

STOP - Limitations! The collaboration ...

- *cannot* engineer your system to be safe.
- *cannot* ensure that you know how to apply the described process and methods.
- *cannot* create an out-of-tree Linux kernel for safety-critical applications. (continuous process improvement argument!)
- *cannot* relieve you from your responsibilities, legal obligations and liabilities.

But...

ELISA provides a <u>path forward</u> and peers to <u>collaborate</u> with!

presented in previous session

ELISA Enabling Linux in Safety Applications WORKSHOP

Premier Members

General Members

Associate Members

Industry Support

presented in previous session

Working Groups (WGs) - Horizontal

Safety Architecture

Red Hat

Open Source Engineering Process

CodeThink

Linux Features

Red Hat

Systems

BOSCH

Tool investigation & Code Improvement

BOEING

Photo by Mike Kiev on Unsplash

Working Groups (WGs) - Verticals

Aerospace

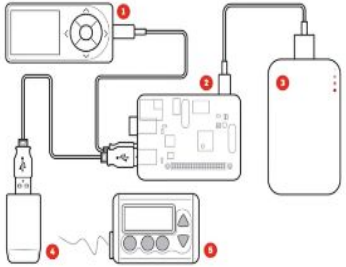
BOEING

Automotive

BOSCH

Medical Devices

THE LINUX FOUNDATION



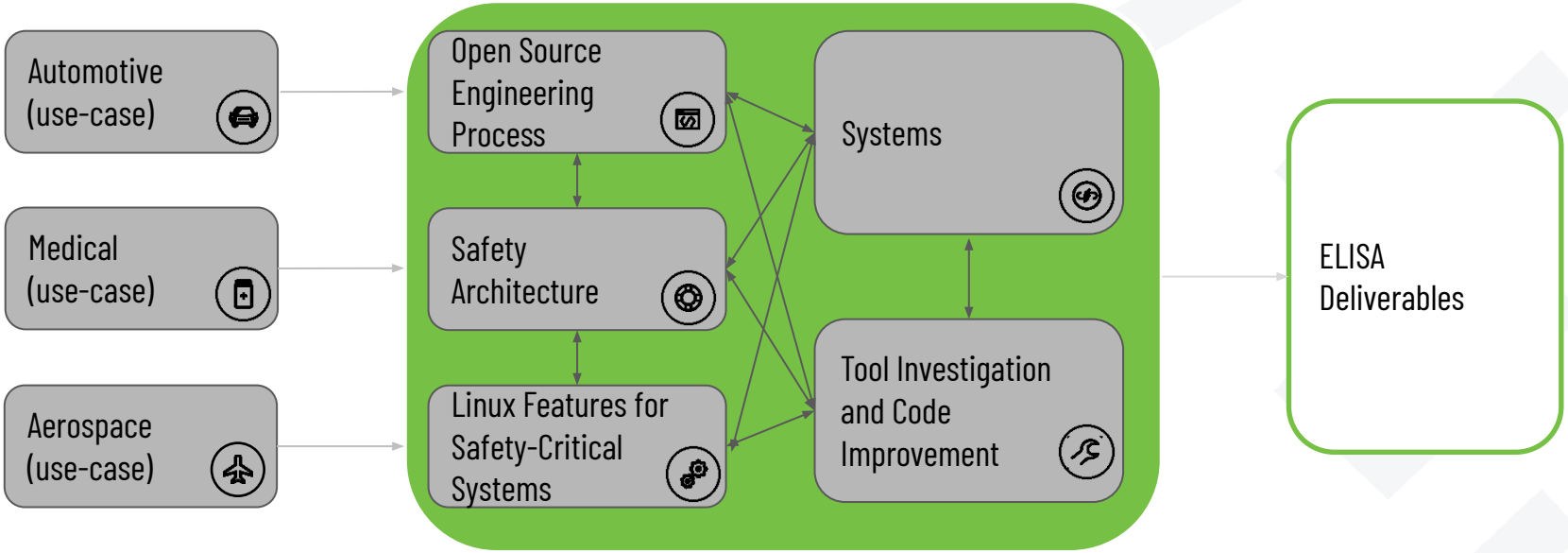
OpenAPS elements

1. Continuous glucose monitor
2. Computer
3. Battery
4. Radio stick
5. Insulin pump

@DanaMLewis

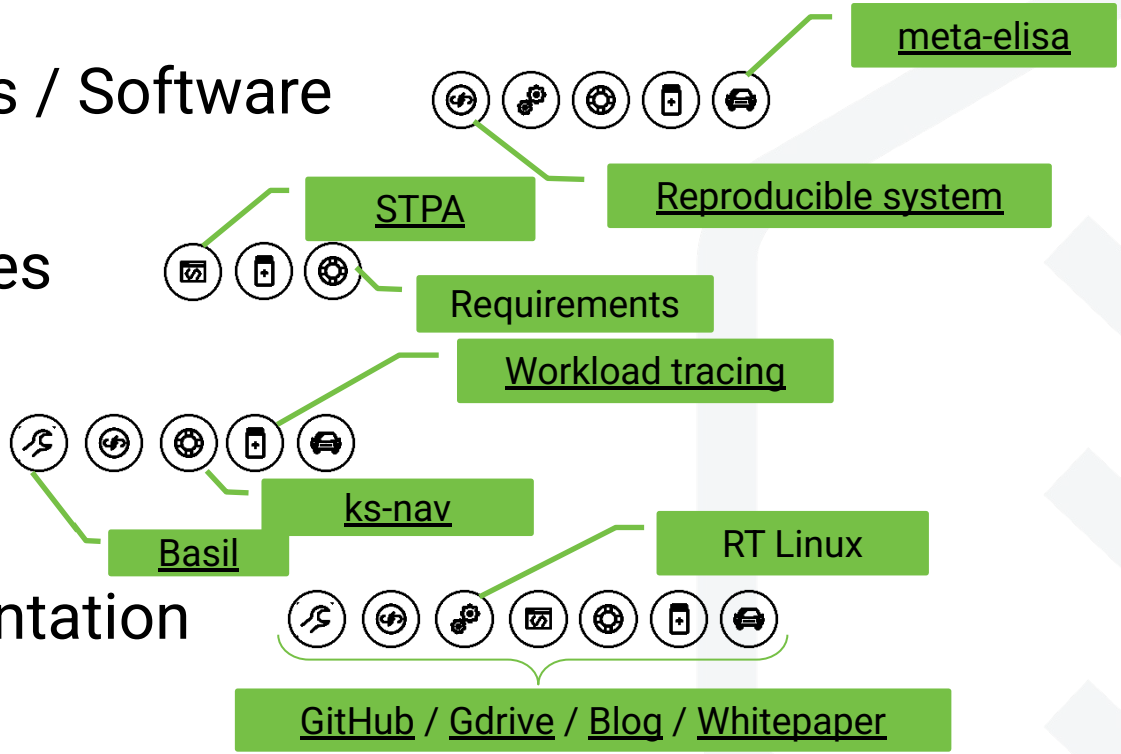
Dana Lewis' OpenAPS project: https://youtu.be/kgu-AYSnyZ8

Relation Between Working Groups



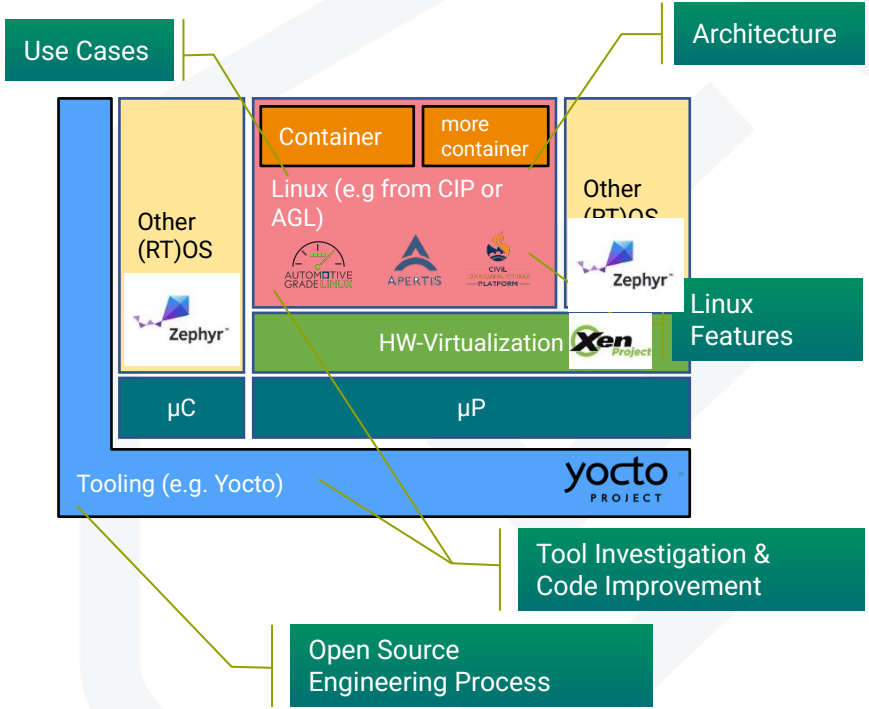
ELISA Working Groups - Deliverables

- Elements / Software
- Processes
- Tools
- Documentation



ELISA Working Groups - Fit in an Exemplary System

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



ELISA Enabling Linux in Safety Applications

WORKSHOP

Interactions Between the Communities

- Open source projects focusing on safety-critical analysis

- Open source projects with safety-critical relevance and comparable system architecture considerations

- Further community interactions

"If you have an apple and I have an apple and we exchange these apples then you and I will still each have one apple
But if you have an idea and I have an idea and we exchange these ideas, then each of us will have two ideas

— George Bernard Shaw

Summary – The storyline for the next 2 days. 😉

- Safety (Integrity Standards) & Open Source
- Processes
- Tools
- Technical Methods and Approaches
- Collaboration beyond project boundaries

A lot of topics will be discussed during the WS, but now...
it is time to ask questions and get you on board!