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

ELISA London WS
June 9-11, 2026
Co-hosted with Canonical

Safety is not Security

(In some languages safety & security are the same word!)

Photo by Annie Spratt on Unsplash

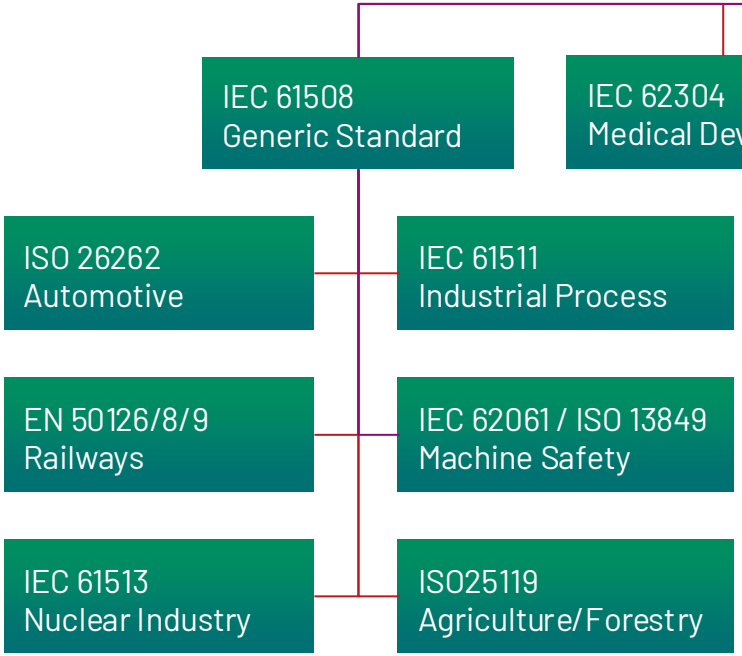
Photo by Jason An on Unsplash

ELISA Enabling Linux in Safety Applications

WORKSHOP

A bit on standards and processes

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

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 → migrates into ISO 26262
- 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

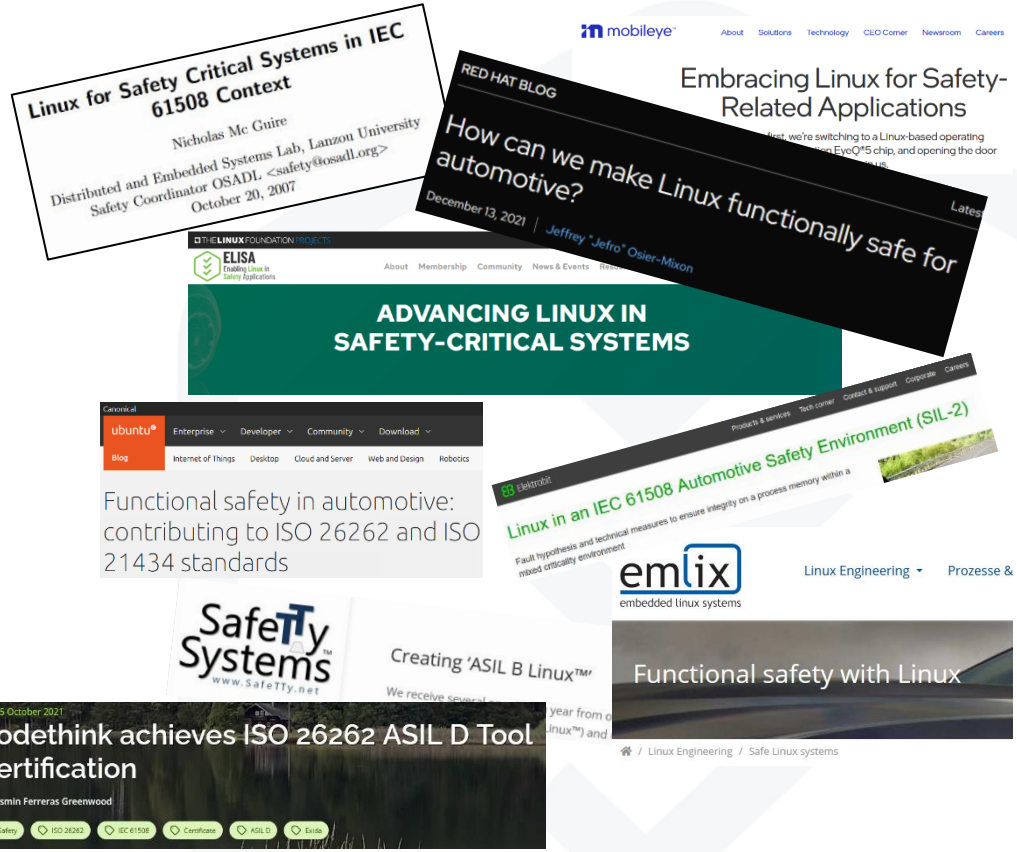
(China is already making heavy use of Open Source e.g. in Automotive systems)

Linux ecosystem
our focus for the next days

The role of Linux

- Open source software superlative.
- Largest community, largest source base.
- Made for flexibility and wide use cases.
- Spread over whole world and in space.
- Several attempts with certification path.
- Gains again momentum for high performance products (e.g. SDV*)
- Prominent open space examples: SIL2LinuxMP and ELISA

SDV: Software-Defined-Vehicle



ELISA Enabling Linux in Safety Applications

WORKSHOP

Photo by Jukan Tateisi on Unsplash

Clash of worlds

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

- Memory management
- Dynamic memory allocation
- Caches
- Interrupt handling
- Non Real time scheduling
- Non functional aspects like: Development process & tools
- …

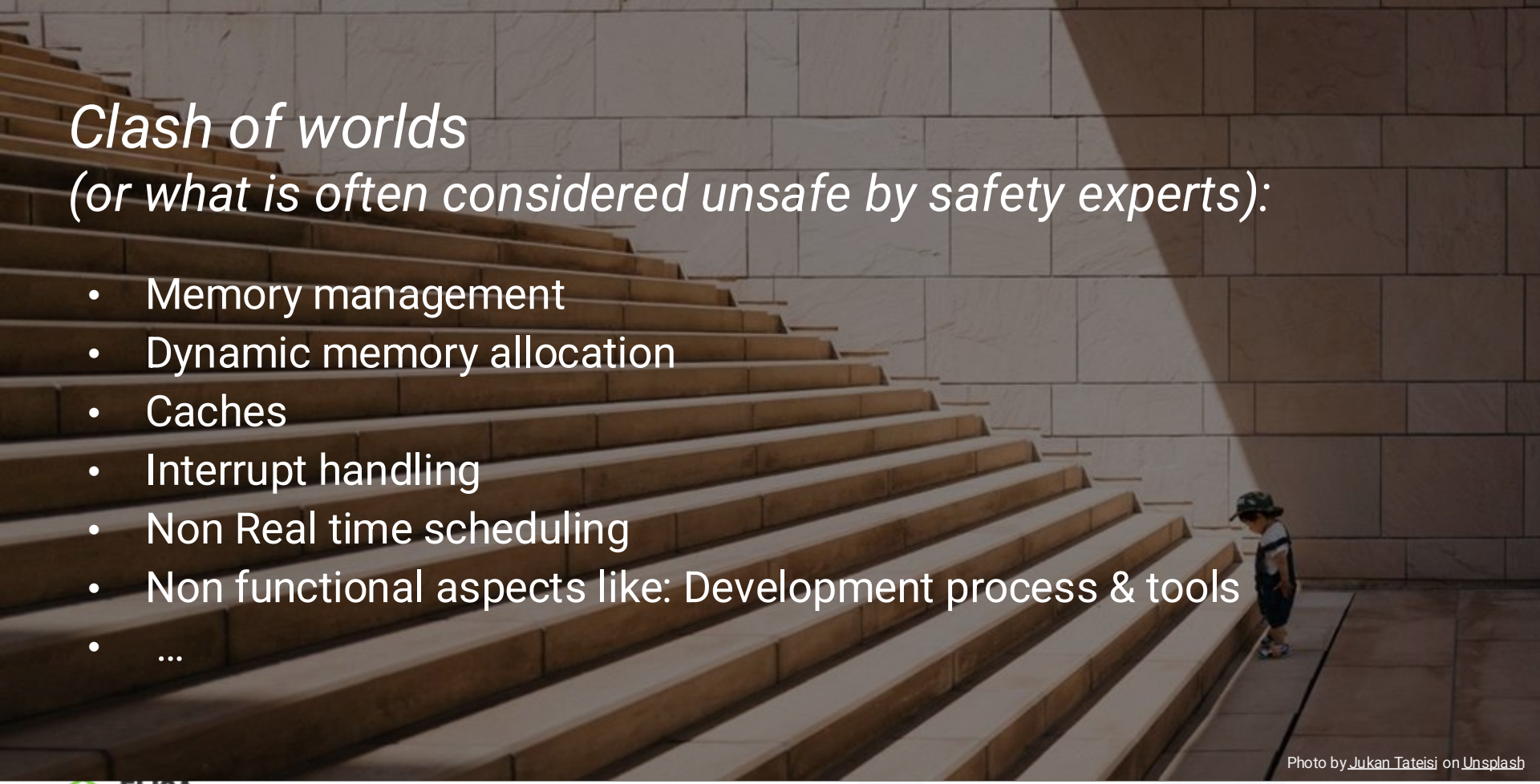


Photo by Jukan Tateisi on Unsplash

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 Enabling Linux in Safety Applications

WORKSHOP

ELISA : Architecture | Processes | Features | Tools | Systems


"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
Work in Progress - License: CC-BY-4.0
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.

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 path forward and peers to collaborate with!

Premier Members

General Members

Associate Members

Industry Support

Working Groups (WGs) - Horizontal

Safety Architecture

Red Hat

Open Source Engineering Process

CodeThink

Linux Features

NVIDIA

Systems

BOSCH

Tool investigation & Code Improvement

THE LINUX FOUNDATION

Photo by Mike Kiev on Unsplash

Working Groups (WGs) - Verticals

Aerospace

BOEING

Automotive

NVIDIA

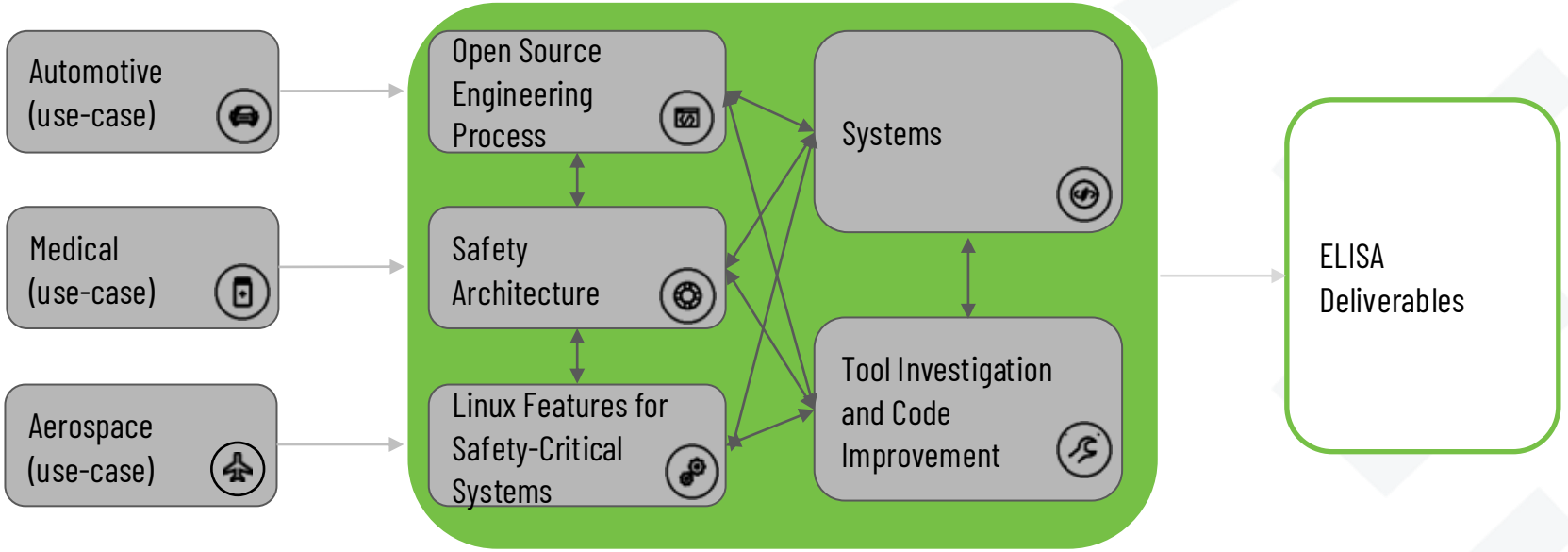
Medical Devices

THE LINUX FOUNDATION

ELISA Enabling Linux in Safety Applications

WORKSHOP

Relation Between Working Groups



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

Thank you ELISA Community!

Get to know the community
and their achievements:
https://elisa.tech/blog/

ELISA
Enabling Linux in
Safety Applications

WORKSHOP

Glimpse on safety critical OSS ecosystem

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)

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

Summary – The storyline for the next 2 days. 😉

- Linux for safety critical systems in Aerospace, Automotive, Railways (~7)
- System architectures & composition (~4)
- Testing & Tracing (~4)
- Requirements & their tools (~4)
- Standards and OSS processes (~4)
- Tools (~5)
- Touching the Linux Kernel (~4)
- Going beyond project boundaries towards adjacent communities (~7)

ELISA Enabling Linux in Safety Applications

WORKSHOP

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

JOIN THE COMMUNITY

ELISA
Enabling Linux in Safety Applications

Our infrastructure and tools are open by default, so jump in and introduce yourself, ask questions and share ideas. Please consider this your invitation to participate.

Subscribe to Mailing Lists

Join Community Meetings

Contribute to Tools and Docs on GitHub

Participate in Working Groups

Attend Events