Project Overview

Philipp Ahmann, Etas GmbH (Bosch)

ELISA
Enabling Linux in Safety Applications

Aerospace · Automotive · Linux Features
Medical Devices · OS Engineering Process
Safety Architecture · Space Grade Linux · Systems · Tools

Photo by Katherine Hood on Unsplash

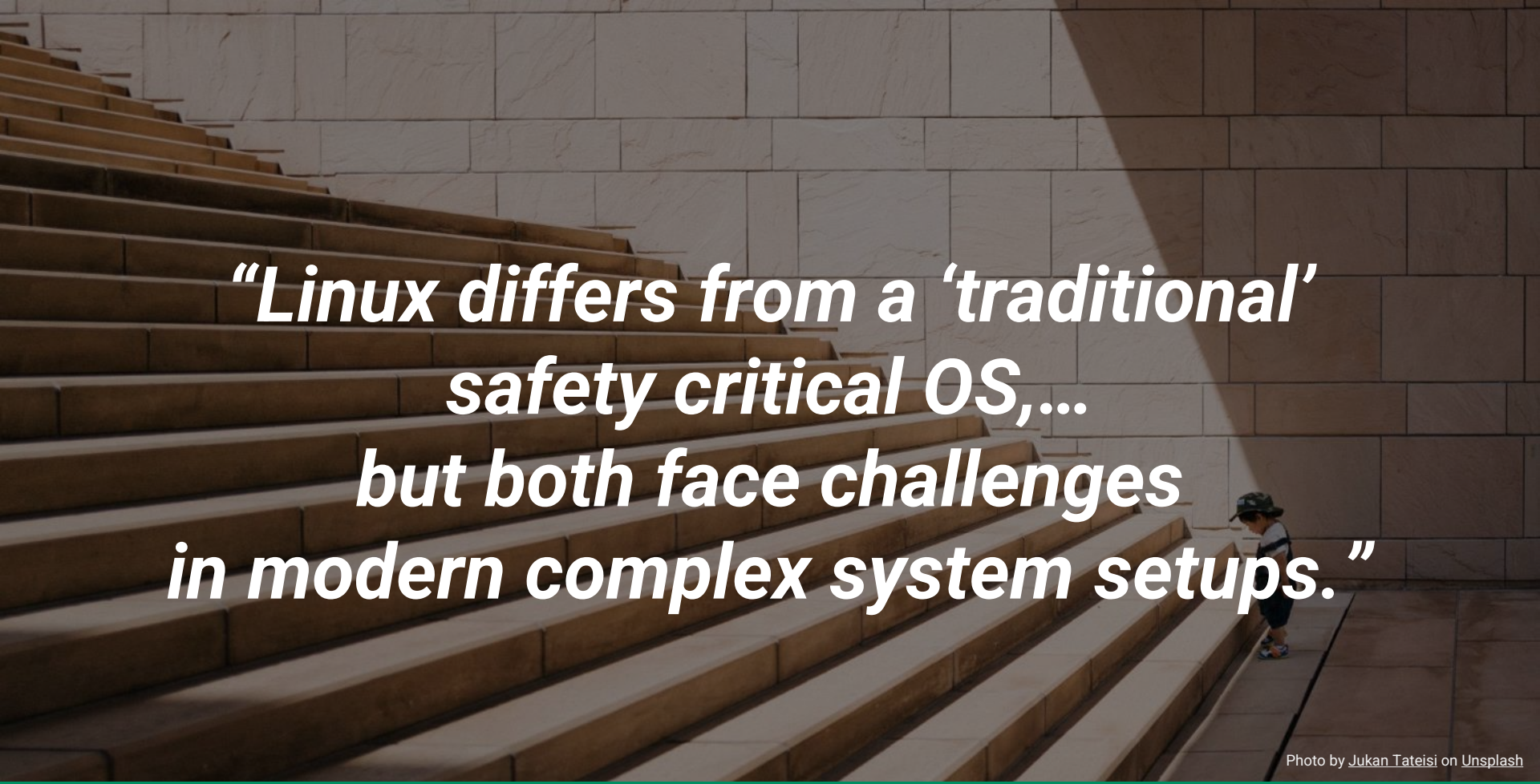
Agenda

- 15:00 **ELISA Project Overview**
  (Philipp Ahmann, ETAS)
- 15:15 **Tools**
  (Matt Kelly, The Boeing Company)
- 15:40 **Open Source Engineering Process**
  (Paul Albertella, Codethink)
- 16:05 **Safety Architecture**
  (Gabriele Paoloni, Red Hat)
- 16:30 **Linux Features for Safety-Critical Systems**
  (Alessandro Carminati, Red Hat)

- 15:00: **Welcome back**
  (Philipp Ahmann, ETAS)
- 15:05: **Systems and Automotive**
  (Philipp Ahmann, ETAS)
- 15:30: **Medical Devices**
  (Kate Stewart, The Linux Foundation)
- 15:55: **Aerospace**
  (Matthew Weber, The Boeing Company)
- 16:20: **Space Grade Linux**
  (Ramon Roche, The Linux Foundation)
- 16:45: **Closing and final thoughts**
  (Philipp Ahmann, ETAS)

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**



“Linux differs from a ‘traditional’ safety critical OS,… but both face challenges in modern complex system setups.”

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
- Real time scheduling
- …

Photo by Jukan Tateisi on Unsplash

Tools + Documentation help to understand complex systems better

- STPA
- strace and csope for workload tracing
- ks-nav (graphical representation kernel sources)
- basil (requirements tracking)
- real-time analysis

Photo by Jukan Tateisi on Unsplash

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!

"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

Photo by Mike Kiev on Unsplash

Premier Members

General Members

Associate Members

Industry Support

ELISA
Enabling Linux in Safety Applications

Technical Strategy Overview

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.

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

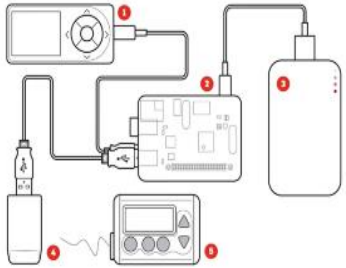
BOEING

Automotive

BOSCH

Medical Devices

THE LINUX FOUNDATION



OpenAPS elements

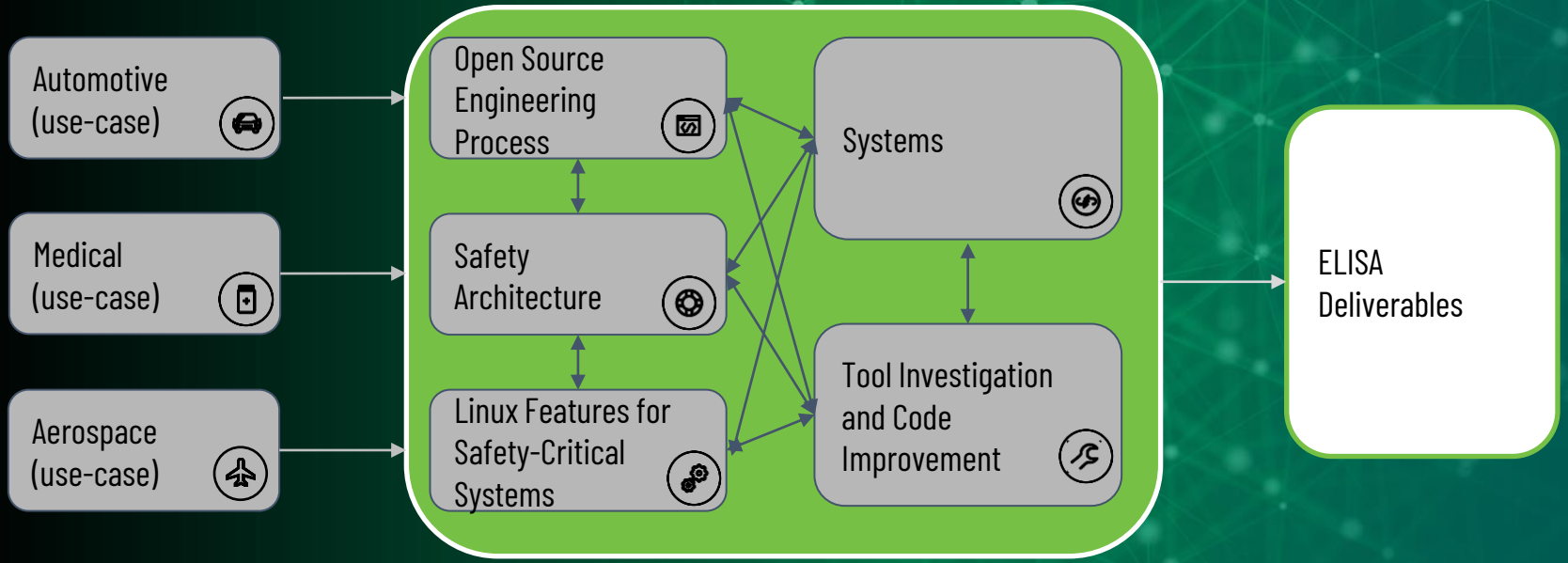
1. Continuous glucose monitor
2. Computer
3. Battery
4. Radio stick
5. Insulin pump

@DanaMLewis

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

ELISA

Enabling Linux in Safety Applications



ELISA Working Groups - Deliverables

- Elements / Software
  - meta-elisa
  - Reproducible system
- Processes
  - STPA
  - Requirements
  - Workload tracing
- Tools
  - ks-nav
  - Basil
  - RT Linux
- Documentation
  - GitHub / Gdrive / Blog / Whitepaper

ELISA
Enabling Linux in Safety Applications

2024 Recap

Photo by Michael Skok on Unsplash

Major (cross WG) achievements

- Welcomed new members and project supporters
- Showcased demonstrator at the Embedded World
- Lead Safe Systems with Linux Micro Conference at Linux Plumbers
- Hosted Safety-Critical-Software Summit at Open Source Summit (again)
- Started the Space Grade Linux SIG
- Hosted 2 in-person workshops & 7 virtual seminars
- Started the „ELISA directory“ as an index for technical content

New members & partners

(Technical University of Hamburg)

Example System at Embedded World

- Based on Xen, Zepyhr, Linux
- Runs on Xilinx ZCU102
- More during Systems WG update

https://elisa.tech/blog/2024/04/09/elisa-project-at-embedded-world/

Safe Systems with Linux MC

- Part of the Linux Plumbers Conference
- Direct exchange with the Linux Kernel community and maintainers
- Closer exchange also with KernelCI
- First steps towards „Requirements inside the kernel“ to manage expecations.

15:00	**Aspects of Dependable Linux Systems**	*Kate Stewart et al.*	
	"Hall N2", Austria Center	15:00 - 15:15	
	Verifying the Conformance of a VirtIO Driver to the VirtIO Specification	*Matias Vara Larsen*	
	"Hall N2", Austria Center	15:15 - 15:45	
	ks-nav	*Alessandro Carminati*	
	"Hall N2", Austria Center	15:45 - 16:00	
16:00	**Source-based code coverage of Linux kernel**	*Wentao Zhang et al.*	
	"Hall N2", Austria Center	16:00 - 16:15	
	BASIL development roadmap	*Luigi Pellecchia*	
	"Hall N2", Austria Center	16:15 - 16:30	
	Break		
	"Hall N2", Austria Center	16:30 - 17:00	
17:00	**Enabling tooling independent exchange of Requirements and other SW Engineering related information with the upcoming SPDX Safety Prof** *Nicole Pappler*		
	Throwing Cinderblocks at Safety Engineering	*Chuck Wolber*	
	"Hall N2", Austria Center	17:25 - 17:50	
	Improving kernel design documentation and involving experts	*Gabriele Paoloni*	
18:00	*"Hall N2", Austria Center*	17:50 - 18:10	
	Discussion of Next Steps	*Kate Stewart et al.*	
	"Hall N2", Austria Center	18:10 - 18:30	

KernelCI

Linux Plumbers Conference
Vienna, Austria | September 18-20, 2024

(Major) Community Engagements

Seminars

- **7 seminars conducted in 2024**
  - Certifying Linux, SEooCs, Making Linux Fly,
  - stressng, cregit, KernelCI, Qualifying Rust compiler
- **Similar amount planned for 2025**
  - Statistical Path Coverage, SDV (cloud & HPC), Formal verification
  - PREEMPT_RT

1 

ELISA Seminar (September 2024) – Meet the New KernelCI
ELISA Project • 239 Aufrufe • vor 5 Monaten

2 

ELISA Seminar (August 2024) –The SEooC concept driven into extreme recording
ELISA Project • 271 Aufrufe • vor 5 Monaten

3 

ELISA Seminar (August 2024) – Cregit: token-level history of Linux
ELISA Project • 111 Aufrufe • vor 5 Monaten

4 

ELISA Seminar (June 2024) Improved system stressing with stress ng
ELISA Project • 338 Aufrufe • vor 7 Monaten

5 

ELISA Seminar (May 2024) Making Linux Fly: Towards Certified Linux Kernel
ELISA Project • 523 Aufrufe • vor 8 Monaten

6 

ELISA Seminar (May 2024): Ferrocene: Qualifying the Rust compiler out in the open
ELISA Project • 291 Aufrufe • vor 9 Monaten

7 

ELISA Seminar (March 2024): Certifying Linux: State of the Art and Lessons Learned after Eight Years
ELISA Project • 506 Aufrufe • vor 10 Monaten

Stay curious how the ELISA journey continues this year!

Photo by Aleksandr Popov on Unsplash

JOIN THE COMMUNITY

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

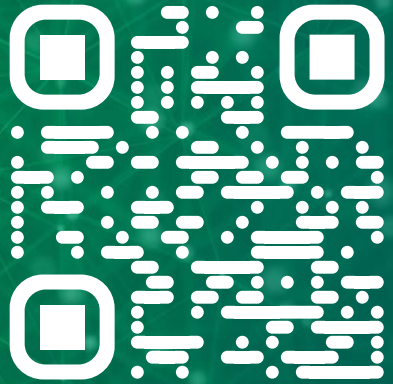
Contribute to Tools and Docs on GitHub

Participate in Working Groups

Attend Events

ELISA
Enabling Linux in Safety Applications

Thank you!



https://elisa.tech