ELISA
Enabling Linux in Safety Applications

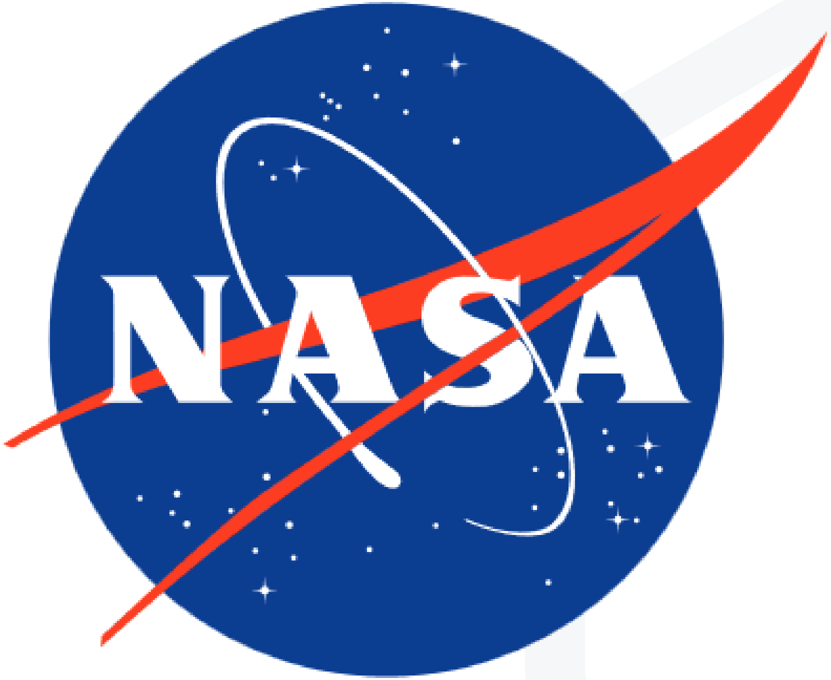
WORKSHOP

NASA Goddard

NASA Goddard Workshop

December 10, 2024

Thank you to our host:



How to access Public Wifi

Network: **Guest-CNE**

Instructions:

1. **Scroll down to Registration**
2. Fill out personal details
3. Sponsor Organization: **587**
4. Submit
5. Check email for password (phone network)
6. Login with username and password details from email
7. Create new password
8. Finish Login
9. Success!

ELISA
Enabling Linux in Safety Applications

WORKSHOP

Welcome

Organizational Overview

- Antitrust Policy
- Licensing of Workshop Results
- Code of Conduct
- Round Table Introductions
- Schedule

Project Orientation

- Mission Statement
- Project Resources
- Technical Strategy Overview

Organizational Notes

ELISA Enabling Linux in Safety Applications

WORKSHOP

LF Antitrust Policy Notice

ELISA Project meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal, or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at ELISA Project meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

Licensing of Workshop Results

All work created during the workshop is licensed under *Creative Commons Attribution 4.0 International* (CC-BY-4.0) [https://creativecommons.org/licenses/by/4.0/] by default, or under another suitable open-source license, e.g., GPL-2.0 for kernel code contributions.

You are free to:

- **Share** — copy and redistribute the material in any medium or format
- **Adapt** — remix, transform, and build upon the material for any purpose, even commercially.

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

ELISA Enabling Linux in Safety Applications

WORKSHOP

Work in Progress - License: CC-BY-4.0

Code of Conduct

All participants are expected to behave in accordance with professional standards, with both the Linux Foundation Code of Conduct as well as their respective employer's policies governing appropriate workplace behavior, and applicable laws.

https://www.linuxfoundation.org/code-of-conduct/

Licensing of Workshop Results

All work created during the workshop is licensed under Creative Commons Attribution 4.0 International (CC-BY-4.0) [https://creativecommons.org/licenses/by/4.0/] by default, or under another suitable open-source license, e.g., GPL-2.0 for kernel code contributions.

You are free to:

- Share — copy and redistribute the material in any medium or format
- Adapt — remix, transform, and build upon the material for any purpose, even commercially.

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Photography & Social Media Notice

IMPORTANT: If you prefer not to have your photo taken or shared on social media, kindly inform the team. We also ask that you avoid appearing in group photos whenever possible. Thank you for your understanding.

Round Table Introductions

Please briefly share:

- Name
- Affiliation
- What made you come to this workshop

Work In Progress - License: CC-BY-4.0

Session Schedule

Schedule – Tuesday December 10 (afternoon)

12:30	ELISA/NASA welcomes and orientations Philipp Ahmann (ETAS), Michael Monaghan (NASA), Ramon Roche (Linux Foundation), Kate Stewart (Linux Foundation)
13:00	NASA tour
15:30	Space Grade Linux Introduction Michael Monaghan (NASA)
16:00	Lessons from Automotive Grade Linux Walt Miner (Linux Foundation)
16:30	Linking external test results to test cases in BASIL to support pre-existing test infrastructure Luigi Pellecchia (Red Hat)
17:00	How to use ks-nav for a feasible and meaningful test campaign in the kernel Alessandro Carminati (Red Hat)
17:30	Space Grade Linux interest survey results Ramon Roche (Linux Foundation), Kate Stewart (Linux Foundation)
18:00	*End of day 1*

ELISA
Enabling Linux in
Safety Applications

WORKSHOP

Schedule – Wednesday December 11 (1/2)

9:00	Verification and validation of the OS and “certification package” Scott Tashakkor (NASA)
9:45	Test and assurance of non-volatile memory devices for space Ted Wilcox (NASA)
10:30	*Break*
10:45	Addressing security topics for future space systems using Linux Joshua Krage (NASA)
11:30	Linux Kernel design documentation Gabriele Paoloni (Red Hat), Kate Stewart (Linux Foundation), Chuck Wolber (Boeing)
12:15-13:15	*Lunch*
13:15	F prime Michael Starch (NASA)
13:45	Space ROS Ivan Perez (NASA)

Schedule – Wednesday December 11 (2/2)

14:15	cFS overview Richard Landau (NASA), Ashok Prajapati (NASA)
14:45	*Break*
15:15	Investigating implementation of Linux-based payload computers: a review of in-orbit demonstrations for Edge AI in space missions Dongshik Won (TelePIX Co., Ltd.)
15:45	Container and immutable patterns for operating systems and wordloads Michael Epley (Red Hat)
16:15	Containerization in space: Podman for mission-critical operations and resilience Douglas Schilling Landgraf (Red Hat), Dan Walsh (Red Hat)
16:45	Wrap up, next steps summary Philipp Ahmann (ETAS), Michael Monaghan (NASA), Ramon Roche(Linux Foundation), Kate Stewart (Linux Foundation)
17:00	*End of day 2*

Schedule – Thursday December 12 (morning)

9:00	Real Time Linux update Steve Rostedt (Google)
10:00	Linux in automotive on safety applications Naresh Ravuri (Magna Electronics)
10:45	*Break*
11:15	Wrap up, next steps summary Presenter: Philipp Ahmann (ETAS), Michael Monaghan (NASA), Ramon Roche (Linux Foundation), Kate Stewart (Linux Foundation)
12:00	*End of day 3 and workshop*

Project Orientation

ELISA
Enabling Linux in
Safety Applications

WORKSHOP

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

> *"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

Linux in Safety Critical Systems

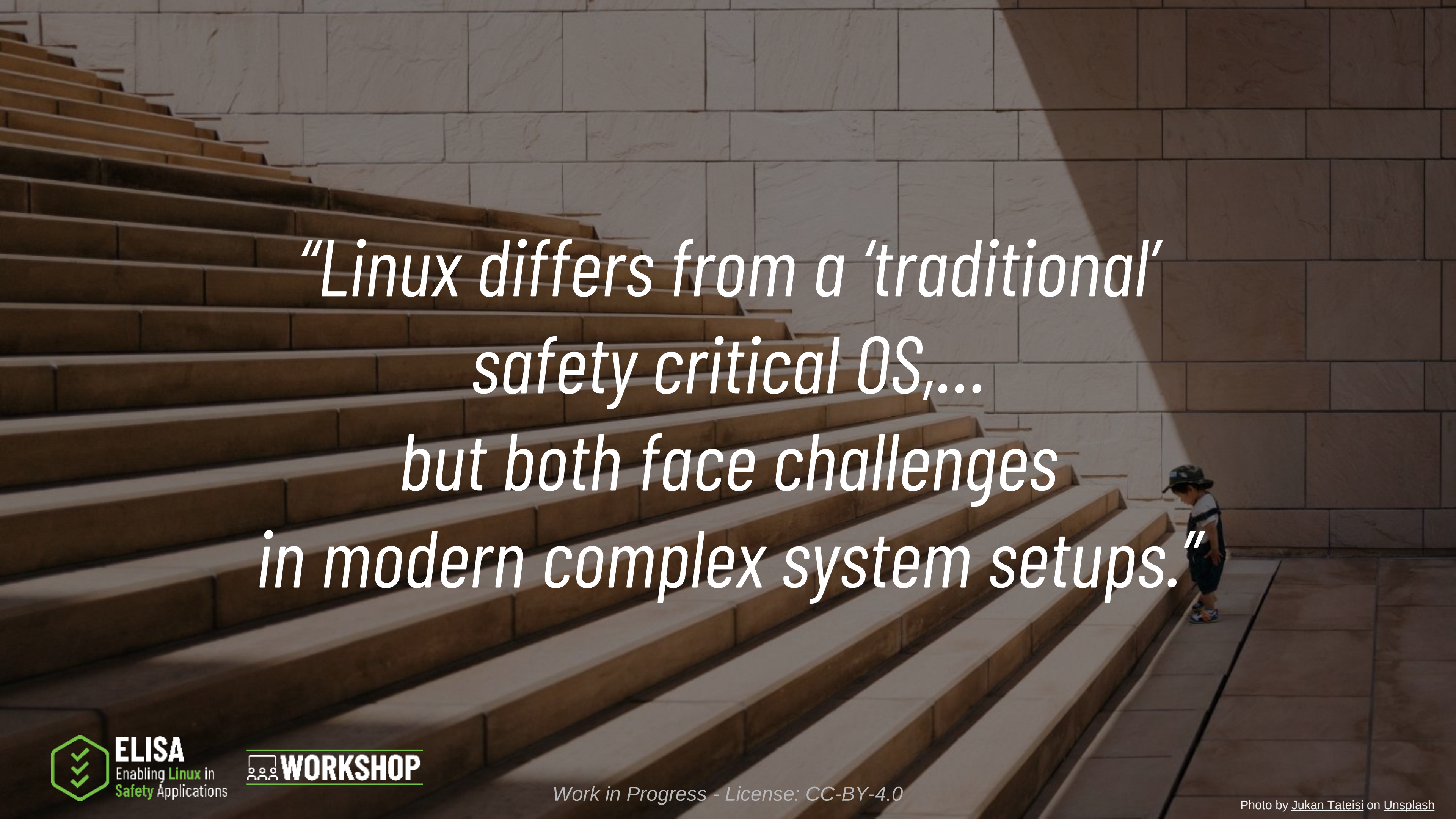
"Assessing whether a system is safe,
requires understanding the system sufficiently."

- 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.

Work In Progress - License CC-BY-4.0



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

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
- Real time scheduling
- …

ELISA Enabling Linux in Safety Applications

WORKSHOP

Photo by Jukan Tateisi on Unsplash

Tools + Documentation help to understand complex systems better

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

ELISA Enabling Linux in Safety Applications

WORKSHOP

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 path forward and peers to collaborate with!

Work In Progress - License: CC-BY-4.0

Premier Members

BOEING

Red Hat

General Members

AISIN

arm

BOSCH

Canonical

Codethink

Elektrobit

EMQ

HONDA
The Power of Dreams

HUAWEI

LINUTRONIX
LINUX FOR INDUSTRY

LYNX
SOFTWARE TECHNOLOGIES

NISSAN
MOTOR CORPORATION

SAIC 上汽集团
SAIC MOTOR

SUSE

WNDRVR

Associate Members

AUTOMOTIVE GRADE LINUX

IFST
INSTITUT FÜR FLUGZEUG-SYSTEMTECHNIK

KernelCI

OTH
OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

Industry Support

CIVIL INFRASTRUCTURE PLATFORM

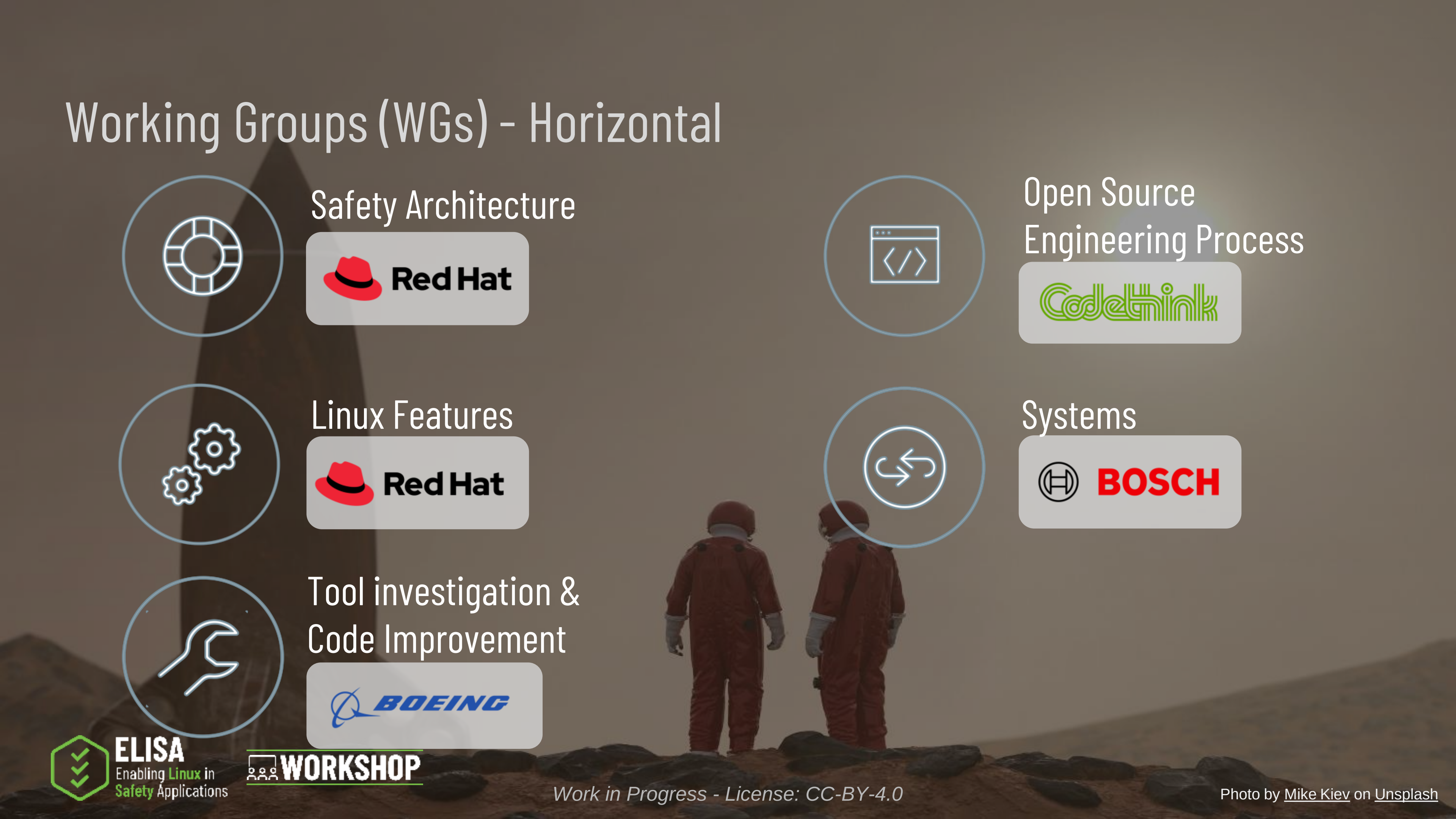
OSADL
Open Source Automation Development Lab eG

UL

Technical Strategy Overview

ELISA Enabling Linux in Safety Applications

WORKSHOP



Working Groups (WGs) - Horizontal

Safety Architecture

Red Hat

Linux Features

Red Hat

Tool investigation & Code Improvement

BOEING

Open Source Engineering Process

Codethink

Systems

BOSCH

Photo by Mike Kiev on Unsplash

Working Groups (WGs) - Verticals

Aerospace

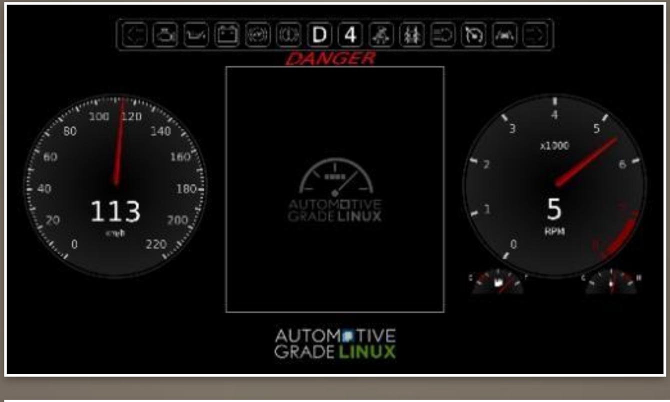
BOEING

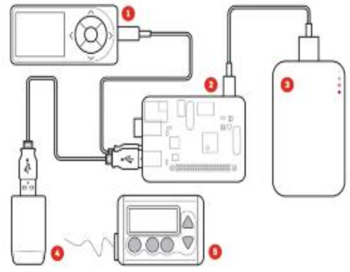
Automotive

BOSCH

Medical Devices

THE LINUX FOUNDATION





OpenAPS elements

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

@DanaMLewis

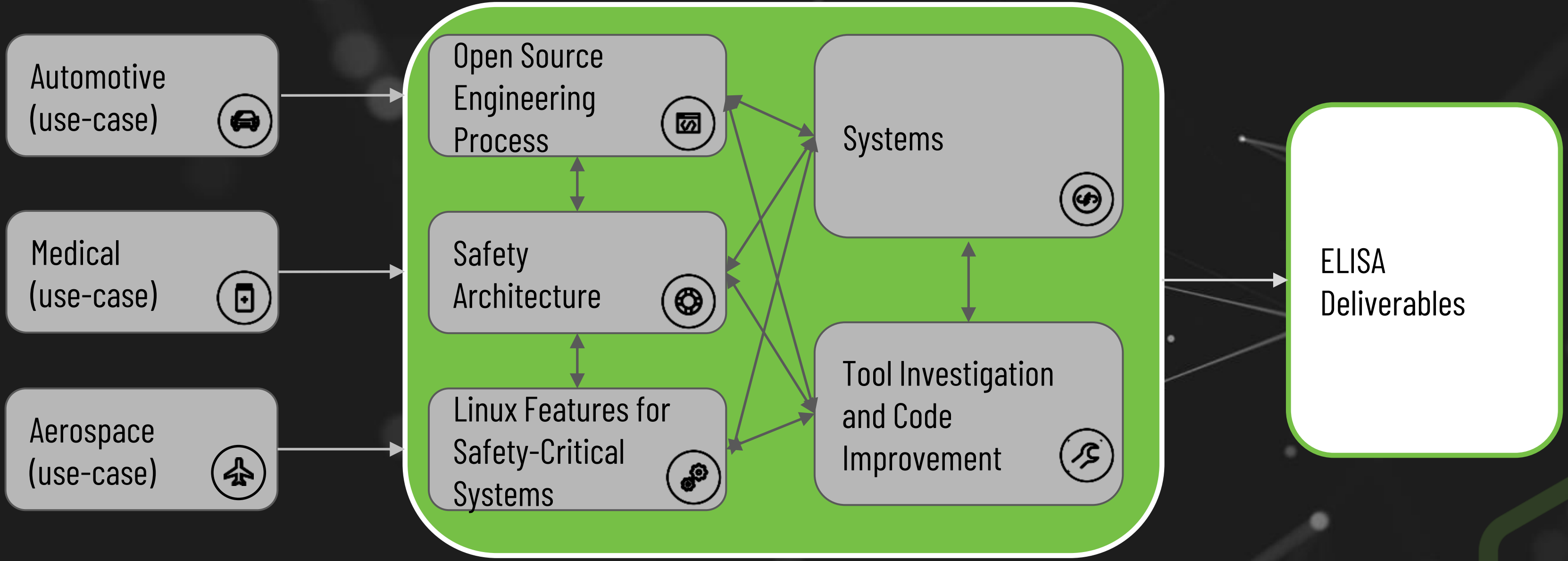
Dana Lewis‘ OpenAPS project: https://youtu.be/kgu-AYSnyZ8

ELISA
Enabling Linux in Safety Applications

WORKSHOP

Photo by Mike Kiev on Unsplash

Artifacts & Activities



Automotive (use-case)

Medical (use-case)

Aerospace (use-case)

Open Source Engineering Process

Safety Architecture

Linux Features for Safety-Critical Systems

Systems

Tool Investigation and Code Improvement

ELISA Deliverables

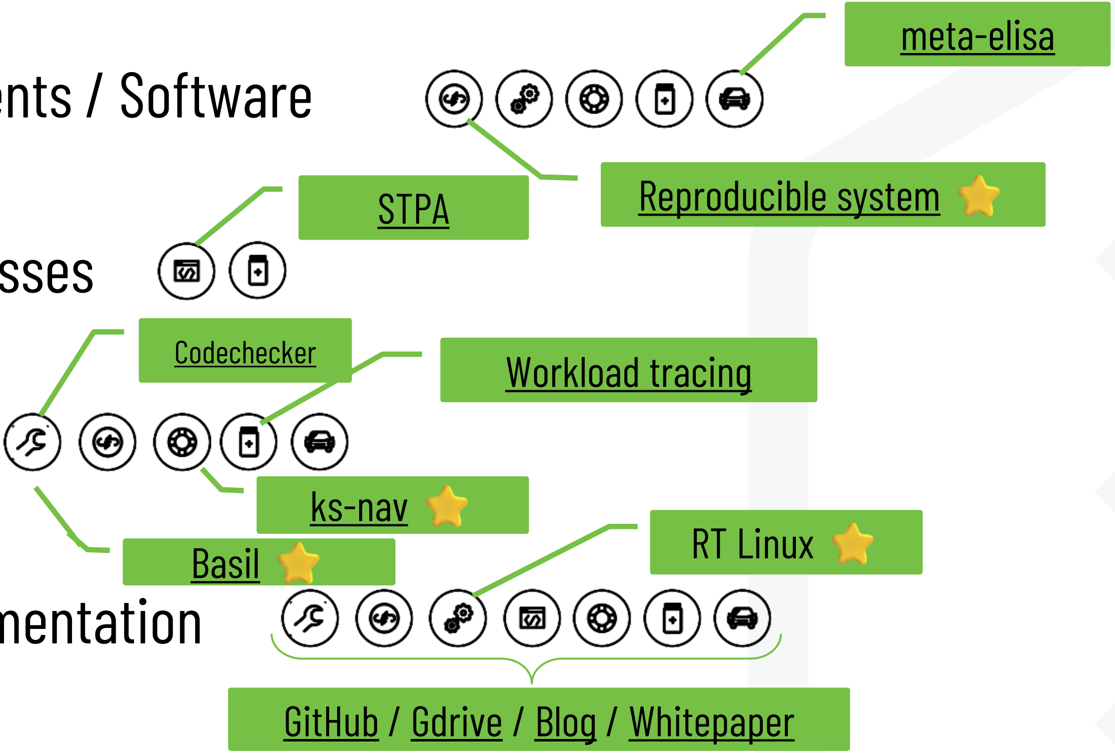
ELISA Enabling Linux in Safety Applications

WORKSHOP

⭐ : part of workshop

ELISA Working Groups - Deliverables

- Elements / Software
- Processes
- Tools
- Documentation



meta-elisa

Reproducible system ⭐

STPA

Codechecker

Workload tracing

ks-nav ⭐

Basil ⭐

RT Linux ⭐

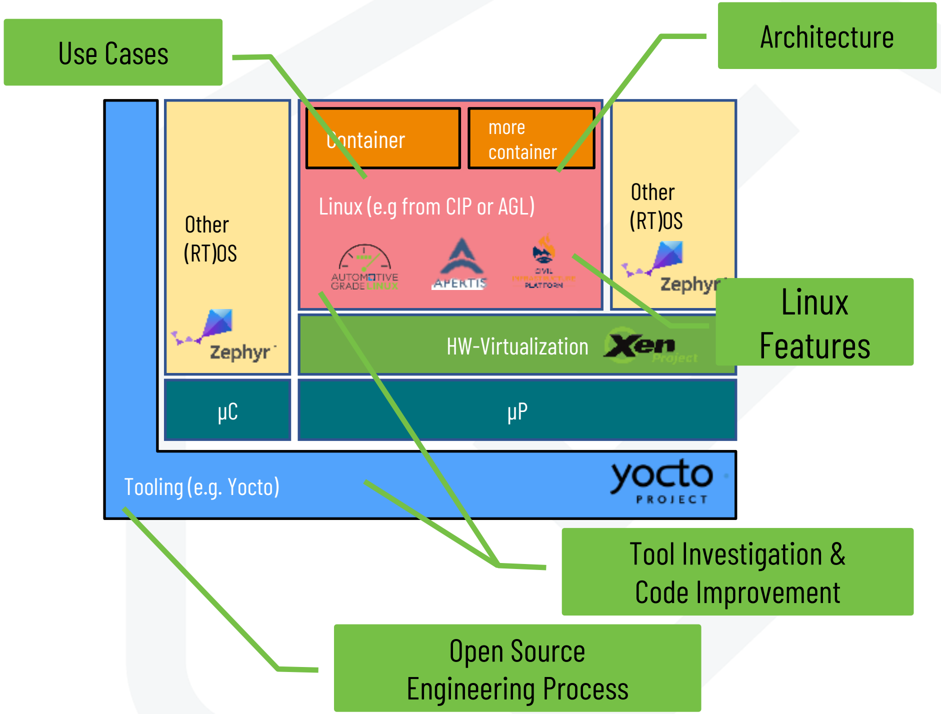
GitHub / Gdrive / Blog / Whitepaper

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 interactions across the communities

- Open source projects focusing on safety-critical analysis

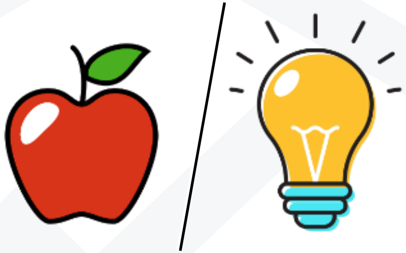
Xen Project   Zephyr™

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

AUTOMOTIVE GRADE LINUX   SOAFEE   SDV Eclipse Software Defined Vehicle™

- Further community interactions

yocto PROJECT   SPDX   KernelCI   linaro



"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

Community challenges for all projects

- Bring the argument of „OSS is not behaving 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

Work in Progress - License: CC-BY-4.0

Recommendations for new contributors

- Just show up – All presented projects are open for the adaptation of new use cases, input, domain-specific working groups etc.
- Share Safety Best Practice: Functional and structural expectations of the component used in the context of the entire system
- Become an OSS evangelist: Open source can already be used in a variety of safety contexts. Knowledge of the actual structure and potential is very scarce in the field of assessors, notified bodies and related authorities.

Work In Progress - License CC-BY-4.0

Getting involved with ELISA

https://elisa.tech

https://github.com/elisa-tech

https://lists.elisa.tech

https://www.youtube.com/@elisaproject8453

Work In Progress - License: CC-BY-4.0

Put on your thinking hats and get to work!

Photo by Annie Spratt on Unsplash

Licensing of Workshop Results

All work created during the workshop is licensed under Creative Commons Attribution 4.0 International (CC-BY-4.0) [https://creativecommons.org/licenses/by/4.0/] by default, or under another suitable open-source license, e.g., GPL-2.0 for kernel code contributions.

You are free to:

- Share — copy and redistribute the material in any medium or format
- Adapt — remix, transform, and build upon the material for any purpose, even commercially.

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.