ELISA

Enabling Linux in Safety Applications

Safety-Critical Linux BOF: Challenges across industries

By Kate Stewart, Susan Remmert, Philipp Ahmann

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

BOF Proposal

Linux is being used more often in safety-critical areas like cars, planes, medical devices, robots, and trains.

But each industry faces similar challenges when trying to meet safety and certification requirements.

This BoF is an open discussion about those real-world problems: timing and determinism, documentation, certification, tooling, and system design.

Anyone interested in safety-critical Linux is welcome to join, share experiences, ask questions, and explore where collaboration could help.

ELISA
Enabling Linux in Safety Applications

What is Functional Safety?

Definition of Safety

The freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly because of damage to property or the environment.

Definition of Functional Safety

The part of safety that depends on a system or equipment operating correctly in response to its inputs. Detecting potentially dangerous conditions, resulting either in the activation of a protective or corrective device or mechanism to prevent hazardous events or in providing mitigation measures to reduce the consequences of the hazardous event.

ELISA
Enabling Linux in Safety Applications

In Functional Safety you expect:

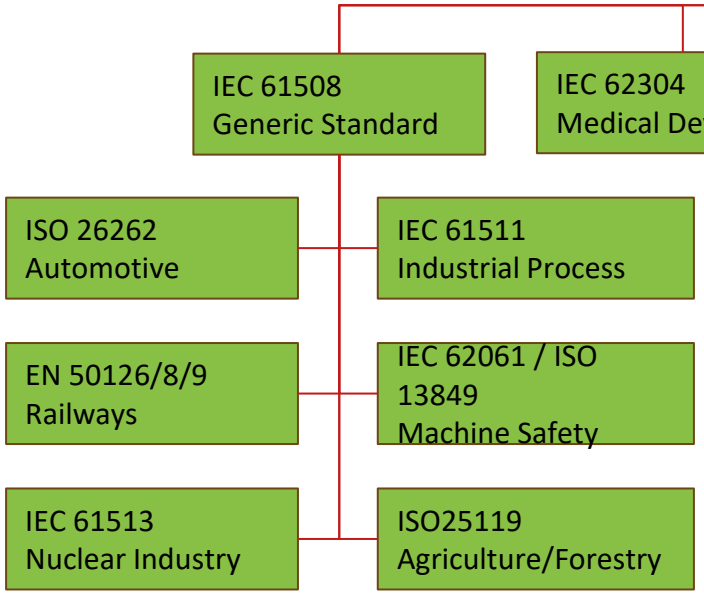
That the software:

- does behave as specified,
- does not interfere or impair other system components
- and all possible erroneous events are addressed somehow or somewhere.

And you have sufficient evidence to prove this.

ELISA
Enabling Linux in Safety Applications

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

ELISA
Enabling Linux in Safety Applications

Demands by standards to increase system quality

- Requirements
- Testing
- Documentation
- Traceability

ELISA
Enabling Linux in Safety Applications

Collaborative editing

https://semestriel.framapad.org/p/fosdem-elisa-bof

Copy QR code and participate in making notes and share your thoughts.

ELISA
Enabling Linux in Safety Applications