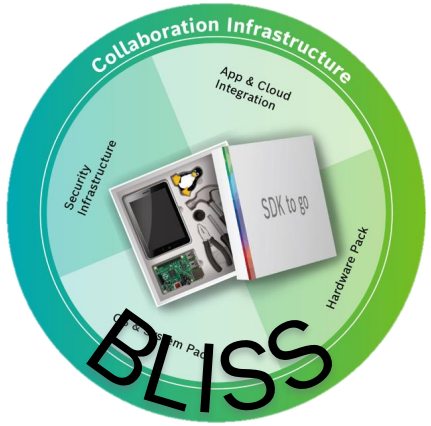
LUND LINUX CON
MAY 12-13, 2022

APERTIS & ELISA
PHILIPP AHMANN

Intro and agenda

- **`whoami`**
  - Technical Business Development Manager for (Linux related) Open-Source topics in Bosch
  - TSC member and ambassador of the Linux Foundation ELISA project
- Here to talk about...

APERTIS



ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

BOSCH

APERTIS is a part of **BLISS**
Bosch Linux IoT Service System…

… helps any developer translating innovative ideas into smart products.

a solution for distributed, reliable, and secure AIoT systems, offering a dedicated Linux environment for industrial applications as well as possibilities for seamless integration of heterogeneous edge devices.

APERTIS

All information availalbe at: www.APERTIS.org

... Free and open source, GNU/Linux-based distribution for infotainment in automotive vehicles, with focus on security and modularity.

- debian derivative tailored for automotive needs
- Fit for a wide variety of electronic devices
- Product-specific images for ARM and Intel x86
- Beyond operating system, it offers frameworks, new APIs, cloud services, SDK, ...

BOSCH

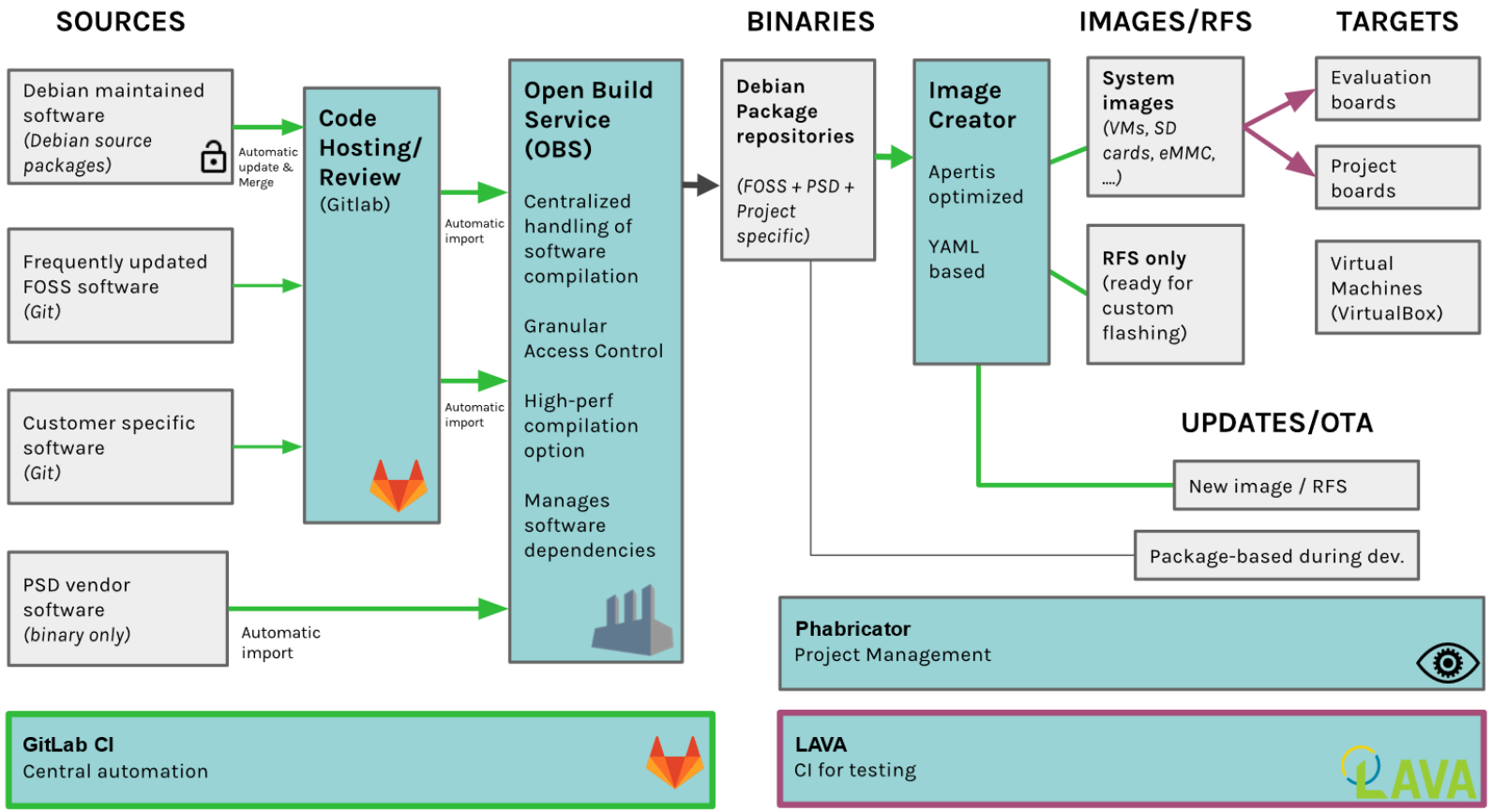
APERTIS
… not only Automotive

APERTIS gaining momentum in various application fields.

Currently enhancing Apertis into a wider AIoT software service eco system of “BLISS”

BOSCH

APERTIS
From source to update



- CI/CT toolchain & SDK for faster product ramp up
- Cross compilation
- Over the air update (package manager for develoment mainly)
- Integration of customer specific software, FOSS packages, Binaries

BLISS OSS engagements

BOSCH

ELISA overview & strategy

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

ELISA

The Enabling Linux in Safety-Critical Applications (ELISA) project has taken on the challenge to make it easier for companies to build and certify Linux-based safety-critical applications.

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

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.

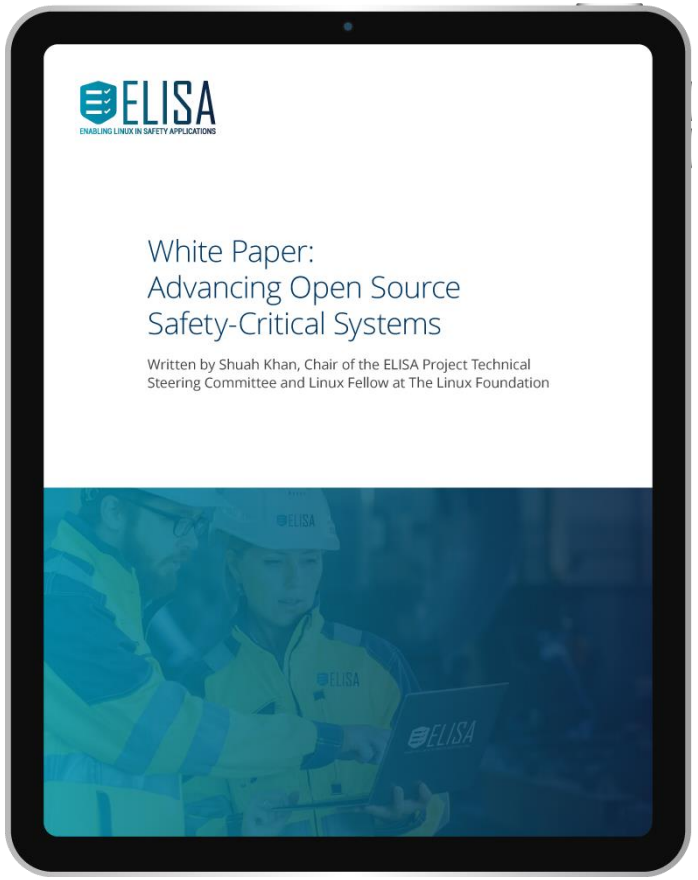
Selecting Linux c**omponents and features** that can be evaluated for safety

Identifying **gaps that exist** where more work is needed to evaluate safety sufficiently.

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

ELISA Mission Statement

Define and maintain a common set of elements, processes and tools that can be incorporated into specific Linux-based, safety-critical systems amenable to safety certification.



Read ELISA Technical Strategy White Paper

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

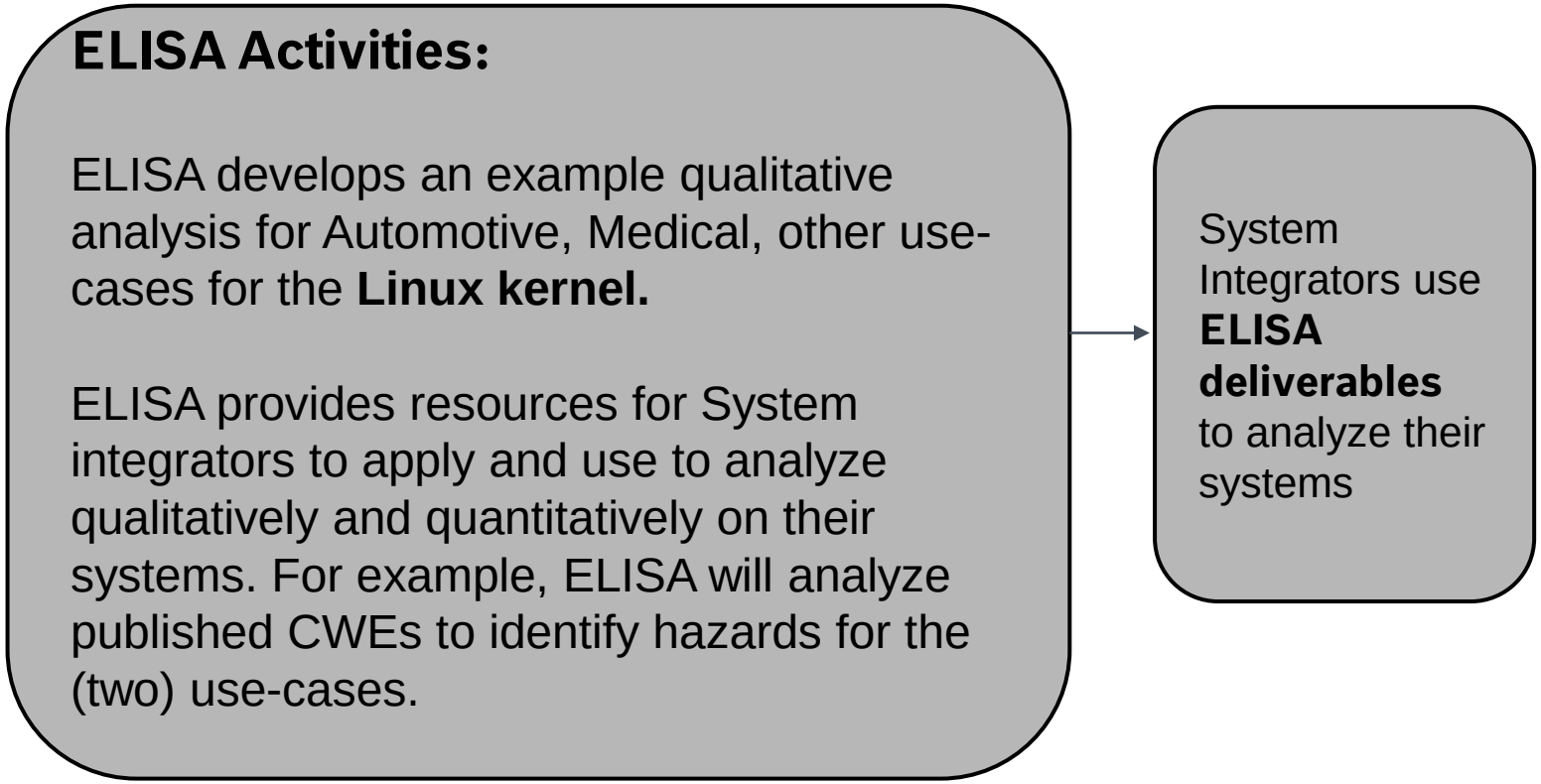
Understanding the Limits

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 (Remember the continuous process improvement argument!)
- *cannot relieve* you from your responsibilities, legal obligations and liabilities.

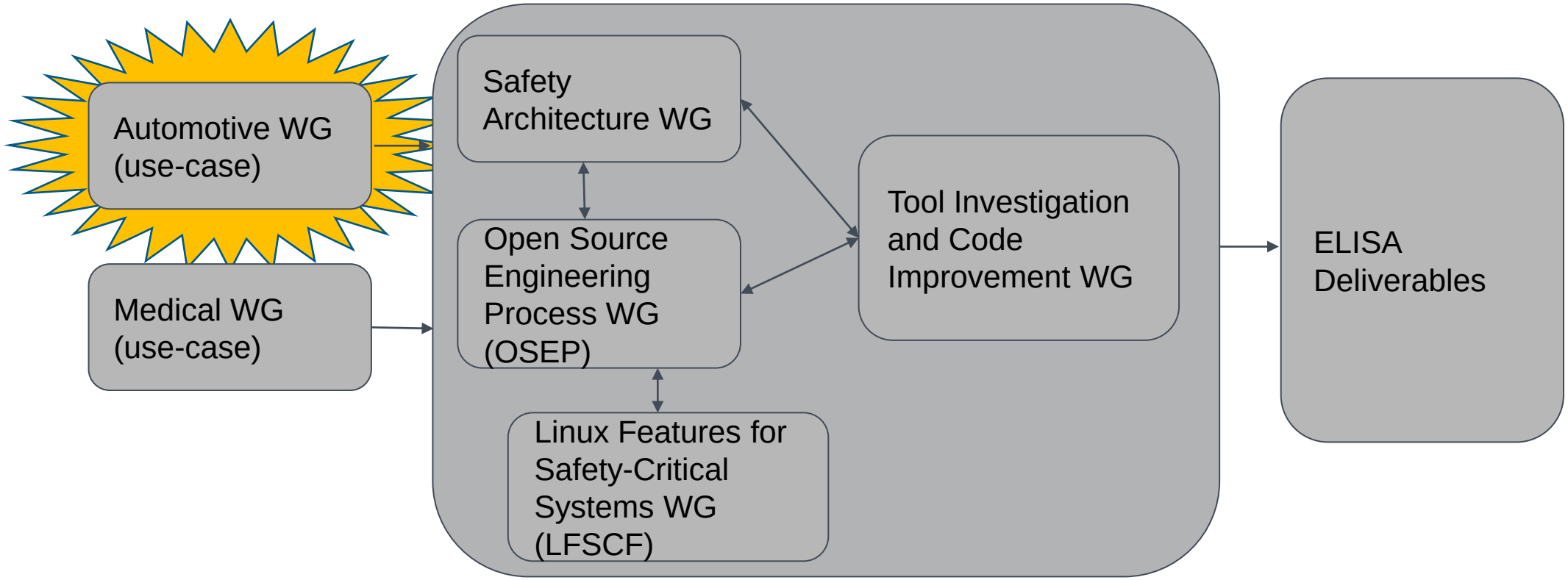
But it we are able to provide a **path forward** and peers to **collaborate** with!

ELISA Technical Strategy



ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

Technical Strategy - WGs



ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

ELISA Work Groups (extract)

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

Tool Investigation and Code Improvement WG

"focus on application of tools and handling the tool results, improving the kernel based on the tools' feedback."

- Fuzzing with syzkaller: see https://syzkaller.elisa.tech/
- Codechecker continuous assessment of dead stores: see https://codechecker.elisa.tech/
  - Sending patches and raising issues with developers
- Identified improvements with Codechecker itself
  - Got one patch merged upstream to prevent some reports from being left out so far: see https://github.com/Ericsson/codechecker/pull/3588/files
- Support kernel development newcomers to contribute to kernel development
- Kernel Documentation cleanup
  - Going through kernel documentation section 'Working with the kernel development community', looking for improvements and writing short summaries
  - E.g. providing rationale of checks in https://www.kernel.org/doc/html/latest/dev-tools/checkpatch.html
- Work group with largest impact on the actual kernel development within ELISA!

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

Linux Features for Safety-Critical Systems WG

“Deep dive into specific kernel features
and their potential value to support safety goals”

- Memory management, kernel configurations with potential value to support safety of various memory types (kernel/user space, heap/stack).
- Deep understanding of Linux stack management (kernel/user) and possible failure modes.
- Virtual memory management, a joint investigation with RedHat, Safety Architecture WG, and Open Source Engineering Process WG.
- Work on Kernel Configurations for safety draft and preparation for publication.
- Discuss possible extensions to cloud based systems.

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

Open Source Engineering Process (OSEP) goals and approach

Develop overall approach to safety processes for systems using Linux

- Linux development practices do not map to ‘reference process’ of safety standards
- How can FOSS developers and product creators provide equivalent confidence?

Current approach based on use of System Theoretic Process Analysis (STPA)

- Top-down analysis methodology developed by MIT
- Use this to identify and analyse responsibilities of FOSS in a safety-related system
- Derive functional and safety requirements to inform verification strategies

Applying the approach to specific ‘topics’ for Linux

- Currently focusing on Address Space Integrity
- Collaborating with LFSCS and Safety Architecture working groups

Software Architecture WG

Telltale Safety Analysis:

- Analysis of the Kernel properties supporting the integrity of user mode address spaces as well as kernel mode address spaces.
- Pull request to document it in github, more extensive & generic investigation and analysis have been passed over to the LFSCS and OSEP WGs respectively
- Introduced the role of RV (Runtime Verification) Monitors as FuSa components, explaining the currently proposed RFC and its use for eventual safety claims

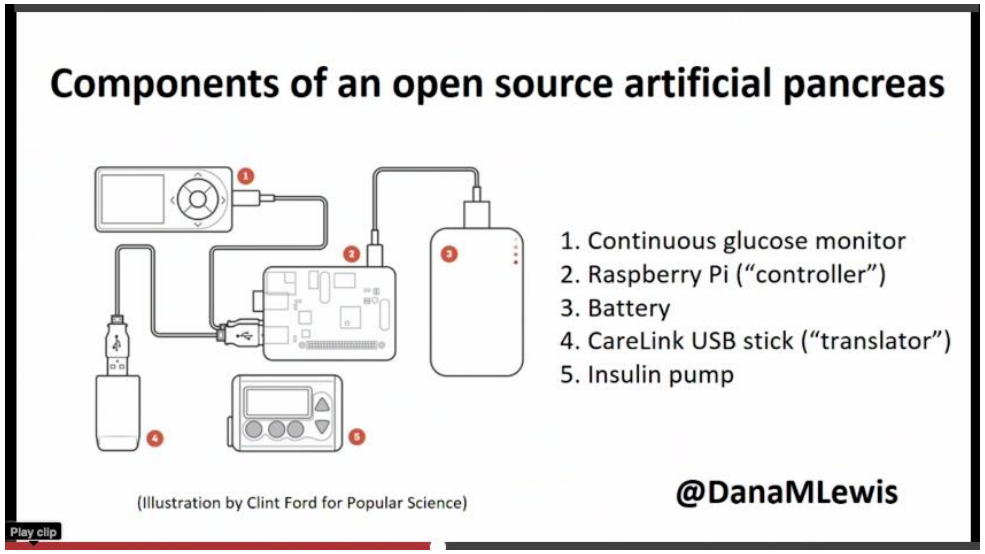
Next Steps

- Analyse the role of the Watchdog RV Monitor in eventual Kernel claims
- Refine the analysis of the Kernel properties supporting the integrity of the user mode and kernel mode address space of the telltale safety app
- Continue the Kernel FFI analysis

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

Medical Devices WG

STPA on OpenAPS - Linux in a medical device



ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

Medical Devices WG

Current State:

- Progressing the work on collecting information for L3 STPA analysis (Raspbian interface to kernel)
  - Collecting traces of activities through the kernel when stimulated by various openAPS key tasks identified during prior analysis.
  - Mentee working with team during the spring to improve the tracing information
- OpenAPS L1 & L2 Requirements generation and then STPA analysis update
- Review of artifacts generated to date to determine structure for publishing

Next Steps:

- Complete publishing of analysis on L1 & L2 analysis github, and submit for TSC review.

Automotive WG

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

Automotive Members (Apr 2022)

https://elisa.tech/membership/members/

BMW GROUP
BMW Car IT

TOYOTA

LOTUS NYO

ADIT

AISIN

斑马智行
Powered by AliOS

SAIC 上汽集团 SAIC MOTOR

Elektrobit

AICC 国汽智控

AUTOMOTIVE GRADE LINUX

SUZUKI

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

Mission Statement

The automotive workgroup discusses the conditions and prerequisites the automotive sector needs to integrate Linux into a safety critical system.

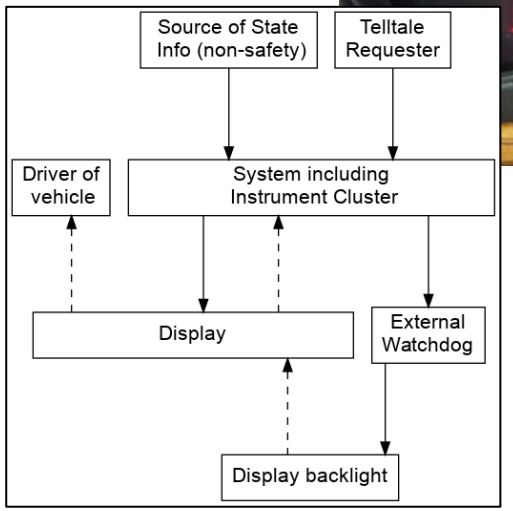
We focus on actual use cases from the Automotive domain to derive the technical requirements to the kernel and the development process as a basis for investigation within the Architecture Workgroup and OSEP to serve as a blueprint for actual projects in the future.

Our output (safety concepts and other material) is stored and maintained in the workgroup repository. Our close collaboration with AGL results in a meta-elisa layer enhancing the instrument cluster demo for safety relevant parts.

ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

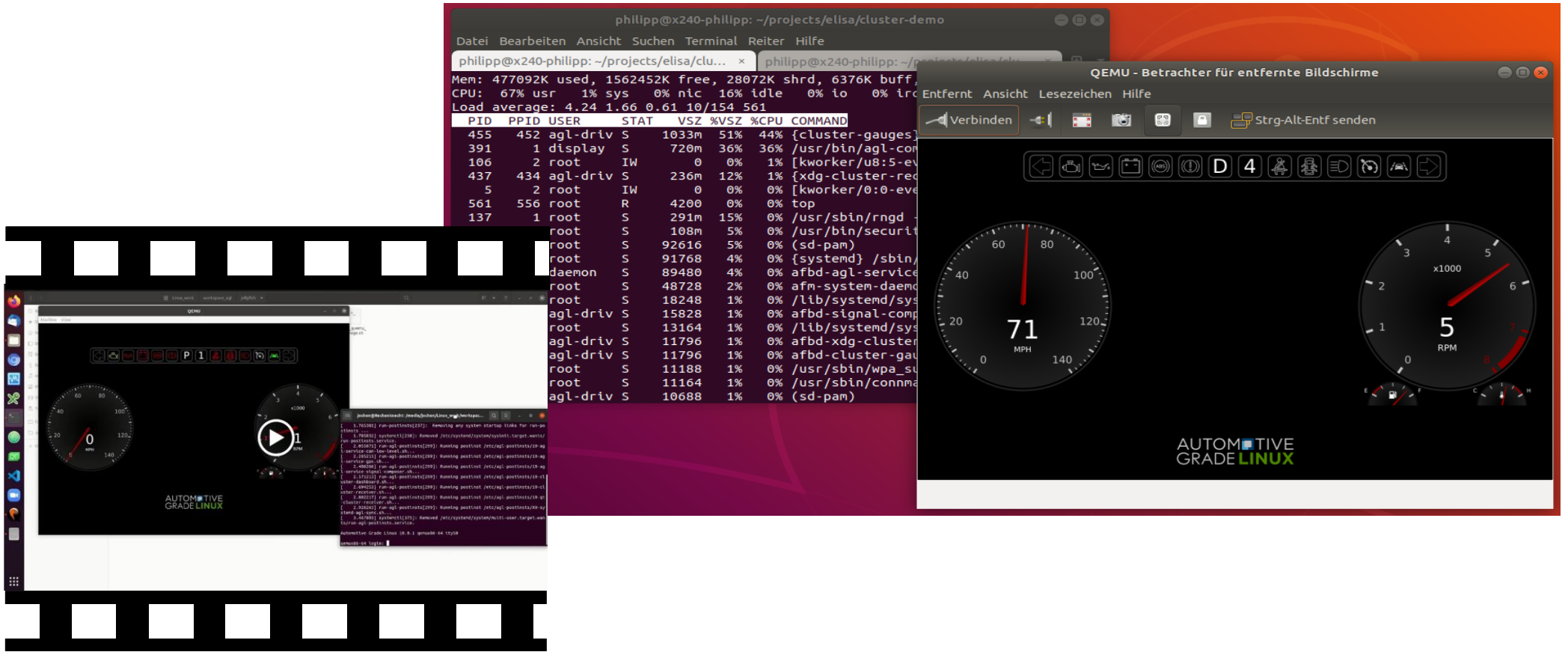
Telltale Use Case

- Typically, ASIL B
- Relaxed timing requirements (reaction time in range of >100ms)
- Interesting for OEMs/Tier1s and an opportunity to cooperate with AGL
- AGL reference HW and telltale demo can be used as starting point
- Mass market use case



ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

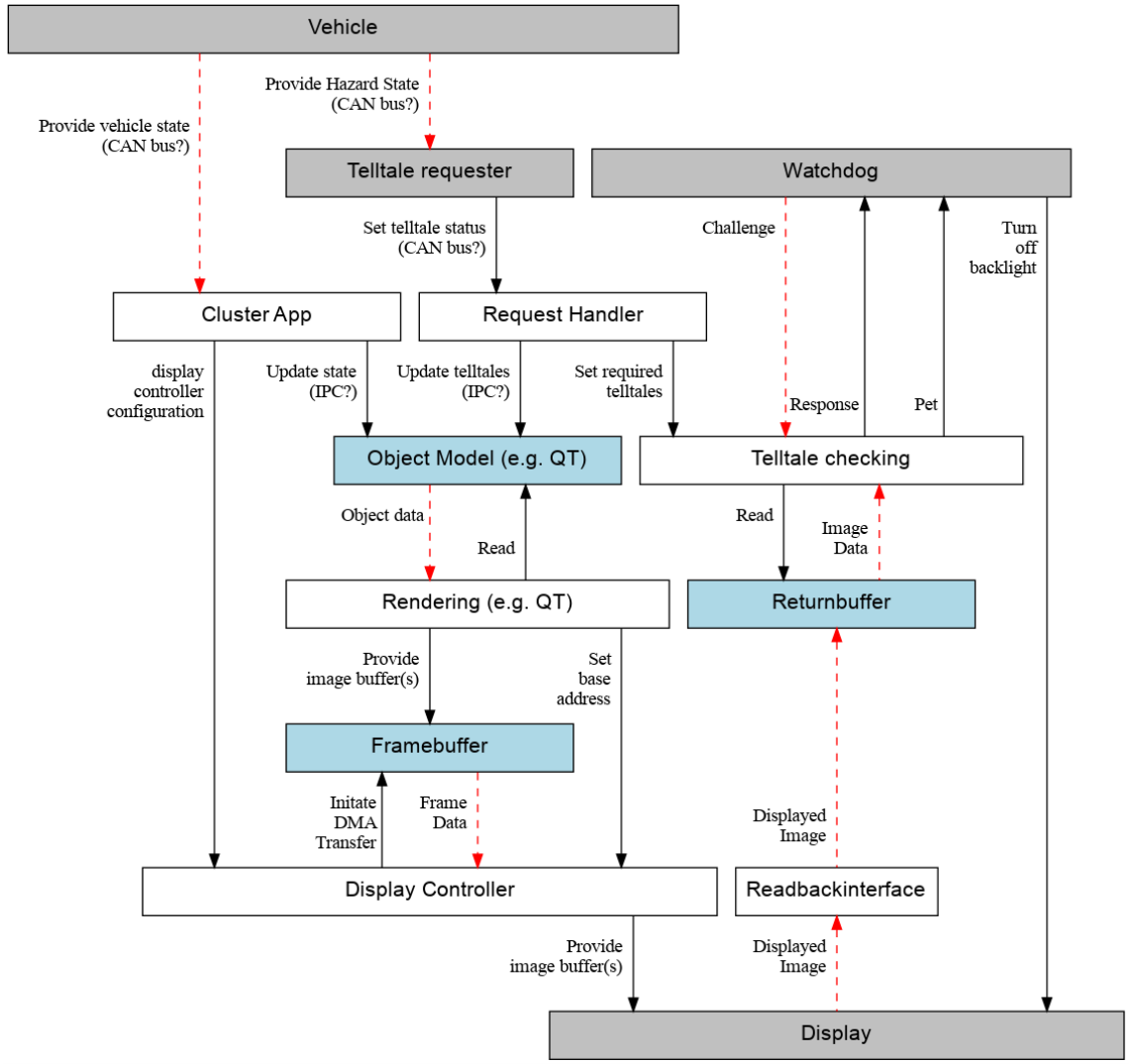
AGL qemu based instrument cluster demo



ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

Current Activities

- STPA Analysis of the telltale use case
- Demo development
  (i.e. kernel config trim down)
- Github based contribution process
  (roll out to other work groups)



ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

Planned Activities

- Continue STPA for the telltale use case.
- Map the STPA results to fit the AGL demo.
- Align with Medical Devices WG on STPA work.
- Further tailoring of AGL instrument cluster demo.
  - Update to latest AGL version.
  - Bring it on hardware.
- **Stronger outreach on other events to find new contributing partners.**

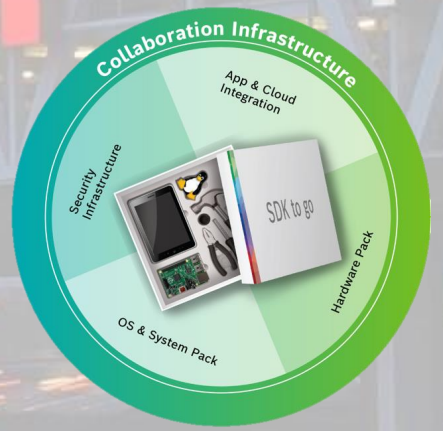
Automotive WG Resources

- Mailing list
  - https://lists.elisa.tech/g/automotive (~150 members)
  - Subscribe: automotive+subscribe@lists.elisa.tech
- Meeting minutes
  - https://docs.google.com/document/d/1qgEkB6HBjq0ojoTSmI_E18BZco3lORK1ZZDrBH1YQo0/
  - Zoom meeting (currently Fridays 12:00 UTC). Link: 95424105908
- Documentation repo.
  - https://github.com/elisa-tech/wg-automotive
  - https://github.com/elisa-tech/wg-automotive/tree/master/Cluster_Display_Use_Case_v2/stpa (STPA analysis entry point)
- Main source/Code repos.
  - https://github.com/elisa-tech/meta-elisa
  - https://github.com/Jochen-Kall/Safety_concept_tool

Interested in BLISS, APERTIS or ELISA?
Just get in touch with me.
Thank you.

Philipp.Ahmann@bosch.com

APERTIS



ELISA
ENABLING LINUX IN SAFETY APPLICATIONS

BOSCH