



AUTOMOTIVE
LINUX SUMMIT



THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
JAPAN

Elements towards functional safety use cases with Linux in Automotive

Philipp Ahmann, Robert Bosch GmbH

#ossummit

@ProjectElisa

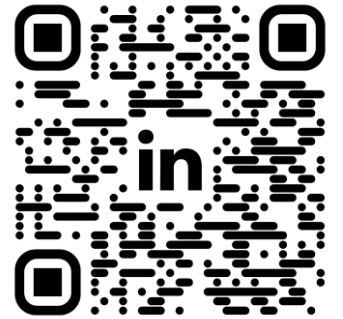




Embedded IoT Linux@Bosch



- **Technical business development manager for embedded open source - Robert Bosch GmbH**
- **Technical Steering Committee Chair & WG Lead - LF's ELISA project**
- **15 years+ Linux user (and open source enthusiast)**
- **10 years+ Linux in Automotive (mainly in field of infotainment)**





Linux in Safety Critical Systems

*“Assessing whether a system is safe,
requires understanding the system sufficiently.”*

Linux in Safety Critical Systems

*Understand Linux within that system context
and how Linux is used in that system.*

Linux in Safety Critical Systems

*Select Linux components and features
that can be evaluated for safety.*

Linux in Safety Critical Systems

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

Challenges: Linux in Safety Critical Systems

The Linux kernel has:

- Large Development Ecosystem
- Security Capabilities
- Multi-Core Support
- Unmatched Hardware Support
- Many Linux Experts at all levels available

Traditional safety-critical OS has:

- Hard Real-time Capabilities
- Proven Safety-compliant Development Process
- ...

Can these differences be tackled?

Premier
Members



BOEING

intel®



Red Hat

TOYOTA

General
Members

ADIT



AISIN

arm



斑马智行
Powered by AliOS



BOSCH



Elektrobit



地平线
Horizon Robotics



LINUTRONIX
LINUX FOR INDUSTRY



上汽集团
SAIC MOTOR



WINDRVR



XPENG

ZTE

Associate
Members



OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

Industry
Support



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...

ELISA provides a path forward and peers to collaborate 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.”



“The scope of the project includes software and documentation development under an OSI-approved license supporting the mission, including documentation, testing, integration and the creation of other artifacts that aid the development, deployment, operation or adoption of the project.”



from the [technical charter](#)

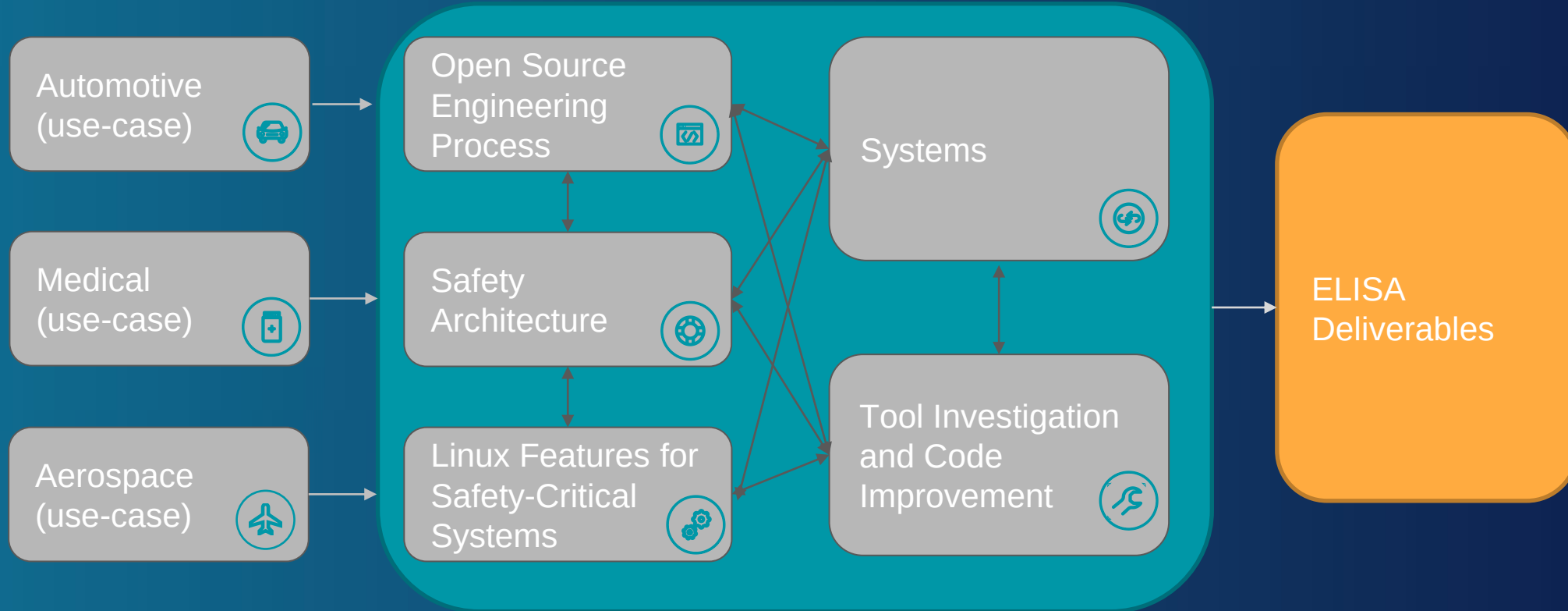
ELISA Working group focus (based on mission)

- Elements / Software
- Processes
- Tools
- Documentation

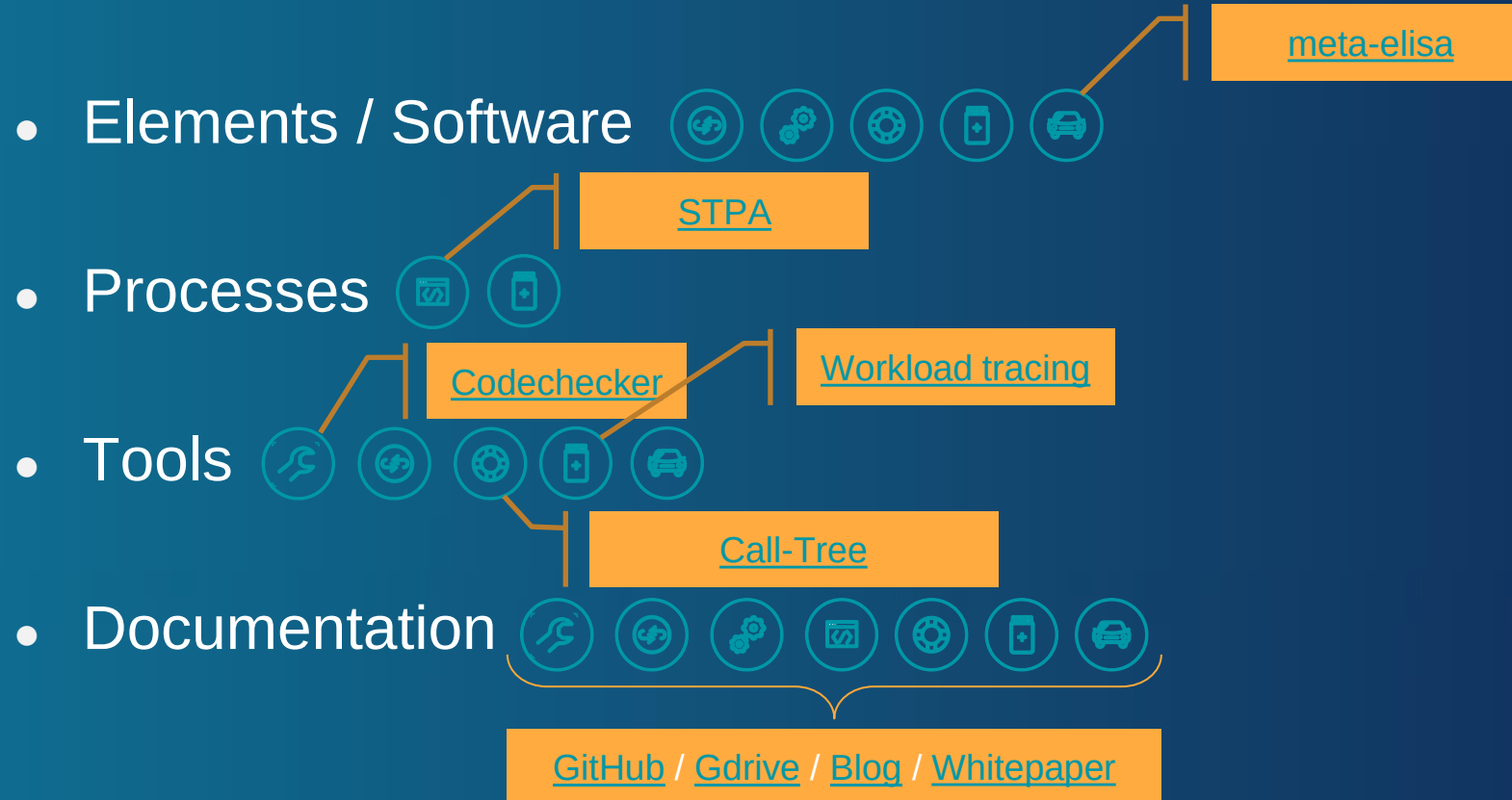
Working groups in(ter)action



ELISA - Working Groups (WGs)



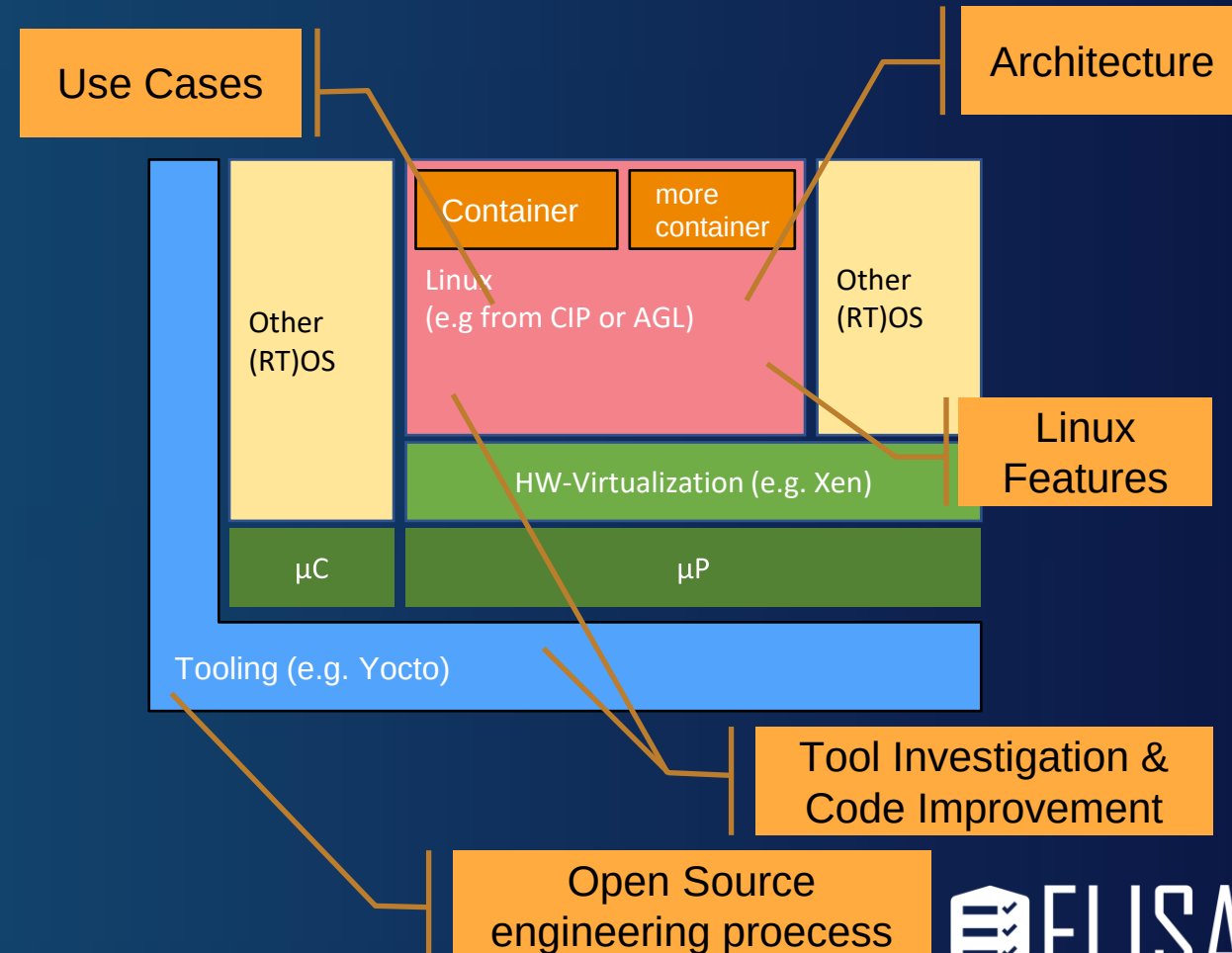
ELISA Working group focus (based on mission)





ELISA working groups fit in a reference 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 working groups fit in a reference system



ELISA MINI SUMMIT



WEDNESDAY, DECEMBER 7 | 9:00 – 12:30

Location: Room 315 (3F)

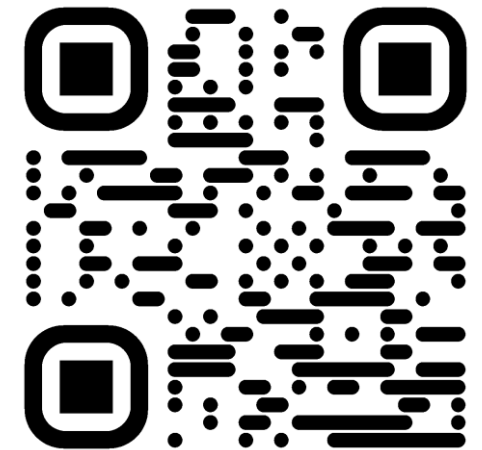
Registration Cost: \$10

Enabling Linux in Safety Applications (ELISA) aims to create a shared set of tools and processes to help companies build and certify Linux-based safety-critical applications and systems whose failure could result in the loss of human life, significant property or environmental damage.

ELISA Mini Summit Speakers:

- Kate Stewart, VP, Dependable Embedded Systems, Linux Foundation
- Philipp Ahmann, Product Manager, Robert Bosch GmbH

REGISTER TODAY!



engineering process





Interact with other communities (outside of ELISA)

- Safety-critical open source projects



- Identified OSS project with safety-critical relevance and comparable system architecture considerations



SOAFEE



“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

Interact with other communities (outside of ELISA)



KEYNOTE

Tuesday, December 6 • 10:00am - 10:20am



Keynote: Kate Stewart, Vice President of Dependable Embedded Systems, The Linux Foundation

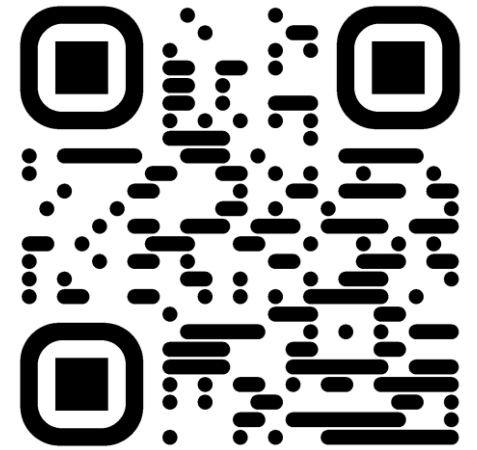
Speakers



Kate Stewart

Vice President of Dependable Embedded Systems, The Linux Foundation

ADD TO SCHED!



ELISA Automotive WG – dashboard warning sign use case



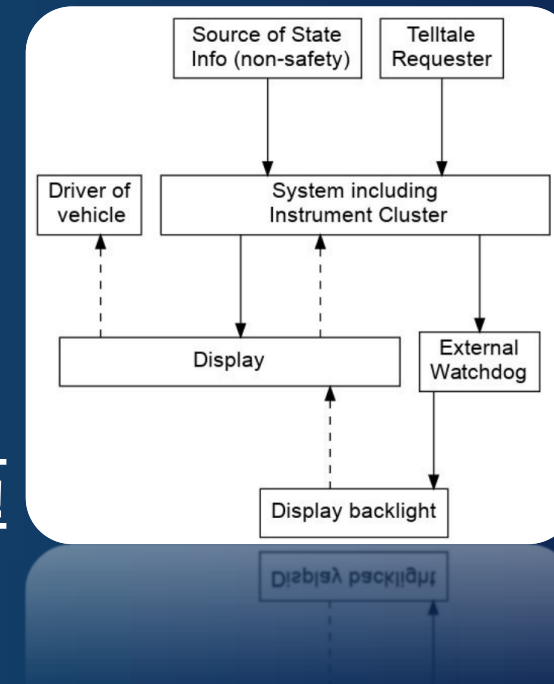
- Mechanical dashboards and LED based safety related warning signs (tell tales) turn into pure display solutions implemented in the OS.
- A use case to derive safety requirements.
- Tell tales don't involve complex sensor/actuator setups.
- Relaxed timing constraints.
- Relatively easy to understand.
- Basic challenges representative for more complex use cases.



Use case benefits

- **Limited subsystems & components.**
(compared to driver assistance use cases)
- **Fairly simple high-level system diagram.**
- **Relaxed timing constraints.**
(Driver reaction time longer than display timing)
- **System level architecture can scale to different hardware and software architectures.**
- **Can increase safety demands to the Kernel step by step.**
- **Good to visualize and explain to others.**
- **Moderate safety integrity level.**
(typically, ASIL A or B)
- **Sample implementations exist e.g. from AGL (though without safety in mind).**

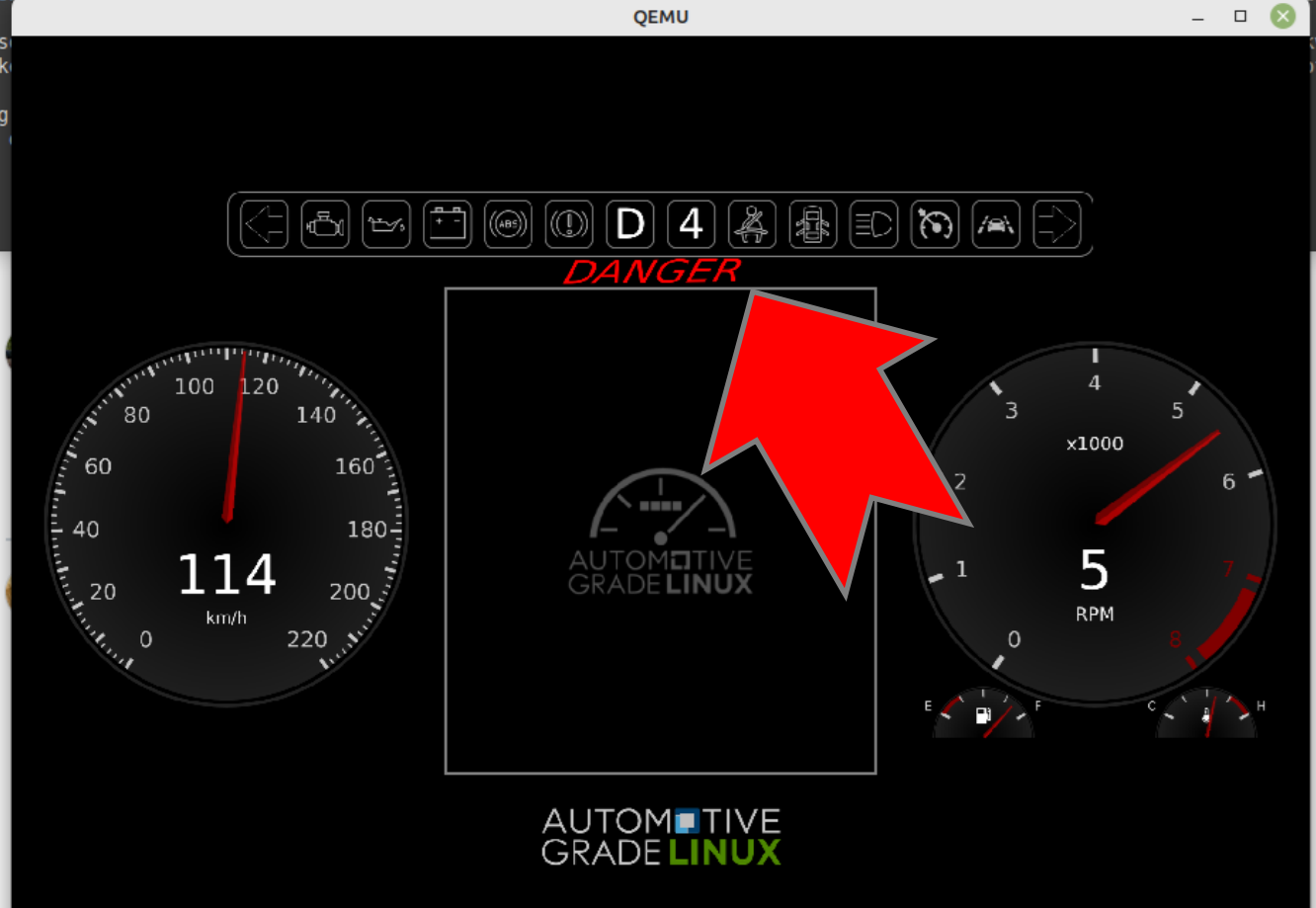
**A way forward towards driver assistance
and other advanced use cases!**



Instrument cluster enhancements

```
philipp@GB-BER7-philipp:~/projects/agl/needlefish$ qemu-system-x86_64 -snapshot -device virtio-net-pci,netdev=net0,mac=52:54:00:12:35:02 -watchdog i6300esb -netdev user,id=net0,hostfwd=tcp::2222-:22,hostfwd=tcp::2323-:23
sb-tablet -device virtio-rng-pci -vga virtio -smp 4 -m 2048 -serial mon:stdio -serial null -k
onsole=ttyS0,115200n8 quiet '
qemu-system-x86_64: -watchdog i6300esb: warning
qemu-system-x86_64: warning: '-soundhw hda' is
Automotive Grade Linux 14.0.1 qemux86-64 ttyS0
qemux86-64 login: □
```

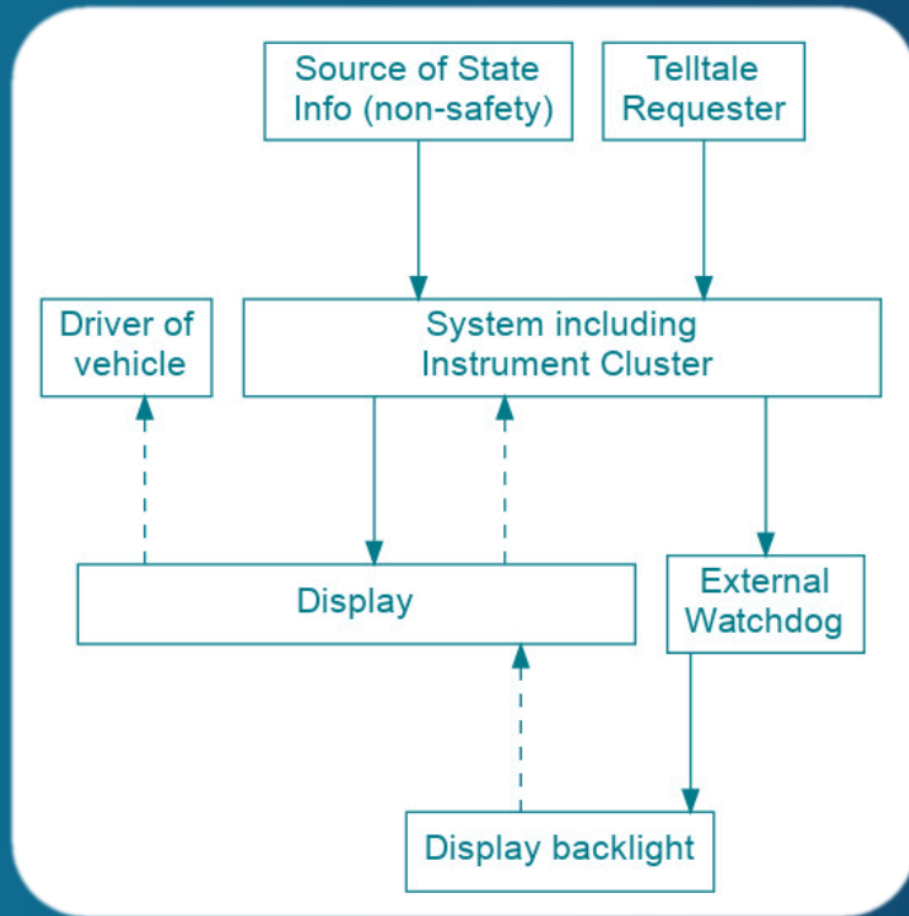
- Demo ported to needlefish ([elisa-tech/meta-elisa/pull/28](https://github.com/elisa-tech/meta-elisa/pull/28))
- QT based running on qemu
- **DANGER** added to illustrate tell tale safety monitoring



More about it during the
ELISA MINI SUMMIT

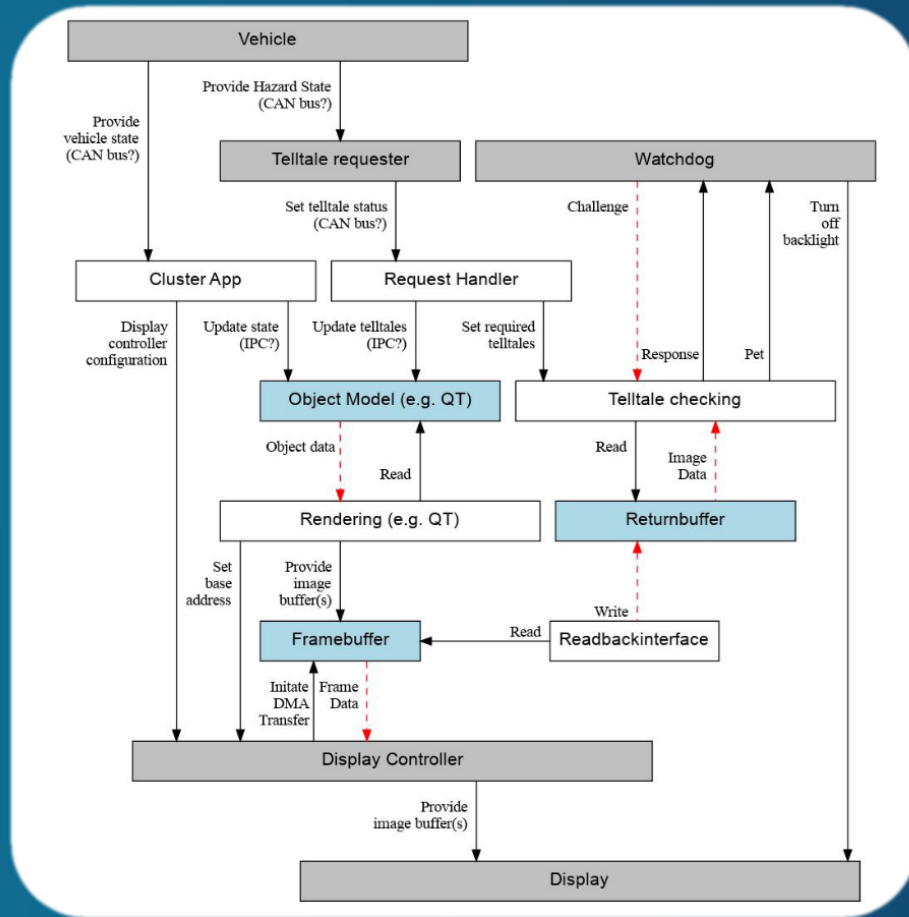


Tell tale system context



- Responsible for displaying safety-critical information (tell tales) as part of cluster display
- Part of a system that includes the Instrument cluster
- System level architecture can scale to different hardware and software architectures.
- Includes an external watchdog
- Can increase safety demands to the Kernel step by step.

Tell tale system context

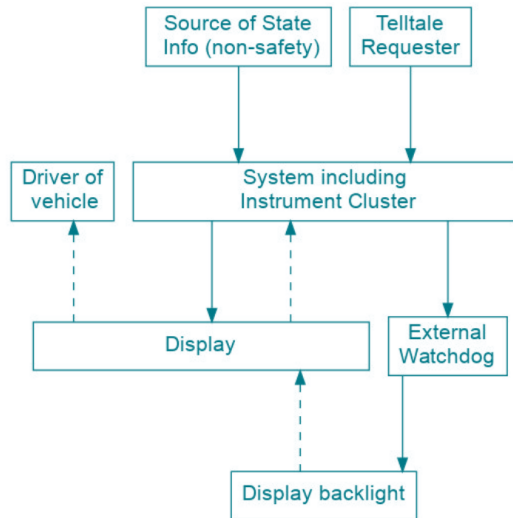


- Responsible for displaying safety-critical information (tell tales) as part of cluster display
- Part of a system that includes the Instrument cluster
- System level architecture can scale to different hardware and software architectures.
- Includes an external watchdog
- Can increase safety demands to the Kernel step by step.

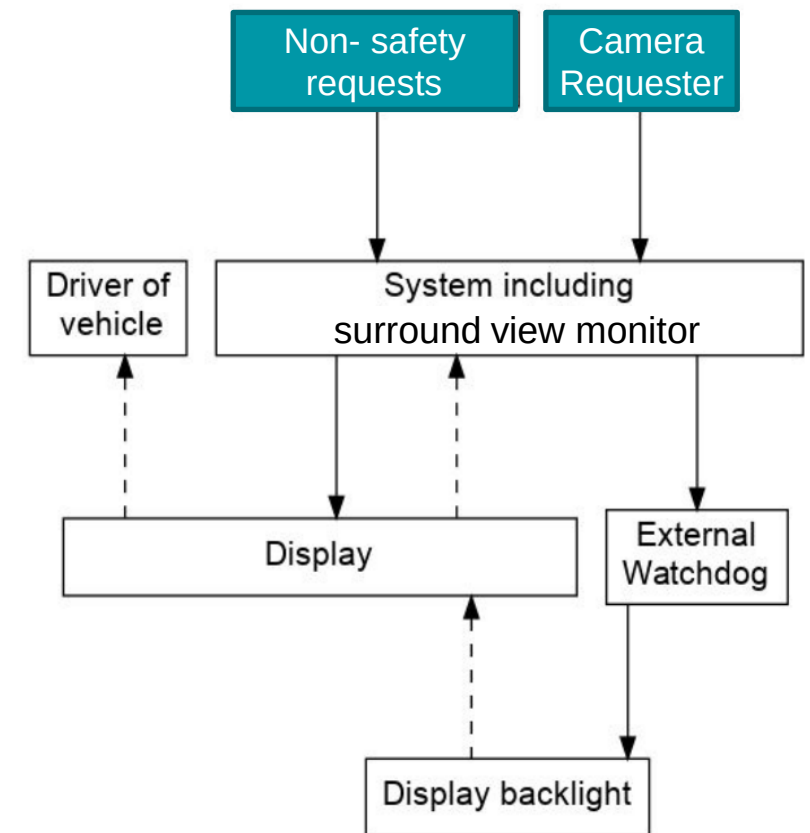
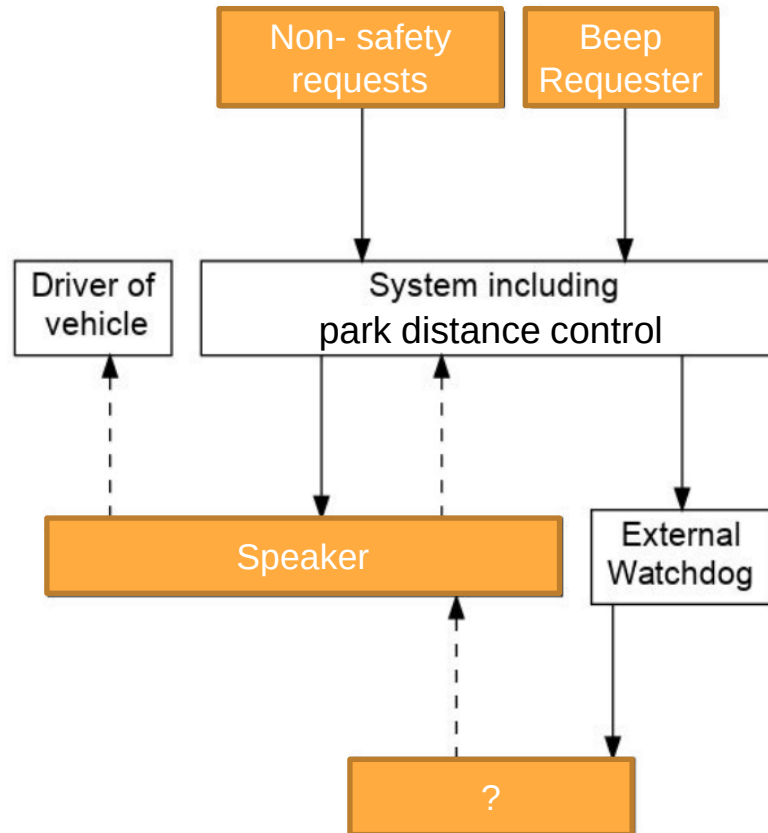
Similarity with other use cases



Basic challenges representative for more complex use cases



Use the tell tale use case work to derive your own use case.

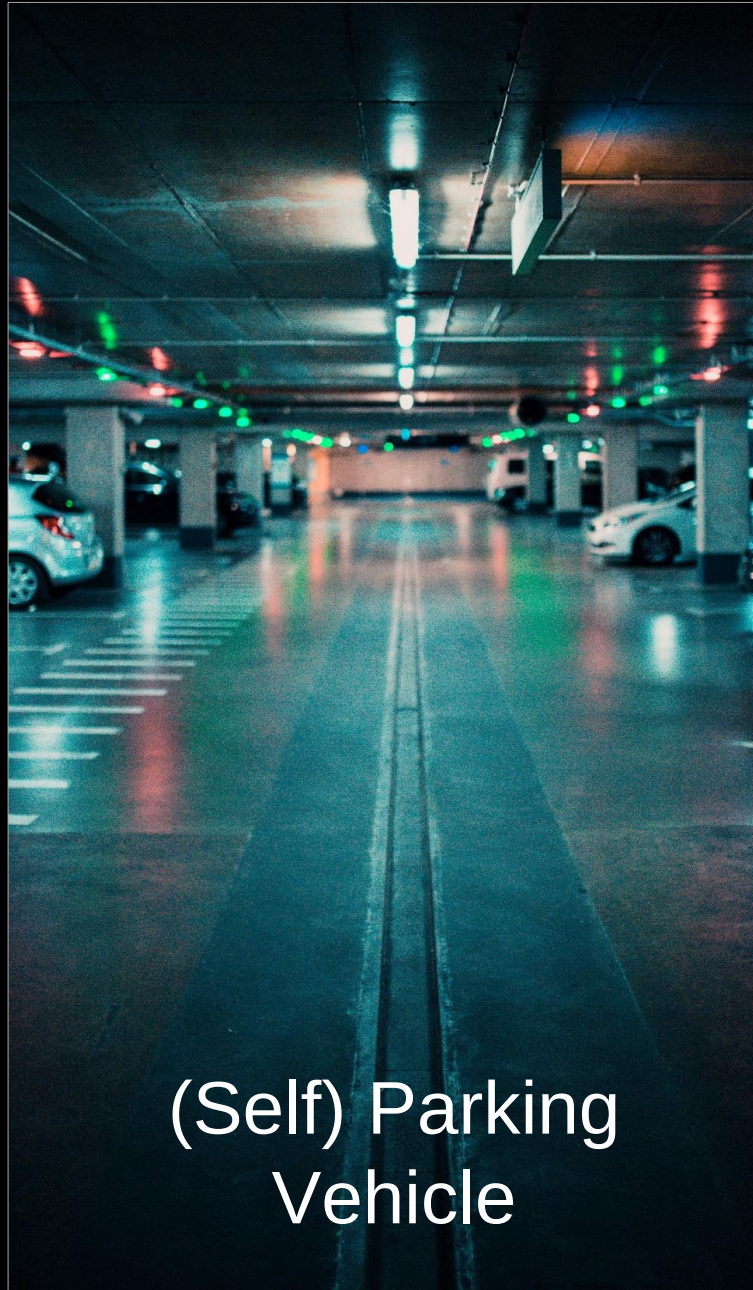


The evolution



Tell tales

Photo by [Randy Tarampi](#) on [Unsplash](#)



(Self) Parking
Vehicle

Photo by [Patrik Sikora](#) on [Unsplash](#)

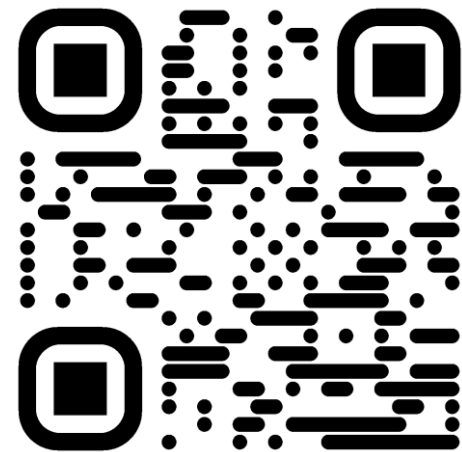


Autonomous
Driving

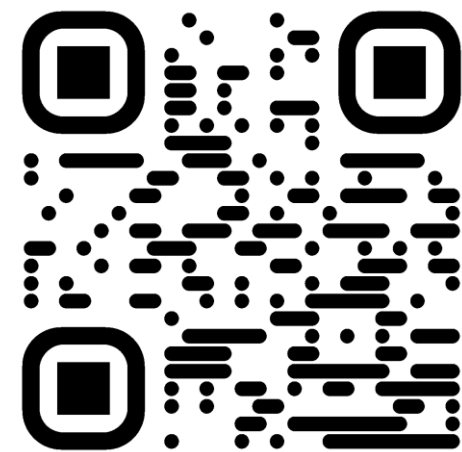
Photo by [Roberto Nickson](#) on [Unsplash](#)

THANK YOU

MINI SUMMIT



KEYNOTE



Getting involved...

- Join main technical and weekly calls of interest:
 - Main Technical List: devel@lists.elisa.tech
 - Safety Architecture Workgroup: safety-architecture@lists.elisa.tech
 - Open-Source Engineering Process WG osep@lists.elisa.tech
 - Linux Features for Safety-Critical Systems WG: linux-features@lists.elisa.tech
 - Automotive Workgroup: automotive@lists.elisa.tech
 - Systems Workgroup: systems@lists.elisa.tech
 - (Full list at: <https://lists.elisa.tech/g/linux-features/subgroups>)
- Contribute content, review materials and add your comments to:
 - ELISA Technical Community google drive: <https://drive.google.com/open?id=1Y6Uwqt5VEDEZjpRe0CBClibdtXPgDwIG>
 - ELISA github repository: <https://github.com/elisa-tech/workgroups>
 - ELISA github issue tracker: <https://github.com/elisa-tech/workgroups/issues>
 - “Final location” for (Architecture/Process/...) documentation on kernel: <https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/tree/Documentation>