Linux for Safe Applications

In April 2024 a completely new approach to run SIL2 safety applications directly on a Linux system has been presented to the public: Elektrobit's EB corbos Linux for safety applications (EbcLfSA) is the first OS-solution assessed by TÜV Nord to be compliant with safety standards up to SIL2/ ASILB and based on embedded Linux. It is suitable for use in ISO 26262 as well as IEC 61508 projects as it can perform safety functions up to SIL2/ ASILB.

Besides very positive press releases so far, the product won the CES innovation award in Vehicle Tech & Advanced mobility 2025. At the Embedded World 2025 the supervisor software has been nominated for the Embedded Award in the category safety & security.

emlix as an Embedded Linux specialist was part of this ambitious project from the beginning. Our main task was to put the Linux kernel under the control of a supervisory element, which enables safety-critical applications to be run in a Linux environment.

Elektrobit

Elektrobit is an award-winning and visionary global vendor of embedded and connected software products and services for the automotive industry. A leader in automotive software with over 35 years of serving the industry, Elektrobit's software powers over five billion devices in more than 600 million vehicles and offers flexible, innovative solutions for car infrastructure software, connectivity & security, automated driving and related tools, and user experience. Elektrobit is a wholly-owned, independently-operated subsidiary of Continental. Triggered by mega trends like Software defined Vehicle (SDV), highly complex cockpit solutions and the availability of high performance computing hardware Elektrobit started an automotive Linux strategy about ten years ago. This has been implemented consistently since then.

Together with Elektrobit's innovative hypervisor solution, the Linux kernel and the supervisor software provide an integrated solution:

Rather than following the attempt to show that Linux "does what it says on the tin", the innovation is based on a completely different approach compared to established „safety" approaches. The "burden of the proof" is shifted from Linux to a "supervision software layer" detecting when Linux does not behave dependably. In other words, rather than trying to demonstrate that Linux is dependable, the choice has been to detect when it is not. The solution follows the following strategies:

- Change the paradigm: use the strength of Linux and detect when things go wrong rather than trying to prevent faults. Let the kernel run as usual. Do not attempt to change it. Use it.
- Just indicate once integrity cannot be ensured and allow fault-reactions to be added as needed by the project.
- Focus on an application's data space. Ensure correctness. Make it a dependable data space.
- Separate lifecycles of all building blocks (Hypervisor, supervisor, kernel, userland applications with its libraries).

Suitable for almost any regulated industry

The supervisor software is a high performance solution bridging the gap between open source software and safety-critical applications. Other than any approach being based on extensive and burdensome testing of the Linux kernel the EbcLsFA solution allows to do the security lifecycle maintenance with established procedures. The Linux kernel can be patched and updated according to security needs with mo-

derate effort and even if performed incorrectly it would not affect the safety but only the reliability The dependability of the safety functions performed does rely on two main software elements: the hypervisor and the supervisor.

The OS-solution developed revolutionizes the market as until yesterday, there was no OS-solution based on embedded Linux for use in highly regulated context and especially not for safety applications. Now customers can. And this is relevant and can be seen as an enabler, as it pairs a well established development environment with functional safety and cybersecurity.

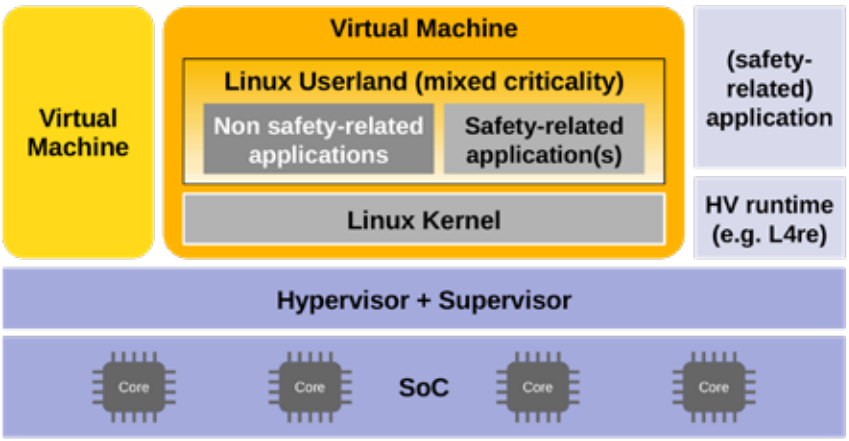
This solution has proven successful: a minimum viable product (which can be considered a technological demonstrator) has been built and is functional while an independent assessor has confirmed not only the dependability of the software, but also that a cyber-physical system implemented using this solution is able to:

- perform safety functions up to SIL2 according to EN 61508
- fulfill safety requirements up to ASILB according to ISO 26262.

This makes this solution suitable for almost any regulated industry: medical technology, robotics, power supply, railway, and for sure automotive.

The advantage for the user is that the effort required to positively assess a system developed using the OS solution is reduced to the minimum in terms of analysis, documentation and testing.

And even for the achievement of higher SILs or ASILs, it offers a broad range of possibilities that can be exploited on a project-specific basis.



Architectural pattern comprising mixed-criticality Linux, any other OS and HV VM.

For more advanced versions, multiple different independent virtual domains are supported. Also a low level of abstraction is supported with a virtual domain directly hosted by the Hypervisor. Further virtual domains can be added with a reasonable effort because their independence is largely covered by the already achieved positive independent safety assessment.

The above mentioned independent domains further allow to apply techniques (like, for instance, diversity, redundancy or cross-check) able to achieve the required level of safety integrity for the most demanding projects. The solution offers features and functionalities that can be exploited to implement the most appropriate fault detection and mitigation techniques.

Elektrobit brings in its market expertise in automotive along with its background in Automotive SPICE® and Functional Safety. Elektrobit further knows customer expectations in the automotive domain along with all its specific processes. And Elektrobit can address large-scale products along with liability obligations.

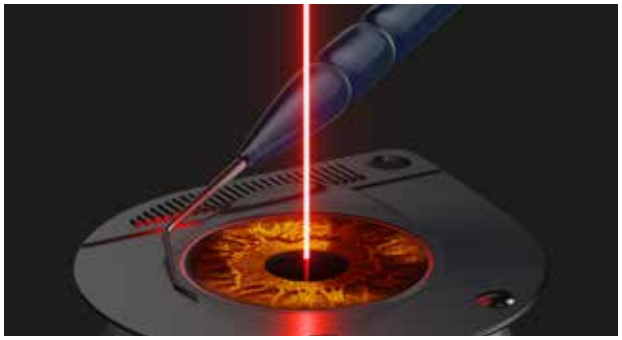
emlix

emlix brings in its expertise in open-source and Linux kernel as well as Linux system development. And given the background of emlix, it knows the regulatory needs from within other domains such as medical and industry automation. And while Elektrobit can supply huge OEMs, emlix can adapt solutions to the specific needs of customers within various domains and even with very low lot sizes. And from now on emlix can do so not only for cybersecure solutions, but also for safety applications within safe and secure embedded systems and throughout engineering and maintenance.

Bridging the gap between the world of safety and open source software

During the more than six years of development Elektrobit and emlix worked together very closely. To successfully learn from each other was undoubtedly one of the keys to success: Elektrobit as software safety experts and emlix as embedded Linux experts.

The foundation of the partnership in between Elektrobit and emlix is a "cultural match". Working in the automotive industry is different than working on open source projects. And working as a supplier in automotive industry is also different from working as a supplier for an embedded Linux for e.g. medical, industry. A collaboration and partnership in between Elektrobit and emlix demands both companies with its teams to go up to each other and to understand each others perspective, motivation and context. The partnership in between Elektrobit and emlix has been and is a learning



journey for both companies. And this learning journey, which is based on openness, curiosity and respect is the foundation for the innovation that has been awarded at the CES and at the Embedded World.

"Open interdisciplinary collaboration and learning, flexibility and development effectiveness are key while looking for a technical solution where none has been available before. Functional Safety, SPICE and automotive development processes and culture need to be brought together with the culture of open source and the character of established Linux kernel development. emlix contributed with openness, curiosity, creativity and deep technical expertise along the evolutionary process. emlix is an important and valued engineering partner, further contribution to the solution and performing operational and maintenance tasks."

(Jens Petersohn, HPC Business Owner & Product Management at Elektrobit)

Enabling efficient mixed-criticality HMIs with one Linux OS solution

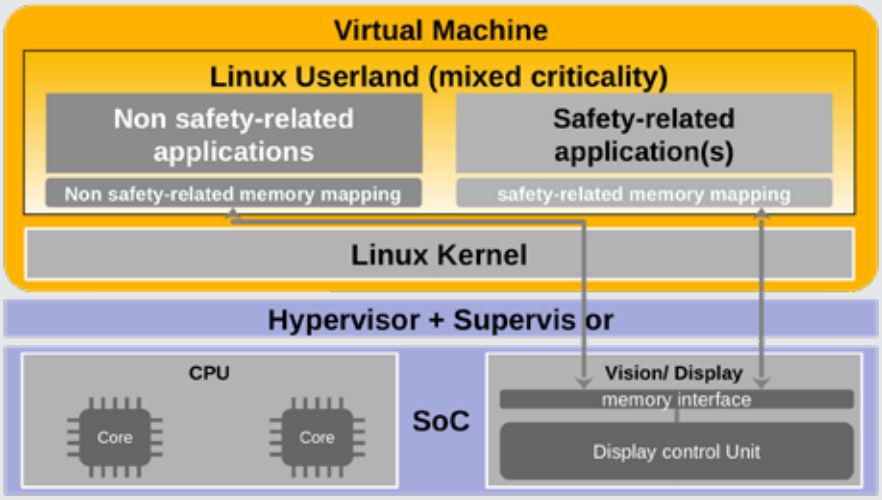
What we are facing in various industries is the need for „mixed-criticality" displays/ HMIs. Non-safety related information is shown in parallel or even overlayed with safety-related information. It is the task of the Hypervisor + Supervisor to ensure, that safety-related information is not overwritten by non-safety related.

This exactly is possible with the OS solution developed by Elektrobit and emlix running on appropriate hardware. Memory access is controlled, violations detected and indicated. The idea is shown in the figure below.

Safety-critcal information can be a vital patients' value in some complex emergency care system as well as an alert signal while steering a production roboter or the information that your cars' oil temperature is too high.

There are multiple other fields of application for e.g. autonomous mobile robots (AMRs), cobots, drones, medical surgery and automotive which can benefit from the applicability of Linux for Safety Applications.

Now, there is an OS solution based on embedded Linux fur use in regulated context that ensures Functional Safety and Security.



Architectural pattern for an architecture with mixed-criticality access to a memory-mapped interface of a display control unit.

emlix GmbH
Phone +49 (0) 551 30664-0
solutions@emlix.com
www.emlix.com