Safety and security based on embedded Linux

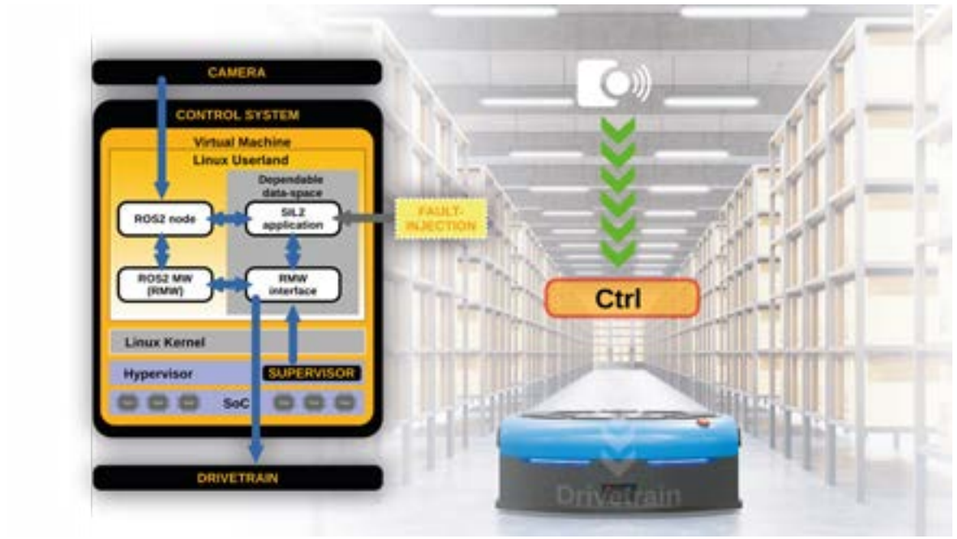
Autonomous mobile robot using ROS2

Until now, there was no option to execute safety-related applications directly on Linux. Now there is.

The OS solution EB corbos Linux for Safety Applications brings together the strengths of embedded Linux with the system characteristics of functional safety. And rather than trying to make it safe, the solution provides an execution environment for applications, which lets them execute correctly. EB corbos Linux for Safety Applications offers „maintainable safety“.

Together with the functionality of a hypervisor, an OS supervisor encapsulates the Linux kernel from the security-relevant applications and their data space in the Linux userland. It creates a “dependable data-space”. SIL2/ ASILB applications can be executed in this space.

The architectural encapsulation of the kernel goes hand in hand with the separation of component lifecycles. Those of the kernel are almost independent of those of the hypervisor and supervisor components. This enables emlix and its customers to carry out efficient maintenance over the product lifecycle and in line with established community procedures.



ROS2 middleware

The OS solution allows the integration of established middleware solutions such as ROS2 to implement complex automation functions using existing libraries. In line with the “separation of concern” strategy, the mixed-criticality capability offers the option of separating non-safety-relevant functional components from safety-relevant ones.

The specific example shows an AMR - autonomous mobile robot - following a line. The environment is detected visually in the demonstrator using a camera. The control of the drive train is calculated within the dependable data-space offered by the OS solution. ROS2-functionality can be executed directly next to the dependable data-space. In the event of an error adversely effecting the dependable data-space, e.g. inadmissible data access or even inadmissible data corruption by the kernel, an error message is issued which can be converted into a vehicle stop in the respective project context, among other things. The data flow from the camera to a ROS2 node to a SIL2 application is visualized in the above figure.

The OS solution allows the integration of established middleware solutions such as ROS2 to implement complex automation functions using existing libraries. In line with the “separation of concern” strategy, the mixed-criticality capability offers the option of separating non-safety-relevant functional components from safety-relevant ones.

The specific example shows an AMR - autonomous mobile robot - following a line. The environment is detected visually in the demonstrator using a camera. The control of the drive train is calculated within the dependable data-space offered by the OS solution. ROS2-functionality can be executed directly next to the dependable data-space. In the event of an error adversely effecting the dependable data-space, e.g. inadmissible data access or even inadmissible data corruption by the kernel, an error message is issued which can be converted into a vehicle stop in the respective project context, among other things. The data flow from the camera to a ROS2 node to a SIL2 application is visualized in the above figure.

Suitable for almost any regulated industry

The architectural concept can apply in many different domains, e.g:

- Industrial automation with AMRs
- Drone control
- Control of autonomous agricultural vehicles
- Medical robots
- Human-machine interfaces with mixed non- and safety-relevant displays and controls
- Driver assistance functions

emlix supports customers from system development including safety conceptual design, software architecture design and component selection to the implementation of customer-specific solutions. Integration and testing are an integral part of the service.

Find out more. Our Embedded Linux for Safety experts will be happy to provide consulting.

Phone +49 551 304460

solutions@emlix.com

■ emlix GmbH | solutions@emlix.com | www.emlix.com | Phone +49 (0)551 / 306 64 - 0