Contribution ID: **32** Type: **not specified**

A maintainable, scalable, and verifiable SW architectural design model for the Linux Kernel

Wednesday, 22 September 2021 10:00 (45 minutes)

Over the last years, many discussions took place in Linux Foundation's ELISA workgroup (elisa.tech) about possible approaches to qualify Linux for safety-critical systems. It is a consensus that one of the main challenges for the qualification of Linux is the lack of SW Architectural Design documentation, especially concerning the kernel internal components/drivers/subsystems. Such documentation is fundamental in functional safety as it provides the baseline required to assess the OS design against the allocated safety requirements (safety analysis). This Architectural Design is also necessary to evaluate the completeness and correctness of the associated test campaign.

However, given the complexity of Linux, the challenge is finding a documentation format that is complete enough to justify the assessment while still keeping a maintainable granularity.

This talk will present an SW architectural design model that, working at the granularity level of the single drivers/subsystems, uses a formal method (automata) to describe the interaction of a target subsystem/driver with the rest of the kernel, whereas a natural language description (kernel-doc headers) is used to describe the behavior of the target subsystem/driver itself.

During the talk, the authors will present how to use computer-aided design tools to help to derive the automata models of target subsystems. They will also show how to take advantage of the proposed Runtime Verification Interface [1] to transform these models into runtime verification monitors that are usable either during the verification phase (to cross-verify the kernel and the documentation) or to monitor safety-related aspects of the system at runtime, avoiding unsafe states.

The discussion of this topic in a more development centric conference (instead of a more safety related audience) is necessary to get the direct feedback of kernel developers/maintainers about the approach and the maintainability of the SW Architectural Design documentation.

[1] https://lore.kernel.org/lkml/cover.1621414942.git.bristot@redhat.com/

I agree to abide by the anti-harassment policy

I agree

Primary authors: Mr PAOLONI, Gabriele; Mr BRISTOT DE OLIVEIRA, Daniel (Red Hat)

Presenters: Mr PAOLONI, Gabriele; Mr BRISTOT DE OLIVEIRA, Daniel (Red Hat)

Session Classification: LPC Refereed Track

Track Classification: LPC Refereed Track (Closed)