LFSCS WG - System Level Safety claims

Out Of Scope

System level safety claims are defined by domain specific working groups

(do we need to change this? should these be defined now by the OSEP WG)?

Work in Progress - License: CC-BY-4.0

LFSCS WG - Kernel Safety claims

- Which assumed Kernel safety requirements or AoUs can be defined to meet System Safety claims?

Work in Progress - License: CC-BY-4.0

ELISA WORKSHOPS

LFSCS WG - Concerns with current proposition

- Can’t evaluate Kernel safety claims if the safe system is not well defined
- External hardware AoUs (e.g. Safety island, watchdogs) might help to meet system level and kernel safety claims

Work in Progress - License: CC-BY-4.0

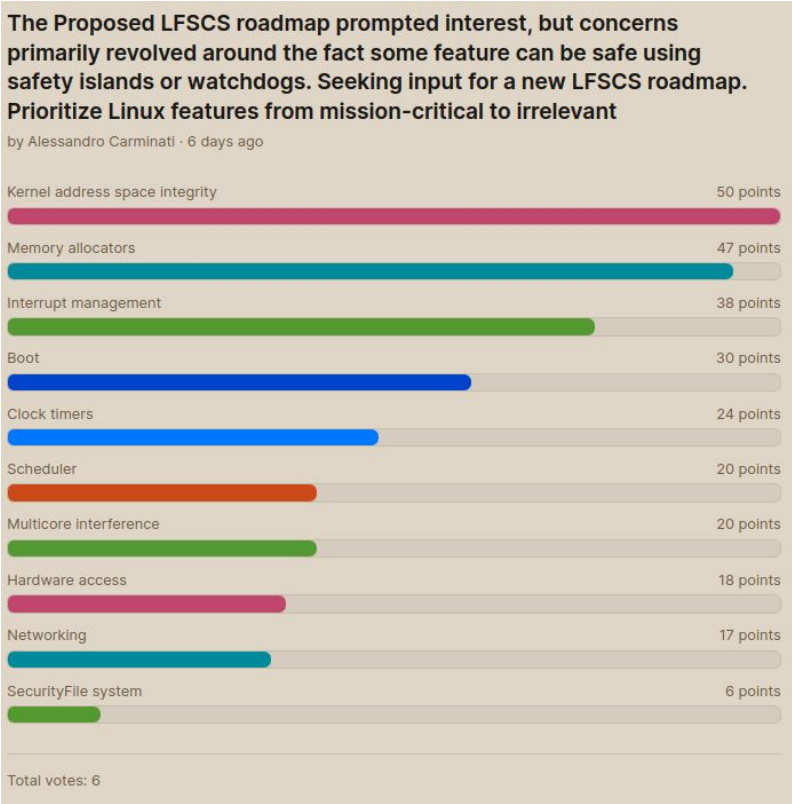
LFSCS WG - Linux Safe problem formalization

- Safe System feature vs Kernel Safety claims
  - External Safety systems maps to new CoUs
  - Cost of having external safety system
    - Material costs
    - Linux costs (some can be effective only if supported)
- Is Linux without external aids, additional CoU, is a condition we want to investigate?

Work in Progress - License: CC-BY-4.0

LFSCS WG - Features priorities - Poll Results

- Modest Turnout
- People think WG should prioritize memory related components



Work in Progress - License: CC-BY-4.0

ELISA WORKSHOPS

LFSCS - Proposal - Feedback

1) According to the Poll results, define safety claims for each component/topic
2) Discuss and agree on system level AoUs that can support such claims (in which WG?)
3) Define Kernel assumed safety requirements (on the basis of 1) and 2)
4) Investigate best Kernel configurations, Kernel level AoUs and Code improvement to support the assumed safety requirements as in 3)

Work in Progress - License: CC-BY-4.0