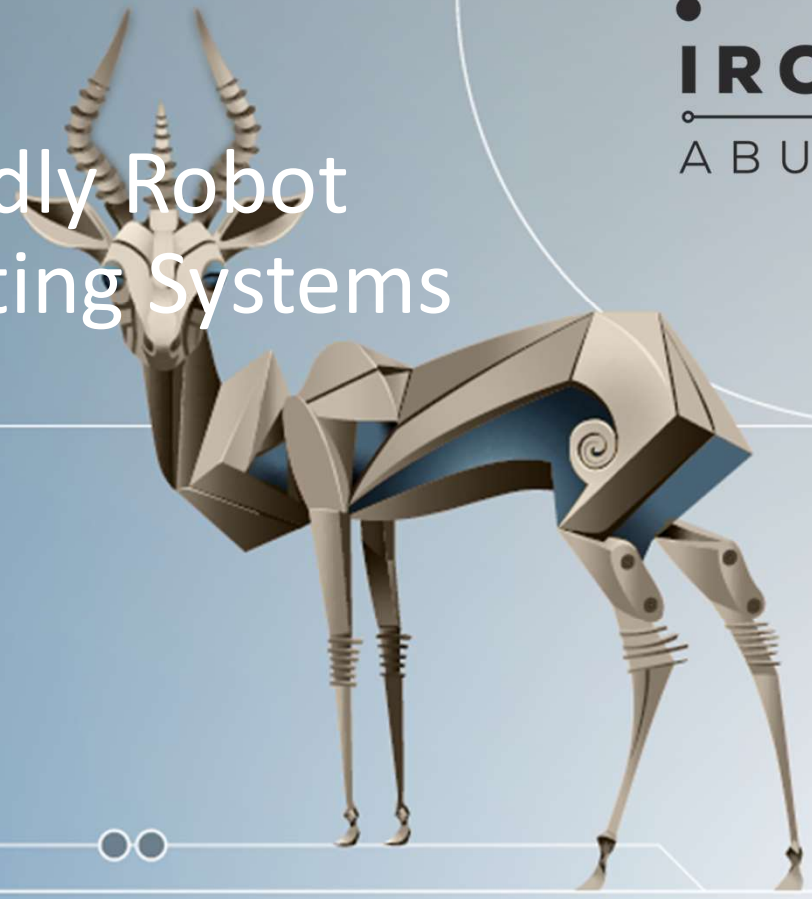
SmartKit: User-Friendly Robot with Multiple Operating Systems



Guanyu Chen
Zhejiang University

Background

- **Single operating system cannot meet the needs of robots.**

  Realtime, General purpose

- **Mixed Criticality System is a trend in robot design.**

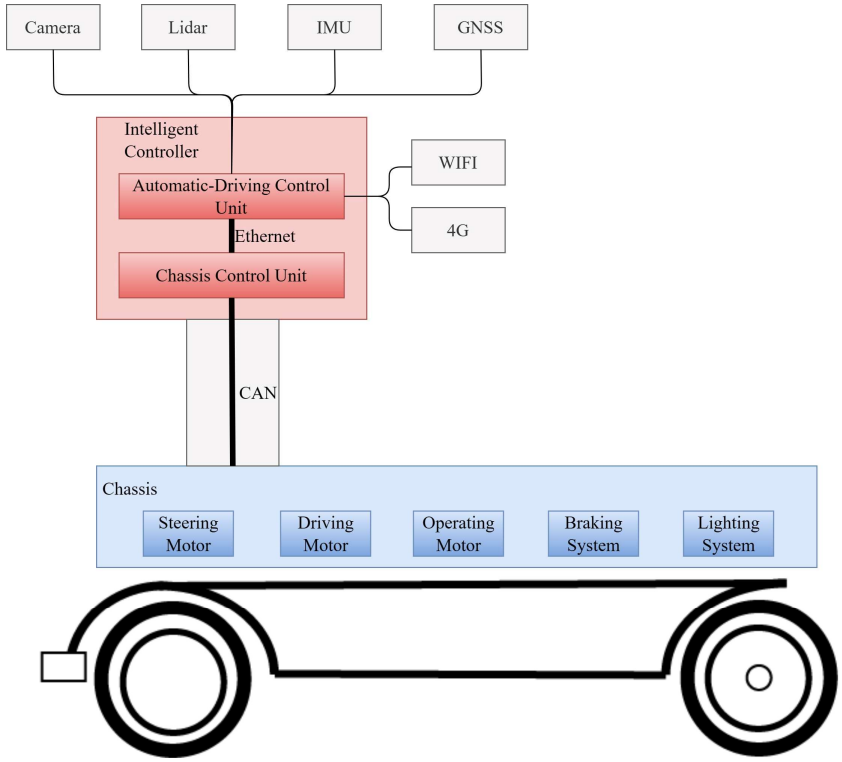
  Multiple subsystem, Multiple Criticality

- **Current academic proposals for new systems exhibit some common application issues.**

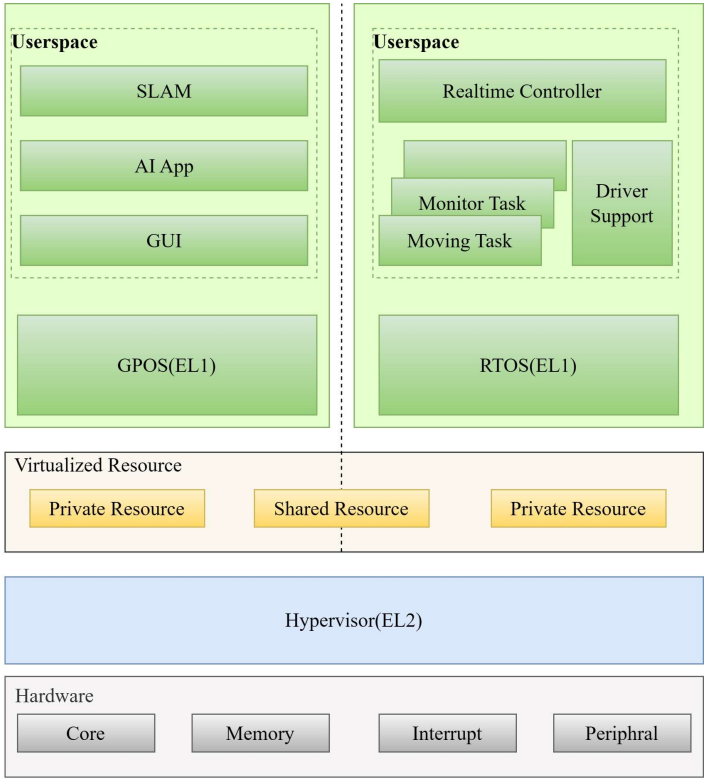
  Slow startup, Difficult updates, Poor reliability

- Develop a practical robotic system based on a microkernel that can handle mobile tasks in most scenarios.

System Design



Hardware Architecture of SmartKit



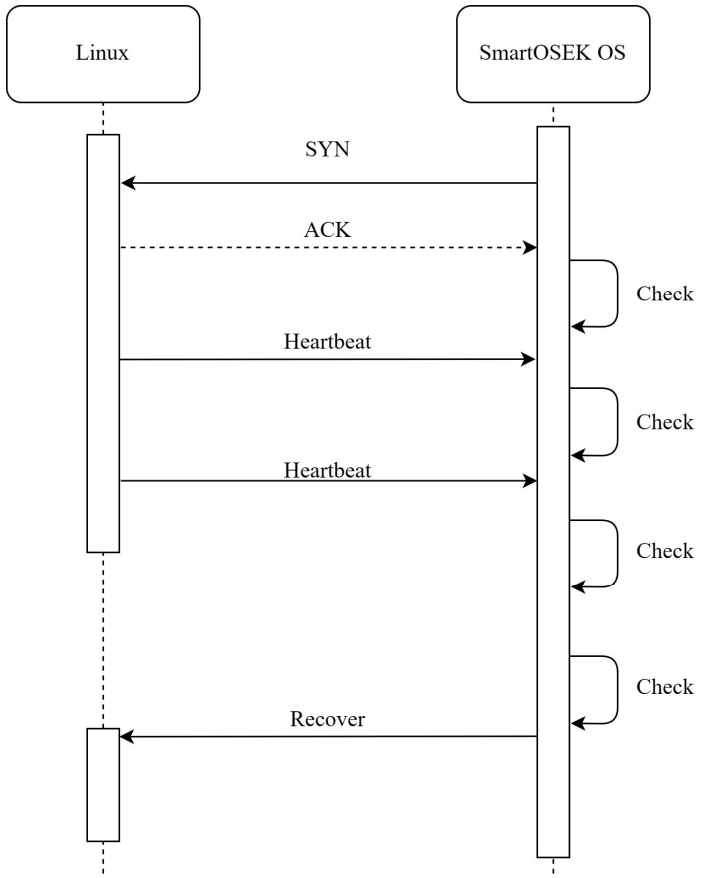
Software Architecture of SmartKit ACU

Recovery module

The system recovery module monitors Linux crashes during robot operation, posing significant risks.

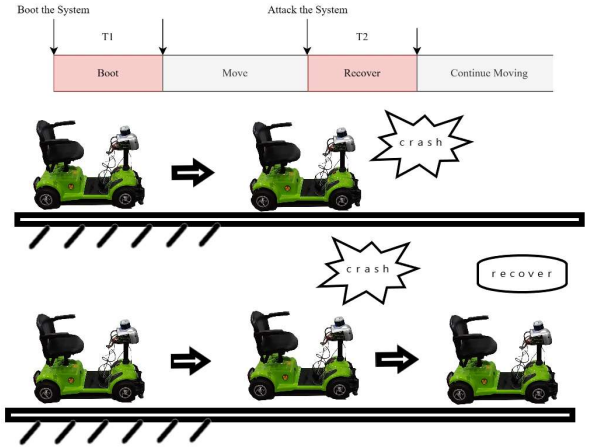
SmartKit uses SmartOSEK OS to send a characteristic value to Linux every 2 seconds, initiating a handshake for monitoring.

If errors accumulate beyond a threshold, SmartOSEK OS triggers a recovery operation, simply rebooting the crashed Linux component.



Crash-Recovery emulation

- Through script settings, the Linux virtual machine will crash after running for a period of time. A hypervisor-based system will detect this issue and initiate recovery, whereas the original system lacks this capability.
- Additionally, the initialization overhead of the SmartVisor system is smaller than that of the seL4 hypervisor-based system.



BOOT-RECOVER OVERHEAD

Boot overhead(s)		Robokit	seL4-based Robokit	Smartkit
T1	Bootloader	26.36	26.36	26.36
	Hypervisor	-	48.91	9.39
	Linux	16.89	19.54	19.54
T2	Reovery	-	25.13	25.13

Thank you!

IROS '24
ABU DHABI