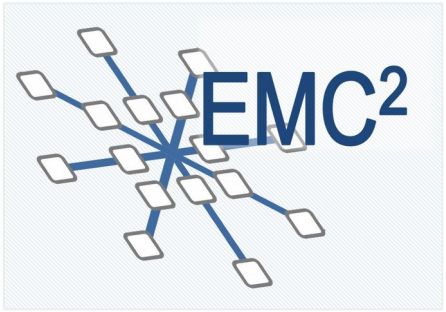
# Safety-critical control in mixed criticality embedded systems

Emil Hjelm





# Presentation outline

- Background
- Research question and problem statement
- What has been done in the field?
- Demonstrator system overview
- Results
- Conclusion

# Background

Today, modern cars have around 100 ECUs, this means:

- Inefficient resource usage
- Clear separation between functions

Moving towards MCS would mean:

- Efficient resource usage
  - Less power consumed
  - Less weight
  - Less volume
  - Lower production cost
- Difficult to separate functions of different criticality
- Fewer but more complex systems

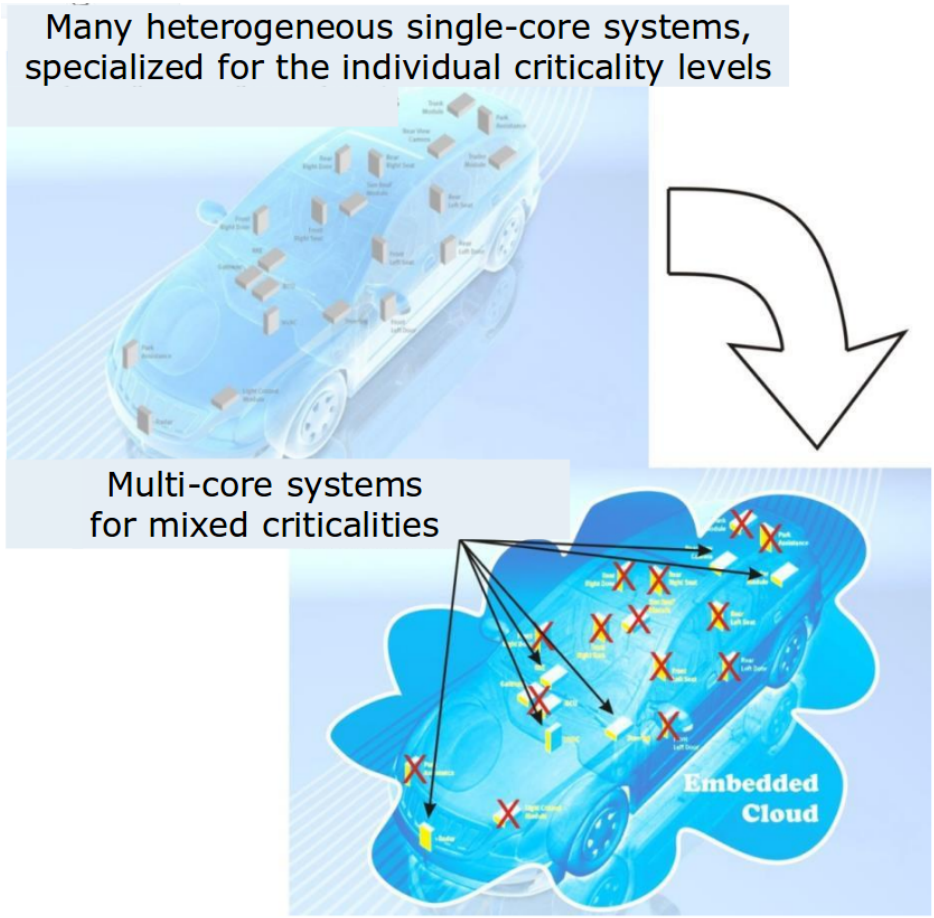



Illustration of combining applications to reduce ECUs [1]

[1] https://www.artemis-emc2.eu/project_overview/ll1_automotive_applications/

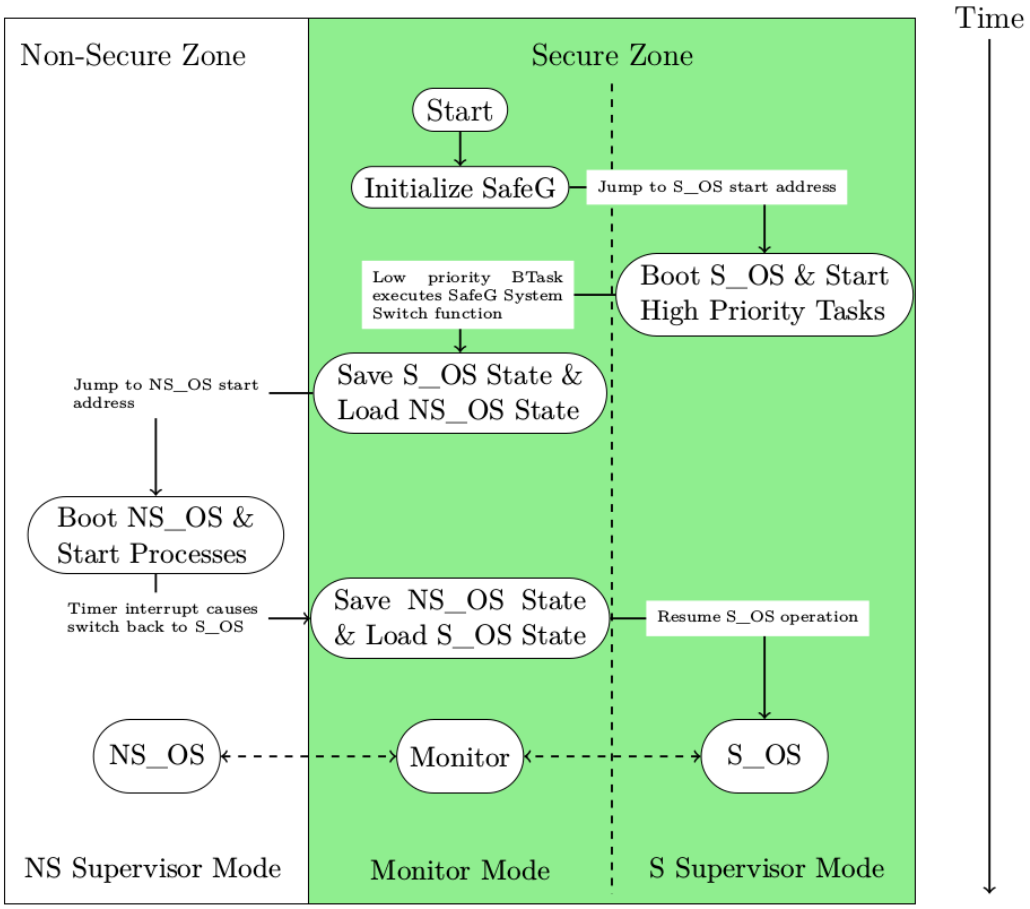
# ISO 26262

## Four different Automotive Safety Integrity Levels, ASILs

| Severity | Probability | Controllability | | |
|---|---|---|---|---|
| | | C1 | C2 | C3 |
| S1 | E1 | QM | QM | QM |
| | E2 | QM | QM | QM |
| | E3 | QM | QM | A |
| | E4 | QM | A | B |
| S2 | E1 | QM | QM | QM |
| | E2 | QM | QM | A |
| | E3 | QM | A | B |
| | E4 | A | B | C |
| S3 | E1 | QM | QM | A |
| | E2 | QM | A | B |
| | E3 | A | B | C |
| | E4 | B | C | D |

[3] Road vehicles – functional safety – part 9: Automotive safety integrity level (asil)-oriented and safety-oriented analyses. Standard, International Organization for Standardization, Geneva, CH, November 2011.

# Alten MCS - Processor switching state

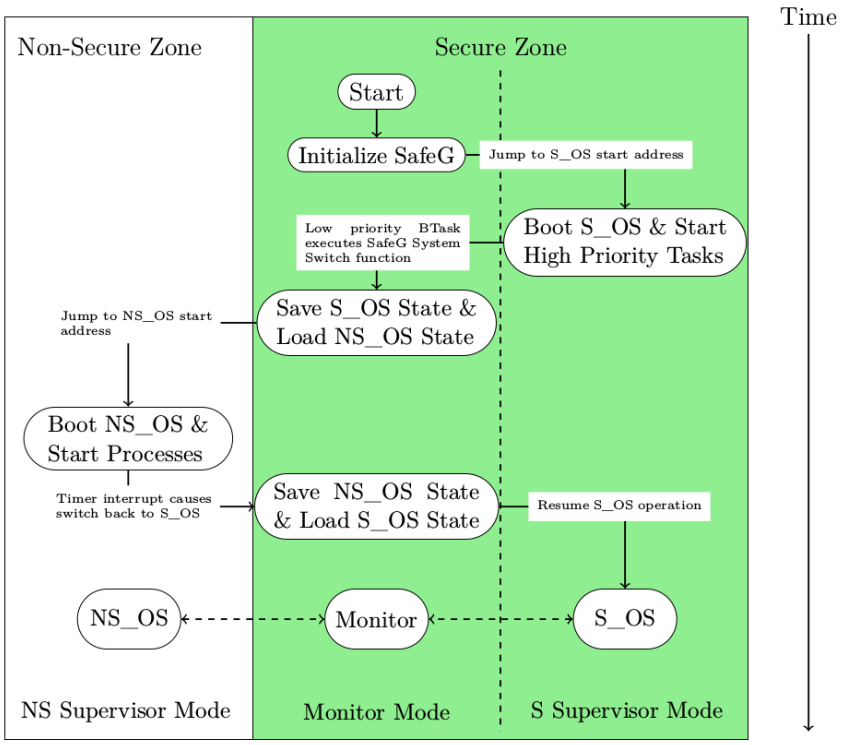



Processor boot sequence [4]

[4] Youssef Zaki. An embedded multi-core platform for mixed-criticality systems: Study and analysis of virtualization techniques. Master's thesis, KTH, School of Information and Communication Technology (ICT), 2016.

# Alten MCS - Processor switching state

- Mode-switch takes ~2 µs
- Theoretical maximum frequency for any control algorithm $f_{max} < 250$ kHz




Processor boot sequence [4]

[4] Youssef Zaki. An embedded multi-core platform for mixed-criticality systems: Study and analysis of virtualization techniques. Master's thesis, KTH, School of Information and Communication Technology (ICT), 2016.

# Research question

Is virtualization an efficient approach when trying to reconcile the conflicting requirements of partitioning for safety assurance and sharing for efficient resource usage when implementing a safety-critical control system?

[5] Alan Burns and Robert I. Davis. Mixed criticality systems - a review. July 2016

# Problem statement

Implement distance keeping control algorithm as a safety critical application on a mixed criticality system. Evaluate performance of processor

- Missed deadlines?
- Robustness of hypervisor
- CPU utilization

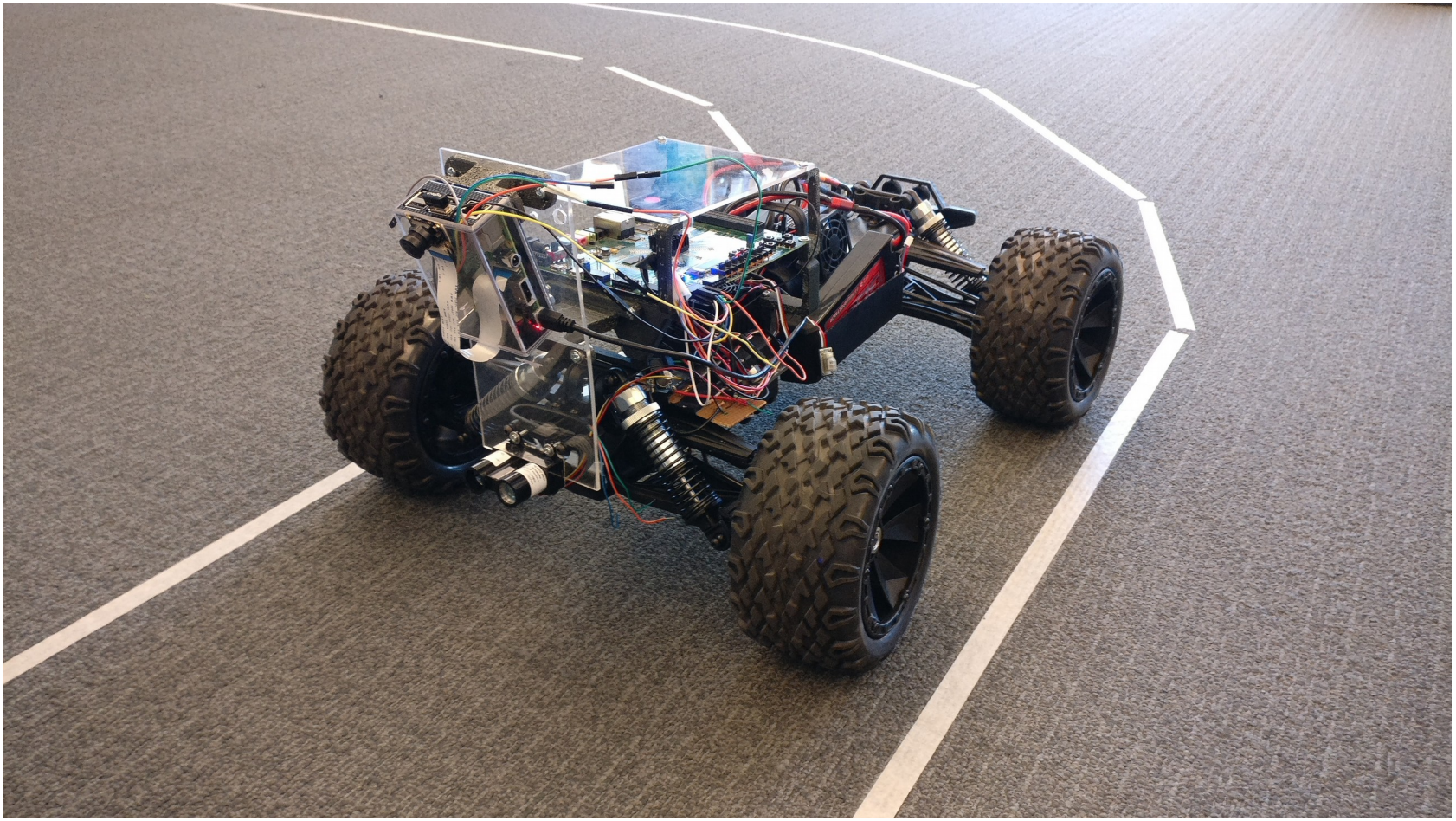
# Schedulers


- Steve Vestal showed that neither RM nor DM was optimal when criticality levels are introduced [6]
- Sanjoy Baruah and Steve Vestal showed that EDF does not dominate FP in mixed criticality systems [7]

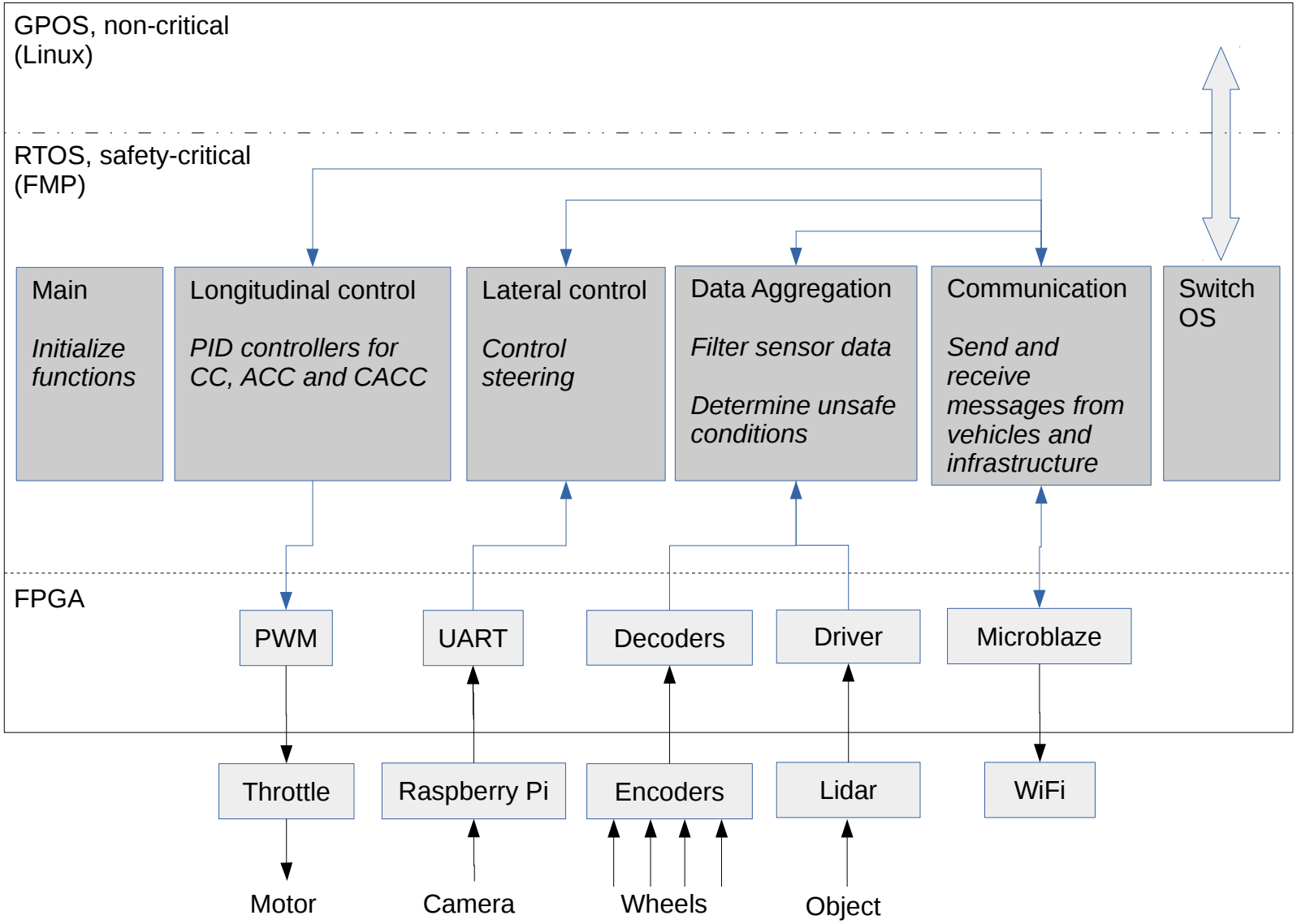
[6] Steve Vestal. Preemptive scheduling of multi-criticality systems with varying degrees of execution time assurance, 2007.

[7] Sanjoy Baruah and Steve Vestal. Schedulability analysis of sporadic tasks with multiple criticality specifications, 2008.

# System overview



# System overview



# Processor scheduling

Data aggregation

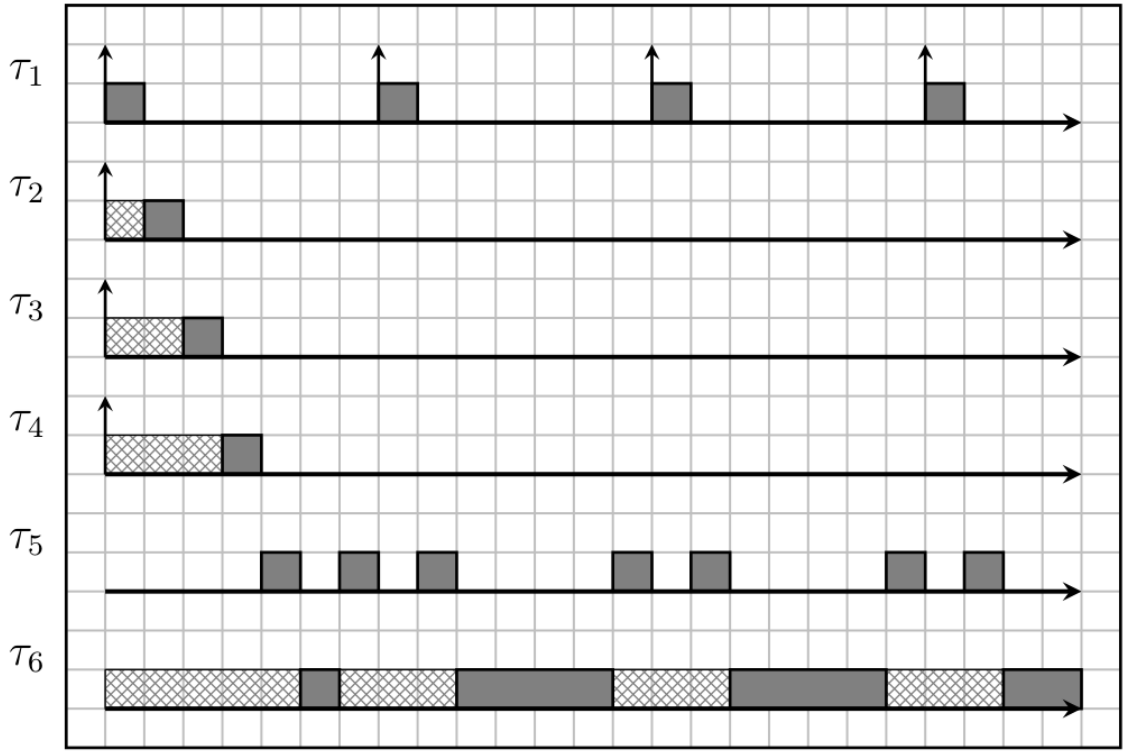
Communication

Lateral control

Longitudinal control

OS switch

GPOS



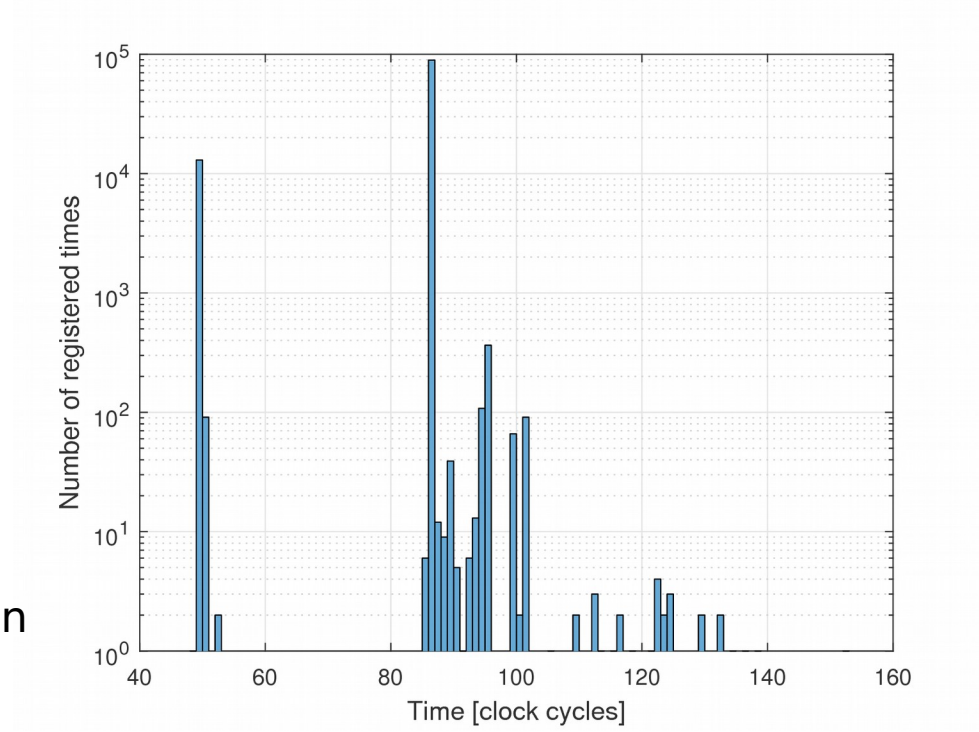

Time not to scale

# OS switch execution times

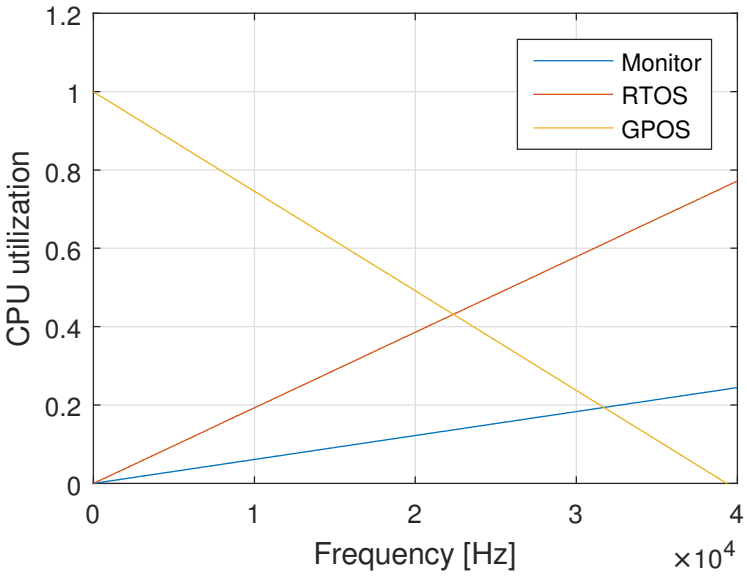
- WCET:
  153 clock cycles
  3.06 us

- Median execution time:
  86 clock cycles
  1.72

- 1 kHz switching frequency:
  - RTOS CPU utilization 0.005%
  - Hypervisor overhead 0.6%
  - Increased  total CPU utilization to potentially 99.4%



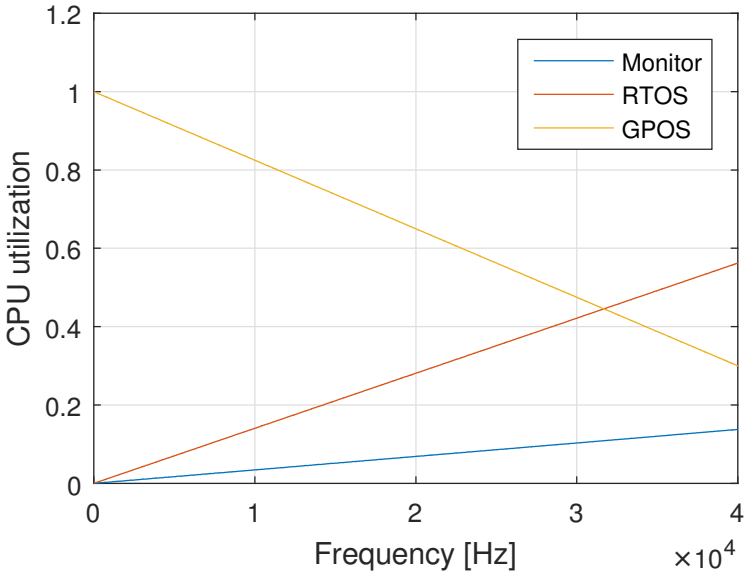
## WCET




100% CPU utilization by RTOS and monitor at 40kHz

(Meaning 0% time for GPOS)

## Median execution time




34% CPU utilization by GPOS at 40kHz if RTOS and monitor runs for median execution time

# Conclusion


Is virtualization an efficient approach when trying to reconcile the conflicting requirements of partitioning for safety assurance and sharing for efficient resource usage when implementing a safety-critical control system?

Yes!

[5] Alan Burns and Robert I. Davis. Mixed criticality systems - a review. July 2016

# Questions