Quest-V – A Virtualized Multikernel for High-Confidence Systems
Ye Li, Eric Missimer, Richard West, Matthew Danish, Ying Ye

Objective
- Operating system for high-confidence systems (NCO/NITRD):
  - Predictable
  - Resistant to component failures & malicious manipulation
  - Self-healing system
    - Online recovery of software component failures
    - Avoid impact on other functional components

Applications
- Healthcare
- Avionics
- Automotive
- Factory Automation
- Robotics
- Space exploration
- Other safety-critical domains

Architecture Overview

Isolation
- Memory virtualization using shadow paging isolates sandboxes and their components
- Dedicated physical cores assigned to sandboxes

Predictability
- Virtual CPUs for time budgeted real-time execution of threads and system events (e.g., interrupts)
- Sandbox kernels perform local scheduling on assigned cores
- Avoid VM-Exits to Monitor – eliminate cache/TLB flushes

Efficiency
- Lightweight I/O virtualization for shared physical devices
  - e.g., VNICs implemented as separate interfaces to single NIC device
  - Hardware performance monitoring for improved efficiency

Example Fault Recovery

Fault Recovery
- Inter-Processor Interrupts (IPIs) for inter-sandbox communication and remote recovery of faulty components

Quest Website