Bridging the space systems performance-reliability gap for future deep space resources exploration and exploitation.

Inês Pinto Gouveia, Rafał Graczyk, Marcus Völp, SnT, University of Luxembourg

uni.lu | SnT
CritiX

Performance-Reliability Gap

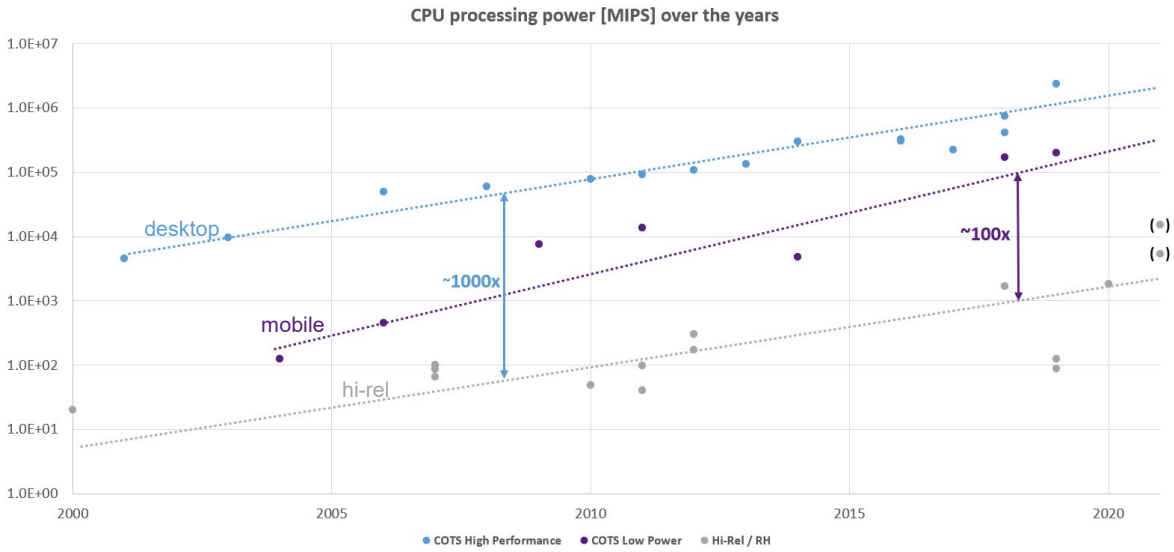
The performance gap between state-of-the-art (COTS) processors and space grade (hi-rel) processors remains a challenge to bridge.

Space-grade equipment can be either:

- reliable, based on rad-hard components, but power hungry and limited in processing capabilities; or
- highly performant (desktop) or performant and power-efficient (mobile), but susceptible to faults, in particular radiation

1000 x increase of COTS vs. hi-rel processing power

100 x increase of COTS mobile vs. hi-rel processing power



How to bridge the gap?

- start from powerful/efficient, but inherently susceptible components
- embrace and accept failures:
  - leverage redundancy of multi-/manycore Systems-on-Chips (SoC)
  - screen out permanently failing cores
  - cope with reversible failures
- mix components of different failure modes and assumptions
- rejuvenate periodically
- build middleware to cope with failures transparently

Solution: Midir

- augment existing SoC architectures with trusted trustworthy components featuring:
  - voting
  - consensually updated access control
- eliminate software Single-Points-of-Failure by:
  - consensual privilege management
  - consensual access to critical resources

Solution: SHARCS & HERA

- hardware-software mechanism for SoC fault tolerance:
  - react to fault manifestations
  - proactively remove dormant faults
- semi-autonomous operation by collective decision making
- adaptive to varying fault rates
- transparent to operating systems and applications
- hardware- and software-agnostic techniques