RUAG

Fault tolerant computers in space applications

Torbjörn Hult

©99 ESA - CNES - ARIANESPACE / Photo Service Optique CSG.

2009-09-24

What characterises space applications?

Long mission times (20 years or more)

Repairs impossible

Hostile environment

- Vibration, vacuum, radiation, temperature variation

Large values

- Launch ≈ 100 M€, satellite 50 – 500 M€

Small series, a few vehicles of the same type

Mass and power limitations

Large distances and high vehicle speed

Different vehicles have different requirements

Launchers

- Unstable, control function outage less than 100 ms
- No backup modes
- Short missions time, 0,3 – 6 hours
- No commanding, except self destruct command
- Low altitude, typically 200 km maximum

Satellites

- Stable, control function outage can be several minutes
- Back-up modes (simple solar pointing, close telescope shutter, . . .)
- Long mission time
- Both telecommanding and telemetry
- Altitudes up to 36000 km (0,25 s communication round trip delay)

Different vehicles have different requirements

Interplanetary probes

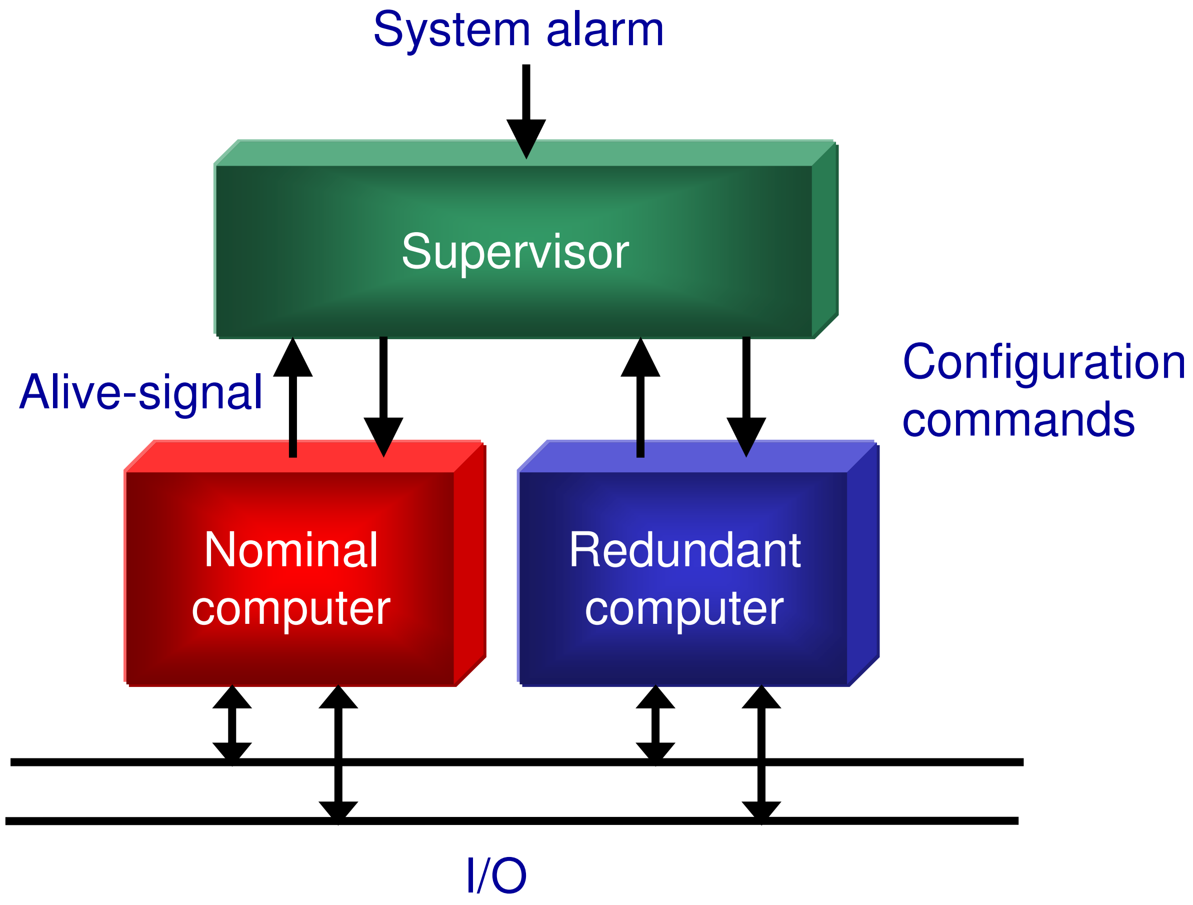
- Stable
- Back-up modes
- Planetary orbit insertion manoeuvres are critical
- Long mission times
- Both telecommanding and telemetry
- Communication round trip delays up to several hours (Voyager1: 24 hours!)
- Communication outages can last for weeks (vehicle behind the sun)

Manned vehicles, space station

- Mostly stable
- Back-up modes with human control
- Short mission times
- Telecommanding, telemetry, audio and video
- Docking manoeuvres, landing etc. critical for human life
- Repairs sometimes possible

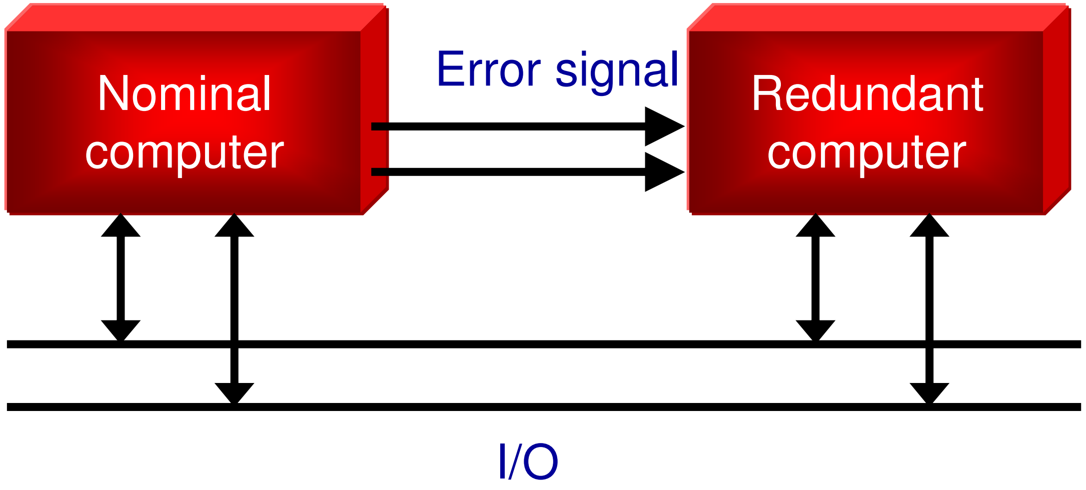
RUAG

Computers in most satellites



- High error detection coverage
- Slow switchover (typically 5 - 10 s)
- Supervisor can be internally redundant
- Context continuously saved in the supervisor

Ariane5 computers

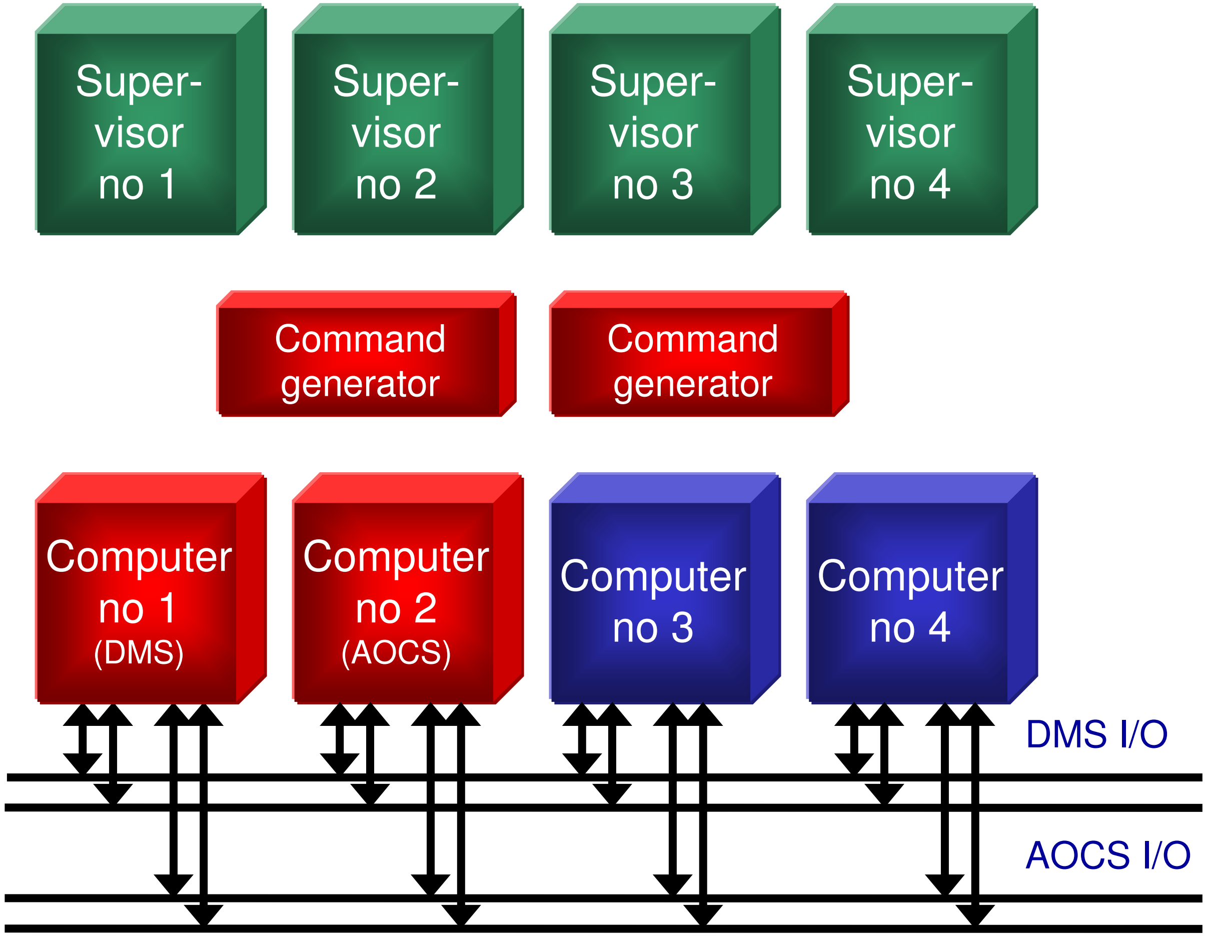


- High error detection coverage
- Fast switchover (typically 50 ms)
- Context continuously exchanged over the I/O bus

Ariane5 computer (right)

Vega computer (left)

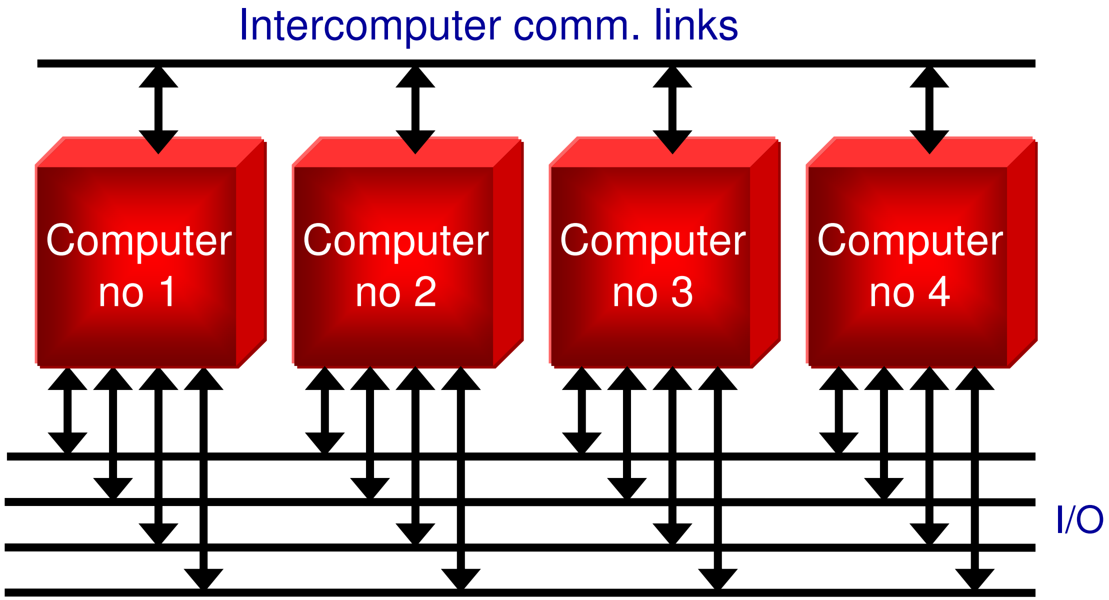
Example of a space probe computer system (Rosetta, Mars Express, Venus Express)



Majority voting computers

Used in manned space applications (International Space Station, ATV)

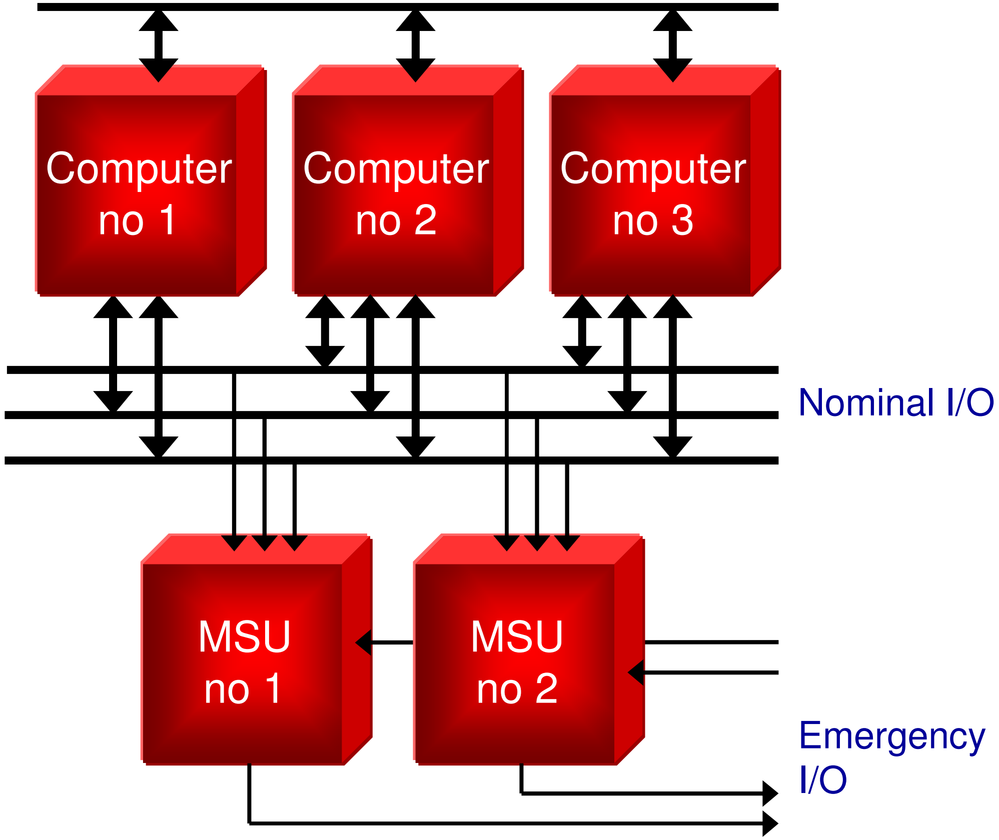
Example: Computers developed for the space shuttle Hermes



- Errors are masked without functional interruption
- Very high reliability for short missions
- Every computer has dual processors for nominal and back-up mode

RUAG

ATV has a separate monitoring computer



- MSU (Monitoring and Safing Unit) supervises the docking process
- In case of hazardous event a Collision Avoidance Manoeuvre is carried out