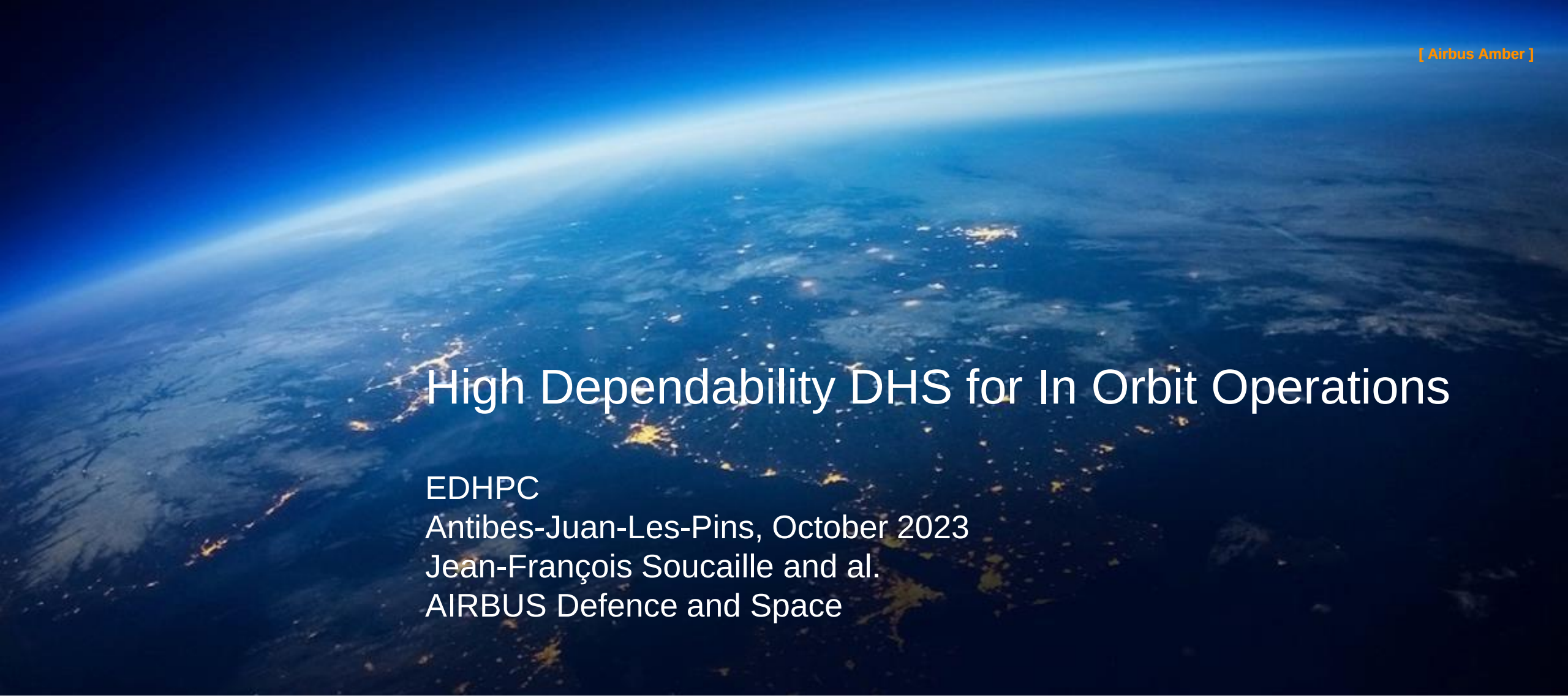


High Dependability DHS for In Orbit Operations

EDHPC
Antibes-Juan-Les-Pins, October 2023
Jean-François Soucaille and al.
AIRBUS Defence and Space

AIRBUS

In Orbit Operations

Operations have to be performed autonomously due to lack of ground visibility (orbital constraints)

Failure is not an option…consequences can be critical/catastrophic

Cost and industrial drivers are varying from fully institutional to new space and commercial

Mars Sample Return

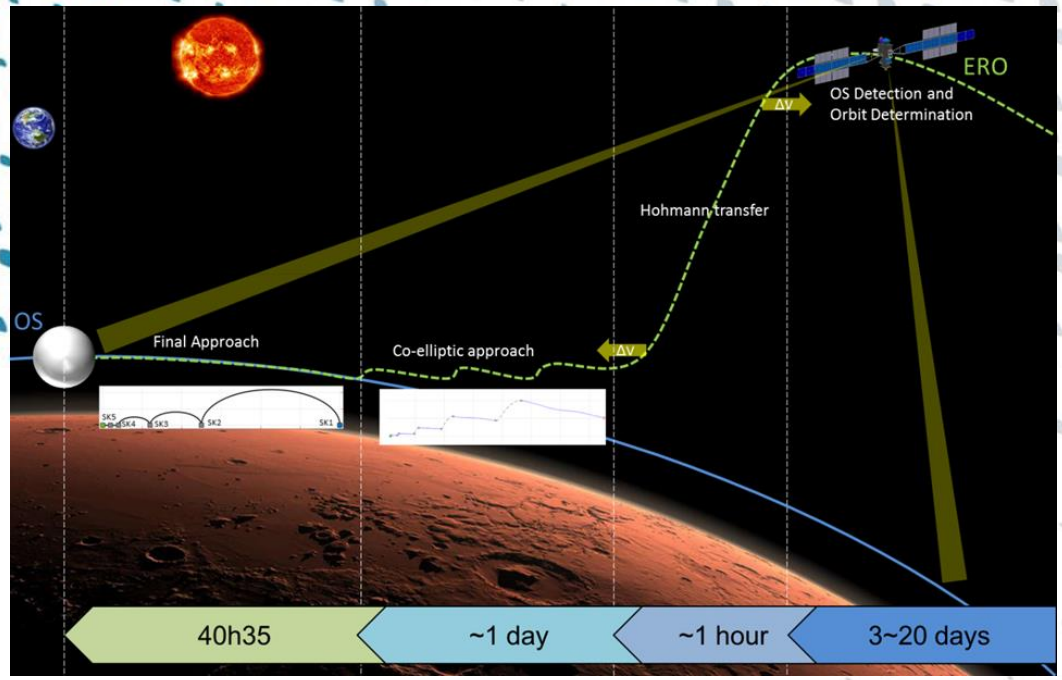
Institutional mission (2FT)

-In martian orbit, capture and transfer of a container with mars soil samples from the Mars Ascent Vehicle to the Earth Return Orbiter. Two ways signal propagation time > 400” (best case)

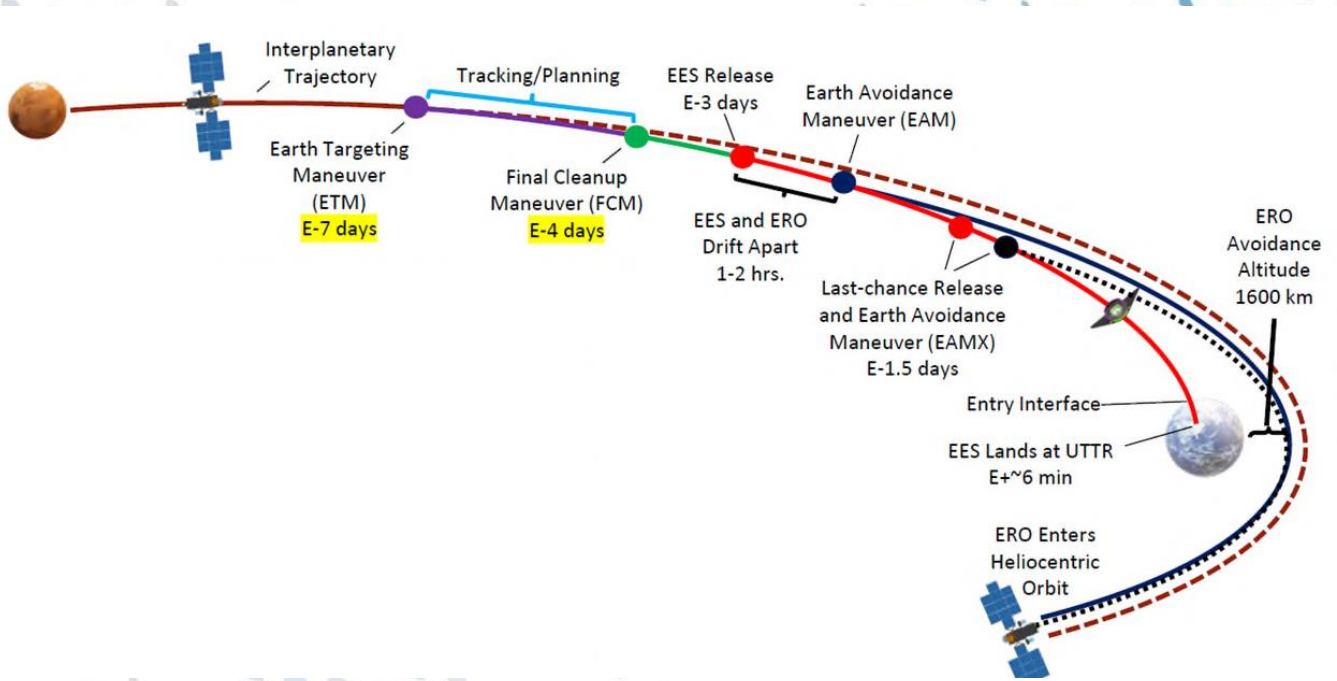
-Avoidance of the Earth after injection of the Earth Entry System in collision trajectory. Earth Avoidance Maneuver is mandatory…

AIRBUS

Mars Sample Return



Samples Capture



Earth Avoidance Maneuver

AIRBUS

LEO Docking

Proof of Concept mission (1FT)

-Autonomous docking to a non cooperative target

-Evolution to all orbits operations (GEO, Lunar…)

-Low cost, tight schedule….

-No debris allowed…

AIRBUS

Commonalities

-Feared events (10^{-6})

-Complete coverage of faults is mandatory

-Low reaction time (1”)

-Use as much as possible existing hardware (flight proven)

AIRBUS

Heritage

[Airbus Amber]

-Ariane V/VI

-ATV

-Bepi-Colombo

AIRBUS

Overall DHS architecture

-Addition of a supervisor function monitoring a state corridor

-Insuring that the supervisor function is 100% fault detectable

-Reducing to a minimum the reconfiguration time

-Providing additional hardware as needed for being 2FT

-Reusing flight proven hardware and architecture as much as possible

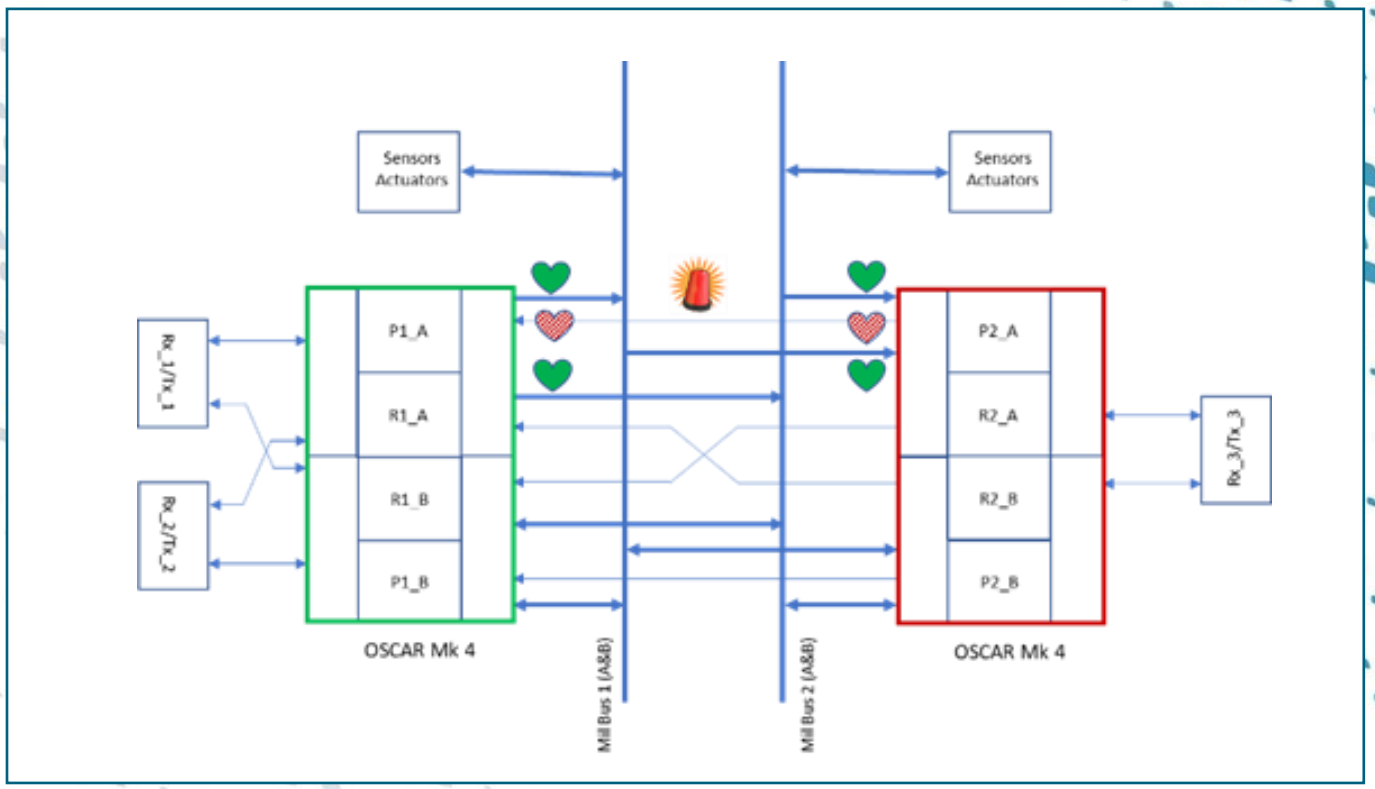
MSR DHS computers pool

-2 OSCAR MK IV in parallel

One Oscar runs the nominal software, the second one is dedicated to monitoring

Heart beat signals used for failure detection and synchronization of hand over

Third TM/TC and additional sensors/actuators used for being 2FT



AIRBUS

MSR OSCAR Mk IV

62 DMIPS and 17 MFLOPS @ 72MHz
• 256Kbytes EEPROM for boot software, 6 Mbytes for Application software and 256Mbytes program RAM memory
• 2Gbytes of exchange memory
• 2 redundant MIL STD 1553 Bus or optionally 2 CAN, for platform and payload management
• 2 SpaceWire links
• CCSDS Telemetry and Telecommand compliant with ESA standard
• Security function compliant with SDLS standard
• Lukewarm redundancy, custom reconfiguration capabilities: up to 8 programmable scenarii are available for HW reconfiguration
• High reliability thanks to full redundant architecture
- 2 Processor boards and 2 DC/DC converter boards, with 1500 fits per channel
- Complete functional cross strap between Processor board
• Architecture proposes a separate box for the I/O's, controlled via the 1553, CAN or SpaceWire
• UARTs and Space Wire links for software development and debugging

Mass: 5kg
Volume: 230 x 184 x 206mm
Power: 25W max
First flight 2012 (Mark I)

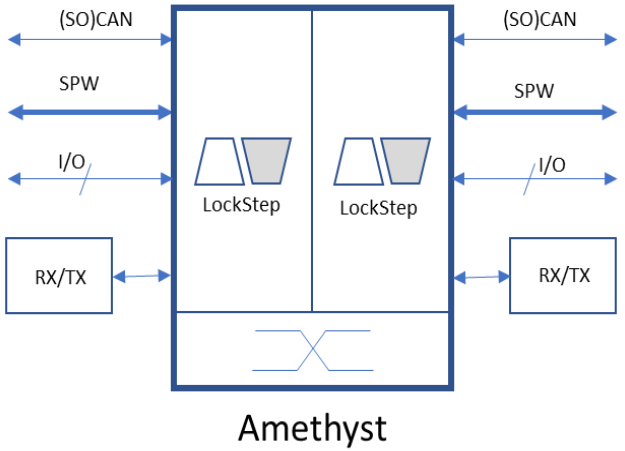
AIRBUS

LEO docking computers pool

-1 FT Requirement avoids triplication.

-LockStep processor guarantees a complete coverage and an immediate detection of OBC failure: supervisor runs on nominal channel only.

-Standard architecture reused from OneWeb platform: more than 400 in orbits.



AIRBUS

Amethyst computer

Single-point-of-failure-free centralized architecture
- Reconfiguration mechanism (50 scenarios)
- GPS Receiver: L1C/A, 10m accuracy in LEO
- CCSDS TM with ciphering & TC with deciphering (AES256)

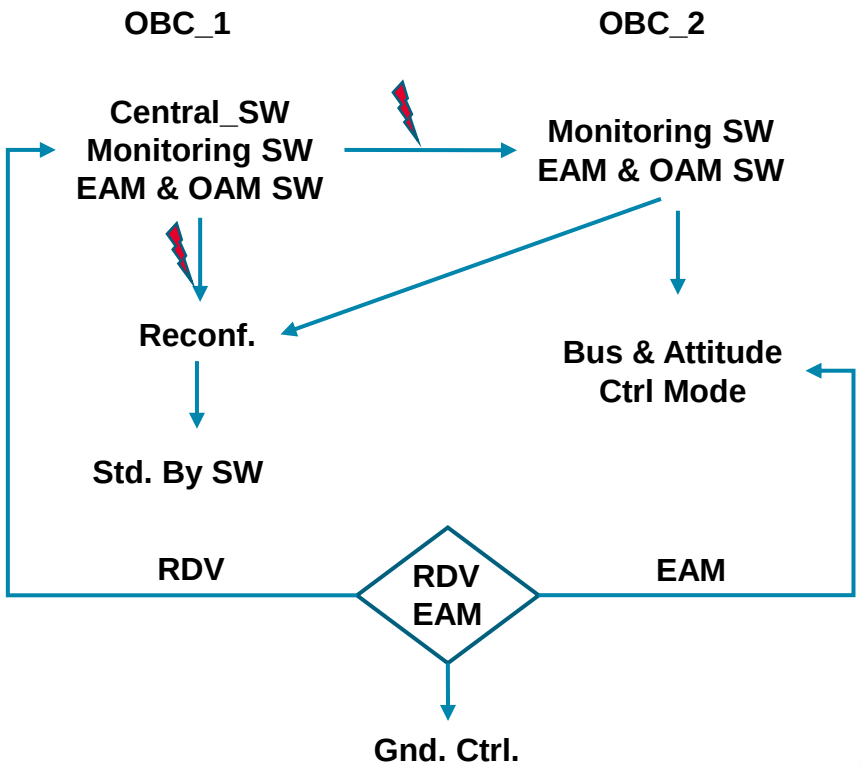
PROCESSING
- ARM processor designed for safety critical applications, fully compatible with ARM ecosystem
- 215 Dhrystone MIPS & Floating Point Unit
- L1 Cache Instruction with ECC / L1 Cache Data with ECC
- Internal RAM, FLASH & EEPROM with ECC
- Time & Space Partitioning hosting several SW applications in a single core implementing RTEMS OS: Central Flight SW, GPS SW, TM/TC SW and STR SW (STR Head in option)
- Avionics delivered with Basic SW: BIOS, Boot SW
- JTAG / Ethernet links for SW development, trace and debug

MEMORY
- Volatile: 192MBytes SDRAM CPU with Error Detection
- Volatile: 64MBytes SDRAM IO with ECC
- Non Volatile: 4GBytes FLASH with ECC

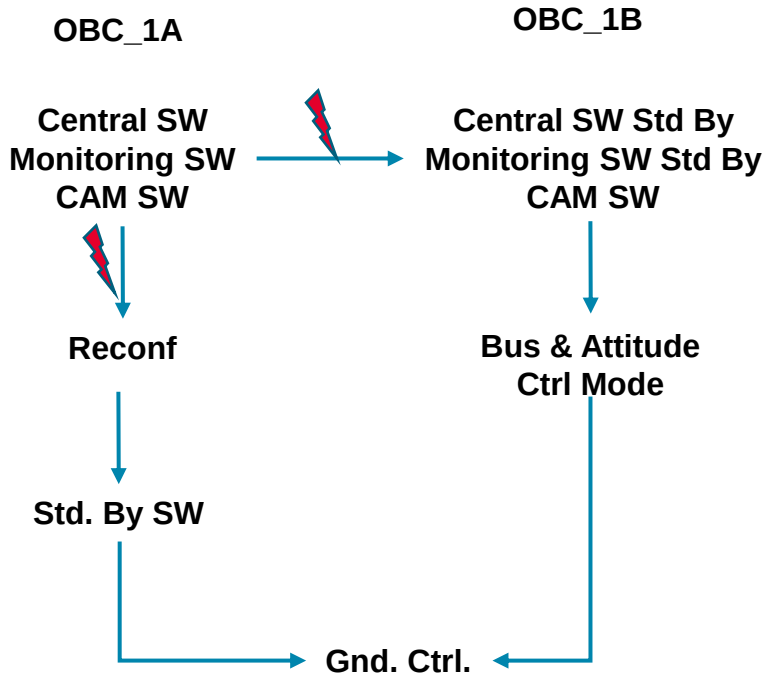
Mass: 3.5kg
Volume: 110 x 240 x 170mm3
Power: 20-50W
First flight: 2019

AIRBUS

Software Architecture



MSR ERO (2FT)
RTEMS on Leon3 SparcV8
Specific softwares on OBC1 and 2



LEO docking (1FT)
Hypervisor and RTEMS on ARM R5
One single software

AIRBUS

Conclusions

-2FT is costly in hardware, design and tests (combinatory explosion).

-LockStep helps a lot.

-New space hardware shall be flight proven. Nothing like real flight data.

-It appears as a paradox that the design is more oriented toward avoiding the feared events than toward the mission itself….

AIRBUS

Acknowledgments

The concepts presented find their roots in the activity conducted by Airbus (then MATRA) for the Ariane V launcher in the 1990s and for the ATV ISS logistics spacecraft in the 2000s (then Aérospatiale).

They have been matured and improved thanks to innumerable and fruitful interactions with Institutional Agencies and other Airbus partners.