SITAEL

# On-Board Computer (OBDH)

SITAEL OBDH is designed to host on-board data handling and AOCS computation functionality. The device is built around a 32-bit ARM Cortex M4, equipped with the peripheral required to communicate with sensors and actuators.

Its functions include

- the collection and monitoring of on-board housekeeping data
- the encoding of telemetry data to be transmitted to ground
- the decoding and execution of telecommands received from ground
- the distribution of on-board time, kept with an RTC
- the execution of AOCS algorithms
- the execution of on-board FDIR policies

The firmware can be re-programmed during the mission, and the unit is equipped with additional flash memory to host housekeeping data history.
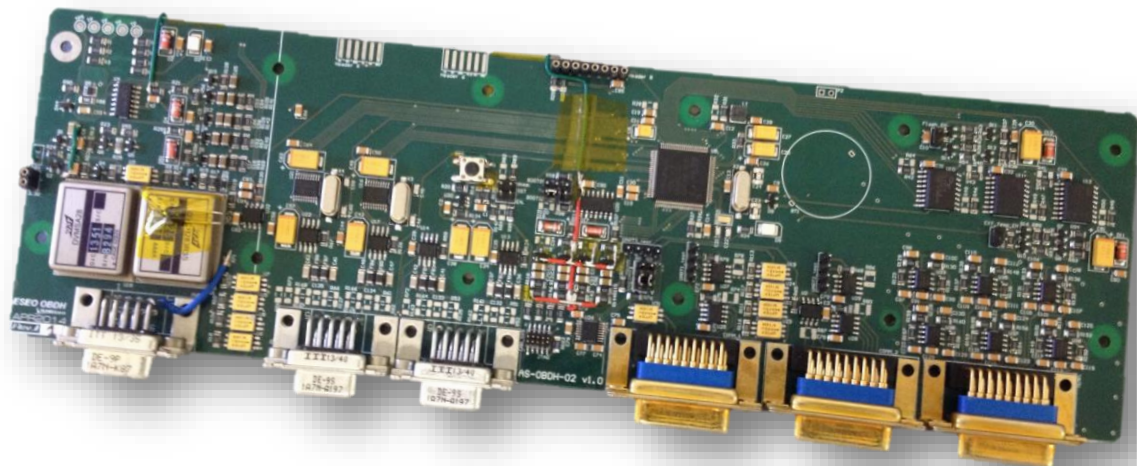
SITAEL OBDH

Features

- Based on 32-bit ARM Cortex M4

- Equipped with independent watchdog, OVP and SEL protection

- Interfaces includes:

    o 4 x CAN-Bus

    o 2 x RS-422

    o 1 x RS-485

    o Isolated pulse command interface to switch on/off the unit, and to activate the reprogramming sequence.

- New firmware can be loaded during mission, using the RS-422 or CAN interface.

- The software is based on RTEMS OS.

- In case of system fault, the units automatically stores death report and reset information that can be retrieved at the next boot

Technical Information

SPECIFICATIONS	
Bus Input Voltage (V)	+12 V to +28 V
Interfaces	4 x CAN-Bus (with CANOpen protocol), 4 x RS-422, 1 x RS-485
Environment	Storage Temperature: -40 °C to +100 °C
	Operating Temperature: -25 °C to +70 °C
Power Consumption	0.5W
Size	287x85x15 mm (L x W x H)
Mass (g)	200
Computational power	>100 DMIPS at 84MHz
OS	RTEMS
TRL	5

General remarks

- The device is developed as part of the low cost product line for small LEO platforms and technological demonstrators.
- All electronic components are selected with industrial and military grades.
- The main computation unit is a 32-bit ARM device, tested for TID, SEL, SEU and SEFI.
  - o   TID test demonstrated no loss of functionality up to 30krads
  - o   SEL protection is implemented at board level (re-triggerable LCL)
  - o   SEU and SEFI impact is mitigated at software level

SITAEL