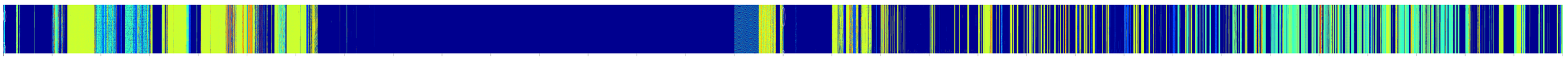
Recovery from File System Corruption on the OPS-SAT-1 Experimental Processor

Maximilian Henkel[1] Vladimir Zelenevskiy[2] Rodrigo Laurinovics[3] Omiros Papadatos Vasilakis[4]
David Evans[5] Georges Labrèche[6] Dominik Marszk[5] Sam Bammens[5]

[1]IKS, Graz University of Technology [2]Telespazio Germany GmbH [3]IrbGS ltd [4]Innoflair UG [5]European Space Agency (ESA)/ESOC [6]Tanagra Space



Objectives

Recover from radiation and wear induced faults on a spacecraft's non-volatile memory:

- Regain communication with the processing platform.
- Identify the root cause of the issues.
- Develop mitigation strategies against further corruption.
- Return to nominal state.

OPS-SAT-1 Mission

Satellites experience degradation over time due to radiation and thermal changes. This study focuses on a defect with the on-board non-volatile memory (eMMC), observed in the experimental on-board computer payload (SEPP) of the European Space Agency (ESA) OPS-SAT-1 Space Lab. Launched in December 2019, OPS-SAT-1 is an in-orbit laboratory for European industry, academia, and research, facilitating over 250 experiments. The SEPP—shown in Figure 1—with its 800 MHz processor and reconfigurable Field Programmable Gate Array (FPGA), uses a non-radiation-hardened commercial off-the-shelf (COTS) Flash Chip (eMMC memory) with 128 Gbit capacity. However, file corruption events have been encountered, requiring extensive investigations and recovery attempts. This poster highlights the timeline of these events and the successful execution of experiments by adopting a new operational approach.

Credit: Reinhard Zeif[1]

Figure 1: SEPP mainboard top view.

Problem Statement

Since the beginning of 2022, several events corresponding to file corruption on the SEPP eMMC memory occurred. The early ones could be solved by rebuilding the file system, but the events in June 2022 led to a corruption of all software processes responsible for the SEPP on-board communications.

Regain Communication

After the problem occurred, the SEPP was non-responsive via the standard means of communication. The first step to regain access to the SEPP consisted in establishing an alternative communication path. As depicted in Figure 2, it could be re-established by activating the Universal Asynchronous Receiver / Transmitter (UART) connection on the On-board Computer (OBC). Thereby, a direct interaction with the bootloader is possible, allowing to boot into a read-only configuration.

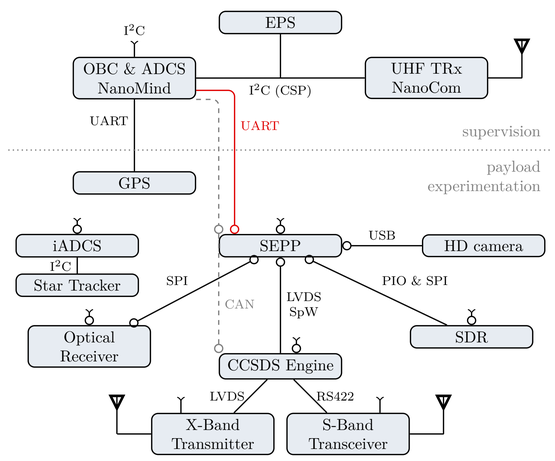


Figure 2: OPS-SAT architecture [1].

Mitigation Strategies

- Keep the entire system as read-only as possible i.e. reduce program/erase cycles on eMMC.
- Activate file system flag to remount to read-only on error.
- Write primarily to volatile memory (overlayfs).

Overlayfs provides a transparent virtual file system layer, combining the read-only file system in eMMC with a light-weight volatile file system (ramfs), as depicted in Figure 3. This results in a writable file system while preventing wear on the eMMC.

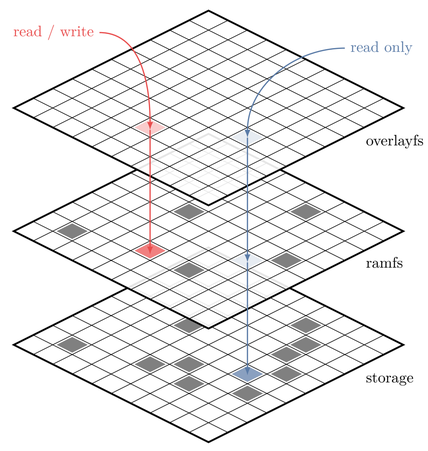


Figure 3: Overlay file system [1].

Root Cause Analysis

- Systematic exclusion of involved components.
- Run eMMC diagnostics, see Figure 4.
- Complete download of affected partitions (4 GB).
- Conduct file system investigations.
- Test direct write reliability with different loads at all possible locations.
- Monitor for unexpected changes during no, low and high activity.

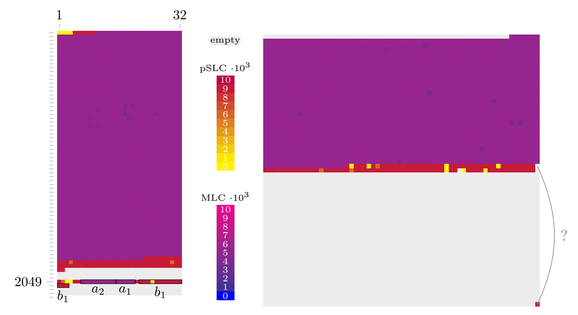


Figure 4: eMMC block erase counters [1].

Software Tools

Open Source tools used for investigation and recovery purposes:

e2fs-tools (e2fsck, ...) for file system analysis.
ramfs is a Linux kernel in-memory file system.
overlayfs combines two underlying file systems.
dd & tar is used to write/read into eMMC bypassing the file system layer. In-house developments were based on these utilities.

Guideline for Future Missions

The experience in recovering OPS-SAT-1 from radiation and wear induced memory faults in space-bound computers can serve as a guideline for future small satellite missions carrying similar equipment.

Results

1. **2022-03-28**: file system failed.
   → 2022-04: rebuilt the file system.
2. **2022-06-01**: communication with SEPP lost.
   → 2022-09: implemented UART communication and a partial read-write/read-only approach.
3. **2022-12-02**: boot from eMMC failed.
   → 2023-01: new, fully volatile concept.
   → Return to nominal payload operations.
   → Successfully executed 15–20 different external experiments, including FPGA.

Conclusion

The eMMC memory corruptions and the recovery techniques used to restore operations and improve resilience, can be generalised to many small satellite missions using non-radiation hard memory. The comparative analysis of innovative concepts offers ideas for improving durability and reliability, contributing to more robust future designs.

Contact

- Web: https://opssat1.esoc.esa.int
- Email: ops-sat-experimenter-support@esa.int

References

[1] Maximilian Henkel.
Use of a reconfigurable FPGA in Space to demonstrate new operational concepts.
PhD thesis, Forthcoming.