The HIFI OD 81 anomaly investigations - executive summary

Version DRAFT 0.1 of 23/11/09, by Peter Roelfsema

Abstract

This document contains an executive summary of the HIFI OD 81 investigations and their follow up towards establishing normal operations with the HIFI instrument.

Document: ICC/2009-015
DRAFT 0.9 of 23/01/16
10 pages

Document approval

Prepared by:	Peter Roelfsema	23 November, 2009
Checked by:		
Authorized by:		

Distribution

ESA:

J. Riedinger	ESTEC
J. Perol	ESTEC

HIFI steering committee

F. Helmich	SRON

HIFI project:

P. Roelfsema	SRON
H. Jacobs	SRON

Revision history

Version	Date	Changes	Author
DRAFT 0.1	20/11/2009	First version	P. Roelfsema
DRAFT 0.9	23/11/2009	Various additions	P. Roelfsema

Applicable documents

Doc. ref.	Title

Reference Documents

Doc. ref.	Title

Contents

1 Introduction

On OD 81, after almost three months of successful operations through commissioning and the first part of performance verification, the HIFI instrument stopped producing telemetry in the middle of a standard AOT verification observation.

This document describes at an overview level the analysis process of this anomaly and the conclusions with respect to anomaly cause and mitigating measures to allow safe operation of the HIFI instrument. It includes a high level description of the proposal for changes to be implemented both at instrument level as well as in operational procedures such that observations with the HIFI instrument can be resumed using the redundant chain, as well as the implementation and verification path for those changes.

2 The anomaly

The incident was reported in the evening of Monday 3rd of August, the Mission Operation Centre (MOC) reported HIFI to be in a non-nominal undocumented state (HL_NOMINAL 14) since 22:45z on August 2nd during the execution of a normal AOT. At the time the instrument had switched state the LCU power consumption was found to have dropped from its operational 2.5 Ampere to 0.36 A, and the temperatures of the HIFI–H panel were dropping. Also the LCU was found to be non-responsive to commands sent to it by the HIFI Instrument Control Unit (ICU), nor was it generating values for HK telemetry. In the cause of week 32 HIFI was switched of entirely.

An attempt to switch on HIFI again on Monday 10th of August was unsuccessful; the LCU after switch on continued to consume only 0.36A, however the LCU processor was communicating again with the ICU. The HK reported back showed many fields undefined, consistent with a malfunctioning unit within the LCU. After about one hour of taking telemetry the instrument was again shut down.

3 The investigations

When the anomaly was reported an investigation was initiated at HIFI. This team used the following sources of information for their research:

- The observed behaviour of the HIFI FM before, during and after the anomaly (including the switch on attempt on August 10th), including the detailed timing of reported HK.
- The archives with HIFI data at the HIFI ICC. These archives contain virtually all telemetry generated by the instrument starting with the lab verification measurements in the ILT setup at SRON in late 2005 and continuing through IST, TB/TV and the full flight operational phase.
- Tests on a breadboard model of the LCU digital components containing processor and memory.
- Tests carried out on the LCU IMD3 in the lab at SRON, this is a refurbished QM of the LCU containing full flight representative hardware for the nominal

LCU. Tests were carried out at component level, at subsystem level in subsystem EGSE context as well as in instrument ILT context with the LCU being commanded by the HIFI operations test facility ICU.
- For specific diodes component level documentation and tests of individual LCU FM quality items.
- The HIFI EIDP as delivered with the instrument (issue 6.0), in particular with respect to the detailed LCU schematics and its interrelations with the rest of the HIFI system.
- Circuit modelling for the relevant LCU circuits with the HIFI ripple filter (LRF) and satellite LCL.

Late August ESA instated a Senior Investigation Team to also look at the anomaly to assess the consequences for the Herschel mission and to add to the insight of the HIFI investigations team. Apart from adding new fields and deepening the fields of expertise in the investigation the ESA IT also provided specific additional sources of information on;
- Herschel platform activities during the anomaly
- Data pertaining to the Herschel LCL characteristics
- Data pertaining to the radiation environment in L2 and the relevant SEU susceptibility of LCU components

The ESA IT and the HIFI team quickly joined forces combining valuable insight at all levels from hardware to software and behaviour knowledge from component level to satellite. Jointly the team uncovered the most likely error scenario.

4 The anomaly scenario

Of several scenarios only a single scenario was found to explain firstly all observed behaviour including the event sequence and the detailed timing of that sequence and secondly be consistent with the potential failure modes of individual hardware components:

1. A single event upset corrupted the memory.
2. The bit-flip brought the micro controller in non-communicado conditions.
3. The micro controller jumped to an erroneous program location and started executing program code not intended to be used during normal operation
4. After 1.6 sec. the standby relay was switched bringing the unit from full operational in standby.
5. The resulting voltage transient on the internal 28V bus is fatal for a secondary rectifier diode type 1N5819 in the HRS4 DC/DC converter.
6. The ultimate situation is an instrument in stand-by, with loss of communication and drawing around 0.36A of current.
7. With the instrument in stand-by the significantly decreased power dissipation results in a temperature drop of the unit and consequently the HIFI-H panel.

Of the scenario steps 2-4 have been fully reproduced on hardware in the test environment after a bitflips introduced patching the LCU memory. Voltage transients on the secondary rectifier diodes in excess of their rating are measured to be generated as a result of step 4, however in lab tests the measured transients did not

lead to failure of any flight quality diode. Steps 6 and 7 are reproduced by actively removing any one of18 secondary rectifier diodes in the of the HRS4 DC/DC converter.

5 Mitigation measures

As a consequence of the failure scenario it is concluded that useful operation of HIFI is only possible by switching to the redundant chains. Before the redundant chain is operated a number of mitigating measures are to be implemented to prevent a similar sequence of events to happen on the redundant chain:

- Prevent instantaneous switching from nominal operation to standby through the standby relay
- Minimize the number of nominal transitions to LSU subband 0 and the nominal LCU standby mode
- Consider to disable or eliminate the function switching the standby relay
- Introduce regular/periodic checksum calculations to monitor the LCU memory integrity

Based on the investigation a number of additional recommendations are given:

- To operate the LCU in the temperature range between 10° en 30°C and explicitly avoid a cold start
- To keep the LCU software changes limited and small carefully trading off risk and benefit
- To make an impact assessment for band 7b, the active LO chain at the time of the anomaly, and review the band 7b commissioning approach in view of these findings.

HIFI reliability is reduced firstly due to the fact that only one unit is left which implies that there are now many single point failures in the system. It is furthermore unknown whether or not a diode degradation mechanism is at play under the identified pulsed-stress operating conditions and to what extent transients due to switching and mode transitions might accelerate such a process. Consequently it is not possible to recommend whether or not HIFI should be switched off or simply left switched on when not used for collecting scientific data. Since limited lifetime cannot be excluded for the remaining HIFI mission it is also recommended to prioritize science and make as efficient scientific use of HIFI as possible harvesting key science first and as soon as possible.

5.1 Modifications

A number of modifications will be introduced in the instrument and its operations; these are itemized in the following subsections.

5.1.1 LCU SW modifications

- A change to disable the stand-by switch
- A change to safely switch off LO components in case of an unexpected drop of the satellite bus voltage

- A change to introduce a dissipative mode for each LO subband
- A change to update the possible LCU modes

Note that since the LCU memory is volatile after an LCU power cycle the LCU SW patch must be re-loaded. This implies that, in consultation with the HIFI ICC, normally a manual procedure needs to be invoked after any loss of power to the LCU.

5.1.2 ICU On Board Software modifications

- A change to detect whether the LCU SW has been patched and if it is detected that the LCU SW patch is not loaded discontinue commanding the LCU and notify ground of the condition
- A change to allow regular LCU checksum verification along with the regular HK sampling when HIFI is non-prime
- A change to recognise LCU failure conditions (checksum error, LCU processor not communicating), and when this happens put the system in an appropriate safe mode and notify ground of the condition
- A change to introduce a command to re-enable LCU commanding after that has been blocked following a non-nominal condition

5.1.3 Modifications in other components

- An operational change at CUS level to regularly introduce an LCU checksum verification when HIFI is prime carrying out science observations
- Instrument database modifications to support all of the SW modifications; additional TC's (enable/disable LCU autonomy functions, clear LCU command lock, set LCU dissipative mode), calibration (new LCU modes) and updates of existing out of limits (LCU error conditions)
- Modifications to HIFI flight procedures

5.2 Verification

All modifications are verified on unit, subsystem as well as system level. The system level validation is based on using real flight procedures on the HIFI operational test facility at the HIFI ICC at SRON/Groningen. This facility contains flight representative hardware for all components of HIFI, a satellite CDMS bus simulator, a full SCOS command and control facility as well as the full complement of Herschel ground segment data handling and analysis functions of the HCSS. This allows execution of flight procedures – manual, commissioning as well as MTL engineering and science modes– in an ILT setting on an instrument model. By using the CDMS bus simulator also the interactions between instrument and Herschel platform are realistically validated.

For the LCU SW modifications unit level tests are executed on the digital board test setup at CBK and subsequently they are validated at LCU subsystem level on the IMD3 unit using the LO SCOE.

ICU OBSW validation follows the standard process as is applied for any OBSW update. Firstly unit level tests are done on a simulator at IFSI, subsequently OBSW regression test are done on the HIFI operational test facility.

Database modifications are first syntactically tested using standard HCSS tool such as the MIB ingest procedure. Subsequently the MIB is loaded onto the HIFI operational test facility where it undergoes again a syntactical validation and subsequently a validation by executing standard operational procedures.

System level test involving all components are carried out by running full flight operational scenarios on the HIFI operational test facility. These system level tests validate both the flight procedures as well as the individual components.

6 Operations

The changed operational conditions for HIFI have a few operational consequences;

- Due to the reduced level of redundancy HIFI science observations need to be reprioritized and executed with some speed to ensure that the core science with the HIFI instrument is realized.
- To minimise the number of band switches operational changes are needed at mission planning level to bias scientific mission scheduling towards performing slews to different sources in stead of switching HIFI LO subbands to continue observing the same source at different frequencies.
- If there is an LCU error condition the ICU will stop commanding the unit and thus observations for the remainder of the OD will fail. Recovery from this condition will require ICC inspection of HK and science data and almost certainly will not be possible within the timescale of the DTCP in which it is detected. As a result this condition likely will affect subsequent ODs that have HIFI observations scheduled. The number of occurrences of this condition are hard to predict. It is not unlikely that in the cause of operation enough confidence is built up to instate an automatic recover of this condition, as a result much less observations would be affected.

7 Timeline

The current activities are supporting the following timeline of events:

25 November	briefing by HIFI project to D/SRE
30 November	HIFI anomaly review
~2 December	Switch on readiness review
7 December	HIFI switch one part I - OBSW loading, FCU SFT
11 – 24 January	HIFI switch on part II: - Redundant chain SFT - LO SFT - Commissioning - Safety table load(s)
25 January - March	HIFI PV phase

4 February	HIFI DSB observing mode released for scientific scheduling
10 March	Remaining HIFI observing modes released for scheduling

8 Caveats and open issues

At the time of the anomaly band 7b was active. There is a remote possibility that components of the chain were adversely affected by the anomaly, thus the operability of band 7b cannot be guaranteed until HIFI has been switched on.