esa

DOCUMENT

document title/ titre du document

REPORT OF INVESTIGATION ON HERSCHEL HIFI INSTRUMENT FAILURE

prepared by/*préparé par* Philippe Pérol (TEC-E),

reference/*réference* TEC-E/005.09/PP
issue/*édition*
revision/*révision*
date of issue/*date d'édition* 16/11/2009
status/*état* ISSUE 1
Document type/*type de document*
Distribution/*distribution*

European Space Agency
Agence spatiale européenne

ESTEC
European Space Research and Technology Centre - Keplerlaan 1 - 2201 AZ Noordwijk - The Netherlands
Tel. (31) 71 5656565 - Fax (31) 71 5656040 www.esa.int

APPROVAL

Title *Titre*	issue *issue*	revision *revision*

author *auteur*	date *date*

approved by *approuvé par*	date *date*

CHANGE LOG

reason for change */raison du changement*	issue/*issue*	revision/*revision*	date/*date*

CHANGE RECORD

Issue: Revision:

reason for change/*raison du changement*	page(s)/*page(s)*	paragraph(s)/*paragraph(s)*

Table Of Contents

REFERENCE DOCUMENTS

1. **Mandate of the senior Investigation team (TEC-Q/09.7037)**
2. **ARTS report H-SC-035 of 2009-08-03: Unknown HIFI mode and LOOP 48 Temperature drop**
3. **NCR report SRC/LCU/NC/2005-034 (NCR on DC/DC2)**
4. **NCR report SRON-U/HIFI/NC/2007-06 (NCR on HRS4)**
5. **SRON-U/LCU/TR/2009-001 (test report on DC/Dc converters)**
6. **SRC/LCU/PR/2009-07-56 (test report on injection of bit flips)**
7. **TEC-QEC-TN-CP9-11 of 26/10/2009 :HM65656 and 80C32E SEU Rates on Herschel**

1 INTRODUCTION

On the 2nd of August 2009, after 70 days of operation, Herschel HIFI instrument suddenly stopped working.

This report describes the activities, conclusions and recommendations from the ESA investigation team set in support of Herschel HIFI instrument Principal .Investigator, SRON, in the time frame of September-October 2009 to find the cause of the failure and make recommendation for the possible re-start of HIFI.

When this investigation team started its work, the SRON and Polish Space Research Centre (PAS Warsaw) team had been already at work in the month of August to understand the failure, had gathered a quantity of information, made vital observations and performed a number of tests on representative hardware which allowed to quickly set the team key orientations for this investigation.

Although many of the key experts of the team were not previously acquainted with HIFI, thanks to the outstanding cooperation, in a friendly atmosphere, of all actors involved in the HIFI instrument, at ESOC and in the Herschel project, the status of progress in investigation achieved by the SRON consortium could be understood and endorsed very quickly and from there, everybody worked together in very close cooperation sharing the investigation work according to expertise , discussing the results and elaborating scenarios together.

As a result, significant progress could be quickly made, conclusions derived and recommendations made for corrective actions to be implemented before restart of the instrument on the redundant path.

2 BRIEF EXPLANATION OF THE HIFI INSTRUMENT ARCHITECTURE AND REDUNDANCY CONCEPT

HIFI, the Heterodyne Instrument for Far Infrared, is a very high resolution heterodyne spectrometer instrument. Based on the heterodyne operation principle, it has to produce frequencies to be mixed with the frequencies of the photons collected by the Herschel Telescope to create a signal at a lower frequency which can be amplified and analysed more conveniently. HIFI observe in the range 480 GHz to 1250 GHz and 1410 GHz to 1910 GHz in 7 bands each split over two sub-bands, hence requiring 14 local oscillator chains (see Fig.1 for basic architecture).

The 14 LO chains are not redundant. Each LO chain generates signal for two orthogonal polarizations providing an extra degree of redundancy at mixer and backend level. According to the HIFI specifications, it is acceptable to lose one LO chain.

The Local Oscillator is controlled through a unit called the Local Oscillator Control Unit, LCU, itself supplying a Local Oscillator Supply Unit (LSU). The LCU ensures the connection of the LOU with the Herschel Platform for the provision of electrical power, through a Latching Current Limiter (LCL) on the 28V bus, and for provision of command and control and telemetry through a data bus interface with the Instrument Control Unit (ICU).

The HIFI instrument also includes the Focal Plane Unit and the Focal Plane Control Unit (FCU) which has its dedicated power supply and command and control and telemetry interface with the ICU.

Then there are the 4 intermediate frequencies processors, 2 for each polarisation, a high Resolution (HRS) and a Wide Band (WBS). The processors are separately supplied from the bus and also provide their data separately to the ICU.

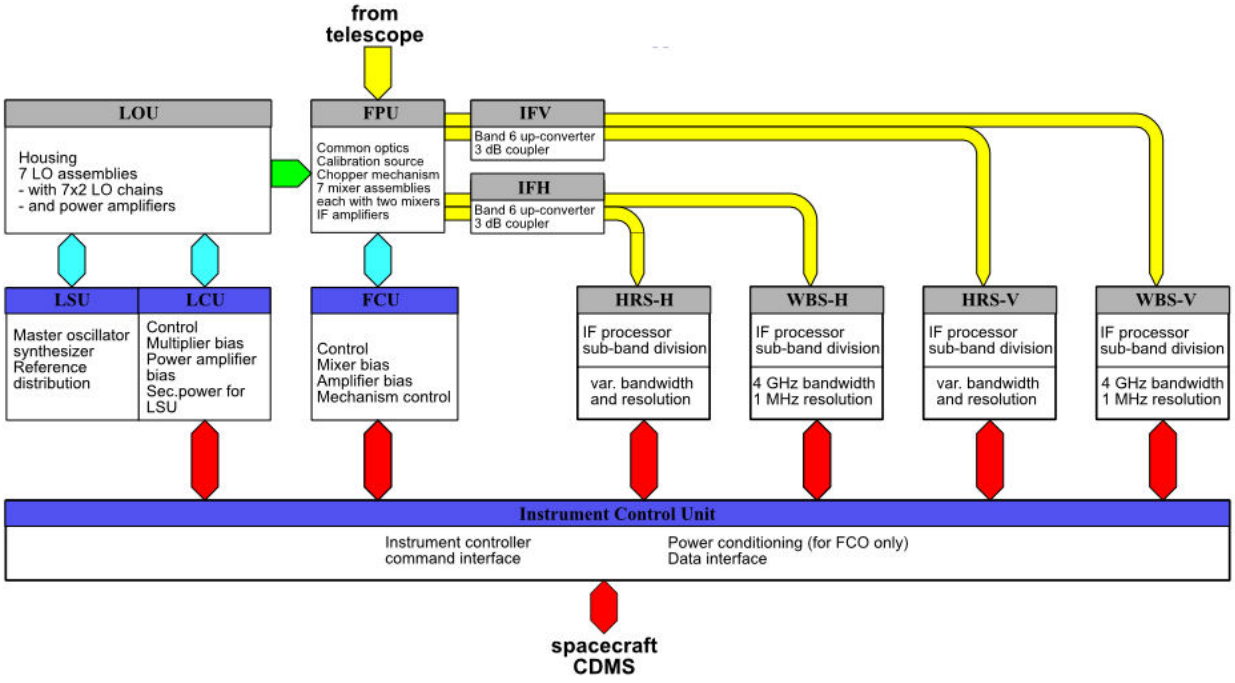

Figure 1: Architecture of HIFI instrument

3 LCU ARCHITECTURE AND FUNCTIONALITIES

A simplified description is given to understand the thread of the investigation (see also Fig. 2).

The Local Oscillator Control Unit supplies power, command, control and telemetries to the Local Oscillator Unit and selects the operational chain for the requested frequency and supplies the chain up-converters and amplifiers, with the required bias and supplies.

The LCU is completely redundant, i.e. there are two independent interfaces to the electrical supply with two separate LCLs, supplying fully redundant data subsystem and interface to the ICU of a redundant data subsystem .It operates in cold redundancy, i.e. only one of the 2 LCL is activated at a time and only one ICU interface is powered.

Since the 14 Local Oscillator chains are not redundant, there is an or-ing of the supply bias current coming from the nominal or the redundant LCU path with a relay driven selection system.

The power supply part within one LCU supply path (one nominal and one redundant) is composed from 7 DC/DC converters fed from the Herschel platform LCL through a filter. These 7 converters are divided in 2 groups, a first group of 3 converters called HRS 3, HRS4 and DC/DC 3 is immediately supplied at turn–on of the LCL and a second group of 4 converters (HRS1, HRS2, DC/DC1 and DC/DC2) is only activated by activation of the stand-by relay and are coming into play for the nominal operation.

As a result of this two stage operation, the input current to LCU in stand-by mode is around 1Ampere and in nominal operation with an LO chain active around 2.5 Amperes.

DC/DC 3 is the converter supplying the data system of the LCU, (microcontroller, memories and Field Programmable Gate Array (FPGA.). HRS4 complements the supply of DC/DC 3 by supplying the A/D converter for the telemetries. Thus, if DC/DC3 and HRS4 converters work nominally the whole data chain of the LCU is supplied nominally. HRS3, also active in stand-by mode, is supplying heater power to pre-condition the temperature of the LOU.

The data subsystem of the LCU is composed for each path, nominal and redundant, of a microcontroller supported by a read only memory (ROM) and a random access memory (RAM) memory and interfacing with the LCU various circuits through an FPGA which essentially implement some combinational interface logic. The microcontroller interfaces with the ICU through the FPGA via a serial data-bus from which it receives its command and through which it supplies its telemetries.

At switch–on of the LCU, the software to be executed and the various data tables used to check the settings of the bias of the various bands, are copied from the ROM to the RAM.

As a standard operation, after the initial switch-on of the instrument, the LCU software is patched in the RAM to correct deficiencies of the resident software in the ROM and to upload the latest LO tuning safety tables.

During operation, and since the instrument is never turned-off, there is no further refreshment of the content of the RAM. No watch-dog mechanism or EDAC system is implemented. For operation of the instrument, the ICU sends the command to change band selection, set the bias and request telemetries.

The main protections designed in the system are:

- In case the Herschel bus voltage would fall below 20V, the instrument directly reverts to stand-by
- In case the bias current of the selected band is too high, after execution of a small routine, the instrument reverts to stand-by
- In case of frequency multiplier lock, also after execution of a small routine, the instrument reverts to stand-by.

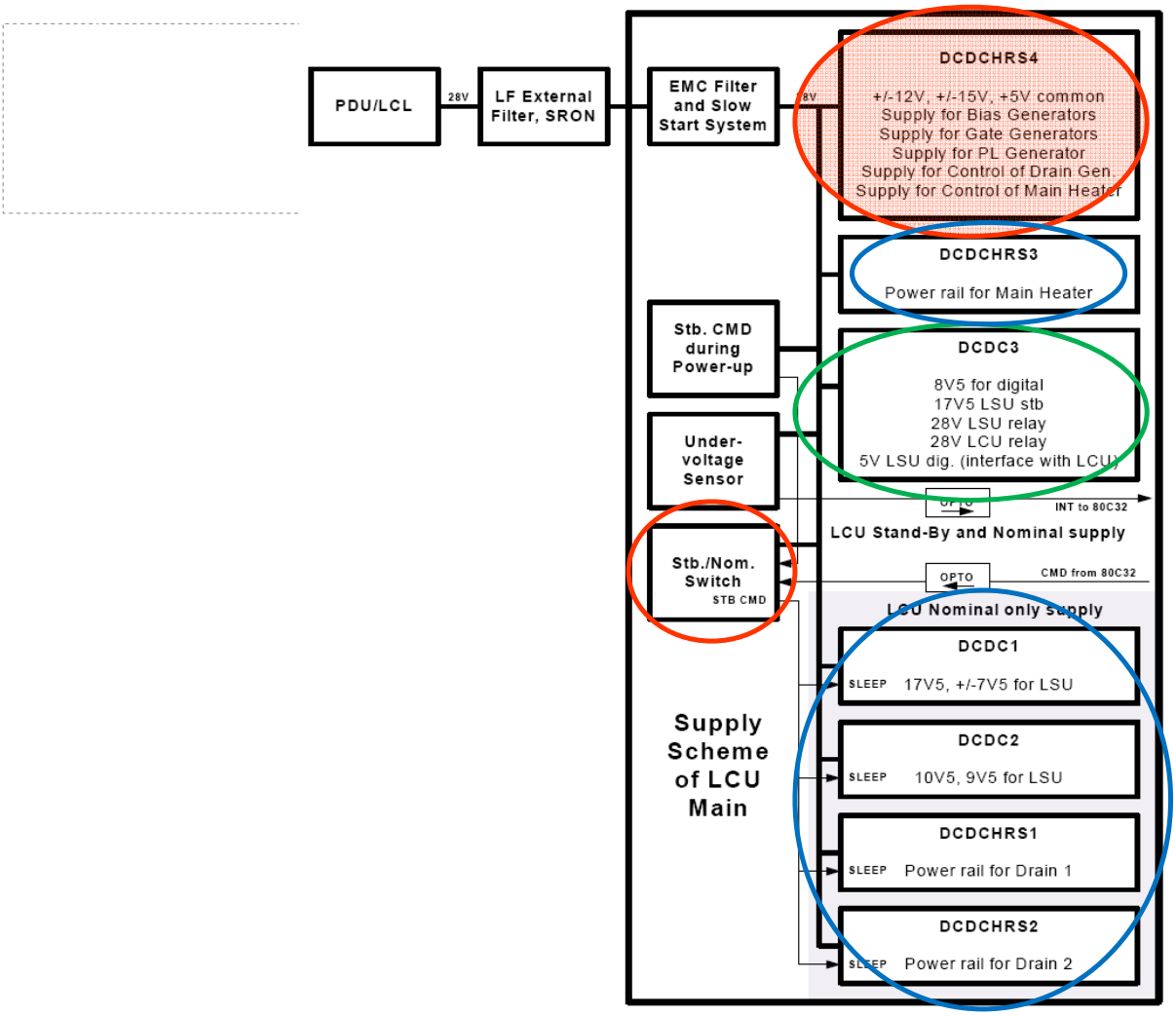

Figure 2: Supply scheme of LCU

4 IN ORBIT FAILURE OBSERVABLES AND GENERIC FAILURE SCENARIO

The in-orbit failure observables have been, on the 2nd of August, a sudden drop of bus supplied current from 2.5A down to 0.36A with a loss of communication of the unit with the ICU, thus with no more data received from the instrument and no way to send commands to it : the LCU is in an “autistic” state.

From the level of current observed, it was realised that a possible scenario was a passage in stand-by of the LCU associated with an abnormal operation of DC/DC converter HRS4. The link between the current drop with the loss of communication with the ICU could not be readily established.

One day later, the instrument was then switched-off by switching-off the Latching Current limiter of the platform. On the 10th of August, an attempt at restart was made. The same abnormal level of 0.36A of current was found in the stand-by mode but the communication with the ICU was recovered although no telemetries were available, pointing to the same problem with HRS4 converter.

5 INITIALLY DISCARDED SCENARIOS WITH RATIONALE

The inquiry team was looking, a priori, to a single failure scenario, but keeping in mind that a single failure may propagate. The 3 elements witnessed on the 2nd of August –drop of current, loss of communication and likely passage in stand-by – were, if possible, to be reconciled with one cause and induced effects.

No requested activity on the instrument was taking place at the time of the failure such as an observation band change. It was verified by ESOC that no abnormal activity or event happened on the platform, e.g. such that would have created a large transient on the power supply or an abnormal command of the LCU or any disturbance to the instrument..

All failure modes of the LCL were also analysed and excluded as a possible cause of abnormal low current supply to the unit. No abnormal activity was recorded on the radiation monitor on board Herschel, but this did not exclude the possibility of a Single Event Upset (SEU) due to a cosmic ray.

6 TWO AVENUES OF INVESTIGATION: ON THE DC/DC CONVERTERS AND ON THE LCU DATA SYSTEM, COMMAND CONTROL AND CODING

A very important observation made by the HIFI team while investigating detailed instrument telemetries received just before the event implied that when communication was lost with the LCU and for around 1.6second after, the local oscillator was still supplied nominally as could be derived from the telemetries of the intermediate frequency processors. This would imply that the anomaly started in the LCU data systems and could have induced a reaction on the power system after circa 1.6seconds… (As a reference the reboot of the microcontroller takes about 1.2 seconds. So 1.6seconds may correspond to some software execution including a reboot which brings the instrument in stand-by.)

Resulting from the observations that the 0.36A observed in stand-by implied an anomalous behaviour of the converter HRS4 and that the analysis of telemetries implied that the anomaly may have first originated in the data subsystem, the investigation was led along two avenues:.

- On the one hand to review in detail the design of the power system of the LCU (7 DC/DC converters), the possible failure modes and the behaviour in nominal and transient modes (start-up, stand-by and nominal), also looking back at two NCRs during ground development caused by the failure of a Schottky diode 1N5819, one for HRS4 converter and one DC/DC2 converter.

- On the other hand to review in detail the data systems embedded in the microcontroller supported by an FPGA and ROM and RAM memory to review effect of interrupts, identify possible initiation of unforeseen actions or conflict of tasks resulting in unexpected actions, and in general anything that could result in an activation of the stand-by relay

It has to be noted that a fully representative model of the LCU (one path) exists at SRON Groningen, allowing to perform representative tests and thus reproduce seen effects in orbit. At the Space Research Center in Warsaw, also models of the DC/DC converters exist and a digital control board allowing to check the software.

7 RESULTS OF THE DC/DC CONVERTERS DESIGN ANALYSIS AND TESTS

The analysis of the 7 converters was facilitated by the fact that they use exactly the same design for auxiliary supply, command and control and primary switching stage. They only differ according to the secondary windings and rectifiers of the required secondary supply, but even there, they obey similar design rules the choice of secondary rectifying diodes according to the transformer turn-ratio.

All voltages and currents levels and all waveforms in the converters could be measured on the representative hardware at SRON.

The design was found to be well thought–out and the control loop stable but a criticality was found in the choice of Schottky diodes of 45V rating (ref 1N5819-1), for the turn ratio 7 to 4 from primary to secondary in the converter transformer. (16 diodes concerned in HRS4, 4 diodes in DC/DC2).

Although the derating is in principle correct in voltage level, when commutation spikes, (which are not sufficiently dampened), are included, the maximum non repetitive reverse voltage recommended by the manufacturer is exceeded at each switching cycle by about 5V and this situation is made worse in some transient modes, such as going from nominal to stand-by. For converter HRS4: the diodes are clearly going into avalanche, with voltage level reaching 60V.

During the ground development programme, in 2 different occasions, the Schottky diodes with these 7 to 4 ratios have failed. . Once on HRS4, once on DC/DC2 .In both instances explanations were provided, for one (HRS4) indeed recognising an additional voltage stress during an accidental operation during EMC test (this failure case was re-tested during this investigation and confirmed to be plausible) and for the other (DC/DC2) an excessive temperature effect which was corrected. In both instances the anomaly was treated thoroughly, but the marginality of the voltage rating was not detected.

8 RESULTS OF THE LCU DATA SUBSYSTEM ANALYSIS AND TESTS

This analysis focused initially in identifying all means by which the unit could be brought suddenly in stand-by (i.e. not due to a request to change frequency band) and by which the unit could end-up in an “autistic” state.

It was verified that since the Herschel bus voltage never went below 28V, although the undervoltage protection is relatively sensitive (needs tens of microseconds of undervoltage to react) there was no credible scenario for this protection to have been activated .Also it would not explain the loss of communication.

Likewise, if there had been an overcurrent in the bias current of the band currently used or a frequency multiplier lock this could have led to stand-by through the interrupt 0 created by the detection circuitry, but would not explain a loss of communication.

However, one issue to consider could be a conflict of interrupt in the microcontroller not properly handled:

The undervoltage overcurrent and multiplier lock create an interrupt in the microcontroller, to be handled in priority (Interrupt zero). Also requests from telemetries by the ICU generate an interrupt (Interrupt 1). Could it be that a certain timing pattern between those two requests for interrupt could an unresolved conflict, ending in an “autistic state” of the LCU and stand-by mode?

If reproduced, could a duration of around 1.6s be estimated between the loss of communication and going into stand-by?

Analysis of the LCU software shows that such interrupt clashes should be handled properly. Thanks to the availability of representative hardware, this analysis could be verified. Sequences of interrupts were tested with nesting of interrupt 1 within interrupt 0 and reciprocally. In no instances did the system lose control and come into an “autistic” state.

The second line of analysis was related to the absence of EDAC of the RAM memory and the possibility that it would degrade with bit-flips due to single event upsets (SEUs) over time.

The RAM used as a sensitivity threshold of around 1.7 MeV cm2/mg, which is not very high and the manufacturer, ATMEL, usually recommends using it associated with an Error Detection And Correction (EDAC) scheme.

Not all RAM memory capacity implemented is used for the LCU programme, and within the part used, only a limited area contain the critical lines of code that, if corrupted by bit-flips, could result in anomalies.

A checksum verification system is implemented but not routinely used.

Could it be that bit flips in some code lines would result in a loss of communication and activation of the stand-by relay after about 1.6s?

Again, thanks to the representative hardware and a possibility to operate it in diagnostic mode, changing bits in the desired code bytes, it was possible to reproduce scenarios of bit flips in the RAM and witness the consequences.

Different bit flips tests (one bit flip at a time) resulted in both the autistic state of the LCU and the activation of the stand-by relay, but with different timing between the loss of communication and the stand-by state such as 1.2 or 1.3 seconds and for one line of code different bit flips on this line resulted 1.6 seconds, as derived from the failure observables.

In total, out of circa 300 individual bit flip tests, 10 resulted in the autistic and stand-by effect.

9 RETAINED FAILURE SCENARIO WITH EVIDENCE

As a result of the analysis described above, both on the converter side and data system side, the following failure scenario has been adopted as the most probable.

- While the HIFI instrument was working nominally on the 2nd of August, an SEU created a bit change in the RAM. The RAM is sensitive to SEU with a threshold of only 1.7MeV (20 times less than needed to be SEU "resistant") and according to TEC radiation specialist analysis could be subject to such event from a few days to a month. (In the first months of operation, no effect of event was witnessed, but it does not preclude that such bit changes happened in an unused part of the RAM or data tables without revealing a problem.)
- This bit change led the programme currently executed to bring the instrument in autistic mode and, after 1.6seconds, in stand-by mode. (Such bit flips sending the instrument in stand-by mode after 1.6s have been reproduced on the ground equipment. According to the bit involved, some bit- flip tests have resulted in the instrument going in stand-by with other timings such as 1.2 or 1.3seconds only. About 10 different bit flips reproduced the problem, out of 300 bit- flip tests of software)

There are still analyses on going to see whether there would be other mechanisms for the first 2 stages of this scenario, but what is sure is that *there are clearly mechanisms* to suddenly activate the stand-by relay.

- The sudden stand-by command, with full bus voltage, results in the stand-by relay to be activated and isolating the 4 converters downstream , creating a load transient on the 28Vbus, reflected in an overvoltage transient of 3-4V above the nominal 28V on the primary of the remaining DC/DC converters connected (HRS4, HRS3, DC/DC3), (These transient voltages have been reproduced on the representative hardware)
- The voltage transient on the primary of the converters, creates voltage transients on the secondaries, in particular for the Schotty diodes in HRS4 converter on the windings with 7 to 4 turn ratio, bringing these diodes in avalanche at around 60V (also reproduced and measured by test). A diode (16 possible diodes are concerned: D 20 to D27, D40, D41, D46, D47, D50 to D53) fails due to that stress which had not been tested and verified during the ground testing of the instrument.(The failure has not been reproduced by the test on ground equipment)
- The resulting situation is an instrument in stand-by, with a loss of communication and drawing around 0.36A of current (normal stand-by current is around 1A, but with HRS4 failed, the calculated current drawn by the remaining converters and HRS4 low level supplied on the primary is estimated to 0.36A (+/-30 mA) as has been observed on the 2nd of August.
- On the 3rd of August, the instrument is switched-off with the platform bus LCL. When the instrument is restarted on the 10th of August , it goes in stand –by mode- as per the normal sequence at switch-on -and the current drawn is again 0.36A (effect of the HRS4 failure) but the communication with ICU is re-established, (although ,due to the failure of HRS4 ,with no supply voltage for telemetries processing). The possible reestablishment of

communication is due to the reset of the RAM with the ROM content, thus having no bit flip and no anomaly in the digital data system any more..

A complete failure scenario, originating in a SEU in the RAM but propagating to a stressful transient on one DC/DC converter resulting in a hard failure has been convincingly analysed and supported by evidence.

This scenario described excludes any failure in the non redundant part of the instrument, such as overcurrent in Band 7 or multiplier lock. Which means that full operation of the instrument could be resumed with a healthy redundant LCU path.

Tests on the effect of multiple interrupts such as would be caused by an overcurrent protection oscillating around its threshold are still outstanding, but the interrupt management has so far be found healthy. You would have to find that multiple interrupt, besides throwing the stand-by switch, end-up in an autistic state.

10 RECOMMENDATIONS FOR CORRECTIVE ACTIONS BEFORE SWITCHING OVER TO THE REDUNDANT PATH

The occurrence of the failure is the result of a combination of hardware weaknesses and the execution of software in the microcontroller of the instrument. Unfortunately, nothing can be done to change the hardware implemented.

The correctives measures to be implemented must result in:

- Suppressing or reducing to the minimum, any voltage transients on the DC/DC converters using a 7/4 transformer turn ratio associated with the Schottky diodes 1N5819. This applies to HRS4 converter , but also .DC/DC 2, which implement Schottky diodes with 7/4 turn ratio (but downstream from the stand-by relay)
- In particular, the possibility of throwing the stand-by switch when the LCU is running nominally with nominal input voltage must be removed by modification of the software. In principle, this is a trivial change, although some care has to be taken in analysing the behaviour of the system after a power drop on the satellite bus.
- Review the LCU software to prevent the “autistic” state, which was the incident at the origin of the failure. Since the microcontroller and its associated RAM has no EDAC system, effects of possible bit flips in the critical code lines should be overcome by resuming correct operation without major reset or going into stand-by. Systematic use of the checksum capability is recommended as part of the corrective action. If this issue cannot be solved, when an autistic situation occurs, the only way to reset the LCU will be by power cycle of the LCL (which should be avoided) and in that case, the stand-by switch will be left on and the instrument will restart in this anomalous situation….
- Review the software to make sure there are no unexpected going into stand-by. Only when a real anomaly case occur and always with a soft load transients.

- Although no conflict of interrupt was witnessed resulting in unexpected status, once the software is modified, retest all possible combinations of interrupts with the modified software.
- When restarting on the satellite, do not start to exercise band 7 first! Just in case…
- Since the ROM cannot be modified, but a critical patch of software will be necessary in the RAM to correct the instrument control, consider to have this software patch resident on board the spacecraft to have it automatically implemented from the spacecraft main computer memory, through the ICU to the LCU RAM in any situation of utilisation of the instrument and not sent each time from ground. It is however understood that there is today a well established procedure to modify the RAM content from ground.

11 DISCUSSION ON RELIABILITY OF OPERATION ON REDUNDANT PATH AFTER SOFTWARE CORRECTIONS

The hardware cannot be corrected on the redundant path of the LCU: The bus voltage of Herschel cannot be adjusted to a lower value, so the LCU DC/DC converters nominal operating points cannot be changed and the nominal stress in particular on Schottky diodes 1N5819-1 will be the same. (16 diodes in HRS4 and 4 in DC/DC2)

From the characterisation, stress tests and endurance tests done so far during this investigation, on the Schottky diodes 1N5819-1 of the same lots used for the HIFI DC/DC converters, it seems that the avalanche voltage of the diode is well grouped in the range 57 to 60V.

In nominal operation of the converter, the switching spikes have been measured on the ground representative model not to exceed 56V, so that one could be confident that nominal operation should not be stressing, although no manufacturer will guarantee it.

Then, there is the effect of the converter transients (switch-on, switch-off, going from nominal to stand-by.)

The instrument is always kept on in stand-by mode. So, apart from the initial switch-on transient, which has been verified to be very soft, the transients are those corresponding to the transition from nominal to stand-by. Each time there is a change of observation frequency band, there is a return to stand-by before selection of the new band, which in principle is a smooth transient, resulting in an increase of voltage on the diode of 1.5 to 2V which has been performed hundred of times during the 70 days of operation of HIFI without failures.

The belief is that there is probably a certain dispersion of the diode characteristics, outside the domain guaranteed by the manufacturer, in the avalanche energy absorbable before breakdown:

5 diodes from the Herschel HIFI flight lot have shown robust behaviour, much above in energy of what is supposed to have killed the Schottky diode in orbit. But statistics with 5 items only are difficult. In setting the test, a commercial diode of the same type was failed…Gathering more diodes and extending the statistics to several tens of items could reinforce the confidence level or give a better insight.

If, following some adjustments of the operations with a new software, as per first recommendation, the load transients can be smoothed to represent, e.g. only a fraction of volt above the nominal 28V, one can be confident that the situation is probably safe, with no entry into avalanche during the transients.

The unit is operated at relatively low temperature and in the HRS4 converter, the current load is low. If there was a time dependant wear-out effect due to the nominal stress the diodes in the DC/DC converters, DC/DC 2, having much more current in the diode and thus operating at higher temperature would be more at risk. No time dependant wear-out phenomenon was found reported for this type of component. On the contrary, it seems that it is rather an effect of threshold of acceptable reverse energy for each component.

12 LESSONS LEARNT

Two design weaknesses are seen at the origin of the failure of the LCU .and one test coverage oversight.

Derating of Schottky diodes:

It has been the principle in switching converter design that the components should be derated for the switching levels and that switching spikes should remain within rating.

This message is sometimes disputed by the community of designers if the spikes are very short and the excess very small with regard to the component rated voltage (e.g. 2-3V excess on a 100V component). Here we have a case of 8V excess spike on a 45V component with transients up to 15V in load transitions situation. The diode is used far outside the specification

This diode is not avalanche rated by the manufacturer. There can be a large dispersion of avalanche current capability between parts…

As soon as one exceeds the maximum rated voltage or current of a component manufacturer, even in a short transient mode, but at a repetition rate, one enters a grey area where nothing can be certain and the manufacturer himself will not guarantee anything. So, it is wise to be eliminated by design.

Test coverage:

The throw of the safety stand-by switch at nominal input voltage was never tested on ground. It was never realised that this could happen and represented a worst case transient for the power system of the LCU.

Use of RAM without EDAC or watch-dog

The second design weakness was the use of a RAM, with relatively low SEU threshold without an error detection and correction system, which is always recommended for such design. The issue was underestimated, possibly as a result of poor or unclear specifications in that area and lack of designer awareness.