Technical note on the new functionalities for HIFI LCU SEU recognition
DT/AdJ/CR/AdG/LD/MM – 30-03-2010

Following one of the recommendations from the review board after the HIFI Anomaly review which took place in Utrecht on November 1st 2009, HIFI has looked into the possibility to perform checksum verification in a segmented fashion, in order to distinguish between various levels of criticality when an SEU is detected in operation. This technical note describes the results of this implementation. A test report will be appended to it whenever available.

1. Segmented checksum concept

The LCU memory has been broken down into 4 categories:

- "Critical": covers all program code area addresses which, if affected by a bit flip, would prevent a memory repair by the mean of the standard upload procedure currently in place. Depending on the very place where the bit flip has occurred, a power cycle of the LCU would be required to recover operations of HIFI
- "Safe": covers all program code area addresses which, if affected by a bit flip, would not prevent repair by the mean of the mean of the standard upload procedure currently in place. This is the complement of the Critical area (only covers program code area), minus the "Unused" area (see below)
- "Table": covers the LCU safety table areas. Those addresses do not affect the execution of the LCU S/W. They store parameters which are needed to protect the LOU chain when they are tuned. Each of the 14 bands has its own set of entries in this table. Note that this table area covers almost 2/3 of whole LCU memory.
- "Unused": cover all program code area which contain no code, and therefore would have no effect at all in case they would be corrupted.

In the present LCU implementation to support the above approach, the Critical area is about 800 bytes in size, in comparison to the full 32kbytes size of the memory (this is about 2.5% of the full memory and 7.5% of the code area).

The idea is to check each of the above areas in a separate command, and act accordingly. The main changes with the current scheme, where the full memory is checked, are the following:

- Upon checksum mismatch in one of the four cases mentioned above, the 5,4 report issued by the OBSW will inform the ground more accurately about the criticality level, even before the memory dump is performed. This will indicate directly to the recovery team which of the procedure branches has to be followed.
- The table area will only be checked for the active band at the time of the observation. If a corruption occurs somewhere else in the table the OBSW will take no action as it will not notice and the observations in the active band

will proceed, limiting therefore the risk of losing science observations when the memory corruption does not justify it

- When the corruption is found in the Unused area, the LCU will not be disabled and but the transition to standby1 will take place.

2. Involved changes in the LCU S/W

The implementation of the above scheme requires a new LCU patch (currently called version 2.4). The detailed description of the changes can be found in the technical note SCR/LCU/TN/2010-0776 attached to this document. Also attached is the corresponding LCU memory map, with Critical area marked as Red.

3. Involved changes in the OBSW

The implementation of the above scheme requires a new OBSW (currently called 6.4.0), which will feature the following changes:

- A new command (see also MIB changes) will allow to pass on a list of LCU memory addresses, lengths, and associated checksums, to be looped over by the OBSW, and which will eventually compare the concatenated checksum to an expected value passed on by the CUS
- The new command will allow to fully controlling the action to be taken upon checksum mismatch. Those actions can be:
    i. Block or no the HK and commanding capabilities to the LCU. This action is the default in the checksum scheme currently in place
    ii. Disable or not the LOU band for which the table area verification has been performed
- The new command will issue three new types of 5,4 event packets:
    i. When the checksum mismatch is found in the "Critical" area, the new packet has code "*H_LCUCRCNOK0*". The associated report "*HIFI_R_LCUCRC_mismatch_critical*" will indicate the expected checksum, the effectively measured checksum, and the fact that we are dealing with a Critical area.
    ii. When the checksum mismatch is found in the "Critical" area, the new packet has code "*H_LCUCRCNOK1*". The associated report "*HIFI_R_LCUCRC_mismatch_safe"* will indicate the expected checksum, the effectively measured checksum, and the fact that we are dealing with a Safe area.
    iii. When the checksum mismatch is found in the "Critical" area, the new packet has code "*H_LCUCRCNOK2*". The associated report "*HIFI_R_LCUCRC_mismatch_table*" will indicate the expected checksum, the effectively measured checksum, the fact that we are dealing with a Table area, and the bandmask that was applied to disable the active LO chain. This bandmask will inform the ground about which band was affected by the memory corruption
- Note that the current functionality (full LCU memory check) will be maintained and will still be the basis of the autonomous function activated

when HIFI is non-PRIME. The 5,4 code “H_LCUCRCNOK” is therefore maintained too.

More details about the implementation can be found in the OBSW 6.4.0 release notes, attached to this document.

4. Involved changes in the MIB

The implementation of the above scheme requires a new MIB (currently called 2154, or ASPI 11.16), which will feature the definition of the new command and TM packets are described in the OBSW section. The details about the new TC can be found in the TC ICD v1.11 (section 4.3.14.9) and TM ICD v1.12 (section 4.3.3.2.13 to 4.3.3.2.15) attached to this document.

5. Involved changes in the CUS backend

The changes in the CUS are at two levels:

New configuration files:

- The CUS will now store three new configuration files which will provide to the OBSW the list of addresses, lengths, and associated checksums to be checked in a loop fashion for each memory areas:
  - LcuAddressCodeCritical_R.config: contains the above information for all blocks involved in the Critical area. This file changes with each new LCU patch, and is provided by the LCU S/W team as part of the new LCU patch delivery. This file is not changed when only LCU safety tables are to be updated.
  - LcuAddressCodeSafe_R.config: contains the above information for all blocks involved in the Safe area. This file changes with each new LCU patch, and is provided by the LCU S/W team as part of the new LCU patch delivery. This file is not changed when only LCU safety tables are to be updated.
  - LcuAddressCodeUnused_R.config: contains the above information for all blocks involved in the Unused area. This file changes with each new LCU patch, and is provided by the LCU S/W team as part of the new LCU patch delivery. This file is not changed when only LCU safety tables are to be updated.
  - LcuAddressTable_R.config: contains the above information for all blocks involved in the Table area. This file changes with each new LCU safety table, and is provided by the LCU S/W team as part of the new LCU patch delivery. The address locations and lengths in this file are fixed. Only the checksums change with new safety tables. This file is not changed when only an LCU patch is to be updated.

Upon reception of the above files, a systematic verification that all inputs are compatible with the LCU image that will be in used will be performed on the flight spare prior to roll-out to a new mission configuration.

New checksum verification scheme:

In the current scheme, we distinguish between two circumstances: 1) when HIFI is non-PRIME instrument, the full LCU memory is checked on the basis of an hourly autonomous verification performed by the ICU, 2) when HIFI is PRIME instrument, the full LCU memory is checked at the start of each obsid.

The situation when HIFI is non-PRIME will be un-changed. The new approach applies to when HIFI is PRIME instrument:

- At the start of each obsid, the three memory areas will be checked on after the other. The table area will be limited to the active band.
- At the end of each obsid, we would check for the last time the table area applicable to the band concerned. This is to monitor a possible corruption in that band table area during the last running obsid, which will not be flagged since the next obsid uses a different band. The time overhead for this is negligible (2 sec).
- At the end of each OD, in the transition to Dissipative_II, a check of the full table area will be performed to monitor the state of that memory area in bands which have not been covered over the OD, and therefore would not have been checked by any of the means described in the above two bullets. The tables will be treated as one single block of contiguous addresses, and therefore the overhead and number of TC (only 1) added is limited to its minimum. Following this, the Unused area will also be checked, since it is not during the rest of the OD and only the autonomous function used in non-PRIME periods would be able to detect it otherwise (because it covers the full memory). In both cases, no locking of the LCU HK and commanding will be involved upon detection, only a transition to standby1 and the issue of a 5,4 packet.

6. Involved changes in the recovery procedures

There is only limited update to the existing procedures. On the one hand, the improved recognition scheme will allow to assess the level of criticality even before the dump is performed. The dump remains a mandatory part of the recovery procedure as it provides a precise idea of where the corruption occurred, and indeed confirmed the level of criticality indicated by the event report. On the other hand, the new codes for SEU reports need to be taken into account in the first steps of the procedure and all the information held by this report should be communicated to the HIFI person(s) on-call.

One of the differences is that HIFI could be hit by an SEU but still not be found with the LCU DISABLED (Red OOL) and therefore still collect HK. This is because some memory corruptions will not be severe enough to deserve interruption of the operations. What will however be always observed is 1) that HIFI in standby1 mode when entering the DTCP (instead of the dissipative mode), 2) there will a (5,4) informing about the nature of the memory corruption.

The other new feature is that the CRP should consider the possibility to put HIFI back into the dissipative mode that may have been exited by the recovery procedure. A set of procedures to do so exists but their application in the CRP is not yet present. This should be added to the end of the CRP's.