Avoiding Cluster Safe Modes

I. Clerigo[*]
LSE Space GmbH, Wessling, 82234, Germany

S. Sangiorgi[†] and J. Volpp[‡]
European Space Agency, Darmstadt, 64293, Germany

Cluster is a multi-spacecraft ESA mission launched in 2000 to study the Earth's magnetic environment. After more than 11 years in space, the performance of the batteries and the solar arrays has decreased dramatically limiting the available power on-board. This is becoming a serious problem for contingency situations because hard-coded sequences executed during safe modes require much more power than what it is provided by the solar arrays. As a consequence safe modes are no longer safe and they can trigger main bus under-voltages, multiple reboots or even an uncontrolled switch off of the on-board computer. Several techniques have been studied to avoid or minimize the impact of safe modes and have been successfully implemented and validated during 2011 eclipse season. An analysis of Cluster safe modes with limited power and the alternatives to deal with them is the subject of this paper.

I. Introduction

Cluster is a mission of the European Space Agency to study the interaction between solar wind and the Earth's magnetosphere with emphasis on small-scale three-dimensional structures which require simultaneous 4-point measurements.[1] The four identical spin stabilized spacecraft, each one carrying a set of 11 instruments, fly in formation orbiting the Earth at a distance between 1,000 km and 135,000 km with a period of 54 hours. Eclipses occur during all phases of the mission. The longest ones can last up to four hours in the so-called long eclipse season.

After the ill-fated launch of Ariane 5 in 1996 which destroyed the original Cluster-I mission, the spacecraft were rebuilt and were launched in July and August 2000 on two Soyuz rockets from Baikonour in Kazakhstan. Routine operations started on February 2001 after instrument commissioning. Designed originally for 27 months, the Cluster satellites have now been flying for almost 12 years. With the spacecraft and most of the payloads still capable of providing valuable science, the mission has now been extended for the third time until 2014 with a mid-term review in 2012. Multiple upgrades of the ground segment have been performed during this period in order to adapt the mission to the new technologies and the evolving ESOC infrastructure, to save costs and to cope with new operational constraints imposed by the natural orbit evolution and the spacecraft ageing.[2]

Cluster is a non-real time mission. All routine payload operations are planned based on the inputs from the instrument teams by the Joint Science Operations Centre at Rutherford Appleton Laboratory, in the UK. The mission is controlled by the Cluster Flight Control Team (FCT) supported by the Flight Dynamics team from the Operations Control Centre (OCC) at the European Space Operations Centre (ESOC) in Germany. The OCC is the primary interface with the spacecraft through the European Space Tracking network and is responsible for monitoring and control of the entire mission.

The FCT routinely plans the ground station passes, executes the uplink of the time tagged commands for the next two or three days and recovers the science data stored on the on-board Solid State Recorder (SSR). Real-time interactive operations are limited to special events like manoeuvres and eclipses, together with contingency

[*] Spacecraft Operations Engineer, ESA/ESOC, HSO-OPC, Robert-Bosch Strasse 5, 64293, Darmstadt, Germany.
[†] Spacecraft Operations Engineer, ESA/ESOC, HSO-OPC, Robert-Bosch Strasse 5, 64293, Darmstadt, Germany.
[‡] Spacecraft Operations Manager, ESA/ESOC, HSO-OPC, Robert-Bosch Strasse 5, 64293, Darmstadt, Germany.

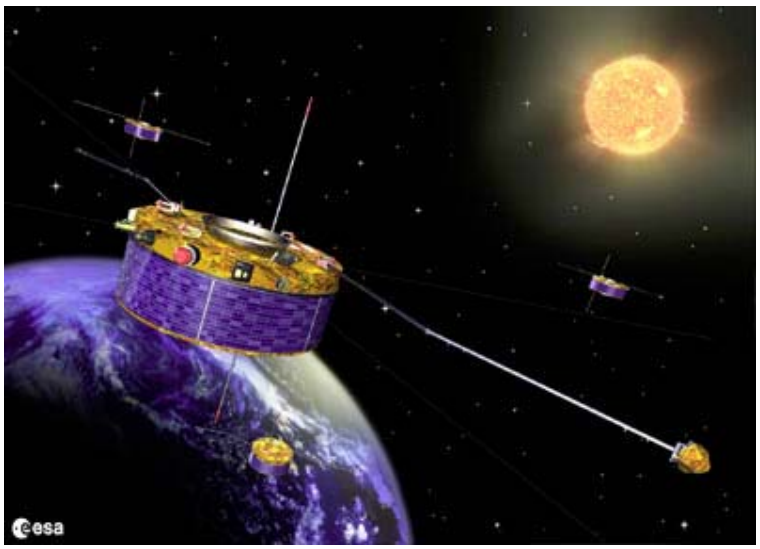

Figure 1. Artist's impression of the Cluster which are named Rumba, Salsa, Samba and Tango. Image: ESA.

recoveries and anomaly investigations. The data are distributed to the Cluster data disposition system where they are accessible via Internet from the principal investigators and transferred to the Cluster Active Archive open to all the Cluster user community.

The paper is organized as follows. Section II provides an overview of the current level of the degradation of the power subsystem and its consequences. Section III and IV describe Cluster safe modes and the associated risks when available power on-board is limited. Section V presents the strategy and workarounds implemented to avoid the negative side effects of safe modes during eclipse operations and section VI analyses how to extend the same principles to routine operations. Section VII concludes.

II. Spacecraft Ageing and Operational Implications

All four Cluster spacecraft are healthy and all redundancies are available except a few failed payloads. Most of the problems are concentrated in the power subsystem and related to the expected ageing of the batteries and the solar array.

A. Solar Array Degradation

The evolution of the Solar Array Power (SAP) since the beginning of the mission is presented in Fig. 2. Due to the natural ageing of the solar arrays, from launch to January 2008, normalized SAP has decreased by 23mW per orbit on average. Between January 2008 and July 2009 and from January 2011 onwards, Cluster orbit has been crossing the inner radiation belt and the degradation has severely increased (up to 120mW per orbit in the worst period).[3]

This has many implications and has introduced new operational constraints which have been extensively discussed in Ref. 2 (e.g. applying power sharing techniques to share available power between the payload and the transponder). Furthermore, as it will be presented in the next sections, it has a huge impact during spacecraft contingencies, as the spacecraft design is such that it requires more power during safe modes than what can be currently provided by the solar arrays.

B. Battery Degradation

Cluster spacecraft have 5 Silver-Cadmium batteries were designed for a 3 years lifetime. Despite special measures have been taken by the FCT to extend their duration most of them have been declared non-operational after one or more cells are suspected to have cracked.[4] As presented in Table 1, three spacecraft have only one or no battery at all, and the storage capacity of the batteries still operational is extremely low compared with the initial 16Ah at the beginning of the mission.

	Bat 1	Bat 2	Bat 3	Bat 4	Bat 5
Cluster 1	0.0	0.0	0.0	0.0	0.0
Cluster 2	1.2	0.0	0.0	2.4	1.9
Cluster 3	0.0	0.0	0.0	0.0	1.1
Cluster 4	0.0	0.0	1.9	0.0	0.0

Table 1. Current battery capacity (in Ah) for all spacecraft.

C. Eclipse Operations

Eclipses without batteries are one of the most significant features of Cluster operations.[5] During eclipses, without SAP and with the batteries not able to provide enough power, the Cluster satellites experience a complete power down (with the exception of spacecraft 2, which still has enough capacity to survive short duration eclipses). While the spacecraft is in the eclipse umbra all payloads and subsystems remain off, including the keep alive lines which

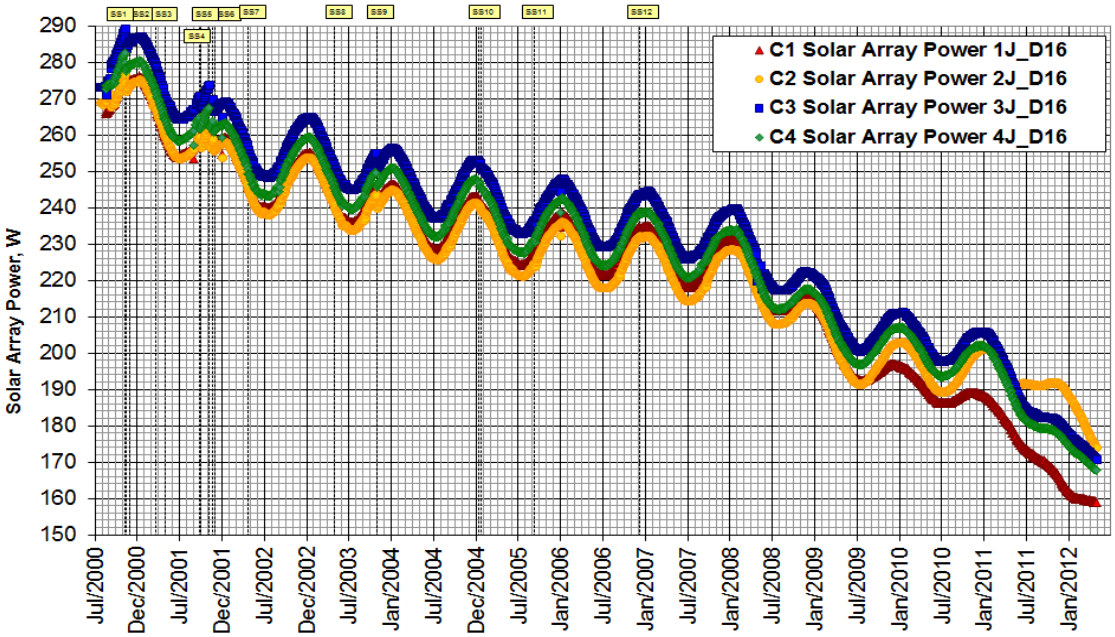

Figure 2. Evolution of the SAP for all spacecraft since the beginning of the mission. Before 2004, solar storms were the main cause of degradation. After 2008, the crossing of the radiation belt has increased the degradation rate.

power a critical memory circuit known as protected memory (PM). After the eclipse, the spacecraft boots with the default software image stored in PROM and all the subsystems have to be reconfigured and the on-board software, on-board time and payload patches have to be loaded again following a complex and long process. Two eclipse strategies have been developed and applied in Cluster operations for power-down eclipses:

1) Power down time-tagged eclipse operations: if one battery is still available but has not enough capacity to provide at least 45 W during the whole eclipse, the battery is charged before the eclipse but disabled by a time-tagged command just after eclipse umbra entry, instantly powering down the entire spacecraft. This approach at least protects the battery from over-discharging and reserves energy in the battery for use during the restart after the eclipse exit. After the eclipse, when the solar arrays are illuminated, the on-board computer restarts automatically.
2) Real time no battery eclipse operations: if all batteries are non-operational and fully discharged, the adopted strategy is to manually switch off all spacecraft subsystems including the on-board computer in the last pass before the eclipse. The spacecraft will remain off and the on-board computer will not restart until it is manually commanded from ground. This approach guarantees a clean and controlled eclipse entry and eclipse exit but at the cost of performing critical real time operations in the blind, i.e. with no telemetry feedback, not only in the post-eclipse pass but also in the pre-eclipse pass.

Despite Cluster spacecraft were not designed for a complete power down in orbit, after hundreds of recoveries these “power-down” eclipse strategies developed by the FCT have proven to be a success and are now part of Cluster routine operations.

III. Cluster Safe Mode Definition

In order to protect the spacecraft in case of failures or unforeseen situation, safe mode configurations are defined. A safe mode offers a minimum control strategy that satisfies the marginal condition for the survival of the satellite until an intervention by ground is possible.[6]

A. Nominal Survival Mode and Reduced Survival Mode

Cluster satellites enter safe mode always as part of the initialization and booting process of the on-board computer named Central Terminal Unit (CTU). This can happen for three different reasons:

- After a CTU reboot triggered by ground or autonomously by the on-board software after detection of an anomalous software condition.

- After a CTU switchover, i.e. reconfiguration to the backup CTU, triggered either by ground or by the on-board software or the reconfiguration logic after detection of a hardware failure.
- After a CTU power on manually triggered by ground (by deliberately switching off the nominal and the redundant CTU first) or following a main bus under-voltage, which is the case faced by the spacecraft after an eclipse without batteries.

Fig. 3 depicts the CTU initialization sequence, which is independent of the reason for the CTU boot. The process involves multiple checks of the On-Board Data Handling (OBDH) subsystem: a check of the CTU microprocessor, an integrity test of the on-board software image stored in ROM, a full check of all the different RAM areas, an integrity test of the protected memory (a special RAM memory always powered on and which maintains its content even during a CTU switch-over), and finally a status check of the Remote Terminal Unit (RTU) which is directly connected to the CTU and is responsible of distributing the commands and acquiring telemetry from the different payloads and subsystems on request by the CTU. The results of all these tests will determine the safe mode configuration. There are two possibilities:

- Nominal Survival Mode (NSM): this is the normal configuration if no errors in PROM, RAM, PM and RTU are detected during the booting process. In this configuration the OBDH is fully operational and all the functionalities are enabled. The information stored in the protected memory is used, including the commands loaded by the FCT into the Survival Mode Execution Command Buffer (SMECB) which are executed at the end of the boot process.
- Reduced Survival Mode (RSM): the spacecraft will enter this configuration if an error condition is detected during the CTU boot. In RSM all the OBDH functionalities which are not critical are disabled. The information of the PM and commands from SMECB are only used during RSM if the PM data were found consistent (i.e. an error on the PM was not reason for the spacecraft to enter in RSM).

During routine operations NSM are not unusual. Since the beginning of the mission the four spacecraft have experienced more than 44 unexpected safe modes, most of them related to transitory failures (e.g. single event upsets). On the other hand, a RSM has never occurred outside eclipse operations. It is important to note that a RSM implies in most of the cases a double failure (the first one which triggers the CTU switch-over and a second failure during the initialization checks) and it is quite unlikely.

A RSM is only expected during eclipse operations without batteries. After such event the spacecraft is always found in RSM because the content of the PM is lost (i.e. the PM data are inconsistent) as a result of the prolonged main bus under-voltage.

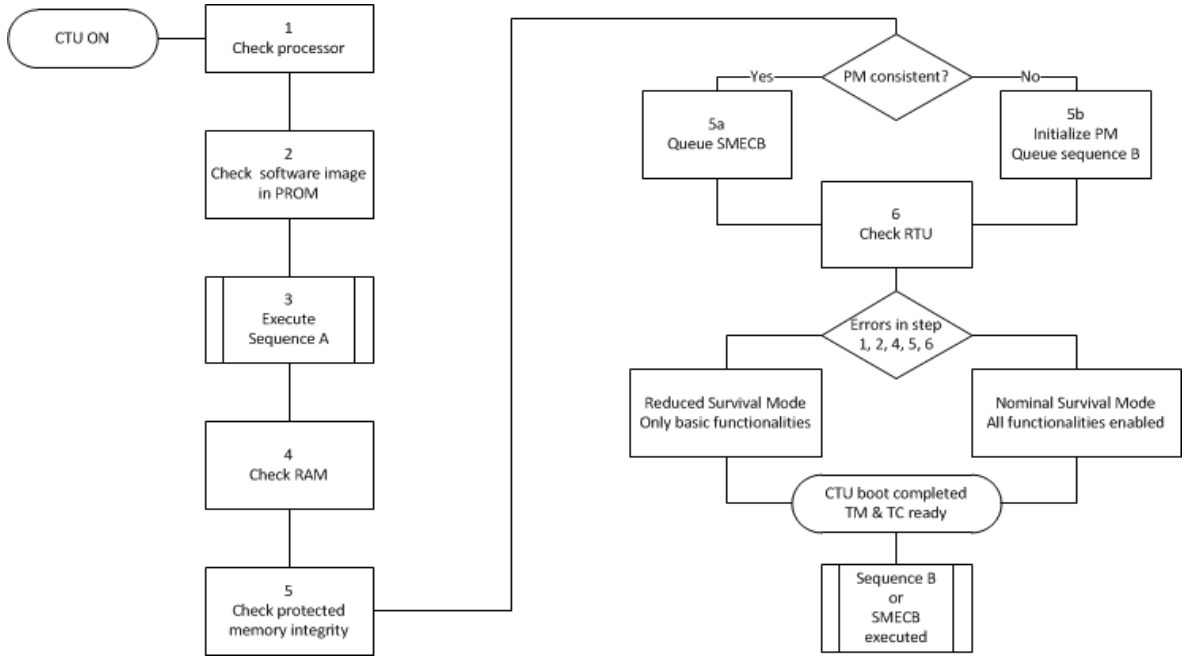

Figure 3. Cluster CTU boot and initialization process. Non-relevant steps are omitted for simplicity.

B. Safe Mode Sequences

As part of the CTU initialization and booting, the on-board computer executes a sequence of commands to re-configure the different payloads and subsystems including most spacecraft heaters, which are one of the main power consumers on-board.

The design of the Cluster spacecraft includes two fix command sequences, named sequence A and sequence B, which are stored on PROM and can not be modified, and a programmable sequence, the Survival Mode Execution Command Buffer (SMECB), maintained by the FCT and stored in the PM. Sequence A is always executed at the very beginning of the CTU boot in NSM and RSM, as shown in Fig. 3. When the booting is completed, either sequence B is executed or the content of the SMECB is executed, but not both of them. The combination of safe mode types and safe mode sequences creates three alternatives after a CTU boot:

- The spacecraft is in NSM and configured according to the content of sequence A and SMECB. This is the most common situation in case of a safe mode during routine operations.
- The spacecraft is in RSM and configured according to the content of sequence A and SMECB. This can happen only if an error is detected during the CTU boot but not on the PM (so the content of the SMECB is valid).
- The spacecraft is in RSM and configured according to the content of sequence A and sequence B. This can happens if the PM is found inconsistent during the boot, which is the scenario after an eclipse with insufficient battery capacity.

The content of sequence A are summarized in Table 2. These commands will be invariably executed at the beginning of the CTU boot, just after the integrity check of the software image stored in PROM. Due to the current degradation of the power subsystem, sequence A is not longer safe and puts the spacecraft in danger. First, because it enables the charging of all batteries including the non-operational ones (which may crack or explode if charged for a long time).[4] Second, sequence A switches on some heaters which are now routinely disabled (heaters G, I, K) and it does it before switching off the payload, significantly increasing the power consumption for a very short period of time. Such design is not optimum and, with no batteries to absorb power peaks, it is a potential source of problems as it will be detailed in the next sections. Unfortunately there is no possibility to modify sequence A, even by modifying the on-board software, as the sequence is loaded from the original software image stored in PROM at the time of the spacecraft integration on ground.

Sequence B is only executed in the case of inconsistent data in the PM, which up to now has only occurred during power down eclipses when the content of this memory is lost due to the permanent main bus under-voltage. The commands listed in Table 2 have a very negative effect when combined with sequence A as they switch on most of the redundant heaters of the spacecraft without switching off first the main heaters. Main and redundant heaters together require a significant amount of power, far beyond what the solar arrays can provided now, especially during the penumbra at eclipse exit when the spacecraft are very cold.

Sequence A	**Required power**
Enable battery charge and discharge	0 W
Switch off all redundant heaters	0 W
Switch off main heaters A and C	0 W
Switch on main heaters E,F,**G**,H,**I,K**	**+ 64 W**
Switch off all payloads	- 41 W
Sequence B	**Required power**
Power cycle main AOCS subsystem	0 W
Abort manoeuvre (if any), main AOCS	0 W
Switch off main AOCS, switch on red.	0 W
Abort manoeuvre (if any), main AOCS	0 W
Switch off transponder	- 21 W
Switch off main heaters A,C,E	0 W
Switch on redundant heaters **F,G,H,I,K**	**+ 68 W**
Switch off mass memory (SSR)	- 6 W

Table 2. Overview of the content of sequence A and sequence B. The second column shows the worst case change in the demanded power for the current default spacecraft 1 configuration during routine operations and assuming that only heaters F and H were on before entering safe mode.

The SMECB commands deal with all the negative aspects of sequence A (stopping the charge of no operational batteries and switching off unnecessary heaters). However they execute at least 20 seconds after sequence A (and only in case of no errors in the PM), so by the time the SMECB sequence can correct the situation is too late to avoid a main bus under-voltage.

Whereas safe modes are the necessary reaction of the spacecraft to a failure or an anomalous situation and can not and should not be avoided, it is desirable to prevent the execution of sequence A and B, as they are not longer safe.

C. Safe Mode Recovery

The process to recover the spacecraft from a NSM and restore routine operations is a complex one which requires several hours to be completed. It can be summarized in the following steps:

1) Load the on-board time and patch the on-board software with the latest software image.
2) Re-load the data for the different on-board software functions (on-board monitoring, time-tag commanding…) which are stored in RAM.
3) Command the different subsystems and payloads to their routine configuration

From the software perspective, a spacecraft in NSM is a fully operational spacecraft; it is only a matter of the setup of the different units and payloads. In NSM all the on-board functions are active.

The situation in RSM is slightly different because not all the on-board software processes are running and only basic functionalities (i.e. telemetry and telecommanding) are available. The standard procedure to recover from a RSM requires first identifying and resolving the reason for the RSM and then forcing a new reboot of the CTU to get the spacecraft in NSM. Such transition from RSM to NSM ensures a clean and consistent status of the on-board software but it requires and additional boot where sequence A will be executed again.

IV. Implications of Limited Solar Array during Safe Modes

A. Power Demand at Boot Time

In safe mode, the data required for the thermal control function implemented by the on-board software is not loaded; therefore when the heater circuits are switched on by sequence A, the heaters are controlled only by thermostats and not by software. The temperature control range of the thermostat is wider than the one of the software control, between 10 and 25 degrees higher. When sequence B is executed, all the redundant heater circuits are also switched on. Therefore, even if the transponder is switched off together with its heater circuit E, the power consumption of the other heater lines is doubled, making the power situation even more critical.

At high spacecraft temperatures, the power consumption in safe mode is similar to the one in routine. However, the lower the spacecraft temperature is the more significant is the increase in power consumption when entering the safe mode.

With the spacecraft ageing, the power problem in safe mode arose and became more and more serious. The solar array degradation has in fact a double contribution: first, the spacecraft temperature is generally lower because there is less power available in routine operations to be dissipated in the internal power dumper (a distributed network of heaters); second, there is less power to cover the increased need when entering safe mode.

Currently the spacecraft temperature in routine operations varies between 8° and 15° Celsius depending on the spacecraft and the season; in eclipse it can drop as low as 0° Celsius. The available solar array power is on average around 170 W. This is not sufficient most of the time to cover the safe mode needs, as shown in Fig. 4, especially en RSM after the execution of sequence A and B.

The transient situation during safe mode reconfigurations is actually even more severe from the power consumption point of view. The payload instruments are switched off only at the end of sequence A, after the heaters are already on as shown in Table 2. This temporary adds around 40 W to the power needed in safe mode.

Batteries are also much degraded, if operational at all, hence it is not possible to keep them fully charged in all routine operations to face the possible power need in safe mode.

When the spacecraft power demand exceeds the power available from the solar array, the power central unit cannot control anymore the spacecraft power bus to the nominal value of 28 V and a main bus under-voltage would occur.

With the present Cluster power and thermal situation, a transient main bus under-voltage is almost unavoidable during any safe mode reconfiguration and often the power budget is still negative even after the reconfiguration is completed.

B. The Risk related to Main Bus Under-Voltage

The spacecraft units are connected to the power bus through Latching Current Limiters (LCL). Those electronic relays can be switched on and off and provide protection against possible power related failures. When the main bus voltage drops below a predefined safe threshold of 23.5 V, the LCLs switch off automatically disconnecting the loads from the bus. The only exceptions are the essential units, i.e. the on-board receivers and decoders, which are connected to the bus through un-switchable foldback current limiters.

The Subsystem Reconnection Logic (SRL) is in charge of reconnecting the LCLs of the CTU and RTU (both main and redundant) when the main bus raises back to the nominal value after an under-voltage is detected.

The LCLs have a tolerance of +/- 1 V, therefore, when the main bus voltage drops, some LCLs switch off earlier than other ones. If the load relieved by the disconnection of the first LCLs is enough to regain a positive power budget, the main bus voltage recovers the nominal value before further units are disconnected.

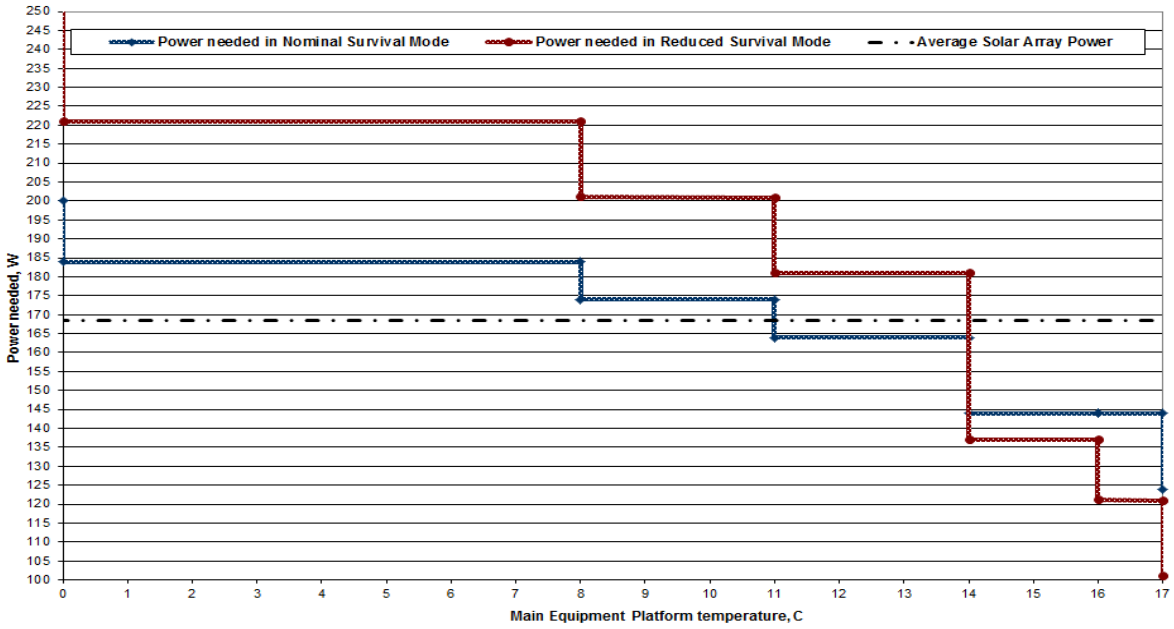

Figure 4. Average power demanded by all spacecraft units in NSM (sequence A) and RSM (sequence A+B) as a function of the spacecraft temperature. An average of the SAP available for the four spacecraft is displayed as a reference.

However, if the LCL of the active CTU switches off, when the main bus Voltage recovers the SRL reconnects the CTU's LCL and the CTU re-initialize. The sequences A is then executed again reconnecting the heaters and if the power budget is still negative causing an additional main bus under-voltage. The entire process will repeat again and again until the CTU LCL remains connected or the thermal situation improves decreasing the heaters consumption.

As a result, when a safe mode is entered causing a main bus under-voltage, the spacecraft resulting status is not really predictable: any of the spacecraft units could be switched off.

During the last years of the Cluster mission, several cases were observed across the four spacecraft. Most of the times the impact was limited: no signal acquisition at the expected time because the transmitter was switched off, all the on board recorded data was lost due to the power off of the SSR or some of the heaters were in an inconsistent configuration. However, the consequences could be really serious. The two following cases show the potential risks of Cluster safe modes.

In March 2012, a CTU switchover to the redundant side occurred on spacecraft 1, recorded as anomaly 212. During the reconfiguration to safe mode, due to a main bus under-voltage, the RTU was disconnected and some of the commands of the sequence A could not be executed: the payload remained on in an undefined status and without surveillance. There was no damage caused to any science instrument, but the event was a serious threat for the payload.

The most critical event, logged as anomaly 191, occurred in June 2011 after a spacecraft 4 eclipse. Neither the nominal nor the contingency post-eclipse recovery procedures achieved to re-establish contact with the spacecraft. It was later discovered that the CTU LCL switched off due to a main bus under-voltage when entering safe mode after the eclipse and was never reconnected by the SRL and had remained off. The anomaly is still under investigation to reach a full understanding. The most probable explanation is that the main bus voltage was trapped to a value slightly below the nominal one due to a marginal power lack situation: the voltage was too low for the SRL to reconnect the CTU LCL, but still higher than the trip-off level of any of the still connected LCLs. The RTU off command unblocked the situation. The CTU and the RTU are the only power loads that can be commanded via high priority commands from ground; to disconnect any other unit it is necessary that the CTU itself is powered. If the situation would re-occur, but this time with all CTU and RTU LCLs disconnected, the only possibility to recover the spacecraft would probably be waiting for the following umbra eclipse to cause a full power down.

V. Avoiding Safe Mode Sequences during Eclipse Operations

The next step after understanding the risks of Cluster safe modes is to investigate possible workarounds to avoid them or at least minimize their consequences. As discussed in previous sections, RSM after a power-down eclipse represents the highest risk because the power demanded is significantly above the current solar array performance due to the low spacecraft temperature combined with the execution of both sequence A and sequence B. Therefore dealing with safe modes during the eclipse season and avoiding main bus under-voltages has become one of the main targets of the FCT, especially after the occurrence of anomaly 191 in June 2011 when the CTU remained off after a power-down eclipse.

A. Command Execution Disruption at Eclipse Exit

The design of the Cluster spacecraft is such that it is impossible to avoid that the CTU enters RSM and executes sequence A and B as part of the initialization process (obviously leaving the on-board computer off is not an option). However, during the investigation of anomaly 191, the idea of switching off the RTU during the CTU booting was proposed by the FCT and recognized as a potential solution by the spacecraft manufacturer.

On the one hand the CTU is responsible for executing sequence A and B but on the other hand it relays on the RTU to distribute any command which is not related to the CTU or the on-board software. The RTU is in charge of processing each command and generating the electrical pulses or transmitting the data to the target unit. If the RTU is off, the commands will still be sent by the CTU but they will not reach their destination and will have no effect.

In such scenario, it is important to understand the reaction of the on-board software and the CTU hardware when the RTU is off. In order to send commands to the RTU, the CTU puts them in the so called OBDH bus, which connects the CTU and the RTU. The management of the bus is delegated to a piece of CTU hardware called the OBDH bus adaptor. The adaptor sends over the bus any request of the CTU to the RTU without any previous check of the RTU status and even if the RTU is off and not listening the bus. This fact is extremely important in this case because it means that commands are not queued in the CTU side; as soon as the CTU puts them in the OBDH bus they are lost forever and they will not be executed when the RTU is turned on again.

However, the OBDH bus adaptor is expecting a response from the RTU for every request it has sent. If the response is not received on time an error counter is increased. The CTU checks this counter and reacts in case of errors. The analysis of the on-board software has shown that the behavior of the CTU is different during the execution of sequence A and sequence B.

- Sequence A is sent during the initialization process and without using the standard command handling routines. In this case, the CTU puts the commands in the OBDH bus one after another and the OBDH bus adaptor error counter is totally ignored.
- Sequence B is sent by the standard command handling routines after the booting is completed. In this case, the error counter is regularly verified and a CTU switch over is autonomously triggered if it is above certain threshold. However as part of the NSM and RSM configuration, a very high threshold is applied by default (higher than maximum value of the error counter). Consequently the execution of sequence B with the RTU off has no side-effects (except that the commands are disregarded which is the final objective).

Additionally, in NSM or during routine operations, the RTU status is regularly verified by the CTU and a switch-over will be triggered in case of problems. As explained in section III, this is not at problem at eclipse exit because the spacecraft is always in RSM and in this configuration the RTU checks are disabled.

The RTU, like the CTU, can be switched on or off by special ground commands called priority 1 in Cluster terminology. They go through the command pulse distribution unit of the spacecraft decoders and do not require the on-board software or even the CTU or the RTU to be powered. In order to avoid the execution of sequence A and B it is necessary that the RTU is off by the time the CTU boots. This can only be achieved by powering the spacecraft on in a controlled way at eclipse exit, which requires manually switching it off, i.e. in real time, before it enters the eclipse.

B. Transition from NSM to RSM without CTU Reboot

The standard procedure to recover a Cluster satellite from a RSM requires a CTU reboot to perform the transition to NSM. Sequence A plus the SMECB commands will execute as a side effect. It is important to highlight that if the RTU is kept off during the CTU initialization, then the spacecraft will always boot in RSM because of the errors detected during the RTU checks (see Fig. 3), so switching the RTU off again for the transition from RSM to NSM does not solve the problem as the spacecraft will end up again in RSM after the reboot.

A new strategy has been developed by the Cluster FCT to reconfigure the spacecraft from RSM to NSM without a CTU reboot by carefully enabling all the software tasks which are not active in RSM to achieve a fully operational on-board computer. The procedure has several steps:

1) Check of all telemetry parameters related to the latest CTU boot to understand why the spacecraft is in RSM and not in NSM and confirm that no failure has been detected during the initialization process (with the only exception of the RTU in case it was kept off during the boot).
2) Enable all software processes related to the handling of the mission time line and the time tag commands.
3) Enable all software processes related to the on-board monitoring service.
4) Enable all software processes related to the spacecraft redundancy and periodic checks of the CTU and RTU hardware.
5) Dump the software processes table to verify that all functionalities are enabled.
6) If necessary, patch the telemetry generation process to obtain the telemetry from the redundant power distribution unit or the redundant attitude and orbit control system in case that the redundant units and not the main ones are in use.

The on-board software code has been analyzed to be sure that all the differences between NSM and RSM are captured by the procedure. Additionally, the new approach has been validated in the spacecraft simulator before being executed for the first time on the spacecraft. The transition from RSM to NSM without a CTU boot has proven to be successful and even simpler and faster than the traditional reboot technique. In such way not only the risk of a main bus under-voltage is avoided, but also the telemetry flow is not interrupted by the reboot, allowing the FCT to keep a better control of the whole transition.

C. Operational Implementation and Results

The two ideas described in this section have been tested for the first time in June 2011, at the end of the 2010-2011 eclipse season, and were successfully applied using manual procedures with three spacecraft almost 50 times.

As explained, keeping the RTU off during the CTU boot, requires that the spacecraft is switched off in a controlled way before entering the eclipse, which has a significant operational impact:

1) Complex real time operations requiring engineer support are required not only after the eclipse to recover the spacecraft but also in the last pass before the eclipse. With eclipses every 54 hours, this has a huge impact on the workload of the FCT.
2) Switching off the spacecraft requires between 10 to 20 minutes which can not be used to dump the data stored in the on-board memory (which will be lost after the eclipse). In some cases it may be necessary to sacrifice science data in order to be able to switch off the spacecraft before the end of the pass.
3) The lass past before the eclipse becomes critical and in case it is lost it will not be possible to switch off the spacecraft in a controlled way.

All these concerns have been addressed for the latest eclipse season, which started in December 2011 and finished in April 2012.

The Cluster automation system, a key component of the Cluster infrastructure to recover the spacecraft after eclipses in a fast and safe way,[2,7] has been extended and updated to the new strategy. The spacecraft controller is now able to switch off the spacecraft in less than 10 minutes during the pre-eclipse pass with minimum engineer supervision using a new automated procedure. After more than 110 pre-eclipse passes, the approach has proven to be extremely successful, and the impact of the new eclipse strategy on the science data return has been negligible.

In order to address 3), time-tagged commands to partially switch off the spacecraft are also uplinked before the last pass. Whereas this is not a full backup and will not prevent the CTU to boot automatically at eclipse exit (i.e. execution of sequence A and B will not be avoided) it ensures that the spacecraft enters the eclipse in a clean way if the last pass before the eclipse would be lost.

Finally, the eclipse recovery procedures have been further streamlined. By avoiding the second reboot of the RSM to NSM transition and with the much cleaner and deterministic state of the spacecraft in the case of the controlled switch on, it has been possible to greatly simplify the automated eclipse recovery procedures reducing by a few minutes the time to recover the spacecraft.

VI. Avoiding Safe Mode Sequences during Routine Operations

A. Safe Modes outside Eclipses

With the decrease of the available SAP and the spacecraft temperature, all the problems of the safe mode sequences during eclipses will be applicable in the near future to safe modes during routine operations. Even if a

RSM is not expected outside eclipses, execution of sequence A in NSM can be enough to trigger a main bus under-voltage as heaters are switched on before switching off the payload.

The main difference with respect to the eclipse scenario is that it is not known a priori when a safe mode will occur therefore it is not possible to switch off the RTU in advance.

B. Proposed On-board Software Modification

Several alternatives have been proposed and analyzed by the FCT to avoid execution of sequence A and B in case of a safe mode during routine operations.

The most promising one is a change of the on-board software to apply a similar strategy than the one used during eclipses. The idea is to modify the behavior of the software when an error leading to a reboot or a switch-over is detected. If the software powers off both RTUs before rebooting the CTU or forcing the CTU switch-over, then by the time the CTU boots again, the RTU will not be available and sequence A and B will have no effect.

Such software change seems feasible, can be easily validated in the simulator and it will only affect a minimum part of the on-board software. In addition, if the new code executes, it will imply a CTU reboot and then the default software image stored in PROM will be loaded, which strongly limits the possibility of introducing any negative side-effects with this software modification.

The only problem is that the useful commands of sequence A and SMECB will as well not execute i.e. switching off the payload. This can be addressed by sending the payload off commands before switching off the RTUs, which should also be feasible.

Together with the on-board software change, it will be necessary to reengineer all the recovery procedures to consider that in case of a CTU boot the RTUs will be off, i.e. no telemetry will be provided to the ground for analysis, and the RTU will have to be switched on in the blind first before starting any recovery action.

Whereas the solution has a few limitations (e.g. will not avoid sequence A execution in the unlikely case of an error detected by hardware and not software) it should protect the spacecraft in the most common NSM scenarios. Final implementation is currently under consideration, depending on the final conclusions of the analysis of anomaly 191.

VII. Conclusion

In this paper the problematic of limited on-board power during Cluster spacecraft safe modes has been analyzed. The importance of designing safe mode sequences which are safe even if the available solar array power is lower than expected has been highlighted, especially when they are hard-coded in PROM and can not longer be modified after launch. Things like switching off the payload before switching on other loads or switching off the main heaters before activating the redundant ones are an important lesson learnt which could be applied to other spacecraft.

Whereas the proposed work around of keeping the RTU off while the CTU boots is quite specific to Cluster, the idea behind it could be applied to other spacecraft, if, for whatever reason, it is required to avoid the execution of commands by the on-board computer and it is not possible to implement it at software level.

Thanks to the workarounds discussed in this paper, Cluster eclipse operations are now much safer and robust, as proven during the 2011-2012 eclipse season. This strategy, and its possible extension to routine operations, would be really valuable for the challenging final years of the Cluster mission.

Appendix A
Acronym List

AOCS	Attitude and Orbit Control System
CTU	Central Terminal Unit
ESOC	European Space Operations Centre
FCT	Flight Control Team
LCL	Latching Current Limiters
NSM	Nominal Survival Mode
OBDH	On-Board Data Handling
OCC	Operations Control Centre
PM	Protected Memory
PROM	Programmable Read-Only Memory
SAP	Solar Array Power
SMECB	Survival Mode Execution Command Buffer
SSR	Solid State Recorder
RAM	Random-Access Memory
RSM	Reduced Survival Mode
RTU	Remote Terminal Unit
SRL	Subystem Reconnection Logic

Acknowledgments

The authors would like to thank all the members of the Cluster Flight Control Team for their contributions to this paper and review effort.

References

[1]Gianolio, A., Ellwood, J., "Cluster II – The spacecraft and the mission," IAF-00-Q.2.03, International Astronautical Congress, 2000.

[2]Clerigo, I., Bartesaghi, M., Bolland, M., Volpp, J., "From VAX to iPhone: 20 Years of Cluster Mission Ground Segment Evolution," IAC-11-D1.5.7, International Astronautical Congress, 2011.

[3]Letor, R., Marie, J., Sangiorgi, and Volpp, J., "Cluster 10 Years Evolution of the Cluster Solar Arrays and Forecasting their Degradation after Entering the Inner Radiation Belt," *Proceedings of the 9th European Space Power Conference* [CD-ROM], SP-690, ESA, 2011.

[4]Sangiorgi, S., Servan, P., Schautz, M., and Volpp, J., "Cluster Spacecraft Batteries through the 2nd Mission Extension," *Proceedings of the 8th European Space Power Conference* [CD-ROM], SP-661, ESA, 2008.

[5]Volpp, J., Godfrey, J., Foley, S., Fornarelli, D., Servan, P., Pullig, C., Appel, P., and Sangiorgi, "Nursing 4 Cluster Spacecraft with Aging Batteries Through Eclipses," AIAA-2008-3278, SpaceOps Conference, 2008.

[6]Schuster, A., *Robust Intelligent Systems*, 1st ed., Springer-Verlag, London, 2008, Chap. 11

[7]Appel, P., Fornarelli, D., Heinen, W., Foley, S., Accomazzo, A., "Cluster Automation Initiative – Lessons Learned," AIAA-2008-3256, SpaceOps Conference, 2008.