Marcin IWIŃSKI [1], Rafał GRACZYK [2], Janusz SOSNOWSKI [1]
[1] INSTITUTE OF COMPUTER SCIENCE, WARSAW UNIVERSITY OF TECHNOLOGY, Nowowiejska 15/19, 00-665 Warsaw
[2] SPACE RESEARCH CENTRE OF POLISH ACADEMY OF SCIENCES, Bartycka 18A, 00-716 Warsaw

Dependability issues in the PPLD-PSU subsystem for the BRITE-PL Hevelius microsatellite

M.Sc. Marcin IWIŃSKI

He is a PhD student in Institute of Computer Science at the Warsaw University of Technology. He is coauthor of software for PW-SAT Satellite. He also works as embedded systems developer in Albatross System. Moreover, he participates in BRITE-PL satellite project in Space Research Center, Polish Academy of Sciences.

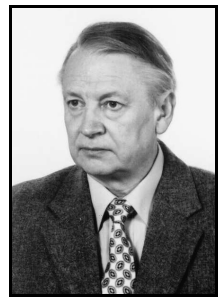
e-mail: m.iwinski@ii.pw.edu.pl

M.Sc. Rafał GRACZYK

He is an electronics specialist in Space Research Center of Polish Academy of Sciences and in Astri Polska. Additionally, he is a PhD student in Institute of Electronic Systems at Warsaw University of Technology. His research interests and field of expertise are in dependable system based on reconfigurable logic devices. He was an engineering team leader for On-Board Computers, Power System and Polish Payload in BRITE-PL Lem and Hevelius satellites.

e-mail: rgraczyk@cbk.waw.pl

Prof. Janusz SOSNOWSKI



He is the professor in Institute of Computer Science at the Warsaw University of Technology. He chairs Department of Computer Software and Architecture. He is the author and coauthor of over 200 publications. His research area relates to computer dependability (diagnostics, fault tolerance, reliability), computer architecture and communication interfaces.

e-mail: jss@ii.pw.edu.pl

Abstract

Due to specific conditions for electronic equipment in satellites and high launching costs, dependability issues of satellite subsystems are of great importance. This paper presents the PPLD-PSU subsystem designed for Polish payload of the BRITE-PL Hevelius microsatellite. When developing software for this system, we have assured some dependability requirements related to testing this equipment before launching (exhaustive external and internal self-testing) and during the whole mission (on-line monitoring). Moreover, special mechanisms have been included to support remote reprogramming. In the paper we also analyze various possible fault effects (transient, intermittent and permanent) and methods of mitigating them locally or remotely.

Keywords: satellite, dependability, reprogramming.

Problem niezawodności w podsystemie PPLD-PSU dla mikrosatelity BRITE-PL Heweliusz

Streszczenie

Rozwój systemów wbudowanych na potrzeby misji kosmicznych jest ostatnio częstym tematem badań w Polsce na świecie. Mając na uwadze środowisko pracy podsystemów elektronicznych oraz wysokie koszty wystrzelenia kwestie niezawodnościowe pełnią kluczową rolę w tego typu zastosowaniach. Celem niniejszej pracy jest przybliżenie podsystemu PPLD-PSU (Polish PayLoaD – Power Supply Unit) opracowanego na potrzeby polskiego ładunku użytecznego dla mikrosatelity BRITE-PL Heweliusz. Głównym jego celem jest zarządzanie polskimi eksperymentami. Posiada on własne niezależne od całego satelity zasilanie z paneli słonecznych oraz akumulatora Li-Ion. Nie jest on jednak wyposażony we własny moduł do komunikacji z Ziemią. Połączenie zapewnia moduł radiowy satelity Heweliusz. Sercem podsystemu jest popularny mikrokontroler ATmega128L. Rozwój oprogramowania dla podsystemu niósł za sobą szereg wymagań niezawodnościowych. Przeprowadzane były liczne testy w trudnych warunkach środowiskowych (komora klimatyczna, komora próżniowa). Przygotowane zostały również funkcje pozwalające zdalnie monitorować poprawną pracę systemu gdy znajdzie się on już na orbicie. Dodatkowo przewidziana została możliwość zdalnej aktualizacji oprogramowania. Wzięte zostały przy tym pod uwagę możliwe problemy komunikacyjne utrudniające poprawne załadowanie nowego oprogramowania. W pracy poruszana jest też kwestia możliwości występowania błędów i radzenia sobie z nimi zdalnie lub lokalnie.

Słowa kluczowe: satelita, niezawodność, aktualizacja oprogramowania.

1. Introduction

The BRITE-PL, a Polish part of BRITE international constellation of six microsatellites is an example of a new approach in conducting space research, i.e. using small and relatively cheap, micro- or nano- sized satellites (1 to 100 kg of total wet mass). Satellites will observe stars, with the minute-range resolution and measure variations in their brightness in order to study their behavior and to infer findings regarding their internal structure. Satellites, by cooperation in the constellation, provide the capability of continuous observation lasting even weeks, a feature not available in astronomical observations up to date. BRITE-PL satellites assure obtaining significant scientific results at reasonable costs using equipment with slightly relaxed reliability requirements.

Space systems are the subjects of strong environmental influence and they are operated remotely which renders all repair activities impossible. The on board equipment operation in the harsh environment is subjected to physical stresses and to errors introduced by particle physic effects. Hence, an important issue is to perform intensive testing before launching [2]. The remote operation means there is no direct access to space equipment and all maintenance has to be done via radio communication links.

Recently, space systems have been built using COTS (Commercial Off-The-Shelf) elements, which assure high functionality at low cost. Unfortunately, they are susceptible to various radiation effects in the space, in particular they can result in SEU (single event upsets) [3]. These effects can be mitigated using radiation hardened elements with lower functionality and higher costs. Hence, an important issue is to mask or tolerate faults in COTS based systems. In the case of short mission experiments, we can assume that permanent faults are less probable than transient ones, so massive circuit redundancy is not required [4]. In this case we have to use software based dependability solutions. This can be enhanced with remote program reconfiguration capability. In the paper we present our experience in dependability related to the developed subsystem PPLD-PSU for the Hevelius microsatellite.

2. Overview of the PPLD-PSU subsystem

A PPLD is a Polish payload onboard of the Hevelius microsatellite. It is almost autonomous and with an additional communication module can act as a standalone satellite. It has its own solar cells and Li-Ion battery independent of the Hevelius. The PPLD-PSU is the main subsystem of the PPLD. It is designed

as a platform to handle Polish experiments on board of the Hevelius microsatellite. This is a combination of an on-board computer and a power supply unit in one device. The communication with Earth is provided by a radio link of the main satellite. Dedicated commands and telemetry are forwarded via the UART interface. The PLD-PSU can be turned on and off from the main computer of the Hevelius. This assures isolation of the PPLD from other experiments included in the Hevelius mission goal (higher dependability). The PPLD structure is shown in Fig. 1.

The heart of the PPLD-PSU is a popular ATmega128L microcontroller. It comprises 128kB of program FLASH memory, 4kB SRAM and 4kB EEPROM. Extra 32kB of external FRAM memory is used for nonvolatile data storage and as a temporary buffer for software update files. This is a new type of nonvolatile memory, which becomes more popular due to the fast read/write speed and almost infinite write cycles.

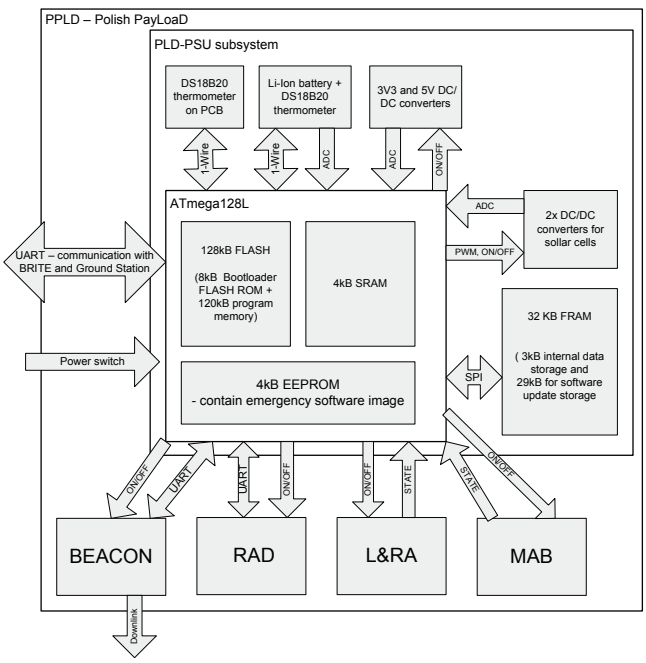


Fig. 1. PPLD-PSU subsystem overview
Rys. 1. Zarys systemu PPLD-PSU

The PPLD-PSU subsystem is powered from two sets of solar cells located on the opposite walls of the Hevelius. The PPLD-PSU uses DC/DC converters and the MPPT (Maximum Power Point Tracking) algorithm to provide the maximum efficiency of power extraction. The MPPT is implemented in software and was previously tested using fault injection simulations [3]. The excessive power is stored in an internal Li-Ion single cell 2600mAh battery. The PPLD-PSU has the possibility to warm up the battery using the attached heating resistor. The PPLD-PSU has two DS18B20 digital temperature sensors. One is mounted on the main PCB, while another measures the temperature of the Li-Ion battery. These temperatures can be monitored and in the case of some anomaly appropriate commands can be issued from the Earth, e.g. warming in the case of too low temperature of the battery.

One of the Polish experiments controlled by the PPLD-PSU is BEACON. This is a kind of radio beacon providing downlink communication to Earth using the Morse code signal at 2,4Ghz. The PPLD-PSU turns it on and provides the data to be sent. Another experiment is RAD. It is a small PCB comprising an FPGA device and various memory chips. Its purpose is to monitor and check radiation effects on space. The PPLD-PSU task is to provide power and periodic requesting RAD for data to be send to Earth. The remaining two experiments are MAB and L&RA. These are one shot electromechanical devices testing methods of deploying various equipment (mostly antennas) in space. PPLD-PSU is responsible for starting experiments, measuring their deployment time and storing collected data for queries from the Earth. The power for all tests is provided from a Li-Ion battery using 5V and 3V3 DC/DC converters. They comprise software on/off function and over current protection. More information on experiments can be found in [6].

3. Software reprogramming

Remote software update was implemented in the PPLD-PSU subsystem to improve dependability and assure flexibility of the internal software. There was another practical reason of this approach which is the lack of a programming interface after integration of the satellite. During extensive testing some software modifications may be necessary and therefore disassembly of some parts may be needed to allow reprogramming without this feature.

The PPLD-PSU uses small piece of a program (called bootloader) located in the dedicated FLASH section of ATmega128L for reprogramming function. For security reason this part of the program memory is hardware write-protected and cannot be modified by the microcontroller itself. This reprogramming approach requires cold start using reset to load a new program code. First of all, the update file (typically 15-20kB) must be loaded to the temporary buffer in the nonvolatile FRAM memory. It is loaded in 64-byte pieces, frame by frame using the communication protocol of the main satellite. The protocol itself provides acknowledgement and frame checksum for reliable data transmission. File uploading can be resumed in any time in case of communication problems. When the data transfer is completed, the software update flag is set for the bootloader to request reprogramming procedure after the next reset of the microcontroller.

The bootloader flow control is presented in Fig 2. At first it checks update request flag and checksum of the uploaded file. Meeting these requirement causes the FLASH memory reprogramming with a new code and clearing the update flag. The bootloader is then restarted and now it checks CRC of the FLASH memory before executing the main program. Checksum mismatch causes checking the integrity of the emergency program image stored in internal EEPROM memory. Meeting the condition causes the reprogramming of the FLASH memory with emergency application. It supports only basic functions and provides essential communication commands to load the new program image to FRAM and try to update again. Having both main and emergency applications corrupted, the bootloader takes the risk of running the damaged code. This is the last thing we can do in this situation to rescue the subsystem.

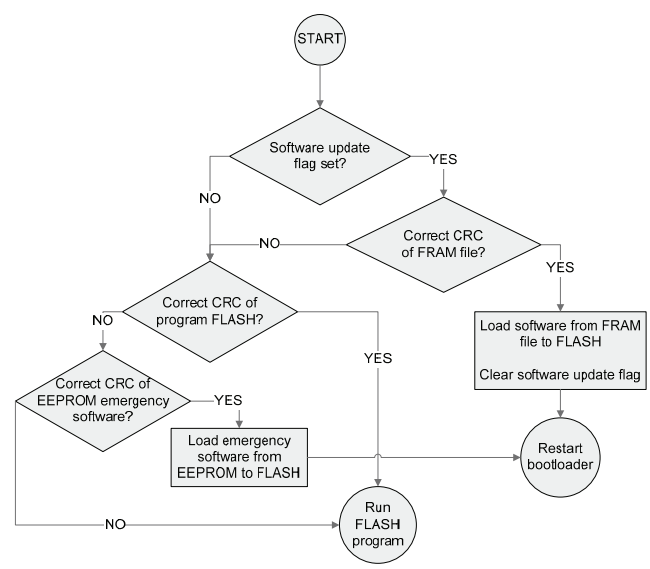


Fig. 2. PPLD-PSU bootloader flow control
Rys. 2. Schemat działania bootloadera podsystemu PPLD-PSU

4. Fault handling mechanisms

Designing PPLD dependability issues were taken into account. The satellite will work on LEO (Low Earth Orbit) and therefore we may expect some radiation effects like SRAM memory bit-flips, latch-ups and slow degradation of electronic components. To overcome negative influence of space environment on the PPLD operation, some special mechanisms have been introduced.

First of all ATmega128L internal watchdog is used for software anti-hang protection. It is set permanently and cannot be disabled from the software. The watchdog timeout is set to 0.2s, which is triple the time of the main control loop. Additionally, periodical refreshments of key configuration registers are performed. This should prevent communication interfaces and microcontroller outputs from abnormal operation. Moreover, we have included various error detection mechanisms, e.g. related to transmission. All detected errors as well as initiated restarts are logged and can be read remotely. To evaluate transient fault occurrence during satellite operation, we have allotted some areas in RAM and FRAM with fixed patterns. These areas are checked periodically to detect bit-flips and report them in the error logs.

Special care must be taken to one shot mechanical experiments (MAB and L&RA). Unexpected activation can waste many hours of hard work of our colleagues. A double software activation mechanism has been implemented. To start a selected experiment, an arming command must be issued prior to the real execution command. Lack of this first step causes blocking the second one. Mechanical experiments are also protected against unexpected activation by accidental output state changes. To start each of them, a 5V DC/DC converter must be activated and the power switch must be on. These two controlling outputs are independent therefore are unlikely to switch accidentally at the same time.

5. PPLD-PSU testing

Environmental interactions with the space equipment are of various origin [2], including mechanical stresses (acoustic shocks and vibration during launch), thermal stresses (heat dissipation in vacuum only by conduction and radiation, no convection) and radiation influence (long term effects related to total dose absorption and single events related to interaction between high energy particle (heavy ions, protons) and semiconductor lattice to name few most important.

In order to achieve high space equipment survivability, given the fact that devices operate in harsh environmental conditions, special attention has to be paid to test campaigns. In typical approaches, tests can be divided into two categories: qualification tests and acceptance tests. The qualification tests are performed in conditions far exceeding those envisioned in baseline operation specification (by even 25-50% margin). Their main goal is to understand the system behavior in wide conditions range that may be present during abnormal situations (failures, loss of control). The qualification tests are often considered as destructive, which aim at finding the limits of the designed equipment and therefore ensure confidence in seamless operation in a typical environment. On the other hand, the acceptance test cannot exceed the equipment nominal operating conditions, as are performed on real flight (or flight spare) units. Their aim is to prove workmanship quality and to confirm that all the system components are behaving within manufacturer specifications. The acceptance tests are often extended by a burn-in test of, for example, 1000 hours operation in order to detect early “infant mortality” failures that may occur. For both qualification and acceptance, a typical test sequence may consist of mechanical, thermal and thermal-vacuum tests interleaved with functional tests in laboratory conditions confirming operational ability of the device under test.

The functional tests of the microcontroller were performed in accordance with the instruction level architecture model (ILA). They cover all the used instructions and logical blocks. Moreover, we used also application driven testing. This was based on our previous study in [5]. The application testing extends the possibility of covering specific fault models, usually skipped in classical universal testing.

The BRITE-PL Hevelius PPLD-PSU controller subsystem is the most thoroughly tested subsystem of the whole satellite. After the standard functional verification, the thermal qualification tests were performed in the range of -60 to +80 degree Celsius, exceeding the nominal specification (which is -20 to +45 deg. C) by around forty degrees. Those tests were considered as destructive, although the device proved itself to be able to withstand extreme conditions. Next, the thermal cycles test was conducted (still in normal ambient pressure), with temperature peaks of -20 and +45 deg. Celsius (within operation range). The first cycle was performed on the device switched off during temperature transition periods, with cold and hot starts in the peak period. The following cycles were conducted with the PPLD-PSU device switched on. The performance measurements were taken during the whole cycle. As a last qualification test, the PPLD-PSU together with other Polish payload subsystems were mounted in a thermal-vacuum chamber and the thermal cycle test was repeated for the whole BRITE-PL Hevelius payload under the vacuum conditions resembling those in Low Earth Orbit. Afterwards the PPLD-PSU and other payload subsystems were integrated into the satellite. The whole satellite system was tested mechanically (sine and random vibrations, shocks), thermally (thermal-vacuum simulations of tens of orbits) and electromagnetically (wide range radio emissions measurements in anechoic chambers, on-board interference checks).

6. Conclusion

The developed PPLD-PSU subsystem has been thoroughly tested and is ready for launching (planned in the middle of this year). It is based on COTS elements and equipped with software based procedures for handling faults and perform remote software reconfiguration if needed. Moreover, it has been equipped also with some circuits and controlling software to collect information on occurring anomalous events in the space. In particular, this will allow us to collect some experience on possible risks, etc. It is worth noting that design, implementation (assembly) and testing of the subsystem have been done in accordance with the spacecraft systems engineering rules [2]. These rules cover the analysis of the environment and mission, the detailed examination of subsystem elements. In particular, this includes mechanical, electrical and thermal aspects.

Further research will relate to observations of the operating satellite on the orbit. In particular, we hope to collect the data on fault statistics related to transmissions, restarts, disturbed memory cells, etc. This experience will be used in developing more efficient fault handling mechanisms.

7. References

[1] Caffrey M., Morgan K., D. Roussel-Dupre et al.: On-orbit flight results from the reconfigurable cibola flight experiment satellite (CFESat), Proceedings of the 17th IEEE Symposium on Field Programmable Custom Computing Machines, (FCCM ’09), April 2009.
[2] Fortescue P., Swinerd G., Stark J. (editors): Spacecraft Systems Engineering, 4th Edition, (EHEP002270), John Wiley, 2011.
[3] Iwiński M., Sosnowski J.: Testing Fault Susceptibility of a Satellite Power Controller, Dependable Computer Systems, Advances in Intelligent and Soft Computing, Vol. 97, Springer, 2011.
[4] Katz D.S.: Application-based fault tolerance for spaceborne applications, http://hdl.handle.net/2014/10574.
[5] Sosnowski J.: Software based self-testing of microprocessors, Journal of Systems Architecture, 52, 2006.
[6] Zawistowski T.: Polish-made payload for the BRITE-PL 2 satellite Heweliusz, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2012. Proceedings of the SPIE, Volume 8454, article id. 84540D, 10 pp.2012.

otrzymano / received: 12.04.2014
przyjęto do druku / accepted: 02.06.2014 *artykul recenzowany / revised paper*