Journal of Zhejiang University-SCIENCE C (Computers & Electronics)
ISSN 1869-1951 (Print); ISSN 1869-196X (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

New technique:

Design and implementation of the highly-reliable, low-cost housekeeping system in the ZDPS-1A pico-satellite*

Yu ZHANG, Yang-ming ZHENG†‡, Mu YANG, Hui LI, Zhong-he JIN

(*College of Aeronautics and Astronautics, Zhejiang University, Hangzhou 310027, China*)

†E-mail: zymsun2002@zju.edu.cn

Received Mar. 31, 2011; Revision accepted Aug. 4, 2011; Crosschecked Dec. 8, 2011

Abstract: The ZDPS-1A pico-satellite designed in Zhejiang University with a mass of 3.5 kg and a power consumption of less than 3.5 W is the smallest satellite in China up to now. The housekeeping system (HKS) is the core part of ZDPS-1A. The reliability of HKS has an important influence on the safety of the satellite. Traditional fault-tolerant methods do not apply to ZDPS-1A due to such pico-satellite characteristics as light weight, compactness in size, energy saving, and high integration. This paper deals with a highly-reliable, low-cost design for HKS using industrial devices. The reliable strategies of HKS include a dual modular redundancy scheme, CPU warm backup, a static triple modular redundancy scheme, and two-level watchdogs. Recursive experiments, special tests, and environmental tests show that this system meets the design target. This design has already been applied to ZDPS-1A, which was launched to execute in-orbit tasks on Sept. 22, 2010. To date, the satellite has been in a proper state for more than 15 months.

Key words: ZDPS-1A, Pico-satellite, Reliability, Housekeeping system (HKS), On-board computer (OBC), Warm backup, Fault tolerance

doi:10.1631/jzus.C1100079 **Document code:** A **CLC number:** TP39

1 Introduction

Recently, considerable effort has been invested in research and development programs for micro-technology for space applications (Hamann *et al.*, 2005). In general, these programs are based on the microminiaturization technology including microelectronics, microelectromechanical systems (MEMS), and multi-chip package (MCP) assembly, and feature highly autonomous control, a light weight, a short research and manufacturing cycle, strong mobility, and low construction and launching costs (Schilling, 2006). The pico-satellite research in Zhejiang University (ZJU) is one of these programs. The ZDPS-1A pico-satellite (Fig. 1) designed in ZJU, with a mass of 3.5 kg, is the smallest satellite in China up to now.

The mass of 3.5 kg and power consumption of 3.5 W confine ZDPS-1A within a cube measuring 0.15 m on all sides. The main mission of the satellite is the testing of a new method for space exploration, as well as onboard micro-scientific experiments. It is in the sun-synchronous circular orbit with an altitude ranging from 400 to 700 km (Meng *et al.*, 2009).

The pico-satellite, as a complete spacecraft, has to experience and meet all the challenges presented by the harsh environment during the active segment and in-orbit segment (Xilinx, 2004). This requires its housekeeping system (HKS) be highly reliable. In traditional designs, people usually use high-level devices and different levels of backups featuring many discrete components and subsystems to ensure the reliability of HKS (Sweeting, 2000). This kind of approach is contrary to the nature of the pico-satellite (Funase *et al.*, 2007).

‡ Corresponding author

* Project supported by the Foundation for the Author of National Excellent Doctoral Dissertation of China (No. 200035) and the Ministry of Education Science & Technology Research Project, China (No. 104069)

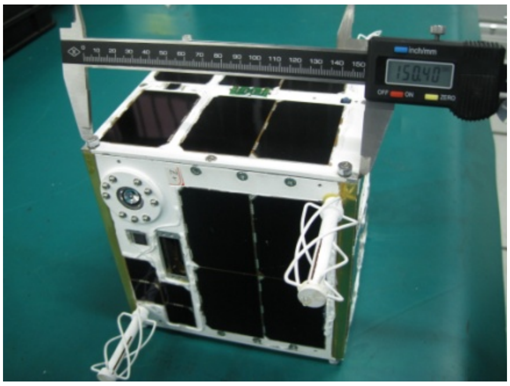

Fig. 1 Photograph of the ZDPS-1A pico-satellite

Usually, the reliability of the computer system may be improved if more mistakes are avoided or tolerated through innovative designs. Traditional satellites usually use fault-tolerant mechanisms, such as hot-backup, cold-backup, and mutual aid backup, owing to abundant space and power. Hot-backup enjoys the best real-time performance; however, its circuit within the arbitration module is so complicated that even when inconsistencies occur between two machines' hot-backups, one still cannot identify the faulty machine. Cold-backup has a monitor module. It has no automatic real-time recovery capability and needs manual intervention from the ground, and thus its real-time performance is the worst. For the HKS of a pico-satellite with high integration, due to limited space and power, we cannot simply copy the fault tolerance design for a traditional satellite (Funase *et al.*, 2007). A more suitable and economic fault-tolerant management system, warm-backup, is needed.

To design the ZDPS-1A satellite control systems based on industrial devices, we adopt CPU warm backup for executing the program, error detection and correction (EDAC) for the reading and writing of the memory, a triple modular redundancy scheme for the reading and writing of part of the data, and two-level watchdogs for switching CPU. A series of recursive experiments, special tests, and environmental tests were undertaken to test the HKS. The size of the HKS system board is within 100 mm×85 mm, and the power consumption is less than 200 mW. This HKS system has already been applied to the ZDPS-1A satellite, which was launched on Sept. 22, 2010 to carry out an in-orbit task. To date, the satellite has been in a proper state for more than 15 months.

2 System design

HKS, as the central system of a pico-satellite, is designed to execute ground communication, data management, energy management, subsystem condition examination, clock check, and payload control. Fig. 2 shows the functional modules of HKS.

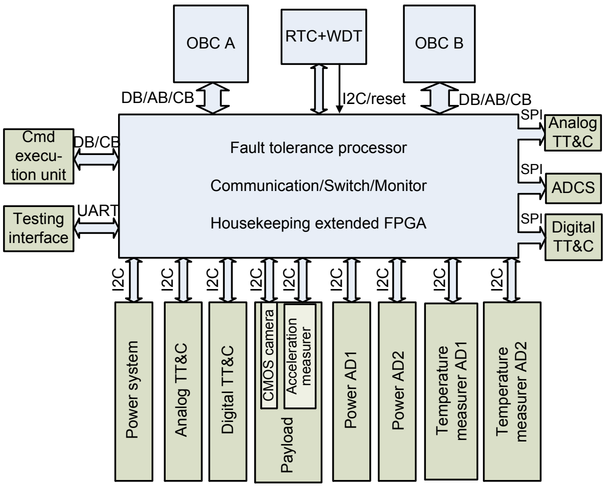

Fig. 2 Block diagram of ZDPS-1's housekeeping system (HKS)
RTC: real-time clock; WDT: watchdog timer; OBC: on-board computer; I2C: inter-integrated circuit; DB: data bus; AB: address bus; CB: control bus; SPI: serial peripheral interface; UART: universal asynchronous receiver/transmitter

As shown in Fig. 2, there are two on-board computers (OBCs) and an extended FPGA for the interfacing and packaging of external sensors and operational parts. Fig. 3 shows the HKS board.

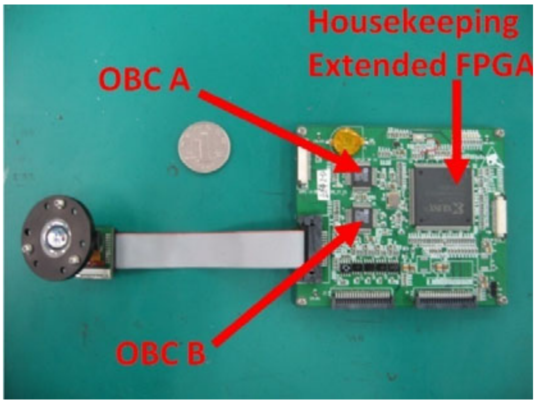

Fig. 3 Photograph of ZDPS-1A's housekeeping system (HKS) board
OBC: on-board computer

The fault tolerance mechanism cannot be too complex because of the limited space and power dissipation, but the reliability is absolutely necessary. This is why the dual redundancy scheme is chosen as the fault-tolerant scheme of OBC (Ma, 2002).

The external subsystems all have communication with HKS. The communication buses are guided outward by the housekeeping extended FPGA, while OBCs A and B are guided inward. The external subsystems can see only one OBC working when OBCs A and B switch seamlessly.

The satellite managing and monitoring modules of HKS use a polling system to collect each subsystem's running data, saving them into the memory, and restarting the related system when errors occur in subsystems (Vladimirova and Sweeting, 2008). The managing and monitoring modules also manage the power supply effectively and ensure a long and stable operation of the satellite through cutting power supplies to certain subsystems, according to the power consumption state. The managing and monitoring modules will respond to the instruction signals from the ground and carry out prearranged operations, thus realizing the ground remote control. Considering that the inter-integrated circuit (I2C) bus may report loss because of damage to one device, OBC thus uses the FPGA to extend the multi-channel I2C bus to communicate with the subsystems. Many important external subsystems are attached to the serial peripheral interface (SPI) bus, which is not good for secure communication. Thus, it is important that each subsystem be attached to only a single SPI bus. The real-time clock and hardware reset modules guarantee the real-time performance for the satellite and are also responsible for resetting the OBC when errors occur. The baseband signal modulation and demodulation modules are responsible for the demodulation and decoding of instruction subcarrier signals, which come from the transponder of the satellite. Those instructions then go through the two-out-of-three screening process. Finally, the indirect instructions are screened out and sent to the main processor. The managing and monitoring modules also receive data from the main processor, encode and modulate them, and then send them to the transponder of the satellite.

3 Reliability design

The reliability design of the pico-satellite's HKS includes such key technologies as CPU warm backup, the static triple modular redundancy scheme, and the two-level watchdog. These technologies are briefly introduced in this section.

3.1 Fault tolerance mechanisms of warm-backup

When the pico-satellite's HKS is working, the fault tolerance mechanism of warm-backup is used. The guest computer is on standby as the system's backup while the host computer is working. This is due to the fact that the running HKS may be influenced by a single event effect such as single event upset (SEU) and single event transient (SET). The chip that has stopped running will not be affected by radiation. Thus, we can disable the input clock of the backup machine. As a result, the guest computer will stop running and the whole system can avoid any effect the radiation might bring. This also decreases the power consumption (Schmidt and Schilling, 2008; Schor *et al*., 2009). Table 1 shows that warm-backup is the most applicable to micro satellites. Although warm-backup needs a longer time for the switchover between the duplex computers, for the pico-satellite which changes its posture slowly by flywheels and magnetic torque, this fault tolerance mechanism is sufficient. Moreover, once a fault occurs, it can be solved by automatic switchover between the two computers, which improves the reliability, real-time performance, and safety of the pico-satellite (Xiang *et al.*, 2005).

Table 1 Comparison of the fault-tolerant mechanisms

Fault-tolerant mechanism	Communications spending	Comeback time	Monitor spending	Invalidation rate	Applicability
Hot-backup	More	Shorter	More	More	Better
Cold-backup	Nothing	Longer	More	Least	Common
Mutual aid backup	Most	Shortest	Most	Most	Poor
Warm-backup	Infinitesimal	Common	Infinitesimal	Less	Good

Warm-backup is a kind of host-guest backup. The host computer is in working state after power-on, and the guest computer is on standby monitoring the host computer. The host computer carries out tasks within a one-second time interval to store key variables and program operation markers into EEPROM. When an error occurs in the host computer, the guest computer takes over and continues its work. We can recover its working state to just one second before the host computer breaks off. Resources are saved and the troublesome mutual judgment activated when the host computer or guest computer breaks down under the dual redundancy scheme is also avoided.

When the system is initiated, by default OBC A begins to work first. OBC A resets the secondary watchdog chip at certain time intervals. If the secondary watchdog is not reset as expected, a reset signal will be produced. When the number of reset signals reaches five, FPGA determines that a serious error has occurred in OBC A and then chooses OBC B to take over the work. OBC B has the same work module as OBC A. To avoid frequent switchovers, OBC B cannot switch to OBC A automatically unless manual interference from the ground is provided. The ground station can track the number of errors, reset the counter, and switch the order of digits. The ground station also decides which computer should be used.

Fig. 4 shows how switchovers between the operation and backup of OBCs are undertaken. It also lists the errors that occur and some temporary operation states.

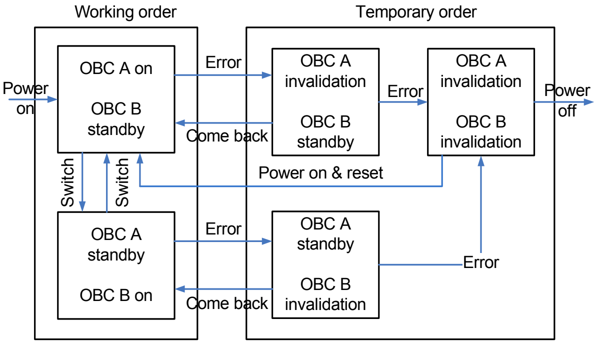

Fig. 4 Fault-tolerant state transformation

The fault-tolerant control scheme of HKS is composed of three stages: (1) error discovering, (2) error dealing, and (3) recovering. When the error is discovered, software will judge if the HKS program has gone into an irrecoverable point. If it can be solved by two-level watchdogs, we may reset only the operations at the task level and component level.

3.2 Two-level watchdog detection mechanism

The watchdogs used in HKS can be divided into two patterns: event-triggering and time-triggering. The event-triggering pattern is used to monitor the number of errors. When the number of errors reaches a certain number, the watchdog then produces a reset signal and the task will be directed back to the boot program. The time-triggering pattern is used to check if the program has run out of time. If the timer is not cleared at an expected time, then the watchdog sends a reset signal to guide the HKS back to standby.

3.3 Fault tolerance structure of the memory module

Along the orbit of the satellite, the memory system in OBC is influenced by space radiation, leading to more errors. That is why in fault tolerance design the encoding technology is adopted to protect the memory module (Eric *et al.*, 2004). The main storage region uses antifuse FPGA to realize the coding for error detecting and correcting (EDAC coding), which is crucial in overcoming the damage brought by the single event upset. The EDAC coding system uses the Hamming code. To visit the data in the main storage region using the coding mechanism, there are four steps:

1. Data preparation. Read the necessary data from the main storage region and prepare to encode.

2. Latch checking. Use the latch to read and check data, and judge if the encoding is correct.

3. Error correcting. If there are errors in the encoding process, correct the wrong codes; if EDAC is carrying out a writing action, reproduce a new code.

4. Updating and recovering. Send the updated data to CPU and correct the related content in the main storage region.

Information stored at the boot area and the system area of a memory system cannot be modified. In other words, it can be accessed only by read only memory. When the information stored at the boot area is needed, we can first check if the encoding is correct and then extract the information to the main storage region. Fig. 5 shows the diagram of the fault tolerance memory module of OBC in which the structure and digit capacity of the data bus are shown. The 32-bit data bus of the CPU is divided into two 16-bit data buses, which are connected to a Hamming encoder and a Hamming decoder, which are identical. The 16-bit data bus and the 6-bit redundant data outputted by the Hamming encoder and decoder are connected to three identical 16-bit static storages. SRAM1 stores the higher 16-bit data while SRAM2 stores the lower 16-bit data. SRAM3 stores the two channels, i.e., the 6-bit data produced by the Hamming encoder and the 6-bit data produced by the Hamming decoder.

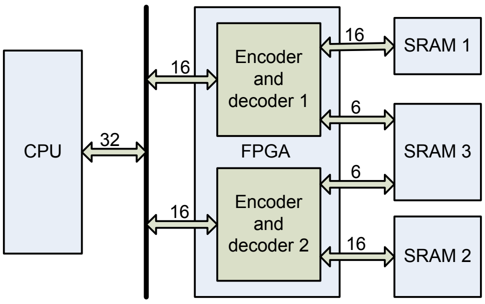

Fig. 5 Fault tolerance memory module of the on-board computer

3.4 Static triple modular redundancy scheme

One of the important applications of the pico-satellite is to collect data from the payload devices in the low earth orbits and monitor and inquire about the state of its subsystems at the same time. When passing by the measurement and control area, the pico-satellite also distributes the framed data in time (Qu *et al.*, 2002). Thus, the correctness of data reading becomes very important. Error tolerance and error diagnosis are needed when errors occur during the data collecting and state monitoring processes. Before the faults reach the output modules, they should all be corrected. HKS uses three identical modules to execute this task and still adheres to the two-out-of-three principle when inputting or outputting the errors (Lashomb, 2002; Majewicz, 2005).

4 Experiments and task data

To evaluate the performance and function of ZDPS-1A's HKS, we undertook a series of recursive experiments, special tests, and environmental tests. Final inspection was verified through the in-orbit tasks, from which we obtained consistent data and curves as per the simulation.

4.1 Recursive experiments

The test team used a simulated ground station and a comprehensive set of software to receive data from HKS. During the test, the HKS was put in different environments and always functioned well. We set up a test platform in the laboratory for SRAM, extracted the data bus of SRAM and the error reporting line, and then injected and detected data from the SRAM on the platform breadboard. Namely, rewrote any bit of any byte of the SRAM by generating a random number, and controlled the CPU to read the data address. As the data unit was upset artificially, the error detected by the decoder can generate reporting-tolerant information. We compared the data from the CPU bus by correcting the device and the data before it was upset. If they are the same, the correction function is realized.

During the test, we created some errors to check if the fault-tolerant system works well:

1. We sent several bad command codes to check the remote control, and the HKS identified the faults and refused to carry out the operations. The status of the operation can be read through the data sent back from the HKS.

2. We lowered the voltage of the power supply. When the voltage was too low, the HKS deemed there is a shortage of energy and closed a part of the system. The whole satellite entered into safe mode to adjust to the power supply. The shutdown of subsystems and the change of voltages and electricity can also be read through the data sent back from the HKS.

3. We undertook a test of the bit error rate (BER): BER=$n_e/(8MN)$, where n_e is the number of error symbols, N is the number of wave channels, and M is the number of total frames tested. As the total number of wave channels is 128 and several channels are always changing, actually the number of effective channels is 70. In experiments, we set a counter M in OBC to calculate the BER. To facilitate counting up the BER, we set M=5000, N=70. The remote test can be replaced by the download format of the real-time tests, and can be uploaded waves for adjusting the remote control. The aforementioned process was repeated three times and an average BER of 8.92×10^{-6} was obtained.

OBCs A and B have been switched normally according to the design strategy. After several recursive experiments, the HKS had been running for

10 800 h without any malfunction. In total, it ran for 10 800 h without an error.

4.2 Special tests

To test the reliability of the HKS, we built a testing platform for SRAM. We guided the SRAM-DB (SRAM_data) bus and input some erroneous data on the platform. We used random numbers to rewrite a random bit of a random byte in the SRAM. When the data was wrongly written, the ERROR bus of the decoder will produce a fault report. If the data modified by the modifier and taken out of the CPU bus was the same as it was before the data was wrongly written, then we can say the error detecting and modifying codes were functioning well.

We used this platform to test the SRAM1, SRAM2, and SRAM3, each for 10 million times. Table 2 shows the results.

Table 2 The error ratios for the three SRAMs

SRAM No.	N_{Error}	N_{Dif}	Error ratio
1	9 999 996	5	5E-7
2	9 999 993	8	8E-7
3	9 999 997	4	4E-7

N_{Error}: the number of fault reports; N_{Dif}: the number of times by which the data is different after the test

Table 2 shows that the error ratios are all within the tolerable range of inaccuracy. Experiments showed that the errors can be discovered and corrected in time.

Regarding the static triple module redundancy scheme, we input a group of incorrect data. Among the three groups of data input, this group of data positions and the positions of its incorrect bytes had all been changed. Moreover, 200 different data combinations were tested. When the three-modular-redundancy mechanism was used, all errors that occurred during the data reading process were corrected. Thus, the expected results were achieved (Mills *et al.*, 2003).

4.3 Environmental tests

To further test the reliability of the HKS, we put the satellite into a Cobalt 60 rad environment where the irradiation dose was 2 rad/s and the total dose was 10 krad, far greater than the total dose in the satellite orbit. The test team used the simulated ground station and the testing software to detect the flip errors and corrected errors eight times within 1.5 h. The system corrected all of these errors. No malfunctions were detected.

When the vacuum degree was below 10^{-3} Pa, the background temperature was below 96 K, and the temperature ranged from −20 °C to 50 °C, the HKS was able to continue working for 16 cycles without committing an error.

In an appraisal mechanics environmental test, bearing a permanent accelerating speed of 8*g*, a random vibration with a total mean square value of more than 12*g*, an impact with a frequency spectrum of more than 1000*g*, the HKS was still able to function without an error.

4.4 Task data

In orbit for 15 months, ZDPS-1A has successfully gone through temperature control, energy management, ground communication, attitude control, imaging control, and other performance verifications.

As in the special test, when the data was wrongly written, the ERROR bus of the decoder will produce a fault report. Thus far, ZDPS-1A has been in a proper state, even though there were 25 error fault reports among the two satellites. All the errors were corrected in time by the fault-tolerant system. The temperature of the satellite was monitored and the temperature inside and outside the HKS was recorded. The temperature curves were consistent with those obtained in simulation. The temperature data on Sept. 22, 2010 (Fig. 6) showed that all parts of the satellite were within a stable temperature range and in thermal equilibrium.

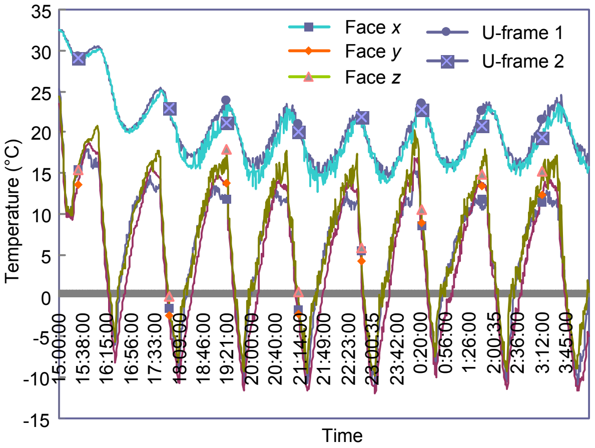

Fig. 6 Temperature curves of the ZDPS-1A pico-satellite on Sept. 22, 2010

Clear photos were taken with the panoramic optical imaging lens with an observation angle of close to 180°. External antennae and fastening screws are outside the field of vision. The blind spot is always in the middle of the picture. Fig. 7 shows the first photo obtained by ZDPS-1A.

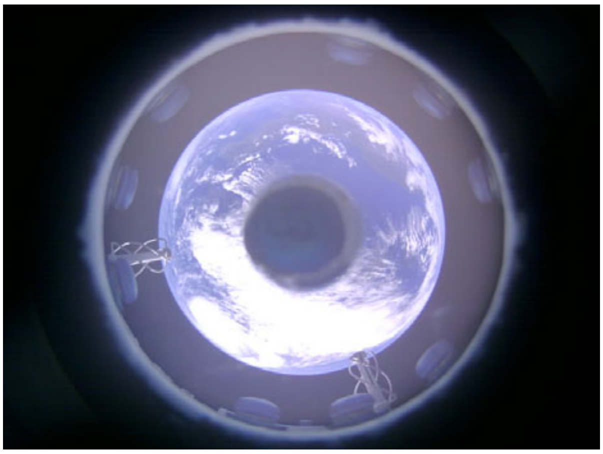

Fig. 7 The first panoramic imaging earth photo obtained by the ZDPS-1A pico-satellite

5 Conclusions

This paper deals with a reliable design of the housekeeping system (HKS) of ZDPS-1A, a pico-satellite designed in Zhejiang University with a mass of 3.5 kg and a power consumption of less than 3.5 W. We used industrial devices to reduce the cost of this satellite. Considering the limits of system volume and energy, we used a dual modular redundancy scheme, a fault-tolerant system, a static triple redundancy strategy for data reading and writing, and two-level watchdogs. Recursive experiments, special tests, and environmental tests showed that ZDPS-1A's HKS is reliable and meets the requirements of the pico-satellite. ZDPS-1A was launched on Sept. 22, 2010 and has been in a proper state for more than 15 months.

References

Eric, J.D., Morgan, K.S., Wirthlin, M.J., Caffrey, M.P., Graham, P.S., 2004. Detection of Configuration Memory Upsets Causing Persistent Errors in SRAM-Based FPGAs. LA-UR-04-7085. Los Alamos National Laboratory, Los Alamos.

Funase, R., Takei, E., Nakamura, Y., Nagai, M., Enokuchi, A., Cheng, Y., Nakada, K., Nojiri, Y., Sasaki, F., Funane, T., Eishima, T., Nakasuka, S., 2007. Technology Demonstration on University of Tokyo's Pico-satellite "XI-V" and Its Effective Operation Result Using Ground Station Network. Department of Aeronautics and Astronautics, University of Tokyo, Japan.

Hamann, R.J., Verhoeven, C.J.M., Bonnema, A.R., 2005. Nano-satellites, a Fast Way to Pre-qualify New Microtechnology. Int. Conf. on MEMS, NANO and Smart Systems, p.263-264. [doi:10.1109/ICMENS.2005.80]

Lashomb, P.A., 2002. Triple Modular Redundant (TMR) Microprocessor System for Field Programmable Gate Array (FPGA) Implementation. MS Thesis, Naval Postgraduate School, Monterey, California.

Ma, X., 2002. Design of Housekeeping System with Fault Tolerance Techniques and Studies up the Reliability of Small Satellite. PhD Thesis, Institute of Technology, Harbin, China (in Chinese).

Majewicz, P., 2005. Implementation of a Configurable Fault Tolerant Processor (CFTP) Using Internal Triple Modular Redundancy (TMR). MS Thesis, Naval Postgraduate School, Monterey, California, USA.

Meng, T., Wang, H., Jin, Z., Han, K., 2009. Attitude stabilization of a pico-satellite by momentum wheel and magnetic coils. *J. Zhejiang Univ.-Sci. A*, **10**(11):1617-1623. [doi:10.1631/jzus.A0820425]

Mills, C.S., Hines, G., Fowler, K.R., Garrison-Darrin, M.A., Conde, R.F., Eaton, H.A.C., 2003. Adaptive Data Analysis and Processing Technology (ADAPT) for Spacecraft. NASA Langley Research Center, Electronic Systems Brand, System Engineering Competency, Hampton.

Qu, F., Cui, G., Yang, X., Tang, X., 2002. The design and implementation of EDAC module in the house-keeping computer system of TS-1.1. *Comput. Eng. Sci.*, **24**(2):70-76 (in Chinese).

Schilling, K., 2006. Design of pico-satellites for education in systems engineering. *IEEE Aerosp. Electron. Syst. Mag.*, **21**(7):S9-S14. [doi:10.1109/MAES.2006.1684269]

Schmidt, M., Schilling, K., 2008. An extensible on-board data handling software platform for pico satellites. *Acta Astronaut.*, **63**(11-12):1299-1304. [doi:10.1016/j.actaastro.2008.05.017]

Schor, D., Scowcroft, J., Nichols, C., Kinsner, W., 2009. A Command and Data Handling Unit for Pico-satellite Missions. Canadian Conf. on Electrical and Computer Engineering, p.874-879. [doi:10.1109/CCECE.2009.5090254]

Sweeting, M.N., 2000. Space at Surry: micro-mini-satellites for affordable access to space. *Air Space Eur.*, **2**(1):38-52. [doi:10.1016/S1290-0958(00)80009-X]

Vladimirova, T., Sweeting, M.N., 2008. System-on-a-chip development for small satellite onboard data handling. *System*, **17**(1):30-35.

Xiang, L., Wu, A., Liao, M., Yang, X., 2005. Fault-tolerant mechanisms of house-keeping computer system for the small satellite. *J. Astronaut.*, **26**(4):400-404 (in Chinese).

Xilinx, 2004. Radiation Effects & Mitigation Overview. Available from http://www.xilinx.com/esp/mil_aero/collateral/presentations/radiation_effects.pdf