Software Fault Tolerance in PISAT

Adithya Krishna*§ , B Naveen Baliga*¶, Harish Kashyap*‖, Mahendra M Nayak†**, Divya Rao A ‡‡†† and V K Agrawal ‡

*Student, Department of Electrical and Electronics Engineering, PES Institute of Technology, Bangalore, India
† Associate Professor, Crucible of Research and Innovation, PES Institute of Technology, Bangalore, India
‡‡ Assistant Professor, Crucible of Research and Innovation, PES Institute of Technology, Bangalore, India
‡ Director, Crucible of Research and Innovation, PES Institute of Technology, Bangalore,India
Email: vk.agrawal@pes.edu
§Email:adithya.krsna@gmail.com
¶Email:naveenbaliga3@gmail.com
‖Email:h.harishkashyap@gmail.com
** Email: mmnayak@pes.edu
†† Email: divyarao@pes.edu

***Abstract*—Systems used in safety critical applications such as satellites are required to be highly reliable. Among these are computing, electrical and electronic systems. High reliability is achieved by using fault avoidance and fault tolerance techniques. Several fault tolerance and avoidance strategies have been used, based on the requirements and constraints of specific missions. These strategies usually lead to an increase in the mass, size and cost of satellites, which makes them a luxury that is not affordable in small scale student satellites. PISAT, a nano-class satellite comprises of Commercial off the Shelf (COTS) components for most of its on-board systems, along with its software being designed and developed by students. Thus, the probability that PISAT is susceptible to faults is higher when compared to a commercial satellite. This paper details the fault tolerance and avoidance strategies implemented and tested in PISAT. These strategies will ensure that the desired mission life of PISAT and any other small scale satellite under mass, size and cost constraints is achieved.**

***Index Terms*— *fault avoidance*; *fault tolerance*; *OBC*; *FDI*; *safe mode*;**

I. Introduction

Satellites need to operate unattended without any failure during their life time. Commercial satellites usually have longer mission lives compared to small scale satellites. There can be no downtime or time for repair during its on-board operation. In case of commercial satellites, this is achieved by using high reliability, radiation hardened space grade components along with fault tolerant software and hardware design. During a mission, satellites must operate successfully without any failure. Satellites are to be designed without any single point failures with adequate redundancy. Commercial satellites use fault avoidance and tolerance techniques to handle faults.

Fault Avoidance is ensured both in hardware as well as in software. In hardware systems, faults are avoided by use of high reliability components and conservative design techniques. Conservative design techniques include use of simple design, adequate de-rating, circuit analysis, simulation and adequate testing in an appropriate environment. De-rating is the operation of a device at less than its rated maximum power to prolong its life. A factor of safety is associated with such components which is simply the number of times the rating of the component is higher than the actual operating value. In software systems, fault avoidance is achieved by following strict guidelines, testing and validation. Testability of the code is another important factor to be considered. The entire code is run and tested; and every possible path and computation is checked using white box testing, black box testing and test automation.

In Fault Tolerance, normal functioning of components is ensured in the presence of faults. When faults occur, they are dealt with such that the functioning of the system is not interrupted. Both hardware and software systems are susceptible to faults and hence both must be made fault-tolerant. The techniques implemented to make commercial satellites tolerant to hardware faults are Redundancy, Fault Detection and Isolation (FDI) and de-graded mode of operation. Redundancy is a technique in which all critical systems of the satellite are replicated. It provides protection from Single Point Failures. These are faults in which the entire system fails due to fault occurring in one system. In case a fault causes one of the systems to malfunction, the redundant system is used to ensure normal operation. By doing so the system works without any interruptions. Care must be taken to keep all the systems updated so that in the event of a failure, the system standing by can quickly replace the faulty one without causing discontinuity in the operation of the system.

The book Fault Tolerant Systems [1] provides a solid introduction to the rich field of fault tolerant computing. It details several hardware and software fault tolerance techniques along with a few case studies implementing these techniques.

In the satellite Hiten, Single Event Upsets in the Microprocessor Unit (MPU) are dealt with using an external Watch Dog Timer (WDT) and an exception handler service routine. In addition to the system program and the user program, the On Board Computer (OBC) has a remote-loading function

978-1-4799-9985-9/15/$31.00 ©2015 IEEE

which allows programs to be loaded from an earth station for house-keeping. This function is important in the OBC mission to modify the experiment scheme after the launch. The components in the OBC experienced 655 single-event upsets (SEU caused by cosmic rays); the bursts of SEU were observed after 9 major solar flares. In spite of these SEU, the OBC worked correctly during the mission time, due to the fault tolerance technique, Stepwise Negotiating Voting [2].

[3] details a small satellite dubbed Icarus, developed by students from the University of Michigan to serve as an active endmass for NASAs ProSEDS (Propulsive Small Expendable Deployer System) electrodynamic-tether propulsion mission. [4] emphasizes the advantages of the COTS approach for future OBCs and reasons for its feasibility. Architecture of the fault tolerant control computer of the BIRD satellite is presented along with 20 months of in-orbit data; especially the experience with its COTS based control computer. [5] describes a technique for incorporating a self-testing capability into the software of a microprocessor-based control system.

A similar study of fault tolerance and avoidance strategies has been carried out for PISAT which deals with failures due to Single Event Upsets, attitude loss of the satellite and handling of unforeseen software errors. This paper details the strategies implemented to overcome the aforementioned conditions.

II. Salient Features Of PISAT

PISAT is a nano-class satellite currently under development at PES Institute of Technology, Bengaluru. The PISAT project was started by a consortium of colleges with the help of Indian Space Research Organization (ISRO) to familiarize students in the area of space technology. The project serves as an educational platform in covering all aspects of build, test, launch and post launch operation of nano-class satellites.

The satellite has dimensions of 254 x 226 x 181 mm. It uses a Magnetic Torquer Rod for attitude control and stabilization. Attitude Determination and Control System (ADCS) is used to maintain the orientation of the satellite. It is three axis stabilized with active magnetic control system. It is controlled using MEMS based Inertial Measurement Unit (IMU) with tri-axial magnetometer, gyroscope and accelerometer and Four Pi Steradian Sun Sensor (FPSS) which is used to determine the orientation of the satellite with respect to the Sun in 4π direction. After separation from the launch vehicle, the satellite goes through four modes of operation - Suspended Mode, Detumbling Mode, Three axis magnetic control Mode and Safe Mode.

PISAT is an imaging satellite, with a GOMSPACE Nanocam C1U as its imaging payload, which uses Cubesat Protocol (CSP) enabled I^2C Serial Communication to communicate with the OBC. The OBC is built around COTS, high performance, low power, 32-bit Atmel AVR Microcontroller, AT32UC3A0512.

TABLE I
SALIENT FEATURES OF PISAT

Subsystem	Features
Payload	GomspaceNANOCam C1U: 3MP 10 bit color CMOS sensor, 2048 x 1536 pixels, ¡80m / pixel resolution from 650 Km, FOV 9.22 deg, I2C communication, onboard compression capability of 6MB to 200KB.
Structure	254 x 226 x 181 mm, Al 6061, Custom made Cuboidal structure, 5 Kg of overall mass.
RF Communication System	Uplink frequency 2030 MHz and Downlink frequency 2240 MHz, Uplink FSK/FM modulation-100BPS Data Rate Downlink BPSK modulation 10kbps, RF Package tested at source.
OBC Hardware and Software	High Performance 32 bit AVR32 RISC C, Clock speed 12MHz, 64 kB Static RAM, 512 kB Storage (Flash Memory), Serial interface I2C Payload -400kbps, SPI IMU 600kbps, External data bus and Address bus, Analog interface : Supports nine temperature sensors, Supports Four Pi Sun Sensor (FPSS), voltage and current monitoring. Software Modular approach, ADCS, all interfaces to OBC, TM and TC is programmed.
Electrical Power System (EPS)	Battery tied bus, DC-DC converters provide supply voltages to OBC and other subsystems, battery safety features provided, current limiter circuit is provided for OBC card to protect C.
Attitude Determination and Control Systems (ADCS)	Pointing accuracy $\pm$ 5 deg, to maintain body rates $\pm$ 0.01 deg/sec, Attitude deviation per one snap shot should be less than one pixel 1 pixel - $7.27 * 10^{-}3$ deg. Sensors FPSS, IMU magnetometer, Gyroscopes and accelerometers, Actuators- Magnetic Torquer Rods, Modes Suspended mode, Safe mode, Detumbling Mode and Three axis magnetic control Mode, ORBIT Determination and Propagation using SGP4 model.
Ground station (S-Band frequency)	3.7m paraboloid antenna with Prime focus and Program tracking, Uplink 2015 to 2125MHz, Downlink 2200 to 2300 MHz.

The tasks performed by the OBC are:

- General housekeeping of the satellite.
- Telecommand, telemetry and payload data processing for communication with ground station.
- Attitude determination and control.

The salient features of PISAT are highlighted in Table I.

A. OBC Software Cycle

The PISAT software cycle as depicted in Figure 1 is designed for a 128 milliseconds major cycle and is divided into 8 minor cycles in which all the required functions are carried out. Once the system is turned on the first function to be executed is the power on initialization which will perform the initialization of CPU, IO, hardware and global variables.

The main program executes all the functionality as required. As the execution enters the main program, it follows a cycle. All the necessary modules, selected based on the mode of operation are executed every minor cycle as shown in Table II.

The following section lists the constraints under which the PISAT project is being designed and highlights the techniques implemented to avoid failures in PISAT.

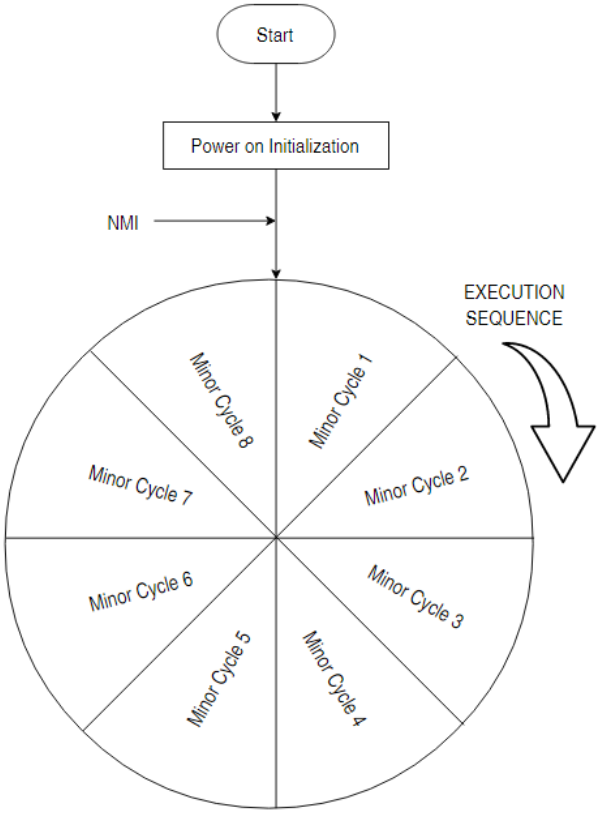

Fig. 1. Software Cycle of the OBC

TABLE II
MODULES INVOKED DURING THE MAJOR CYCLE

Minor Cycle	Functions Called
1	Data acquisition Mode preprocessing TM formatting Battery safety logic check Telemetry Dump
2	Payload image storage Telecommand processing Telemetry dump Orbit propagation
3	GH coefficients generation Magnetic field computation module 1 Telemetry dump
4	WDT reset Magnetic field computation module 2 Telemetry dump
5	Magnetic field computations 3rd routine Telemetry dump
6	Magnetic field computations 4th routine Ground commanded bias estimation routine Mag bias estimation and correction routine Data normalization Discrete attitude determination Telemetry dump
7	Telemetry dump Angular rate estimation and rate filtering
8	Telemetry buffer fill Detumbling mode controller Safe mode controller Three axis mode controller Duty cycle generation Actuator processing Payload, storage telemetry acquisition Telemetry dump

III. Techniques Implemented in PISAT

Despite comprising of COTS components, Conservative Design techniques have been adapted in PISAT hardware design to ensure simple design, adequate de-rating, circuit analysis, simulation and adequate testing in an Electro-Static Discharge (ESD) environment. High Reliability, radiation hardened space grade components have not been used due to cost constraints. The entire code bank of PISAT has been developed by students while strictly adhering to strict guidelines, possible testing and validation.

Due to mass, size and cost constraints, Redundancy in hardware systems is not implemented in PISAT. With the limitations listed in this section, PISAT needs to operate for at least six months without any failure. Hence, a few techniques are implemented in PISAT to ensure reliable operation. This section gives details of the techniques used in PISAT. They are Fault Detection and Isolation (FDI) using WDT, Safe Mode and Remote Programming.

A. Fault Detection and Isolation

This is a minimalistic approach adopted to ensure system operation in case the processor stops functioning due to design limitation and/or single event upset. As per the design, OBC needs to complete all the functions within 128 milliseconds. An external independent watchdog timer is used to time the execution of a major cycle. The timer is programmed to count up to 200 milliseconds. The main program resets the timer every time the OBC completes execution of the major cycle in 128 milliseconds. If the execution of the major cycle is not completed in 200 milliseconds, it implies that the CPU is in an infinite loop and the OBC needs to be reset.

If the OBC takes longer than 200 milliseconds to execute the major cycle, the external watchdog timer generates NMI to the OBC as shown in Figure 2. The NMI tries to bring the control back to start of the major cycle as shown in Figure 1. FDI logic thus attempts to get the system back on track. [6] details a survey of concurrent system-level error detection techniques using a watchdog processor.

B. Safe Mode

Before Safe Mode operations are detailed, this section provides the details of the operating modes of PISAT and

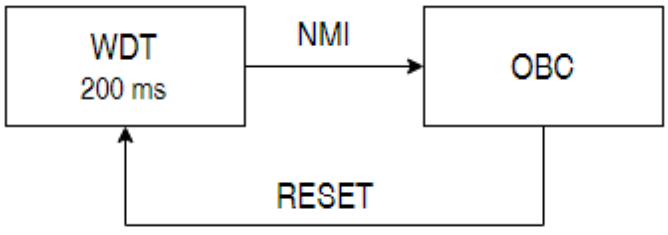

Fig. 2. NMI generation using WDT

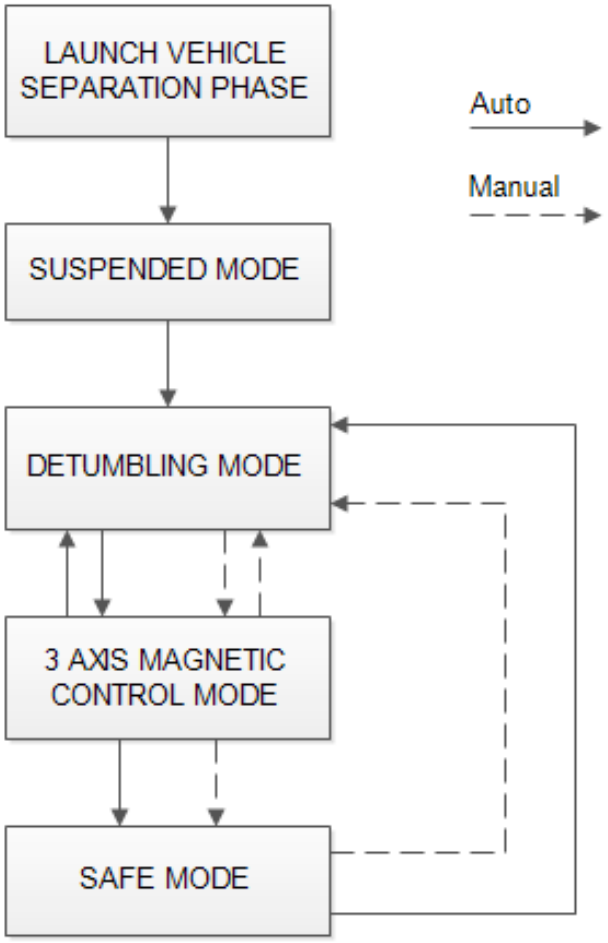

Fig. 3. Operation Sequence

mode transitions. After separation from the launch vehicle, the satellite goes through the following modes of operation as shown in Figure 3.

1) Suspended Mode: The satellite enters Suspended Mode once it has separated from the launch vehicle. All the magnetic torquers are disabled. The operations initiated in this mode by the OBC are: Active telemetry and telecommand function and the monitoring of magnetic field data, rate data, temperature and other sensor data. The transition from Suspended Mode to Detumbling Mode is automatic and happens after 1 minute time duration after separation.

2) Detumbling Mode: This mode is provided to reduce the body rates of the satellite before acquiring three axis attitude control. The transition from Detumbling Mode to Three Axis Magnetic Control Mode can be done both manually and automatically. Manual transition is performed from ground commanding. The automatic transition involves continuous verification of change in magnetic field on-board.

3) Three Axis Magnetic Control Mode: Three axis magnetic control mode includes both three axis attitude determination and control operations. This mode is used for payload operations, i.e., imaging. It will ensure that the payload points towards the Earth and adequate power is available for the satellite. IMU (Tri axial Magnetometer and Gyro + Low Pass Filter) provides the instantaneous magnetic field and angular rate measurements in body frame. The on-board magnetometer measurements and reference magnetic measurements are exclusively used to estimate the three axis attitude in terms of quaternions [7].

The payload is placed pointing in the positive yaw direction. The solar panels are mounted other faces apart from the positive pitch plate, or base plate which interfaces with the satellite ejection mechanism. The Three axis mode has a provision to perform automatic or manual transition to Safe and Detumbling Mode. Auto Transition to Detumbling mode is performed by continuous check on the change in magnetic field with respect to a threshold limit. Auto Transition to Safe Mode is discussed further in this section.

Due to unforeseen disturbances, there exists probability of PISAT positive yaw axis or positive pitch being oriented towards the Sun. These conditions are considered as attitude loss in PISAT control design. During this orientation, it is possible that the power generation on-board may not be adequate for sustained satellite operations. Hence, these conditions are considered as the triggers to Safe Mode. Entry to Safe Mode is determined by the use of Four Pi Sun Sensors (FPSS) placed on the diagonally opposite corners of PISAT to achieve 4 Pi coverage as shown in Figure 4. For auto transition to Safe Mode, the solar cell present in the bottom FPSS must ensure sustained current flow in the positive yaw and positive pitch directions; and FPSS data must cross a certain threshold.

Safe mode performs spin up of about $\pm$ 4 rpm along the maximum moment of inertia axis (Pitch axis) and detumbling about the other two axes. Thus, adequate power generation for the spacecraft is ensured. High rotation about the Pitch axis in Safe Mode implies that the orientation of the payload changes constantly. This ensures that direct exposure of the payload optics to the sun is minimised, thereby protecting the payload from permanent damage.

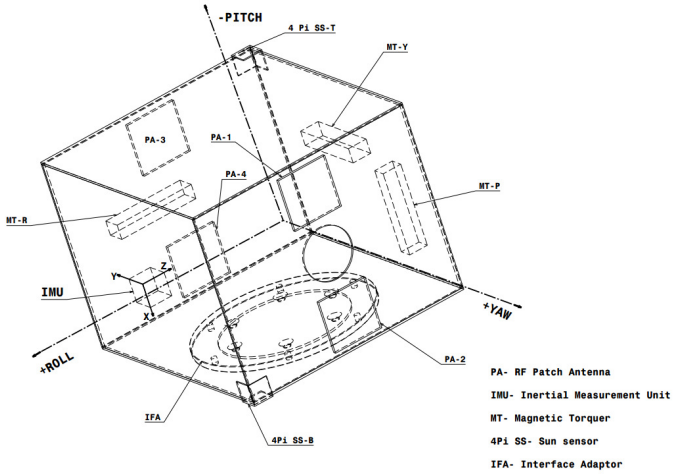

Fig. 4. PISAT Axis Definition

C. Remote Programming

The control gains are fine tuned during the design of the controller. The controller design for detumbling, three axis magnetic control and safe mode is done using Spacecraft dynamics simulation on MATLAB.

Every operating mode of the satellite has its own preprocessing module. The preprocessing module selects the sensor input and controller required for that specific mode. One specific mode preprocessing module will be in execution at any given point of time. In an unforeseen circumstance where the logic in a specific mode is to be modified, dummy mode can be used. PISAT provides for dummy mode 1 and 2 which are placed in RAM, as shown in Figure 5. Using Telecommand, a new mode processing module is uploaded as dummy mode. By selecting dummy mode, control gets transferred to the new mode processing module.

The simulation is performed using actual moment of inertia and assumed spacecraft disturbances. Three sets of fine tuned values are finalized and are flashed into memory. Any one of the aforementioned sets can be selected using telecommand. If it is found that the gain values are not optimal in an actual space environment, there is a provision to introduce a new gain set. This is known as remote gain. This gain set is loaded into RAM, as shown in Figure 6, from ground using existing Telecommand interface. Using remote gain select command the controller can be made to use the new gain set in RAM.

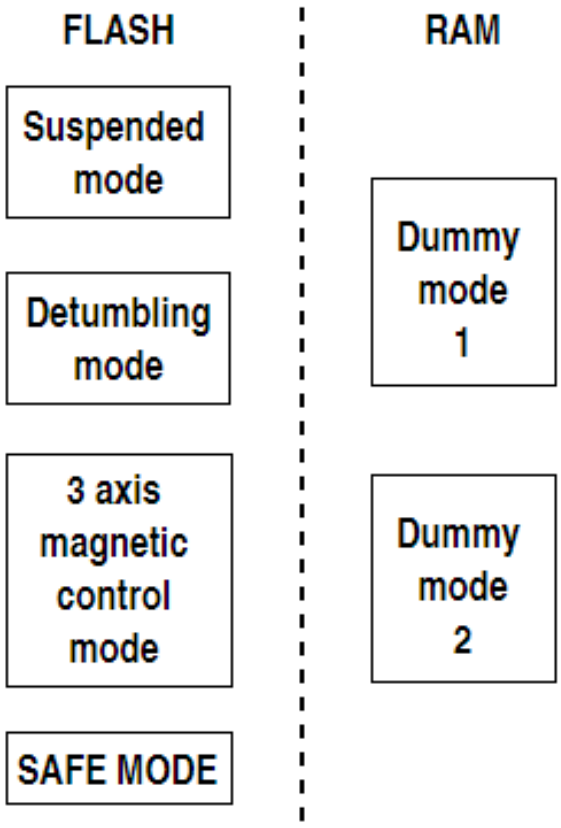

Fig. 5. Location of the four operating modes and dummy modes in memory

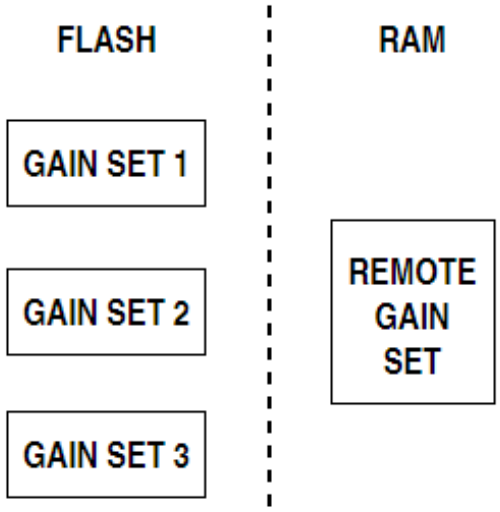

Fig. 6. Gain sets in their respective memory locations

IV. Conclusion

Student satellites cannot implement comprehensive fault avoidance and fault tolerance techniques which are implemented in commercial satellites due to size, weight and cost constraints. Despite this, to ensure nominal mission operations, minimal fault tolerant techniques and remote programming are implemented in PISAT.

This study ensures that -

- Failures due to Single Event Upsets are handled by FDI implementation using WDT.
- Power loss due to incorrect orientation of the satellite is rectified by the satellite entering Safe Mode.
- To take care of unforeseen failures in software, a feature called Remote Programming is implemented which allows the designers to make changes in software even after the spacecraft is launched.

It is expected that these steps will help in making mission operations successful. The features listed in this paper are implemented and tested by bench testing. The test results indicate nominal operation of FDI, Safe Mode and Remote Programming. Going forward, one can look into the feasibility of implementing Triple Modular Redundancy in software for critical parameters.

Acknowledgment

We are extremely grateful to Crucible of Research and Innovation (CORI) for the confidence bestowed in us and entrusting us with the project entitled Fault Tolerance in PISAT. We are very grateful to Prof. K S Shridhar , Principal and Director, PES Institute of Technology, for fostering an excellent academic climate. A special note of thanks to Dr. B K Keshavan, HoD, Department of Electrical and Electronics Engineering and Dr. K N B Murthy, Vice Chancellor of PES University. We also thank research assistant Mr. Raman Gouda, who worked with us on the project and helped us with the equipment at the PISAT Testing and Integration Lab.

REFERENCES

[1] I. Koren and C. M. Krishna, *Fault-tolerant systems*. Morgan Kaufmann, 2010.

[2] T. Takano, T. Yamada, K. Shutoh, and N. Kanekawa, "In-orbit experiment on the fault-tolerant space computer aboard the satellite hiten," *Reliability, IEEE Transactions on*, vol. 45, no. 4, pp. 624–631, 1996.

[3] H. R. Goldberg and B. E. Gilchrist, "The icarus student satellite project," *Acta Astronautica*, vol. 56, no. 1, pp. 107–114, 2005.

[4] P. Behr, W. Bärwald, K. Brieß, and S. Montenegro, "Fault tolerance and cots: next generation of high performance satellite computers," in *DASIA 2003*, vol. 532, 2003, p. 76.

[5] J. G. Tront, J. R. Armstrong, and J. V. Oak, "Software techniques for detecting single-event upsets in satellite computers," *Nuclear Science, IEEE Transactions on*, vol. 32, no. 6, pp. 4225–4228, 1985.

[6] A. Mahmood and E. J. McCluskey, "Concurrent error detection using watchdog processors-a survey," *Computers, IEEE Transactions on*, vol. 37, no. 2, pp. 160–174, 1988.

[7] S. N. Bhat, A. H. Krishnamurthy, and D. A. Rao, "Implementation of three axis magnetic control mode for PISAT," http://icubesat.org/papers/2014-2/2014-b-3-3-implementation-of-three-axis-magnetic-control -mode-for-pisat/, accessed: 2015-03-23.