Proceedings of the 9th World Congress on Electrical Engineering and Computer Systems and Sciences (EECSS'23)
Brunel University, London, United Kingdom - August 03-05, 2023
Paper No. EEE 105
DOI: 10.11159/eee23.105

FS8 Power System Anomaly Protection and Recovery Design

Che Cheng Huang, Chia Wen Hsu
Satellite Avionics Division, Taiwan Space Agency
HsinChu, Taiwan
walton_huang@tasa.org.tw; kevinhsu@tasa.org.tw

Abstract - The Power Control Unit (PCU) in the FORMOSAT-8 (FS8) satellite is to condition energy from the solar arrays and distribute power for all subsystems on the satellite. In order to provide power control and distribution functions in FS8 spacecraft, great reliability and failure recovery for PCU is necessary during the 3-years mission life. Once the spacecraft encounters unknown anomalies and approaches the depletion of the spacecraft battery on-board, the PCU can enter a master emergency condition and introduces PCU master lockout, i.e. spacecraft lockout to dormancy. The spacecraft can be recovered if the space power condition is back to normal. Battery (MainBus) voltage values are monitored to protect the battery from over-charging. Some enable-flags are connected to prevent critical components from activating in accidents, e.g. solar array deployment mechanism.
In this paper, we will discuss PCU hardware anomaly protection and software recovery Fault Detection, Isolation, and Recovery (FDIR).

Keywords**:** PCU, FDIR, OVP, Undervoltage-Lockout, LCL

1. Introduction

FORMOSAT-8 (FS8) is the remote sensing satellite self-developed in Taiwan after FORMOSAT-5. The major mission is earth observation in the low earth orbit. The image data have provided for environment conservation, land development plan, agricultural survey, and international disaster relief.

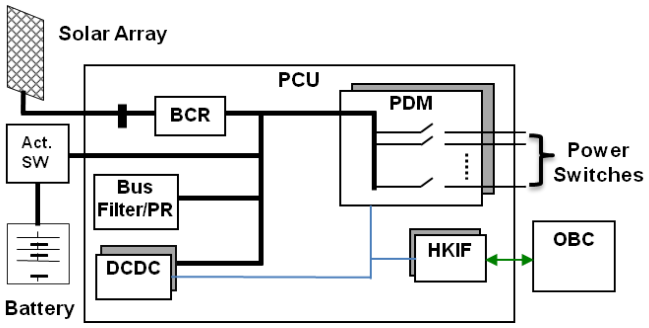

Fig. 1: Function Diagram of Power Control Unit

The Power Control Unit (PCU) in the FS8 program is similar to a human heart. As Figure 1 shows, PCU is in charge of receiving solar power from solar arrays and regulating battery charging current according to On Board Computer (OBC) commands. It also controls and distributes power to various satellite load users upon the request of the OBC command. Any power failures will trig flags and record to Housekeeping Interface(HKIF), and HKIF with communicate with OBC.

Once the spacecraft encounters unknown anomalies and approaches the depletion of the spacecraft battery on-board, the PCU can enter a master emergency condition and introduces PCU master lockout, i.e. spacecraft lockout to dormancy. The spacecraft can be recovered if the space power condition is back to normal. Battery (Main Bus) voltage values are monitored to protect the battery from over-charging. Some enable-flags are connected to prevent critical components from activating in accidents, e.g. solar array deployment mechanism.

In this paper, we will discuss PCU hardware anomaly protection and software recovery Fault Detection, Isolation, and Recovery (FDIR).

2. 2 HARDWARE ANOMOLY PROTECTION

2.1. Over Voltage Protection

In order to get the maximum possible power from solar arrays, maximum power point tracking (MPPT) [1] is planned in the Battery Charge Regulators (BCRs) module The BCRs condition the power from the solar panels for supply to the Li-Ion battery. The battery voltage is monitored by connecting an input from the battery to the BCRs Battery Sense lines. There are 6 BCRs which design with Buck topology [2]. Each BCR frequency is set to around 156.2 kHz. Figure 2 illustrates BCR module functions.

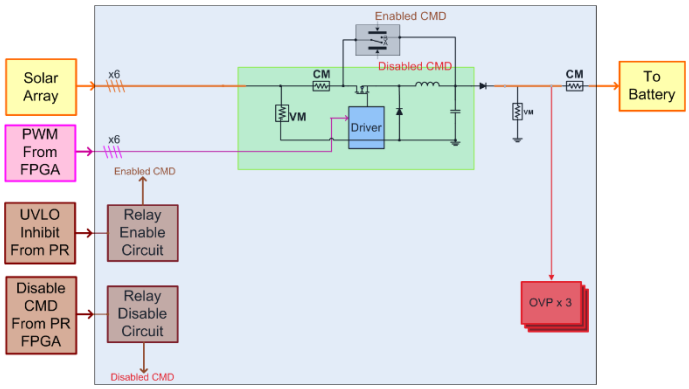

Fig. 2: BCRs module Function Diagram

The BCRs contain battery over voltage protection (OVP) which limited voltage levels to prevent damage to the battery. BCR itself has only passive OVP, which is operated per Table 1.

Table 1: Hardware battery overvoltage protection

Protection On	Protection Off	Panel 1	Panel 2
Level	**Level**	**Off section**	**Off section**
32.75 V	31.5 V	Section 1	Section 1

When OVP is active, the pre-assigned Buck converter switch will skip PWM signal and stays at OFF state, i.e. prohibit associated solar power input, in order to reduce total solar power input spacecraft. The hardware OVP function is done by a major-vote (two of three) circuit to avoid single detection error. A hysteresis loop is used so that the clamp activation voltage is set at least 200mV above the de-activation voltage.

2.2. Undervoltage-Lockout

Undervoltage-Lockout (UVLO) is designed to monitor MainBus voltage and turn off the PCU for protection, when MainBus voltage drop to a specific threshold, all spacecraft will be OFF. Before that, the bypass relay on each Buck converter in BCR is set to a closed state in order to accept all possible solar power without control and wait for spacecraft recovery, as figure 2 shows. This is a latching-type relay.

UVLO enable voltage is set to 22.0V, and the starting from severe failure to nominal spacecraft operation is recovered at MainBus greater than 28.0V. At this moment, all switches are back to their default state. OBC will turn on

other load switches according to flight software procedures. Satellite receivers are able to receive any command from ground operators. Table 2 is the specification of UVLO.

Table 2: The specification of UVLO

Item	UVLO 1~3	
UVLO signal	ON	OFF
MainBus Voltage	22V±2.5%	28V±2.5%

To avoid single point failure, the UVLO hardware detection circuit is designed by three independent detect circuits, which are implemented in an Inhibit voting circuit. Fig. 3 shows UVLO functional block module.

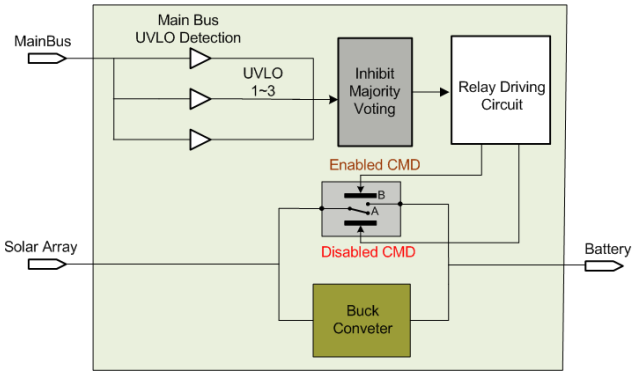

Fig. 3: UVLO functional block module

2.3. Latching Current Limiter

MainBus is the tie point for primary power from the solar panels and the battery. All spacecraft load users are controlled by MOSFET switches with Latch Current Limiter (LCL) [4] protection, as Figure 4 shows. The ON/OFF instruction comes from the OBC CANBUS command.

The LCL will be triggered off if the current is higher than the specified threshold and lasts for 5ms. After trip-off, a flag is set for this condition and the LCL can be reset by reading its trip-off flag from the ground request. The LCL protection is grouped in some outlet, e.g. heater, to save the total number of LCL. All LCLs and MOSFET switches provide ON/OFF status for health data as well. In order to meet the required design and management, the power outlets can be allowed in three protection levels.

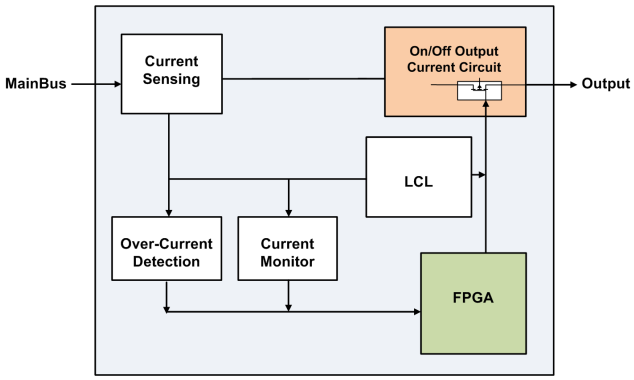

Fig. 4: LCL functional block module

For different failure recovery, four types of LCLs are available on each outlet and can be configured as needed:

- Standard LCLs with one single switching barrier with configurable trip-off currents between level A to level C as in Table 3, and trip-off times up to 5ms.
- Safe-Off (SO-) LCLs with two independent switching barriers allow to switch off the outlet even in case of one failure inside the LCL. Trip-off current up to 1.36A is available.
- Permanent-On (PO-) LCLs which are intended to supply the vital loads of a spacecraft between level A and level C. They are automatically re-activated after trip-off until reactivation is inhibited by command.
- Heater Group (HG-) LCLs supply and protect a group of heater outlet switches. They are standard LCLs available in classes up to 7.5A trip-off current and can be used as Standard LCLs if not needed for heater groups.

Table 3: List of Outlet Protection Level

LEVEL	LATCH CURRENT LIMITATION	TRIP-OFF CURRENT	TRIP-OFF TIME
A	6.82A	3.41A	5ms
B	-	7.50A	5ms
C	2.73A	1.36A	5ms

2.4. Under Voltage

To supply power for PCU internal use, the DC module provides DC voltages which include: digital 5V DC, analog 5V DC, and 45V DC. There are two sections of the DC module, DC-A, and DC-B designed for normal operation and cold redundancy.

Each output voltage in DC-DC converter sections has an under voltage detector to monitor the voltage anomaly. When under voltage occurs, the switchover command will be enabled automatically to switch the nominal set to the redundancy set. If the redundancy set occurs under voltage, it does not allow switching over to the nominal set but the power cycle redundancy set.

3. FAULT DETECTION, ISOLATION, AND RECOVERY (FDIR) DESIGN

The FS8 program design employs on-board software logic and hardware redundancy to satisfy Fault Detection, Isolation, and Recovery (FDIR) [5] requirements for on-board autonomous fault detection and maintaining the satellite in a safe condition. The FDIR covers system, subsystem, and hardware (component, and circuitry) fault monitoring and recovery.

The main purpose of FDIR functions is to detect and isolate hardware and software failures to avoid fault effects that lead to loss of control. The main purposes are as follows:

1.To define fault monitoring items and associated algorithms represented by a set of rules.

2.For flight software responsible engineer to implement the FDIR functions in flight software based on this document.

3.To be used for FDIR software validation plan development.

4.To be used for FDIR validation test plan development for spacecraft integration test.

5.To be a reference document used for system level integration and test.

PCU provides MainBus power to spacecraft components and payload instruments. It consists of hardware components and a software controller residing in OBC. Since power failure is too fast for FSW to detect, it is implemented by hardware or FPGA, and the trigger flag can be accessed by FSW. The following critical credible failures are identified and detection, isolation, and reconfiguration are implemented.

1.MainBus power outlet over current detection by hardware and PCU FPGAs, and isolation by turning off outlet by FPGAs in PCU.

2.MainBus power over voltage detection (as described in 2.1), and isolation by shunt of one section of each solar panel by hardware and FPGA in PCU.

3.MainBus power under voltage level #1 detection by flight software, and isolation by powering off all payload instruments by FSW.

4.MainBus power under voltage level #2 detection by flight software, and isolation by switching over PCU side by FSW via OBC to PCU discrete command.

5.MainBus power under voltage lockout detection (as described in 2.2) by hardware, and isolation by powering off all loads except the detection circuit in PCU.

6.PCU 45V DC under voltage detection by hardware (as described in 2.4), and isolation by switching over PCU side by PCU hardware.

7.PCU +5V DC fail detected by hardware software (as described in 2.4), and isolation by switching over PCU side by PCU hardware.

8.Battery voltage monitoring:

a. FSW will detect the battery voltage failure by comparing the two sets of the battery voltage, if inconsistency occurs, FSW will use bus voltage to continue the monitoring and report the failure event, the one close to bus voltage will be used as good battery voltage, and use the good battery voltage for power control without any isolation and reconfiguration actions. If the two battery voltages are consistent, FSW will use the average to perform power control.

b. After one battery voltage fails, and in case the inconsistency happens between battery and bus voltage, an Auto-Recovery Operating(ARO) will be generated.

9.Battery charge current monitoring:

a. Two sets of battery charge currents will be checked for consistency. If a discrepancy takes place, the BCRs output current and load current will be used to identify the valid one. FSW will report the failure flag and use the good one for battery charge control. If both two are consistent, FSW will use the average of the two telemetries for battery control.

b. If a second fault occurs, the battery charging control algorithm will be changed without using battery current data.

4. Conclusion

We present the PCU architecture description for FS8 Satellite and the anomaly Protection circuit design in the PCU in this study. We have finished the measurement and fine-tuning of this design in Elegant Breadboard (EBB), and Evaluation Module (EM) and implemented it in the Fly module(FM). Extreme environment certifications, like vibration test, thermal cycle test, and temperature vacuum test, are verified as well.

The design of the PCU provides effective, reliable, and redundant solution for the electrical power system of the FS8 satellite. The requirements of an efficient energy conversion and storage, power control, and distribution, both from the solar panels to the battery and from the battery to the PCU, have been realized with precise analysis and verification.

Acknowledgements

The authors appreciate Satellite Avionics Division, FORMOSAT-8 program office and all colleagues at TASA.

References

[1] R. Faranda, S. Leva, and V. Maugeri,“MPPT Techniques for PV Systems: Energetic and Cost Comparison”. Milano Elect. Eng. Dept.Politecnicodi Milano, 2008.

[2] Subudhi, Bidyadhar and Pradhanhen, Raseswari “A comparative study on maximum power point tracking technique for photovoltaic power system,” IEEE Trans. on Sustainable energy., vol. 4, pp. 89-98, Jan.2013.

[3] C. C. Huang, J. J. Yeh, Z. Y. Huang, and C. K. Tseng “FORMOSAT-5 Satellite Power Protection Design,” Applied Mechanics and Materials, Vol. 145, Dec. 2011, pp 536-541.

[4] Herrick, Robert J., “DC/AC circuits and electronics: principles & applications,” Thomson Learning, pp. 378, 2002.
[5] As’ad Michael Salkham, “Fault Detection, Isolation and Recovery inOnBoard Software”,International Master’s Program in Dependable Computer Systems, CHALMERS UNIVERSITY OF TECHNOLOGY Department of Computer Science and Engineering, Göteborg 2005.