SPACE EXPLORATION SYMPOSIUM (A3)
Interactive Presentations (IP)

Author: Mr. SASI SAKETH KURRA
India

FAULT TOLERANT RECONFIGURABLE LUNAR ON BOARD PAYLOAD CONTROLLER

Abstract

The journey of Team Indus has started in 2010 as one of the 32 teams participating in the Google Lunar X Prize competition which challenges any private entity to land on the moon, traverse 500 meters and transmit high-definition images and data back to the earth. As of 2017 only 5 teams have acquired verified launch contracts, Team Indus being one of them and the only team from India has secured a launch contract from ISRO for PSLV with a scheduled launch in December 2017. The Lunar On Board Payload Controller sits on the lunar rover module and commands the on board cameras to capture HD images and video, controls the wheel motors for traversing the moon, interfaces with other payloads for establishing telecommand and telemetry links with the ground station. This paper emphasizes the fault tolerant capabilities, reconfigurability and security features implemented on the Lunar On Board Payload Controller which constitutes a System on Chip (SoC) as its central processing element. The SoC embeds a dual core cortex A9 ARM v7 processor and FPGA fabric on a single monolithic die. The navigational course correctional algorithms of the lunar rover run on the processor and the FPGA caters to the requirements of interfacing and data processing. There is a continuous Cyclic Redundancy Check (CRC) at regular intervals to check for any Single Event Upset's (SEU) in the configuration memory, if there is mismatch in the CRC check the SoC is reconfigured by TC from ground station to bring it back to known state. The Castagnoli CRC (CRC32C) algorithm with the polynomial 0x1EDC6F41 is implemented for its efficient process cycles. The SoC also has an on-chip ADC which monitors the voltages and die junction temperatures and triggers programmable alarms in case of any anomaly caused due to the SEU's. The overall system is made robust with implementation of RSA-2048 authentication protocol and AES-256 encryption algorithm which enhances the integrity and reliability of the design. The configuration bitstream is encrypted and stored in the external flash and the AES key will be loaded into the Non Volatile Memory (NVM) of the FPGA so as to configure the FPGA upon system boot. The BootROM will also have to authenticate the encrypted first stage boot loader (FSBL) using the RSA-2048 authentication protocol adding one more level of security on top of encryption.