IAF SPACE EXPLORATION SYMPOSIUM (A3)
Moon Exploration – Part 3 (2C)

Author: Mr. SASI SAKETH KURRA
India

PAYLOAD DATA INTEGRITY ON LUNAR DATA PROCESSING MODULE USING ENCRYPTION AND AUTHENTICATION

Abstract

Google Lunar XPRIZE was a global competition to land a spacecraft on the moon, traverse for 500 meters and transmit high definition imagery back to the earth. Team Indus was one of the 32 teams which entered the competition in 2010 and was one among the five finalists. Team Indus had also ended up being the only team from India and had won the landing milestone prize upon being evaluated on various structural aspects by the Google Lunar XPRIZE judges. Axiom Research Labs, the parent company of Team Indus is collaborating with various launch providers for securing a launch contract.

The Team Indus spacecraft comprises of a lander and a rover with few other scientific payloads. The lunar data processing module is the core processing system on the rover. It receives data(telemetry) from the rover and other payloads over a multi-drop full duplex data bus. The module relays the telecommands from the lander to the rover over the RF link for the locomotion of the rover, imaging and sends back the images and housekeeping data of various sensor units as telemetry. So, integrity of the data stored on board the rover is of high significance to avoid any sort of error accumulation on its transmission path back to the ground station through the lander communication link. This paper emphasizes the importance of establishing a chain of trust in the data propagation path by use of encryption and authentication. This level of integrity is achieved by employing robust encryption engines like AES (Advanced Encryption Standard) and Hashed Message Authentication Code (HMAC) along with the RSA authentication mechanism.

The lunar data processing module has special registers to handle the key management requirements specific for the implementation of AES-256 algorithm. A total of $1.1 * 10^{77}$ combinations is possible for the AES-256 key. The HMAC SHA-256/ RSA-2048 authentication provides additional security encompassing the encryption algorithm for the module. In addition to these cryptographic security features any anomaly can be identified and handled appropriately by using the on-chip sensors available within the lunar data processing module which can monitor variations in temperature, current and voltage during its course of operation.