23rd IAA SYMPOSIUM ON SMALL SATELLITE MISSIONS (B4)
Generic Technologies for Nano/Pico Platforms (6B)

Author: Mr. Fernando Rodriguez
Clyde Space Ltd, United Kingdom, fernando.rodriguez@clyde-space.com

Ms. Libby Hoban
Clyde Space Ltd., United Kingdom, libby.hoban@clyde-space.com
Ms. Jenni Doonan
Clyde Space Ltd, United Kingdom, jenni.doonan@clyde-space.com
Mr. Craig Clark
Clyde Space Ltd, United Kingdom, craig.clark@clyde-space.com

ERROR MITIGATION TECHNIQUES FOR ON-BOARD COMPUTER SYSTEMS

Abstract

As the applications of CubeSats become more sophisticated, there are increasing demands on the CubeSat platform to deliver the required system performance. These demands include the ability to realize fine attitude control, better on-board processing ability and higher data downlink rates.

As the profile of the CubeSat customers moves towards those looking for commercial services and an increased guarantee of performance and reliability, risk reduction is becoming a dominant metric, from supply chain management to deployment, operation and decommissioning. While the use of COTS components is essential to meet the power, performance and cost requirements expected by our clients, their use introduces specific vulnerabilities which need to be addressed before a robust product can be produced.

In this paper we present the technical approach taken by Clyde Space in the design of reliable and robust on-board computer systems constructed from unreliable state of the art COTS components, in particular exploring techniques used to detect and correct errors within memory and communication subsystems including defensive mechanisms, component selection, architectural design, protocol and software design, system integration and testing.

Amongst the distinctive features of our approach are defensive subsystems which include a real-time ionising radiation sensor (which is used to implement pro-active defence protections), and a TID sensor, which is used to anticipate system failures. Memory contents is protected via a modified Hsiao code, and error detection is furthered by inclusion of an address protection Hash to guard against SEFI transients. Systems registers employ similar techniques and in particular guard against software corruption via the aforementioned address hashing mechanism.

Finally we present results from simulations and from our hardware prototypes and compare them against more standard protection mechanisms.