Paper ID: 17251
oral

SPACE SYSTEMS SYMPOSIUM (D1)
Enabling Technologies for Space Systems (2)

Author: Prof. Nicholas Mc Guire
Beijing Shenzhou Aerospace Software Technology Co., Ltd., China

Mr. Andreas Platschek
OpenTech EDV Research GmbH, Austria

ROOT-VOTER BASED RELIABLE COMPUTING BASE

Abstract

With increasing autonomy of space systems, growing complexity of applications and increasing computational capabilities of space grade processors suitable for critical systems, the operating systems (OS) architecture for critical on-board computing needs to evolve as well. Partitioning as one of the key strategies for co-locating applications of different criticality is well established and reflected in some of the main domain specific standards (e.g. 178C/ARINC 653), but re-using these avionics concepts, designed to cover relatively low single event upset (SEU) rates, in space born systems poses some challenges. While the concepts can satisfy the safety requirements, they can not provide the availability and reliability demands given the high SEU rate without further measures.

In this paper we introduce the root-voter concept as the basis for extending the triple modular redundancy (TMR) to provide improved availability and reliability of software components. We argue that SEU and TDI/SEL must be treated at different levels of the overall system design. To achieve the necessary flexibility and computational capabilities of the next generation space born systems though we believe that a de-coupling of the reliability/availability and safety properties from the traditional hierarchical OS design is needed, transforming the highest complexity components into a gray-channel and mitigating the space-environment impact by virtual replicas. At the same time the safety properties of the application layer can be ensured by providing a pool of reliably cross-node voted objects directly managed by the hypervisor. This pool of reliable objects is accessed from the application through hypercalls that bypass the complex intermediate layers. Similar to trusted computing - this allowing to deduce application level properties through objects that are cross-node voted.

Starting at the system level requirements we develop the OS requirements and the allocation to the main OS components. From this SW-architecture we then develop the application architectural requirements and the operational demands to achieve suitable reliability and availability without compromising safety. While there have been many proposals based on elaborate hardware design to achieve fault tolerance we focussed on the use of software methods and minimizing the constraints placed on the hardware design. The goal is the use of highly complex software components including full featured operating systems for the NextGenOS space born platform.

This report is based on the current status of the NextGenOS at Shenzhou Aerospace Software Technology, we present our design strategy and current architecture based on the novel concept of a root-voter.