Paper ID: 46835
oral
student

25th IAA SYMPOSIUM ON SMALL SATELLITE MISSIONS (B4)
Highly Integrated Distributed Systems (7)

Author: Mr. Johan Carvajal-Godinez
Delft University of Technology (TU Delft), The Netherlands

Dr. Jian Guo
Delft University of Technology (TU Delft), The Netherlands
Prof. Eberhard Gill
Delft University of Technology, The Netherlands

ACHIEVING CONSENSUS IN DISTRIBUTED SOFTWARE ARCHITECTURES FOR SATELLITE MISSIONS

Abstract

Spacecraft buses using distributed software architectures are being adopted in space missions design due to their increased performance and reliability. However, to achieve reliability in highly distributed and concurrent systems, fault-tolerant mechanisms must be implemented to mitigate non-nominal behavior of components and software processes. One of the most significant challenges in designing distributed software is related to the consensus of processes running in parallel. For instance, consider the attitude determination and control subsystem is trying to estimate the current satellite orientation. For that purpose, it has to request measurements to multiple sensors connected to the spacecraft data bus, and it has to organize this information in the right chronological order for proper state estimation. A wrong data sequence can lead to an increased pointing error during satellite operations. Consensus protocols in distributed software architectures are mainly focused on voting mechanisms, which work well when the process in charge of the decision making (leader) can trust the data coming from all processes and components supplying information. In an execution environment with faulty processes, the system can reach decisions that do not reflect the true status of the system due to corrupted or missing information. This paper describes and analyzes software consensus scenarios in spacecraft with distributed data buses operating in a linear topology. These scenarios include state estimation with networked components, temporal consistency of telemetry packets and on-board scheduling planning. The work presents a comparison of strategies for process leader election and task agreement. It takes as a reference the Paxos algorithm family to establish an optimal configuration for achieving consensus in distributed software architectures. The proposed approach also introduces mechanisms to reach measurements consensus under intermittent sensor failures, as well as analyzing scalability issues. Finally, the work proposes the adoption of software design patterns that guarantee consensus on time-critical processes such as attitude determination and control. By adopting these patterns, the satellite is capable of adapting the scheduling of data broadcasting on the bus from a first-in-first-out scheme to a priority based implementation that benefits both performance and reliability. This work enables to define and evaluate software performance and reliability with respect to the criticality of its processes to achieve consensus. It also facilitates fault detection and recovery capabilities by design, during the software development phase of the satellite. Finally, a set of software design rules is provided that can be used to improve the resilience of satellite's on-board software.