Paper ID: 44320
oral

IAF SPACE SYSTEMS SYMPOSIUM (D1)
Technologies to Enable Space Systems (3)

Author: Mr. Andreas Wortmann
OHB System, Germany

BEYOND FUNCTIONAL CORRECTNESS - GETTING FLIGHT SOFTWARE TIMING RIGHT

Abstract

Many functions realized by software in satellite systems are subject to real-time constraints. Such functionality ranges from complex control algorithms including Attitude and Orbit Control to governance of communication bus systems and direct interface and I/O accesses. Even in contingency situations and in the case of hardware anomalies the software execution must be correct and obey all timing constraints in order to ensure safety and reliability of the satellite and its mission. With increasingly large and complex flight software the traditional approach for ensuring timing-wise correctness of the overall system according to the "look whether it works for all my test cases" approach is not sufficient anymore. This is acknowledged and addressed by the ECSS, calling for a computational model of the software that may serve as a mathematical model for the software schedulability analysis. Even though the foundation of formal schedulability proofs reaches back to the 1970's, applying the theoretical achievements to commercial satellite software is not yet standard. In the latest missions developed at OHB we have gradually improved awareness and skills in this regard. Being able to efficiently perform timing analysis requires integration of several steps throughout the design and development process, including strict coding, modeling and design rules. Such additional steps need to be in accordance with many other quality and process requirements imposed on flight software.

Roughly speaking, Software Schedulability Analysis consists of three components. A) The tasking model that represents the software comprising tasks, task interactions, the scheduling policy and external triggers. B) Timing information of a large number of code snippets and procedures that are executed by the different tasks. C) A set of constraints that are required to be met. Each of these components impose requirements on the software specification, design and development that are crucial for an analysis to be carried out successfully. The process that hopefully proves the flight software to be compliant with the timing constraints under all conditions engages a set of commercially available and inhouse software tools.

The presentation provides an overview on the techniques and tools successfully engaged at OHB, present some lessons learned and summarizes coding and design guidelines. Furthermore, an outlook on possible future achievements with respect to toolchain optimization (e.g. improved developer guidance and "push-button" analysis) and future processor hardware (e.g. multi-core and distributed systems) will be given.