On Board Model Checking for Space Applications

A. Cimatti[1] A. Guiotto[2] Marco Roveri[1]

[1]Fondazione Bruno Kessler
{cimatti,roveri}@fbk.eu

[2]Thales Alenia Space Italy
andrea.guiotto@thalesaleniaspace.com

Abstract

In the framework of the European Space Agency (ESA) research studies, Thales Alenia Space and Fondazione Bruno Kessler have investigated the use of model-checking in on-board space systems in order to increase their degree of autonomy.

In the traditional approach, the control of a spacecraft takes place mostly from ground, through the exchange of sequences of low level commands. Spacecraft is typically unable to deal alone with unexpected events from the environment or unpredicted on-board failures. In deep space and remote planetary exploration missions the limits in communication between ground and spacecraft (in time and bandwidth) increase reaction times and can decrease the efficiency of corrective actions.

Providing remote systems with the ability to create their own plans based on up-to-date information and enabling them to –re-plan in response to dynamic events would greatly improve the efficiency of a mission and potentially improve the safety of systems. Ground operators can use the restricted communication link to forward high-level mission objectives, which the on-board system can turn into detailed commands. Execution can be monitored continuously and re-planning invoked when any execution problem occurred.

The software prototype developed in the study, called Autonomous Reasoning Engine (ARE), is based on model-based-reasoning. It is structured according to generic three-layer hybrid autonomy architecture: Deliberative, Executive and Control Layers. The Deliberative layer provides goal-driven planning and scheduling, plan validation and system-level FDIR facilities. The Executive Layer provides facilities to execute and monitor the correct execution of the current mission plan. The Control Layer provides low level interactions with the controlled system (sensor acquisition and commands to actuators sending).

The ARE relies on NUSMV, a symbolic model checker in the Deliberative and Executive Layers, where it performs all its reasoning on a formal model of the system it controls. The feedback control loop algorithms of the Control Layer are not based on symbolic reasoning, since complex numerical computations may be involved. The Control layer uses the model to encode low level sensor information, and to decode commands to be sent to actuators.

However, such computations are directly connected to the formal model through abstraction of the computation results into logical predicates. In this way, the computation steps are interleaved with logical reasoning at the higher levels. The formal model captures the intrinsic partial observability of the controlled system (available system sensors may not allow for conclusive determination of the controlled component's

status). Development and validation of models is supported by a set of off-line model checking tools.

The approach is evaluated on two case studies (a planetary rover and an orbiting spacecraft), in order to characterize the approach in terms of reliability, availability and performances.