Software Modeling and Verification Chair

RWTH AACHEN UNIVERSITY

— Master's Thesis —

Modeling and Analysis of a Spacecraft Mission

What is it all about? New spacecraft are continuously being developed. As spacecraft become more and more complex, the use of formal methods are necessary to ensure their reliability, to avoid potentially dangerous, and costly, failures. The COMPASS [com] toolset aims to improve our capabilities of performing formal analysis of spacecraft.
Currently however, there is no openly accessible case study available for the toolset. Therefore, we are looking for someone interested in performing such a case study and help improve the possibilities of the industry adopting COMPASS.
As the COMPASS toolset is developed jointly with `FBK` and the `ESA`, the case study will be developed together with them (this may include for instance a research visit at either location).
To give an idea of what is possible, some possible case studies are listed below.

SAFER NASA has published a case study called SAFER (Simplified Aid for EVA - a secondary safety device used to allow astronauts to return to the spacecraft when performing a spacewalk) as part of their practitioners' companion (part 2) of the Formal Methods guidebook [Cov95]. Several publications already exist modeling this case study which of course may be helpful.

FireSat The book Space Mission Analysis and Design by Larson and Wertz [JW99], a classic text used in teaching aerospace engineering, contains a running example called FireSat, a system to detect forest fires to speed up dispatching of fire services. The book presents the case study from the mission perspective all the way down to the spacecraft design. A case study based on FireSat has been performed at the OMG [omg] as well, using SysML.

EagleEye EagleEye is a "fake" earth observation mission defined by ESA to demonstrate the capabilities of the Avionics Test Bench (another project of ESA). Less information is available for this case study, as the project is still under development and collecting documentation ay take some time. Nevertheless, the people at ESA are interested in evaluating the possibilities.

What is to be done?

1. Determine which case study is the most suitable: Which aspects does the case study offer, and what can be done using the toolset;
2. Model the case study and define the formal properties of interest;
3. Evaluate the case study using the COMPASS toolset.

Requirements

- A basic understanding of discrete, hybrid and probabilistic systems is required, along with some of the common formal logics that are used for verifying properties on such systems (e.g. LTL, CTL, MTL or CSL).

Contact

- Harold Bruintjes, h.bruintjes@cs.rwth-aachen.de, Tel. 0241/80-21206 or drop by in room 4203.

References

[com] COMPASS, `http://compass.informatik.rwth-aachen.de`, Accessed 07.03.2016.

[Cov95] Rick Covington, Formal methods specification and verification guidebook for software and computer systems; volume 1: Planning and technology insertion, Tech. report, volume NASA-GB-002-95. National Aeronautics and Space Administration, 1995.

[JW99] R Wertz James and J Larson Wiley, Space mission analysis and design, MicrocosmPress, Torrance (1999).

[omg] Object Management Group, `http://www.omg.org/`, Accessed 07.03.2016.