Evolving and Traceable Non-Functional System Requirements in Space Mission Design

PhD Research in Cooperation with the German Aerospace Center (DLR)

Jafar Akhundov & Prof. Dr. Matthias Werner
Chemnitz University of Technology, Computer Science

Philipp Fischer & Dr. Andreas Gerndt
German Aerospace Center (DLR), Institute for Simulation and Software Technology

Contact Information:
Jafar Akhundov
Operating Systems Group, TU Chemnitz
Straße der Nationen 62
09111 Chemnitz

Phone: (++49) 0371 531 32559
Email: `jafar.akhundov@cs.tu-chemnitz.de`

Abstract

Because of the complexity of spacecraft systems, many domain experts are involved at different design phases. Systems engineering process is applied in iterative and recursive manner in each phase until the design of distinct components becomes manageable. Therefore, baseline properties proven and verified for a subsystem must hold with respect to composition of system components to a whole. The goal of this research is to provide a formal refinable modelling formalism which would allow for compositional analysis, design and verification of system requirements. Essentially, the properties of interest are non-functional system properties, such as timing, including clock synchrony, and fault tolerance. Such a meta-model can be applied for generating a new or integration into an existing operational timeline of a space mission from system description, code generation for a matured project in later phases, generation of specifications and documentation for Key Decision Points (KDPs) and mission reports.

As a formal basis for describing system's behaviour linear time-invariant hybrid automata have been introduced. The goal of this research is to apply this newly developed formalism to specify and verify system feasibility, stability, existence of invariants from the earliest design phases, as well as non-functional system properties. It is furthermore necessary to define transformation rules for refinement and composition for the the LTI-HA models with respect to the verifiable properties which will formalise their transition through the design phases. The introduced formal method along with the verification algorithms are implemented and integrated into the Virtual Satellite software tool developed at the German Aerospace Center (DLR) which applies model-based systems engineering to model highly complex spacecraft systems.

Introduction

Spacecraft industry is developing at a rapid pace with the tendency towards distributed complex systems (swarms, constellations, formation flying, etc.) with many possible applications: planet surface observation, deep space (asteroid mining, planetary research, etc), human bases on the Moon and the Mars, etc. New space missions present new challenges due to their complexity. Non-functional system properties, with the exception for fault analysis, are not always considered to be of thorough investigation. Such as, the first unmanned space shuttle probe crashed due to unsynchronised board computers, Pathfinder rover has experienced operational problems due to the priority inversion problem, etc.

It is therefore reasonable to develop a necessary formalism and tools to support engineers in their efforts and automatise verification of such properties as far as possible, or provide necessary feedback information at the earliest during the design so that design costs are minimised.

Main Objectives

The current research has two main objectives:

1. To find a refinable and composable formal method to specify, analyse and verify non-functional system properties from the earliest design phases when information is quite scarce, and
2. to develop a space mission meta-model with transformation rules as a formalism for composition and refinement of formal models (possibly defined using different methods) under specific conditions.

The first goal is represented by the marbles in the Fig. 1. The growing amount of information with every new design phase is represented by the increasing circumference of the marbles. This is motivated by the refinement property. The second goal corresponds with the arrows in this diagram, which represent possible transformation of representation, more refinement, composition of several components to a whole, etc.

As an example for analysable properties for a system at early design phases feasibility of the space mission, its stability, existence of invariable properties could be mentioned. As a use case for non-functional system properties, timing, such as meeting deadlines and synchrony, and fault tolerance will be used.

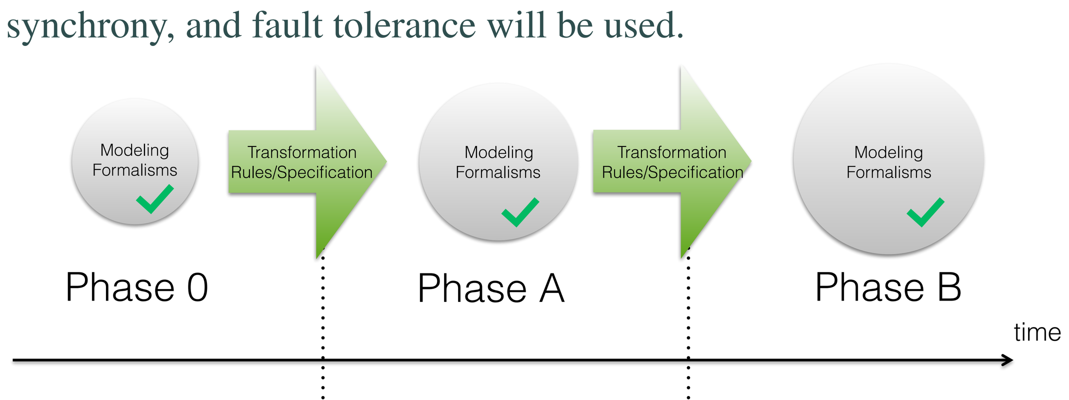

Figure 1: Multi-phase model-based spacecraft design process with growing amount of information and transformation rules for transitions between the phases

Methods and Tools

It has been demonstrated that both timed and hybrid automata can be used for the formal specification of spacecraft systems at the earliest design stages [3][2][4]. Hybrid automata are be more expressive in terms of describing second and higher order phenomena such as acceleration of mechanical systems. However, even timed automata have been demonstrated to be applicable for spacecraft systems with linear rate of state change [2]. They have been used to check for mission feasibility. System description in this case has been limited to system components (e.g. payload experiment, battery charge, downlink, etc.) being either active or inactive, whereby their activity would continuously change the system's state. That is, the question of mission feasibility has been translated to the problem of automata reachability.

The property of composition and refinement is crucial for building complex systems from smaller components and has been addressed in [4]. As such, for the purpose of composition a new hybrid automata formalism - linear time-invariant hybrid automata (LTI-HA) - has been introduced because of the lack of support for superposition in the other methods [4].

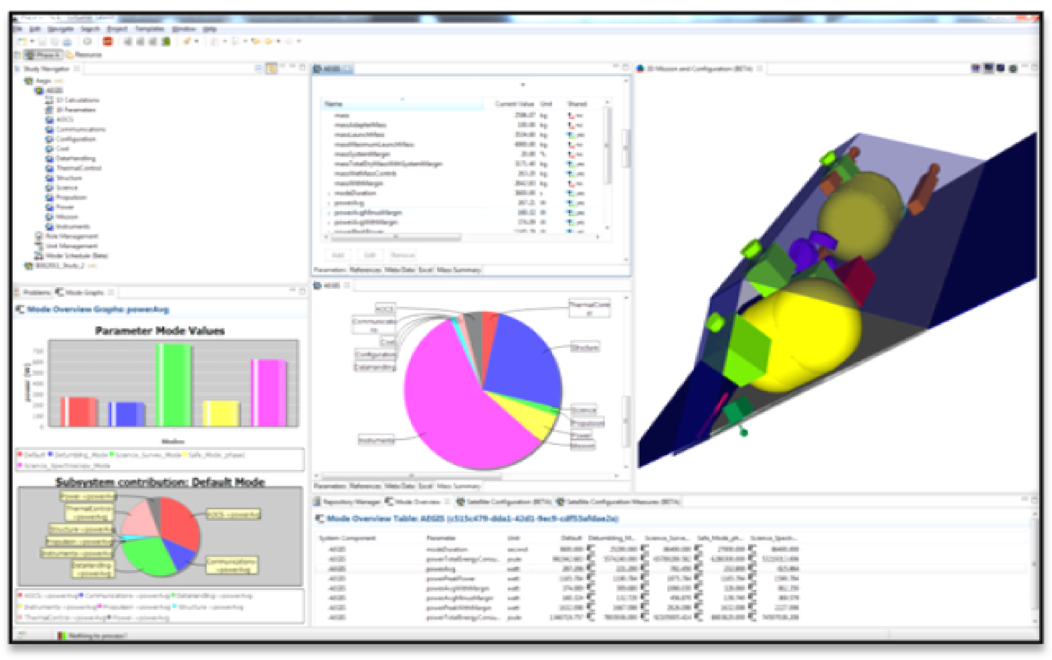

Figure 2: Virtual Satellite is a tool developed at the Simulation and Software Technology Institute (http://www.dlr.de/sc/en/) of the German Aerospace Center (DLR) which enables many domain experts to design a spacecraft from the earliest design phases concurrently

To further support spacecraft engineers in modelling and analysis of space missions using the new LTI-HA formalism, software tool is being implemented using Eclipse Modelling Framework and integrated into the highly successful Virtual Satellite Project (VirSat). VirSat (Fig. 2) is a general tool designed at the institute for Simulation and Software Technology of the German Aerospace Center (DLR). It accommodates model-based systems engineering to support spacecraft system designers, e.g. at the Concurrent Engineering Facility (also DLR) in Bremen.

Figure 3: European Space Agency's (ESA) ATHENA mission is an X-Ray telescope that is to launch in 2028 and must answer the questions: How does ordinary matter assemble into the large-scale structures we see today? and How do black holes grow and shape the Universe? (Source: ESA)

Current and Planned Work

Current and upcoming work includes but is not limited to:

1. Defining the analysis procedures for the LTI-HA formalism, investigate their complexity and decidability, and implementing them;
2. Comparison of the LTI-HA formalism's expressiveness with the established HA modelling methods;
3. Definition of correctness criteria for the LTI-HA models;
4. Using the LTI-HA formalism to define space mission in the earliest design phase so that feasibility can be analysed from the beginning of the design. The used method should be able to generate an operational mission plan which can be later refined and will be used as a basis for integration and analysis of non-functional system properties;
5. Classification and parametrisation of space missions, study of existing mission reports to derive a generalised refinable spacecraft meta-model;
6. Determine when in the design phase specific non-functional requirements are available for modelling and analysis by studying mission reports and documents. For this purpose, distinct types of space missions should be considered, such as manned (space shuttle) or unmanned (ATHENA, Mars rovers), deep space (Juno, Rosetta) or near-Earth (TandemX), single spacecraft (TET-1) or a constellation/swarm (LISA), etc;
7. Investigating the ways of representing timing and fault model information in the LTI-HA formalism, analysing it;
8. Studying how does a formal non-functional requirement in form of a model(s) transform and evolve over time by comparing different mission reports;
9. Implementation of necessary software tools, their testing and integration.

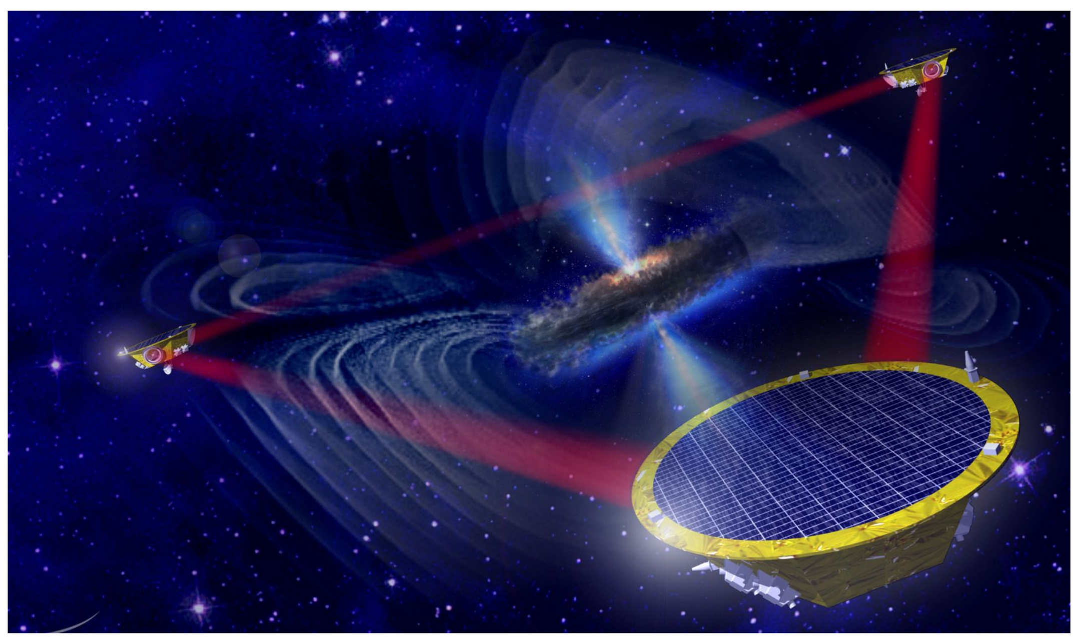

Figure 4: The LISA mission is a cooperation between European Space Agency (ESA) and NASA. Its mission is to detect gravitational waves in space. (Source: ESA)

References

[1] Jafar Akhundov. Implementation of the global physical time for the domain model of the virtual path of the dlr hand-arm system. DLR-IB 572-2013/24 5, DLR Oberpfaffenhofen, 6 2013.

[2] Jafar Akhundov, Volker Schaus, Andreas Gerndt, and Matthias Werner. Using timed automata to check space mission feasibility in the early design phases. In *IEEE Aerospace 2016 Proceedings (in print)*, Big Sky, Montana, USA, 3 2016.

[3] Jafar Akhundov, Peter Tröger, and Matthias Werner. Considering concurrency in early spacecraft design studies. In *CS&P 2015 Proceedings*, pages 22–30, Rzeszow, Poland, 9 2015.

[4] Jafar Akhundov, Peter Tröger, and Matthias Werner. Considering superposition in the composable hybrid automata. In *Proceedings of the 25th International Workshop on Concurrency, Specification and Programming*, pages 125–140, Rostock, Germany, 9 2016.

Your Possible Contributions

If you are interested in contributing to our research and feel yourself up to the challenge, email us your CV and your current grades. We are always looking for good students to participate in our projects (these can be seminar research works, internship or a final thesis). Prerequisites for participation are (very) good grades, (at least) basic understanding of formal methods, modelling tools, formal specification and verification, as well as solid math and programming skills.