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

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 to each phase until the design system is complete. In order to design the most effective system components, the whole system needs to be designed at the same time, from the earliest stage. The goal of this research is to develop 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 time-consuming and iterative issues involved in the design process. Such a meta-model can be applied for generating a new or integrating into an existing operational timeline of a space mission from system description, code generation for a manned mission in later phases, generation of specifications and code for design synthesis (KDP) and mission reports.

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 of fault analysis, are not always considered to be of high priority. Such as, the first unmanned space shuttle probe cooled due to unexpected board computers, Pathfinder rover has experienced operational problems (possibly defined using different methods) under specific conditions. It is therefore reasonable to develop a necessary formalism and tools to support engineers in their efforts and automate verification of such properties as far as possible, or provide necessary feedback information at the earliest stage in the design so that design costs are minimised.

Main Objectives
The current research has two main objectives:
1. To find a refirable 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 for transitions between the phases.

As an example for analysable properties for a system at early design stage, real-time, such as meeting deadlines and proving mission feasibility. System description in this case has been limited to system components (e.g. payload experiment, battery charge, downlink, etc.).

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 stage. 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. They have been used to check for mission feasibility. System description in this case has been limited to system components. It has been demonstrated that both timed and hybrid automata can be used for the formal specification of spacecraft systems at the earliest design stage. In such a way, the purpose of composition and refinement is crucial for building complex systems from smaller components and has been addressed in the LTI-HA formalism.

The property of composition and refinement is crucial for building complex systems from smaller components and has been addressed in the LTI-HA formalism. 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 supersposition in the other 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 parameterisation of space missions, study of existing mission reports to derive a generalised refirable 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 (wLISA), etc.
7. Investigating the ways of representing timing and fault model in the LTI-HA formalism, analysing it;
8. Studying how does a formal non-functional requirement in form of a model(transform and evolve over time by comparing different mission reports);

Current and Planned Work
Current and upcoming work includes but is not limited to:
1. Defining the analysis procedures for the LTI-HA formalism, investigating their complexity and decidability, and implementing them;
2. Comparison of the LTI-HA formalism expressive power with the established HA modelling methods;
3. Defining the analysis procedures 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 parameterisation of space missions, study of existing mission reports to derive a generalised refirable 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 (wLISA), etc.
7. Investigating the ways of representing timing and fault model in the LTI-HA formalism, analysing it;
8. Studying how does a formal non-functional requirement in form of a model transform and evolve over time by comparing different mission reports;
9. Implementation of necessary software tools, their testing and integration.

References

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.