D. Gurov

/ DILIAN GUROV /

cost
EUROPEAN COOPERATION
IN SCIENCE & TECHNOLOGY

Report on the outcomes of a Short-Term Scientific Mission[1]

Action number: CA20111

Grantee name: Khaoula Boukir

Details of the STSM

Title: ***Designing a high-level software specification language for deductive verification***

Start and end date: 05/04/2025 to 12/04/2025

Description of the work carried out during the STSM

Description of the activities carried out during the STSM. Any deviations from the initial working plan shall also be described in this section.

(max. 500 words)

The objective of this STSM was to support a collaboration between the host, Pr. Dilian Gurov (KTH Royal Institute of Technology), and the grantee, Dr. Khaoula Boukir, focusing on the formalization of natural language requirements for software verification. The goal is to design a structured specification format for expressing natural-language requirements, provided by stakeholders, that can be compiled into a precise formal ACSL contracts required for deductive verification using Frama-C.

The STSM began with a meeting involving researchers from KTH and SCANIA to discuss some examples of requirements used in safety-critical software. The grantee presented a preliminary version of a structured requirement template that captures system-level properties through declared sections: target functions, relevant variables, conditional expressions, and state-modifying actions. Discussions were carried out to improve the expressiveness and practical applicability of the template.

During the rest of the week, daily meetings were held to refine the structure of the requirement language and study its formal semantics. Several discussions were about the development of a denotational semantics for the template language, modeled as a binary relation over pre- and post-program states. For this, they built on the host's earlier work on defining a denotational semantics for Hoare logic contracts, using it as a basis for formalizing the semantics of the requirement template.

[1] This report is submitted by the grantee to the Action MC for approval and for claiming payment of the awarded grant. The Grant Awarding Coordinator coordinates the evaluation of this report on behalf of the Action MC and instructs the GH for payment of the Grant.

Description of the STSM main achievements and planned follow-up activities

Description and assessment of whether the STSM achieved its planned goals and expected outcomes, including specific contribution to Action objective and deliverables, or publications resulting from the STSM. Agreed plans for future follow-up collaborations shall also be described in this section.

(max. 500 words)

Grantee enters max 500 word summary here.

The main achievement of the STSM was to design a final version of the requirement template syntax, and to elaborate a first version of its denotational semantics by defining how requirements describe a relation between pre- and post-states of a program. Planned follow-up activities include the definition of a translation function that maps each requirement template into an equivalent ACSL contract, as well as the formulation of a formal proof of correctness for this translation. The discussions also explored potential extensions of the template language to support temporal requirements, particularly through the integration of LTL-inspired constructs. As a continuation of the collaboration, the host and the grantee agreed to co-author a joint publication that presents the template language, its formal semantics, and the translation process.