Short-Term Scientific Mission Grant
- APPLICATION FORM[1] -

Action number: CA20111

Applicant 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 -> 12/04/2025

Applicant: Dr. Khaoula Boukir, Ibn Tofail University, Morocco

Host: Prof. Dilian Gurov, KTH Royal Institute of Technology, Sweden

Detail of the cost in EUROS:

- Transport (screenshots attached): 658.44 euros (**prices checked on November 22th, 2024**)

- Hotel/day (screenshots attached): 107,14 euros per day = 750 euros (**prices checked on November 22th, 2024**)

- Food/day (estimation based on daily allowance for Sweden) : 2 x 20 euros (7 days) = 280 euros

TOTAL: 1688,44 euros

Goals of the STSM

Software in safety-critical systems requires a high level of confidence due to the potentially severe consequences of malfunctions. Deductive verification emerges as an exhaustive method to ensure their reliability and correctness. However, it's application requires the existence of formal specifications against which the software can be verified. In practical industrial settings, the requirements (specifications) are typically formulated in natural language, which introduces ambiguity and makes formal analysis challenging and error-prone. The purpose of this STSM is to support a collaboration between the host (Dilian Gurov) and the applicant (Khaoula Boukir), with long term objective to design a high-level specification language that bridges the gap between the informal specification provided by stakeholders, and the precise, formal contracts required by proof assistants within verification frameworks. The intended language will facilitate the automatic translation of requirements, initially expressed in (restricted) natural language, into their formalized specification embedded at the C source code level in the form of ACSL [BFM+21] annotations. During this STSM, the host and the applicant plan to work on the following:

- Define the syntax and semantics of the high-level specification language.
- Outline a foundational approach for integrating the language into existing verification frameworks such as Frama-C [CCK+].

Working Plan

[1] This form is part of the application for a grant to visit a host organisation located in a different country than the country of affiliation. It is submitted to the COST Action MC via-e-COST. The Grant Awarding Coordinator coordinates the evaluation on behalf of the Action MC and informs the Grant Holder of the result of the evaluation for issuing the Grant Letter.

A first step, during the STSM, will be to discuss prior experience of the collaborators with formalizing and verifying high-level requirements:

- The applicant's experience in translating requirements of a real-time operating system's scheduler into CTL properties for OS-level verification [BBD20].
- The host's work [UAG+24] on formalisation and verification of natural-language requirements of an embedded software module in the form of ACSL [BFM+21], LTL and MITL [AFH96] specifications.

Then, the collaborators will work together to elaborate the types of requirements to be formalized and determine the required expressiveness of the specification language within the domain of embedded systems software. This also requires defining a syntax capable of effectively expressing natural language requirements in a manner that is accessible to both stakeholders and verifiers.

Another step will be to establish a formal semantics of the high-level language and the translation process into ACSL contracts. For this, the host's prior experience in defining a denotational semantics for Hoare logic contracts [GW18] can be a beneficial theoretical foundation for establishing an initial draft for the proof system of the translation.

During the STSM, a visit to SCANIA, a heavy vehicle manufacturer and a collaborative partner of the host, is also planned. This visit will allow the collaborators direct access to the automotive software code and the associated requirements documentation. It will also allow the identification of potential use cases where the high-level specification language and the verification process can be applied.

Expected outputs and contribution to the Action MoU objectives and deliverables.

By proposing a high-level specification language that compiles natural language requirements into formal contracts, this STSM falls within the domain of deliverable 6 in terms of extending and improving the automation of software contract generation. This, contributes directly to the following EuroProofNet's objectives :

- O3: Make techniques for program verification more effective and more accessible to all stakeholders.
- O8: Develop the use of natural or controlled languages in proof systems.

Additionally, this work aligns with the objectives of WG3 by making program verification techniques more accessible to stakeholders without deep expertise in formal methods. On the other hand, since the long-term goal of this collaboration is to integrate the language into existing verification frameworks, the STSM supports WG3's second aim to enhance synergies and interoperability among different proof systems.

The collaboration also focuses on exchanging expertise between academic researchers (the applicant and the host) and industrial partners from SCANIA, which directly supports to O6 in the capacity building objectives. Furthermore, by involving the applicant in this collaboration, The STSM addresses both O1 and O5 from the same objectives

Working groups to which this mission contributes: WG3

References

[AFH96] Rajeev Alur, Tom´as Feder, and Thomas A Henzinger. The benefits of relaxing punctuality. Journal of the ACM (JACM), 43(1):116–146, 1996.

[BBD20] Khaoula Boukir, Jean-Luc B´echennec, and Anne-Marie D´eplanche. Requirement specification and model-checking of a real-time scheduler implementation. In Proceedings of the 28th International Conference on Real-Time Networks and Systems, pages 89–99, 2020.

[BFM+21] Patrick Baudin, Jean-Christophe Filliˆatre, Claude March´e, Benjamin Monate, Yannick Moy, and Virgile Prevosto. Acsl: Ansi/iso c specification. URL https://frama-c.com/html/acsl.html , 2021.

[CCK+] Lo¨ıc Correnson, Pascal Cuoq, Florent Kirchner, Andr´e Maroneze, Virgile Prevosto, Armand Puccetti, Julien Signoles, and Boris Yakobowski. Frama-C User Manual. CEA LIST, Inria. http://frama-c.com/download/frama-c-user-manual.pdf

[GW18] Dilian Gurov and Jonas Westman. A Hoare logic contract theory: An exercise in denotational semantics. Principled Software Development: Essays Dedicated to Arnd Poetzsch-Heffter on the Occasion of his 60th Birthday, pages 119–127, 2018.

[UAG+24] Gustav Ung, Jesper Amilon, Dilian Gurov, Christian Lidstr¨om, Mattias Nyberg, and Karl Palmskog. Post-hoc formal verification of automotive software with informal requirements: an experience report. In 2024 IEEE 32nd International Requirements Engineering Conference (RE), pages 287–298. IEEE, 2024.