# Short-Term Scientific Mission Grant

# - APPLICATION FORM[1] -

**Action number: CA20111**

**Applicant name: Dorel Lucanu**

## Details of the STSM

Title: Translation of Generic Symbolic Execution Steps into Dedukti

Start and end date: 20/03/2023 to 01/04/2023

## Goals of the STSM

*(max.200 word)*

*The context is that of translating K prover executions into Dedukti proofs. There already exists significant progress in translating K semantic definitions into Dedukti performed by Amelie Ledein (Inria Saclay). The main goal of this STSM is to make further steps in translating K Prover symbolic execution steps into Dedukti proofs.*

## Working Plan

*(max.500 word)*

*Symbolic execution is intensively used in program analysis and verification. In order to be able to supply a proof object for a symbolic execution, we need a logical framework where*
*- the semantics of the programming language is given as a theory;*
*- the desired behaviour of the program is expressed as a formula;*
*- a symbolic execution step becomes an implication of formulas; and*
*- the proofs that the implications are semantic consequences of the semantic theory are given via a sound proof system.*

*A canonical example of such a framework is K, where the programming languages can be described as Matching Logic (ML) theories, the behaviour of programs as ML formulas, and the execution steps are applied by the K Prover (KP).*

*The basic ML formulas handled by KP are conjunctions between functional patterns (describing the current configuration) and predicate patterns (expressing the constraints the current configuration must satisfy).*

[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.

Funded by
the European Union

*For applying one step from semantics, KP uses external algorithms for unification between the current configuration pattern and the axiom patterns.*

*The work will focus on:*
*- a deep understanding of how the symbolic execution is handled by KP;*
*- how the KP symbolic execution steps can be translated in Dedukti proofs;*
*- how KP can benefit from the rich library system of Dedukti by borrowing proofs for the results given by the external algorithms it uses.*

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

Main expected results and their contribution to the progress towards the Action objectives (either research coordination and/or capacity building objectives) and deliverables.

*(max.500 words)*

The main expected result is a methodology of translating KP symbolic execution steps into Deduct proofs and it will contribute to the following MoU objectives:

Express new proof systems in the Dedukti logical framework.
Promote the output of detailed, checkable proofs from automated theorem provers.

The methodology will be exemplified on several case studies.