Contract-based Analysis Toolnet
Orchestrating a Formal Verification Design Flow in OSLC

Marco Carloni, Orlando Ferrante, Alberto Ferrari,
marco.carloni@ales.eu.com, orlando.ferrante@ales.eu.com, alberto.ferrari@ales.eu.com
Advanced Laboratory on Embedded Systems S.r.l. Via Barberini, 50, Rome, Italy

Introduction

- Open Service Lifecycle Collaboration (OSLC) is a specification for tool interoperability.
- FormalSpecs Verifier (FSV) is a tool for the formal verification of system properties based on model checking.
- Contract Theory:
  - the Block-based Contract Language (BCL) is an ALES proprietary language for requirement formalization as contracts.
  - a contract \( C = (A, G) \) is a specification of a component that defines the properties \( G \) that a component must be able to guarantee, and the context \( A \) or the assumptions under which the guarantee must be established.
- FSV OSLC Adapter is a tool that supports the following capabilities:
  - OSLC Consumer: SCM, RM.
  - OSLC Provider: AUTO, RM, QM.

Model-Based Analysis Tool Chain

FSV Analysis is a new Resource defined by the implemented OSLC Adapter that equips the FSV tool for the interaction in the OSLC world. Specifically, through the OSLC Automation domain the Adapter enables to use FSV by the creation of:
- an automation plan resource associated to the analysis
- request & result resources for each FSV command execution request

Running Formal Verification in OSLC network. By using the OSLC language the Adapter enables to execute all the available FSV commands such as Simulink model translation, contract extraction and contract verification.

Traceability in Contract Analysis

The FSV adapter represents a Contract as a standard Requirement resource of the OSLC RM domain. The analysis performed by FSV on a Contract is traced by setting its specified properties to build a consistent set of RDF triples:
- decomposed links to the related original Natural Language requirement
- implemented by links to the component input Simulink/BCL artefact resource representing the contract
- elaborated by links to the specific FSV analysis
- satisfied by links to the result of the analysis

Distributed Semantic Database

RDF Triples collecting analysis information

User Interface for Remote Analysis

Links to OSLC Defined Resources managed by OSLC Service Providers in the related OSLC Domains (AUTO, RM, QM)

Acknowledgements

The research leading to these results was partially funded by the EU ARTEMIS Joint Undertaking under grant agreement no. 269335 (project MBAT) and the Italian Ministry of Education, University and Research (MIUR).