ACTIVE: A Tool for Integrating Analysis Contracts

Submitted by ivan on Wed, 06/24/2015 - 12:36pm. Contributors:
Ivan RuchkinDionisio de NizSagar ChakiDavid Garlan

Abstract: Development of modern Cyber-Physical Systems (CPS) relies on a number of analysis tools to verify critical properties. The Architecture Analysis and Design Language (AADL) standard provides a common architectural model to which multiple CPS analyses can be applied. Unfortunately, interaction between these analyses can invalidate their results. In this paper we present *ACTIVE*, a tool developed within the OSATE/AADL infrastructure to solve this problem. We analyze the problems that occur when multiple analyses are applied to an AADL model and how these problems invalidate analysis results. Interactions between analyses, implemented as OSATE plugins, are formally described in *ACTIVE* in order to enable automatic verification. In particular, these interactions are captured in an analysis contract consisting of inputs, outputs, assumptions, and guarantees. The inputs and outputs help determine the correct order of execution of the plugins. Assumptions capture the conditions that must be valid in order to execute an analysis plugin, while guarantees are conditions that are expected to be valid afterwards. ACTIVE allows the use of any generic verification tool (e.g., a model checker) to validate these conditions. To coordinate these activities our tool uses two components: *ACTIVE EXECUTER* and *ACTIVE VERIFIER. ACTIVE EXECUTER* invokes the analysis plugins in the required order and uses ACTIVE VERIFIER to check assumptions and guarantees. *ACTIVE VERIFIER* identifies and executes the verification tool that needs to be invoked based on the target formula. Together, they ensure that plugins are always executed in the correct order and under the correct conditions, guaranteeing correct results.To the best of our knowledge, *ACTIVE* is the first extensible framework that integrates independently-developed analysis plugins ensuring provably-correct interactions.

Ivan Ruchkin │ Dionisio de Niz │ Sagar Chaki │ David Garlan

License: Creative Commons 2.5

Other available formats:

ACTIVE: A Tool for Integrating Analysis Contracts
Switch to normal viewerSwitch to experimental viewer

Aerospace Avionics Real-Time Systems Symposium - RTSS 2014 Conference paper Academia USA Research Organization Papers