Consolidation of COMPASS Tools

COMPASS is a toolset for the evaluation of system-level correctness, safety, dependability and performability of on-board computer-based aerospace systems, based on state-of-art formal verification techniques. COMPASS supports a comprehensive process for system-software co-engineering, by covering requirements validation, functional correctness, safety and dependability analysis, performability analysis, fault detection, identification and recovery, and contract-based design. The COMPASS toolset has been developed since 2008, with funding of the European Space Agency, by Fondazione Bruno Kessler (FBK), Trento and RWTH Aachen University, in several projects such as COMPASS, AUTOGEF, FAME, HASDEL, D-MILS and CATSY.

The COMPASS3 project (Consolidation of COMPASS tools) aimed at consolidating the work carried out in previous projects over the last eight years, by integrating, harmonizing, and updating selected features and functionality. The result is a new release of the toolset, called COMPASS 3.0.

COMPASS 3.0 supports a new version of the input language, called SLIM 3.0, a variant of AADL, with a consolidated syntax and semantics, and new features such as real-time constructs, security-related concepts, a new form of communication, new data types, and abstract component types. Newly added functionality include failure propagation analysis based on Timed Failure Propagation Graphs (TFPG), real-time specifications and real-time RAMS analyses, and Monte Carlo simulation. Moreover, COMPASS3 incorporates the new features developed in the CATSY project, namely the definition of a Catalogue of System and Software Properties (CSSP) derived from a taxonomy of requirements, contract-based design, property validation, and hierarchical fault tree generation. COMPASS 3.0 also features several technological advances implemented in the underlying verification engines. Finally, COMPASS 3.0 is accompanied by an improved documentation material, namely a user manual, a tutorial, and a newly design web portal.

COMPASS 3.0 is the basis for new developments and further work that will aim at improving the visibility, market penetration and usability of the toolset, and its suitability for industrial usage.

In this talk, we will summarize the main achievements of COMPASS 3.0, demonstrate the use of the toolset, and present the roadmap for future developments, which include the integration of COMPASS with other modeling languages and design environments, and the synergy with other ESA-related initiatives such as the TASTE development environment and OSRA (On-board Software Reference Architecture).