Applications of Goal-directed Answer Set Programming to Avionics Industry

Brendan Hall†, Sarat Chandra Varanasi‡, Jan Fiedor‡, Joaquin Arias§, Kinjal Basu†,
Fang Li†, Devesh Bhatt†, Kevin Driscoll†, Elmer Salazar‡, Gopal Gupta†

†Honeywell Advanced Technology, Plymouth, USA
‡Department of Computer Science, The University of Texas at Dallas, Richardson, TX, USA
§Honeywell International s.r.o, Brno, Czech Republic & Brno Univ. of Technology

We explore: calculus and query-driven answer set programming. Specifically, we explore:

1) How to systematically capture design and intent within the MIDAS framework.
2) How ASP-based model checking (over dense time) can validate specified system behaviors wrt system properties.
3) How application of abductive reasoning can extend ASP-based model checking to incorporate domain knowledge and real-world/environmental assumptions/concerns.
4) How knowledge-driven analysis can identify typical requirement specification errors, and/or requirement constructs which exhibit areas of potential/probable risk.

The talk will be organized as follows. We will give motivation for our work and discuss the importance of writing requirements that are consistent and complete. We will present how MIDAS enables a formal flow-down of functional intent through different stages of design refinement. We will summarize the two faces of requirements (outward and inward facing), as they support validation and verification objectives (respectively). We will then discuss the enabling background technologies (EC and ASP), before presenting how they can be integrated within the MIDAS platform to support our goals. We will illustrate our approach using an altitude alerting case study from an actual aerospace system and discuss adjacent real-world examples to show how one can use generalized knowledge within other system contexts. We will illustrate requirement defect discovery using s(CASP) for property-based model-checking as well as discuss how more general knowledge of potential requirements defects may detect defects that traditional techniques may not be able to find.

REFERENCES