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
[§]Universidad Rey Juan Carlos, Madrid, Spain

Developing effective requirements is crucial for success in building a system. The more complete, consistent, and feasible the requirements, the fewer problems system developers will encounter later. Current automation of requirements engineering tasks attempt to ensure completeness, consistency, and feasibility. However, such automated support remains limited. In this work, we present novel automated techniques for aiding the development of model-augmented requirements that are complete (to the extent possible), consistent, and feasible—where consistency and feasibility are validated. Thus, we can have more confidence in the requirements. We limit ourselves to requirements for cyber-physical systems, particularly those in avionics. We assume that requirements are generated within the MIDAS (Model-Assisted Decomposition and Specification) [4] environment, and are expressed in CLEAR (Constrained Language Enhanced Approach to Requirements) [3], a constraint natural requirement language.

Our main contribution in this work is to show how the *Event Calculus* [5] (EC) and *Answer Set Programming* (ASP) [2] can be used to formalize constrained natural language requirements for cyber-physical systems and perform knowledge-assisted reasoning over them. ASP is a logic-based knowledge representation language that has been prominently used in AI. Our work builds upon recent advances made within the s(CASP) system [1], a query-driven (or goal-directed) implementation of predicate ASP that supports constraint solving over reals, permitting the faithful representation of time as a continuous quantity. The s(CASP) system permits the modeling of event calculus elegantly and directly. A major advantage of using the event calculus—in contrast to automata and Kripke structure-based approaches—is that it can directly model cyber-physical systems, thereby avoiding "pollution" due to (often premature) design decisions that must be made in the other modeling formalisms. The event calculus is a formalism—a set of axioms—for modeling dynamic systems and was proposed by artificial intelligence researchers to solve the *frame problem* [5]. The primary goal of this work is to explore how constrained natural language requirements, specified within MIDAS [4] using the CLEAR notation, can be automatically reasoned about and analyzed using the event 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

[1] Joaqu´ın Arias et al. "Constraint answer set programming without grounding". In: *TPLP* 18(3-4):337-354 (2018).

[2] M. Gelfond and Y. Kahl. *Knowledge representation, reasoning, & design of intelligent agents: The answer-set programming approach*. Cambridge Univ. Press, 2014.

[3] B. Hall, D. Bhatt, et al. "A CLEAR Adoption of EARS". In: *IEEE EARS Workshop*. 2018, pp. 14–15.

[4] B. Hall, J. Fiedor, and Y Jeppu. "Model Integrated Decomposition and Assisted Specification (MIDAS)". In: *INCOSE Int'l Symp.* Vol. 30(1):821-841. Wiley.

[5] Murray Shanahan. "The event calculus explained". In: *Artificial intelligence today*. Springer, 1999, pp. 409–430.