An Aircraft Electric Power System Domain-Specific Language for Reactive Control Protocols

Submitted by brad_martin on Tue, 04/22/2014 - 12:53pm. Contributors: Huan Xu Necmiye Ozay Richard Murray

Abstract:
Domain-specific languages are languages adapted to a particular application or set of tasks. While general purpose languages (e.g., C or Java) may offer broader programming features, domain-specific languages (e.g., HTML or Verilog) provide more expressiveness and ease of use within a given domain [3]. Examples of languages used in the context of cyber-physical systems can be found in [1] and [2]. In aerospace, next-generation aircraft have moved away from purely mechanical and hydraulic subsystems, instead increasing reliance on electric power to supply subsystems, including flight-critical ones [4]. The growing complexity of electric power systems on aircraft, coupled with the need for safety, reliability, and autonomy, has increased the need to utilize formal methods and verification tools in order to properly analyze and design such large-scale systems. Previous work on embedded control software synthesis has been explored by Piterman and Pnueli [6]. Wongpiromsarn et al. [8] and Ozay et al. [5] have used the temporal logic planning toolbox TuLiP [9] to address the issue of creating correct-by-construction control protocols for aircraft management systems. Given a system topology, Xu et al. [10] show how text-based requirements can be converted to linear temporal logic (LTL), a formal specification language (see [7] for more details) to synthesize centralized and distributed controllers. While the use of formal specification languages and correct-by-construction synthesis methods is beneficial in the area of controller design, unfamiliarity of formal methods amongst engineers may provide a challenge to widespread implementation of formal methods. We propose a domain-specific language that combines tools already in existence: visual programs for single-line diagrams, which engineers are familiar with, and primitives, which provide a more formal structure to specifications. The development of a domain-specific language, therefore, provides an easy interface between industry engineers knowledgeable in aircraft systems and the methods/tools used by computer scientists and software engineers.

This talk describes the use of a domain-specific language, and an accompanying software tool, in constructing correct-by-construction control protocols for aircraft electric power systems. Given a base topology, the language consists of a set of common "primitives," which correspond to some set of standard specifications. The accompanying tool converts these primitives into formal specifications, which are used to synthesize control protocols. We then use TuLiP to synthesize centralized and distributed controllers. For systems with no time involved in the specifications, this tool also provides an option to output specifications into a SAT-solver compatible format, thus reducing the synthesis problem to a satisfiability problem. We provide the results of our synthesis procedure on a range of topologies.

References:

Bio:
Huan Xu is a Research Assistant Professor jointly appointed in the Institute for Systems Research and
the Department of Aerospace Engineering. She received her S.B. degree in mechanical engineering and
material science from Harvard University in 2007, M.S. and Ph.D. in mechanical engineering from the
California Institute of Technology in 2008 and 2013, respectively. Her doctoral work focused on the use
of formal methods and timed specification languages in the design and analysis of large-scale, complex,
distributed control systems.

Other available formats:

An Aircraft Electric Power System Domain-Specific Language for Reactive Control Protocols

License: Creative Commons 2.5