Insertion of Formalism Into Systems Level Design

Perry Alexander
ECECS Department
PO Box 210030
The University of Cincinnati
Cincinnati, OH 45221-0030
perry.alexander@uc.edu

Society's increasing dependence on complex technology mandates high assurance of system correctness. Traditional engineering disciplines such as civil or mechanical engineering achieve such assurance through application of mathematics to system modeling. The formal nature of mathematics allows practitioners in traditional engineering domains to predict the behavior of systems prior to implementation. Furthermore, the common feature of engineering disciplines is the application of pragmatic, formal, mathematical models during systems design and analysis.

Unfortunately, systems and software engineering disciplines do not enjoy pervasive use of mathematics in design activities. Most efforts in design improvement involve only the design process. Although sometimes effective, such improvements are limited without support for systems level mathematical modeling. Formal methods is simply the application of sound mathematical modeling and analysis techniques. Formal methods in engineering of computer-based systems is the application of mathematics to modeling systems and should be a central goal of systems engineering research.

Three general impediments must be overcome for formal methods in systems design to become pervasive: (i) establishment of common modeling paradigms; (ii) development of engineer friendly tools; and (iii) educating new engineers as well as continuing education for current practitioners.

Most engineering disciplines have pervasive domain specific mathematical models and techniques. These techniques are common throughout the discipline and form a means of communications between engineers. Such models are highly pragmatic and of high utility. They represent specialization of general techniques within the specific domain. Computer-based systems engineering must define such models and make them widely accessible.

Most formal methods tools are accessible only to formal methods researchers and are rarely specialized to a particular domain. Tools must be defined and constructed that allow engineers to apply techniques in their domain of interest. Furthermore, these tools must use abstractions that are appropriate for the discipline.

Efforts to introduce formal methods into the systems design process will ultimately fail without appropriate educational support. Students must learn necessary mathematics and study its application to problems in their discipline. The use of formal methods must be more pervasive in the undergraduate and graduate education process. Furthermore, continuing education materials must be made for practicing engineers. Current formal methods materials are difficult to approach and require extensive background information.