Integrated Reliability and Performance Evaluation using Information Flow Models

Ramesh Rao, Barry W. Johnson, Ronald D. Williams, James H. Aylor
Department of Electrical Engineering, University of Virginia
Charlottesville, VA 22903

Abstract

Information flow models provide a natural and convenient representation of the structure, function, and data/control flow of digital electronic systems at a high level of abstraction and interpretation. Design engineers prefer to use such models for performance trade-offs and analysis. Adding the capability to model and analyze the dependability characteristics of a system within such a paradigm allows design engineers, as opposed to reliability engineers, to perform dependability analysis and trade-offs at the early stages of the design process. A design environment supporting such a philosophy would bring dependability analysis and trade-offs into the mainstream of the design process.

The Advanced Design Environment Prototype Tool (ADEPT) is based on such a philosophy. This paper presents an overview of ADEPT with a focus on the dependability modeling paradigm. The various solution paths for the evaluation of dependability metrics are presented. The paper will demonstrate the capabilities of ADEPT by modeling the controller for a jet engine magnetic bearing.

1. Introduction

From the point of view of dependable system design, existing methodologies do not support the full range of system-level design and evaluation capabilities that are essential for the achievement of fault tolerance in critical applications. One of the major drawbacks of existing design methodologies is the need to switch between different environments and models during the different phases of a design and while performing different types of analyses.

The need to deal with several models of the same system during the design process results in three major problems: 1) any change in the design has to be correctly reflected across all the models of the system, 2) there is no way of ensuring that all the different models correspond to the same system, and 3) users must be familiar with several modeling languages and tools. Further, analysis of design alternatives is difficult and is likely to be limited by time constraints.

ADEPT overcomes the above mentioned drawbacks by emphasizing stepwise refinement in a top-down fashion, using a common simulation environment based on VHDL. There are three important and novel aspects of the ADEPT unified design methodology: 1) Bridge the gap between system-level (performance) models and functional models by using hybrid modeling and up-annotation to provide full model continuity; 2) Support hardware/software co-design by providing the ability to specify a systems abstract behavior independent of the hardware or software implementation used and the subsequent refinement into a realization consisting of actual hardware and software components; 3) Incorporate dependability modeling and analysis as a part of the design process by using the same paradigm for the analysis of performance and dependability. The features mentioned above are not isolated from each other but co-exist and interact with each other. Since performance, dependability, and hardware/software features of a system are encapsulated by a single model, ADEPT allows the designer to meet stringent requirements such as reliability and to consider reliability and performance concurrent with the development of function.

ADEPT uses the VHSIC Hardware Description Language (VHDL)[6] for verification through simulation and colored Petri Nets [1] for analytical approaches to analysis. A library of predefined elements (called ADEPT modules) [2,4,3,15] has been developed from which systems can be constructed. Performance and reliability models can be developed by interconnecting a collection of the ADEPT modules. Using ADEPT, the designer can

---

The authors would like to acknowledge the support provided by the Advanced Research Projects Agency under contract number F33615-93-C-1313, the Semiconductor Research Corporation under contract number 93-DJ-152, the International Business Machines Corporation under contract number WM-226181, NASA-

avoid interaction with any VHDL code or the underlying Petri Net description.

The remaining portions of this paper are organized as follows. Section 2 provides a brief overview of the ADEPT and Section 3 discusses dependability modeling and analysis using ADEPT. Section 4 presents the example and some results. Finally, a summary is provided in Section 5.

2. ADEPT overview

This section provides an overview of the ADEPT environment. A more detailed overview may be found in [4,23]. ADEPT is available on a SPARC™ platform and uses Mentor Graphics' Design Architect (DA) [5] as the front end schematic capture system. DA is used to graphically construct the system model from a library of ADEPT module symbols. ADEPT automatically produces 1076 VHDL code. Facilities and programs to collect and analyze the simulation results are provided as part of the ADEPT system.

ADEPT provides front end independence by utilizing EDIF as an intermediate hierarchical design format. Thus, any schematic capture system that can generate EDIF can be used as a front end to ADEPT. Also, the capability of generating hierarchical VHDL code is provided. ADEPT supports model reduction using Petri Net reduction algorithms developed specifically for system models constructed from modules. The CPN reduction is used to reduce the model size in the hope of reducing simulation time. These features are depicted in Figure 1. The CPN representation can also be used to perform analytical reliability analysis. This path allows the CPN description of the system model to be abstracted, reduced and mapped to reliability models such as Markov models and fault trees. The analytical techniques are presented in more detail in the section on dependability analysis using ADEPT.

One of the key features of ADEPT is that the user interacts with a single model of the system, the ADEPT model. All simulation and analytical based studies of the system are performed on models that are automatically derived from the ADEPT model using provably correct transformations/mappings. This ensures that any change in the system design is correctly reflected in all models used in the analysis of the system. ADEPT has been designed to support several aspects of system design including integrated performance/dependability modeling [9,10,15,17], model reduction [12,13], hybrid modeling [19], hardware/software codesign [22], and the integration of operational specifications with performance models [20].

In the ADEPT environment, a system model is constructed by interconnecting a collection of *ADEPT modules*. The modules model the information flow, both data and control, through a system. The modules communicate by exchanging *tokens*, which represent the presence of information, using a uniform, well defined handshaking protocol. Higher level modules can be constructed from the basic set of ADEPT modules. In addition, custom modules can be incorporated into a system model as long as the handshaking protocol is adhered to.

The entire set of ADEPT modules is divided into six categories: control modules, color modules, delay modules, fault modules, miscellaneous parts modules, and hybrid modules. The modules are based on the Petri net structures defined by Dennis [3]. The control modules are used to model the data flow within the system. The color and delay modules enable the manipulation of the token color and model temporal aspects of a system, respectively. The fault modules are used to model the failure process within the system. The miscellaneous parts category contains modules that are used for data collection with the ADEPT system. The last category contains modules which aid in the construction of hybrid models. A detailed description of the entire ADEPT module set can be found in [4].