Cover ERCIM News 52

This issue in pdf
(64 pages; 7,6 Mb)

Free subscription

Archive:

cover ERCIM News No. 51

previous issue (Number 51 October 2002): Special theme: Semantic Web

all previous issues

Next issue:
April 2003

Next Special theme:
Cognitive Systems

Model Checking of Embedded Sys

by Stefania Gnesi

The integration of different dependability techniques is an open resea We address problems that arise when attempting to combine fault tol mechanisms with formal methods and formal verification tools in the an embedded system.

In recent years, the wide spread deployment of embedded systems on whi activities depend has raised many concerns about safety issues. A combin prevention, fault tolerance, fault removal and fault forecasting techniques used in order to achieve a high degree of dependability. However, there is agreement on a standard method to combine and integrate individual techi example, industries with different backgrounds and application fields tenc own particular development trajectories when applying techniques aimed dependability.

The application of formal methods in the rigorous definition and analysis functionality and the behaviour of a system means that the system is desig to a set of predefined abstract properties that guarantee its 'correct' behavi astonishing to see how seldom formal methods are actually used by the sa system industry, despite the fact that their adoption is increasingly require international standards and guidelines for the development of such system that industrial acceptance of formal methods is strictly related to the inves introduce them, to the maturity of the tool support available, and to the ea these reasons, the current industrial trend is to adopt formal verification te validate system design and integration within the existing development pr prefer to use formal verification techniques assessing the quality attributes products, obtained by a traditional life cycle, rather than adopting a fully f development, simply because it is cheaper to do so.

Several approaches to the application of formal methods in the developme been proposed; they mainly differ with respect to the degree of involveme method. Starting from rigorous specifications, formal methods can be use derivation of test cases, as a validation technique aimed at proving that th satisfies the requirements, or just as an auxiliary technique in the automat code.

Formal verification methods based on model checking are applied on a fir representation of system behaviour. Verification is usually carried out by checking algorithms to demonstrate the satisfiability of certain properties logical formulae over the model of the system. For example, safety and li requirements can be expressed as temporal logic formulae and can be che

About ERCIM News

model of the system. Unfortunately, this approach suffers from the so-call Explosion' problem that can arise when a system is composed of several s this case, a finite state model with a number of states, which is exponentia of the component subsystems, can be generated. Systems that are highly d data values share the same problem, producing a number of states expone number of data variables. Hence, traditional model checking techniques h insufficiently powerful for many 'real' systems, when their models are larg states.

Recent advances in model checking techniques, however, have managed t large state spaces by using symbolic manipulation algorithms inside mode tools have been successfully applied to very large state spaces in the realn verification.

Embedded computer-controlled systems often include fault tolerance tech tolerance is the property of a system to provide, through redundancy, a se complies with the specification despite the occurrence of faults. The rigor and verification of this class of systems is extremely important since it ma to demonstrate that a system is correct even in the presence of faults and f

Figure

Embedded computer-controlled systems often include fault tolerance techniques. These are, for example, applied to a Railway Interlocking System.

We have applied model checking verification techniques to embedded sys how certain characteristics of embedded systems, such as the use of redun to reduce the state space explosion problem. In this work, we have consid studies. Two interesting examples were the verification of the safety requi Railway Interlocking System developed by Ansaldo Trasporti and the ver fault tolerant mechanisms defined inside the EU project GUARDS (Gene Architecture for real-time Dependable Systems).

Both studies have shown that:

- the application of model checking formal verification methodology well accepted in the industrial context of embedded fault tolerant sy
- the formalization process strictly depends on the application domai rules for the passage from the semi-formal description of the syste specification can be successfully applied to the field of embedded fa systems. This passage is generally recognized as one of the critical introduction of formal methods in the software development cycle
- the reduction in the state space due to the phased structure of redun

makes the model checking approach viable in this application doma
- the use of finite state machines as the specification language has the ensuring the adherence of the formal specification to the original se

Link:
http://matrix.iei.pi.cnr.it/FMT/

Please contact:
Stefania Gnesi, ISTI-CNR
ERCIM Formal Methods for Industrial Critical Systems (FMICS) Workin
Tel: +39 050 3152918
E-mail: gnesi@iei.pi.cnr.it

Survey:

Please click the button if you find this article interesting Yes!
See the results without recommending this article.