

 [ERCIM News online](#) header image[subscribe](#) | [search](#) | [back issues on-line](#) | [order back issues](#)[ERCIM website](#)[< Contents](#) ERCIM News No. 52, January 2003

Special Theme: En

 Cover ERCIM News 52

# Model Checking of Embedded Systems

by Stefania Gnesi

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

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

In recent years, the wide spread deployment of embedded systems on which many activities depend has raised many concerns about safety issues. A combination of fault prevention, fault tolerance, fault removal and fault forecasting techniques is used in order to achieve a high degree of dependability. However, there is no agreement on a standard method to combine and integrate individual techniques. For example, industries with different backgrounds and application fields tend to follow their own particular development trajectories when applying techniques aimed at increasing dependability.

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

Several approaches to the application of formal methods in the development of embedded systems have been proposed; they mainly differ with respect to the degree of involvement of the developer. Starting from rigorous specifications, formal methods can be used for the derivation of test cases, as a validation technique aimed at proving that the system satisfies the requirements, or just as an auxiliary technique in the automatic generation of code.

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

## About ERCIM News

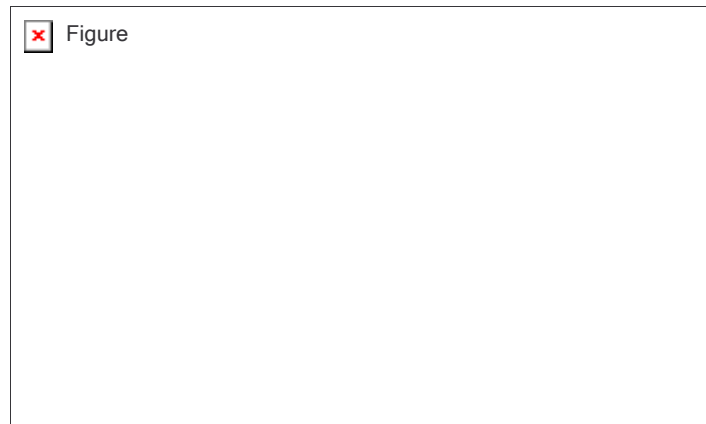
---



model of the system. Unfortunately, this approach suffers from the so-called 'Explosion' problem that can arise when a system is composed of several subsystems. In this case, a finite state model with a number of states, which is exponential in the number of component subsystems, can be generated. Systems that are highly distributed and share the same problem, producing a number of states exponential in the number of data variables. Hence, traditional model checking techniques have been insufficiently powerful for many 'real' systems, when their models are large.

Recent advances in model checking techniques, however, have managed to handle large state spaces by using symbolic manipulation algorithms inside model checkers. These tools have been successfully applied to very large state spaces in the realm of hardware verification.

Embedded computer-controlled systems often include fault tolerance techniques. Fault tolerance is the property of a system to provide, through redundancy, a service that complies with the specification despite the occurrence of faults. The rigorous analysis and verification of this class of systems is extremely important since it may be required to demonstrate that a system is correct even in the presence of faults and failures.



*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 systems. We have shown how certain characteristics of embedded systems, such as the use of redundancy, can be used to reduce the state space explosion problem. In this work, we have considered two interesting examples: the verification of the safety requirements of a Railway Interlocking System developed by Ansaldo Trasporti and the verification of fault tolerant mechanisms defined inside the EU project GUARDS (General Architecture for real-time Dependable Systems).

Both studies have shown that:

- the application of model checking formal verification methodology is well accepted in the industrial context of embedded fault tolerant systems
- the formalization process strictly depends on the application domain: the rules for the passage from the semi-formal description of the system specification to the field of embedded fault tolerant systems. This passage is generally recognized as one of the critical steps in the introduction of formal methods in the software development cycle
- the reduction in the state space due to the phased structure of redundancy

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

Link:

<http://matrix.iei.pi.cnr.it/FMT/>

Please contact:

Stefania Gnesi, ISTI-CNR

ERCIM Formal Methods for Industrial Critical Systems (FMICS) Working Group

Tel: +39 050 3152918

E-mail: [gnesi@iei.pi.cnr.it](mailto:gnesi@iei.pi.cnr.it)

**Survey:**

Please click the button if you find this article interesting

[See the results without recommending this article.](#)

□