Published in IET Software
Received on 21st June 2013
Revised on 15th January 2014
Accepted on 27th January 2014
doi: 10.1049/iet-sen.2013.0236

ISSN 1751-8806

Runtime verification monitoring for automotive embedded systems using the ISO 26262 Functional Safety Standard as a guide for the definition of the monitored properties

Donal Heffernan, Ciaran MacNamee, Padraig Fogarty

Department of Electronic and Computer Engineering, University of Limerick, Ireland
E-mail: donal.heffernan@ul.ie

Abstract: The ISO 26262 Road vehicles Functional Safety Standard is intended to guide the derivation of appropriate requirements and processes for avoiding systematic and/or random failures in automotive electrical/electronic equipment. Functional safety statements can be captured in the requirements specifications for automotive embedded control units and systems. However, the process of verifying the behaviour of resulting products continues to be incomplete; because embedded programme verification is unsolvable in general. This study shows that it is possible to monitor some proof obligations in the testing phase, or even in the actual operating phase of a system by the use of an on-chip, real-time runtime verification monitor. In this work, the ISO 26262 standard for functional safety is used to guide the definition of the functional safety requirements for a product, and the specific requirements are mapped to logic formulae, such that the actual runtime behaviour of the system for selected properties can be formally verified throughout the lifetime of a product. A case study example for an automotive gearbox control system is presented to demonstrate the feasibility of the scheme. The monitor is constructed as a permanent feature within an integrated circuit that can continuously observe the system's runtime behaviour.

1 Introduction

Complex embedded processing systems in safety-critical applications require assurances of good functional lifetime operation without significant cost overhead. However, embedded program verification is unsolvable in general, as theorem prover solutions do not in practice scale to large embedded software systems [1]. A more realisable approach is to formally observe some selected proof obligations during the actual operating phase of a system. This approach is not a substitute for full program and system verification but does provide a solution for confirming correct behaviour for some key aspects of a system during runtime. The concept of formally monitoring specific properties during a program's execution is referred to as runtime verification [2]; where a monitor is designed to detect or to react to property violations so as to provide a level of fault protection. In this paper, the ISO 26262 standard for functional safety in road vehicles is used to guide the definition of the functional safety requirements; these specific requirements are mapped to logic formulae, and a runtime monitor is developed to evaluate adherence to the properties during runtime. ISO 26262 is particularly relevant to this process because of the exacting standards it imposes and because of its emphasis on test and verification throughout the product lifecycle, even as far as deployment in the field.

This paper focuses on development of the actual non-invasive monitor solution, without the need for any additional instrumentation. Knowledge of such violations can be used by the designers to modify the system so as to understand and eliminate those violations. However, it is envisaged that such a monitor could further be used during the operating phase of a vehicle's life, but systems would then need to react to violations in real time and take appropriate remedial actions, as the sole act of detection cannot lead to safety.

The paper is organised as follows: Section 2 describes the ISO 26262 standard in the context of this paper, Section 3 summarises some previous research work in the area, Section 4 describes the monitoring concept, Section 5 describes a case study example, and Section 6 summarises the conclusions.

2 ISO 26262 overview and relevance

Over the past two decades, significant developments in the automotive industry include the proliferation of electrical and electronic (E/E) (including software) systems in cars