Fault-Tolerance Analysis of Mixed CAN/Switched Ethernet Architecture

Cláudia Betous-Almeida, Jean-Luc Scharbarg,
Christian Fraboul

IRIT-ENSEEIHT-University of Toulouse
2, Rue Charles Camichel
31000 Toulouse, France
claudia.betous,jean-luc.scharbarg, christian.fraboul@enseeiht.fr

Abstract. CAN is a well known fieldbus standard used in safety critical applications of embedded systems. However, steadily increasing amount of exchanged information in such systems has led to the use of Switched Ethernet like solutions. Mixed CAN/Switched Ethernet architectures allow to bypass CAN limitations while preserving the widely used CAN technology. In order to use this kind of architecture in safety critical applications a complete fault tolerance analysis is mandatory. In this paper, we use a simulation-based fault-injection technique to analyse the impact of different types of errors on the percentage of application frames missing their deadlines. Results show that different types of errors don't have the same impact on different types of traffic. Moreover, it is shown that the re-emission of corrupted frames can have a negative impact on the system's global performance.

1 Introduction

The Controller Area Network (ISO-CAN, 1993) is a well-known fieldbus standard that provides a real-time performance with a fair reliability degree, at a very low cost. The growing use of CAN in safety-critical real-time applications of embedded systems, such as automotive or avionic ones, has led to concerns regarding the reliability evaluation of these systems. Moreover, the amount of exchanged information in such systems has steadily increased over the years and is now reaching the traditional fieldbusses' limits, namely bandwidth limits.

So as to overcome those limits, Switched Ethernet like solutions are more and more envisioned, for example in avionics systems with the AFDX (ARI, 2002), (Charara et al., 2006). We have proposed a mixed CAN/Switched Ethernet architecture as an alternative between pure CAN and pure Switched Ethernet architectures (Scharbarg et al., 2005b).

In order to successfully use this architecture in safety-critical applications, a complete fault-tolerance analysis is needed. Fault-injection is the technique the most often used by system's designers in order to analyse the dynamic behaviour of the system, in the presence of faults.

This paper is an elaboration of the work presented in Betous-Almeida et al. (2006). In this paper we present an overview of the different types of models and consequently different fault-