A MODEL BASED ON A STOCHASTIC PETRI NET APPROACH FOR DEPENDABILITY EVALUATION OF CONTROLLER AREA NETWORKS

Paulo Portugal, Adriano Carvalho, Francisco Vasques

University of Porto, FEUP, Rua Dr. Roberto Frias s/n, 4200-465 Porto, Portugal
Tel.: +351.22.5081815, Fax: +351.22.5081443, E-mail: {pportugal,asc,vasques}@fe.up.pt

Abstract: The paper proposes a dependability model to evaluate the behavior of a CAN network in scenarios of transient faults which affect data communications. Fault occurrence is modeled by a Markov Modulated Poisson Process (MMPP) which is capable to describe the typical behavior of electromagnetic interferences (EMI) that occur in industrial environments. An accurate and efficient representation of the network behavior is achieved by adopting a set of assumptions that reduce the pessimism level and which are closer to the real operating conditions. The model is based on Stochastic Petri Nets, which are a high-level modeling formalism able to produce very compact and efficient models, supporting both analytical and simulation solutions. Dependability measures are established from the fulfillment of the real-time constraints (deadlines) defined on messages exchanged between network nodes. Analytical and simulation solutions are both investigated. A case study is proposed to asses both model performance and network dependability. Copyright © 2005 IFAC.

Keywords: Petri-nets; Reliability; Real-time communication; Safety; Stochastic modelling.

1. INTRODUCTION

Dependability attributes, like safety, reliability and availability, have become essential parameters on industrial automation systems design. Nowadays fieldbuses have a central role in these systems, with large application domains which extend to almost any area in manufacturing and process industries. They are presently the backbone of distributed industrial control architectures, providing a communication infrastructure which supports control, monitoring and supervision applications (Thomesse, 2005).

Industrial environments are characterized by the existence of a high diversity of equipments which are source of large patterns of electromagnetic interferences (EMI). These interferences induce faults in electronics circuits that disturb their normal operation. In communication systems these types of faults usually affect the transmission medium and related circuits, since, in most situations, these are the system components most exposed to them. EMI faults are generally characterized by occurring in bursts, a long latent period followed by relatively short period of presence, and by having a short duration (transient faults) (Kim *et al*., 2000).

In this context faults produce errors on transmitted messages by corrupting their contents. To recover from these situations fieldbus networks implement several fault-tolerant mechanisms. However, this creates a communication overhead by introducing delivery delays in messages which could imply performance degradation in the control system. When messages have real-time requirements, which is common in control systems, these problems can seriously disturb the system operation and can even lead to its failure (Shin and Kim, 1992; Kim and Shin, 1994).

The importance assumed presently by these control systems compels to evaluate their dependability (Navet*, et al.*, 2005). In a distributed system, determining the dependability of the communication channel is of particular importance, especially when this component is susceptible to EMI problems. Therefore in these systems it is vital to evaluate how the system dependability is affected by faults on communication (Broster, *et al.*, 2002).

This paper deals with a specific fieldbus: CAN (Controller Area Network) (Bosh, 1991). It proposes a model that enables to evaluate the network dependability with respect to deadline failures in the presence of transient faults induced by external sources (EMI). Shortly, the effect of faults on the real-time properties of the network is investigated.

In contrast to most of the previous works (Tindell, *et al.*, 1995; Punnekkat, *et al.*, 2000; Hansson *et al.*, 2002) a stochastic model is used to describe the fault occurrence and its duration, which guarantees a better representation of the phenomena involved. Although some recent works have already included this aspect (Navet, *et al.*, 2000; Broster, *et al.*, 2002; Broster, *et al*,. 2004), this paper provides a more realistic fault model, a representation of the network behavior much closer to the real operation conditions and the use of less pessimistic assumptions. The combination of all these aspects will provide more accurate dependability results.

2. ANALYSIS OF THE PREVIOUS WORK

The growing diffusion of CAN in safety- or mission-critical applications (Navet*, et al.*, 2005) asks for suitable techniques to assess the dependability of CAN networks. In the last decade, these aspects have motivated the aca-

demic community to study these problems and to propose answers to them. The following subsections present the most important works concerning the CAN behavior in fault scenarios.

2.1 General Behavior in Fault Scenarios

An analysis of the efficiency of the error detection mechanisms was performed by (Charzinski, 1994). By assuming a two-state channel model for the physical transmission medium, a set of expressions are derived which permits to quantify the probability for errors to be undetectable at receivers (residual error probability). Although (Bosh, 1991) defines this value as 4.7×10^{-11}, due to the combination of several aspects: error bursts, bit-stuffing, frame structure, spatial node distribution and efficiency of error detection mechanisms, it is shown that in scenarios with a high *Bit Error Rate* (BER) this value is overestimated (takes lower values).

The previous work is extended by (Tran, 1999), where the effects of multi-bit errors on those mechanisms are studied. By adopting a simulation model many of the restrictions imposed in (Charzinski, 1994) are removed, which permits to cover a larger number of fault scenarios. The results obtained confirm that the value presented in (Bosh, 1991) is in fact overestimated, as well as some scenarios evaluated in (Charzinski, 1994). As an example, a double-bit error (that should be detectable by the CRC mechanism) could result in a 1.3×10^{-7} residual error probability.

In a different context (Barrenscheen, *et al.*, 1997) performs a study about behavior of the CAN physical layer in environments with electromagnetic interferences. This work focuses in the electrical aspects of the physical layer (terminating resistors, stubs, cables, signal levels, etc.) and permits to establish the best conditions, from an EMI viewpoint, for data communications.

In a near context (Rufino, *et al.*, 1999) identifies the main causes that lead to a medium failure (permanent and transient faults, e.g. one-wire interruption or short-circuits), and proposes a fault-tolerant communication architecture to cope with these problems. This solution is based in the assumption of several failure mode scenarios and it uses redundancy (dual) both at medium and transceiver level.

The execution of the CAN error recovery mechanisms results in an inaccessibility period where the network isn't able to provide its service. The consequences of this behavior are studied by (Rufino and Verissímo, 1995). Several error scenarios are defined and for each one an expression for the inaccessibility time is derived.

The problem of message inconsistencies or omissions in CAN networks is addressed by (Rufino, *et al.*, 1998), where the occurrence of these scenarios is quantified by a simple probability model based on the BER. To cope with this problem, it is proposed a communication stack, on top of CAN, which supports a set of fault-tolerant broadcast protocols (atomic, reliable, etc.) which provides different degrees of group communication services.

On the sequence of the previous work (Ferreira, *et al.*, 2004) proposes a fault-injection experiment to evaluate the BER in different scenarios: aggressive and normal environments. The results confirm that in practice the effective BER is very small: normal (10^{-11}), aggressive (10^{-7}).

The behavior of the CAN fault-confinement mechanisms (TEC and REC counters) in fault scenarios is addressed by (Guajal and Navet, 2001). By using mean value rates both for message traffic and fault occurrence, the temporal evolution of these counters is modeled by a Markov chain. Two scenarios are analyzed: Bus-Off hitting time (TEC Markov chain: time until Bus-Off state) and Error-Passive hitting time (REC Markov chain: time spent in Error-Passive state). This study shows that these values strongly depend from the BER. For low / medium BER, Bus-Off hitting times are very high and Error-Passive hitting times are very small. Meanwhile, if the BER takes high rates the previous values can suffer a dramatic reduction or increasing respectively. Some improvements to these mechanisms are also presented.

2.2 Message Scheduling in Fault Scenarios

A simple schedulability analysis of CAN in the presence of faults is provided by (Tindell, *et al.*, 1995). Faults are incorporated into the traditional analysis by introducing an additional term, called *error recovery overhead function*, which is the upper bound of the overhead due to error recovery that could occur in a time interval. The fault model is very simple and based on a minimum inter-arrival time between faults. The main drawback of the analysis is the use of a deterministic model to describe fault occurrence. A model with these characteristics is not suitable for two reasons: **(i)** In a realistic scenario faults have a random nature (Kim, *et al.*, 2000); **(ii)** It assumes that the number of faults that can occur in a time interval is bounded, which is in contradiction with the previous statement.

The previous work is extended by (Pinho, *et al.*, 2000) by introducing the inaccessibility periods obtained in (Rufino and Verissímo, 1995). The fault model is slightly changed by introducing new terms (e.g. an erratic transmitter), but maintains its determinist nature.

Another extension to (Tindell, *et al.*, 1995) is presented by (Punnekkat, *et al.*, 2000), by providing a more general fault model which can deal with interferences (faults) caused by several sources. This model assumes that every source of interference has a typical pattern, consisting of an initial group of bursts with a fixed period and a distribution of single interferences, with a know minimum inter-arrival time. Since it uses a deterministic fault model, it suffers from the same problems as discussed previously.

Unlike the previous works, (Navet, *et al.,* 2000) proposes a stochastic fault model which is closer to the typical EMI behavior. This model considers both the frequency of the faults, modeled as a homogeneous Poisson Process, and its gravity (burst or single errors) modeled by a distribution function. This work doesn't try to determine whether a systems is schedulable (as the previous works), but it calculates the probability (WCDFP – *Worst Case Deadline Failure Probability*) that a message doesn't meet its deadline. Although this work is an important improvement face the previous ones, it includes two inaccuracies that increase the pessimism in the estimation of the WCDFP. First, the WCDFP definition doesn't reflect properly the conditions in which a message can miss its deadline (see (Broster, *et al.*, 2002) for details). Second, a burst of *n* errors is treated as a sequence of *n* single errors, each causing a maximum error overhead. This causes pessimism of several orders of magnitude.

An extension to (Punnekkat, *et al.*, 2000) is presented by (Hansson, *et al.*, 2002), by using a fault model which reduces the pessimism of the analysis (a lower error overhead during bus idle time). To guarantee this aspect, faults are modeled as fixed patterns of interferences (with different phases) which simplifies the model. The analysis is carried out only during the least common multiple (LCM) of the messages periods, being the remaining behavior extrapolated from that. Simulation is used to ob-