Mechatronics 24 (2014) 1189–1202

Contents lists available at ScienceDirect

Mechatronics

journal homepage: www.elsevier.com/locate/mechatronics

Probabilistic error propagation model for mechatronic systems

Andrey Morozov *, Klaus Janschek

Institute of Automation, Technische Universität Dresden, 01062 Dresden, Germany

ARTICLE INFO

Article history:
Received 5 November 2013
Accepted 15 September 2014
Available online 7 October 2014

Keywords:
Control flow graph
Data flow graph
Error propagation analysis
Discrete time Markov chain
Dependability
UML

ABSTRACT

This paper addresses a probabilistic approach to error propagation analysis of a mechatronic system. These types of systems require highly abstractive models for the proper mapping of the mutual interaction of heterogeneous system components such as software, hardware, and physical parts. A literature overview reveals a number of appropriate error propagation models that are based on Markovian representation of control flow. However, these models imply that data errors always propagate through the control flow. This assumption limits their application to systems, in which components can be triggered in arbitrary order with non-sequential data flow. A motivational example, discussed in this paper, shows that control and data flows must be considered separately for an accurate description of an error propagation process.

For this reason, we introduce a new concept of error propagation analysis. The central idea is a synchronous examination of two directed graphs: a control flow graph and a data flow graph. The structures of these graphs can be derived systematically during system development. The knowledge about an operational profile and properties of individual system components allow the definition of additional parameters of the error propagation model. A discrete time Markov chain is applied for the modeling of faults activation, errors propagation, and errors detection during operation of the system. A state graph of this Markov chain can be generated automatically using the discussed dual-graph representation. A specific approach to computation of this Markov chain makes it possible to obtain the probabilities of erroneous and error-free system execution scenarios.

This information plays a valuable role in development of dependable systems. For instance, it can help to define an effective testing strategy, to perform accurate reliability estimation, and to speed up error detection and fault localization processes. This paper contains a comprehensive description of a mathematical framework of the new dual-graph error propagation model and a Markov-based method for error propagation analysis.

1. Introduction

The research results presented in this article belong to a rather young scientific domain – *system dependability*. By this reason, in various papers devoted to error propagation analysis, different terms can describe similar entities. In this article, the term "error" is used in a general context that fits for the engineering domain. This paper adheres to the definition proposed by Laprie [1]. A brief overview of the dependability research domain helps to distinguish the term "error" from other similar terms.

Dependability is the ability of a system to deliver a service that can be justifiably trusted. The service, delivered by a system, is its behavior as it is perceived by its user. Laprie describes dependability from three points of view: the *attributes* of dependability, the *means* by which dependability is attained, and the *threats* to dependability. We are focused on the threats:

Fault is a *defect* in the system that can be activated and cause an error.

Error is an *incorrect internal state* of the system, or a discrepancy between the intended behavior of a system and its actual behavior.

Failure is an instance in time when the system displays behavior that is contrary to its specification.

Activation of a fault leads to the occurrence of an error. The invalid internal system state, generated by an error, may lead to another error or to a failure. Failures are defined according to the system boundary. If an error propagates outside the system, a failure is said to occur.

* Corresponding author. Tel.: +49 351 46332202; fax: + 49 351 46337039.
E-mail address: andrey.morozov@tu-dresden.de (A. Morozov).

http://dx.doi.org/10.1016/j.mechatronics.2014.09.005
0957-4158/

Analysis of fault activation, error propagation, and error (or failure) detection is defined in this article as *error propagation analysis*. The results of this analysis is extremely helpful in a wide range of analytical tasks associated with dependable systems development. The error propagation analysis gives sound support for reliability evaluation, because error propagation has significant influence on the system behavior in critical situations. The error propagation analysis is a necessary activity for safety system design. It helps to estimate the likelihood of error propagation to hazardous parts of the system and identify parts of the system that should be protected with error detection or error recovery mechanisms more strongly than the others. Another possible application area is system testing and debugging. An accurate error propagation analysis assists selecting an appropriate testing strategy. It helps to identify the most critical parts of the system (from either reliability or safety points of view) and to generate such a set of test-cases that will stimulate fault activation in these particular parts and allow the detection of occurred errors. Probabilistic error propagation analysis can be used for system diagnostics. In the case of error detection in observable system outputs, it helps to trace back an error propagation path up to an error-source. It speeds up the error localization process, system testing, and debugging.

In real systems, fault activation and further error propagation are very complex processes. This causes the need for a strong mathematical framework to perform an accurate error propagation analysis. Specifics of the mechatronic domain brings additional complexity. The fact is that mechatronic systems incorporate the assembly of heterogeneous components (mechanical, electrical, computer, and information technology) with various mutual interactions. The goal of mechatronic system design is to ensure a proper and coordinated operation of these elements within a feedback structure under all possible operational conditions. According to Janschek [2], one of the big challenges of mechatronics is the use of appropriate models, which describe this mutual interaction on a common abstract layer. The error propagation analysis, as an essential part of the mechatronic system design, also requires a specific model. This model must be able to operate with abstract entities to represent various properties of the heterogenous mechatronic components. A sufficient error propagation model is presented in this article in details. Also, some of the basic ideas you can find in our previous publications [3–5].

2. State of the art

Most of safety–critical mechatronic systems consist of a mix of software and hardware elements. Typically, error propagation analysis of hardware is based on one of the classical reliability evaluation techniques: *failure modes and effect analyses* (FMEA), *hazard and operability studies* (HAZOP), *fault trees analysis* (FTA), *event trees* (ET), etc. Generally, the process of failure analysis consists of several activities: identifying failures of individual components, modeling the failure logic of the entire system, analyzing the effect of a failure on other components, and determining and engineering the migration of potential hazards. With the emergence of component-based development approaches, investigations began exploring component oriented safety analysis techniques, mainly focusing on creating encapsulated error propagation models. These failure propagation models describe how failure modes of incoming messages, together with internal component faults, propagate to failure mode of outgoing messages [6–10].

In the software engineering domain, the majority of classical error propagation approaches are based on *fault injection* or *error injection* techniques, conjugated with further statistical evaluation. Three of them were introduced by Voas [11–13]. An empirical study about propagation of data-state errors was presented in [14]. Candea et al. present a technique for automatically capturing dynamic fault propagation information in [15]. The authors use instrumented middleware to discover potential failure points in the application. Khoshgoftaar et al. [16] describe identification of software modules, which do not propagate errors, induced by a suite of test cases. A number of papers depict the influence of software error propagation phenomena on system reliability [17,18].

Four error propagation models that can be considered as the best candidates for the analysis of mechatronic systems are listed in this section. Unlike the models discussed above, these four candidates are abstract enough to cope with the heterogeneity of components of mechatronic systems and have a strong mathematical foundation. The key properties of these models are compared in Table 1.

Abdelmoez's model [19–21] is a design-level model for error propagation analysis of COTS systems that was also extended for reliability evaluation in [22]. This model uses information about system states and messages in order to compute the probability

Table 1
The comparison table of the suitable models for the error propagation analysis of mechatronic systems.

Author and years	Abdelmoez et al., 2002/2004/2005
Application areas	COTS
Required data	State and sequence UML diagrams
Main idea	An early estimate of the error propagation probabilities between system components in terms of states and messages
Purpose	General use and reliability assessment
Deficiencies	Not abstract enough. Requires very specific and detailed system models
	Hiller et al., 2001/2005/2007
Application areas	Modular software for embedded systems
Required data	Source code and reliability measurements
Main idea	The concept of error permeability through a system module
Purpose	Placement of EDM and ERM. Reduction of error propagation by design
Deficiencies	More oriented to module level rather than system level analysis. Applicable only for a software part of the system
	Mohamed et al., 2008/2010
Application areas	COTS
Required data	Component UML diagrams, estimated fault activation and error propagation probabilities
Main idea	Error propagation through an architectural service route
Purpose	Reliability assessment
Deficiencies	Not comprehensive enough. Can be considered an offshoot of Cortellessas model
	Cortellessa et al., 2006/2007
Application areas	COTS and SOA
Required data	Fault activation, error propagation, and control flow transition probabilities
Main idea	Probabilistic error propagation analysis using Markovian representation of control flow
Purpose	Placement of error detection and error recovery mechanisms. Identification of critical components Development of cost-effective testing strategies
Deficiencies	Does not distinguish between control and data flows