Reliability Engineering and System Safety 149 (2016) 148–163

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Transient fault tolerant control for vehicle brake-by-wire systems

Shuang Huang [a,b], Chunjie Zhou [a,b,*], Lili Yang [c], Yuanqing Qin [a,b], Xiongfeng Huang [a,b], Bowen Hu [a,b]

[a] School of Automation, Huazhong University of Science and Technology, Wuhan 430074 China
[b] Key Laboratory of Ministry of Education for Image Processing and Intelligent Control, Wuhan, China
[c] School of Business and Economics, Loughborough University, Leicestershire, UK

ARTICLE INFO

Article history:
Received 12 September 2013
Received in revised form
28 December 2015
Accepted 1 January 2016
Available online 15 January 2016

Keywords:
Brake-by-wire
Transient fault tolerance
Task reallocation
Sliding mode control
Architecture analysis and design language

ABSTRACT

Brake-by-wire (BBW) systems that have no mechanical linkage between the brake pedal and the brake mechanism are expected to improve vehicle safety through better braking capability. However, transient faults in BBW systems can cause dangerous driving situations. Most existing research in this area focuses on the brake control mechanism, but very few studies try to solve the problem associated with transient fault propagation and evolution in the brake control system hierarchy. In this paper, a hierarchical transient fault tolerant scheme with embedded intelligence and resilient coordination for BBW system is proposed based on the analysis of transient fault propagation characteristics. In this scheme, most transient faults are tackled rapidly by a signature-based detection method at the node level, and the remaining transient faults, which cannot be detected directly at the node level and could degrade the system performance through fault propagation and evolution, are detected and recovered through function and structure models at the system level. To jointly accommodate these BBW transient faults at the system level, a sliding mode control algorithm and a task reallocation strategy are designed. A simulation platform based on Architecture Analysis and Design Language (AADL) is established to evaluate the task reallocation strategy, and a hardware-in-the-loop simulation is carried out to validate the proposed scheme systematically. Experimental results show the effectiveness of this new approach to BBW systems.

1. Introduction

Automotive electronic systems have been continuing to grow in quantity and complexity with increasing demands for safety, driving comfort, and driving excitement. To further enhance vehicular safety and performance, the concept of X-by-wire is inspired by the idea of fly-by-wire and applied in the automotive industry. Vehicle brake-by-wire (BBW) systems as a typical X-by-wire system are safety critical, i.e., any failure has the potential to result in death or serious injury of people [1–3]. According to statistics, more than 40% of road accidents were due to brake system faults [4]. Therefore, fault tolerant brake systems are significant to road safety.

The faults existing in BBW systems can be classified as permanent or transient faults according to their duration. Permanent faults have been handled by many methods in BBW systems and other X-by-wire systems [5–7]. Transient faults are caused by electromagnetic interference, radiation, temperature variations, etc. and happen very frequently in modern day electronics [5]. With the proliferation of electronic devices in cars, especially in modern high-end cars, nearly 2500 signals are exchanged by up to 70 electronic control units (ECUs), and transient-to-permanent fault ratios can reach up to 100:1 [8]. Transient fault-tolerance of ECUs has become a great challenge to the development of X-by-wire systems.

In BBW systems, transient faults are propagated not only between components but also from low abstraction level to high abstraction level [9]. The transient fault produces an error when it is activated. In turn, if the error propagates to the border of this level, a failure is said to have occurred, and this failure will be regarded as a fault at the next higher level [5]. Transient faults, which cannot be handled in time at the node level, will be propagated to the system level [5] and eventually degrade the system performance and be reflected in the functional structure.

Based on the characteristics of transient fault propagation, this paper intends to deal with transient faults at both the node and system levels, i.e. in a hierarchical structure. It then proposes a hierarchical transient fault tolerant control system with embedded intelligence and resilient coordination schemes at both the node

* Corresponding author at: School of Automation, Huazhong University of Science and Technology, Wuhan 430074, China. Tel.: +86 27 87558001; fax: +86 27 87543130.
E-mail address: cjiezhou@hust.edu.cn (C. Zhou).

http://dx.doi.org/10.1016/j.ress.2016.01.001
0951-8320/

Nomenclature

ABS	anti-lock braking system
AADL	architecture analysis and design language
BBW	brake-by-wire
CAN	controller area network
CI	communication interface
CRC	cyclic redundancy check
ECU	electric control unit
EBCN	electronic brake control node
FEBCN	front electronic brake control node
REBCN	rear electronic brake control node
FLWN	front left wheel node
FRWN	front right wheel node
RLWN	rear left wheel node
RRWN	rear right wheel node
FCU	fault collection unit
GFM	goal-function-module
HIL	hardware-in-the-loop
PC	personal computer
PN	pedal node
PS	pedal sensors
QoC	quality of control
RBF	radial basis function
SMC	sliding mode control
TTCAN	time-triggered CAN
TTP/C	Time-Triggered Protocol/CAN

and system levels that would tackle the transient faults of the vehicle BBW systems. At the node level, a signature-based fault detection method is used to detect transient faults, and these transient faults are recovered by pre-set strategies. Obviously, due to the characteristics of transient faults, not all transient faults can be detected and recovered at the node level due to the characteristics of transient faults [10]. Thus, at the system level, anomaly-based fault detection is employed to detect the transient faults, which are not detected at the node level from the two aspects of quality of control (QoC) and functional structure, and it focuses on the influence of transient faults on BBW systems. A fault diagnosis module is used to coordinate the handling of these transient faults at the system level. On aspect of the QoC, an online fault estimator, is designed to approximate the influence of transient faults affecting QoC, and a sliding mode fault tolerant control algorithm is employed to implement the anti-lock braking system (ABS) control for each wheel. Regarding the system functional structure, a system structure model is designed to detect the transient faults affecting functional structure, and a dynamic task reallocation strategy is proposed to recover them. The effectiveness of the proposed transient fault BBW system is verified systematically in the following three aspects: validation of transient fault tolerance at the node level by using an architecture analysis and design language (AADL) environment [11–12], simulation of a fault tolerance for single type of transient fault at the system level in a Simulink environment and an AADL tool suite, and a whole system experiment through a hardware-in-the-loop (HIL) simulation based on Matlab and CANoe tools.

The outline of the paper is as follows. Section 2 reviews related work in this area. Section 3 presents the BBW system architecture and discusses its transient fault propagation. Section 4 proposes the transient fault tolerant approach for the BBW system. Section 5 verifies the effectiveness of the approach. The concluding remarks are provided in Section 6.

2. Related work

BBW technology has been extensively studied in literatures in recent decades [1,3,7,13,14,15,16], which is an active area of research given the emergence of advanced technologies in both brake control principles and implementation techniques of control system. Fault tolerance is an important safety aspect of BBW systems and has to be considered in the process of design, development, and integration.

Relevant work has been done to improve the reliability of BBW systems from a safety perspective. Roberts and Chhaya [13] presented a BBW system design and development method with an emphasis on hazards analysis. Cheon et al. [14] investigated the concept phase of functional safety based on ISO26262 for a BBW system. Peng et al. [15] studied the optimal structure of redundant systems based on various settings of fault coverage factor. These approaches are mainly for preventing permanent failures during the design stage, and are not suitable for transient fault tolerance. Meanwhile, a large amount of work has been done to develop fault tolerant algorithms based on brake control principles. Saric et al. [16] proposed a new design-friendly and cost-effective approach to control an automotive brake-by-wire actuator. Wang et al. [17] presented a novel fault-tolerant control method based on control allocation via dynamic constrained optimization for electric vehicles with XBW systems. Some other works suggested fault diagnosis and fault tolerant control strategies for ground vehicles [18,19]. Zhang et al. [20] designed a novel redundant and fault-tolerant actuator unit that can tolerate some faults caused by being out-of-sync. Naidu et al. [1] presented and analyzed the suitability of three fault-tolerant inverter configurations for automotive X-by-wire systems, which can deal with various inverter faults. Gadda et al. [2] suggested modeling and fault detection filter design techniques, which can be used to construct a set of diagnostic residuals and are suitable for detecting and isolating a wide variety of steering system faults. In [21–23], some fault-tolerant control algorithms for BBW systems and other vehicle control systems were presented. These works integrated fault tolerance with controller design, but ignored transient fault in corresponding software implementation. Due to their the unpredictable nature, different variables and short duration characteristics, transient faults cannot be detected completely [10]. Therefore, it is difficult to achieve the goal of a transient fault tolerant control that depends on fault characteristics. In addition, the control system structure with an emphasis on the implementation of a control system is also an important aspect of transient fault tolerance for BBW systems. Thus, some other studies try to solve this problem from a software engineering perspective. Pinello et al. [5] suggested a fault-tolerant distributed deployment approach by using replication and scheduling technologies. Aidemark et al. [24] presented a node-level transient fault tolerant method based on time-redundant execution of application tasks. Through these works, system reliability can be statically promoted. However, transient faults affect the system reliability of BBW systems from both the QoC and the functional structure through fault propagation [25]. Furthermore, these two aspects influence each other. Therefore, it is necessary to design a transient fault tolerant control considering the transient fault propagation process.

This paper presents a hierarchical transient fault tolerant control system with embedded intelligence and resilient coordination