Control Engineering Practice (xxxx) xxxx–xxxx

Contents lists available at ScienceDirect

Control Engineering Practice

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

Model-based diagnosis and fault tolerant control for ensuring torque functional safety of pedal-by-wire systems

Jiyu Zhang[a,*], Giorgio Rizzoni[a], Andrea Cordoba-Arenas[a], Alessandro Amodio[b], Bilin Aksun-Guvenc[a]

[a] Department of Mechanical and Aerospace Engineering, Center for Automotive Research, The Ohio State University, 930 Kinnear Rd, Columbus, OH 43212, United States

[b] Politecnico di Milano, Dipartimento di Elettronica, Informazione e Bioingegneria, 5, Via Ponzio, 34, 20133 Milano, Italy

ARTICLE INFO

Keywords:
Functional safety
ISO 26262
Model-based
Fault diagnosis
Fault tolerant control
Pedal-by-wire system

ABSTRACT

This paper presents a model based approach for defining automotive functional safety requirements and provides a solution to ensure functional safety through model-based diagnosis and fault tolerant control. This model-based approach is consistent with ISO 26262 – functional safety standard. In particular, this paper presents the necessary steps for defining and implementing functional safety requirements, including item and function definition, Hazard Analysis and Risk Assessment, as well as the design of a model-based diagnostic and fault tolerant control (FTC) system that can lead to a systematic solution to automotive functional safety problems. The methodology proposed in this paper is applied to the problem of torque functional safety of pedal-by-wire systems.

1. Introduction

With the widespread use of on-board electrical and electronic (E/E) components and subsystems, the automotive industry has been facing increasingly critical safety challenges in the E/E system development process. To guarantee functional safety of various components and subsystems of a vehicle, the automotive industry has developed its own functional safety standard – ISO 26262. The standard defines functional safety as "absence of unreasonable risk associated with each hazardous event caused by the malfunctioning behavior of E/E systems" (Christiaens, Ogrzewalla, & Pischinger, 2012; Dardar, 2014; ISO 26262, 2011). Therefore, functional safety can be guaranteed by preventing or eliminating the risk of potential hazards. This is usually achieved by developing *safety cases*, which provide safety arguments, supported by sufficient evidence to show the absence of unreasonable risk associated with each hazardous event. Palin and Habli (2010), Palin, Ward, Habli, and Rivett (2011), and Birch et al. (2013) discuss safety case approaches for ensuring functional safety in compliance with ISO 26262. In these references, a general framework for building safety cases is presented. A safety case must provide enough evidence to show that fault events can be safely managed, which requires the implementation of risk mitigation strategies if any component is detected to be faulty. However, the discussions on risk management and risk mitigation in these references are rather qualitative, and they do not address the problem on how the fault mitigation strategies can be practically designed and implemented to meet the functional safety goals.

This paper, on the other hand, proposes a quantitative approach using explicit models to implement automotive functional safety requirements. This approach not only helps define functional safety requirements in a quantitative way, but also introduces a model-based diagnosis and fault tolerant control approach that fulfills the functional safety requirements and leads to an integrated solution to functional safety problems.

ISO 26262 (2011) relies on a "V-model" to represent each phase of a safety lifecycle. In this paper, an analogous approach is proposed to illustrate a model based approach for ensuring functional safety. It starts from functional safety requirements definition, and works through the design process of model-based diagnosis and fault tolerant control (FTC) system that leads to the implementation of diagnosis and FTC algorithms. The process is described by the V-model diagram in Fig. 1.

The key elements of this approach include:

1. Item definition to clearly define the various components comprising a system as well as the functions they perform.
2. Hazard Analysis and Risk Assessment (HARA) to identify the various hazards and their Automotive Safety Integrity Level (ASIL).

* Corresponding author.
E-mail address: zhang.1919@osu.edu (J. Zhang).

http://dx.doi.org/10.1016/j.conengprac.2016.11.017
Received 16 May 2015; Received in revised form 29 November 2016; Accepted 30 November 2016

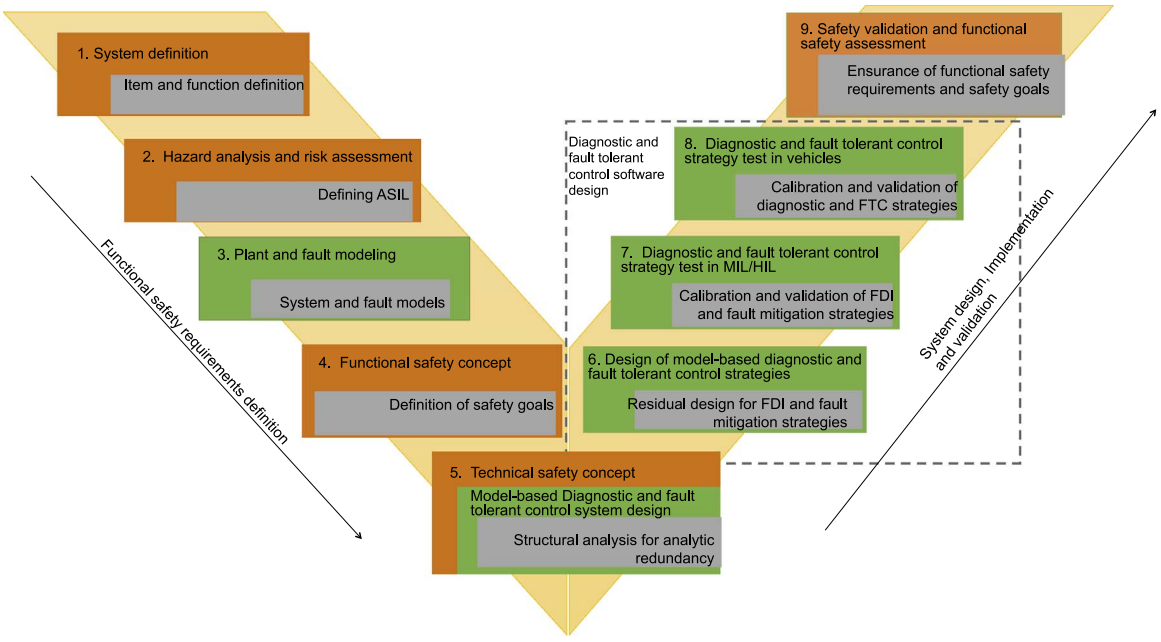

Fig. 1. A systematic model-based methodology for automotive functional safety through model-based diagnosis and fault tolerant control.

3. Detailed plant and fault modeling to assist HARA so that a suitable ASIL is assigned for each considered hazard and safety goals are set.
4. The technical design of a model-based fault diagnosis and FTC approach that is generally applicable to any systems performing safety functions, in particular, the various steps of implementation, calibration and validation of the diagnostic and fault tolerant control functions.
5. Functional safety assessment of the diagnostic and FTC strategies to ensure functional safety goals.

This paper studies the necessary steps for achieving functional safety using this model-based approach, and presents a case study on torque functional safety of electrified vehicles, though the methods developed would be applicable to any pedal-by-wire systems, regardless of powertrain type. The torque functional safety problem, also referred to as sudden unintended acceleration in this paper, is defined as the occurrence of unintended, unexpected, high-power accelerations starting from a stationary position or a very low initial speed accompanied by an apparent loss of braking effectiveness (Pollard, 1989). This paper shows that the proposed model-based approach can be used to define a quantitative functional safety goal related to torque functional safety for pedal-by-wire systems in electrified vehicles, and studies how model-based diagnosis and FTC can help achieve the goal to avoid unreasonable risk associated with unintended acceleration event.

Model-based diagnosis has the advantage of providing a deep understanding of the process behavior and is effective in detecting incipient faults (Gertler, 1998; Rizzoni, Onori, & Rubagotti, 2009). In particular, this paper presents a model-based diagnostic tool which is referred as structural analysis for Fault Detection and Isolation (FDI), which is a methodology that uses the *structural model* of a system to identify the analytic redundant relations in the system model, leading to a systematic approach to fault diagnosis (Blanke & Schröder, 2003; Krysander, 2006). One advantage of the structural FDI approach is that it does not depend on specific numerical parameters, but it depends on the structure of the model, as is shown later in the paper. Therefore, it is applicable in the early stages of the design process to any diagnostic system, even when the final system specifications are not determined. A further advantage of the structural analysis approach is that it decomposes a complex system into smaller subsystems. This decomposition allows for efficient design of diagnostic algorithms that are more easily implementable. This approach is especially useful in the diagnosis of large complex systems such as automobiles.

The structural FDI approach has been well developed in the literature, mostly with focus on its theoretical development, for example in Krysander and Nyberg (2002), Krysander and Aslund (2005), Krysander and Frisk (2008), Krysander, Aslund, and Nyberg (2008), and Flaugergues, Cocquempot, Bayart, and Pengov (2009). As to the application side, structural FDI has been applied to engine systems (Svard & Nyberg, 2010; Svärd, Nyberg, & Frisk, 2013; Svärd, Nyberg, Frisk, & Krysander, 2013), battery systems (Liu, Ahmed, Rizzoni, & He, 2014), hybrid vehicle systems (Sundström, 2011; Sundstrom, Frisk, & Nielsen, 2014), and permanent magnet synchronous machine (PMSM) drive systems (Zhang & Rizzoni, 2014; Zhang, Yao, & Rizzoni, 2016). The structural analysis approach has proven to be an efficient tool in analyzing the fault detectability and isolability in a complex engineering model, and provides guidance to the architecture of diagnostic algorithms for fault detection and isolation. The work presented in this paper is the first in which structural analysis is linked to the torque functional safety problem. This paper develops FDI and FTC strategies based on structural analysis to show its application to solve the torque functional safety problem and therefore to ensure functional safety.

This paper is organized as follows: Section 2 presents a systematic model based approach for functional safety. The section covers the relevant aspects of ISO 26262, using an electrified powertrain as an example. Section 3 introduces a safety case of torque functional safety of pedal-by-wire systems in electrified vehicles. In particular, a structural approach for FDI and FTC is introduced to identify the fault location and mitigate the effects of faults in order to achieve torque functional safety. Then, simulation results are presented to show the effectiveness of the proposed FDI and FTC strategies. Finally in the section, functional safety assessment are presented to show that the safety goal can be met using the proposed strategies.