

Safety Analysis of Software-intensive Motion Control Systems

Rami Debouk, Barbara Czerny and Joseph D'Ambrosio

General Motors Corporation

Jeffrey Joyce

Critical Systems Labs., Inc.

Copyright © 2009 GM Global Technology Operations, Inc. Published by SAE International with permission.

ABSTRACT

The auto industry has had decades of experience with designing safe vehicles. The introduction of highly integrated features brings new challenges that require innovative adaptations of existing safety methodologies and perhaps even some completely new concepts.

In this paper, we describe some of the new challenges that will be faced by all OEMs and suppliers. We also describe a set of generic top-level potential hazards that can be used as a starting point for the Preliminary Hazard Analysis (PHA) of a vehicle software-intensive motion control system. Based on our experience with the safety analysis of a system of this kind, we describe some general categories of hazard causes that are considered for software-intensive systems and can be used systematically in developing the PHA.

A comprehensive PHA for a software-intensive motion control system may reveal potential interactions of features that are not due to malfunctions of the features' individual components but that may lead to hazardous conditions. This insight and other lessons learned from our experience with such systems have influenced the drafting of ISO CD 26262.

Finally, this paper reports on our preliminary experience with the method of risk assessment proposed for ISO CD 26262 Part 3, Concept Phase.

INTRODUCTION

The auto industry has had decades of experience with designing safe vehicles. One key aspect of designing these vehicles relates to the development of dependable motion control systems. All vehicles include several motion control systems, such as steering, braking, and propulsion. In early vehicles, motion control systems were designed using mechanical components and operated independently of one another. Over the last two decades, vehicle design has evolved to include the use of electronics and software in these motion control systems. For example, steering systems are now often

implemented by electric power steering systems, comprised of mechanical components and electronics that include software. Currently, motion control systems still operate mostly independent from one another and mostly activate based on driver input.

Given that these systems control the motion of the vehicle, they have the potential to create safety-related issues if they do not operate properly. Such systems are commonly called safety-critical systems [1,2]. Safety-critical systems are designed and analyzed to help verify not only that they operate as they were intended, but also to prevent them from independently operating in any way that is not desired. A system safety process, based on best practice techniques, may be used to guide the design and analysis activities applied to safety-critical systems [2,3,4].

Recently, the automotive industry has begun introducing new features in vehicles that command its motion control systems, such as crash mitigation braking. These features when providing commands to the vehicle motion control systems, may direct them to take actions independent of the driver under some conditions. This represents a departure from previous motion control systems, in that they may now operate independent of the driver and multiple motion control systems may activate simultaneously based on commands received from one or more features. Thus, the introduction of highly integrated features brings new challenges that may require innovative adaptations of existing system safety methodologies and perhaps even some completely new concepts.

In this paper, we describe some of the new challenges that will be faced by all OEMs and suppliers when developing features that command motion control systems. We also describe a set of generic top-level potential hazards that can be used as a starting point for the PHA of vehicle software-intensive motion control systems. Based on our experience with the safety analysis of a system of this kind, we describe some general categories of hazard causes that are considered for software-intensive systems and that can be used

systematically in developing the PHA. A comprehensive PHA for a software-intensive motion control system is likely to reveal potential concerns that may not simply be due to the malfunctions of individual components, but also may potentially be due to the interaction of its integrated features. Finally, this paper reports on our preliminary experience with the method of risk assessment proposed for ISO CD 26262 Part 3, Concept Phase.

CHALLENGES OF FEATURE INTERACTIONS

Previously, vehicle motion control systems did not typically interact with one another. However, with the incorporation of multiple features on the vehicle, some of which may act independently of the driver, it is possible for these features to independently command the same or different motion control systems on the vehicle. This is known as feature interaction [5]. Thus, there is the potential for conflicting or opposing requests to be made to the motion control systems from the different features. Assessing the potential for feature interaction and designing the system to avoid or mitigate these potential conflicts is a new challenge that needs to be addressed by the system safety process.

Given that these features are designed to enhance vehicle safety, we want to overcome the challenges. Applying a rigorous system safety process to the design and development of these features can help to address the new challenges faced by their introduction.

In this paper we investigate one possible application of a system safety process to the design and development of a system that demonstrates these new challenges. The system consists of several individual features, each acting to achieve their individual goals. In addition, these individual features must interact with each other to achieve their goals in a safe and effective manner. The features of this system control the motion of the vehicle either in conjunction with the driver or independent of the driver. These systems are referred to as software-intensive motion control systems in this paper. Ensuring that the features interact with each other in a safe manner, introduces new challenges and requires new considerations during the safety analysis activities. In the next section of the paper, we present the investigated approach for addressing and dealing with these challenges.

APPROACH

The approach we investigated for the safety analysis of the software-intensive motion control system as described in the previous section consisted of the following main steps:

- Preliminary hazard analysis and risk assessment
- Elicitation and analysis of the functional safety concept
- Hazard analysis and risk assessment

- Design of diagnostics and fault management
- Safety verification
- Safety case preparation

This paper only investigates one application of this approach to software-intensive motion control systems. Any approach should be flexible to enable changes as factors influencing the definition of the system safety process may vary in the near future. Hence, there should be opportunities for flexibility and reconfiguration of the process as the automotive functional safety standard ISO 26262 evolves.

The following is a description of the six steps of the investigated approach presented above. It is worth noting here that the execution of the above process steps is not entirely sequential. Moreover, the above steps have substantial interactions with the rest of the development effort. Some of the above steps have been influenced by the guidance contained in draft versions of ISO CD 26262 [6-14], especially the method used to assess risk by assigning an Automotive Safety Integrity Level (ASIL).

PRELIMINARY HAZARD ANALYSIS AND RISK ASSESSMENT - Conventionally, the preliminary hazard analysis is the first attempt to understand the potential hazards associated with the system, along with potential causes and effects. Our approach to the preliminary hazard analysis had the objectives of: a) producing a list of the potential hazards, b) defining each potential hazard in terms of an event and/or a set of conditions that are observable at the system boundary, and c) providing an initial assessment of the safety risk associated with each potential hazard in terms of an ASIL.

In planning our approach to the PHA, we took a step back from the details of the features to define a generic set of potential hazards for software-intensive vehicle motion control systems. The motion control systems considered were brake, throttle, and steer and the failure modes of interest were unintended or excessive amount of a primary motion control action (in this analysis we assumed that an excessive control action can be categorized as unintended) and missing or insufficient amount of a primary control action (in this analysis we assumed that a missing control action can be categorized as insufficient). The six different combinations of these three different motion control actions and these two different failure modes yields the following list of generic potential hazards for a vehicle motion control system:

- Unintended or Excessive Braking
- Missing or Insufficient Braking
- Unintended or Excessive Acceleration
- Missing or Insufficient Acceleration
- Unintended or Excessive Steering
- Missing or Insufficient Steering