

Development of a Method for Comprehensive Derivation of Public Road Situations for Functional Safety Analysis

Miyata Yoshihiro¹⁾ Kashihara Shuhei¹⁾ Nakano Takayuki¹⁾

*1) Nissan Motor Co., Ltd.
560-2 Okazu Koku, Atsugi-shi, Kanagawa 243-0126, Japan*

KEY WORDS: electronics and control, autonomous driving, functional safety (E1)

In recent years, vehicle development in the automotive industry has become large scale and increasingly complex in step with the advancement of automated driving, and the importance of functional safety development (ISO 26262) to ensure product safety has accordingly grown. The operational design domains (ODD) of systems such as automated driving systems are expanding, and functional safety development must therefore address not only highways but also public roads. However, hazard analysis and risk assessment (HARA) activities face a practical issue: the scenes a vehicle may encounter on public roads are effectively innumerable, making exhaustive analysis extremely time consuming and rendering demonstration of coverage difficult. This paper reports a method we developed for comprehensively deriving public road situations and presents an application example intended to address these issues.

Next, we examine the situations that the system may encounter for the purposes of hazard analysis and risk assessment. The system considered is a hypothetical Level 2 automated driving system that recognizes preceding vehicles and lane markings, controls throttle, brake and steering, and assists driving to a destination, with an ODD that includes public roads. Unlike highways or limited access roads, public roads involve a vastly larger number of situational factors—such as pedestrians, bicycles, and crosswalks—so the number of situation patterns the system may encounter is effectively unbounded and exhaustive enumeration is impractical.

To enable comprehensive derivation of situations, we systematized constituent factors of situations beginning from a simple example scene. We initially classified factors according to the three factors used for ASIL determination (S, E, C), but some factors overlapped across these categories; unless each factor is uniquely assigned to one factor, duplicated situations occur. We therefore optimized the factor assignments to eliminate overlap. As a result, situations were organized into three groups aligned with ASIL factors: Collision (Severity related) as Collision factor (S); Behavior (Controllability related) as Behavior factor (C); and Environment (Exposure related) as Environmental factor (E). The factor composition was structured as follows: S (one factor) — Object or Road obstacle; C (three factors) — Own vehicle behaviour, Surrounding object location, Surrounding object motion; E (six factors) — Road condition, Weather, Time of day, Traffic information, Curvature, and Road gradient. Concrete examples for each factor were enumerated with reference to ISO 21448 (Safety of the Intended Functionality), ISO 34502 (Scenario based safety evaluation framework for automated driving systems), and related literature. By enumerating all possible combinations of the factors and their examples, we derived approximately 630 million distinct situations. The derivation method is presented in this paper.

However, hazard analysis and risk assessment require combining each hazard with situations to identify hazardous events and judge whether they lead to harm, and directly combining every hazard with 630 million situations would make HARA prohibitively time consuming. To address this, we developed methods to narrow down hazardous events relevant to a given system hazard, and we describe these methods using the example hazard “unintended sudden acceleration.” The narrowing approach combines five techniques: (1) exclude constituent factors outside the system ODD; (2) exclude or consolidate examples within the Collision factor (S); (3) exclude or consolidate examples within the Environmental factor (E); (4) exclude or consolidate examples within the Behavior factor (C); and (5) exclude factors and examples unrelated to system operation. By applying the five techniques in combination, we reduced the candidate hazardous events from 630 million to 30 representative hazardous event patterns.

By applying the methods presented in this paper to functional-safety development, hazard analysis and risk assessment can incorporate situations comprehensively, thereby enabling assurance of the safety of increasingly large-scale and complex automated-driving systems. Furthermore, the approach makes it possible to extract the hazardous events that warrant consideration from a vast set of potential events, allowing functional-safety development to be conducted more efficiently. We expect this work to assist practitioners in ISO 26262 development when addressing the myriad hazardous events encountered on public roads.

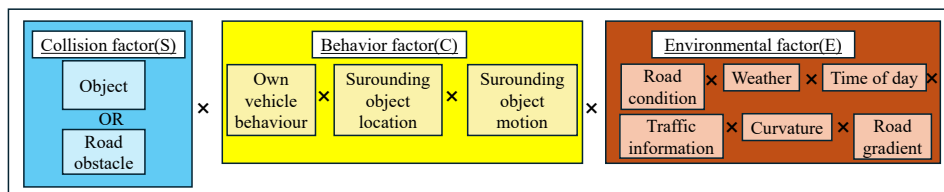


Fig.1 Optimized Situation Factors