講演番号	182

Applying ISO 21448 (SOTIF) to a Hypothetical Case of Automated Mobility Service

Miharu Oiwa[1)] **Yoshihiro Miyazaki**[1)] **Kazuyoshi Fukuda**[1)]

1) Japan Automobile Research Institute
1-1-30, Shibadaimon, Minato-ku, Tokyo, 105-00112, Japan (E-mail: moiwa@jari.or.jp)

KEY WORDS: **Software and its underlying technologies, Safety (functional safety, SOTIF),** Automated driving [E3]

This paper presents a concept-level case study on applying ISO 21448:2022 (Safety of the Intended Functionality; SOTIF) to a hypothetical case of automated mobility service. The need for SOTIF compliance has increased, yet publicly available examples that specifically address mobility services remain limited. This lack of shared knowledge presents a barrier for practitioners. Therefore, this paper systematically presents how ISO 21448 can be applied to such a service, following clauses 5 through 8 of the standard to provide practical insights to the industry.

Under ISO 21448, SOTIF is achieved by addressing hazards that arise from combinations of functional insufficiencies and triggering conditions. Accordingly, the overall process is to identify those functional insufficiencies and triggering conditions and to modify the system specifications and design so as to mitigate or avoid the resulting harm.

First, specification and design are carried out in accordance with ISO 21448 clause 5. The hypothetical service assumes an SAE Level 4 automated vehicle traveling on a two-way shared lane where pedestrians and cyclists coexist with authorized automated vehicles. Several weather conditions, including clear weather, rain, and fog, are considered within the Operational Design Domain (ODD). The vehicle's maximum speed is limited to 12 km/h. An initial functional architecture is defined, consisting of fixed-direction cameras, environmental perception, vhecle speed and trajectory computation, and motor.

An identification and evaluation of hazards are then conducted in accordance with ISO 21448 clauses 6.3 and 6.4. Six hazards related to basic driving functions are considered in this analysis. Each hazard is analyzed by examining possible scenarios derived from the ODD and system design, and by assessing severity (S) and controllability (C). In this analysis, hazards that present both $S > 0$ and $C > 0$ are classified as having potentially unreasonable risk. Five of the six hazards fall into this category, meaning they must be addressed through subsequent SOTIF activities.

Next, the residual risk acceptance criterion is defined in accordance with ISO 21448 clause 6.5. This paper adopts the principle that the introduction of a technical system should not increase societal risk. Applied to automated driving, this means the system must achieve safety performance at least equivalent to a competent and attentive human driver—in this case, a bus driver operating within the same environment. This benchmark is used to evaluate whether functional insufficiencies and triggering conditions could lead to unacceptable behavior.

Next, potential functional insufficiencies and triggering conditions are analized in accordance with ISO 21448 clause 7.3. We analyze the situations in which this hazard may occur in a way that fails to meet the acceptance criteria, using the system specifications, design, and assumptions. For the hazard of fails to decelerate as intended, the deductive analysis identified three combinations of functional insufficiencies and triggering conditions related to objedt detection.

Next, to mitigate SOTIF-related risks, functional modifications are carried out in accordance with ISO 21448 clause 8. Adding radar sensors and 360-degree cameras addresses detection challenges. Thus, under ISO 21448, it is required to modify the system specifications and design so that hazards caused by triggering conditions and functional insufficiencies do not lead to harm.

In conclusion, this case study clarifies a practical and systematic approach to applying ISO 21448 to automated mobility services. Thus, this paper contributes to reducing knowledge gaps and supporting the wider adoption of SOTIF within industry.

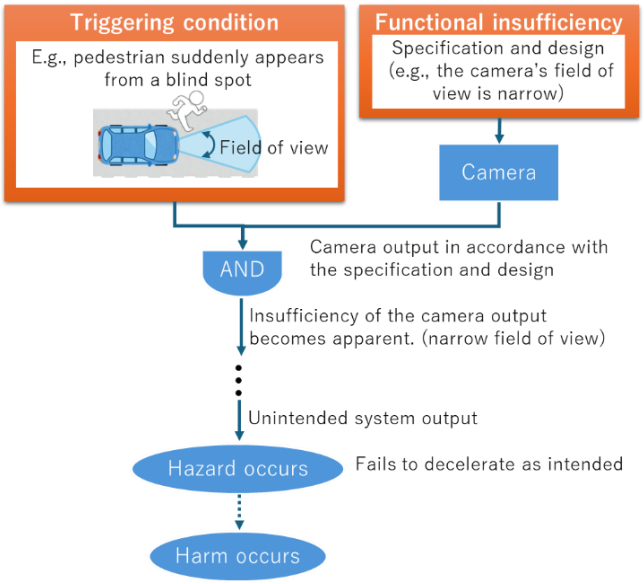

Fig.1 SOTIF-related hazardous event model