講演番号	202

Leveraging the Safety Concept Description Language (SCDL) for Harmonized Development of SOTIF and Functional Safety

Tanaka Nobuaki [1)] Takada Akira [2)] Yamashita Shuhei [2)] Imai Misako [2)] Ogasawara Toyokazu [3)] Murata Tomoyoshi [4)] Sasaki Kiyoshi [5)] Nishihara Hideaki [6)]

1) OTSL
1-21-27 Izumi, Higashi-ku, Nagoya, Aichi, Japan (E-mail: tanaka_nobuaki@otsl.jp)
2) DNV Business Assurance Japan.
7-1-15 Gokodori, Chuo-ku, Kobe, Hyogo, Japan
3) Ota Development Efficiency Project.
1085-79 Hamada-cho, Ota, Gunma, Japan
4) Japan Automobile Research Institute.
2530 Karima, Tsukuba, Ibaraki, Japan
5) Astemo.
2520 Takaba, Hitachinaka, Ibaraki, Japan
6) National Institute of Advanced Industrial Science and Technology.
1-8-31 Midorigaoka, Ikeda, Osaka 563-8577, Japan

KEY WORDS: **Software and its underlying technologies, Modeling Language, ISO 26262, Safety (Functional safety, SOTIF), Software development process, SCDL, SRVA (E3)**

This study investigates the applicability of the Safety Concept Description Language (SCDL) and Safety Requirement Violation Analysis (SRVA)—methods developed for ISO 26262 functional safety—to the development of Safety of the Intended Functionality (SOTIF: ISO 21448). As autonomous driving (AD) and advanced driver assistance systems (ADAS) continue to increase in complexity and size, the importance of SOTIF has been increasing. However, despite the fact that many of the activities in the functional safety processes and those in SOTIF are similar, a method for executing them in an efficiently integrated process has not yet been established. This work addresses the need for a unified architectural approach that supports consistent design and safety analysis across both standards.

SCDL provides a modeling language for system requirements and architecture based on ISO 26262 principles. SRVA complements this modeling framework by enabling early-stage and requirement-level safety analysis. Unlike traditional failure-mode-focused methods such as FMEA, SRVA identifies requirement-violation modes independent of the underlying cause. This characteristic makes SRVA suitable not only for functional-safety-related faults but also for performance insufficiencies and triggering conditions in SOTIF.

A case study involving a virtual autonomous driving system is conducted to evaluate the proposed integration. Intended functionality (IF) requirements are derived from both the item definition used in functional safety and the system definition used in SOTIF. Shared requirements are consolidated into a unified IF architecture expressed in SCDL. A common safety goal is adopted as the analytical anchor across both standards. Applying SRVA to the IF requirements identifies two major safety goal violation modes: capturing non-existent objects and generating non-existent objects. From these modes, the study derives both design-based and process-based mitigations, including conflict-detection, AD mode degradation, and machine-learning improvement. These mitigations are formalized as IF safety requirements (IFSRs) and IF process requirements (IFPRs) and are subsequently allocated to the architecture, demonstrating how results of SRVA can be seamlessly integrated into SCDL models.

The case study shows that SCDL can effectively represent SOTIF-oriented architectures and that SRVA can systematically identifies performance-related insufficiencies at an architecture design level. By introducing ISO 26262 concepts such as, architectural allocation, and safety mechanism formulation, into SOTIF development, the proposed approach clarifies the relationships between functional safety and SOTIF-related concerns. The findings suggest that incorporating SCDL and SRVA into SOTIF processes can enhance ~~traceability~~, analytical consistency, and development efficiency while promoting closer alignment between functional safety and SOTIF.

Overall, the research demonstrates the feasibility and benefits of applying SCDL and SRVA to SOTIF development. Future work will extend the analysis scope to include component faults, detailed triggering conditions, and performance insufficiencies, and will further evaluate the efficacy of integrated, cross-standard development workflows using SCDL throughout downstream design phases.

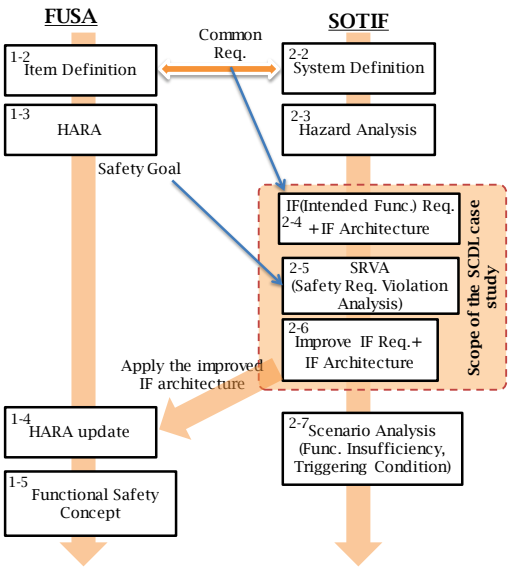

Fig.1 Unified process for our case study