Road vehicles – Safety Of The Intended Functionality Using STPA

Presenter Name: Madhusudan Lingarajappa

Company Name: Continental, Email ID: madhusudan.vaderahalli.lingarajappa@continental-corporation.com

In 2019, ISO published ISO/PAS 21448, Road vehicles - Safety of the Intended Functionality complementary process to functional safety. The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons is referred to as the SOTIF. The SOTIF risk identification and evaluation step determines if credible harm may result from hazardous events. After identifying hazardous events, the SOTIF process then focuses on identifying triggering events that may lead to unintended system behavior, identify system weaknesses as well as the related scenarios that could lead to an identified hazardous event.

Triggering events can be divided into two classifications:
1. The first category contains events that exceed the performance limitations of the system and components. E.g., Sensor limitations, limitations in algorithms and functional insufficiencies of the intended functionality or diverse environmental conditions.

2. The second category contains human factor limitations, or foreseeable misuse by persons/driver/operator particularly in relation to the driver-vehicle interface.

According to ISO/PAS 21448, scenarios may be classified as known-safe or known-unsafe depending on whether the mitigation strategies sufficiently reduce the SOTIF risk. A third category, unknown-unsafe, represents those scenarios that are not known at the time of system design and are identified through long-term vehicle tests, simulations, random input testing, and other measures.

The current approach applies a combination of analysis, simulation, test track, and on-road testing to identify unknown and potentially unsafe scenarios. However, there is no proper framework defined to identify the scenarios with respect to known-unsafe and unknown-unsafe scenarios. This would increase efforts in re-design and development of the system basically increasing the cost and impact on product time to market if the triggering events causing hazardous situations are found late.

System-Theoretic Process Analysis (STPA) is a hazard analysis technique which can be used to identify the scenarios with respect to known-unsafe and unknown-unsafe scenarios that were previously found in operations can be identified early in the development process and either eliminated or mitigated.

Unlike the traditional hazard analysis methods, STPA can be started in early concept analysis to assist in identifying safety requirements and constraints. These can then be used to design safety into the system architecture and design, eliminating the costly rework involved when design flaws are identified late in development or during operations. As the design is refined and more detailed design decisions are made, the STPA analysis is also refined to help make more and more detailed design decisions. Complete traceability from requirements to all system artifacts can be easily maintained, enhancing system maintainability and evolution.

STPA found all the causal scenarios found by the more traditional analyses but it also identified many more, often performance-related and operator misuse, scenarios that the traditional methods did not find. Finally, feasibility of SOTIF using STPA will be illustrated with an example in the presentation.

Keywords: SOTIF, STPA, Functional Safety, Automated Driving Systems, System Engineering.