Titel: "System Theoretical Process Analysis – Applied to a new mobility concept for automated cargo transport in urban areas"

Schwerpunktthema:	Methodik - Anwendungsbeispiel für eine Analysemethode im Umfeld automatisierter Systeme mit komplexer Mensch-Maschine-Interaktion
Bereich:	Mobilitätstechnick, ISO 21448 (SOTIF)
Beitragsart:	Vortrag / Anwendungsbeispiel

Author and Presenter: Stefan Braun, s.braun@fsq-experts.com, +49 (0) 151 420 746 75

Co-Author: Matthias Größler, m.groessler@fsq-experts.com, +49 (0) 160 156 411 8

FSQ Functional Safety & Quality Experts GmbH, Balanstr. 14, 81669 München

Due to an increasing number of automatic driving features in the vehicles and an increasing level of automation, OEMs and suppliers on all levels must adopt to ensure the safety of the vehicles. With respect to the term safety, functional safety was the main reference point in the automotive industry for the past decades. Now the focus is shifting from functional safety to system safety which includes additional areas. Currently most OEMs are working on the development and implementation of automated driving features up to level 3 according to SAE J3016. On this level safety of the intended functionality (SOTIF) is a key issue to be considered to achieve system safety. SOTIF is focused on hazards caused by limitations related to the perception of the environment and the processing of this information. This includes sensor fusion as well as the machine learning algorithms processing the sensor data. Examples for SOTIF relevant aspects are object detection, trajectory planning or decision-making algorithms. Failures of the system are not in scope of SOTIF as those are covered by functional safety. For high automation of level 4 and 5 as well as for autonomous driving even more challenges must be considered. And even for level 3 additional measures might be required in addition to SOTIF as the standard is focused on ADAS systems on level 1 and 2.

One implication of this development is that safety managers and engineers must extent their toolkit for safety analysis. Established methods are not capable to cover functional safety as well as cybersecurity and SOTIF to full extent. According to ISO26262:2018, 4: Clause 6.4.4.1 inductive analysis methods are highly recommended for all ASIL while deductive methods are recommended up to ASIL B and highly recommended for higher ASIL. Safety engineers are not limited to specific methods, but FMEA (inductive) and FTA (deductive) are the applied in most cases. With respect to SOTIF especially the human machine interfaces as well as the interaction between the driver and the vehicle must be considered for potential risks and hazards. In this regard those methods are limited. A detailed overview of the limitations will be provided as part of the presentation. The System Theoretical Process Analysis (STPA) has been recognized as a potential solution to overcome the limitations of FMEA and FTA to systematically analyse HMI-related risks and hazards. STPA is based on the control flow inside a system which is modelled using System-Theoretic Accident Model and Processes (STAMP). It provides a variety of benefits compared to FTA and FMEA when applied in a SOTIF context.

This presentation provides a practical case study on how STPA is applied to analyse an automated vehicle. The context is a research project of the German government (Helios project BMVI). The scope of development in the Helios project is a cargo bicycle capable to automatically follow the user. This feature is called Follow-Me mode. The main use case of the Helios bike is to support parcel delivery workers in their daily work in urban areas. In the context of this project the STPA is applied to analyse the symbiotic interaction between the user and the bicycle while using the Follow-Me mode to identify SOTIF related hazards.

The presentation will demonstrate the execution of the STPA while highlighting lessons learned and best practices. The analysis has been performed by safety experts which had little experience with the method. As it is assumed this applies to most safety managers and engineers in the automotive industry, it is expected that the findings and learnings gained are beneficial for a large audience. The intention is to provide a practical example of the benefits when STPA is applied to analyse HMI-related events for an automated vehicle.

Finally, the presentation will provide an overview where STPA might be able to contribute to other topics and domains. For example, STPA applied on higher levels of automotive automation or in the railway industry to analyse the interactions between the train driver, the machine and the railway signal box.