Combining functional safety and SOTIF Analysis using Component Fault and Deficiency Trees (CFDTs)

Marc Zeller, Siemens AG

Abstract:

In order to assess AI/ML-based systems in terms of safety, is it not sufficient to assure the system in terms of possible failure but also consider functional weaknesses/insufficiencies of the used algorithms according to Safety Of The Intended Functionality (SOTIF). Therefore, we introduce the concept of the so-called Component Fault and Deficiency Tree (CFDT). With this extension of the Component Fault Tree (CFT) methodology cause-effect-relationships between individual failures as well as functional insufficiencies and system hazards of the specified system can be described. Hence, it is possible to conduct safety analysis to apply for AI/ML-based systems. Thereby, we are able to show that all risks have been sufficiently mitigated and document efficiently the various mitigation schemes on different system levels.