**ISBN** 978-93-84422-37-0
**2015 International Conference on Advances in Software, Control and Mechanical Engineering (ICSCME'2015)**
*Antalya (Turkey) Sept. 7-8, 2015 pp. 1-7*

# Analysis and Development of Fail-Operational Automotive Mechatronic Systems

Stephan Reinhofer[1], Markus Ernst[1], Jürgen Fabian[1], and Adam Schnellbach[1]

[1]Graz University of Technology, Institute of Automotive Engineering,
Inffeldgasse 11/II, 8010 Graz, Austria

***Abstract*:** *Ongoing advances in mechatronic components and power electronics help to improve control systems within automotive applications. New developed or designed components enable more efficient system architectures and control. The management of several parameters of future drive architectures, such as high torque and power output, high system efficiency, low mass, low energy consumption, very low exhaust gas emissions, and low costs is essential for future propulsion concepts. Based on these development trends, mechatronic systems within automotive engineering are gaining more and more importance. At the same time, quality and safety requirements become challenging for automotive manufacturers as well as their suppliers regarding the reduction of the initial risk and increase of component reliability in a high degree. Therefore, safety-relevant aspects in the development of modern mechatronic systems have to be considered thoroughly. The high number of technical properties and complex connections of mechatronics systems in the development of modern vehicles are very challenging for state-of-the-art analysis methods. For this reason, new and innovational safety concepts are required to optimize existing safety concepts using conventional components and methods in combination.*

*This paper includes a detailed comparison of different analysing methods to identify systematic and random failures, as well as safety standards such as IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems) and ISO 26262 (Road vehicles – Functional safety). To fulfil safety standards nowadays for complex mechatronic systems, several different analysis methods have to be applied. Only the connection of a safe fault recognition with a safe fault reaction enables a system to avoid harmful consequences. Regarding product development, there is an ongoing change from routine tests (durability tests) to testing selected parts of a safety function (fault injection tests). How action is taken is changing, with a trend towards a further development of IT tools, supporting functional safe systems holistically, including hazard analysis and risk assessment, integrated system analysis of systematic and random failures, and hardware metrics. The publication closes with an overview of a functional safety concept and presents an outlook to future trends of safety systems analysis*

***Keywords:*** *Failure Mode and Effects Analysis FMEA, Fault Tree Analysis FTA, IEC 61508, ISO 26262, Automotive Safety Integrity Level ASIL, Fail-Operational, Automotive Mechatronic Systems, Drive Architectures.*

## 1. Introduction

The increasing amount of electronic components and use of electro-mechanical actuators in the automotive sector raises reliability and system integrity needs. As removing mechanical back-up systems is more and more considered, safety related electronic structures must be designed to work under any circumstances. As failure rates for electronic components are higher than for mechanical ones, the skill lies in creating reliable structures out of less reliable elements. Redundancy in software and hardware are the keys to overcome reliable products from single point failures. A combination of these approaches allows a creation of a structural design, which can deal with a restricted number of failures [1].