Safety as Service: Service Oriented Architectures for safety-critical Systems

One of the major issues in the automotive industry is the constant growing complexity of E/E (Electrics/Electronics) systems and the thereof resulting fault propagation due to the strong interconnection of the systems. The area of *functional safety* is concerned with the prevention of non tolerable risks in event of error. This is conducted by identifying possible hazards, estimating the potential risks and developing necessary countermeasures, based on these investigations. The requirement therefore is an accurate and thorough comprehension of the observed E/E system.
Thus, this Bachelor's thesis focuses on *functional safety* and *fault tolerance* concepts in *Service-oriented Architectures*. The first part of the work will concentrate on literature review and investigation of existing safety ensuring systems. On this basis it shall be defined what *Safety as a Service* can mean in general and how non-tolerable risks are preventable at different levels of abstraction, in order to meant with the requirements specified in ISO 26262. This is an ISO standard for safety-critical E/E systems in vehicles with a maximum gross weight of 3500 kg.
Although the research was done on basis of an automotive standard, the same overall concepts may apply for other safety-critical industries, such as aviation.