Safety-oriented Modular Function Deployment

Abstract:

While markets demand for individual products, the importance of safety also continuously increases. Modularization methods are a common approach, but they mainly focus on technical dependencies or other module drivers. From a safety perspective, this leads to non-optimal module concepts, which further increase the efforts connected to safety. To avoid this, safety aspects should be better considered. Thus, this paper presents the safety-oriented Modular Function Deployment (sMFD), which integrates safety aspects in a modularization method. It aims to develop safety-oriented module concepts. Hence, sMFD contributes to a shift of safety considerations to early stages of design and supports the evaluation of alternative concepts. The paper analyses existing modularization methods and assesses their suitability. MFD is identified as most suitable and adapted to support the safety-oriented modularization. Therefore, safety aspects (e.g., safety integrity levels or classes of safety requirements) are defined as module drivers. The resulting sMFD is applied and evaluated in two industrial case studies.