Simulation for verification and validation of functional safety

Lars Mikelsons Zhou Su
Bosch Rexroth AG
Rexrothstr. 3, 97816 Lohr am Main

Safety of machinery is the most critical issue in the design of mechatronic systems. The verification and validation procedure for functional safety of machinery is thoroughly discussed in ISO 13849-2. Following this procedure, the system behavior in case of a component failure has to be analyzed. Up to now this analysis bases on expert knowledge and real experiments. In this contribution a simulation based approach is presented. This approach has several advantages over the state-of-the-art. First, real experiments are more time consuming and costly than simulation. Moreover, according models can be used for further investigations like optimizing the sensor setup.
To enable failure simulation as a substitute of testing on real machinery for validation of functional safety, typical hydraulic failures are added to safety-related components of an in-house Modelica hydraulics library. This library is then used for the verification and validation of functional safety of a hydraulic test bench. Moreover, error propagation is considered.

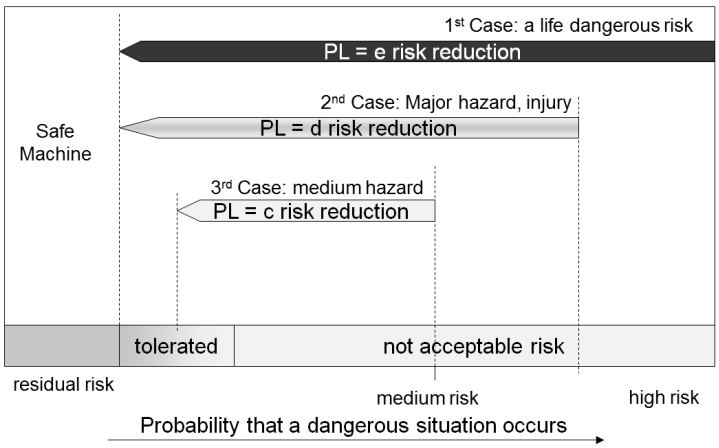

Figure 1: Principle of the risk reduction by the safety function