In this paper, the current situation of how PLC software is tested in industry is analyzed and the challenges on new testing approaches are identified using real industry code and a survey conducted within industry. The different possible and most relevant faults that may occur and must be dealt with are identified and requirements for testing approaches concerning component failures are derived. Further on, an approach to generate tests for error handling routines, which test the reliability of plants by injecting the corresponding faults is presented. The test cases are generated from timing sequence diagrams in combination with Failure mode and effects analysis. In order to inject the faults at relevant points during the execution of the control software, IEC 61131-3 code is analyzed for the derivation of the test cases.
entries: