Hardware-Centric Modular Framework for Continuous Testing of Autonomous Cyber-Physical Systems

Abstract

Cyber-Physical Systems (CPS) are increasingly finding their way into society, for example in transportation, smart buildings, drones and robots. It is a commonly known challenge to test CPS, as they take input from sensors and can operate in an unconstrained environment, which is difficult to simulate in tests in a constrained environment. Disturbances from either the environment or internal errors can potentially cause an undesirable behaviour of the CPS that cannot be accepted. The presented research addresses this specific problem within electromagnetic interference (EMI), and deals with improving electromagnetic compatibility (EMC) for CPS including but not limited to autonomous Unmanned Aerial Vehicles (UAV)s. It is our thesis that by using Field-Programmable Gate Arrays (FPGAs) as an embedded device for field tests, we can record logic-level disturbances in internal communication links of CPS caused by EMI from both the environment and from immunity tests, and that we can test software fault-tolerance by injecting these recordings into a data stream of an active communication link to the control unit in real-time.

The work is based on a novel methodology named Hardware-based EMI Injection for Software Testing (HEIST). HEIST comprises a framework for testing and for collecting data in order to substantiate the thesis. HEIST has been experimentally evaluated in comparison with a test using real EMI burst noise, and the fault rate in transmissions showed an almost identical fault rate. Moreover, HEIST has been used in two experiments recording disturbance in communication links on a UAV. First, using a professional EMC test facility, the grounded UAV has been exposed to noise from three different sources: electrostatic discharge (ESD), induction, and radiation. The experiment showed that HEIST was able to record noise from all tests. Second, using an airborne UAV physical contact was established with a 400 kV overhead power line. When the UAV approaches the power line arc discharges occur because of the voltage potential difference. HEIST was in this experiment used for recording disturbances in internal communication lines on the UAV caused by these arc discharges. These recordings can be used as fault injection and test for reliability of the UAV for flight operations near power lines without the need to enter the harsh environment.