Hardware-centric Modular Framework for Continuous Testing of Autonomous Cyber-physical Systems

PhD student: Martin Skriver, maskr@mmmi.sdu.dk
Principal supervisor: Assoc. Prof. Anders Stengaard Sørensen, anss@mmmi.sdu.dk; Co-supervisor: Assoc. Prof. Ulrik Pagh Schultz, ups@mmmi.sdu.dk

Background

Autonomous cyber-physical systems controlling high-risk operations require a high level of robustness to avoid instability in case abnormalities occur in peripherals. Drone systems in particular require a high level of robustness to minimize the probability of hazards: In the near future they will be used in high-risk tasks where losing control can have catastrophical consequences. It is crucial to create a method for measuring how robust these systems are and define what system parts need improvements for these flight operations to be carried out safely.

Knowing the behavior of a system for all types of errors could contribute to a measure on how robust a system is. This knowledge can be used by developers to create safer autonomous cyber-physical systems by creating systems that are able to detect if received data is corrupted or faulty, thus preventing them from responding incorrectly to the data and instead handle the specific error.

Mission

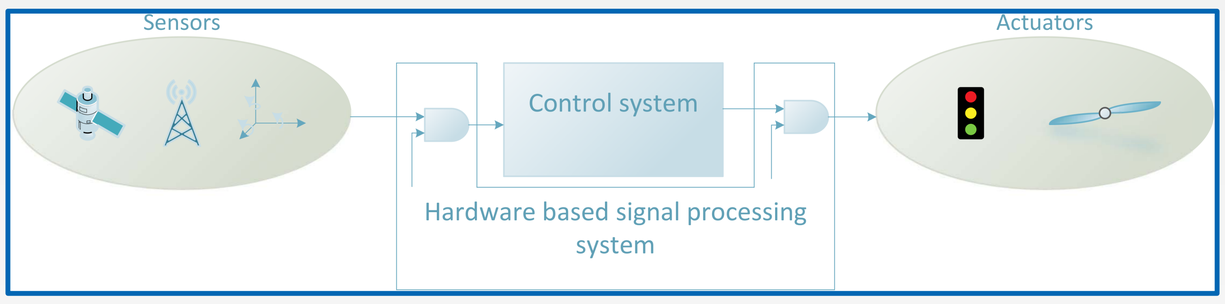
To **create technology** that by applying a **systematic in-flight test** quantifies robustness against foreseeable internally and externally caused errors in flight controllers.

Experimental setup

Development of a **generic hardware platform**, based on modular **programmable electronics**, enabling the possibility of **manipulating signals** going between sensors and controller, and controller and actuators, of cyber-physical systems. The signals can be manipulated in the **digital and the analog domain**, extending the possibilities of testing scenarios in the physical layer and the application layer of the tested control system.

Method of testing from the proposed modular test bench:

- **Error injection** [1]**.**
- **Hardware-in-the-loop simulation** [2]**.**
- **In-flight test.**



An example of usage of the test bench is to measure control system behavior in case of injecting:

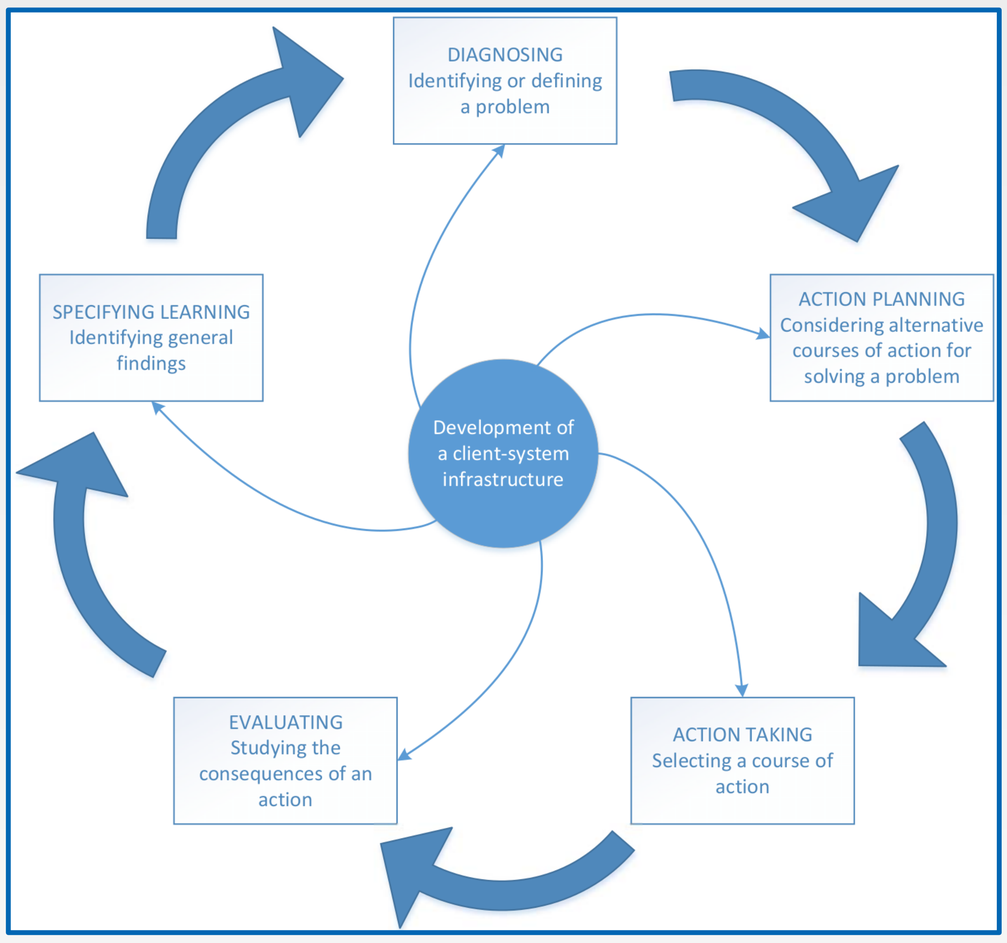
- **Faults in redundant systems.**
- **Noise errors on sensors.**
- **Change of actuator power.**

The test setup allows replacing peripheral systems e.g. radio, sensors and actuator with a PC-driven simulation environment. This makes it possible to do the same test in a virtual setup before field testing to spare time and costs of damaged equipment.

A key feature of this platform is that the control system being tested must undergo a minimum of changes, as it is crucial for the validation that no error sources are added from the test. The control system software is therefore the original and the electronics undergo minimal modifications. A significant part of the project is therefore to develop the generic test bench in such a way that added error sources are limited.

Methodology

The research methodology is inspired by Susmans' definition of **action research** [3]. This is an **iterative process** solving one problem per iteration. An iteration consist of identifying a problem, planing and taking action, evaluation and identifying outcomes. This method have been preferred because of the flexibility it adds in terms of getting results fast and it gives the **possibilities of collaborating** with other research projects.



In this project, a cycle of the iterative process is to:

1) Identify an abnormal peripheral behavior.
2) Plan and prepare a test method with injection.
3) Perform simulation and field testing.
4) Post processing on measured data.
5) Identifying findings and dissemination of result.

Each iteration will improve the client system, which in this case is a system that measures the robustness of cyber-physical systems, and give a more extensive and reliable test method.

Iterations should continue until the relevant cases have been covered. For this project and with the timeline considered, the tests will focus on a narrow subset e.g. adding noise and testing functionalities of redundant systems.

SDU

UAS CENTER

References

[1] Mei-Chen Hsueh, Timothy K. Tsai, and Ravishankar K. Iyer., Fault Injection Techniques and Tools, Computer vol 30, 1997, pp. 75-82.

[2] T. Shih and H. Chang, FPGA based hardware in the loop test platform of small size UAV, IEEE International Symposium on Computational Intelligence in Robotics and Automation - (CIRA), Daejeon, 2009, pp. 551-556.

[3] Susman, Gerald I., and Roger D. Evered. "An Assessment of the Scientific Merits of Action Research." Administrative Science Quarterly, vol. 23, no. 4, 1978, pp. 582–603