Contents

1. Introduction **1**
- 1.1. Motivation . . . 1
- 1.2. Problem Statement . . . 2
- 1.3. Research Questions . . . 2
- 1.4. Hypothesis . . . 3
- 1.5. Objectives . . . 3
  - 1.5.1. General Objectives . . . 3
  - 1.5.2. Specific Objectives . . . 3
- 1.6. Contributions . . . 3
- 1.7. Publications . . . 4
  - 1.7.1. Scientific Journals (ISI) . . . 4
  - 1.7.2. International Conferences and Workshops . . . 4
- 1.8. Outline of the Thesis . . . 4

2. Conceptual Framework **5**
- 2.1. Fundamental Concepts . . . 5
  - 2.1.1. CubeSats . . . 5
    - 2.1.1.1. System's Communication and Operation . . . 6
  - 2.1.2. Testing Techniques in CubeSats' missions . . . 6
    - 2.1.2.1. Hardware in the Loop Simulation . . . 6
    - 2.1.2.2. Software in the Loop Simulation . . . 7
- 2.2. State of the Art . . . 8
  - 2.2.1. CubeSats' software design . . . 8
  - 2.2.2. CubeSats' testing techniques . . . 9
  - 2.2.3. Fuzz Testing in Other Contexts . . . 11

3. The SUCHAI Flight Software **12**

4. Fuzz Testing **16**
- 4.1. Fuzz Testing in the SUCHAI Flight Software . . . 16
- 4.2. Strategies . . . 17
- 4.3. Execution . . . 19

5. Results **21**
- 5.1. Experiment execution results . . . 21
- 5.2. Experiment replications results . . . 24
- 5.3. Failures Fixing and Characterization . . . 24
- 5.4. Fuzzing Into a Continuous Integration System . . . 27

6. Discussion **30**
6.1. Threats to validity . . . 30
6.2. Applicability to Other Architectures . . . 31
6.2.1. Experiments . . . 33
6.2.1.1. Star Tracker . . . 33
6.2.1.2. OBC . . . 34
6.3. Applicability to Other Missions . . . 34
6.3.1. F Prime . . . 35
6.3.1.1. Preliminary Experiments . . . 38

7. Conclusions **40**

8. Future Work **42**

Bibliography **43**

Appendix A. Fuzzing the SUCHAI Flight Software **46**

Appendix B. Fuzzing the FPrime Software **53**