DSVerifier-Aided Verification Applied to Attitude Control Software in Unmanned Aerial Vehicles (Journal-First Presentation)

Lennon Chaves, Iury Bessa, Hussama Ismail
Federal University of Amazonas
Manaus, Brazil

Adriano Frutuoso
Federal Institute of Amazonas
Manaus, Brazil

Lucas Cordeiro
University of Manchester
Manchester, United Kingdom

Eddie de Lima Filho
TPV Technology
Manaus, Brazil

***Abstract*—The present study proposes the application of a bounded model checking tool, named as Digital System Verifier (DSVerifier), to the verification of digital-system implementation issues, in order to investigate problems that emerge in digital controllers designed for UAV attitude systems. Experimental results show that low-level failures in UAV attitude control software used in aerial surveillance are identified by DSVerifier, which can also be used for developing sound and correct implementations, through its integration into development processes. Finally, given that the proposed approach handles C source code and takes into account hardware specifications, it is suitable for verifying final controller implementations, which is a more practical scenario.**

***Index Terms*—Unmanned Aerial Vehicle, Symbolic Model Checking, Fixed-Point Digital Controllers, Formal Verification.**

I. Overview

Formal methods have been important in the development of more reliable UAVs. This paper proposes the application of DSVerifier for verifying UAV attitude control software, while considering hardware constraints. In addition, our experimental results [1] show that digital controllers might present failures after their implementation, depending on the chosen numerical format and realization. In particular, DSVerifier can identify LCO and overflow in digital controllers designed with the Ziegler-Nichols tuning and also with the CEGIS-based approach, the latter via DSSynth [2]. Basically, DSVerifier receives an ANSI-C program with a digital controller implementation, *i.e.*, coefficients, fixed-point representation, and dynamical ranges, and then checks if a violation occurs, according to a given property to be verified.

Contributions. The main contribution of this study is the introduction of a verification method based on DSVerifier and also its theoretical foundations, which aims to investigate FWL effects in digital controllers developed for UAV systems. In particular, this research proposes a DSVerifier-aided verification methodology for UAV attitude control software that takes into account implementation aspects, whose non-observance may cause incorrect behavior. In addition, DSVerifier can detect issues related to arithmetic overflow in wrap-around and saturation modes and also check for round-offs errors, which could generate LCOs, *i.e.*, undesirable errors that UAV digital controllers are susceptible to. The proposed method substantially extends the one presented by Ismail *et al.* [3], and, specifically, its application to UAV attitude control is an important step towards safe and reliable avionics modules, which is crucial for navigation and positioning systems.

Experimental results. The resulting simulations showed that failures due to FWL effects caused significant changes in UAV attitude angles. Indeed, our method based on DSVerifier is repeated until a sound and non-fragile implementation is found. Consequently, a suitable combination of realization and numerical representation can be identified, regarding a digital attitude controller designed for a specific hardware platform. From our experimental results, we found that 28,6% of our controller implementations presented overflow, when checked by DSVerifier in wrap-around overflow mode (overflow violations were detected only in system outputs). In saturate mode, verification procedures failed for 38,1% of our controller implementations, which means that violations were detected in intermediate nodes. In LCO verification procedures, 34,5% of our controller implementations failed and 9,5% led to timeout. The large number of timeouts, regarding LCO verification procedures, are explained by the high-complexity algorithm employed for that, with non-deterministic initial states and inputs, in addition to variable oscillation periods. Besides, we have performed some additional tests to evaluate verification bounds regarding different values of k, which indicated that, as k increases, the number of timeouts also gets higher. Finally, when employing the k-induction approach, we have also identified the same errors found in our initial experiments, which were performed without that technique.

Availability of Data and Tools. Our experimental results are based on a real quadcopter attitude control system for aerial surveillance. All benchmarks, tools, and results mentioned here are available for downloading at http://dsverifier.org/.

References

[1] L. Chaves, I. V. Bessa, H. Ismail, A. B. dos Santos Frutuoso, L. Cordeiro, and E. B. de Lima Filho, "Dsverifier-aided verification applied to attitude control software in unmanned aerial vehicles," *IEEE Trans. Reliability*, vol. 67, no. 4, pp. 1420–1441, Dec 2018.

[2] A. Abate, I. Bessa, D. Cattaruzza, L. Chaves, L. C. Cordeiro, C. David, P. Kesseli, D. Kroening, and E. Polgreen, "Dssynth: an automated digital controller synthesis tool for physical plants," in *ASE*, pp. 919–924, 2017.

[3] H. Ismail, I. Bessa, L. C. Cordeiro, E. B. de Lima Filho, and J. E. C. Filho, "Dsverifier: A bounded model checking tool for digital systems," in *SPIN*, LNCS 9232, pp. 126–131, 2015.