TRANSACTIONS ON RELIABILITY

DSVerifier-Aided Verification Applied to Attitude Control Software in Unmanned Aerial Vehicles

Lennon Chaves, Iury Bessa, Hussama Ismail, Adriano Frutuoso, Lucas Cordeiro, Eddie de Lima Filho

Abstract—During the last decades, model checking techniques have been applied to improve overall system reliability, in unmanned aerial vehicle (UAV) approaches. Nonetheless, there is little effort focused on applying those methods to the controlsystem domain, especially when it comes to the investigation of low-level implementation errors, which are related to digital controllers and hardware compatibility. The present study addresses the mentioned problems and 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. A verification methodology to search for implementation errors related to finite word-length effects (e.g., arithmetic overflows and limit cycles), in UAV attitude controllers, is presented, along with its evaluation, which aims to ensure correct-by-design 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 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, Embedded Systems.

L. Chaves, H. Ismail, E. Lima Filho, and I. Bessa are with Graduate Program in Electrical Engineering, Federal University of Amazonas, Brazil. A. Frutuoso is with Federal Institute of Amazonas, Brazil. L. Cordeiro is with Department of Computer Science, University of Oxford. E-mails: {lennonchaves, iurybessa, hussamaibrahim}@ufam.edu.br, {adriano.frutuoso}@ifam.edu.br, {lucas.cordeiro}@cs.ox.ac.uk, {eddie_batista}@yahoo.com.br