Verifying Fragility in Digital Systems with Uncertainties using DSVerifier $v2.0$ (Journal-First Presentation)

Lennon Chaves
CESAR
Manaus, Brazil

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

Lucas Cordeiro
University of Manchester
Manchester, United Kingdom

Eddie de Lima Filho
TPV Technology
Manaus, Brazil

***Abstract*—We describe and evaluate novel verification procedures for digital systems with uncertainties, based on software model checking and satisfiability modulo theories, named as DSVerifier $v2.0$, which can check robust stability of closed-loop control systems w.r.t. FWL effects. In particular, we describe our verification algorithms to check for limit-cycle oscillations (LCOs), output quantization error, and robust non-fragile stability on common closed-loop associations of digital control systems (*i.e.*, series and feedback). DSVerifier $v2.0$ checks new properties of closed-loop systems (*e.g.*, LCO), including stability and output quantization error for uncertain plant models, and considers unknown parameters and FWL effects. Experimental results over a large set of benchmarks show that 35%, 34%, and 41% of success can be reached for stability, LCO, and output quantization error verification, respectively, for a set of 396 closed-loop control system implementations and realizations.**

***Index Terms*—Fixed-Point Digital Controllers, Formal Methods, Bounded Model Checking, System Reliability, Uncertainty.**

I. Overview

DSVerifier $v2.0$ [1] provides a formal framework that checks simultaneously fragility and robustness of digital control systems, while evaluating merit figures specific to digital systems, such as stability, limit-cycle oscillations, and output quantization error. In particular, DSVerifier $v2.0$ included novel verification methods w.r.t. its previous release [2], and it is now able to consider hardware implementation aspects during verification of closed-loop control systems, which consist of digital controller and uncertain plant models.

Contributions. We extended the previous work of Ismail *et al.* [2] (*i.e.*, DSVerifier $v1.0$) to enable closed-loop system verification in uncertain systems as follows:

- **Closed-loop System Verification -** DSVerifier $v2.0$ checks stability of closed-loop systems, considering FWL effects in controllers and plant models with uncertainties.
- **Stability and LCO -** DSVerifier $v2.0$ checks closed-loop systems w.r.t. stability and LCO occurrence, considering non-deterministic inputs and states.
- **Output Quantization Error -** DSVerifier $v2.0$ computes the output of a closed-loop control system, considers round-off and FWL effects, and compares it with an ideal response (*i.e.*, without FWL effects), in order to check whether the output error is inside tolerable bounds.
- **Support for CBMC -** DSVerifier $v2.0$ now supports two efficient software verifiers: ESBMC and CBMC.
- **Support for New SAT/SMT Solvers -** DSVerifier $v2.0$ now supports Yices, MathSAT, CVC4 by means of ESBMC, and MiniSat by means of CBMC, in addition to Boolector and Z3 by ESBMC.

Experimental results. Our experimental evaluation consists of a set of fourteen closed-loop systems, with different aspects of implementation, *i.e.*, fixed-point representation, realization form and uncertainty employed. For the stability verification, we found that 8 and 16-bits implementations produced more than 50% of unstable systems, while the same systems turned from failure to success when implemented in 32 bits of precision. In addition, we concluded if the implementations are combined with an uncertainty of 5%, failures are higher when compared with uncertainties of 0%, 0.5% and 1.5%, which states that the disturbance related to uncertanties indeed influences the system stability. In LCO verification, we noticed a reasonable amount of time, which was related to the system's order, and increased the model checking procedures. In addition, we concluded that the appropriate implementation should use DFII realization and 32-bit implementation to avoid LCO. From quantization error verification, 100% of our systems did not present quantization error for DFII realization with all bits implementation and all uncertainties levels, which means that the DFII realization is the most suitable to avoid output quantization error. Additionally, we were able to check that even for stable closed-loop systems, their implementations are still susceptible to FWL effects, i.e., they produce round-offs (limit-cycles) and output quantization error violation. Finally, greater number of bits is also desirable for any representation, because it helps mitigating FWL effects.

Availability of Data and Tools. Our experimental results are based on set of closed-loop systems benchmarks. All benchmarks, tools, and results of this evaluation are available for downloading at http://dsverifier.org/.

References

[1] L. C. Chaves, H. I. Ismail, I. V. Bessa, L. C. Cordeiro, and E. B. L.?Filho, "Verifying fragility in digital systems with uncertainties using dsverifier v2.0," *Journal of Systems and Software*, vol. 153, pp. 22 – 43, 2019.

[2] 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.