

ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA'17)



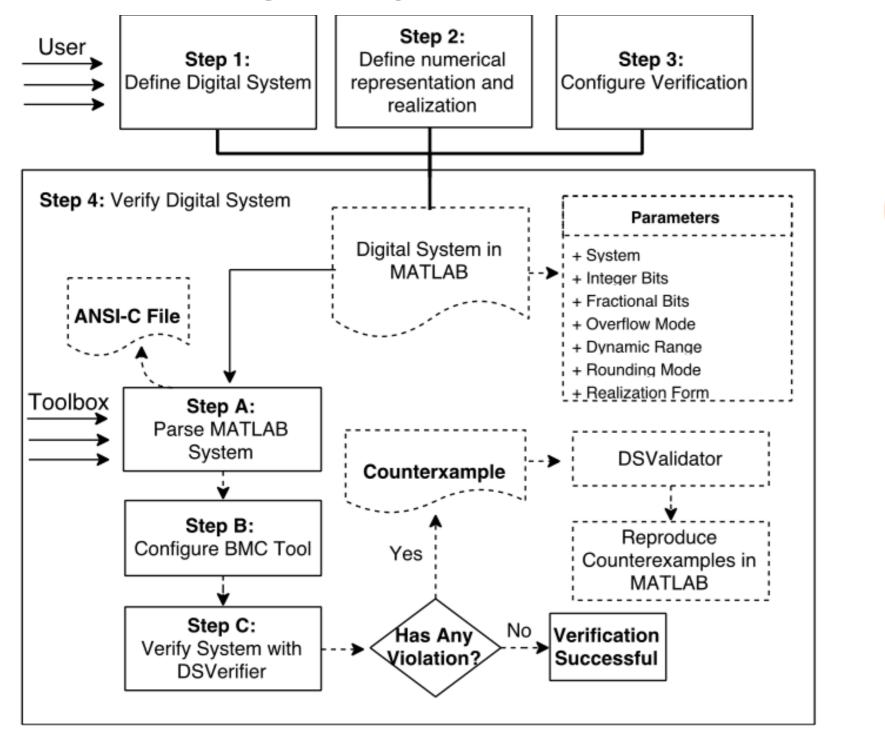
Verifying Digital Systems with MATLAB

Joint work with Lennon Chaves, lury Bessa, Daniel Kroening and Eddie Lima

> Lucas Cordeiro University of Oxford / DiffBlue lucas.cordeiro@cs.ox.ac.uk

diffblue Al for Code

DSVerifier Toolbox: BMC tool to check design errors in digital systems with MATLAB



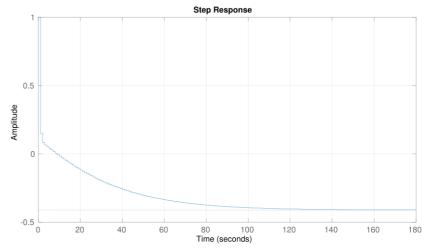
CBMC

ESBMC

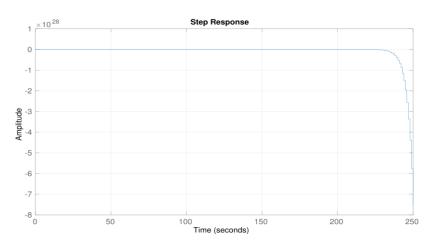
DSVerifier Toolbox: Illustrative Example

 The different numerical representations for a given digital system can yield different verification results

Transfer Function	Closed-Loop	State-Space	
Closed-Loop Representation			Implementation
Plant Numerator [1 -1 -2]			Integer Bits 13 + Fractional Bits 3 +
Denominator [1 1 0.5	0.576]		max range 1 — min range -1 —
Controller			Delta
Numerator [1 0.576 0.927]			Timeout 3600
Denominator [1 -4.867 0.736] Sample Time 0.02 Configurations			Realization Form DFII
			K bound 0 10 20 30 40 50 60 70 80 90 100
BMC ESBMC 🔻			Properties
Solver Boolector Overflow Mode Wrap-Around Rounding Mode Round Error Mode Absolute			 Stability Limit Cycle Quantization Error
			Reset Verify



successful verification: **stable** system using <2,13>



failed verification: **unstable** system using <13,2>