

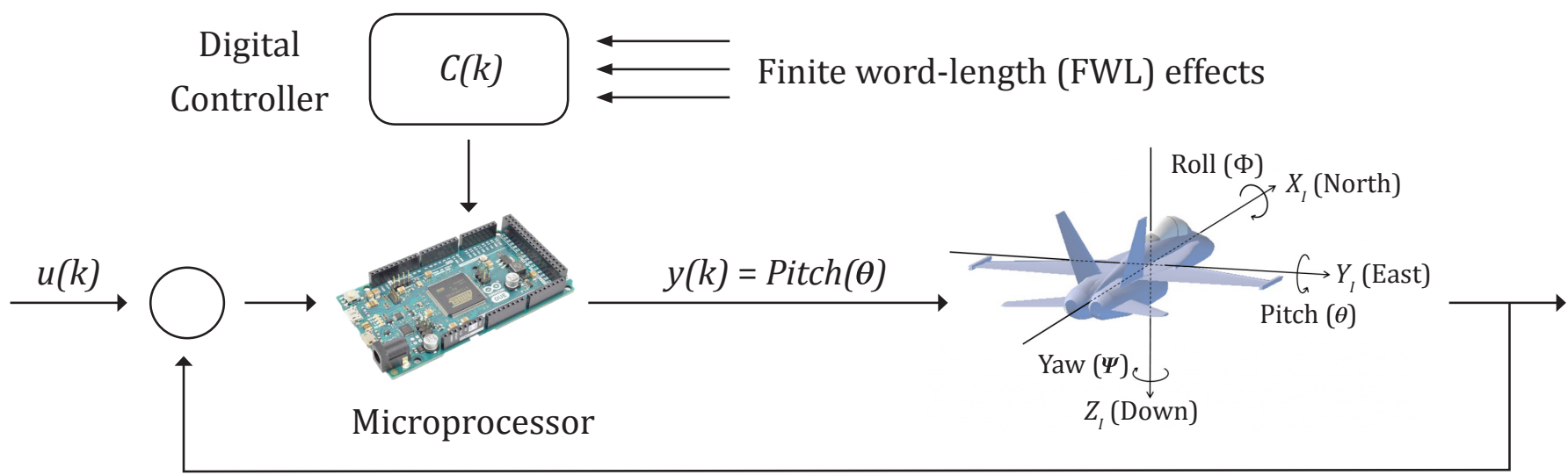
# Verifying Digital Systems with MATLAB (Tool Demo)

Lennon Chaves<sup>1</sup>, Iury Bessa<sup>1</sup>, Lucas Cordeiro<sup>1,2</sup>, Daniel Kroening<sup>2</sup> and Eddie Lima<sup>1</sup>

<sup>1</sup>Federal University of Amazonas, Brazil <sup>2</sup>University of Oxford, United Kingdom

lennonchaves@ufam.edu.br • iurybessa@ufam.edu.br • lucas.cordeiro@cs.ox.ac.uk • kroening@cs.ox.ac.uk • eddie\_batista@yahoo.com.br

## I Motivation



"...guaranteeing the correctness of cyber-physical systems (CPS) remains an a stounding challenge"

Xi Zheng *et al.*, 2014.

"Simulation alone is not sufficient to support verification and validation of CPS."

Sayan Mitra *et al.*, 2013.

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) \\ y(k) = Cx(k) + Du(k) \end{cases} \leftarrow \text{State-space model}$$

$$H(z) = \frac{b_0 + b_1z^{-1} + \dots + b_mz^{-m}}{1 + a_1z^{-1} + \dots + a_nz^{-n}} \leftarrow \text{Transfer-function model}$$

## Step A

DSVerifier builds an ANSI-C code representation of the digital system based on the specification.

## Step B

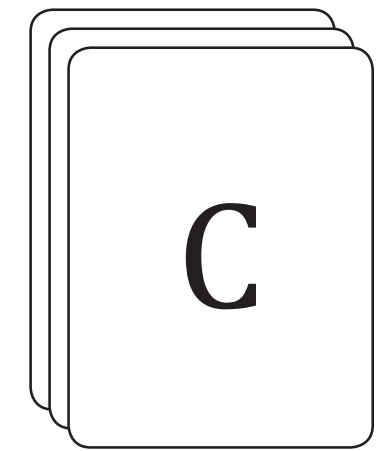
DSVerifier formulates a FWL model based on fixedpoint arithmetic:

$$\text{FWL } [\bullet]:\mathbb{R} \rightarrow \mathbb{Q}[\mathbb{R}]$$

## Step C

DSVerifier checks a property  $\Phi$  up to a bound  $k$ :

$\Phi$	Bits $\langle I, F \rangle$	Result
Quantization error	32-bits $\langle 15, 16 \rangle$	>1%
	16-bits $\langle 7, 8 \rangle$	>1%
	8-bits $\langle 3, 4 \rangle$	<1%
Stability	8-bits $\langle 3, 4 \rangle$	Unstable



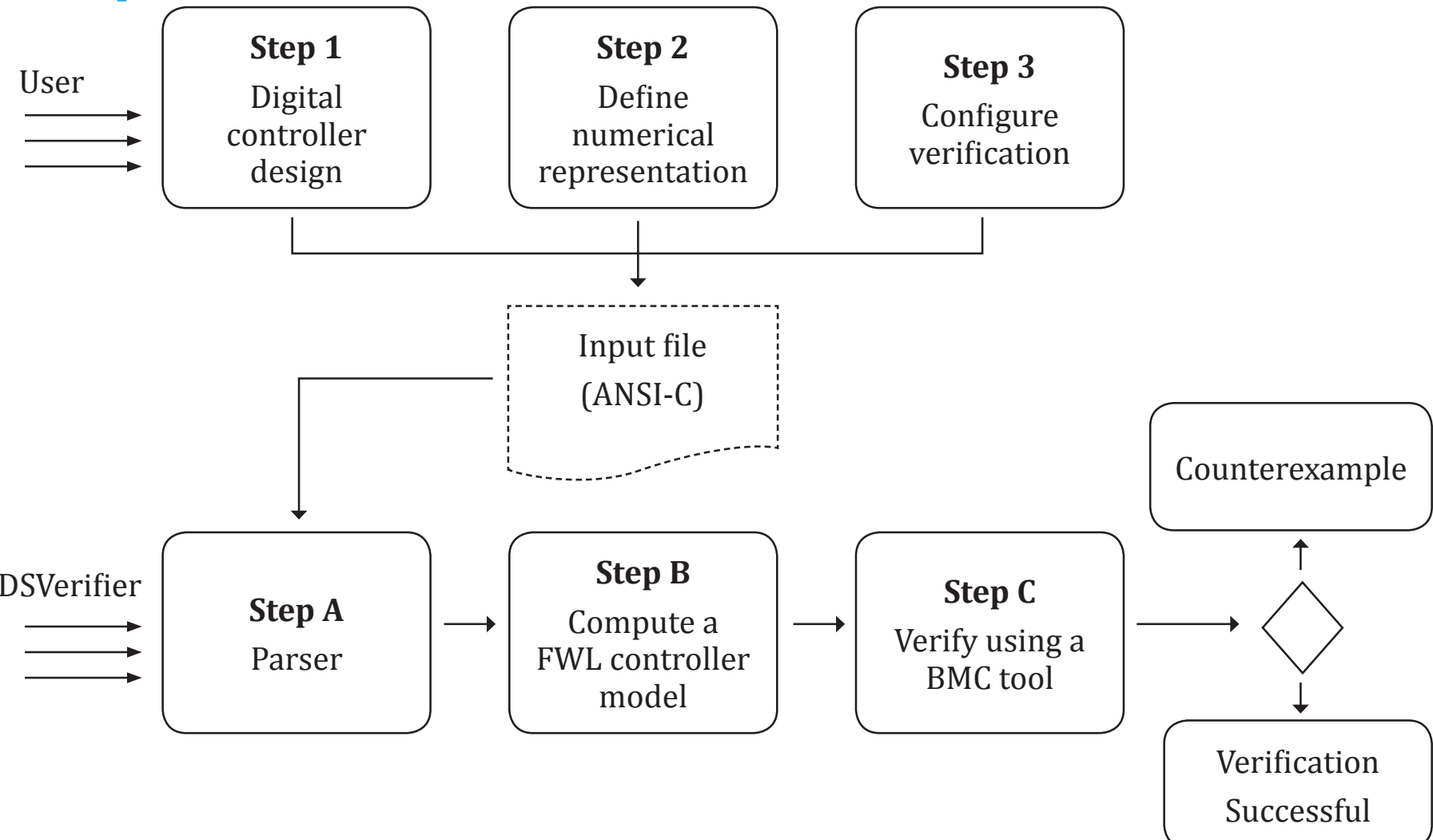
## II Approach and Uniqueness

Bounded model checking

Translate the model into a VC  $\psi$  such that:

$\psi$  is satisfiable iff  $\phi$  has counterexample of max. depth  $k$

### Step 1



$$\begin{cases} x(k+1) = \begin{bmatrix} 0.9969 & 0.05649 & 0 \\ -0.0001 & 0.99570 & 0 \\ 0 & 0.5658 & 1 \end{bmatrix} x(k) + \begin{bmatrix} 0.0024 \\ 0.0002 \\ 0.0001 \end{bmatrix} u(k) \\ y(k) = [0 \quad 0 \quad 1]x(k) + [0]u(k) \end{cases}$$

### Step 2

Numerical representation  $\langle I, F \rangle$ :

- $I$  is the integer part and
- $F$  is the fractional part

```
implementation <3,4>
states = 3;
inputs = 1;
outputs = 1;
A = [...];
B = [...];
C = [...];
D = [...];
```

### Step 3

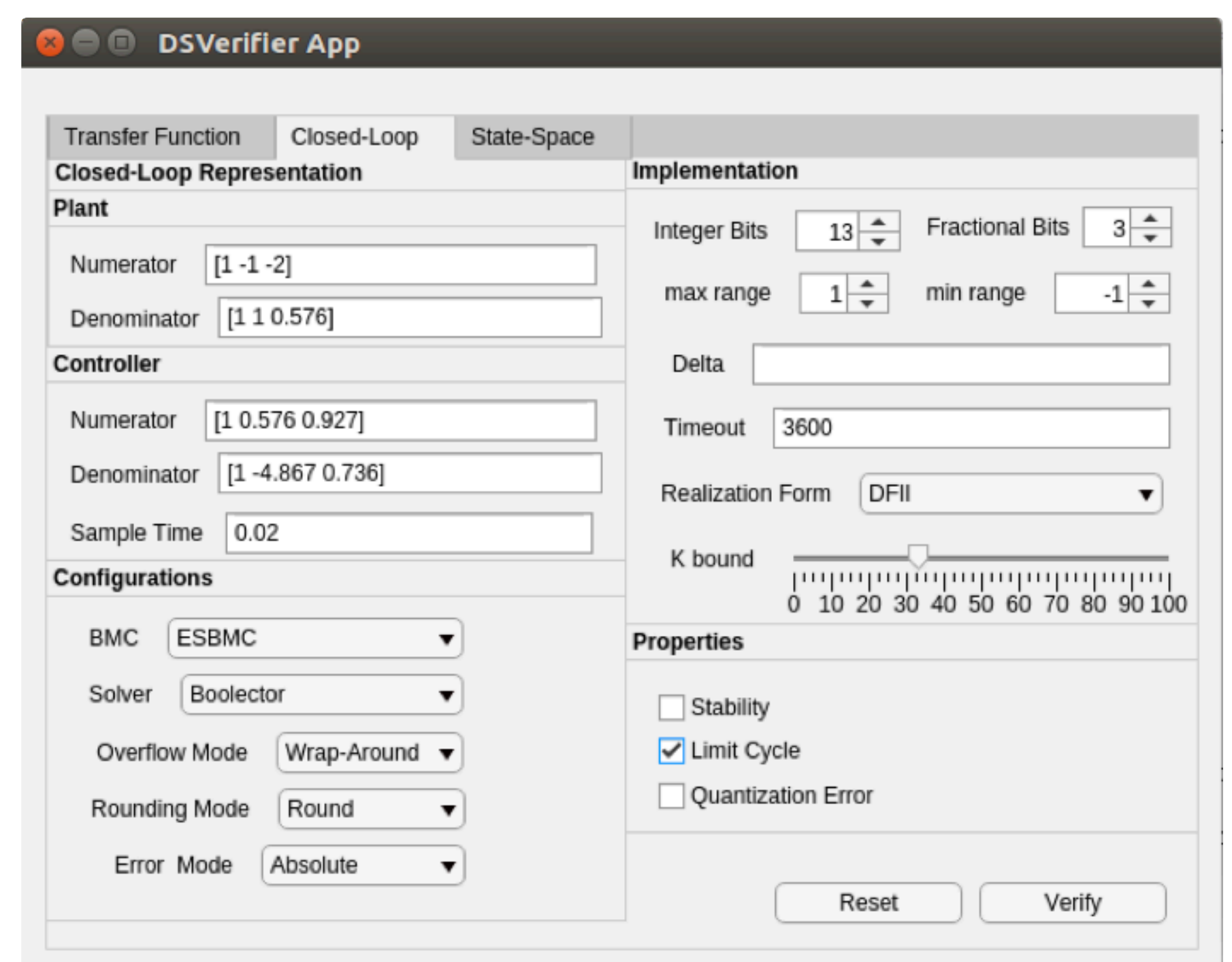
Setup verification:

- choose a property  $\Phi$ ;
- a maximum verification time;
- a bound  $k$ ;
- a BMC tool.

Properties:

- stability;
- quantization error;
- controllability;
- observability;

## III DSVerifier Toolbox



## IV Contributions

- support for transfer-function and state-space representations in open- and closed-loop form;
- verify different numerical representations and realization forms of digital systems;
- provide a MATLAB toolbox to check specific properties of digital systems while taking into account FWL;

As future work:

- verify uncertainties in digital systems represented by state-space;
- integrate counterexample reproducibility for digital systems

Sponsors:

