Computer Aided Formal Verification for Power Electronics Based Cyber-Physical Systems

UNIVERSITY OF TEXAS ARLINGTON

Omar Ali Beg • PhD student at University of Texas at Arlington, Electrical Engineering • omar.beg@mavs.uta.edu • Advisors: Dr. Taylor T. Johnson and Dr. Ali Davoudi

Motivation

Despite advancement in design verification and validation techniques, safety recalls of power electronics based CPS are frequent, e.g., recall of Toyota Prius cars due to error in interaction between its cyber component (software controller) and physical component (DC-DC power converter).

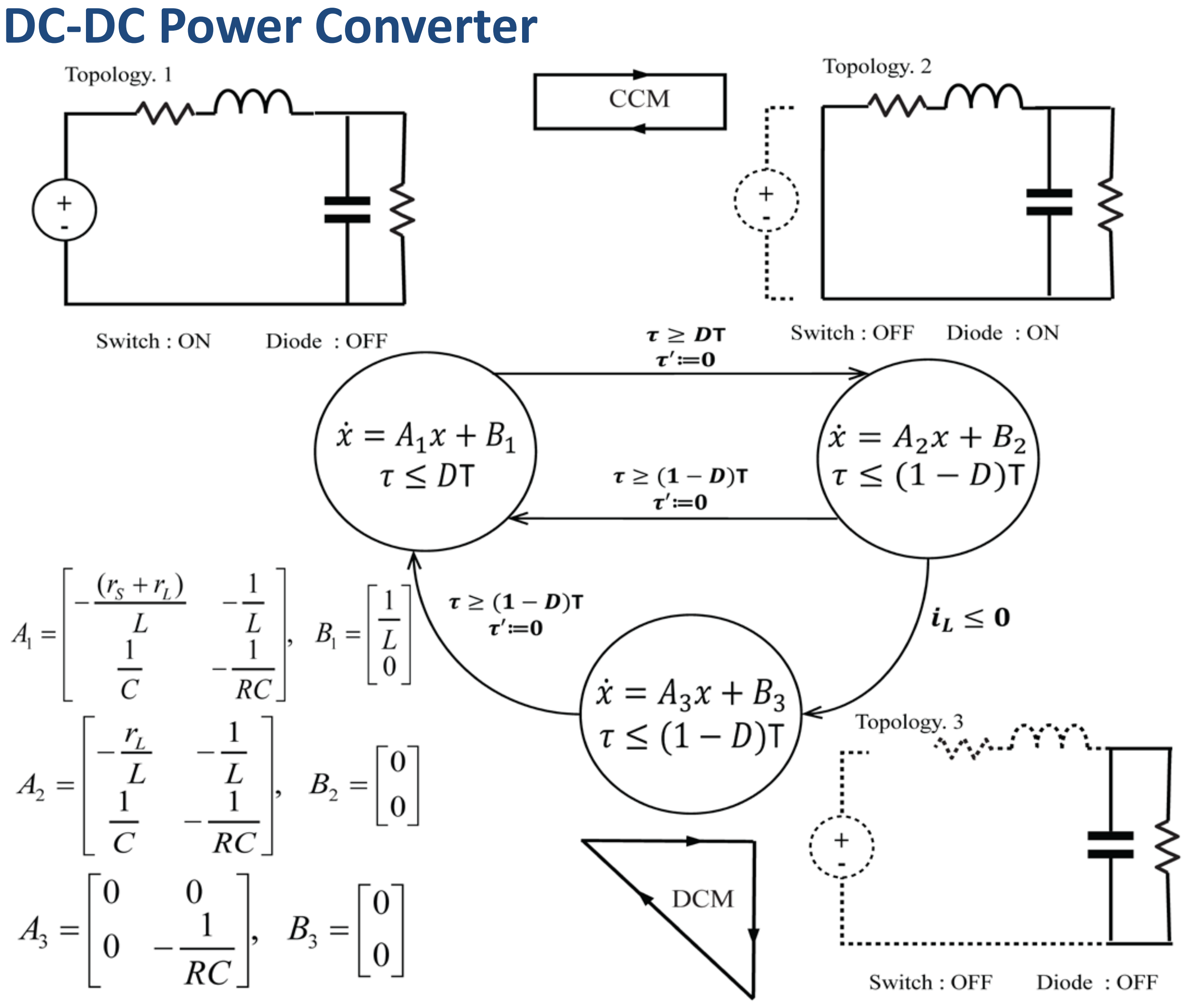
Selected Case Studies

- DC-DC Power Converter
- DC Microgrid (Future Work)

Approach

- Develop ODEs for each CPS & model non-determinism
- Construct hybrid automaton model
- Implement in Stateflow and SpaceEX
- Formally verify that the model does not violate a given stability specification
- Use reachability analysis for formal verification

DC-DC Power Converter



Modeling Non-determinism Using Interval Matrices

- For system of n variables, ith state is expressed as

$$\dot{x}_i = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{ij}x_j + \cdots + a_{in}x_n$$

- To model non-determinism, the intervals are used

$$\dot{x}_i \in \left[\underline{a_{i1}}, \overline{a_{i1}}\right] x_1 + \left[\underline{a_{i2}}, \overline{a_{i2}}\right] x_2 + \cdots + \left[\underline{a_{ij}}, \overline{a_{ij}}\right] x_j + \cdots + \left[\underline{a_{in}}, \overline{a_{in}}\right] x_n$$

- In midpoint-radius format

$$\dot{x}_i \in [mid(a_{i1}) \pm rad(a_{i1})]x_1 + \cdots + [mid(a_{in}) \pm rad(a_{in})]x_n$$

- Midpoints are the constant terms, so

$$\dot{x}_i \in a_{i1}x_1 + r_{i1} + a_{i2}x_2 + r_{i2} + \cdots + a_{ij}x_j + r_{ij} \ldots + a_{in}x_n + r_{in}$$

- Where the radius, r_{ij} is

$$r_{ij} = [-rad(a_{ij}), rad(a_{ij})]x_j$$

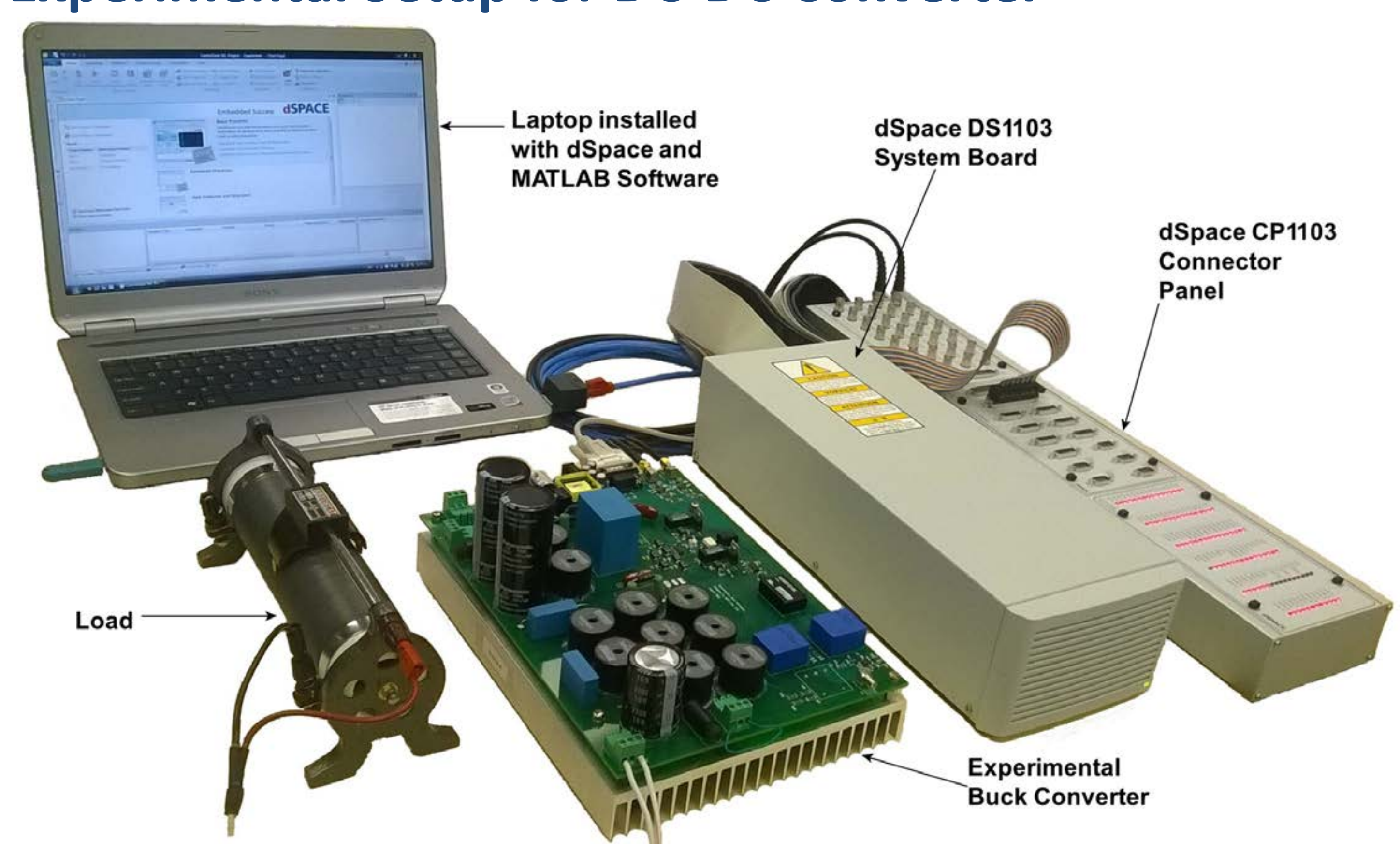
- Invariants are

$$-[-rad(a_{ij}), rad(a_{ij})]x_i \geq r_{ij} \leq [-rad(a_{ij}), rad(a_{ij})]x_i$$

Formal Specifications for DC-DC Converters

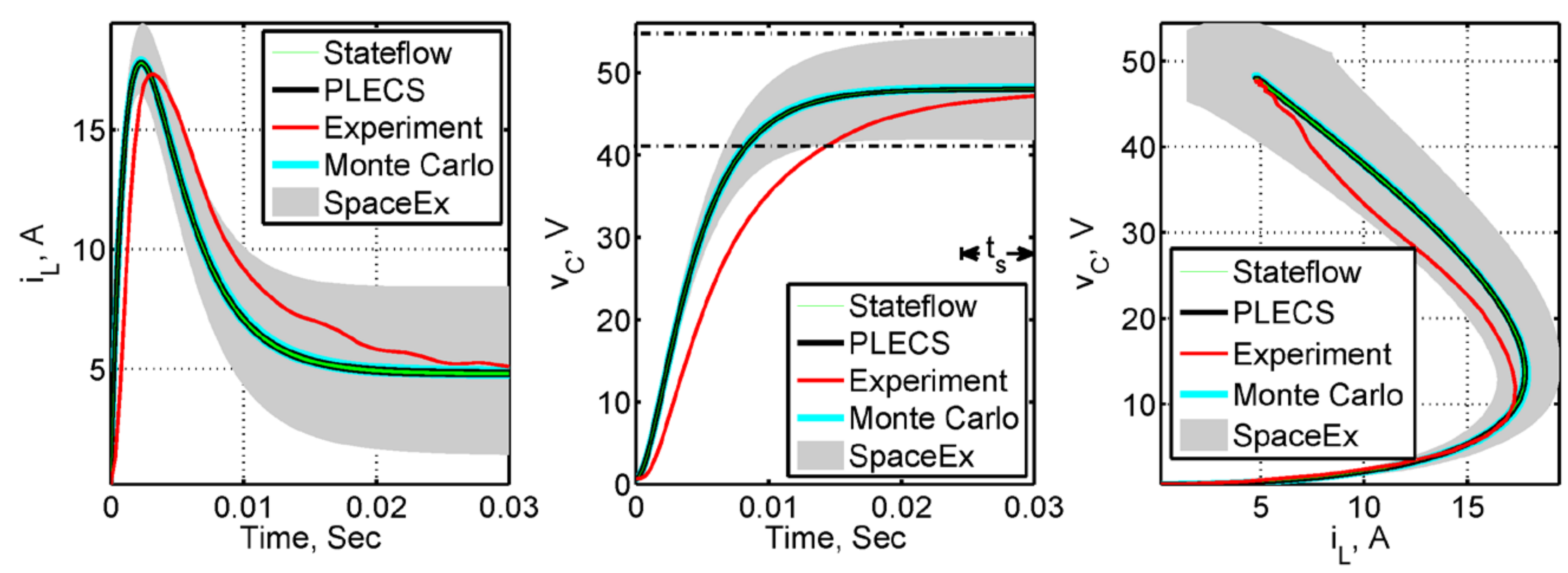
- Lyapunov stability: $\dot{x} = f(x(t))$ is stable if $\forall \epsilon > 0\ \exists \beta > 0$ such that if $\|x(0)\| \leq \beta \Rightarrow \|x(t)\| \leq \epsilon \forall t \geq 0$
- We define a bounded region and verify that the output eventually reaches and always remains there
- For startup time t_s, the output voltage $V_{out}(t)$ should remain bounded within a tolerance γ of the reference voltage $V_{ref}(t)$: for $t \geq t_s \Rightarrow V_{out}(t) = V_{ref}(t) \pm \gamma$
- For open−loop: $v_C(t) \in [41, 55]$ in steady state
- For closed−loop: $v_C(t) \in [9, 15]$ as $t \to \infty$

Experimental Setup for DC-DC Converter



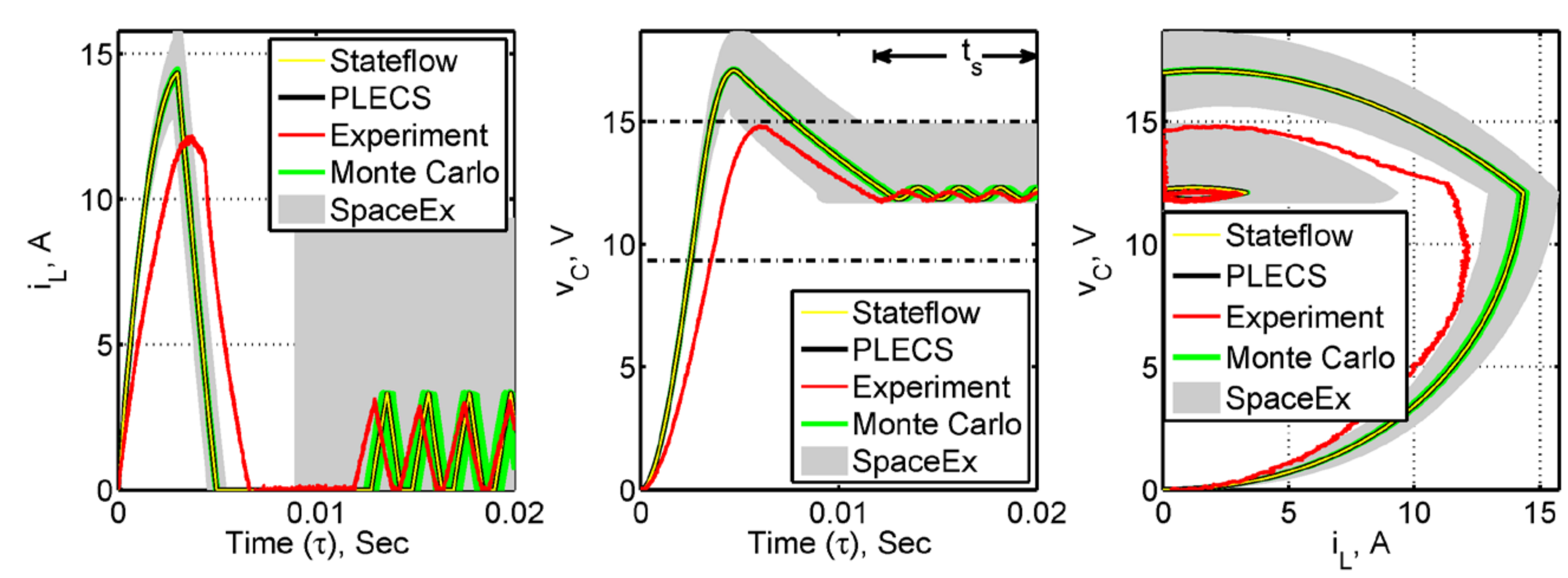
Experimental and Analysis Results

a. Open-loop DC-DC Converter



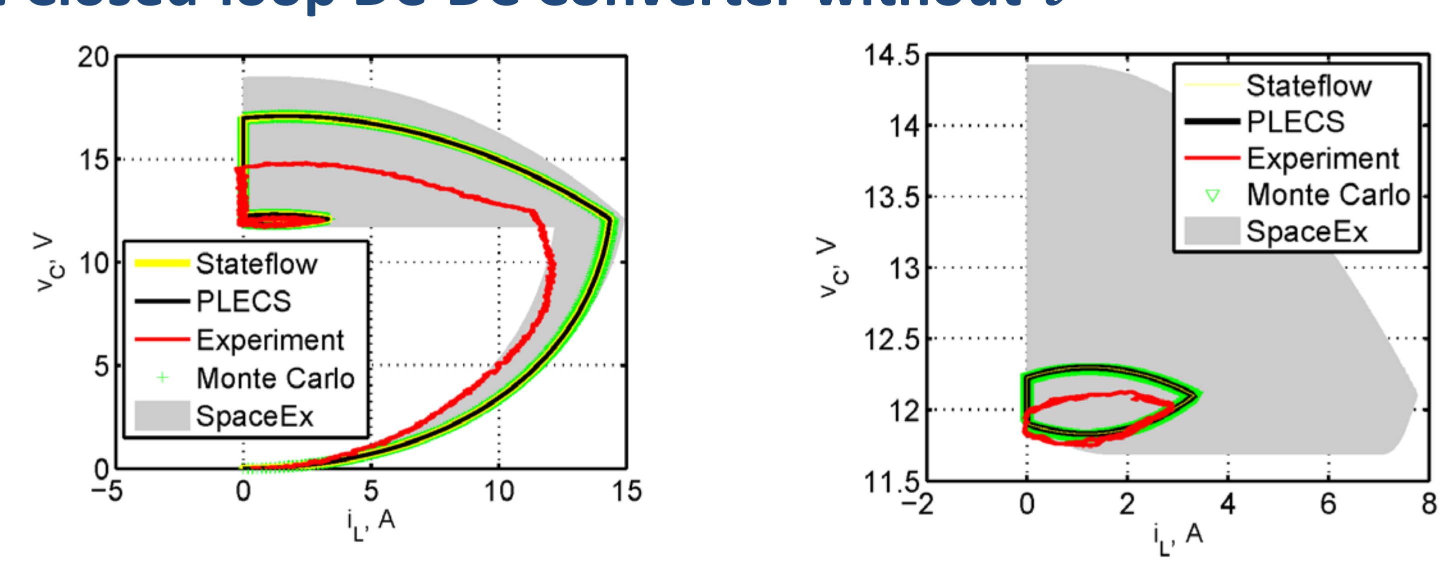
(a) Current vs. time (b) Voltage vs. time (c) Voltage vs. current

b. Closed-loop DC-DC Converter with τ



(a) Current vs. time (b) Voltage vs. time (c) Voltage vs. current

c. Closed-loop DC-DC Converter without τ



(a) Startup (b) Steady State

Future Work for DCPS – DC Microgrid