An Event-based Approach to Hybrid Systems Diagnosability

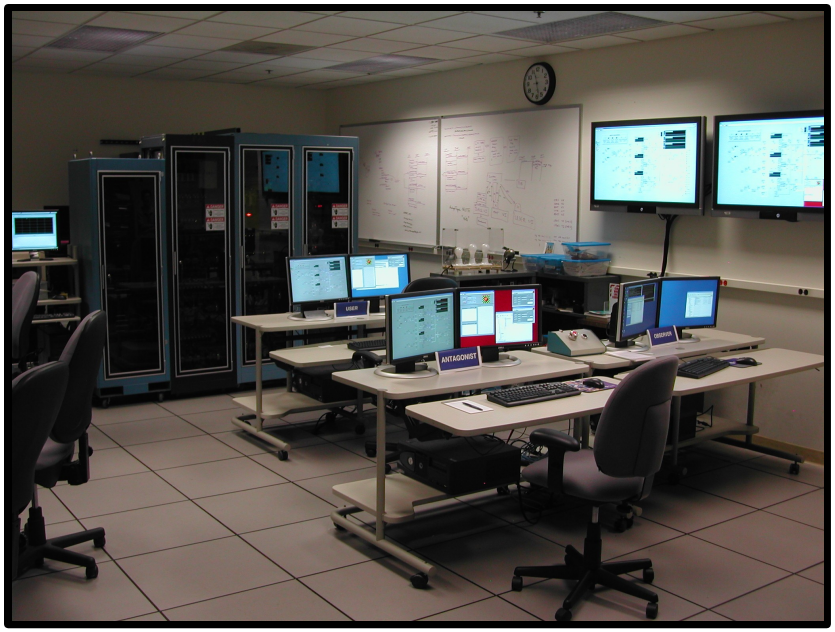
Matthew Daigle[1], Xenofon Koutsoukos[2], and Gautam Biswas[2]

[1] University of California, Santa Cruz,
NASA Ames Research Center, Moffett Field, CA, USA

[2] Institute for Software Integrated Systems/Department of EECS,
Vanderbilt University, Nashville, TN, USA

Motivation

- Many practical, modern engineering systems are **hybrid systems**
  - Mix continuous and discrete behaviors
  - Faults can be parametric (change in parameter) and discrete (change in mode)
- Diagnosability is a measure of ability to achieve unique diagnosis results
  - Definitions required for measurement selection task
  - Challenging in hybrid systems due to mode changes



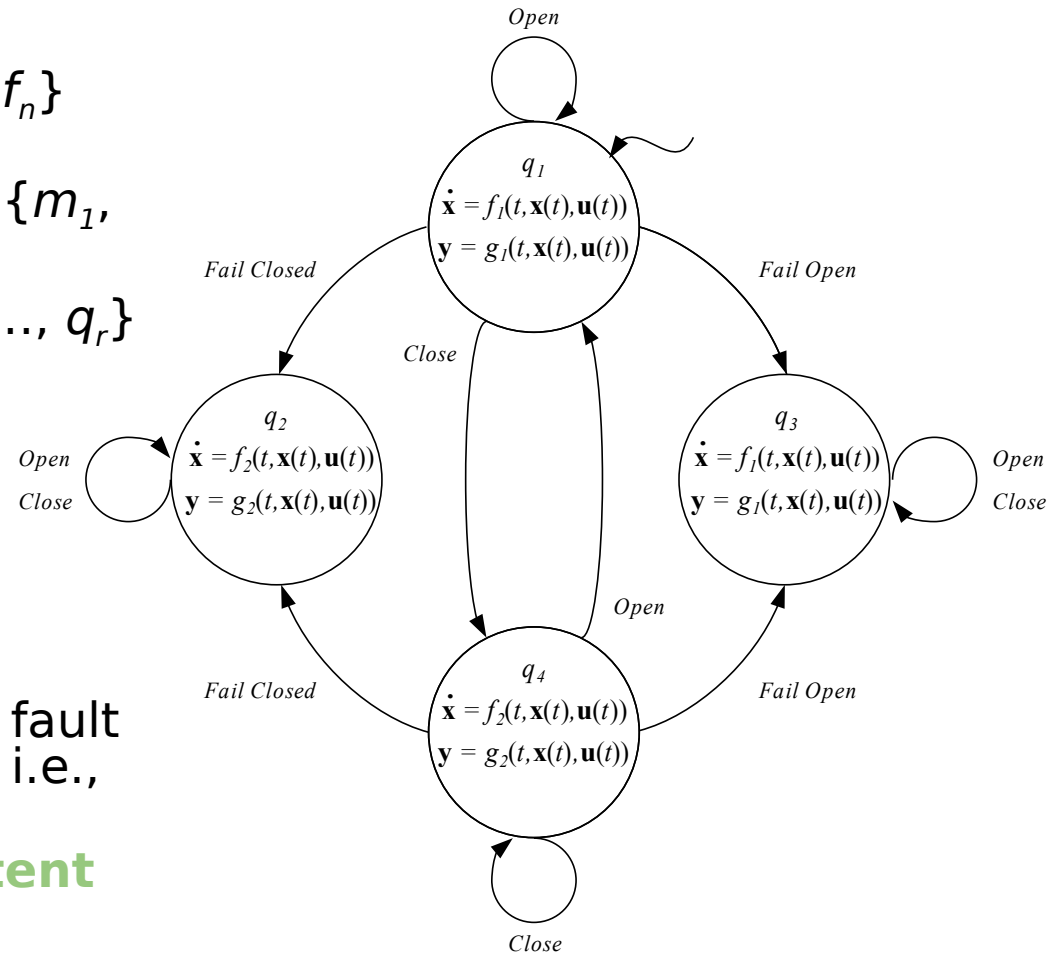
Advanced Diagnostics and Prognostics Testbed, NASA Ames

Outline

- Problem Formulation
- Diagnosis Architecture
- Modeling
- Diagnosis Using Transients
- Event-based Fault Modeling
- Candidate Languages
- Diagnosers
- Diagnosability
- Case Study: Advanced Diagnostics and Prognostics Testbed
- Conclusions

Problem Formulation

- Starting from hybrid system model
  - Set of faults $F = \{f_1, f_2, \ldots, f_n\}$ (events)
  - Set of measurements $M = \{m_1, m_2, \ldots, m_p\}$
  - Set of modes $Q = \{q_1, q_2, \ldots, q_r\}$
- Assumptions
  - Single faults
  - No autonomous mode changes after fault occurrence
- Terminology
  - Candidate = hypothesized fault and a hypothesized mode, i.e., $c = (f,q)$
  - Diagnosis = set of **consistent** candidates, e.g., $d = \{(f_1,q_1),(f_2,q_2)\}$

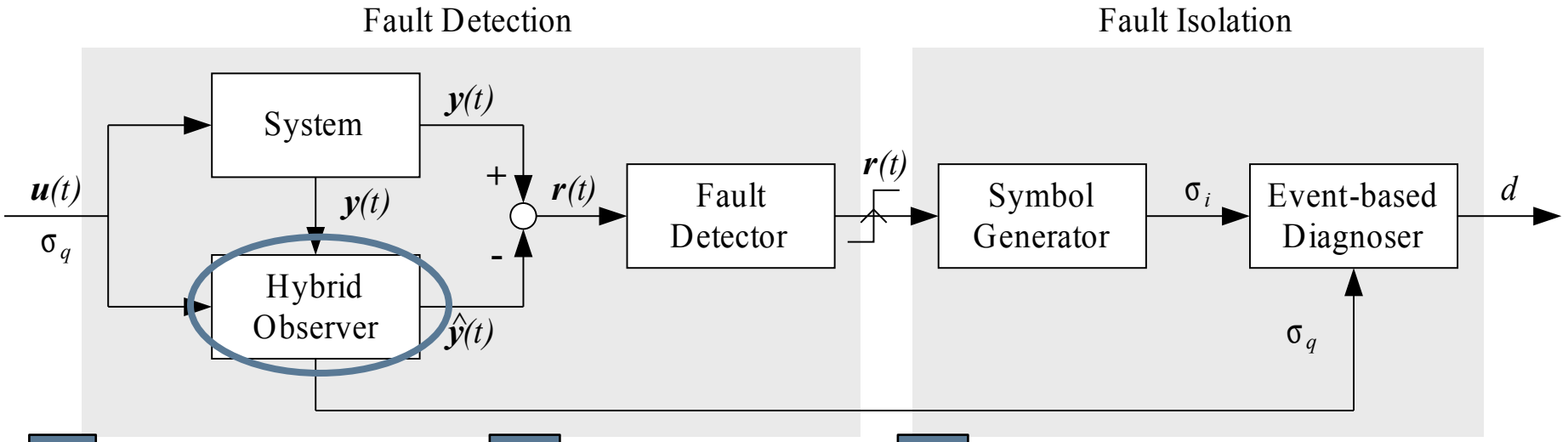


Diagnosis Architecture

2 Compute difference between estimated and observed outputs

4 Abstract deviations to qualitative +/- values

6 Isolate faults based on observed **sequence of events**



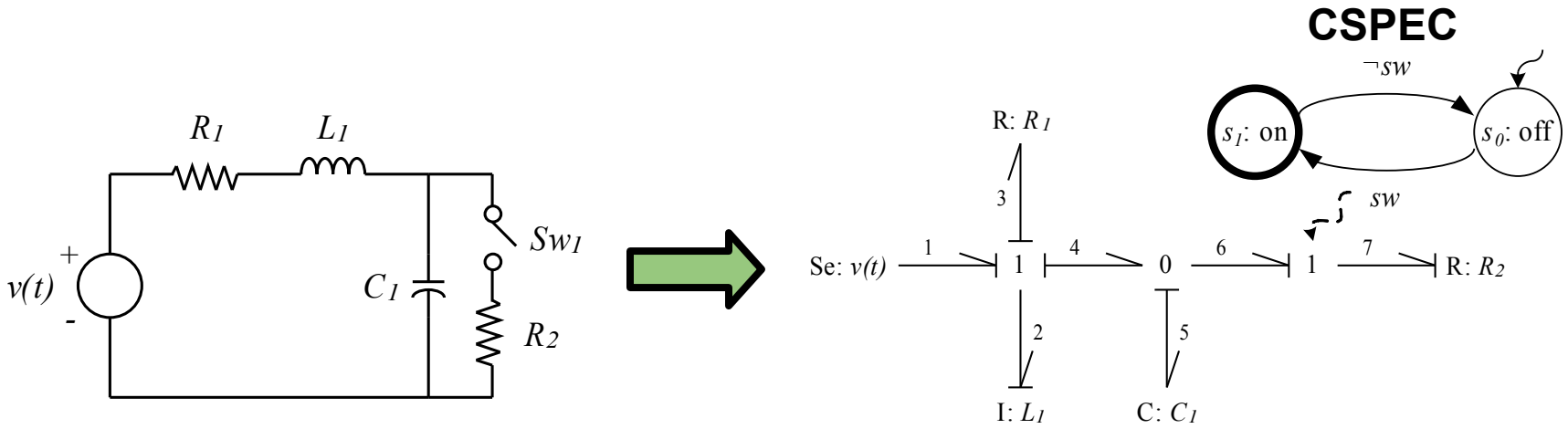
1 Track system behavior

3 Determine significant deviations

5 Measurement deviations or controlled mode change events

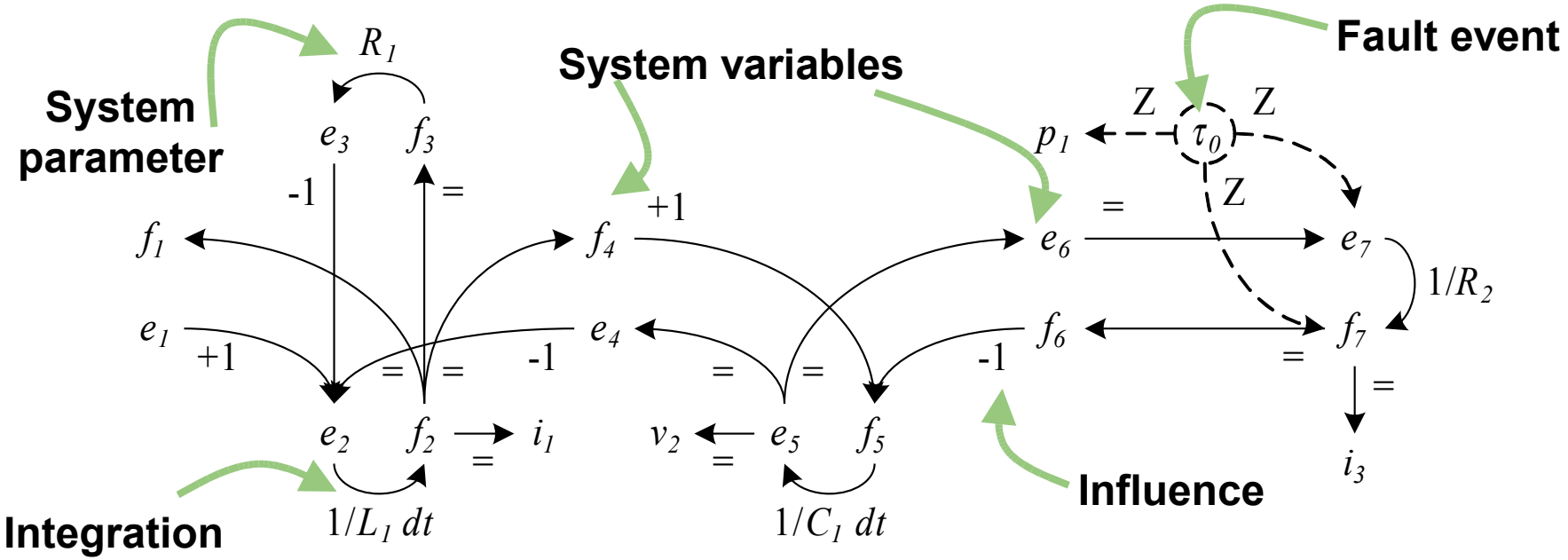
Modeling

- Hybrid bond graphs (HBGs)
  - Energy-based, topological, lumped parameter models
  - Ideal switching of energy connections through locally-defined automata termed **control specifications** (CSPECs)
- Modeling faults
  - Parametric faults captured as change in HBG element parameter (e.g., resistance change)
  - Discrete faults captured as fault events in CSPECs



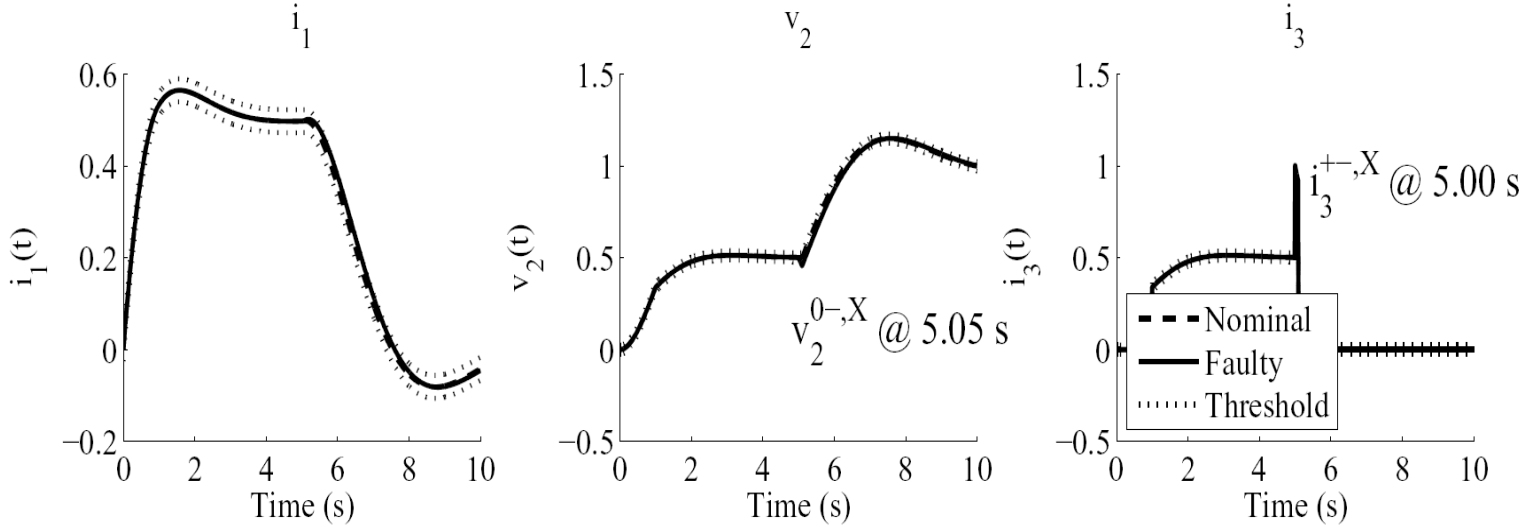
Temporal Causal Graphs (TCGs)

- Diagnosis model of our approach
- Derived automatically from HBG, for a particular mode
- Similar to signal flow graphs
- Causality represented by directional links
- Temporal relations (delays) captured by integration operators
- Allow automatic generation of **fault signatures** and **relative measurement orderings**



Diagnosis Using Transients

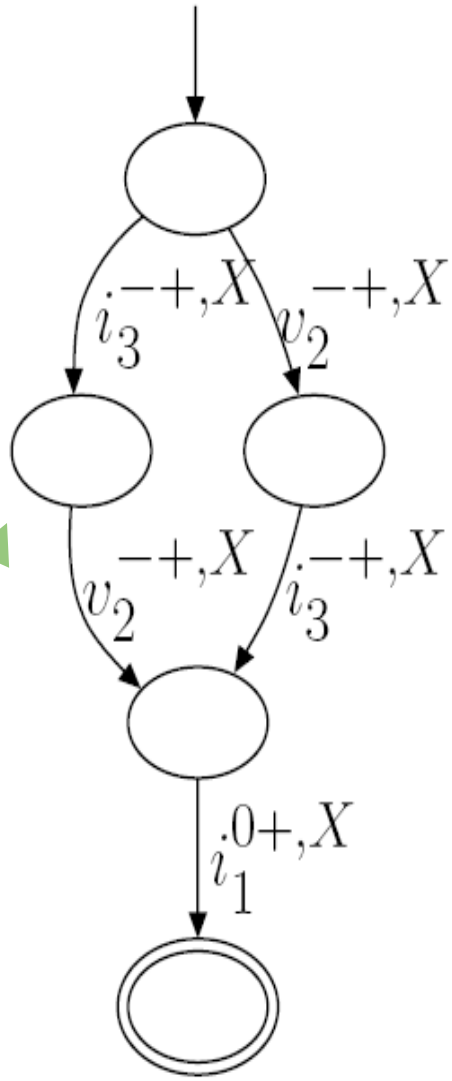
- Fault signatures
  - Effects of fault on measurements expressed as qualitative changes (+, 0, and -) in magnitude and slope of signal
  - Additional symbols for discrete behavior including nonzero to zero (Z), from zero to nonzero (N), or no change (X)
- Relative measurement orderings
  - Faults manifest in some measurements before others due to delays
  - If fault *f* manifests in m_1 before m_2, define as $m_1 <_f m_2$



Event-based Fault Modeling

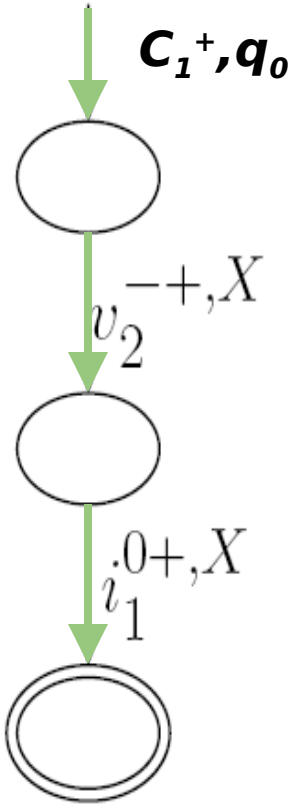
- Signatures with orderings can be combined into an event-based fault representation
  - **Fault trace** = sequence of measurement deviations produced by a fault in a mode
  - **Fault language** = all possible fault traces for a fault in a mode
- **Fault model** = Automata representation of fault language
  - Accepting states correspond to **maximal** traces

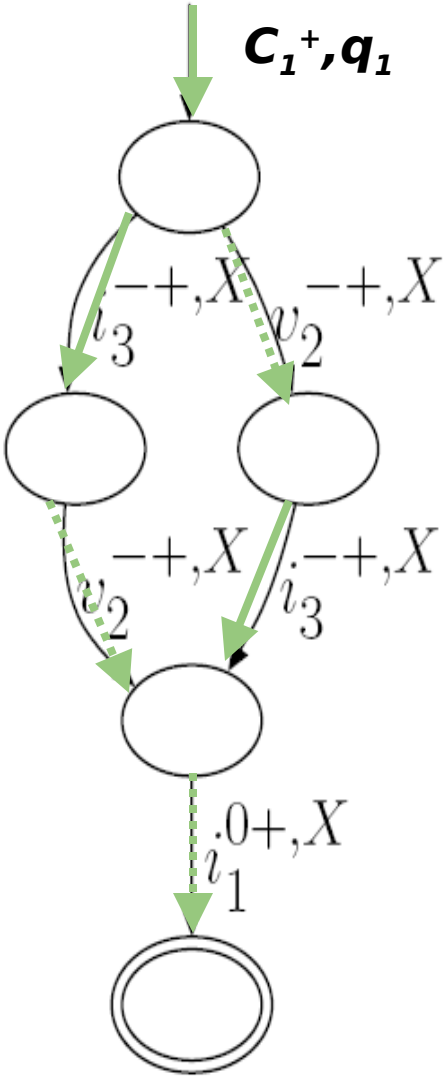
Candidate	i_1	v_2	i_3	Measurement Orderings
(C_1^+, q_1)	0+,X	-+,X	-+,X	$v_2 \prec i_1, i_3 \prec i_1$
(C_1^-, q_1)	0-,X	+-,X	+-,X	$v_2 \prec i_1, i_3 \prec i_1$
(L_1^+, q_1)	-+,X	0-,X	0-,X	$i_1 \prec v_2, i_1 \prec i_3$
(L_1^-, q_1)	+-,X	0+,X	0+,X	$i_1 \prec v_2, i_1 \prec i_3$
(R_1^+, q_1)	0-,X	0-,X	0-,X	$i_1 \prec v_2, i_1 \prec i_3$
(R_1^-, q_1)	0+,X	0+,X	0+,X	$i_1 \prec v_2, i_1 \prec i_3$
(R_2^+, q_1)	0-,X	0+,X	-+,X	$v_2 \prec i_1, i_3 \prec i_1, i_3 \prec v_2$
(R_2^-, q_1)	0+,X	0-,X	+-,X	$v_2 \prec i_1, i_3 \prec i_1, i_3 \prec v_2$



Candidate Traces

- **Candidate trace** = event sequence that is consistent with a candidate
  - For continuous systems diagnosis, candidate trace = fault trace
  - For hybrid systems, candidate trace = interleavings of fault traces with mode change events





EXAMPLE ***Start in q_0: $v_2^{-+,X}$ $i_1^{0+,X}$ σ_{q1} $i_3^{-+,X}$***

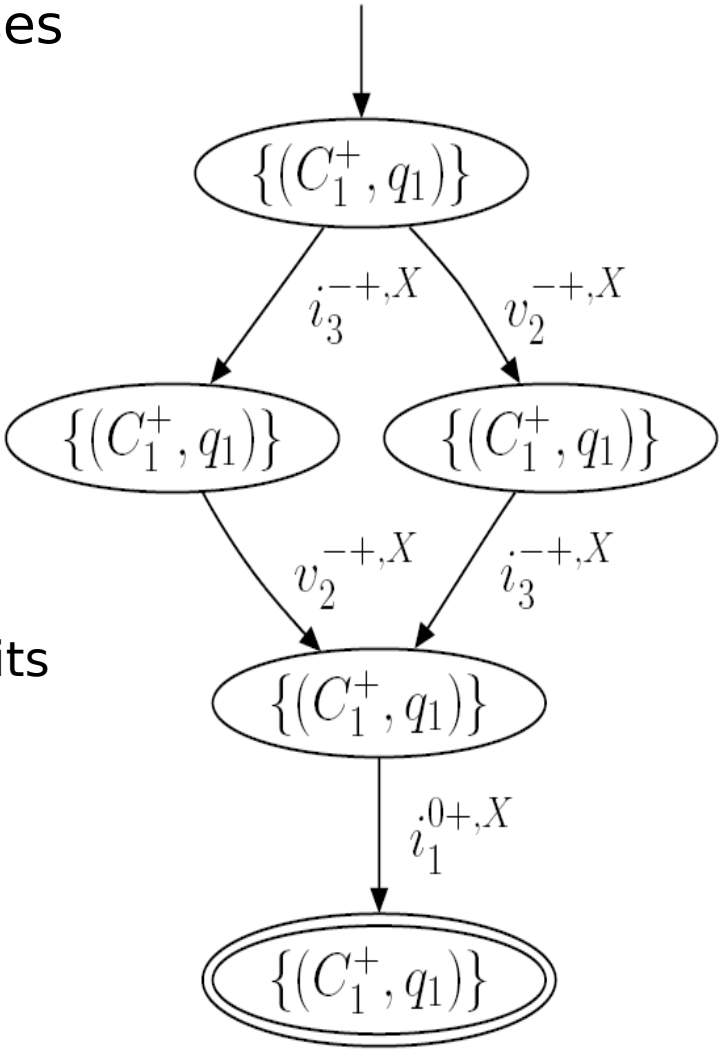
Candidate trace for C_1^+, q_1

Candidate Languages

- Candidate traces may be infinitely long if mode change events keep occurring
- Only **maximal** traces are helpful
  - Maximal candidate trace = trace for (c,q) is maximal if all measurements that should deviate in mode q for c have deviated
- **Candidate language** = set of maximal traces for a candidate
- From an initial mode, two candidates are **distinguishable** if no maximal trace for one candidate is a prefix of a maximal trace for the other
  - Otherwise, when the shorter maximal trace occurs, no new measurement deviations may occur to distinguish the candidates
- System is **diagnosable** if all candidates distinguishable for each initial mode

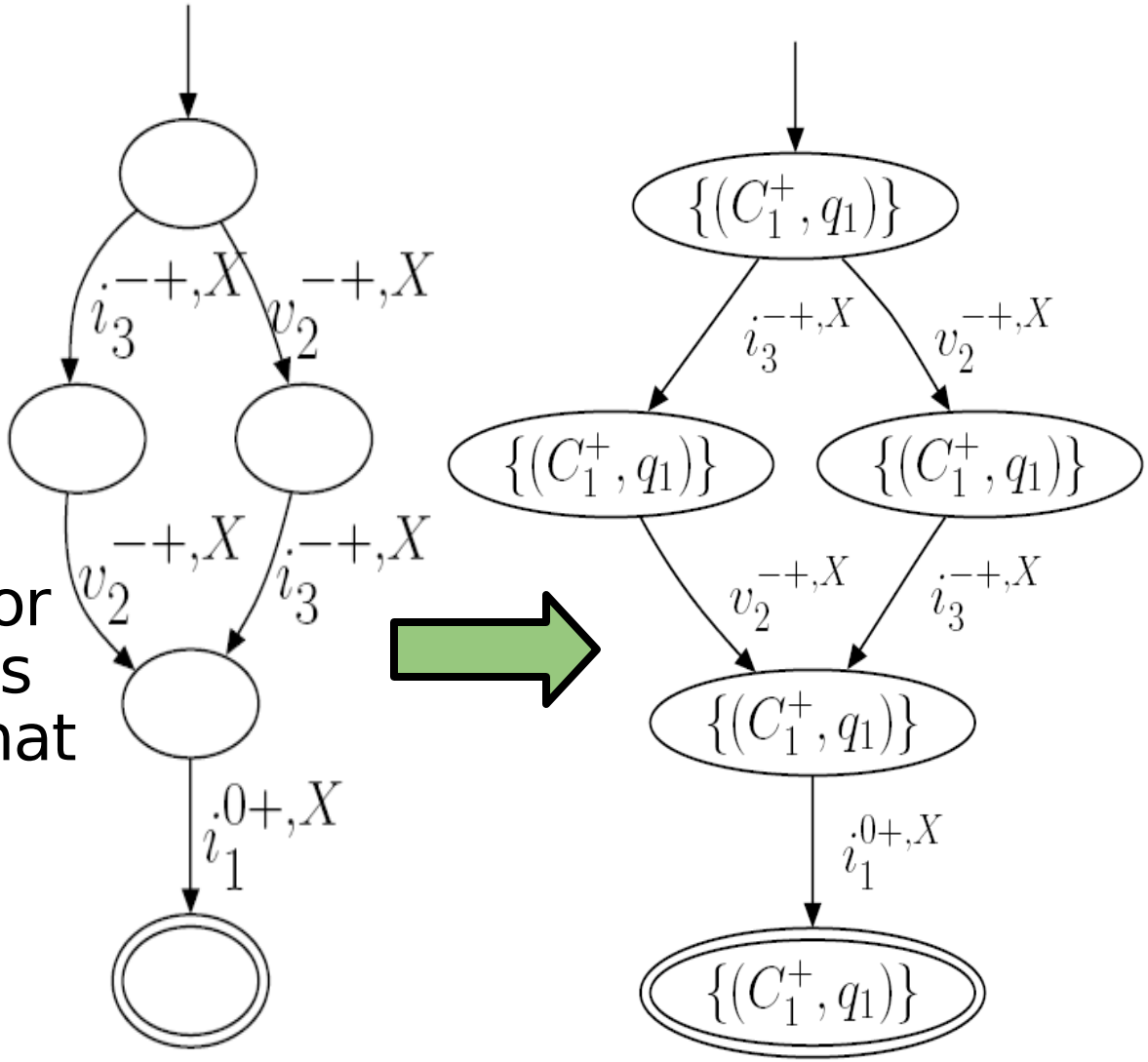
Diagnosers

- Finite automata extended with diagnoses
- Capture possible traces of candidates
- Diagnoser **isolates** a candidate if:
  - It accepts all its traces
  - Each accepting state contains the candidate in its diagnosis
- Diagnoser **uniquely isolates** a candidate *c* if:
  - It accepts all its traces
  - Each accepting state contains only *c* in its diagnosis
- Unique isolation occurs if **maximal** traces always linked back to a unique fault
  - Links back to diagnosability



Individual Diagnosers

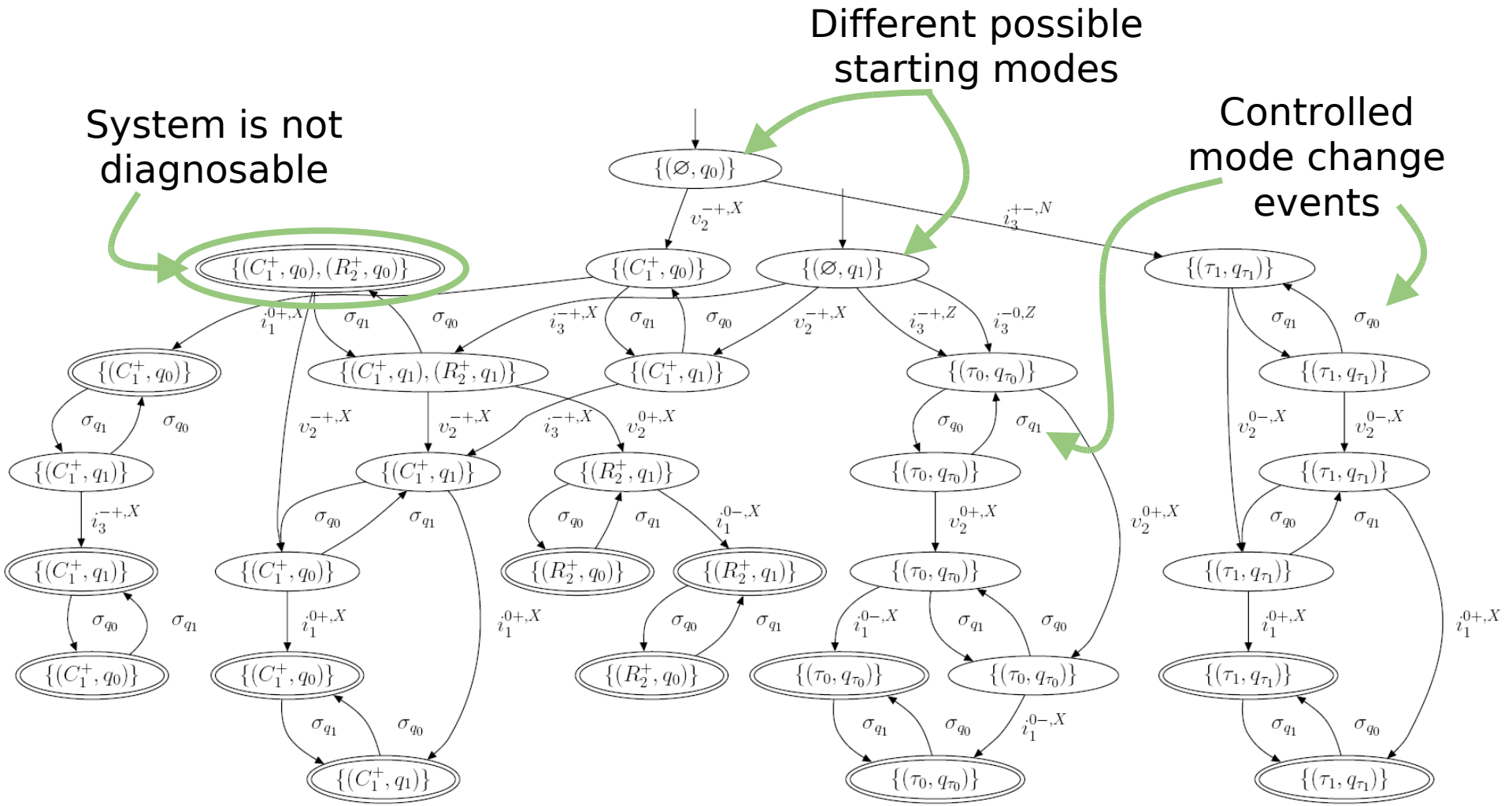
- Augment fault model with diagnoses
  - States contain the fault as the sole candidate
- Easy to show that this diagnoser $D_{f,q}$ isolates the fault for the fault model it is derived from for that mode only
  - By definition of its fault model, it accepts all traces



Diagnoser Composition

- Define $D_{F,Q}=\Pi_L(D_{f1,q1},D_{f2,q1},\ldots,D_{fn,qn})$
  - Common subtraces map to common states with both candidates in the diagnosis
- Composition defined such that composed diagnoser contains all possible **interleaved** traces of single faults, for all possible sequences of controlled mode changes
  - Result of measurement deviation event is a new state where new diagnosis retains only consistent candidates
  - Result of controlled mode change event is new state where new diagnosis has updated modes for candidates in the diagnosis
- Have shown the following (proofs in paper)
  - $D_{F,Q}$ isolates all candidates
  - System is diagnosable iff diagnoser uniquely isolates all valid candidates

Hybrid Diagnoser Example



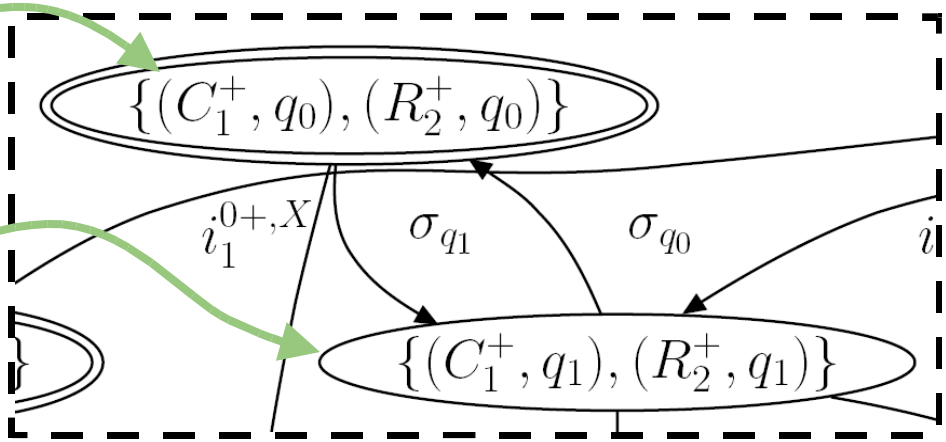
Hybrid Systems Diagnosability

- Diagnosability for hybrid systems
  - For any possible **maximal** candidate trace, unique candidate can be isolated
- Q-diagnosability
  - Controlled mode changes can affect whether traces are maximal
    - In some modes, fault has different effect on a measurement
  - System is **Q-diagnosable** if for every trace that "breaks" diagnosability, we can prevent that maximal trace
    - Can **block** certain controlled mode changes or **execute** certain controlled mode changes
    - Actions prevent bad maximal traces, or change to a mode where the trace is no longer maximal

In this state, execute σ_{q1}

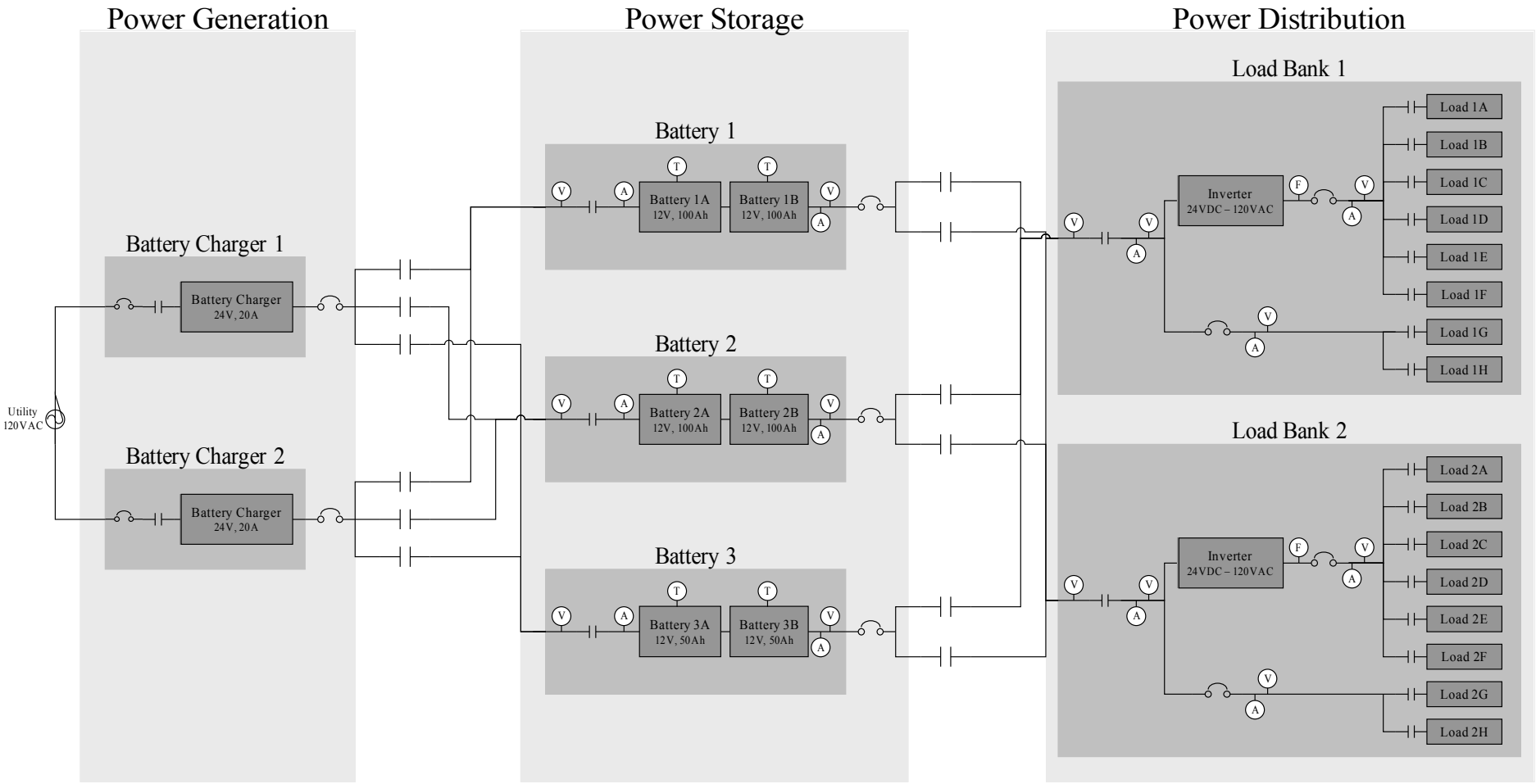
OR

In this state, prevent σ_{q0}



Case Study

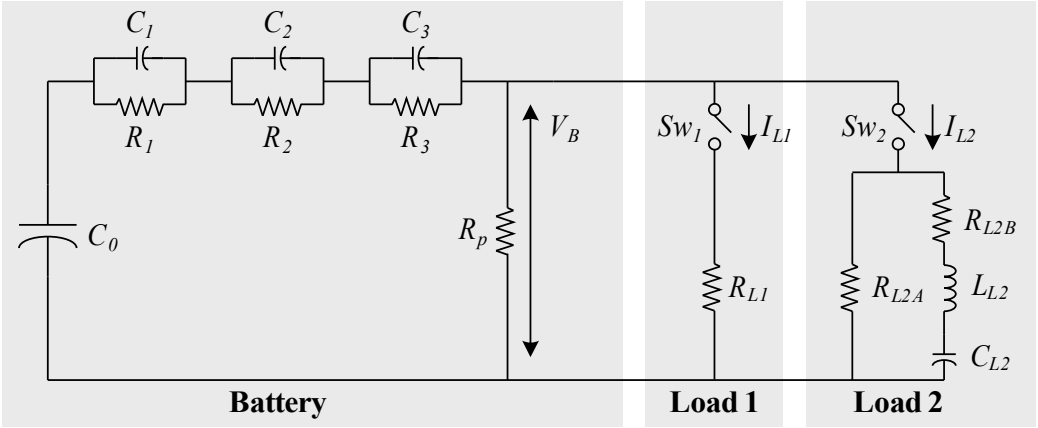
- Advanced Diagnostics and Prognostics Testbed (ADAPT) at NASA Ames Research Center



ADAPT

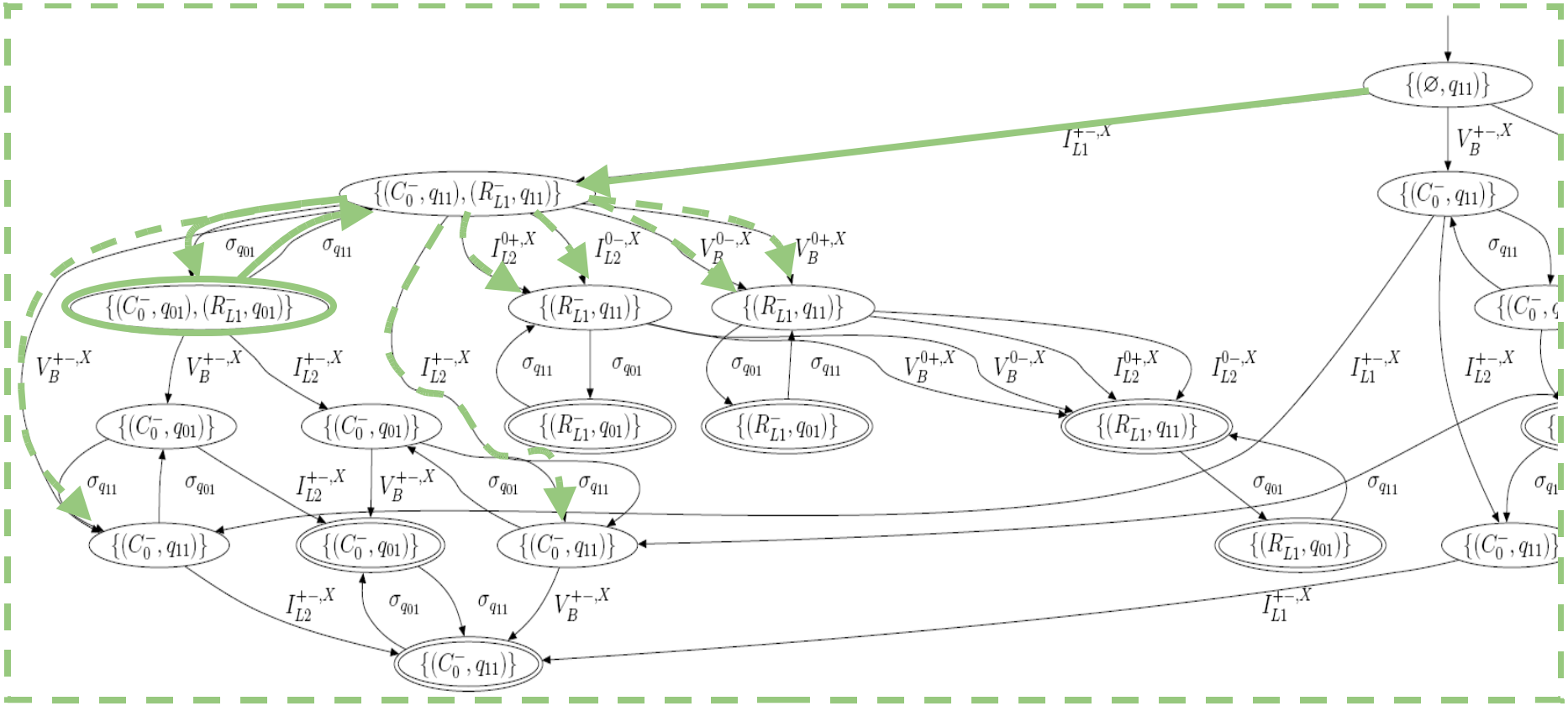
- Consider subset to demonstrate our approach
  - Battery discharging to two DC loads
  - Measure battery voltage and load currents
  - Faults include battery capacitance and resistance, load resistances, and sensor bias

Fault	V_B	I_{L1}	I_{L2}	Measurement Orderings
(V_B^+, q_{**})	+0,X	00,X	00,X	$V_B \prec I_{L1}, V_B \prec I_{L2}$
(V_B^-, q_{**})	-0,X	00,X	00,X	$V_B \prec I_{L1}, V_B \prec I_{L2}$
(I_{L1}^+, q_{**})	00,X	+0,X	00,X	$I_{L1} \prec V_B, I_{L1} \prec I_{L2}$
(I_{L1}^-, q_{**})	00,X	-0,X	00,X	$I_{L1} \prec V_B, I_{L1} \prec I_{L2}$
(I_{L2}^+, q_{**})	00,X	00,X	+0,X	$I_{L1} \prec V_B, I_{L2} \prec I_{L1}$
(I_{L2}^-, q_{**})	00,X	00,X	-0,X	$I_{L1} \prec V_B, I_{L2} \prec I_{L1}$
(C_0^-, q_{11})	+-,X	+-,X	+-,X	$\varnothing$
(R_1^+, q_{11})	0-,X	0-,X	0-,X	$\varnothing$
(R_{L1}^+, q_{11})	0*,X	-+,X	0*,X	$I_{L1} \prec V_B, I_{L1} \prec I_{L2}$
(R_{L1}^-, q_{11})	0*,X	+-,X	0*,X	$I_{L1} \prec V_B, I_{L1} \prec I_{L2}$
(R_{L2A}^+, q_{11})	0*,X	0*,X	-+,X	$I_{L2} \prec V_B, I_{L2} \prec I_{L1}$
(R_{L2A}^-, q_{11})	0*,X	0*,X	+-,X	$I_{L2} \prec V_B, I_{L2} \prec I_{L1}$
$(\alpha_0, q_{\alpha_0 1})$	0*,X	-*,Z	0*,X	$I_{L1} \prec V_B, I_{L1} \prec I_{L2}$
$(\alpha_1, q_{\alpha_1 1})$	0*,X	+*,N	0*,X	$I_{L1} \prec V_B, I_{L1} \prec I_{L2}$
$(\beta_0, q_{1\beta_0})$	0*,X	0*,X	-*,Z	$I_{L2} \prec V_B, I_{L2} \prec I_{L1}$
$(\beta_1, q_{1\beta_1})$	0*,X	0*,X	+*,N	$I_{L2} \prec V_B, I_{L2} \prec I_{L1}$



Diagnosability Analysis

- System is not diagnosable
  - But it is Q-diagnosable



Conclusions

- Systematic framework to create event-based diagnosers for hybrid systems
  - HBG model → TCG → signatures and orderings → fault models → individual diagnosers → global diagnoser
- Diagnosers useful for diagnosability analysis
- Introduced Q-diagnosability, where unique isolation results can be achieved by blocking or executing certain controlled mode changes
- Demonstrated framework for ADAPT
  - Is not diagnosable, but is Q-diagnosable