Just-Ahead-Of-Time Controller Recovery

Sriharsha Etigowni, Shamina Hossain-McKenzie*, Maryam Kazerooni*, Kate Davis*, Saman Zonouz

Department of Electrical and Computer Engineering
Rutgers University, *University of Illinois

Introduction

Motivating Scenario: Recent major attacks on the electric grid necessitate domain-specific formal security monitoring solutions for cyber-physical system operations. Detecting unsafe states aids mitigation measures, but preventing unsafe states provides more beneficial and significant impact for recovery.

Just-Ahead-of-Time Controller Recovery

- Parallel, on-the-fly model checking using symbolic execution for pruning unreachable states to determine unsafe states before execution on PLC

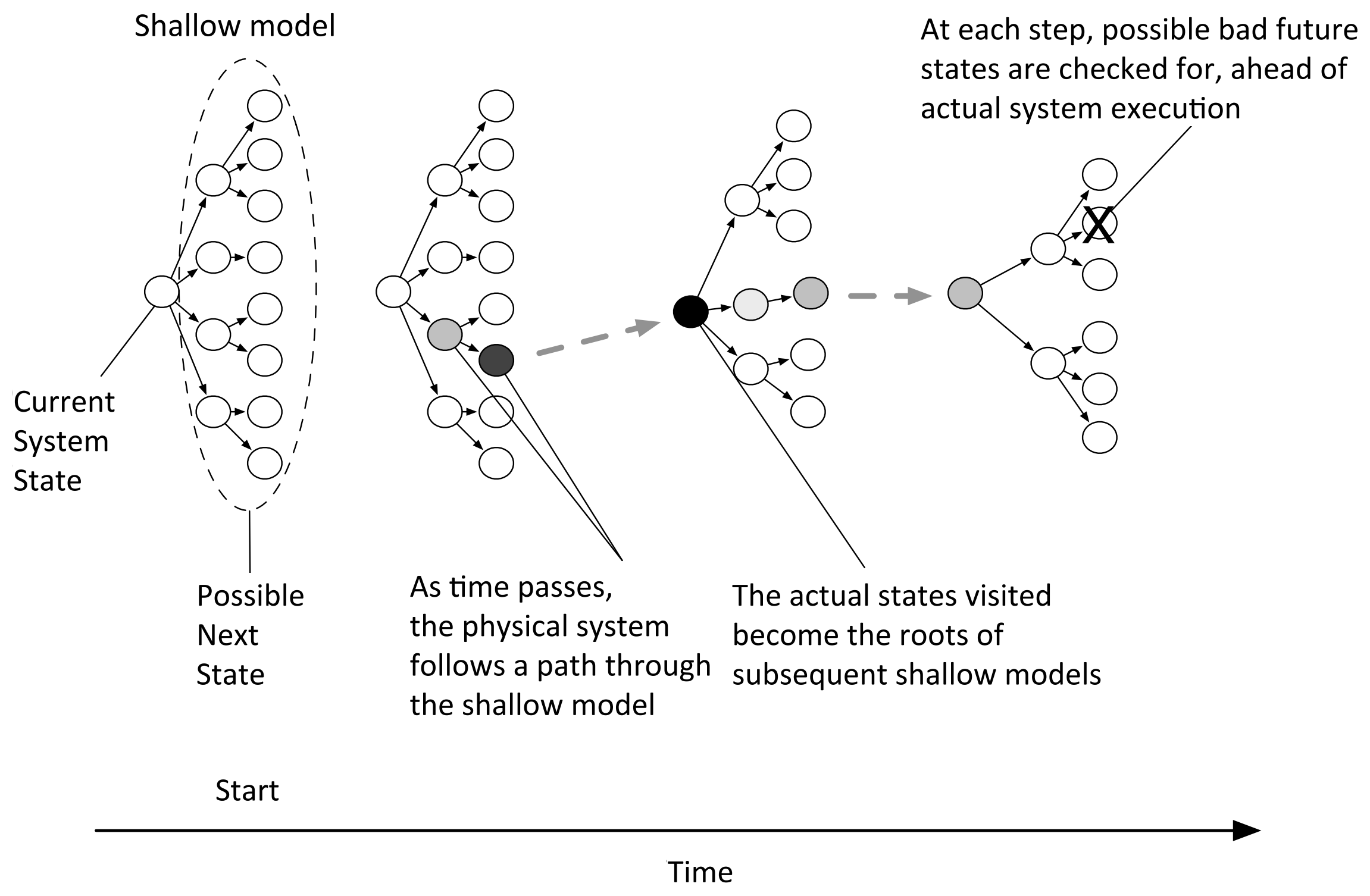

Shallow model
At each step, possible bad future states are checked for, ahead of actual system execution
X
Current System State
Possible Next State
As time passes, the physical system follows a path through the shallow model
The actual states visited become the roots of subsequent shallow models
Start
Time

Figure 1: Discarding unreachable states

Controller Logic Modified Attack

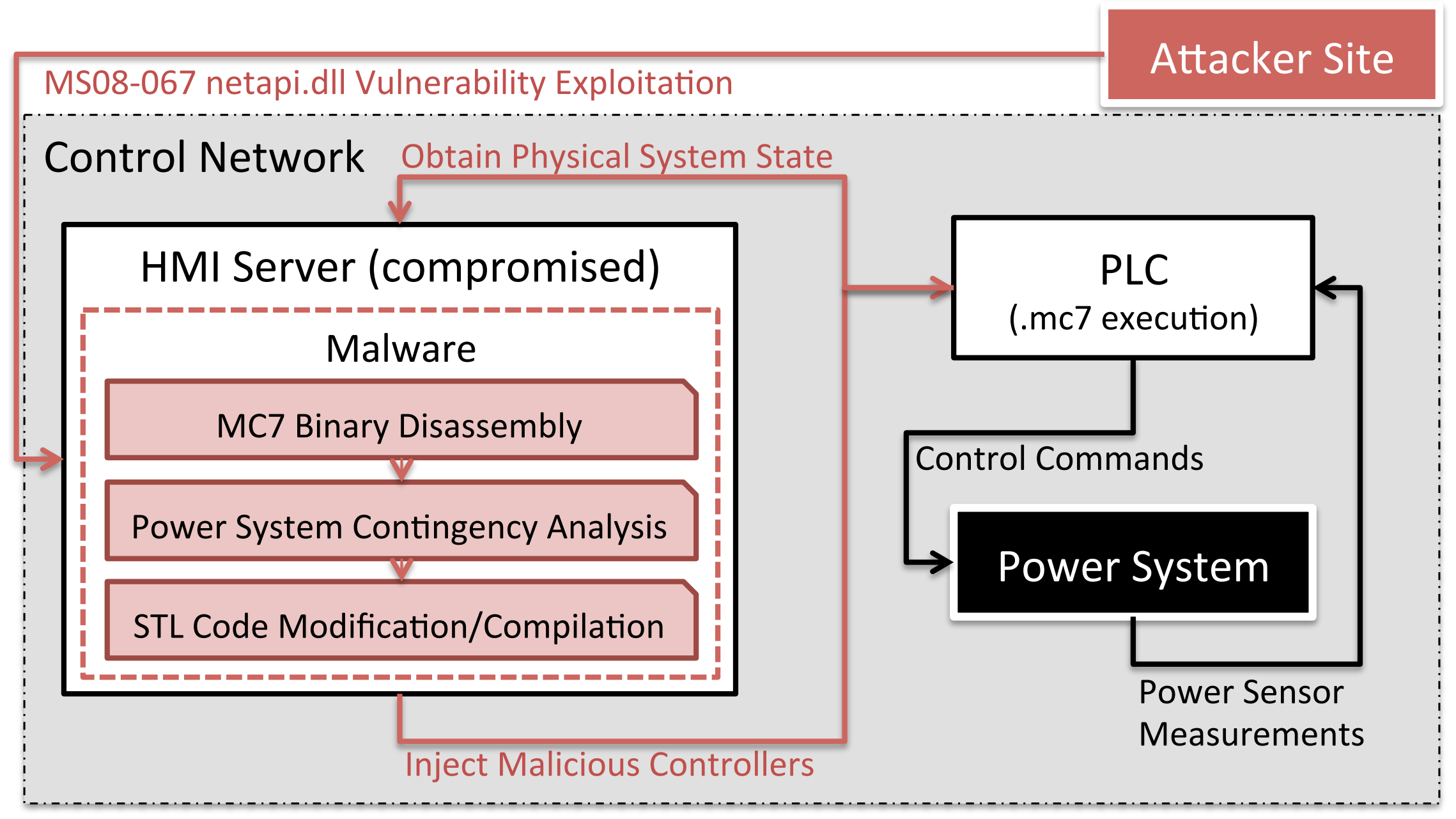

Attacker Site
MS08-067 netapi.dll Vulnerability Exploitation
Control Network
Obtain Physical System State
HMI Server (compromised)
Malware
MC7 Binary Disassembly
Power System Contingency Analysis
STL Code Modification/Compilation
PLC
(.mc7 execution)
Control Commands
Power System
Power Sensor Measurements
Inject Malicious Controllers

Figure 2: Controller logic modified attack

1. Exploits MS08-067 vulnerability in netapi.dll
2. Injects malicious instructions to the running PLC dynamically
3. The malware copies the dynamic memory, disassembles, injects malicious instruction, assembles, and then uploads it back into the PLC
4. JCR was successful against this attack

JCR Architecture

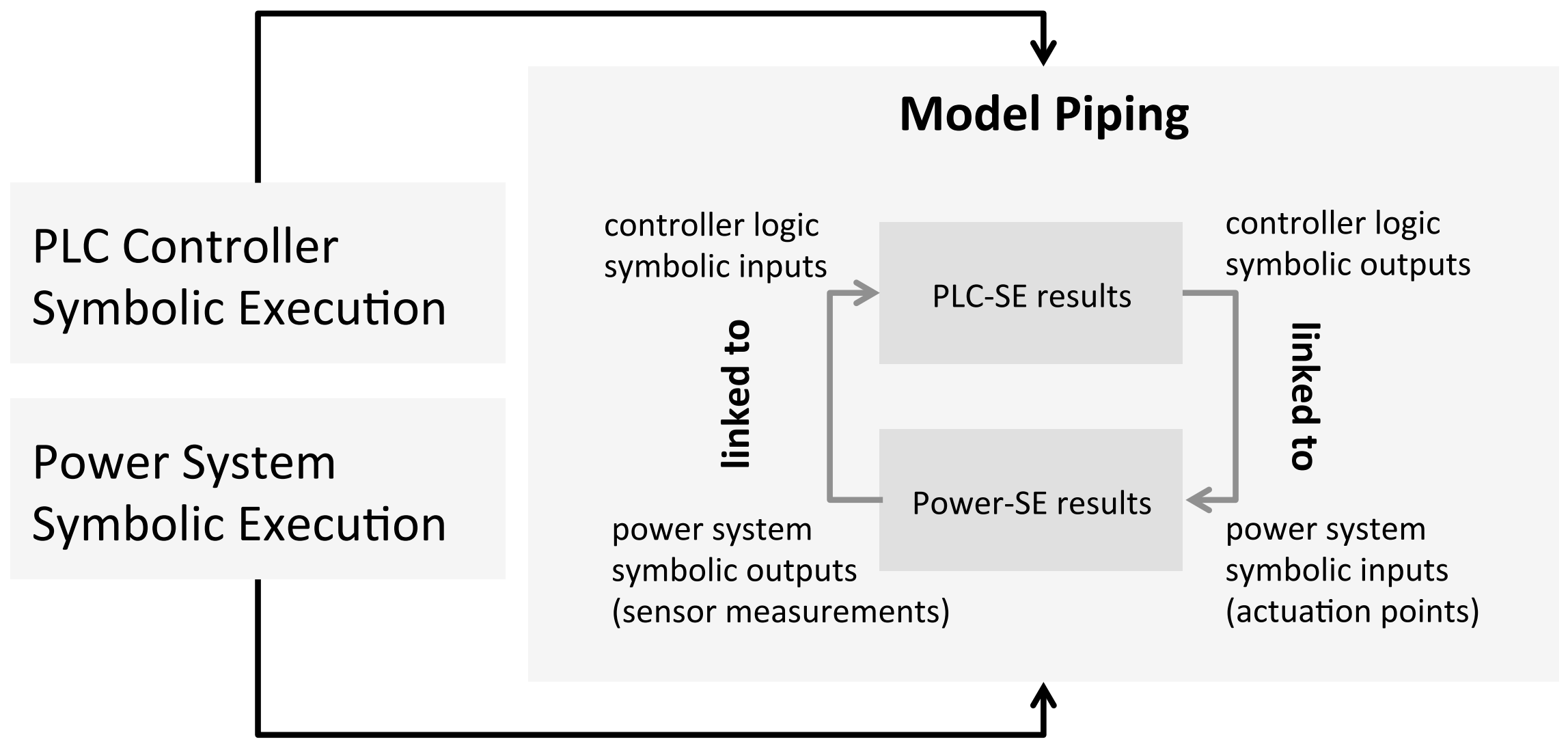

Model Piping
PLC Controller Symbolic Execution
Power System Symbolic Execution
controller logic symbolic inputs
PLC-SE results
controller logic symbolic outputs
linked to
linked to
Power-SE results
power system symbolic outputs (sensor measurements)
power system symbolic inputs (actuation points)

Figure 3: Hybrid Cyber-Physical Symbolic Execution

- JCR uses hybrid symbolic execution to eliminate the unreachable states, thus increasing the speed of verification
- JCR performs parallel, on-the-fly model checking and informs the operator well in advance about the future unsafe states
- With this in-advance warning, the operator can take necessary actions to prevent the unsafe state

Verification and Recovery

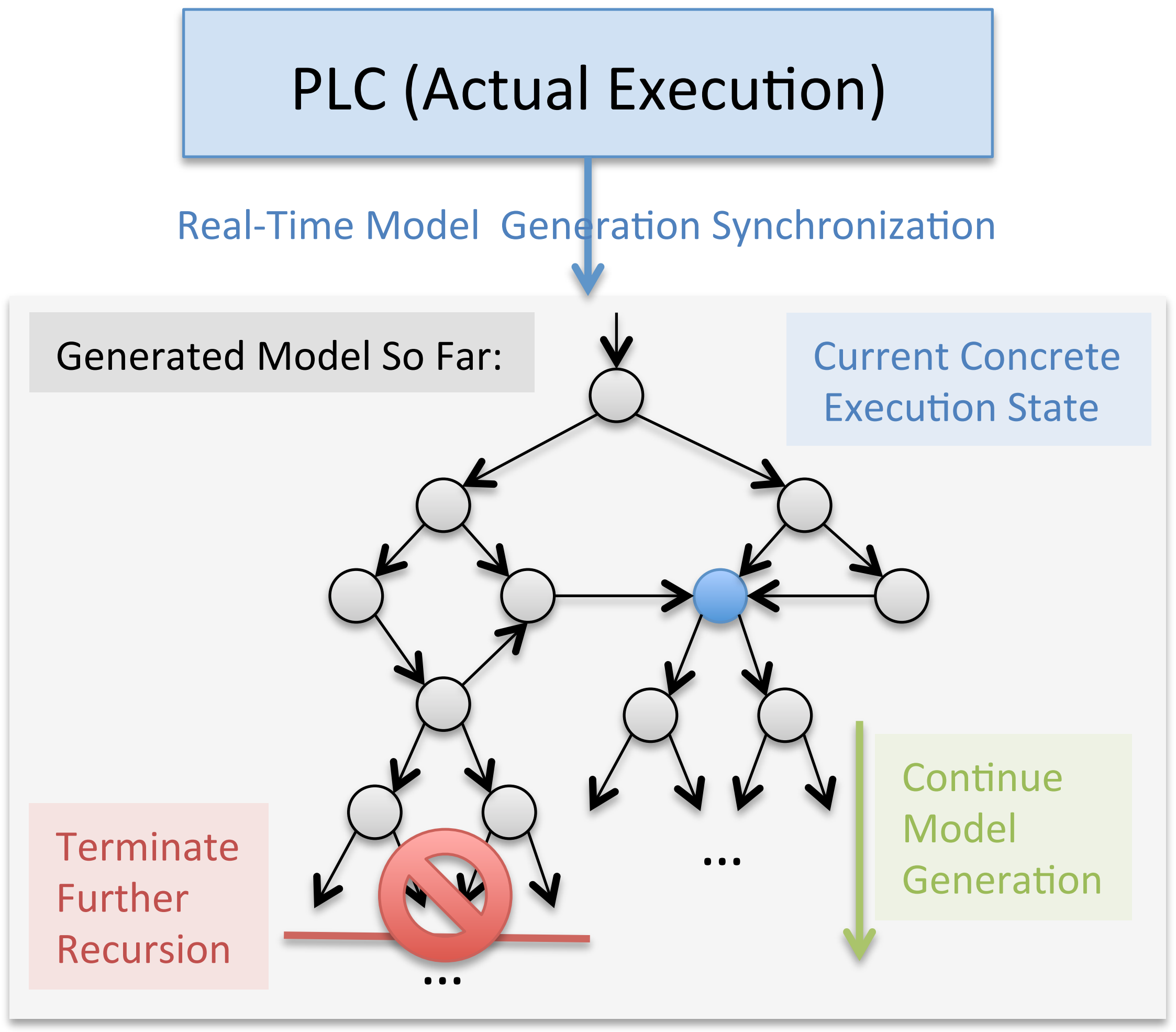
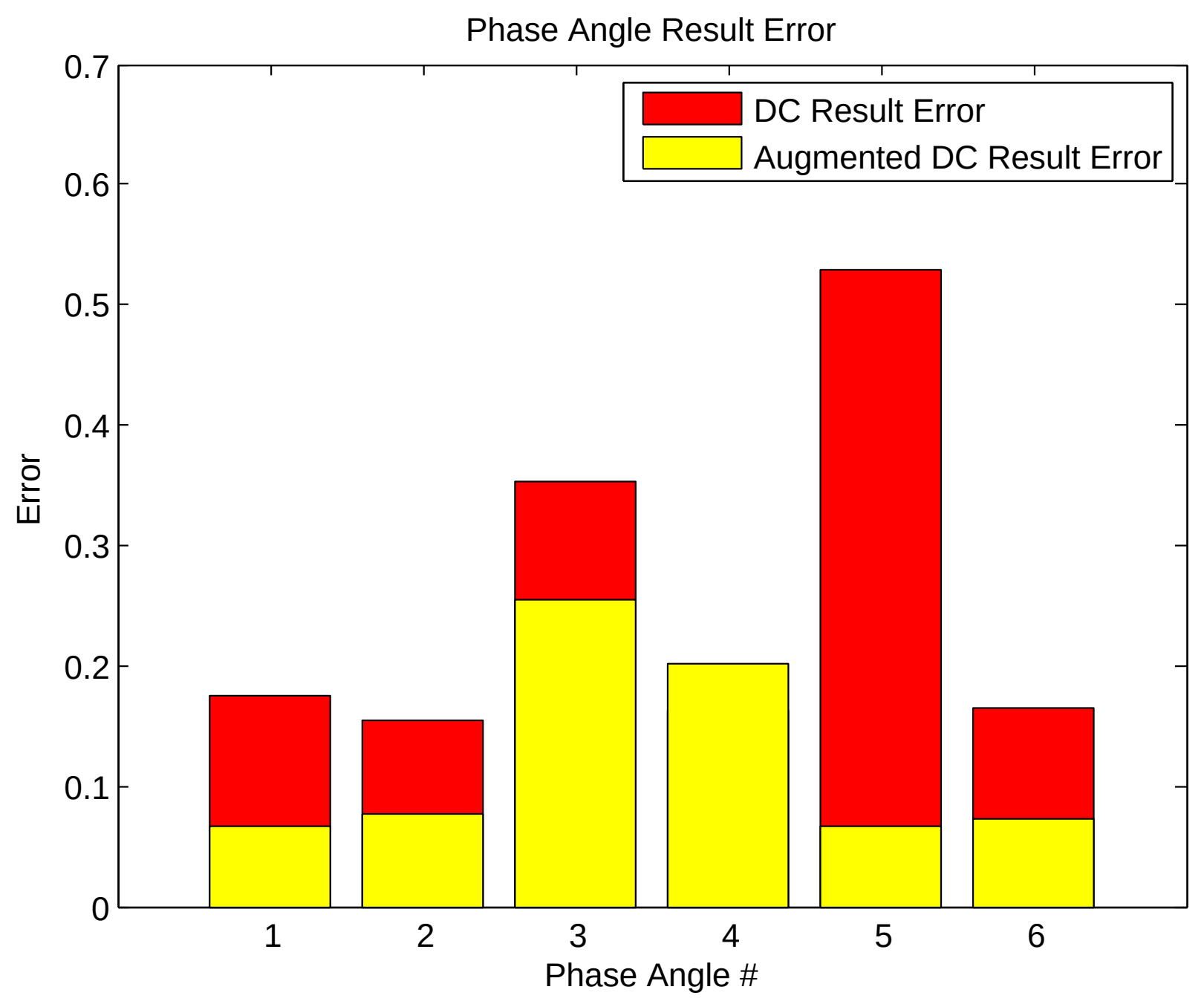

PLC (Actual Execution)
Real-Time Model Generation Synchronization
Generated Model So Far:
Current Concrete Execution State
Terminate Further Recursion
...
...
Continue Model Generation

Figure 4: Model Generation, Refinement and Checking

- To address subsequent scan cycles, JCR explores the possible states by creating the corresponding state-based finite state automaton
- JCR avoids exploration of the states that are not reachable from the system's current concrete state

Physical System Symbolic Analysis

- JCR enhances the traditional numerical state estimation algorithms for a symbolic execution (analysis) of the power system
- An augmented DC power flow analysis method was developed that, with the inclusion of symbolic variables, maintained speed and accuracy



Evaluations

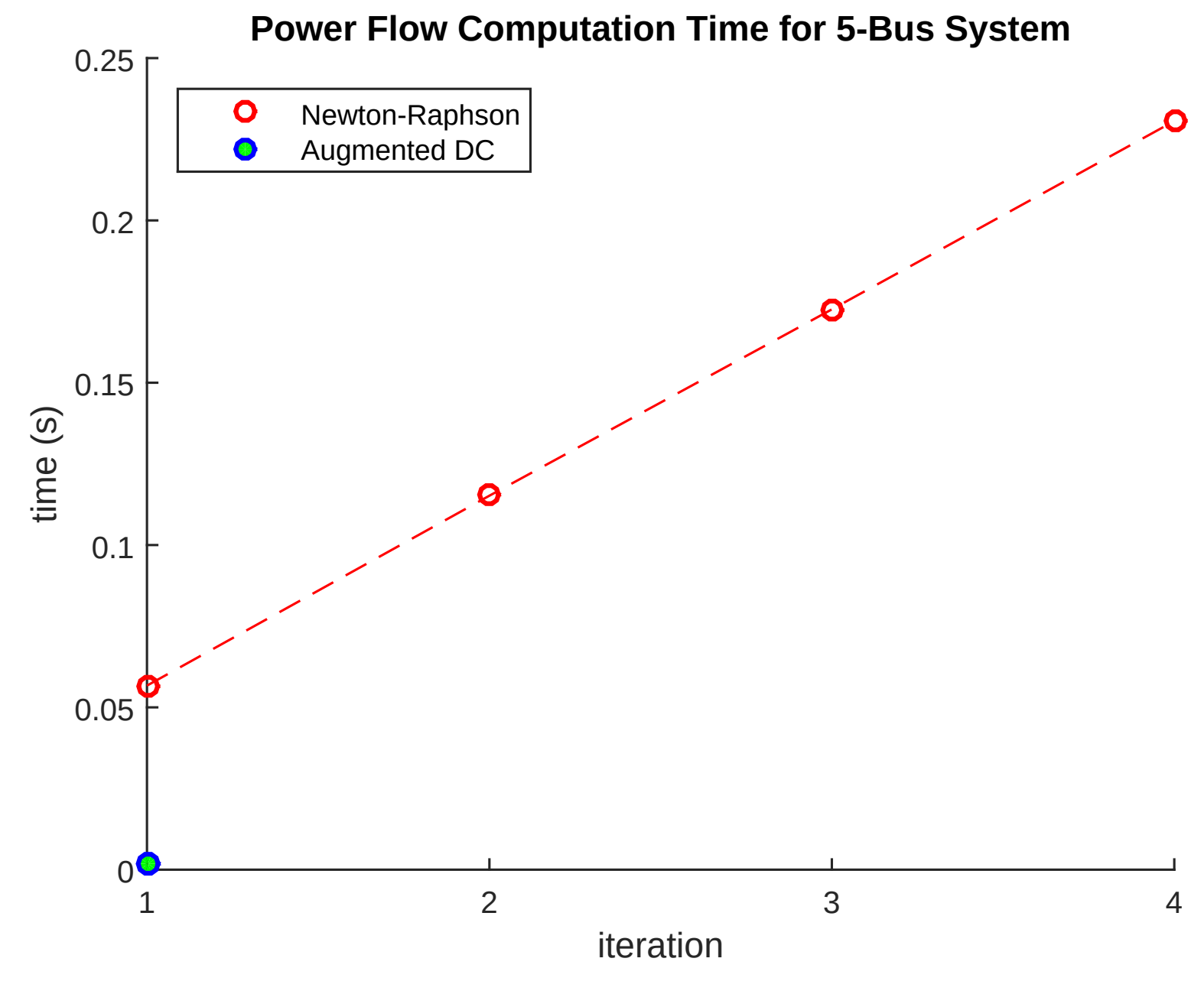


Figure 5: The computation time for the NR-PF method involves many iterations, increasing the total time, whereas the augDC-PF algorithm requires only one iteration.

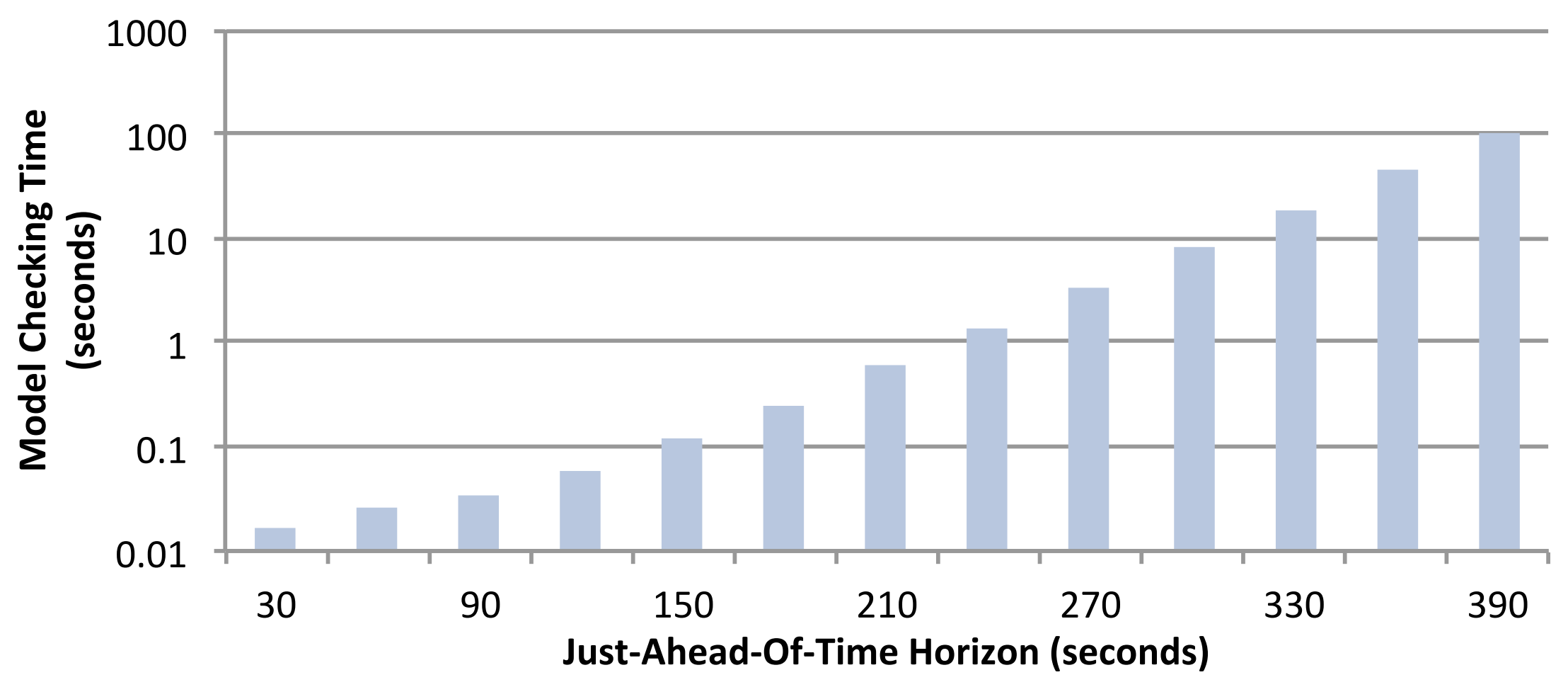


Figure 6: JCR on 2700-bus

References

[1] Saman Zonouz, Charles M Davis, Katherine R Davis, Robin Berthier, Rakesh B Bobba, and William H Sanders. Socca: A security-oriented cyber-physical contingency analysis in power infrastructures. *Smart Grid, IEEE Transactions on*, 5(1):3–13, 2014.

[2] Stephen McLaughlin, Saman Zonouz, Devin Pohly, and Patrick McDaniel. A trusted safety verifier for process controller code. In *Proc. ISOC Network and Distributed Systems Security Symposium (NDSS)*, 2014.

[3] Edward J Schwartz, Thanassis Avgerinos, and David Brumley. All you ever wanted to know about dynamic taint analysis and forward symbolic execution (but might have been afraid to ask). In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 317–331. IEEE, 2010.

Acknowledgements

We would like to thank our sponsor:
National Science Foundation (NSF)

Contact Information

- Saman Zonouz, Ph.D.
- Assistant Professor, Rutgers University
- Web: https://sites.google.com/site/samanzonouz4n6/
- Email: *saman.zonouz@rutgers.edu*
- Phone: +1 (217) 721 8280