PLC Code Verification and Neural Network Approximation

Aolin Ding, Sriharsha Etigowni, Saman Zonouz
Rutgers University

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

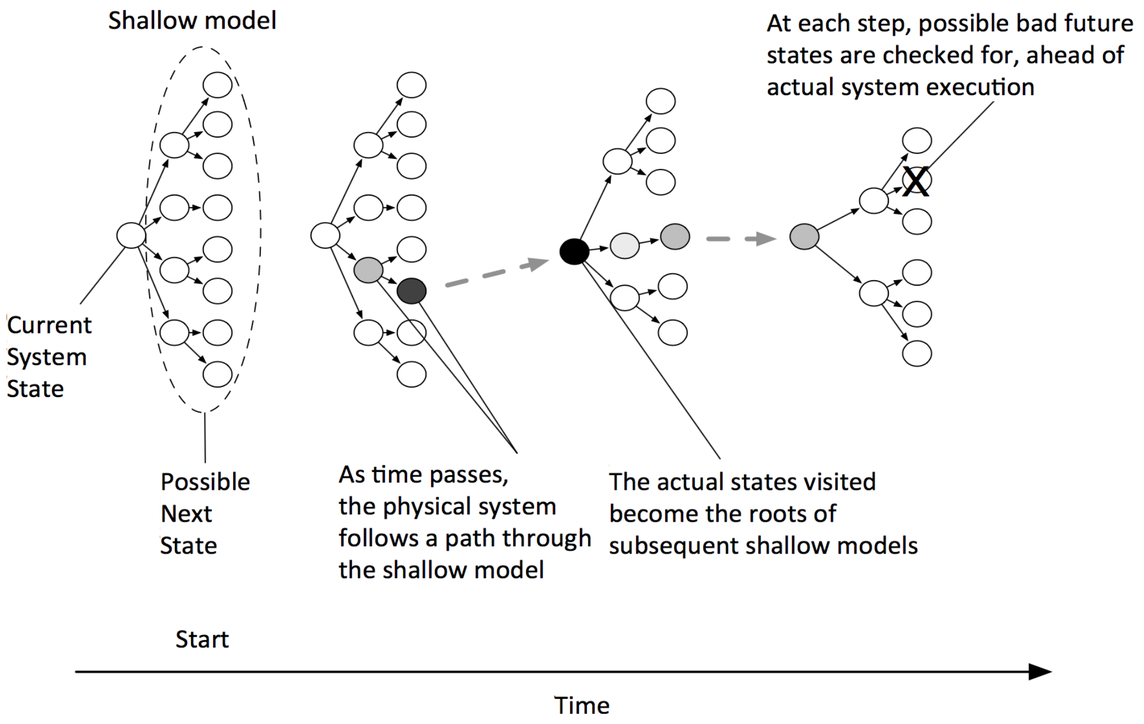

Figure1: Discarding unreachable states

CONTROLLER LOGIC MODIFIED ATTACK

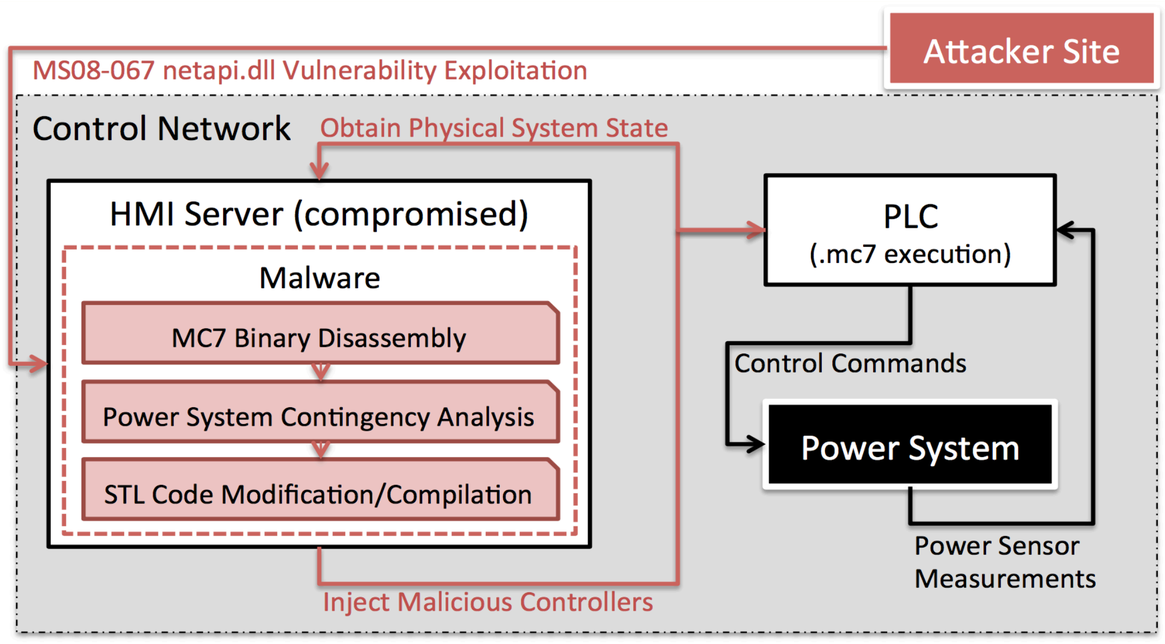

Figure 2:Controller logic modified attack

CODE VERIFICATION

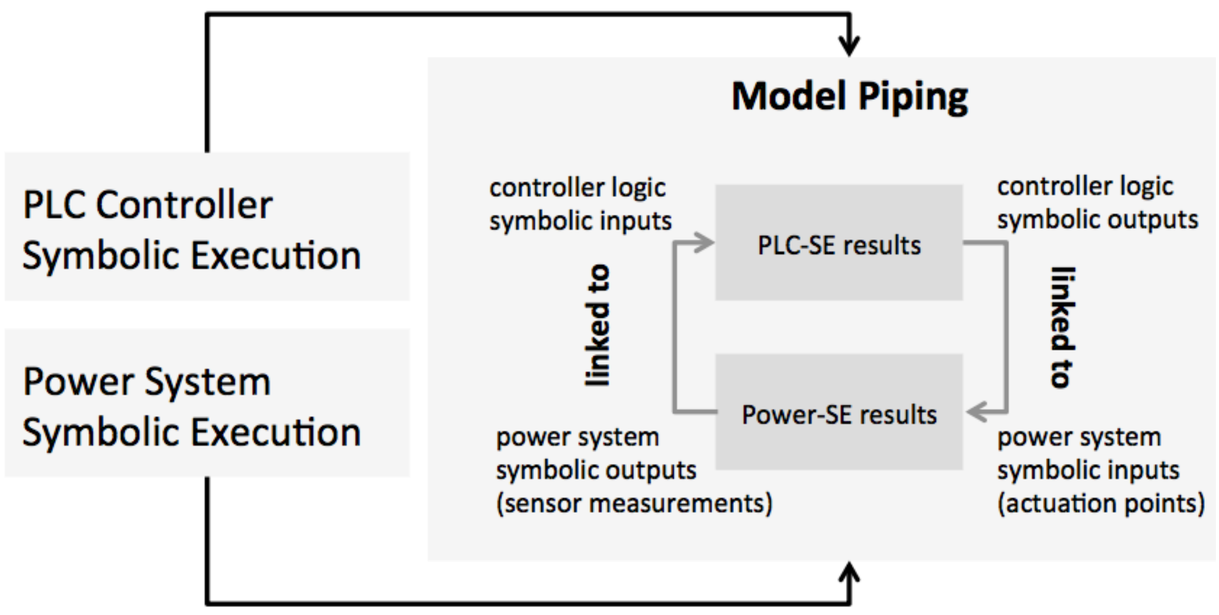

Figure 3: Hybrid Cyber-Physical Symbolic Execution

- 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
- JCR avoids exploration of the states that are not reachable from the system's current concrete state
- With this in-advance warning, the operator can take necessary actions to prevent the unsafe state

NEURAL NETWORK APPROXIMATION

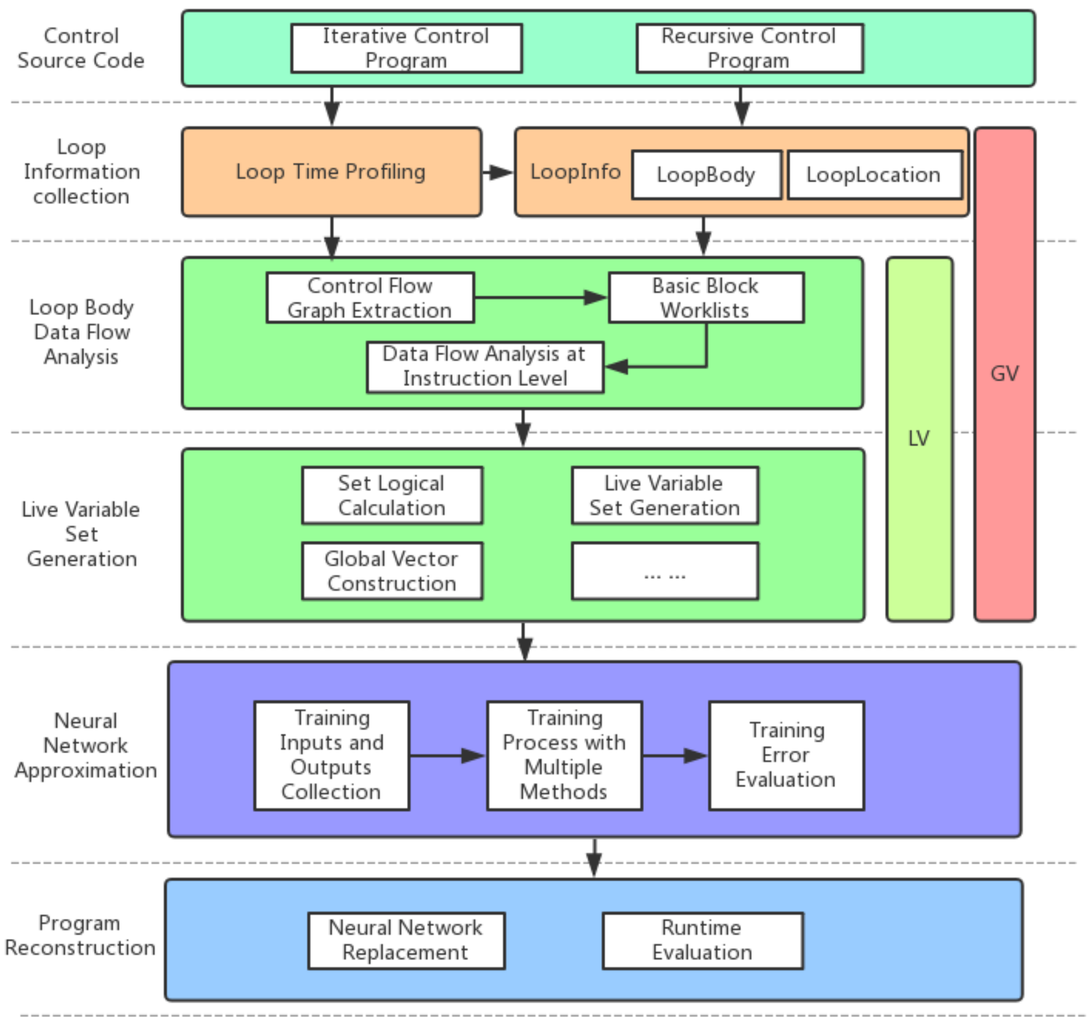

Figure 4: Program Approximation Architecture

SEMANTIC RECONSTRUCTION

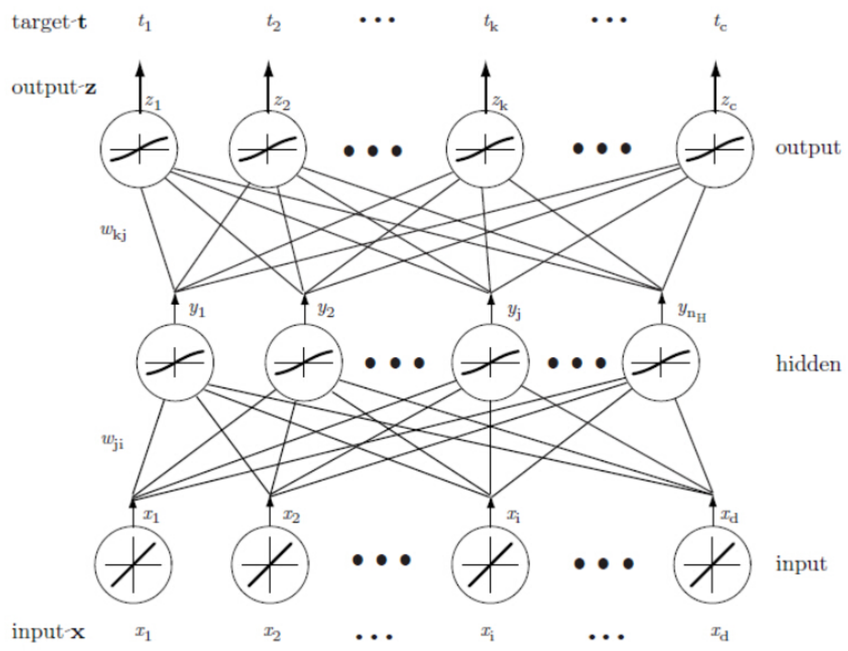

Figure 5:Neural Network Architecture

- Trained neural network has the same semantics with the original code
- Reconstructed code obtains faster running speed but lower accuracy
- Approximated implementation provides alert comparison for vulnerabilities

FUTURE EFFORTS

- Provide smartly selective neural network models for best training results
- Establish the complete evaluation process to increase the effectiveness
- Automate the whole processes and improve reliability

REFERENCES

- Sriharsha Etigowni, Maryam Kazerooni, Shamina Hossain-Mckenzie, Katherine Davis, Saman Zonouz.
  Just-Ahead-Of-Time Controller Recovery
  2016 IEEE international Conference on Smart Grid Communications
- 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.
- 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.

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY