Protect Controller Software Using Approximate Computing and Semantic Matching-based Binary Patching

Aolin Ding, Pengfei Sun, Saman Zonouz
Rutgers University

INTRODUCTION

❑ **Approximate Computing:** Recent major attacks on the electric grid necessitate domain-specific formal security monitoring solutions for cyber-physical system operations. We developed an online monitoring framework based on modeling the cyber-physical input-output dynamics of the industrial controller in real-time operation.

❑ **Semantic Matching:** We performs semantic-matching at an algorithmic level that can be used for firmware vulnerability assessment, memory forensics analysis, targeted memory data attacks, or binary patching for dynamic selective memory protection.

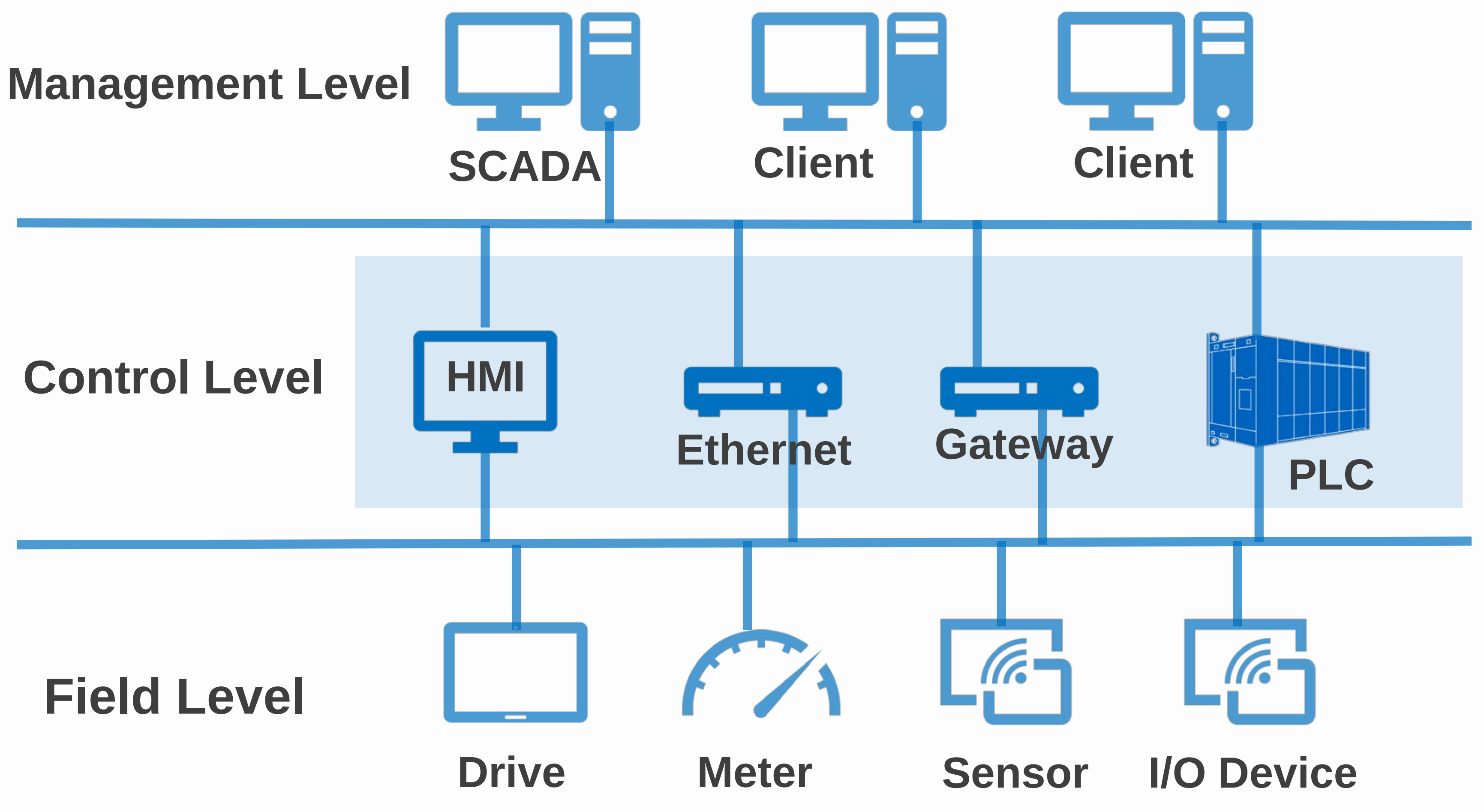


Figure 1: Industrial Control System

CONTROLLER LOGIC MONITORING FRAMEWORK

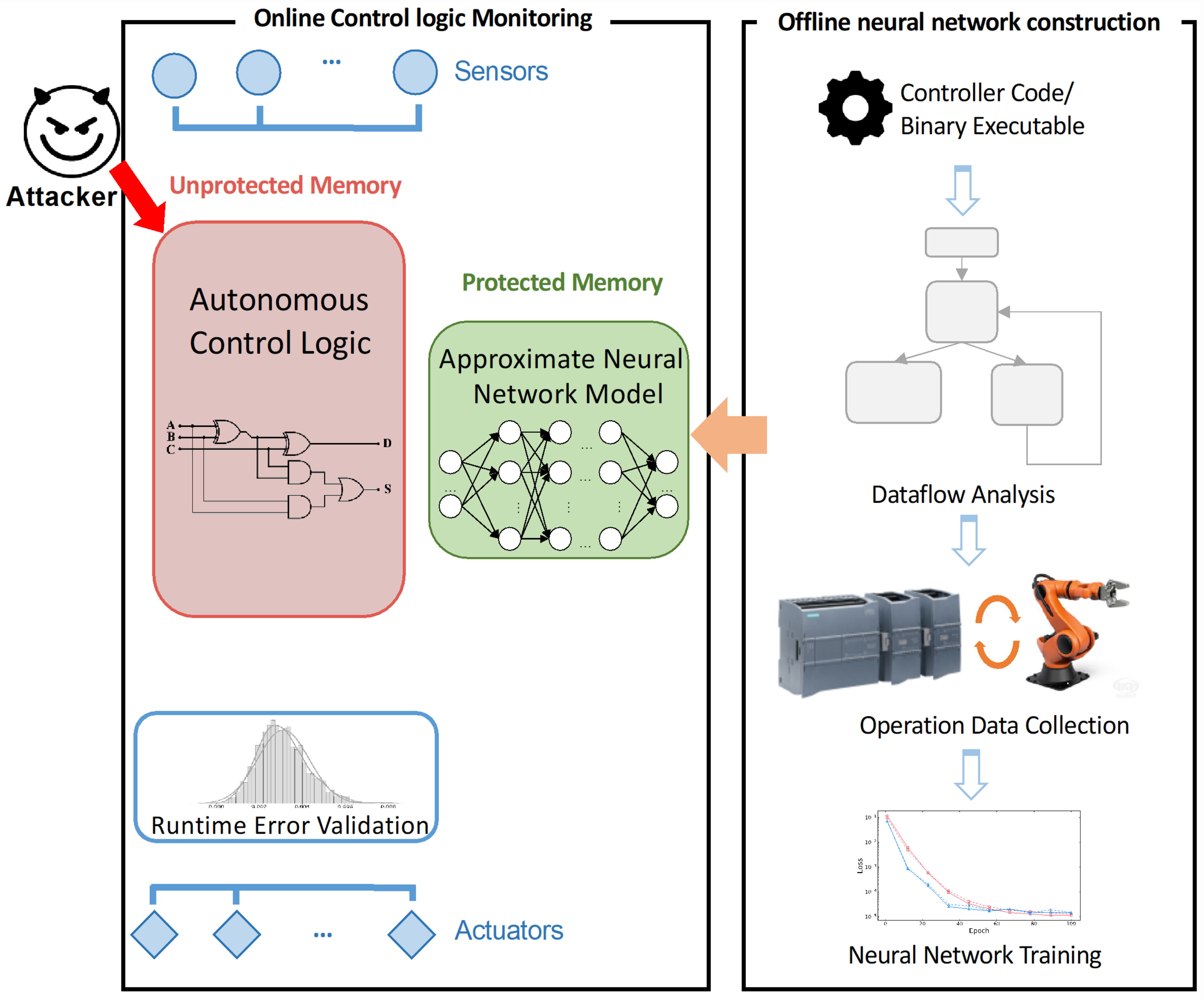


Figure 2: High-level Architecture of Monitoring Framework

ONLINE CONTROL LOGIC VERIFICATION

❑ **Construct:** We establish a neural network-based learning model by using time profiling and data flow analysis.

❑ **Monitor:** The lightweight, pre-trained neural network will be stored in protected memory space to monitor the main controller system automatically.

❑ **Alert:** The approximate computing results generated by neural network model will be compared with original actuation outputs to detect potential mismatches as anomalies.

SEMANTIC REVERSE ENGINEERING

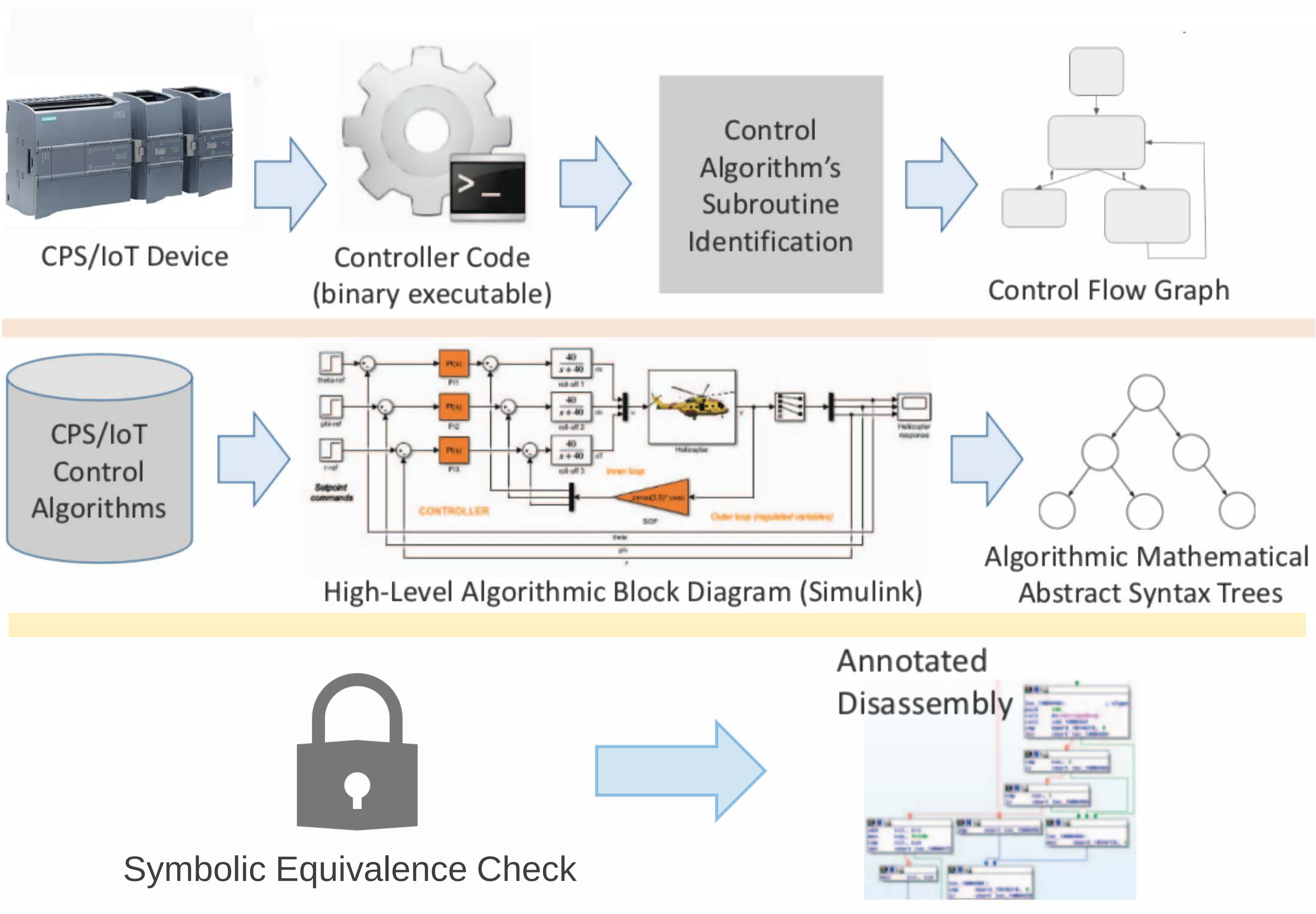
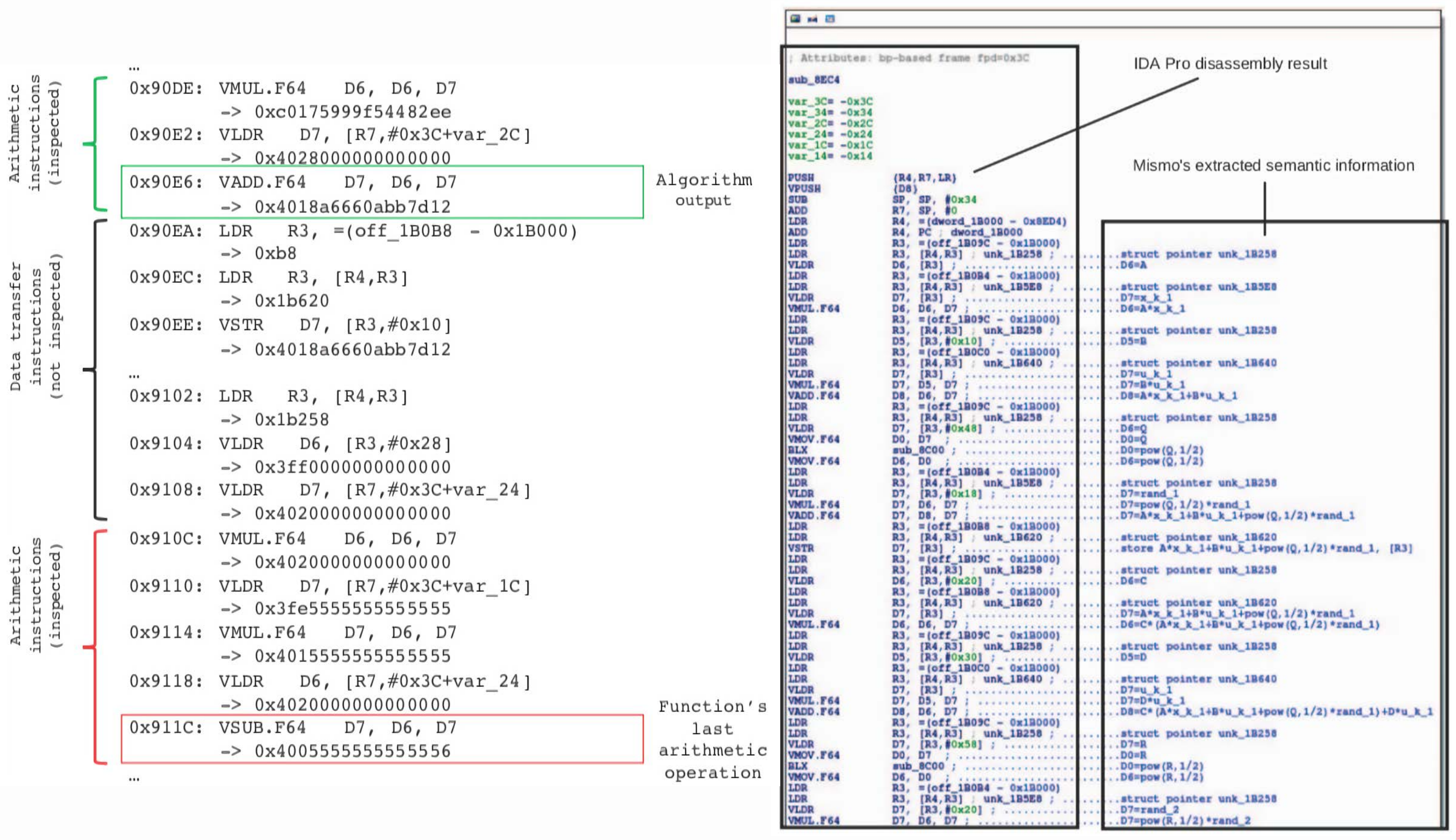

CPS/IoT Device
Controller Code (binary executable)
Control Algorithm's Subroutine Identification
Control Flow Graph
CPS/IoT Control Algorithms
High-Level Algorithmic Block Diagram (Simulink)
Algorithmic Mathematical Abstract Syntax Trees
Symbolic Equivalence Check
Annotated Disassembly

Figure 3: Semantic Reverse Engineering of Controller Binary

ANNOTATED DISASSEMBLY



```
...
0x90DE: VMUL.F64   D6, D6, D7
        -> 0xc0175999f54482ee
0x90E2: VLDR   D7, [R7,#0x3C+var_2C]
        -> 0x4028000000000000
0x90E6: VADD.F64   D7, D6, D7
        -> 0x4018a6660abb7d12
0x90EA: LDR   R3, =(off_1B0B8 - 0x1B000)
        -> 0xb8
0x90EC: LDR   R3, [R4,R3]
        -> 0x1b620
0x90EE: VSTR   D7, [R3,#0x10]
        -> 0x4018a6660abb7d12
...
0x9102: LDR   R3, [R4,R3]
        -> 0x1b258
0x9104: VLDR   D6, [R3,#0x28]
        -> 0x3ff0000000000000
0x9108: VLDR   D7, [R7,#0x3C+var_24]
        -> 0x4020000000000000
0x910C: VMUL.F64   D6, D6, D7
        -> 0x4020000000000000
0x9110: VLDR   D7, [R7,#0x3C+var_1C]
        -> 0x3fe5555555555555
0x9114: VMUL.F64   D7, D6, D7
        -> 0x4015555555555555
0x9118: VLDR   D6, [R7,#0x3C+var_24]
        -> 0x4020000000000000
0x911C: VSUB.F64   D7, D6, D7
        -> 0x4005555555555556
...
```

Arithmetic instructions (inspected)
Data transfer instructions (not inspected)
Arithmetic instructions (inspected)
Algorithm output
Function's last arithmetic operation
IDA Pro disassembly result
Mismo's extracted semantic information

Figure 4: Semantic Annotation Information for Disassembly

❑ **Extract:** A general framework to extract semantic information of an embedded firmware binaries with respect to its associated high-level control algorithm.

❑ **Matching:** Using dynamic binary analysis and symbolic comparison of the mathematical and binary expressions to fill the semantic gap between high-level algorithm descriptions and low-level stripped binary segments.

POTENTIAL INDUSTRIAL USE-CASES

❑ Binary vulnerability assessment

❑ Memory forensics analysis

❑ Sensitive code and data segment protection

❑ Correct algorithm implementation verification and find zero-day bugs

❑ Binary level software similarity measures

ACKNOWLEDGEMENT AND REFERENCE

- This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780.

- Sun, Pengfei, Luis Garcia, and Saman Zonouz. "Tell Me More Than Just Assembly! Reversing Cyber-Physical Execution Semantics of Embedded IoT Controller Software Binaries." *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG
FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY