2021 NSF CYBER-PHYSICAL SYSTEMS PRINCIPAL INVESTIGATORS' MEETING

CAREER: Trustworthy and Adaptive Intrusion Tolerance Capabilities in Cyber-Physical Critical Infrastructures (Award # 1453046)

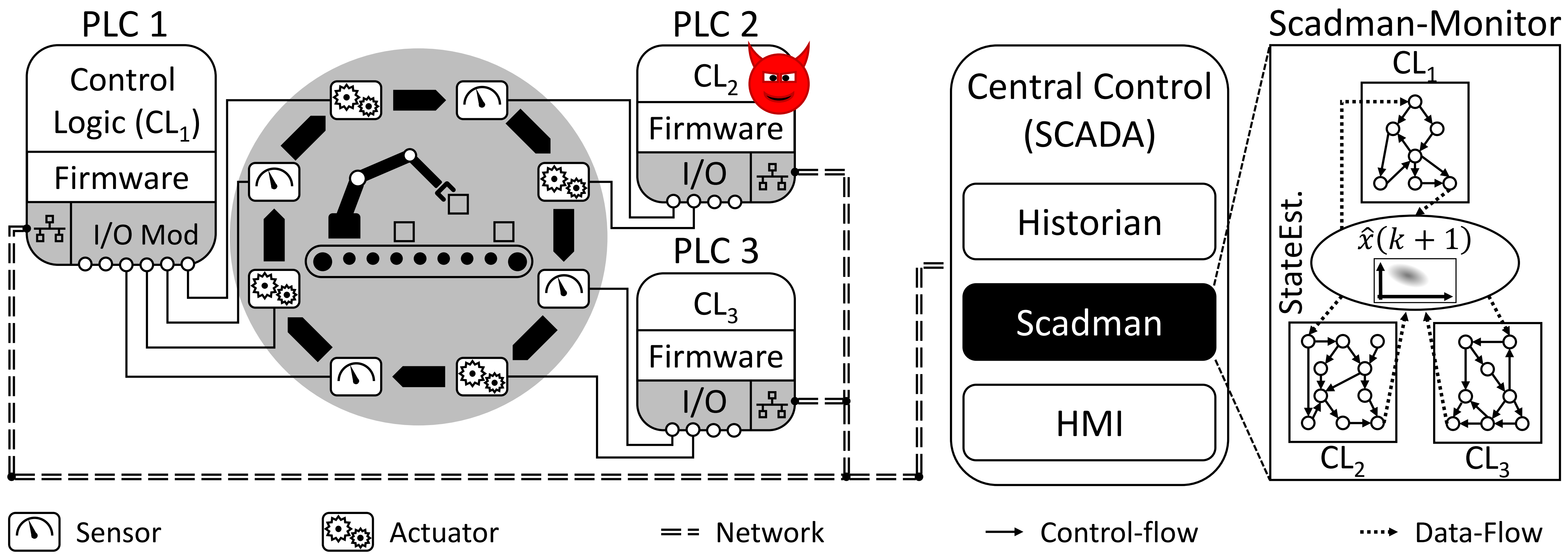
Saman Zonouz (Rutgers University)

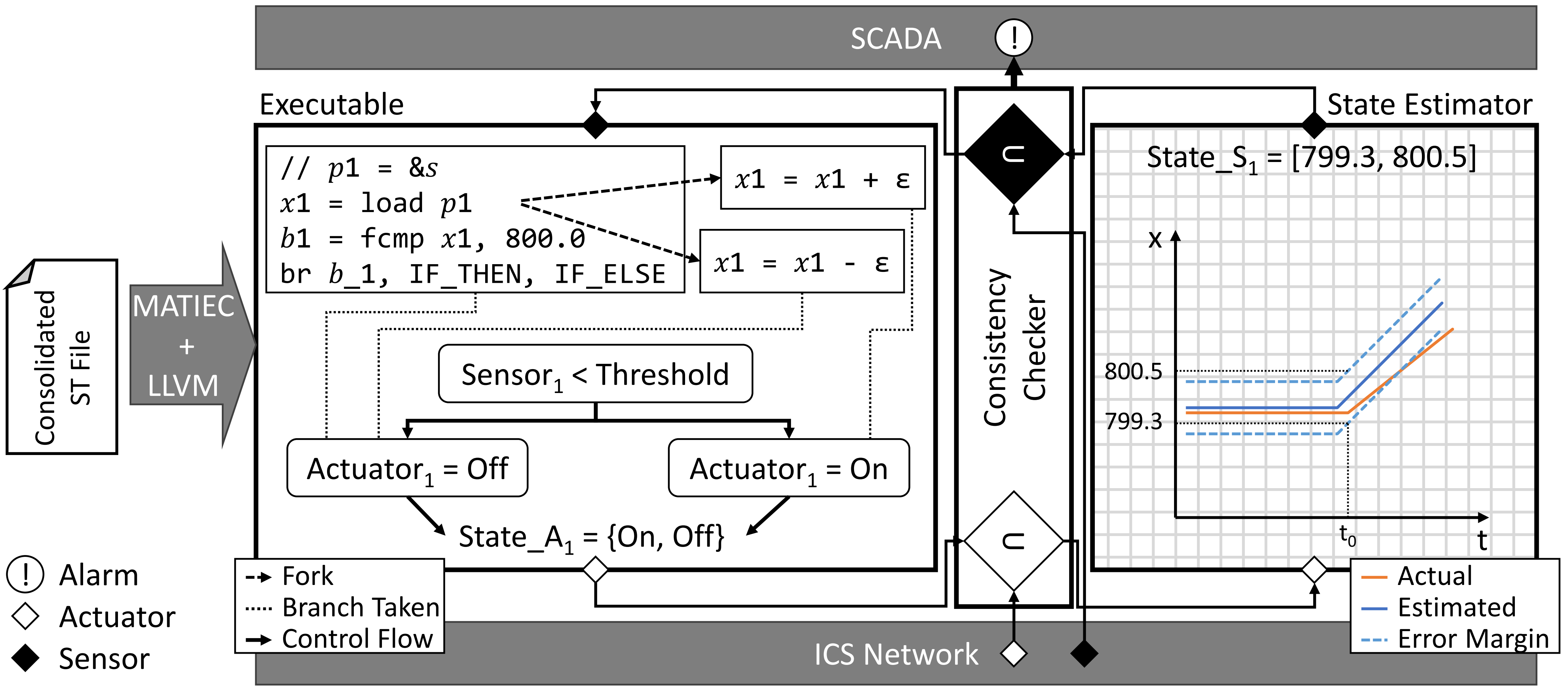
Challenge:

- Automated reverse engineering and assembly of CPS controller software for physics-aware vulnerability assessment
- Extraction of control theoretic algorithms from low-Level binary executables
- Online intrusion detection and response in ICS platforms with distributed PLC controllers

Solution:

- A CPS-specific recursive disassembler for CPS controller executables and algorithms (DSN'20)
- Automated multiple-PLC logic consolidation and predictive sensor data corruption detection using real-time cyber-physical co-simulation (ICCPS'20)

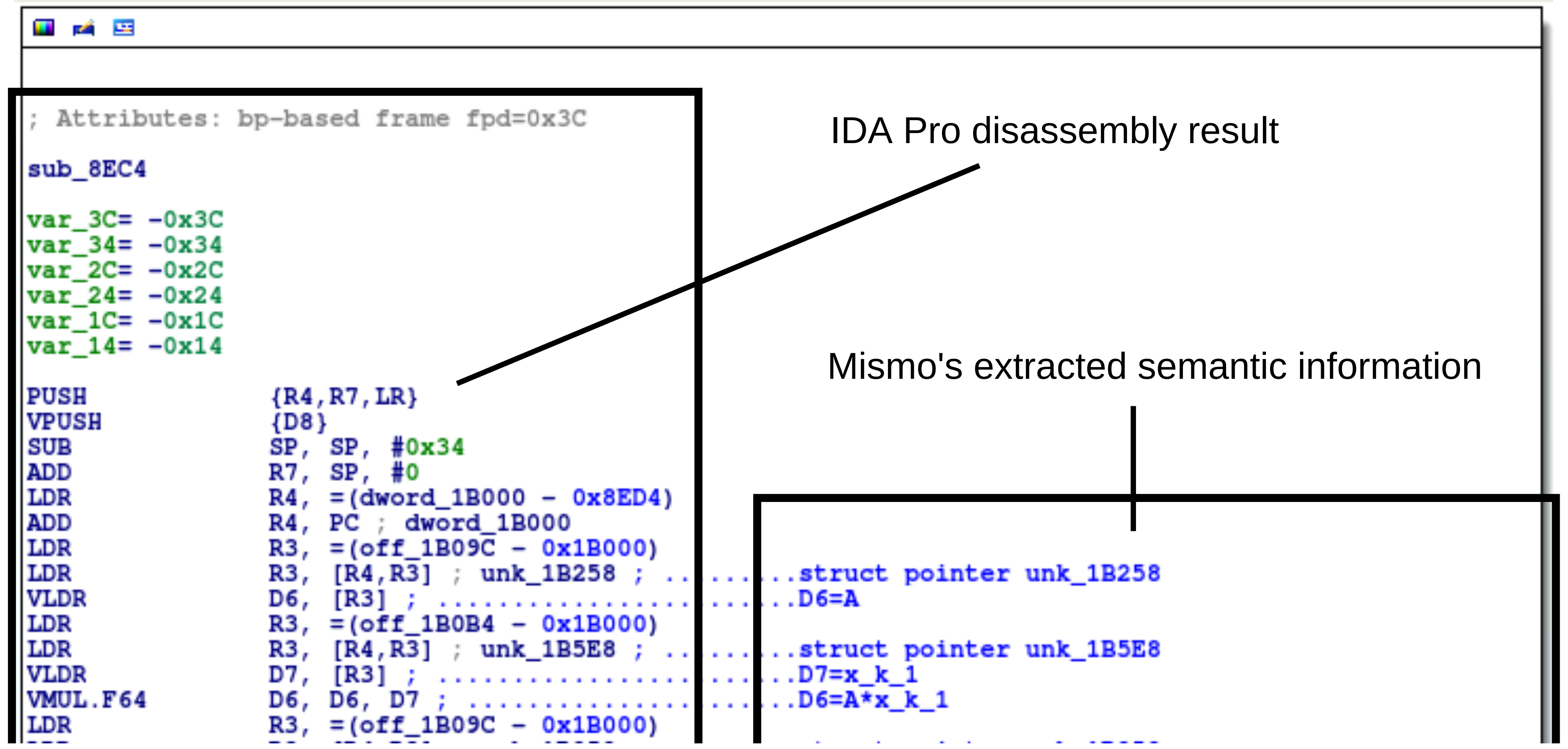




```
// p1 = &s
x1 = load p1
b1 = fcmp x1, 800.0
br b_1, IF_THEN, IF_ELSE
```

```
x1 = x1 + ε
```

```
x1 = x1 - ε
```


IDA Pro disassembly result

Mismo's extracted semantic information

```
; Attributes: bp-based frame fpd=0x3C

sub_8EC4

var_3C= -0x3C
var_34= -0x34
var_2C= -0x2C
var_24= -0x24
var_1C= -0x1C
var_14= -0x14

PUSH            {R4,R7,LR}
VPUSH           {D8}
SUB             SP, SP, #0x34
ADD             R7, SP, #0
LDR             R4, =(dword_1B000 - 0x8ED4)
ADD             R4, PC ; dword_1B000
LDR             R3, =(off_1B09C - 0x1B000)
LDR             R3, [R4,R3] ; unk_1B258 ; ...........struct pointer unk_1B258
VLDR            D6, [R3] ; ........................D6=A
LDR             R3, =(off_1B0B4 - 0x1B000)
LDR             R3, [R4,R3] ; unk_1B5E8 ; ...........struct pointer unk_1B5E8
VLDR            D7, [R3] ; ........................D7=x_k_1
VMUL.F64        D6, D6, D7 ; ......................D6=A*x_k_1
LDR             R3, =(off_1B09C - 0x1B000)
```

Scientific Impact:

- Our CPS controller reverse engineering and physics-aware vulnerability assessment applies to all CPS domains
- Our online cyber-physical intrusion detection using programming language techniques is generalizable to other domains fairly simply

Broader Impact:

- ICS operators can detect and response to attacks and anomalies with high accuracy in real-time
- Security analysts can perform efficient CPS-specific malware analysis and reverse engineering
- Edu: we worked with several undergraduates on research projects; and developed teaching modules for malware analysis