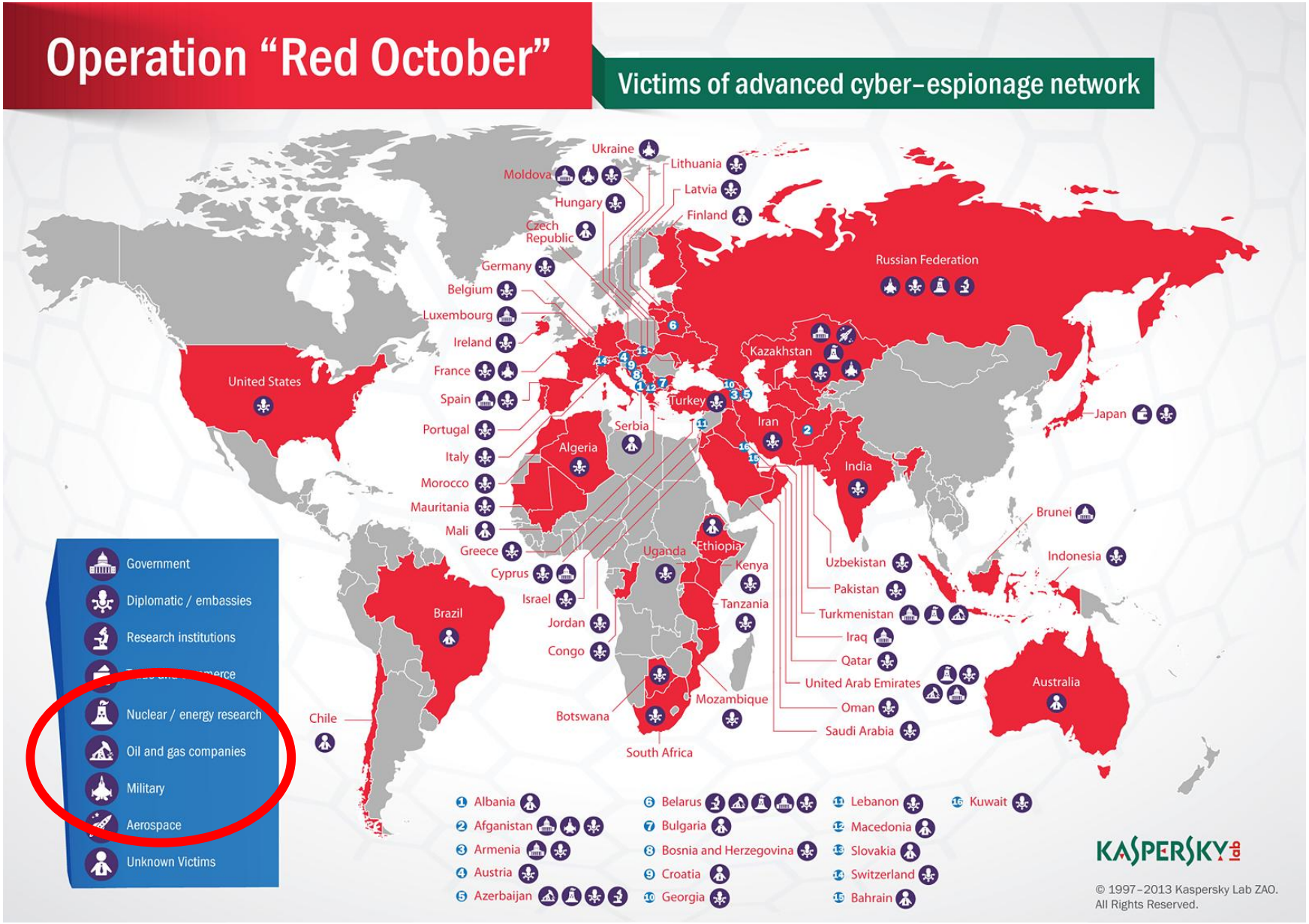
A malware-tolerant, self-healing Industrial Control System framework

Michael Denzel, Mark Ryan, Eike Ritter
University of Birmingham

2017-05-29



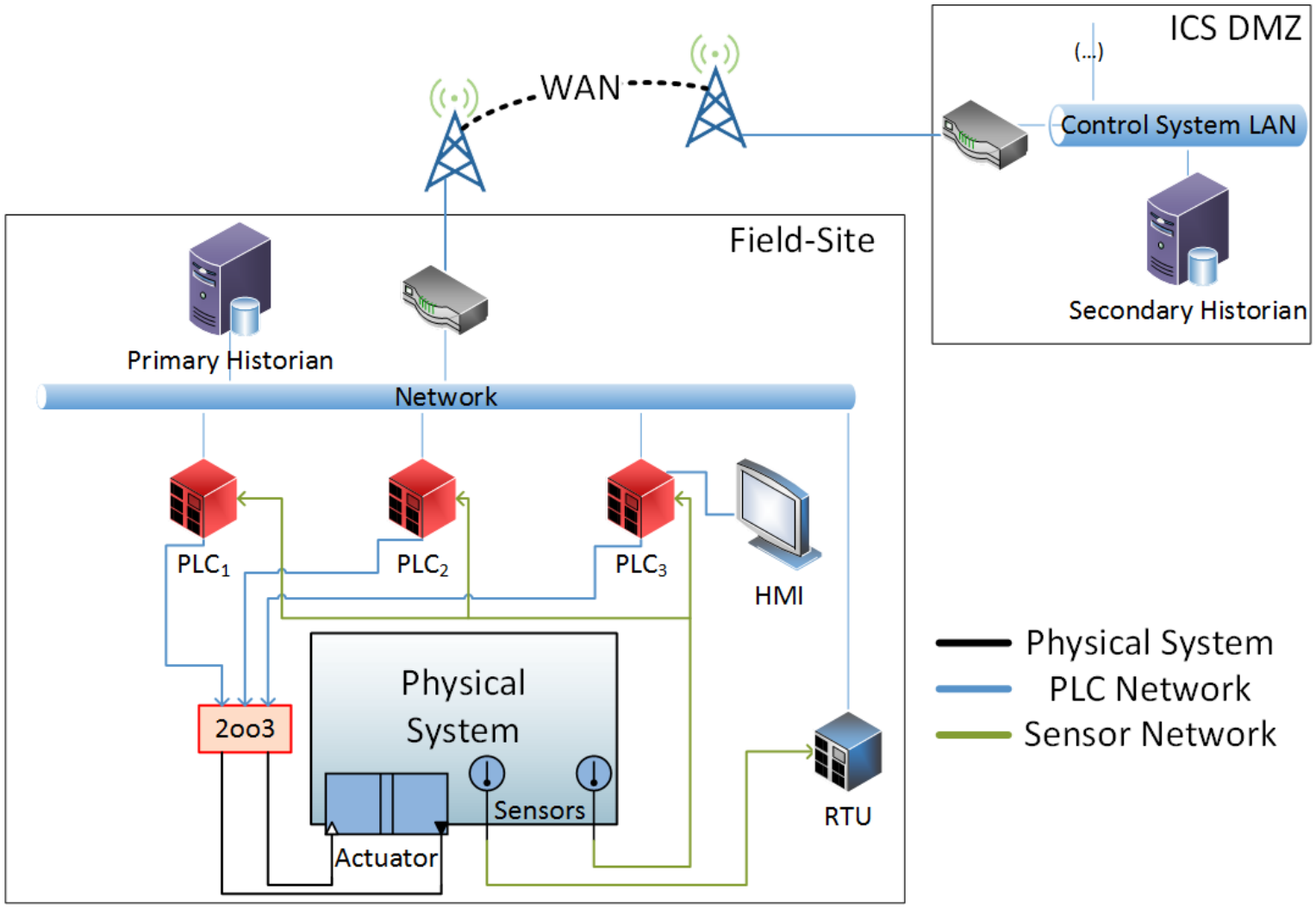
https://cdn.securelist.com/files/2013/01/208194085.png

Malware Tolerance: Distribute Trust!

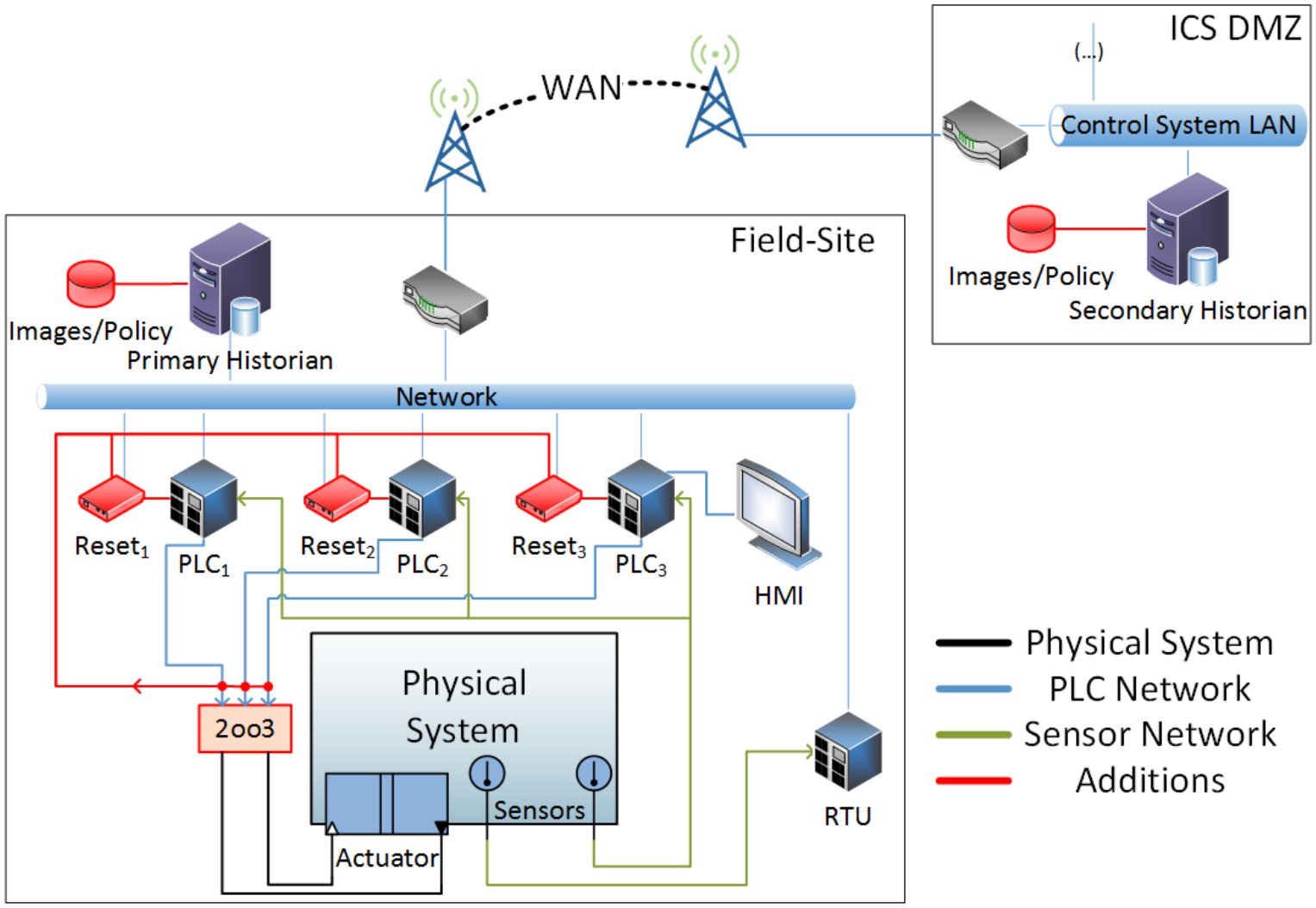
Proposed Architecture

1. Malware-tolerant (ICS-)network
2. Self-healing hardware
3. Self-healing operating system

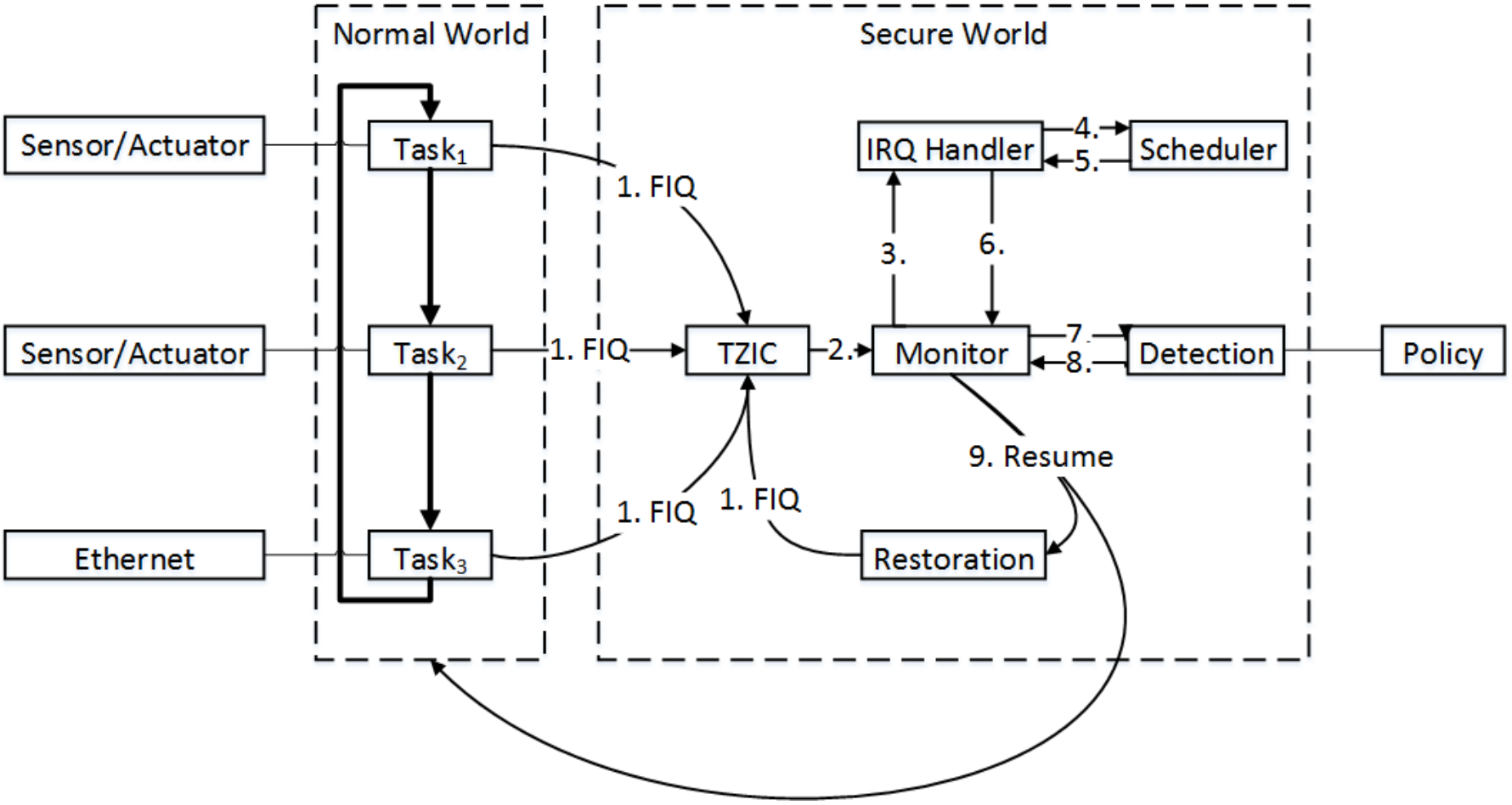
Malware Tolerant Architecture



Self-healing Hardware



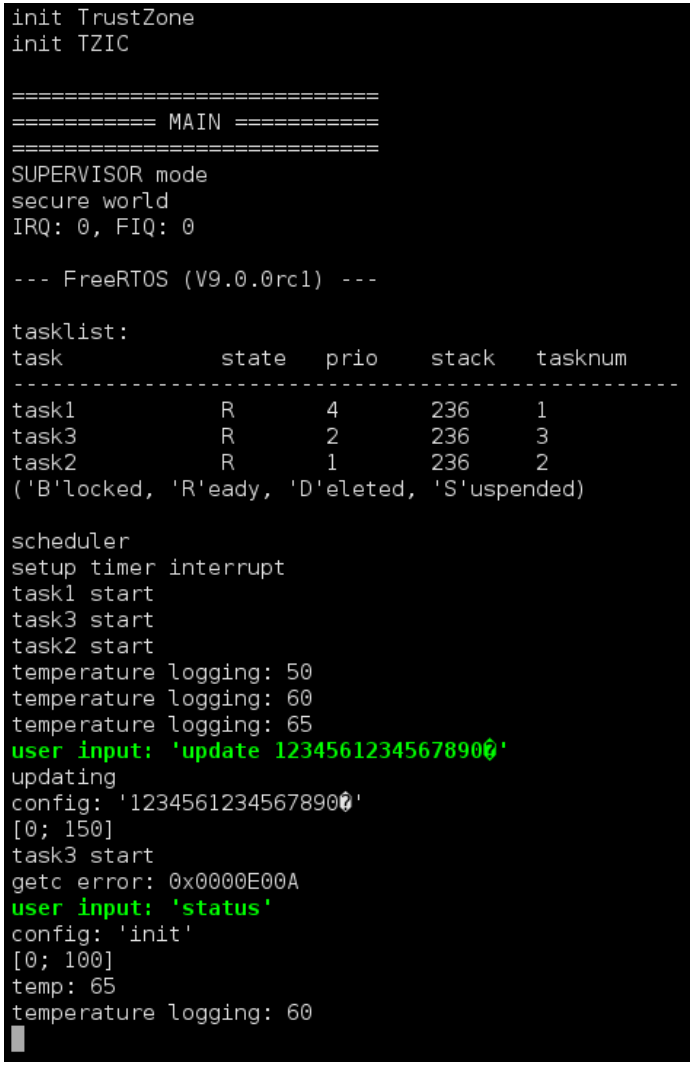
Self-healing Operating System



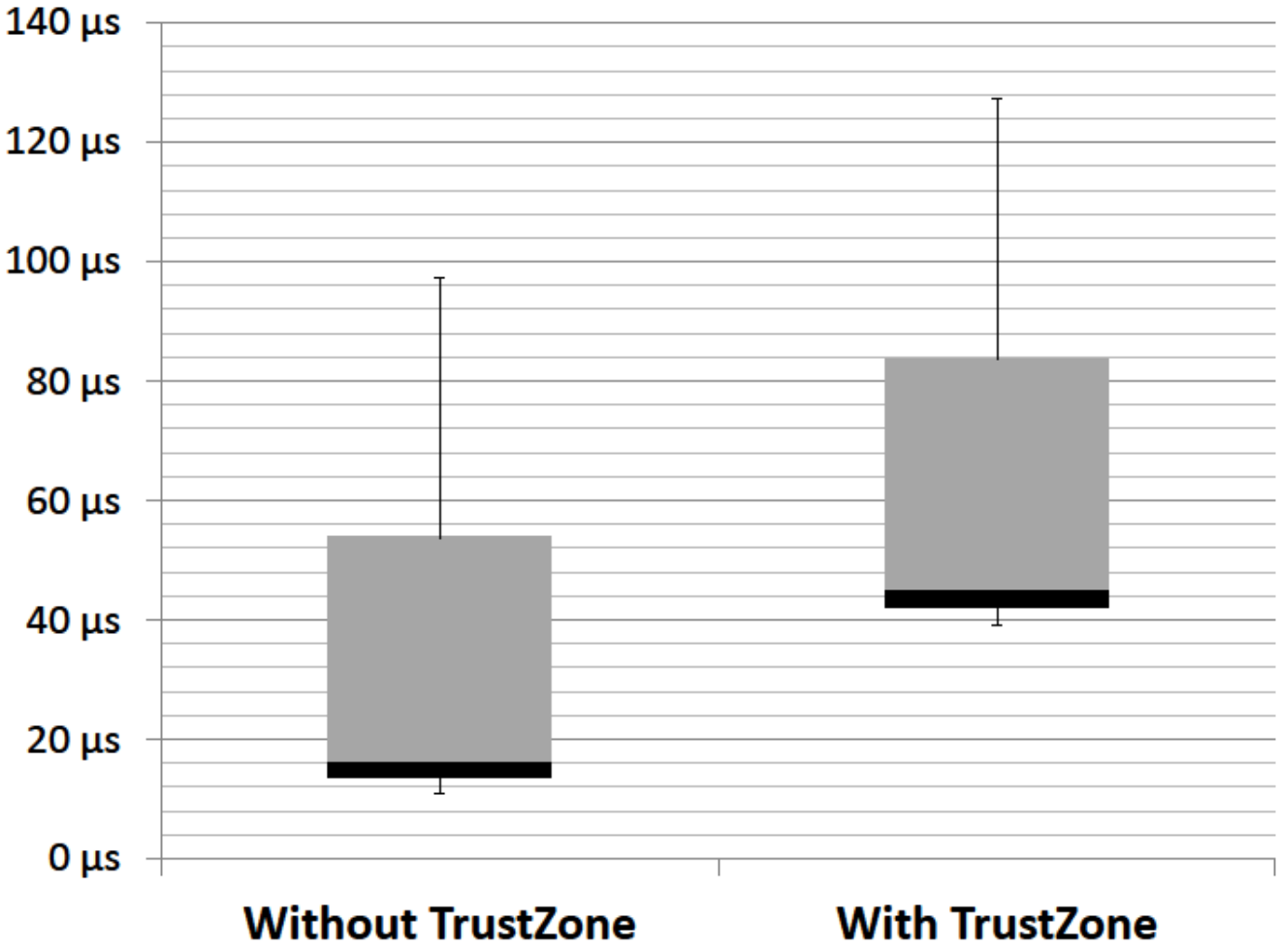
Results: Attacks

```
typedef struct temperature{
    char info[16];
    int max;
    int min;
} temperature;

void set_config_temperature(char* str){
    strcpy(temp_config.info, str);
}
```



Results: Performance TrustZone



Results: ProVerif proofs

№	Compromised Devices	1^{st} Iteration (1.)	2^{nd} Iteration (2.)	Self-Healing (3.)	(4.)	End reached (5.)
1	None	✓	✓	✓	✓	✓
2	PLC_1	✓	✓	✓	✓	✓
3	PLC_2	✓	✓	✓	✓	✓
4	PLC_3	✓	✓	✓	✓	✓
5	2oo3					✓
6	R_1	✓	✓			✓
7	R_2	✓	✓			✓
8	R_3	✓	✓			✓
9	PLC_1, R_1	✓	✓			✓
10	PLC_2, R_2	✓	✓			✓
11	PLC_3, R_3	✓	✓			✓
12	PLC_1, R_2	✓				✓
13	PLC_1, PLC_2					✓
14	PLC_1, 2oo3					✓
15	2oo3, R_1					✓
16	R_1, R_2	✓				✓
17	PLC_{1-3}					✓
18	PLC_{1-2}, 2oo3					✓
19	PLC_1, 2oo3, R_1					✓
20	2oo3, R_{1-2}					✓
21	PLC_1, R_{1-2}	✓				✓
22	PLC_1, R_{2-3}	✓				✓
23	R_{1-3}	✓				✓
24	All					✓

Summary

1. Malware-tolerant ICS
2. Self-healing hardware
3. Self-healing operating system (stay online as long as possible)

Thank you!