

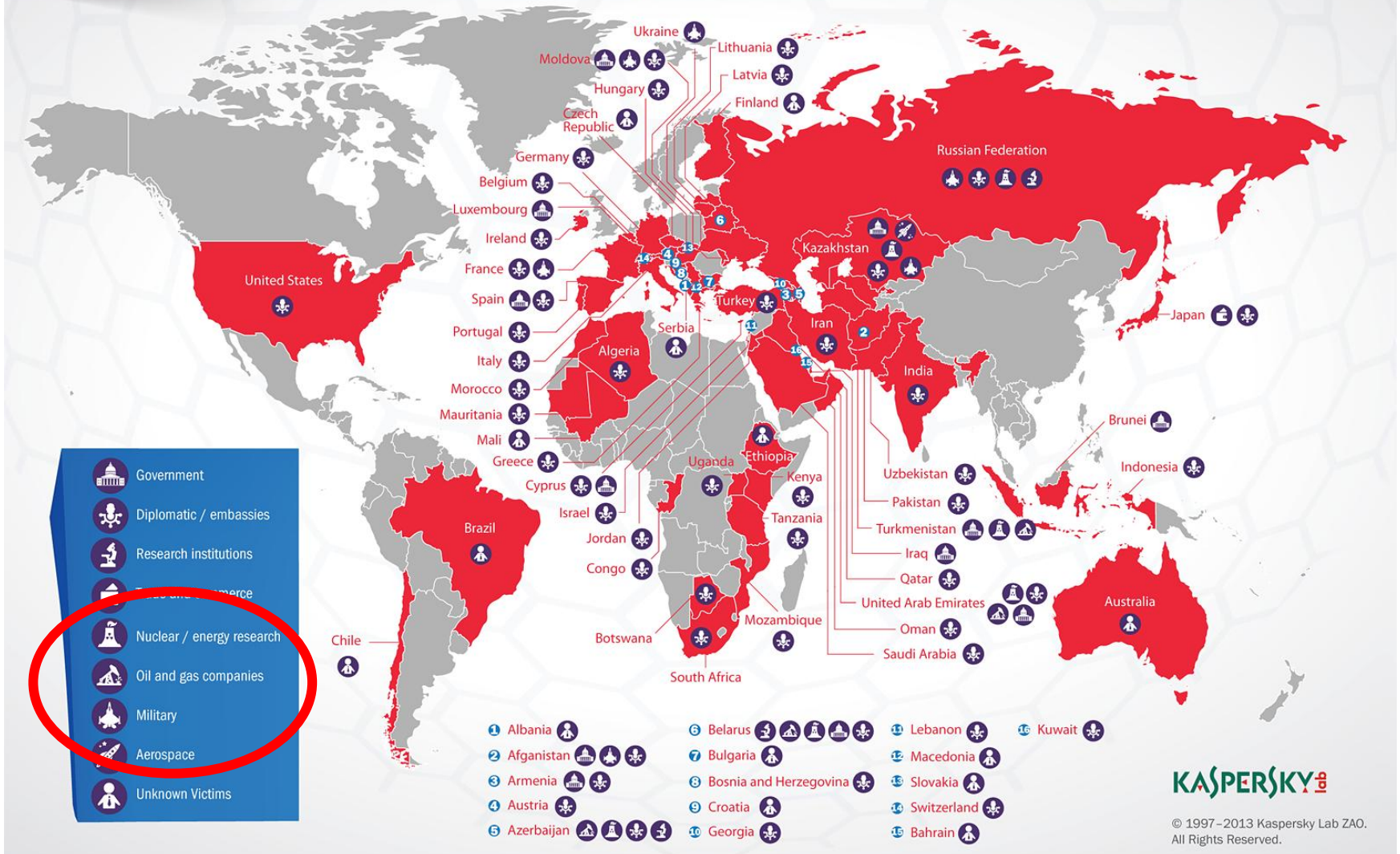
A malware-tolerant, self-healing Industrial Control System framework

Michael Denzel, Mark Ryan, Eike Ritter
University of Birmingham

2017-05-29

Operation "Red October"

Victims of advanced cyber-espionage network



KASPERSKY

© 1997–2013 Kaspersky Lab ZAO. All Rights Reserved.

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

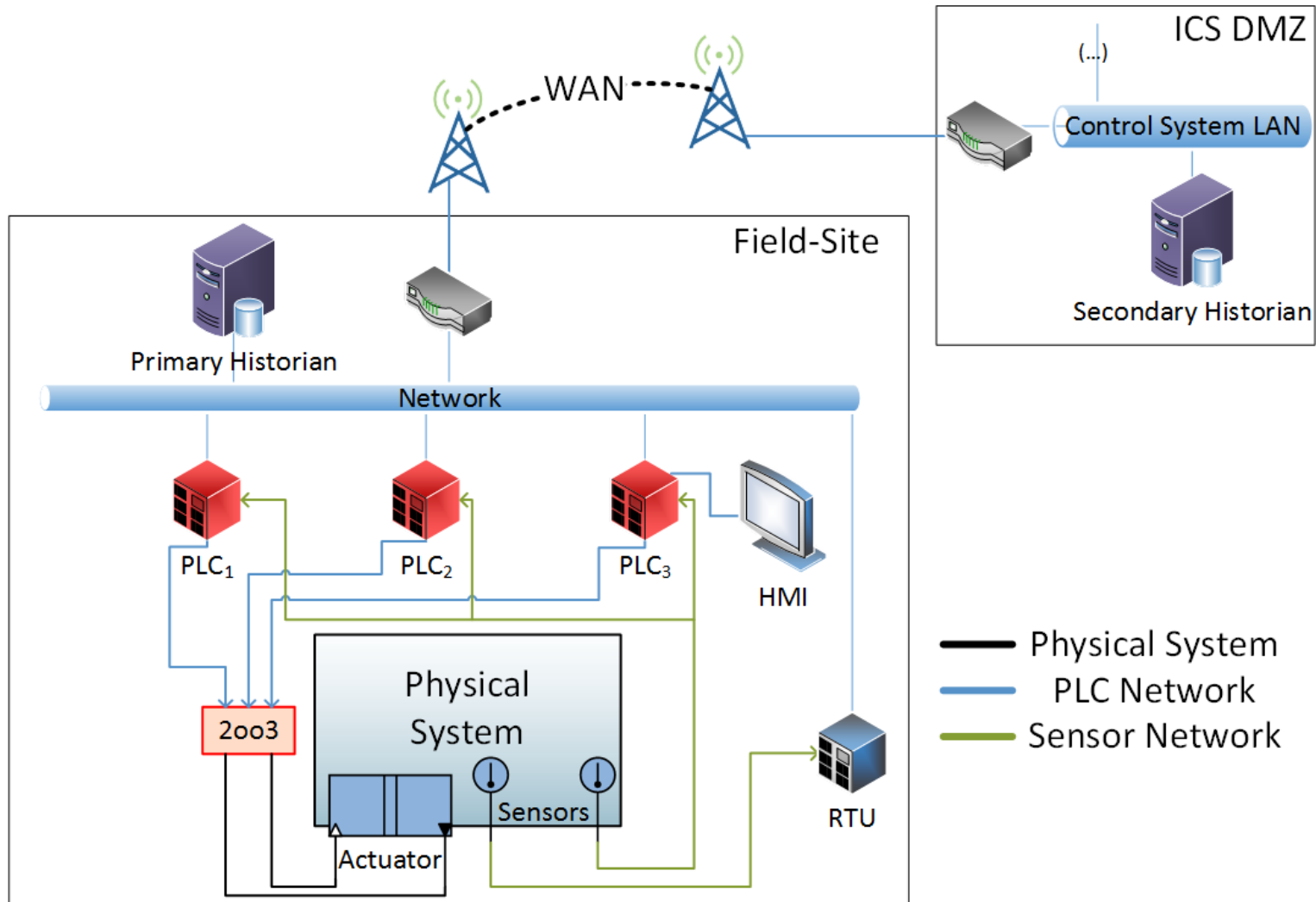
Malware Tolerance: Distribute Trust!



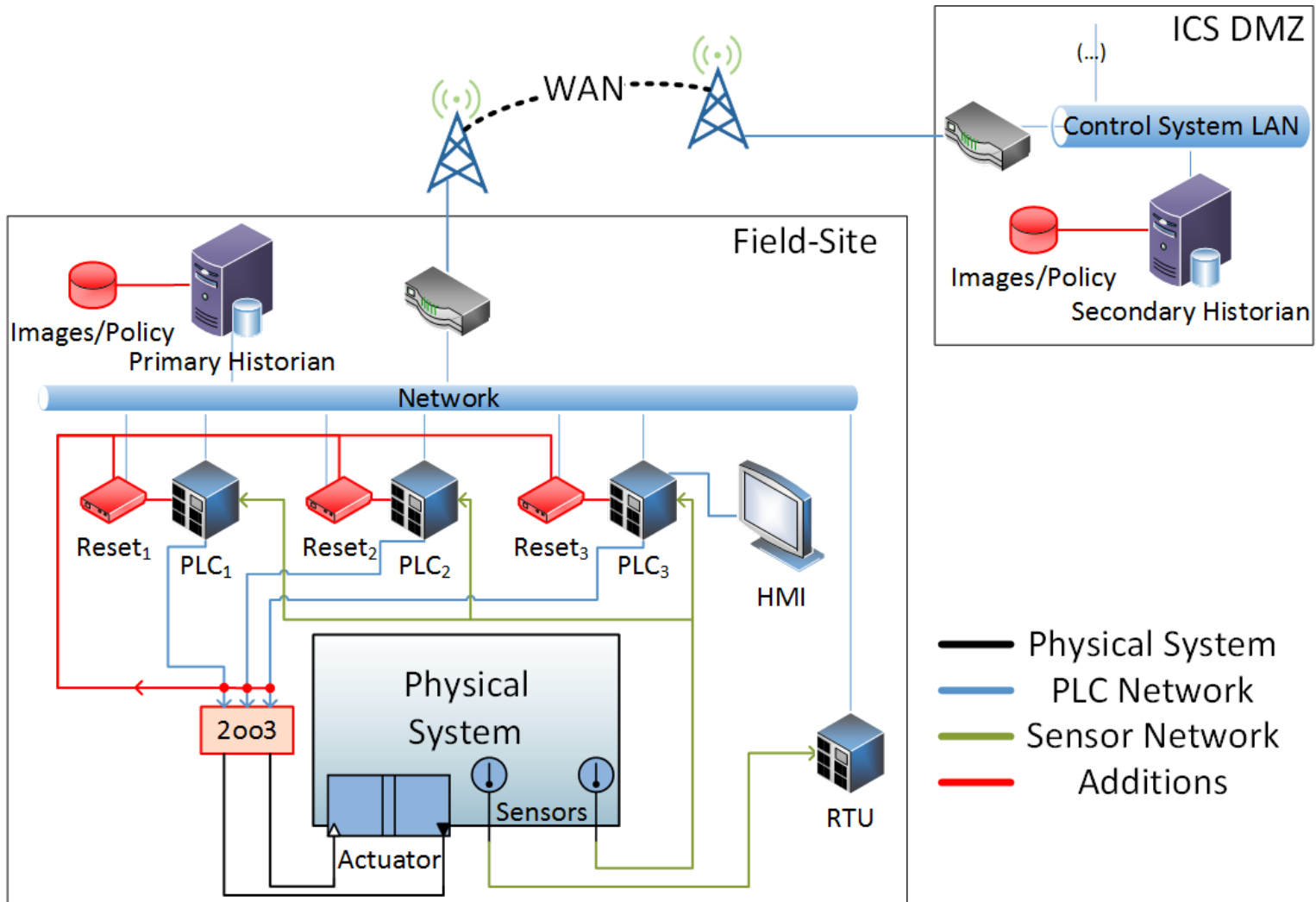
Proposed Architecture

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

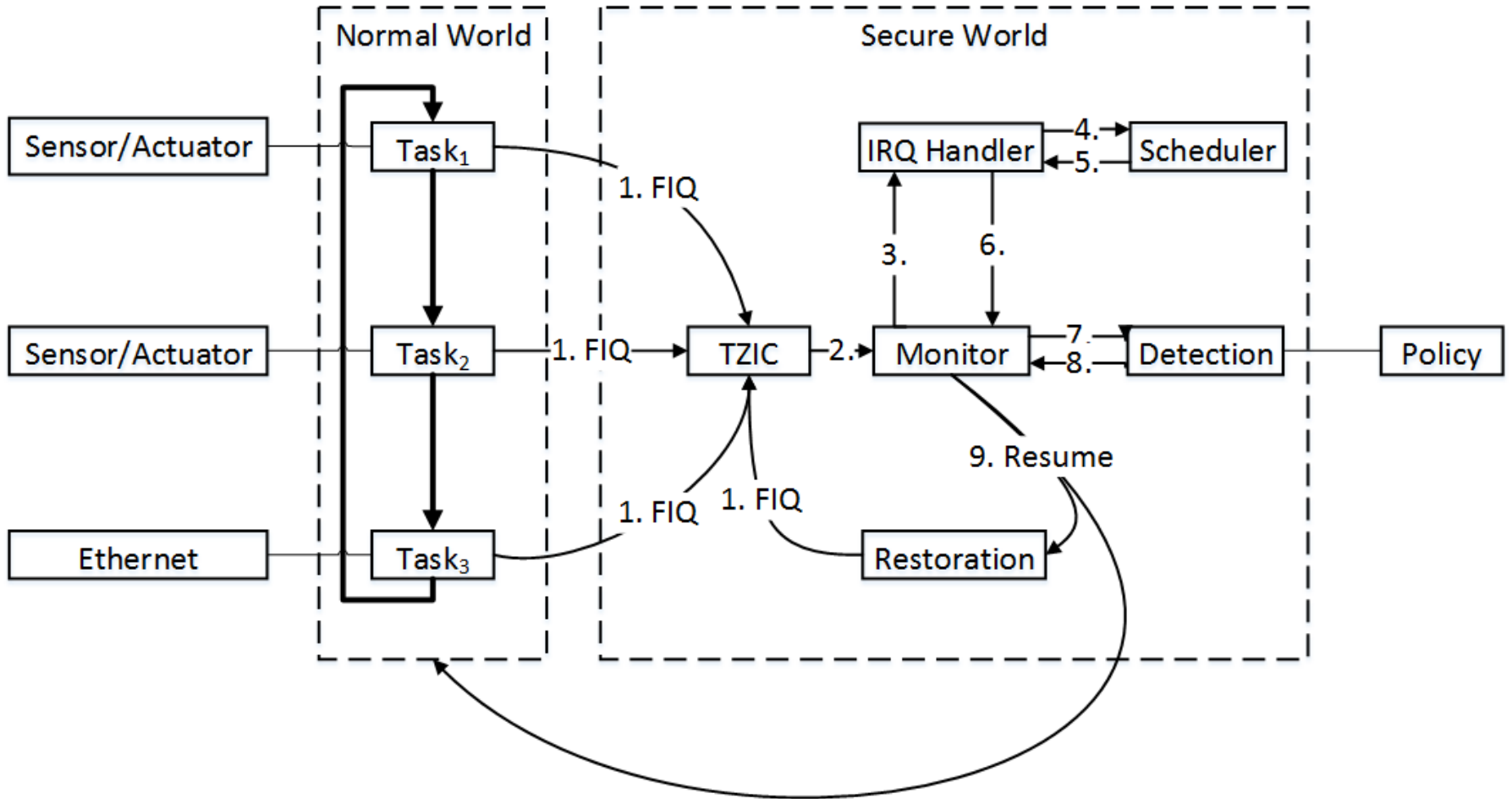
Malware Tolerant Architecture



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);
}
```

```
init TrustZone
init TZIC

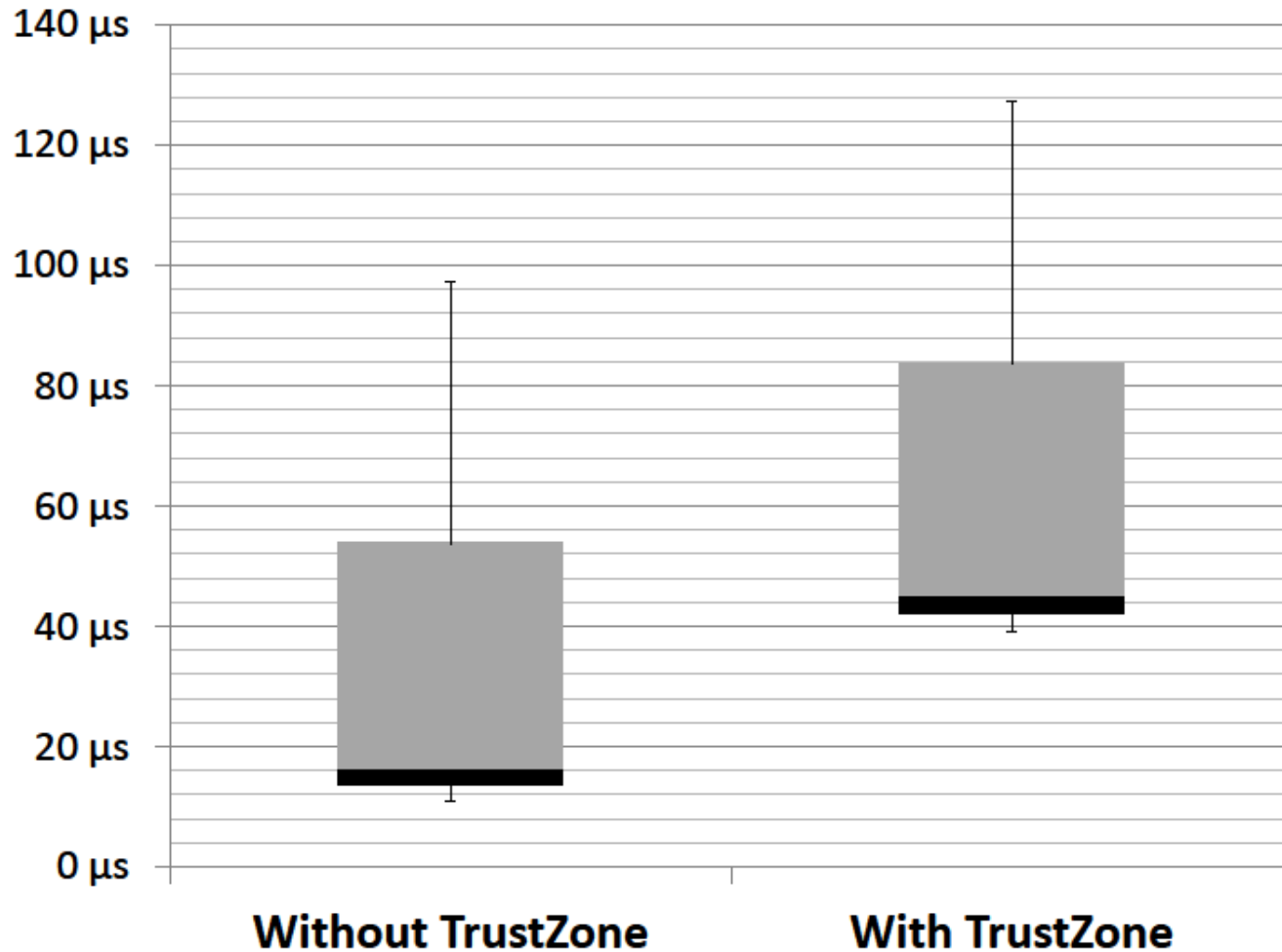
=====
===== MAIN =====
=====
SUPERVISOR mode
secure world
IRQ: 0, FIQ: 0

--- FreeRTOS (V9.0.0rc1) ---

tasklist:
task          state  prio  stack  tasknum
-----
task1         R      4     236    1
task3         R      2     236    3
task2         R      1     236    2
('B'locked, 'R'eady, 'D'eleted, 'S'uspended)

scheduler
setup timer interrupt
task1 start
task3 start
task2 start
temperature logging: 50
temperature logging: 60
temperature logging: 65
user input: 'update 1234561234567890'
updating
config: '1234561234567890'
[0; 150]
task3 start
getc error: 0x0000E00A
user input: 'status'
config: 'init'
[0; 100]
temp: 65
temperature logging: 60
```


Results: Performance TrustZone



Results: ProVerif proofs

№	Compromised Devices	1 st Iteration	2 nd Iteration	Self-Healing		End reached
		(1.)	(2.)	(3.)	(4.)	(5.)
1	None	✓	✓	✓	✓	✓
2	<i>PLC</i> ₁	✓	✓	✓	✓	✓
3	<i>PLC</i> ₂	✓	✓	✓	✓	✓
4	<i>PLC</i> ₃	✓	✓	✓	✓	✓
5	2003					✓
6	<i>R</i> ₁	✓	✓			✓
7	<i>R</i> ₂	✓	✓			✓
8	<i>R</i> ₃	✓	✓			✓
9	<i>PLC</i> ₁ , <i>R</i> ₁	✓	✓			✓
10	<i>PLC</i> ₂ , <i>R</i> ₂	✓	✓			✓
11	<i>PLC</i> ₃ , <i>R</i> ₃	✓	✓			✓
12	<i>PLC</i> ₁ , <i>R</i> ₂	✓				✓
13	<i>PLC</i> ₁ , <i>PLC</i> ₂					✓
14	<i>PLC</i> ₁ , 2003					✓
15	2003, <i>R</i> ₁					✓
16	<i>R</i> ₁ , <i>R</i> ₂	✓				✓
17	<i>PLC</i> ₁₋₃					✓
18	<i>PLC</i> ₁₋₂ , 2003					✓
19	<i>PLC</i> ₁ , 2003, <i>R</i> ₁					✓
20	2003, <i>R</i> ₁₋₂					✓
21	<i>PLC</i> ₁ , <i>R</i> ₁₋₂	✓				✓
22	<i>PLC</i> ₁ , <i>R</i> ₂₋₃	✓				✓
23	<i>R</i> 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!