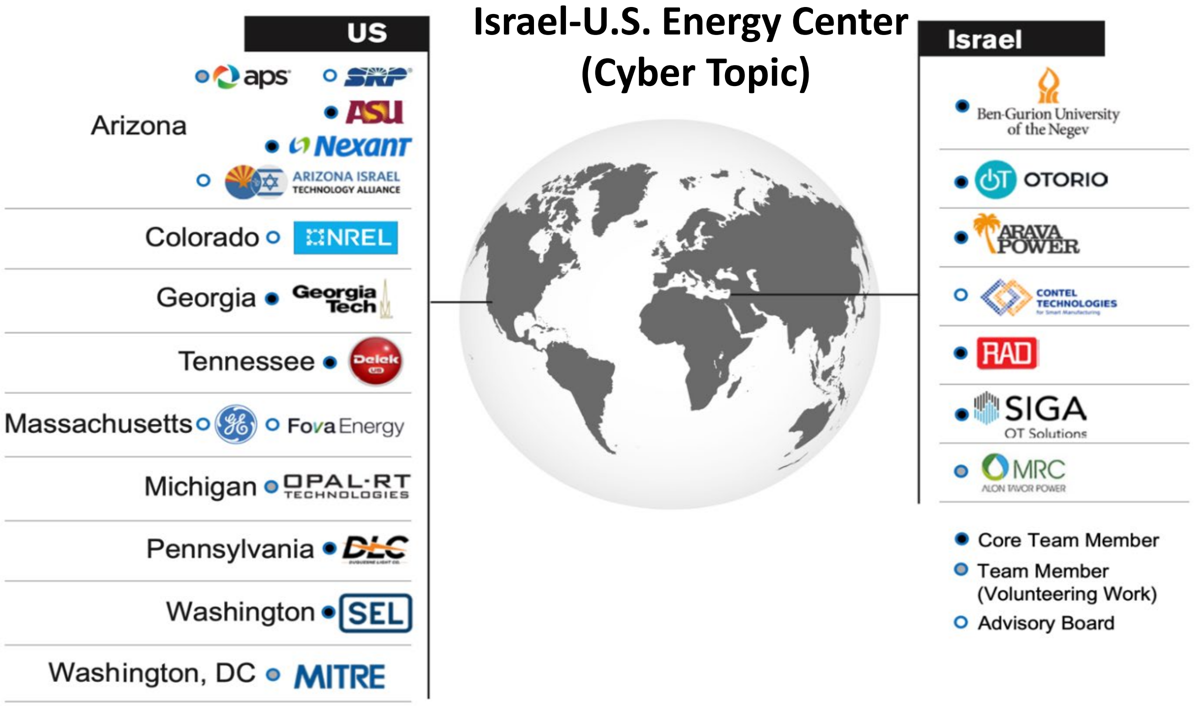
# Cybersecurity Technology for Critical Power Infrastructure AI-Based Centralized Defense and Edge Resilience

## Quarterly Review Workshop IV



Israel-U.S. Energy Center
(Cyber Topic)

US

Arizona ○ aps ○ SRP ● ASU ● Nexant ○ Arizona Israel Technology Alliance

Colorado ○ NREL

Georgia ● Georgia Tech

Tennessee ● Delek US

Massachusetts ○ GE ○ Fova Energy

Michigan ○ OPAL-RT Technologies

Pennsylvania ● DLC

Washington ● SEL

Washington, DC ○ MITRE

Israel

● Ben-Gurion University of the Negev

● OTORIO

● Arava Power

○ Contel Technologies

● RAD

● SIGA OT Solutions

○ MRC Alon Tavor Power

● Core Team Member

○ Team Member (Volunteering Work)

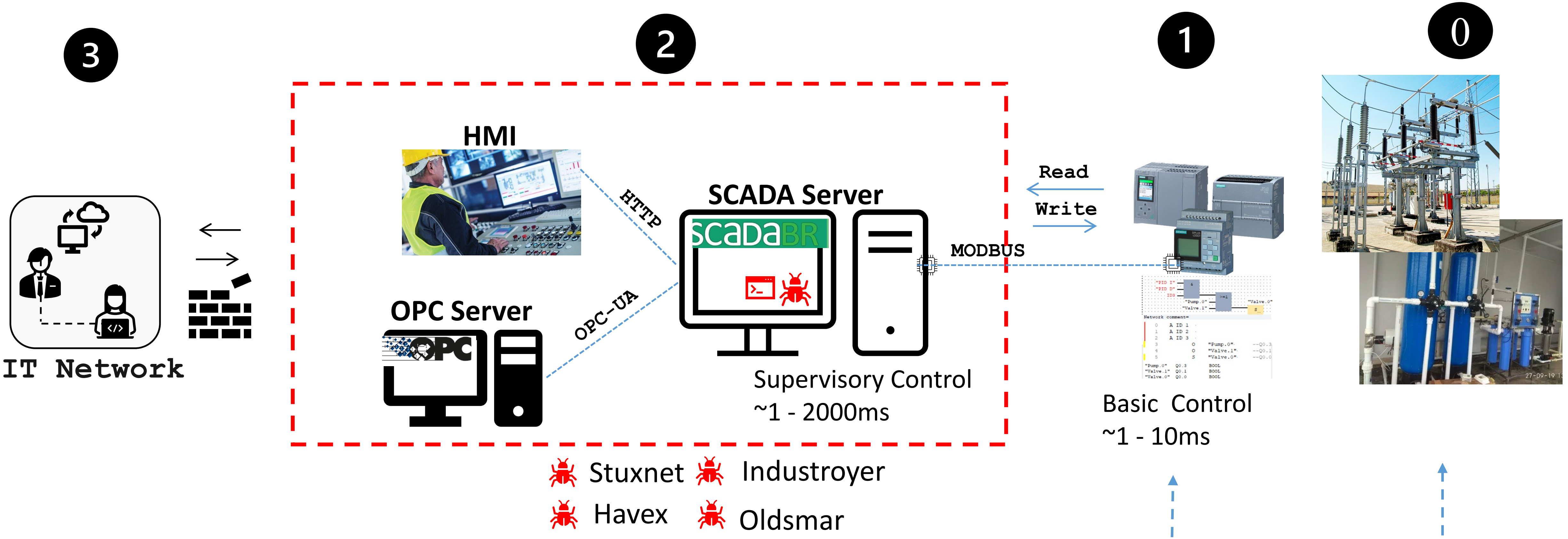
○ Advisory Board

## Task 7

## **Malware Threat Mitigation**

Dr. Wenke Lee, Moses Ike
Georgia Institute of Technology
March 21, 2023

# Detecting Malware Code Execution in SCADA Hosts



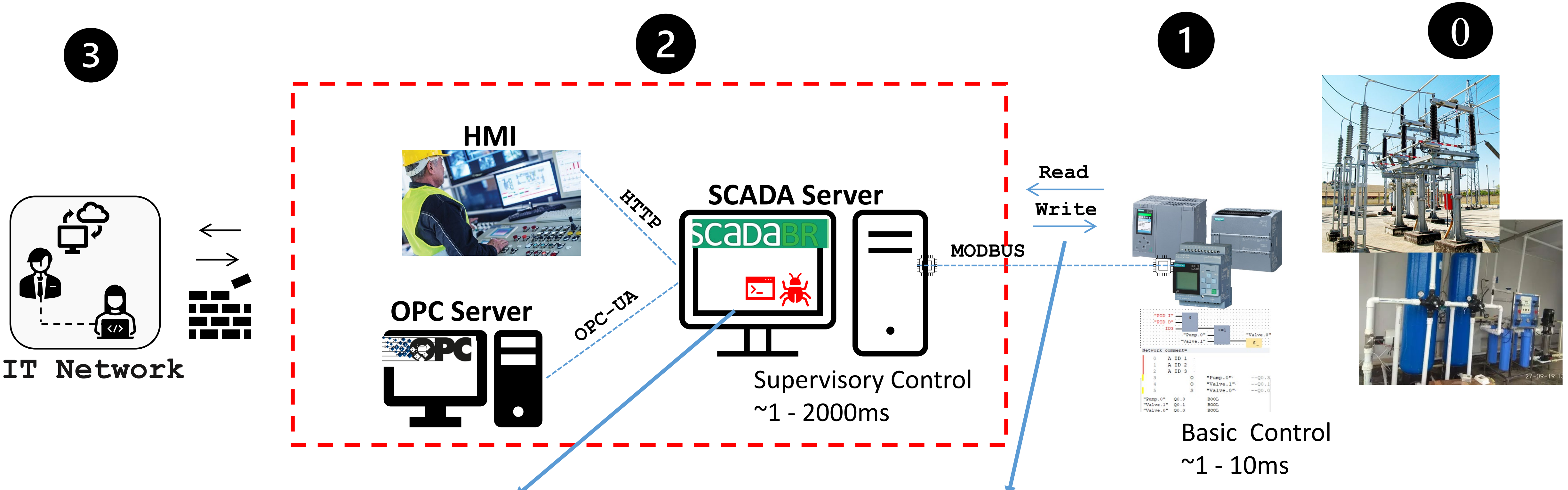
- SCADA is the critical-path for a cyber attacker to disrupt/damage the physical side
- Majority of in-the-Wild  ICS malware were launched from the SCADA hosts systems

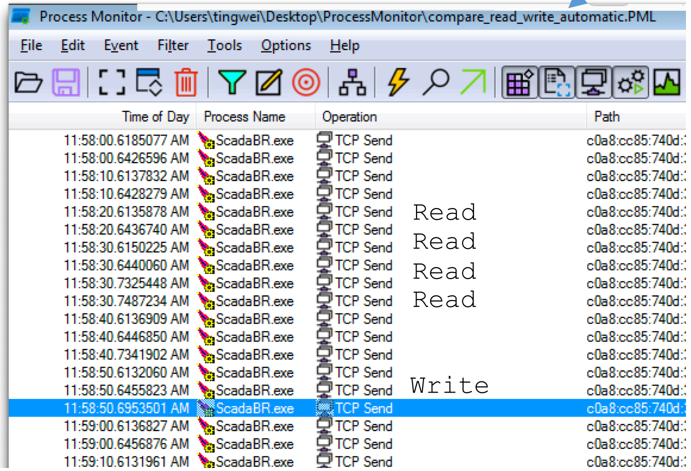
Focus for BIRD Task 14
Dr. Surkano
Controller Tolerance
and Resilience

Focus for BIRD Task 11
Dr. Yisroel
AI-based Intrusion
Detection

**Task 7 Integration Collaborators**

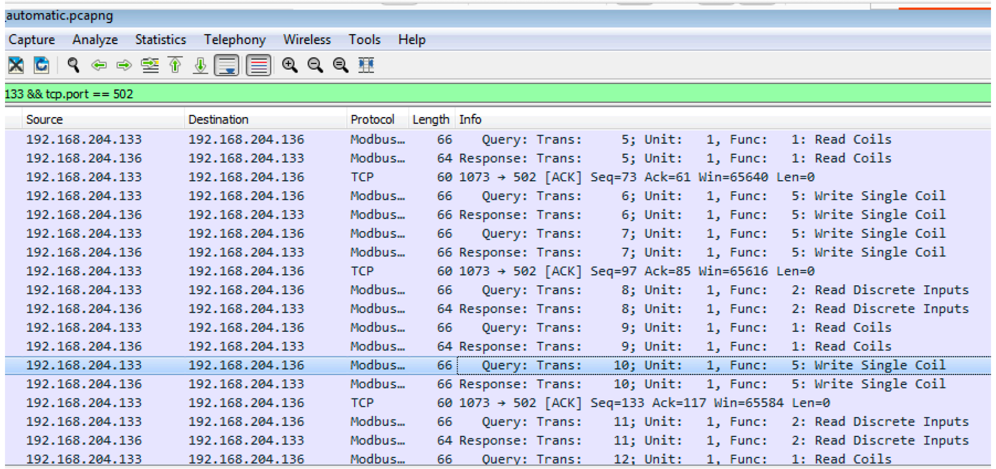
# SCADA Host Execution vs. Network Traffic Analysis





Process Monitor - C:\Users\tingwei\Desktop\ProcessMonitor\compare_read_write_automatic.PML

```
       Time of Day  Process Name  Operation          Path
11:58:00.6185077 AM ScadaBR.exe   TCP Send           c0a8:cc85:740d:
11:58:00.6426596 AM ScadaBR.exe   TCP Send           c0a8:cc85:740d:
11:58:10.6137832 AM ScadaBR.exe   TCP Send           c0a8:cc85:740d:
11:58:10.6428279 AM ScadaBR.exe   TCP Send           c0a8:cc85:740d:
11:58:20.6135878 AM ScadaBR.exe   TCP Send   Read    c0a8:cc85:740d:
11:58:20.6436740 AM ScadaBR.exe   TCP Send   Read    c0a8:cc85:740d:
11:58:30.6150225 AM ScadaBR.exe   TCP Send   Read    c0a8:cc85:740d:
11:58:30.6440060 AM ScadaBR.exe   TCP Send   Read    c0a8:cc85:740d:
11:58:30.7325448 AM ScadaBR.exe   TCP Send           c0a8:cc85:740d:
11:58:30.7487234 AM ScadaBR.exe   TCP Send           c0a8:cc85:740d:
11:58:40.6136909 AM ScadaBR.exe   TCP Send           c0a8:cc85:740d:
11:58:40.6446850 AM ScadaBR.exe   TCP Send           c0a8:cc85:740d:
11:58:40.7341902 AM ScadaBR.exe   TCP Send           c0a8:cc85:740d:
11:58:50.6132060 AM ScadaBR.exe   TCP Send           c0a8:cc85:740d:
11:58:50.6455823 AM ScadaBR.exe   TCP Send   Write   c0a8:cc85:740d:
11:58:50.6953501 AM ScadaBR.exe   TCP Send           c0a8:cc85:740d:
11:59:00.6136827 AM ScadaBR.exe   TCP Send           c0a8:cc85:740d:
11:59:00.6456876 AM ScadaBR.exe   TCP Send           c0a8:cc85:740d:
11:59:10.6131961 AM ScadaBR.exe   TCP Send           c0a8:cc85:740d:
```



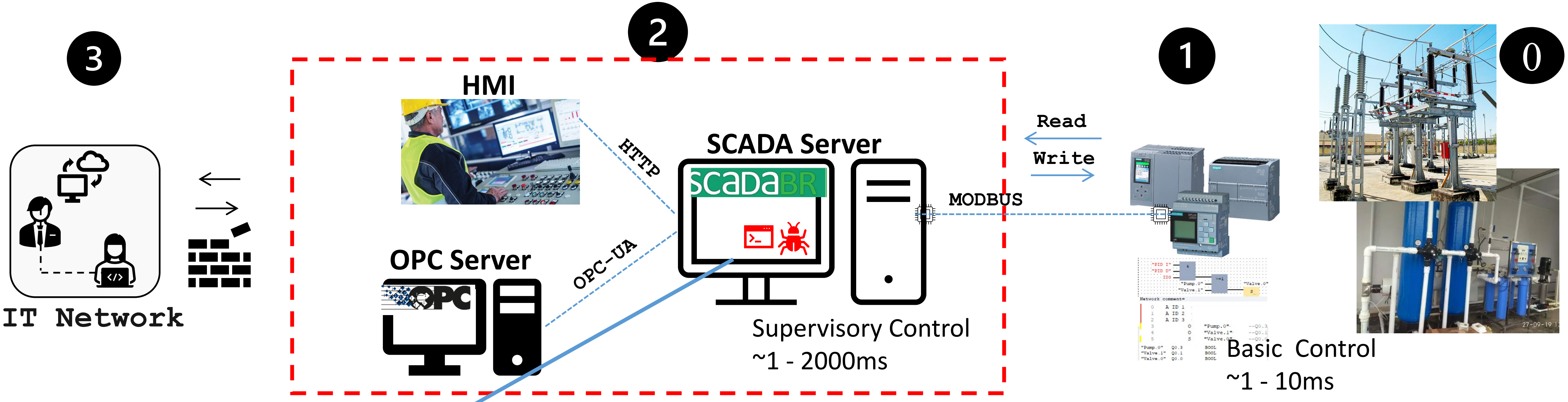
automatic.pcapng

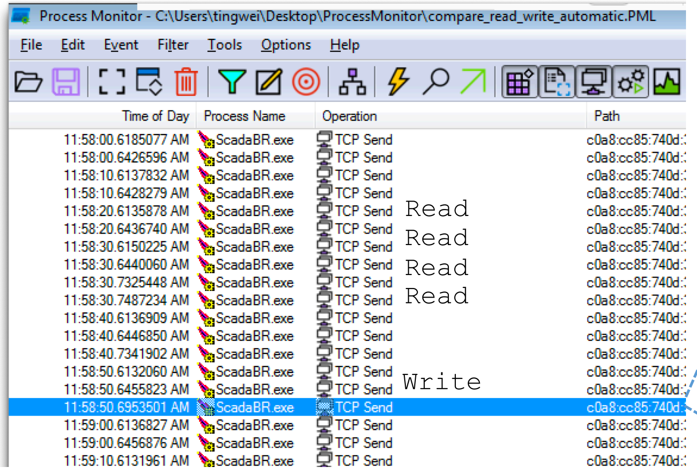
133 && tcp.port == 502

```
Source          Destination     Protocol  Length Info
192.168.204.133 192.168.204.136 Modbus…   66     Query: Trans:     5; Unit:   1, Func:   1: Read Coils
192.168.204.136 192.168.204.133 Modbus…   64  Response: Trans:     5; Unit:   1, Func:   1: Read Coils
192.168.204.133 192.168.204.136 TCP       60  1073 → 502 [ACK] Seq=73 Ack=61 Win=65640 Len=0
192.168.204.133 192.168.204.136 Modbus…   66     Query: Trans:     6; Unit:   1, Func:   5: Write Single Coil
192.168.204.136 192.168.204.133 Modbus…   66  Response: Trans:     6; Unit:   1, Func:   5: Write Single Coil
192.168.204.133 192.168.204.136 Modbus…   66     Query: Trans:     7; Unit:   1, Func:   5: Write Single Coil
192.168.204.136 192.168.204.133 Modbus…   66  Response: Trans:     7; Unit:   1, Func:   5: Write Single Coil
192.168.204.133 192.168.204.136 TCP       60  1073 → 502 [ACK] Seq=97 Ack=85 Win=65616 Len=0
192.168.204.133 192.168.204.136 Modbus…   66     Query: Trans:     8; Unit:   1, Func:   2: Read Discrete Inputs
192.168.204.136 192.168.204.133 Modbus…   64  Response: Trans:     8; Unit:   1, Func:   2: Read Discrete Inputs
192.168.204.133 192.168.204.136 Modbus…   66     Query: Trans:     9; Unit:   1, Func:   1: Read Coils
192.168.204.136 192.168.204.133 Modbus…   64  Response: Trans:     9; Unit:   1, Func:   1: Read Coils
192.168.204.133 192.168.204.136 Modbus…   66     Query: Trans:    10; Unit:   1, Func:   5: Write Single Coil
192.168.204.136 192.168.204.133 Modbus…   66  Response: Trans:    10; Unit:   1, Func:   5: Write Single Coil
192.168.204.133 192.168.204.136 TCP       60  1073 → 502 [ACK] Seq=133 Ack=117 Win=65584 Len=0
192.168.204.133 192.168.204.136 Modbus…   66     Query: Trans:    11; Unit:   1, Func:   2: Read Discrete Inputs
192.168.204.136 192.168.204.133 Modbus…   64  Response: Trans:    11; Unit:   1, Func:   2: Read Discrete Inputs
192.168.204.133 192.168.204.136 Modbus…   66     Query: Trans:    12; Unit:   1, Func:   1: Read Coils
```

Who is issuing observed commands? Attacker or legitimate SCADA ?

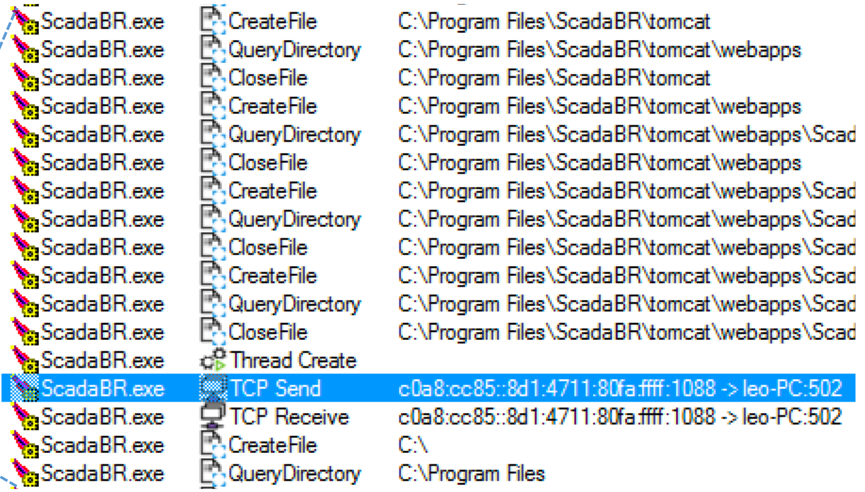
# Physical-Bound SCADA Host Execution





Process Monitor - C:\Users\tingwei\Desktop\ProcessMonitor\compare_read_write_automatic.PML

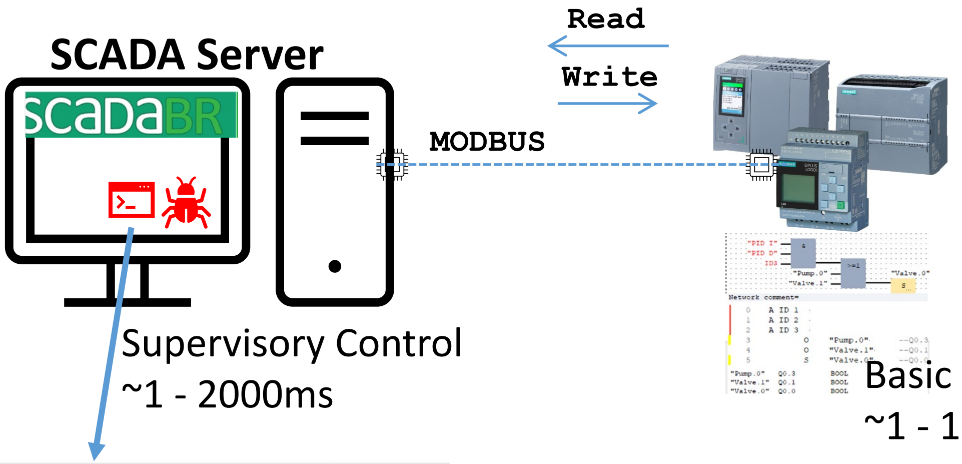
```
            Time of Day  Process Name  Operation              Path
11:58:00.6185077 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:58:00.6426596 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:58:10.6137832 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:58:10.6428279 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:58:20.6135878 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:58:20.6436740 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:58:30.6150225 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:58:30.6440060 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:58:30.7325448 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:58:30.7487234 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:58:40.6136909 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:58:40.6446850 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:58:40.7341902 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:58:50.6132060 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:58:50.6455823 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:58:50.6953501 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:59:00.6136827 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:59:00.6456876 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
11:59:10.6131961 AM  ScadaBR.exe  TCP Send               c0a8:cc85:740d:
```



```
ScadaBR.exe   CreateFile       C:\Program Files\ScadaBR\tomcat
ScadaBR.exe   QueryDirectory   C:\Program Files\ScadaBR\tomcat\webapps
ScadaBR.exe   CloseFile        C:\Program Files\ScadaBR\tomcat
ScadaBR.exe   CreateFile       C:\Program Files\ScadaBR\tomcat\webapps
ScadaBR.exe   QueryDirectory   C:\Program Files\ScadaBR\tomcat\webapps\Scad
ScadaBR.exe   CloseFile        C:\Program Files\ScadaBR\tomcat\webapps
ScadaBR.exe   CreateFile       C:\Program Files\ScadaBR\tomcat\webapps\Scad
ScadaBR.exe   QueryDirectory   C:\Program Files\ScadaBR\tomcat\webapps\Scad
ScadaBR.exe   CloseFile        C:\Program Files\ScadaBR\tomcat\webapps\Scad
ScadaBR.exe   CreateFile       C:\Program Files\ScadaBR\tomcat\webapps\Scad
ScadaBR.exe   QueryDirectory   C:\Program Files\ScadaBR\tomcat\webapps\Scad
ScadaBR.exe   CloseFile        C:\Program Files\ScadaBR\tomcat\webapps\Scad
ScadaBR.exe   Thread Create
ScadaBR.exe   TCP Send         c0a8:cc85::8d1:4711:80fa:ffff:1088 -> leo-PC:502
ScadaBR.exe   TCP Receive      c0a8:cc85::8d1:4711:80fa:ffff:1088 -> leo-PC:502
ScadaBR.exe   CreateFile       C:\
ScadaBR.exe   QueryDirectory   C:\Program Files
```

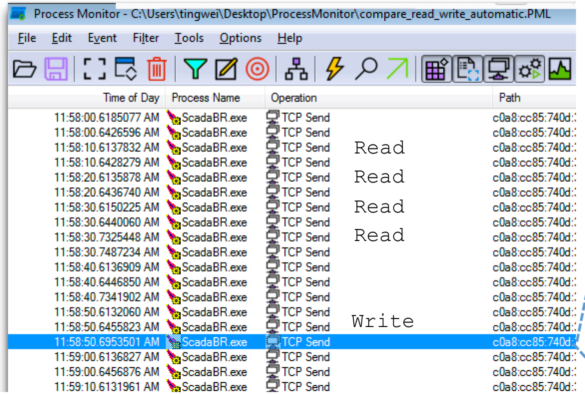
Statistical Analysis of Physical-bound Host Execution

# Statistical Analysis of Physical-bound Host Execution

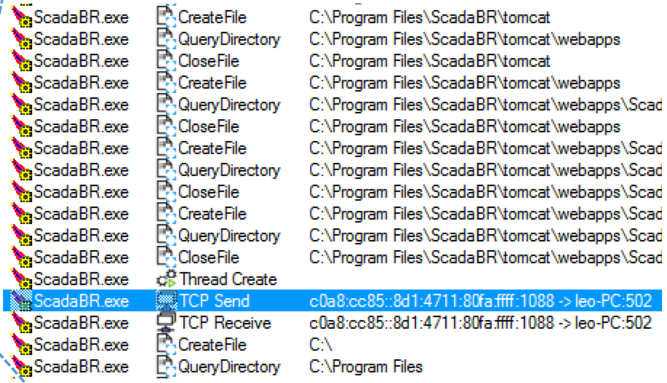


Supervisory Control
~1 - 2000ms

Basic Control
~1 - 10ms


Process Monitor - C:\Users\tingwei\Desktop\ProcessMonitor\compare_read_write_automatic.PML
File Edit Event Filter Tools Options Help

```
           Time of Day  Process Name   Operation                  Path
11:58:00.6185077 AM  ScadaBR.exe    TCP Send                   c0a8:cc85:740d:
11:58:00.6426596 AM  ScadaBR.exe    TCP Send                   c0a8:cc85:740d:
11:58:10.6137832 AM  ScadaBR.exe    TCP Send       Read        c0a8:cc85:740d:
11:58:10.6428279 AM  ScadaBR.exe    TCP Send                   c0a8:cc85:740d:
11:58:20.6135878 AM  ScadaBR.exe    TCP Send       Read        c0a8:cc85:740d:
11:58:20.6436740 AM  ScadaBR.exe    TCP Send                   c0a8:cc85:740d:
11:58:30.6150225 AM  ScadaBR.exe    TCP Send       Read        c0a8:cc85:740d:
11:58:30.6440060 AM  ScadaBR.exe    TCP Send                   c0a8:cc85:740d:
11:58:30.7325448 AM  ScadaBR.exe    TCP Send       Read        c0a8:cc85:740d:
11:58:30.7487234 AM  ScadaBR.exe    TCP Send                   c0a8:cc85:740d:
11:58:40.6136909 AM  ScadaBR.exe    TCP Send                   c0a8:cc85:740d:
11:58:40.6446850 AM  ScadaBR.exe    TCP Send                   c0a8:cc85:740d:
11:58:40.7341902 AM  ScadaBR.exe    TCP Send                   c0a8:cc85:740d:
11:58:50.6132060 AM  ScadaBR.exe    TCP Send                   c0a8:cc85:740d:
11:58:50.6455823 AM  ScadaBR.exe    TCP Send       Write       c0a8:cc85:740d:
11:58:50.6953501 AM  ScadaBR.exe    TCP Send                   c0a8:cc85:740d:
11:59:00.6136827 AM  ScadaBR.exe    TCP Send                   c0a8:cc85:740d:
11:59:00.6456876 AM  ScadaBR.exe    TCP Send                   c0a8:cc85:740d:
11:59:10.6131961 AM  ScadaBR.exe    TCP Send                   c0a8:cc85:740d:
```



```
ScadaBR.exe   CreateFile      C:\Program Files\ScadaBR\tomcat
ScadaBR.exe   QueryDirectory  C:\Program Files\ScadaBR\tomcat\webapps
ScadaBR.exe   CloseFile       C:\Program Files\ScadaBR\tomcat
ScadaBR.exe   CreateFile      C:\Program Files\ScadaBR\tomcat\webapps
ScadaBR.exe   QueryDirectory  C:\Program Files\ScadaBR\tomcat\webapps\Scad
ScadaBR.exe   CloseFile       C:\Program Files\ScadaBR\tomcat\webapps
ScadaBR.exe   CreateFile      C:\Program Files\ScadaBR\tomcat\webapps\Scad
ScadaBR.exe   QueryDirectory  C:\Program Files\ScadaBR\tomcat\webapps\Scad
ScadaBR.exe   CloseFile       C:\Program Files\ScadaBR\tomcat\webapps\Scad
ScadaBR.exe   CreateFile      C:\Program Files\ScadaBR\tomcat\webapps\Scad
ScadaBR.exe   QueryDirectory  C:\Program Files\ScadaBR\tomcat\webapps\Scad
ScadaBR.exe   CloseFile       C:\Program Files\ScadaBR\tomcat\webapps\Scad
ScadaBR.exe   Thread Create
ScadaBR.exe   TCP Send        c0a8:cc85::8d1:4711:80fa:ffff:1088 -> leo-PC:502
ScadaBR.exe   TCP Receive     c0a8:cc85::8d1:4711:80fa:ffff:1088 -> leo-PC:502
ScadaBR.exe   CreateFile      C:\
ScadaBR.exe   QueryDirectory  C:\Program Files
```

## Frequency and Temporal Properties

### Control Command Dependency

$$P(V_k) := \{C_j, C_{j+1}, .....C_n\} \cup \{M_j, M_{j+1}, .....M_n\}$$

$$\forall M_i, C_j \in P(V_k) \wedge (ts(M_i) < ts(C_j)) : \quad C_j \hookleftarrow C_i$$

### 1 Control Time-Interval

$$\forall C_i, C_j \in P(V_k) \;\; s.t. \;\; i \neq j : \quad \Delta(i,j) := ABS(ts(C_i) - ts(C_j))$$

$$\boxed{R_{D\Delta}(i-1,i)} = \frac{Deviation(j) + \epsilon_{(i-1,i)}}{Mean(j)}$$

### 2 Control Burst-Interval

$$(\forall B_{C_i}, B_{P_i} \in P(V_k) : \quad \mu_j := |B_{C_i}| - |B_{P_i}|$$

$$\boxed{R_{D\mu}(i)} = \frac{Deviation(j) + \lambda_{(i)}}{Mean(j)}$$

### 3 Control Frequency

$$\forall C_i \in P(V_k) \quad F(i) := |C_i|$$

$$\boxed{R_{DF}(i)} = \frac{|C_i \in P(V_k)|}{|P(V_k)|}$$

# Code Release on Github: SCAWATCH

https://github.com/lordmoses/SCAWATCH

## Installation Steps

```
1.git clone https://github.com/lordmoses/SCAWATCH.git
2.cd SCAWATCH
3.pip install -r requirements.txt
4.Edit config.json
5.python3 scawatch.py
6.To end things, press CTRL -C
```

## Configuration config.json

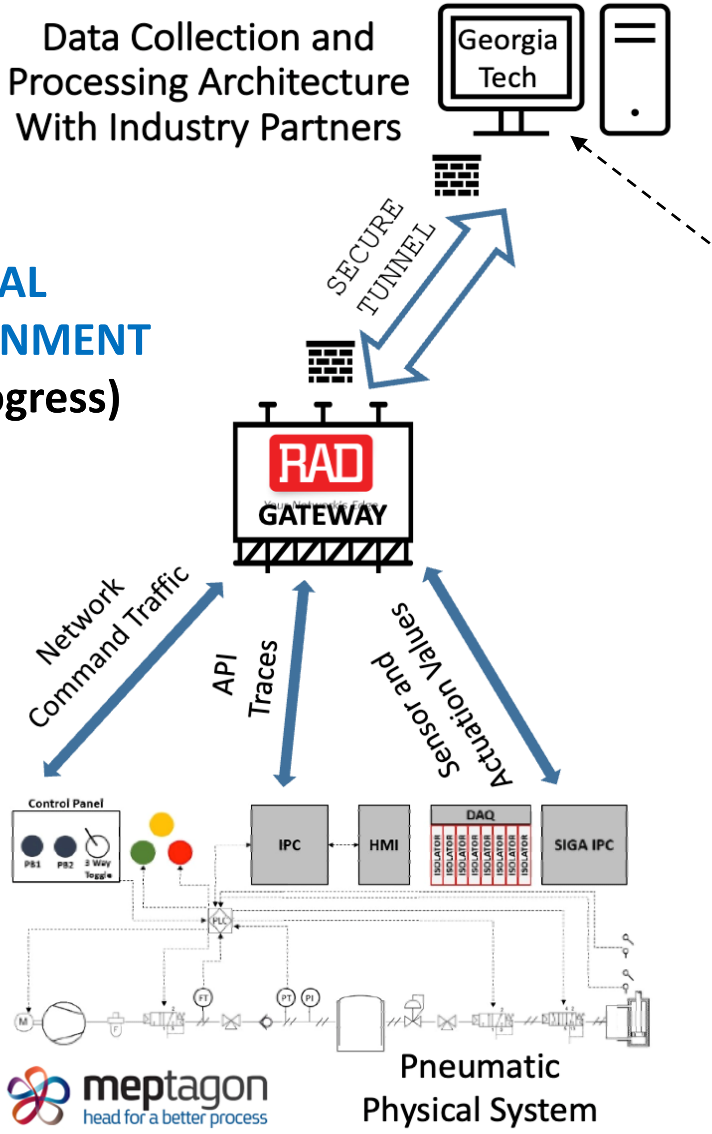
```
{
   "size_limit" : 50,
    "check_interval" : 5,
    "procmon_location" : "C:/Users/Desktop/Procmon.exe",
    "scada_process" : "ScadaBR.exe",
    "ENABLE_LOCAL_STORAGE": 1,
    "SEND_LOGS_TO_REMOTE_SERVER": 1,
    "remote_server_machine" : "avatar@AVATAR.gatech.edu",
    "remote_server_folder" : "/home/AVATAR",
    "ssh_client_identity_file" : "C:/Users/.ssh/id_rsa",
    "DEBUG_MODE" : 0
}
```

The software process that talks to the PLC. If using **MODBUS**, use **netstat** to check for communication to port **502**

- Functionality on this code release
  - Fully automated SCADA execution tracing, capture, storage management, and remote transfer

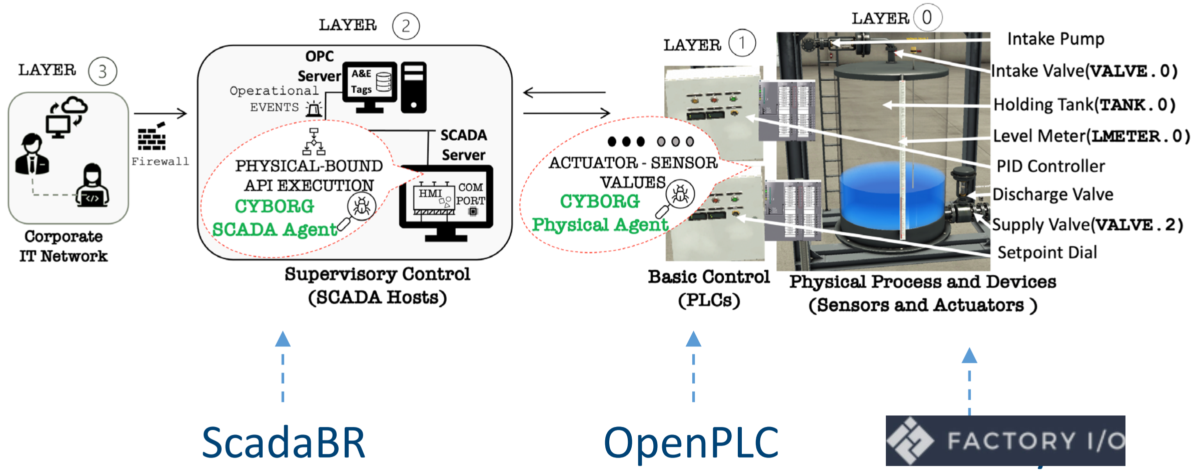
# End-to-End Deployment Scenario (Passive Monitoring and Alerting)

**REAL ENVIRONMENT**
**(In Progress)**



Anomaly correlation and detection runs here. VM and code will be released

## TEST ENVIRONMENT (Tested)

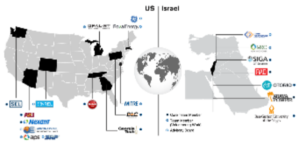


Review Workshop IV Checklist

- Collaboration
  - RAD and Meptagon
- Commercialization Potential
  - Architecture/algorithm for SCADA host anomaly alerting
- Integration
  - Dr. Sukarno (Task 14 GIT) and Dr. Yisroel (Task BGU)
- End-to-End Demonstration
  - End of FY Segment, November (Webinar)

Georgia
Tech

# QUESTIONS



- Thank You