CSI OT 3D Platform Cyber Attack Demonstration

User manual

VERSION: CORPLAB-2021-T5F-A1
30/03/2021

Liu Yuancheng
Senior Security Development Engineer
yuancheng.liu@trustwave.com
Wong Jun Wen
Asst R&D Manager
junwen.wong@trustwave.com
Dr. Shantanu Chakrabarty
NUS Research Fellow
shantanu1088@gmail.com

CSI OT 3D Platform Cyber Attack Demonstration User Manual

Introduction

This menu will introduce the steps to show three new cyberattack demo on the CSI OT Demo platform, namely the “False Data Injection Attack”, “Blackout Attack” and “Stealthy Command Injection Attack”.

False Data Injection Attack: In this attack, we assume an additional foreign hardware (IoT/Raspberry Pi) has been plug in to the OT network. This attack will manipulate the SCADA commands and PLC feedback, which causes the SCADA HMI to show the opposite feedback on the actual system.
This demo will attack on airport lights control, where the operator will see reverse PLC feedback on the actual system, e.g. When the operator tries to turn on the runway lights in the airport via HMI, the actual runway lights will be turned off.

Blackout Attack: This attack is model after 2015 Ukraine Power Grids Cyber-attack. This attack will assume the system do not properly air-gapped from the internet, whereby the malware is entering to the system via spear phishing email. When the attack launched, all the PLC output coils (energy output) will be forced to turn off.

Stealthy Command Injection Attack: In the context of smart grids, our research has established that it is possible to craft stealthy attacks that can evade the attention of both the control center (a computer system) and the human operator. Such stealthy attacks when crafted to introduce a set of malicious commands are referred to as a False Command Injection (FCI) attack in our research. These attacks are catastrophic resulting in black outs or widespread damages to grid users. For a smart grid or even a user of electrical energy, voltage of the supply is crucial. In other words, an erratic or abnormal voltage can damage equipment, and in certain cases, result in collapse of the entire grid. Voltages in a smart grid are controlled using various electrical devices or machines. One such device is the tap changing transformers. In our research, vulnerabilities of this device to stealthy attacks are studied along with techniques to detect intrusions that exploit these vulnerabilities. In this demonstration, our research is implemented on the platform. We will simulate how the attack try to break control system of the substation to generate the stealthy PWR load changes which will make influence of the power generator and make parts of the OT system paralysis. (Railway track-A, Train station and Airport.)

Recommend showing “False Data Injection” attack first in the demonstration as this will not require to reset the whole OT platform via the HMI.

Steps to Show Attack Demo

Step 1 - Hardware power check

1.1 Switch ON the OT platform’s power socket.

1.2 Check and make sure the network switches, “Technical PC”, “Orchestrator PC” and the “SCADA HMI PC” are working normally.

1.2.1 Login Information (username/password):
Technical PC: admin/Qazqwerty123
HMI PC: root/Qazqwerty123
Orchestrator PC: 00000000/00000000 => orchestrator/Qazqwerty123

1.3 Check and make sure the PLC is running on correct ladder diagram and all 3 PLCs are working normally (please refer to Radiflow documentation).

1.3.1 REMEMBER to close all PLC program BEFORE proceeding to the next step.

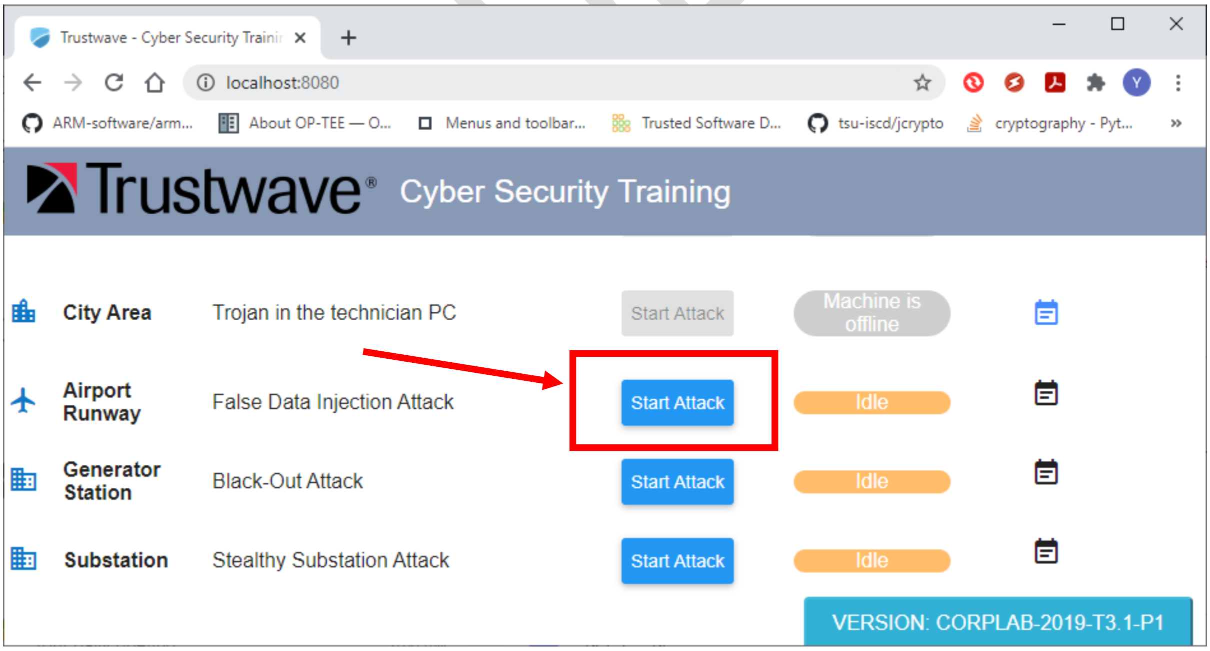
1.4 Make sure the attack Raspberry PI is power ON. (The Raspberry PI's green power light is on.)

Step 2 – Show false data injection attack demo

2.1 Turn on and off the airport runway lights to show the HMI control works normally, **leave the runway lights at ON state for the next step.**

2.2 Login the orchestrator PC, open the web browser and type in URL: http://localhost:8080 or http://127.0.0.1:8080 and the attack control webpage will show as below. (Figure_1)

2.3 To START the attack, press the 'False Data Injection Attack' section blue color "Start Attack" button (marked in the red rectangle in figure_1).



City Area	Trojan in the technician PC	Start Attack	Machine is offline	
Airport Runway	False Data Injection Attack	Start Attack	Idle	
Generator Station	Black-Out Attack	Start Attack	Idle	
Substation	Stealthy Substation Attack	Start Attack	Idle	

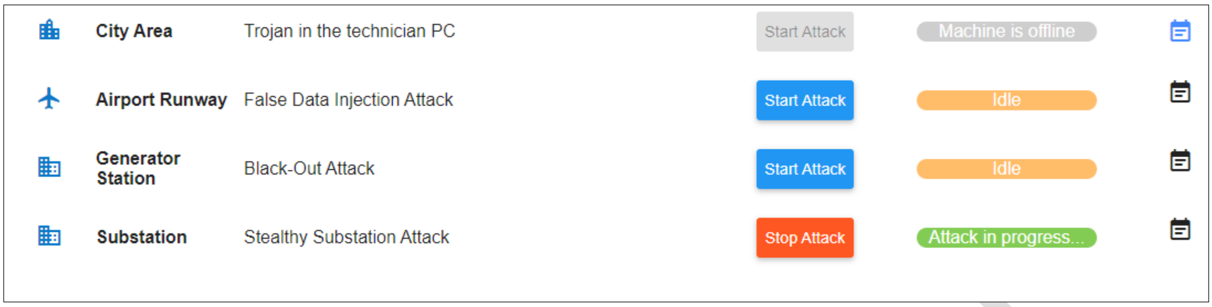
VERSION: CORPLAB-2019-T3.1-P1

<Figure_1 Attack Control Webpage>

2.4 Wait for 10 to 20 seconds until the 'Training HMI' page shown the airport runway light was turn off. This indicated the false data injection attack has started successful.

2.5 Try to turn on/off the runway light from the 'Training HMI' page and you can see the control signal has been reversed.

2.6 To STOP the attack, press the red color “Stop Attack” button (as shown in figure_2), wait for 20 to 30 seconds until the runway lights is same as the state shown on the ‘Training HMI’ page. This indicates the false data injection attack has stopped successfully.



City Area	Trojan in the technician PC	Start Attack	Machine is offline
Airport Runway	False Data Injection Attack	Start Attack	Idle
Generator Station	Black-Out Attack	Start Attack	Idle
Substation	Stealthy Substation Attack	Stop Attack	Attack in progress...

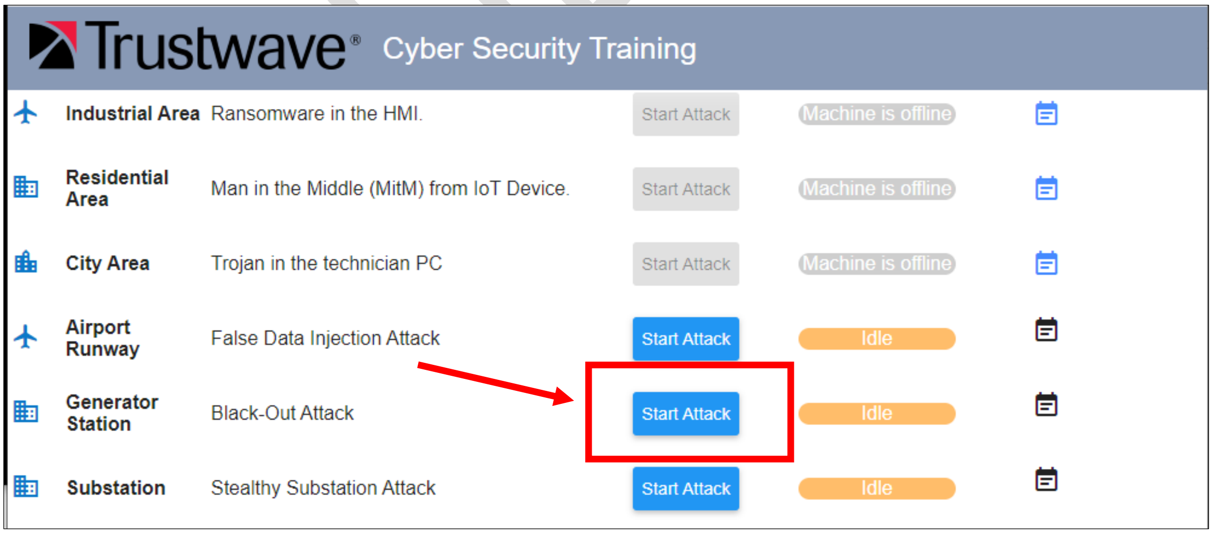
<Figure_2 Stop attack control>

2.7 Try to turn on and off the airport runway light again to show the HMI control has recovered after the attack was stopped.

Step 3 – Show Blackout attack demo

3.1 Check and turn on all the PLC outputs via training HMI, to show the audience that the system is working normally.

3.2 Refer to Step 2.2; press the blue color “Start Attack” button under the Black-Out Attack section to start the attack. (As shown below figure_3.2)



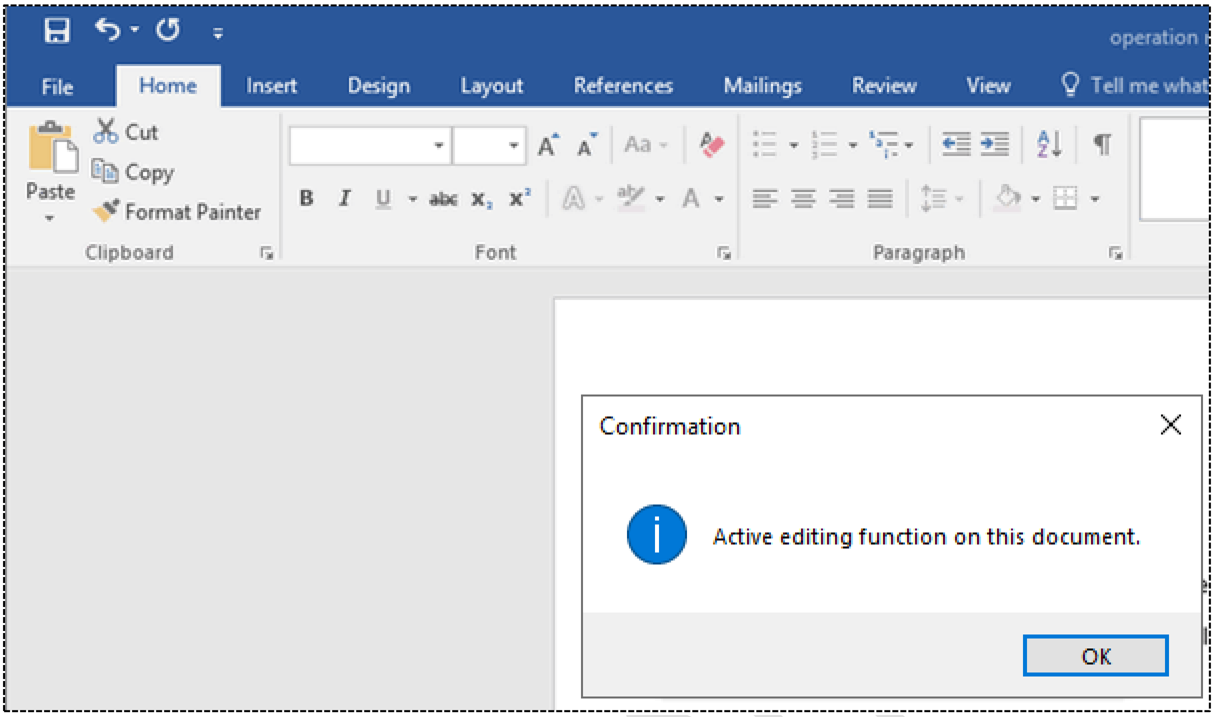
Trustwave® Cyber Security Training

Industrial Area	Ransomware in the HMI.	Start Attack	Machine is offline
Residential Area	Man in the Middle (MitM) from IoT Device.	Start Attack	Machine is offline
City Area	Trojan in the technician PC	Start Attack	Machine is offline
Airport Runway	False Data Injection Attack	Start Attack	Idle
Generator Station	Black-Out Attack	Start Attack	Idle
Substation	Stealthy Substation Attack	Start Attack	Idle

<Figure_3.2 Start Black-Out attack>

3.3 Please direct the audience attention to ‘Technical PC’. After 5 to 10 seconds, a ‘Microsoft Word’ document named “Operation menu” will open automatically on the ‘Technical PC’ screen.

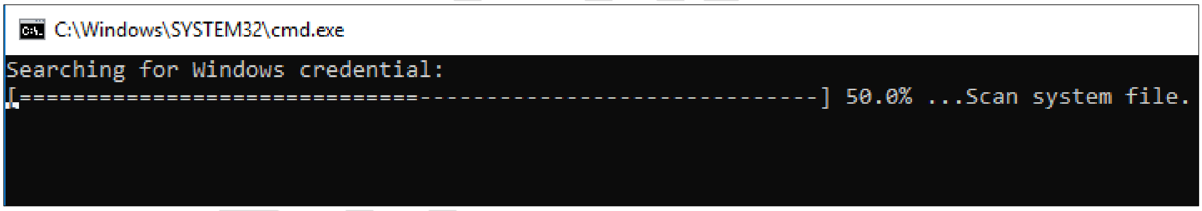
3.4 Press the “OK” button in the “Confirmation” Word document’s pop-up window. (As shown below in figure_3.4)



Active editing function on this document.

<Figure_3.4 Operation menu >

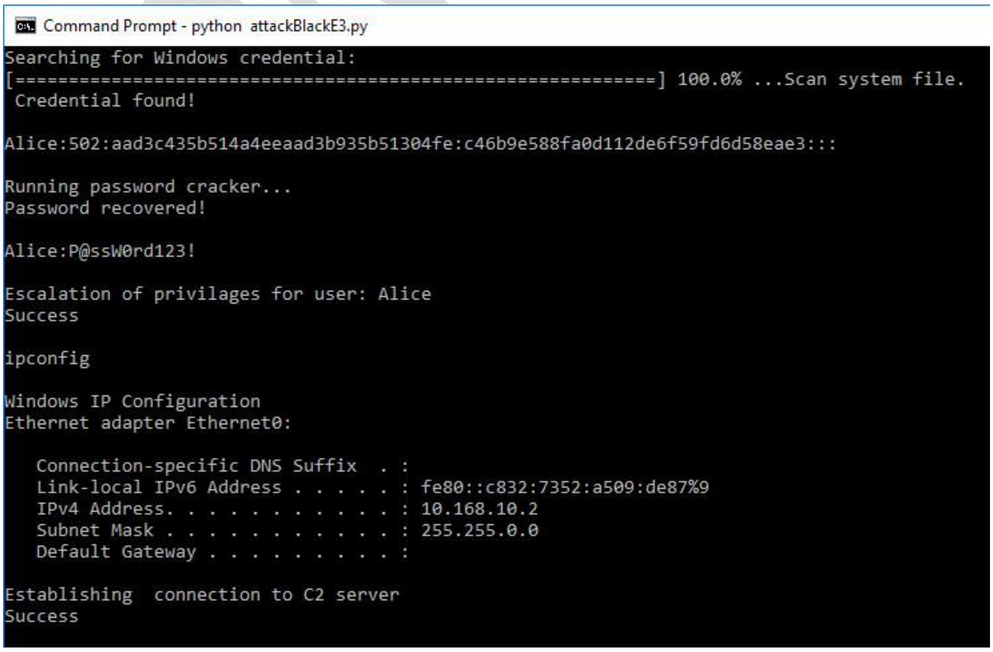
3.5 After clicking the 'OK' button, a 'Command Prompt Terminal' window will pop up and the attack detail information will show as below:



C:\Windows\SYSTEM32\cmd.exe

```
Searching for Windows credential:
[==============================------------------------------] 50.0% ...Scan system file.
```

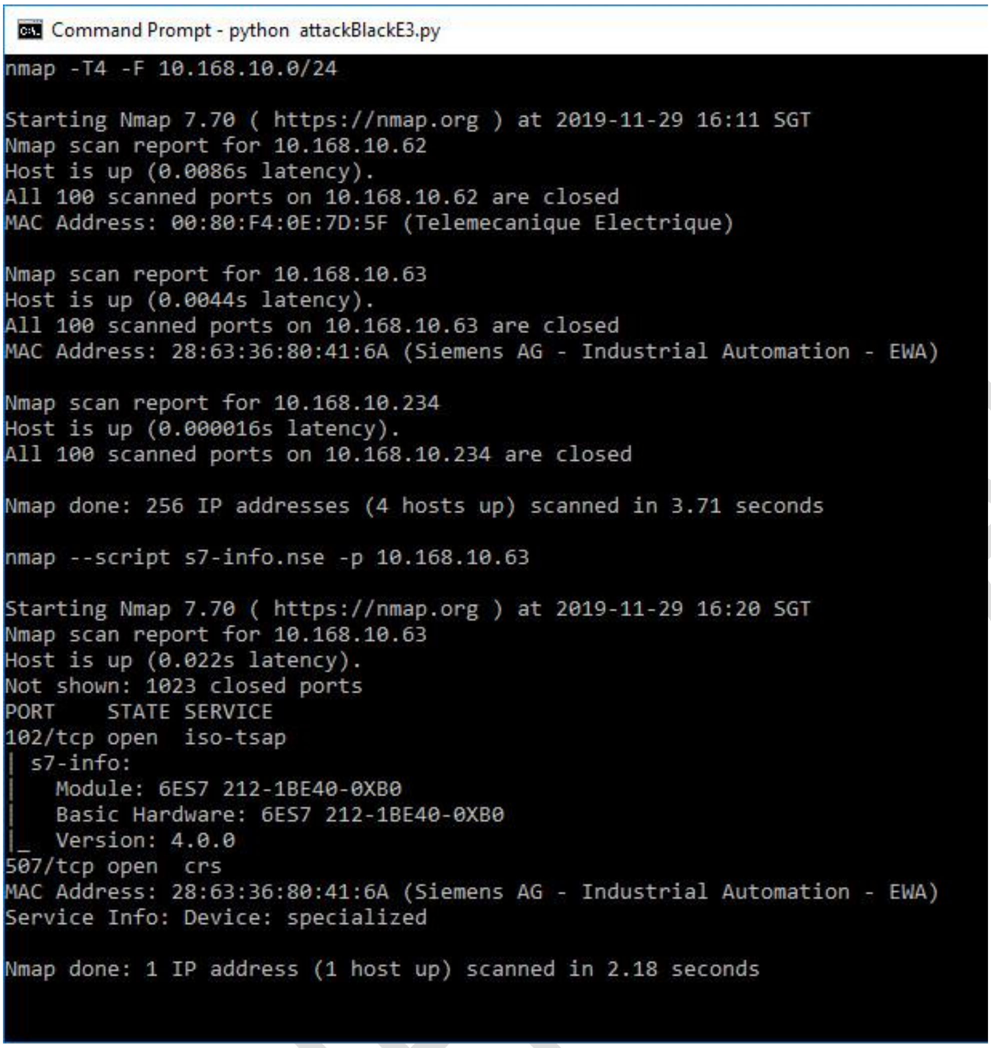
System information scanning result will be shown after the scanning process finished:



Command Prompt - python attackBlackE3.py

```
Searching for Windows credential:
[============================================================] 100.0% ...Scan system file.
 Credential found!

Alice:502:aad3c435b514a4eeaad3b935b51304fe:c46b9e588fa0d112de6f59fd6d58eae3:::

Running password cracker...
Password recovered!

Alice:P@ssW0rd123!

Escalation of privilages for user: Alice
Success

ipconfig

Windows IP Configuration
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c832:7352:a509:de87%9
   IPv4 Address. . . . . . . . . . . : 10.168.10.2
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Establishing  connection to C2 server
Success
```

Detail information of the system attack running in the background:



```
nmap -T4 -F 10.168.10.0/24

Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-29 16:11 SGT
Nmap scan report for 10.168.10.62
Host is up (0.0086s latency).
All 100 scanned ports on 10.168.10.62 are closed
MAC Address: 00:80:F4:0E:7D:5F (Telemecanique Electrique)

Nmap scan report for 10.168.10.63
Host is up (0.0044s latency).
All 100 scanned ports on 10.168.10.63 are closed
MAC Address: 28:63:36:80:41:6A (Siemens AG - Industrial Automation - EWA)

Nmap scan report for 10.168.10.234
Host is up (0.000016s latency).
All 100 scanned ports on 10.168.10.234 are closed

Nmap done: 256 IP addresses (4 hosts up) scanned in 3.71 seconds

nmap --script s7-info.nse -p 10.168.10.63

Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-29 16:20 SGT
Nmap scan report for 10.168.10.63
Host is up (0.022s latency).
Not shown: 1023 closed ports
PORT    STATE SERVICE
102/tcp open  iso-tsap
| s7-info:
|   Module: 6ES7 212-1BE40-0XB0
|   Basic Hardware: 6ES7 212-1BE40-0XB0
|_  Version: 4.0.0
507/tcp open  crs
MAC Address: 28:63:36:80:41:6A (Siemens AG - Industrial Automation - EWA)
Service Info: Device: specialized

Nmap done: 1 IP address (1 host up) scanned in 2.18 seconds
```

3.6 After the program finished running, all PLC outputs will be turned off. Try to press any of the 'Training HMI' control buttons to show audience that the HMI cannot control the system.

3.7 To STOP the attack, press the green color "Stop attack" button at the 'Orchestration PC'. The 'Training HMI' will normalize after 20 to 30 second. (same as section 2.6 figure2)

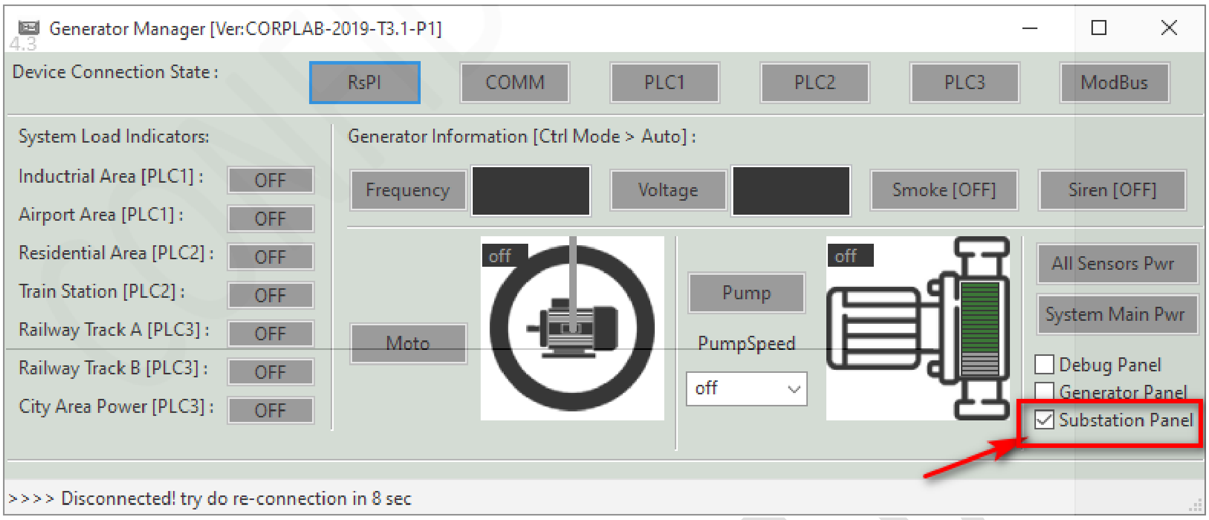
Step 4 – Show Stealthy Command Injection Attack demo on substation

4.1 Check and turn on all the PLC outputs via Training HMI page (Appendix:figure_2), to show the audience that the system is working normally. (Make sure the inner track's power was turned on and the train is running.)

4.2 Run the Generator remote control program (GeneratorMgr icon on the desktop). Turn on the substation information display panel on the Power Generator Control program. (As shown in figure_4.1)

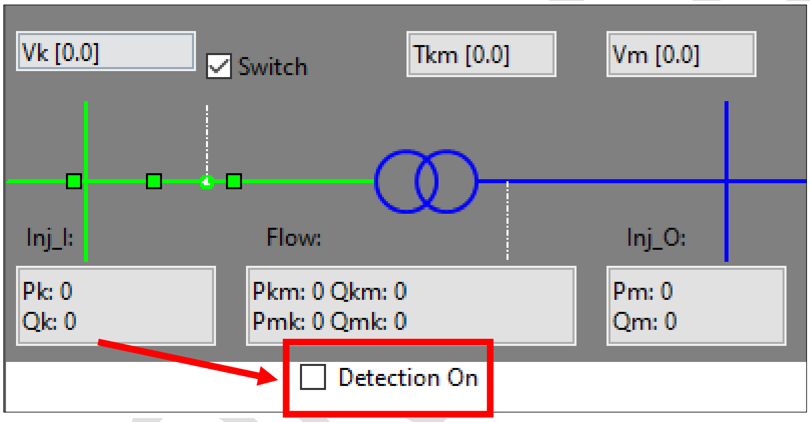
4.2.1 Select "Generator Panel" checkbox at the right bottom corner of the main program window to show the generator display UI window at the bottom side of the screen.

4.2.2 Select "Substation Panel" checkbox at the right bottom corner of the main program window to show the generator display UI at the top right side of the screen. (As shown below)


Generator Manager [Ver:CORPLAB-2019-T3.1-P1]
Device Connection State :
RsPI
COMM
PLC1
PLC2
PLC3
ModBus
System Load Indicators:
Inductrial Area [PLC1] : OFF
Airport Area [PLC1] : OFF
Residential Area [PLC2] : OFF
Train Station [PLC2] : OFF
Railway Track A [PLC3] : OFF
Railway Track B [PLC3] : OFF
City Area Power [PLC3] : OFF
Generator Information [Ctrl Mode > Auto] :
Frequency
Voltage
Smoke [OFF]
Siren [OFF]
off
Moto
Pump
PumpSpeed
off
off
All Sensors Pwr
System Main Pwr
□ Debug Panel
□ Generator Panel
☑ Substation Panel
>>>> Disconnected! try do re-connection in 8 sec

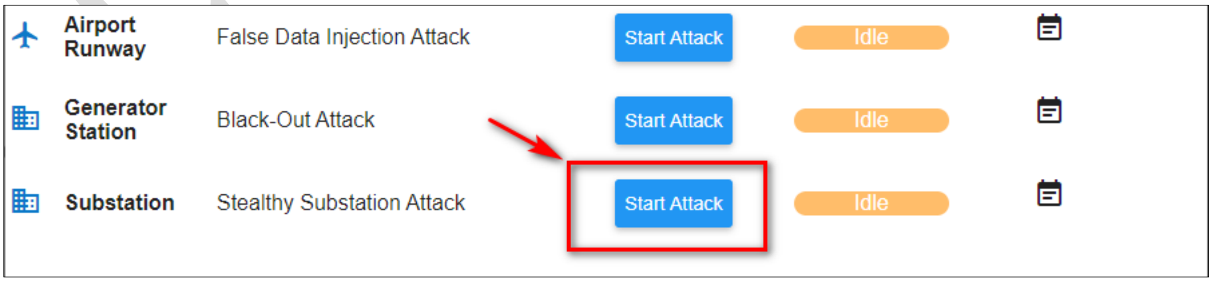
<Figure_4.1 Generator remote manager main UI>

4.3 Select the "Detection On" checkbox on the substation information display window to turn on the Stealthy Command Injection Attack detection function for on the substation parameters data.



<Figure_4.2 Substation parameter display UI>

4.3 Refer to Step 2.2; press the "Start Attack" button under the Stealthy attack section to start the attack (As shown below). The attack will start after 10 seconds.



Airport Runway	False Data Injection Attack	Start Attack	Idle
Generator Station	Black-Out Attack	Start Attack	Idle
Substation	Stealthy Substation Attack	Start Attack	Idle

<Figure_4.3 Stealthy substation attack start control>

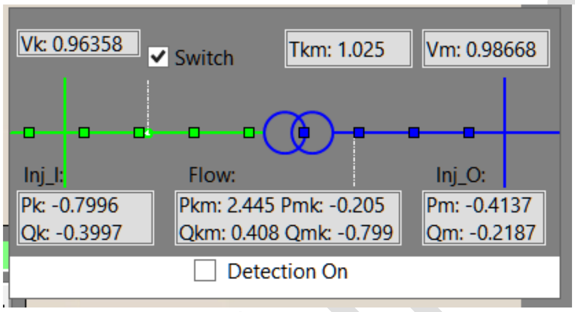
4.3 After the attack was started, the attack situation would be different base on whether we have turned on the detection function. (The detail is shown in the below diagram)

Idx	Without attack detection algorithm working	With attack detection algorithm working
0	Airport runway lights start flickering	Airport runway lights start flickering
1	Inner track train stop/start moving	Inner track train stop/start moving
2	Effect of the runway light and inner track train lasted for 30 seconds	Attack detected - Generator sound alarm and attack caution information show on HMI.
3	Switch off airport runway lights	Effect lasted for 30 secs
4	Wait for 10 secs	Operator clicks on [Manual] button on HMI to switch the control to manual mode --- if not follow the "without detection" scenario
5	Switch off train running in the inner track	Stop all the attack situation and alarm sound
6	Wait for 10 seconds	Everything back to initial state
7	City light change to red	
8	Generator alarms stop and system power off	

<Figure_4.3 attack situation>

During the attack, the substation information display window will show the calculated threshold value calculated based on the substation working parameters and changed to red color:

Normal state scenario:



Vk: 0.96358 ☑ Switch Tkm: 1.025 Vm: 0.98668

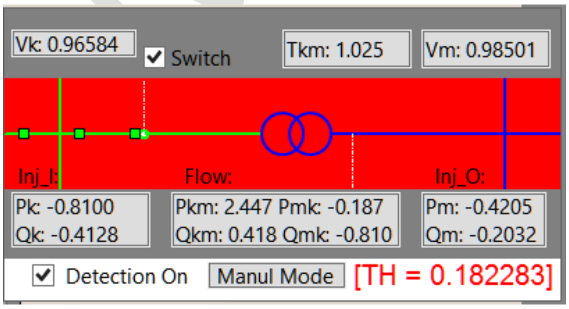
Pk: -0.7996
Qk: -0.3997

Pkm: 2.445 Pmk: -0.205
Qkm: 0.408 Qmk: -0.799

Pm: -0.4137
Qm: -0.2187

□ Detection On

Attack detection on state scenario:



Vk: 0.96584 ☑ Switch Tkm: 1.025 Vm: 0.98501

Pk: -0.8100
Qk: -0.4128

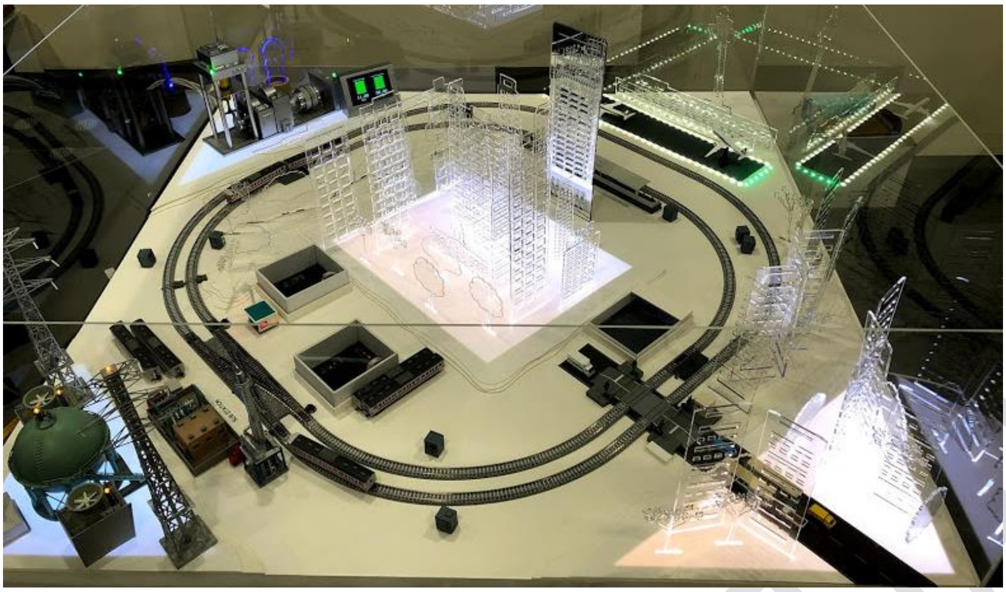
Pkm: 2.447 Pmk: -0.187
Qkm: 0.418 Qmk: -0.810

Pm: -0.4205
Qm: -0.2032

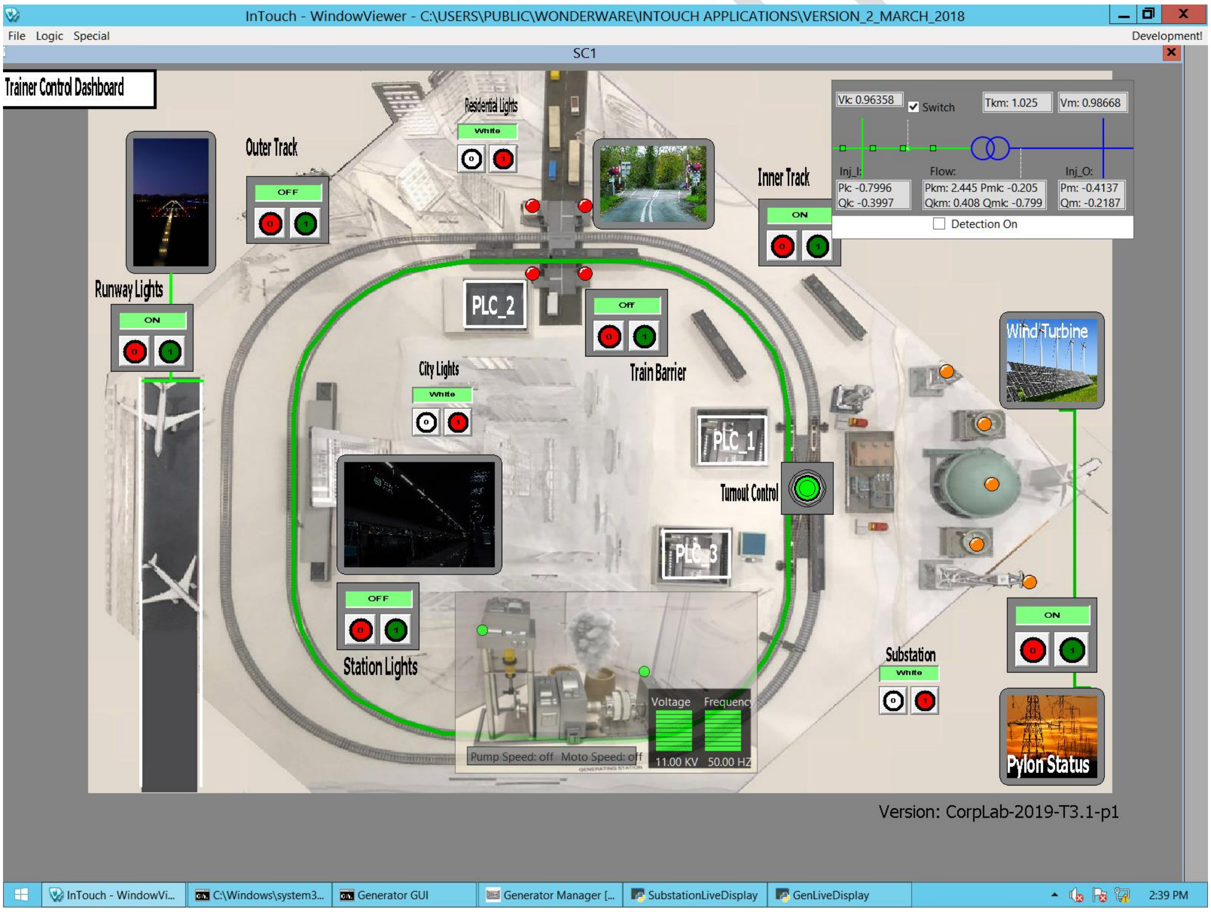
☑ Detection On Manul Mode [TH = 0.182283]

4.4 To STOP the attack, press the green color "Stop attack" button at the 'Orchestration PC'. The 'Training HMI' will get back to normal state automatically after 5 to 10 seconds.

Appendix: Default state of the OT Platform



<Figure_1 Platform system view >



InTouch - WindowViewer - C:\USERS\PUBLIC\WONDERWARE\INTOUCH APPLICATIONS\VERSION_2_MARCH_2018

Vk: 0.96358 ☑ Switch Tkm: 1.025 Vm: 0.98668

Inj_I: Pk: -0.7996 Qk: -0.3997

Flow: Pkm: 2.445 Pmk: -0.205 Qkm: 0.408 Qmk: -0.799

Inj_O: Pm: -0.4137 Qm: -0.2187

□ Detection On

Pump Speed: off Moto Speed: off

Voltage 11.00 KV

Frequency 50.00 HZ

Version: CorpLab-2019-T3.1-p1

<Figure_2 Training HMI page>

Training HMI control buttons:

1. Residential Lights = White
2. Substation Lights = White

3. City Lights = White
4. Pylon Status LED = ON
5. Station Lights = ON
6. Turnout Control = OFF
7. Train Barrier = ON
8. Inner Track = ON, with Trains
9. Outer Track = OFF
10. Runway Light = ON
11. Power Plant motor LED = Green
12. Power Plant pump LED = Green
13. Power Plant LCD = Green bar, Green bar, 11kV, 50 Hz
14. Power Plant siren = OFF
15. Power Plant smoke LED = ON