

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>

Confidentiality Notice: This document is confidential and contains proprietary information and intellectual property of Trustwave, a Singtel company, its parent company and its subsidiaries. Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances. Please be aware that disclosure, copying, distribution or use of this document and the information contained therein is strictly prohibited.

CSI OT 3D Platform Cyber Attack Demonstration

User manual

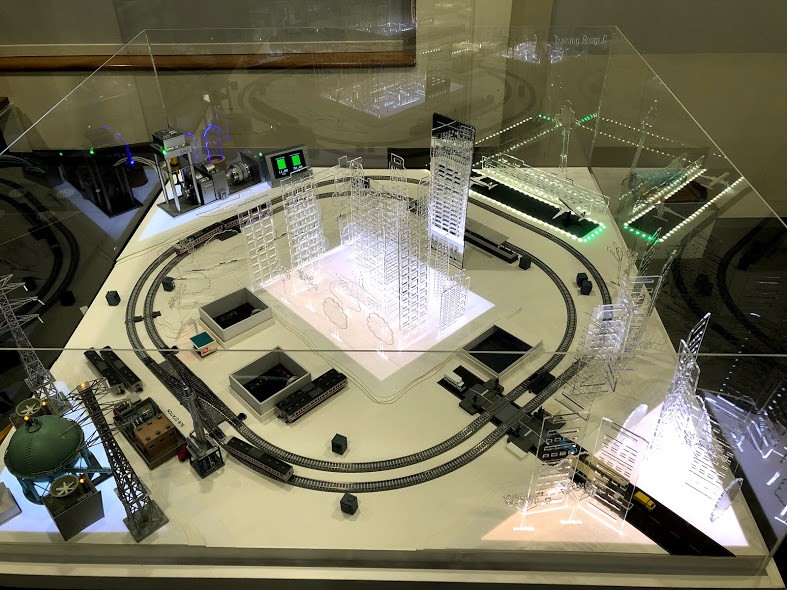
VERSION: CORPLAB-2021-T5F-A1

30/03/2021

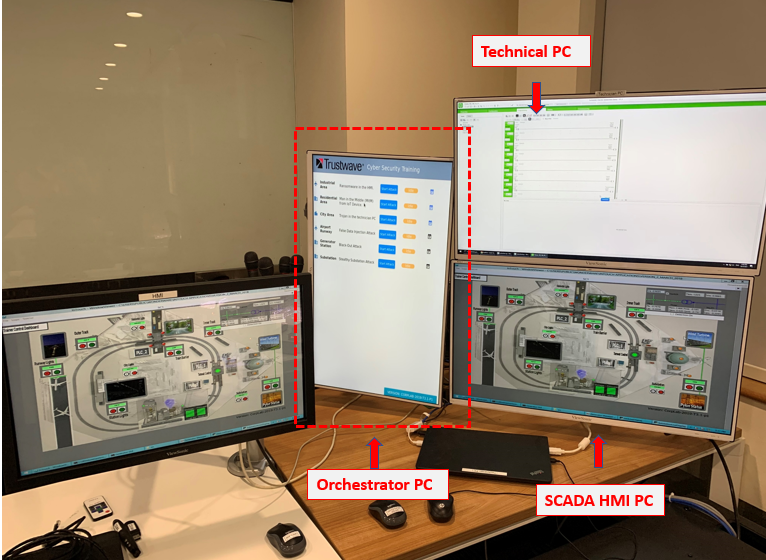
**CSI OT 3D Platform Cyber Attack Demonstration User Manual**

**Introduction**

This menu will introduce the steps to show three new cyberattack demo on the CSI OT Demo platform (As shown in the Figure\_0.0), namely the “False Data Injection Attack”, “Blackout Attack” and “Stealthy Command Injection Attack”. During the demo, the presenter will control the platform the SCADA PC, start/stop the attack from the Orchestrator PC and show some “user action under attack” on Technical PC (as shown in the Figure\_0.1).

****

<Figure\_0.0 CSI OT Demo platform view >



<Figure\_0.1 CSI OT Demo platform computer view>

**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 construct a stealthy attack 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 Different Attack Demo**

**Step 1 - Hardware power check.**

* 1. Switch ON the OT platform’s power socket.
  2. Check and make sure the network switches, “Technical PC”, “Orchestrator PC” and the “SCADA HMI PC” are working normally.
     1. Login Information (username/password):

Technical PC: **admin** / **Qazqwerty123**

HMI PC: **root** / **Qazqwerty123**

Orchestrator PC: BIOS Login user/password: **00000000** / **00000000**

System Login user/password: **orchestrator** / **Qazqwerty123**

* 1. 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. REMEMBER to close all Schneider PLC SoMachine program running on Technician PC BEFORE proceeding to the next step.
  2. Make sure the attack Raspberry PI is power ON. (As marked with red rectangle in the Figure\_1.4, the Raspberry PI’s green power light is on.)



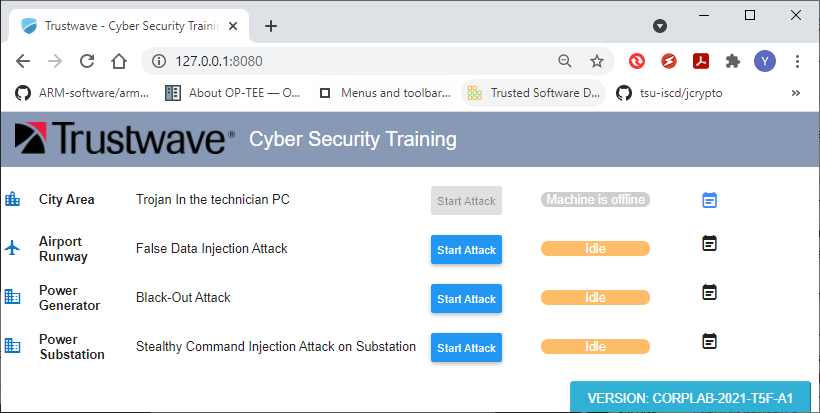
<Figure\_1.4 Location of the attack Raspberry PI>

**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 colour “Start Attack” button (marked in the red rectangle in Figure\_2.3).

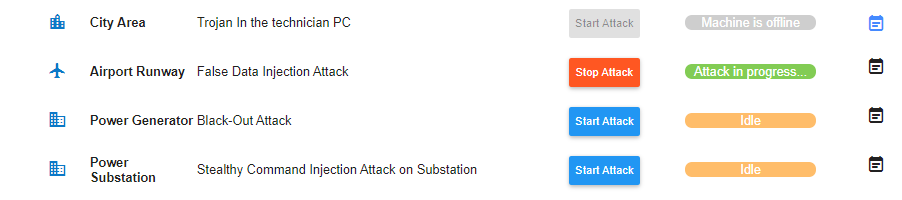


<Figure\_2.3 Attack Control Webpage>

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 colour “Stop Attack” button (As shown in Figure\_2.6), 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.



<Figure\_2.6 Stop false data injection 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.

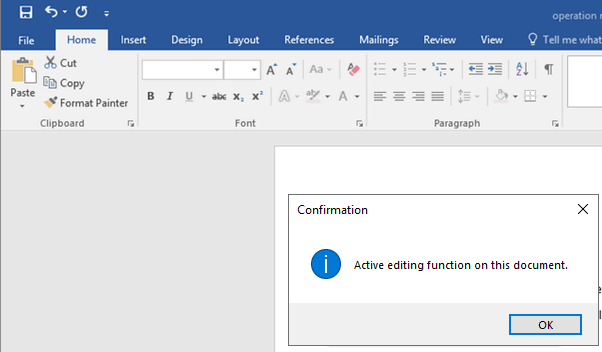
3.2 Refer to Step 2.2; press the blue colour “Start Attack” button under the Black-Out Attack section to start the attack. (As shown below Figure\_3.2)



<Figure\_3.2 Start Black-Out attack>

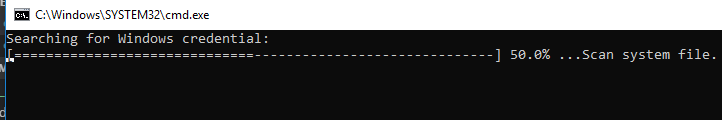
3.3 Please direct the audience attention to ‘Technical PC’. After 5 to 10 seconds, a ‘Microsoft Word’ document named “Operation menu” will open automatically on the ‘Technical PC’ screen.

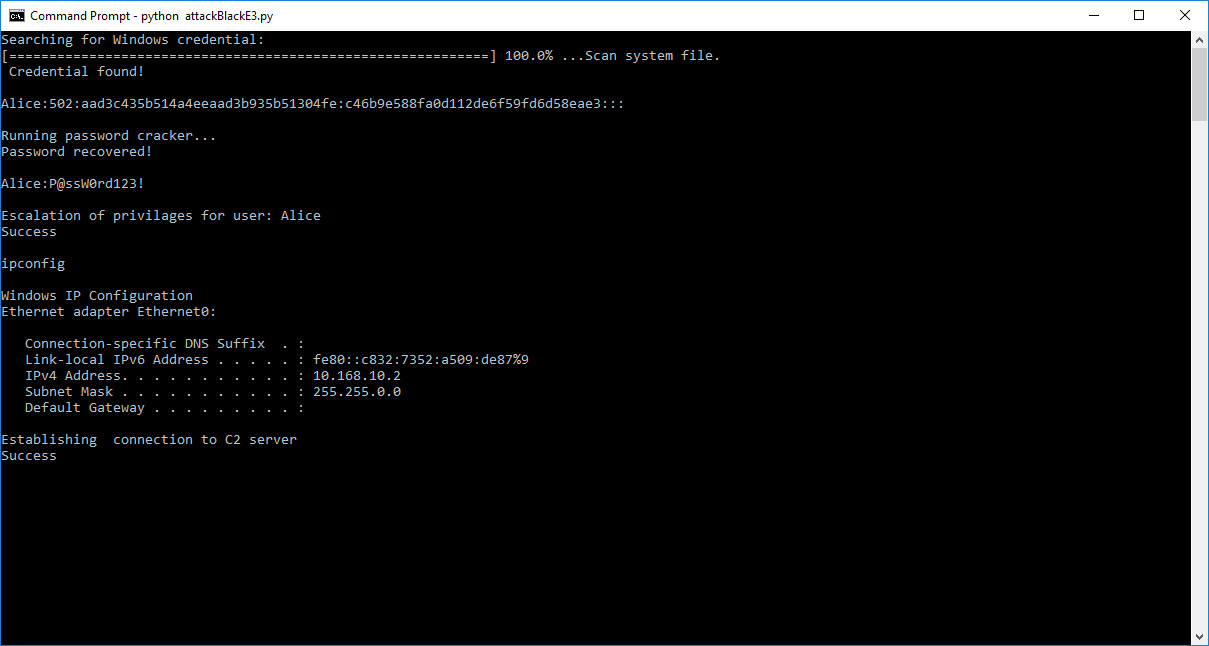
3.4 Press the “OK” button in the “Confirmation” Word document’s pop-up window. (As shown below in Figure\_3.4)



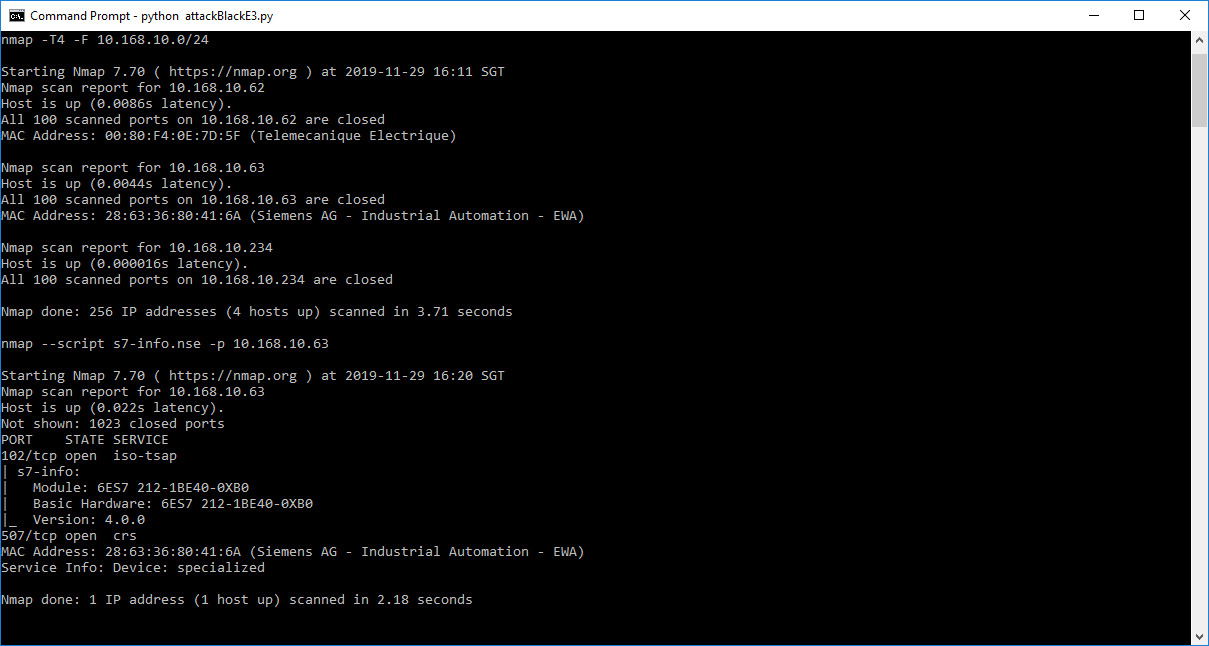
<Figure\_3.4 Operation menu >

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

System information scanning result will show after the scanning process finished:

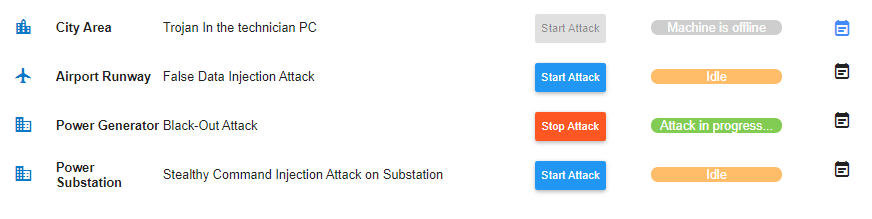


Detail information of the system attack running in the background:



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.

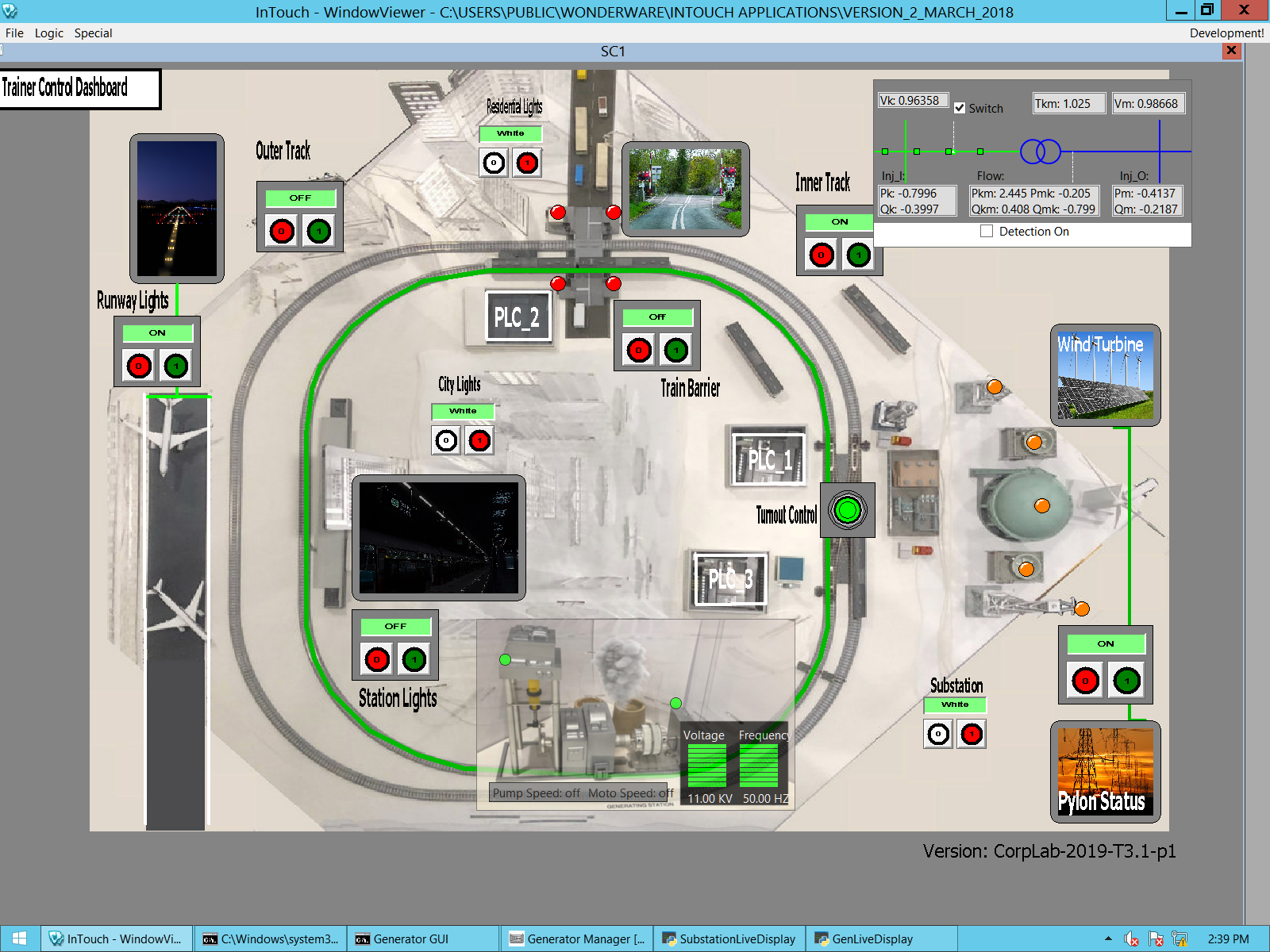
3.7 To STOP the attack, press the green colour “Stop attack” button at the ‘Orchestration PC’. The ‘Training HMI’ will normalize after 20 to 30 second. (As shown in Figure\_3.7)



<Figure\_3.7 Stop Blackout attack control>

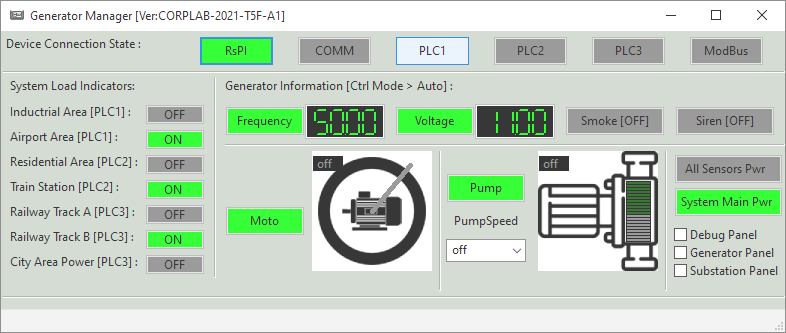
**Step 4 – Show Stealthy Command Injection Attack demo on substation**

4.1 Check and turn on all the PLC outputs via Training HMI page (As shown in Figure\_4.1), 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.)



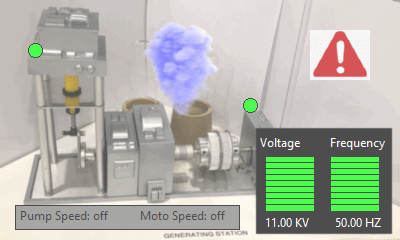
<Figure\_4.1 SCADA view under normal situation>

4.2 Run the Generator remote control program (“GeneratorMgr” icon on the desktop) and the main program UI will be shown as Figure\_4.2.0. Wait the indicators” RsPI”, “COMM”, “PLC1”, “PLC2” and “PLC3” in “Device Connection State” section change to green colour (All of them should be green before we start the cyber-attack demo). After all the information shows on the main UI, press the checkbox at the right bottom corner (marked with red rectangle) of the main window to enable the subsystem’s display window.



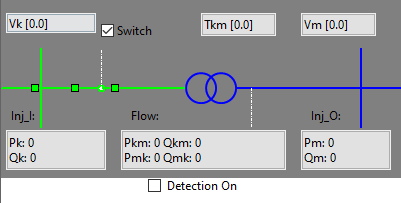
<Figure\_4.2.0 Generator remote manager main UI>

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. (As shown in Figure\_4.2.1)



<Figure\_4.2.1 Power generator display UI>

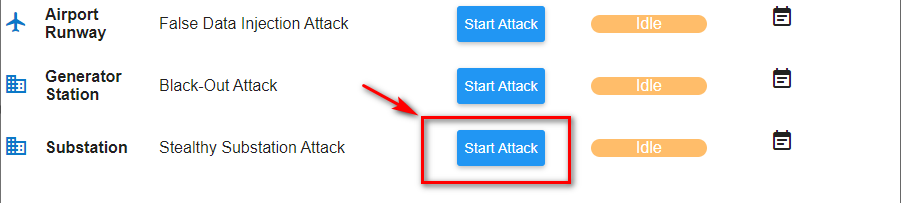
4.2.2 Select “Substation Panel” checkbox at the right bottom corner of the main program window to show the generator display UI at the top right side of the screen. (As shown in Figure\_4.2.2)



<Figure\_4.2.2 Substation parameter display UI>

4.2.3 To turn on the Stealthy Command Injection Attack detection based on substation parameters data**,** select the “Detection On” checkbox on the substation information display window. (As shown in the Figure\_4.2.2 red rectangle box)

4.3 Press the “Start Attack” button under the Stealthy attack section to start the attack (As shown below Figure\_4.3). The attack will start after 10 seconds. The main SCADA HMI situation will be show in Figure\_4.4.2.

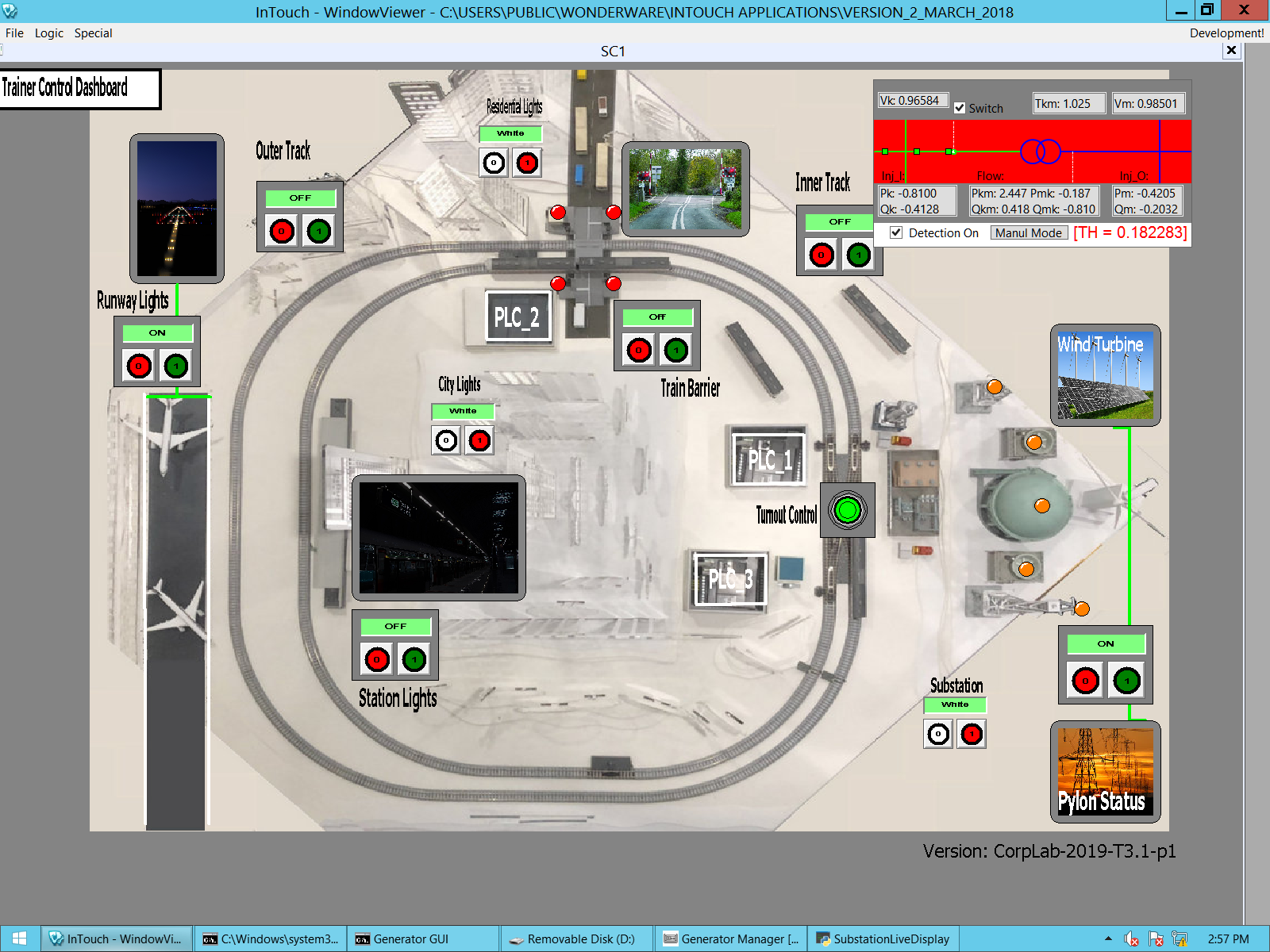


<Figure\_4.3 Stealthy substation attack start control>

4.4 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 table Figure\_4.4.1)

|  |  |  |
| --- | --- | --- |
| 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 |  |

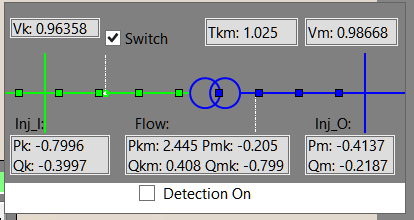
<Figure\_4.4.1attack situation>



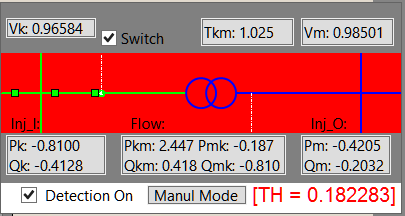
<Figure\_4.4.2 SCADA HMI View under attack situation>

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

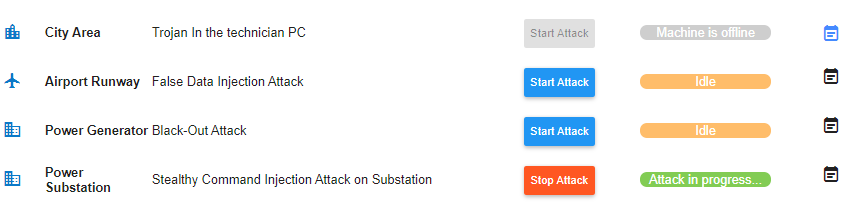
Normal state scenario:



Attack detection on state scenario:

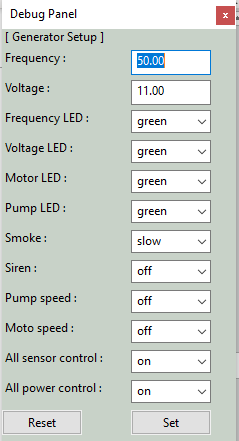


4.5 To STOP the attack, press the green colour “Stop attack” button at the ‘Orchestration PC’. The ‘Training HMI’ will get back to normal state automatically after 5 to 10 seconds. (As shown in Figure\_4.5)



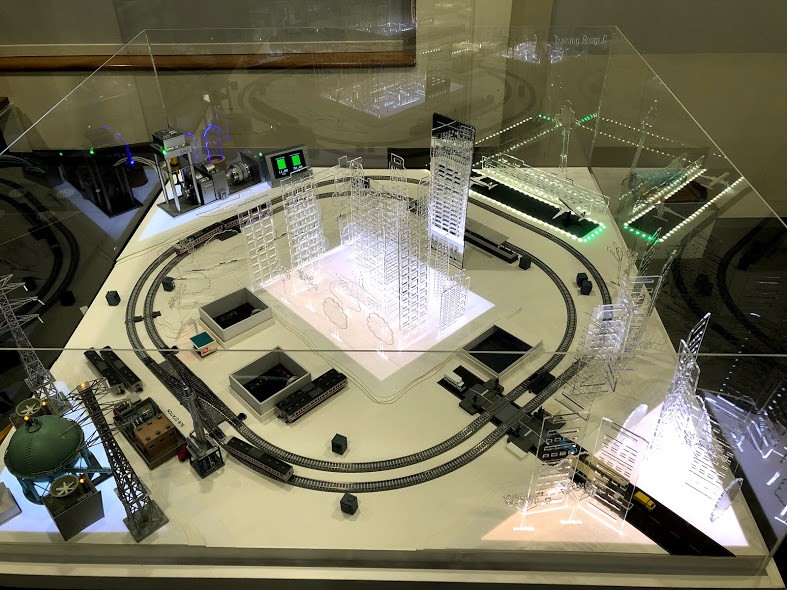
<Figure\_4.5 Stop Blackout attack control>

4.6 To recover the power generator and substation, press the “debug Panel” check box (As shown in Figure\_4.1). Press the “Reset” button to load the default value, then press the “Set” button to set the power generator and substation’s state. (As shown in the Figure\_4.6)

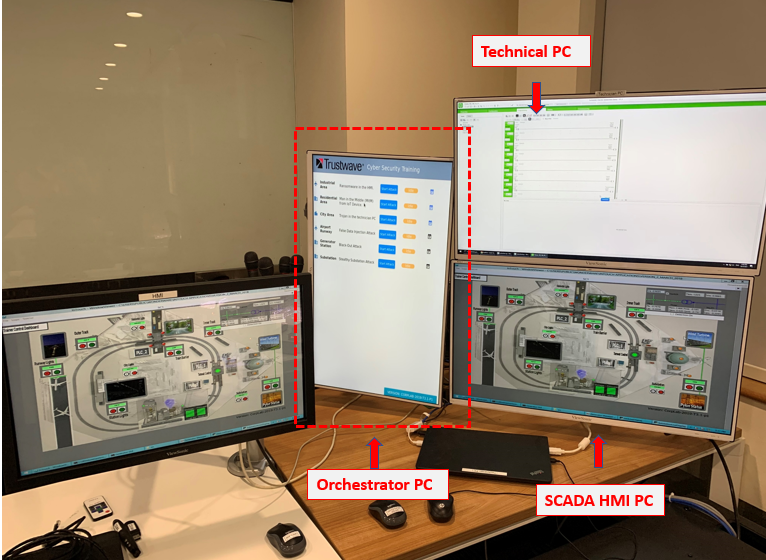


<Figure\_4.5 attack situation>

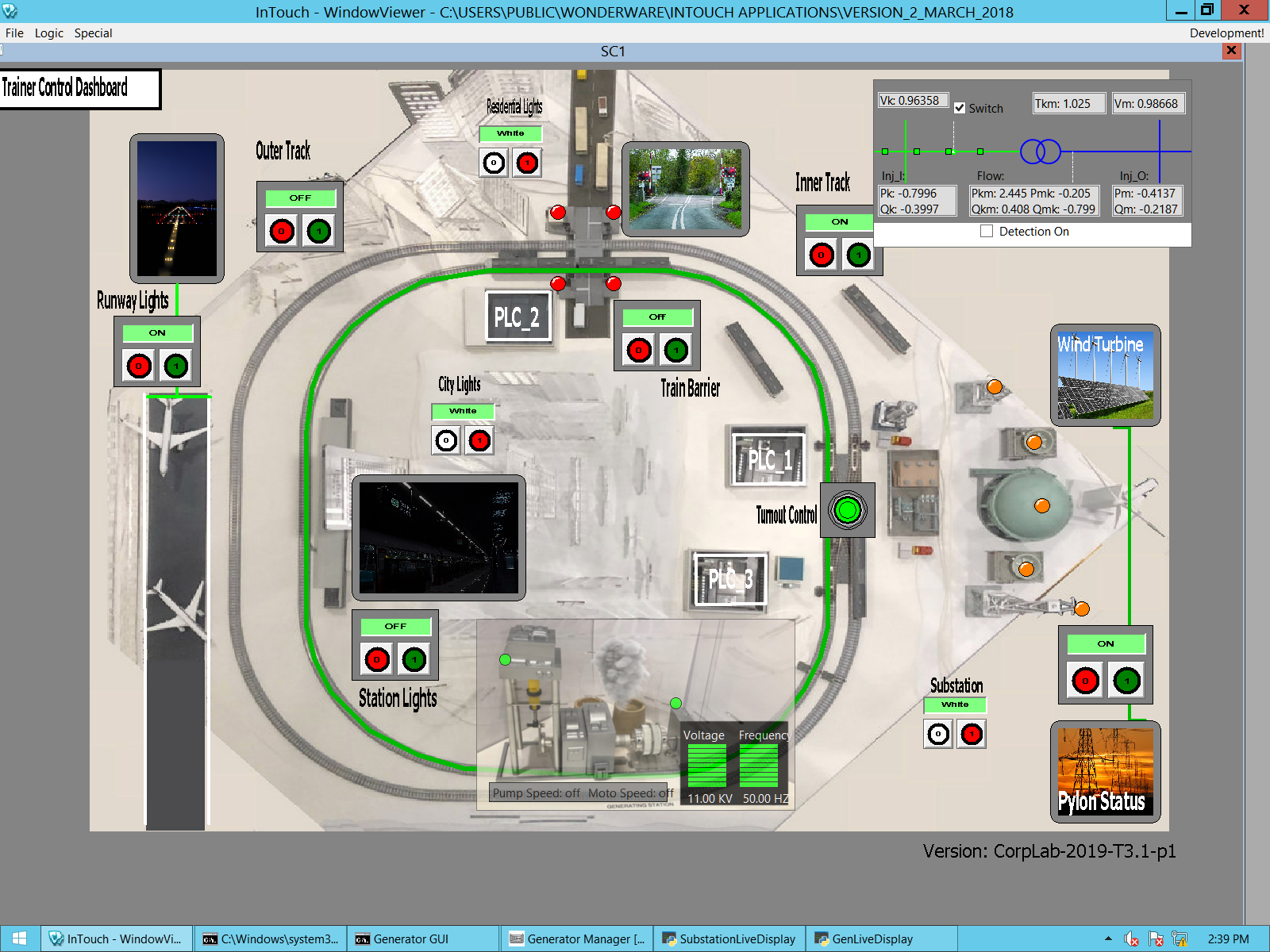
**Appendix: Default state of the OT Platform**

****

<Figure\_A1 Platform system view >



<Figure\_A2 Platform control computers view>

****

**12**

**11**

**10**

**9**

**8**

**7**

**6**

**5**

**4**

**3**

**2**

**1**

<Figure\_A3 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

**Troubleshooting**

1. Attack control Webpage does not show up when typed in the URL on orchestrator PC browser.

Solution:

* Open folder /home/attack/server on the orchestrator PC and type in cmd: node app.js or reboot the orchestrator PC can fix the problem.

1. The attack does not start after pressed the “Start Attack” button.

Solution:

* Check whether other attack has already started, only can demo one kind of attack situation at one time.
* Check whether the attack device is connected in the system. (Attack Raspberry power show on and network LED green light should flash)
* Cycle the attack device power. (Unplug the Raspberry pi power supply and plug back).

1. HMI Cannot start after clicked the HMI “Viewer” Icon on SCADA PC.

Solution:

Check whether the USB licence dongle was plugged in the SCADA PC’s USB port. Re-plug in the USN licence dongle again in the SCADA PC to let the program HMI viewer detect the licence.

1. The train was not moving when press the inner track/out track power on button.

Solution:

* Check the PLC2’s power LED and network LED light are green.
* Open SoMachine Basic V1.5 program from technician PC to confirm the controller setting is not under “Stop/Programming” mode.
* Check the Train to make sure the wheels are not jammed (This is the situation most of time will happen). Make sure all the wheels touch the inner side of the railway track so the current can flow from the rail way to train moto.

1. During the Blackout attack demo the MS-word document is not auto popup after starting the attack.

Solution:

* Make sure you login account you used for the technician PC is “Administrator” instead of “Guest” or “Admin”.
* Make sure there is no opened word document on the technician PC before demo the Blackout attack. And make sure the “ActionServer.py” and the “AttackHost.py” program are running on the technician PC.
* If the previous step does not fix the problem, check the network connection to Technician PC (USB to CAT-5 convertor) and reboot the computer.

1. Only the PLC indicators on the GeneratorManager program does not show green colour, “RsPI” and “Comm” indicator are green.

Solution:

* Check whether the blackout attack was started, if not which means the generator control Raspberry PI are not login the PLC correctly. Reboot the generator control Raspberry Pi or reboot the whole system power.