# CSI OT 3D Platform Cyber Attack Demonstration HMI

# SCADA HMI Design Manual

VERSION: CORPLAB-2021-T5F-A1

30/03/2021

Prepared by

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 SCADA HMI Design Manual

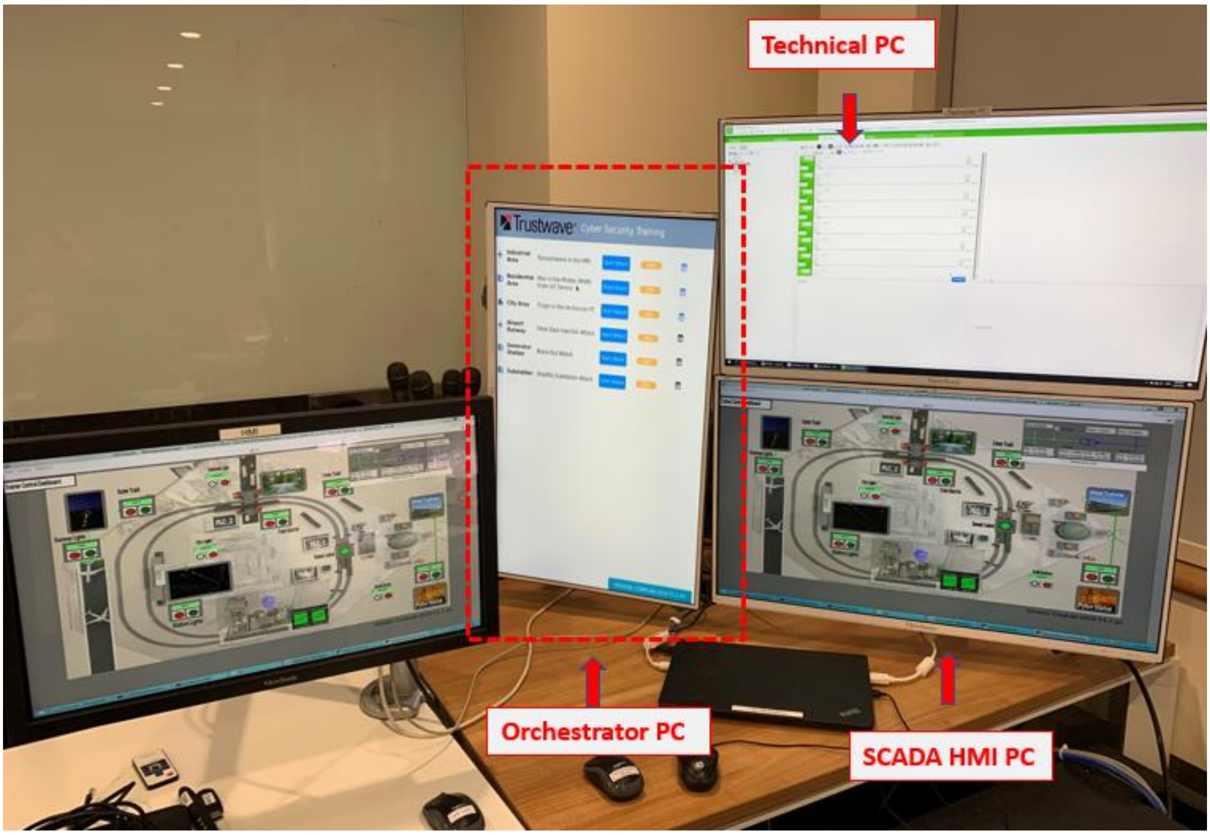
## 1.Project Introduction

This project will provide supervisory control and data acquisition (SCADA) human-machine interface (HMI) programs to control the components in CSI OT 3D Cyber-attack demonstration platform. We will create two kinds of SCADA HMI system by using Schneider-Wonderware(R) software and python to let the user control the PLC railway modules or simulate different kinds of railway operation for training or research purpose.

The Schneider-Wonderware HMI program are mainly used for the demo purpose, it contents three main pages:

- Training SCADA HMI page is mainly used for training and demonstration task.
- PLC Status View HMI page is used the for showing the working flow logic of the PLC modules in the system.
- Railway Command and Control HMI page is used to simulate and demonstrate the railway command control centre's operational sequence.

The Schneider-Wonderware HMI Program will be shown in the SCADA PC in the system with duplicate screen display as shown below (Figure_1.0):



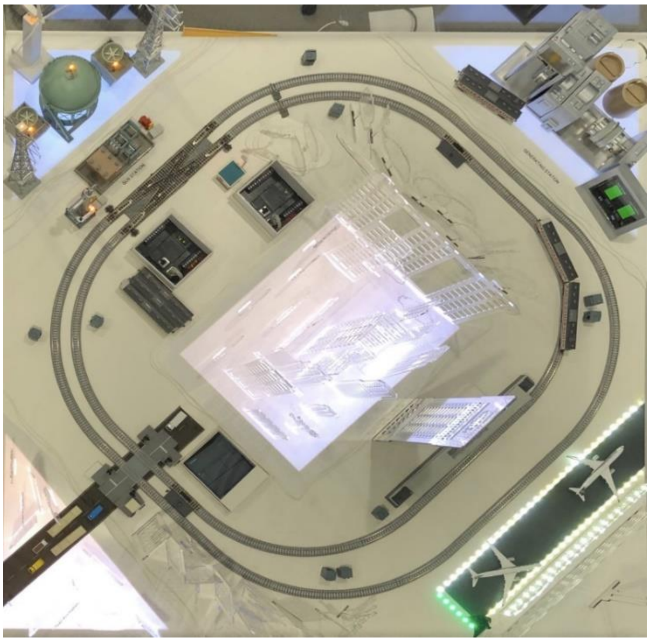
<Figure_1.0 System Computers View>

The Development and Debug HMI is implemented by Python-3.7. This program is used for showing the developer the deeper/lower-level system running/debug information. To make the developer can do offline development, it can simulate all the real action of the OT 3D-platform without physically connected to the real hardware. It can also simulate some extend function which is not provide by the 3D-Platform hardware for the further development. It will also be used for simulating the four kinds of IT/OT cyber-attack situation for the system.

To control the real OT 3D-platform by the python Development and Debug HMI, the user needs to disable the test mode flag of the program and plug the computer which executes the program to the network switch of the OT 3D-platform. Config the computer's IP address to any one in range 192.168.10.150 to 192.168.10.170. The python Development and Debug HMI can be used as same as the Schneider-Wonderware HMI program.

## 1.1 Training SCADA HMI Page

1.1.1 Training SCADA HMI page is mainly used for training and demonstration task. The page is made based on the top view of the 3D platform (as shown below Figuer_1.1.1.1) by added the control buttons and indicators at the same position of the image.



<Figure_1.1.1.1 Top view of OT-Platform>

The Training HMI contents 3 section:

Main system page:

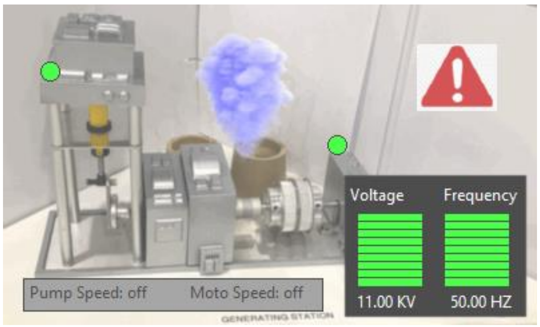
Figure_1.1.1.4

Power generator situation dashboard:

Figure_1.1.1.2

Power substation dashboard:

Figure_1.1.1.3



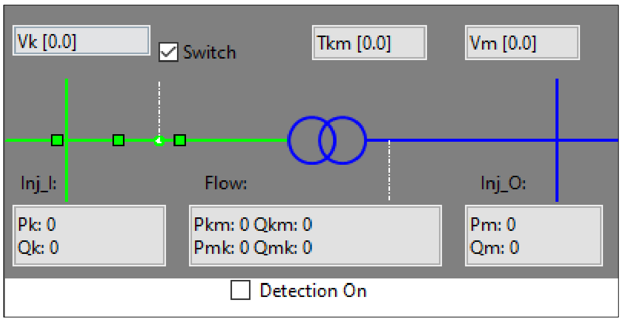
Pump Speed: off

Moto Speed: off

11.00 KV

50.00 HZ

<Figure_1.1.1.2 Generator dashboard>



Vk [0.0]

☑ Switch

Tkm [0.0]

Vm [0.0]

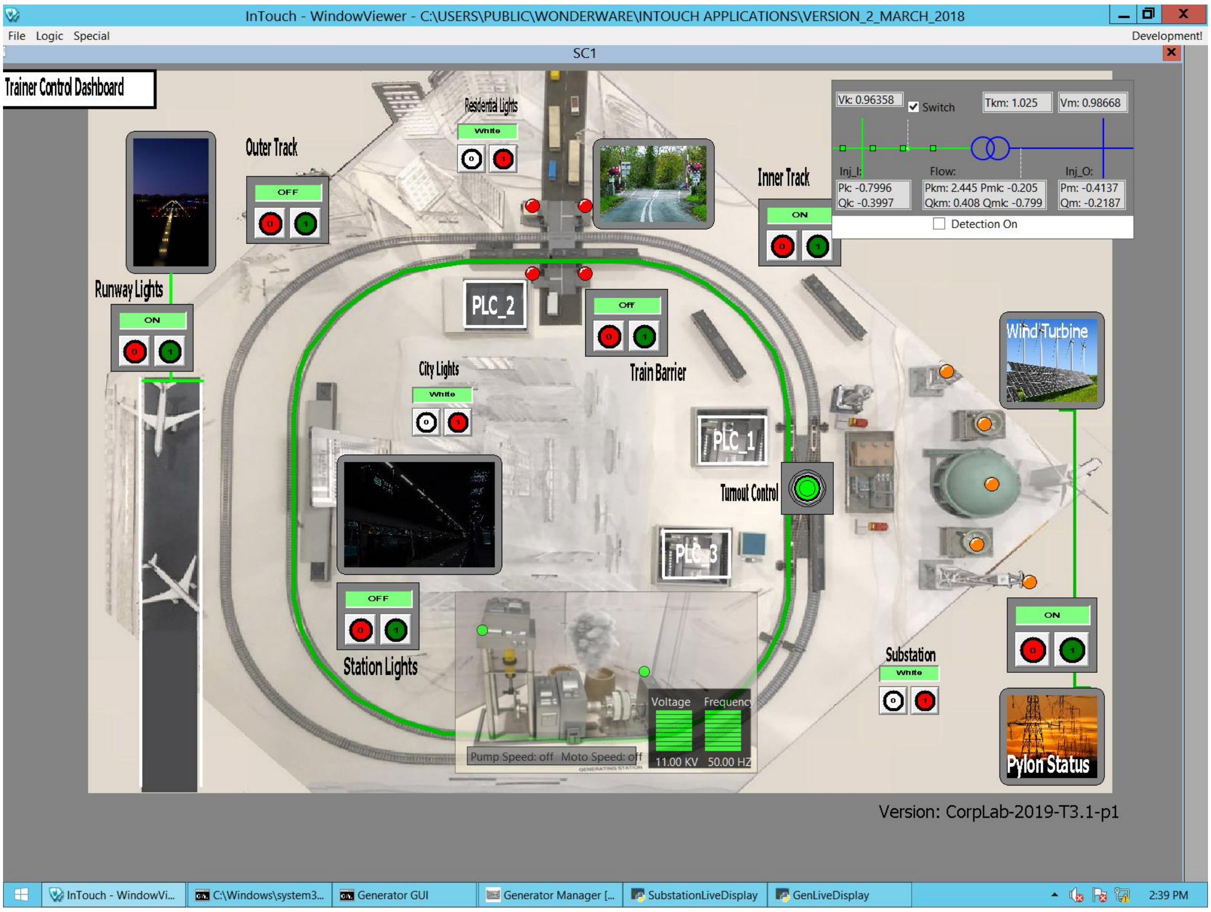
Pk: 0
Qk: 0

Pkm: 0 Qkm: 0
Pmk: 0 Qmk: 0

Pm: 0
Qm: 0

☐ Detection On

<Figure_1.1.1.3 Substation dashboard>



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

Vk: 0.96358 ☑ Switch Tkm: 1.025 Vm: 0.98668

Inj_I: Flow: Inj_O:

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

Pump Speed: off Moto Speed: off

Voltage 11.00 KV Frequency 50.00 HZ

Version: CorpLab-2019-T3.1-p1

<Figure_1.1.1.4 Main system page >

1.1.2 Control buttons on the main system page: the components' power is controlled by the buttons (red and green colour) with on/off label near it in the page (As shown in the Figure_1.1.5):

- Airport runway light on/off control.
- Outer railway track power on/off control.
- Train station light and train position sensor power on/off control.
- City lights colour white/red control.
- Industrial area background lights colour white/red control.
- Train barrier at the cross power and train position on/off control.
- Inner railway track power on/off control.
- Inner/outer track fork switch control.
- Substation pylon and wind turbine indicators on/off control.
- Substation background light colour while/red control.

1.1.3 Camera view simulation window

There are five camera simulation view windows for airport, train station, train barrier, wind turbine and pylon station in the HMI page. They will show the different image view based on the current component state.

1.1.4 Components state indicators on main page

Runway light indicator: white colour outline and green base line will appear when the power is on.

Cross barrier indicator: four dot indicators will change to red when the barrier at down block position, they will change to green when the barrier at up position.

City, Industrial and Residential area background indicators: The outline of these area will change to red and flash if the red button was pressed, otherwise the outline will not show.

Railway track indicator: the railway will change to green colour if the track's power is on.

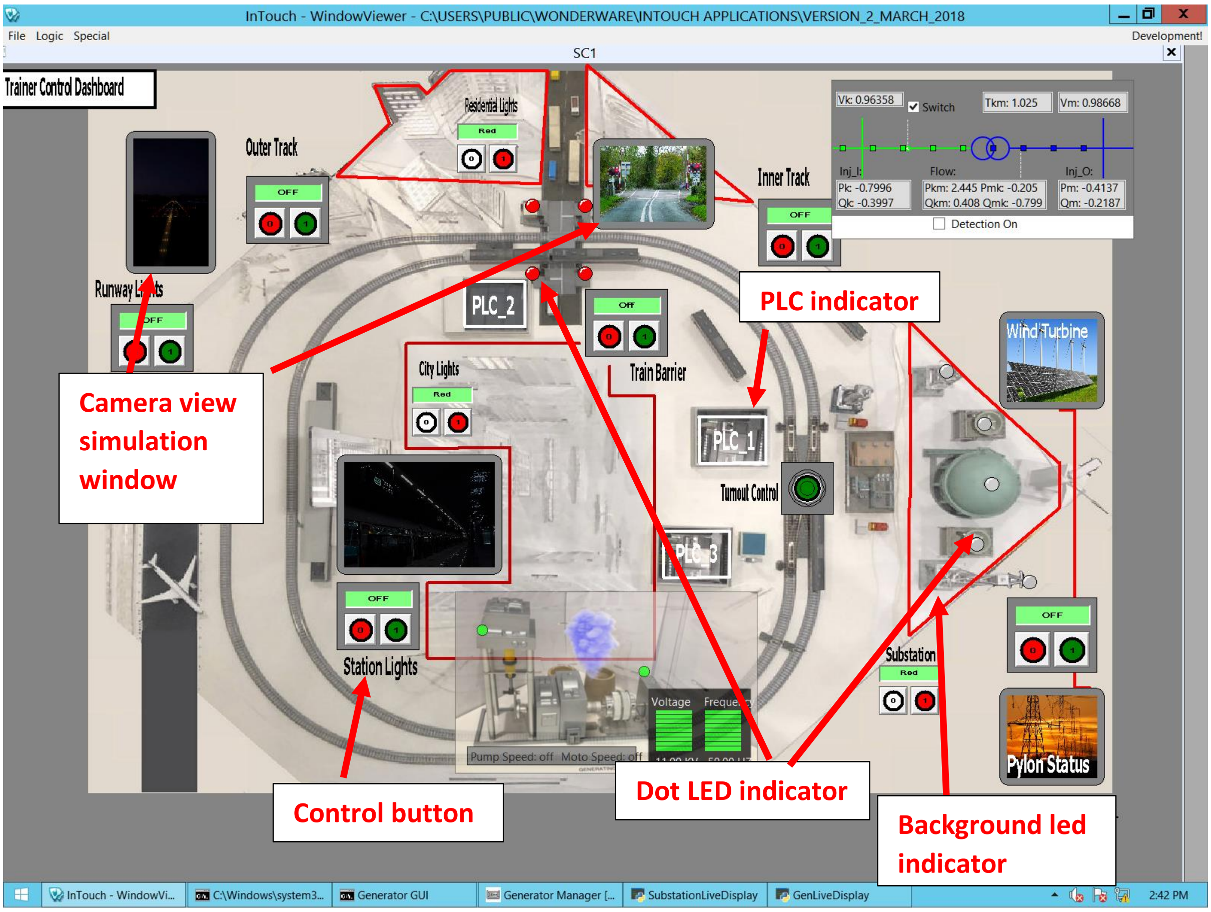
Railway track toggle indicator: a link line will be shown under the fork toggle switch to link the inner and outer tracks if the fork switch is on.

Power substation indicator: the five dots indicator will change to orange colour if the power substation's power is on.

Train station indicator: The train station will be highlighted with while colour outline if its power is on.

PLC position indicator: White colour rectangle box with PLC index label to show the real position of the three PLC in the platform.

1.1.5 Control button, view window and Indicator position view:



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

Camera view simulation window

PLC indicator

Control button

Dot LED indicator

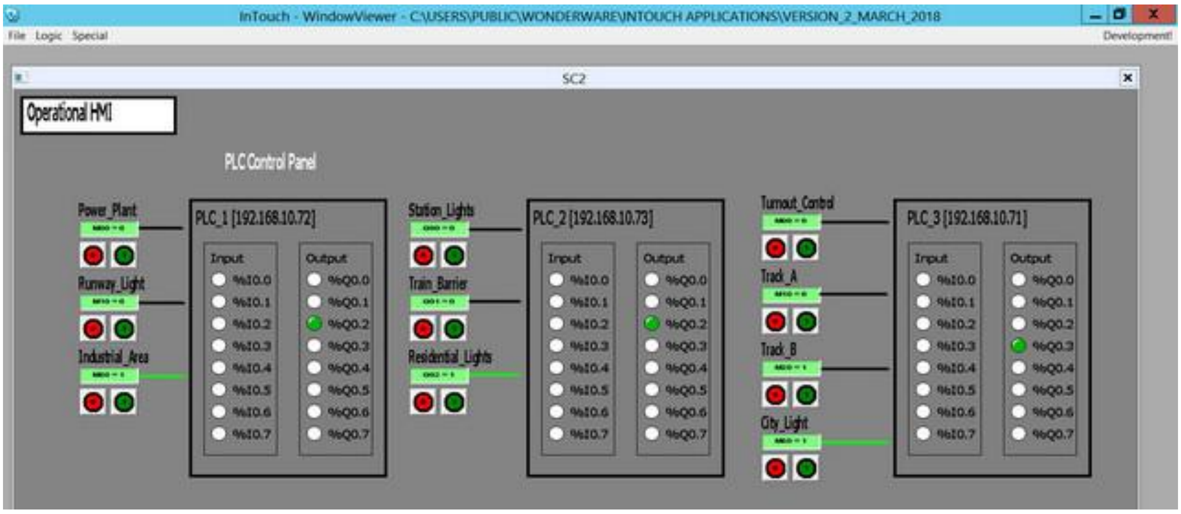
Background led indicator

<Figure_1.1.5 display components position>

1.1.6 Active the Training HMI page: Double Click the InTouch icon on the desktop => File => View => check the "Page SC1" checkout box in the pop-up window.

## 1.2 PLC Status View HMI page

1.2.1 The PLC status view page will show the current three PLC modules' input and output coils signal state. (white dot means signal low and green dot means signal high). The link will show the control relationship between the buttons (shown in the Training HMI page in section 1.1) and the PLCs. (Black linking line means the button sent the turn off signal and the green linking line means the button sent the turn on signal). The PLC index and its IP address are shown in the label.

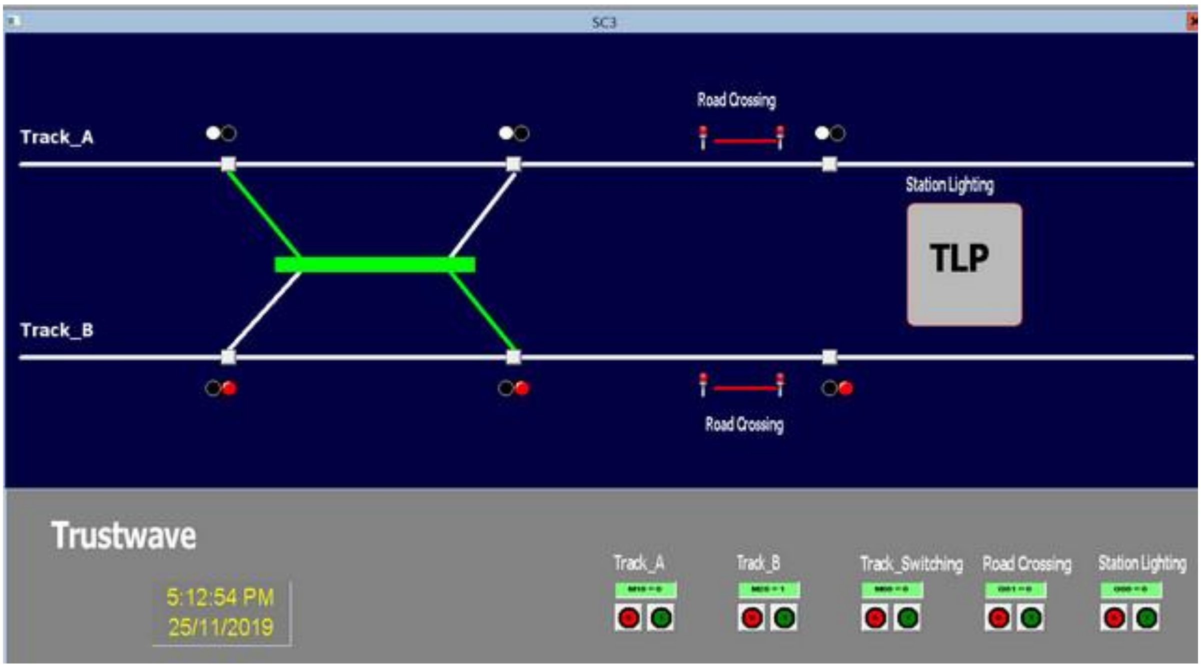


<Figure1.2.1 PLC status page view >

1.2.2 Active the PLC status page: Double Click the InTouch icon on the desktop => File => View => check the "Page SC2" checkout box in the pop-up window.

## 1.3 Railway Command and Control HMI page

1.3.1 HMI Page View:



<Figure1.3.1 Railway command and control page view >

The Railway Command and Control HMI page will simulate the control of the railway system. It contents four main kinds of indicators:

- Fork switch indicator: The “X” shape linkage line between the two tracks will show the current linkage status (linked/parallel) of the two tracks. If the path is green colours, which means the train will go through that path when it is running through.

- Cross barrier indicator: It will show a green pass road when the barrier is at the up position, the road will disappear, and the two sides will be blocked by red line if the barrier is at down and block position.

- Train station indicator: The grey rectangle wit label “TLP” will show the current power supply situation of the train station. When the train stops at the station the outline of the station will change to green colour.

- Train position dot indicator: The pair dots LED near the tack line will indicate the position of the train. (This indicator’s function was under development.)

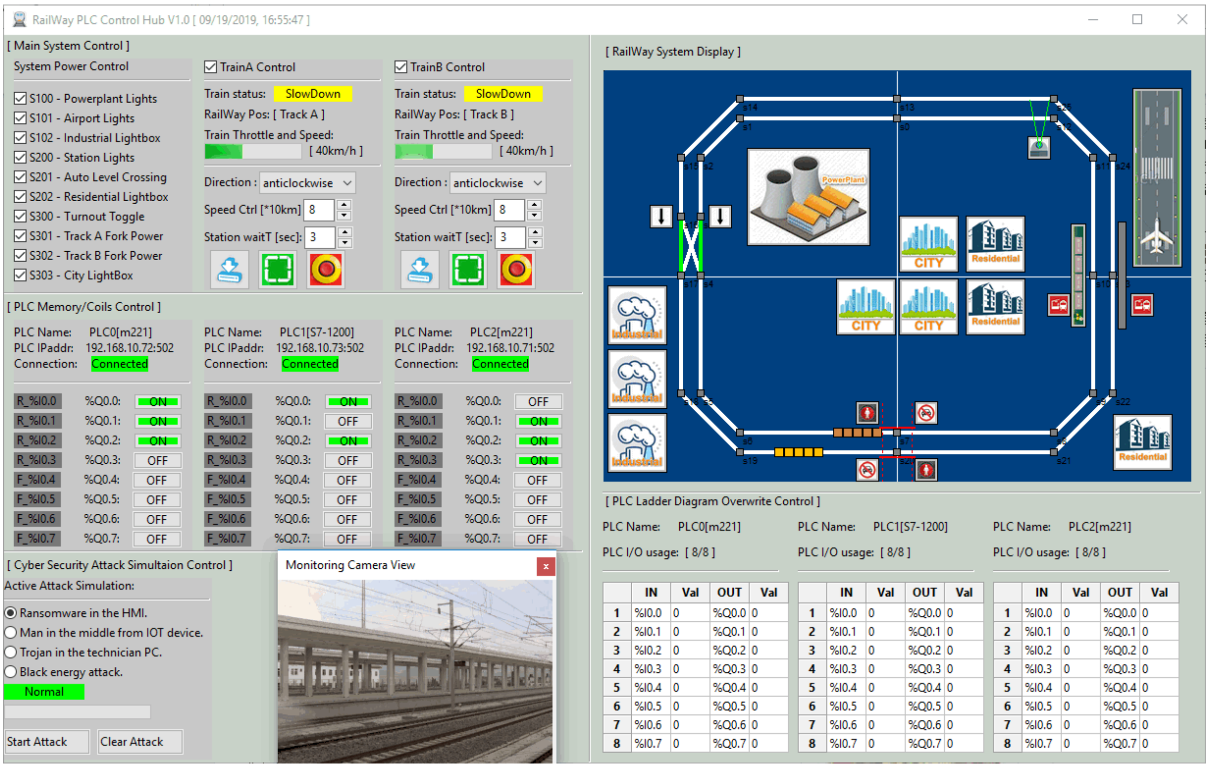
1.3.2 Button area

The buttons at the bottom line are used to control the power supply of the railway system: Inner track and outer track power, the fork switch, cross barrier, and train station power.

1.3.4 Active the Railway command and control HMI page: Double Click the InTouch icon on the desktop => File => View => check the “Page SC3” checkout box in the pop-up window.

## 1.4 Development and Debug HMI

1.4.1 HMI Page View:



RailWay PLC Control Hub V1.0 [ 09/19/2019, 16:55:47 ]

[ Main System Control ]

System Power Control

☑ S100 - Powerplant Lights
☑ S101 - Airport Lights
☑ S102 - Industrial Lightbox
☑ S200 - Station Lights
☑ S201 - Auto Level Crossing
☑ S202 - Residential Lightbox
☑ S300 - Turnout Toggle
☑ S301 - Track A Fork Power
☑ S302 - Track B Fork Power
☑ S303 - City LightBox

☑ TrainA Control

Train status: SlowDown
RailWay Pos: [ Track A ]
Train Throttle and Speed: [ 40km/h ]
Direction : anticlockwise
Speed Ctrl [*10km] 8
Station waitT [sec]: 3

☑ TrainB Control

Train status: SlowDown
RailWay Pos: [ Track B ]
Train Throttle and Speed: [ 40km/h ]
Direction : anticlockwise
Speed Ctrl [*10km] 8
Station waitT [sec]: 3

[ PLC Memory/Coils Control ]

PLC Name: PLC0[m221]
PLC IPaddr: 192.168.10.72:502
Connection: Connected

| | | |
|---|---|---|
| R_%I0.0 | %Q0.0: | ON |
| R_%I0.1 | %Q0.1: | ON |
| R_%I0.2 | %Q0.2: | ON |
| R_%I0.3 | %Q0.3: | OFF |
| F_%I0.4 | %Q0.4: | OFF |
| F_%I0.5 | %Q0.5: | OFF |
| F_%I0.6 | %Q0.6: | OFF |
| F_%I0.7 | %Q0.7: | OFF |

PLC Name: PLC1[S7-1200]
PLC IPaddr: 192.168.10.73:502
Connection: Connected

| | | |
|---|---|---|
| R_%I0.0 | %Q0.0: | ON |
| R_%I0.1 | %Q0.1: | OFF |
| R_%I0.2 | %Q0.2: | ON |
| R_%I0.3 | %Q0.3: | OFF |
| F_%I0.4 | %Q0.4: | OFF |
| F_%I0.5 | %Q0.5: | OFF |
| F_%I0.6 | %Q0.6: | OFF |
| F_%I0.7 | %Q0.7: | OFF |

PLC Name: PLC2[m221]
PLC IPaddr: 192.168.10.71:502
Connection: Connected

| | | |
|---|---|---|
| R_%I0.0 | %Q0.0: | OFF |
| R_%I0.1 | %Q0.1: | ON |
| R_%I0.2 | %Q0.2: | ON |
| R_%I0.3 | %Q0.3: | ON |
| F_%I0.4 | %Q0.4: | OFF |
| F_%I0.5 | %Q0.5: | OFF |
| F_%I0.6 | %Q0.6: | OFF |
| F_%I0.7 | %Q0.7: | OFF |

[ Cyber Security Attack Simultaion Control ]

Active Attack Simulation:

● Ransomware in the HMI.
○ Man in the middle from IOT device.
○ Trojan in the technician PC.
○ Black energy attack.

Normal

Start Attack
Clear Attack

Monitoring Camera View

[ RailWay System Display ]

[ PLC Ladder Diagram Overwrite Control ]

PLC Name: PLC0[m221]
PLC I/O usage: [ 8/8 ]

| | IN | Val | OUT | Val |
|---|---|---|---|---|
| 1 | %I0.0 | 0 | %Q0.0 | 0 |
| 2 | %I0.1 | 0 | %Q0.1 | 0 |
| 3 | %I0.2 | 0 | %Q0.2 | 0 |
| 4 | %I0.3 | 0 | %Q0.3 | 0 |
| 5 | %I0.4 | 0 | %Q0.4 | 0 |
| 6 | %I0.5 | 0 | %Q0.5 | 0 |
| 7 | %I0.6 | 0 | %Q0.6 | 0 |
| 8 | %I0.7 | 0 | %Q0.7 | 0 |

PLC Name: PLC1[S7-1200]
PLC I/O usage: [ 8/8 ]

| | IN | Val | OUT | Val |
|---|---|---|---|---|
| 1 | %I0.0 | 0 | %Q0.0 | 0 |
| 2 | %I0.1 | 0 | %Q0.1 | 0 |
| 3 | %I0.2 | 0 | %Q0.2 | 0 |
| 4 | %I0.3 | 0 | %Q0.3 | 0 |
| 5 | %I0.4 | 0 | %Q0.4 | 0 |
| 6 | %I0.5 | 0 | %Q0.5 | 0 |
| 7 | %I0.6 | 0 | %Q0.6 | 0 |
| 8 | %I0.7 | 0 | %Q0.7 | 0 |

PLC Name: PLC2[m221]
PLC I/O usage: [ 8/8 ]

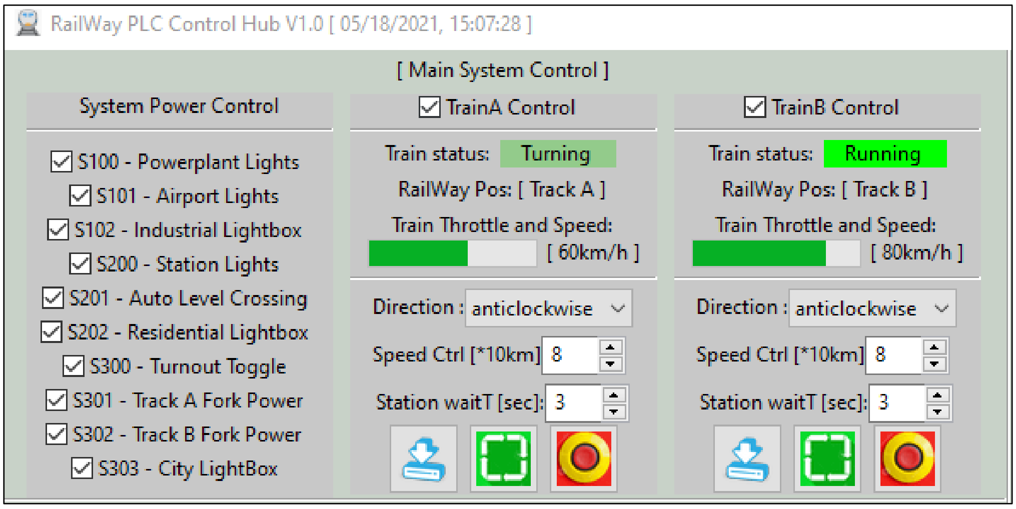
| | IN | Val | OUT | Val |
|---|---|---|---|---|
| 1 | %I0.0 | 0 | %Q0.0 | 0 |
| 2 | %I0.1 | 0 | %Q0.1 | 0 |
| 3 | %I0.2 | 0 | %Q0.2 | 0 |
| 4 | %I0.3 | 0 | %Q0.3 | 0 |
| 5 | %I0.4 | 0 | %Q0.4 | 0 |
| 6 | %I0.5 | 0 | %Q0.5 | 0 |
| 7 | %I0.6 | 0 | %Q0.6 | 0 |
| 8 | %I0.7 | 0 | %Q0.7 | 0 |

<Figure_1.4.1 Development and debug HMI view>

The Development and debug HMI is developed by using Python3.7 and wxPython. This program is used for showing the developer the deeper/lower-level debug information during the system is running. When enabled the test mode, it can simulate all the real action of the 3D platform based on the user’s action without connecting to the read hardware. It can also simulate some extend function which is not provided by the 3D-Platform hardware for further development. It contents 6 main sections for simulating or implementing the different function: Main system control section, PLC output status display section, Cyber security attack simulation control section, train surveillance camera simulation section, Railway system display section and the PLC ladder diagram overwrite control section.

### 1.4.2 Main system control section

The checkboxes in the system power control are used to turn on/off all the power buttons in the system. The two trains control panel is used to control the two trains simulation state in the inner and outer track. In the train control panel, the user can simulate configuring the train speed, running direction, stop duration in the train station. Press the blue load button will load the current train configuration shown on the panel into the right-side display simulation section. The green button will start the train and the red button is the emergency stop button.



RailWay PLC Control Hub V1.0 [ 05/18/2021, 15:07:28 ]

[ Main System Control ]

System Power Control

☑ S100 - Powerplant Lights
☑ S101 - Airport Lights
☑ S102 - Industrial Lightbox
☑ S200 - Station Lights
☑ S201 - Auto Level Crossing
☑ S202 - Residential Lightbox
☑ S300 - Turnout Toggle
☑ S301 - Track A Fork Power
☑ S302 - Track B Fork Power
☑ S303 - City LightBox

☑ TrainA Control

Train status: Turning
RailWay Pos: [ Track A ]
Train Throttle and Speed: [ 60km/h ]
Direction : anticlockwise
Speed Ctrl [*10km] 8
Station waitT [sec]: 3

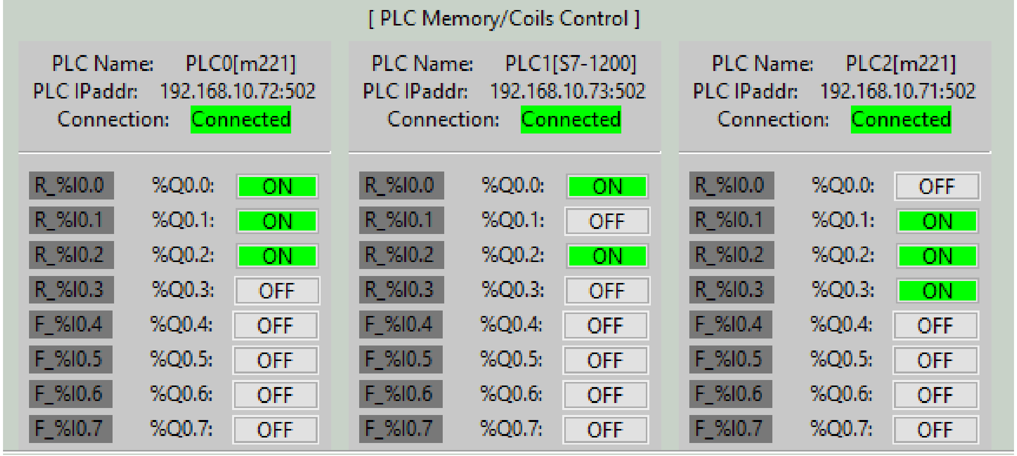
☑ TrainB Control

Train status: Running
RailWay Pos: [ Track B ]
Train Throttle and Speed: [ 80km/h ]
Direction : anticlockwise
Speed Ctrl [*10km] 8
Station waitT [sec]: 3

<Figure_1.4.2 Main system control section >

### 1.4.3 PLC memory/coils control section

This section will show the control sequence from an input signal to the related PLC memory register and the changeable register to output coils control /state of the 3 PLCs based on the ladder diagram. 5V signal high will be marked as green colour and 0V signal low will be marked as grey colour. Input read register will be marked as "I_%" and output register will be marked as "Q_%".



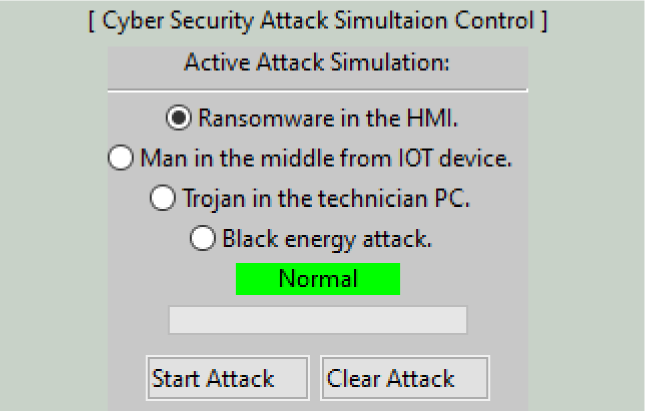
[ PLC Memory/Coils Control ]

| PLC Name: PLC0[m221]<br>PLC IPaddr: 192.168.10.72:502<br>Connection: Connected | | | PLC Name: PLC1[S7-1200]<br>PLC IPaddr: 192.168.10.73:502<br>Connection: Connected | | | PLC Name: PLC2[m221]<br>PLC IPaddr: 192.168.10.71:502<br>Connection: Connected | | |
|---|---|---|---|---|---|---|---|---|
| R_%I0.0 | %Q0.0: | ON | R_%I0.0 | %Q0.0: | ON | R_%I0.0 | %Q0.0: | OFF |
| R_%I0.1 | %Q0.1: | ON | R_%I0.1 | %Q0.1: | OFF | R_%I0.1 | %Q0.1: | ON |
| R_%I0.2 | %Q0.2: | ON | R_%I0.2 | %Q0.2: | ON | R_%I0.2 | %Q0.2: | ON |
| R_%I0.3 | %Q0.3: | OFF | R_%I0.3 | %Q0.3: | OFF | R_%I0.3 | %Q0.3: | ON |
| F_%I0.4 | %Q0.4: | OFF | F_%I0.4 | %Q0.4: | OFF | F_%I0.4 | %Q0.4: | OFF |
| F_%I0.5 | %Q0.5: | OFF | F_%I0.5 | %Q0.5: | OFF | F_%I0.5 | %Q0.5: | OFF |
| F_%I0.6 | %Q0.6: | OFF | F_%I0.6 | %Q0.6: | OFF | F_%I0.6 | %Q0.6: | OFF |
| F_%I0.7 | %Q0.7: | OFF | F_%I0.7 | %Q0.7: | OFF | F_%I0.7 | %Q0.7: | OFF |

<Figure_1.4.3 PLC memory/coils control section >

### 1.4.4 Cyber Security attack simulation control section

This section will simulate the four kinds of IT/OT cyber-attack scenario to the simulation system: ransomware to the main system control part, Man in the mid to the PLC sensor and system auto-control part, Trojan program attack to the PLC control part and computer connect to the system, Black energy attack to the whole system's power supply. The attack indicator and progress bar under the attack category will show the current attack status. Gray colour indicator means the attack is clear, yellow means the attack has been activated, red means the system was under the attack situation.



[ Cyber Security Attack Simultaion Control ]

Active Attack Simulation:

● Ransomware in the HMI.

○ Man in the middle from IOT device.

○ Trojan in the technician PC.

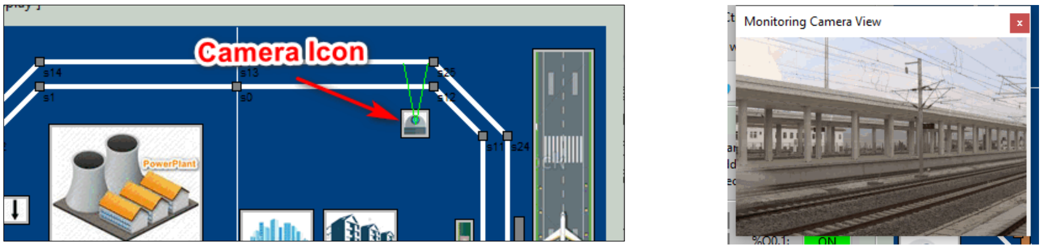
○ Black energy attack.

Normal

<Figure_1.4.4 Cyber Security attack simulation control section>

### 1.4.5 Surveillance camera simulation section

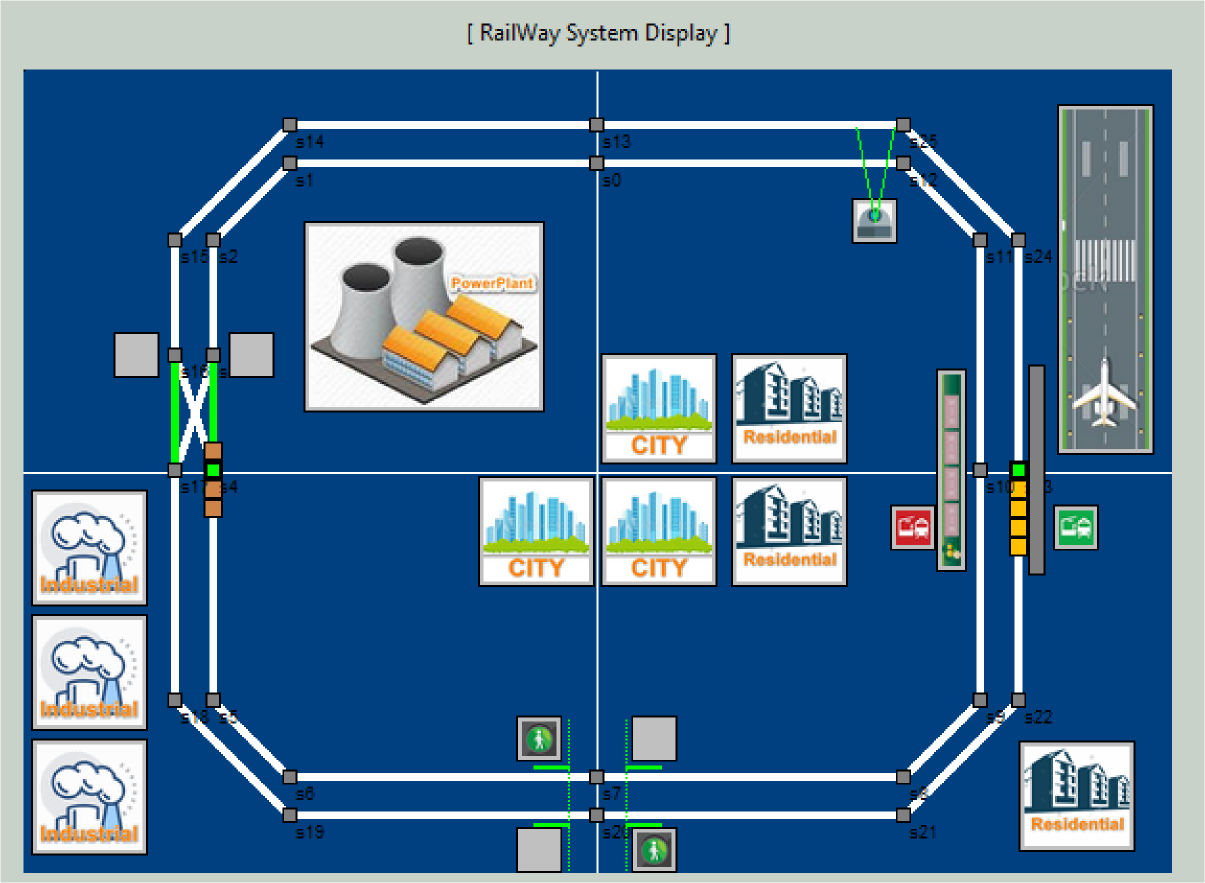
The surveillance camera simulator is a pop-up window which used to simulate the time when a train pass through a railway surveillance camera. Press the camera icon (As shown below Figure_1.4.5) in the Railway system display section, the window will pop up at the bottom of the screen. When the train icon running pass the camera's view line (2 dash line from the camera icon), the window will show a real train pass in the window view.



<Figure_1.4.5 Camera view Icon position and the pop-up camera window>

### 1.4.6 System display section

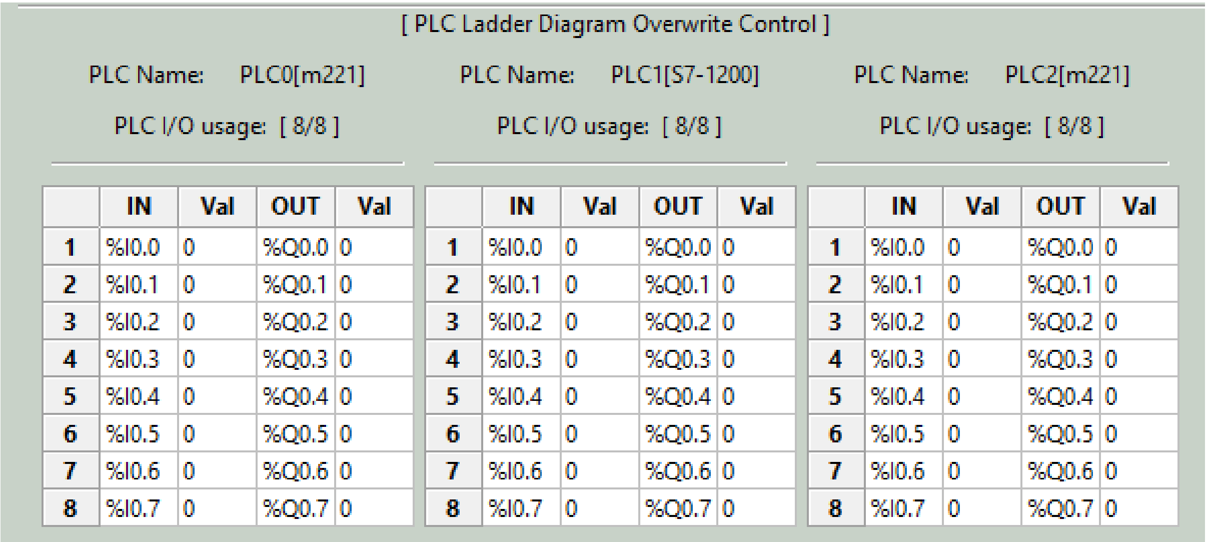
This section will show the simulation of all the system hardware's action by animation. The icon of the components will change to grey colour if their power is turned off. It can also simulate the train running on difference direction, the sensors detecting trains pass and the emergency of the system during the cyber-attack. (such as the accident two train crash with each other or the accident when the train pass a cross which the barrier will not at block position) When the auto control system detects an accident happens, it will pop-up a red alert window.



<Figure_1.4.6 System display section >

### 1.4.7 PLC Ladder diagram overwrite control section

This section will be used to simulate the user manually change the register value in the three PLCs' ladder diagram directly with the Schneider's PLC programming software. The list under the plc information label will show all the memory registers' value, the user can change the value and press the "set" button to override the current system configuration setting. This adjustment will have the highest change priority overall other sections.



[ PLC Ladder Diagram Overwrite Control ]

PLC Name: PLC0[m221]

PLC I/O usage: [ 8/8 ]

| | IN | Val | OUT | Val |
|---|---|---|---|---|
| 1 | %I0.0 | 0 | %Q0.0 | 0 |
| 2 | %I0.1 | 0 | %Q0.1 | 0 |
| 3 | %I0.2 | 0 | %Q0.2 | 0 |
| 4 | %I0.3 | 0 | %Q0.3 | 0 |
| 5 | %I0.4 | 0 | %Q0.4 | 0 |
| 6 | %I0.5 | 0 | %Q0.5 | 0 |
| 7 | %I0.6 | 0 | %Q0.6 | 0 |
| 8 | %I0.7 | 0 | %Q0.7 | 0 |

PLC Name: PLC1[S7-1200]

PLC I/O usage: [ 8/8 ]

| | IN | Val | OUT | Val |
|---|---|---|---|---|
| 1 | %I0.0 | 0 | %Q0.0 | 0 |
| 2 | %I0.1 | 0 | %Q0.1 | 0 |
| 3 | %I0.2 | 0 | %Q0.2 | 0 |
| 4 | %I0.3 | 0 | %Q0.3 | 0 |
| 5 | %I0.4 | 0 | %Q0.4 | 0 |
| 6 | %I0.5 | 0 | %Q0.5 | 0 |
| 7 | %I0.6 | 0 | %Q0.6 | 0 |
| 8 | %I0.7 | 0 | %Q0.7 | 0 |

PLC Name: PLC2[m221]

PLC I/O usage: [ 8/8 ]

| | IN | Val | OUT | Val |
|---|---|---|---|---|
| 1 | %I0.0 | 0 | %Q0.0 | 0 |
| 2 | %I0.1 | 0 | %Q0.1 | 0 |
| 3 | %I0.2 | 0 | %Q0.2 | 0 |
| 4 | %I0.3 | 0 | %Q0.3 | 0 |
| 5 | %I0.4 | 0 | %Q0.4 | 0 |
| 6 | %I0.5 | 0 | %Q0.5 | 0 |
| 7 | %I0.6 | 0 | %Q0.6 | 0 |
| 8 | %I0.7 | 0 | %Q0.7 | 0 |

<Figure_1.4.6 PLC Ladder diagram overwrite control section>

## 2. Program Setup and Configuration

This section will show how to setup the execution environment and install the program on the computer for testing and further development.

### 2.1 Program Setup

2.1.1 Development Environment:

Python 2.7 & python 3.7, HTML5, Schneider Wonderware IDE

2.1.2 Additional Lib/Software Need:

- wxPython 4.0.6 (build UI this lib need to be installed): `$ pip install -U wxPython`

- snap7 + python-snap7 (need to install for S71200 PLC control) Install instruction:

http://simplyautomationized.blogspot.com/2014/12/raspberry-pi-getting-data-from-s7-1200.html

### 2.2 Program Files List

| Program File | Execution Env | Description |
|---|---|---|
| src/M2PLC221.py | python 2.7/3 | This module is used to connect the Schneider M2xx PLC. |
| src/railwayAgentPLC.py | python 3 | This module is the agent module to init different items in the railway system or create the interface to connect to the hardware. |
| src/railwayGlobal.py | python 3 | This module is used as the local config file to set constants, global parameters which will be used in the other modules. |
| src/railwayHub.py | python 3 | This function is used to create a rail control hub to show the different situation of the cyber-security attack's influence for the railway HMI and PLC system. |
| src/railwayMgr.py | python 3 | This function is the railway function manager to connect the agent element with their control panel. |
| src/railWayPanel.py | python 3 | This module is used to provide different function panels for the railway hub function. |
| src/railWayPanelMap.py | python 3 | This module is used to show the top view of the main city map in the railway system. |
| src/ S7PLC1200.py | python 3 | This module is used to connect the siemens s7-1200 PLC |
| attack/ City_Zone.smbp | Schneider Wonderware IDE | City Zone PLC ladder diagram used to load for PCL1. |
| attack/Industrial_Zone.smbp | Schneider Wonderware IDE | Industrial Zone PLC ladder diagram used to load for PCL3. |

## 3. Program Execution

This section will show how to execute the two HMI program on your computer and demo cyber-attack .

### 3.1 Wonderware HMI Execution

Plug in the Schneider-Wanderware USB licence key into your computer, double click the “InTouch Viewer” icon, then select the related page in the main window.

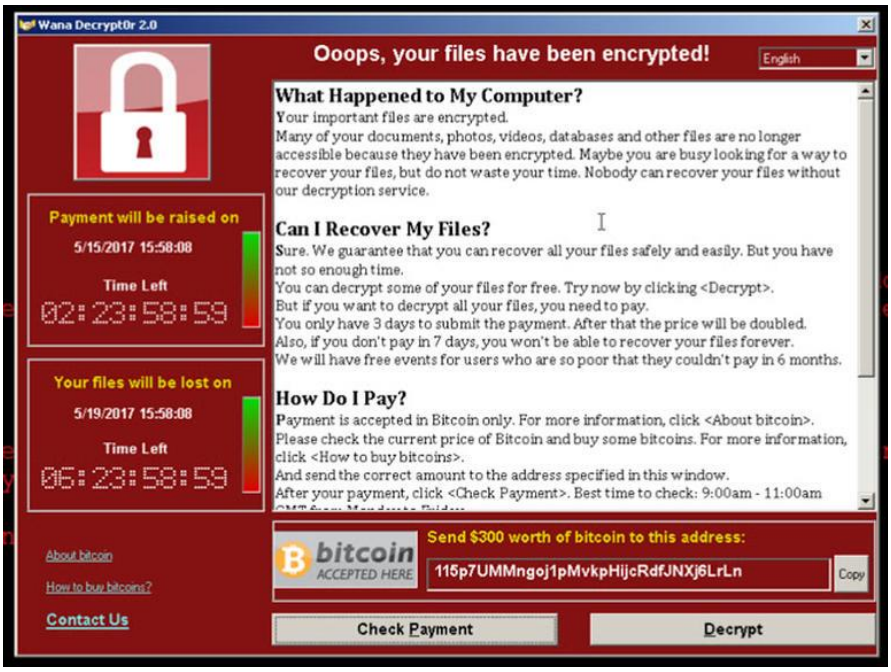
### 3.2 Development and Debug HMI Execution

Open the “src” folder and run program execution cmd: **$python railwayHub.py**

### 3.3 Development and Debug HMI Cyber Attack Active

3.3.1 Ransomware attack

Check the “Ransomware in the HMI” checkbox in the attack control section, then press the “Start attack” button. In the HMI main system control section, all the checkboxes and buttons will be freezing during the attack and when you click the other part of the HMI program, a Ransomware attack message box will pop up as shown below (Figure 3.3.1):



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

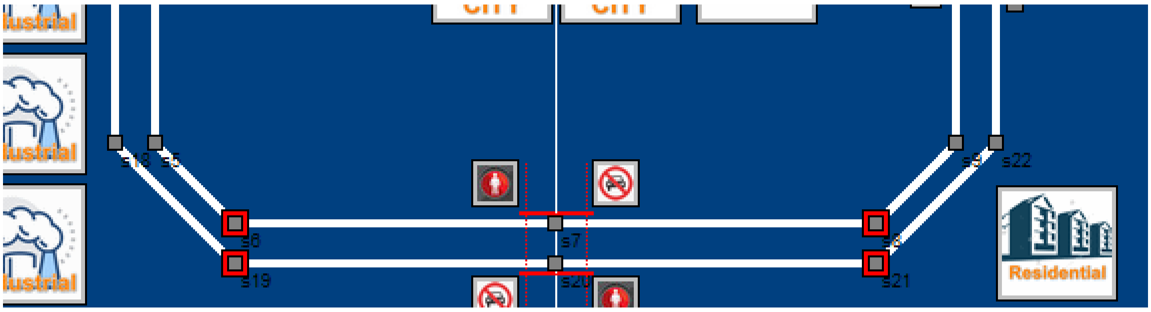
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

<Figure_3.3.1 Ransomware attack alert message window>

Recover: Press the “Clear attack” button will stop the attack directly.

3.3.2 Man in the middle attack

Check the “Man in the middle attack” checkbox in the attack control section, then press the “Start attack” button. The camera will be used as the attack device, when the attack started you can see the train position sensors before and after the barrier will be block and the attack will insert the fake position feedback data to the system which cause the accident happens at the railway cross barrier position. The hacked train sensor will be marked as red colour and will not feedback any signal when the trains go pass them. (As shown below Figure_3.3.2)

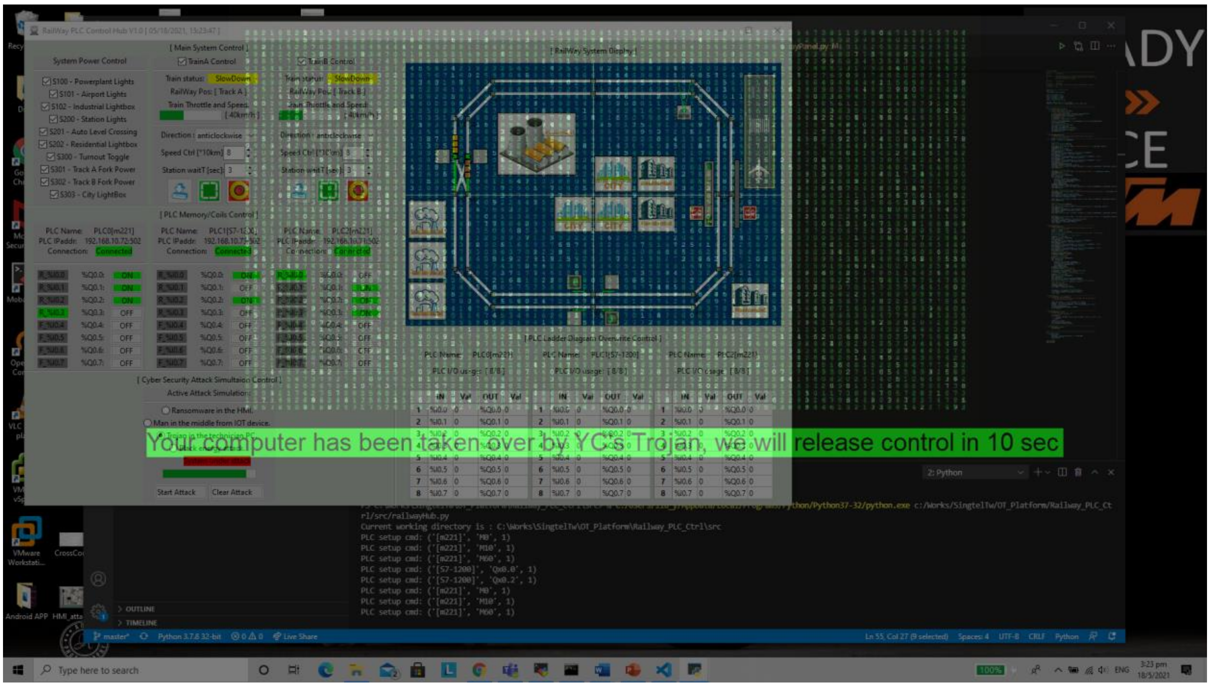


<Figure_3.3.2 Train barriers situation under man in the middle attack >

Recover: Press the “Clear attack” button will stop the attack directly.

3.3.3 Trojan program in the technical PC.

Check the “Trojan in the technical PC” checkbox in the attack control section, then press the “Start attack” button. During the attack, whole PC will be freezing (as the PC control has been taken over by Trojan, the user can only move his mouse, but cannot click anything), and the attack screen will show to block the normal desktop of the PC. (As shown below Figure_3.3.3, the transparency of the block window will keep change in range 0% ~100%). Most of the computer’s keyboard buttons will also be disabled during the attack happening.



Your computer has been taken over by YC's Trojan, we will release control in 10 sec

```
rl/src/railwayHub.py
Current working directory is : C:\Works\SingtelTw\OT_Platform\Railway_PLC_Ctrl\src
PLC setup cmd: ('[m221]', 'M0', 1)
PLC setup cmd: ('[m221]', 'M10', 1)
PLC setup cmd: ('[m221]', 'M60', 1)
PLC setup cmd: ('[S7-1200]', 'Qx0.0', 1)
PLC setup cmd: ('[S7-1200]', 'Qx0.2', 1)
PLC setup cmd: ('[m221]', 'M0', 1)
PLC setup cmd: ('[m221]', 'M10', 1)
PLC setup cmd: ('[m221]', 'M60', 1)
```

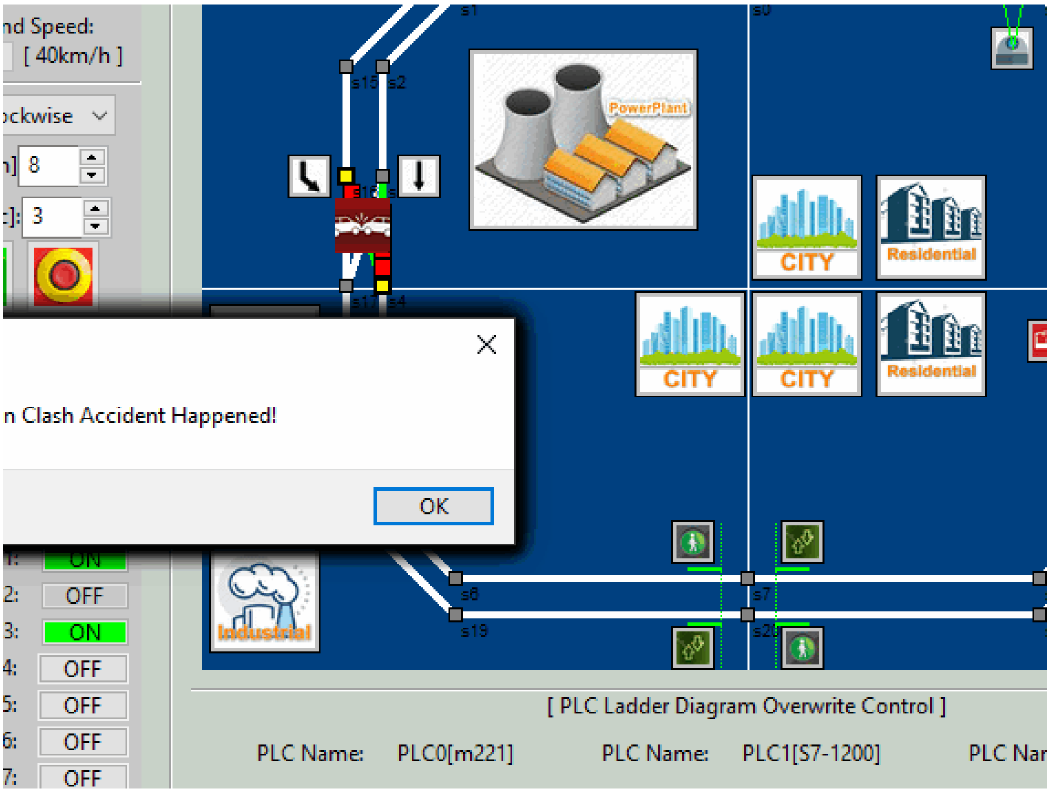
<Figure_3.3.3 Trojan program in the technical PC >

Recover: Press the windows button of the computer and close the block screen first, then press the “Clear attack” button.

3.3.4 Black Out attack:

Blackouts are one of the worst situations, not just for a power utility but for society. Blackouts cause severe financial losses, loss of life due to unavailability of healthcare facilities and bottlenecks in certain critical sectors of society. It is interesting to note that in power grids, a simple mal operation of a critical circuit breaker can cause a blackout. This mal operation of circuit breaker to cause a blackout happened in Ukraine in 2015. A conceptual demonstration of this attack is presented in the platform with special emphasis on various ways this attack could have been averted.

Check the “Black out attack HMI” checkbox int the attack control section, then press the “Start attack” button. During the attack, the power supply for the City and airport will be cut off. The HMI main system control section will not be functioning: the user can still press the button/checkbox, but the display section will not change based on the user’s action. After 20 second the two trains fork will setup to cross and the train crash accident will happen two trains are passing the fork section under the same speed. (As shown below Figure_3.3.4)



nd Speed:
[ 40km/h ]

ckwise

n] 8

:]: 3

n Clash Accident Happened!

OK

1: ON
2: OFF
3: ON
4: OFF
5: OFF
6: OFF
7: OFF

[ PLC Ladder Diagram Overwrite Control ]

PLC Name: PLC0[m221]  PLC Name: PLC1[S7-1200]  PLC Nar

<Figure_3.3.4 Black Out attack >

Recover: Press the “Clear attack” button will stop the attack directly.

# 4.Reference

**N.A**

End (last edited 16/05/2021)