

CSI OT 3D Platform Cyber Attack Demonstration SCADA 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](https://nusu-my.sharepoint.com/personal/dcsshch_nus_edu_sg/Documents/Work%20Related%20Files/Singtel%20OT%20Training/yuancheng.liu@trustwave.com)

Wong Jun Wen

Asst R&D Manager

[junwen.wong@trustwave.com](https://nusu-my.sharepoint.com/personal/dcsshch_nus_edu_sg/Documents/Work%20Related%20Files/Singtel%20OT%20Training/junwen.wong@trustwave.com)

Dr. Shantanu Chakrabarty

NUS Research Fellow

[shantanu1088@gmail.com](https://nusu-my.sharepoint.com/personal/dcsshch_nus_edu_sg/Documents/Work%20Related%20Files/Singtel%20OT%20Training/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.

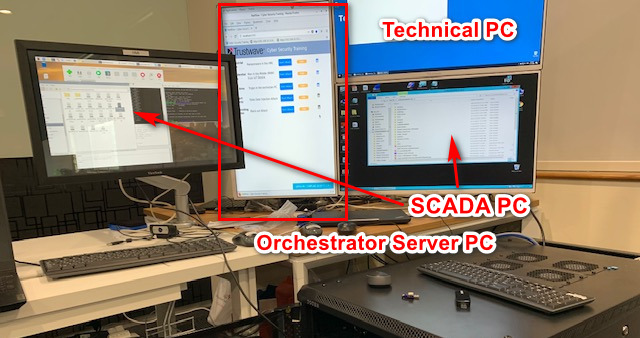
**CSI OT 3D Platform Cyber Attack Demonstration SCADA HMI Design Manual**

**1.Project Introduction**

This project will implement a Supervisory control and data acquisition (SCADA) Human-machine interface (HMI) program to control the main components on the CSI OT-3D Platform. we will create 2 kinds of SCADA HMI system with schneider wonderware(R) program and python for the user to control the PLC railway modules or simulate different railway operation for training or research purpose. The wonderware HMI program are mainly used for the demo purpose, it contents three main pages:

* Training SCADA HMI page used for training and demonstration for the whole system.
* PLC Status View HMI page are using the for the working flow logic of the PLCs 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 wonderware HMI Program will be shown in the SCADA PC in the system with duplicate screen display as shown below:

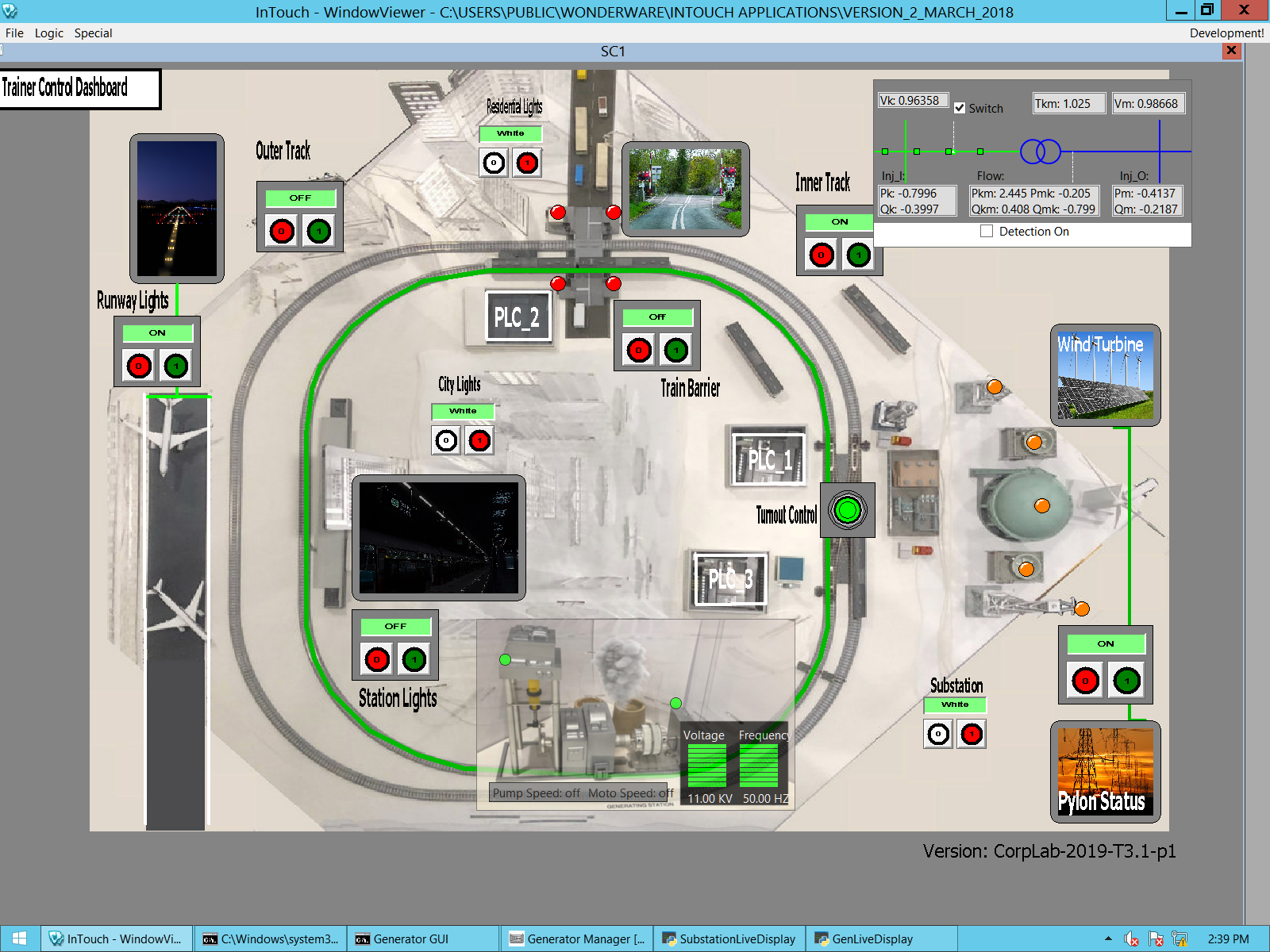


The Development and Debug HMI is created by Python. This program is used for showing the developer the deeper/lower-level debug information during the system is running. I can also simulation some extend function which is not provide by the 3D-Platform hardware for further development. It will also be used for simulating the 3 kinds of cyber-attack situation launched from hacker for the system.

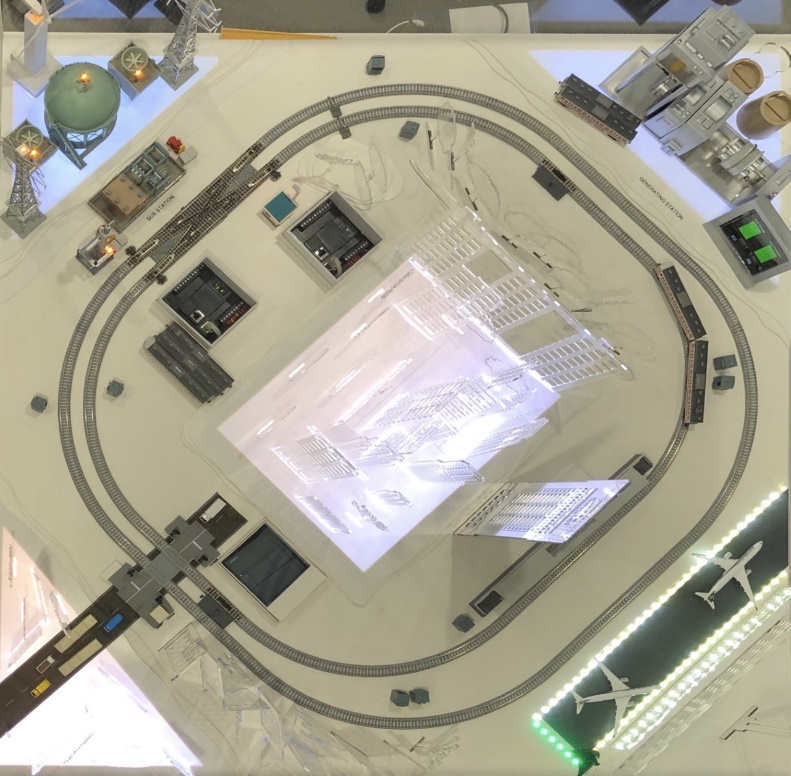
The python HMI can run on any computer which plug in to the system with the IP setup to 192.168.10.150 to 192.168.10.170.

* 1. **Training SCADA HMI Page**

**HMI Page view:**



The page is made based on the top view of the 3D platform system by added the control buttons and indicators at the real position of the image as shown below.

1.1.1 Control buttons: the component power is controlled by the button (red and green colour) with on/off label near it:

* Runway light on/off.
* Outer railway track power on/off.
* Train Station power on/off ctrl.
* City lights colour white/red ctrl.
* Industrial Area background lights colour white/red control.
* Train barrier power control.
* Inner railway track power on/off.
* Inner/outer track fork switch ctrl.
* Substation indicator on/off ctrl.
* Substation light background colour while/red control

1.1.2 Camera view window

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

1.1.3 State indicators

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

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

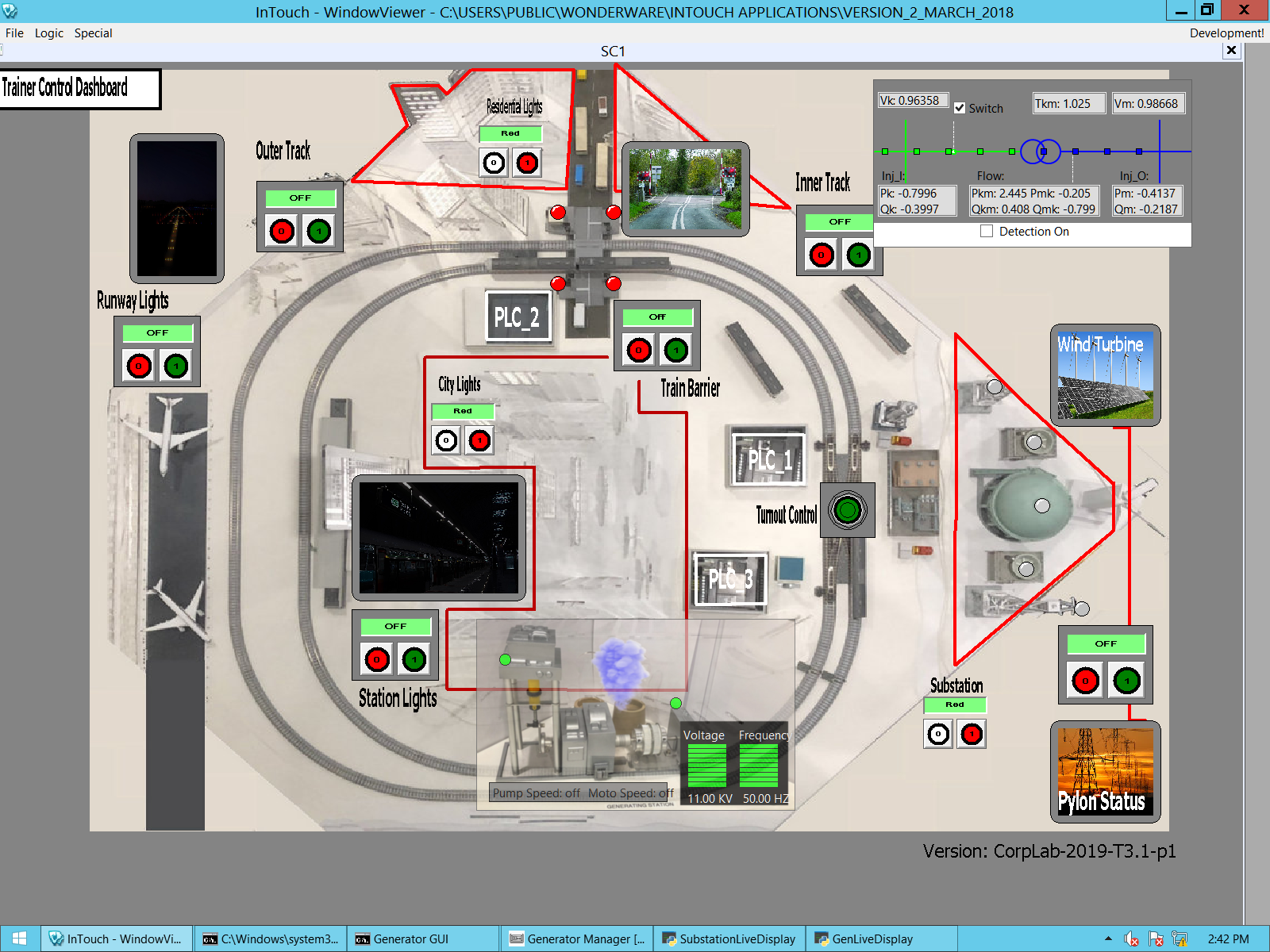
City, Industrial and Residential area background indicator: The outline of the area will change to red and flash if the red button was pressed, otherwise the outline will now show.

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 2 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.

1.1.4 Control button, view window and Indicator position view:



**Dot LED indicator**

**Camera view simulation window**

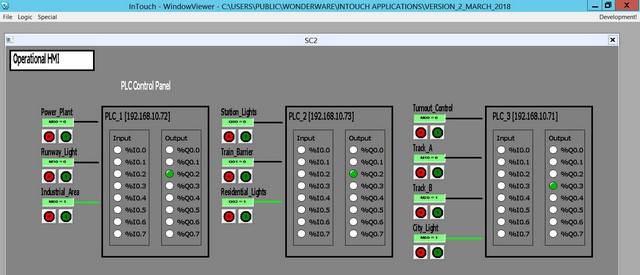
**Background led indicator**

**Control button**

1.1.5 Active the Training HMI page: Double Click the InTouch icon on the desktop => File => View => check the “Page 1” checkout box in the pop-up window.

**1.2 PLC Status View HMI page**

1.2.1 HMI Page View:

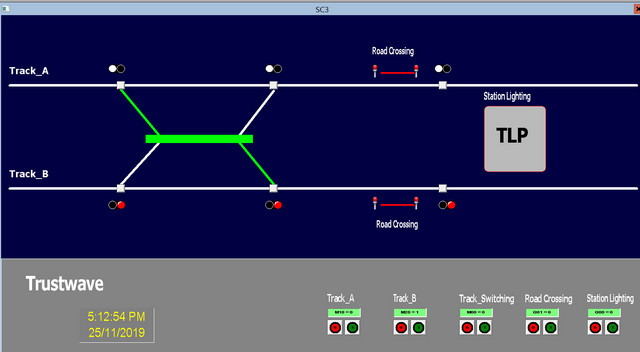


The PLC status view page will show the current three PLC modules’ input and output coils signal state. (While dot means signal low and green dot means signal high). The link will show the control relationship between the buttons shown in the Training HMI page in section 1.1 and the PLCs. (Black linking 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.

1.2.2 Active the PLC status page: Double Click the InTouch icon on the desktop => File => View => check the “Page 2” checkout box in the pop-up window.

**1.3 Railway Command and Control HMI page**

1.3.1 HMI Page View:



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

- Train position dot indicator: The pair dots LED near the tack line will indicate the position of the train.

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

- The barrier indicator: It will show a green pass road when the barrier is is at the up mode, the road will disappear and the two side 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 translation. When the train has stopped at the station the outline of the station will change to green.

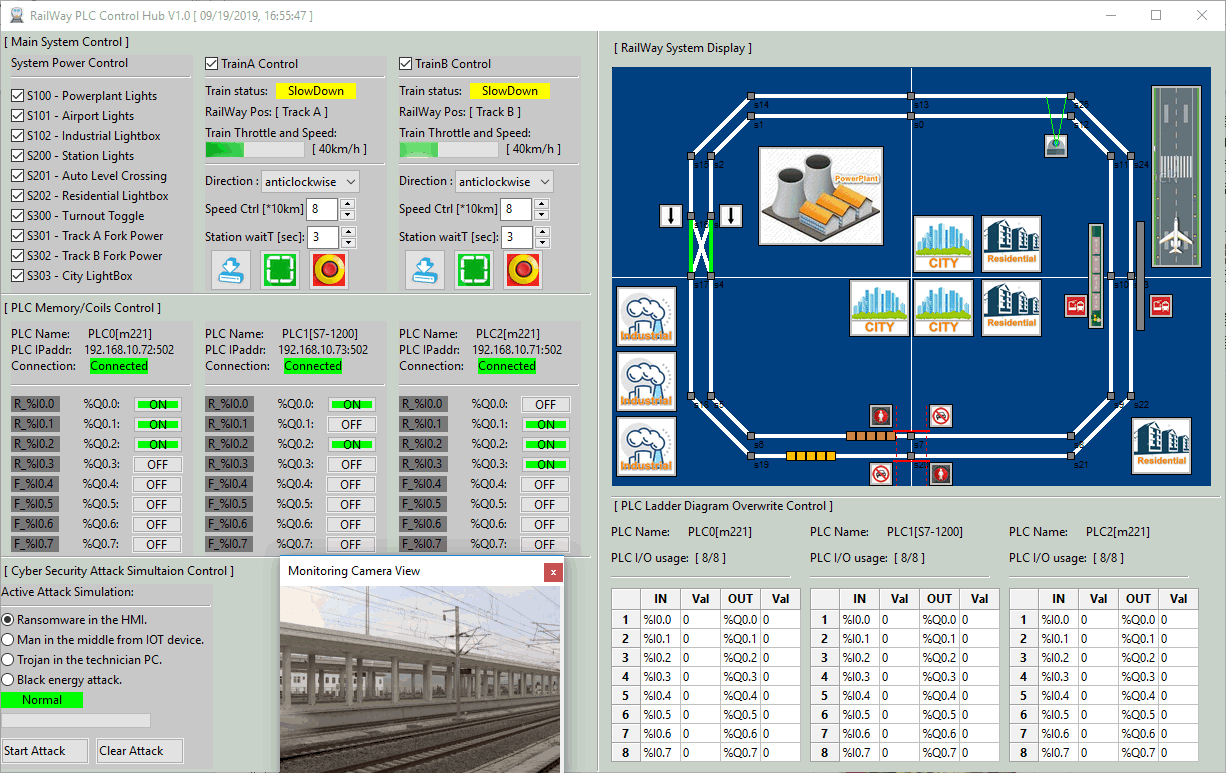
1.3.2 Button area

The button at the button line is used to control the power supply of the railway system: Inner tack and outer tracker’s power. The fork switch, 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 3” checkout box in the pop-up window.

**1.4 Development and Debug HMI**

1.4.1 HMI Page View:



The Development and debug HMI is developed by using python and wxptyhon. This program is used for showing the developer the deeper/lower-level debug information during the system is running. When enable the test mode, it can simulate all the real action of the 3d platform based on the user’s action without connect to the read hardware. It can also simulation some extend function which is not provide by the 3D-Platform hardware for further development. It contents 6 main section for simulating or implementing 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 on/off all the power buttons in the system. The two trains control button is used to control the two trains simulation in the inner and outer track. In the train control button, the user can simulate config the train speed, running direction, stop duration in the train station. The load button will load the current shows train configuration into the left side simulation part. The green button will start the train and the red button is the emergency stop button.

1.4.3 PLC memory/Coils control section:

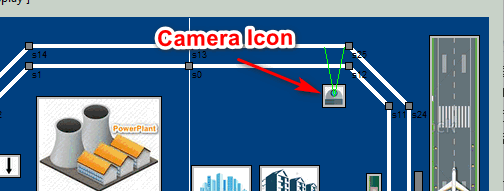
This section will show the input signal to PLC memory register and the changeable register to output coils control /state of the 3 PLCs.

1.4.4 Cyber Security attack simulation control section:

This section will simulate the 3 kinds of attack to the simulation system: ransomware to the main system control part, Trojan attack to the PLC control part and Black energy attack to the whole system. The attack indicator and progress bar under the attack category will show the current attack status.

1.4.5 Surveillance camera simulation section

The surveillance camera simulation is a pop-up window which used to simulate the time when a train pass through a camera. Press the camera icon (As shown below) in the Railway system display section, the window will popup at the bottom of the screen.



1.4.5 System display section

This section will show the simulation of the hardware’s action by animation. The icon of the components will change to grey colour if their power is turn off. It can also simulate the train running on difference direction, the sensors detecting trains pass and the emergency situation of the system during the cyber-attack. (such as two train crash with each other)

1.4.6 PLC Ladder diagram overwrite control section

This section will used to simulate the user change the register value in the three PLCs’ diagram directly. 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.

**2 Program Setup and Configuration**

**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 rail way 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**

**3.1 Wonderware HMI Execution**

Plug in the wanderware USB licence key into your computer, double click the “InTouch Viewer”, the 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

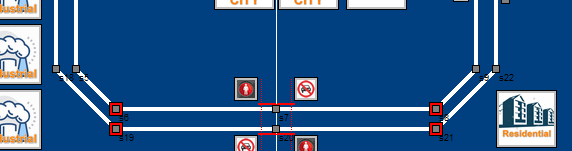
Check the “Ransomware in the HMI” checkbox int the attack control section, then press the “Start attack” button. The HMI main system control section all the checkbox and buttons will be froze during the attack and when you click the main other part of the HMI the Ransomware attack message box will pop up as shown below:



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

3.3.2 Man in the middle attack

Check the “Ransomware in the HMI” checkbox int 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 set the Train position sensor before and after the barrier will be block and the attack will insert the fake position feed back data to the system which cause the accident 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)



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

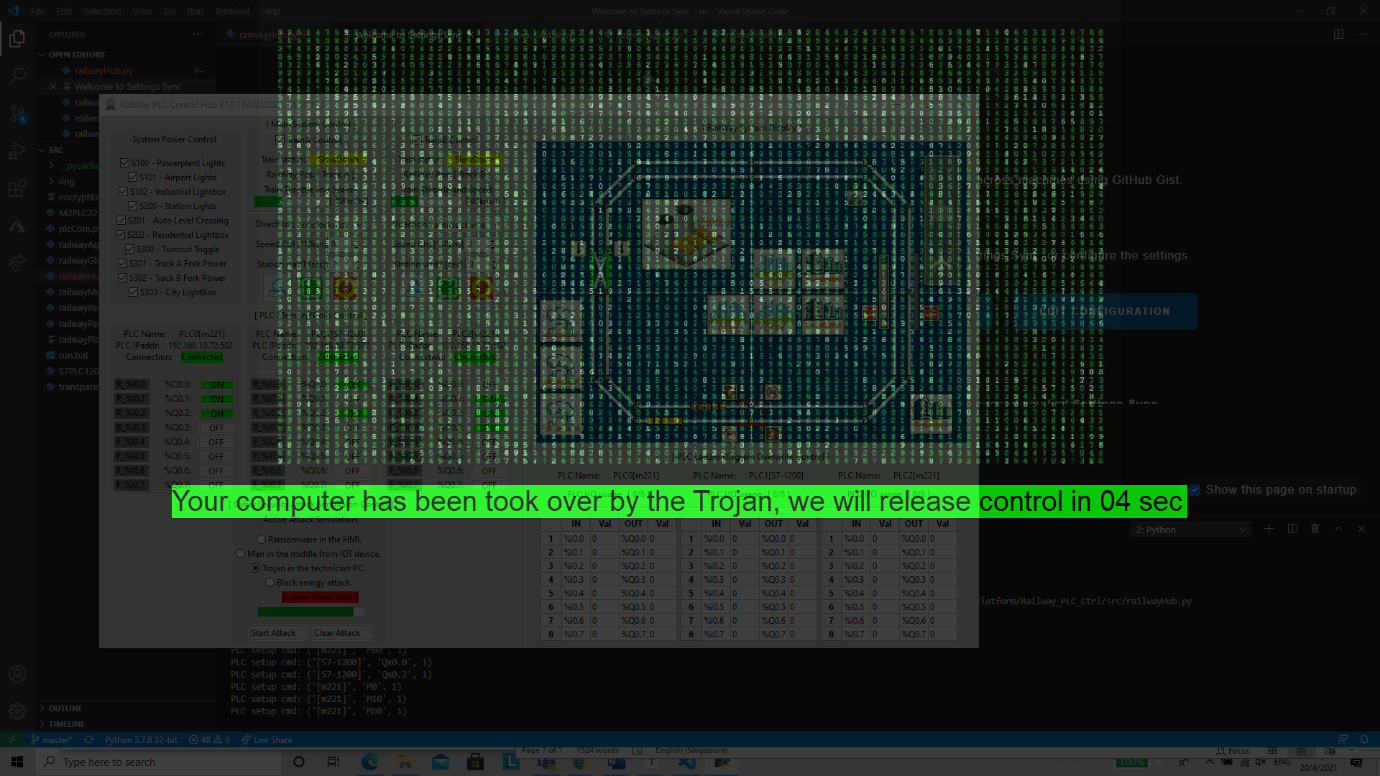
3.3.3Black Out attack:

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 functioning: the user can still press the button/checkbox, but the display section will not change base on the user’s action. After 20second the 2 train fork will setup to cross and the train crash accident will happen on the fork section.

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

3.3.4 Trojan in the technical PC.

Check the “4 Trojan in the technical PC” checkbox int the attack control section, then press the “Start attack button”. During the attack, whole PC will be freezing and the attack screen will show to block the normal desktop of the PC. (As shown below)



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

**4.Reference**

**N.A**

End (last edited 20/04/2021