

CSI OT 3D Platform Cyber Attack Demonstration PLC Control

Project Introduction 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 PLC Project Introduction Manual**

**1. Project Introduction**

This project will implement an HMI for the OT-3D-City simulator platform and power management simulator platform (generator and substation). Then we will demonstrate different kinds of cyber-attack situation on both simulator platform. The project contains four main sections:

**1.1 OT-City Simulator HMI Program**

In this section we will create a SCADA HMI system with Schneider Wonderware(R) program running on the SCADA PC for the user to control the OT-3D-city simulator modules for the training and research purpose. The system control function is implemented by changing the output coils’ status of 3 PLC (Schneider M221 X2 + Siemens S7-1200 PLC X1).

Detail reference doc:

* “CSI OT 3D Platform Cyber Attack PLC Setup.pdf”
* “CSI OT 3D Platform Cyber Attack HMI design.pdf”

**1.2 OT Platform Cyber Attack Simulation**

In this section we will demonstrate 3 different kinds of cyber-attack situation on the OT-platform and power management module: False data injection attack, Blackout attack and the Stealthy situation attack. The attack demonstration will be activated by the attack control website and launched from an attack control device (Raspberry PI) which connected to the system network. The influence of different attack situation will be introduced in the section “Cyber-attack implementation”.

Detail reference doc:

* “CSI OT 3D Platform Cyber Attack Introduction.pdf”

**1.3 OT-Cyber-Attack Control Website**

In this section, we will create a website server running on the “orchestrator PC” to provide a web interface to let the user control different cyber-attack demos on OT-platform and show current system feedback/attack detail information during the presentation. The user will active/stop the attack demo via the attack control webpage.

Detail reference doc:

* CSI OT 3D Platform Cyber Attack Web Design.pdf
* CSI OT 3D Platform Cyber Attack User Manual.pdf

**1.4 OT-Cyber-Attack Power Generator and Substation Manager**

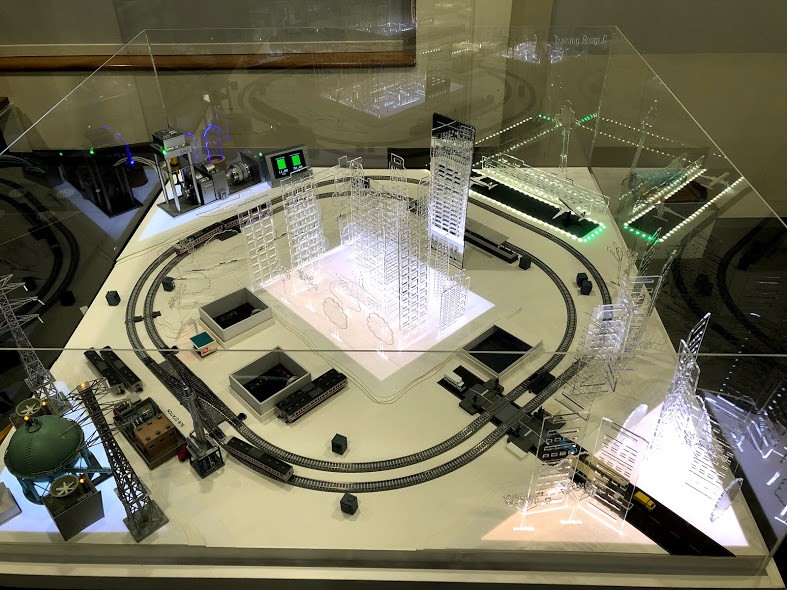
We will provide a user interface running on the “SCADA PC” to remote control the OT-Power Generator Module. We will provide a module controller made by one Raspberry PI and an Arduino to receive the control request from the remove controller UI and change the state of the hardware components of Power Generator Module such as Pump, Motor, and LED display panel. The control program will also automatically update and adjust the generator's motor and pump speed based on the loads in the system.

* “CSI OT 3D Platform Cyber Attack Generator and Substation Deisgn.pdf”

**2. Hardware Introduction**

OT 3D Platform contents 2 main sections, the platform module which simulate a city system with different function area (City Area, Industry Area and Residential Area), traffic system (expressway, railway and airport) and power generation and power grids system (Power generator and substation).

**2.1 Section 1: CSI OT 3D Platform Top View:**

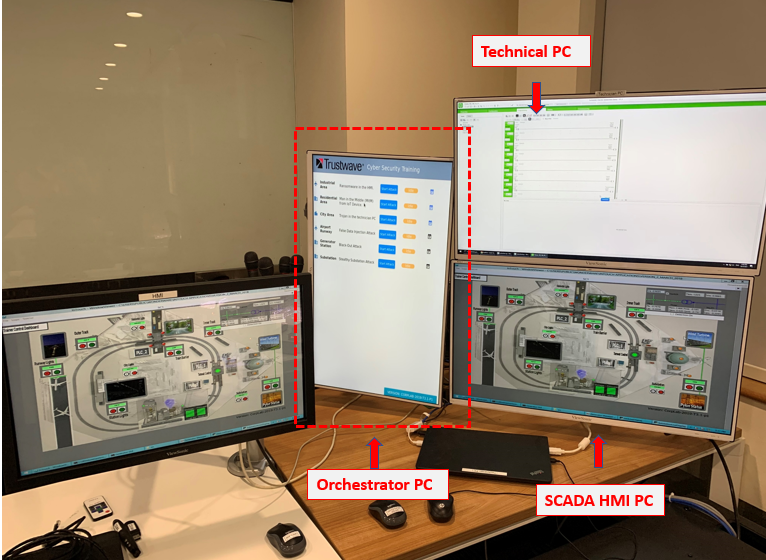
****

<Figure\_2.1.1 CSI OT Demo platform view >

****

<Figure\_2.1.2 Server rack and network switches view>

**2.2 Section 2: Computers for User to Control the OT 3D Platform:**



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

**2.3 Hardware list and functionality**

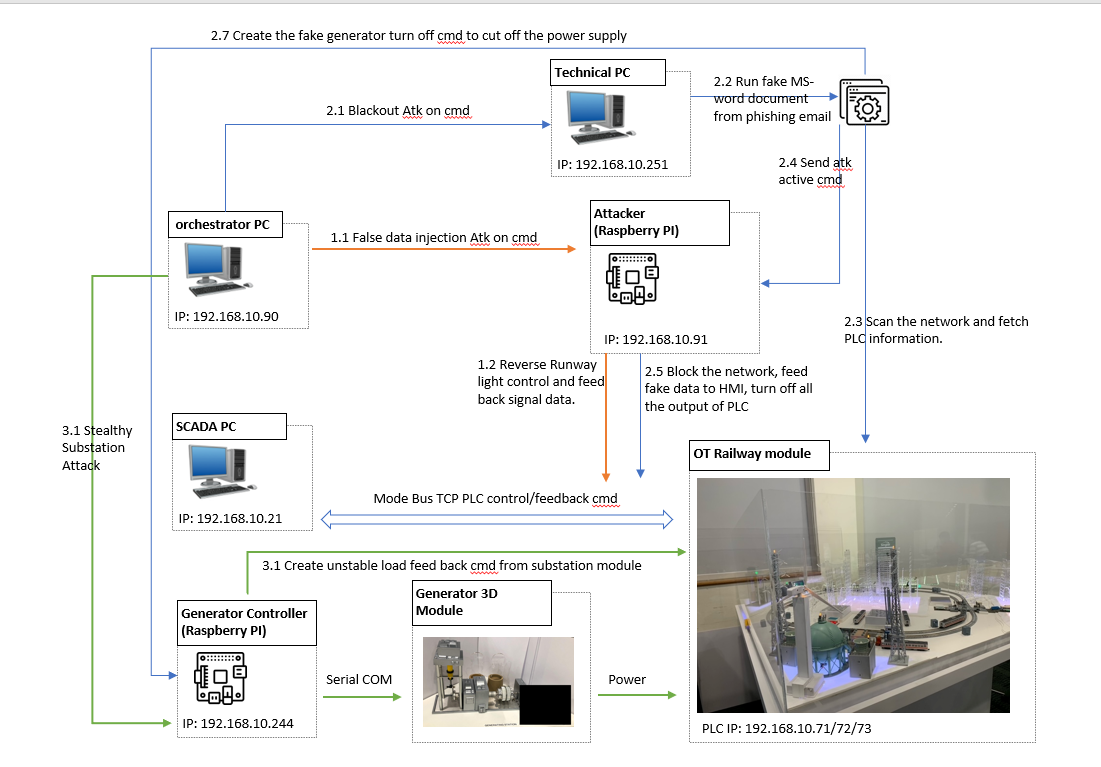
|  |  |  |  |
| --- | --- | --- | --- |
| Idx | Name | Components | Function |
| 0 | OT 3D Platform | OT 3D Platform  M221 PLC X 2  S7-1200 PLC X 1  Control Arduino #1 | Main OT-City simulator platform. |
| 1 | SCADA PC | Dell server #2  Monitor 3  Touch screen | Show the HMI for user to control and show the presentation. |
| 2 | Technical PC | ThinkPad laptop  Monitor 2 | Edit the PLC ladder diagram and show the Back out attack presentation. |
| 3 | Orchestrator PC | Dell server #3  Monitor 1 | Host the attack control website and for user to launch/stop the attack. |
| 4 | Attack Raspberry PI | Control Raspberry PI #1 | Implement the attack at the background. |
| 5 | Power Generator Control Raspberry PI | Power generator platform  Control Raspberry PI #2  Control Arduino #2 | Control the power generator module. |
| 6 | Network switch | Network switch X2 | Config the network. |

For OT-3D platform, the Arduino is controlled by PLC by using the jumper wire.

For Power Generator, the Arduino is controlled by Raspberry PI by USB serial communication.

**2.4 Network Configuration Introduction**

Control Flow Diagram and hardware IP configuration of the System:



<Figure\_2.4 System Control Flow Diagram >

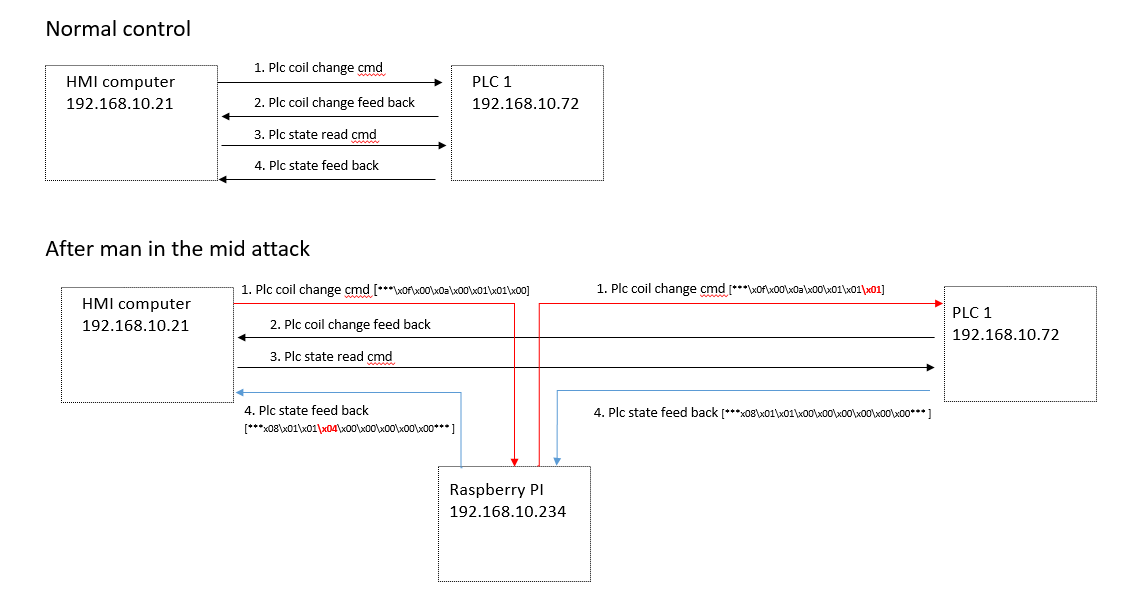
**3. Introduction of Three Attack Situation**

**3.1 False Data Injection Attack**:

In research related to OT security, it is established that careful falsification of measurement or field data can result in erratic control actions without the knowledge of the operator. Such attacks in general are known as False Data Injection (FDI) attacks. These attacks are studied extensively in the context of OT security, mainly in Smart grid security. A conceptual demonstration of this attack is done on the OT platform. In this attack, we assume an additional foreign hardware (IoT/Raspberry Pi) was plugged in to the OT network. This attack will manipulate the SCADA command and feedback; causes the SCADA HMI to show the opposite feedback on the actual system.

This demo will attack on airport light 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 turn off. During the attacking phase, the attacker program running on the foreign hardware uses the “Ettercap” script to perform man-in-the-middle attacks on the Modbus TCP traffic between the PLC and HMI computer. The detail message capture and replacement are shown below.

False data injection attack data flow diagram.

****

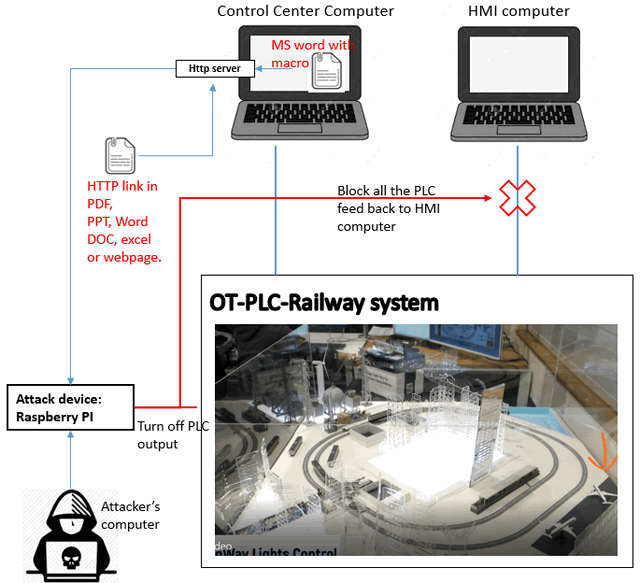
<Figure3.2 False data injection data flow diagram>

**3.2 Blackout Attack**:

Blackouts are one of the worst situations, not only for a power utility but also 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 malfunction of a critical circuit breaker can cause a blackout. The malfunctioning 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.

These attacks happen when systems are not properly air-gapped, whereby the malware is entering to the system via spear phishing email. When the attack launched, all the PLC output coils (energy output) will forced to turn off. During attacking, we will simulate the user opens a malicious word document download from the phishing email, then the macro built in the document will scan the network, then trigger the attack script running the foreign hardware to use the “Ettercap” script to block all the Modbus TCP communication between the HMI and all the PLCs. At the same time, the foreign hardware will send the PLC Modbus control command to turn off all the output coils of the PLCs. The detail message capture and replacement are shown below.

Black out attack control flow diagram



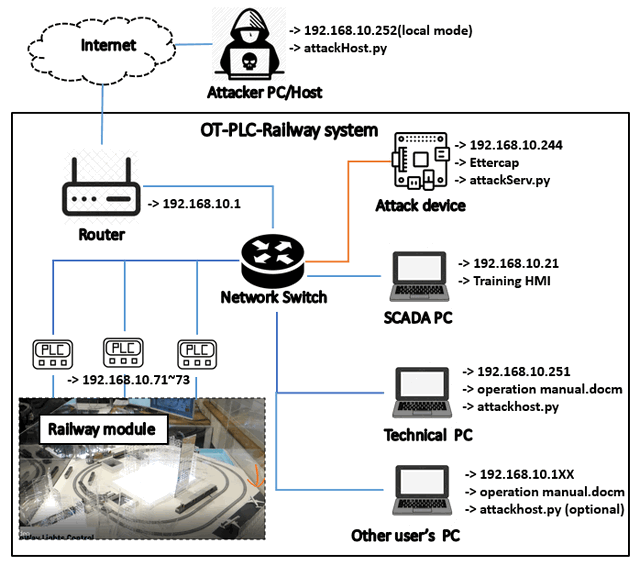
<Figure3.2 Blackout attack control and data flow diagram>

**3.3 Stealthy Attacks In a Smart Grid**:

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 centre (a computer system) and the human operator. Such stealthy attacks were crafted to introduce a set of malicious commands that are referred 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 supply stability 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 equipment. 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.

During the attack, the attack device will send the fake Modbus TCP control message to PLCs to flick the PLC output, then confused the generator’s power auto control function. During the generator power supply doing the auto adjustment, the attack device will also send control command directly to the generator control raspberry PI to change the status of the generator and substation to destroy the tap changing transformers, finally, cause the blackout.

Stealthy Substation Attack Implement Diagram:



<Figure3. Stealthy Attacks In a Smart Grid control and data flow diagram>

- Raspberry PI Mode 3 B+ with Ettercap installed and IP set (First time setup a new Raspberry PI):

$ ifconfig eth0 192.168.10.244 netmask 255.255.255.0 up

**4. Program/Demo Setup**

**4.1 Additional Lib/Software Need**

snap7 + python-snap7 (required for S71200 PLC control)

Install instruction:

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

Ettercap-graphical (need to install on Raspberry PI to do the attack)

$ sudo apt-get update -y

$ sudo apt-get install -y ettercap-graphical

**4.2 Program File list**

| **Program File** | **Execution Env** | **Description** |
| --- | --- | --- |
| attckBlackE3.py | python2.7/python3 | This module will be called from the macro in doc "operation manual.docm" to simulation the blackout attack on the OT-PLC-platform. |
| attackhost.py | python2.7/python3 | This module is used to create a http server on port 8080 to handle the attack get request. |
| attackServ.py | python3 | This module will create a attack service program to run the Ettercap false data injection attack. |
| controlPanel.py | python2.7/python3 | This module will create attack control panel to start and stop the man in the middle attack. |
| M2PLC221.py | python2.7/python3 | This module is used to connect the Schneider M2xx PLC. |
| S7PLC1200.py | python3 | This module is used to connect the siemens s7-1200 PLC |
| m221\_1 filter/m221\_1.ef | C | This filter is used do reverse all the PLC communication command between HMI and the PLC1. (192.168.10.21<=> 192.168.10.72) |
| m221\_3 filter/m221\_2.ef | C | This filter is used to do block all the PLC feedback data to the HMI computer. (192.168.10.21) |
| operation manual.docm | MS word/VBA | MS-Word document with Macro to active the attack. |
| attackWeb/attackHost.py | python3 | flask server to create a attack control web for the people who does the presentation. |

**4.3 Demo step:**

Refer to the user manual doc < CSI OT 3D Platform Cyber Attack User Manual.pdf>

**5. Reference**

S. Chakrabarty and B. Sikdar, "Detection of Hidden Transformer Tap Change Command Attacks in Transmission Networks," in IEEE Transactions on Smart Grid, vol. 11, no. 6, pp. 5161-5173, Nov. 2020.  
doi: 10.1109/TSG.2020.3005238

End (last edited 06/04/2021)