

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.

Power Generator and Substation

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)

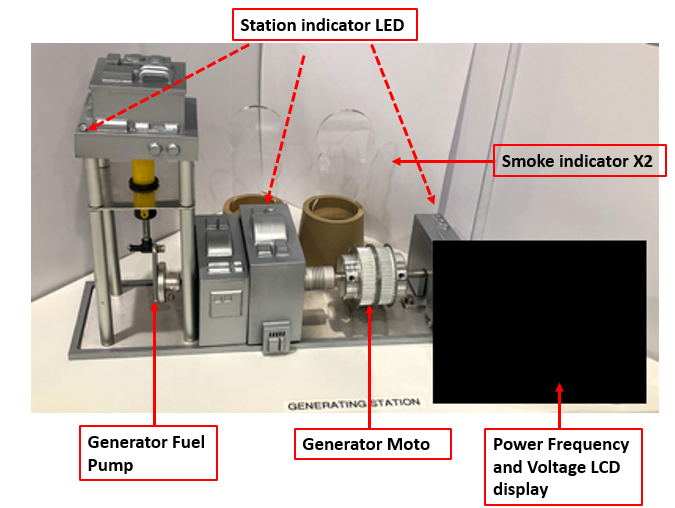
CSI OT 3D Platform Cyber Attack Demonstration

**CSI OT 3D Platform Cyber Attack Demonstration Power Generator and Substation Design Manual**

**1. Project Introduction**

The OT 3D Platform contents a power generator module which use to simulation the power generation for the module’s inner and outer railway, train substation and system’s power supply. The power generator is controlled by an Arduino, then we use the Raspberry PI to connect to the Arduino to control the LEDs, LCD screen, smoke indicator frequency and siren with serial commands. The Arduino also has 4 pins to control the speed of Moto and sensor. The 4 pins are connected to the PLC. For the software part, we have implemented 2 programs: Power generator auto-control program and Remote generator controller.

* 1. **View of the power generator hardware**



1.1.1 Generator Infor LCD Display: Show current generator output frequency and voltage value. I will also show 2 indicators bar to show the load. (Green for normal, yellow for no no-load, red for overload)

1.1.2 Station Indicator LEDs [green/amber/red]: Frequency LED, Voltage LED, Moto LED and Pump LED.

1.1.3 Generator Fuel Pump: A pump with a driving moto and single cylinder moving up and down to show the fuel transfer speed to the generator. (speed selection: stop, slow and fast)

1.1.4 Generator Moto: A rotate wheel with a driving moto to show the moto speed/power output of the generator. (speed selection: stop, slow and fast)

1.1.4 Smoke indicator: Two smoke shape transparency panel with flashing blue LED at the bottom to show the speed generation speed. (slow/fast)

1.1.5 Siren: Play siren sound to show the alter to the user when the generator got exception.

**1.2 Power generator auto-control program**

The power generator auto-control program will be running in the Raspberry PI to control the OT-Power Generator Module's hardware. It will send ModBus TCP command to PLC and serial cmd to Arduino, then receive the control request from the remove controller. The control program will do the adjust of the generator's motor and pump speed based on the loads in the system. The program contents 4 thread to finish the different task parallel:

1.2.1 Main thread: In the main thread, we will read the 3 PLCs load, do the generator frequency and handle the PLC reconnection if any of the PLC was disconnected.

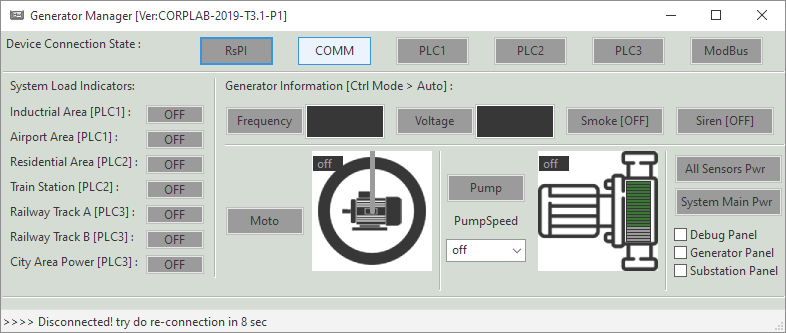
1.2.2 UDP Communication thread: A thread with UDP server to handle the control request from the generator control HMI.

1.2.3 TCO communication thread: A thread with TCP server to response the parameters Modbus message fetching request.

* + 1. Attack handling thread: The thread will active and simulate the attack scenario.

**1.3 Remote generator controller HMI**

This module will provide a UI to connect to the power generator auto control program by UDP and display the generator states. The main UI as shown below:



1.3.1 Device Connection State: Show the control raspberry PI connection (UDP), the connection state between the raspberry PI, PLC and the Modbus message.

**1.4 System data communication**

Components communication diagram:

