**CSI OT 3D Platform Cyber Attack Demonstration Design Document**

Date: 15/12/2020

VERSION: CORPLAB-2019-T3.1-P1

Edited by LiuYuancheng

**Introduction**

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

**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-city simulator modules for the training or 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).

**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 connect to the system network. The influence of different attack situation will be introduced in the section “Cyber attack implementation”.

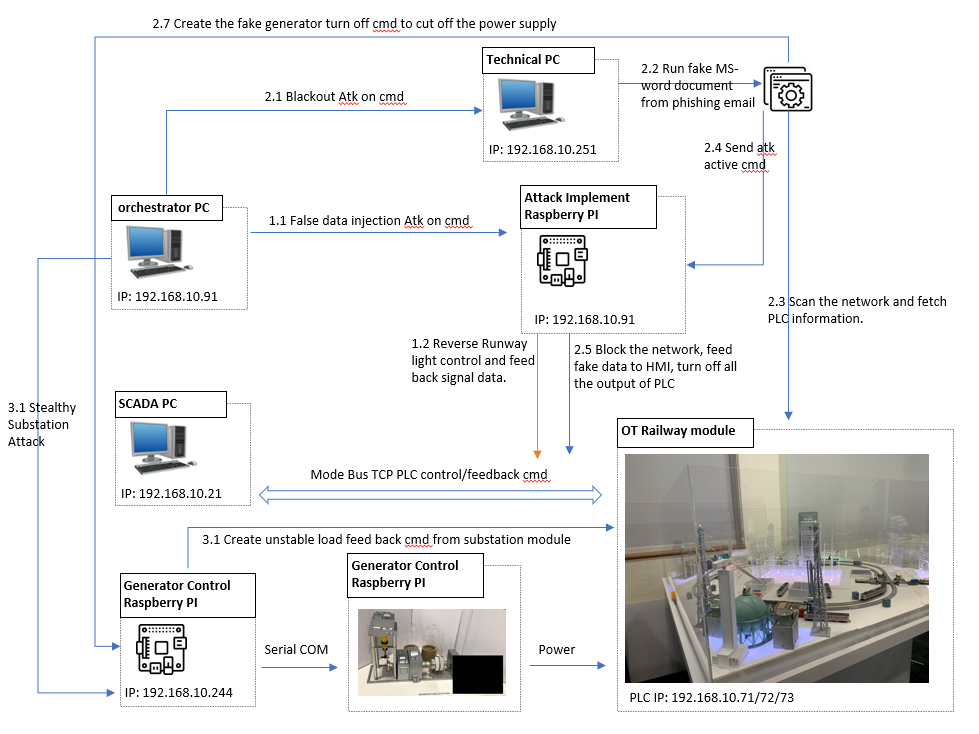
**OT-Cyber-Attack Control Website**

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 by login the attack control webpage.

**Power Generator 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, moto and LED display panel. The control program will also do the automatically adjustment of the generator's motor and pump speed based on the loads in the system.

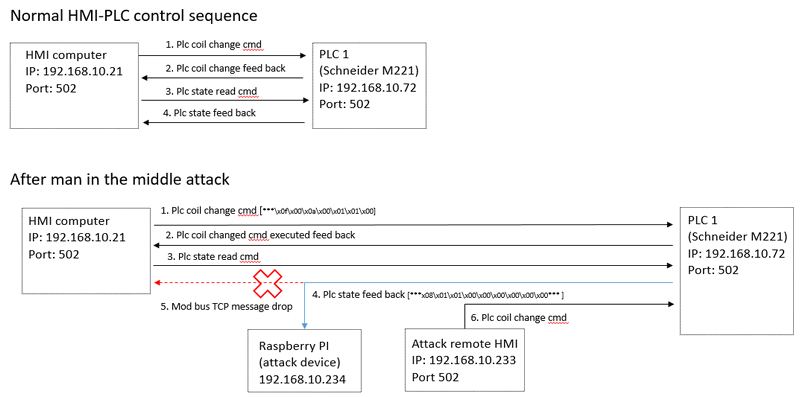
System hardware connection and IP address configuration:



Cyber attack

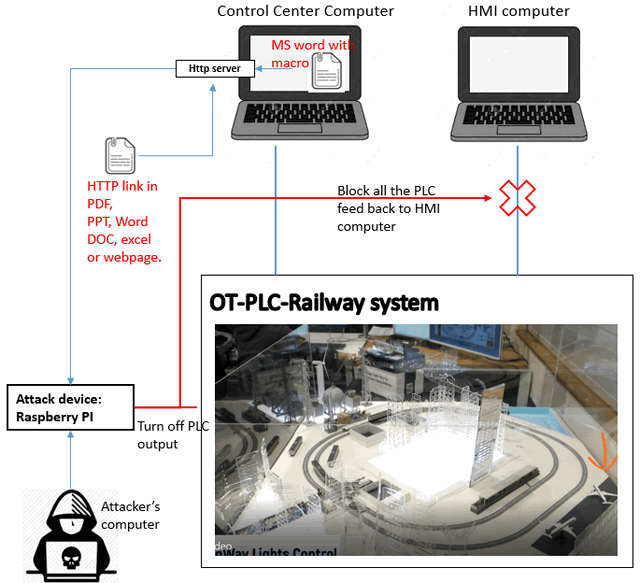
False Data Injection Attack:

In this attack, we assume an additional foreign hardware (IoT/RaspberryPi) was plug in to the OT network. This attack will manipulate the SCADA command and feedback.causes the SCADA HMI 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 theactual system, e.g. When the operator try to turn on the runway lights in the airport via HMI, the actual runway lights will be turn 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, whereby the malware is enter to the system via spear phishing email. When the attack launched, all the PLC output coils (energy output) will forced to turn off.



Stealthy situation attack:

Technically, known as False Command Injection attack.[Attack introduction will follow Shantanu ‘s paper]

Attack Control website:

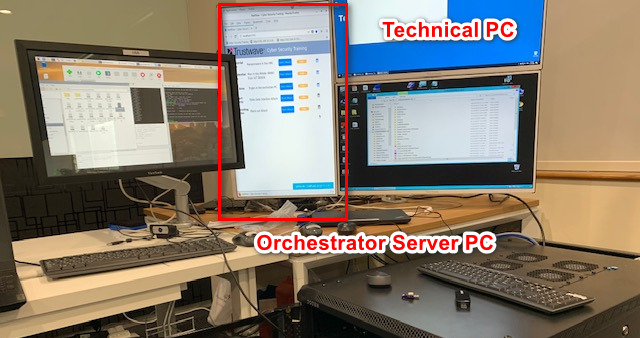
Development Environment: NodeJs(v12.18.4)/JavaScript HTML5

Additional Lib/Software Need : NodeJs(v12.18.4)

Webpage View:



Login the orchestrator PC:



open web browser and type in URL: <http://localhost:8080> or <http://127.0.0.1:8080>.

When the user pressed the “Start” attack button, the web host will send the attack activation command to the related agent. (Communication use the asynchronous UDP)

False Data Injection Attack:

The attack server sends the “Attack active cmd” “Atk:A:2” to the attack device.

Black Out Attack:

The attack server send the Attack active cmd” “Atk:A:1” to the technical PC to open the MS-Word document with macro setup.

The macro start to execute the