**Cyber Attack on OT-PLC-Railway System**

**Introduction**

This project will show the step to demo two kinds of cyber attack situation on the OT-PLC-Railway system.

**False Data Injection Attack**: When the attack happens, the reversed user control commend will be injected into the system and the exception situation is not detectable from the SCADA HMI system. (When the user try to turn on the Runway lights in the airport, all the runway lights will be turn off.)

**Black Out Attack**: This is one attack situation of Black Energy 3 cyber attack. When the attack happens, all the PLC output coils (energy output) will be turned off. The system HMI center energy may detect the exception situation but the user cannot recover to normal situation by using the SCADA PC. (The SCADA HMI shows everything normal when the user tries to do recover action but actually all the related PLC output will still keep turned off state)

**Attack Demo**

Step 1 Hardware check

* 1. Make sure the OT platform’s power has been turned on and all 3 PLC works normally.
  2. Make sure the technical PC and the HMI are working normally.

1.3 Make sure the attack device (Raspberry PI) is also powered up.