Cross Sword 2023
NCL Railway IT-OT System Cyber Security Test Platform

Attack Demo [IT-System attack and OT-System attack]

National Cybersecurity R&D Laboratory

Funded under National Cybersecurity R&D (NCRD) Programme since Nov 2015

By NCL Development Team

10 Oct 2023

Cross Sword 2023 NCL Railway IT-OT System Attack Demo

National Cybersecurity R&D Laboratory

Attack Introduction

The cyber attack demo to the Railway IT-OT system contents two parts: IT-System attack and OT-System attack. The demo will show how a hacker can launch cyber attack on the ICS OT system via a successful IT-network attack and how the IT-System attack can make influence of the OT-system.

Railway-IT-System Attack

The IT-System attack will show two attack scenarios on the railway company's cooperate(IT) network:

- **Scenario 1: Servers remote compromised attack**
  This attack shows how an attacker gains the company's internal node/server's remote access via security information leakage.
- **Scenario 2: Backdoor trojan attack**
  This attack shows how a hacker uses phishing email, fake software update installer to bypass the company's firewall to penetrate the internal network from internet, then use the trojan to steal security information, insert and run the malware in the company's protected ICS network.

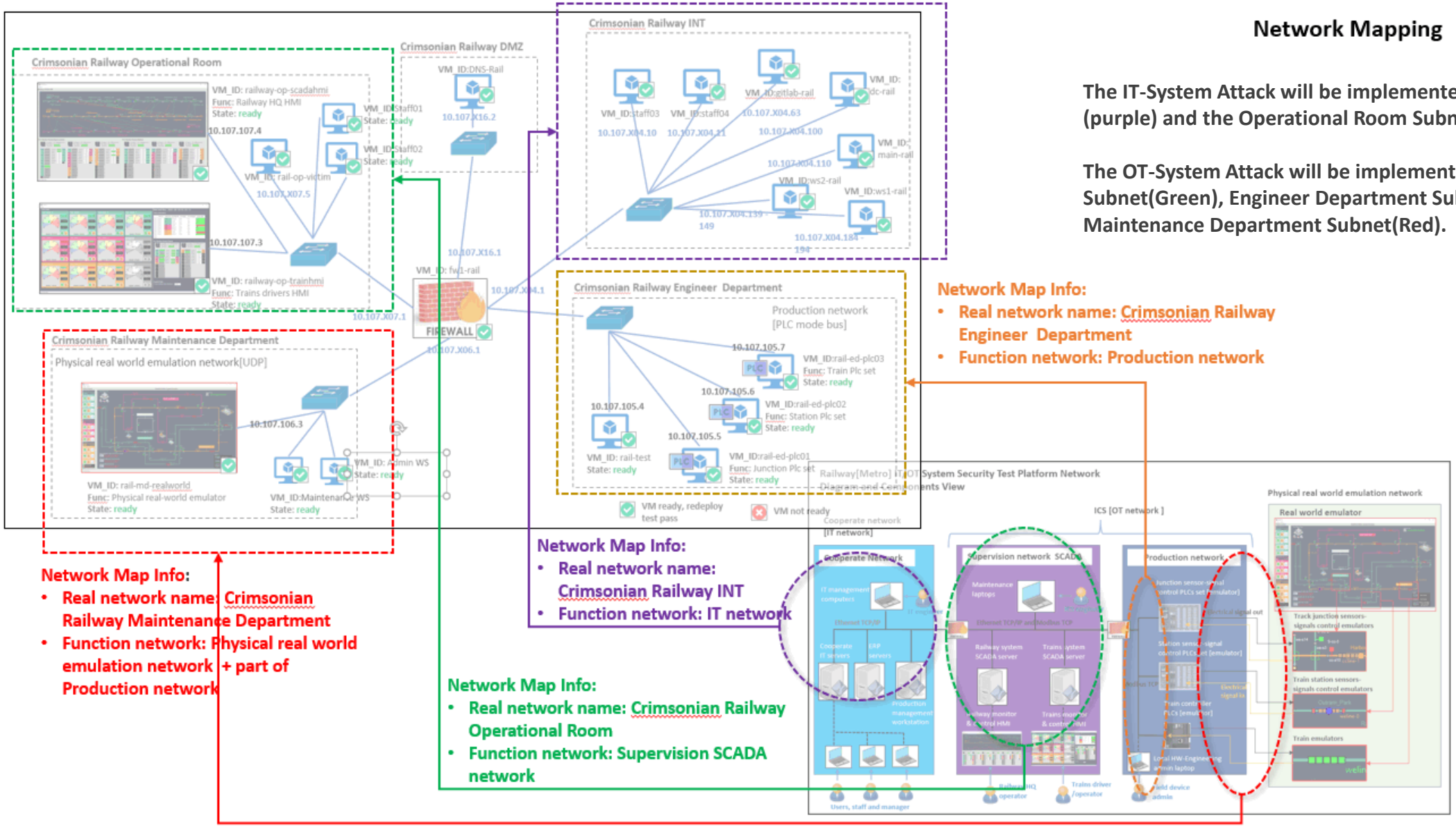
Railway-OT-System Attack

The OT-System attack will show how the hacker can attack the OT-System after he has successfully implemented the IT-System attack. The attack contents three scenarios:

- **Scenario 1: malware ARP attack**
  This attack will show how hacker uses ARP attack tool "Ettercap" to do MiTM traffic block attack.
- **Scenario 2: False data/command injection attack**
  This attack will show how hacker uses customized malware to inject illegal command or false data to PLC to make trains collision accident happen**.**
- **Scenario 3: DDoS on Modbus channel attack**
  This attack will show how hacker uses the customized DDoS attack program to jam the HMI-PLC communication channel.

National Cybersecurity R&D Laboratory

Railway IT-OT System Network Topology View



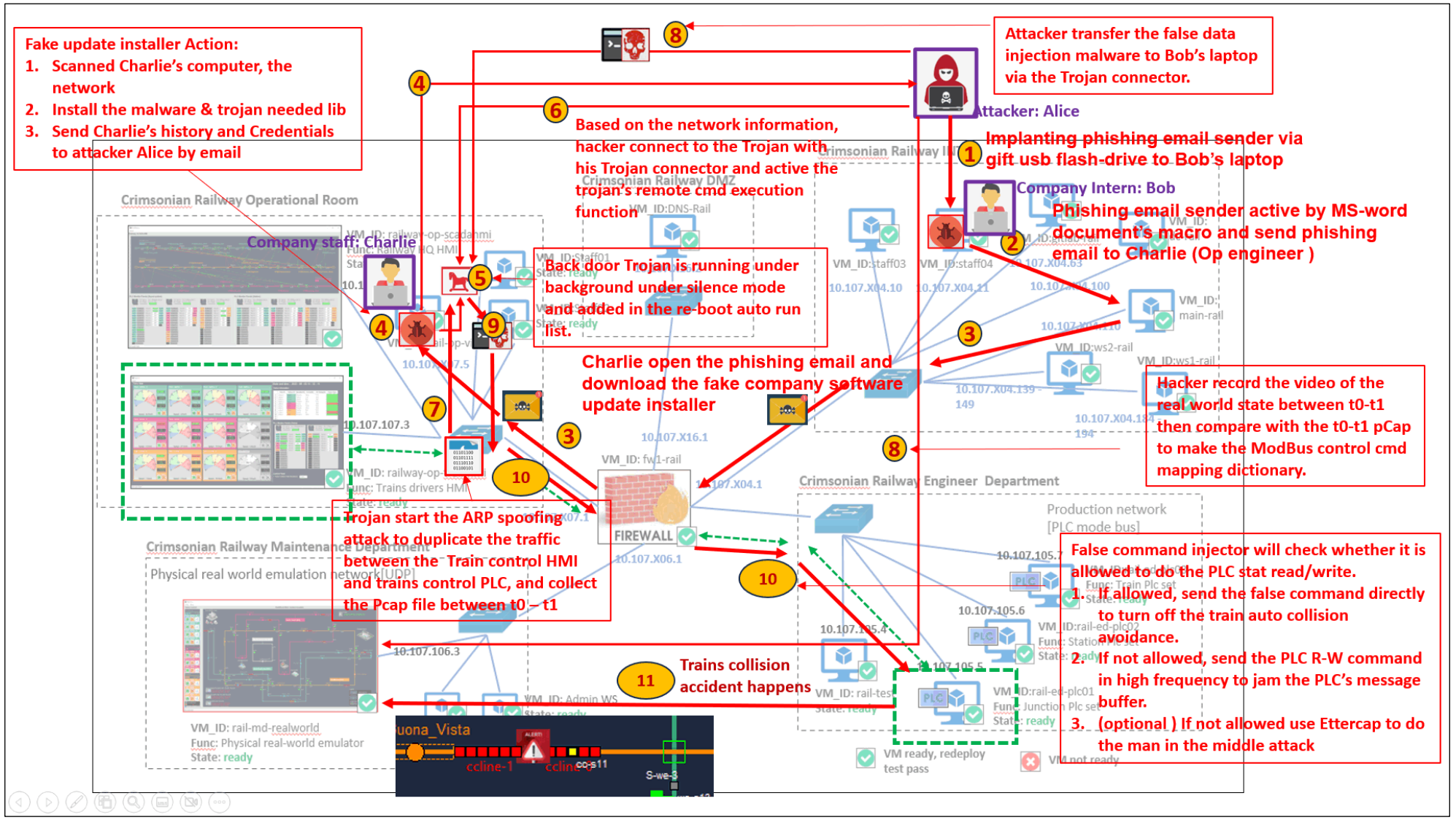
Network Mapping

The IT-System Attack will be implemented on INT subnet (purple) and the Operational Room Subnet (Green).

The OT-System Attack will be implemented on Operation Room Subnet(Green), Engineer Department Subnet(Orange) and Maintenance Department Subnet(Red).

National Cybersecurity R&D Laboratory

IT-System Attack Playbook Example:



Detail attack demo refer to the : IT-System attack instructor manual.

ARP Spoofing Attack (Packet drop) [Attack Scenario Introduction]

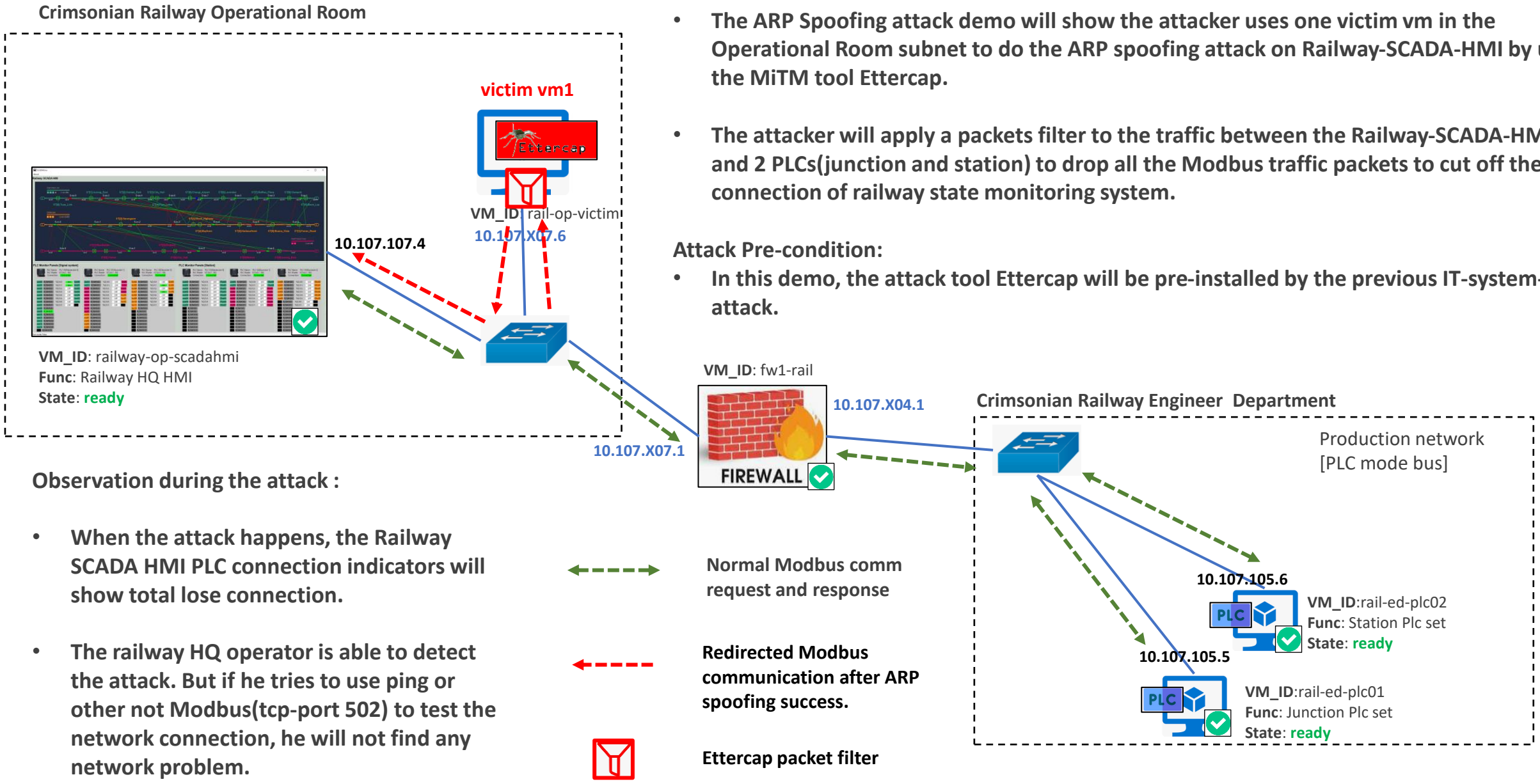
National Cybersecurity R&D Laboratory

OT-Attack Scenario:

- The ARP Spoofing attack demo will show the attacker uses one victim vm in the Operational Room subnet to do the ARP spoofing attack on Railway-SCADA-HMI by using the MiTM tool Ettercap.
- The attacker will apply a packets filter to the traffic between the Railway-SCADA-HMI and 2 PLCs(junction and station) to drop all the Modbus traffic packets to cut off the connection of railway state monitoring system.

Attack Pre-condition:

- In this demo, the attack tool Ettercap will be pre-installed by the previous IT-system-attack.



Observation during the attack :

- When the attack happens, the Railway SCADA HMI PLC connection indicators will show total lose connection.
- The railway HQ operator is able to detect the attack. But if he tries to use ping or other not Modbus(tcp-port 502) to test the network connection, he will not find any network problem.

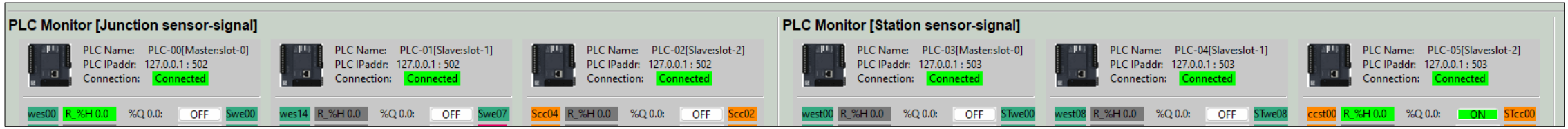
National Cybersecurity R&D Laboratory

ARP Spoofing Attack Observation

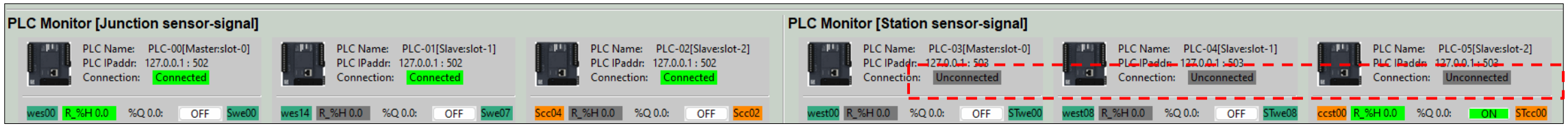
When the attack happens, the railway HQ operator may observe below situation :

- **All the data on the railway-SCADA-HMI will not update.**
- **The PLC connection indicators on railway-SCADA-HMI will show lose connection (change from green color to gray color).**

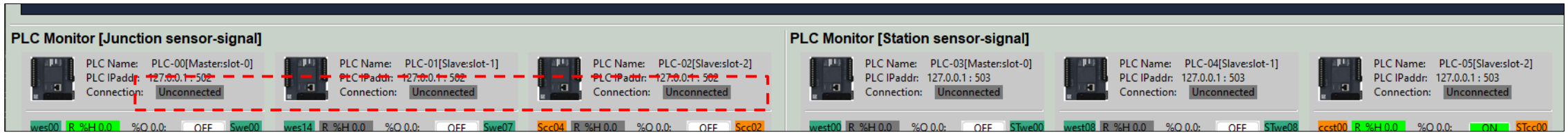
Normal states :



Attack happens (start to drop all outgoing PLC Modbus request):

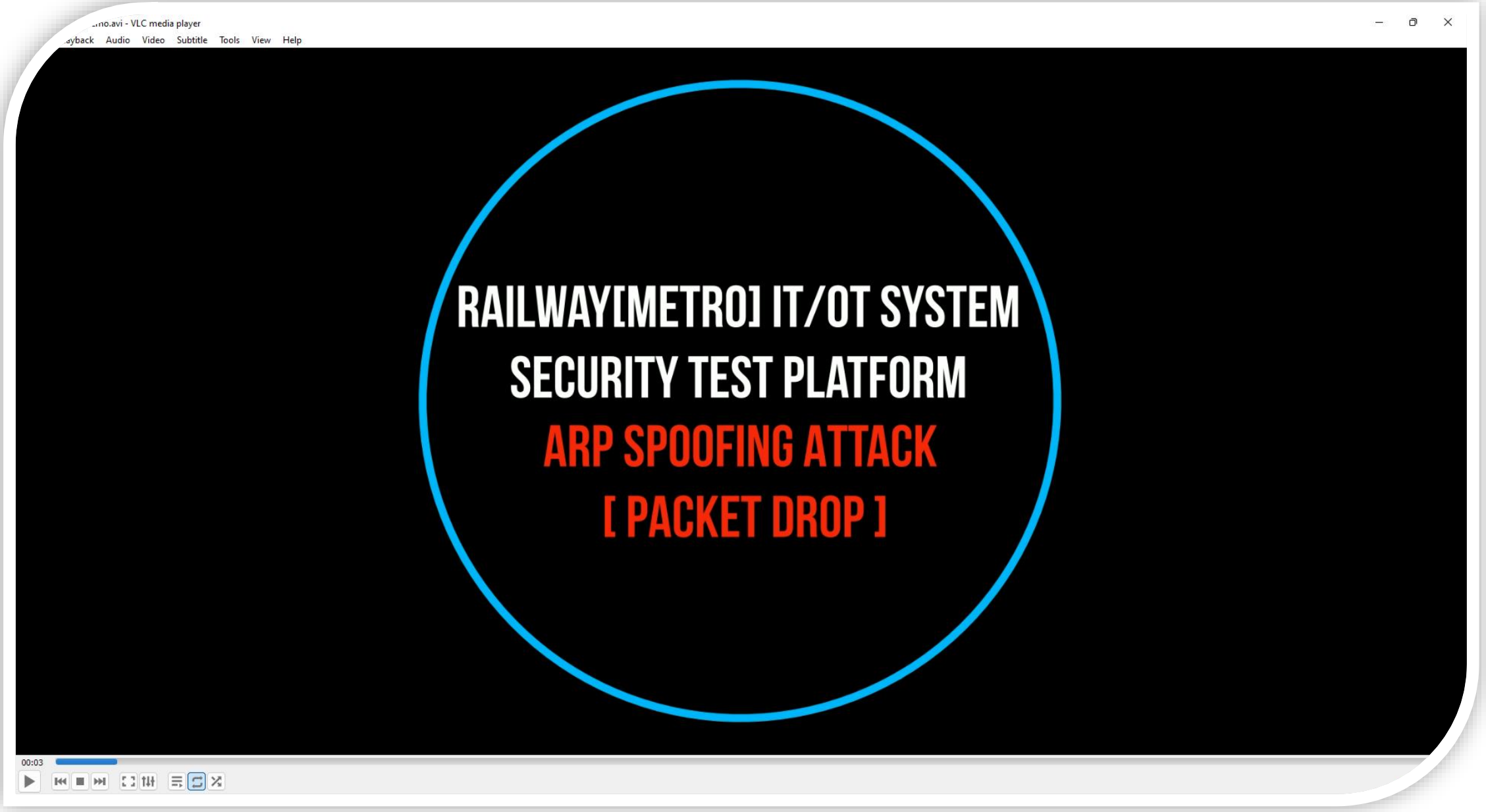


Attack happens (start to drop all incoming PLC Modbus response):



ARP Spoofing Attack[Demo Video]

National Cybersecurity R&D Laboratory



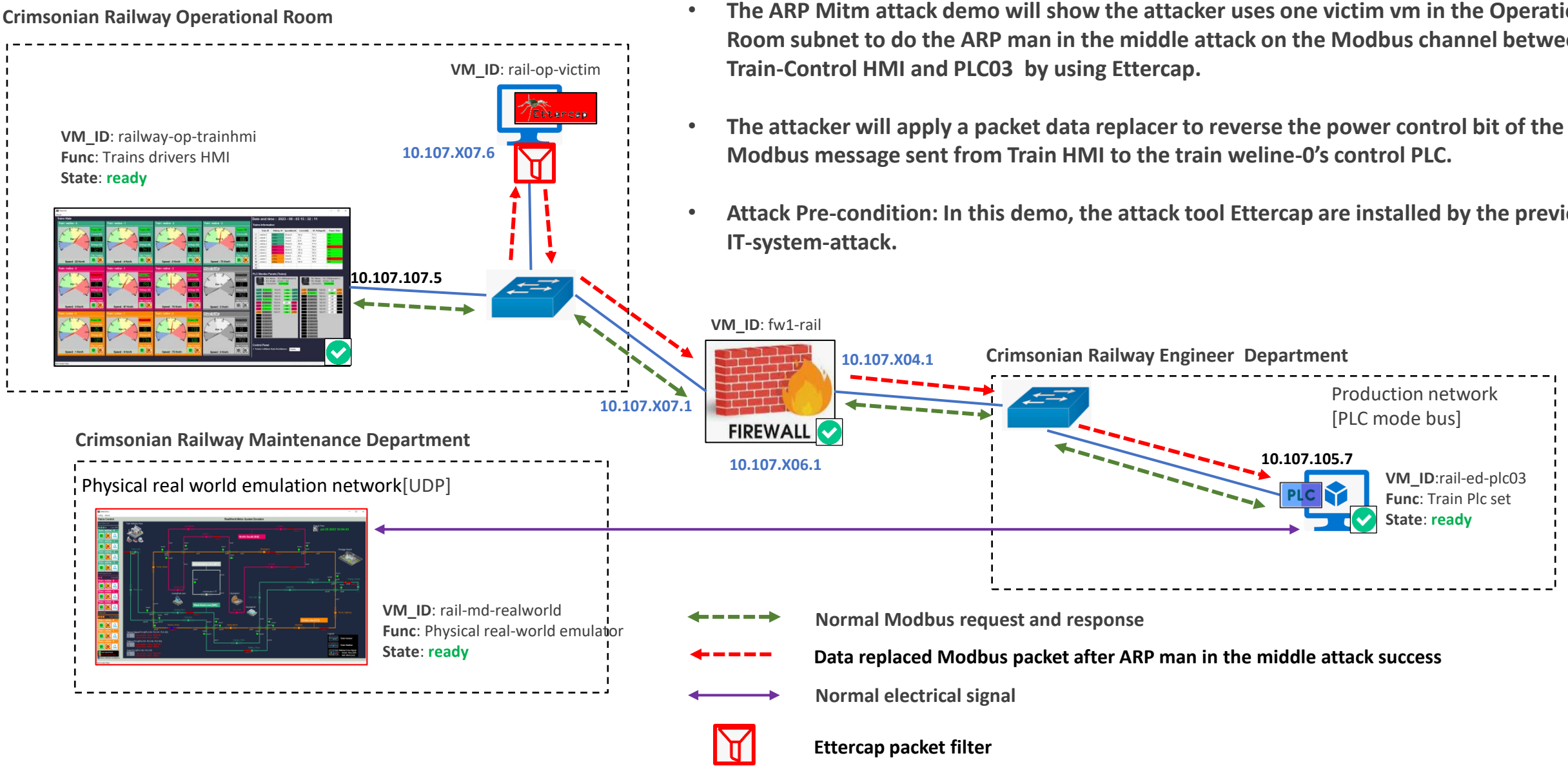
Online Video link: https://www.youtube.com/watch?v=QmB0nJU1_q4

ARP Mitm Attack Demo (Signal reverse) [Attack Scenario Introduction]

National Cybersecurity R&D Laboratory

Attack Scenario:

- The ARP Mitm attack demo will show the attacker uses one victim vm in the Operational Room subnet to do the ARP man in the middle attack on the Modbus channel between Train-Control HMI and PLC03 by using Ettercap.
- The attacker will apply a packet data replacer to reverse the power control bit of the Modbus message sent from Train HMI to the train weline-0's control PLC.
- Attack Pre-condition: In this demo, the attack tool Ettercap are installed by the previous IT-system-attack.



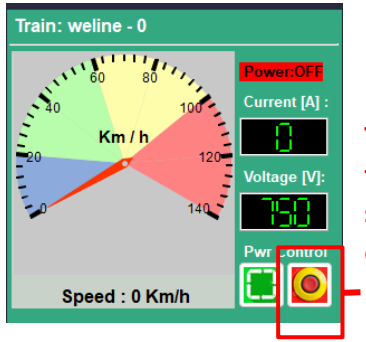
National Cybersecurity R&D Laboratory

ARP Man In The Middle Attack Observation

When the attack happens, the railway train HQ operator will observe below situation :

- **If the train operator press the train weline-0 “power on” button the train’s power will be cut off.**
- **If the train operator press the train weline-0 “power off” button the train’s power will be turn on.**

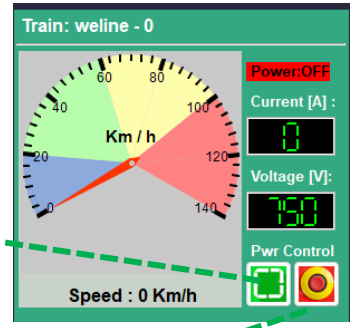
Under Mitm attack (signal reverse):

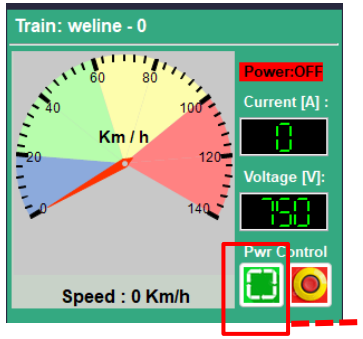


Train operator press the train emergency stop button [power cut off]

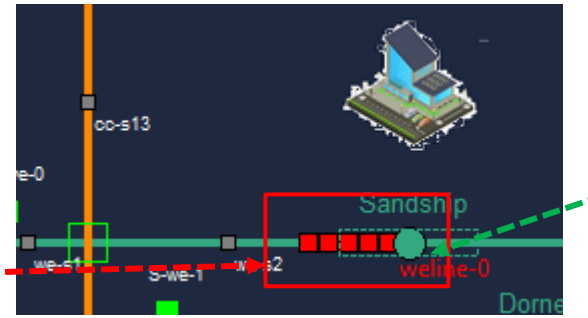
The real train’s power will be turn on

Normal train control :





Train operator press the train reset button [power recover]



The real train’s power will be cut off

Normal HMI control state

Under Mitm attack HMI control state

ARP Mitm Attack demo [Demo Video]

Online Video link: https://www.youtube.com/watch?v=fUC-DeNE_oM

False data Injection Attack [Attack Scenario Introduction]

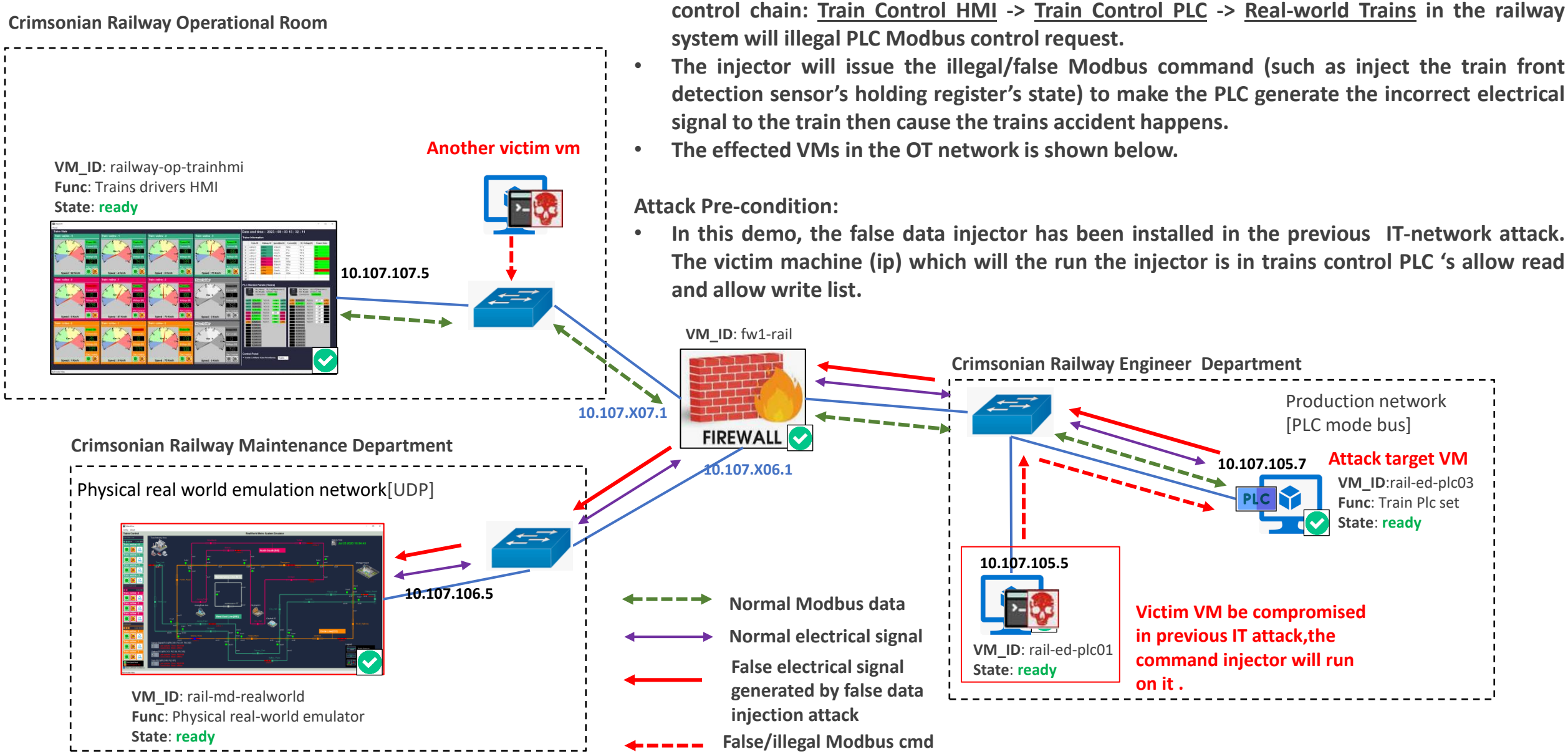
National Cybersecurity R&D Laboratory

OT-Attack Scenario:

- **The attack demo will show a false command injector program to attack the OT-system control chain: Train Control HMI -> Train Control PLC -> Real-world Trains in the railway system will illegal PLC Modbus control request.**
- **The injector will issue the illegal/false Modbus command (such as inject the train front detection sensor's holding register's state) to make the PLC generate the incorrect electrical signal to the train then cause the trains accident happens.**
- **The effected VMs in the OT network is shown below.**

Attack Pre-condition:

- **In this demo, the false data injector has been installed in the previous IT-network attack. The victim machine (ip) which will the run the injector is in trains control PLC 's allow read and allow write list.**



False data Injection Attack [Background Introduction]

Real world train operation introduction

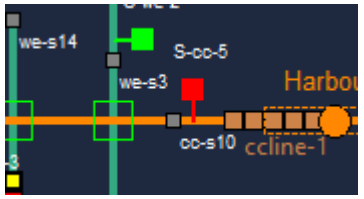
The trains on the real-world emulator will be under one of the below three states :

Normal states :

Normal Operation Scenario 1 (Green) : Train power on , Train speed is normal (56 km/ h – 90 km/ h)

Power: on
Throttle: on
Break: off
Front sensor: no detection
Speed sensor: val

Normal Operation Scenario 2(Orange) : Train power on , Train speed is low (0 km/ h – 20km/h)



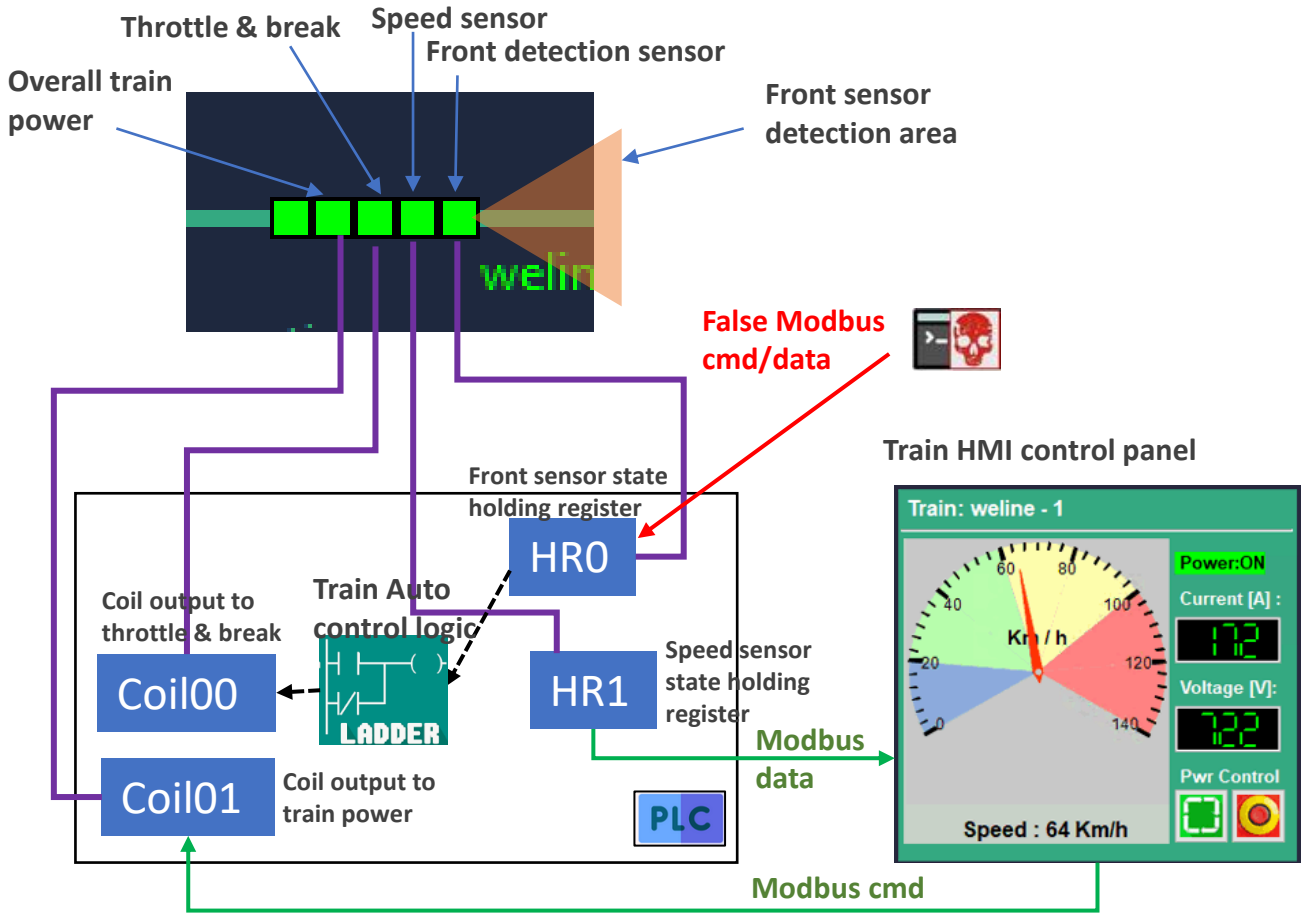
Power: on
Throttle: Neutral
Break: on
Front sensor: detected
Speed sensor: 0

Exception states :

Operation Scenario 1(Red) : Train power off, Train speed is 0 km/ h, Train emergency stopped or accident

Power: off
Throttle: Neutral / On
Break: On/Off
Front sensor: detected / no detection
Speed sensor:0

Train's Senor-Power physical wire connection to PLC and auto control logic



- **In normal state, the front collision detection sensor is not allowed to be changed by any Modbus control cmd from HMI. It can only be set by the train's electrical sensor (such as a radar).**
- **Attack malware will use illegal cmd to overwrite the front collision sensor's state to mess up the train's auto control logic to cause the trains accident.**

False data Injection Attack [Attack detail]

National Cybersecurity R&D Laboratory

Attack (Injection) detail

To make the train collision accident happens below:

The attack malware (injector) need to repeat inject at less 3 commands in two trains PLC under the frequency which higher than trains operator.

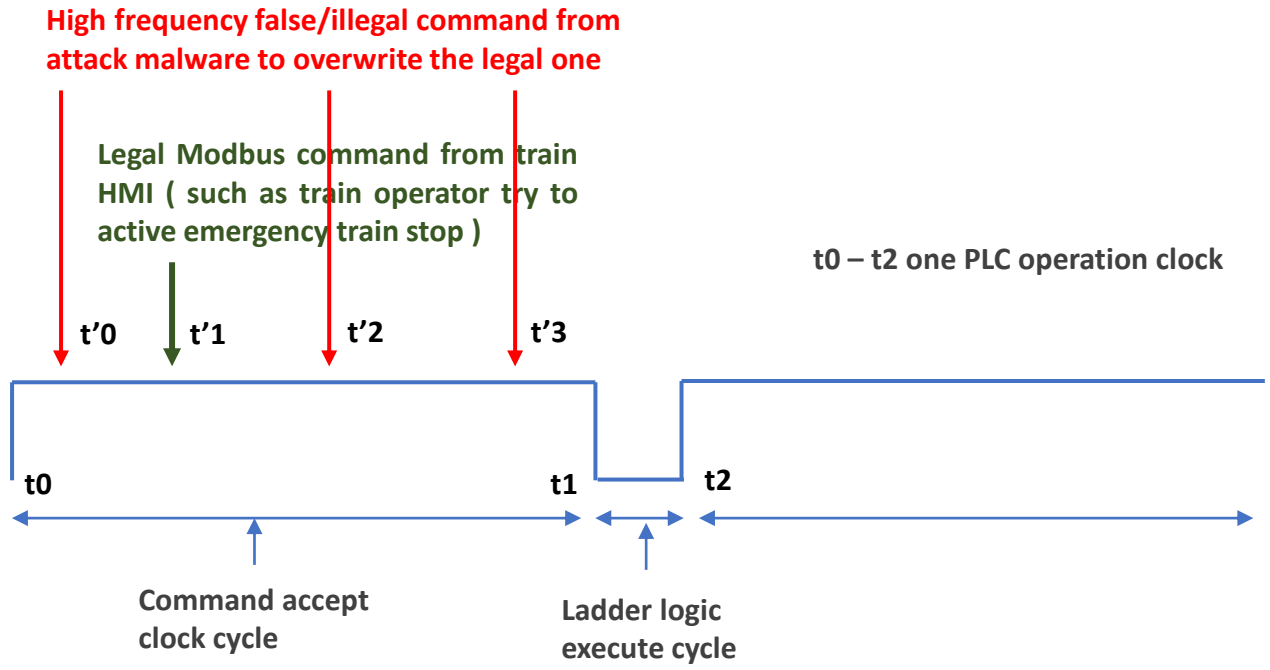
1. Keep sending power cut off command to the front train (ccline-0) to make it stop.

2. Keep send full throttle command to behind train (ccline-1) to make it rush to the front train (ccline-0) .

3. To avoid the behind train (ccline-1) collision detection sensor trigger train break, keep injecting the detection sensor clear cmd (holding register val=0, front safe) to ccline-1 PLC.

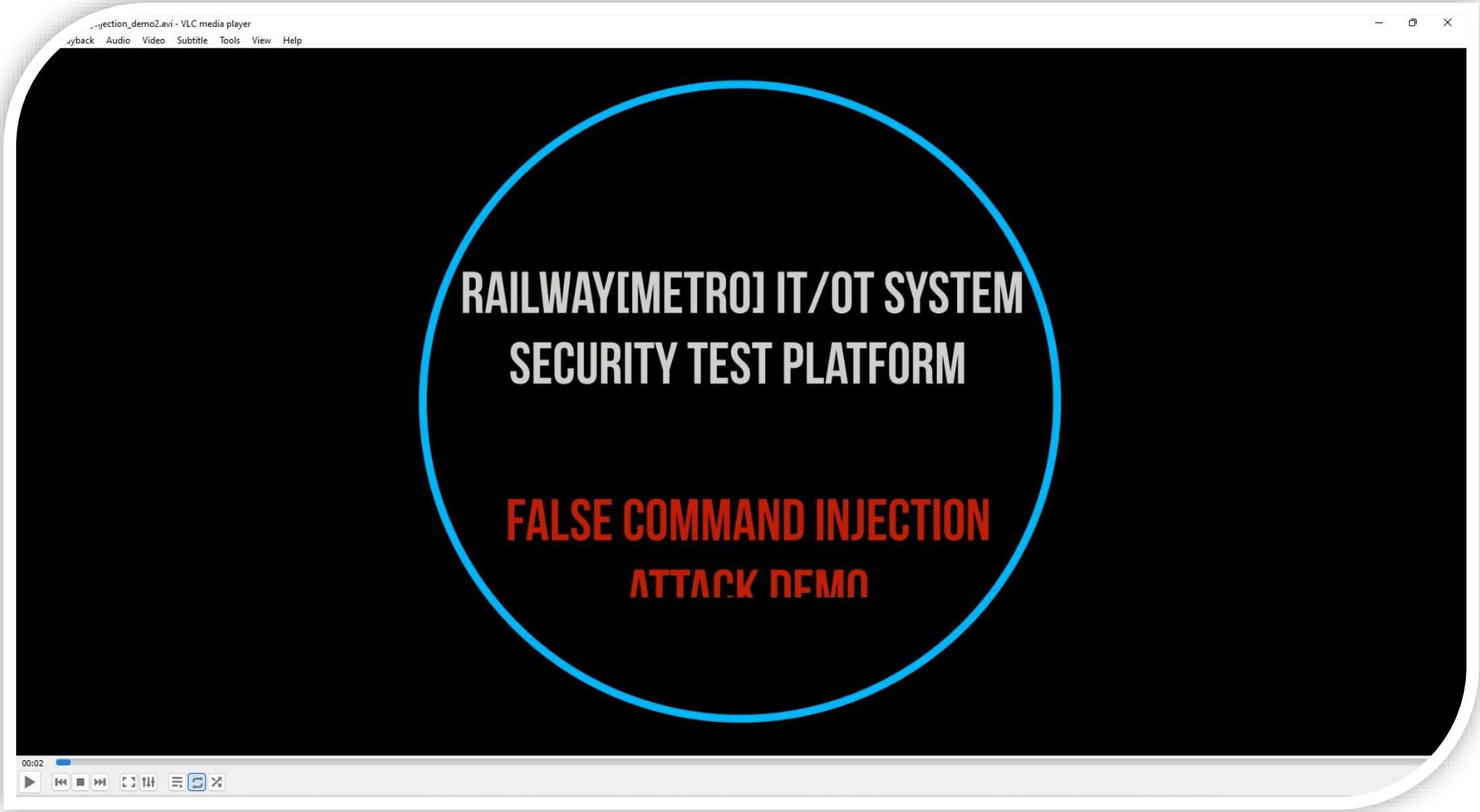
Then the accident will happen, the attack is possible to be detected by train operator if he found the train ccline-1's throttle and speed is unusual.

How the malware to prevent the train operator do emergency stop to save train if he detected the attack/exception state:



- **PLC will accept the command from t0 to t1 and update its memory.**
- **Plc will execute its ladder logic based on the latest memory state at t1. the execute take a very short period t1 - t2.**
- **The attacker will send multiple false cmd in high sequency try to overwrite the train operator's correct control command. Unless the operator can press the train emergency stop button supper fast (which is impossible faster than the malware program), then he will not be able to stop the train accident.**

False data Injection Attack [Demo Video]



Online Video link: https://www.youtube.com/watch?v=J0qpOhigNL8&t=16s

DDoS Attack on PLC in OT-Network [Attack Scenario Introduction]

National Cybersecurity R&D Laboratory

Crimsonian Railway Operational Room

victim vm1

10.107.107.5

VM_ID: railway-op-trainhmi
Func: Trains drivers HMI
State: ready

VM_ID: fw1-rail

10.107.X07.1

FIREWALL

10.107.X06.1

10.107.X04.1

Crimsonian Railway Engineer Department

Production network
[PLC mode bus]

10.107.105.7 Attack target VM

VM_ID:rail-ed-plc03
Func: Train Plc set
State: ready

10.107.105.6

VM_ID:rail-ed-plc02
Func: Station Plc set
State: ready

victim vm3

10.107.105.5

VM_ID:rail-ed-plc01
Func: Junction Plc set
State: ready

victim vm2

Attack Scenario:

- The DDoS attack on PLC will show 3 attacker machines sending high frequency DDoS Modbus request to jam the Modbus channel Train Control HMI -> Train Control PLC (as shown in the below diagram)
- The attack programs will send high frequency Modbus data read/write requests to the PLC to try full filling the PLC's requests buffer queue, so when the HMI sends the control request to PLC, the HMI's request may be dropped or get delay.

Attack Pre-condition:

- In this demo, the DDoS attackers are installed by the previous IT-system-attack. The victim machines which do the DDoS attack are not in the PLC 's R/W white list.

Observation during the attack :

- When the attack happens, the Modbus packet lose rate of any HMI who wants to communicate with the PLC will increase. The HMI PLC connection indicator will show lose connection (change from green color to gray color) if the Modbus request timeout (2s).
- The Train operator is able to detect the attack happens.

Normal Modbus request and response

High frequency DDoS Modbus request

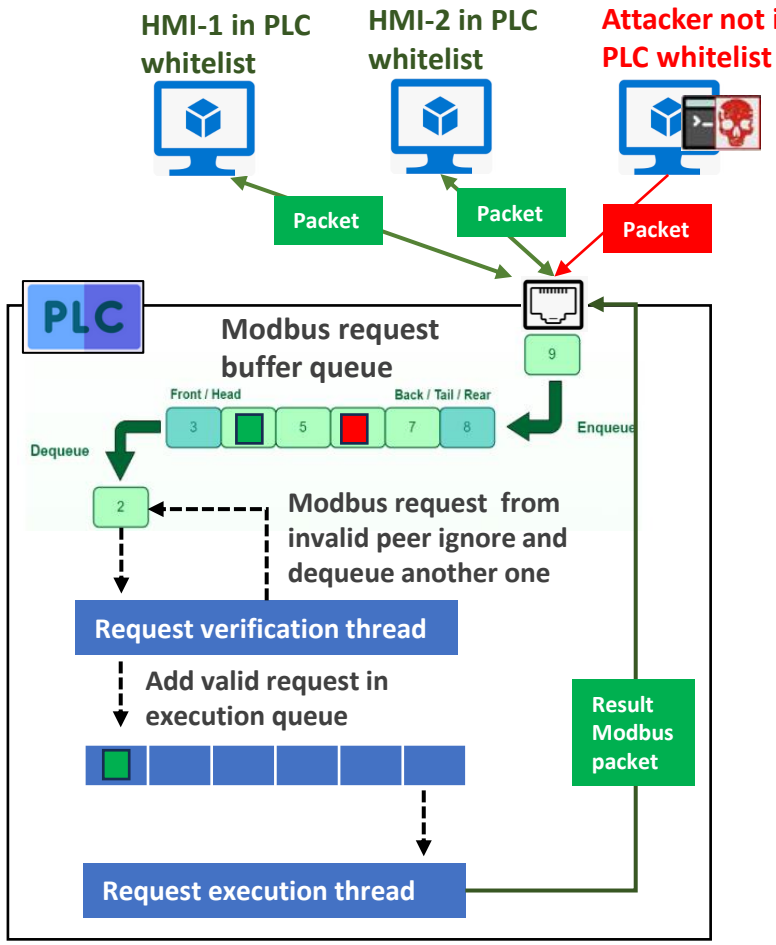
DDoS Attack on PLC in OT-Network[Background Introduction]

National Cybersecurity R&D Laboratory

PLC operation introduction

Each PLC contents 2 IP address whitelist:

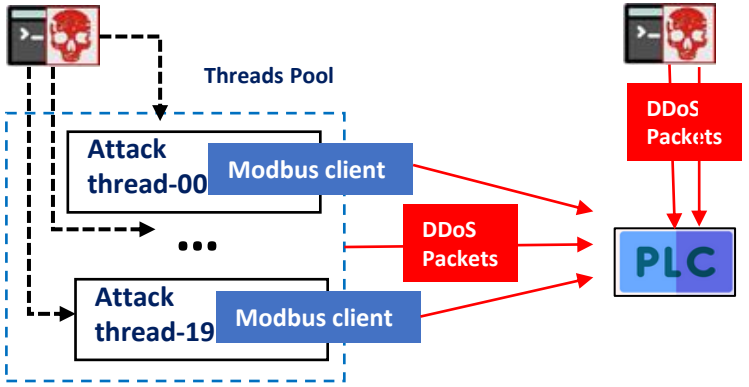
- Allow read list: only Modbus request from IP address in the allow read list is allowed to get information from PLC.
- Allow write list: only Modbus request from IP address in the allow write list is allowed to set PLC state.



Modbus packet from IP not in whitelist will be ignored.

DDoS attacker introduction

Each DDoS attack program will init a threads pool to start 20 attack threads at same time to keep parallel sending Modbus request to the target PLC as fast as it can.



As the PLC requests buffer queue is big and the verification process is also very fast (less than several nano seconds). We need more than one attacker (the more the better) to do the attack to make the attack successful. During the demo, we manually added a small delay in the PLC request verification code to pull down the verification speed ,so we can be easier to observe the attack happens:

```
modbusTcpCom.py
modbusTcpCom.py > plcDataHandler > _checkAllowWrite
131
132     def _checkAllowRead(self, ipaddress):
133         """ Check whether the input IP addres is allowed to read the info."""
134         time.sleep(0.0001) # Improtant: Add a sleep to pull down the verfication speed to make the DDos
135         # attack easier to be observed, during the real event must remote/comment this this line.
136         if (self.allowRipList is None) or (ipaddress in self.allowRipList): return True
137         return False
138
139     def _checkAllowWrite(self, ipaddress):
140         """ Check whether the input IP addres is allowed to write the info."""
141         time.sleep(0.0001) # Improtant: Add a sleep to pull down the verfication speed to make the DDos
142         # attack easier to be observed, during the real event must remote/comment this this line.
143         if (self.allowWipList is None) or (ipaddress in self.allowWipList): return True
144         return False
145
```

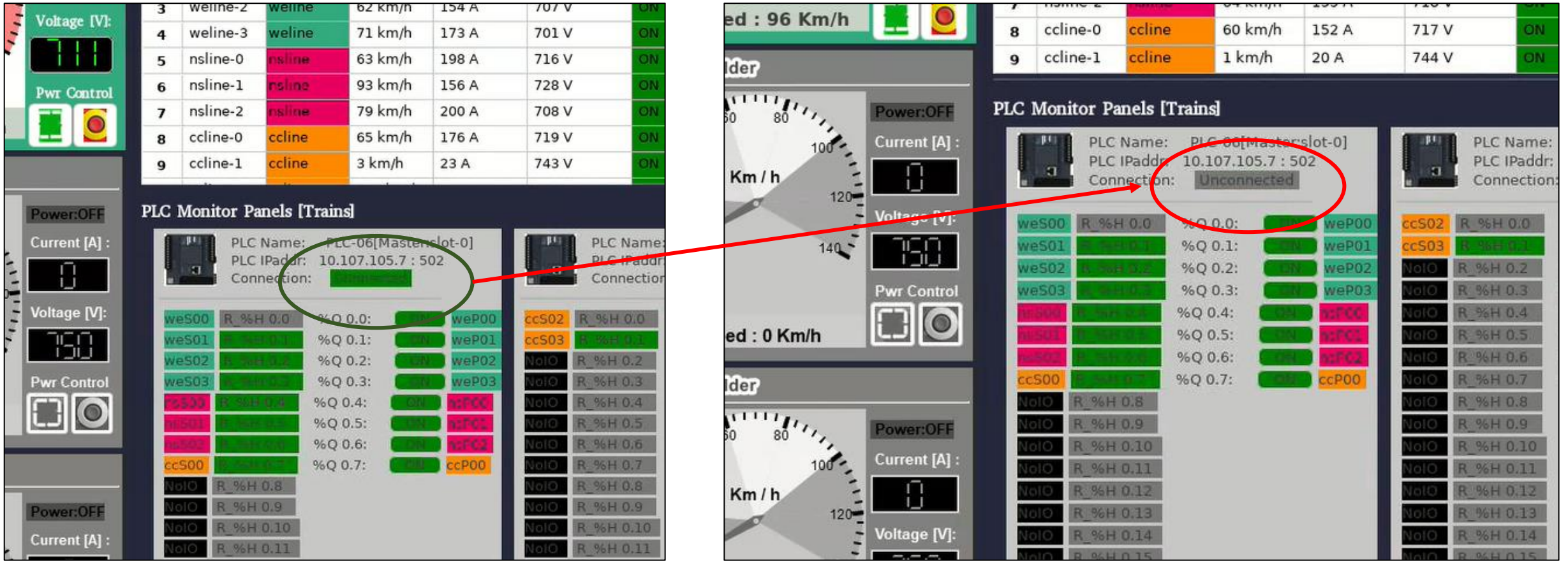
After added the delay, packet lost will be observed when the DDoS packet sending rate reach to about 80k ~ 100K requests / second

DDoS Attack on PLC in OT-Network [Attack Observation]

DDoS Attack Observation

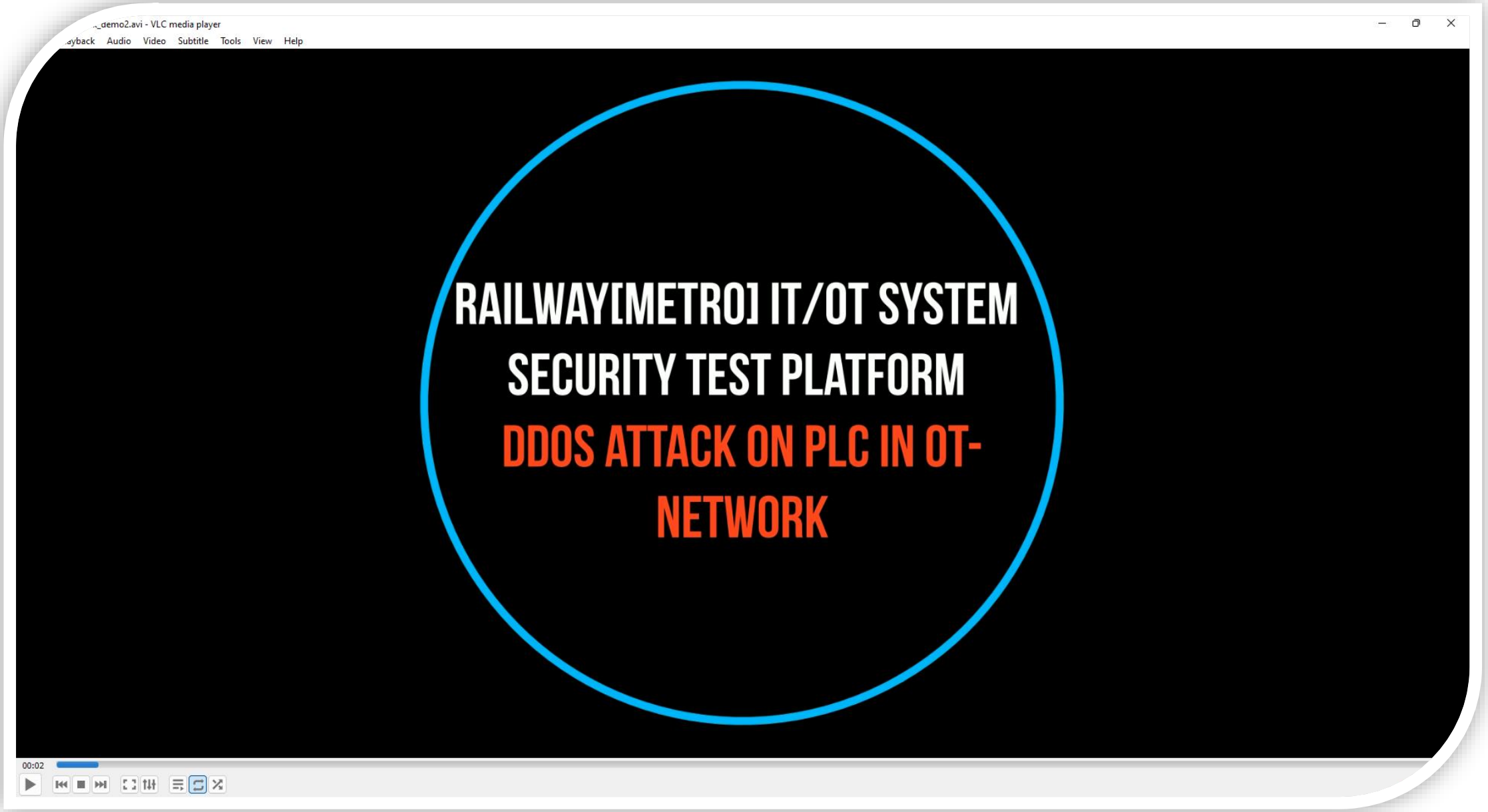
When the attack happens, the trains operator may observe below situation :

- **The PLC connection indicator on the Train-Control-HMI will show lose connection (change from green color to gray color).**
- **The data on the HMI will not update or hang for a short while.**
- **He can not control the train by using the HMI or he will feel lag when control the train.**



DDoS Attack on PLC in OT-Network [Demo Vide]

National Cybersecurity R&D Laboratory



Online Video link: https://www.youtube.com/watch?v=ZG5Y1A3nbKY&t=9s

National Cybersecurity R&D Laboratory

Funded under National Cybersecurity R&D (NCRD) Programme since Nov 2015

Thank you very much

Q & A