Hes·so // VALAIS WALLIS

Haute Ecole d'Ingénierie
Hochschule für Ingenieurwissenschaften

# PV presentation scenarios

**Date :** 24/06/2024
**Houre :** 15h35 → 16h14
**Participants :** M. Clausen et R. Heredero

## 1 Agenda

1. Presentation and choice of attacks scenarios
2. Presentation and choice of Simulation environment

## 2 Meeting

### 2.1 Attacks scenarios

Rémi present some attacks scenarios as it can be seen on the slides. During discussion, it appears that DigiMesh 868 MHz with XBee isn't a good choice because it's a proprietary protocol. Michael suggest to use Zigbee or wireless M-Bus. He'd like that M-Bus is used for this work. Michael also said that Zigbee have a symmetric key encryption capability.

The scenarios that have been choose are:

#### 2.1.1 Wireless Replay attack

More on wireless M-Bus or Zigbee. Sniffing communication for find interresting packets and replay them. Can be secure with encryption like sysmetric key. Still possible to replay packets but not to decrypt them. Best secure option is to sign packets.

#### 2.1.2 DoS by external sensor

Ping of Death is an option. Saturate the communication medium can also be an option.
Rémi prefer to saturate the PLC itself with valid packet. For example an external sensor that send a lot of data. Can be an attack or a bad design (like overloading CPU during an Apollo mission).

#### 2.1.3 Man in the Middle without encryption

Attack on Modbus/TCP. Scenario where no security is implemented. The attacker can intercept and modify packets. Can say anything to the PLC like is a true device. Can be secure with symetric encryption key and exchange with Diffie-Hellman.

#### 2.1.4 Man in the Middle with basic encryption

Idea is to continue previous scenario (Section 2.1.3) but with encryption. But now, the attacker intercept packet since the beginning. He is able to impersonnate and give his own key. For secure against this, we have to use certificates like Modbus over TLS.

## 2.2 Simulation environment

During the meeting, Rémi talk about Factory I/O and Minecraft. Michael also suggest to use Home I/O.

### 2.2.1 Factory I/O

Factory I/O is such more realistic than Minecraft. It's expensive (~4300.-). Some scenes are already implemented and it's possible to create a custom scene. Rémi don't like that Factory I/O can only communicate with modbus over TCP. The simulation doesn't include anything about security. It have to be implemented by a third soft that interface with Factory I/O for add security layer. Rémi test it on Linux and it work quite well with wine

### 2.2.2 Minecraft

Rémi said that it can be interresting for student to continue previous lab on Minecraft. Almost everything is bad in term of security. It can be a good idea to secure the communication on this lab. On Minecraft it also possible to do security with Open Computer or even create a mod.

### 2.2.3 Home I/O

Home I/O is made by the same compagny than Factory I/O. It simulate an House with a lot of domotic devices. It's such cheaper than Factory I/O (~300.-) and can maybe used by ETE students too. Home I/O have to be tested by Rémi.

# 3 Tasks

- Take a look on picoCTF. Maybe integrate some challenges.
- Take a look on wireless M-Bus and Zigbee
- Define a example of simulation environment with :
  - Winter Resort Simulator 2 (least probable)
  - Factory I/O
  - Home I/O
  - Minecraft