# Launching MiTM on ICS

# Introduction & Background

In this chapter we will discuss what industrial control systems are and their use in critical infrastructures. We will look at the statistics of the usage of Modbus TCP protocol whose vulnerabilities can be exploited to launch a MiTM attack on ICS, the high-level architecture of ICS, and Impact on the society if such attacks take place. We will also determine the scope of the project, its timeline, and the goals and objectives we are trying to achieve. Along with that, we will also be giving a brief overview of what tools and technology, and hardware components we will need for this project.

## 1.1 Introduction

Industrial Control Systems (ICS) are used for monitoring and controlling systems such as power grids, water treatment plants, power plants, and oil refineries along with many other systems [1]. For automating Industrial control systems (ICS), Programmable logic controllers (PLCs) and Supervisory Control and Data Acquisition (SCADA) systems can be used along with other components like Human-machine interface (HMIs) and local/remote IOs. Programmable Logic Controllers (PLCs) are small industrial computers that can automate specific processes or entire production lines. They receive information from connected sensors and other input devices, process them, and generate an output based on process logic, and these outputs control actuators. SCADA systems, on the other hand, are the software that can be interfaced with PLCs for reading and presenting the information in graphical or animated form or to make logs [2]. HMIs are interface similar to the SCADA systems but HMIs are local to the machine meaning that they are placed close to a system or near a part of a machine while SCADA systems would be placed in a control room far away from the system. local/remote IOs are IO modules that transfer data to and from PLCs. Devices like sensors and actuators are connected to the IO modules. The input module detects input signals from devices like sensors and the output module controls devices like the actuators [4]. Sensors and actuators can be wired or wireless and the modern industries are moving towards using wireless sensors and actuators. One of the most widely used communication protocol in Industrial Control Systems (ICS) is the open-source Modbus protocol. It is an application layer protocol and one of its variations is the Modbus/TCP which means that the Modbus protocol is used on top of TCP/IP. The TCP/IP port reserved for Modbus is 502. It is a request/reply protocol between a server and a client. As this Modbus TCP/IP is being published as a ('de-facto) automation standard, it is frequently used in PLCs, SCADA systems, and other physical ends such as sensors and actuators. However, the protocol itself does not have any authorization, authentication, or encryption mechanisms [3]. This makes the protocol vulnerable to different types of attacks and by exploiting these vulnerabilities we can perform a Man in the Middle Attack (MiTM) to compromise the integrity or the availability of the Modbus/TCP communication in Industrial control systems. Assume that in a waste-water treatment plant, we have a water tank that gets filled with water through a motor, a sensor is placed at the top of the tank such that when the water reaches a certain level it will send a signal to the Remote IOs input module, which will be processed and sent to the PLC to generate an output which will cause the motor to stop pumping more water into the tank. At this point, the attacker can compromise the integrity of the Modbus/TCP packets such that the motor will continue to pump water and overflow the tank ultimately causing harm to the industry and the society.

By searching on shodan.io, which is a search engine that lets users search using a variety of filters about various servers connected to the internet, we found about 29 searchers which showed us the countries along with the organization where there are servers with Modbus port 502 open. Following are the statistics that were found using shodan.io when we search "Modbus tcp port:502".

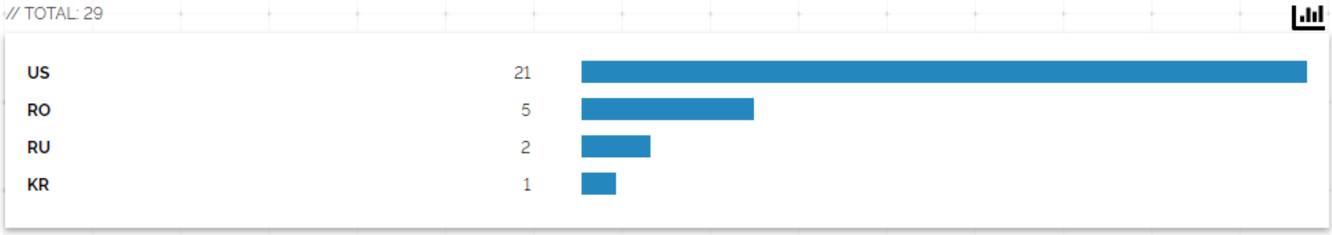

*Figure 1: Countries using Modbus TCP*

Figure 1 shows us the countries and the number of hosts/servers that have the Modbus port 502 open.

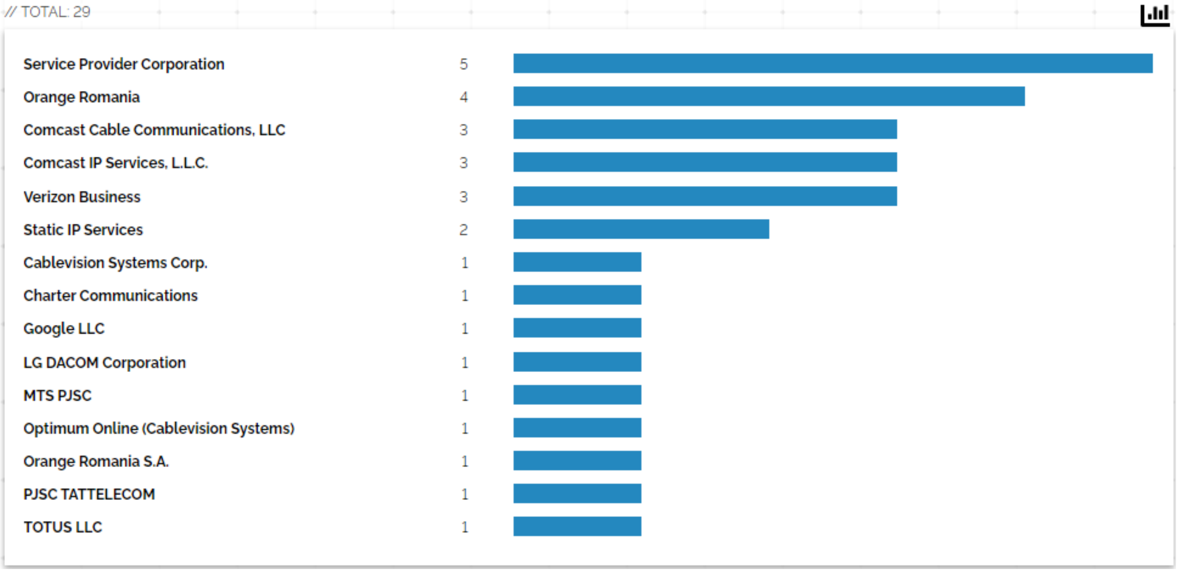

*Figure 2: Top organization using Modbus TCP*

Figure 2 shows top organizations and the number of Modbus TCP hosts in that organization.

**Note: These statistics only show the countries and organizations that use Modbus TCP which are connected to the internet. There may be many more, they are just not connected to the internet. These results are from May 2022.**

## 1.2 Goals and Objectives

The main goals and objectives of the project are:

- Provide a Proof of concept that MiTM attacks can be effectively launched on ICS
- To analyze the security of industrial control systems by compromising the integrity or the availability of the communication between the components in our implemented scenario by performing a Man in the Middle attack.
- To raise awareness among the research community about the automation standard protocol i.e., Modbus/TCP, and its vulnerabilities to identify various attack scenarios and possible solutions for those attacks.
- To raise awareness in the industry about the automation standard protocol i.e., Modbus/TCP, and its vulnerabilities to make the industry understand the consequences of using this protocol.

## 1.3 High-level System Components

A High-level architecture of ICS components is as follows:

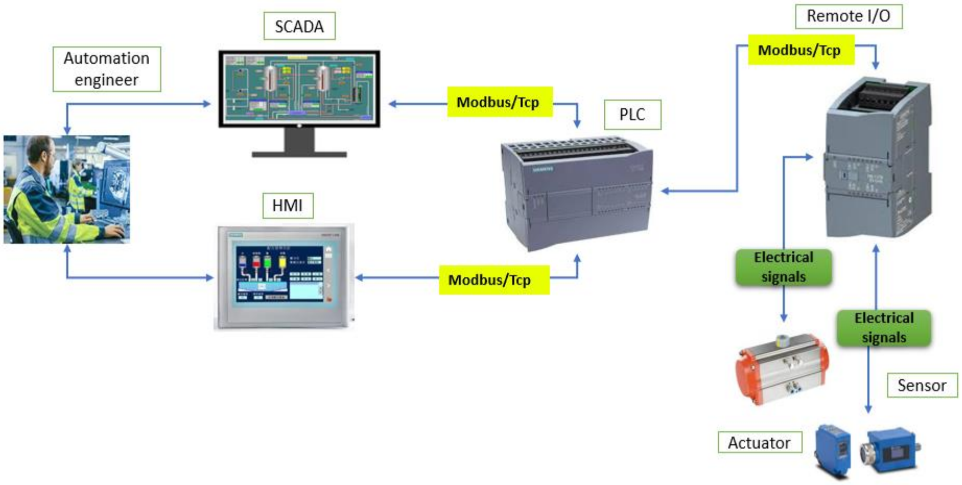

*Figure 3: Normal working - general components*

Figure 3 shows us the normal working of industrial control systems. In this figure, we can observe that the automation engineer interacts with the HMI/SCADA systems that will send/receive data from the PLC via Modbus TCP. Then we have the Remote IO that has PLC connected to one end and sensors and actuators on the other. The input module in the Remote IO will take the signals from the sensor or on/off switches, process it, and send it to PLC in a form understood by the PLC via Modbus TCP. The PLC will execute a program that will take the data it received as input and will generate a corresponding output which will then again be sent to the Remote IO, however this time at the output module. This module will process the output generated and send the corresponding signal to the actuators.

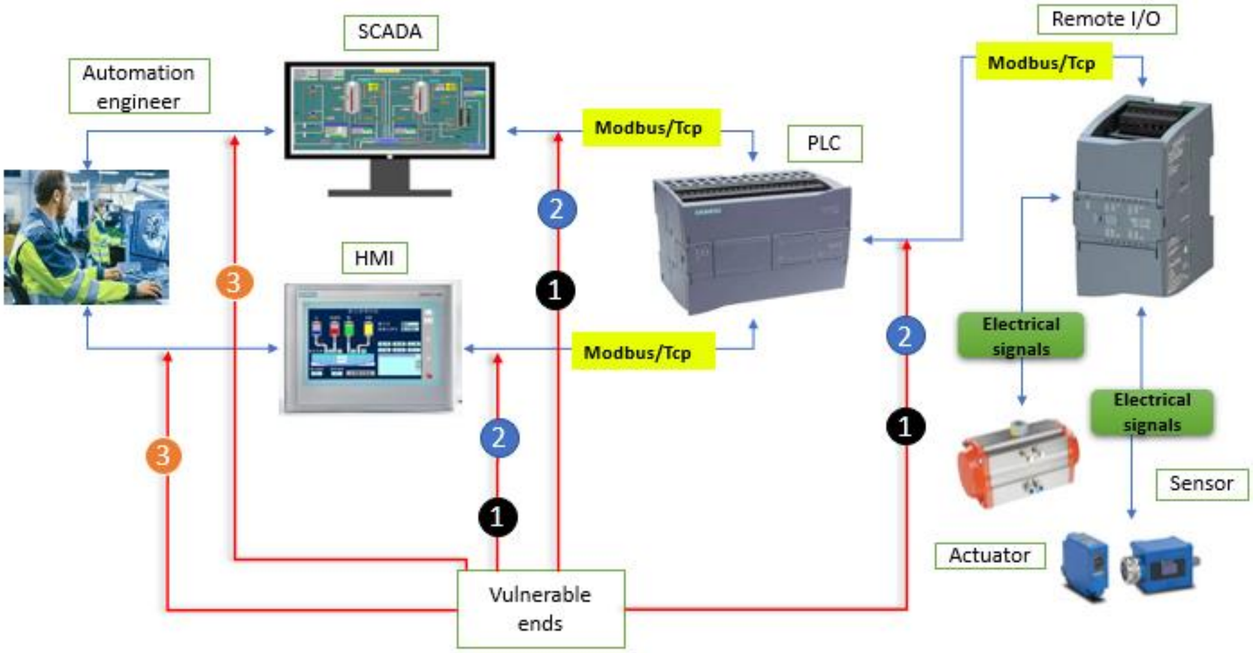

*Figure 4: Vulnerable ends in ICS*

Figure 4 shows us the different vulnerable ends in ICS. The attacker can take advantage of these vulnerable ends to perform malicious activities. What the attacker can do at these ends:

1 Denial of Service (DoS)
   - Flood Modbus packets
   - Flood TCP packets
   - Disconnect Wires

2 Man in The Middle (MiTM)
   - Sniff Modbus packets
   - Manipulate Modbus packets

3 Malware Propagation
   - Physically damaging machines
   - Removing the commodity

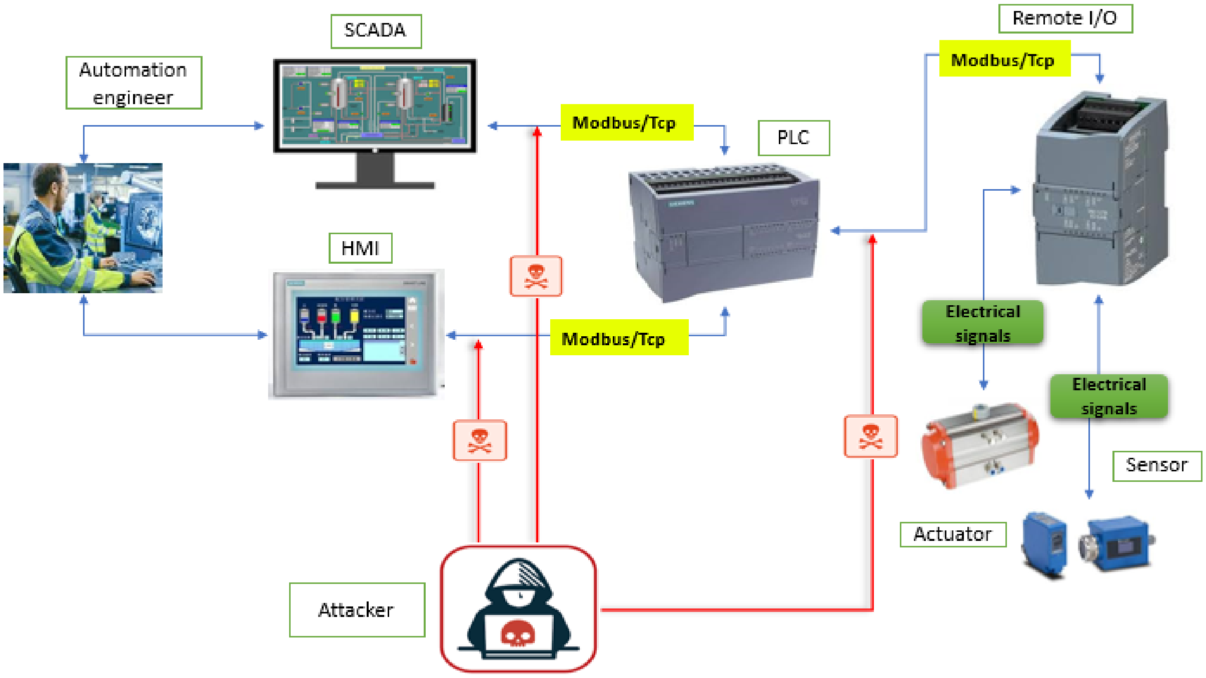

*Figure 5: MiTM attack ends*

Figure 5 shows us the different points where a Man in The Middle attack can be performed on a normal working scenario of industrial control systems. When data is being sent between HMI/SCADA systems and the PLC, an attacker can inject/manipulate packets. This can also be done when Modbus packets are being sent between the PLC and Remote IO

## 1.4 Scope

The Attack in our project will not target the components like PLCs, HMIs, SCADA systems, sensors, etc., rather we will be attacking the communication that takes place between these components which is done by using the Modbus/TCP variation of the Modbus communication protocol on Port 502. For demonstrating the attack, we will be using a web server, domain controller, and a jump server to make an Information technology (IT) network, and to make an Operational Technology (OT) network we will be using a NAS system, PLC, HMI, and factory IO simulator for simulating a physical process and configure them in a wired network such that it replicates an Industrial process and then perform a Man in The Middle attack. We are considering both cases where the attacker is an insider and an outsider and will perform a MiTM attack that will require less resources and will be feasible for the attacker to execute.

## 1.5 Impact of Project on the Society

A successful attack on Industrial Control Systems has a serious impact on an organization. These effects may include operational shutdown, damaged equipment, financial loss, and harm to society.

If we consider an automated solution of waste water treatment plant that uses components like PLCs that monitors and controls the operation of pumps, motors, and other devices then by simply intercepting and manipulating the data being transmitted to/from the PLC to the pumps, motors, etc., disastrous events could occur like water contamination incidents which result in disease outbreaks, which is a result of using products from contaminated water, this may ultimately lead to an operational shutdown, financial loss for an organization and may have some other serious impacts as well.

For understanding the impact of a successful attack, assume that one of the phases of an automated waste water treatment plant is to store water in a water tank which is as follows:

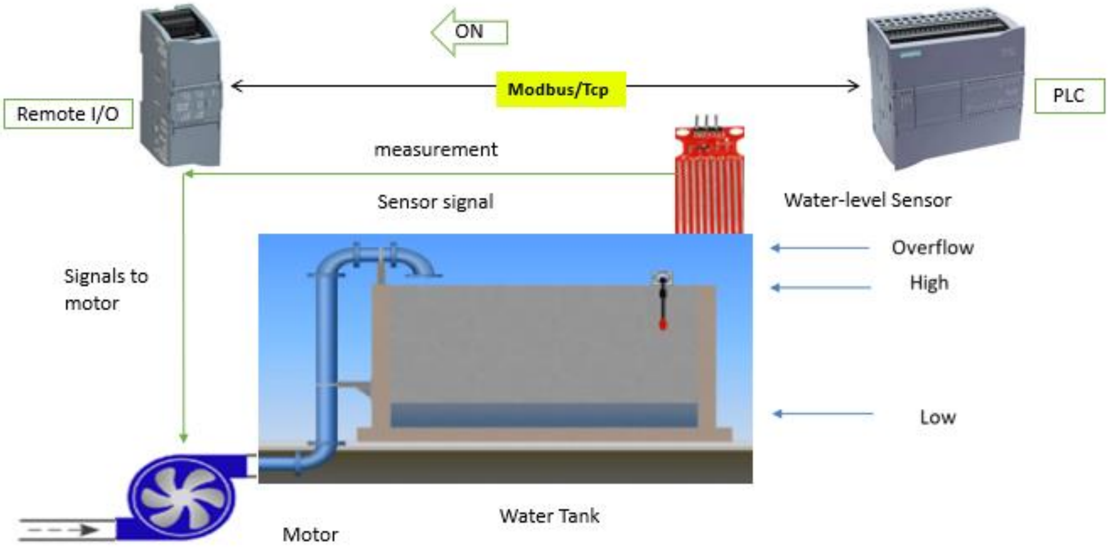

*Figure 6: Normal working of a specific scenario*

In Figure 6 we can see that initially, the water tank is empty so the water level sensor will send a signal to the remote IOs input module which will process it and send it to the PLC. The PLC will then generate an output (ON in this case) based on the input received and send it to the remote IOs output module via Modbus/TCP which will send the signal to the motor for it to start and pump water into the tank. Similar operations will take place once the tank reaches the water-level sensor (High), however, now the measurement received by the remote IOs input module will be different such that when the PLC processes it and sends it to the remote IOs output module (OFF in this case), the output module will then send a signal to the motor to stop pumping water in the tank.

**Note: Only one water-level sensor is used (HIGH). low and overflow points are shown just to give an idea.**

Now what the attacker can do in the given scenario is as follows:

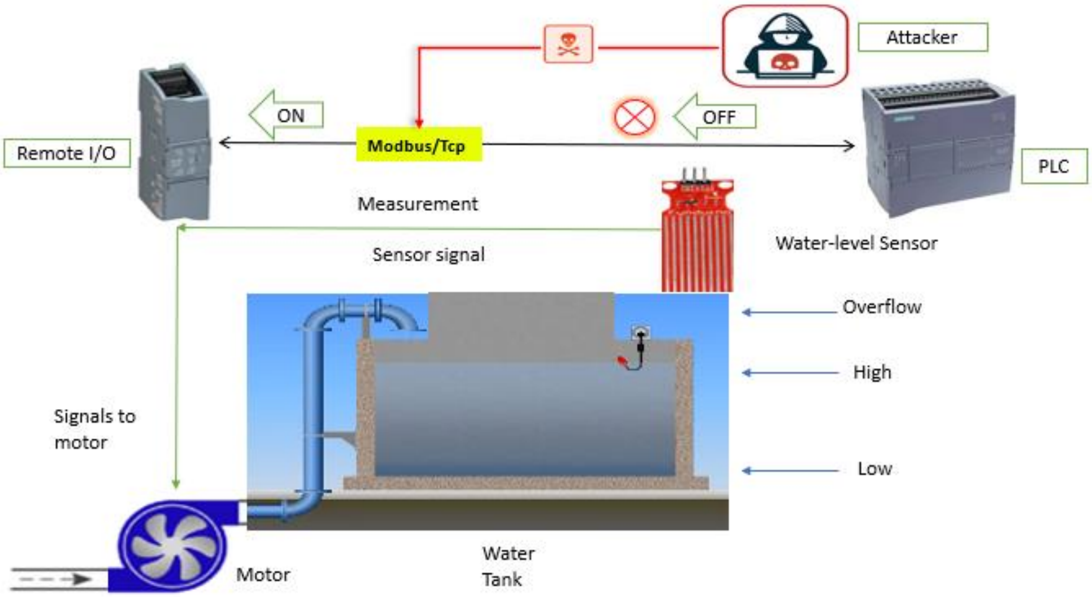

*Figure 7: Working of attack on a specific scenario*

In Figure 7 we can see that the communication that takes place between the Remote IO and the PLC is via Modbus/TCP. So, whenever the water tank gets full and the sensor sends its signal to the remote IOs input module which gets processed and is sent to the PLC, according to the logic implemented, the PLC will send an OFF command back to the remote IOs output module so that the remote IO can send a signal to the motor to stop, at this point the attacker can become the Man in the Middle and can manipulate the Modbus/TCP packets such that the OFF command becomes ON, causing the motor to continue pumping water in the tank and ultimately overflowing it.

Such scenarios can be extended to sensitive operations in a critical infrastructure like nuclear power plants, oil pipelines, electric grids, etc., and their impact can be disastrous. An example would be the **colonial pipeline ransomware attack**. In May of 2021, the American pipeline system i.e., colonial pipeline, suffered from a ransomware attack that impacted the computerized equipment controlling the pipeline. Because of this colonial pipeline had to shut down its operations which caused a shortage of fuel in several different states of America and the average fuel prices rose to their highest. Even American Airlines had to change their flight schedules temporarily due to fuel shortages at some airports.

Another case would be the **Ukraine power grid hack.** In December 2015, the power grid system of Ukraine was hacked and caused power outages for roughly 230,000 consumers for about 1-6 hours. Through different social engineering techniques, the attackers gained remote access to the ICS. They seized control of the SCADA system and remotely turned the substations off, along with that they also destroyed the IT infrastructure components and the files stored on servers and workstations.

Availability is the top priority of industries using ICS and running critical infrastructures. This is because they continuously need to run their operations, otherwise, they will face a lot of financial loss. So the CIA triad (Confidentiality, Integrity, and Availability) becomes the AIC triad (Availability, Integrity, and Confidentiality). This results in industries being very reluctant to change which leads to the emergence of vulnerabilities that if exploited, could cause disastrous outcomes as discussed above.

## 1.6 Literature review

ICSs are used to control critical infrastructures and PLCs are considered as the heart of any ICS to implement control logic and manage the interaction with sensors and actuators [1]. These interactions are made possible through industrial protocols such as Modbus TCP and are critical for communication with control devices. Unfortunately, such protocols were designed without any sort of security, allowing remote execution of commands on ICS because of no authentication, authorization, and encryption [2].

The security of ICSs is rarely a concern. A reason for this is because of their historic development. Initially, ICS were air-gapped systems using specialized software, hardware, and system parts that only a few people were familiar with. So, performing attacks was very unlikely as the physical presence of a highly skilled person was required. However, this is not the case now. To improve operational efficiency, ICSs are now connected to enterprise networks and in some cases also to the Internet. Along with that the systems are also easy to use and program and the knowledge to interact with these systems is now widespread and therefore increases the likelihood of attacks on ICS [1].

In 2003, the International Electrotechnical Commission and others introduced a standard structure of ICSs in IEC 62264. They divided the ICSs structure into 6 layers. Namely: Corporate level (level 4), Plant level (level 3), Process control level (level 2), Control level (level 1), Field level (level 1), and Process level (level 0). So, the following is a certainly not comprehensive list of possible attacks on some of the ICS levels [4]

- Attacks on level 0 (Process level):
    - Manipulation of physical process by removing commodity.
    - Physically damage the machines.
- Attacks on level 1 (Field level):
    - DoS attack on sensors and actuators.
    - Interfering with availability by disconnecting the network or the plug
    - MiTM between PLC and remote IO
- Attacks on level 1 (Control level):
    - DoS attack on PLC or HMI
    - Sniffing network traffic
    - MiTM between PLC or HMI
- Attacks on level 2 (Process Control level):
    - DoS attack on SCADA or historian systems.
    - Sniffing network traffic.
    - MiTM to manipulate data of SCADA or historian.

So, these studies clearly show us that ICSs are and can be vulnerable and it is possible to launch attacks on them. We will be performing a MiTM attack on industrial control system where our main goal is to disrupt the working of a physical processes. We will be taking the help of existing researches to make our testbed and to make custom scripts to successfully launch an MiTM on ICS by exploiting the vulnerabilities of Modbus TCP.

## 1.7 Gantt Chart

The timeline of our project is as follows:

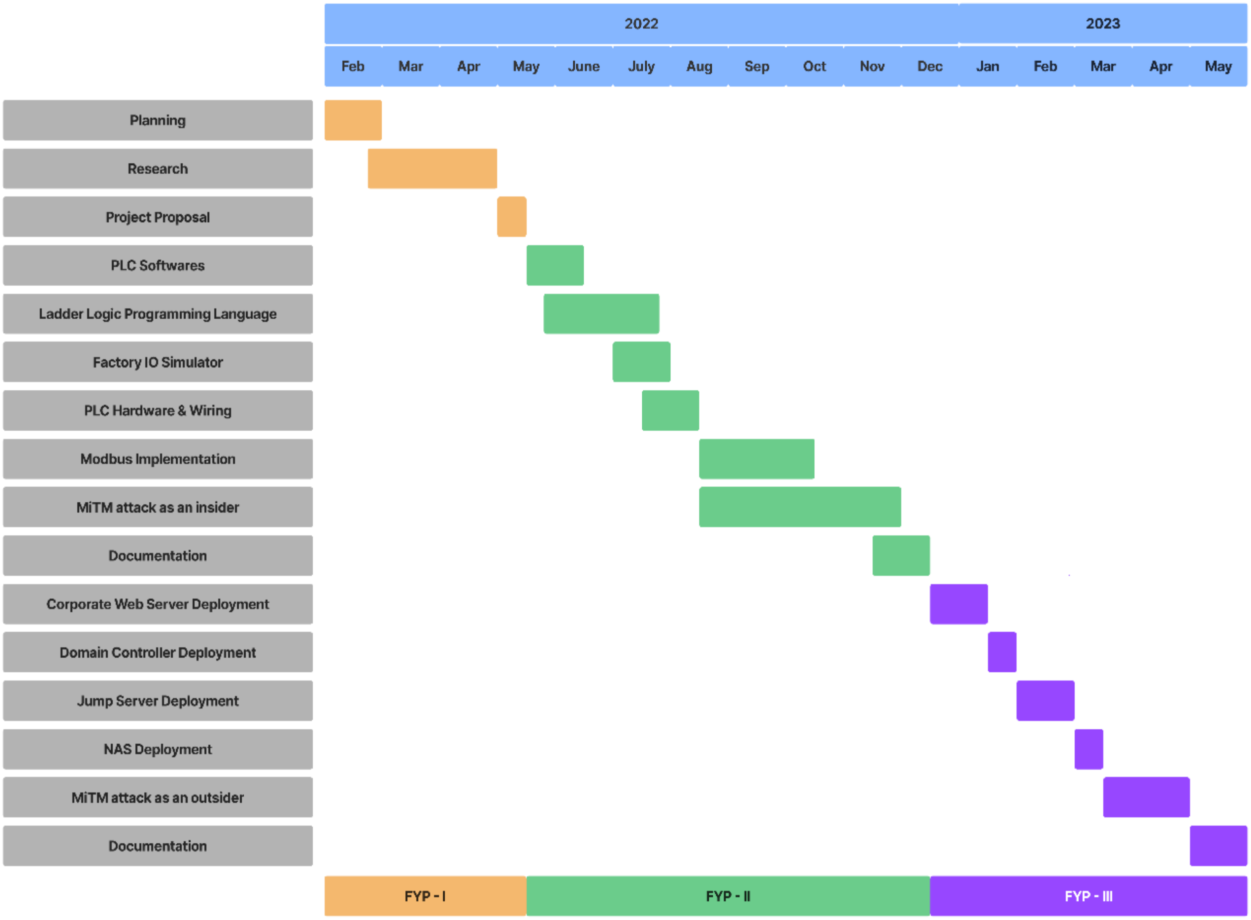

*Figure 8: Gantt chart*

## 1.8 Hardware and Software Requirements

The hardware and software requirements of our project are as follows:

**Hardware requirements:**

- Siemens PLC (Programmable Logic Controller) + power supply.
- Raspberry Pi.
- Switch.
- LAN cables.
- external Wi-Fi adapters.
- portable routers
- 6 laptops.

**Software requirements:**

- TIA (Total integrated automation) portal for PLC configuration.
- Factory IO for simulating physical process.
- Wientek EasyBuilder pro for making a HMI.
- Oracle VM VirtualBox for hosting VMs of a Web Server (Linux VM), Domain Controller (Windows Server 2016 VM) and Kali-Linux for performing the attack.
- WordPress for making a website.
- A Linux distribution for a Network-Attached-Storage running samba software package.
- Windows 10 for installing the TIA portal and Factory IO.
- Windows 10 for installing Wientek EasyBuilder pro.
- Pi OS for making a jump server running apache guacamole.

## 1.9 Tools and Technologies Used

The tools and technologies used in our project are as follows:

- Ladder Logic/Diagram for programming the PLC.
- Python modules:
    - Scapy for manipulating network packets and perform ARP spoofing
    - Netfiltetqueue for accessing packets match by rules in iptables, allowing us to accept, drop and alter packets.
    - pymodbusTCP for testing Modbus Client/Server communication over TCP.

    - http.server for transferring files.
- Kali-Linux since netfilterqueue module and iptables are available in it.
- WPscan for WordPress website scanning.
- Sqlmap for automated SQLi.
- John for cracking password hashes.
- Metasploit for using exploits and pivoting.
- Nmap for port scanning.
- Google for reconnaissance.
- MITRE ATT&CK framework for ICS.
- Purdue model.

## 1.10 Conclusion

In this chapter, we have shown how industrial control systems like PLCs, HMI, sensors, and actuators, SCADA systems can be used in critical infrastructures and how we can theoretically perform a MiTM attack on one of the phases of an automated water treatment plant and its devastating impacts on the society. We have also determined the scope of our project along with our hardware and software requirements to make our testbed, and that we will be exploiting the vulnerabilities of Modbus TCP to launch a MiTM on ICS. Our research is backed by the existing research about attacks on ICS which will help us in performing the MiTM attack.