

INTEGRATION OF TECHNOLOGY TO ACCESS THE MANUFACTURING PLANT VIA REMOTE ACCESS SYSTEM - A PART OF INDUSTRY 4.0

A Thesis Submitted

In partial fulfillment for the award of the degree of

Master of technology

In

Production Engineering



SUBMITTED BY

Biswojeet Kumar Gupta

(2K19/PIE/02)

Under the supervision of

Prof. Vikas Rastogi

DEPARTMENT OF MECHANICAL ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

Bawana Road, delhi-110042

July, 2021

Department of Mechanical Engineering
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CANDIDATE'S DECLARATION

I, Biswojeet Kumar Gupta, Roll No. 2K19/PIE/02 student of M.Tech (Production Engineering), hereby declare that the project Dissertation titled “Integration of technology to access the manufacturing plant via Remote Access System – A part of Industry 4.0” which is submitted by me to the Department of Mechanical Engineering, Delhi Technological University, Delhi in partial fulfilment of the requirement for the award of the degree of the Master of technology, is original and not copied from any source without proper citation. This work has not previously formed the basis for the award of any Degree, Diploma Associateship, Fellowship or other similar title or recognition.

Biswojeet

Place: Delhi

Date: 06/10/2021

Biswojeet Kumar Gupta

(2K19/PIE/02)

Department of Mechanical Engineering
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CERTIFICATE

I hereby certify that the Project Dissertation titled “Integration of technology to access the manufacturing plant via Remote Access System – A part of Industry 4.0” which is submitted by Biswojeet Kumar Gupta, Roll No. 2K19/PIE/02 Department of Mechanical Engineering, Delhi Technological University, Delhi in partial fulfillment of the requirement for the award of degree of Master of Technology, is a record of the project work carried out by the student under my supervision. To the best of my knowledge this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.



Place: DTU, Delhi

Date: 08-10-2021

Prof. Vikas Rastogi

Supervisor
Department of Mechanical Engineering
Delhi Technological University, Delhi

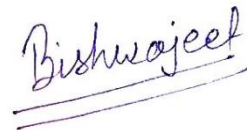
Department of Mechanical Engineering
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

ACKNOWLEDGEMENT

It is a matter of great pleasure for me to present my dissertation report on “Integration of technology to access the manufacturing plant via Remote Access System - A part of Industry 4.0”. First and foremost, I am profoundly grateful to my guide Prof. Vikas Rastogi, Department of Mechanical Engineering for their expert guidance and continuous encouragement during all stages of the thesis. I feel lucky to get an opportunity to work with him. Not only understanding the subject but also interpreting the results drawn thereon from the simulation model was very thought-provoking. I am thankful for the kindness and generosity showed by them towards me, as it helped me morally complete the project before actually starting it.

I would like to extend my gratitude to Prof. S. K. Garg, Head, Department of Mechanical Engineering for providing this opportunity to carry out the present work.

Finally, and most importantly, I would like to thank my family members for their help, encouragement, and prayers through all these months. I dedicate my work to them.



Place: Delhi

Date: 06/10/2021

Biswojeet Kumar Gupta

(2K19/PIE/02)

ABSTRACT

During Covid-19 many manufacturing industries had to stop production operations and close the plant for someday as there was a lockdown and people were not allowed to go out. Meanwhile, the IT sector and some other industries are growing very fast. The reason is that they have the facility of Work from Home. Why shouldn't the manufacturing industry have such a system through which production operations can be monitored and controlled from home? Remote Access System is such technology through which manufacturing operations can be monitored and controlled remotely from any part of the world. This is formed by integrating the existing technology such as SCADA, microcontroller, OPC server, Internet, Sensor, and Actuator. The simulation model of the Remote Access System is designed on Proteus and Wonderware Intouch to demonstrate its possibility and how it will work. The SCADA model of the manufacturing plant which is designed in Intouch successfully communicated with the Arduino model of Proteus. Operators with Desktop remote connection software get access to HMI and control the operation which is designed in the simulation model. The simulation model shows a latency of 326 milliseconds which shows the requirement of a fast data transmission network with proper protocol for the industrial device. From this study, we conclude that the Remote Access system is possible but it will not be effective until the infrastructure of IIoT is developed. Remote Access System is a part of Industry 4.0 as in this model of the industry every device is connected with the central controlling unit which can monitor and control them. Much research is carried out under Industry 4.0 which will develop infrastructure for IIoT and make the Remote Access system effective.

Keywords: Remote Access; Control and Monitoring; SCADA; Integration of Technology; Industry 4.0

CONTENTS

CANDIDATE’S DECLARATION	ii
CERTIFICATE	iii
ACKNOWLEDGEMENT	iv
ABSTRACT.....	v
Chapter 1: INTRODUCTION.....	1
1.1 Introduction	1
1.2 Overview	2
1.3 Benefit of Remote Access System	3
1.4 Statement of Problem	3
1.5 Organization of Dissertation	4
Chapter 2: LITERATURE REVIEW.....	5
2.1 Literature Review	5
2.2 Objective of Present Study	7
Chapter 3: METHODOLOGY	8
3.1 Implementation.....	8
3.2 Configuration Step	34
3.3 Issue while implementing this model in the Real Manufacturing Plant	35
3.4 Issue related to the implementation of SCADA in Today World for Remote access systems	36
3.5 Issues and Challenges of Remote access system	38
3.6 Industry 4.0 based solution to the implementation of Remote access system	39
Chapter 4: RESULTS AND DISCUSSION	45
4.1 Results	45
4.2 Discussion	57
Chapter 5: CONCLUSION AND FUTURE SCOPE	59
5.1 Conclusion.....	59
5.2 Future Scope.....	59
Reference	60

LIST OF FIGURES

FIGURE 1.1 INDUSTRIAL REVOLUTIONS	1
FIGURE 2.1 EVOLUTION OF SCADA	6
FIGURE 3.1 SIMULATION MODEL OF PLANT IN PROTEUS	8
FIGURE 3.2 PULSE WIDTH MODULATION.....	9
FIGURE 3.3 FLOW CHART OF THE PROGRAM OF 1 ST AND 2 ND UNIT.	10
FIGURE 3.4 FLOW CHART OF THE PROGRAM OF THE 3 RD UNIT.	17
FIGURE 3.5 REMOTE ACCESS NETWORK ARCHITECTURE	20
FIGURE 3.6 SYSTEM MANAGEMENT CONSOLE.....	21
FIGURE 3.7 INTOUCH SCADA	23
FIGURE 3.8 FLOW CHART OF SCADA SCRIPT	24
FIGURE 3.9 HUMAN MACHINE INTERFACE (HMI)	34
FIGURE 3.10 INTELLIGENT SENSOR.....	40
FIGURE 3.11 CYBER-PHYSICAL SYSTEM.....	41
FIGURE 3.12 BIG DATA ANALYSIS.....	42
FIGURE 3.13 CLOUD COMPUTING	43
FIGURE 3.14 DEVICE CONNECTED IN IIOT	44
FIGURE 4.1 CONNECTION BETWEEN SIMULATION MODEL	45
FIGURE 4.2 SUCCESSFULLY ESTABLISHING CONNECTION BETWEEN PLANT UNIT AND COMPUTING UNIT.....	46
FIGURE 4.3 CONNECTING HMI (2 ND COMPUTER) THROUGH REMOTE DESKTOP CONNECTION (3 RD COMPUTER).....	46
FIGURE 4.4 HMI VIEW WHEN MAIN SWITCH OFF.....	47
FIGURE 4.5 PROTEUS VIEW WHEN MAIN SWITCH OFF	47
FIGURE 4.6 HMI VIEW WHEN MAIN SWITCH ON	48
FIGURE 4.7 PROTEUS VIEW WHEN MAIN SWITCH ON.....	48
FIGURE 4.8 CONVEYOR UNIT START AND WORKPIECE MOVE FORWARD	49
FIGURE 4.9 CONVEYOR MOTOR ROTATED IN COUNTER-CLOCKWISE	49
FIGURE 4.10 WORKPIECE REACH TO ELECTRIC PRESS AND HEAD MOVE DOWNWARD.....	50
FIGURE 4.11 ELECTRIC PRESS MOTOR ROTATED CLOCKWISE AND CONVEYOR MOTOR STOP. ...	50
FIGURE 4.12 WORKPIECE PRESS BY ELECTRIC PRESS	51
FIGURE 4.13 ELECTRIC PRESS MOTOR ROTATED IN CLOCKWISE AND CONVEYOR MOTOR STOP	51
FIGURE 4.14 PRESS HEAD MOVING UPWARD AND WORKPIECE MOVING FORWARD	52
FIGURE 4.15 PRESS MOTOR AND CONVEYOR MOTOR ROTATED IN COUNTER-CLOCKWISE.....	52
FIGURE 4.16 WORKPIECE REACH AT PROCESSING PLACE AND PRESS AND DRILLING HEAD MOVING DOWNWARD.....	53
FIGURE 4.17 PRESS AND DRILLING MACHINE MOTOR ROTATED IN CLOCKWISE AND CONVEYOR MOTOR STOP	53
FIGURE 4.18 WORKPIECE PROCESS BY DRILLING AND PRESS HEAD.....	54
FIGURE 4.19 PRESS AND DRILLING MACHINE MOTOR ROTATED IN CLOCKWISE AND CONVEYOR MOTOR STOP	54
FIGURE 4.20 WORKPIECE MOVING FORWARD AND DRILLING AND PRESS HEAD MOVING UPWARD	55
FIGURE 4.21 PRESS AND DRILLING MOTOR ROTATED COUNTER-CLOCKWISE AND CONVEYOR MOTOR ROTATED IN CLOCKWISE.....	55

FIGURE 4.22 MANUFACTURING UNIT RUNNING IN AUTOMATIC MODE56
FIGURE 4.23 PRESS MOTOR ROTATED COUNTER-CLOCKWISE AND DRILLING MOTOR ROTATED IN
CLOCKWISE.....56
FIGURE 4.24 HISTORICAL TREND.....57

LIST OF TABLES

TABLE 3.1 CYBER ATTACK ON SCADA SYSTEM	36
TABLE 3.2 PROTOCOL VULNERABILITIES FOR SCADA	38

Chapter 1: INTRODUCTION

1.1 Introduction

Invention of technology bring different Industrial revolution as Steam Engine bring 1st Industrial Revolution (1784), Electricity brings 2nd Industrial Revolution (1870), Computer and Electronic bring 3rd Industrial Revolution (1969), IIoT will bring 4th Industrial Revolution (2011) [1]. There is different technology which has been developed to make the process easy and effective. Some of the technologies are integrated together so that advantages of both technologies can be utilized at a time or to get different facilities such as Smart sensor and actuator are integrated together for Automatic.

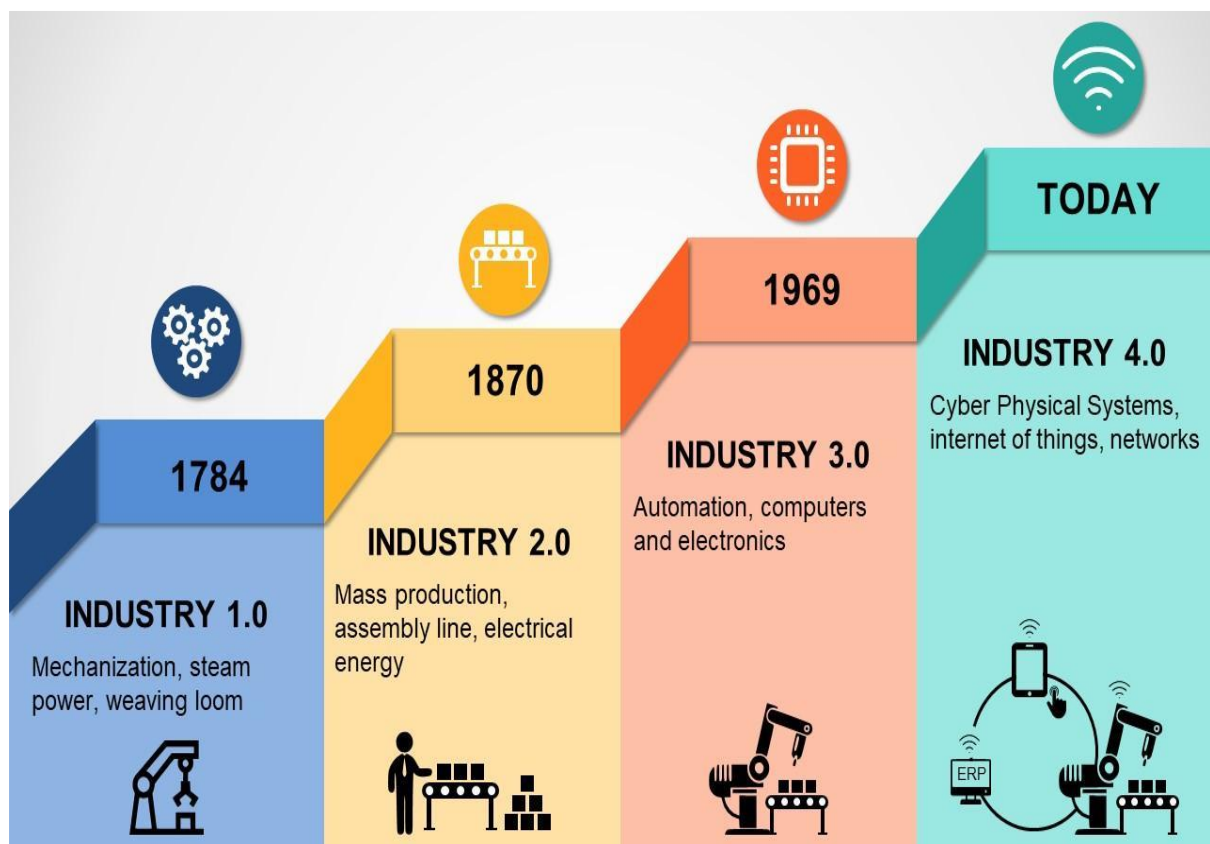


Figure 1.1 Industrial Revolutions [1]

Remote access is defined as a system through which a process can be monitored and controlled remotely from any place. So, a Remote access system for Manufacturing Plant is a system through which a User with Id and Password can Monitor and Control the operation of Manufacturing from any place in the world. The User feels like he/she is present in the factory and controlling the operation. This system is formed by integrating the existing Technology. As there are different techniques to control the process from a far distance such as controlling the Robot from a centralized controlling Unit, SCADA, etc. So, it doesn't require developing new technology. It only required certain improvements in an existing one.

The technology which we have integrated here to form Remote Access System is Smart Sensor which collects data from its surrounding, Microcontroller which process that data, Actuator which actuated the process, IoT which make a connection between different component for communication, Cloud computing for processing the data, and HMI to provide interacting Platform for User. This technology is already developed. We simply integrated them together to form a Remote access system. To make the system more effective, improvement of some technology is required.

1.2 Overview

Development of the internet makes people able to connect to different parts of the world. It also enables people to monitor and control other systems in real-time. So, there is an advantage of getting the help of some expert person who is far from that place. Such as through the TeamViewer app expert can monitor and control other computers or systems as he/she is present there. Nowadays distance learning systems are getting popular. Students get a chance to learn from an expert teacher. With the development of the Internet, people can work from a far distance. During Covid-19 some people are working from their homes. But there is no such system for Manufacturing industries. People of such industries need to go to the factory for monitoring and controlling the operation.

As many working sectors have the advantage of working Remotely. Such advantages should be there with Manufacturing Industries People. There should be a Remote Access system through which people can monitor and control the manufacturing operation in real-time from any part of the world as they are present there. This also brings an opportunity to get help from an expert who is far from Plant.

In Industry there are some sophisticated processes such as pipeline pressure, gas flow, and temperature which need to be monitored continuously. Before 1970 this process was done manually. But when the process increases with the increase in the size of the industry, the monitoring, and controlling process become very difficult to carry out. In 1970 Supervisory Control And Data Acquisition (SCADA) was Developed through which operators can monitor and control the sophisticated process from one location of Industry [2]. This is based on isolated network architecture design. The continual expansion of all industries, the rise in the number of automated processes, and the proliferation of industrial equipment providers present a problem of linking disparate hardware and software [3]. To solve this issue in 1996 Open Architecture was adopted with WAN network (Internet). The evolution of SCADA system design and functions can be divided into three primaries "generations": Monolithic SCADA, Distributed SCADA, and Networked SCADA [2]. A task force of the industrial automation industry developed the Object Linking and Embedding (OLE for Process Control) for Process Control standard in 1996. In the same year, the OPC Foundation was created to maintain the standards [4]. The usage of standardized protocols allows equipment from many manufacturers to be connected. EGAT-SCADA was created in 2000 to monitor and control operations on Thailand's electric power transmission infrastructure [5].

SCADA systems from the past functioned on separate networks, making them less vulnerable to Internet threats. Furthermore, the systems' security was enhanced by the limited

availability of technical knowledge about the protocols in use. These networks have now been connected to public networks such as the Internet, allowing them to benefit from the robustness of common network protocols, improve remote access, and save money on capital and operating costs. However, connecting SCADA systems to the Internet raises serious security concerns [3]. According to many authors, the number of security incidents and cyber-attacks against important SCADA systems is on the rise. As a result, security considerations for SCADA systems are given greater weight and consideration than those for normal IT systems due to the potential impact on the physical safety of personnel, customers, or communities [6]. Many Protocols are developed to protect SCADA from cyber-Attack. Some authors have recently identified a new "generation" that is currently evolving - Internet of Things SCADA. This approach is based on the concept of cloud computing, which was recently invented [2].

SCADA systems are used in a variety of industries for remote monitoring and control, including controlling the flow of gas and oil through pipes in the oil industry, water flow management in water and sewage systems, management of power plant electrical output to the power grid, process control in chemical plants, product transmission, and distribution management in manufacturing units, and so on [7]. But no Industry uses this system in Manufacturing operations. This paper mainly focuses on the implementation of the Remote Access system for Manufacturing operations in different Industries. To demonstrate this a simulation model is designed which will be presented later.

1.3 Benefit of Remote Access System

Remote Access System can provide many facilities depending upon its design, feature adds, equipment uses, infrastructure, and implementation. During situations like covid-19, Remote Access System helps to run the manufacturing and other plants smoothly from any place of the world. During Online classes this model can create virtual Labs for College or School students where they perform practical work as they are there and the results of the practical work can be submitted to the teacher. This method can be applied to the Education sector where resources are limited and many students are deprived of access to proper lab or study material. An expert from different places of the world can help to improve the process through a remote access system without being physically present within the factory. They can observe the process properly and can suggest some improvement. Experts don't need to travel frequently to provide their service. Real-time monitoring and control of different branches of a company from a single place are possible through the Remote Access system.

1.4 Statement of Problem

The statement of the problem is described below. This can be split into smaller tasks that can be well understood.

- Investigate the various available technology or processes which are used for Remote control or monitoring by any Industry and select the best and standard technique for implementation.
- Finding the way to integrate available technology for remote monitoring and control of the manufacturing operation.

- Simulating the process of integrating the technology and trying to find its result.
- Finding the issue which may come while applying the process for the Real manufacturing process. As well as finding their possible solution.

1.5 Organization of Dissertation

- Chapter 1 includes a brief introduction to the Remote Access System concepts. It introduces different Industrial revolutions, defines Remote Access System, background and motivation of Remote monitoring and control process, its need for the process control applications, and its benefits. The statement of the problem of the dissertation is explained.
- Chapter 2 includes a Literature review of the work previously done by different authors. It discusses various methods and processes to implement a Remote access system. Objective of the study is described in this section.
- Chapter 3 discusses the method which is used to study the possibility of Remote Monitoring and Control. It includes a Simulation model which shows how technology can be integrated together to form a Remote access system. Simulation of the controller is designed in Proteus, HMI is designed in Intouch, Proteus and Intouch are connected through Arduino OPC server.
- Chapter 4 discusses the various issues that may arise while implementing Remote access systems in Real Manufacturing operations as well as their solution. It includes Cyber-attack, Improper Protocol, Component issues. It also stated how the development of Industry 4.0 solved this problem.
- Chapter 5 summarizes the various results and discussions. The results included in this chapter are those which cannot be provided as a part of the other chapters but have overall significance.

Chapter 2: LITERATURE REVIEW

2.1 Literature Review

During the Covid-19 situation, we see that many Industries run Remotely. People are working from their homes. Is this possible for the Manufacturing Plant operator? The answer is No. As there is no system through which we can monitor and control production operations remotely. A SCADA system is used to monitor and control processes such as controlling the flow of gas and oil through pipes in the oil industry, water flow management in water and sewage systems, management of power plant electrical output to the power grid, process control in chemical plants, management of product transmission and distribution in manufacturing units, and signaling. But SCADA has not been used for controlling the Production process in Manufacturing plants. In this paper, we are trying to develop a Remote Access System which can monitor and control the production process. For this first, we discuss the development which has taken place in the field of remote monitoring and control systems.

Alexandru Ujvarosi [2] shows the evolution of the Supervisory Control And Data Acquisition (SCADA) system. Author stated that PLC-based SCADA has been developed in 1970 to remove manual operation of monitoring and controlling of sophisticated processes such as temperature, pressure, humidity, the flow of gas and liquid, production lines which need to be monitored continuously. As stations are at different locations, several human forces have to travel to the station to control and monitor the process which is very difficult. Telemetry-based First SCADA was Developed in 1950 (not actual SCADA which we know today), which is based on the Telephone wire. With the development of microprocessor PLC and RTU replaced Telemetry-based SCADA.

Different generations of SCADA are explained by Stamatis Karnouskos and Armando Walter Colombot [8] as technological vendors developed various SCADA designs as a result of evolution and the demand for more intelligent and secure systems. Monolithic SCADA, Distributed SCADA, and Networked SCADA are three key “generations” of the system architecture and functions offered. SCADA's early (Monolithic SCADA) architecture concept was based on mainframe computers, in which networks were essentially non-existent. As a result, the early control systems were unable to communicate with one another, making them stand-alone systems. The growth and advancements in system miniaturization, as well as LAN technology, were major drivers in the development of Distributed SCADA. All of the devices linked to the SCADA LAN, however, were unable to communicate with other external devices utilizing different protocols. The third generation of SCADA systems (Networked SCADA) is essentially similar to the second, with one major difference: instead of a vendor-controlled and proprietary environment, it is aimed toward open system architecture. The introduction of WAN protocols, such as Internet Protocol (IP), was a crucial role in the rapid development of the third generation of SCADA systems.

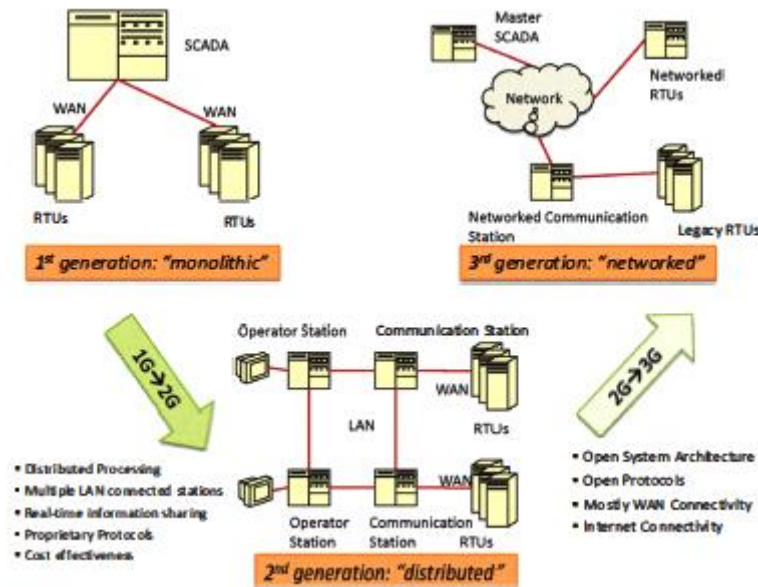


Figure 2.1 Evolution of SCADA [8]

A task force of the industrial automation industry developed the Object Linking and Embedding for Process Control standard in 1996. (OLE for Process Control). In the same year, the OPC Foundation was established to keep the standards updated. OPC interface handles interoperability in industrial control and automation applications (OPC Foundation Online). According to Pérez et al. [4] currently, OPC is one of the front-runners for leading standardization and system integration in sophisticated frameworks.

EGAT-SCADA was developed in 2000 for monitoring an operation involving an electric power transmission grid across Thailand. Both policy and technology are used to ensure the security of EGAT-SCADA. A general-IT-based security strategy has been established and recommended for the deployed sites. The North American Electricity Reliability Council (NERC) recommends cyber security as one of the most essential sources of security recommendations. Based on the thought of the Paukatong [5] "even though all required procedures for maintaining the security of the EGAT-SCADA have been applied, there is still some undiscovered exposure," according to the report, and research into further security techniques is ongoing.

Pliatsios, et al. [3] compared traditional SCADA systems with today's SCADA, where they found traditional SCADA systems ran on separate networks, making them less vulnerable to cyber-attacks. These networks were connected to common networks like the Internet in 1996 to take advantage of the robustness of common network protocols, allow remote access, and lower capital and operating costs. Authors [3] also show that the SCADA system interface with the internet raises serious security concerns. The author in [6] studies the incidence of security incidents and cyber-attacks on critical SCADA systems is increasing. Security considerations for SCADA systems are given higher priority and consideration than those for normal IT systems because of the potential threat to the physical safety of personnel, customers, or communities. Due to which researchers have been focused on increasing the security and reliability of the SCADA system. Authors [3] found, most of the security proposals are based

on classifying traffic using SVM, traffic encryption, attack detection, Neural Networks, and traffic encryption. The overall evaluation findings show a high degree of accuracy and a low number of false positives. Authors [3] present the latest trend in the SCADA system which includes the design of new SCADA protocols to meet the needs of industry 4.0 applications. Alexandru Ujvarosi [2] showed the development of a new generation of SCADA which is known as the Internet of Things SCADA.

2.2 Objective of Present Study

The literature survey has revealed that a lot of work has been carried out on remote monitoring and control of processes since 1950. It already implements in different sectors of industry including material movement and production line observation of manufacturing plants but there is no implementation of such a system in the production operation of the manufacturing plant. As production operation can be done through automation then this operation can also be done using microcontroller, sensor, and actuator with other technology. So, we try to find a way to integrate remote monitoring techniques with microprocessors, sensors, and actuators to control machines of manufacturing plants such as Lathe, Drilling machines, Milling machines, conveyor belts, etc. This will enable the operator of the manufacturing plant to monitor and control production operations remotely. The objectives of this study are as follow:

- i. Finding the way to integrate existing technology to form a Remote access system to control the machine of the manufacturing plant remotely.
- ii. Implementing this process in simulating software and finding the results of the process.
- iii. Study different aspects of this simulation model to know the issue and difficulties which may arise while implementing it in a Real Manufacturing Plant.

Chapter 3: METHODOLOGY

3.1 Implementation

To demonstrate the Remote access process, we have simulated a section of the plate Manufacturing Plant using Intouch-SCADA, Remote Desktop Connection, and Proteus Simulation Software. The methodology applied for this simulation is an integration of existing technology. We have integrated Sensor, Actuator, Arduino (Microcontroller), Virtual Serial Ports Emulator (VSPE), Arduino OPC Server, System Management Console, and SCADA.

A brief description of the Simulation model is given below:

3.1.1 Proteus

Proteus represents Manufacturing Plant where Sensor (Temperature Sensor), Actuator (Motor), and Microcontroller (Arduino) are integrated with the machine. Sensors are connected with Arduino, so they transfer data to Arduino. Arduino, send that data to Cloud via OPC server. Cloud Processor processes data and sends an instruction to Arduino. Arduino IDE is used to program the Arduino Uno. As there are so many devices used in this project. To identify each device there should be a nomenclature rule, so we have developed a rule which states that the name of the device starts with its type followed by 2 numbers which is separated by “- “.

First No.: Signifies the unit to which the component belongs.

Second No.: Signifies the number of the same element in that particular unit.

For Instance: 2nd led device of unit 3 will be named led3-2.

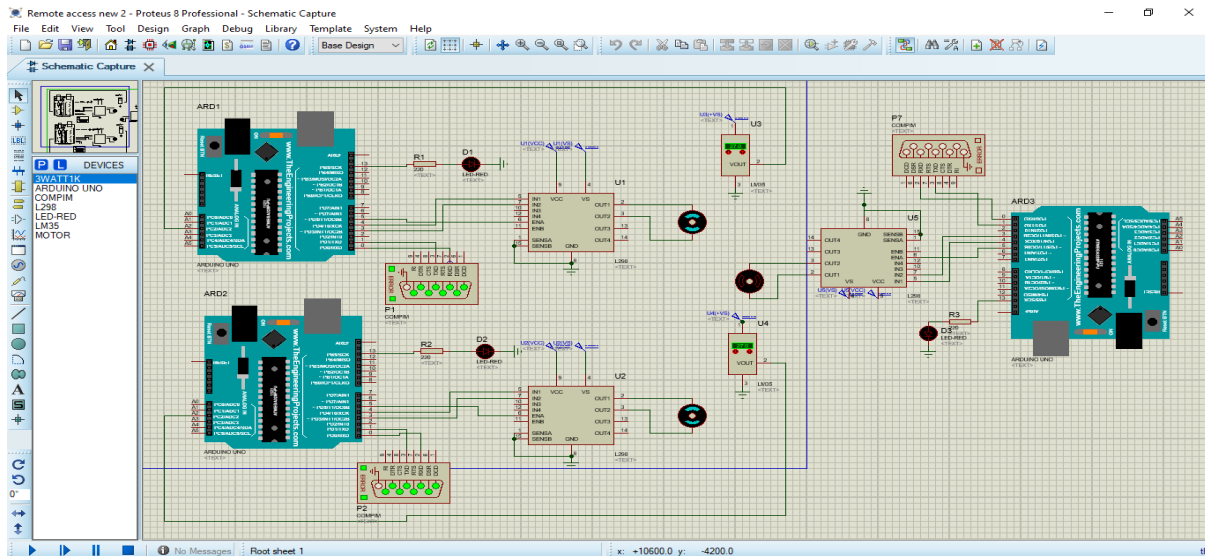


Figure 3.1 Simulation model of Plant in Proteus

In this simulation model we take 3-units, 1st unit represents Electric Press, 2nd unit represents Drilling Machine, and 3rd unit represents Conveyor Belt. Each unit is independent of the other. In the 1st unit, Arduino received a motor controlling signal which varies from 1-10 from Cloud (User). Arduino map controlling signal and find motor speed which varies from 0-250 rpm. Now Arduino sends this value to the L298D PWM module. PWM (pulse width modulation) is a technique for altering the average voltage going to an electrical device by

rapidly switching on and off the power. The duty cycle, or the time the signal is ON vs the time it is OFF in a single period of time, determines the average voltage.

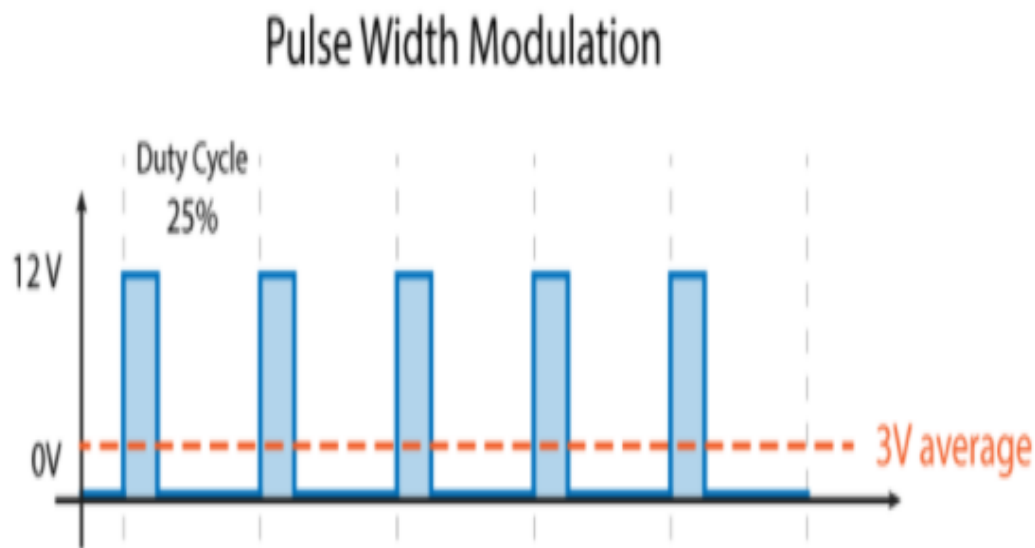


Figure 3.2 Pulse Width Modulation

Using the PWM technique L298D controls the speed of the motor. This motor provides the desired motion to Press the machine head. It controls speed as well as the direction of motion. In this way, the user can control the motion of the Press head via the Cloud system. The Motor control system used in this simulation is an open-loop system as there is no feedback Arduino gets about motor speed. If high precision is required then a feedback system (Encoder) should be used.

The temperature sensor senses the temperature of the machine and sends it to the cloud. The User can monitor the temperature of the machine in real-time so if the temperature exceeds a certain limit, then necessary actions such as reducing speed or stopping the motion can be carried out by the user automatically.

To connect Arduino to the OPC server we use COMPIIM. In Proteus, COMPIIM is used to model physical COM interfaces. Before presenting serial signals to the electrical circuit, it catches and buffers them. All serial data from the CPU or the UART model will be sent through the serial ports on the PC. This COMPIIM is connected to Physical COM port 1 and COM port 1 is connected to the OPC server via TCP/IP Server-Client system.

A similar mechanism is used in the 2nd and 3rd units to control the Drilling machine and Conveyor Belt respectively. In the Conveyor Belt, there is no temperature sensor as there is no process that can increase its temperature.

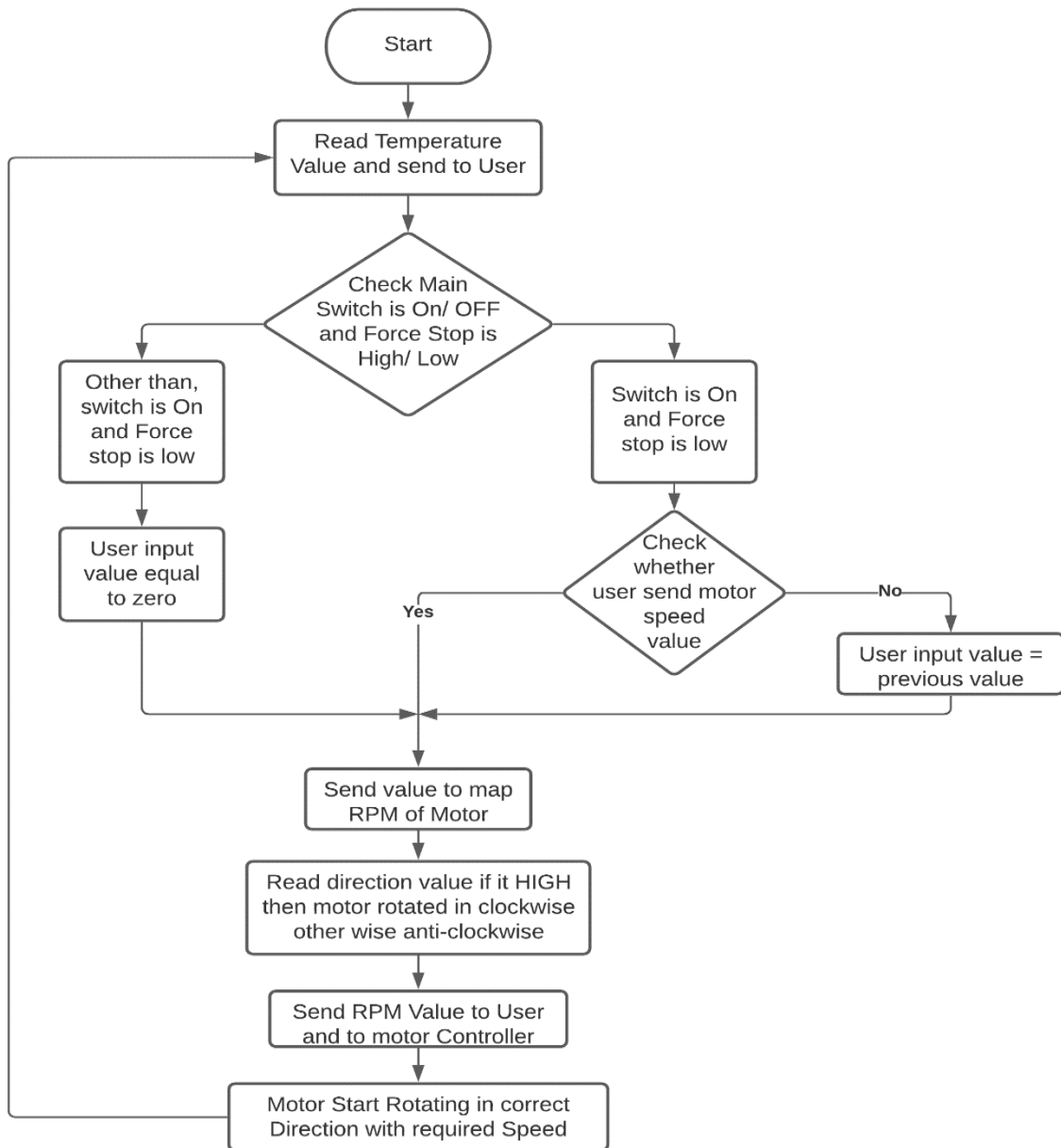


Figure 3.3 Flow chart of the program of 1st and 2nd Unit.

Program of 1st Unit

```

#include <OPC.h>
#include <Bridge.h>
#include <Ethernet.h>
#include <SPI.h>

```

```

// OPC object declaration
OPCSerial aOPCSerial;

```

```

// Set the status of the Led using the OPC Client.

```

```

int ledPin1 = 13;
int temp = A2;
int val=0;
int val1 = 0;
int val2 = 0;
int val3 = 0;
int val4 = 0;
int enA = 5;
int dir1 = 4;
int dir2 = 3;
int motion = 1;

// For the OPCItem, formation of the callback function

// For led
bool callback1(const char *item, const opcOperation opcOP, const bool value){
static bool ledval = false;

// Check written command of OPC Client
if (opcOP == opc_opwrite) {
ledval = value;
if(ledval){
val=1;
}
else {
val=0;
}
if (ledval)
digitalWrite(ledPin1, HIGH);
else
digitalWrite(ledPin1, LOW);
}
else

// Find led state
return ledval;
}

// For Force stop
bool callback2(const char *item, const opcOperation opcOP, const bool value){
static bool force = false;
if (opcOP == opc_opwrite){
force = value;
if(force){

```

```

        val4=1;}
    else{
        val4=0;
    }
}
return force;
}
// For Temperature
int callback3(const char *item, const opcOperation opcOP, const int value){
    val1=analogRead(temp)-1;
    return val1/2;
}
// For Motor speed
int callback4(const char *item, const opcOperation opcOP, const int value){
    if (opcOP == opc_opwrite){
        val2=value;
    }
    if(val==0 || val4==1){
        val2=0;
    }
    return val2;
}
// For RPM
int callback5(const char *item, const opcOperation opcOP, const int value){
    return val3;
}
// For Direction
bool callback6(const char *item, const opcOperation opcOP, const bool value){

    // If the operation is an OPC Client write command
    if (opcOP == opc_opwrite) {
        motion = value;
    }
    else
        // Read the direction status
        return motion;
}
void setup() {
    Serial.begin(57600);
    pinMode(ledPin1, OUTPUT);
    pinMode(enA,OUTPUT);
    pinMode(dir1,OUTPUT);
    pinMode(dir2,OUTPUT);
}

```

```

// Configuration of OPC Objects
aOPCSerial.setup();

// Configuration of OPC Item
aOPCSerial.addItem("led1-1",opc_readwrite, opc_bool, callback1);
aOPCSerial.addItem("forcestop1-1",opc_readwrite, opc_bool, callback2);
aOPCSerial.addItem("temp1-1",opc_readwrite, opc_int, callback3);
aOPCSerial.addItem("motor1-1",opc_readwrite, opc_int, callback4);
aOPCSerial.addItem("rmp1-1",opc_read, opc_int, callback5);
aOPCSerial.addItem("direction1-1",opc_readwrite, opc_bool, callback6);
}

void loop() {

// Using the OPC command

aOPCSerial.processOPCCommands();
if (motion){
    digitalWrite(dir1, HIGH);
    digitalWrite(dir2, LOW);
}
else{
    digitalWrite(dir1, LOW);
    digitalWrite(dir2, HIGH);
}
int motorspeed=map(val2,0,10,0,255);
val3=motorspeed;
if(motorspeed>0){
    analogWrite(enA,val3);
}
else{
    analogWrite(enA, 0);
}

}

```

Program of 2nd Unit

```

#include <OPC.h>
#include <Bridge.h>
#include <Ethernet.h>
#include <SPI.h>

```

```

// OPC object declaration

```

```
OPCSerial aOPCSerial;
```

```
//Set the status of the Led using the OPC Client.
```

```
int ledPin1 = 13;
```

```
int temp = A2;
```

```
int val=0;
```

```
int val1 = 0;
```

```
int val2 = 0;
```

```
int val3 = 0;
```

```
int val4 = 0;
```

```
int enA = 5;
```

```
int dir1 = 4;
```

```
int dir2 = 3;
```

```
int motion = 1;
```

```
// For the OPCItem, formation of callback function
```

```
// For led
```

```
bool callback1(const char *item, const opcOperation opcOP, const bool value){
```

```
    static bool ledval = false;
```

```
// Check written command of OPC Client
```

```
if (opcOP == opc_opwrite) {
```

```
    ledval = value;
```

```
    if(ledval){
```

```
        val=1;
```

```
    }
```

```
    else {
```

```
        val=0;
```

```
    }
```

```
    if (ledval)
```

```
        digitalWrite(ledPin1, HIGH);
```

```
    else
```

```
        digitalWrite(ledPin1, LOW);
```

```
    }
```

```
    else
```

```
// Find led state
```

```
    return ledval;
```

```

}
//For Force stop
bool callback2(const char *item, const opcOperation opcOP, const bool value){
    static bool force = false;
    if (opcOP == opc_opwrite){
        force = value;
        if(force){
            val4=1;
        }
        else{
            val4=0;
        }
    }
    return force;
}
// For Temperature
int callback3(const char *item, const opcOperation opcOP, const int value){
    val1=analogRead(temp)-1;
    return val1/2;
}
// For Motor speed
int callback4(const char *item, const opcOperation opcOP, const int value){
    if (opcOP == opc_opwrite){
        val2=value;
    }
    if(val==0 || val4==1){
        val2=0;
    }
    return val2;
}
// For RPM
int callback5(const char *item, const opcOperation opcOP, const int value){
    return val3;
}
// For Direction
bool callback6(const char *item, const opcOperation opcOP, const bool value){

// If the operation is an OPC Client write command

    if (opcOP == opc_opwrite) {
        motion = value;
    }
    else

```



```

// Read the direction status

    return motion;
}
void setup() {
  Serial.begin(57600);
  pinMode(ledPin1, OUTPUT);
  pinMode(enA,OUTPUT);
  pinMode(dir1,OUTPUT);
  pinMode(dir2,OUTPUT);
  // Configuration of OPC Objects
  aOPCSerial.setup();

  // Configuration of OPC Item

  aOPCSerial.addItem("led2-1",opc_readwrite, opc_bool, callback1);
  aOPCSerial.addItem("forcestop2-1",opc_readwrite, opc_bool, callback2);
  aOPCSerial.addItem("temp2-1",opc_readwrite, opc_int, callback3);
  aOPCSerial.addItem("motor2-1",opc_readwrite, opc_int, callback4);
  aOPCSerial.addItem("rmp2-1",opc_read, opc_int, callback5);
  aOPCSerial.addItem("direction2-1",opc_readwrite, opc_bool, callback6);
}
void loop() {
  // Using the OPC command

  aOPCSerial.processOPCCommands();

  if (motion){
    digitalWrite(dir1, HIGH);
    digitalWrite(dir2, LOW);
  }
  else{
    digitalWrite(dir1, LOW);
    digitalWrite(dir2, HIGH);
  }
  int motorspeed=map(val2,0,10,0,255);
  val3=motorspeed;
  if(motorspeed>0){
    analogWrite(enA,val3);
  }
  else{
    analogWrite(enA, 0);
  }
}

```

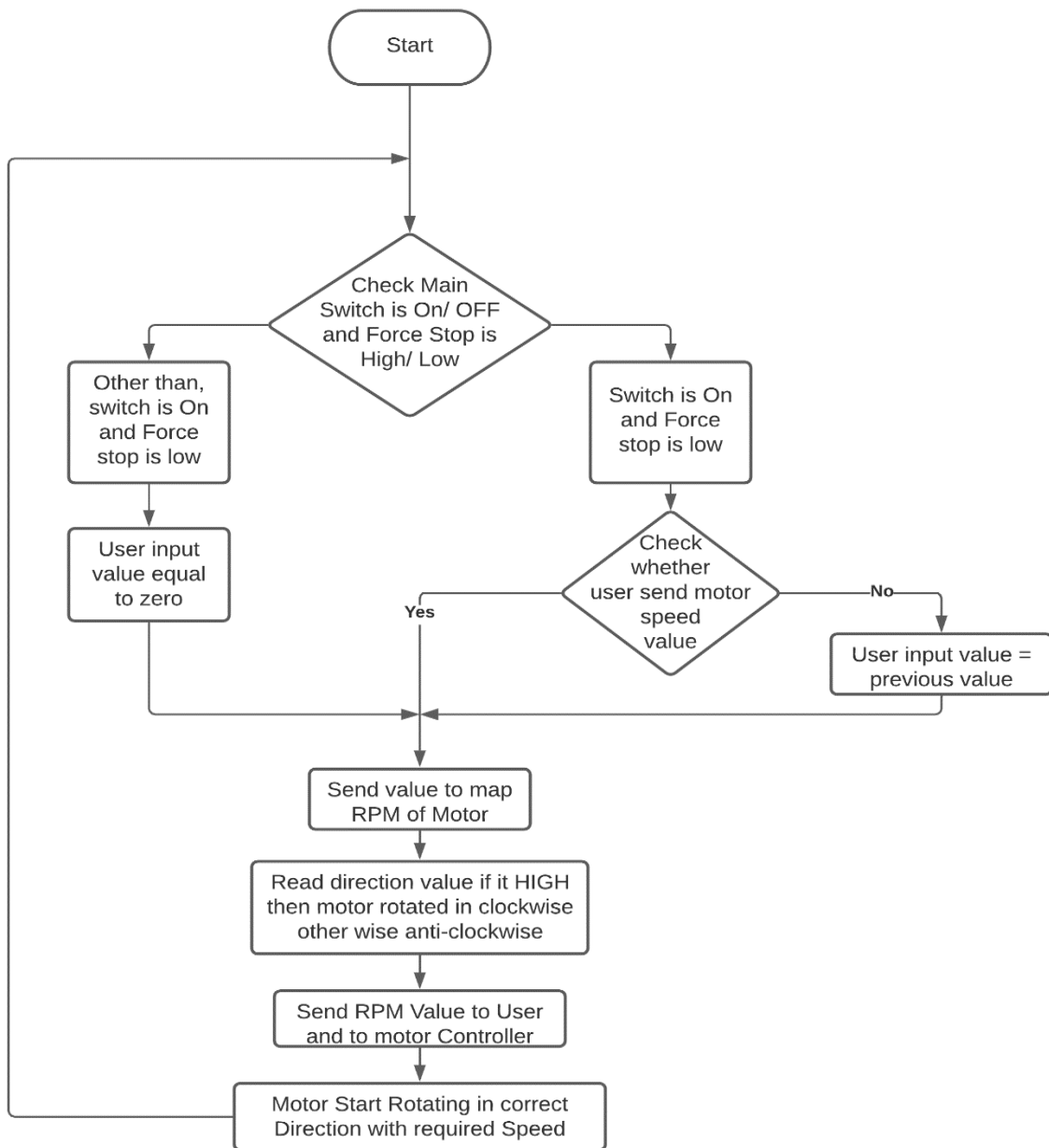


Figure 3.4 Flow chart of the program of the 3rd Unit.

Program of 3rd Unit

```

#include <OPC.h>
#include <Bridge.h>
#include <Ethernet.h>
#include <SPI.h>

```

```

// Declaring the OPC object

```

```
OPCSerial aOPCSerial;
```

```
// Set the status of the Led using the OPC Client.
```

```
int ledPin = 13;  
int enA=5;  
int val=0;  
int val1=0;  
int val2=0;  
int val3=0;  
int dir1=4;  
int dir2=3;
```

```
// For the OPCItem, formation of callback function
```

```
bool callback1(const char *item, const opcOperation opcOP, const bool value){  
    static bool ledval = false;
```

```
// Check for written command of OPC Client
```

```
if (opcOP == opc_opwrite) {  
    ledval = value;  
    if (ledval) {  
        digitalWrite(ledPin, HIGH);  
        val=1;}  
    else{  
        digitalWrite(ledPin, LOW);  
        val=0;}  
}  
else
```

```
// Find led state
```

```
    return ledval;  
}
```

```
// For Force stop of Motor 1
```

```
bool callback2(const char *item, const opcOperation opcOP, const bool value){  
    static bool force1 = false;  
    if (opcOP == opc_opwrite){  
        force1 = value;  
        if(force1){  
            val1=1;  
        }  
    }
```

```

        else{
            val1=0;
        }
    }
    return force1;
}
// For Motor 1
int callback3(const char *item, const opcOperation opcOP, const int value){
    if (opcOP == opc_opwrite) {
        val2 = value;
    }
    if (val==0 || val1==1){
        val2=0;
    }
    return val2;
}
// For RPM of Motor 1
int callback4(const char *item, const opcOperation opcOP, const int value){
    return val3;
}
void setup() {
    Serial.begin(57600);
    pinMode(ledPin, OUTPUT);
    pinMode(enA, OUTPUT);
    pinMode(dir1, OUTPUT);
    pinMode(dir2, OUTPUT);
    digitalWrite(dir1,HIGH);
    digitalWrite(dir2,LOW);

    // Configuration of OPC Objects
    aOPCSerial.setup();

    // Configuration of OPC Item

    aOPCSerial.addItem("led3-1",opc_readwrite, opc_bool, callback1);
    aOPCSerial.addItem("forcestop3-1",opc_readwrite, opc_bool, callback2);
    aOPCSerial.addItem("motor3-1",opc_readwrite, opc_int, callback3);
    aOPCSerial.addItem("rpm3-1",opc_readwrite, opc_int, callback4);
}

void loop() {

    // OPC process commands

```

```

aOPCSerial.processOPCCommands();
int motorspeed1=map(val2,0,10,0,255);
val3=motorspeed1;
analogWrite(enA,motorspeed1);
}

```

3.1.2 Network Architecture

The interconnection between the different components of the Remote access system for the Manufacturing Plant is depicted in figure 3.5.

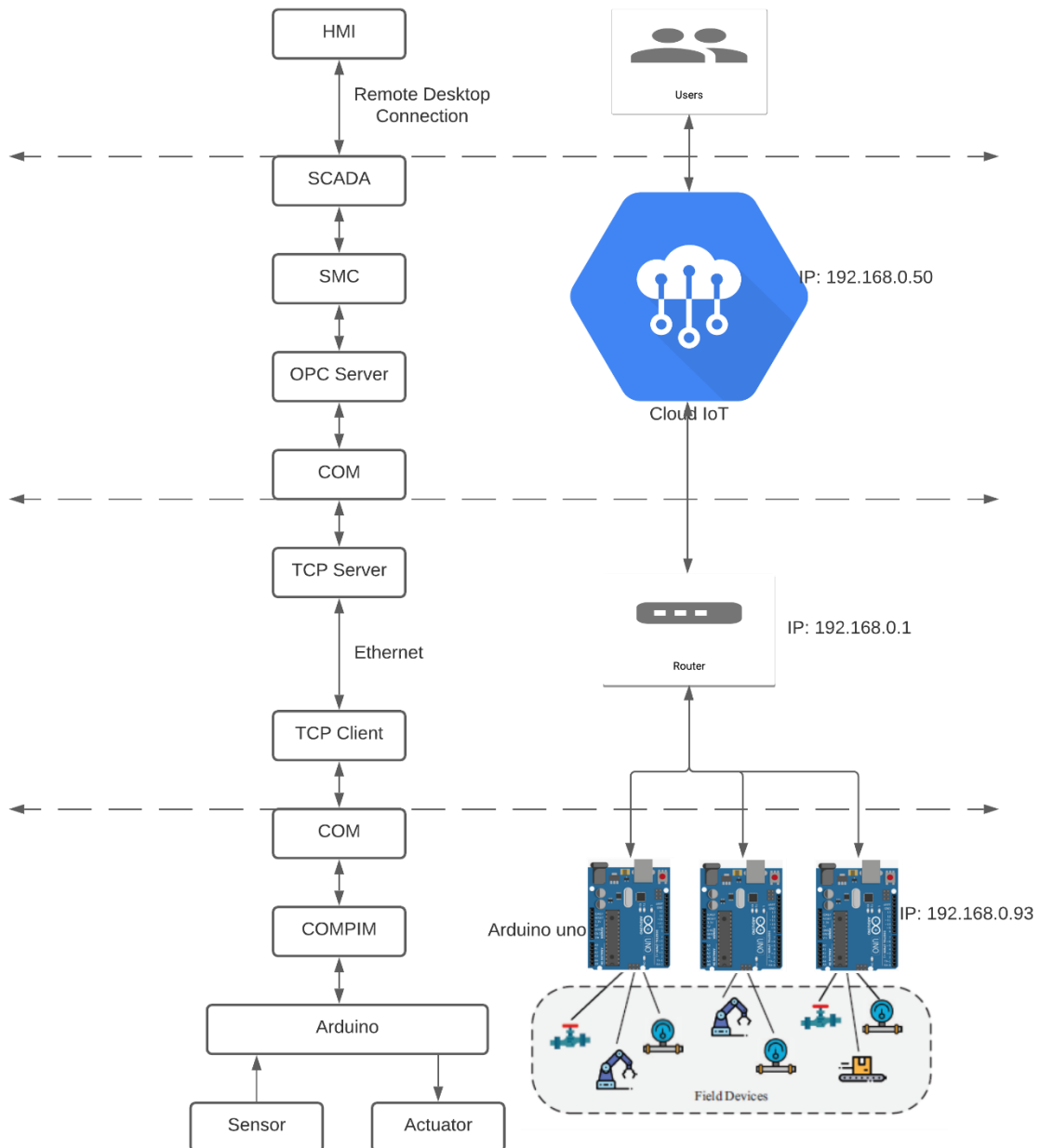


Figure 3.5 Remote access Network Architecture

The network is divided into four Sub-parts i.e., laptop which consists of Proteus, Router which connects different devices for data exchange, Cloud which consists of SCADA, and

HMI which helps users to interact with manufacturing plants. Ethernet can connect SCADA with Arduino, however, this solution requires a thorough understanding of such communication systems. To make it simple OPC server is used with the TCP/IP server-client model.

VSPE allows many apps to share physical serial port data while also exposing the serial port to a local network (via TCP protocol). So VSPE is used to connect the COM pin of the Laptop to the COM pin of the Cloud computing unit by creating a TCP client on the Laptop and TCP server on Cloud. Now both ports can exchange data. COM pin of Cloud is connected to OPC server which makes its data available to any device which is connected to OPC server. System Management Console (SMC) is a client which is connected with the OPC server via FS Gateway. FS Gateway is a communications protocol converter that runs as software. The FS Gateway connects clients and data sources that use different data access protocols. When SMC is activated, it starts communication with Intouch SCADA HMI. In this way, Intouch SCADA can communicate with Proteus. Now when the user gets connected to HMI (Cloud) via Remote Desktop Connection, the User has access to all data.

3.1.3 System Management Console (SMC)

System Management Console is a system-specific web application that lets you connect with the OPC server via FS Gateway. It simply established a connection between the OPC server present in the host or local node and SCADA (InTouch).

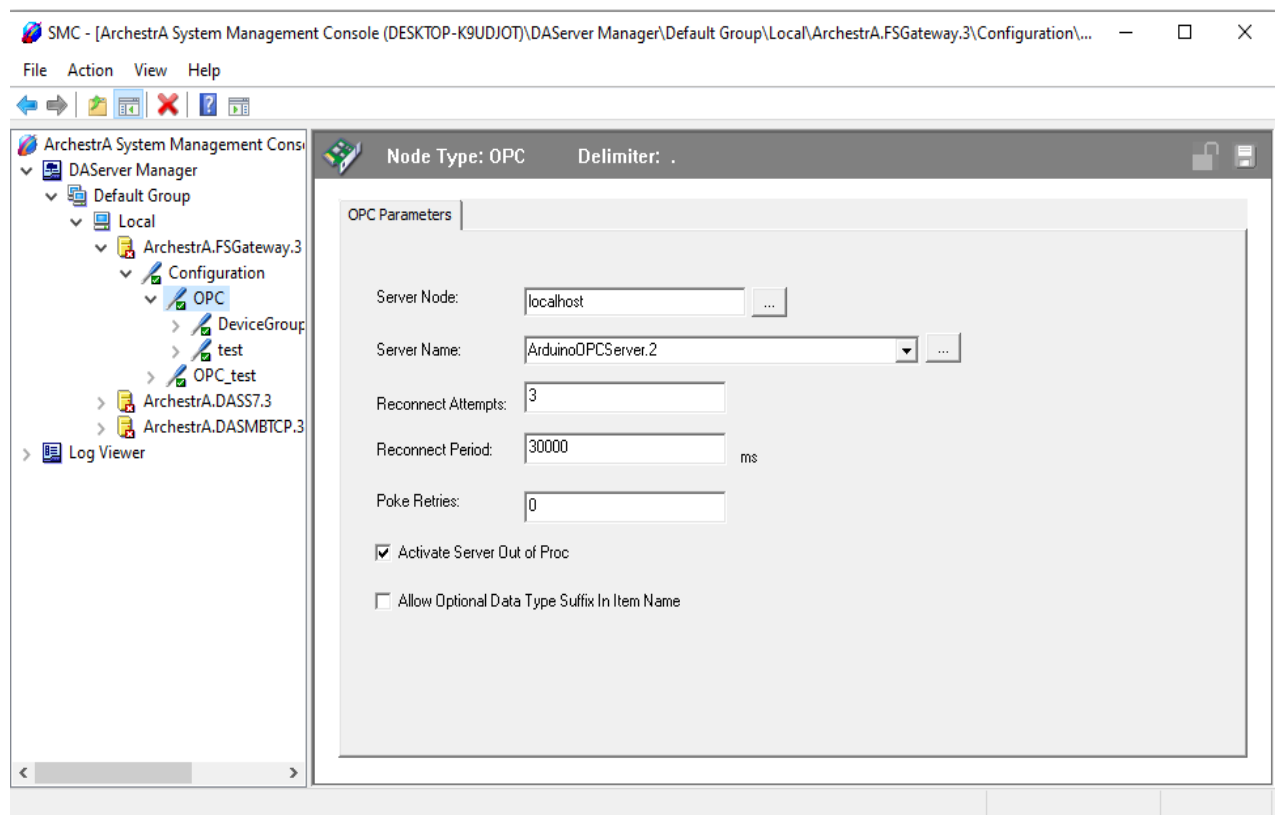


Figure 3.6 System Management Console

3.1.4 SCADA

SCADA stands for "Supervisory Control and Data Acquisition," and it's an integrated system for controlling and monitoring the plant's various components. In this project, PLC is replaced with Arduino Microcontroller to process a large amount of data and transfer it very fast to Cloud via Ethernet. 2-D animation of a small part of the Manufacturing Plant is designed in Intouch SCADA which mimics the motion and process of the Plant in real-time. When a user Observes HMI, it looks like an observing Manufacturing Plant.

In this model, there are three sections. To control each section there is a control panel. This control panel consists of Direction control button, Speed control button, Force stop button, and Digital display to show speed and gear. Direction button is used to change the direction of vertical motion for the Electric Press and both vertical and horizontal motion for the Drilling Machine. Speed button change Gear which varies from 0-10 corresponding to its speed change from 0-250 of the motor. The Force stop button is used when needed to stop a certain part of the Plant. In the control panel of the Conveyor Unit, there is no direction control button as it moves in the forward direction only. This Panel helps in manual control of the Plant. On the left side, there is a switch that is used to ON/OFF the Plant. It basically cut the power supply of the Plant. Temperature panel that shows the temperature of the Press machine and drilling machine. If the operation of the machine is not proper then the temperature starts rising, so by observing the temperature necessary action can be taken to reduce the temperature. To run the Plant in Automatic mode there is an Automatic button. By pressing it, every process of the plant takes place automatically. So, through SCADA Plant can be run in Manual as well as in Automatic mode. It is not possible to make any change in some products when the CNC machine is running. To make changes, the machine needs to stop, and the program should be modified. But in SCADA it is possible to make changes in some products when the Plant is running in Automatic mode without stopping or modifying the Program. If the response time of SCADA is reduced then it will be better than the CNC machine.

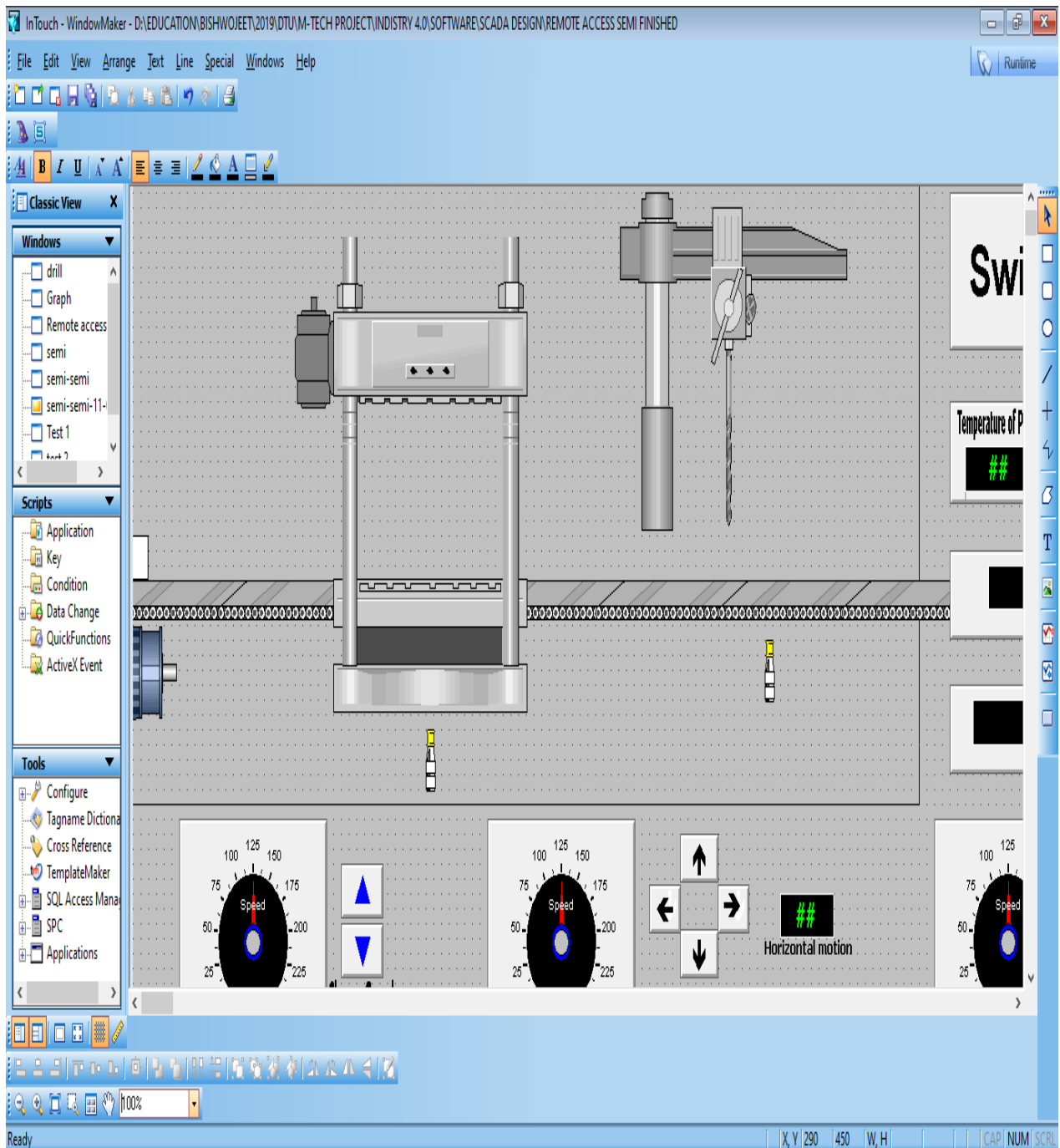


Figure 3.7 Intouch SCADA

For processing the Data to produce useful output programming is required. Programming in SCADA is known as Script. The programming type mainly used in SCADA is conditional base programming. The Script which is used in this Simulation is given below:

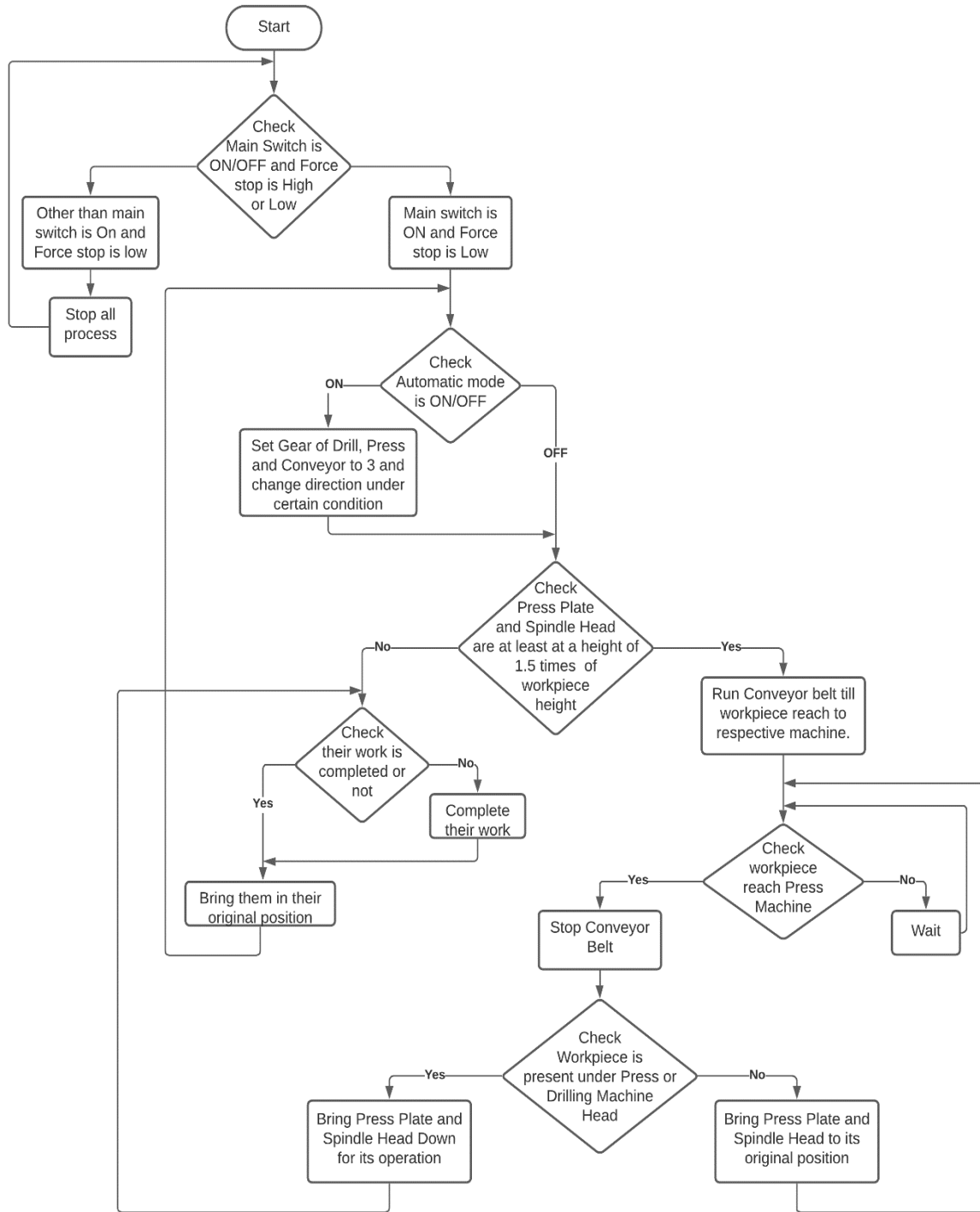


Figure 3.8 Flow Chart of SCADA Script

Script on Show:

l2=0;
 l1=0;
 l3=0;
 l4=0;
 a=0;

```
b=0;
l5=0;
l6=0;
l7=0;
c=5;
fs=0;
d=5;
e=5;
fs2=0; {for l5}
g=1; {for l5}
h=1; {for l6}
f=5; {for l6}
fs3=0;
fs4=0;
k=1;
l=1;
n=0;
motor1-1=0;
motor2-1=0;
motor3-1=0;
led1-1=0;
led2-1=0;
led3-1=0;
```

Script while showing, every 1 millisecond:

```
IF
mainswitch==1
THEN
led1-1=1;
led2-1=1;
led3-1=1;
IF
automatic==1
THEN
forcestop1-1=0; forcestop2-1=0; forcestop3-1=0;
{For press in automatic mode}
IF
l4==43 OR l5==43 OR l6==43
THEN
motor1-1=3;
IF
l1<=0 AND k==0
THEN
```

```

direction1-1=1;
k=1;
ELSE
IF I1>=100
THEN
direction1-1=0;
ENDIF;
ENDIF;
ELSE
direction1-1=0;
ENDIF;
{For Drill in Automatic mode}
IF
I4==86 OR I5==86 OR I6==86
THEN
motor2-1=3;
IF
I2<=0 AND I1==0
THEN
direction2-1=1;
a=1;
l=1;
ELSE
IF I2==100 AND I3<=0 AND n==1
THEN
n=2;
direction2-2=1;
ELSE
IF I2==100 AND I3>=100 AND n==2
THEN
a=1;
ELSE
IF I2==100 AND I3>=100 AND n==1
THEN
direction2-2=0;
n=2;
b=1;
ELSE
IF I2==100 AND I3<=0 AND n==2 AND b==1
THEN
direction2-1=0;
n=0;
b=0;
ENDIF;

```

```

ENDIF;
ENDIF;
ENDIF;
ENDIF;
ELSE
direction2-1=0;
ENDIF;
IF
{I1<=0 AND I2<100 AND } direction1-1==0 AND direction2-1==0
THEN
motor3-1=1;
k=0;
l=0;
ENDIF;
ENDIF;
{To stop conveyor Belt when press or drill operation take place}
IF
I1>79 OR I2>100
THEN
motor3-1=0;
ENDIF;
{For Press}
IF
direction1-1==1 AND I1<100 AND forcestop1-1==0
THEN
I1=I1+1 * motor1-1;
IF
I1<=80
THEN
c=5;
ELSE
IF I1>80 AND I1<=84
THEN
c=4;
ELSE
IF I1>84 AND I1<=88
THEN
c=3;
ELSE
IF I1>88 AND I1<=92
THEN
c=2;
ELSE
IF I1>92 AND I1<=96

```

```

THEN
c=1;
ELSE
IF l1>96 AND l1<=100
THEN
c=0;
ENDIF;
ENDIF;
ENDIF;
ENDIF;
ENDIF;
ENDIF;
ENDIF;
IF
direction1-1==0 AND l1>0 AND forcestop1-1==0
THEN
l1=l1 - 1 * motor1-1;
IF
l1<=80
THEN
c=5;
ELSE
IF l1>80 AND l1<=84
THEN
c=4;
ELSE
IF l1>84 AND l1<=88
THEN
c=3;
ELSE
IF l1>88 AND l1<=92
THEN
c=2;
ELSE
IF l1>92 AND l1<=96
THEN
c=1;
ELSE
IF l1>96 AND l1<=100
THEN
c=0;
ENDIF;
ENDIF;
ENDIF;

```

```

ENDIF;
ENDIF;
ENDIF;
{For Drill}
IF
direction2-1==1 AND l2<100 AND forcestop2-1==0
THEN
l2=l2+1 * motor2-1;
ENDIF;
IF
direction2-1==0 AND l2>0 AND forcestop2-1==0
THEN
l2=l2 - 1 * motor2-1;
ENDIF;
IF
direction2-2==1 AND l3<100 AND forcestop2-1==0
THEN
l3=l3+1 * motor2-1;
ENDIF;
IF
direction2-2==0 AND l3>0 AND forcestop2-1==0
THEN
l3=l3 - 1 * motor2-1;
ENDIF;
{For Drill bit}
IF
direction2-1==1 AND l2>=100 AND forcestop2-1==0 AND a==1
THEN
l2=l2+1 * motor2-1;
IF
l2>=120
THEN
a=0;
n=1;
ENDIF;
ENDIF;
IF
direction2-1==1 AND l2>100 AND forcestop2-1==0 AND a==0
THEN
IF
l2 - 1 * motor2-1 <=100
THEN
l2=100;
ELSE

```

```

l2=l2 - 1 * motor2-1;
ENDIF;
ENDIF;
{For 1st conveyer belt}
IF
h==0
THEN
IF
forcestop3-1==0
THEN
l6=l6+1 * motor3-1;
IF
l6>=43 AND fs3==0
THEN
l6=43;
fs3=1;
l4=0;
i=1;
fs=0;
d=5;
ELSE
IF
l6>=110 AND fs3==2
THEN
fs3=3;
f=5;
ENDIF;
ENDIF;
ENDIF;
IF
l6==43 AND f>=c
THEN
f=c;
ENDIF;
ENDIF;
ENDIF;
IF
g==0
THEN
IF
forcestop3-1==0
THEN
l5=l5+1 * motor3-1;
IF
l5>=43 AND fs2==0

```

```

THEN
l5=43;
fs2=1;
h=0;
fs3=0;
l6=0;
f=5;
ELSE
IF
l5>=110 AND fs2==2
THEN
fs2=3;
e=5;
ENDIF;
ENDIF;
IF
l5==43 AND e>=c
THEN
e=c;
ENDIF;
ENDIF;
ENDIF;
IF
i==0
THEN
IF
forcestop3-1==0
THEN
l4=l4+1 * motor3-1;
IF
l4>=43 AND fs==0
THEN
l4=43;
fs=1;
g=0;
l5=0;
fs2=0;
e=5;
ELSE
IF
l4>=110 AND fs==2
THEN
fs=3;
d=5;

```



```

ENDIF;
ENDIF;
IF
l4==43 AND d>=c
THEN
d=c;
ENDIF;
ENDIF;
ENDIF;
IF
forcestop3-1==0
THEN
l7=l7+1 * motor3-1;
IF
l7>=43 AND fs4==0
THEN
motor3-1=0;
l7=43;
fs4=1;
ELSE
IF l7>=86 AND fs4==1
THEN
motor3-1=0;
l7=86;
fs4=2;
ELSE
IF
l7>=129 AND fs4==2
THEN
motor3-1=0;
l7=0;
fs4=0;
i=0;
ENDIF;
ENDIF;
ENDIF;
ENDIF;
ELSE
led1-1=0;
led2-1=0;
led3-1=0;
ENDIF;

```

3.1.5 Database entries used in "Remote Access System":

a
automatic
b
c
d
direction1-1
direction2-1
direction2-2
e
f
forcestop1-1
forcestop2-1
forcestop3-1
fs
fs2
fs3
fs4
g
graph
h
i
k
l
l1
l2
l3
l4
l5
l6
l7
led1-1
led2-1
led3-1
mainswitch
motor1-1
motor2-1
motor3-1
n
rpm1-1
rpm2-1
rpm3-1
temp2-1

3.1.6 Remote access HMI

A Human-Machine Interface (HMI) is a user interface or dashboard that connects a human to a machine, system, or device (HMI). While a human-machine interface (HMI) can theoretically refer to any screen that allows a user to communicate with a device, it is most often linked with industrial processes.

When SCADA is in Runtime, we get a screen through which we can monitor and control the machine. It is a screen through which the user can interact with the machine. In this project when a User login into the Remote Desktop connection app using IP address, User-id, and Password. Users see an interface that is an Intouch HMI. Through this HMI users can monitor and control the manufacturing plant from any place of the world. The user only required internet access and login details.

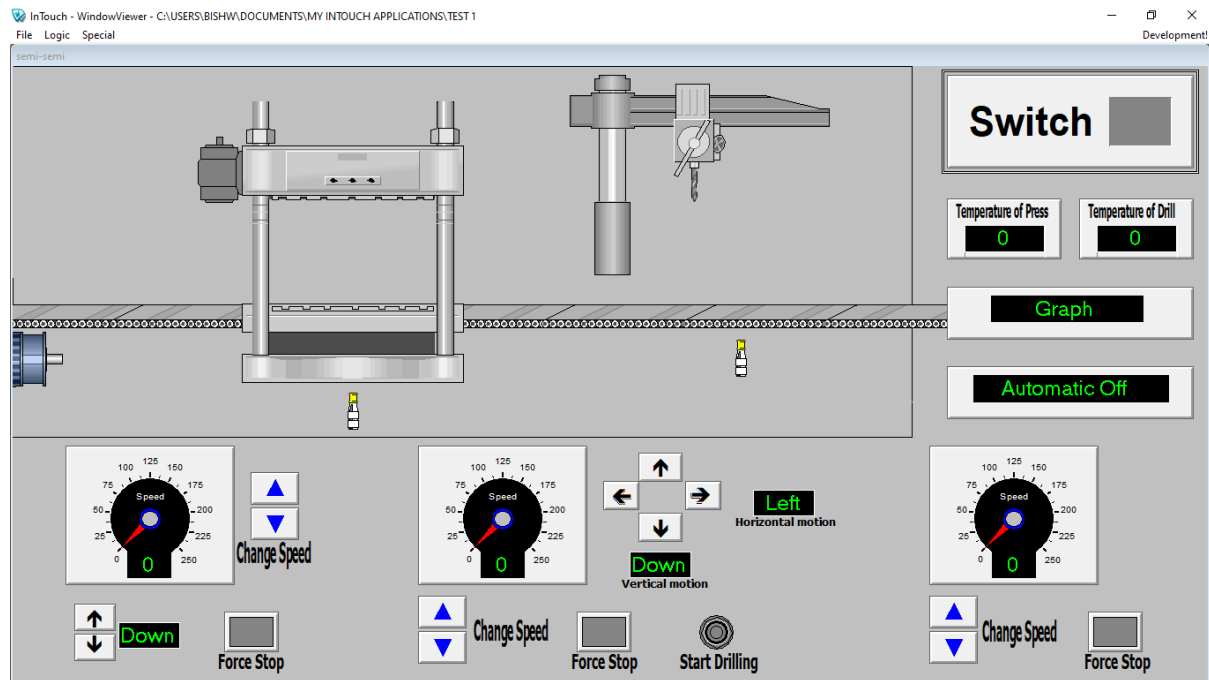


Figure 3.9 Human Machine Interface (HMI)

3.2 Configuration Step

1. Open Virtual Serial Ports Emulator (VSPE) and add three COM Ports as COM1, COM2, and COM3 from Create a New Device. After adding, these COM ports start the emulator.
2. Open Arduino IDE and copy the link of the .hex file of each unit.
3. Open Proteus and add the .hex file to Arduino of the respected unit. After it, run the simulation.
4. Open Virtual Serial Ports Emulator (VSPE) in Cloud server (**in this project we have taken another Laptop as Cloud which can be accessed from any place**) and add

three COM Ports as COM1, COM2, and COM3 from Create a New Device. Create 3 TCP/IP servers from this COM port. After this starts the emulator.

5. Again, open VSPE on the Laptop which has a proteus. Using TCP host and TCP port of server create TCP/IP client with initial COM port. Now the COM Port of both laptops is connected.
6. Open Arduino OPC server in Cloud. Go to configuration and add 3 Arduino Serials. In each serial select the respected COM port. Save the Configuration.
7. Run register file as administrator. Now an Arduino OPC server is created which will be visible to every device within the same Domain.
8. Open System Management Console and go to DA Server Manager>Default Group>Local>ArchestrA.FSGateway.3>Configuration>OPC. Select Server name as ArduinoOPCServer.2. Save the changes.
9. Go to Device Group and Browse OPC items. You will see the name of the device which is used in Proteus (Plant). Save the device name. Save the changes.
10. Click on ArchestrA.FSGateway.3. Now activate the server. In this way data from Proteus reaches SCADA via Arduino OPC server.
11. Open Intouch and open the remote access file.
12. Click on Runtime. Now HMI will open.
13. User Go to Remote Desktop connection from his/her system. Enter IP address, User-id, and Password of Cloud server. In this project, the IP address of the Cloud is 192.168.1.93.
14. When the user enters the correct detail, the HMI of SCADA opens.
15. Now the user can monitor and control the Plant from this system from any place of the world.

3.3 Issue while implementing this model in the Real Manufacturing Plant

The Simulation model successfully demonstrated the working of the Remote access system. Any person with a valid IP address, User name, and Password can access the HMI of simulation, and Monitor and Control Proteus manufacturing model. But the method, device, and connection process which we use here are not be effecting, efficient, and safe to use in a real manufacturing plant due to the following reason:

- Data transfer rate is low.
- Latency is high.
- 3 Protocols are combined to establish Communication between SCADA and Microcontroller which make complex data transmission systems.
- Weak security system.
- Huge amount of data is processed without using Big Data Analysis so redundancy in the process is High.

3.4 Issue related to the implementation of SCADA in Today World for Remote access systems

Since 1970 SCADA has been used in different industries for monitoring and controlling critical equipment or processes. Before 1996, the SCADA system operated on an isolated network. So, any person outside the network can't access SCADA. The SCADA system is safe from many vulnerabilities. As the use of SCADA increases complex networks are required. To fulfill this requirement SCADA network is connected to the Internet. SCADA gets all the facilities which other systems enjoy with the internet along with risk. Cyber-attacks possess a greater threat to the SCADA system than that to the IT system [20]. As in SCADA, the lives of living beings are at risk whereas in IT systems data are at risk. So, there are certain issues in the implementation of SCADA in today world which are given below:

3.4.1 Cyber Attack

Many authors' SCADA reports suggest an uptick in security incidents and cyber-attacks against important SCADA systems [6], [9]. Security considerations for SCADA systems are given higher priority and consideration than those for normal IT systems because of the potential threat to the physical safety of personnel, customers, or communities. Internal and external cyber-related incidents, Denial of Service (DoS) assaults, virus/worm infiltrations, remote access attacks, and any other cyber-related incident that has an impact on the process environment are all included in RISI. A list of high-impact SCADA security [10], [11], [12], [13], [14], [15], [16], [17], [18], [19] incidents is provided in Table 3.1.

Table 3.1 Cyber Attack on SCADA System

Name	Method	Results	Year
Maroochy Water System	User Compromise	Operation disruption	2000
Davis-Besse Nuclear Power Plant	Worm	Network disruption	2003
Tehama Colusa Canal Authority	User Compromise	-	2007
Dallas Carrell Clinic	User compromise	HVAC Equipment disruption	2009
Stuxnet	Worm, Root Compromise, Trojan	Disruption of operations, Equipment destruction	2010
Night Dragon	Social Engineering, User Compromise, Root Compromise, Spear	Unauthorized access to control and information systems	2011

	Phishing, Windows-based Exploits		
Aramco	Virus	Service Disruption, Cyber Espionage	2012
Dragonfly Campaign	Worm, Trojans, Backdoors, Spear Phishing	Cyber Espionage	2014
Ukrainian Power Grid	User Compromise, Trojan, Worm	Service Disruption	2016
Dragonfly 2.0	Phishing, Malicious email attachments, Trojan	Cyber espionage, Equipment Destruction, Unauthorized information disclosure	2017
Saipem Company	Virus	Service disruption	2018
Colonial Pipeline	Ransomware	Data Stolen, Operation stops	2021

Note: Adapted from Journal, Dimitrios Pliatsios et al. pp 1942 – 1976, 2020. Copyright 2020 by IEEE

3.4.2 Improper Protocol

Protocol is a set of rules used to establish effective communication between two devices. It tells in which format data should be transferred/ received. So, Protocol is an important tool to stop an unauthentic person from entry to the system. Common computer protocols and capabilities, such as file transfer across the network and remote access, are frequently used in SCADA systems [21]. An attacker can get sensitive information by intercepting unencrypted data transmission. Furthermore, certain open network ports are required for system applications and services. An attacker could utilize such ports to obtain access to the SCADA system, collect data, and get administrative access. Furthermore, the attacker can upload malicious code to gain unauthorized access by exploiting a vulnerable program [22]. Security awareness was not taken into account during the creation of the initial SCADA systems because they were isolated from other systems. Newer SCADA systems, on the other hand, can communicate with other networks. As a result, a communication network attack can swiftly escalate into a full-fledged attack on the SCADA system. The vulnerabilities of SCADA communication protocols have been investigated and analyzed in several research. Table 3.2 summarizes several protocol shortcomings that make it vulnerable to cyber threats [10], [11], [12]. Authentication Control is used to authenticate network devices, while encryption techniques are used to encrypt data before it is transmitted over the communication channel. The integrity check ensures that messages are received in the same state as when they were sent. The Anti-replay Mechanisms stop attackers from sending harmful communication into the network that looks like legitimate traffic.

Table 3.2 Protocol Vulnerabilities for SCADA

Protocol	Authentication Control	Encryption Techniques	Integrity Check	Anti-replay Mechanisms
Distributed Network Protocol 3	Not available	Not available	Not available	Not available
Common Industrial Protocol	Not available	Not available	Not available	Not available
Foundation HSE	Not available	Not available	Available	Not available
Foundation Fieldbus H1	Not available	Not available	Not available	Not available
Modbus	Not available	Not available	Available	Not available
IEC 61850	Available	Not available	Not available	Not available
SERCOS III	Available	Not available	Available	Not available
PROFINET	Available	Available	Available	Not available

Note: Adapted from Journal, Dimitrios Pliatsios et al. pp 1942 – 1976, 2020. Copyright 2020 by IEEE

3.4.3 Specific components

SCADA systems have been adopting technology utilized in ordinary computer systems in recent years. Microcontrollers and electronic devices, for example, have replaced relays and mechanical devices, respectively, while operating systems have been integrated into SCADA systems. As a result, SCADA systems have inherited the flaws of traditional computer systems. Furthermore, the chance of implementation problems increases as software becomes more complex. One of the most significant obstacles is the lack of established security technologies that are customized to the needs of SCADA systems [3].

As IoT devices are mostly made up of small sensors with limited computational power and bandwidth, they have a significant resource restriction. This renders the use of advanced encryption and dependability techniques impossible. The recent Mirai malware-based Denial of Service attack on IoT devices highlighted the fragility of the technology and the urgent need to protect against such attacks [7].

3.5 Issues and Challenges of Remote access system

The discovery of new Technology brings four Industry revolutions, from the mechanical system to a highly automated system that is required for dynamic market

requirements and demands. Development of infrastructure of Industry 4.0 helps in the implementation of a Remote access system. For this, different issues and challenges need to be overcome such as scientific and technological challenges, economic challenges, social and political issues, geographical problems.

Some of the challenges and fundamental issues occur during the implementation of Remote access system in the current manufacturing plant are given below:

1. The development of smart devices: Device in industry 4.0 is intelligent which interacts with the environment and performs its operation. It can reconfigure itself when required. So, such smart devices need to be developed which fulfill the requirement of a Remote access system. [23].
2. Construction of the network environment: The network in Industry 4.0 mainly consists of CPS and IoT. This network should support the collection and transformation of data between different components at a very fast rate. So, the construction of such a network all over the country is an issue. 5G technology may be the solution to it [23].
3. Big data analysis and processing: All the components such as machine, product, equipment, tools, processing unit, etc. generated data continuously in a Remote access system. A huge amount of data is collected by cloud computing services. To optimize the process and to make a meaningful full decision analysis of data in a short time is necessary. So, such mechanisms need to develop [23].
4. Intelligent Decision-Making and Negotiation Mechanism: In a smart manufacturing system decentralized control system is followed. For this, every unit should be capable of making its own decision. So, such an intelligent mechanism needs to be developed [24].
5. Cyber Security: In Industry 4.0 the whole system is connected to the cloud server which may be accessed by other people. So, to protect such unauthorized access, data, and research, a secure mechanism should form [24]. Many attacks take place on the cyber system daily. So, such a mechanism should be developed which can save the system as well as enable fast data transmission.

3.6 Industry 4.0 based solution to the implementation of Remote access system

As a Remote access system seen as effective and efficient from the simulation model. But there are many issues associated with this integrated technology. Without solving this issue proper implementation of a Remote access system is not possible. The solution to this issue is the development of technology, some of them are developed while some are under developing process. Some of them are given below:

3.6.1 Intelligent Sensors

The integration of sensors and actuators with a processor, memory, storage, microcontroller, and communication module which can collect, process, and communicate the sensor data is known as an Intelligent Sensor. Customizations of embedded algorithms to individual applications are possible due to the intelligent sensor structure in an application;

additionally, customization can be accomplished by reprogramming the flash memory. As a result, a sensor, a compact microcontroller, memory, and a sensor-optimized architecture have been created. In the Remote access system, data is collected from the environment via sensors. The sensor processes the data and sends meaningful information to the server. After processing the data by the server, it sends instructions to the sensor to actuate certain processes. So real-time monitoring and collecting of data take place [25]. So, such sensors should be developed.

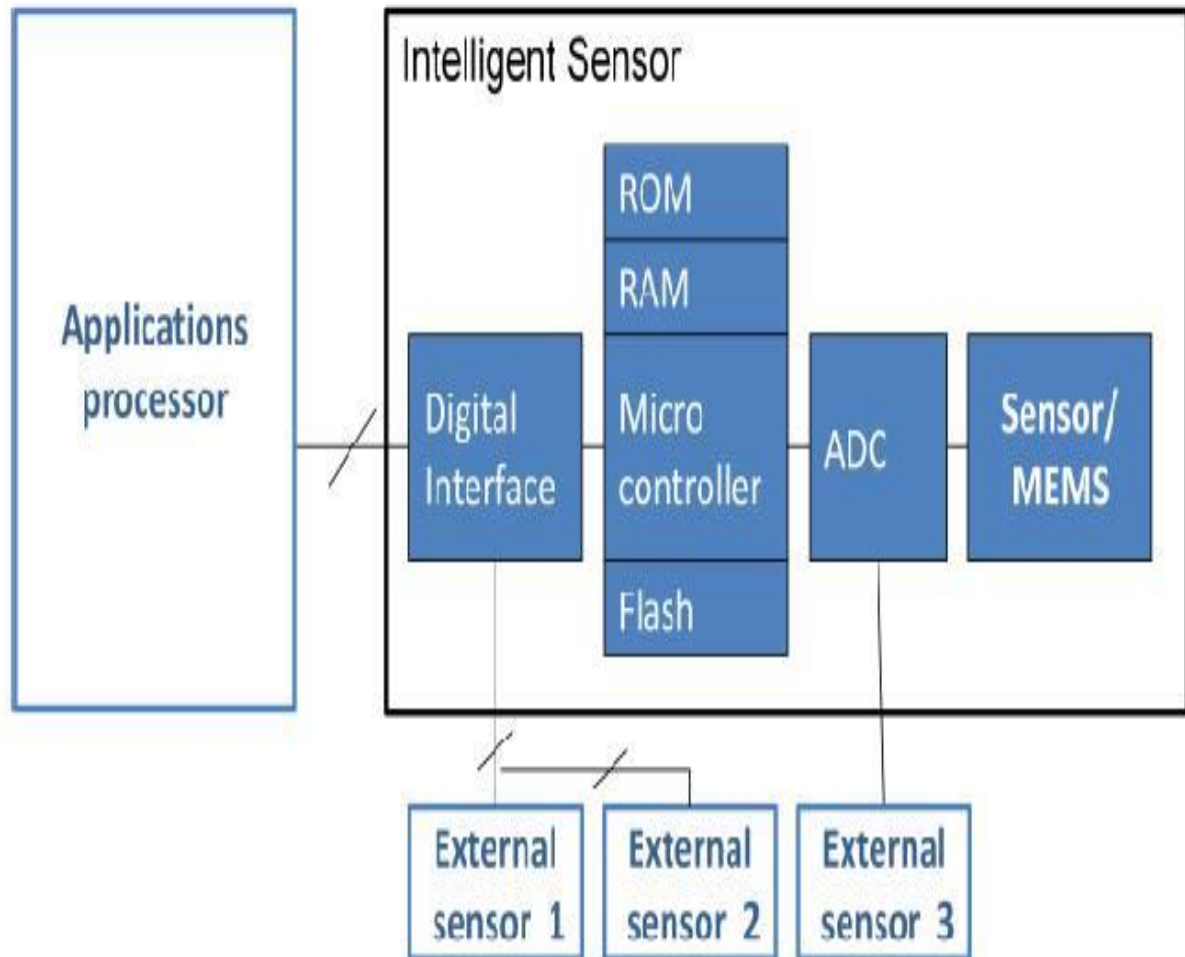


Figure 3.10 Intelligent Sensor

3.6.2 Development of Cyber-Physical Systems (CPS) and Cybersecurity

CPS is the integration of an Embedded system and Physical system. Embedded systems possess compute communication, and control capabilities to interact with the physical world through sensors and actuators. CPS enables the communication of Human to Machine, Machine to Machine (M2M), and Machine to Human [26]. The continuous interchanging of data is carried out between the systems linked through CPS with the help of a cloud system in real-time. In manufacturing, CPS enables the intelligent creation of autonomous productive processes based on double representation: components can decide on their configuration and path in the production line using communication and decision algorithms. The 5C architecture

i.e., connection, conversion, cyber, cognition, and configuration of Industry 4.0 can be achieved through the Cyber-Physical system [27].

As a result of Industry 4.0's increased connectivity and adoption of standard communication protocols, the requirement to secure vital industrial systems and manufacturing lines against cybersecurity assaults is fast growing. As a result, secure, dependable communications, as well as advanced machine and user identity and access control, are critical. CPS will provide better security to the manufacturing plant in the Remote access system.

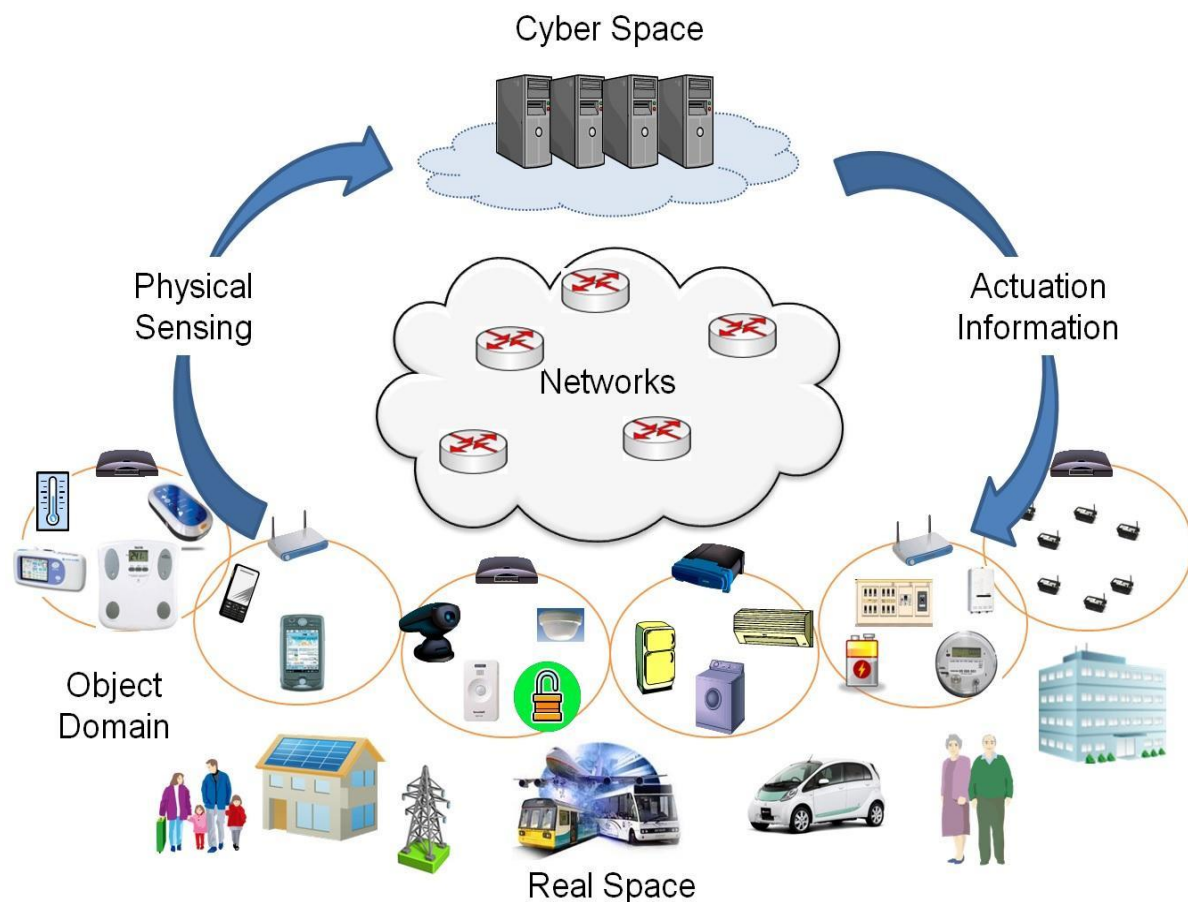


Figure 3.11 Cyber-Physical System

3.6.3 Big Data and Analytics

Remote access systems have many sensors and microprocessors, which generate data continuously. Collecting and evaluating this data by a traditional method is not possible. Manufacturing firms must manage a wide range of data, including production data, operational data, value chain data, and external data, as well as vast amounts of structured and unstructured data. Companies will need to accept individual tailored data from the Web in real-time as part of Industry 4.0, which also manages additional sorts of relevant data. Big data technology employs novel processing modes to extract useful information from a variety of data sources quickly, allowing for in-depth analysis, insight, and discovery in order to make appropriate

decisions. Manufacturing firms will profit from big data analysis in a variety of ways, including process optimization, cost reduction, and improved operational efficiencies [28].



Figure 3.12 Big Data Analysis

3.6.4 Cloud Computing

Cloud computing is a platform for storing and processing data in one place which can be accessed from any place with any device. Cloud computing, in terms of remote access systems, is the concept of connecting many devices to the same cloud in order to share information, and it can be extended to a group of machines on a shop floor as well as the entire plant. A large amount of data needs to be shared at a very fast rate between different devices which is possible through cloud computing [24]. The cloud computing approach makes software, hardware, platforms, and other IT infrastructure resources available to users as needed. The user merely consumes resources as needed by the application, relying on on-demand computer and storage infrastructure [28].

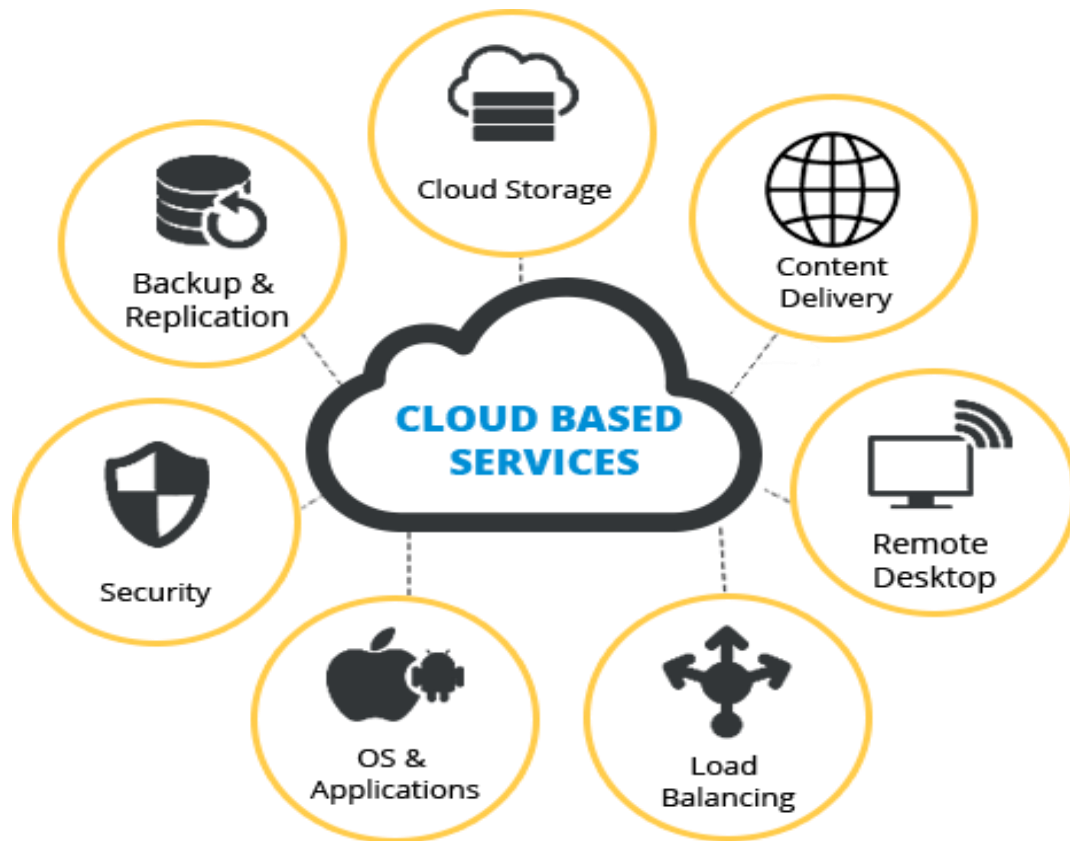


Figure 3.13 Cloud Computing

3.6.5 Industrial Internet of Things (IIoT)

The Internet of Things (IoT) is a global network of interconnected and universally addressed devices that communicate via industry standard protocols. The three key features of IoT are context, omnipresence, and optimization. Context refers to the possibility of advanced object interaction with an existing environment and immediate response if anything changes, omnipresence provides information on an object's location, physical or atmospheric conditions, and optimization demonstrates how today's objects are more than just connected to a network [24]. The use of the Internet and the Internet of Things for human-machine interactions enables intelligent production and brings the fourth revolution. IIoT provides remote access to design, manufacture, and manage the industrialization process owing to its computing power and storage capacity. RFID devices, infrared sensors, global positioning systems, laser scanners, and other information sensing devices and other arbitrary objects that can be connected to the Internet via an agreed-upon protocol for data transmission and communication to achieve intelligent identification, tracking, monitoring, and management are descriptions of the Internet of Things [28].

Chapter 4: RESULTS AND DISCUSSION

4.1 Results

The Remote Access system is successfully deployed in the simulation model and the manufacturing unit (1st Computer in which the manufacturing unit is designed in Proteus) established successfully communicated with the cloud computing unit (2nd Computer in which the computing unit is designed in Intouch SCADA). The following figure shows the implementation of the Remote Access System in the Simulation model.

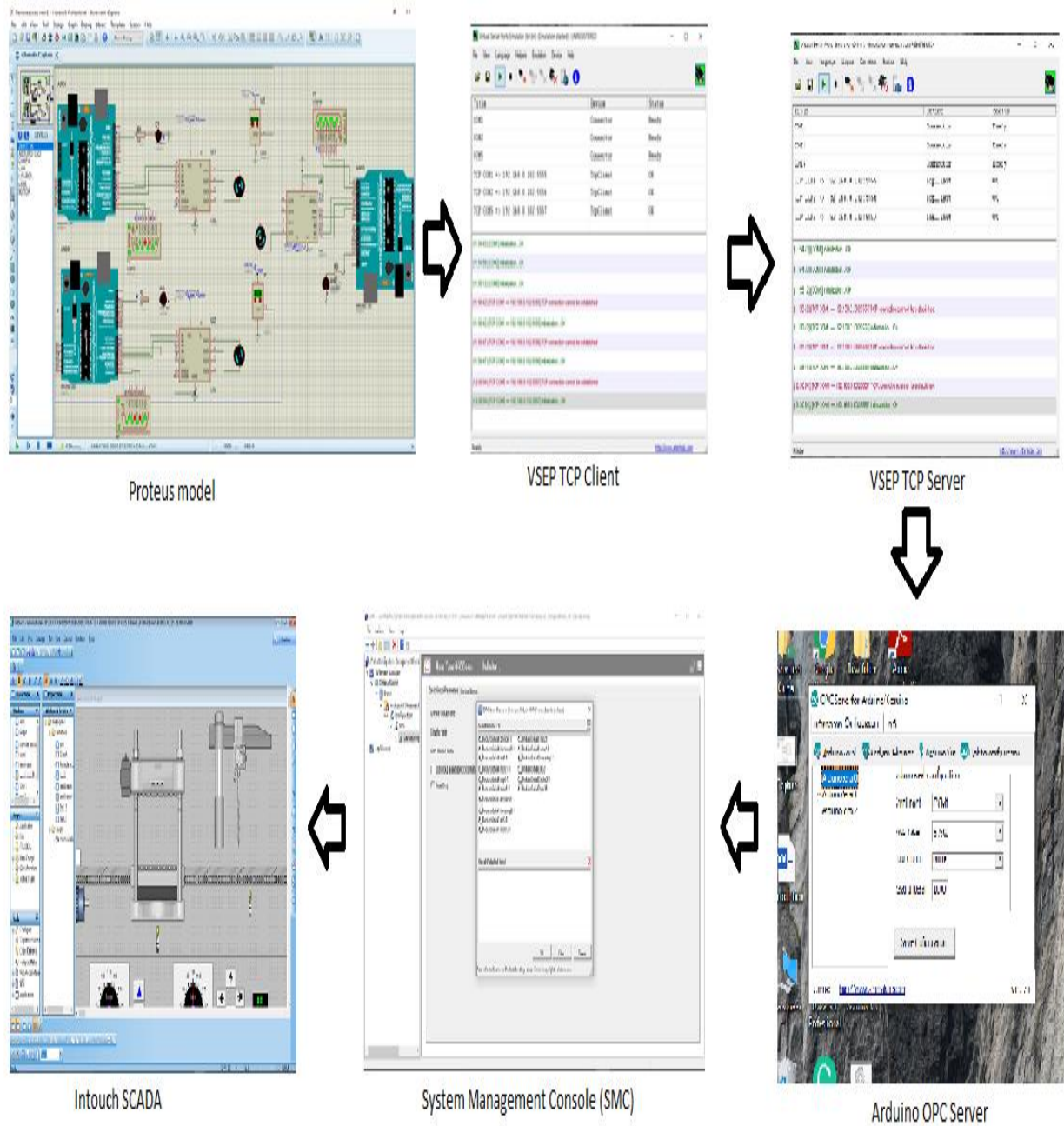
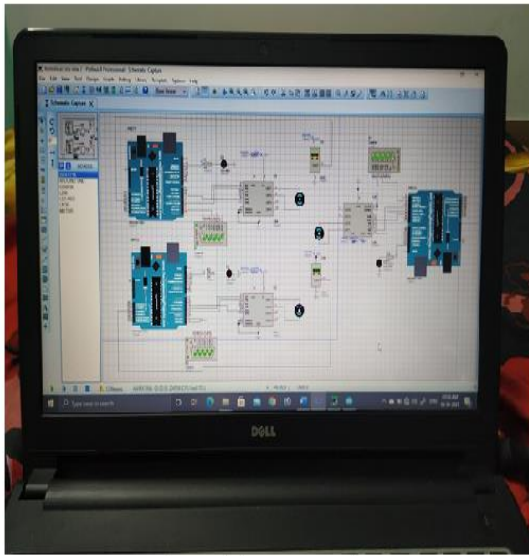
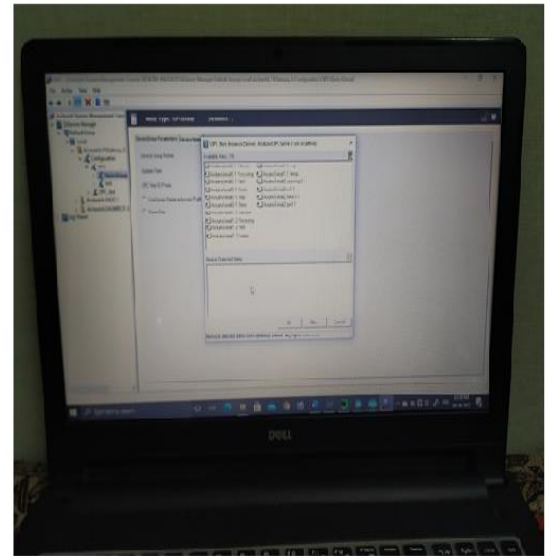
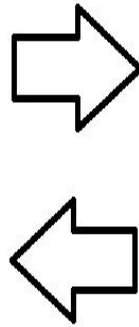


Figure 4.1 Connection between Simulation Model



Plant Unit (1st Computer)



Computing Unit (2nd Computer)

Figure 4.2 Successfully establishing connection between Plant Unit and Computing Unit

Using the Remote Desktop connection feature of Windows from 3rd computer users can access the HMI of SCADA using the IP address of the Cloud computing unit (2nd Computer), User-Id, and Password. Users can view and make changes in HMI which are on the 2nd computer.

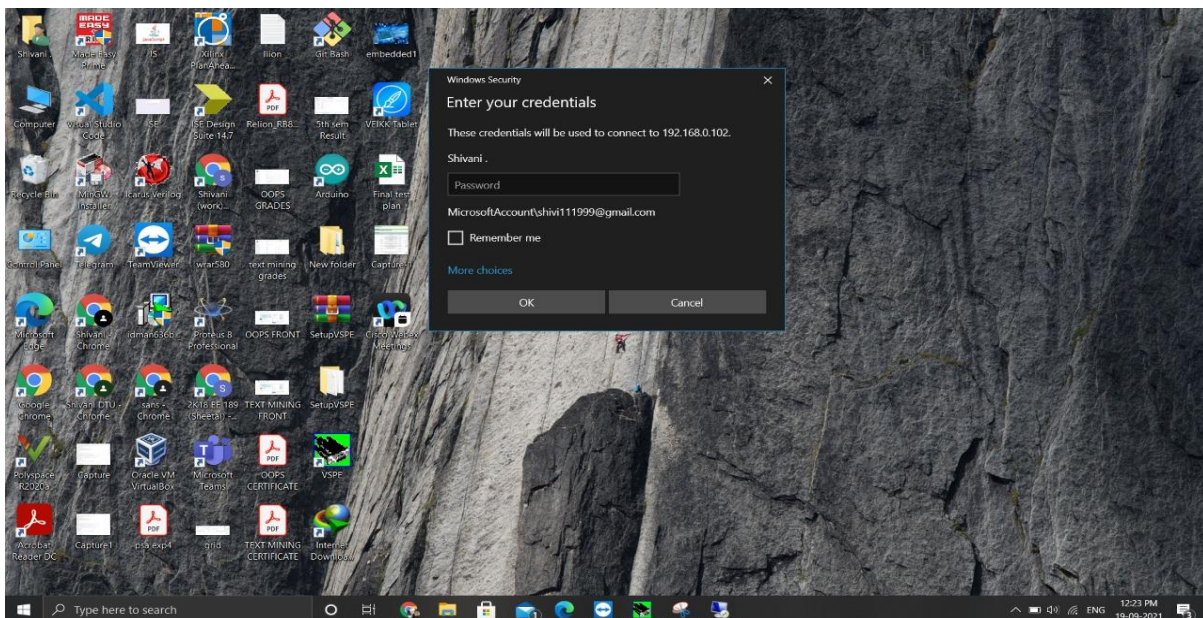


Figure 4.3 Connecting HMI (2nd computer) through Remote Desktop Connection (3rd computer)

Users can control the operation of the manufacturing plant which is running in Proteus (1st Computer) through HMI of SCADA (running in 2nd computer) using 3rd computer.

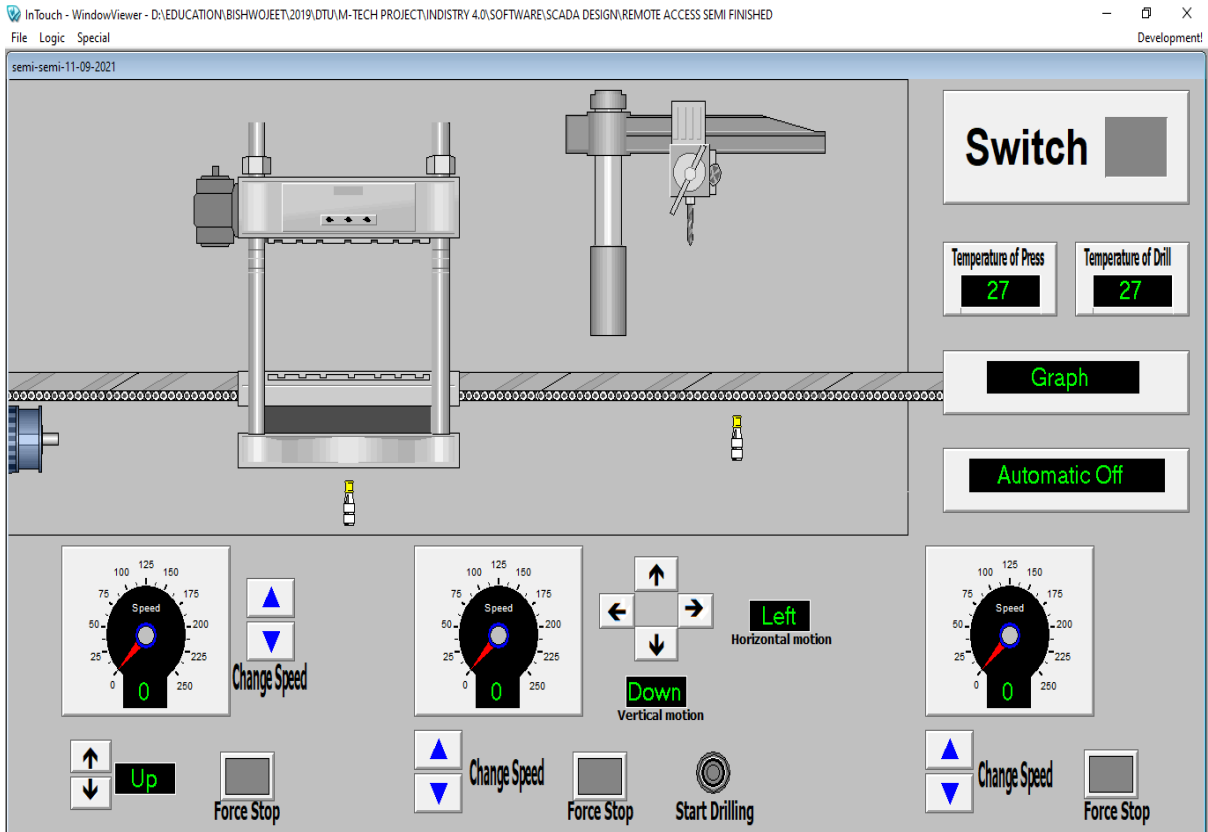


Figure 4.4 HMI view when Main switch OFF

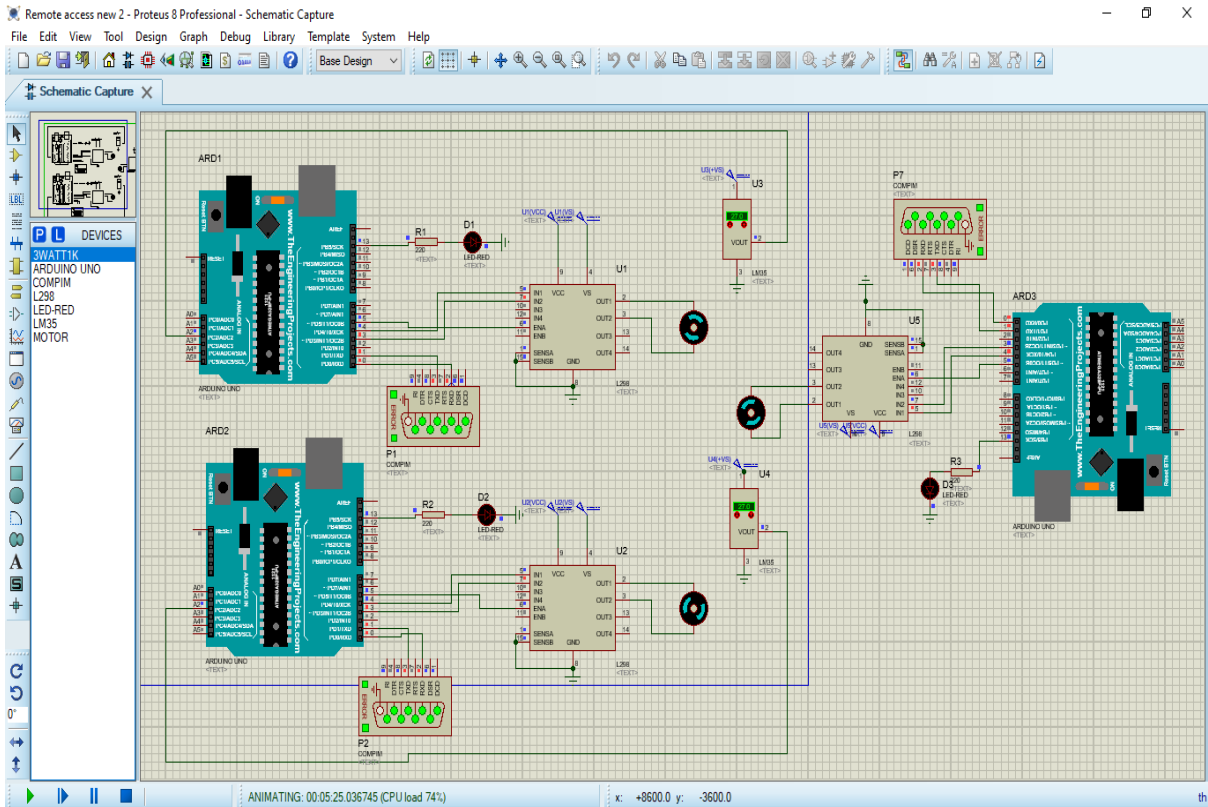


Figure 4.5 Proteus view when Main switch OFF

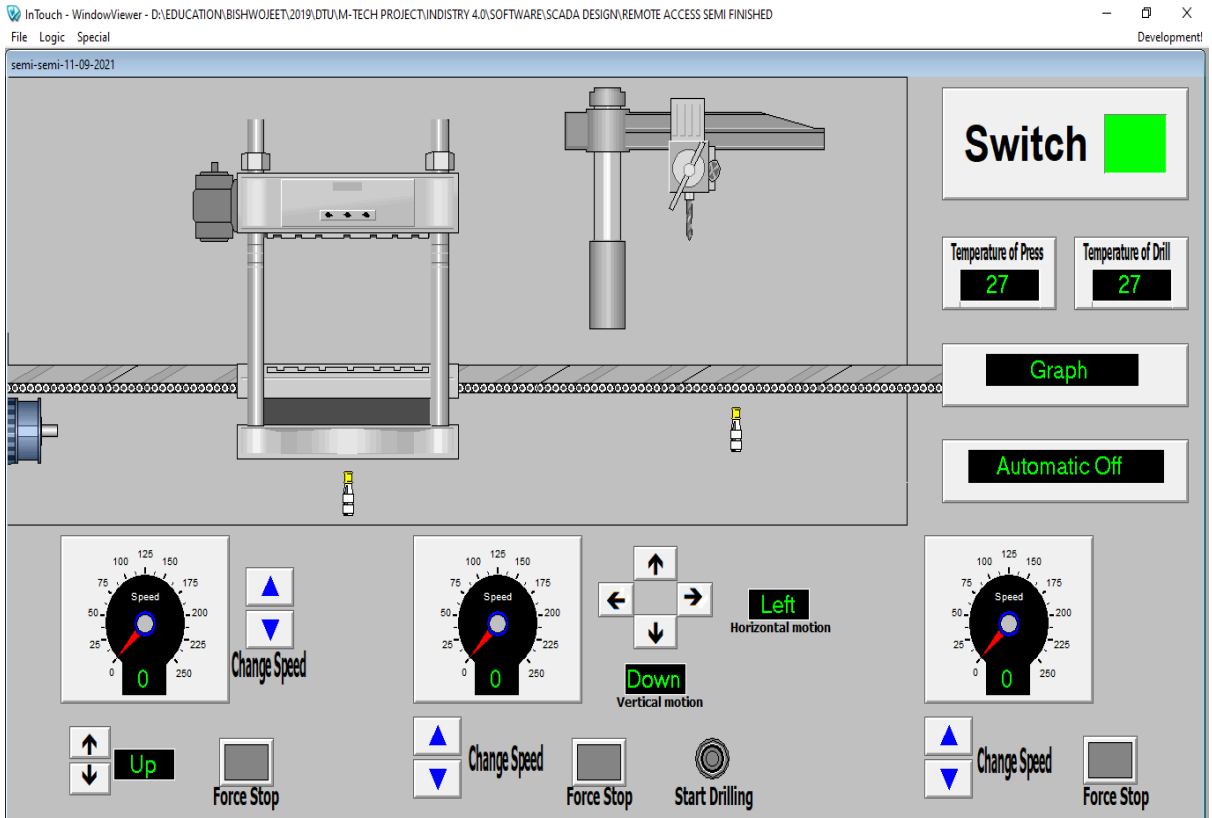


Figure 4.6 HMI view when Main switch ON

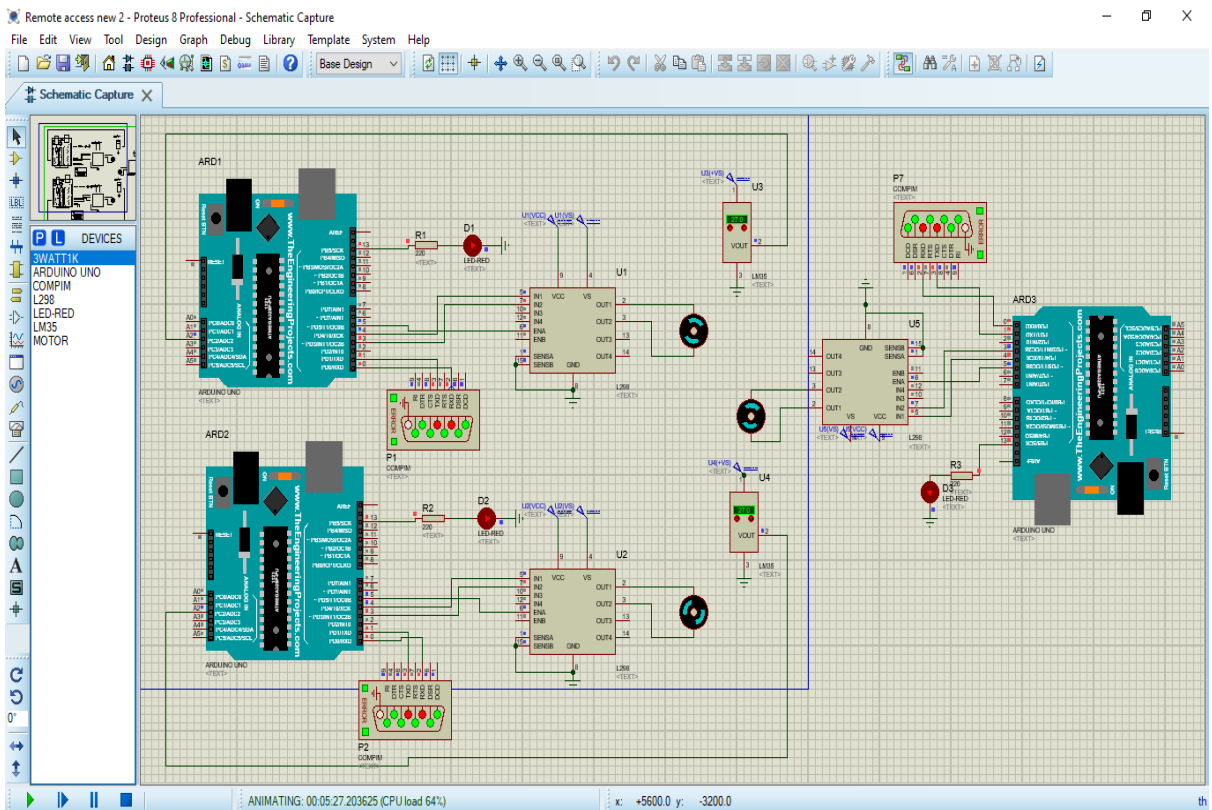


Figure 4.7 Proteus view when Main switch ON

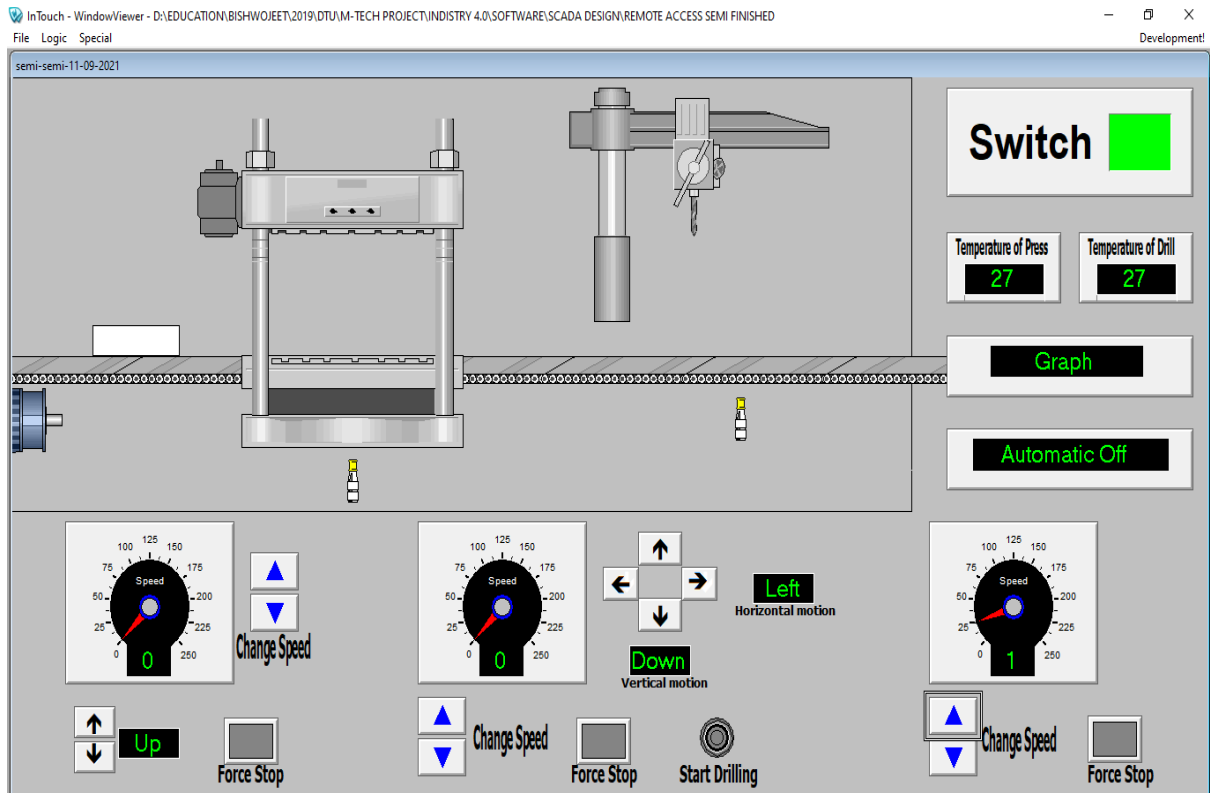


Figure 4.8 Conveyor Unit start and workpiece move forward

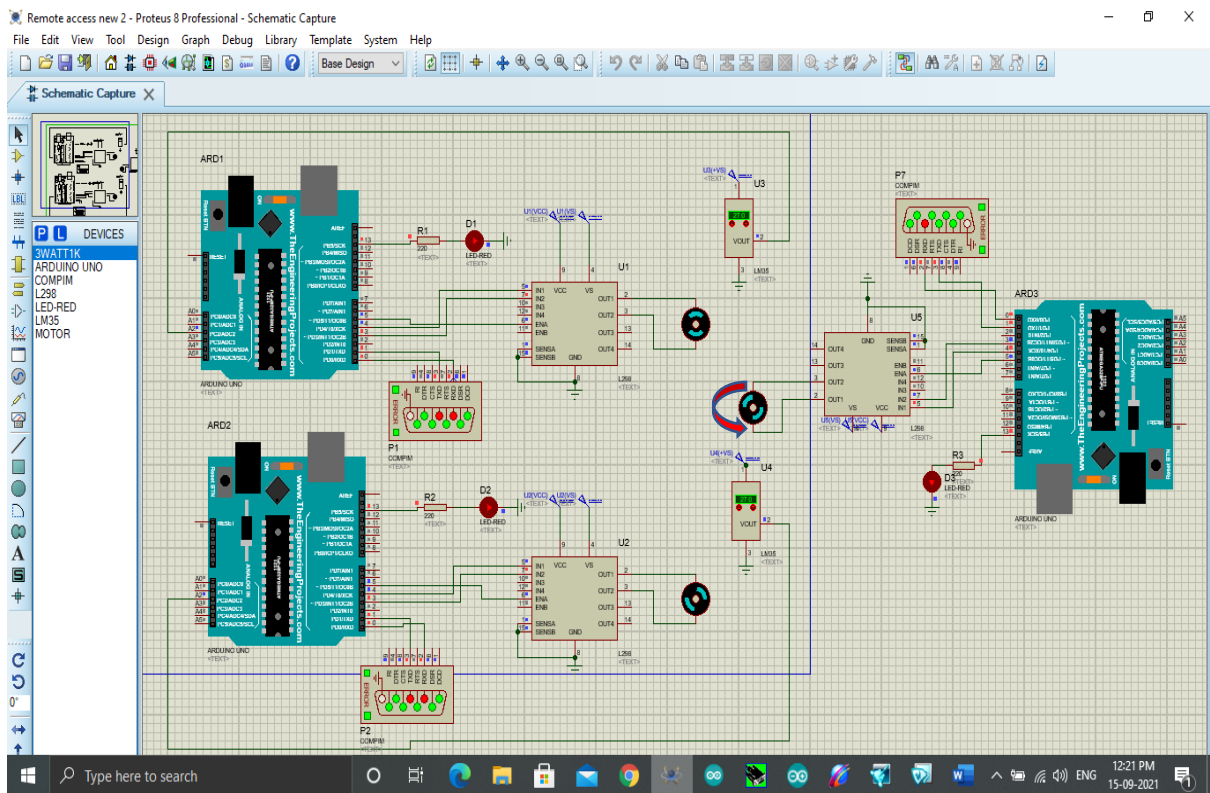


Figure 4.9 Conveyor motor rotated in counter-clockwise

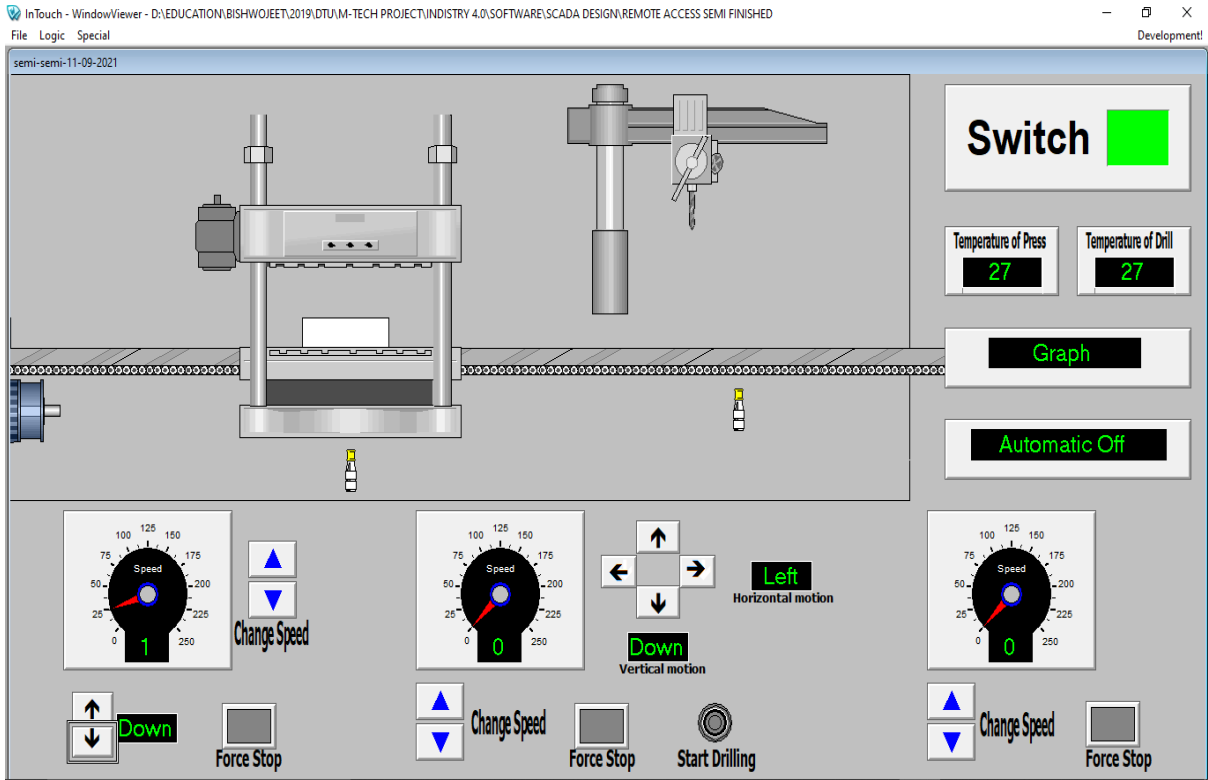


Figure 4.10 Workpiece reach to Electric Press and head move downward

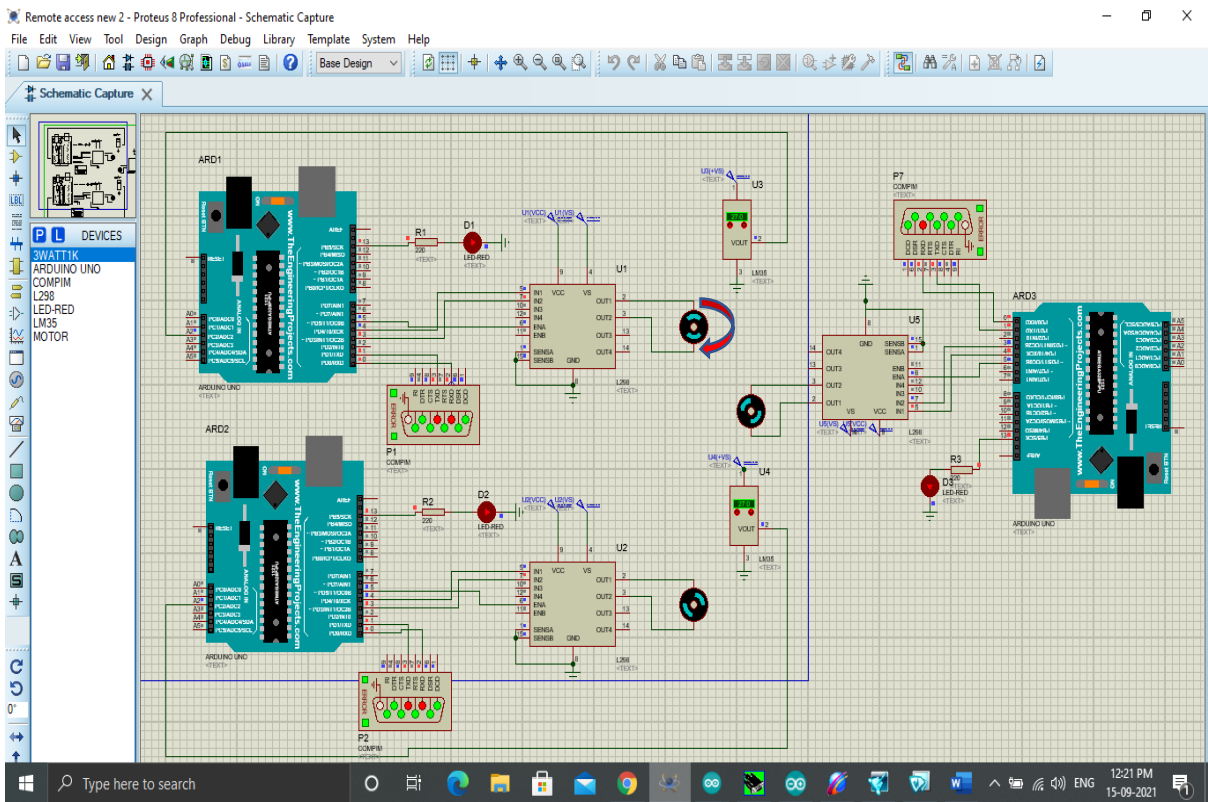


Figure 4.11 Electric Press motor rotated clockwise and Conveyor motor stop.

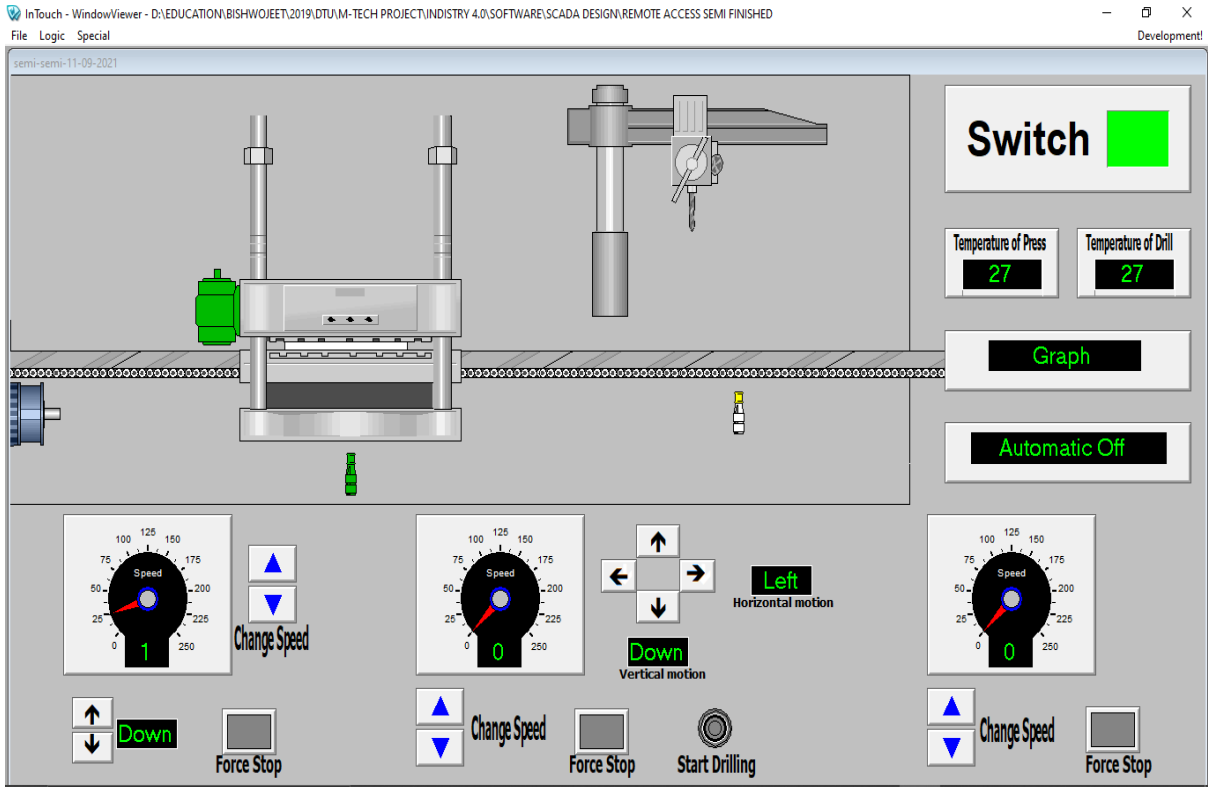


Figure 4.12 Workpiece press by Electric press

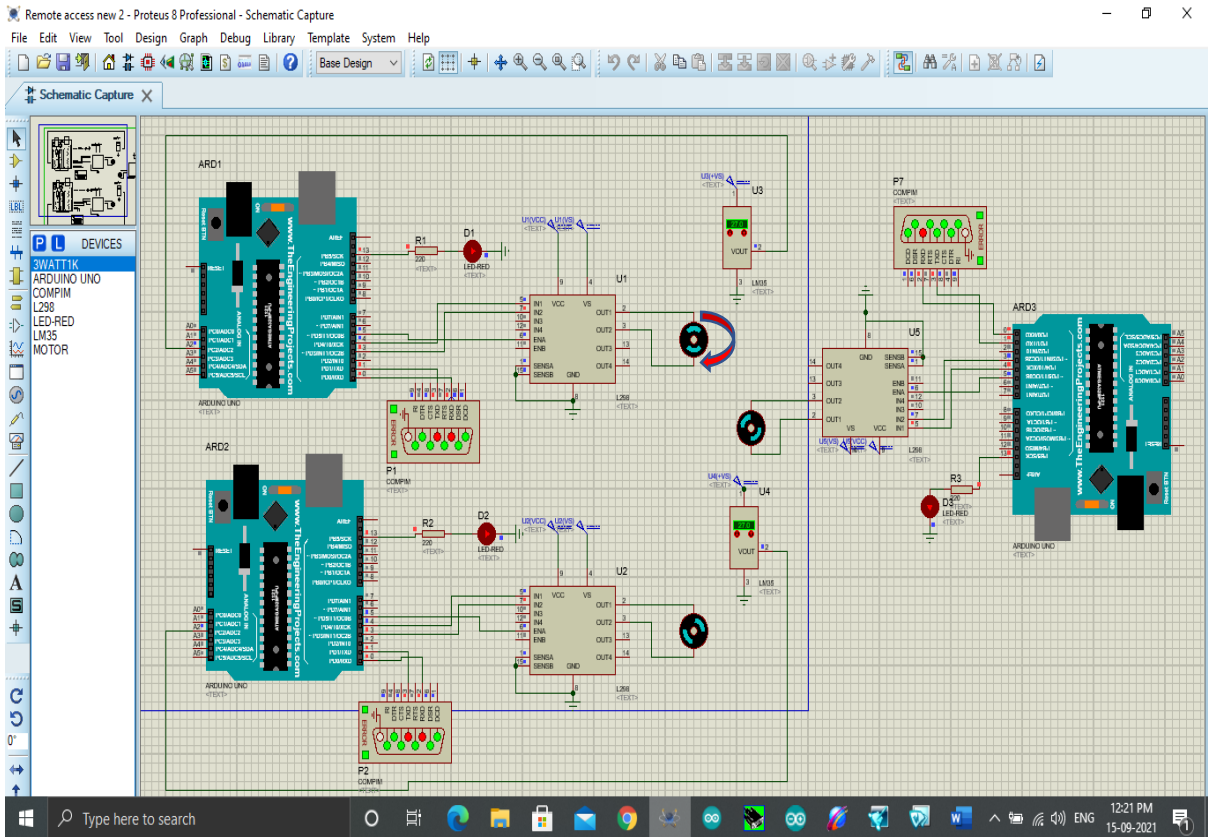


Figure 4.13 Electric Press motor rotated in clockwise and Conveyor motor stop

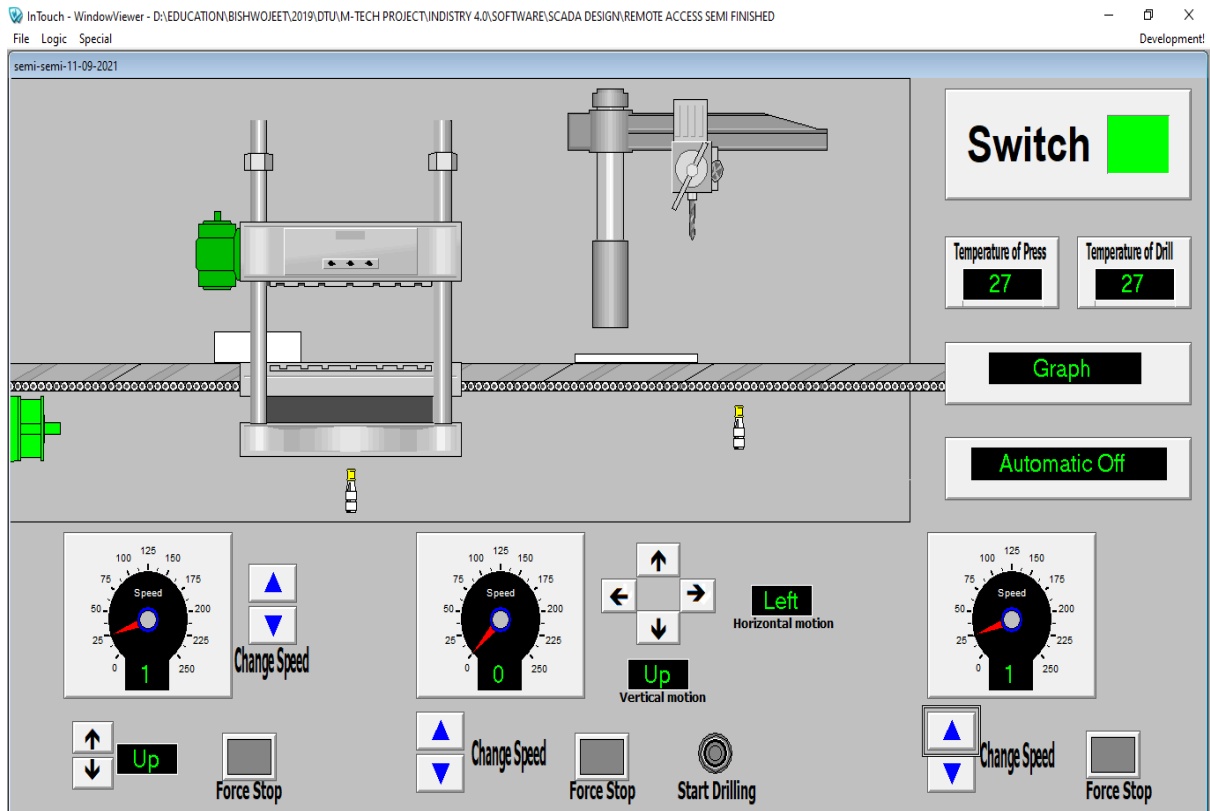


Figure 4.14 Press head moving upward and workpiece moving forward

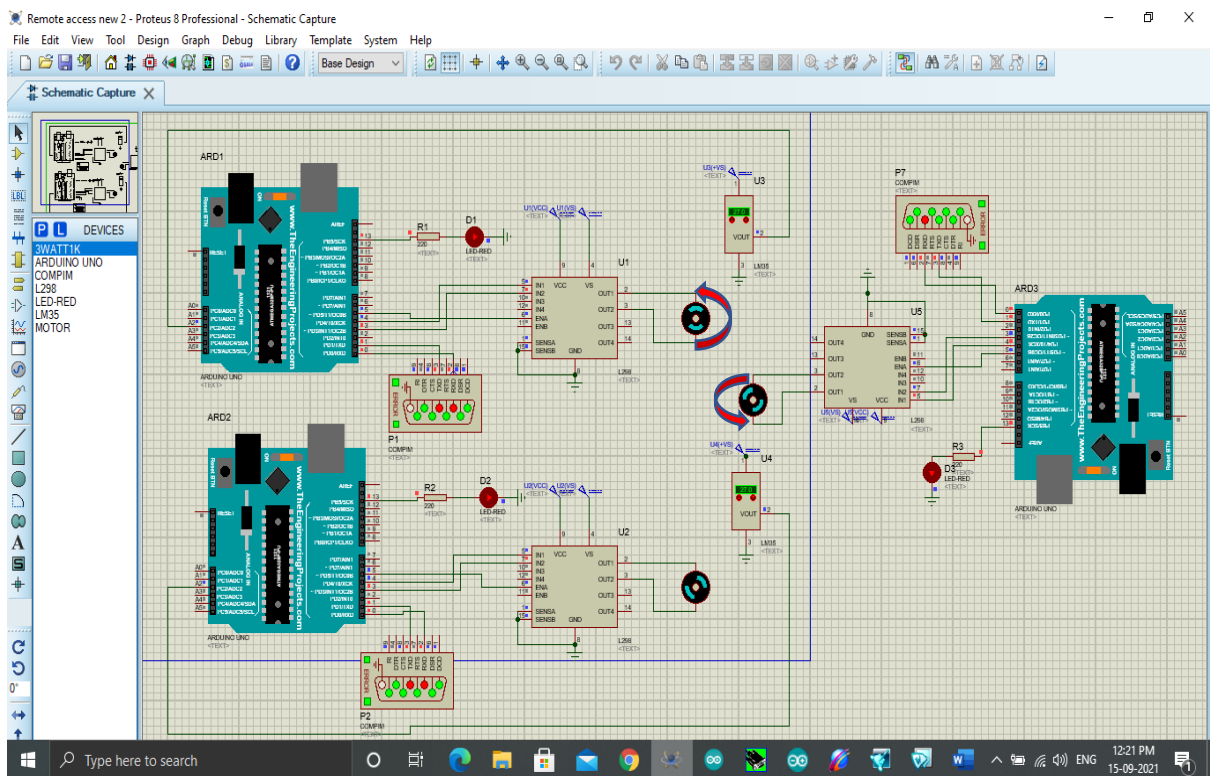


Figure 4.15 Press motor and Conveyor motor rotated in counter-clockwise

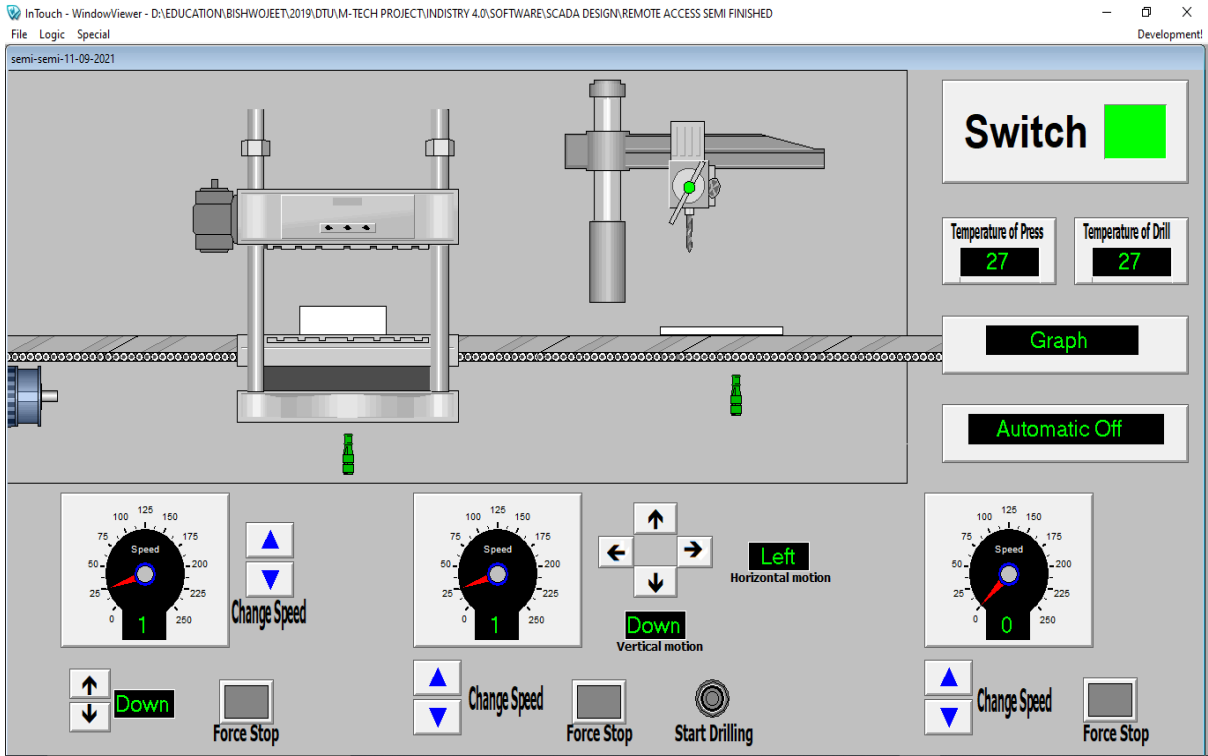


Figure 4.16 Workpiece reach at processing place and Press and Drilling head moving downward

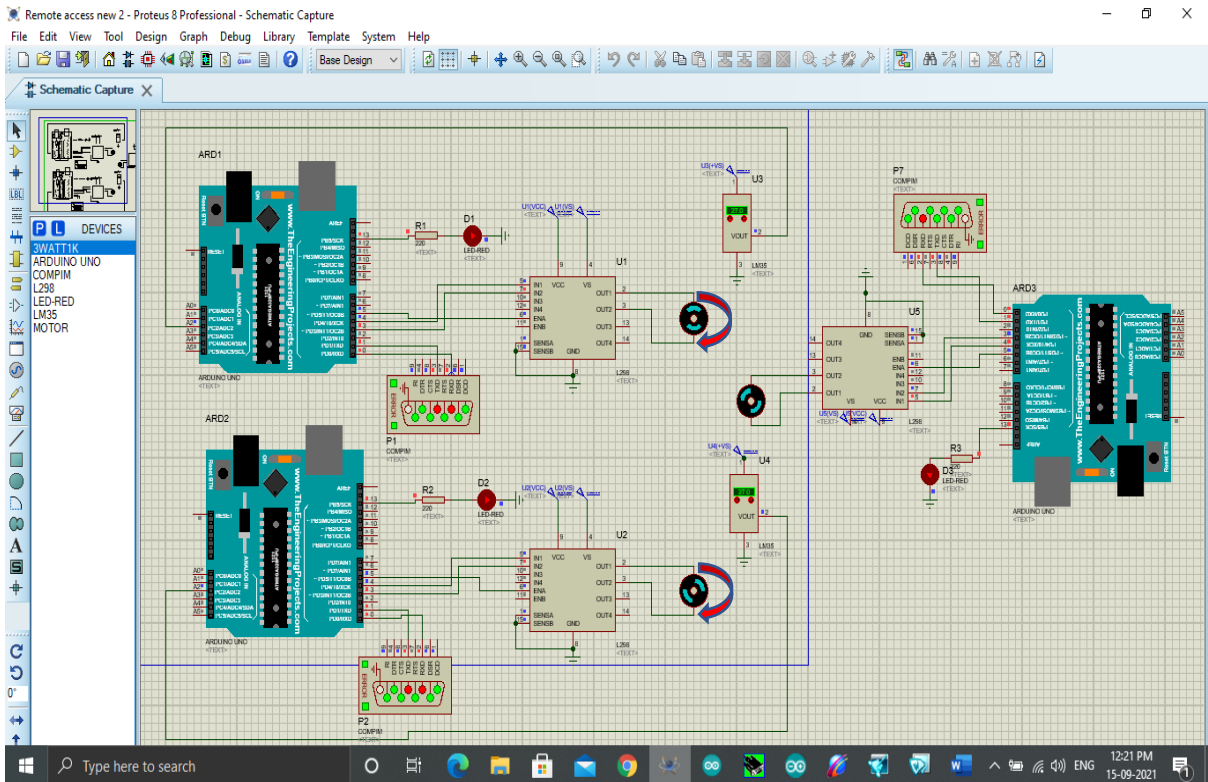


Figure 4.17 Press and Drilling Machine motor rotated in clockwise and Conveyor motor stop

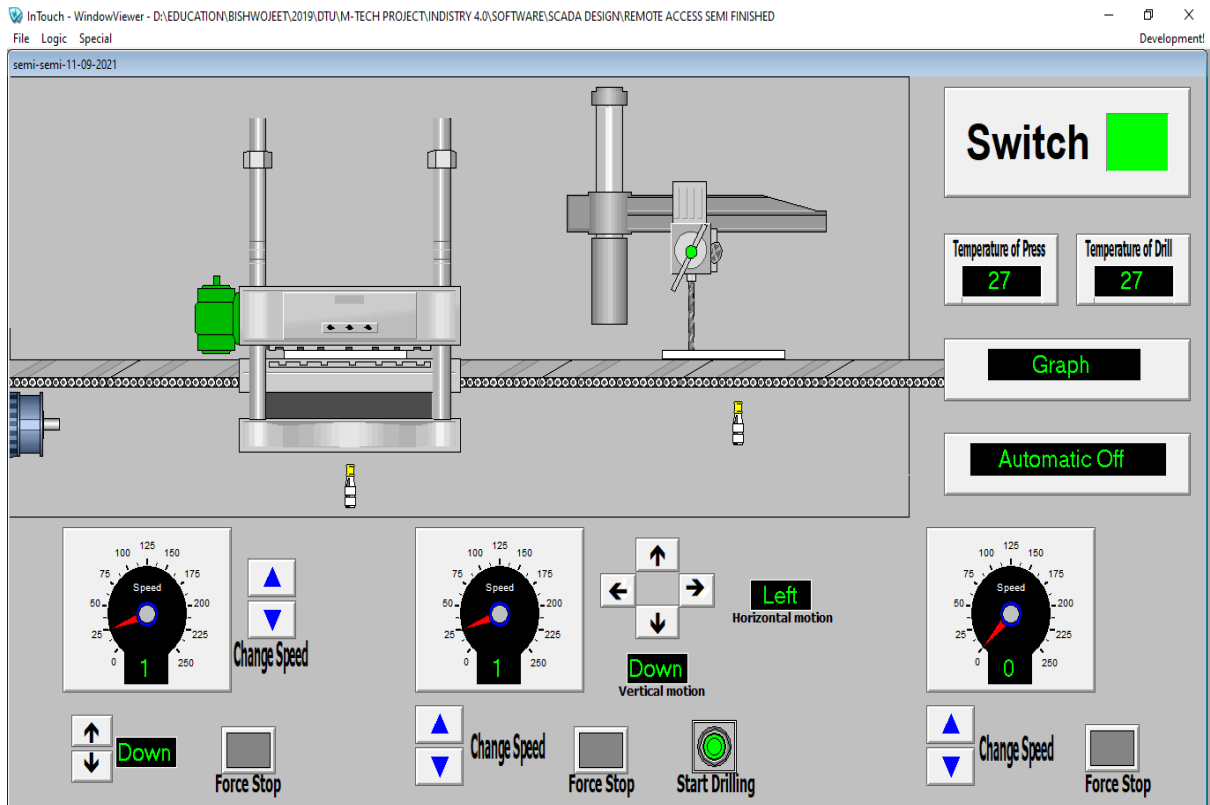


Figure 4.18 Workpiece process by Drilling and Press head

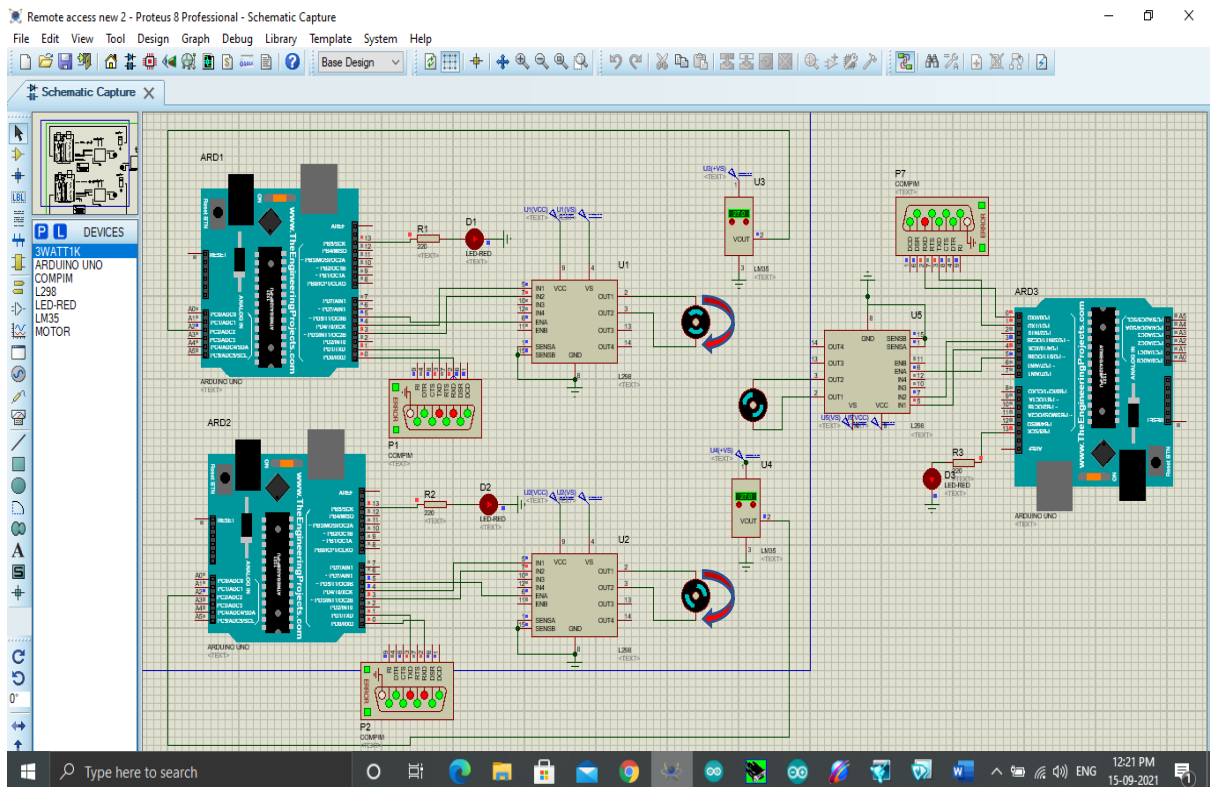


Figure 4.19 Press and Drilling Machine motor rotated in clockwise and Conveyor motor stop

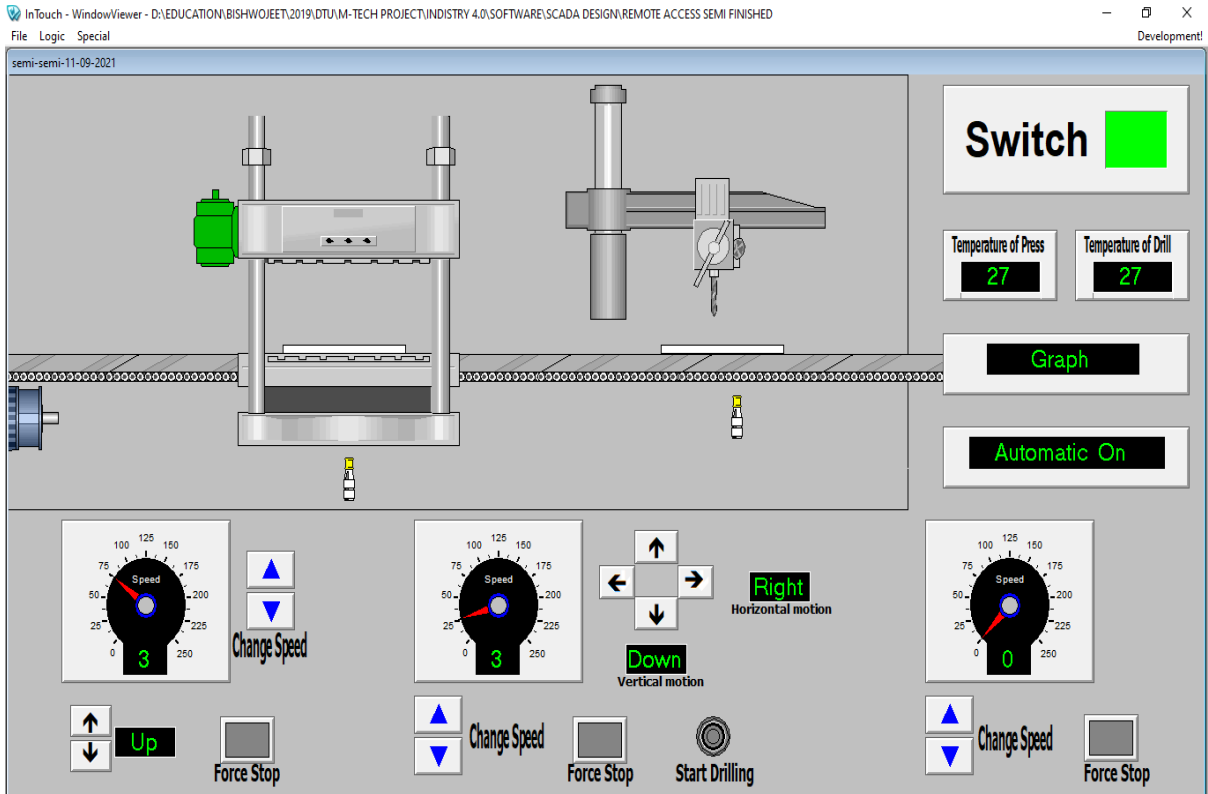


Figure 4.22 Manufacturing unit running in Automatic mode

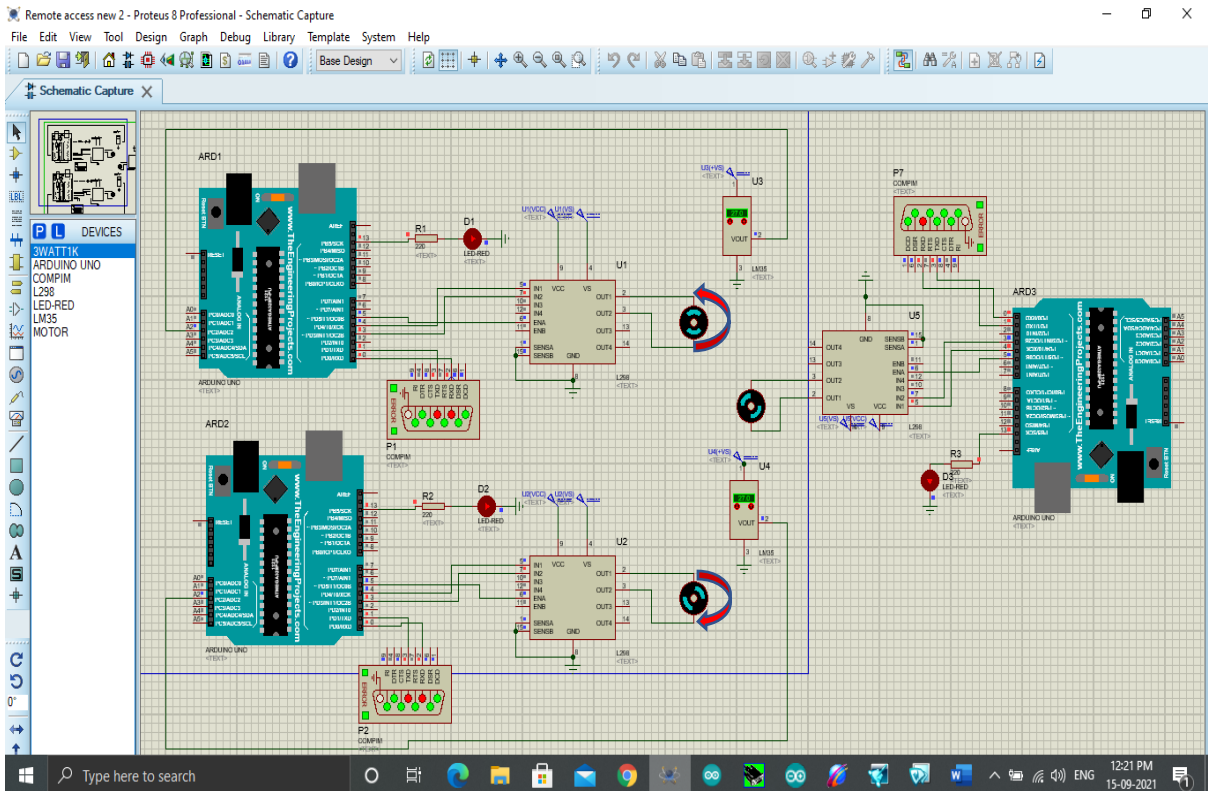


Figure 4.23 Press motor rotated counter-clockwise and Drilling motor rotated in clockwise

All the process data is plotted with time to observe the whole process if any issue arises. This Graph helps to find when the issue comes and in which section of the plant. So, issue identification and their solution become easy.

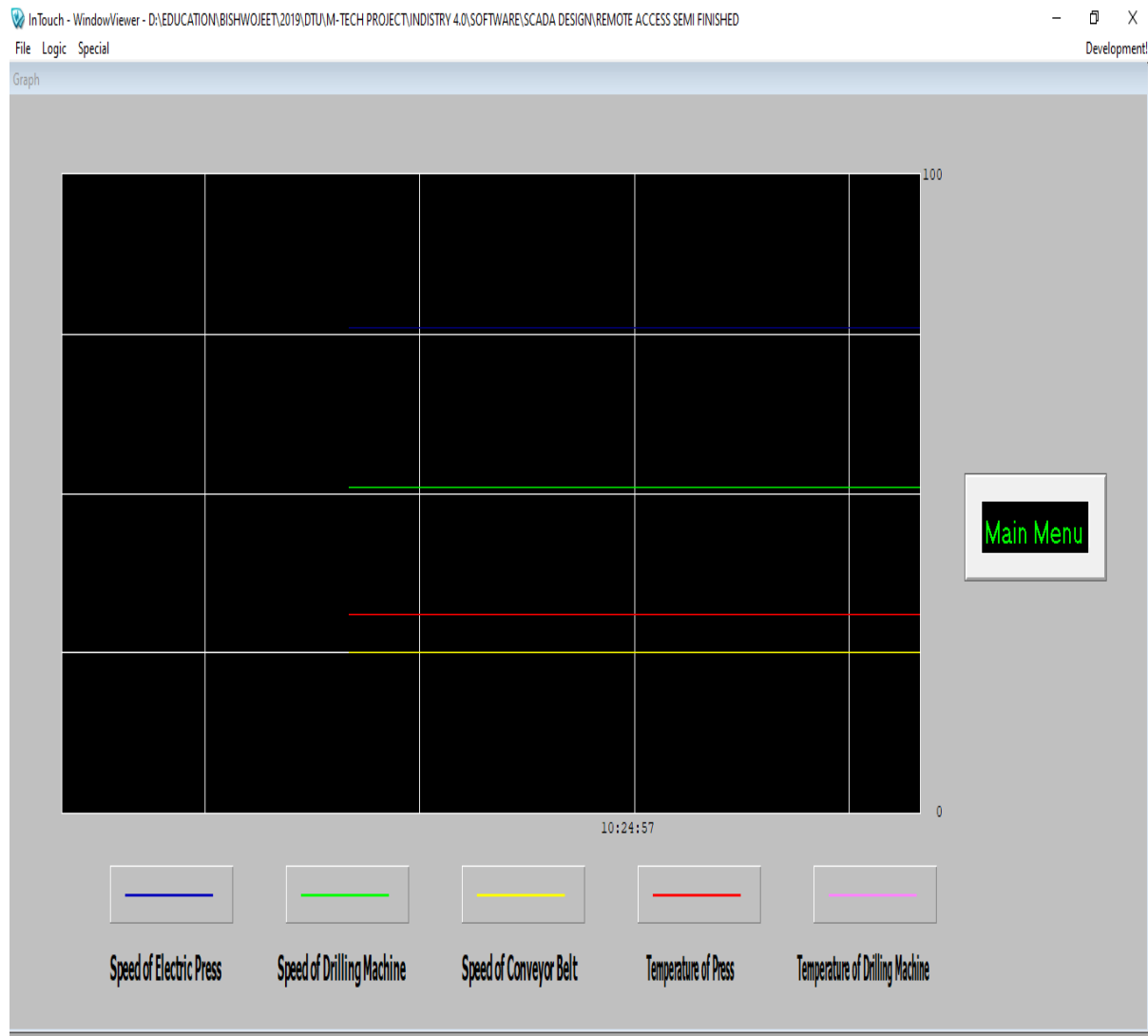


Figure 4.24 Historical Trend

4.2 Discussion

With the integration of technology, manufacturing operations can be controlled remotely. SCADA will play a vital role in monitoring and controlling operations. The technology which is needed for this is already available. The requirement is only to integrate this technology and its implementation. The simulation model based on the integration of technology shown above validated the possibility of a Remote access system for manufacturing operation. Users can monitor and control the operation from any part of the world where high-speed internet is available.

Different work had been carried out in the field of remote monitoring and control of the sophisticated operation of industries. In the manufacturing industry, the remote-control system is used to monitor and control material flow and observe production lines. But this system has

not been used so far in the production operation of the manufacturing industry. In the manufacturing industry, production operation is done either manually or by an automatic machine (CNC). During the Covid-19 situation, both types of manufacturing industry face problems in operation as workers cannot reach the plant to carry out their basic operation so that machines can run. This caused a huge loss in the production sector. If there is a Remote access system then these losses can be reduced to some extent. Some industries are running during covid-19 as they are fulfilling the basic requirement of people. The operator of this industry keeps their life at risk during this situation. If there is a remote access facility then the number of operators who physically need to run the industry is less and some operators can work from their homes.

This remote access system not only allows the operator to control the process but warns them when an issue arises such as temperature or pressure high, and also indicates critical information to the operator. Operators can also run the manufacturing operation in automatic mode. As a remote access system is connected to the internet there is a high chance of cyber-attack on it. This attack has a higher impact than a cyber-attack on an IT company as the lives of people are at risk. So high security is required with a remote access system. There is no proper protocol for the communication of industrial devices. So, an industrial device has to use a common communication protocol which increases the latency of the system. In the simulation model two protocols i.e., OPC server and serial communication are used to make communication between Arduino and SCADA. And while the program is running continuously. Due to this, latency in the simulation model is high. So, when the user changes speed or direction in HMI then the time taken by the actuator (motor) to react on it is about 326 milliseconds There should be a fast data transmission system that has a latency of about 10-20 milliseconds. 5G technology can provide fast data transmission with very little latency.

Remote Access System is possible but to make it effective and reliable more research is needed to do in this field and develop intelligent sensors, high-speed networks, data processing systems, etc. As technology has a certain risk of failure when the Remote Access system fails then huge losses will take place even if some people lost their life. So, there should be a backup technology (system) that can take care of the process in case of failure of the Remote access system.

Chapter 5: CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

This study discusses features that will be provided by the Remote Access System in the manufacturing plant and how this system can be achieved. Although remote access systems have been used in different industries, there is no industry which uses this system in its manufacturing operation. Remote Access System which controls the manufacturing operation remotely is successfully simulated with Proteus, Arduino OPC Server, and Wonderware InTouch software. The SCADA model of the manufacturing plant which was designed in InTouch successfully communicated with the Arduino model of Proteus. Remote Desktop connection software successfully gets access to HMI through which operation monitors and controls the operation. In this simulation model, the user gets control of the SCADA model from another computer that is connected to the same network. This simulation model shows different features which a remote access system may have such as remote control, combination of human intelligence with machine precision, automation of plant, combination of manual and automatic mode for user defined product, use QC tool with sensor data to analyze the process in real-time, etc. This paper also shows many cyber-attacks which took place on the SCADA system in the past and these cyber-attacks also possess a significant threat to the Remote Access System. For effective and safe utilization of the Remote Access System, the proper security system should develop. This simulation model also shows the latency of 326 milliseconds which is caused due to integration of Serial communication with TCP/IP protocol. Integration of existing technology such as AWS, Azure, Wonderware Intouch 2020, etc., can form a Remote Access System for manufacturing operation but it will not be effective due to lack of fast data transmission network, lack of proper protocol for the industrial device, lack of smart sensor and actuator for industrial work, etc. To make it possible, infrastructure for IIoT should develop. Many researches are carried out in the field of Industry 4.0. With the development of Industry 4.0, smart manufacturing systems have started. This will change the whole process and improve the efficiency of the manufacturing Plant.

5.2 Future Scope

With the development of IIoT infrastructure, Remote access systems can be implemented in the manufacturing industry. Operator of a manufacturing plant able to monitor and control operation from any part of the world. This Remote access system can be used to create a virtual lab for the student. This will help to improve the quality of Online Education. This system can also be used to train operators of manufacturing plants without damaging the product.

Reference

- [1] Kagermann, H., Wahlster W., Helbig, J. (2013). Recommendations for implementing the strategic initiative Industrie 4.0: Final report of the Industrie 4.0 Working Group.
- [2] Alexandru UJVAROSI, "EVOLUTION OF SCADA SYSTEMS", Bulletin of the Transilvania University of Braşov • Vol. 9 (58) No. 1 – 2016.
- [3] Dimitrios Pliatsios, Panagiotis Sarigiannidis, Thomas Lagkas, and Antonios G. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," IEEE Communications Surveys & Tutorials, IEEE, vol 22, pp 1942 – 1976, 2020.
- [4] Isaías González Pérez, A. José Calderón Godoy and Manuel Calderón Godoy, "Integration of Open-Source Arduino with LabVIEW-based SCADA through OPC for Application in Industry 4.0 and Smart Grid Scenarios" Automation and Robotics (ICINCO 2019), pages 174-180.
- [5] Paukatong, T. (n.d.). "SCADA Security: A New Concerning Issue of an In-house EGAT - SCADA". 2005 IEEE/PES Transmission & Distribution Conference & Exposition: Asia and Pacific.
- [6] B. Miller and D. Rowe, "A survey SCADA of and critical infrastructure incidents," in Proceedings of the 1st Annual conference on Research in information technology. ACM, 2012, pp. 51–56.
- [7] Darshana Upadhyay, Srinivas Sampalli, "SCADA (Supervisory Control and Data Acquisition) Systems: Vulnerability Assessment and Security Recommendations," Computers & Security, vol 89, Science Direct, 2020.
- [8] Stamatis Karnouskos and Armando Walter Colombot, "Architecting the next generation of service-based SCADA/DCS system of systems", IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society.
- [9] S. A. Baker, S. Waterman, and G. Ivanov, In the crossfire: Critical infrastructure in the age of cyber war. McAfee, Incorporated, 2009.
- [10] T. Smith, "Hacker jailed for revenge sewage attacks," October 2001.[Online]. Available:
https://www.theregister.com/2001/10/31/hacker_jailed_for_revenge_sewage/.
- [11] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the slammer worm," IEEE Security & Privacy, vol. 99, no. 4, pp. 33–39, 2003.
- [12] D. Goodin, "Electrical supe charged with damaging California canal system," Nov 2007. [Online]. Available:
https://www.theregister.co.uk/2007/11/30/canal_system_hack/
- [13] D. Goodin, "Feds: Hospital hacker's 'massive' DDoS averted," Jul 2009. [Online]. Available: https://www.theregister.co.uk/2009/07/01/hospital_hacker_arrested/
- [14] G. Keizer, "Is stuxnet the 'best' malware ever" Sep 2010. [Online]. Available: <https://www.computerworld.com/article/2515757/malwarevulnerabilities/is-stuxnet-the-best-malware-ever.html>
- [15] K. Zetter, "Son of stuxnet found in the wild on systems in Europe," Oct 2011. [Online]. Available: <https://www.wired.com/2011/10/sonof-stuxnet-in-the-wild/>

- [16] D. Starkey, "Hacker group dragonfly takes aim at us power grid," Sep 2017. [Online]. Available: <https://www.geek.com/tech/hacker-groupdragonfly-takes-aim-at-us-power-grid-1715157/>
- [17] A. Greenberg, "How an entire nation became Russia's test lab for cyberwar," Jun 2017. [Online]. Available: <https://www.wired.com/story/russian-hackers-attack-ukraine/>
- [18] M. Kumar, "Dragonfly 2.0: Hacking group infiltrated European and US power facilities," Sep 2017. [Online]. Available: <https://thehackernews.com/2017/09/dragonfly-energy-hacking.html>
- [19] Luke Sharrett, "How a major oil pipeline got held for ransom", June 2021. [Online]. <https://www.vox.com/recode/22428774/ransomware-pipeline-colonial-darkside-gas-prices>.
- [20] K. Coffey, L. A. Maglaras, R. Smith, H. Janicke, M. A. Ferrag, A. Derhab, M. Mukherjee, S. Rallis, and A. Yousaf, "Vulnerability assessment of cyber security for scada systems," in Guide to Vulnerability Analysis for Computer Networks and Systems. Springer, 2018, pp. 59–80.
- [21] Q. S. Qassim, N. Jamil, M. Daud, A. Patel, and N. Ja'afar, "A review of security assessment methodologies in industrial control systems," Information & Computer Security, vol. 27, no. 1, pp. 47–61, 2019.
- [22] Q. Wanying, W. Weimin, Z. Surong, and Z. Yan, "The study of security issues for the industrial control systems communication protocols," Joint International Mechanical, Electronic and Information Technology Conference, China, 2015.
- [23] Kelian Zhou, Taigang Liu, Lifeng Zhou, (2015). Industry 4.0: Towards Future Industrial Opportunities and Challenges. 12th International Conference on Fuzzy Systems and Knowledge Discovery.
- [24] Vaidya, S., Ambad, P., & Bhosle, S. (2018). Industry 4.0 – A Glimpse. Procedia Manufacturing, 20, 233–238.
- [25] S.Gervais-Ducouret; Next smart sensors generation Publication Year: 2011, Page(s): 193–196.
- [26] Cristina Orsolin Klingenberg, Cristina Orsolin Klingenberg. (2017). Industry 4.0: what makes it a revolution? The EurOMA conference was held in July 2017.
- [27] Lee, Jay, Behrad Bagheri, and Hung-An Kao. "A cyber-physical systems architecture for industry 4.0-based manufacturing systems." Manufacturing Letters 3(2015): pp 18-23.
- [28] Kelian Zhou, Taigang Liu, Lifeng Zhou, (2015). Industry 4.0: Towards Future Industrial Opportunities and Challenges. 12th International Conference on Fuzzy Systems and Knowledge Discovery.