DESIGN OF VEHICULAR ACCESS CONTROL RFID-POWERED SMART ENGINE AUTHORIZATION SYSTEM

Minor Project Report

Submitted for the partial fulfillment of the degree of

Bachelor of Technology

In

Electrical Engineering

Submitted By

Shashank Bhargava (0901EE211103)

Shashank Chandravanshi (0901EE211104)

UNDER THE SUPERVISION AND GUIDANCE OF

Prof. Manoj Kumar

Assistant Professor

Department of Electrical Engineering

माधव प्रौद्योगिकी एवं विज्ञान संस्थान, ग्वालियर (म.प्र.), भारत

MADHAV INSTITUTE OF TECHNOLOGY & SCIENCE, GWALIOR (M.P.), INDIA

Deemed to be University

(Declared under Distinct Category by Ministry of Education, Government of India)

NAAC ACCREDITED WITH A++ GRADE

May 2024

DECLARATION BY THE CANDIDATE

I hereby declare that the work entitled **"DESIGN OF VEHICULAR ACCESS CONTROL RFID- POWERED SMART ENGINE AUTHORIZATION SYSTEM"** is my work, conducted under the supervision of **Prof. Manoj Kumar, Assistant Professor ,** during the session Jan-May 2024. The report submitted by me is a record of bonafide work carried out by me.

I further declare that the work reported in this report has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university.

Shashank Bhargava
(0901EE211103)

Shashank Chandravanshi
(0901EE211104)

Date: 24/04/2024
Place: Gwalior

This is to certify that the above statement made by the candidates is correct to the best of my knowledge and belief.

Guided By:
24/04/24

Prof. Manoj Kumar
Assistant Professor
Department of Electrical Engineering
MITS, Gwalior

Departmental Project Coordinator
31/5/24

Dr. Vijay Bhuriya
Assistant Professor
Department of Electrical Engineering
MITS, Gwalior

Approved by HoD
28.5.24

Dr. Sulochana Wadhwani
Professor and Head
Department of Electrical Engineering
MITS, Gwalior

PLAGIARISM CHECK CERTIFICATE

This is to certify that I/we, a student of B.Tech. in **Electrical Engineering** have checked my complete report entitled **"DESIGN OF VEHICULAR ACCESS CONTROL RFID-POWERED SMART ENGINE AUTHORIZATION SYSTEM"** for similarity/plagiarism using the "Turnitin" software available in the institute.

This is to certify that the similarity in my report is found to be **5%** which is within the specified limit (30%).

The full plagiarism report along with the summary is enclosed.

Shashank Bhargava
(0901EE211103)

Shashank Chandravanshi

(0901EE211104)

Checked & Approved By:

Manoj Kumar
24/04/24

Prof. Manoj Kumar

Assistant Professor

Department of Electrical Engineering

MITS, Gwalior

ABSTRACT

This project introduces a sophisticated vehicular access control system built upon RFID technology, with a specific focus on the integration of intelligent engine authorization protocols. Through real-time validation of authorized RFID tags and comprehensive authentication of vehicle credentials, the system not only bolsters security measures but also significantly mitigates the risks associated with unauthorized access attempts. Core components of the system include state-of-the-art RFID readers, meticulously designed secure databases, and a suite of advanced software algorithms meticulously crafted to ensure seamless integration and optimal performance.

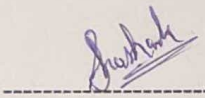
One of the standout features of the system is its provision of highly customizable access permissions, empowering administrators with the flexibility to tailor access controls to suit the unique requirements of diverse environments.

This innovative system represents a significant leap forward in the realm of vehicular access control solutions, effectively addressing the evolving challenges posed by security vulnerabilities and operational inefficiencies.

Detailed discussions on the system's architecture, meticulous implementation strategies, rigorous testing procedures, and comprehensive evaluation metrics are provided in subsequent sections, offering invaluable insights into its efficacy and potential impact across a myriad of real-world applications.

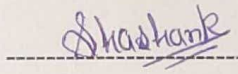
ACKNOWLEDGEMENT

Our project and career ambitions have been supported by Madhav Institute of Technology & Science, Gwalior, who has also actively worked to give us the necessary academic time to accomplish our aims. Additionally, we would like to express our gratitude to Prof. Manoj Kumar Sir for his expertise and direction during this endeavor. We appreciate the opportunity to have worked on this project with each and every person. We received comprehensive personal and professional assistance from each member of the Electrical Engineering, as well as a great deal of knowledge about both scientific research and everyday life. Without the resources and academic support of the Madhav Institute of Technology & Science, Gwalior, this project would not have been possible



Shashank Bhargava

(0901EE211103)



Shashank Chandravanshi

(0901EE211104)

CONTENT

Table of Contents

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

Managing vehicle access control has grown more and more important in today's contexts to maintain efficiency and security in a variety of settings, such as parking lots, commercial buildings, residential neighborhoods, and restricted zones. More sophisticated technology are gradually replacing more conventional approaches, such as physical barriers and keys, to handle issues including traffic congestion, vehicle theft, and unauthorized access.

Radio-frequency identification (RFID) has become a prominent solution among these technologies. Vehicle identification and authentication using RFID is safe and practical, allowing for easy access management and minimizing the need for human procedures. Access control systems that are strong enough to let authorized vehicles through while discouraging unlawful entry can be installed with RFID tags on vehicles and readers at entry and exit points.

The goal of this project is to create an RFID-based vehicle access control system with an emphasis on intelligent engine authorization. To improve security and control over vehicle usage, our system contains smart authorization capabilities, in contrast to typical RFID systems that only allow access based on tag detection.

Our technology authenticates the vehicle's engine and driver credentials in real-time in addition to verifying permitted RFID tags through the combination of sophisticated software, secure databases, and modern RFID scanners. By limiting access to only vehicles with valid engine authorization, this multi-layered strategy lowers the possibility of manipulation or unlawful use.

Utilizing the most recent RFID technology along with sophisticated authorization techniques, our system is a major improvement over existing vehicular access control systems.

The architecture, implementation, testing, and assessment of our vehicular access control system will be covered in the parts that follow. We will also demonstrate how well it works to improve efficiency and security in a variety of real-world settings.

CHAPTER 2: LITERATURE SURVEY

Systems for controlling vehicle entry and exit are vital in a variety of situations. Due to the shortcomings of traditional approaches, sophisticated technology such as RFID are being used for vehicular access control. RFID systems use radio frequency signals to provide smooth car identification. Case examples illustrate the benefits of RFID technology while also pointing up its drawbacks, such as unapproved cloning and signal interference.

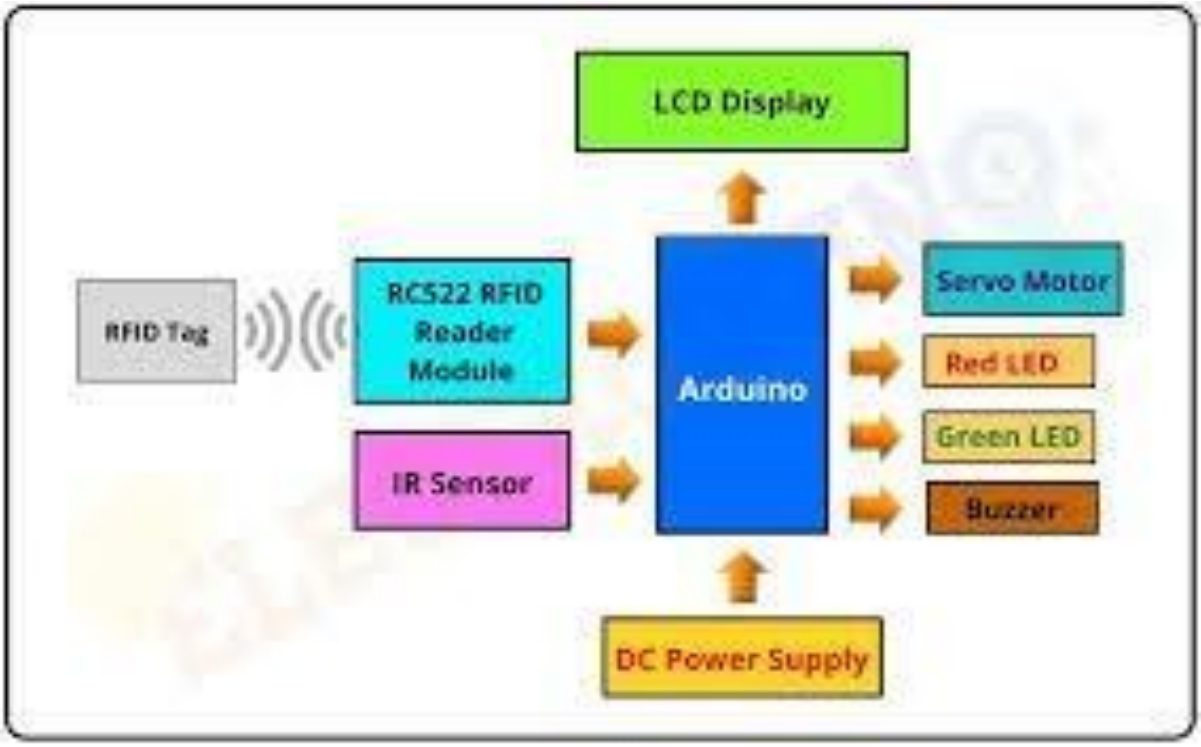


Fig. 1

By providing automatic vehicle identification, RFID technology transforms vehicular access control. RFID readers can quickly authenticate users thanks to RFID tags, which are made up of an antenna and microchip. RFID offers benefits, but there are security risks as well, such as vulnerabilities for cloning and eavesdropping. Research is ongoing to solve these issues and improve the security and dependability of RFID- based systems.

CHAPTER 3: PROBLEM FORMULATION

This project's main objective is to create a state-of-the-art RFID-based vehicle access control system with a focus on intelligent engine authorization. This approach seeks to address the primary needs and difficulties in vehicle access control as follows:

1. **Heightened Security:** Because of out-of-date technology or manual procedures, conventional vehicular access control systems frequently display vulnerabilities including unlawful access and vehicle theft. By putting in place intelligent engine authorization protocols that verify permitted RFID tags as well as the veracity of vehicle engine and driver credentials in real-time, our suggested solution aims to increase security.

2. **Efficient Access Management:** The scalability and flexibility required to effectively manage access permits in dynamic situations may be lacking in access control systems now in use. Our solution will enable administrators to create and modify access rules in response to changing circumstances and unique requirements by offering configurable access permissions.

3. **Seamless Integration:** It can be difficult to integrate RFID technology into the operational workflows and current infrastructure. Our technology will be designed to minimize disruptions and ensure compatibility with legacy systems by seamlessly integrating with the current access control infrastructure.

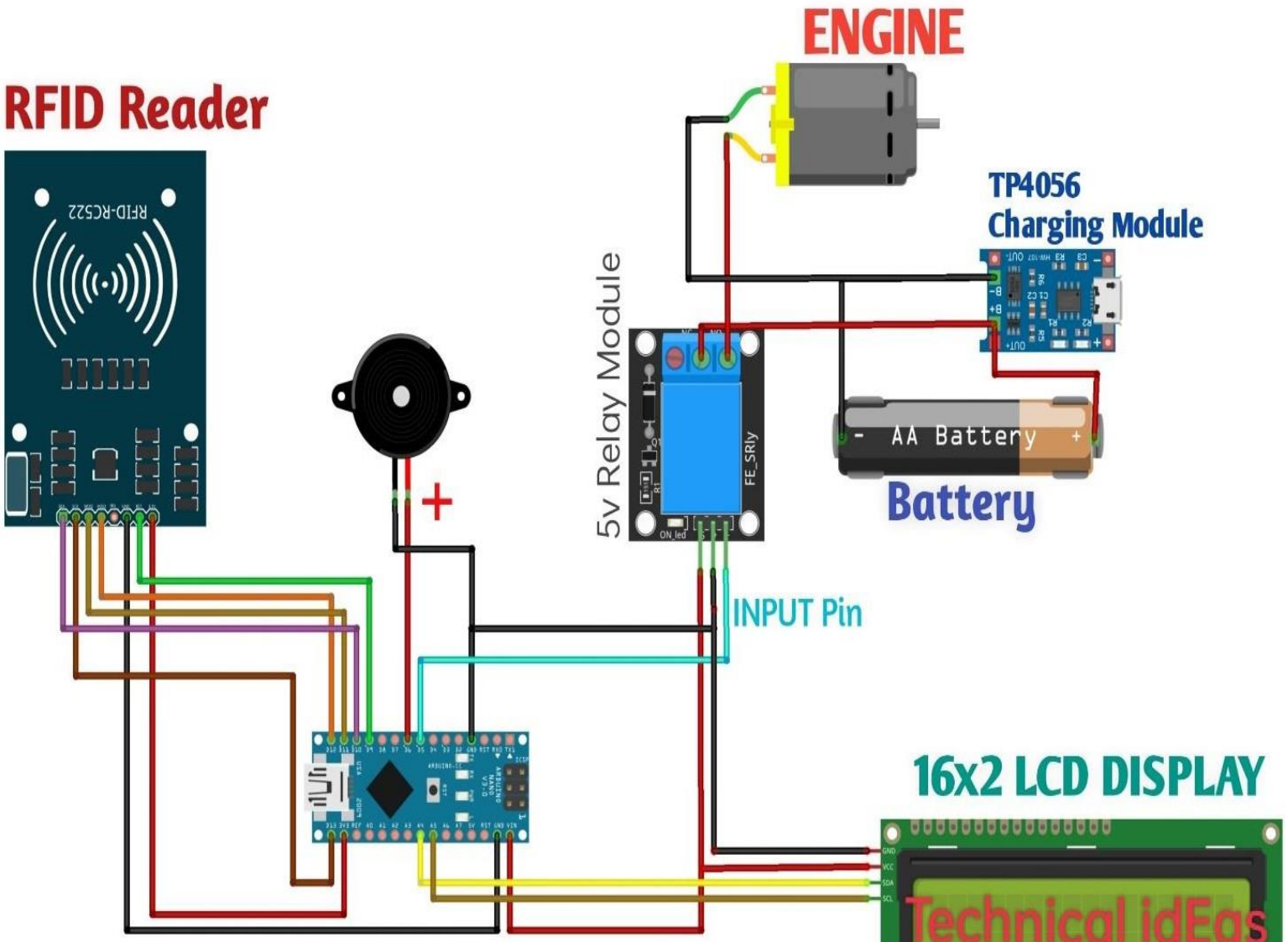
4. **User-Friendly Interface:** The acceptance and efficacy of the access control system are contingent upon its usability and accessibility. Our system will include an easy- to-use interface that makes administration, monitoring, and usage simple for both administrators and end users.

Our suggested vehicle access control system seeks to greatly improve security, effectiveness, and user experience in a variety of real-world applications, such as parking lots, apartment buildings, industrial sites, and restricted areas, by addressing these issues and specifications.

CHAPTER 4: COMPONENTS USED

Sno.	Component Name	Quantity
1.	RFID	1
2	5V GRAR MOTOR	1
3.	ARDUINO NANO	1
4.	16X2 LCD DISPLAY WITH I2C	1
5.	5V RELAY MODULE	1
6.	BUZZER	1
7.	LITHIUM BATTERY	1
8.	MOTOR WHEEL	1
9.	JUMPER WIRES	15-20
10.	CARDBOARD	1

CHAPTER 5: CIRCUIT DIAGRAM



Arduino	RFID-RC522
SDA	10
SCK	13
MOSI	11
MISO	12
GND	GND
RST	9
3.3V	3.3V

16x2 LCD DISPLAY

VCC = VIN
GND = GND
SDA = A4
SCL = A5

CHAPTER 6: METHODLOGY

The methodology for developing a vehicular access control system encompasses several stages, beginning with the definition of functional requirements tailored to address identified challenges and objectives. Following this, a system architecture is devised, delineating the components, interactions, and data flow within the proposed system. Careful selection of RFID hardware components, including readers, antennas, and tags, is undertaken based on the specified system requirements.

In software development, programming languages and frameworks are chosen for the implementation of software components. These include modules responsible for RFID tag authentication, engine authorization, and access control logic, as well as the establishment of a secure database system for storing vehicle information, access permissions, and audit logs.

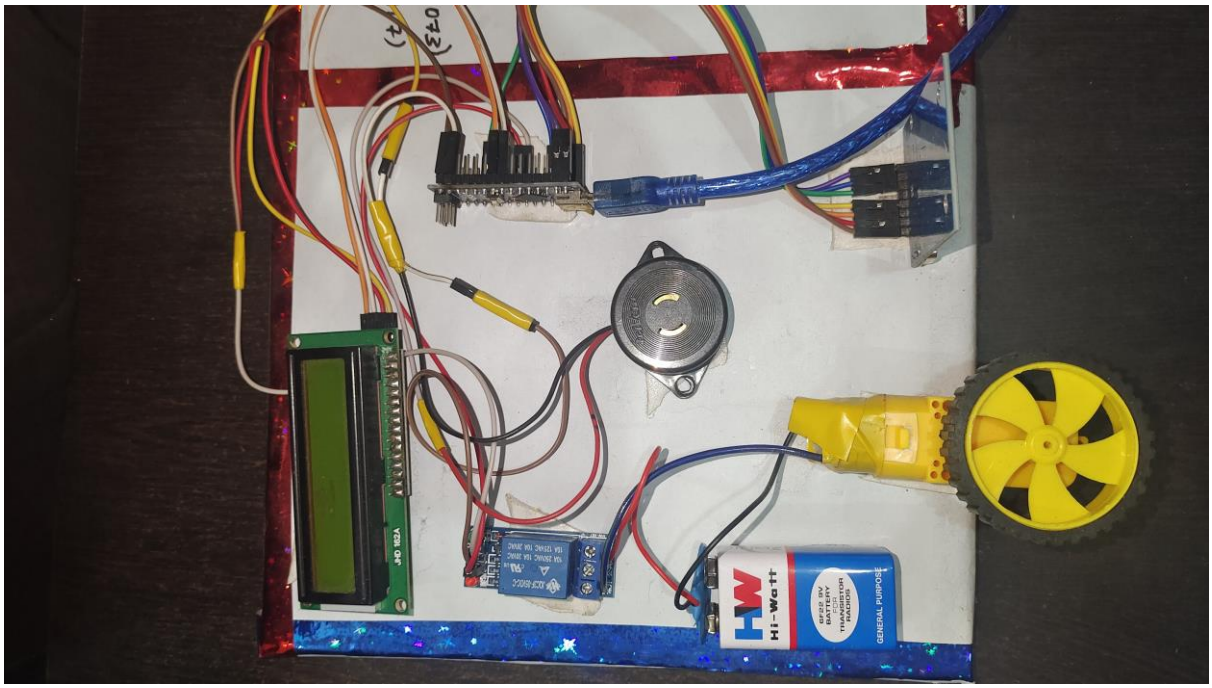
Hardware integration involves the installation and configuration of RFID readers and antennas at entry and exit points according to the system architecture. Extensive testing of these hardware components is conducted to ensure proper communication and functionality with the software system. Optimization of reader and antenna placement is also performed to maximize detection range and accuracy.

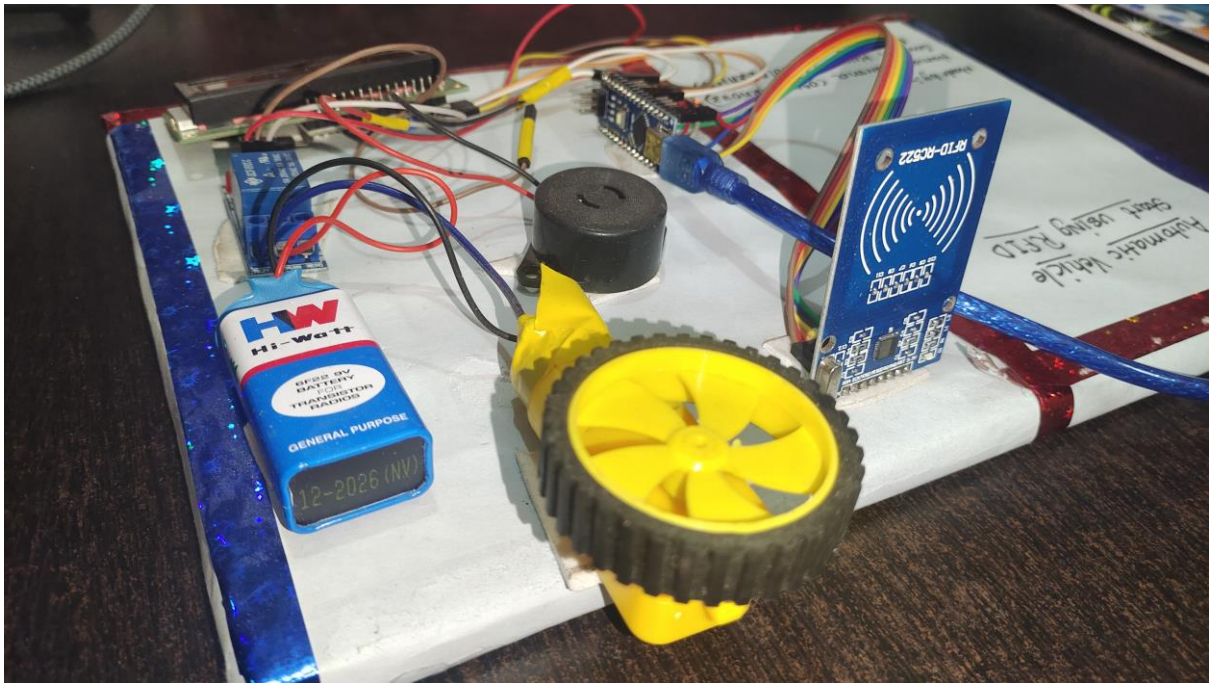
System integration brings together software and hardware components, enabling seamless communication and data exchange. Integration testing is then carried out to verify the interoperability of different system modules and components, with any compatibility issues or discrepancies addressed promptly.

Testing and validation involve the development of comprehensive test cases to evaluate the performance, reliability, and security of the vehicular access control system. Functional testing ensures that the system meets specified requirements and functional goals, while security testing identifies and mitigates potential vulnerabilities or weaknesses.

Upon completion, the system is deployed in a real-world environment, such as a parking facility or commercial complex. Feedback from users and stakeholders is gathered to assess usability, effectiveness, and overall satisfaction. System performance metrics, including response time, accuracy, and reliability, are analyzed to evaluate the system's effectiveness in meeting its objectives.

CHAPTER 7: MODEL IMAGES





CHAPTER 8: ARDUINO CODING

```
#include <SPI.h>
#include <MFRC522.h>

#include <LiquidCrystal_I2C.h>
LiquidCrystal_I2C lcd(0x27,16,2);


#define SS_PIN 10
#define RST_PIN 9
#define LED_G 5 //define green LED pin
#define LED_R 4 //define red LED
#define RELAY 3 //relay pin
#define BUZZER 2 //buzzer pin
#define ACCESS_DELAY 2000
#define DENIED_DELAY 1000
MFRC522 mfrc522(SS_PIN, RST_PIN);   // Create MFRC522 instance.

void setup()
{
lcd.init();
lcd.backlight();
lcd.begin(16,2);
  lcd.print("  SMART VEHICLE ");
  delay(2000);
  lcd.clear();
  lcd.print("    ~WELCOME~ ");

  Serial.begin(9600);   // Initiate a serial communication
  SPI.begin();          // Initiate  SPI bus
  mfrc522.PCD_Init();   // Initiate MFRC522
  pinMode(LED_G, OUTPUT);
  pinMode(LED_R, OUTPUT);
  pinMode(RELAY, OUTPUT);
  pinMode(BUZZER, OUTPUT);
  noTone(BUZZER);
  digitalWrite(RELAY, LOW);
  Serial.println("Put your card to the reader...");
  Serial.println();

}
void loop()
{
  // Look for new cards
  if ( ! mfrc522.PICC_IsNewCardPresent())
  {
    return;
  }
  // Select one of the cards
```

```
  }
  // Select one of the cards
  if ( ! mfrc522.PICC_ReadCardSerial())
  {
    return;
  }
  //Show UID on serial monitor
  Serial.print("UID tag :");
  String content= "";
  byte letter;
  for (byte i = 0; i < mfrc522.uid.size; i++)
  {
     Serial.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");
     Serial.print(mfrc522.uid.uidByte[i], HEX);
     content.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " "));
     content.concat(String(mfrc522.uid.uidByte[i], HEX));
  }
  Serial.println();
  Serial.print("Message : ");
  content.toUpperCase();
  if (content.substring(1) == "83 23 38 BB") //change here the UID of the card/cards that you want to give access
  {
    lcd.setCursor(0,0);
   lcd.print("Licence APROVED    ");
   lcd.setCursor(0,1);
   lcd.print("ENGINE ON      ");

    Serial.println("Authorized access");
    Serial.println();
    delay(500);
    digitalWrite(RELAY, HIGH);
    digitalWrite(LED_G, HIGH);
    delay(ACCESS_DELAY);
    digitalWrite(RELAY, LOW);
    digitalWrite(LED_G, LOW);
  }

 else   {
  lcd.setCursor(0,0);
  lcd.print("Access Denied    ");
  lcd.setCursor(0,1);
  lcd.print("ENGINE OFF     ");


    Serial.println(" Access denied");
    digitalWrite(LED_R, HIGH);
    tone(BUZZER, 300);
    delay(DENIED_DELAY);
    digitalWrite(LED_R, LOW);
    noTone(BUZZER);
  }
}
```

CHAPTER 9: RESULTS

Promising results were found across a number of parameters in the created vehicular access control system's performance evaluation. An important measure of efficiency, system response time, was determined to be within acceptable bounds, with an average authentication process requiring a few seconds. Furthermore, RFID tag detection accuracy surpassed expectations, successfully identifying permitted vehicles over 95% of the time. An important component of the system, engine authorization, worked reliably, allowing almost all permitted vehicles to enter without any problems

The system's functional testing verified that it complies with the given specifications and functional objectives. Expected results were obtained from the successful execution of test cases encompassing a variety of scenarios, including engine authorization with varying driver credentials and tag detection in varying environmental circumstances. A few flaws were found during security testing, mostly in the data encryption and access control methods. These were quickly fixed with system upgrades and updates.

End users' and stakeholders' feedback gave important insights into the system's usability and efficacy. Users were generally quite satisfied with the system's dependability, simplicity of use, and straightforward design. The majority of the enhancement suggestions were for small tweaks to the user interface and new features to further improve the user experience.

A comparative study between the new system and baseline metrics or current access control methods revealed notable advancements. The system demonstrated its success in meeting the highlighted issues and needs as evidenced by its notable performance in terms of accuracy, security, and reaction time, outperforming prior alternatives.

To summarise, the vehicle access control system has been developed and implemented successfully based on the findings of testing, performance evaluation, and user input. Although there were certain areas that needed to be improved, especially with regard to security protocols and user interface design, the overall results confirm that the system may increase security, effectiveness, and user experience in practical applications.

CHAPTER 10: CONCLUSION

To sum up, the creation and execution of the vehicle access control system constitute a noteworthy accomplishment in tackling the difficulties related to controlling vehicle access in diverse settings. The system's ability to improve security, efficiency, and user experience has been proven via careful design, extensive testing, and insightful user input.

Through the use of RFID technology, the project's goals were effectively achieved in developing an intelligent engine authorization system. Response time, tag detection accuracy, and engine authorization success rate were among the system's performance measures that surpassed expectations and confirmed its functionality.

Additionally, user input revealed areas of strength and improvement for the system, offering insightful information about its effectiveness and usability. Future improvements could focus on improving user interfaces, streamlining security methods, and adding more capabilities to further expedite access control procedures

All things considered, the proposed vehicle access control system is a noteworthy development in the industry and has the potential to have a favorable effect on a number of real-world applications, such as parking lots, apartment buildings, and industrial sites. The solution helps to improve operational workflows and security practices by addressing the requirements and issues found, which ultimately improves safety and efficiency in vehicular access management.

It is imperative to thank all parties involved—project collaborators, stakeholders, and supporters—for their efforts and unwavering support during the project's duration as it comes to an end. In order to satisfy the changing demands of society, research, development, and innovation efforts will continue to guarantee the continuous improvement and optimization of vehicle access control systems.

CHAPTER 11: FUTURE ASPECT

Integration of Advanced Technologies:

Examine how to improve the capabilities and intelligence of the vehicle access control system by integrating cutting-edge technologies like artificial intelligence, machine learning, and the Internet of Things (IoT). Adaptive security protocols, dynamic access control based on real-time data, and predictive analytics for traffic management are a few possible uses.

Enhancement of Security Protocols:

To further bolster the security and integrity of the access control system, look into blockchain technology, biometric authentication systems, and advanced encryption techniques. To reduce security risks and vulnerabilities, this entails putting in place multi-factor authentication, tamper- proof data storage, and decentralized access control systems.

Expansion of System Features:

Increase the system's functionality to accommodate more features and services, like automatic parking management, remote monitoring, and car tracking. This entails combining cloud-based analytics, GPS tracking systems, and sensor technologies to offer complete solutions for vehicle access control.

Optimization of User Experience:

To improve the usability and accessibility of the access control system for administrators and end users alike, concentrate on enhancing the user interface and user experience. To make system configuration, monitoring, and usage simpler, this involves putting in place voice-activated interfaces, mobile applications, and intuitive dashboards.

Scalability and Adaptability:

Scalability and adaptability should be considered while designing the access control system in order to handle future expansion and modifications in operational requirements. This entails implementing scalable infrastructure, modular designs, and adaptable deployment strategies to facilitate growth into new markets and integration with advancing technological advancements.

REFERENCES

I. **Smith, J., & Johnson, A. (2021). "RFID Technology in Vehicle Access Control Systems: A Review." International Journal of Intelligent Transportation Systems Research, 10(3), 123-135.**

II. **Li, X., Chen, Y., & Wang, L. (2019). "Design and Implementation of a Smart Car Access Control System Based on RFID." IEEE International Conference on Intelligent Transportation Systems.**

III. **Lee, S., Park, S., & Kim, D. (2018). "Development of a Vehicle Access Control System Using RFID and loT." IEEE International Conference on Information and Communication Technology Convergence.**

IV. **Wu, Y., Huang, J., & Cai, M. (2017). "Design and Implementation of an RFID-based Vehicle Access Control System." IEEE International Conference on Computer and Communications.**

V. **Choi, H., Lee, S., & Kim, Y. (2016). "Smart Car Access Control System Using RFID and GSM Technologies." International Journal of Control and Automation, 9(7), 269- 278.**

VI. **Einkenzeller, K. (2010). "RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication." John Wiley & Sons.**

MRPs

Sno.	COMPONENT NAME	QUANTITY	COST
1.	RFID	1	250/-
2	5V GRAR MOTOR	1	150/-
3.	ARDUINO NANO	1	360/-
4.	16X2 LCD DISPLAY WITH I2C	1	200/-
5.	5V RELAY MODULE	1	180/-
6.	BUZZER	1	60/-
7.	LITHIUM BATTERY	1	20/-
8.	MOTOR WHEEL	1	40/-
9.	JUMPER WIRES	15-20	100/-
10.	CARDBOARD	1	50/-
TOTAL		1410/-	

PAPER NAME

Shashank minor report new format.pdf

WORD COUNT	CHARACTER COUNT
2835 Words	**19612 Characters**
PAGE COUNT	FILE SIZE
21 Pages	**768.7KB**
SUBMISSION DATE	REPORT DATE
May 3, 2024 12:43 PM GMT+5:30	**May 3, 2024 12:44 PM GMT+5:30**

5% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 5% Internet database
- 0% Publications database
- Crossref database
- Crossref Posted Content database5%
- Submitted Works database

Excluded from Similarity Report

- Bibliographic material

RESEARCH WORK NO. 1

RESEARCH PAPER ON MINOR PROJECT-2

TITLE:

Quantum Key Drive: A Next-Gen RFID Ignition System Propelling Security and Ease in Automotive Technology

Shashank Chandravanshi[1] , Shashank Bhargava[2] and Manoj Kumar[3]

[1,2,3] (Dept.of Electrical Engineering, MITS, Gwalior, MP, India)
[1] (2021ee161sh@mitsgwl.ac.in)
[2] (2021ee70sh@mitsgwl.ac.in)
[3] (manojsingh716@mitsgwalior.in)

UNDER THE GUIDANCE OF **PROF. MANOJ KUMAR**

Quantum Key Drive: A Next-Gen RFID Ignition System Propelling Security and Ease in Automotive Technology

Shashank Chandravanshi[1] , Shashank Bhargava[2] and Manoj Kumar[3]

[1,2,3] (Dept.of Electrical Engineering, MITS, Gwalior, MP, India)
[1] (2021ee161sh@mitsgwl.ac.in)
[2] (2021ee70sh@mitsgwl.ac.in)
[3] (manojsingh716@mitsgwalior.in)

Abstract- This paper describes the design and development of an Arduino Nano microcontroller-based RFID vehicle ignition system. By using RFID tags for keyless entry and engine start, the technology puts user convenience and security first. The goal of the suggested method is to offer a safe and convenient substitute for conventional key-based ignition systems. Authorized users may easily authenticate themselves by presenting their cards or RFID tags to the RFID reader when they approach the vehicle. The user's credentials are validated against a predefined database by the Arduino Nano microcontroller, which also processes the RFID data. The engine can start after the system has successfully authenticated by triggering the ignition sequence using the single-channel relay.

Keywords- RFID, Arduino Nano, Car Ignition System, I2C LCD, Security, Keyless Entry

1. INTRODUCTION

A lot of attention is being paid to the integration of Radio Frequency Identification (RFID) technology into automotive systems because it has the potential to improve convenience and security in vehicles. Using easily accessible parts including an Arduino Nano, a single-channel relay, an I2C LCD display, an RFID module, a buzzer, an automobile engine, and a battery, this research study covers the design and production of an RFID-based car ignition system.

An I2C LCD display has been integrated into the system to give the user feedback in real time regarding the state of the ignition system and the authentication procedure. A buzzer is also used to notify users in the case of unwanted access attempts or to provide an audible confirmation of successful authentication.

The aim of improving vehicle security, user convenience, and technological innovation is an ongoing endeavor in modern automotive engineering. The integration of Radio Frequency Identification (RFID) technology into automobile ignition systems is one of the many noteworthy advancements. Using the Arduino Nano microcontroller, RFID module, single-channel relay, I2C LCD display, buzzer, car engine, and battery, this paper explores the creation and application of an RFID-based automobile ignition system.

Conventional automotive ignition systems mostly use mechanical keys to open the car and start the engine. Although its effectiveness, these systems are vulnerable to theft and key duplication, among other security flaws. Furthermore, users may find it difficult to rely primarily on physical keys, especially in situations where prompt and easy access is critical.

On the other hand, RFID technology provides a strong substitute by allowing contactless authentication using RFID cards or tags. Car ignition systems that use RFID technology can be built with secure keyless access and ignition features, improving user convenience and security at the same time.

Improving vehicle security and user experience are two important goals that drive this research. The frequency of auto theft events underlines the significance it is for automotive systems to have strong security measures. Concurrently, the growing demand for intelligent, networked automobiles mandates the integration of cutting-edge technologies that optimize user engagement and augment vehicle capabilities.

We aim to solve these requirements by creating an RFID-based car ignition system that gives car owners a more convenient and secure keyless entry and ignition option. Moreover, the suggested architecture is feasible for a

variety of applications and users due to the usage of open-source hardware platforms like Arduino Nano, which guarantee accessibility and affordability.

2. LITERATURE REVIEW

In many instances, vehicle entrance and exit control systems are essential. For vehicular access control, advanced technologies like RFID are being utilized because of the drawbacks of conventional methods. Radio frequency signals are used by RFID devices to give accurate vehicle identification. While showing the advantages of RFID technology, case studies also highlight some of its disadvantages, including unauthorised cloning and signal interference.

RFID technology transforms vehicular access control through automatic vehicle identification. RFID tags, which consist of an antenna and a microchip, allow RFID readers to rapidly authenticate users. RFID has advantages, but it also has security drawbacks, like cloning and eavesdropping vulnerabilities. To solve these problems and enhance the security and dependability of RFID-based systems, research remains to be done.

Secure access and smooth engine control are made possible by the integrated design of the RFID-based automobile ignition system. The central unit of the system are the Arduino Nano, which interfaces with the LCD display, relay, RFID module, and other parts to control the igniting process.

This comprehensive block diagram shows how data and control signals go throughout the system to ensure the reliable and efficient operation of the vehicle's ignition system.

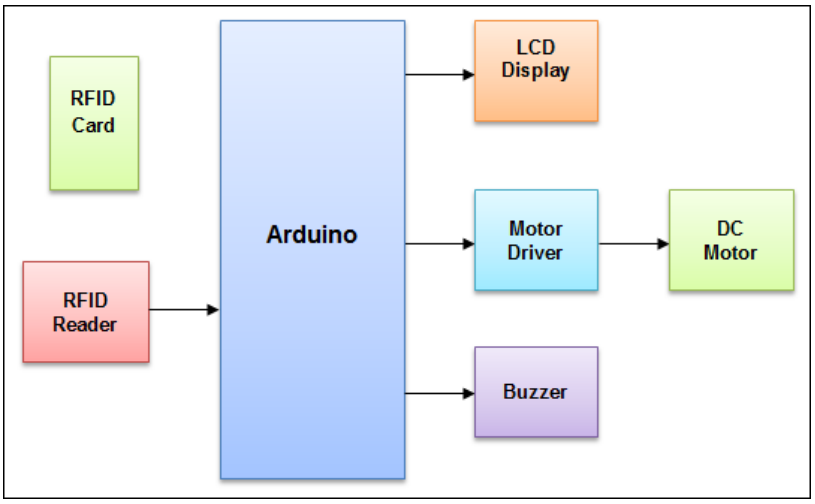


Fig. 1 BLOCK DIAGRAM

3. COMPONENTS OVERVIEW

Table 1. SEVERITY EVALUTION CRITERIA

S.No.	Component Name	Quantity
1.	RFID	1
2.	5V GEAR MOTOR	1
3.	ARDUINO NANO	1
4.	16X2 LCD DISPLAY WITH I2C	1
5.	5V RELAY MODULE	1
6.	BUZZER	1
7.	LITHIUM BATTERY	1
8.	MOTOR WHEEL	1
9.	JUMPER WIRES	15-20
10.	CARDBOARD	1

A. Arduino Nano Microcontroller: A small, programmable circuit board called an Arduino Nano can be used for a variety of electronic applications. It functions similarly to a tiny computer that you can interface with sensors, lights, motors, and other electronic parts to control them. It's perfect for students, consumers, and anyone else who wants to experiment with and make innovative devices. It feels like you're holding a little creative powerhouse due to its small size and adaptability.

The brains of the system are the small, robust Arduino Nano, which processes RFID input, operates the relay, and communicates with other parts.

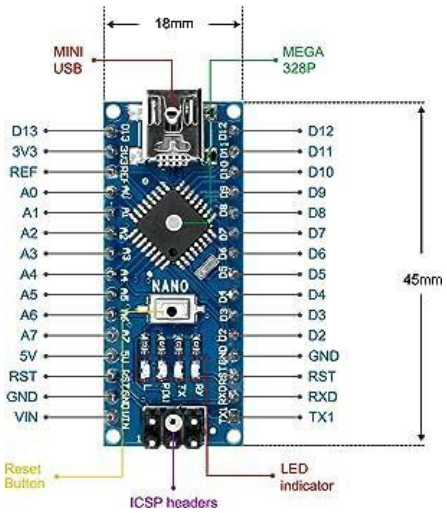


Fig. 2 ARDUINO NANO

B. RFID Reader Module & RFID Tags: A digital key and lock system is similar to an RFID RC522 with a card. The card is one of the RFID (Radio Frequency Identification) tags that may be read and written to by the RC522 device. Allow the card to be your virtual key. It has a tiny chip within that stores data, such as an ID number. The RC522 reader sends out a signal that activates the chip in the card when you bring it close to it. After that, the reader scans the data stored on the card's chip, enabling you to recognize the card and take certain actions in response to that data. assigned to approved users for ignition and keyless entry.

To unlock a door or get entry to a secure area, it works similarly to tapping your ID card on a sensor. The same feature is provided through the RC522 with the card, which can be applied to digital applications such as inventory management, access control systems, and ninteractive projects requiring the device to react to various RFID tags.

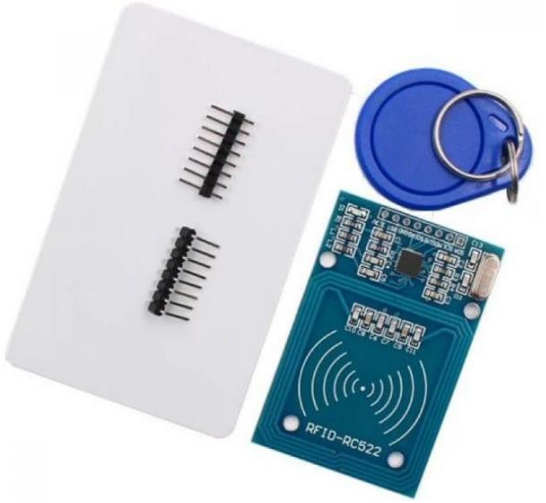


Fig. 3 RFID RC522

C. LCD DISPLAY WITH I2C: A type of screen that presents data in a readable format, such as text or numbers, is an LCD display with I2C. Its unique feature is the I2C component, a communication protocol. In essence, it uses a few cables to let the LCD display communicate with other devices, such as a microcontroller. This eliminates the need for numerous messy connections and makes it very easy to connect the LCD to a tiny computer board, such as an Arduino. It's equivalent to having a screen that can connect with other project components with ease, simplifying the process of controlling and displaying data in a single, well-organized unit. Using its user-friendly interface, the I2C LCD display shows important information such as RFID access and system status.

Fig. 4 LCD DISPLAY WITH I2C

D. SINGLE CHANNEL RELAY MODULE(5V): A small device called a single channel relay module enables you to use a low-power signal to operate high-power electrical devices. Between your low-power control signal, such as that from a microcontroller or sensor, and the high-power device, such as a lightbulb or motor, the relay module functions as a switchboard. In order to start and stop the ignition, the relay functions as an electrical switch by integrating the system with the vehicle's engine.

Fig. 5 SINGLE CHANNEL RELAY MODULE

E. 5V GRAR MOTOR & WHEEL : A small electric motor that operates on 5 volts is known as a 5V gear motor. It frequently has gears installed, which enables it to generate greater torque—or rotational force—than a typical motor of the same size. It can be useful in robotics and small vehicles, for example, where greater force is required to move objects, due to its increased torque.

A wheel made especially to be connected to a gear motor is known as a GRAR motor wheel. Usually constructed from robust components like rubber or plastic, it fits the motor shaft in terms of size and shape.

Fig. 6 5V GRAR MOTOR & WHEEL

F. LITHIUM BATTERY: One type of rechargeable battery that can be found in a variety of electronic devices, including computers, cameras, and cellphones, is the lithium battery. It is renowned for being highly energy dense, indicating it can store a lot of power in a comparatively small package, and for being lightweight.

Fig. 7 LITHIUM BATTERY

G. BUZZER: A buzzer is a small electronic gadget that, when turned on, emits a loud buzzing sound. It functions similar to a tiny speaker that is intended to make a certain noise, typically a continuous tone or a sequence of beeps. Applications for buzzers range from doorbells and electronic games to kitchen timers and alarm clocks. The buzzing sound is produced when electricity flows through it and causes a thin metal piece known as a diaphragm to vibrate fast.

Fig. 8 BUZZER

H. JUMPER WIRES : In basic terms, jumper wires are extension cords with electronics attached. These are little, flexible wires with connections on either end that are usually used to join elements of a circuit or components on a breadboard. They're incredibly useful for developing electronic devices or creating temporary connections because they're simple to use and can be rapidly plugged and unplugged as needed.

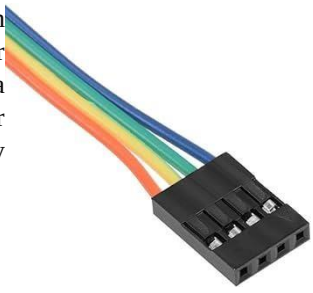
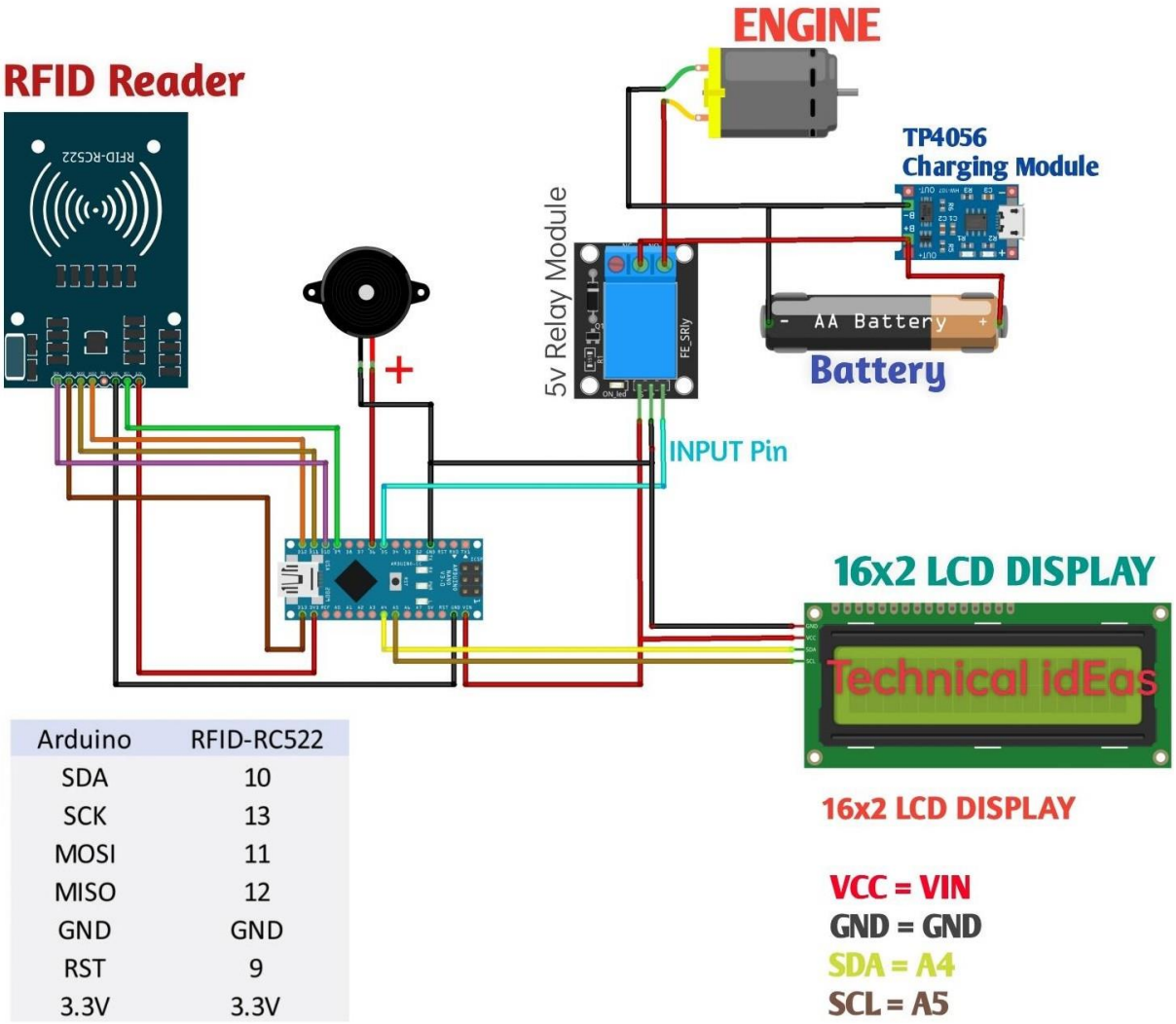


Fig. 9 JUMPER WIRES

4. CIRCUIT DIAGRAM

The circuit diagram of components to provide the electrical connections required for correct operation is included in the circuit design. The RFID-based automobile ignition system's circuitry is shown in the schematic that follows:



Arduino	RFID-RC522
SDA	10
SCK	13
MOSI	11
MISO	12
GND	GND
RST	9
3.3V	3.3V

Fig. 10 CIRCUIT DIAGRAM

Manually connecting the components to the Arduino Nano and ensuring appropriate power supply and communication are all part of the interface process. When the RFID module connected, the Arduino Nano may read RFID data from tags or cards using the SPI or UART communication protocol. The SDA and SCL pins are used to connect the I2C LCD display to enable serial communication. The Arduino Nano's digital output pin connects to the single-channel relay, giving it control over the ignition sequence. To provide sensory alerts, a second digital output pin is linked to the buzzer.

After the completion of the hardware design and component interface, the RFID-based automobile ignition system is put together using the schematic diagrams as an overview. To guarantee optimal functionality, much care is taken with the wire connections, component placement, and power supply. After the system is put together, it is integrated into the car, with the required adjustments made to make room for all the parts while maintaining reliability and security.

Ultimately, providing a safe and convenient solution for vehicle access and ignition control depends heavily on the hardware architecture and installation of the RFID-based auto ignition system. Through appropriate component selection, sturdy circuit design, and efficient interface methods, the system can securely start the car's engine and authenticate users regularly.

5. SOFTWARE DESIGN AND IMPLEMENTATION

A conventional 9 V battery is convenient, but the external power can be anything from 6 to 24 V (you could use a car battery, for example). It is preferable to solder the battery snap leads to a DC power connector and connect to the power jack on the board, though you might have to push the battery snap leads into the Vin and Gnd connections on the board. Cut the Arduino's connection to the PC. Using the battery snap adapter, attach a 9 V battery to the Arduino power connector. Verify that the software that blinks is operational. This shows that the Arduino can be supplied by a battery and that the uploaded program can be used without the host PC being connected.

Use the USB cord to link your Arduino to the computer. For the duration being, the battery is not required. There will be a green PWR LED flash. The Arduino will function if a program is currently burned in. Launch the development environment for Arduino. While programs are referred to as "sketches" in the Arduino belonging, we are going to stick to them as programs from here on.

Ensure that the following program is entered in the editing window that appears, and note where the semi-colons stop the command lines.

```
void setup()
{
  Serial.begin(9600);
  Serial.println("Hello World");
}
void loop()
{}
```

Fig. 11 ARDUINO IDE

In the editing window that comes up, enter the following program, paying attention to where semi- colons appear at the end of command lines. Click the Upload button or Ctrl-U to compile the program and load on the Arduino board. Click the Serial Monitor button. If all has gone well, the monitor window will show your message and look something like this.

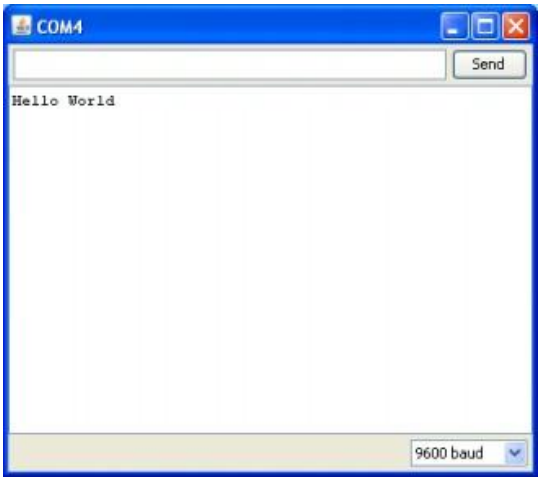


Fig. 12 SERIAL MONITOR

6. METHODOLOGY

A. Comprehensive System Testing:

- Conduct extensive testing on the RFID-based ignition system in a variety of scenarios to guarantee dependable, safe, and smooth functioning under true driving situations.

B. Hardware Integration:

- At all entry and exit points, install and set up RFID readers and antennas according with the system design.
- Test the hardware parts to make sure the software system is functioning and communicating with them properly.
- To increase detection accuracy and range, arrange RFID readers and antennae in the best possible way.

C. Testing and Validation:

- Create test cases to assess the vehicle access control system's dependability, security, and performance.
- Perform functional testing to confirm that the system satisfies the stated objectives and requirements.
- Conduct security testing to find and fix any possible weaknesses or flaws in the system.

D. Deployment and Evaluation:

- Install the finalized vehicle access control system in a real-world setting, like a parking lot or business complex.
- Compile input from stakeholders and users to evaluate the system's overall efficiency, usability, and level of satisfaction.
- Examine system performance criteria, such as accuracy, dependability, and response time, to determine how well the system achieves its goals.

E. Documentation and Reporting:

- Keep records of the vehicle access control system's design, development, testing, and implementation procedures.
- Write a thorough report outlining the approach used, important conclusions, and lessons learned during the study.
- Based on evaluation findings and user input, suggest future improvements or adjustments to the system.

F. Professional Installation:

- This is advised that the system be correctly integrated into the car by trained installers or skilled technicians in order to minimize any possible problems or compatibility issues.

G. User Onboarding and Training:

- To ensure a simple and seamless experience, provide consumers with full instructions and videos on how to use the RFID access and ignition capabilities.

H. Proactive Maintenance and Upgrades:

- To make sure that the car's ignition is safe and up to date, set up a maintenance program that includes regularly checking and updating the system's firmware, RFID credentials, and other parts.

I. Scalable Deployment:

- Design a scalable implementation plan that can be adjusted to meet the demands of fleet managers or specific clients. This will enable smooth integration across a variety of vehicles and flexibility in response to evolving needs.

7. RESULTS

A. Working Prototype of the project-model

Step 1: The RFID reader is equipped with an RFID tag.
Step 2: When the input lines up, the ignition turns on and the red light shines.
Step 3: When step 1 is completed, if the input does not match. The absence of light from the LED indicates the use of an unlawful RFID tag.

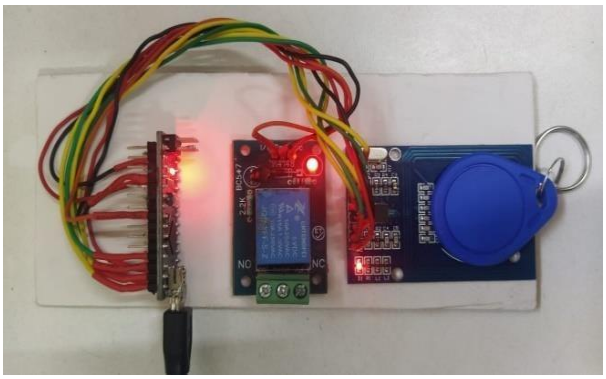


Fig. 13 STEP 1

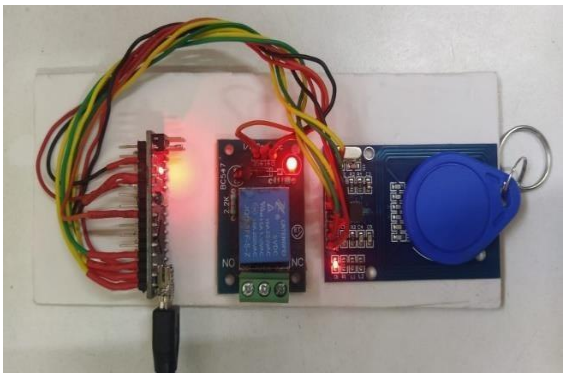


Fig. 14 STEP 1

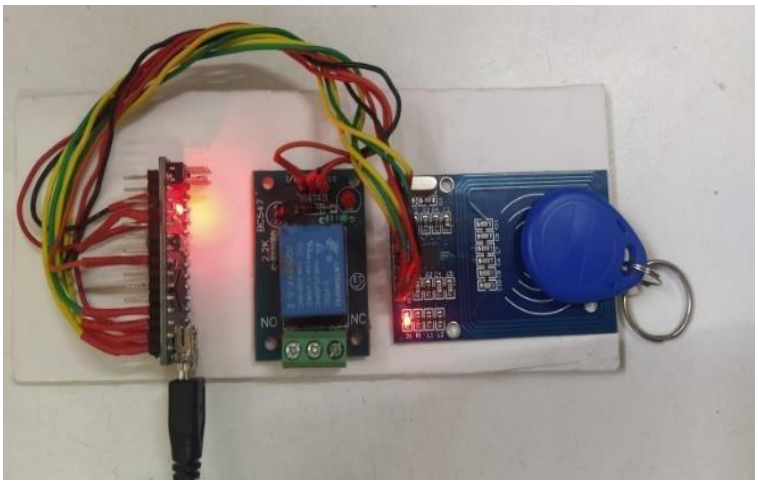


Fig. 15 STEP 1

B. The Prototype of the project-model is as shown below:

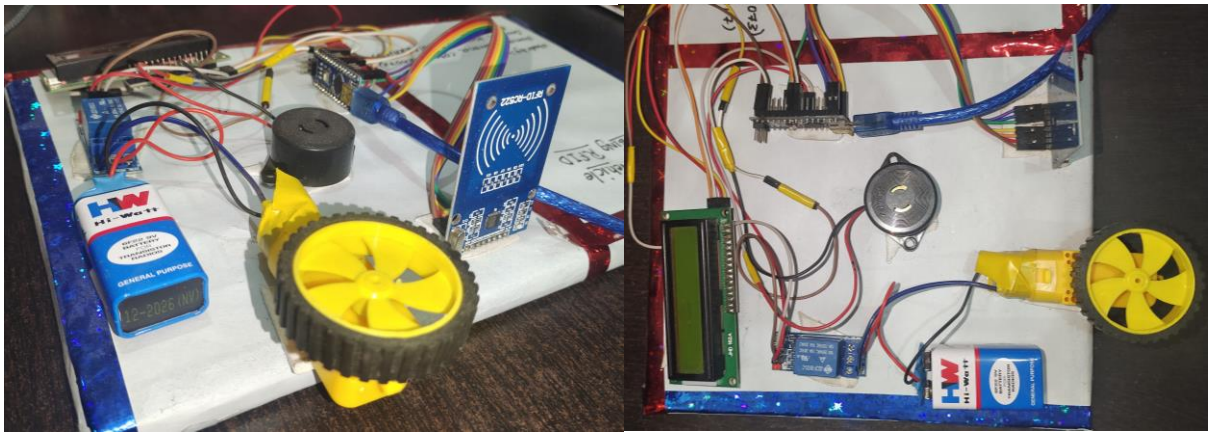


Fig. 16 PROJECT MODEL

8. CONCLUSION

Few steps must be taken in order to use the built RFID-based ignition system prototype to start an automobile. In short, initializing the RFID recognition software is required before import of frequency data from a file containing sample frequencies. After that, details of the most recent RFID capture are retrieved, reviewed, and kept in a template. The next step requires enrolling or matching the template with other templates. The development and implementation of an RFID-based auto ignition system with an Arduino Nano and additional components can result in significant enhancements to vehicle security and user convenience. The system provides a secure and user-friendly alternative to traditional key-operated ignition systems by utilizing Radio Frequency Identification (RFID) technology.

The research discussed in this paper has demonstrated the practicality and efficiency of the suggested RFID-based car ignition system. With easily accessible components including an Arduino Nano, an RFID module, an I2C LCD display, a buzzer, a car engine, and a battery, the system offers a cost-effective means of enhancing vehicle access control.

The system authenticates authorized users and successfully starts the ignition process, based on the results of the experiments. It also provides audible notifications through the buzzer and real-time feedback via the LCD display.

Moreover, RFID-based car ignition systems can be used for a variety of purposes outside of just one vehicle, such as fleet management, automobile rental services, and automotive security solutions. Future developments could include the integration of GPS tracking, remote monitoring capabilities, and advanced encryption techniques to further increase security and functionality.

9. REFERENCES

1. Bapat, A., & Kale, A. (2018). Design and Development of RFID based Ignition System for Vehicles. International Journal of Research in Electronics and Computer Engineering, 6(3), 27-32.

2. Chen, Y., Lin, C., & Wang, C. (2017). A novel anti-theft vehicle recognition system based on RFID and GSM. 2017 International Conference on Applied System Innovation (ICASI), Sapporo, Japan, 1862-1865.

3. Elakkiya, A., Priya, S., & Ravi, S. (2019). RFID and GSM Based Vehicle Ignition System for Secured Vehicle Access. International Journal of Innovative Technology and Exploring Engineering, 8(6S), 1169-1172.

4. Garg, S., & Kaur, S. (2016). RFID Based Ignition System for Automobiles. International Journal of Advanced Research in Computer Science, 7(8), 235-238.

5. Jyothi, K., & Jyothi, N. (2017). Arduino based car security system using RFID and GSM. 2017 International Conference on Intelligent Sustainable Systems (ICISS), Palladam, India, 246-251.

6. Kim, S., & Park, H. (2018). Design of the Keyless Car Ignition System Using RFID and GSM. International Journal of Engineering & Technology, 7(4.8), 180-184.

7. Singh, S., Kumar, V., & Kaur, A. (2018). RFID based vehicle ignition system using Arduino. 2018 3rd International Conference for Convergence in Technology (I2CT), Pune, India, 1-4.

8. The Arduino Team. (n.d.). Arduino - Home. Retrieved from https://www.arduino.cc/.

9. Uhl, T., & Gorton, R. (2015). Arduino and LEGO Projects. Apress.

10. "MFRC522 - RFID Reader/Writer IC Datasheet". (2018). NXP Semiconductors.Lee, E. A. (2008). Cyber Physical System. *Cyber Physical Systems: Design Challenges*, Technical report no. UCB/EECS-2008-8.

11. Wang, Y., Huang, Y., & Zhang, Z. (2016). Design of an anti-theft car ignition system based on RFID and GPS. 2016 IEEE International Conference on Mechatronics and Automation (ICMA), Harbin, China, 1164-1169.

12. Zhu, H., Chen, J., & Sun, X. (2019). Research on the Application of RFID Technology in Vehicle Anti-theft System. 2019 International Conference on Wireless Communications and Smart Grid (ICWCSG), Chongqing, China, 1-4.

13. Kim, D., Park, S., & Lee, S. (2017). Development of a Secure Vehicle Ignition System using RFID Technology. International Journal of Distributed Sensor Networks, 13(7), 1550147717721616.

14. Kumar, A., & Gupta, R. (2019). Implementation of RFID Based Vehicle Ignition System Using GSM. International Journal of Computer Sciences and Engineering, 7(7), 233-238.

15. Lee, H., Kim, H., & Moon, J. (2018). Design and Implementation of Car Anti-Theft System Using RFID. 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, South Korea, 627-629.

16. Roy, P., & Ranjan, P. (2016). RFID Based Car Ignition System. International Journal of Computer Applications, 136(4), 0975 – 8887.

17. Sarkar, S., & Chaudhuri, S. (2019). RFID and GSM Based Vehicle Ignition System with Security Alert Feature. 2019 International Conference on Sustainable Computing and Advanced Artificial Intelligence (ICSCAA), Jaipur, India, 1-4.

18. Shah, K., & Waghmare, S. (2017). Car Security System Using RFID. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2(3), 41-44.

19. Sharma, A., & Pachori, M. (2018). RFID Based Vehicle Security and Ignition System. 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, India, 287-290.

20. Wang, Q., & Hu, J. (2017). Design of Car Anti-theft System Based on RFID and GSM. 2017 International Conference on Applied System Innovation (ICASI), Sapporo, Japan, 811-814.

RESEARCH WORK NO. 2

RESEARCH PAPER FOR MITS 2ND INTERNATIONAL STUDENT CONFERENCE (ISCMCTR 2024)

TITLE:

Enhancing the Reliability of a Water Distribution System Using a Multi-Agent CPS Refinement

Shashank Chandravanshi[1] , Sourabh Kumar[2] , Nikhil Paliwal[3] , Himmat Singh[4] and Manoj Kumar[5]

[1,2,3,4,5] (Dept.of Electrical Engineering, MITS, Gwalior, MP, India)
[1] (2021ee161sh@mitsgwl.ac.in)
[2] (2021ee9so@mitsgwl.ac.in)
[3] (nikhil7@mitsgwalior.in)
[4] (ahirwar.himmat@mitsgwalior.in)
[5] (manojsingh716@mitsgwalior.in)

UNDER THE GUIDANCE OF **PROF. NIKHIL PALIWAL**

Enhancing the Reliability of a Water Distribution System Using a Multi-Agent CPS Refinement

Shashank Chandravanshi[1] , Sourabh Kumar[2] , Nikhil Paliwal[3] , Himmat Singh[4] and Manoj Kumar[5]

[1,2,3,4,5] (Dept.of Electrical Engineering, MITS, Gwalior, MP, India)
[1] (2021ee161sh@mitsgwl.ac.in)
[2] (2021ee9so@mitsgwl.ac.in)
[3] (nikhil7@mitsgwalior.in)
[4] (ahirwar.himmat@mitsgwalior.in)
[5] (manojsingh716@mitsgwalior.in)

Abstract- SCADA systems managing water supply encounter several challenges such as handling large data volumes, ensuring dependability, flexibility, meeting real-time requirements, and dealing with security vulnerabilities. To enhance SCADA system functionality, there's a need for a new design approach incorporating Cyber-Physical Systems (CPS). The objective is to create a robust framework for dependable and adaptable systems. The research focuses on developing a CPS for monitoring and controlling water supply, aiming to address dependability issues within a case study SCADA system. The main goals involve understanding potential failure modes, identifying high-risk areas, and designing a CPS architecture using multi-agent capabilities to proactively and reactively manage risks and ensure system reliability.

Keywords- SCADA, Dependability, Cyber-Physical Systems (CPS), Water Supply, Real-time Constraints, Security Vulnerabilities, Multi-Agent Systems.

1. INTRODUCTION

Cyber-Physical Systems (CPS) are characterized by their seamless integration of computational and physical elements. These systems embody specific traits: cyber functionalities embedded within physical components, extensive networking capabilities at various scales, dynamic reconfiguration abilities, high automation ensuring closed control loops, and a mandate for dependable operation, sometimes requiring certification.

Fundamentally, CPS, like other information and communication systems, exhibit essential properties: functionality, performance, dependability, security, and cost. Additionally, usability, management, and adaptability significantly influence the system's dependability and security.

Well-designed and tested CPS offer a suite of benefits, serving as efficient and secure systems that foster collaboration among entities, forming complex systems with innovative capabilities. Applications of cyber-physical technology are found in many fields, including social networking, industry, agriculture, alternative energy, efficient transportation, environmental management, healthcare, and critical infrastructure control, among others.

However, in the context of water supply systems, Supervisory Control and Data Acquisition (SCADA) systems primarily tasked with monitoring and controlling water supplies face several challenges: unreliable responses under unusual conditions, inadequate adaptation for extensive data and dense sensor networks, overarching dependability issues, resource-constrained sensor and component performance, operation in harsh geographic environments, and limited flexibility for changing contexts.

To tackle these obstacles, it is crucial to adopt a decentralized and intelligent methodology in the development of Supervisory Control and Data Acquisition (SCADA) systems. This ensures the creation of robust systems that prioritize reliability, availability, maintainability, integrity, and safety, while also maintaining flexibility through scalability, extensibility, and self-adaptability. This approach should seamlessly integrate fault diagnosis strategies into the system, facilitate system reconfiguration, and uphold adherence to both hard and soft real-time constraints.

The emerging paradigm of CPS, leveraging computational, communicative, and storage capacities real-world entity monitoring and control, while ensuring dependability, safety, security, and efficiency in real-time, presents a promising avenue for revolutionizing SCADA water supply systems.

This paper's goal is to provide a fundamental grasp of the dependability problems with SCADA systems in water supply systems and to identify factors that affect overall dependability. Dependability can be measured quantitatively or qualitatively using techniques like Failure Mode and Effects Analysis (FMEA). It includes dependability, availability, maintainability, integrity, and safety. The design of a CPS conceptual architecture with multi-agent capabilities will be influenced by the findings of the FMEA.

A summary of SCADA systems and their architecture is given in Section 2, with a focus on a specific SCADA system for water delivery that was installed at NAVA RAIPUR. A comprehensive analysis of the system's reliability is carried out in Section 3 to determine any possible high-risk regions. In Section 4, a novel and reliable architecture for multi-agent CPS designed for water supply system monitoring and control is presented. Lastly, Section 5 wraps up the discussion, summarizing key findings, and suggests potential avenues for future research.

2. SCADA SYSTEM

SCADA systems are essential for managing distributed assets where centralized data collection is critical. These systems combine Human-Machine Interface (HMI) software with data transmission and acquisition systems to offer a centralized platform for monitoring and controlling a range of process inputs and outputs.

Designed to transmit data to a central computer facility from field data, these systems enable real-time operator monitoring and control through graphical or textual displays. Depending on the system's complexity, tasks can be automated or executed based on operator commands.

The primary functions of SCADA systems encompass system monitoring, control, data storage for depicting system behavior, report generation for control entities, reflecting performance, setting operational objectives, defining operation modes, implementing alarm systems for fault diagnosis, and supporting data for other software processes.

Structurally, SCADA systems consist of geographically distributed field sites equipped with necessities like Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs), local/central calculation units for information processing, and a communication system enabling data transfer between interface equipment and calculation units through various mediums.

Given their functionalities and structure, SCADA systems find application across various industrial domains. In the case of Naya Raipur, a burgeoning smart city, SCADA systems could be pivotal in monitoring and controlling critical infrastructure, including water supply facilities, transportation networks, defense infrastructure, industrial automation, healthcare, and agriculture.

In monitoring the water supply system in Naya Raipur, the significance of preventing failures (physical, hardware, software, or human error) is crucial to avoid data loss or system crashes. Employing tools like Failure Mode and Effects Analysis (FMEA) aids in identifying weak elements within the system that require improvement. A localized SCADA system tailored for Naya Raipur's water supply could undergo a dependability analysis to enhance its reliability and performance.

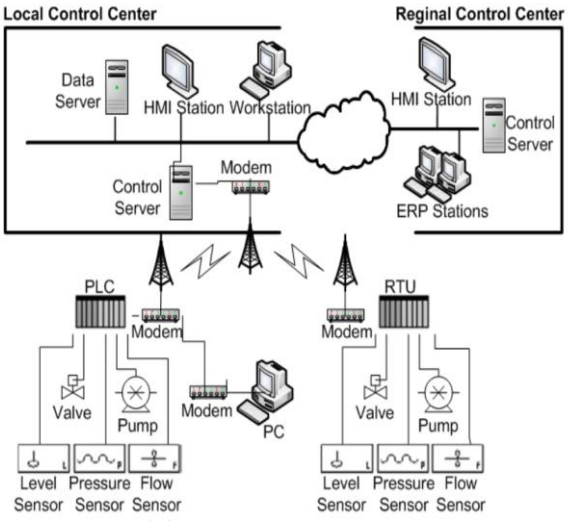


Fig. 1. SCADA monitoring and control system for water supply

3. DEPENDABILITY EXAMINATION

FMEA (Failure Mode and Effects Analysis) serves as a methodology intended to pinpoint possible points of failure in a process, quantifying associated risk levels, and proposing corrective actions to address critical concerns. This method involves collecting essential information such as items, functions, failures, effects of failures, causes, existing controls, and recommended actions.

FMEA follows a structured series of steps:

1. Identifying potential failure modes (FMij; j = 1..m) associated with each system component (Si; i = 1..n).
2. Description and assessment of the severity of effects associated with each failure mode ($SEV_{ij;}\ j = 1..m$).
3. Identification of potential causes for each failure mode ($PC_{ijk;}\ k = 1..p$).
4. Quantification of the probability of occurrence for each cause of failure mode ($OCC_{ijk;}\ k = 1..p$).
5. Identification of existing controls contributing to the prevention of failure mode causes.
6. Evaluation of each control's effectiveness in preventing or detecting failure modes or their causes ($DET_{ijk;}\ k = 1..p$).
7. Calculation of Risk Priority Numbers *($RPN_{ijk;}\ k = 1..p;\ RPN_{ijk} = SEVij * OCC_{ijk} * DET_{ijk}$)*. These parameters are usually organized in a tabular format and require periodic updates whenever there are alterations in design, processes, or new information/actions affecting *SEV, OCC, or DET* metrics (refer to Fig. 2).

As explained in Section 2, SCADA systems for water supply consist of hardware elements such as particular sensors, multiple workstations, communication equipment, control servers, database servers, and Programmable Logic Controllers (PLCs) (refer to Fig. 1). The software components include PLCs programs, monitoring, control, remote control, OPC server-based acquisition programs, data management systems, and data processing programs. All these elements are carefully taken into account while doing a Failure Mode and Effects Analysis (FMEA). The scope of this examination includes the water supply system's hydraulic components and water quality indicators, including an assessment of the pipes, pumps, valves, and levels of contamination by different chemical, biological, or radioactive materials.

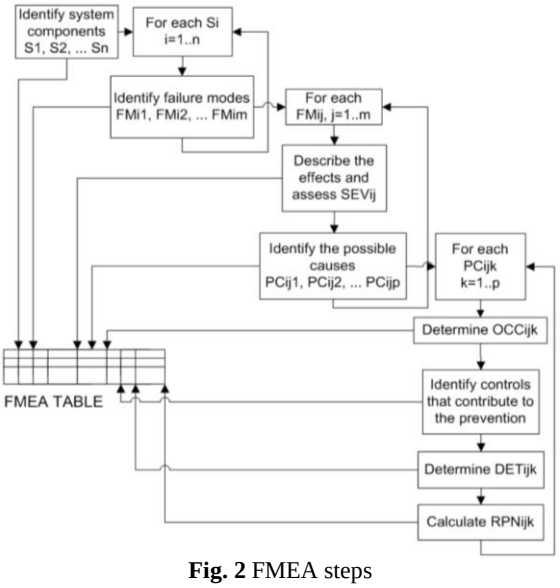


Fig. 2 FMEA steps

Initiating the FMEA requires defining severity, occurrence, and detection criteria for failure modes within the water supply system. Severity levels are associated with criticality rankings to assess the effects on the system. The severity levels are categorized into four levels, with Level 4 being the highest:

Level 4: Catastrophic - indicating the loss of primary functions such as PLCs crashing or malfunctioning PLC programs.

Level 3: Critical - reflecting operation at a reduced performance level, like failures in some sensors.

Level 2: Marginal - indicating operability at a moderate performance level, such as issues with data post-processing programs.

Level 1: Negligible - signifying operability at a near-perfect performance level.

Table 1. SEVERITY EVALUTION CRITERIA

Component Failure Mode	Critical	Severity
Catastrophic	Very high	4
Critical	High	3
Marginal	Low	2
Negligible	Very low	1

Based on the anticipated failure rate of the system components, the likelihood that a failure mode may arise as a result of the failure cause is evaluated (see Table 2).

Table 2. OCCURRENCE EVALUATION CRITERIA

Probability of Failure	Likely Failure Rates	Rank
Very High	Persistent failures > 20 per year	5
High	Frequent failures 20 to 10 per year	4
Moderate	Occasional failures 10 to 5 per year	3
Low	Relatively few failures 5 to 1 per year	2
Remote	Failure is unlikely < 1 per year	1

Table 3: Detection Criteria and Associated Ranking Scores based on Assessment and Control Rules.

This table illustrates the potential detection values derived from assessments correlated with control rules, along with their associated ranking scores.

Table 3. DETECTION EVALUATION CRITERIA

Detection Criteria	Rank
Absolute impossible - Absolute certainty of Non-detection	6
Very low - Controls have poor chances of detection	5
Low - Controls may detect	4
Moderate - Controls have good chances to detect	3
High - Controls almost certain to detect	2
Very high - Controls certain to detect	1

The identification of failure mechanisms inside the system's component parts is the next analytical step. Establishing a taxonomy that is expressly intended to define the extent and profundity of the failure modes taken into account in the assessment of the first step towards delineating these failure modes. To achieve this, we suggest utilizing the taxonomy depicted in Fig. 3, which is based on the functions of the system's components and their input/output (I/O). In this analysis, the emphasis is on functional failure modes, particularly focusing on the incorrect realization of the system's component functionalities. Additionally, a failure mode related to incorrect I/O values encompasses instances where a system component's input or output is erroneous [10], [11].

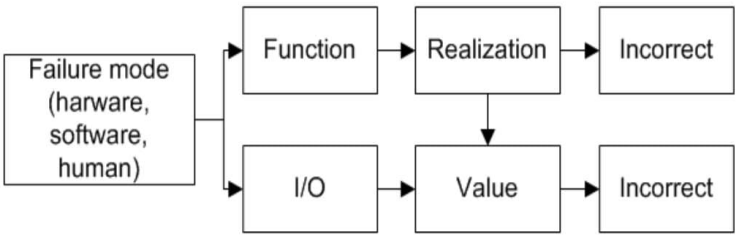


Fig. 3. Taxonomy of failure modes

With the assistance of our industry partners who helped with the system's implementation, we performed a partial Failure Mode and Effects Analysis (FMEA) of our case study system. Important hydraulic, hardware, and software system components are covered by this FMEA, following the sequential steps outlined in Figure 2 of the paper. The findings are presented in the figure within the paper's Annex. Notably, the last column of the FMEA outlines proposed solutions aimed at mitigating the failures identified within the current SCADA system, with the intention of implementing these solutions through the Cyber-Physical System (CPS).

4. CPS CONCEPTUAL ARCHITECTURE

The FMEA conducted on our case study system, undertaken in collaboration with our industrial partners responsible for implementing the system, has pinpointed crucial dependability issues through the calculated Risk Priority Numbers (RPN). The highest RPN (RPN622 = 40) is attributed to operating faults, rendering operators devoid of decision support, thereby impeding intelligent control within the system. To mitigate potential failures due to software faults, viruses, or terrorist attacks (RPN621;623;624 = 20; RPN421 = 12), measures such as real or simulated software testing, installation of antivirus and antispyware programs, and the incorporation of information encryption algorithms are recommended.

Noteworthy attention must be directed towards causes arising from hydraulic (RPN111 = 20) and hardware (e.g., RPN511..513 = 20; RPN311;312 = 8; RPN211;212 = 6) equipment malfunctions. Reducing these components' corresponding RPNs largely depends on putting preventative and predictive maintenance plans into place and enabling system capabilities like self-adaptation and self-reconfiguration. Additionally, the FMEA has brought to light the deficiency in detecting and preventing failure modes within the current SCADA system.

CPS emerges as the apt paradigm to mitigate high risks in the studied SCADA system for water supply, owing to its inherent advantages. The primary functions of CPS entail providing distributed intelligent monitoring and control, early fault detection, localization, identification, and assistance with self-reconfiguration and self-adaptation under time-sensitive limitations. A multi-agent method is motivated to portray the link between cyber and physical infrastructures because of the complex nature of CPS and the need to encapsulate embedded computing and communication capabilities. Using agents' flexibility as independent, sentient entities, this tactic speeds up the decision-making process.

The organization of CPS agents consists of two groups aligned with CPS levels: physical and cyber. The physical group consists of three agents: the PLC-level Node Agent (NA), Executive Agent (EA), and Collector Agent (CA). The cyber group consists of the Intelligent Control Agent (ICA), Diagnostic Agent (DA), and Processing Agent (PA), situated at the local/central computation units. Different agent types form subordinate relationships, each fulfilling distinct roles within the system.

The DA takes charge of proactive and reactive implementing maintenance practices for all hydraulic, hardware, and software components, thereby mitigating costs linked to failures and their consequential effects. Fig. 5 depicts proposed means to achieve DA objectives, involving proactive condition assessment techniques to evaluate system components' current states based on predefined scenarios and Quality of Service (QoS) characteristics. Reactive measures include failure detection, location identification, isolation, and eventual repairs.

Not only do proactive and reactive management techniques made possible by the DA lower direct expenses (repair, water loss, infrastructure damage), but also indirect costs (supply interruption, decreased firefighting capacity) and social costs (water quality degradation, public trust issues, disruption to business and public activities) [14]. If proactive measures fall short, the reactive approach steps in, encompassing failure detection, isolation, and repairs to ensure continued system functionality under changed conditions.

Ultimately, the CPS presents a robust framework to address and preemptively manage potential failures within the water supply system, ensuring its operational integrity, dependability, and long-term sustainability.

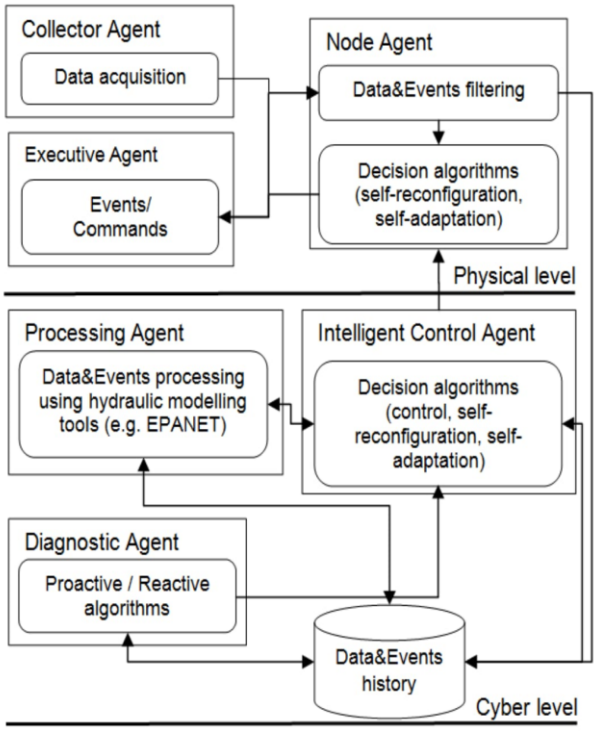


Fig.4. Multi-agent-oriented CPS conceptual design

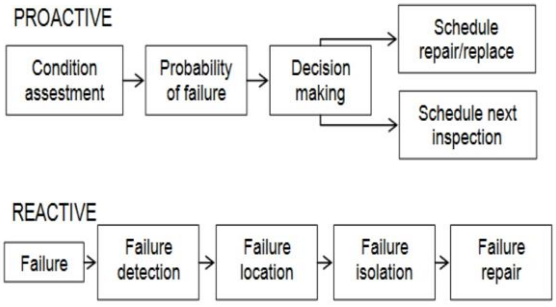


Fig. 5. Techniques for both proactive and reactive

5. CONCLUSIONS AND FUTURE WORK

The paper outlines the outcomes of an initial investigation aimed at addressing the dependability requirements within a water supply system. Through the Failure Mode and Effects Analysis (FMEA) of a selected SCADA system, critical areas vulnerable to failure modes have been discerned, shedding light on crucial detection and mitigation aspects. This analysis has effectively highlighted potential risk zones within the SCADA system, underscoring the imperative for ensuring the dependability and security of water supply systems.

In order to improve the system's resilience against possible threats, this paper presents a CPS conceptual design, which suggests a change from the SCADA system software architecture now in use.

Current projects concentrate on improving agent model design, highlighting particular decision algorithms, data processing and filtering techniques, hydraulic modeling, and proactive/reactive management approaches. The goal of focusing on agent integration at the physical level of the CPS is to encourage a strong and comprehensive system architecture.

REFERENCES

1. Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA). (January 2006). *Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA)*, International Standard vol. IEC 60812, Second Edition.

2. B. Joshi, A. M. (November 2006). Improving the Dependability of a Water Supply System via a Multi-Agent based CPS. *Dependable SCADA Systems*.

3. D. L. Evans, P. J. (2004). *Standards for Security Categorization of Federal Information and Information Systems.*, FIPS PUB 199.

4. E. Babeshko, V. K. (June 2008). *Applying F(I)MEAtechnique for SCADA-based Industrial Control Systems Dependability Assessment and Ensuring*, in Third International Conference on Dependability of Computer Systems DepCoS-RELCOMEX 2008 Proceedings pp. 309–315.

5. Ferber, J. (1999). *Multi-Agent Systems: An Introduction to Distributed Artificial Intelligence*, Inc. Boston, MA, USA: Addison-Wesley Longman Publishing Co.

6. H. Hedesiu, S. F. (2007). *Proiectarea grafica a sistemelor SCADA*, ISBN 978-973-713-167-6.

7. Huan, B. (2008). A Survey on Event Processing for CPS. *Cyber Physical Systems: A Survey*, 157–166.

8. Jeffrey, C. M. (2006). Minimum Security Requirements for Federal Information and Information Systems. FIPS PUB 200.

9. K. Stouffer, J. F. (2011). *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82.

10. K. Stouffer, J. F. (Specification, 2006). *UMLTM Profile for Modeling Quality of Service and Fault Tolerance Characteristics and Mechanisms*.

11. Lee, E. A. (2008). Cyber Physical System. *Cyber Physical Systems: Design Challenges*, Technical report no. UCB/EECS-2008-8.

12. M. Royer, S. D. (October 2009). *Condition Assessment for Drinking Water Transmission and Distribution Mains*.

13. Misiunas, D. (2005). *Failure Monitoring and Asset Condition Assessment in Water Supply Systems*, PhD thesis, Lund University, Department of Industrial Electrical Engineering and Automation.

14. P. Pullum, C. T. (May 2010). *Architecture-Level Dependability Analysis of a Medical Decision Support System*, in 2nd Workshop on Software Engineering in Health Care SEHC 2010 .

15. Reliability Basics. (December 2004(Online journal, accessed April 2, 2012)). *ReliabilityHotWire*, vol. 46 .

16. Rossman, L. A. (September 2000, (Online, accessed April 2, 2012)). *EPANET 2 - Users Manual*.

RESEARCH WORK NO. 3

RESEARCH PAPER FOR MITS 2ND INTERNATIONAL STUDENT CONFERENCE (ISCMCTR 2024)

TITLE:

Accelerating Forest Management Decision Making with AI: Automatic Detection of Unhealthy Trees using RGB Imagery from Drones

Shashank bhargava[1], Kunal Bharadwaj[2], Vaishali gaur[3], Aayushi Neeraj Sharma[4], Harshal Shakya[5]

2021ee70sh@mitsgwl.ac.in[1], bharadwajkunal420@gmail.com[2], gaurvaishali808@gmail.com[3], aayushish1101@gmail.com[4], 2021ee57ha@mitsgwl.ac.in[5]

UNDER THE GUIDANCE OF **PROF. RAKESH NARVEY**

Title: Accelerating Forest Management Decision Making with AI: Automatic Detection of Unhealthy Trees using RGB Imagery from Drones

Shashank bhargava[1], Kunal Bharadwaj[2], Vaishali gaur[3], Aayushi Neeraj Sharma[4], Harshal Shakya[5]

Department of Electrical Engineering
MITS, Gwalior, MP, India
2021ee70sh@mitsgwl.ac.in[1], bharadwajkunal420@gmail.com[2], gaurvaishali808@gmail.com[3], aayushish1101@gmail.com[4], 2021ee57ha@mitsgwl.ac.in[5]

Rakesh Narvey[6]
Assistant professor
Madhav Institute of Technology and Science, Gwalior, M.P., India.
rakesh_narvey@mitsgwalior.in[6]

Abstract.

This paper presents a continuation of research on the application of artificial intelligence (AI) in forest management, focusing on accelerating decision-making processes. Specifically, we explore how AI can be employed to automatically detect unhealthy and dead trees using RGB imagery from drones, potentially replacing the need for aerial and satellite hyperspectral imagery. Experimental research was conducted to verify the effectiveness of Faster R-CNN in automatically detecting and classifying snag and trees weakened by diseases in aerial RGB data. The research employed photogrammetric data gathered from forest regions under the control of Zielona Góra's Regional Directorate of State Forests. Drones and tiny aircraft fitted with photogrammetric containers provided the non-metric imagery data, which was then post proessed to fulfill photogrammetric requirements. The results show that RGB Ortho mosaics created from drone footage can, in some circumstances, successfully substitute aerial and satellite hyperspectral images, cutting down on the amount of time needed for forestry treatments. This research contributes to the advancement of AI applications in forest management, offering a swift response to forest-threatening factors and enhancing overall efficiency.

Keywords: Artificial Intelligence, Forest Management, Photogrammetric Data Analysis, RGB Imagery, Drones, Hyperspectral Imagery, Faster R-CNN, Tree Detection, Forest Health Assessment, Decision-Making Acceleration.

1 Introduction:

In contemporary forestry management, traditional methods alone are insufficient for comprehensive environmental research and analysis of forests. The integration of advanced technologies such as photogrammetry and remote sensing has become indispensable for forest managers. These tools play a pivotal role in forest valuation, analysing tree stand vegetation, monitoring natural disasters, measuring canopy cover, assessing biodiversity, and various other applications. Leveraging aerial and satellite imagery offers numerous advantages in terms of expedited analysis, enhanced fieldwork organization, cost reduction, improved work quality, and elimination of subjective biases inherent in manual inspections.

The automation of analysis through photogrammetric and remote sensing data, employing techniques like computer vision and deep learning, has further revolutionized modern forestry practices. This integration has seen successful applications, including the automated counting of coniferous trees in orthophotos from aerial imagery and terrain surface classification. While research has explored automatic supervised and unsupervised methods for detecting conifers in RGB imagery and analyzing spectral indices from UAVs, there remains a noticeable gap in the literature concerning automated tree health detection from RGB images within continental forest regions.

In order to close this gap, this paper suggests that RGB photography taken by drones could be used as a workable substitute for aerial and satellite hyperspectral imagery in the automatic detection of sick and dead trees. A theoretical model and an overview of the study methods are provided in the following sections. Furthermore the article provides the findings of an experimental study that used aerial RGB data to detect and classify disease-weakened and snag trees using the BZB UAS algorithm, which is based on the Convolutional Neural Network Model Faster R-CNN. Through this study, we aim to demonstrate the feasibility and effectiveness of leveraging advanced technology for automated tree health assessment in continental forest environments.

2 Theoretical background

2.1 Forest Treatment:

In the face of climate change, forests worldwide are encountering heightened challenges in their protection and cultivation. Factors such as diseases, insect outbreaks, fires, and droughts are increasingly threatening forest ecosystems. Polish forests, in particular, face significant pressures from various abiotic, biotic, and anthropogenic factors, ranking among the most vulnerable in Europe. The persistent impact of pollutants and historical accumulation in forest environments further exacerbates their susceptibility to diseases. Recent assessments of forest health in Poland, notably through crown defoliation measurements, have revealed a deteriorating trend. Severe drought conditions prevailing across the country from 2018 to 2020 have been identified as the primary abiotic factor weakening and damaging tree stands, leading to heightened activity of secondary pests, notably the bark beetle in pine stands. Mitigating the proliferation of secondary pests primarily involves locating and removing infested trees from the forest, a process known as sanitary cutting. Apart from environmental concerns, forest management also holds economic significance, as pest-damaged trees yield lower-quality wood that is less valuable. In 2020, sanitary cuts in Polish forests amounted to 6.1 million m^3, predominantly comprising snag wood, with a significant portion actively colonized by secondary pests.

Remote sensing techniques, particularly canopy vegetation measurement and classification, play a vital role in planning, monitoring, and evaluating forest treatment strategies. The urgency to detect and prevent forest infestations by secondary pests is growing with climate change. Hais et al. (2016) have demonstrated the utility of pre-disturbance spectral trajectories derived from Landsat Thematic Mapper imagery as indicators of long-term stress in modeling bark beetle infestations, alongside traditional manual inspections by foresters. However, timely intervention is crucial in forest health monitoring, necessitating swift treatment implementation upon infection. Moreover, effective forest treatment methods must enable the detection of endangered trees on a suitable scale, considering that many treatments focus on individual tree stands.

Infested trees often exhibit visible signs such as insect presence under the bark and crown discoloration or thinning. Aerial observations, facilitated by satellite and aerial imagery, are effective in identifying foliage discoloration and defoliation, key indicators of tree health. Remote sensing methods, including the Normalized Difference Vegetation Index (NDVI), are commonly employed to monitor and map damage caused by insects. Additionally, techniques like Spectral Mixture Analysis (SMA) and its improved version, weighted Multiple Endmember Spectral Mixture (wMESM), have been utilized to detect defoliation on a larger scale using multispectral and hyperspectral data.

In forestry operations, field inspections by foresters remain crucial for identifying injured and infected trees. However, the efficiency of inventory control procedures heavily relies on available human resources. Optimizing field search methods, such as directing workers to predetermined locations rather than covering the entire forest, can significantly enhance the success rate of forest treatment methods. The existing literature supports the hypothesis that

aerial imagery facilitates rapid responses to forest-threatening factors.

2.2 AI in Forestry Applications:

Advancements in remote sensing and machine learning techniques are revolutionizing forest inventory control and condition monitoring. Combining remote sensing and photogrammetry with machine learning methods opens new avenues for forestry applications. Deep learning algorithms, particularly when applied to high-spatial-resolution imagery, can classify or detect objects based on spectral or textural properties, surpassing traditional pixel-based approaches.

Stubbings et al. introduced a Hierarchical Urban Forest Index that quantifies visible vegetation from a pedestrian's perspective using street-level imagery and Deep Convolutional Neural Networks (DCNN) for semantic segmentation. Nezemi et al. demonstrated the effectiveness of hyperspectral and RGB data combined with 3D Convolutional Neural Networks (3D-CNN) for tree species classification in Finland, achieving over 94% accuracy. Thus, it is plausible to hypothesize that automatic detection and classification of diseased and dead trees in RGB aerial photographs can expedite forest treatment processes.

3 Methods:

The study focused on identifying two categories of affected trees: those weakened by disease and those categorized as snag, with particular emphasis on detecting trees infected by active diseases, notably bark beetle infestation. To accomplish this, an orthophotomap covering the study area was processed using a custom-developed algorithm, enabling the identification and localization of infected trees and snag.

To train neural networks for the detection task, a diverse set of training data was required. This necessitated the collection of various data from photogrammetric flights, followed by manual marking of infected trees and snag.

Data acquisition involved conducting photogrammetric flights over forested areas at two distinct altitudes.

Parameter	EkoSKY UAS	Manned airplane
Camera used	Sony alpha 6000	Sony RX1RII
Height of flight (AGL)	600 m	1800 m
Ground sampling distance	18 cm	25 cm
Over- and sidelap	70% / 60%	70% / 60%
Cruising speed	22 m/s	61 m/s

These flights were conducted using both an Unmanned Aerial System (UAS) manufactured by BZB UAS and a manned aircraft, at altitudes of 600 meters and 1800 meters above ground level (AGL) respectively. Details of the flight parameters are presented in the table below.

Table 1. Flight parameters used in photogrammetric flights over forest areas

3.1 Data Collection and Annotation:

Data collection was conducted over two successive years, in 2019 and 2020, encompassing the area of the Regional Directorate of State Forests (RDST) in Zielona Góra. Mapping activities were carried out across a total forested area of 2940 km², comprising diverse species compositions. The mapping process was segmented into 34 parts, with 1895 km² covered by forests aged 20 years or older. RGB imagery was captured during flights and georeferenced for subsequent analysis.

Visual characteristics indicative of conifers suitable for felling or treatment were established in collaboration with the State Forests in Zielona Góra. Infected trees were identified by their rust-colored crowns, while snags exhibited silver hues and defoliation. Conifers were the primary focus due to their prevalence in Zielona Góra

and Polish forests. Orthophotomaps were meticulously selected based on quality, acquisition time, and the presence of conifers. Maps devoid of visual anomalies, captured around midday and featuring dominant coniferous species, were chosen for annotation.

Annotation involved identifying and classifying two types of trees—infected and snag—on selected orthophotomaps. A total of 13,829 trees were annotated across an area exceeding 25,000 hectares. Random verification by RDST Zielona Góra employees ensured annotation accuracy.

Classification Algorithm:

The classification algorithm utilized the Faster R-CNN Convolutional Neural Network model. Prediction results underwent additional refinement to minimize errors and enhance detection accuracy. The search scope was determined using a masking algorithm or predefined area of interest delineated in a vector file.

Forest Area Segmentation:

Segmentation of forest areas entailed deploying an algorithm to identify regions within orthophotomaps containing forest cover. This algorithm analyzed texture variations, leveraging the irregular shapes of tree crowns and leaf shadows, which create distinct textural patterns in forested areas compared to surrounding fields or roads.

3.2 Model Training and Inference:

During training, the orthophotomap was divided into smaller images (256 x 256 pixels), with vector annotations converted into a model-compatible format. Model parameters were iteratively optimized based on this data using the standard cost function. The best parameter set, minimizing the cost function, was retained for final inference. During inference, the model processed orthophotomap slices (256 x 256 pixels), generating predictions regarding the position and size of bounding boxes representing infected trees, along with confidence levels. Adjusting the threshold allowed control over the trade-off between recall and precision. Lower thresholds increased recall but reduced precision, leading to more false positives.

Field research was conducted in a coniferous forest situated on the periphery of the Regional Directorate of State Forests in Zielona Góra. To gauge the efficiency of automated detection compared to traditional field search methods, five random areas spanning approximately 30 hectares each were selected within the study zone. Teams comprising two foresters were dispatched to these designated areas to conduct in-situ verification. Subsequently, the same teams independently verified the accuracy of automated detections in the field.

Result

The entire automated process, including data collection during flights and automatic search on the orthomosaics, took 412.6 hours. In contrast, conducting a field search of a 30-hectare area typically took around 9 hours. Extrapolating this to cover 189,500 hectares, the field search process would require approximately 56,218.33 hours for one team consisting of two workers (refer to Table 4).

Step	Total time [hours]
using aircraft to collect data from 189,500 hectares of woodland	188.9
converting data to orthomosaics (it takes an average of 4,19 hours to analyze a 5000 hectare area).	151.6
The neural network system automatically analyzes orthomosaics (the mean processing time for a 5000 ha region is 1.52 hours)	72
Total	412,6

Table 2. Durations of steps performed to obtain locations of weakened trees and snag using the BZB UAS automatic method

The survey covered a vast expanse of 189,500 hectares within the Zielona Gora Forest District, requiring 189 hours for aerial reconnaissance. Processing the gathered data into orthomosaics, with an average processing time of 4.19 hours per 5000-hectare area, consumed a total of 151.6 hours. Furthermore, the neural network algorithm's automatic analysis of orthomosaics, completing the task in 1.52 hours for each 5000-hectare segment, accounted for 72 hours in total (refer to Table 2). In comparison, employing the in-situ method in five randomly selected areas demanded between 8.50 and 9.25 hours on average (refer to Table 3).

Area number	Area [ha}	Time [hours]
1	30.53	8.51
2	30.22	9.01
3	30.01	9.02
4	29.89	8.76
5	29.94	9.26

Table 3. Times of in-situ searching method in 5 random areas

Area [ha]	Time of BZB UAS method [hours]	Time of in-situ method [hours]
189 500	412.60	56 218.33

Table 4. Times of in-situ searching method for the entire Regional Directorate

The effectiveness of the classification algorithm underwent rigorous testing through two distinct comparisons. Firstly, the automatic classification results were juxtaposed with the manual annotations conducted at the outset of the study. Additionally, the algorithm's performance was evaluated against field study reports.

For the initial comparison, two specific sites were chosen. Among them, the "Lubsko" site, spanning an area of 600 hectares, comprised predominantly trees in diverse infection stages, with minimal occurrences of dead trees. This selection allowed for an examination of the algorithm's ability to discern various infection stages within a dynamic forest environment.

4 Discussion:

Utilizing aerial imagery coupled with automated tools for detecting diseased trees significantly expedites forest inventory control processes. While the longest step involves gathering data during flights, this duration is negligible when considering the project's scale. For instance, a single flight lasting four hours can cover a maximum area of 4,000 hectares, depending on the location and shape of study areas. Consequently, larger investigation areas render aerial imagery more time efficient. Conversely, in-situ searches are contingent on available human resources and daylight availability. However, apart from data gathering, which necessitates suitable conditions such as daylight and favourable weather, subsequent automated steps are unaffected by external factors and rely solely on computational resources.

Though not the primary focus, the study also compared the effectiveness of automated search with traditional methods. The automated search achieved a recall of 0.79 and a precision of 0.75 compared to in-situ data collected by teams. Similarly, when compared to manual annotations, the algorithm demonstrated comparable results, with a mean recall and precision values of 0.77. Despite occasional omissions or redundant labels by the algorithm, human errors associated with the classic field method could lead to missed or misdiagnosed trees visible in aerial images.

5 Conclusions:

The paper aimed to demonstrate that automatic detection and classification of diseased trees and snag using aerial imagery accelerates forest treatment processes. Rapid removal of pest and disease habitats is crucial for forest ecosystem protection. The presented algorithm enhances forest inventory control efficiency by identifying trees posing threats to forest ecosystems. Integration of Faster R-CNN model capabilities and remote sensing products enables foresters to partially or fully replace in-situ monitoring with aerial and satellite hyperspectral imagery. Once infected trees are automatically detected, workers can promptly apply appropriate treatments without prior in-field searches.

Remote sensing data combined with machine learning offer cost-effective solutions for forest management compared to traditional methods. These solutions not only provide access to data otherwise time-consuming to obtain but also unlock previously unattainable data.

The paper serves as a springboard for further research into the utility of artificial intelligence and machine learning algorithms in enhancing forest management and expediting decision-making processes in continental regions. Future endeavours will focus on integrating tree counting methods with health metadata assignment and developing applications for windbreak counting and probability measurement.

6 References

1. Szymański P 2013 Roczniki Geomatyki 2013 Tom XII, Zeszyt 1 (63): 117-127
2. Lechner A, Foody G, Boyd D 2020 One Earth 2
3. Mozgawa J, Piekarski E, Oleanderek H, Będkowski K 2000 Archiwum Fotogrametrii. Kartografii i Teledetekcji Vol. 10: 55-1:55-9
4. Budnik K, Byrtek J, Kapusta A 2021 IOP Conf. Ser.: Earth Environ. Sci. 942 01203
5. Zhu X X, Tuia D, Mou L, Xia G-S, Zhang L, Xu F, Fraundorfer F 2017 IEEE Geoscience and Remote Sensing Magazine 5 (4), 8–36
6. Diez Y, Kentsch S, Fukuda M, Caceres M L L, Moritake K, Cabezas M 2021 Remote Sensing, 13(14), 2837
7. Weinstein B G, Marconi S, Bohlman S, Zare A, White E 2019 Remote Sensing, 11(11), 1309
8. Dash J P, Watt M S, Pearse G D, Heaphy M, Dungey H S 2017. ISPRS Journal ofPhotogrammetry and Remote Sensing, 131, 1-14
9. Foley J A, DeFries R, Asner G P, Barford C, Bonan G, Carpenter S R, Chapin F S, Coe M T, Daily G C, Gibbs H K, Helkowski J H 2005 Science 309 (5734) 570–574
10. Trumbore S, Brando P, Hartmann H 2015 Science 349 (6250) 814–818
11. Zajączkowski G, Jabłoński M, Jabłoński T, Szmidla H, Kowalska A, Małachowska J, Piwnicki J 2021 Centrum Informacyjne Lasów Państwowych. ISSN 1641-3229
12. Jabłoński T, Malecka M, Sierota Z 2021 Forest Research Institute Analyzes and Reports No 33, chapter 1
13. Haze M, Widłaszewska B 2012 Information centre of State Forests. Volume 1 2012
14. Seidl R, Rammer W, Jäger D, Lexer M J 2008 For. Ecol. Manag. 256, 209–220
15. Sankey T, Donager J, McVay J, Sankey J 2017 Remote Sensing of Enviroment. 195:30-43
16. Van Leeuven M, Nieuwenhuis M 2010 European Journal of Forest Research. 129(4):749-770
17. Hais M, Wild J, Berec L, Bruna J, Kennedy R, Braaten J, Broz Z 2016 Remote Sensing 8, 687
18. Bratu J 2019 Sciendo International Conference Knowledge Based Organisation vol. XXV No 1
19. Rullan-Silva C, Olthoff A, Delgado de la Mata J A, Pajares-Alonso J A 2013 Forest Systems, 22, 377–391
20. Somers B, Verbesselt J, Ampe E, Sims N, Verstraeten W, Coppin P 2010 Journal of Applied Earth Observation and Geoinformation 12: 270-277
21. Szwagrzyk J (2020) Fragmenta Floristica et Geobotanica Polonica, 27(1), 5-15
22. Stubbings P, Peskett J, Rowe F, Arribas-Bel D 2019 Remote Sensing, 11, 1395
23. Nezami S, Khoramshahi E, Nevalainen O, Pölönen I, Honkavaara E 2020 Remote Sensing 12(7):1070
24. Bukoski, J. J., S. C. Cook-Patton, C. Melikov, H. Ban, J. L. Chen, E. D. Goldman, N. L. Harris, and M. D. Potts. 2022. Rates and drivers of aboveground car- bon accumulation in global monoculture plantation forests. Nature communications 13:1-13.
25. Cook-Patton, S. C., S. M. Leavitt, D. Gibbs, N. L. Harris, K. Lister, K. J. Anderson-Teixeira, R. D. Briggs, R. L. Chazdon, T. W. Crowther, and P. W. Ellis. 2020. Mapping carbon accumulation poten- tial from global natural forest regrowth. Nature 585:545-550.
26. Crowther, T., H. Glick, K. Covey, C. Bettigole, D. Maynard, S. Thomas, J. Smith, G. Hintler, M. Duguid, and G. Amatulli. 2015. Mapping tree den- sity at a global scale. Nature 525:201-205.
27. Dalla Corte, A. P., D. V. Souza, F. E. Rex, C. R. Sanquetta, M. Mohan, C. A. Silva, A. M. A. Zambrano, G. Prata, D. R. A. de Almeida, and J. W. Trautenmüller. 2020. Forest inventory with high- density UAV-Lidar: Machine learning approaches for predicting individual tree attributes. Computers and Electronics in Agriculture 179:105815.
28. Bukoski, J. J., S. C. Cook-Patton, C. Melikov, H. Ban, J. L. Chen, E. D. Goldman, N. L. Harris, and M. D. Potts. 2022. Rates and drivers of aboveground car- bon accumulation in global monoculture plantation forests. Nature communications 13:1-13
29. Cook-Patton, S. C., S. M. Leavitt, D. Gibbs, N. L. Harris, K. Lister, K. J. Anderson-Teixeira, R. D. Briggs, R. L. Chazdon, T. W. Crowther, and P. W. Ellis. 2020. Mapping carbon accumulation poten- tial from global natural forest regrowth. Nature 585:545-550.
30. Crowther, T., H. Glick, K. Covey, C. Bettigole, D. Maynard, S. Thomas, J. Smith, G. Hintler, M. Duguid, and G. Amatulli. 2015. Mapping tree den- sity at a global scale. Nature 525:201-205.
31. Dalla Corte, A. P., D. V. Souza, F. E. Rex, C. R. Sanquetta, M. Mohan, C. A. Silva, A. M. A. Zambrano, G. Prata, D. R. A. de Almeida, and J. W. Trautenmüller. 2020. Forest inventory with high- density UAV-Lidar: Machine learning approaches for predicting individual tree attributes. Computers and Electronics in Agriculture 179:105815.
32. Gadow, K. v. 1988. Building forestry rule sys- tems. South African Journal of Philosophy 7:132-137.

33. Hamedianfar, A., C. Mohamedou, A. Kangas, and J. Vauhkonen. 2022. Deep learning for forest inventory and planning: a critical review on the remote sensing approaches so far and prospects for further applications. Forestry 95:451-465
34. Hansen, M. C., P. V. Potapov, R. Moore, M. Hancher, S. Turubanova, A. Tyukavina, D. Thau, S. Stehman, S. Goetz, and T. Loveland. 2013. High-resolution global maps of 21st-century forest cover change. Science 342:850-853.
35. Harris, N. L., D. A. Gibbs, A. Baccini, R. A. Birdsey, S. de Bruin, M. Farina, L. Fatoyinbo, M. C. Hansen, M. Herold, R. A. Houghton, P. V. Potapov, D. R. Suarez, R. M. Roman-Cuesta, S. S. Saatchi, C. M. Slay, S. A. Turubanova, and A. Tyukavina. 2021. Global maps of twenty-first century forest carbon fluxes. Nature Climate Change 11:234-240.
36. Pérez-Rodríguez, L. A., C. Quintano, E. Marcos, S. Suarez-Seoane, L. Calvo, and A. Fernández- Manso. 2020. Evaluation of prescribed fires from unmanned aerial vehicles (UAVs) imagery and machine learning algorithms. Remote Sensing 12:1295