Microcontroller-Based Security System for an Industrial Complex: Design, Fabrication and Testing

ABSTRACT

Aims: The necessity by man to protect his life, investment and property has called for security which is essential in maintaining law and order in a society.
Study design: For effective realization of these goals, the security system must be able to incorporate different functions and monitor several activities instantaneously in real time. These activities include access, motion detection, fire hazard, plant production control etc.
Place and Duration of Study:
Methodology: In this study, the concept of real time central monitoring security systems was adopted with emphasis on industrial security. The industrial complex needs to have a way of authenticating individuals requesting access to the complex as well as reactively responding to intruder attempts. To achieve these, a simple hardware data acquisition unit based on a microcontroller was designed. With the microcontroller, many sub systems (access, intrusion, motion detection, surveillance) were integrated into one module and monitored continuously. A central monitoring unit was also implemented using a PC. The software for analysis and display of the data was designed using an object oriented approach and is GUI based for easier monitoring. When tested, the GUI provides graphic display of the trends from the sensor device. The data from the hardware unit was connected to the PC via the parallel port interface.
Results: The designed and fabricated microcontroller-based security system performed effectively for the industrial complex with no reported issue or failure.
Conclusion: Microcontroller-based security system is an effective tool for the industrial complex

Keywords: Security system, Microcontroller, Graphical User Interface, Software Module, Hardware Module

1. INTRODUCTION

"Security is the state of being safe and protected. It includes the precautions taken to keep an individual or property safe from crime, attack or danger. Since the beginning of mankind, there has been an overwhelming need for man to secure his life and property. Security systems are employed to monitor the state of a property and access of persons unto and around the property"[1"The security system alerts the property owner when the integrity of the property is about to be jeopardized or in case of imminent danger to any authorized person on the property be detected. In the present day industry, security systems play an important role in the protection of lives and investment. This is achieved by the incorporation of various subsystems into the security system with a single control unit. These subsystems usually perform different functions such as access control, intruder control, motion detection, surveillance, fire detection and production control. The most prominent of these is the access control" [2].
"Access control is used to restrict access to certain facilities, information or resources on the industrial property. It involves a process whereby personnel are identified and granted access. The access control subsystem is a collection of components used to identify and authenticate personnel and to authorize access to a resource" [3]. "It controls the entry to and exit of persons from the property and also access to rooms and facilities on the property. This subsystem also records all transactions made on it. These records contain the details and times of the access; it therefore functions as a personnel log. Intruder control is used to detect intrusion into the property and alert as necessary" [1]. "They consist of detectors mounted on windows and doors. A simple window intrusion circuit consists of a coupled IR emitter and IR receiver such that when activated, a short interruption of the beam results in an intrusion alert trigger" [4].

Motion detection is used to detect physical movement within a restricted zone and alert as necessary. The motion detector employed may be electrically connected to security, lighting, audio alarms and the like [5]. "This system functions as an intruder control mechanism especially in situations where no obvious break-in has occurred. Surveillance employs security cameras which used to monitor the activities and movement of individuals and personnel on and around various locations of the property" [6]. They may also be integrated into the access control system with facial

thermogram for facial identification of personnel at entry to or exit from a room or facility on the property. Motion detection systems may also employ security cameras to monitor the presence of activity in an area under surveillance so as to alert as necessary. IR imagers may also be employed under no-light conditions [7].
"Fire detection is used to detect and alert against a possible fire outbreak. It incorporates smoke detectors and temperature sensors. Smoke detectors detect presence of smoke particles as an early indication of fire. Temperature sensors measure temperature levels in test areas and indicate when the temperature becomes very high. It protects against significant property damage and endangerment to life within the property. Production control may be incorporated into security systems located in industrial complexes that have several production and storage plants. Depending on the substance been manufactured or stored, different sensors/detectors could be employed" [8].

The various properties and necessary components of an industrial security system are centralized monitoring and management, and real-time monitoring. A central monitoring unit is usually present in an industrial security system. All installed security units are coupled to this central unit which is often located in a control room. The unit consists of displays for the CCTV, indicators for the various detectors, control switches for the detectors and triggers for the alarm circuits. Pressure, temperature and fluid level monitors are present where necessary. It also consists of an interface for monitoring access control, access log database and administration privileges to modify access codes of personnel [9]. The access control subsystem consists of small user interfaces at various doorways where restriction is required. These interfaces are networked to the central monitoring unit in a client-server mode. In the case of an off-site central monitoring unit, an internet-enabled system can be utilized. All activities monitored by the various detectors on the property are relayed immediately to the monitoring unit [3]. Most real-time monitoring systems employ all the aforementioned technologies. Access control and surveillance subsystems help provide real time activity monitoring within the facility. This is an optimal configuration.

Microcontroller-based security systems play a crucial role in the scientific community for several reasons. Firstly, they provide a reliable and efficient way to protect sensitive data, equipment, and facilities from unauthorized access or tampering. This is especially important in research labs, where valuable experiments and prototypes need to be safeguarded. Secondly, they help monitor and control access to restricted areas within scientific facilities, ensuring that only authorized personnel are allowed entry. This helps maintain a secure environment and prevents theft or sabotage. Additionally, these systems can be integrated with other technologies such as biometric scanners or RFID systems to enhance security measures further. This multi-layered approach can provide a high level of protection for valuable scientific assets and ensure the safety of researchers and staff. Overall, microcontroller-based security systems are essential in the scientific community to maintain confidentiality, protect valuable resources, and ensure the smooth operation of research activities.

1.1 ACCESS CONTROL SYSTEMS FOR MICROCONTROLLER-BASED SECURITY SYSTEM FOR AN INDUSTRIAL COMPLEX

Access control is any mechanism by which a system grants or revokes the right to access a protected area. Normally, personnel must first present their token (card/pin) to a reader. The access control mechanism controls what operations the user may or may not make by comparing the personnel card status (programmed data) to an access control database. Some of these are passwords and personal identification numbers; biometrics; and card based mechanisms [10].

"A password is a unique string of characters that a user types in as an identification code. The system compares the code against a stored list of authorized passwords and users. If the code is legitimate, the system grants the user access, at whatever security level has been approved for the owner of the passwords. A Personal Identification Number (PIN) is a unique multidigit number that functions just like a password. The password/PIN access control systems use keyboard or key panels with minute displays on the access unit. These systems are slow since the user must key in the password or PIN character by character before being validated" [11]. "Passwords are often used in conjunction with a username or some other access mechanism. Biometrics is an automatic method for identifying an individual on the basis of some biological or behavioral characteristic of the individual. Many biological characteristics, such as fingerprints, and behavioral characteristics, such as voice patterns, are distinctive to each person. Therefore, biometrics is more reliable and more

capable in distinguishing between a specific individual and an impostor than any technique based on an identification document, access card or a password" [12].

"Portrait ID cards are widely used for identification of personnel. It is one of the simplest forms of access control. These cards are made of plastic and may embed a hologram to avoid counterfeiting. Its capability can be enhanced by including electronic access control technologies on the card. A smart card or integrated circuit card is any pocket-sized card with embedded integrated circuits which can process information" [13]. "It can receive input which is processed – by way of the smart card application – and delivered as an output. Card data is transferred to the central administration system through card reading devices. There are two broad categories of smart cards: Memory cards contain only non- volatile memory storage components, and perhaps some specific security logic. Microprocessor cards contain volatile memory and microprocessor components" [14]. "A swipe card is a credit card sized badge incorporating a magnetic strip, a transponder device and/or a microchip mostly used for industrial property access control or electronic payment. Swipe cards in their strict sense need to be swiped through the slot of a swipe card reader. Swipe cards have a magnetic strip, containing information coded on it during or after manufacturing. It is made of plastic coated with a ferromagnetic material. The information regarding the user is encoded on the ferromagnetic material by alignment of the polarity of the magnetic strip. A magnetic stripe card is a card capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card. The magnetic stripe, sometimes called a magstripe, is read by physical contact and swiping past a reading head" [15].

Table 1 summarizes previous studies on the design, fabrication and application of microcontroller-based security system using different approaches. The methods used at arriving at the final design of the system and the components employed revolve around a compromise between effectiveness and compactness. The main aim of any security system is to provide effective monitoring, access and reactive services. In this study, an efficient version of a centralized monitoring security system was designed, fabricated and tested for small organizations and industrial application. The access control subsystem is of the contact card type. The sensors employed in the other subsystems are generally cheap and efficient. A microcontroller forms the main control unit which performs real time monitoring and is interfaced with a PC. The PC runs an application that consists of a Graphical User Interface (GUI) which displays access characteristics and sensors level which can be monitored and controlled by an administrator (a human user). All sensory response is fed by the microcontroller to the PC which is then displayed on the GUI. The PC application performs the acquisition and authentication of access card information. It controls access to the various restricted resources and contains a database of activity and access logs.

Table 1: Previous studies on microcontroller-based security system

Aim of study	Microcontroller type	Mechanism	Reference
Programming of a microcontroller to control the hardware in sliding door.	Microcontroller 89S52	The microcontroller sends a signal to the multiplexers on insertion of the smart card in the card slot. The multiplexers consist of ICS which prompts for a display of the identity of the card user in the liquid crystal display (LCD). On validation of the card, the LCD displays a welcome note to the user and prompts for a pin code. Which then decide whether access should be granted or not.	[16]
Develop a highly efficient and affordable security system to countermeasures against possible security risks to man and property.	AT89C52 microcontroller	Automated Fingerprint Identification System (AFIS) ensures that only registered staff are allowed access into the industrial complex at any point in time and a doorway counter determines the number of people present in the building at any given time.	[17]
Create a system that make the surveillance of home devices easily using GSM	PIC18F452 microcontroller	The GSM module is used to communicate with the owner of the home whenever the sensor senses a fault, a specific message is sent to the	[18]

(Global System for digital mobile telecommunication) and microcontroller		owner in order to take a necessary action. The microcontroller is a tool that use a specific code to do some functions by using MikroC programmer. The temperature, smoke, intrusion motion, magnetic lock door, garage door and irrigation are controlled and monitored	
Design and implement of a microcontroller based home security system with GSM technology	ATMEGA16 Microcontroller	The user is informed about the security breach through GSM network that provides a special opportunity whenever the user stays at far away from home.	[19]
Design of a low-cost automated security lighting control system	ATMEGA8 Microcontroller	An authenticated signal is sent from the user's cellular phone via Global System for Mobile Communication (GSM) network to the equipment. The signal consists of information made up of the function or action expected to take place i.e. whether the light should be switched Off/On. The receiver phone receives the SMS message that is sent from the user's phone and then sends it via the GSM modem which in turn sends the output digital signal to the microcontroller. Then the microcontroller, on receiving the signal, controls the different relays and triggers the required appliance.	[20]
Design and building of a community surveillance system	STM32F103C8 microcontroller	The system uses Passive Infrared sensors that detect human motions by sensing the infrared radiations from the body of non-residents when they are 6 meters away or nearer to the sensor. A detected intruder will trigger the UART camera to send the image footages through the GSM/GPRS to a cloud database and trigger an alarm for 2 minutes so as to attract the attention of nearby persons.	[21]
Design and construction of a micro controller based smart automated system for controlling various home appliances	ESP8266 microcontroller	If any hazard is being sensed like smoke, excess heat, unauthorized movements etc.; the system warns the homeowner in real-time using Short Message Service (SMS).	[22]

2. MATERIAL AND METHODS

The design of the security system takes on an overall top-down modular approach. The two major modules are the hardware module and the software module. Each top module has a defined function and is further divided into sub-modules which work together to achieve a specified goal.

2.1 HARDWARE MODULE UNITS AND FUNCTIONS

The hardware module was designed to consist of the card reader, window intrusion detector, motion detector, temperature sensor, smoke sensor, security camera, alarm system, comparator, data acquisition and power supply units.

2.1.1 CardReaderUnit

For effective improvisation, the cards are designed to be contact based. On contact with the reader, each card sends a unique binary code to the data acquisition unit. The available options are spring contacts and pin contacts. The pin contact type is chosen for simplicity.

2.1.2 IntrusionDetectorUnit

The opposed sensing method is employed for this unit as the body to be detected is opaque. Here an IR emitter and an IR receiver are used to form an optocoupler whose continuous beam is broken by the intruder upon intrusion unto the property. This method is effective and at the same time suitable as the emitter and receiver can be placed behind the window frames at opposing ends hidden from possible intruders. The emitters and receivers used are cheap IR emitting diodes and IR detecting diodes (photodiodes).

2.1.3 MotionDetectorUnit

The motion detector response was simulated using the PC central monitoring unit as motion detector chips were both scarce and expensive at the time of design. IR intrusion detector could also function as a motion detector with a linear range as against the spatial detection field of the PIR motion detector or microwave motion detector.

2.1.4 Temperature Sensor Unit

In order to conform to the outlined factors, the LM35 is used. The LM35 is aprecisionintegratedcircuittemperaturesensorwhoseoutputislinearlyproportionalto the Celsius (Centigrade) temperature. The LM35 does not require any external calibration or trimming to provide typical accuracies of ±¼ ºC at room temperature and ±¾ ºC over a full -55 to +150 ºC temperature range. Low cost is assured by trimmingandcalibrationatthewaterlevel.TheLM35'slowoutputimpedance,linear output, and precise inherent calibration make interfacing to readout or controlcircuitry especially easy. As it draws only 60µA from its supply, it has very low self- heating, less than 0.1 ºC in still air. Figure 1 is the bottom view of LM35 temperature sensor showing pin out.

Figure 1: BottomviewofLM35temperaturesensorshowingpinout

2.1.5 Smoke Sensor Unit

A smoke box which implements a scatter-type photoelectric smoke sensor is used.The smoke box is hollow with slits at its edges and a matt black coated inner surface. It has a lamp and a light dependent resistor, LDR, separated by a screen. Normally,the opaque screen blocks light from reaching the LDR. The black surface also prevents reflection over the screen. As smoke enters the room, the temperature heats the air in the chamber which rises up drawing the smoke filled air through the lower chamber. The smoke particles help in scattering light thereby allowing light to fall on the LDR and activating it. The LDR is connected to a comparator circuit which gives a signal if the threshold value is exceeded. The threshold is variable hence the smoke sensor has adjustable sensitivity.

2.1.6 Security Camera Unit

A typical security camera is quite expensive. Webcams are used for the modelinstead. They provide video recording and playback at a lower resolution and frame rate than the security camera. Webcams are typically for video transmission over the internet. However, the video is channeled to the PC GUI. Analysis isn't carried out by the external hardware module but is done by specialized graphics hardware in the PC. Hence, the webcam links bypass the external hardware and are connected directly to the PC via USB ports.

2.1.7 Alarm System Unit

In order to reduce hardware circuitry, the alarmsystemmakes use of the PC's internal buzzer. The PC monitoring unit is hence also a reactive system displaying both video and audio alert signals.

2.1.8 Comparator Unit

The model represents a two-room monitoring security system. For this we have two general comparator circuits each handling the sensors for the rooms. To implement this, variable resistors, capacitors, transistors and an IC voltage comparator are employed. These are readily available. The LM339 is a quad analog voltage comparator. It is an analog linear IC that contains four voltage comparators. Use of this IC reduces hardware circuitry.

2.1.9 Data Acquisition Unit

For easy integration of monitoring and interfacing activities, a programmable controller is necessary. Atmel AT89C51 microcontroller is employed here. Thechoice of this chip is based on cost, availability of development tools and familiarity with the instruction set.

2.1.10 8951 MICROCONTROLLERS

The 8951 belongs to the 8051 series of microcontrollers. Some features of the 8051series are:

- *80C51centralprocessingunit*
- *On-chipflashprogrammemory*

- *Speedupto33MHz*
- *Fullystaticoperation*
- *RAMexpandableexternallyupto64kB*
- *4interruptprioritylevels*
- *6interruptsources*
- *Four8-bitI/Oports*
- *Full-duplexenhancedUART*
- *Three16-bittimers/countersT0,T1(standard80C51)andadditionalT2(capture and compare)*
- *Powercontrolmodes*
- *Programmableclockout*
- *Asynchronousportreset.*

The 8951 has a 4 k on-chip ROM which is a non-volatile flash program memory that is parallel programmable (10000 minimum erase/program cycles for each byte). Italso has a 128 byte internal Data RAM. An extra 128 bytes of internal RAM is for the Special Function Registers (SFR). *Fig 2*shows the block diagram of the internal components of the 8951. The 8951 has a 12-bit address bus and an 8-bit data bus. The type employed in the program has a Dual In-line Package (DIP) pin configurationwith 40 pins. Figure 2 is the block diagram of 8951 microcontroller.

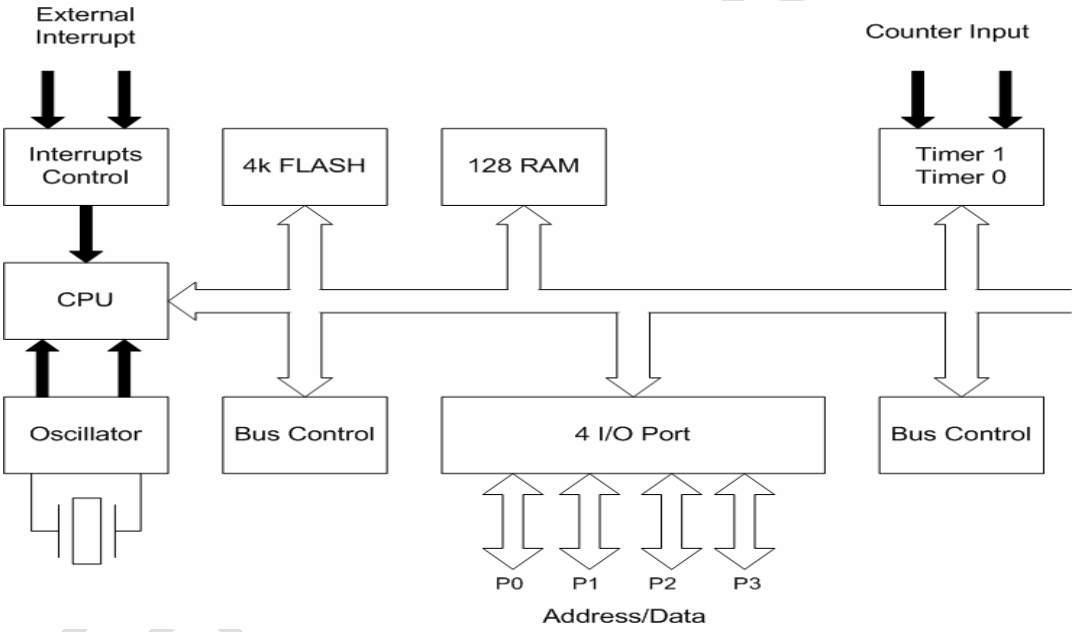

Figure 2: Block diagram of 8951 microcontroller

Programming of the microcontroller 8051 series is done using the instruction set formed by mnemonics that specify various functions. The function mnemonic specifies when program memory or external data memory is used in conjunction with the internal data memory. The syntax, in assembly language instructions, consists of a function mnemonic followed by a “destination, source” operand field. The microcontroller program is written and compiled on a PC with a macro assembler.The compiled hex code is then transferred to the flash ROM of the microcontroller with a parallel programmer.
The 8951 has many features and functions whose discussion is beyond the scope of this project (see reference for further reading). However, a basic knowledge of the microcontroller, its instruction set, and microcontroller-specific assembly language is necessary in order to connect the pin outs properly and program the chip effectively.

2.1.11 Interface Unit

The computer standard parallel port (LPT1) is chosen to serve as the interfacebetween the PC GUI application and the microcontroller monitored hardware. It is chosen because of its relative ease of transmission and reception of data compared to thatoftheserialport.Moreover,thestandardparallelhasbeenoptimizedforhardware and digital logic

interfacing. The standard parallel port serves as the channel for transferring data from the hardware module to the software module. The standard parallel port comes as a twenty-five pin (DB 25) connector with three addressable ports: data port; status port; control port, at addresses 0×378, 0×379 and 0×37A respectively.

2.1.12 Power Supply Unit

A simple power supply unit constructed from basic and readily available ICs would have been ideal. However, since the unit operates with a PC interface, a battery- powered supply unit is unnecessary as there has to be ac mains supply for the PC to operate. A readily available variable dc adapter is therefore employed for thehardware module.

2.2 Software Module Organization

ThePCinterfaceapplicationsoftwareshouldpossessthefollowingcapabilities:

- Ability to handle data collection from microcontroller based security system, logging of access times.
- Abilitytointegratesecuritycamerahardwaremoduleanddisplayvideo.
- Audiovisualrepresentationofingressandegresswithaccesscontrolsystem.
- Virtualinstrumentationforsensors/transducersandaudiovisualalertupon triggering.

Based on these functions, the software is divided into modules which interact using a top-down, object oriented design approach. This modular application can be designed optimally using a programming language that has the following characteristics:

- ObjectOrientation
- Portinterfacing
- Networkcapability.
- GraphicUserInterfacemode

The Microsoft Visual Basic.NET programming language is used since it possesses all the aforementioned characteristics and the designers are proficient in its use.However, been more web and network driven, the port interfacing extensioncapability is optimized using drivers written in C language. Visual Basic.NET employs the Visual Studio.NET IDE suite which is a complete suite of tools for building both desktop and team-based Enterprise Web applications. Figure 3 presents thesoftwarecomponentinteractionatthemodularlevel.

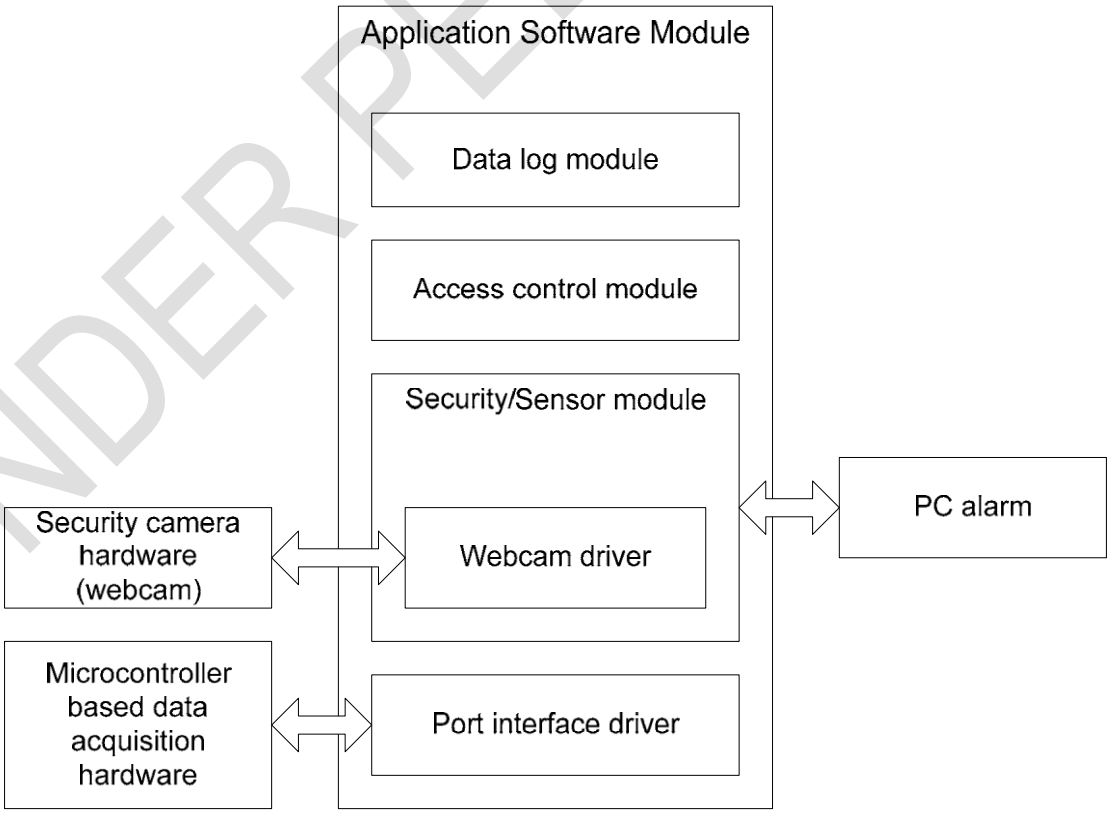

Figure 3: Software component interaction at the modular level

Results and discussion

3. HARDWARE DESIGN AND IMPLEMENTATION

The hardware module is made up of various sub modules connected to the microcontroller unit. These sub modules are designed to function independently.

3.1 Card and Card Reader Unit Design

The card reader unit diagram is shown in Figure 4. The functions of the labeled pins are thus:

- A, B, C represent the code bits. It is coded differently for each card. As there are 3 bits to represent data/personnel, it is possible to assign access codes to 2^3 = 8 different personnel for this particular model.
- RS – Room Select. The proposed model monitors two rooms;therefore, the RS pin selects the particular room been accessed.
- INT1, INT2 represent interrupt lines to the microcontroller. These lines pass through an OR gate so that the interrupt is enabled only when both pins are activated. They interrupt the normal cyclic sensor checking operation of the microcontroller to perform an interrupt service routine which transfers access code data once a card is inserted into the card reader. It is positioned at the ends of the unit to ensure that all the code bit pins make contact with the card before triggering the interrupt.
- GND – Ground. The GND pin sends all the ground signals to the card for coding and interrupt.

The cards are made from credit card size carton-like material wrapped with aluminum foil to form the conducting edges. The conductor edge is separated into ten partitions: each partition corresponding to a bit value. The functions follow the corresponding contact pins of the card reader circuit diagram. The code bits of the card readers are connected to port 2 of the microcontroller. The construction of the card readers for access to two rooms is based on the assumption that only one room can be accessed at any instance.

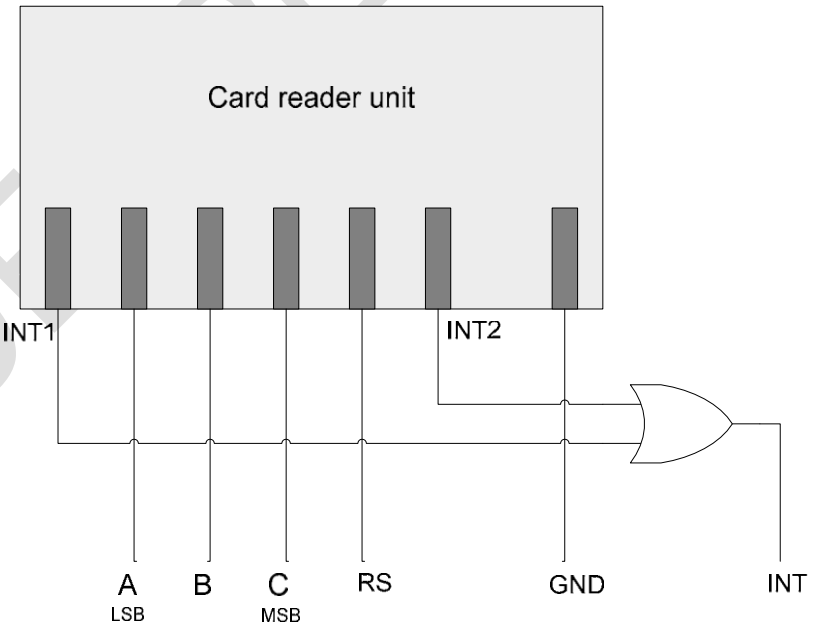

Figure 4: Card reader unit diagram

3.2 Smoke Sensor Unit Design

The circuit diagram for the smoke sensor unit module is shown in Figure 5. The smoke sensor unit employs basically a Light Dependent Resistor (LDR) and a comparator circuit. TheLM339op-ampisconfiguredinthevoltagecomparisonmode.Resistor RV_1(4.7 kΩ)is used in setting the reference

voltage on the inverting pin input of the op-ampIC.Whenthevoltageacrossthenon-invertingpininputoftheop-ampis greaterthanthereferencepotential(V_{ref})thatwassetwithRV_1i.e.inthepresenceof smoke,theoutputoftheop-ampchangesfrom0.12Vto≈4.6V(dependingonthe supply potential) with the help of the output pull-up resistor. The LDR is a transducer whose resistance is inversely proportional to the light intensity. The output of the circuit is connected to Port 0 of the microcontroller.

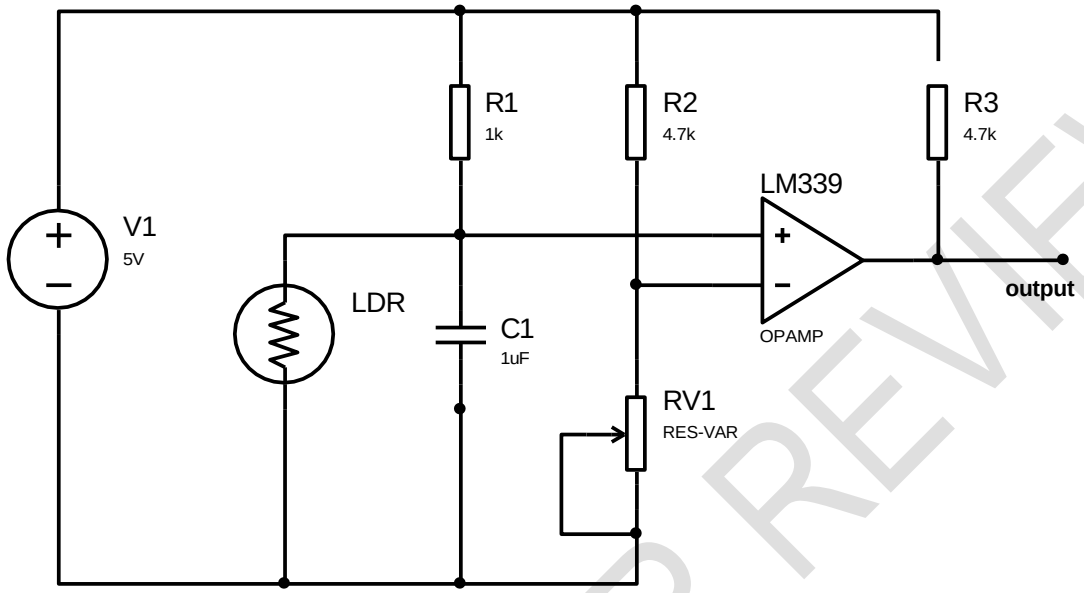

Figure 5: The circuit diagram for the smoke sensor unit module

3.3 Temperature Sensor Unit Design

The temperature sensor unit circuit diagramis shown in *Fig 6*. It employs the LM35 temperature sensor and a comparator circuit. The LM35 is a transducer with a linear scaling factor output of 10mV/ºC -55 ºC to +150 ºC. The R_2 resistor is used to set the reference voltage across the inverting input of the op-amp. When the temperature of the environment increases, the voltage output of the LM35 also increases. When the voltage rises above a set threshold i.e. the reference potential, the op-amp outputs a high logic state. The output is connected to Port 0 of the microcontroller. Figure 6 is the temperature sensor unit circuit diagram.

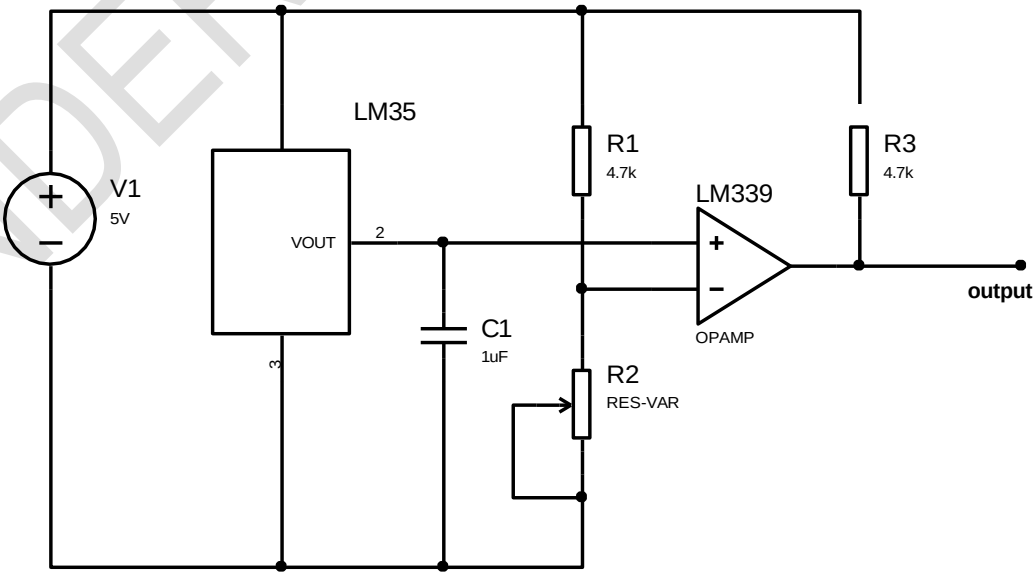

Figure 6: Temperaturesensorunitcircuit diagram

3.4 Infrared Emitter/ Receiver Unit Design

The IR optocoupler unit doubles as a window intruder module and a motion detector module. It consists of an IR emitter unit and an IR receiver unit. The IR emitter is activated using a 555 timer. The555timerisbiasedtooperateintheastablemodei.e.outputpin3producesafree runningpulse.Figure 7 is the infrared emitter unit circuit diagram. When connectedasshown(pins2and6connected),the 555 will run as a multivibrator. Theexternalcapacitor C_1 chargesthrough$R_1$and R_2anddischargesthroughR_2.Thedutycyclemaybepreciselysetbytheratio ofthesetworesistors. Inthismodeofoperation,thecapacitorC_1chargesanddischargesbetween⅓$V_{CC}$and ⅔V_{CC}.Thechargeanddischargetimesandthefrequencyareindependentofthe supply voltage. Figure 8 is the infrared emitter unit circuit diagram.

Thechargetime(outputhigh)isgivenby Equation 1.

$$t_1 = 0.693(R_1 + R_2)C_1 \quad (1)$$

Andthedischargetimeisgiven by Equation 2:

$$t_2 = 0.693(R_2)C_1 \quad (2)$$

Thus,thetotalperiodis given as Equation 3:

$$T = t_1 + t_2 = 0.693(R_1 + 2R_2)C_1 \quad (3)$$

Thefrequencyofoscillationis given as Equation 4:

$$f = \frac{1}{T} = \frac{1.44}{(R_1 + 2R_2)C_1} \quad (4)$$

ThefrequencyofoscillationemployedbytheIRemittercircuitiscalculated f = 640 *Hz.*

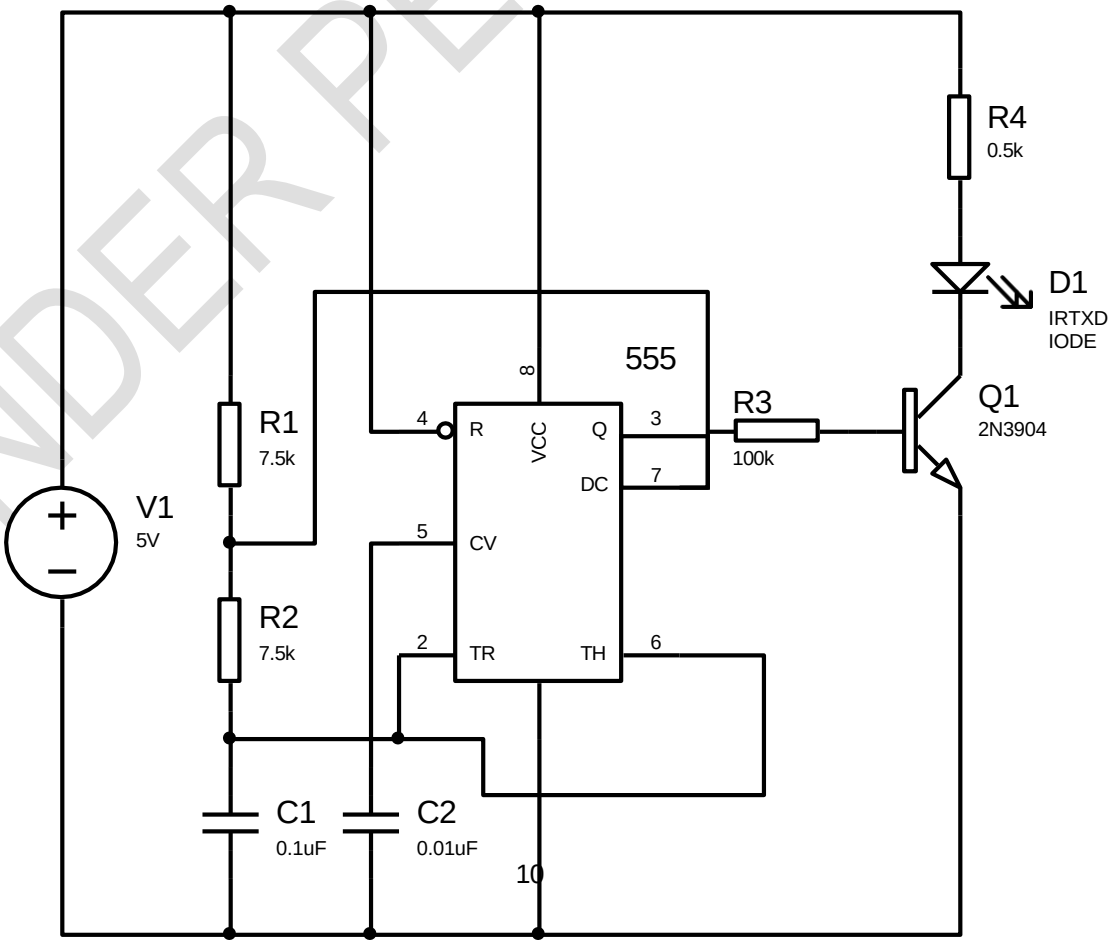

Figure 7: Infraredemitterunitcircuitdiagram

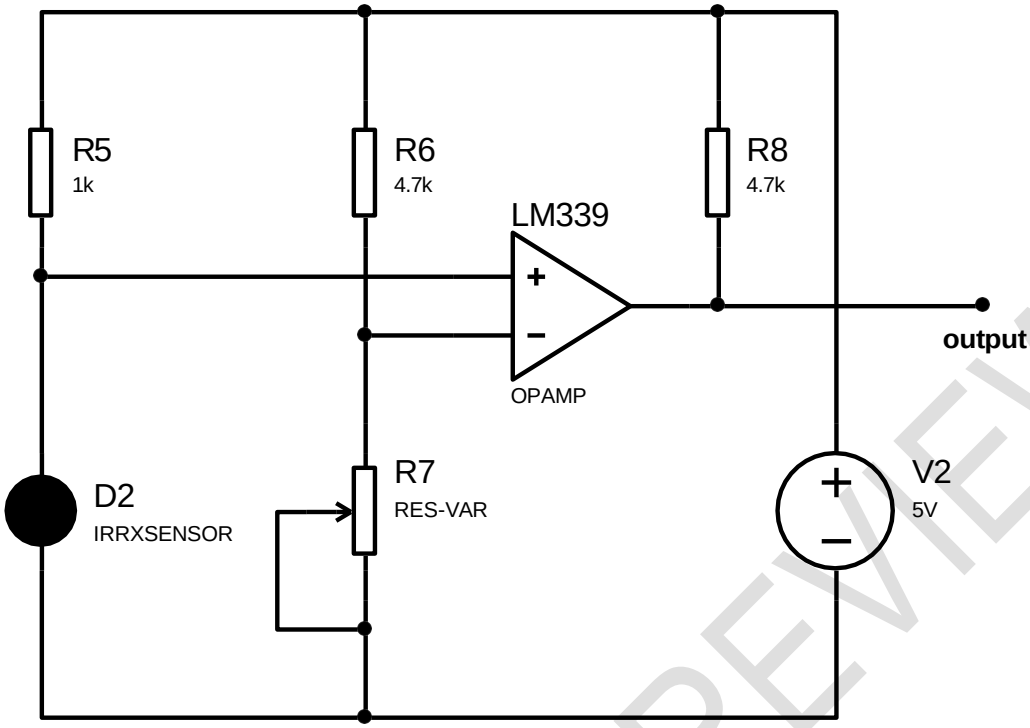

Figure 8: Infraredreceiverunitcircuitdiagram

Pin3ofthe555timerisconnectedtothebaseofatransistorviaresistorR_3.The transistorisbiasedtooperateintheactiveregioni.e.asaswitch.Theconfiguration activates the IR emitter, $D_1$with a steady pulse train. IR receiver/sensor, D_2 isactivated whenever an IR signal is sensed. The op-amp is configured in the voltage comparison mode. D1 and D2 are positioned to face each other with the same collinear axis to form an optocoupler unit. D_2 and R_5 form a voltage divider network. In the normal conducting state, a beam is set up across D_1 and D_2. The internal resistance of D_2 is low with respect to R_5, therefore the potential drop across it is low. When there is an intrusion or an opaque object is passed between D_1 and D_2, the beam is cut off from reaching D_2. This increases the resistance of D_2 to a very large value such that the voltage drop across it will approximately equal V_{cc}. This voltage value is greater than the threshold set at the op-amp, therefore the output is enabled.

3.5 Microcontroller Data Processing Unit Design

The hardware sub modules are all connected to a microcontroller unit (8951) for processing and transfer to the PC GUI via the interface unit. The block diagram of the microcontroller unit connection is shown in Figure 9.

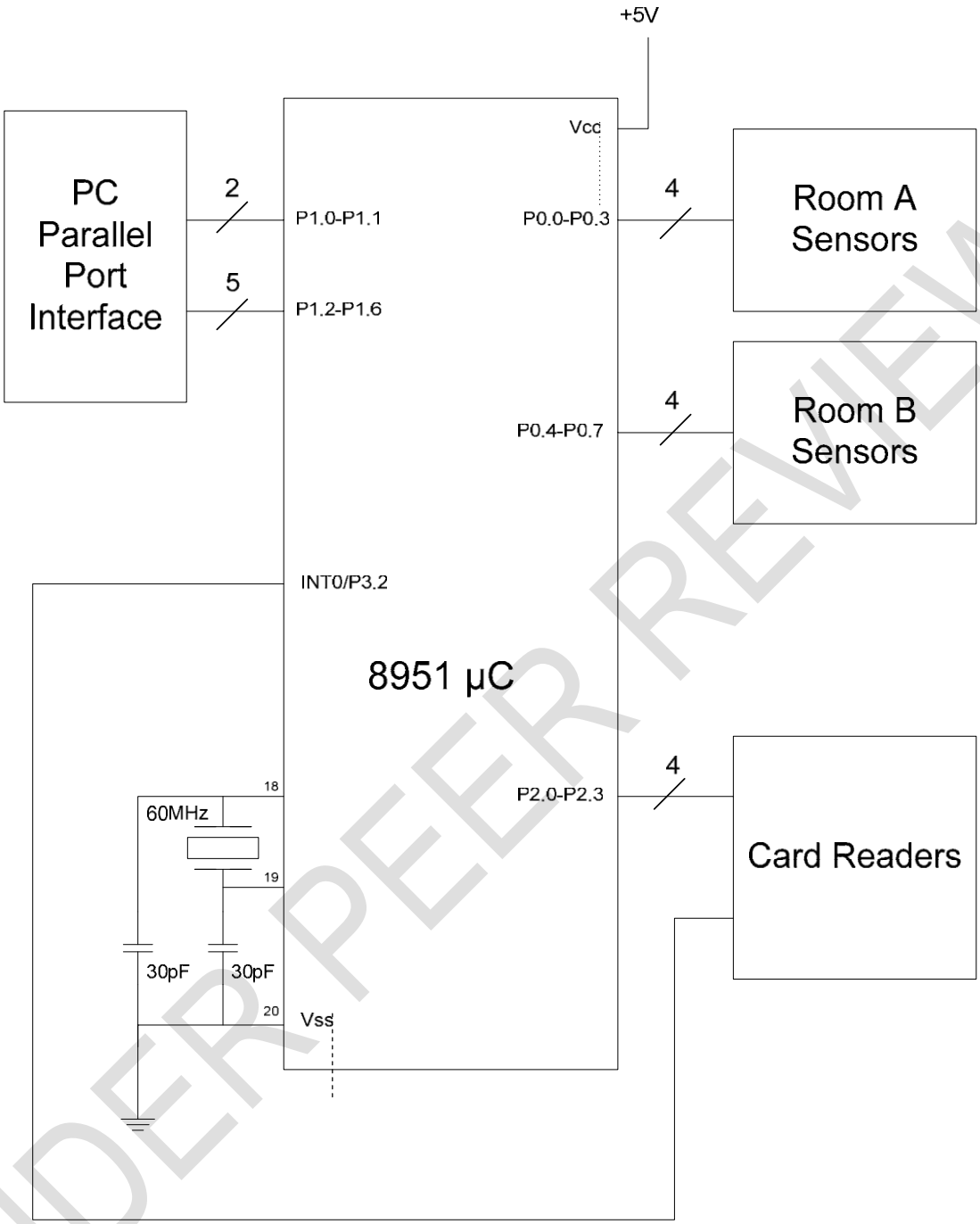

Figure 9: Microcontrollerconnectiondesignforsecuritysystem

Themodulesofthesystemareconnectedtothemicrocontrollerasfollows:

- SensorsforRoomAareconnectedtoPort0(P0.0–P0.3)
- SensorsforRoomBareconnectedtoPort0(P0.4–P07)
- The cardreader data bits are connected Port 2 (P2.0 – P2.3) while its interrupt pin is connected to INT0 (P3.2)
- A60MHzcrystaloscillatorisconnectedtoXTAL1andXTAL2
- TheunitislinkedtoaPCwhichisconnectedtoaparallelportinterfacevia Port 1 (P1.0 – P1.6)

Themicrocontroller-baseddataprocessingunitperformstwomajorfunctions:

- Responsetosensortrigger
- Responsetoaccessrequest(cardinsertion)

The former is the main continuous loop operation of the microcontroller while the latter is interrupt-based. The flow chart for the main routine of the microcontroller is shown in Figure 10.

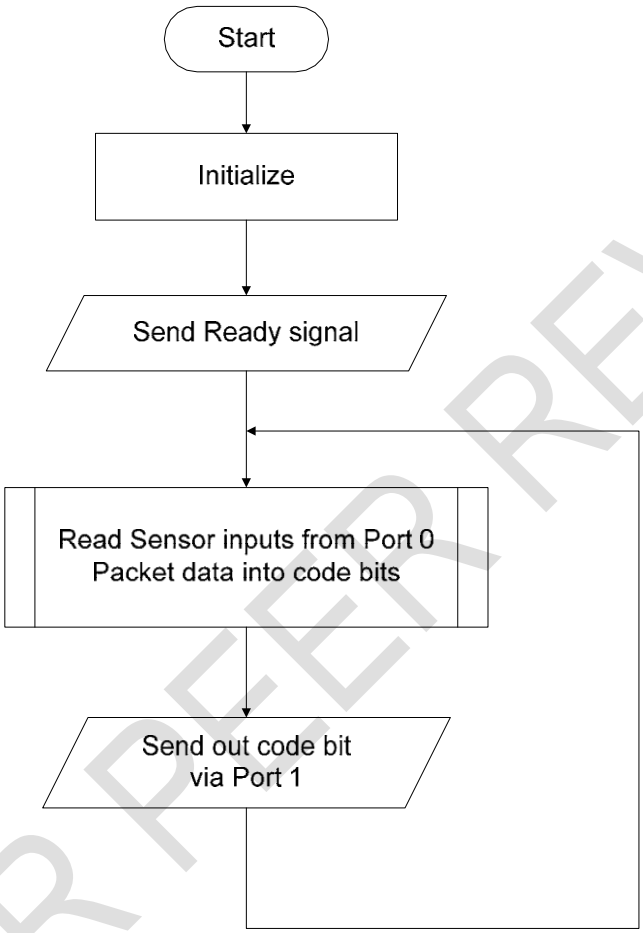

Figure 10: Microcontrollermainroutineflowchart

When a user slots a card into any of the card readers, it sends an interrupt into the INT0 pin of the microcontroller. An interrupt service routine handles this routine. The flowchart for the interrupt service routine is shown in Figure 11.

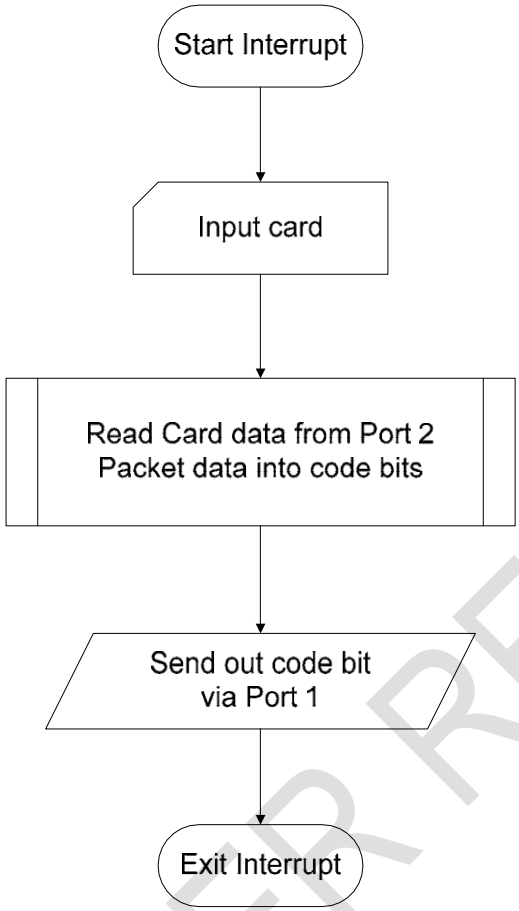

Figure 11: Microcontrollerinterruptserviceroutineflowchart

The data from the microcontroller is sent to the parallel port interface in code bits. These code bits are a binary sequence of numbers each interpreted as a separate function by the PC GUI. Given a 5 bit value say 00000, the first and second Most Significant Bits (MSB) are used to select the operation carried out. Hence 00 selects a Room A operation; 01 selects a Room B operation; 10 selects Card Reader A data operation; 11 selects Card Reader B data operation. The remaining 3 bits select the function carried out.

4. SOFTWAREDESIGNANDIMPLEMENTATION

The PC software is designed using a top-down modular approach. It is object- oriented, consisting of various classes interacting with a main class. The various classes and their functions are:

- Main class – which initializes the controls and performs a continuous loop operation checking the status and data ports of the parallel port. It also coordinates the other classes. The main class also controls the Windows form and all the display controls.
- Access class – which handles access control related events. It stores the personnel data corresponding to the access code bits and transfers the information to the main class when called.
- Security class – which handles security sensor related events. It stores the response paths and values for a sensor trigger event and transfers the information to the main class when called.
- Webcam class – which handles webcam related events. It contains the start-up information and prompts for the webcam.
- Log class – which handles personnel log related events. It contains settings for log display and printing.
- Port module – this is a module (a Windows console class) which containslinks and settings for the Dynamic Link Library (DLL) which accesses the parallel port.

Figures 12a and 12b are the main flowcharts of the PC GUI. Figure 13 is the PC GUI webcam subroutine flowchart. Figure 14 is the PC GUI with tab positioned to Access. Figure 15 is the PC

GUI with tab positioned to Security (Room A smoke indicator active). Figure 16 is the PC GUI with tab positioned to Log.

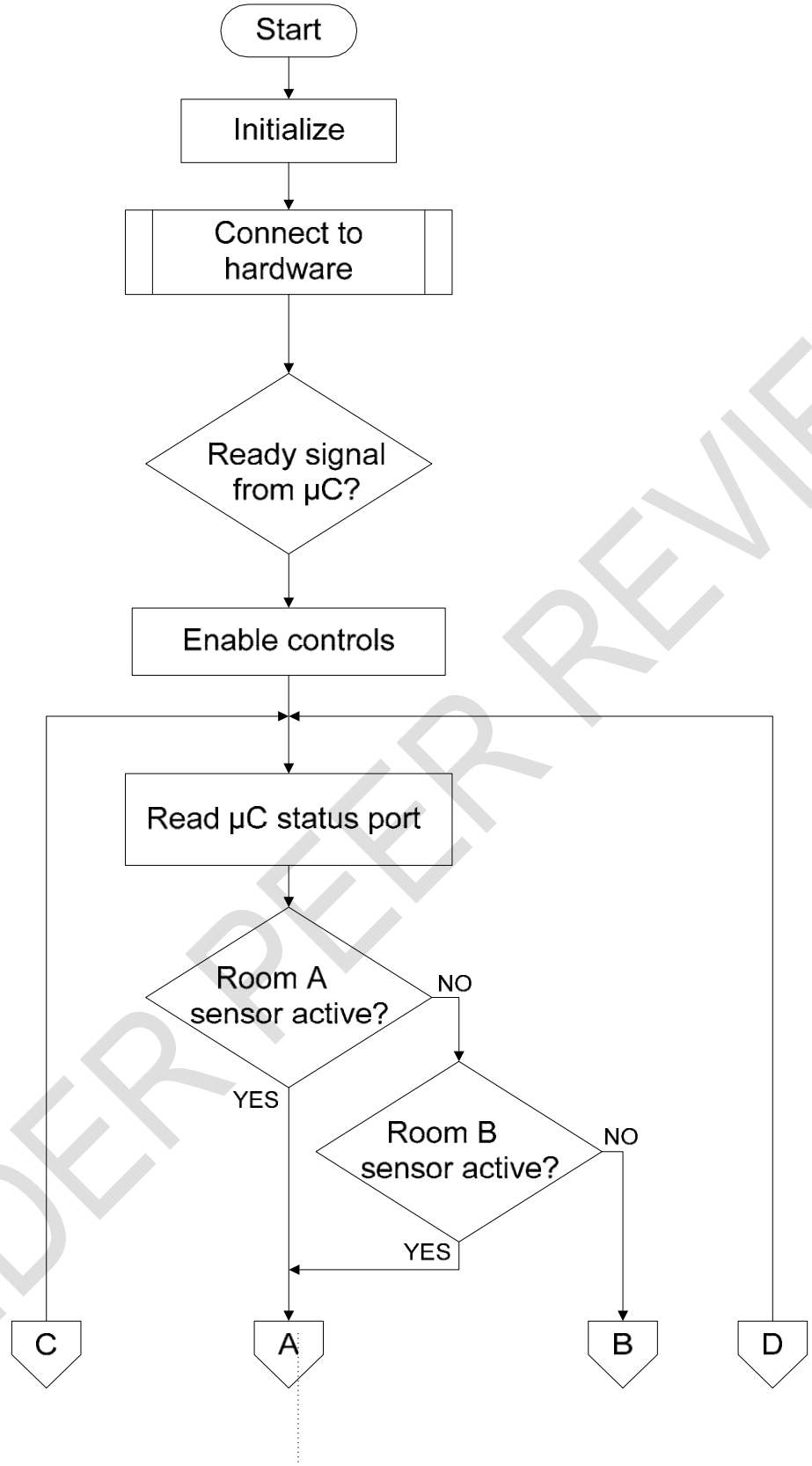

Figure 12a: Main flowchart of the PC GUI

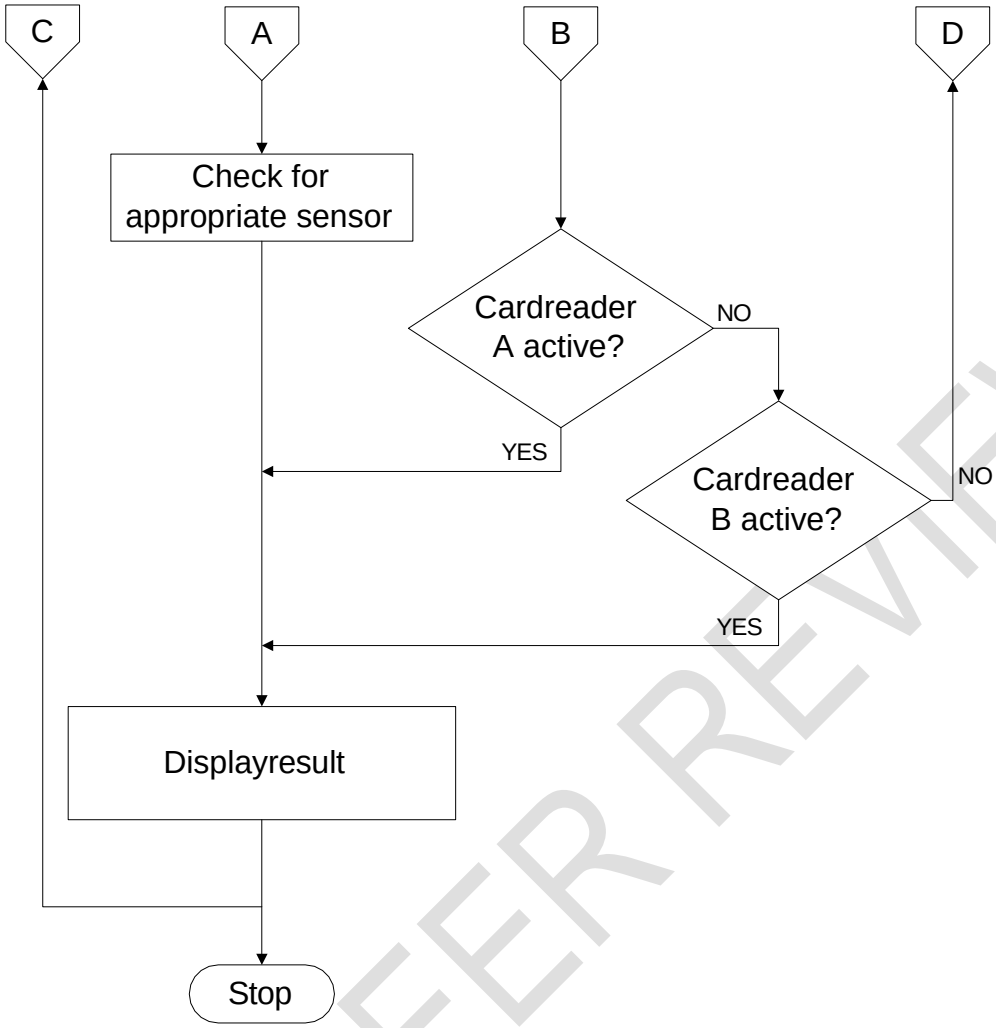

Figure 12b: Main flowchart of the PC GUI

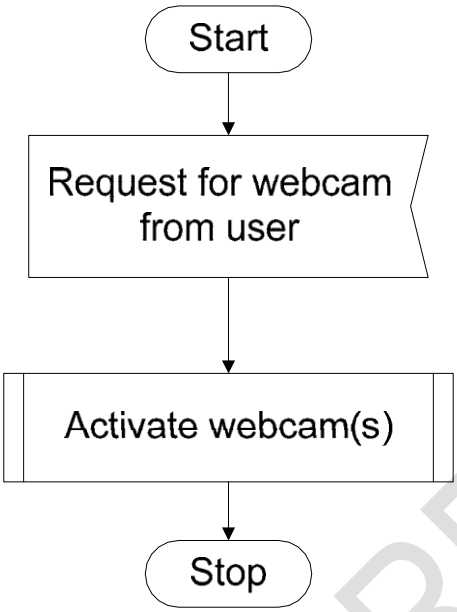

Figure 13: PCGUIwebcamsubroutine flowchart

TheGUIshowingthedifferenttabpositionsisshowninFig14

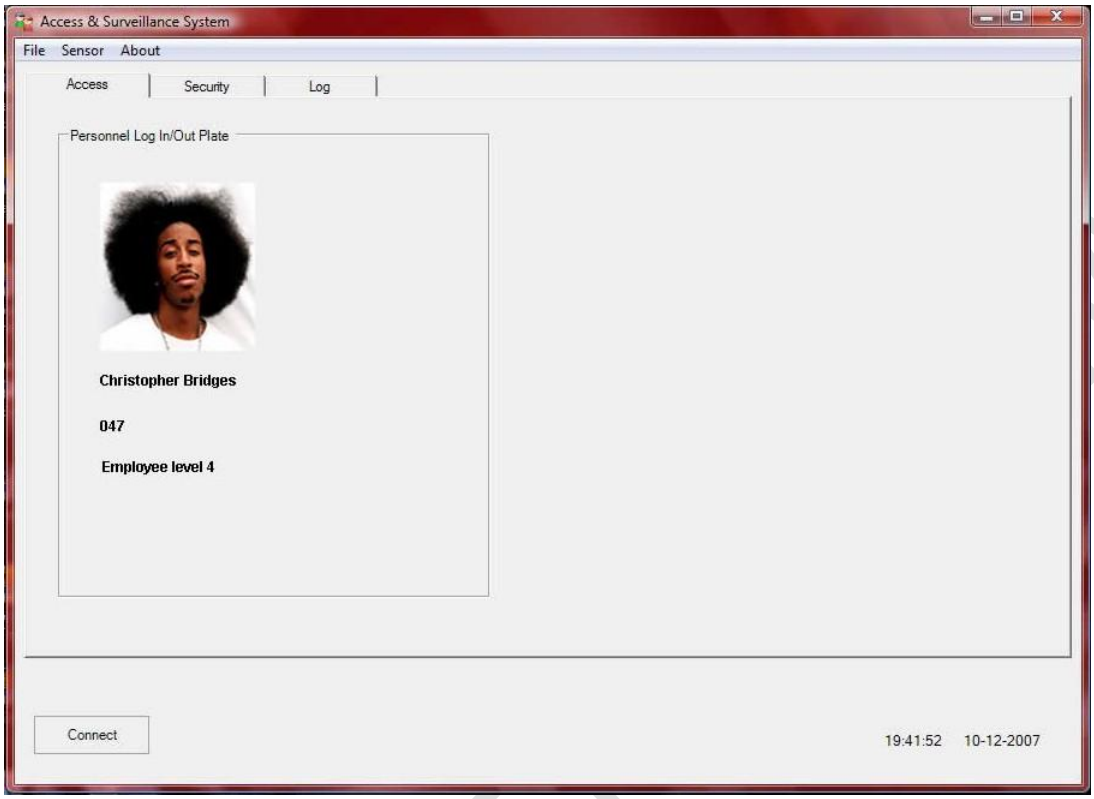

Figure 14: PCGUIwithtabpositionedtoAccess

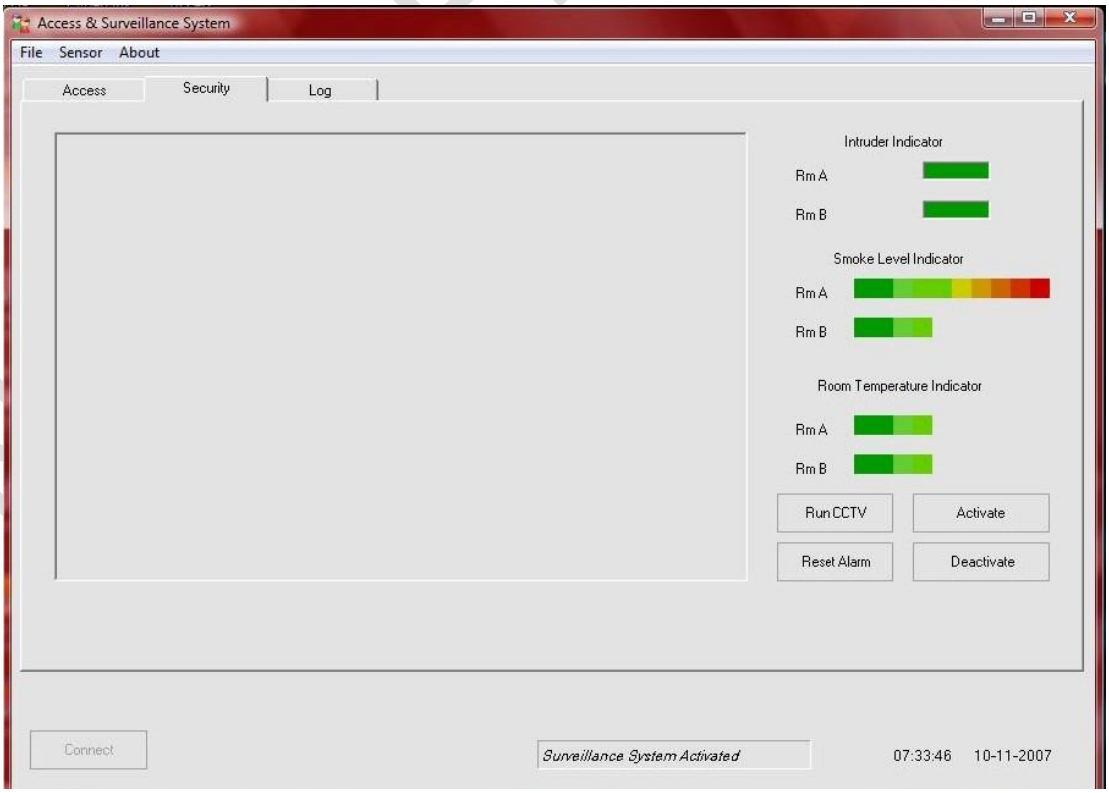

Figure 15:PCGUIwithtabpositionedtoSecurity(RoomAsmokeindicatoractive)

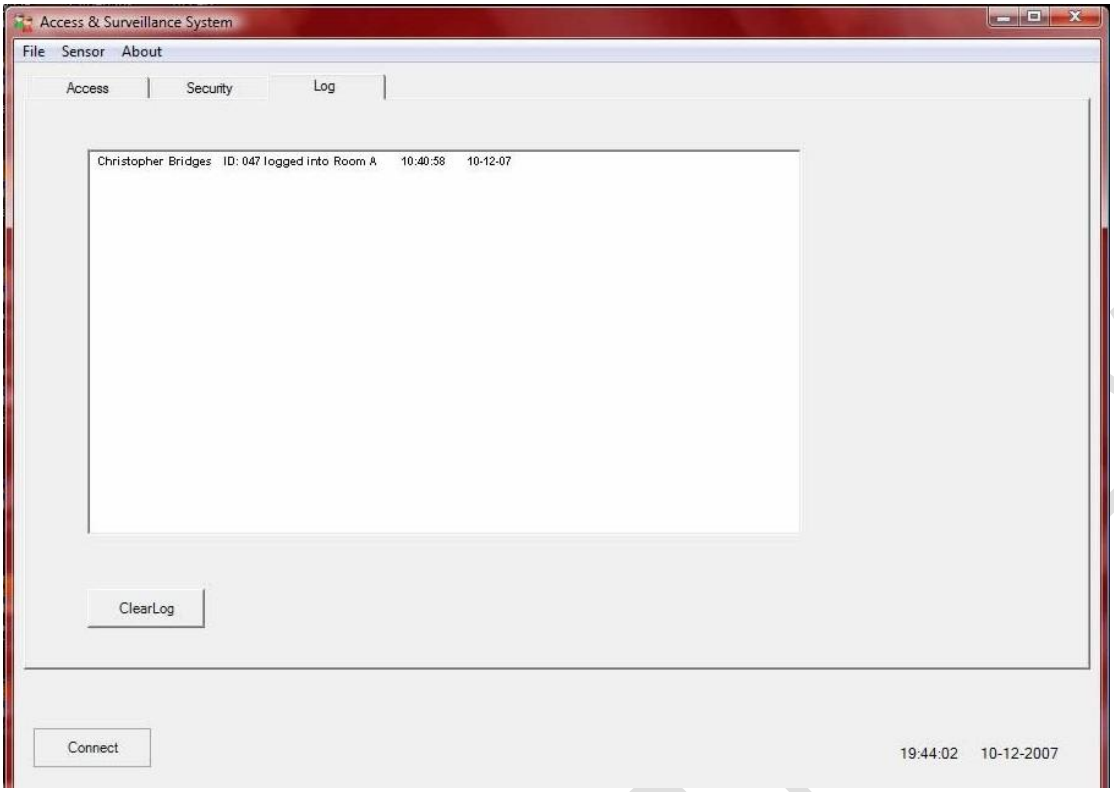

Figure 16: PCGUIwithtabpositionedtoLog

4.1 SYSTEMTESTING

The circuit was first designed and simulated on Electronic Workbench circuit simulation software. The simulation design was then implemented on a *bread board* for real life testing. After troubleshooting, the final design was then soldered unto a pre-etched board. The different modules were connected together with the hardware components soldered on a pre-etched board.
Thesystemwastested,andthefollowingobservationsweremade:

- The GUI worked well though more efficient code partitioning would reduceits memory usage.
- Thehardwaremoduleworkedwellexceptforrandomdiscontinuitiesinthe circuit consistent with pre-etched perforated boards.
- The card reader was effective. However, due to the card material and the card reader contact type, data errors occurred.

5.0 LIMITATIONS

Microcontroller-based security systems offer many advantages, such as cost-effectiveness, flexibility, and ease of implementation. However, they also have some limitations that should be considered:

- Limited processing power: Microcontrollers have limited processing power compared to more powerful computing devices. This limitation can affect the complexity and speed of security algorithms and protocols that can be implemented on the system.

- Memory constraints: Microcontrollers have limited memory capacity, which can restrict the amount of data that can be stored and processed by the security system. This limitation can impact the storage of encryption keys, logs, and other critical security information.

- Security vulnerabilities: Like any electronic system, microcontroller-based security systems are susceptible to security vulnerabilities such as buffer overflows, side-channel attacks, and hardware-based attacks. Proper security measures and protocols must be implemented to mitigate these risks.

- 4. Scalability issues: Microcontroller-based security systems may face challenges when it comes to scaling up to accommodate larger networks or more complex security requirements. Upgrading or expanding the system may require significant redesign and reconfiguration.

- 5. Limited connectivity options: Some microcontrollers have limited connectivity options, which can restrict the ability to integrate with other devices or systems in a network. This limitation can impact the overall effectiveness and interoperability of the security system.

By being aware of these limitations, designers and developers can make informed decisions when designing and implementing microcontroller-based security systems to ensure they meet the desired security objectives effectively.

6.0 CONCLUSIONS AND RECOMMENDATIONS

The concept of real time central monitoring security systems was used for the design, fabrication and testing of microcontroller-based security system for an industrial complex. The need for authenticating individuals'requests to have access to the complex as well as reactively responding to intruder attempts necessitated this study. A simple hardware data acquisition unit based on a microcontroller was designed. With the microcontroller, many sub systems were integrated into one module and monitored continuously. A central monitoring unit was also implemented using a PC. The software for analysis and display of the data was designed using an object-oriented approach and is GUI based for easier monitoring. When tested, the GUI provides graphic display of the trends from the sensor device. The data from the hardware unit was connected to the PC via the parallel port interface. The microcontroller possesses an upgradeable model attribute. However, its functionality was restricted due to certain limitations. Possible upgrades or enhancements of the model include:

- Internet based PC Interface Application – this allows the user or administrator to monitor the security system over a long distance via the internet.
- UniversalSerialBus(USB)portinterfacing–althoughmorecomplexthanthe parallel port, USB has the advantage of being fast and convenient. Moreover, with the parallel port slowing becoming obsolete in the new technological era, the USB port has to be embraced.
- More secure access card system– the use of a more sophisticated and efficient card system to reduce or eliminate forgery and false authentication.
- Programmable Logic Devices (PLD) – The use of PLDs to replace the Transistor-TransistorLogic(TTL)employedinthehardwarecircuit.This increases the circuit capability and reduces the space required (a circuit consisting of many TTL ICs can be programmed on a single PLD) as well as development time.

References

[1] Uddin, M.M.; Al Mahmud, A.; Islam, N. Design & implementation of a microcontroller based automatic power factor rectification system for different loads. In Proceedings of the 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT), Dhaka, Bangladesh, 3–5 May 2019; pp. 1–6

[2] Islam, J.; Habiba, U.; Kabir, H.; Martuza, K.G.; Akter, F.; Hafiz, F.; Haque, M.A.S.; Hoq, M.; Mannan, M.A. Design and development of microcontroller based wireless humidity monitor. *IOSR J. Electr. Electron. Eng.* **2018**, *13*, 41–46..

[3] Cermeño, E., Pérez, A. and Sigüenza, J. A. (2018). Intelligent Video Surveillance beyond Robust Background Modeling, Expert Systems with Applications, 91:138- 149.

[4] Levshun, D.; Chechulin, A.; Kotenko, I. Design of Secure Microcontroller-Based Systems: Application to Mobile Robots for Perimeter Monitoring. *Sensors* **2021**, *21*, 8451

[5] Levshun D, Chechulin A, Kotenko I. Design of Secure Microcontroller-Based Systems: Application to Mobile Robots for Perimeter Monitoring. *Sensors*. 2021; 21(24):8451

[6] Levshun, D.; Kotenko, I.; Chechulin, A. The application of the methodology for secure cyber–physical systems design to improve the semi-natural model of the railway infrastructure. *Microprocess. Microsystems* **2021**, *87*, 103482

[7] Levshun, D.; Kotenko, I.; Chechulin, A. The integrated model of secure cyber-physical systems for their design and verification. In Proceedings of the International Symposium on Intelligent and Distributed Computing, St. Petersburg, Russia, 7–9 October 2019; pp. 333–343..

[8] Pivarčiová, E.; Božek, P.; Turygin, Y.; Zajačko, I.; Shchenyatsky, A.; Václav, Š.; Císar, M.; Gemela, B. Analysis of control and correction options of mobile robot trajectory by an inertial navigation system. *Int. J. Adv. Robot. Syst.* **2018**, *15*

[9] K. Cabaj, G. Mazur, and M. Nosek, “Compromising an iot device based on harvard architecture microcontroller,” in Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2018, vol. 10808, p. 108082G, International Society for Optics and Photonics, 2018
[10] Schaefer, F. M., Kays, R. (2019), A Wireless Multi-Channel Transmission System for Smart Home Applications. Proceeding of European Wireless Conference, pp. 1-6.
[11] STMElectronics (2018) STM32F103XX Reference Manual, 1134 pp
[12] Sharma, P. and Kamthania, D. (2020), "Intrusion Detection and Security System", Tanwar, P., Jain, V., Liu, C.-M. and Goyal, V. (Ed.) Big Data Analytics and Intelligence. Emerald Publishing Limited, Leeds, pp. 139-151
[13] Zou, H., Zhou, Y., Jiang, H., Chien, S. C., Xie, L., Spanos, C. J. (2018). Win Light: A Wi-Fi-based occupancy-driven lighting control system for smart building. Energy and Buildings, 158, 924- 938.
[14] Karapetyan, A., Chau, S. C. K., Elbassioni, K., Khonji, M., Dababseh, E. (2018) Smart lighting control using oblivious mobile sensors. In Proceedings of the 5th Conference on Systems for Built Environments (pp. 158-167).
[15] Xia X., Liu C., Wang H. and Han Z. A Design of Cyber-Physical System Architecture for Smart City // Recent Trends in Intelligent Computing, Communication and Devices. Springer, Singapore, 2020. P. 967-973.
[16] Alguliyev R., Imamverdiyev Y., Sukhostat L. Cyber-physical systems and their security issues // Computers in Industry. 2018. Vol. 100. P. 212-223.
[17] David, N., Ajah, G. (2014) A Microcontroller Based Security System. Sch. J. Eng. Tech., 2(6B), 868-873.
[18] Cardin O. Classification of cyber-physical production systems applications: Proposition of an analysis framework // Computers in Industry. 2019. Vol. 104. P. 11-21.
[19] Gaifulina D., Kotenko I., Fedorchenko A. A Technique for Lexical Markup of Structured Binary Data for Problems of Protocols Analysis in Uncertainty Conditions. Systems of Control, Communication and Security. 2019. Vol. 4. P. 280–299
[20] Gbadamosi K. O., Adebayo, S., Charles, G., Ogbewey, L. (2021) Design of a Microcontroller Based Mobile Security Lighting Control System. American Journal of Engineering Research (AJER), vol. 10(5), pp. 85-91.
[21] Louis, U., Goshwe, N. Y., Enokela, J. A. (2022) Design and Implementation of a Microcontroller Based Community Surveillance System. International Journal of Advances in Engineering and Management, Volume 4, Issue 11, 872-884.
[22] Stephen N.A., Okere M.G., Egwu U.A., Uchechukwu J.O., Benson M.S. (2023) Design and Construction of a Micro Controller Based Smart Automated System for Controlling Various Home Appliances, International Journal of Electrical and Electronics Engineering Studies, Vol.9, No.1, pp. 1-36.