ACCESS AND ASSET MANAGEMENT OF AN ACADEMIC INSTITUTE

A DISSERTATION

Submitted in partial fulfillment of the requirements for the award of the degree

of

MASTER OF TECHNOLOGY

in

ELECTRICAL ENGINEERING

(With Specialization in Measurement and Instrumentation)

By

KULKARNI ABHIJEET SUDHAKAR

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE-247 667 (INDIA)

JUNE, 2011

CANDIDATE'S DECLARATION

I hereby declare that the work that is being presented in this dissertation report entitled **"Access and Asset Management of an Academic Institute"** submitted in partial fulfillment of the requirements for the award of the degree of **Master of Technology** in **Electrical Engineering** with specialization in "Measurement and Instrumentation", submitted to the **Department of Electrical Engineering, Indian Institute of Technology Roorkee,** Roorkee, is an authentic record of my own work carried out, under the guidance of, **Dr. H. K. Verma,** Professor, Department of Electrical Engineering, Indian Institute of Technology, Roorkee and **Dr. Vinod Kumar,** Professor, Department of Electrical Engineering, Indian Institute of Technology, Roorkee. The matter presented in this dissertation report has not been submitted by me for the award of any other degree of this institute or any other institute.

Date: June 27 - 11

Place: Roorkee

Kulkarni Abhijeet Sudhakar.

Enrollment No. 09528008

CERTIFICATE

This is to certify that the above statement made by the candidate is true to the best of our knowledge.

27.6.11

Dr. H. K. Verma
Professor,
Department of Electrical Engineering,
Indian Institute of Technology,
Roorkee – 247667.

27/6/11

Dr. Vinod Kumar
Professor,
Department of Electrical Engineering,
Indian Institute of Technology,
Roorkee – 247667.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my guides **Dr. H. K. Verma**, Professor, Department of Electrical Engineering, Indian Institute of Technology, Roorkee and **Dr. Vinod Kumar**, Professor, Department of Electrical Engineering, Indian Institute of Technology, Roorkee for their valuable guidance, support, encouragement and immense help.

I express my deep and sincere sense of gratitude to all the faculty members of Measurement and Instrumentation group.

I am thankful to Mr. Jawale, Mr. Navin Kumar and all my friends who have helped directly or indirectly for the completion of this Dissertation.

I gratefully acknowledge my heartiest thanks to all my family members for their inspirational impetus and moral support during the course of work. Finally, I would like to express my deepest gratitude to the Almighty for showering blessings on me.

Kulkarni Abhijeet Sudhakar.

(Enrollment No. 09528008)

ABSTRACT

Radio Frequency Identification (RFID) and Global Positioning Systems (GPS) are two very important emerging fields of technology which are opted for prevalent application types, like item tracking, tracing, antitheft, access monitoring, asset monitoring and management, management of outdoor and mobile assets, vehicle tracking etc. Wireless Sensor Networks (WSN) technology is widely used for monitoring environmental parameters. In access monitoring and control, RFID smart cards are used, to allow or to deny entry to members, as per a predetermined policy. Detection and identification of objects carrying RFID tags is much easier and reasonable than other sensor technologies. GPS is indispensable system in vehicle tracking and tracing of assets in outdoor environment. Its integration with RFID facilitates the identification of vehicle and monitoring of its position.

In this dissertation, access management system is implemented by using RFID smart cards with the available database containing information about each individual working or studying in the institute along with the facility which allows entering information about visitors. RFID is also used to track, manage and secure institute assets which are broadly classified in seven categories viz. electronic products, laboratory equipments, library stuff, office documents, furniture, vehicle, thesis. Asset management also includes monitoring condition of assets for which mainly environmental parameters are monitored such as temperature, pressure, humidity and light intensity. Any sudden environmental disturbances or intended deeds to damage or destroy the assets results in change in these parameters which are sensed and displayed along with alarm by using WSN technology. GPS integrated in Crossbow sensor board (MTS420) is used to track institute vehicle while the Zigbee protocol based MTS 400 is used to monitor environmental parameters. Integration of these technologies will help in enhancement of productivity, efficiency and satisfaction of user. LabVIEW provides the necessary platform required to integrate these technologies along with Microsoft Office Access database. The database maintains the complex relations between assets and their access to different users. Security and integrity of database is maintained by allowing its access only to respective authority. Highly informative and user friendly GUIs developed in LabVIEW display the obtained results.

INDEX

LIST OF FIGURES

LIST OF TABLES

CHAPTER-1

INTRODUCTION

RFID (Radio Frequency IDentification) is the most widely used technology in item tracking. It is an Auto Identification and Data collection technology which helps to automate business processes and allows identification of large number of tagged objects. The GPS (Global Positioning System) is the most promising technology to acquire the position information in outdoor environments [1]. Always it is chosen for tracking of vehicles, assets over a wide geographical area. With simultaneous data received from four satellites and ideal conditions and minimal ionosphere, users can calculate an object's location including mainly latitudinal and longitudinal position [2]. Wireless Sensor nodes (also called as motes) provide the information about the environmental parameters such as temperature, humidity, light intensity etc. in the environ enclosing critical assets. The combination of the information and integration of these intelligent technologies improve the asset monitoring and managing capabilities.

1.1 Asset Management:

"Asset management" is largely dependent on the perspective from which we are analyzing the assets and the purpose of the study.

1.1.1 Assets: [3, 4, 5, 6, 7]

From an infrastructure perspective, according to the International Infrastructure Management Manual [3], an asset is defined as "A physical component of a manufacturing, product or service facility which has value, enables services to be provided, and has an economic life of more than twelve months". The BSI PAS 55-1 standard specifications [4] describes an asset as "Plant, machinery, property, buildings, vehicles and other items and related systems that have a distinct and quantifiable business function or service."

References [5] and [6] distinguish between the broad range of assets an enterprise has, and classify them as:

i. Intangible assets: designs, knowledge, software, intellectual property, and processes.
ii. Tangible assets: liquid assets (cash or inventories) and fixed assets (building and infrastructures, IT equipment, machineries, hardware, and product and service equipment.

In short, An asset is defined as any physical core, acquired elements of significant value to the organization, which provides and requests services for this organization" [7].

1.1.2 Definition of Asset Management: [4, 7, 8, 9]

According to the BSI PAS 55-1 [4], asset management is defined as "Systematic and coordinated activities and practices through which an organization optimally manages its assets, and their associated performance, risks and expenditures over their lifecycle for the purpose of achieving its organizational strategic plan." Woodhouse [9] define asset management as "The set of disciplines, methods, procedures and tools derived from business objectives aimed at optimizing the whole life business impact of costs, performance and risk exposures associated with the availability, efficiency, quality, longevity and regulatory/safety/environmental compliance of an organization's assets." According to Koronios [8], "Asset management entails preserving the value function of an asset during its lifecycle and maintaining it to as designed or near original condition through maintenance, upgrade, and renewal until sustainable retirement of the asset due to end of need or technology refresh."

Hence, "Asset management is the process of organizing, planning and controlling the acquisition, use, care, refurbishment, and/or disposal of physical assets to optimize their service delivery potential and to minimize the related risks and costs over their entire life through the use of intangible assets such as knowledge based decision-making applications and business processes." [7]

For Asset management, we require:

i. Monitoring of asset location.
ii. Monitoring of asset condition.

1.1.2.1 Monitoring of Asset Location. [5, 7]

Asset information is very important for organizations because it represents the collective knowledge used to manage assets. Understanding what information is needed to support management process and what data can be gathered as raw material for such information, is an essential starting point to build up the management strategy. Knowing the location of the assets is critical to effectively manage them. Providing relevant, timely and useful location information to the people and the systems responsible for managing assets provides a number of significant benefits, such as ease in making quick and informed decisions based on real-time information, reduction in costs, time associated with searching for misplaced or lost assets, and improves overall productivity and throughput. [5] Furthermore, one of the major reasons to track assets is when the cost of not knowing the location of an asset at a given time can be considerable. Sometimes the value of the asset itself is not as important as the cost of the consequence of losing track of the asset or information about its location. Hence, asset location tracking involves understanding (i) where your assets are at present; (ii) where they were at last; and (iii) how many of them are in a given location. [7]

1.1.2.2 Monitoring of Asset Condition: [7, 9]

The benefits and necessity of tracking asset condition should be discussed from both perspectives: an asset user perspective and an asset provider perspective. From an asset provider perspective, it has become more important to understand and track how each asset is used and behaves. The fundamental issues in ensuring asset reliability are capturing information during its operational stage and using it to predict asset behavior as well as failure conditions. The information captured could be used to trigger appropriate and timely follow up actions. From an asset user perspective, flawless operation of the assets is required. The process of asset acquisition, deployment, operation, maintenance and replacement is a complex process. Hence, Continuous condition monitoring is required to predict failures as soon as the asset starts deviating away from its standard operational behavior.

1.2 Access Management: [11]

Monitoring access to an academic institute is very essential in asset management of an academic institute. Physical access control, which is essential in access control, is primarily based on smart card technology and numerous commercialized solutions are available in the market. [11] Proximity access control systems are very useful in universities, academic institutes for handling and controlling physical access of users to individual facilities and rooms. Physical access systems usually deal with hardware or electronic devices that mainly control the locking mechanisms on doors or gateways. It is generally based on some access control lists, which are sets of predefined rules and constraints used to validate the access permission of cardholders. The lists are usually updated periodically within a certain period of time, which might reduce security holes within the system. These systems trigger the hardware devices to open doorway locks if authorized is granted to the user.

Smart cards are portable and highly reliable medium for storage of personal identification data of individual users. By simply presenting a card to access devices, permission will be either granted or denied based on comparison to an access control list.

1.3 Relevant Technologies: [7, 10, 34]

An RFID-based traceability system and its wireless communication technology are emerging technologies in asset management. An RFID system basically consists of three components, tags (transponders), reader (scanners or antenna) and an application system for further processing of the acquired data. A tag contains a microchip, capacitors and an antenna coil that is embedded into an encapsulation material, e.g., a coin, glass body, plastic substrate, smart label etc. The tags communicate via radio signals with an RFID–Reader, which is a central component of an RFID System. A reader can either be a peripheral or handheld device. RFID systems usually operate on the ISM (Industry, Scientific, and Medical) frequency bands. For locating assets in transit, technologies such as GPS can also be used. GPS consists of three segments: the space segment, the control segment, and the user segment. The space segment consists of the 24-satellite constellation. Each GPS satellite transmits a signal. It consists of following components: two sine waves (also known as carrier frequencies), two digital codes, and a navigation message. The control segment of the GPS system consists of a worldwide network of tracking stations. It has a master control station (MCS) located in the United States at Colorado Springs, Colorado. The primary task of the operational control segment is tracking the GPS satellites in order to determine and predict satellite locations, system integrity, behavior of the satellite atomic clocks, atmospheric data. This information is then packed and uploaded into the GPS satellites through the S-band link. The user segment includes all military and civilian users. With a GPS receiver connected to a GPS antenna, a user can receive the GPS signals, which can be used to determine his or her position anywhere in the world. In addition to these technologies, sensors can be used to provide information about the condition of an asset. This information can be a set of variable quantities, which can completely describe the system at a given point in time. Sensors can be used to measure many different parameters, including temperature, humidity, light intensity, pressure etc. To satisfy the requirement of asset management, the use of a single sensor is not always enough and an integration of various sensor technologies is required (e.g. wireless sensor networks (WSN)).

Identification technologies are only part of the solution for asset management. Consequently, there is a need for an overall framework to specify, design, and operate these technologies. Laboratory Virtual Instrumentation Engineering Workbench (LabVIEW) can provide a common platform to integrate all of these technologies. LabVIEW is a high-level programming language with Graphical Language developed by National Instruments. It can support interfaces such as GPIB, USB IEEE1394, MODBUS, SERIAL, PARALLEL, IRDA, TCP, UDP, Bluetooth, NET ActiveX, SMTP, etc. LabVIEW is usually used for data acquisition, instrument control, and industrial automation on all kinds of platforms such as Microsoft Windows, UNIX, Linux, and Mac OS. LabVIEW can integrate the RFID system and the database. The interface of LabVIEW can help us to find out which asset is not in the correct place. Access is used to set up a database containing all the required information for asset management. Access is one of the members of the Microsoft Office system. It is a relational database management system from Microsoft which combines the relational Microsoft Jet Database Engine and graphical user interface. Access can use data stored in Access/Jet, Microsoft SQL Server, Oracle, or any ODBC-compliant data container.

1.4 Problem Definition:

A robust Asset Management solution is required in case of academic institute, so as to provide automated access to contents or services. A core issue in the design of Asset Management solution of such institutes is the capability to model complex assets and their dependencies in an environment, where such assets are continually being defined, accessed, modified, tracked, and reused [27]. Asset Management along with Access management majorly ensures anti-theft platform with many other aspects such as detailed record of visitors, better human resource management, and centralized database etc. In this dissertation, access and asset management is intended to automate many aspects of operations and day to day activities of an academic institute. A small academic institute, having a single building and covering small area is considered in this dissertation. Medium and large sized buildings can be covered with this solution by using networked database. Major issues covered in access and asset management are:

1. Provide anti-theft platform.

2. Quick access to information of entrants.
3. Better utilization of security resources.
4. Centralized database covering complex relations between assets and their access.
5. Tracking and location detection of assets.
6. Monitoring condition of assets and their environment.
7. Tracing and tracking mobile assets in the outdoor environment.
8. Automated system to keep a track of people present inside of academic building.

1.5 Organization of the Dissertation:

As the name suggests, "Access and asset management of an academic institute", it covers both access management and asset management. The first chapter discusses the introduction to the access management, asset management, their definitions, relevant technologies and the exact problem definition.

Chapter-2 covers relevant technologies used in this dissertation which are RFID and GPS. In brief, it covers their working principle, operating frequencies, relative standards and their use in access and asset management systems.

Chapter-3 deals with the hardware platform used for access management system and hardware platform used for the asset management system, while Chapter-4 describes the software platform used for access management system and software platform used for asset management system. These chapters also describe the subsystems incorporated in access management and asset management system and their flowcharts.

Chapter-5 provides details about implementation of these systems. It also shows the results obtained by implementing the subsystems described in Chapter-4.

Chapter-6 concludes the dissertation and also enlists the major possible enhancements in access and asset management system for a typical or average academic institute. The specifications and brief details about the hardware used are covered in the appendices provided at the last of this report.

CHAPTER-2
TECHNOLOGIES USED

Radio Frequency Identification (RFID) and Global Positioning System (GPS) are two important wireless item tracking technologies. Combination of both technologies is a major area of interest of many organizations for the purpose of asset tracking and monitoring , and wide research is in progress in this regard. Wireless Sensor Networks (WSNs) are large networks made of number of sensor nodes. These offer low-cost solution in many areas such as environmental monitoring and conservation, automation in transportation, manufacturing and asset management.

2.1 RFID Technology:

Radio frequencies, mostly microwaves in the UHF region, are analog like other physical signals in nature. These radio frequency waves were selected by the Auto-ID (Automatic Identification) Center at MIT for its passive RFID initiative. The first RFID applications were developed in conjunction with radar technology in the Second World War, for Identification Friend or Foe (IFF) systems. In this system the RF transponder (tag) and interrogator (reader) were designed to detect friendly airplanes [13]. A precursor to passive RFID was the Electronic Article Surveillance (EAS) systems. It was deployed in retail stores in the 1970s. The system used Dedicated Short-Range Communication (DSRC) RF technology for anti-theft detection [12]. In the 1960s, Los Alamos National Laboratory incorporated RFID tags into employee badges to automatically identify people, limit access to secure areas, and make it harder to duplicate the badges.

2.1.1 RFID Working Principle [15, 16, 17]:

In a typical system tags are attached to objects. Each tag has a certain amount of internal memory (EEPROM) in which it stores information about the object, such as its unique ID (serial) number, or in some cases more details including manufacture date and product composition. When these tags pass through a field generated by a reader, they transmit this information back to the reader, thereby identifying the object

2.1.1.1 Communication between Reader and Tag:

The communication process between the reader and tag is managed and controlled by one of several protocols, such as the ISO 15693 and ISO 18000-3 for HF or the ISO 18000-6, and EPC for UHF. In general, when the reader is switched on, it starts emitting a signal at the selected frequency band (typically 860 - 915MHz for UHF or 13.56MHz for HF) [2]. Any corresponding tag in the vicinity of the reader will detect the signal and use the energy from it to wake up and supply operating power to its internal circuits. Once the Tag has decoded the signal as valid, it replies to the reader, and indicates its presence by modulating (affecting) the reader field.

The communication between a reader and a tag can be one of the following:

1. Modulated backscatter: Modulated backscatter communication applies to passive as well as to semi-active tags. In this type of communication, the reader sends out a continuous wave (CW) RF signal containing AC power and clock signal to the tag at the carrier frequency. Through physical coupling (that is, a mechanism by which the transfer of energy takes place from the reader to the tag), the tag antenna supplies power to the microchip. Thus reader initiates the communication.
2. Transmitter type: This type of communication applies to active tags only. In this type of communication, the tag broadcasts its message to the environment in regular intervals, irrespective of the presence or absence of a reader. Therefore, in this type of communication, the tag always initiates the communication.
3. Transponder type: It applies to a special type of active tags called transponders. In this type of communication, the tag goes to a "sleep" mode in the absence of interrogation from a reader. In this state, the tag might periodically send a message to check whether any reader is listening to it. When a reader receives such a query message, it can instruct the tag to “wake up”. When the tag receives this command from the reader, it exits its current state and starts to act as a transmitter tag again.

2.1.1.2 Anti-Collision:

If many tags are present then they will all reply at the same time, which at the reader end is seen as a signal collision and an indication of multiple tags. The reader manages this problem by using an anti-collision algorithm designed to allow tags to be sorted and individually selected. There are many different types of algorithms (Binary Tree, Aloha....) which are defined as part of the protocol standards. The number of tags that can be identified depends on the frequency and protocol used, and can typically range from 50 tags/s for HF and up to 200 tags/s for UHF.

Once a tag is selected, the reader is able to perform a number of operations such as read the tags identifier number, or in the case of a read/write tag write information to it. After finishing dialoging with the tag, the reader can then either remove it from the list, or put it on standby until a later time. This process continues under control of the anti collision algorithm until all tags have been selected.

2.1.2 Overview of RFID Systems [15, 16]:

An RFID system is an integrated collection of components that implement an RFID solution. The schematic diagram of RFID system is shown in Fig. 2.1.

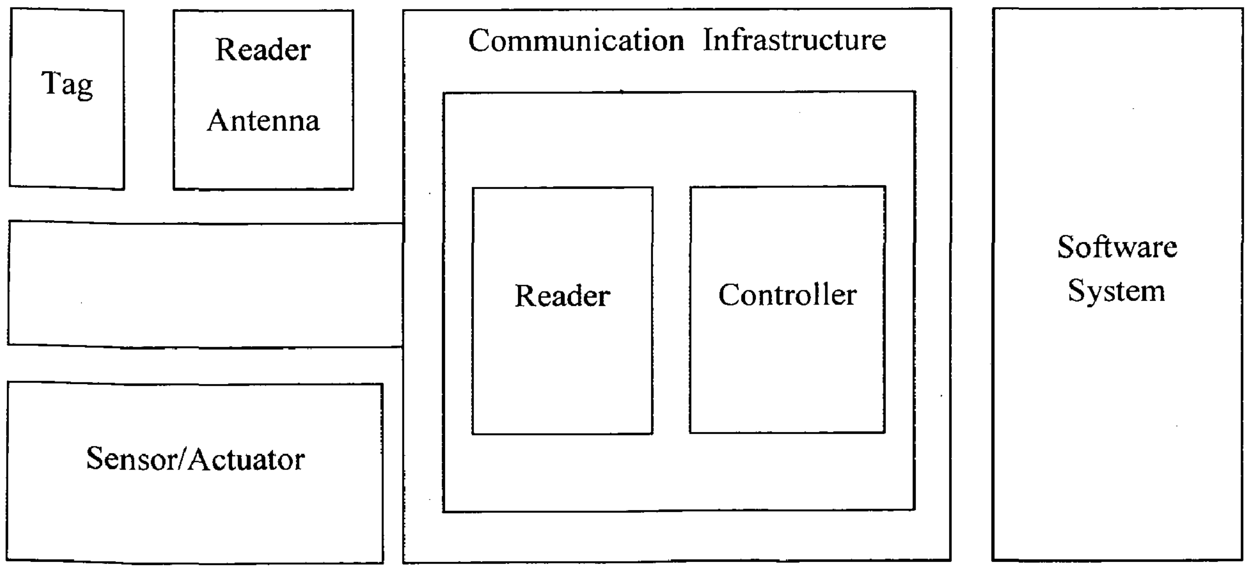


Fig. 2.1 Schematic Diagram of RFID System [16]

1) RFID Tags:

Every object to be identified in an RFID system will need to have a tag attached to it. An RFID tag is a device that can store and transmit data to a reader in a contactless manner using radio waves.

Tags are manufactured in a wide variety of packaging formats. These formats are designed for different applications and environments. In the basic assembly process, at first a substrate material (Paper, PVC), upon which an antenna made from one of many different conductive materials like Silver ink, Aluminum and copper, is deposited. Then the Tag chip is connected to the antenna; using techniques such as wire bonding or flip chip. Finally a protective overlay made from materials such as PVC lamination, Epoxy Resin or Adhesive Paper, is added. This protective layer allows the tag to support some of the physical conditions found in many applications like abrasion, impact and corrosion. These four steps of RFID tag packaging are shown in Fig. 2.2.

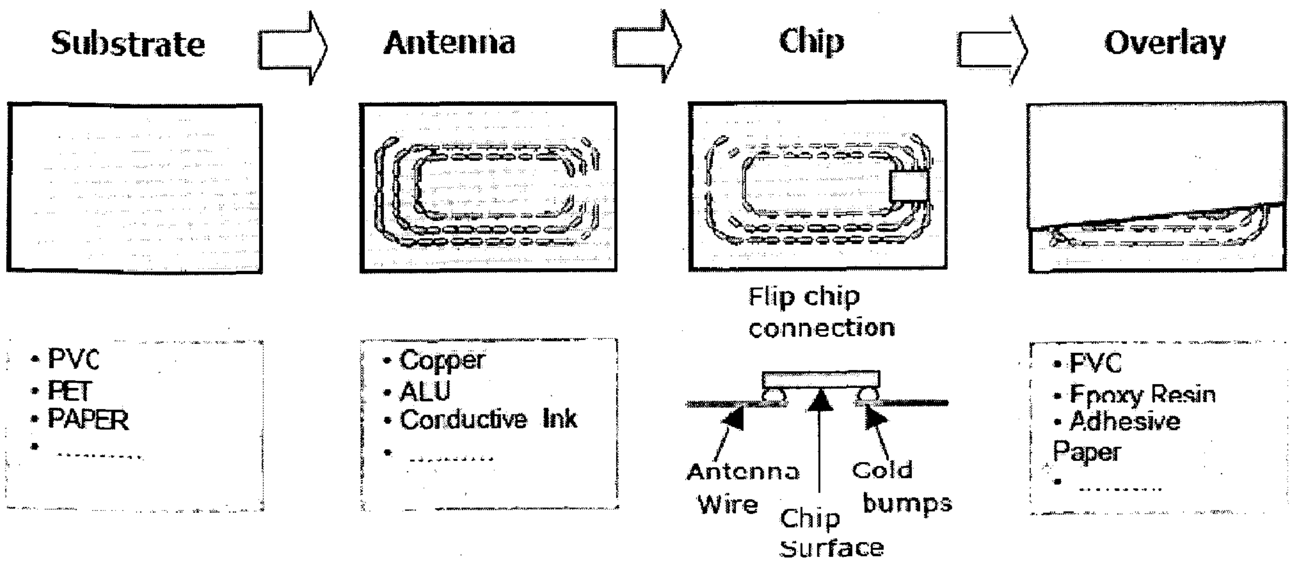


Fig. 2.2 Basic Tag Manufacturing Steps [15]

Classification of RFID Tags:

RFID tags can be classified in three different ways, which is based on whether the tag contains an on-board power supply and/or provides support for specialized tasks. These classes of RFID tags are described below:

Comparison between active, passive and semi-passive tags is given in Table 2.1.

	Advantages	Disadvantages	Remarks
Passive	• Longer life time • Tags are more mechanically Flexible Lowest cost	• Distance limited to 4 - 5m (UHF) • Strictly controlled by local regulations	Most widely used in RFID applications. Tags are LF ,HF or UHF
Semi-passive	• Greater communication distance • Can be used to manage other devices like sensors (Temp°, pressure etc) • Do not fall under the same strict power regulations imposed on passive devices	• Expensive - due to battery, and tag packaging • Reliability impossible to determine whether a battery is good or bad, particularly in multiple transponder environments. • It presents an environmental hazard from potentially toxic chemicals in batteries.	Used mainly in real time systems to track high value materials or equipment throughout a factory. Tags are UHF
Active			Used in logistics for tracking of containers on trains and trucks etc. Tags are UHF or microwave

Table 2.1. Comparison between Active, Passive and Semi-Passive Tags

2) Readers:

An RFID reader, also called an interrogator, is a device that can read from and write data to compatible RFID tags. The act of writing the tag data by a reader is called creating a tag.

The basic components of RFID reader are shown in Fig. 2.4.

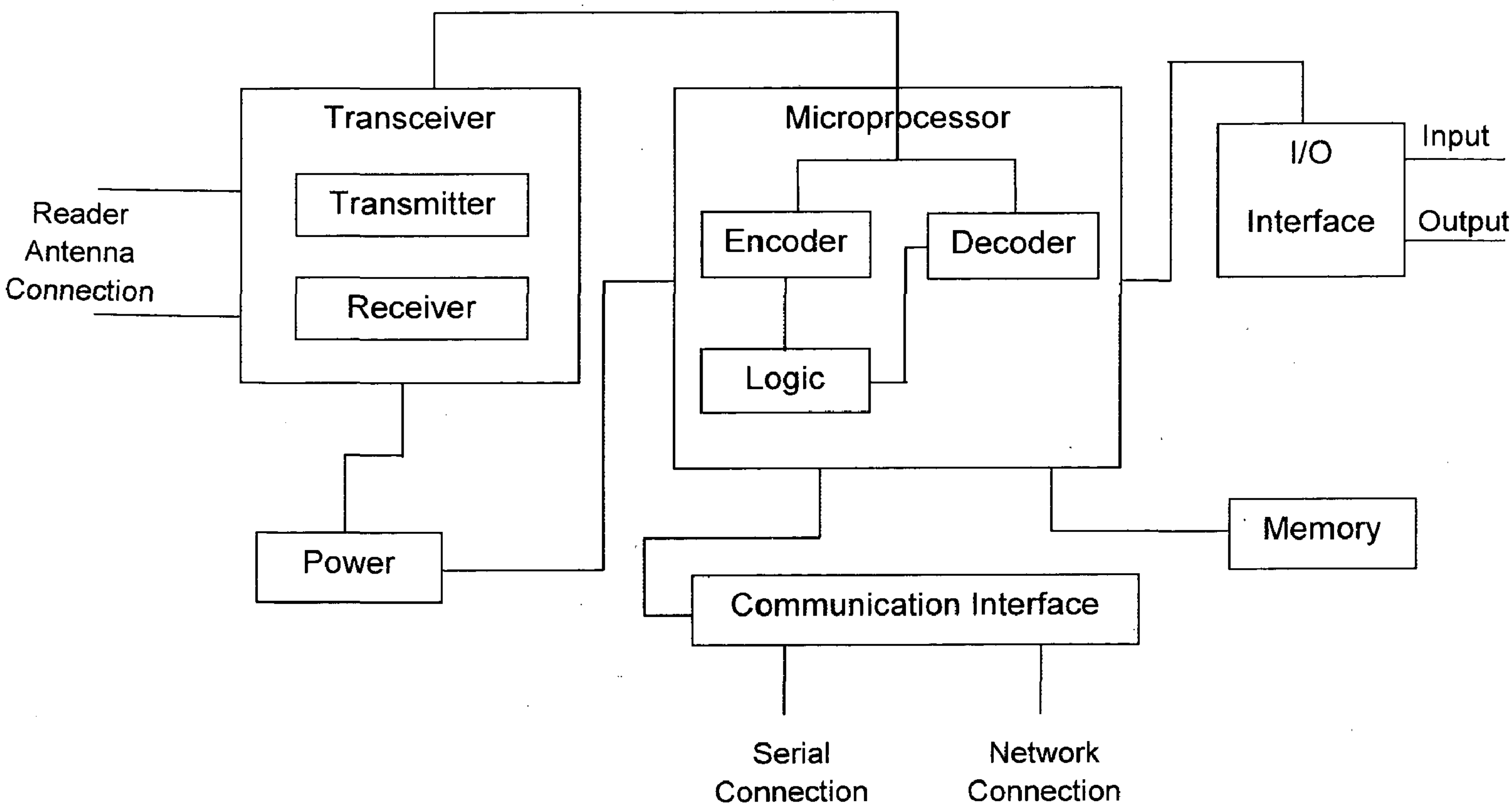


Fig. 2.3 Basic Components of a Reader [16]

a) Transmitter: The reader's transmitter is used to transmit AC power and the clock cycle via its antennas to the tags in its read zone. The antenna ports of a reader are connected to its transceiver component.

b) Receiver: It receives analog signals from the tag via the reader antenna. It then sends these signals to the reader microprocessor, where it is converted to its equivalent digital form

c) Microprocessor: This component is responsible for implementing the reader protocol to communicate with compatible tags. It is performs decoding and error checking of the analog signal from the receiver. In addition, the microprocessor might contain logic unit for doing low-level filtering and processing of read tag data.

d) Memory: Memory is used for storing data such as the reader configuration parameters and a list of tag reads. Therefore, if the connection between the reader and the controller/software system goes down, not all read tag data will be lost. Depending on the memory size, a limit applies as to how many such tag reads can be stored at any time. If the connection remains down for an extended period, with the reader reading tags during this downtime, this limit might be exceeded and part of the stored data may be lost.

e) Input/Output Channels: Readers do not have to be turned on for reading tags at all times. The tag might appear only at certain times and leaving readers perpetually ON would just waste the reader's energy. This component provides a mechanism for turning a reader ON and OFF depending on external events. A sensor like motion or light sensor, detects the presence of tagged objects in the reader's read zone. This sensor can then set the reader ON to read this tag.

f) Communication Interface: The communication interface component provides the communication instructions to a reader that allow it to interact with external entities through a controller, to transfer its stored data and to accept commands and send back the corresponding responses. Serial and network interface is generally provided.

g) Power: This component supplies power to other reader components.

3) Reader Antenna:

For low power proximity range (< 10cm) HF applications such as access control, antennas tend to be integrated in with the reader. For longer range, HF (10cm < 1m) or UHF (< 3m) applications, the antenna is external and connected at some distance to the reader via a shielded and impedance matched coaxial cable. RFID antennas used in UHF applications fall in the following main categories:

a) Linear polarized: The RF waves emanate in a linear patter from the antenna. These waves have only one energy field. A linear polarized antenna has a narrower radiation beam with a longer read range compared to a circular polarized antenna. However, a linear polarized antenna is sensitive to tag orientation with respect to its polarization direction. These types of antenna are therefore useful in applications where the tag orientation is fixed and predictable.

b) Circular polarized: RF waves radiate from a circular polarized antenna in a circular pattern. These waves have two constituting energy fields that are equal in amplitude and magnitude, but have a phase difference of 90°. Therefore, when a wave of an energy field is at its highest value, the wave of the other field is at its lowest. Because of the nature of polarization, a circular polarized antenna is largely unaffected by tag orientation.

4) Controller: A controller is an intermediary agent that allows an external entity to communicate with and control a reader's behavior together with the sensors and actuators associated with the reader. A controller for a reader can be embedded inside the reader or can be a separate component by itself.

5) Sensors and Actuators: A sensor can be attached with a reader for this purpose. This sensor can then be used to turn ON/OFF the reader based on some external event detected by this sensor. A sensor can thus be used to provide some kind of input trigger to a reader. An actuator is a mechanical device for controlling or moving objects e.g. PLC, robot arm etc. Sensors and actuators can thus be used to provide some kind of local output from an RFID system.

6) Communication Infrastructure: This component provides connectivity and enables security and systems management functionalities for different components of an RFID system, and is therefore an integral part of the system. It includes the wired and wireless network, and serial connections between readers, controllers, and computers. The wireless network type can range from a personal area network (PAN, provided by Bluetooth), to a local area network (LAN, offered by 802.11x technology), to a wide area network (WAN, provided by 2.5G/3G technologies).

7) Software System: The software system establishes communication with the readers. This component's main task is to get data from the readers, control the readers' behavior and use the readers to activate the associated external actuators. It also performs several tasks as filtering out duplicate reads from different readers, remote reader management.

2.1.3 RFID Standards and Operating Frequencies:

2.1.3.1 Electronic Product Code (EPC): [15]

In October 1999 the Auto-ID center was created in the Department of Mechanical Engineering by a number of leading figures at MIT. To reduce the cost of the tag, Auto-Id recognized that tags should be simple, fast and should provide the detail information of the product. Hence, it developed EPC code ranges from 64 bits to 256 bits with 4 distinct fields as shown in Fig. 3.1.

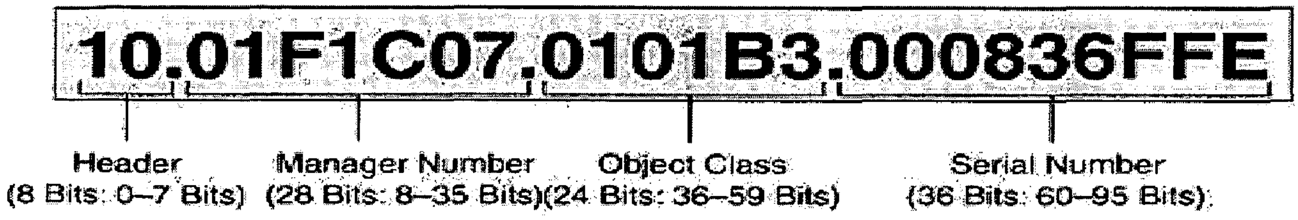


Fig. 2.4 Electronic Product Code [16]

Header (0- 7) bits: The Header is 8 bits, and defines the length of the code. The EPC length ranges from 64 to 256 bits. Here, 96 bits EPC is used.

EPC manager (8- 35) bits: It contains the manufacturer of the Product the EPC tag is attached to.

Object Class (36-59) bits: These bits refer to the exact type of product.

Serial Number (60 – 96) bits: These bit provide a unique identifier for up to products.

2.1.3.2 ISO Standards: [15, 16]

i. ISO 11784: Radio frequency identification of animals 'Code structure'. This specifies the identification 'code structure' for identifying an animal using RFID.
ii. ISO 11785: This specifies the transmission procedure between an RFID tag and reader.
iii. ISO 14443: It is used in contactless smart cards, identity cards. It deals with the physical characteristics, Radio frequency power and signal interface, initialization and anti-collision and transmission protocol.
iv. ISO 18046: RFID Tag and Interrogator Performance Test Methods. This is yet to be published.
v. ISO 18047: This is composed of the following three parts: 1) Test methods for air interface communications at 13.56 MHz. 2) Test methods for air interface

communications at 2.45 GHz. 3) Test methods for air interface communications at 433 MHz.

vi. The ISO 18000 series covers the air interface protocol for systems likely to be used to track goods in the supply chain. They cover the major frequencies used in RFID systems around the world. The seven parts are:

vii. 18000–1: Generic parameters for air interfaces for globally accepted frequencies

viii. 18000–2: Air interface for 135 KHz

ix. 18000–3: Air interface for 13.56 MHz

x. 18000–4: Air interface for 2.45 GHz

xi. 18000–5: Air interface for 5.8 GHz

xii. 18000–6: Air interface for 860 MHz to 930 MHz

xiii. 18000–7: Air interface at 433.92 MHz

2.1.3.3 Operating Frequencies: [19]

Band	LF Low frequency	HF High frequency	UHF Ultra high frequency	Microwave
Frequency	30–300kHz	3–30MHz	300 MHz–3GHz	2–30 GHz
Typical RFID Frequencies	125–134 kHz	13.56 MHz	433 MHz or 865 – 956MHz 2.45 GHz	2.45 GHz
Approximate read range	less than 0.5 metre	Up to 1.5 metres	433 MHz = up to 100 metres 865-956 MHz = 0.5 to 5 metres	Up to 10m
Typical data transfer rate	less than 1 kilobit per second (kbit/s)	Approximately 25 kbit/s	433–956 = 30 kbit/s 2.45 =100 kbit/s	Up to 100 kbit/s
Characteristics	Short-range, low data transfer rate, penetrates water but not metal.	Higher ranges, reasonable data rate (similar to GSM phone), penetrates water but not metal.	Long ranges, high data transfer rate, concurrent read of <100 items, cannot penetrate water or metals	Long range, high data transfer rate, cannot penetrate water or metal
Typical use	Animal ID Car immobiliser	Smart Labels Contact-less travel cards Access & Security	Specialist animal tracking Logistics	Moving vehicle toll

Table 2.2 RFID Operating Frequencies and Associated Characteristics.

2.1.4 RFID and Access and Asset Management:

A RFID tag is attached to the asset item to be monitored. The tag contains the unique identifier of the asset. This tag is read on a periodic as well as on demand basis. It provides the information about location and other properties such as state of this item in real time. Generally stationary readers or mobile readers read the asset tags and the data and readers location is then passed to the asset monitoring system. The distinguishing aspect of this type of application from the tracking and tracing application is collection of asset properties in real time, together with its unique ID, to aid in management of this asset. One example is collection of vehicle diagnostic data together with the vehicle's unique ID to find out its efficiency. Thus, using the data from the tagged items and vehicles, an asset-management system can locate, control, and manage resources to optimize utilization on a continuous, real-time basis. The data captured from the tagged items is fast and accurate. Also it eliminates the need of manual entry methods, which, in turn, reduces wait times in lanes.

Some of the benefits of asset management and monitoring are-

1. Better use of assets: The ability to locate, control, and use an asset when needed allows optimum use of an asset.
2. Improved operations: Accurate and automatic data capture coupled with intelligent control leads to better security of controlled areas.
3. Improved communication: Real-time, accurate data provides better communication to customers, management, and operation personnel.

In access control application the RFID tag contains unique identification data and it is carried by the object or the person to gain access e.g. a tag placed on a vehicle windshield, embedded in a person's ID badge or under his skin [16]. This tag id data is read at the access control points and the information is then forwarded to the security systems. Using this information the security systems decide the actual access permission. Such systems can be used for building security and parking access. In building security system, the entry and exit gate is accessed by using the tag Id information of the person's ID badge. In July 2004, the Mexican government announced that it was implanting RFID tags under the skin of the employees of its $30 million anti-crime computer center in Mexico City to ensure secure access to this facility and to track an employee if he or she is kidnapped [16]. It provides benefits of flexible and fast security control along with fairly economical solution. Also, the tags to be used in this application are specified by ISO 15693 standard. But the limitations include stealing the tag provided the original tag owner is unaware of this theft.

2.2 GPS Technology [20, 22, 23] :

The Global Positioning System (GPS) is satellite based navigation system that was developed by the U.S. Department of Defense (DoD) in the early 1970s. Initially, GPS was developed as a military system to fulfill U.S. military needs. However, it was later made available to civilians. Now it is being used by both the military and civilian users [20]. GPS provides continuous timing and positioning information, anywhere in the world and in any weather conditions. GPS is one way ranging system means users can only receive the satellite signals [22].

2.2.1 Current Constellation:

GPS consists of constellation of 24 operational satellites. This Constellation is known as Initial Operational Capability (IOC) was completed in July 1993. The official IOC announcement was made in December 8, 1993 [23]. Today, GPS includes the Standard Positioning Service (SPS), which provides civilian users with 100-m accuracy, and it serves military users with the Precise Positioning Service (PPS) which provides 20-m accuracy. GPS system was officially declared to have achieved full operational capability (FOC) on July 17, 1995.

The GPS constellation contained 5 Block II, 18 Block IIA, and 6 Block IIR satellites. This made the total number of satellites in GPS constellation to be 29. The GPS satellites are placed in six orbital planes, which are labeled A through F. Since more satellites were available than the currently nominal 24-satellite constellation, an orbital plane had four or five satellites. The current GPS constellation is shown in Fig. Each GPS satellite transmits a microwave radio signal. The signal consists of two carrier frequencies (or sine waves) modulated by two digital codes and a navigation message. The two carrier frequencies are generated at 1,575.42 MHz (referred to as the L1 carrier) and 1,227.60 MHz (referred to as the L2 carrier).

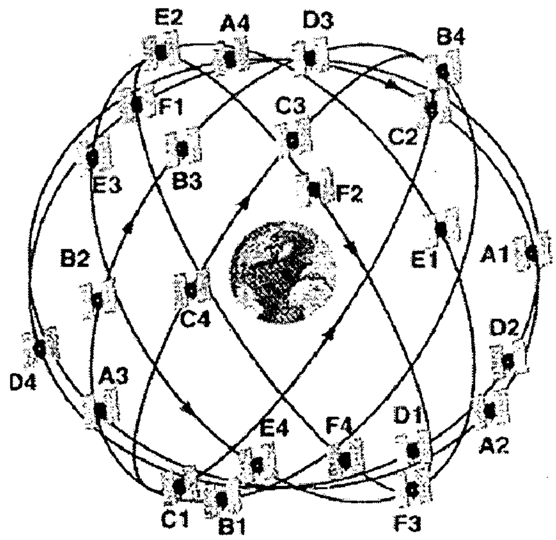


Fig.2.5 Current GPS Constellation [23].

2.2.2 Working of GPS [20, 24, 25, 26]:

The working of GPS can be explained in a better way with the help of Fig. 4.2.

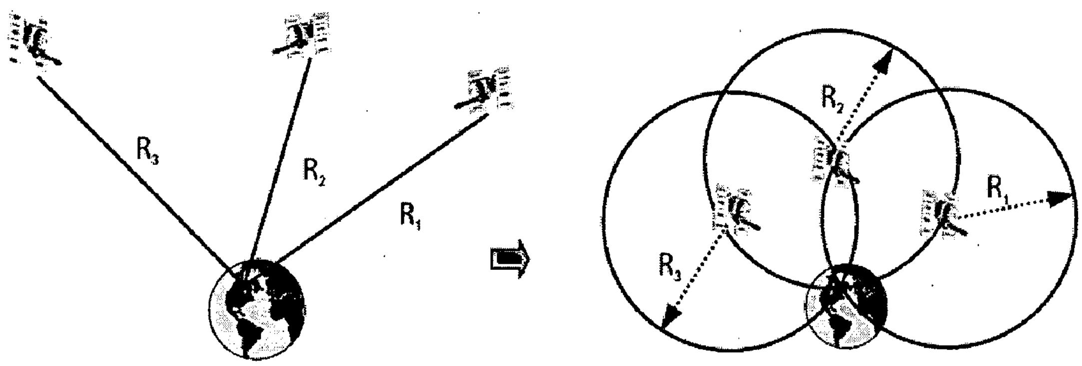


Fig. 2.6 Basic Idea of GPS Positioning [20].

If the distances from a point on the Earth (i.e. a GPS receiver) to three GPS satellites are known along with the satellite locations, then the location of the point (i.e. the GPS receiver) can be determined. Each GPS satellite continuously transmits a microwave radio signal composed of two carriers, two codes, and a navigation message. When a GPS receiver is switched on, it will pick up the GPS signal through the receiver antenna. Once the receiver acquires the GPS signal, it will process it using its built-in software. The outcome of the processing gives the distance of the satellite from receiver and satellite coordinates. That is, one GPS receiver simultaneously tracks four GPS satellites to determine its own coordinates with respect to the center of the Earth. The receiver would be located at the intersection of three spheres; each has a radius of one receiver-satellite distance and is centered on that particular satellite. The fourth satellite is required to account for the receiver clock offset. This is also called as point positioning.

In the GPS relative positioning two GPS receivers simultaneously track the same satellites to determine their relative coordinates. It is also called as differential positioning. One receiver is selected as a reference, or base, which remains stationary at a site with precisely known coordinates. The other receiver, known as the rover or remote receiver, has its coordinates unknown. It may or may not be stationary, depending on the type of the GPS operation. A minimum of four common satellites is required for relative positioning. However, tracking more than four common satellites simultaneously would improve the precision of the GPS position solution [24].

2.2.3 Use of GPS in Asset Management [20]:

GPS can be used with the digital maps and a computer system for route guidance in vehicle navigation system. GPS system continuously determines the vehicle's location. In obstructed areas, such as tunnels etc., GPS is supplemented by a terrestrial system such as the DR system to overcome the GPS signal blockage. DR system uses the vehicle's odometer and accelerometer and/or gyros to determine the vehicle's direction and inertia or velocity and determines the traveled distance. But this system is accurate only over a short period of time. Integrating GPS and DR systems overcomes the limitations of both systems. GPS provides the initialization and the calibration to the inertial DR system and the latter bridges the GPS gaps when the satellite signal is blocked or temporarily lost.

Apart from vehicle navigation GPS is also useful in tracking of mobile assets in outdoor environment. In this case, GPS device is attached to the assets. Its use also provides following benefits:

i. Tracking of mobile assets.
ii. Reduction in loss and theft.
iii. Locating missing assets.
iv. Proper and improved utilization of assets.
v. Improved management and control.
vi. Quick and real-time checking of assets.

<u>CHAPTER-3</u>

ACCESS/ASSET MANAGEMENT SYSTEM DEVELOPED: HARDWARE

Main hardware used in this dissertation is RapidRadio RFID HF evaluation kit, RFID tags, Crossbow MTS-420CC wireless sensor node for GPS, Crossbow MTS-400 for monitoring environmental parameters, Crossbow MIB-520 USB Interface board as base station and Crossbow MPR 2400 (MICAz).

3.1 System for Access Management:

ISO/IEC 14443 is a four-part international standard for Contactless Smart Cards operating at 13.56 MHz in close proximity with a reader antenna. These ISO-14443 cards and RRHFEK reader are used for access management system. The initial communication between this proximity coupling device i.e. reader and the proximity coupling card happens in four steps as described below:

1. Activation of the smart card by the RF operating field of the reader.
2. Smart card waits silently for a command from reader.
3. Then reader transmits command addressed to smart card.
4. Smart card responds by transmitting appropriate data, in this case tag Id number.

These operations use RF power which is produced by reader and got coupled to the smart card. Smart card modulates the received power and uses it for communication with reader.

Access Management mainly involves three subsystems:

1) Access to visitors:

In this strategy, visitors have to first consult the security persons available at the entry gate. For security reasons, entry gate will normally remain closed and user needs to have smart card to open it. Each visitor will get one smart card and each visitor has to fill-up the primary details such as name, purpose of visit, contact number and address. Since each smart card has unique 8 digit alphanumeric identification number, when the visitor swaps the card to enter, automatically the Identification number and entry time gets entered into the database. Similarly it gets updated in the entry-exit table of the database, which keeps the track of number of persons present in the building. When the visitor present inside of the building swaps the card to go outside, the database automatically gets updated with the exit time of the visitor. At the same time, it also shows all the details about the visitor to the security person which he had given at the time of entry. Hence, any suspicious movement can be easily verified by the security person. The system also gives a visual indication about entry or exit of the visitor to a security person sitting at a distance.

2) Access to daily entrants such as students, staff, faculty etc.:

To speed-up the process, database of the daily entrants such as students, staff and faculty is prepared at a single time and will be updated only by the administrative authority on individual request. Permission to access the database to other users will not be granted and hence high level data security and integrity will be achieved. Hence, these users need not enter the data at the time of entry. Since, entry gate will normally remain closed and user needs to have smart card to open it, each one will carry smart card given permanently to him till his/her stay in the institute. After swapping the card for entry, the entry-exit table will be automatically updated by entering user's smart card identification number and entry time. When the user swaps smart card at the time of exit, the entry-exit table will get updated by deleting respective entry. Hence, this table keeps a track about the persons present in the institute building. By examining this table and running simple queries, which are presented in form of buttons, security persons can easily get the information about the user.

3) Daily attendance:

In this strategy, each class will have attendance table. The students will require to swap their cards to mark presenty. Once student swaps his/her card, his attendance will be marked in the presenty table with date and time of swapping. One can easily check the attendance details of a particular student by executing a query present in the form of a button. This system can be made resistant to proxies by integrating biometric identification technique along with smart card.

3.1.1 Hardware Used for Access Management:

3.1.1.1 RapidRadio RRHFEKv2.0 HF Evaluation Kit: [35, 36]

Radio Frequency Identification (RFID) has been used for more than a decade and still provides growing benefits most commonly associated with Access Control. This evaluation kit is based on RFID. RRHFEKv2.0 is a basic HF RFID kit for technology enthusiasts to play with and know RFID technology. It can be used to develop small applications for personal use. It is working on 13.56MHz High frequency and it supports ISO14443-3A and ISO-15693 protocol based transponders. It also supports custom transponder of NXP like MIFARE STANDARD 4k, and ICODE SLI.

The kit includes:

1. RFID reader.
2. USB cable.
3. Driver and sample application software.
4. User manual and reference documents.
5. ISO-14443-3A and ISO-15693 tags.

3.1.1.2 Specifications of Evaluation Kit:

Some of the important specifications of RapidRadio RRHFEKv2.0 HF evaluation kit are enlisted here.

1. Frequency of operation: 13.56MHz.
2. Power Consumption : 300mW (Maximum)
3. Interface: USB.
4. Temperature range: -10C to +70C.
5. Protocol Supported: ISO14443-3A and ISO-15693.
6. Power supply: self powered by USB.
7. Read range: 5cm.
8. Weight: 200gms (approximately.)
9. Dimensions: 4.35 x 2.74 x 1.10 inch
10. Color: off white.
11. Indicator: LED and buzzer.
12. Enclosure material: ABS plastic.

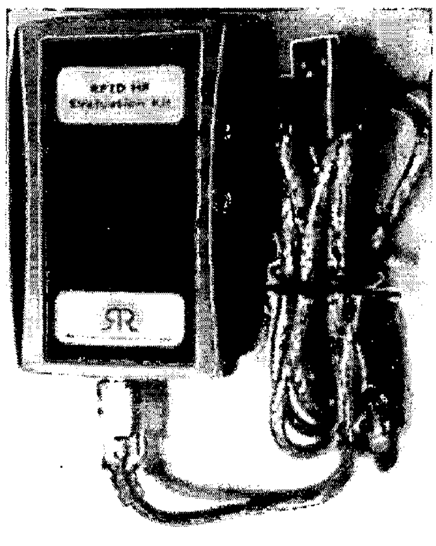


Fig. 3.1 RRHFEKv2.0 HF Evaluation Kit [35]

3.1.1.3 HF RFID Tag RRHFT01:

RRHFT01 is HF Tag working on 13.56 MHz frequency. They are available in different form factors depending on required range and various applications. These tags are also available in various memories starting from 256 bits to 2048 bits. It is also available in inlay and label form.

3.1.1.4 Features and Specifications:

1. Up to 256 Byte rewritable memory
2. ISO 15693 compliant Customized tags available for different applications
3. Application Family Identifier
4. Fast Anti-collision
5. Operating Frequency: 13.56 MHz
6. Operating Temperature: -25°C to +70°C
7. Storage Temperature: -40°C to +85°C
8. Transmission Principle: ASK / FSK
9. Data Retention: 10 Years
10. Supported Standard: ISO 15693
11. User Programmable Memory: Upto 2048 Bits
12. Programming Cycles: 100000

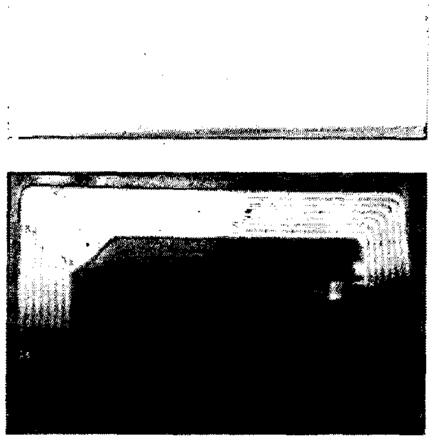


Fig. 3.2 HF RFID Tags [35]

3.2 System for Asset Management:

ISO-15693 standard cards and RRHFEK reader are used for access management system along with LabVIEW platform. In asset management, the institute assets are broadly classified in following categories:

1. Electronic products such as computers, projectors, lamp/tube, fans, A.C., watercoolers, aquaguards, printers, zerox, telephones, various panels etc.
2. Laboratory equipments: Sensors, various kinds of machines, motors, circuits, various laboratory equipments etc.
3. Furniture: Tables, chairs, sofas, cupboards, benches etc.
4. Documents: Registers, files, reports, floppies, cds, various documents.
5. Library Stuff: Books, dissertations, thesis, manuals, journals etc.
6. Institute vehicles.

The subsystems implemented in asset management are:

1) Asset identification using RIFD tags and reader:

As we discussed earlier, monitoring of location of assets and tracking of assets is important in asset management. In this dissertation, each asset of institute will have RFID tag attached to it and the tag will carry unique identification number. The identification number of tag is 16 digit alpha-numeric characters. All information about the asset has to be entered in the database prepared manually along with date of entry into database. Once information is entered, each tag detected by the RFID reader will be compared and its information will be given at front panel of LabVIEW.

Hierarchy of permissions to access the database created for asset management will maintain the data security and data integrity. Also, the location information in the database can easily give about the current presence of asset and minimizes loosing of assets.

2) Environmental parameters monitoring:

For monitoring condition of assets, mainly environmental parameters are monitored, which mainly includes temperature, pressure, humidity and light intensity. Any sudden environmental disturbances or intended deeds to damage or destroy the assets will definitely result in changed environmental conditions. These reflect in the changed temperature, humidity, pressure or light intensity at particular location. Each location, where environmental parameters are to be monitored, consist wireless sensor motes to monitor the parameters. A WSN network of such motes keeps track of environmental parameters of numerous locations and also gives alarm indication if any parameter crosses allowed limit. The upper and lower limit for temperature, humidity, pressure or light intensity can be given by user and can also be changed later by concerned authority. Database of these parameters is continuously updated and time duration to update the database is user defined.

3) Tracking of institute vehicle:

Asset management of academic institute also involves tracking of institute vehicles. The institute vehicle's position can be detected by using GPS sensor module such as MTS-420CC. It gives latitudinal and longitudinal position in terms of degrees and minutes. This information can either be periodically taken or at will. The period of tracking of vehicle is also programmable. Vehicles can be identified the RFID tags attached to it, which carries unique identification number. Prepared database gives vehicle information and position information, along with monitoring date and time, in detail.

3.2.1 Hardware Used for Asset Management:

3.2.1.1 Crossbow MPR 2400 (MICAz): [38]

The MICAz is the latest generation of Motes from Crossbow Technology. MPR2400 (2400 MHz to 2483.5 MHz band) uses Chipcon CC2420. It is compliant with IEEE 802.15.4 standard and ZigBee protocol. A ready radio frequency transceiver integrated with an Atmega128L micro-controller is used in it.

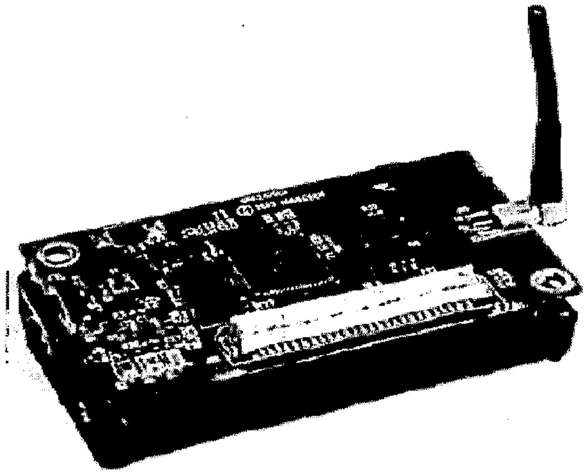


Fig. 3.3 MPR 2400 (MICAz) [38]

In this mote MICA2, 51 pin I/O connector, and serial flash memory is used. All MICA2 application software and sensor boards are also compatible with the MPR2400 (MICAz generation). Fig. shows one of the MPR-2400 Mote (MICAz).

3.2.1.2 Main Features of MICAz MPR 2400:

1. Processor chip used: ATMega 128L.
2. MCU type: 7.37MHz, 8 bit.
3. Program memory: 128kB
4. SRAM: 4kB.
5. Sensor Board Interface: 51 pin, 10-Bit ADC with 7, 0, 3V input
6. Interface type: 2UART, DIO, I^2C
7. Default power source type: AA, 2× Coin (CR2354)
8. Typical capacity: 2000 mA-hr
9. Flash Data Logger Memory: AT45DB014B chip, SPI Connection Type, 512 kB
10. RF transceiver: CC2420 chip, 2400 MHz frequency, 250 kbps (maximum data rate), MMCX antenna connector
11. External power supply: 2.7V to 3.6V

3.2.1.3 MIB 520 USB Interface Board: [31, 38]

The MIB520 provides USB connectivity to the IRIS and MICA family of Motes for communication and in-system programming. It supplies power to the devices through USB bus. MIB520CB has a male connector while MIB520CA has female connector. MIB 520CB is used in this dissertation. It will be connected to MICAz MPR-2400 through 51-pin connector. Some of the specifications of MIB-520 USB interface board are as follows:

1. Baud rate: 57.6 kbps.
2. Connector: 51-pin.
3. Power: USB powered.
4. JTAG interface connector: 10-pin male.
5. Indicators: Red LED (ISP programming indicator), Green LED (power indicator), Yellow LED.

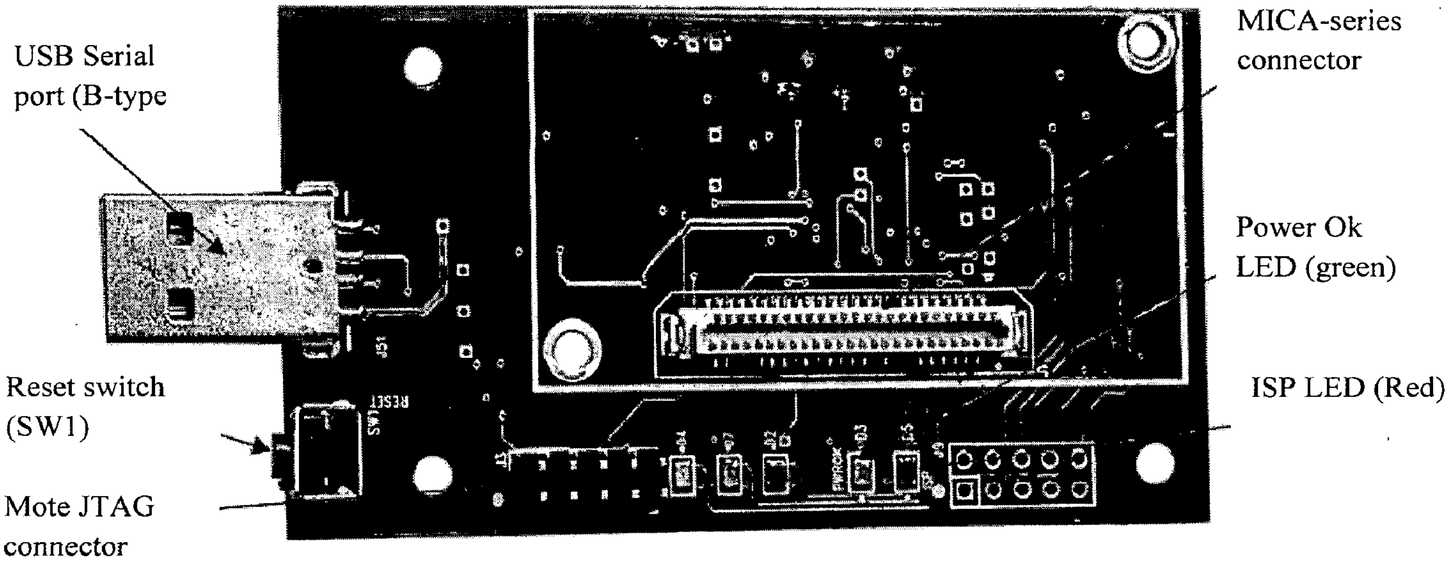


Fig. 3.4 MIB 520CB (MICAz) [38]

The MIB520 has an on-board in-system processor (ISP)—an Atmega16L to program the Motes. First, Code is downloaded to the ISP through the USB port. Next the ISP programs the code into the Mote. For programming the Motes, it requires MoteWorks installed in the host PC. The IRIS, MICAz and MICA2 Motes connect to the MIB520 for ISP programming from host PC through USB. The "RESET" push button switch resets both the ISP and Mote processors. It also resets the monitoring software which runs on the host PC. The MIB520 has a connector, J3 which connects to an Atmel JTAG pod for in-circuit debugging. This connector will supply power to the JTAG pod; no external power supply is required for the pod and MIB520 is powered by the USB bus of the host. The MIB520 offers two separate ports: one dedicated to in-system Mote programming and a second for data communication over USB.

3.2.1.4 Sensor Board MTS-400CA: [33, 37]

The MTS400CA offers five basic environmental sensors. The Sensirion SHT11 is a single-chip humidity and temperature multi-sensor module comprising a calibrated digital output. The chip has an internal 14-bit analog-to-digital converter and a serial interface. SHT11s are individually calibrated. This sensor's power is enabled through a programmable switch. The control interface signals are also enabled through a programmable switch. An analog-to-digital converter in the sensor does the conversion from humidity and temperature to digital units. Its accuracy is ±3.5%RH and operating range is 3.6 to 2.4V. The interface used is digital interface and analog-to-digital converter in the sensor does the conversion from humidity and temperature to digital units.

The Intersema MS55ER sensing unit is a SMD-hybrid device including a piezoresistive pressure sensor and an ADC interface IC. It provides a 16-bit data word from pressure and temperature measurements. A 3-wire interface is used for all communications. The measuring pressure range is 300 to 110 mbar while its temperature range is -10°C to +60°C. Its measurement accuracy in case of pressure is ±3.5% and temperature is ±2°C. Its operating voltage range is 2.2 to 3.6V. This sensor's power is enabled through a programmable switch. The control interface signals are also enabled through a programmable switch. Digital interface is provided along with an analog-to-digital converter in the sensor, which does the conversion from pressure and temperature to digital units.

The TLS2550 is a digital light sensor with a two-wire, SMBus serial interface. It is manufactured by TAOS. It combines two photodiodes and a companding analog-to-digital converter on a single CMOS integrated circuit to provide light measurements over an effective 12-bit dynamic range.

It can detect light rays in the range of 400-1000nm. Its operating voltage range is slightly different than MS55ER. Voltage range for TLS2550 is 2.7 to 3.6V. This sensor's power is enabled through a programmable switch. The control interface signals are also enabled through a programmable switch. Digital interface is provided along with an analog-to-digital converter in the sensor, which does the conversion from pressure and temperature to digital units.

It also encloses accelerometer, which is basically a MEMS surface micro-machined 2-axis, ± 2 g device. It draws very low current (< 1mA). The sensor can be used for tilt detection, movement, vibration, and/or seismic measurement.

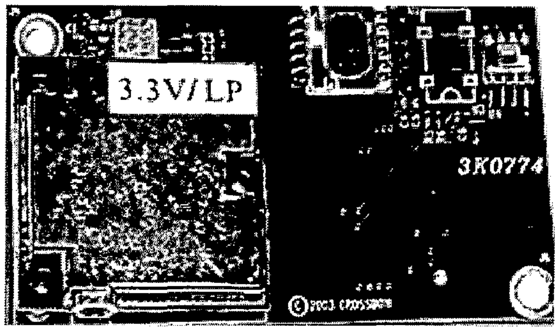


Fig. 3.5 MTS 400/420CC (MICAz) [37]

3.2.1.5 Sensor Board MTS-420CC: [37]

The GPS module is powered via a DC-DC booster, which maintains a constant 3.3 volt input regardless of battery voltage. The booster output is programmable. The output from the GPS module is connected to a serial UART and USART1 interface of the Mote. An active, external, antenna is supplied with the module. The GPS module supplies the antenna power. The GPS chipset used is SiRF starlle LP with 12 channels.

The start time is 45 seconds in cold, 38 seconds in worm and 8 seconds in hot environment. Reacquisition time is typically 0.1seconds in normal weather conditions and varies in dense fog. Protocol used for communication is NEMA-0183 and SIRF binary protocol. Its input current is 60 mA at 3.3V and interface used is serial interface.

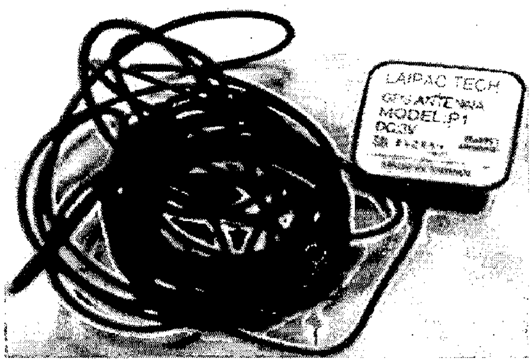


Fig. 3.6 MTS 420CC GPS Antenna (MICAz) [37]

CHAPTER-4
ACCESS/ASSET MANAGEMENT SYSTEM DEVELOPED: SOFTWARE

This dissertation work is mainly based on four software platforms, which are LabVIEW, C#, MoteWorks, MS Access. Details about the software prepared for access management and asset management will be followed by a brief introduction to these software platforms. Their use in access and asset management is also described here.

4.1 Software Subsystem for Access Management:

The main concern in access management is to keep a track of people entered into the institute building. Hence, after a person enters, the Software subsystem updates the concerned table in database by entering unique Id of the smart card given to that person. Once the person exits, software system deletes the entry, so that, counting the number of persons present in the building becomes easier. If the person is a visitor then the software permanently keeps its data in the database and it can be further referred. The entry and exit action is automatically detected by the sequence detector circuit and a signal is send to software system so as to execute specified program to mark entry or exit of the person. Since date and time are also entered with Id, exact referencing becomes much easier. Suitable indications and alarms are provided for security purpose.

It also includes attendance monitoring subsystem for students, which keeps record of time, date and present students. The whole database is created in Microsoft Access and is connected to LabVIEW by using Microsoft Jet 4.0 OLE DB Provider. C# is used for attractive and convenient user interface with RFID reader. The program also outputs the number of RFID tags read at a single time.

Once entry or exit is detected by sequence detector circuit, the LabVIEW program calls driver program for RFID reader software. RFID reader software reads the tag Id and stores it in a text file and returns back to calling LabVIEW program. Main LabVIEW program then extracts the Id from the text file and updates the respective database entities. It also monitors about any query request and if any present, it executes the query. This process repeats so as to continuously monitor and manage the access to building.

4.1.1 Software Flow Chart for Entry-Exit Monitoring Subsystem:

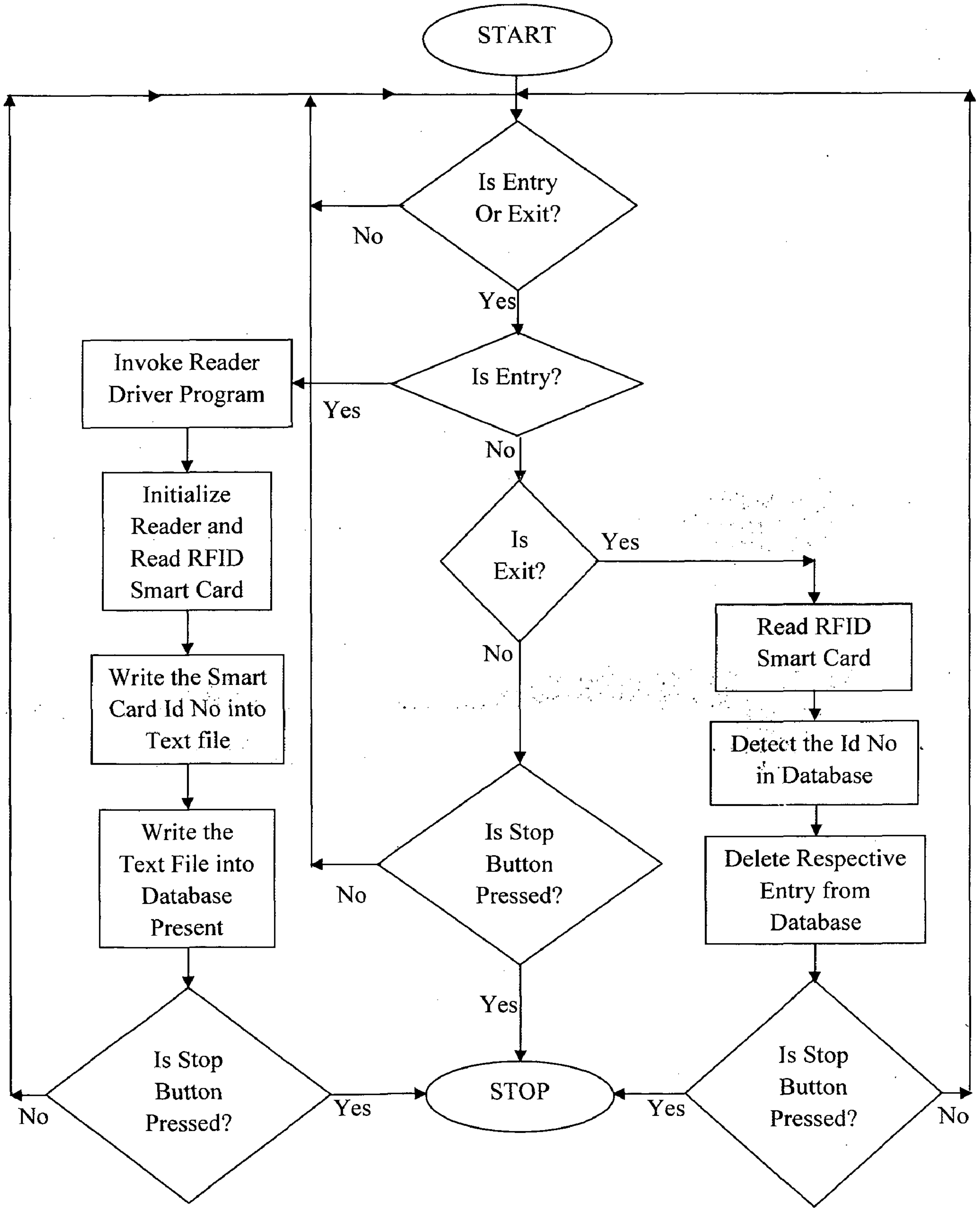


Fig.4.1 Flow-chart for Access Monitoring Subsystem

4.1.2 E-R Diagram for Access Management System:

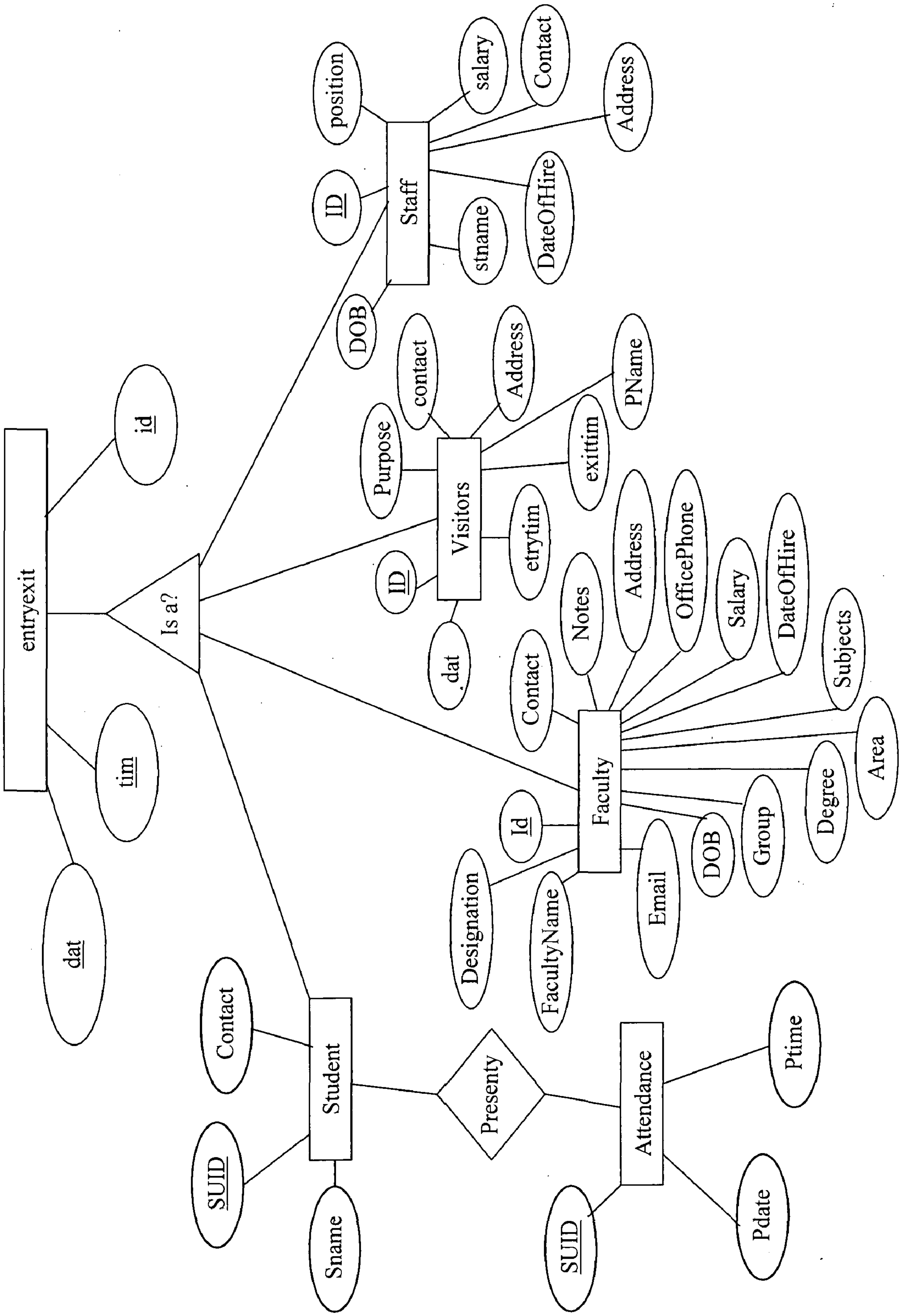


Fig. 4.2 E-R Diagram for Access Management Subsystem

4.2 Software System for Asset Management:

A robust Asset Management solution is a critical component of any system that seeks to provide automated access to content or services. A core issue in the design of such systems is the capability to model complex assets and their dependencies in an environment where such assets are continually being defined, accessed, modified, tracked, and reused. For identifying assets, RFID tags complying ISO standards 14443 and 15693 are attached to them. The identification number of tag is 16 digit alpha-numeric characters. All information about the asset has to be entered into the database prepared manually along with date of entry. Once information is entered, each tag detected by the RFID reader will be compared and its information will be given at front panel of LabVIEW. Schema expansion is expensive when a table is populated, and in some databases not possible at all [27]. If the object schema as created by the user maps directly to the storage schema, then there is a direct dependence on the database schema expansion mechanism. However, the meta data model used here allows the asset manager to extend objects through the addition of custom properties. The most basic object in this framework is the Attribute, which maps to generic database types such as Text, Boolean, or Date.

Monitoring condition of assets is an important aspect of asset management. Environmental parameters, such as temperature, pressure, humidity and light intensity, play a crucial role in monitoring the physical condition of assets. Any sudden environmental disturbances or intended deeds to damage or destroy the assets definitely results in changed environmental conditions. These reflect in the changed temperature, humidity, pressure or light intensity at particular location. Each location, where environmental parameters are to be monitored, consist wireless sensor motes to monitor these parameters. A WSN network of such motes keeps track of environmental parameters of numerous locations and also gives alarm indication if any parameter crosses allowed limit. The upper and lower limit for temperature, humidity, pressure or light intensity can be given by user and can also be changed later by concerned authority. WSN is a special kind of ad-hoc network composed of hundreds of low-powered wireless sensor motes. Ad-hoc networking incorporates plug and play strategy which gives flexibility to develop structured software. Continuous loops and user-interactive development makes the system less prone to bugs, still initial knowledge about the user interface is required to user. Since it is structured software, the whole software can be partitioned and distributed on multiple systems to achieve more reliability and effective management. Distributed database and dedicated systems are also possible according to user requirements

4.2.1 Software Flow Chart for Environmental Parameters Monitoring Subsystem:

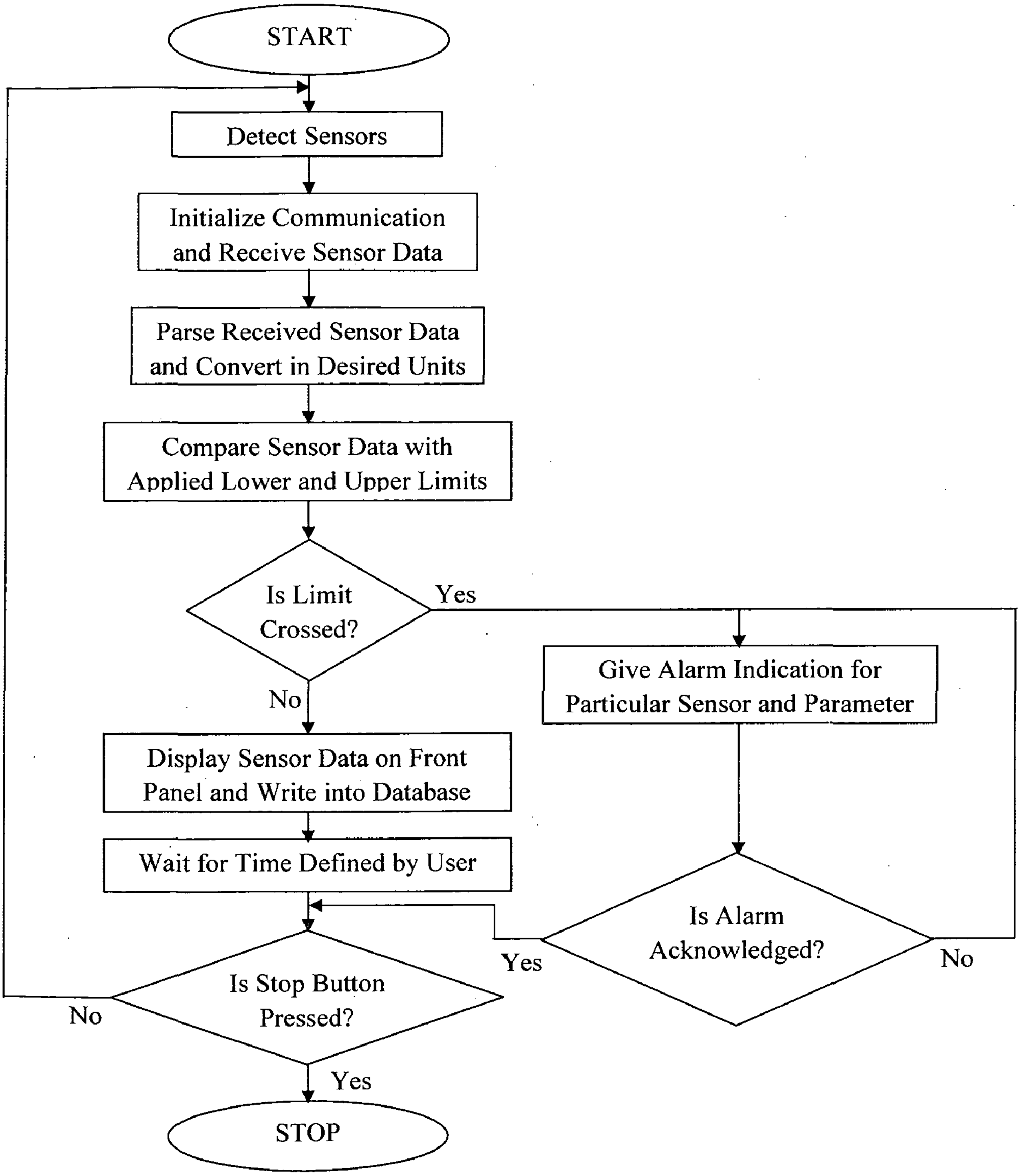
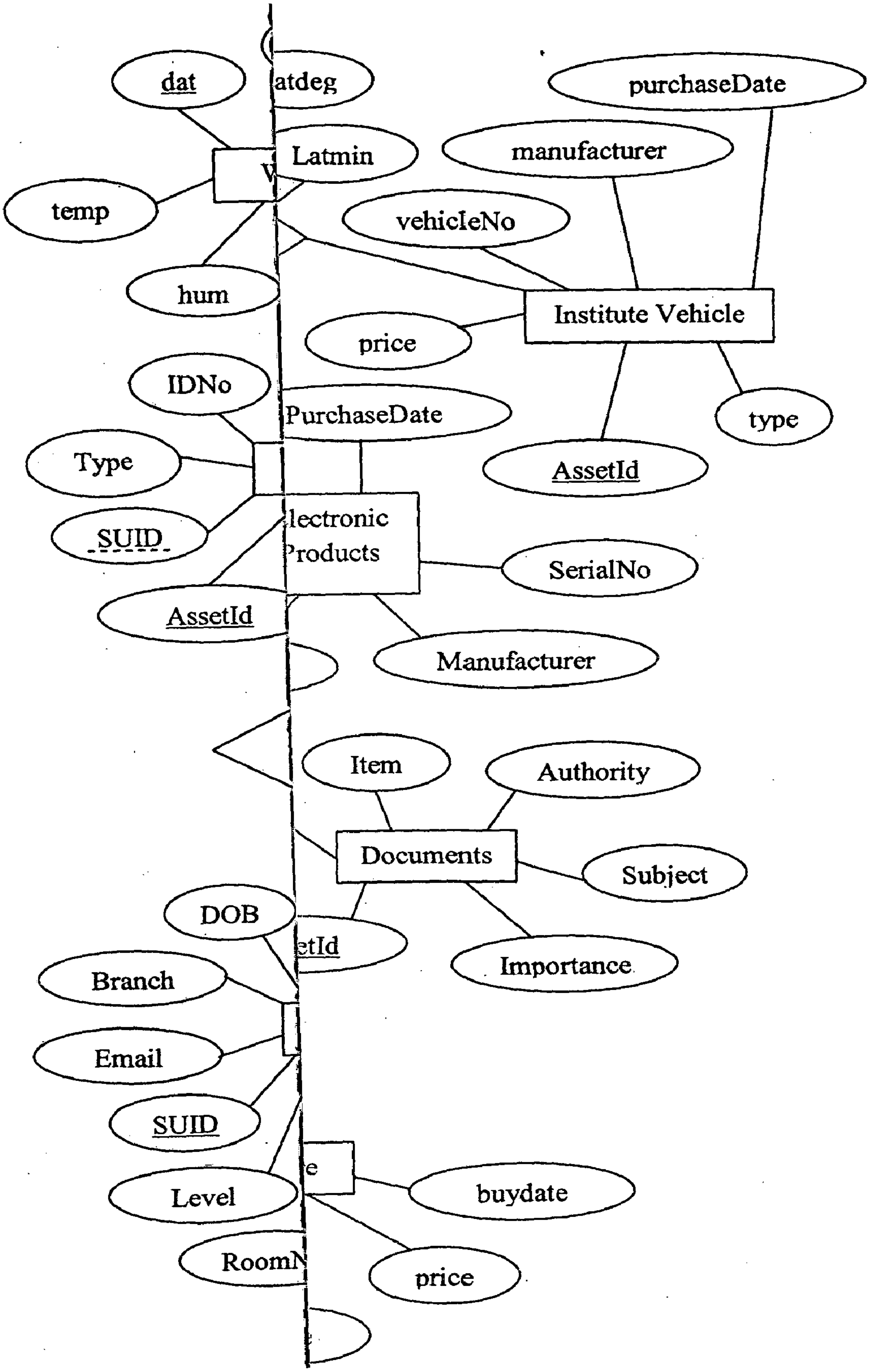


Fig.4.3 Software Flow Chart for Environmental Parameters Monitoring Subsystem

4.2.2 E-R Diagram fo



4.3 Software Used in Subsystems:

In this dissertation, LabVIEW, C#, MoteWorks, MS Access are four main used software platforms. A brief discussion about these softwares and their relevant use are described in following section.

4.3.1 LabVIEW: [28, 29]

Laboratory Virtual Instrument Engineering Workbench (LabVIEW) is a graphical programming language developed by National Instruments [28]. LabVIEW uses dataflow programming where the flow of data through nodes on the block diagram determines the execution order of the Vis and functions. It uses icons instead of lines. LabVIEW programs are called as virtual instruments, or VIs, because their appearance and operation resembles physical instruments, such as oscilloscopes and multi-meters. It contains a comprehensive set of VIs and functions for acquiring, analyzing, displaying, and storing the data. It also contains tools to provide help in troubleshooting errors in the code.

LabVIEW VIs contain three main components—the front panel, the block diagram, and the icon/connector pane. The front panel is the user interface for the VI. Front panel contains controls and indicators, which are the interactive input and output terminals of the VI, respectively. The block diagram contains graphical source code. A VI can be used as a subVI. A subVI is a VI that is used inside of another VI, similar to a function in a text-based programming language. To use a VI as a subVI, it must have an icon and a connector pane. Every VI displays an icon, shown at left, in the upper right corner of the front panel and block diagram windows. An icon is a graphical representation of a VI. The icon can contain both text and images. Different LabVIEW palettes are shown in following fig.

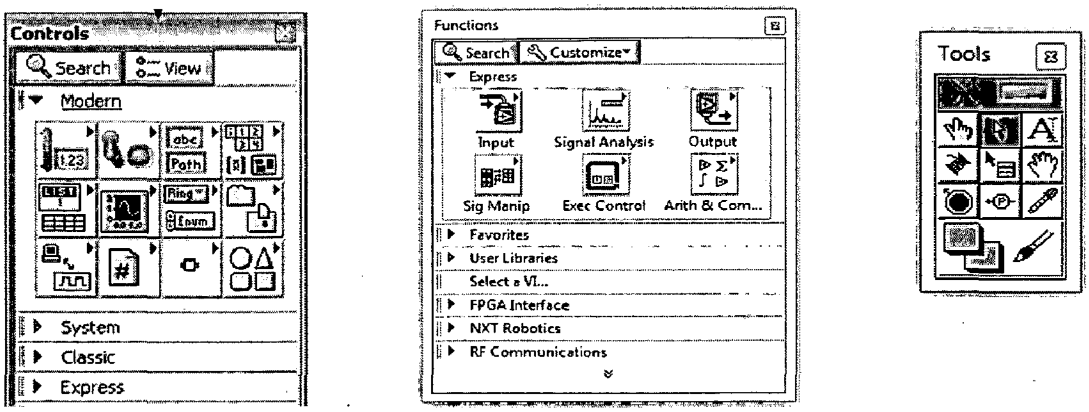


Fig. 4.5 Controls Palette, Functions Palette, Tools Palette. [28]

4.2.2 E-R Diagram for Asset Management:

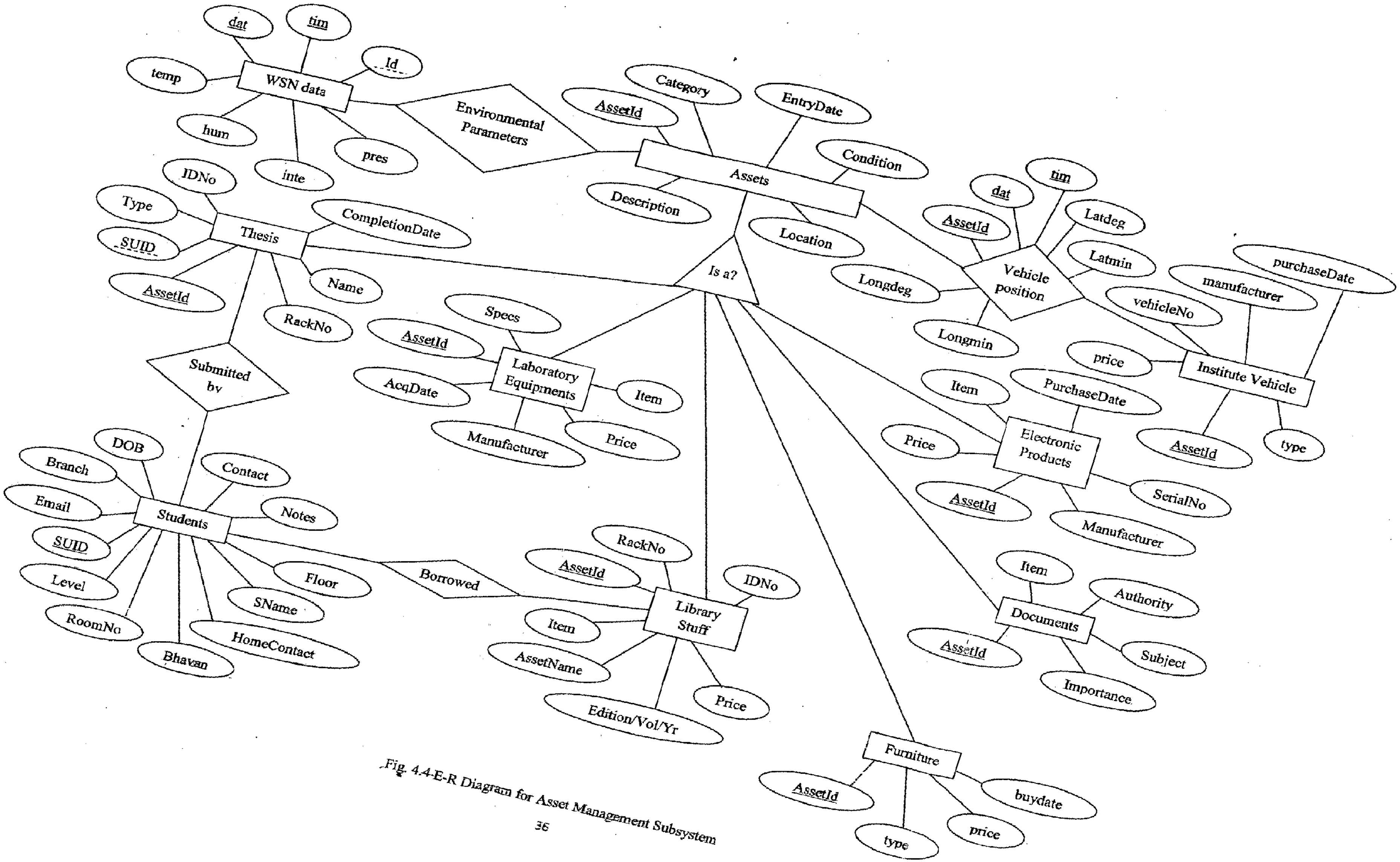


Fig. 4.4 E-R Diagram for Asset Management Subsystem

Often, there is a need to program multiple tasks so that they execute at the same time. In LabVIEW tasks can run in parallel if they do not have a data dependency between them, and if they are not using the same shared resource. An example of a shared resource is a file, or an instrument.

A general VI design pattern has three main phases. Each phase may contain code that follows another type of design pattern. The three main phases include the following:

1. Startup: This phase initializes hardware, reads configuration information from files, or prompts the user for data file locations.
2. Main Application: This phase consists of at least one loop that repeats until the user decides to exit the program or the program terminates for other reasons such as I/O completion.
3. Shutdown: This phase closes files, writes configuration information to disk, or resets I/O to the default state.

LabVIEW also supports common design techniques such as Single Loop Architectures, Parallelism, Multiple Loop Architectures, Timing a Design Pattern which are used in this dissertation.

4.3.2 Microsoft Office Access 2007: [30, 31]

Access tables support a variety of standard field types, indices, and referential integrity. Access also includes a query interface, forms to display and enter data, and reports for printing. Repetitive tasks can be automated through macros with point-and-click options. Microsoft Access is popular among non-programmers and professional developers alike. Non-programmers can create visually pleasing and relatively advanced solutions with very little or no code. It is also easy to place a database on a network and have multiple users share and update data without overwriting each other's work. Microsoft offers a wide range of template databases within the program and for download from their website. These options are available upon starting Access and allow users to enhance a database with pre-defined tables, queries, forms, reports, and macros. Popular templates include tracking contacts, assets, issues, events, projects, and tasks. Templates do not include VBA code. Microsoft Access also offers the ability for programmers to create solutions using the programming language Visual Basic for Applications (VBA), which is similar to Visual Basic 6.0 (VB6) and used throughout the Microsoft Office programs such as Excel, Word, Outlook and PowerPoint. Most VB6 code including the use of Windows API calls, can be used in VBA. Power users and developers can extend basic end-user solutions to a professional solution with advanced automation, data validation, error trapping, and multi-user support.

Recent versions of Access make it easier to track, report, and share data with others. It also provides newly added web databases at newly added Access Services in Microsoft SharePoint and allows sharing them across any organization. It also provides enhanced protection to help meet data compliance, backup, and audit requirements, providing increased agility and manageability. One of the benefits of Access from a programmer's perspective is its relative compatibility with SQL (structured query language) — queries can be viewed graphically or edited as SQL statements, and SQL statements can be used directly in Macros and VBA Modules to manipulate Access tables. Users can mix and use both VBA and "Macros" for programming forms and logic and offers object-oriented possibilities. VBA can also be included in queries.

4.3.3 MoteWorks: [33]

MoteWorks is the end-to-end enabling platform for the creation of wireless sensor networks. The optimized processor/radio hardware, industry-leading mesh networking software, gateway server middleware and client monitoring and management tools support the creation of reliable, easy-to-use wireless OEM solutions.

A wireless network deployment is composed of the three distinct software tiers:

1. Mote Tier: It is the Tier where XMesh resides. It is the software that runs on the cloud of sensor nodes forming a mesh network. The XMesh software provides the networking algorithms required to form a reliable communication backbone that connects all the nodes within the mesh cloud to the server.

2. Server Tier: It handles translation and buffering of data coming from the wireless network and provides the bridge between the wireless Motes and the internet clients. XServe and XOtap are server tier applications that can run on a PC or Stargate.

3. Client Tier: It provides the user visualization software and graphical interface for managing the network. Crossbow provides free client software called MoteView, but XMesh can be interfaced to custom client software as well.

The MoteWorks InstallShield Wizard setup offers the following software packages:

Software Package	**Necessity**
TinyOS and MoteWorks Tools	An Event driven OS for Wireless sensor networks; tools for debugging
nesC compiler	An extension of C language for TinyOS
Cygwin	A Linux-like environment of windows
AVR Tools	A suite of software development tools for Atmel's AVR processors
Programmer's Notepad	Provides IDE for code compilation and debugging
XSniffer	Provides Network Monitoring tool for RF environment
MoteConfig	Provides GUI environment for Mote programming and OTAP
Graphviz	Enables to View Files made from make docs
PuTTY and Tortoise CVS	Provides Source access through CVS server for Enterprise Users

Table 4.1 MoteWorks InstallShield Software Packages and Their Necessity

4.3.3.1 Mote Programming Description:

For programming Mote first it needs to compile the code. Code can be compiled from Programmer's Notepad, Tools > make micaz . The "Output" section of the Programmers Notepad will print the compiling results to the screen.

After the compilation has completed, "writing TOS image" is displayed as the last line in the Output window. An error typing in nesC code files don't display this message. The files provided in the /lesson_1 folder can be used to verify user programmed files and detect error. Successful compilation is much needed before proceeding for programming activity. The "Output" section of the Programmers Notepad will print the installation results to the screen. "Uploading: flash" line without errors indicates successful writing process is in progress. Red

LED on the Mote blinking on and off every second indicates that Mote is successfully programmed according to the uploaded program.

4.3.4 C# (Sharp): [34]

It is the first component oriented language in the C/C++ family language developed by Microsoft to compete with Java. C++, Java are like blackbox do not interoperate with objects. Also performance cost in case of C++ is much higher than C#. Simplicity throughout the system is also improved in case of C#. Improved extensibility and reusability provide additional benefit to the user. Newly included primitive types such as decimal, SQL offers an edge over other languages. Its focus on no memory leaks and stray pointers reduces extra efforts of detecting it. Exceptions handling is drastically improved and error handling does not remain an afterthought. Type safety is improved because it does not allow any uninitialized variables and unsafe casts. It preserves C++ heritage as namespaces, enums, unsigned types, pointers (in unsafe code). C# implementation also provides interoperations with XML, SOAP, MS, COM, DLLs, and any .NET language. It supports very huge lines of C# codes which in terms increases productivity and reduces the learning time.

<u>CHAPTER-5</u>

ACCESS/ASSET MANAGEMENT SYSTEM DEVELOPED: IMPLEMENTSTION AND RESULTS

This chapter discusses the implementation of the subsystems and results acquired. The whole access and asset management system is divided into subsystems such as Access Monitoring Subsystem, Environmental Parameters Monitoring Subsystem, GPS Vehicle Tracking Subsystem, Asset Management Subsystem and Attendance Monitoring Subsystem.

5.1 Access Management Subsystem:

The entry and exit is identified by the Ir-LED sensor-receiver pairs attached at entry-exit doors. One transceiver pair of Ir-LED is fixed at each of the entry-exit gate. These pairs detect whether the guest is entering into building or leaving from the building and produce a hardware trigger to the access monitoring subsystem. The guest's entry or exit detection is described in the following fig.

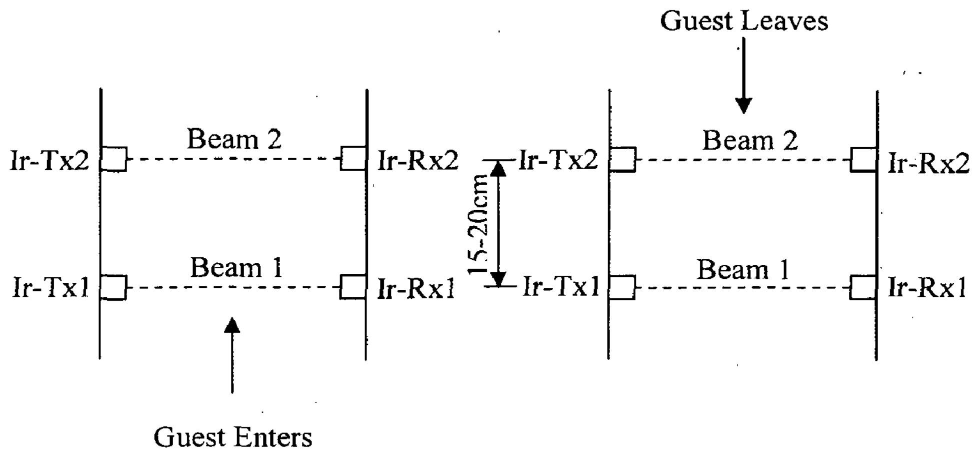


Fig. 5.1 Guest Entry-Exit Detection

The system consists of 2 Ir-transceiver pairs at each gate. They are fixed at a distance of 15-20 cm so that both beams are not obstructed at the same time. When guest comes into the building from outside, Beam 1 is obstructed followed by Beam2. When guest leaves from the building, Beam 2 is cut followed by Beam 1. This action is detected by the following circuit. It produces output 1 when beam is interrupted.

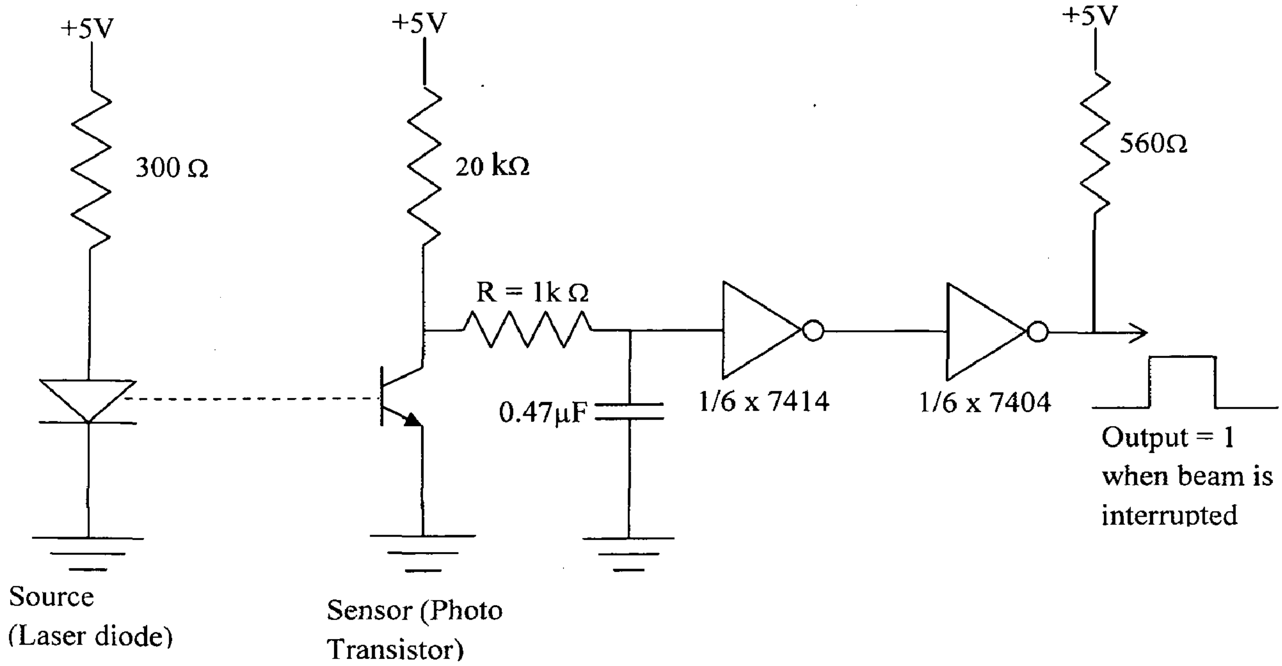


Fig. 5.2 Circuit Diagram for Each Sensor Unit

The output of the above circuit is given to a sequence detector circuit. Its circuit diagram and timing diagrams are shown below.

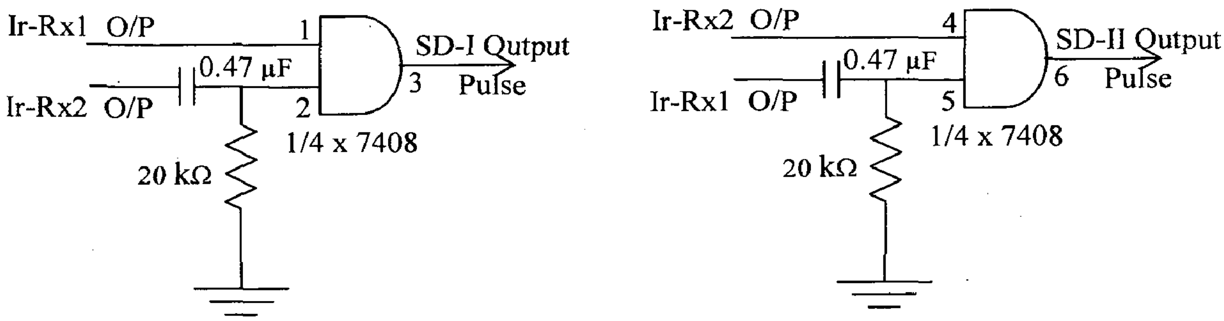


Fig. 5.3 Circuit Diagram of Sequence Detector

The above circuit produces SD-I and SD-II output pulses because of the AND gate. The combination of these pulses can be used to determine entry or exit action. If SD-I output pulse is present while and SD-II output is zero then we can consider that guest is entering in the building. If SD-II output pulse is present and SD-I output pulse is absent then we can consider that guest is leaving the building.

The timing diagram of the circuit shown in fig. 5.3 is shown below in Fig. 5.4.

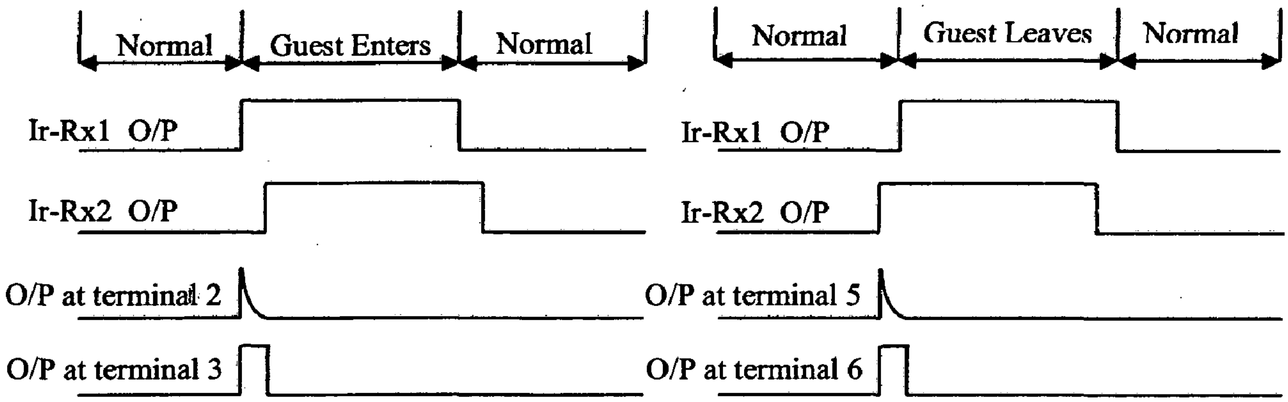


Fig. 5.4 Timing Diagram of Sequence Detector Circuit

As can be viewed from above timing diagram, when guest enters, output at terminal 3 is high, which in terms is output of Sequence Detector Circuit –I. Similarly, when guest exits, output at terminal 6 is high, which in terms is output of Sequence Detector Circuit-II. Hence, we can determine whether guest is entering or leaving by examining output of Sequence Detector Circuit-I and Sequence Detector Circuit-II.

5.1.1 Access Monitoring Subsystem:

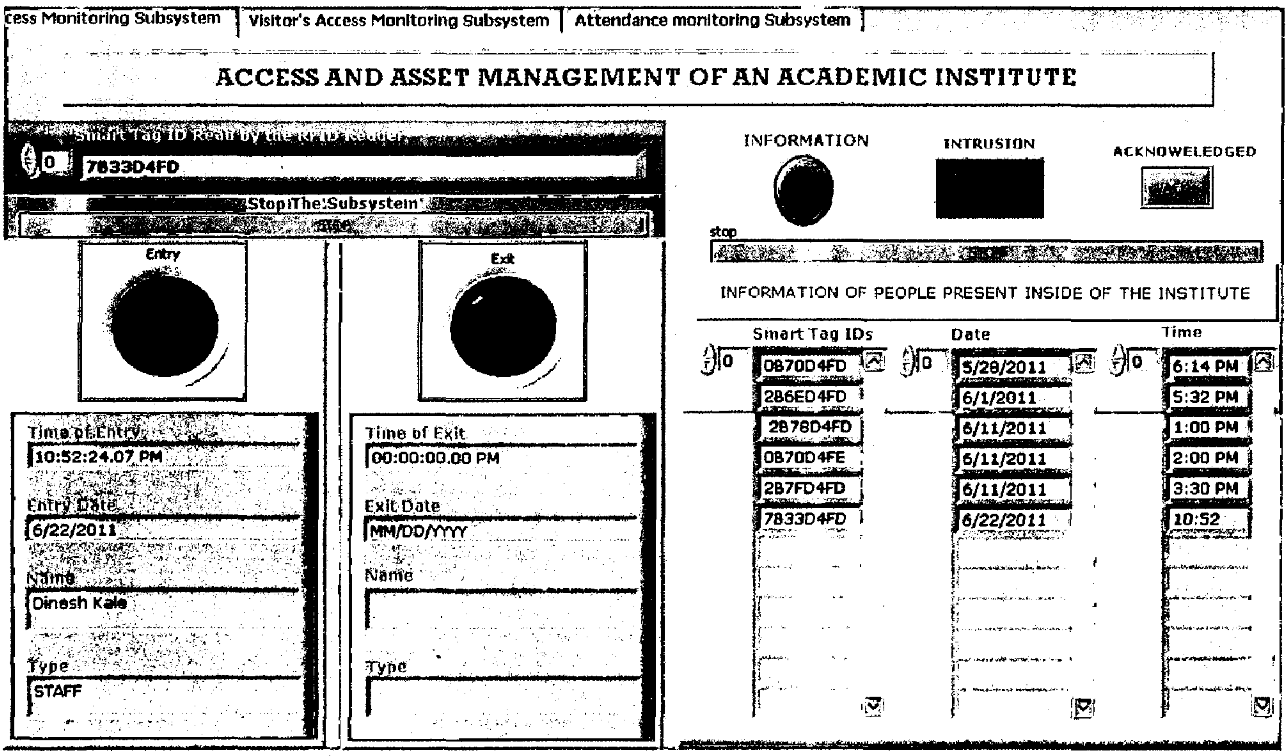


Fig. 5.5 Front Panel of Access Monitoring Subsystem

As can be seen from the fig. 5.5, when the guest enters, its details such as time of entry, date, Name and type (role in institute) are displayed on the Front-panel. These details are popped-up by the system by matching his/her Id with the existing one in the system. Similarly, when the guest exits, same details such as time of exit, date, name and type are displayed. With these details, security person can quickly confirm that guest is a known person and no intrusion has occurred. If the system doesn't identify the guest, then it signals a visual alarm to indicate intrusion has occurred. The indication will continue to glow till it is identified and acknowledged by any security personnel. The Management person can also check the details such as Ids of the person present inside, their entry time and date, which in term gives the details about no. of people present inside.

When a person enters into institute building, above Access Monitoring System inserts tuples (date, time and id) into database which is shown in the following fig. 5.6

entryexit

dat	tim	id	Add New Field
5/28/2011	6:14 PM	0B70D4FD	
6/1/2011	5:32 PM	2B6ED4FD	
6/11/2011	1:00 PM	2B78D4FD	
6/11/2011	2:00 PM	0B70D4FE	
6/11/2011	3:30 PM	2B7FD4FD	
6/22/2011	10:52 PM	7B33D4FD	
*			

Fig. 5.6 Database for Access Monitoring Subsystem

The "dat" field indicates date while "tim" indicates time of entry ("id" being smart card Id). For exiting, the smart card has to again read to access the exit gates. If the smart card Id is found in the database, the relevant designation of the person is indicated and corresponding entry is deleted. In this case, Id "7B33D4FD" is assigned to "Dinesh Kale". who is a staff and same is entered into data base when the smart card is swaped.

5.1.2 Visitor's Access Monitoring Subsystem:

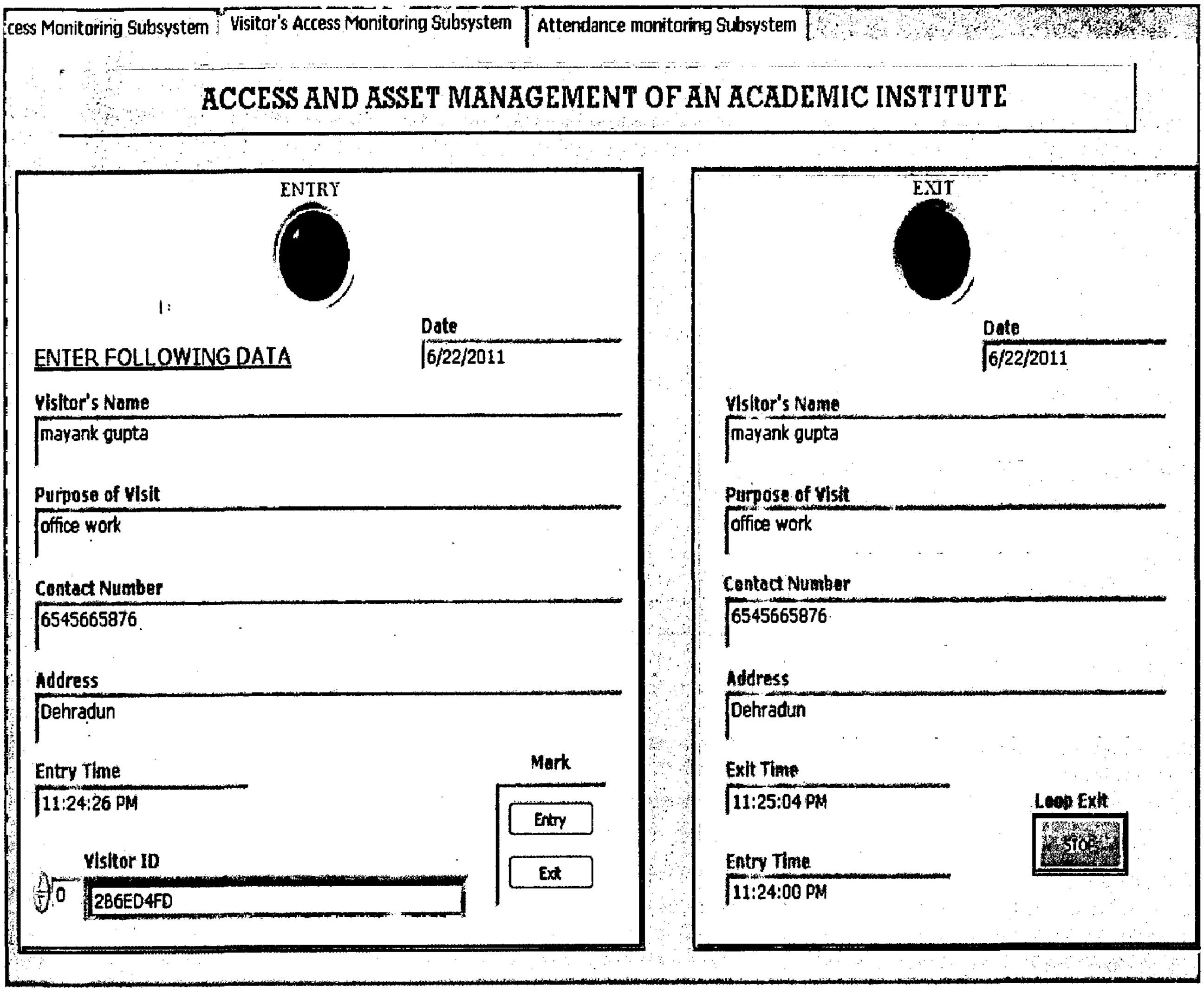


Fig. 5.7 Front Panel of Visitor's Access Monitoring Subsystem

As shown in the fig. 5.7, Visitor has to submit details before entering in the institute. Security persons have to first verify the details and then enter into the database by filling the red form. This will keep a record of people entered into building along with entry date and time. The system is made less prone to intrusions, by introducing the blue form. The system checks the smart card of the visitor and popup the details such as purpose of visit, name, contact no, address and entry and exit time of visitor. These can be quickly verified incase of doubt. Clear indications are also provided to mark entry and exit. Since visitors details cannot be made available to the database system earlier, facility provided to manually enter essential details marks the important role of security.

This subsystem when executed enters visitor's details into the database. An example of visitor "mayank gupta" is given above and the resulting change in database is shown in fig. 5.8. With the above details one can quickly verify this entry into database.

Visitors

ID	dat	entrytim	exittim	PName	purpose	contact	Address
2B6ED4FD	5/31/2011	2:30:00 PM	11:25:00 PM	mayank gupta	office work	6545665876	Dehradun
2B6ED4FD	6/22/2011	11:24:00 PM	11:25:00 PM	mayank gupta	office work	6545665876	Dehradun
AB80D4FD	6/2/2011	5:14:00 PM	7:40:00 PM	abhi	meeting	9045620757	roorkee
AB80D4FD	6/2/2011	7:32:00 PM	7:40:00 PM	abhi	meeting	1234567890	jawahar bhavan
AB80D4FD	6/2/2011	7:37:00 PM	7:40:00 PM	abhi	meeting	1234567890	jawahar bhavan
AB80D4FD	6/2/2011	7:40:00 PM	7:40:00 PM	suhas	timepass	321897456	EG-15 Jawahar bhavan
*							

Fig. 5.8 Database for Visitor's Access Monitoring Subsystem

When the visitor exits, again these details are displayed on the screen as shown in fig. 5.7. The details entered in "Visitors" database are preserved and not deleted for further reference.

5.1.3 Attendance Monitoring Subsystem:

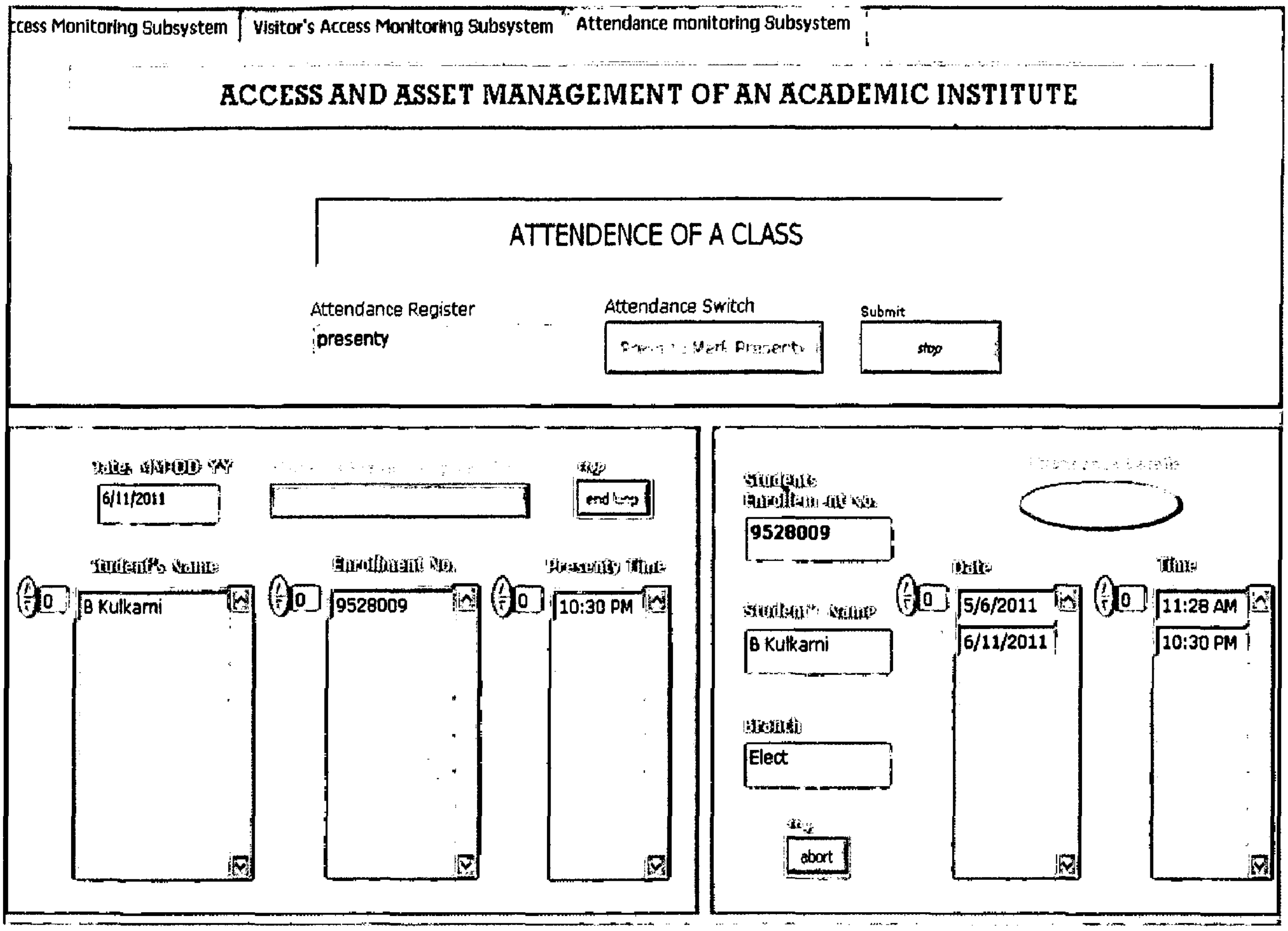


Fig. 5.9 Front Panel of Attendance Monitoring Subsystem

This system marks the attendance in the specified database as shown in fig. 5.9. Concerned faculty has to mention the database name according to the class. The faculty can check students present at any date and also can inspect name of the students, their enrollment no.s and presenty time. By using students enrollment no, it is also possible to check attendance details of a particular student. This system minimizes the efforts of faculty and helps in better utilization of resources. Hence, better access management and use of resources is possible.

The "attendance of a class" section shown in the above GUI is for marking presenty of students while entering into class. The details about students present at a particular date can be examined by the switch "students present at a given date" given on GUI (in this example students present at date 6/11/2011). Attendance details of a particular student (in this example student having enrollment no 9528009) are displayed by using button provided for the same. Enrollment no is required for these details.

5.2 Asset Management Subsystem:

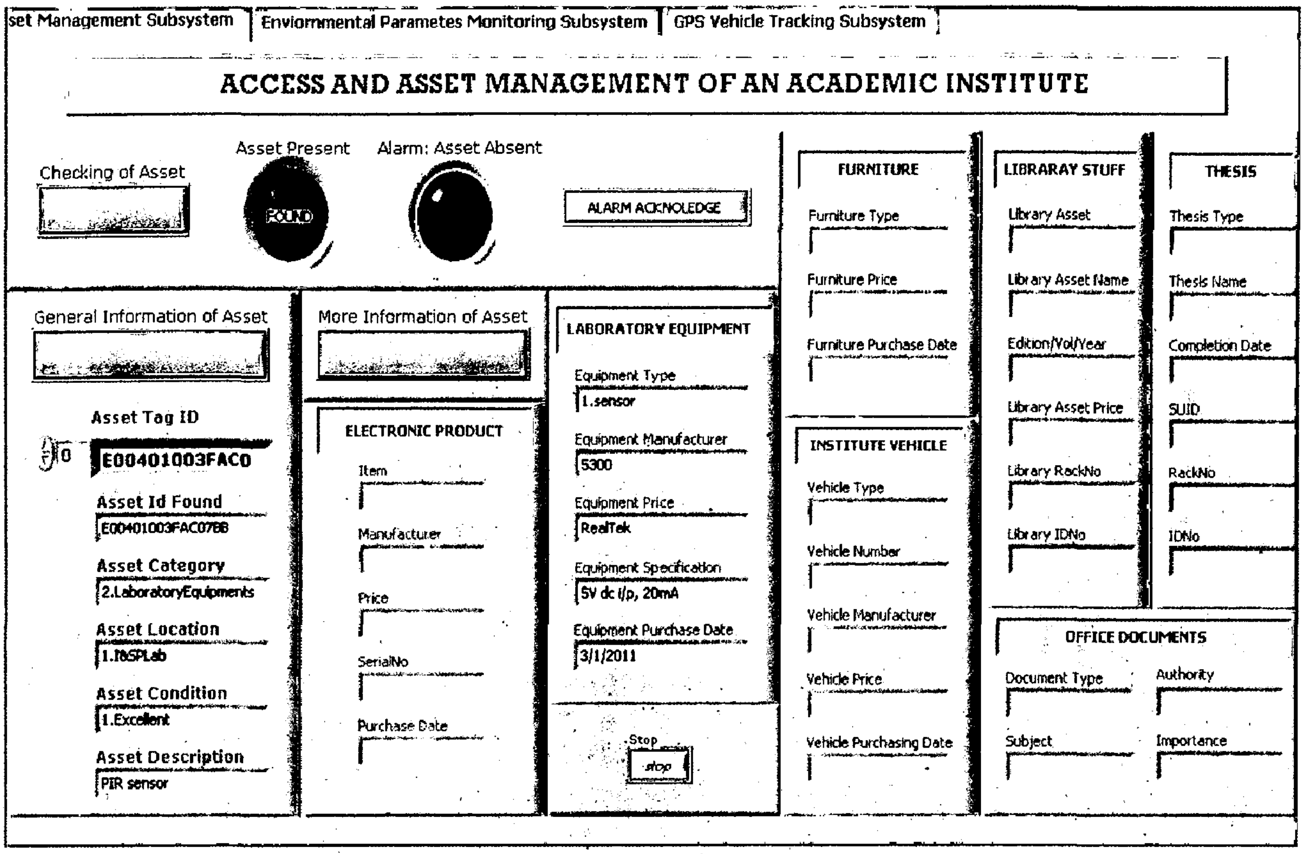


Fig. 5.10 Front Panel of Asset Management Subsystem

For better Asset management and proper utilization of resources, we require monitoring of asset location and monitoring of asset condition. In most of the cases, physical condition of assets can be predicted by their purchase date and date at which they became functional. Environmental parameters also affect the physical condition of the assets which is described further.

By using the "Check" button as shown in fig. 5.10, we can detect the tag-ids of the assets of the institute. Since each asset carries an irremovable RFID tag, detecting the tag marks the presence of the asset. If the tag is not detected, then it signals a visual alarm. It will continue its signaling till it is acknowledged. More information about the asset detected can be available by using "General Information of Assets" and "More Information of Assets" tabs. The management system checks its records about the asset and displays it accordingly.

Checking of more attributes is an option; hence only detecting the presence of asset is possible and also fast. This system also isolates the user from editing the actual database and maintains its integrity and security. Hence, database can only be modified by respective authority.

In the example shown in Fig. 5.10, Asset having tag-Id "E00401003FAC4F3B" is detected first by using "Checking of Asset" button. The "General Information of Asset" button gives common information while "More Information of Asset" gives specific information along with its type. Asset in this example is a sensor and its details are indicated in the LABORATORY EQUIPMENT section.

5.2.1 Environmental Parameters Monitoring Subsystem:

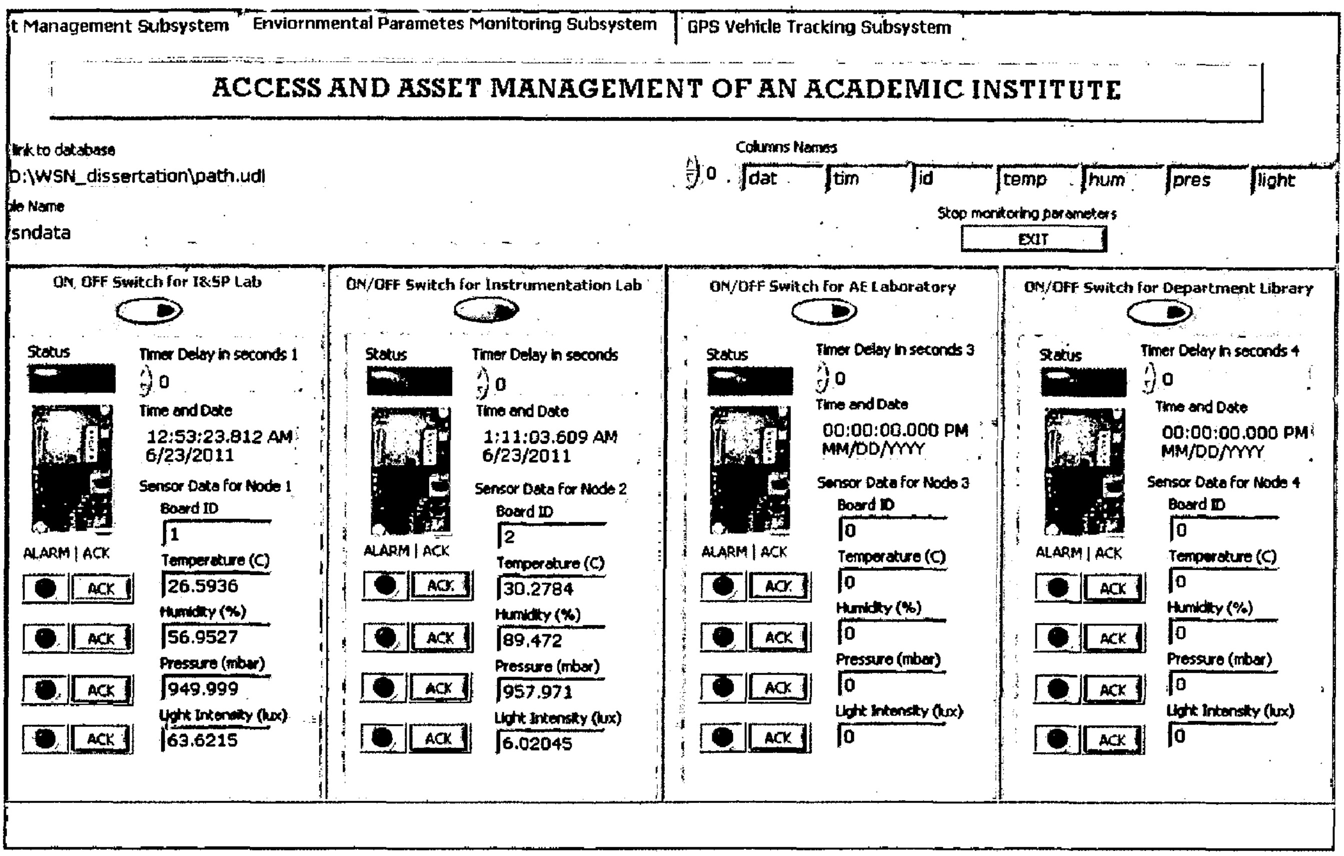


Fig. 5.11 Front Panel of Environmental Parameters Monitoring Subsystem

Physical condition of assets depends on environmental parameters such as temperature, pressure, humidity and light intensity. Any sudden environmental disturbances or intended deeds to damage or destroy the assets will definitely result in changed environmental conditions. These reflect in the changed temperature, humidity, pressure or light intensity at particular location. At each location, where environmental parameters are to be monitored, a wireless sensor mote is fixed to monitor the parameters. A WSN network of such motes keeps track of environmental parameters at numerous locations and also gives alarm indication if any parameter crosses allowed limit. The upper and lower limits of temperature, humidity, pressure or light intensity are user defined. Database of these parameters is continuously updated and time duration to update the database is also user defined.

The monitoring system updates the database. It also gives an alarm if a parameter crosses allowed limit. The alarm is a blinking LED which stops after acknowledging the alarm. An example of four locations is given in fig. 5.11, but this system can be further modified according to user requirements and more locations can be monitored. As we can see in above GUI, pressure and light intensity parameters of the I&SP lab section are giving alarm. This is because the maximum limit of pressure parameter is set to 900 mbar and minimum limit to light intensity parameter is set to 65 lux in case of I&SP lab. While these parameters are normal in case of "Instrumentation lab". This is because upper and lower limits of these parameters are set different according to requirements. Humidity parameter is showing alarm because it has crossed the upper limit (85% in this case). These parameters can be logged into the database as shown in fig 5.12 below.

wsndata

dat	tim	id	temp	hum	pres	light
5/14/2011	11:43 AM	2	25.1334	41.32773248	957.891684889793	525.731825515545
5/14/2011	11:51 AM	2	25.5058	49.09140788	958.033032536507	546.559332066455
5/14/2011	12:34 PM	2	24.761	50.60185012	957.495444118977	681.938124647369
5/14/2011	12:36 PM	2	25.1726	50.1647	957.284308075905	723.593137749189
5/14/2011	12:38 PM	2	25.2608	47.182325	957.128801494837	723.593137749189
5/15/2011	11:30 AM	2	25.2216	40.84927232	958.856982856989	400.766786210086
5/15/2011	11:32 AM	2	25.2314	43.16108272	958.779463768005	291.422376817809
5/15/2011	11:36 AM	2	25.6038	46.10789888	958.553682431579	525.731825515545
5/15/2011	11:38 AM	2	25.3882	44.1968	958.581954479218	484.076812413726
5/15/2011	11:40 AM	2	25.2608	43.16108272	958.529994249344	546.559332066455
5/15/2011	11:44 AM	2	25.1236	42.36411952	958.522582232952	442.421799311906
5/15/2011	11:46 AM	2	24.9668	42.12498688	958.529322162271	442.421799311906
5/19/2011	11:44 AM	1	30.984	39.413408	960.089121453464	187.28484406326
5/19/2011	12:05 PM	1	28.1714	41.72638768	961.713843747973	322.663636644174

Fig. 5.12 Database for Environmental Parameters Monitoring Subsystem

5.2.2 GPS Vehicle Tracking Subsystem:

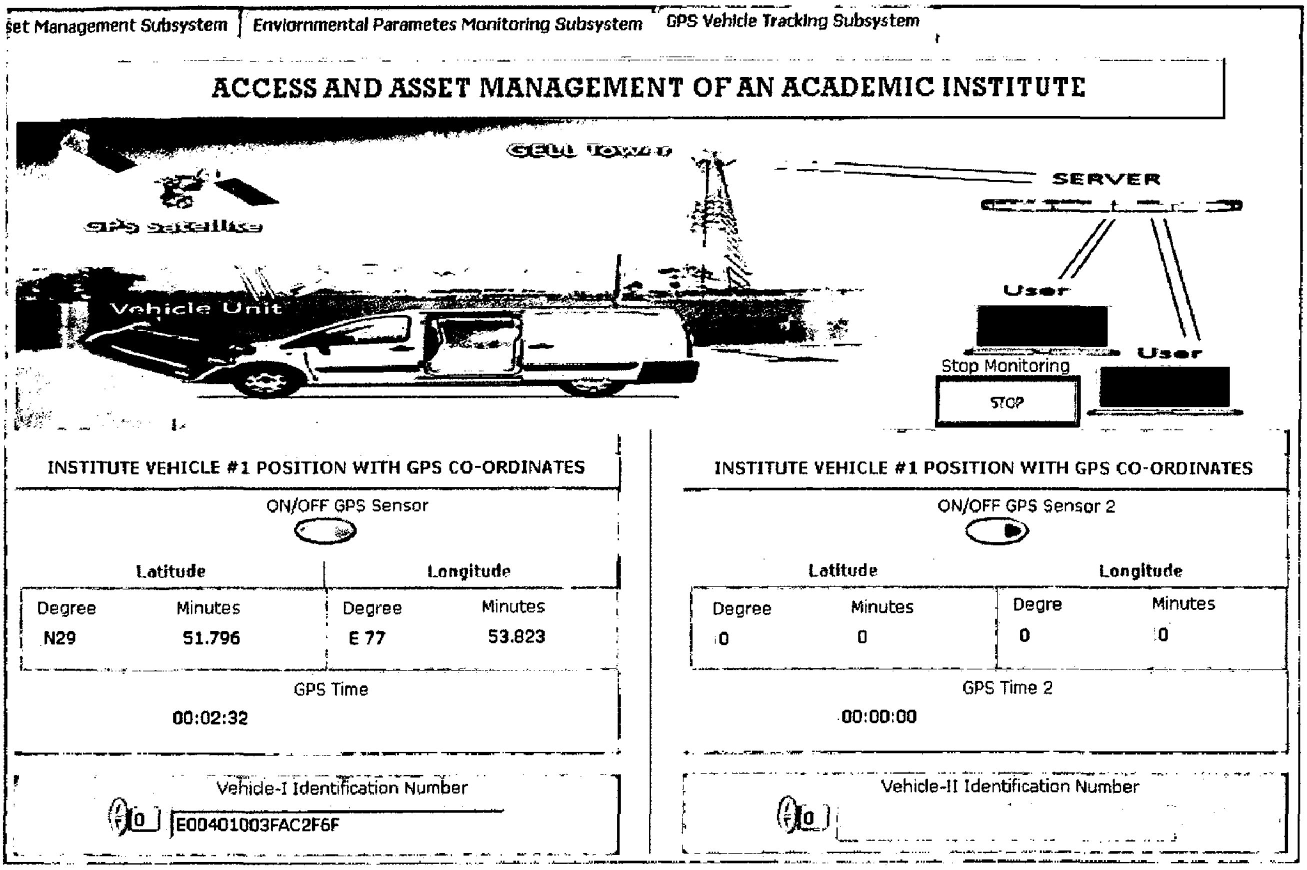
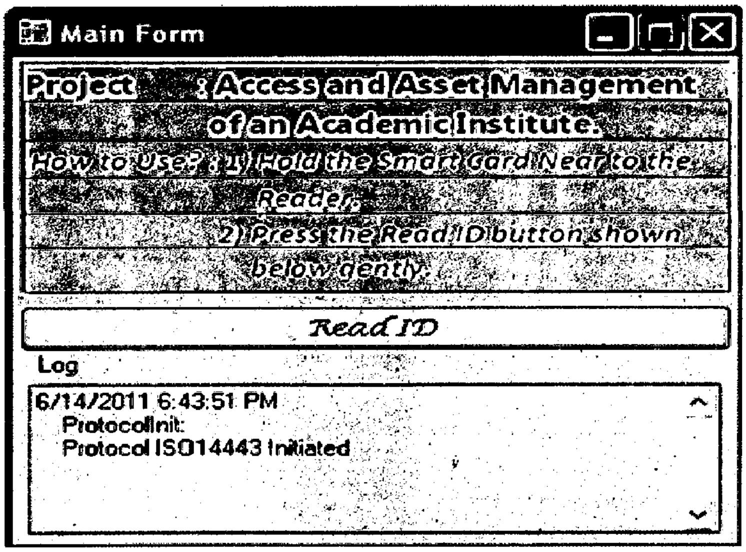


Fig. 5.13 Front Panel of GPS Vehicle Tracking Subsystem

Fig.5.13 describes the GPS positioning system. It detects the GPS sensor and shows Latitudinal and Longitudinal position of the sensor. "On/Off GPS Sensor" switch provides the facility to detect the position at will. The system also displays the time of measurement. The Vehicle Identification number indicates Id of RFID tag attached to identify institute vehicle. Fig.5.13 shows system for two vehicles, which can be increased according to requirements.

Vehicle Identification no is "E00401003FAC2F6F" in case of vehicle-I which is detected in above GUI. Respective position and GPS time is also shown above. This GPS position indicates the current position of GPS sensor MTS420 which when embodied in vehicle-I represents the position of the vehicle-I.

5.3 RFID Tag Detection Display:



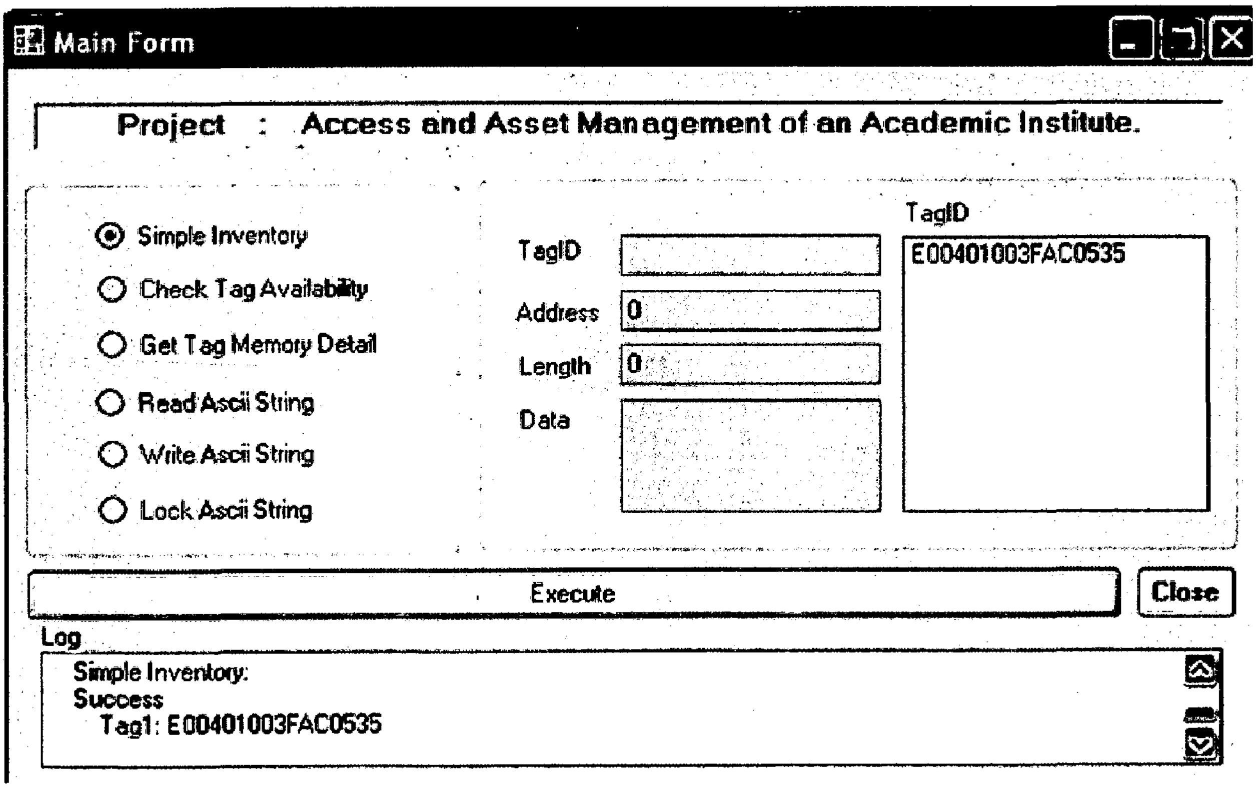


Fig. 5.14 User Interfaces for Detecting RFID Tags.

As seen from the fig.5.14, the interfaces are different for smart cards and ISO15693 compatible tags. In case of smart cards, Interface just provides a single button to read the tag. It also indicates instructions for the new users. The interface is simple and easy. The tag Id is shown in case of ISO-15693 tags while it's not necessary for ISO-14443 tags. In this example tag-Id detected is "E00401003FAC0535". Log of events is also shown to facilitate the user for a close look on events.

In case of ISO15693 tags, the user is asset manager. Hence, some facilities are provided along with the tag identification. The facilities provided are,

1. Write some date into tag.
2. Read the data written in tag.
3. Lock the data written in tag.

CHAPTER-6
CONCLUSIONS AND FUTURE SCOPE

Conclusions related to the work presented in this report are described here. It also takes a glance at possible work in future and scope about this dissertation.

6.1 Conclusions:

Basic concepts of assets, access and asset management and an overview of RFID and GPS technologies which are used to achieve access and asset management have been described. Some of the possible strategies for their implementation and incorporation of these strategies into subsystems have also been discussed. RFID technology is effectively used in access and asset management system because detection and identification of objects carrying RFID tags is much easier and reasonable than other sensor technologies. GPS is indispensable system in vehicle tracking and tracing of assets in outdoor environment and along with RFID it facilitates the identification of vehicle and monitoring of its position. Wireless Sensor Networks made up of Crossbow wireless sensor boards (MTS400) effectively monitors the environmental parameters by using Zigbee protocol. LabVIEW offers necessary platform to integrate these technologies by which their overall functionality and capacity is increased. This project uses Microsoft Access which is very convenient and useful in mapping complex relations between assets and their access to limited users. This project maintains the security and integrity of the database by providing hierarchal power to different users for its access and isolated view to some of them.

The main concern in access management is to keep a track of people entered into the institute building which is accomplished by providing a database which already contains information about each individual working or studying in the institute. The facility of entering information about visitors helps in keeping a permanent record about them. Institute assets, which are broadly classified in to seven categories (viz. electronic products, laboratory equipments, library stuff, office documents, furniture, vehicle, thesis), and individuals working or studying in the institute are included into database. Integration of RFID system is successfully done with this database by using LabVIEW software. Different visual indications in different subsystems as well as the facility of attendance monitoring system provided to the faculty ensure better utilization of resources. Tracking of the institute vehicle ensures proper utilization of the vehicle. User friendly interfaces developed for detecting RFID tags speed up the tag detection process and minimize the complexities in entering tag Id into database. The GUIs developed in LabVIEW being highly informative and user friendly boosts the overall management process.

6.2 Future Scope:

Some of the improvements needed to enhance the scope of the project are listed below.

a) Real-Time Location Systems (RTLS) is an emerging field and can be adopted as an alternative and cost effective method for tracking of asset location and their status within local areas. In RTLS systems, tagged assets need not be scanned or passed within close proximity of the reader in order to be detected. In contrast, RTLS tags transmit their ID's and status information at frequent intervals via a low power radio signal to a central processor.

b) Distributed database (in which data about the same asset can be distributed over different systems) and networked database (which can be used to duplicate the original database maintaining its integrity and providing additional robustness to architecture) can be developed and implemented by using the existing centralized database.

c) More flexibility to user can be provided while limiting schema expansion in the database by using Extensible Markup Language (XML). XML enabled databases are available in market and can be efficiently used to transport complex attributes over networks.

d) Pictorial representation of institute vehicle on a digital map (representing nearby geographical area) by using the acquired GPS coordinates is an added advantage.

e) Improved security in access control can be achieved by integrating RFID smart cards with bio-identification techniques such as iris detection or finger print recognition.

f) Institute IT asset management is also an additional advantage.

REFERENCES

[1] Masakatsu Kourogi1, Nobuchika Sakata, Takashi Okuma1, and Takeshi Kurata, "Indoor/outdoor pedestrian navigation with an embedded GPS/RFID/Self-contained sensor system," *Springer-Verlag Berlin Heidelberg* pp.1310-1321, 2006.

[2] Kumar, S., and K. B. Moore."The Evolution of Global Positioning System (GPS)," *Journal of Science Education and Technology*, pp 59-80, 2002.

[3] IIMM (2002), International Infrastructure Management Manual, Australia/New Zealand Edition, The Institute of Public Works Engineering, Australia.

[4] British Standards Institute (2004) PAS 55: Asset Management. Part 1: Specification for the Optimised Management of Physical Infrastructure Asset.

[5] Snitkin, S. (2003) "Collaborative asset lifecycle management vision and strategies", Research Report, ARC Advisory Group, Dedham, USA.

[6] IIMM (2002), International Infrastructure Management Manual, Australia/New Zealand Edition, The Institute of Public Works Engineering, Australia.

[7] Mohamed Zied Ouertani, Ajith Kumar Parlikad, Duncan Mcfarlane, "Towards an approach to select an asset information management strategy", International Journal of Computer Science and Applications, 2008, Vol. 5, No. 3b, pp 25 – 44

[8] Koronios, A, Nastasie, D, Chanana, V & Haider, A, (2007), "Integration Through Standards – An Overview Of International Standards For Engineering Asset Management", 2nd World Congress on Engineering Asset Management and the Fourth International Conference on Condition Monitoring (WCEAM 2007), Harrogate, United Kingdom, 11-14 June.

[9] John Woodhouse (2006), "PAS-55 - Asset Management: concepts & practices", 21st International Maintenance Conference, IMC-2006, December 5-8, Daytona Beach Florida, USA.

[10] Wern-Kueir Jehng, ShihSen Peng and Wei-Hsun Huang, "Using LabVIEW to Integrate RFID System and Database for Supply Chain Efficiency Improvement", international journal of intelligent control and systems vol. 13, no. 3, september 2008,189-195

[11] António Leong, Simon Fong, Shirley Siu, "Smart Card-Based Irregular Access Patterns Detection System", Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'04).

[12] Stephen B. Miles and Sanjay E. Sarma and John R. Williams, *RFID Technology and Applications* [Online]. Available:http://assets.cambridge.org/97805218/80930/excerpt/9780521880930_excerpt.pdf (downloaded on Nov 2, 2010).

[13] Roy want, *An introduction to RFID technology* [Online]. Available:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1593568 (downloaded on Nov 12, 2010).

[14] Matsuda Reiko, Tsuji Toshiyuki, "Asset Management Solutions for Improving Business Operational Efficiencies", NEC Technical Journal, Vol. 1, No.2, PP. 87-91, 2006.

[15] Steve lewis, *A basic introduction to RFID technology and its use in the supply chain* , Available: http://hosteddocs.ittoolbox.com/laran032604.pdf (downloaded on Dec 12, 2010).

[16] Sandip Lahiri, *RFID Sourcebook*, First printing, September 2005, Prenitice Hall PTR, ISBN: 0-13-185137-3.

[17] "The State of RFID Implementation and Its Policy Implications", An IEEE-USA White Paper, published 15 April 2009. [online] Available:http://www.ieeeusa.org/volunteers/committees/ccp/documents/RFIDwhitepaperFinal15April2009_000.pdf (downloaded on Dec 15, 2010).

[18] Klaus Finkenzeller (Translated by Rachel Waddington), *RFID Handbok*, Second Edition, Wiley & Sons Inc, ISBN 0-470-84402-7.

[19] Matt Ward, Rob van Kranenburg, "RFID: Frequency, Standards, Adoption and Innovation", JISC Technology and Standards Watch, PP. 4-30, May 2006.

[20] Ahmed El-Rabbany, *Introduction to GPS: The Global Positioning System*, First printing, Artech House mobile communication series, ISBN 1-58053-183-1.

[21] "U.S. Federal Radionavigation Plan", FRP, published in 1999. [online] Available: http://www.navcen.uscg.gov/pdf/frp/frp2001/FRP2001.pdf (downloaded on Mar 2, 2011)

[22] R.B. Langley, *"Why is the GPS signal so complex?" GPS World*, proceedings of the IEEE, Vol. 1, No.3, May/June 1990, pp. 56-59.

[23] Per Enge and Pratap Mishra, "Scanning the issue technology: special issue on global positioning system", proceedings of the IEEE, Vol. 87, No. 1, January 1999 [online]

Available: http://www.cs.columbia.edu/~drexel/CandExam/SpecIssueGPS.pdf (downloaded on Mar 20, 2011)

[24] B. Hoffmann-Wellenhof and H. Lichtenegger, and J. Collins, *Global Positioning System: Theory and Practice*, third edition, New York: Springer-Verlag, 1994.

[25] M. Shaw and K. Sandhoo, and D. Turner, *Modernization of the Global Positioning System*, GPS World, proceedings of the IEEE, Vol. 11, No. 9, September 2000, pp. 36.44.

[26] Ivan A. Getting, "perspective/ navigation Global Positioning System", IEEE spectrum, December 1993.

[27] Garfield Hamilton, "CataLogger: A Framework for Building Asset Management Solutions", Proceedings, IEEE Computer Society, 1999.

[28] "LabVIEW Basics I Development Course Manual", National Instruments, Part Number 320628N-01, Oct. 2005.

[29] "LabVIEW Basics II Development Course Manual", National Instruments, Part Number 320628N-01, Oct. 2005.

[30] "Microsoft Access 2007 product guide", Microsoft, 2007

[31] Mrutyunjay Raut, "Development of Wireless Sensor Networks for Asset Management", Dissertation report, Department of Electrical Engineering, IIT Roorkee, 2010.

[32] http://msdn.microsoft.com/en-us/library/ff402351.aspx (Downloaded on May 1, 2011)

[33] "MoteWork Getting Started Guide", Crossbow Technology, Document no 7430-0102-05, March 2007.

[34] news://msnews.microsoft.com (Downloaded on Apr 3, 2011)

[35] "RRHFEKv2.0 User's Manual", RapidRadio Solutions Pvt Ltd, 18 Feb. 2010.

[36] "HF RFID Tag RRHFT01", RapidRadio Solutions Pvt Ltd.
available at www.rapidradio.com. (Downloaded on May 12, 2011)

[37] "MTS/MDA Sensor Board Users Manual", Crossbow Technology, Document no 7430-0020-05, June 2007.

[38] "MPR-MIB Users Manual", Crossbow Technology, Document no 7430-0021-08, Revision A, June 2007.

APPENDIX A: RapidRadio RRHFEKv2.0 HF Evaluation Kit: User's Manual

Product Description:

Radio Frequency Identification (RFID) has been used for more than a decade and still provides growing benefits most commonly associated with Access Control (employee badge entry), Animal ID and Auto Immobilizer (theft prevention); RFID can be used for many additional applications. This Evaluation Kit 2.0 is based on RFID. It is working on 13.56MHz. It supports ISO-14443-3A and ISO-15693 based transponders. Evaluation Kit supports custom transponder of NXP like MIFARE STANDARD 1K, MIFARE STANDARD 4K and ICODE SLI.

Specifications of Evaluation Kit:

Some of the important specifications of RapidRadio RRHFEKv2.0 HF evaluation kit are enlisted here.

1. Frequency of operation: 13.56MHz.
2. Power Consumption : 300mW (Maximum)
3. Interface: USB.
4. Temperature range: -10C to +70C.
5. Protocol Supported: ISO14443-3A and ISO-15693.
6. Power supply: self powered by USB.
7. Read range: 5cm.
8. Weight: 200gms (approximately.)
9. Dimensions: 4.35 x 2.74 x 1.10 inch
10. Color: off white.
11. Indicator: LED and buzzer.
12. Enclosure material: ABS plastic.

Installation:

- Power up the reader by connecting USB port of PC via USB cable.
- Operating System will ask to install driver for another reader.
- Insert the CD which provided with the Evaluation Kit.
- Open the demo application provided with the CD.
- Check Connection using connect button.
- Check information of reader using information button.

Definitions:

WORDS	Description
BOOL	Boolean
BYTES	8-Bit Unsigned Character
LPWSTR	16-bit Unsigned Integer Array
WORD	16-bit Unsigned Integer
VOID	Variable without data type
Reader	RapidRadio RFID HF Reader
Tag	Tags, which are pasted on Assets
Card	Cards, which are available for each and every Ptrons
Application	Middleware Application
User	End user of the application
PICC	Proximity Integrated Circuit Cards
VICC	Vicinity Integrated Circuit Cards
0xXX	Hex number
UID	Unique Identification number on card or tag
ATQ	Acknowledgement to request card
NVB	Number of Valid Bytes
SAK	Select Acknowledgement of card
AFI	Application Family Identifier
DSFID	Data Storage Format Identifier
EAS	Electronic Article Surveillance

DLL Command Description:

1. **Simple Inventory:**

Description	This will search for the card in the field and return the available cards in the field
Syntax	BOOL ISO14443Inventory(BYTE bUID[][10], BYTE bUIDLen[][10], BYTE *bTags, LPWSTR strUID, BYTE *bError);
Parameters	bUID[in]: Detected UID will be stored in this two dimensional array inventory bUIDLen[in]: In this array the length of the respective UID will store of the detected UIDs bTags[in-out]: User has to assign maximum number of card should detect in inventory. This variable will contain number of cards detected in inventory. strUID[in]: The UIDs detected in inventory will be stored in this variable and each UID will be separated by ";". bError[in]: If process is success it will return 0 else it will return error specified in error list.
Return Values	TRUE if success False if fail
Remarks	All card detect in the inventory will be in halt state so after inventory if user wants to process then he has to sent wakeup to card.

2. **Read ASCII string:**

Description	This will read data from specified block of the tag
Syntax	BOOL ISO15693ReadSingleBlock (BYTE bFlags, BYTE bUID[8], BYTE bBlockNumber, BYTE *bBStat, BYTE bReadData[], BYTE *bDataLen, BYTE *bError);
Parameters	bFlags[out]:supported flags and description 0x02 – Non Addressed 0x42 - Non Addressed with option flag if supported 0x12 – Selected flag

	0x52 – Selected Flag with option flag if supported 0x22 - Addressed flag 0x62 - Addressed flag with option flag if supported bUID[out]: This is optional field if addressed flag is set than pass UID of the tag else not bBlockNumber[out]: The block from which user wants to read. Block range from 0 to 255 depends upon manufacturer. bBStat[in]: If option flag is supported and it is set in request than tag will return security status of block in response. bReadData[in]: Data to be read. Data byte can be range from 0 to 32 as per manufacturer and protocol specification. bDataLen[in]: Function will return length of the data returns from the tag in response of the request. bError[in]: If process is success it will return 0 else it will return error specified in error list.
Return Values	TRUE if success False if fail
Remarks	If the multiple tags in field and read single block is called without address than the collision will occur in response. It is good practice to read single block in addressed mode.

3. **Write ASCII string:**

Description	This will write data from specified block of the tag.
Syntax	BOOL ISO15693WriteSingleBlock (BYTE bFlags, BYTE bUID[8], BYTE bBlockNumber, BYTE bWriteData[], BYTE bDataLen, BYTE *bError);
Parameters	bFlags[out]:supported flags and description 0x02 – Non Addressed 0x12 – Selected flag 0x22 - Addressed flag bUID[out]: This is optional field if addressed flag is set than pass UID of the tag else not bBlockNumber[out]: The block from which user wants to write. Block range from 0 to 255 depends upon manufacturer. bWriteData[out]: Data to be written to tag. Data byte can be range from 0 to 32 as per manufacturer and protocol specification. bDataLen[out]: Data length of the data to be written in tag, length of the data must be specified in tag manufacturer datasheet. bError[in]: If process is success it will return 0 else it will return error specified in error list.
Return Values	TRUE if success False if fail
Remarks	It is good practice to write data in addressed mode.

4. **Lock ASCII string:**

Description	This will lock the specified block of the tag.
Syntax	BOOL ISO15693WriteSingleBlock (BYTE bFlags, BYTE bUID[8], BYTE bBNum, BYTE *bError);
Parameters	bFlags[out]:supported flags and description 0x02 – Non Addressed 0x12 – Selected flag 0x22 - Addressed flag bUID[out]: This is optional field if addressed flag is set than pass UID of the tag else not bBNum[out]: The block which user wants to lock. Block range from 0 to 255 depends upon manufacturer. bError[in]: If process is success it will return 0 else it will return error specified in error list.
Return Values	TRUE if success False if fail
Remarks	This will make the block read only. User will not be able to write on this block once locked the block. If user tries to write the block, tag will return an error.

APPENDIX B: MTS/MPR User's Manual

1. MTS400CA / MTS420CA

The MTS400CA offers five basic environmental sensors with an additional GPS module option (MTS420CA). The features offered on these boards allows for a wide variety of applications ranging from a simple wireless weather station to a full network of environmental monitoring nodes. Applicable industries include agriculture, industrial, forestry, HVAC and more. These environmental sensor boards utilize the latest generation of energy efficient digital IC-based board-mount sensors. This feature provides extended battery life where a low maintenance, field deployed, sensor node is required. The GPS module offered on the MTS420CA (Figure 1-1) may be used for positional identification of Motes deployed in inaccessible environments and for location tracking of cargo, vehicles, vessels, and wildlife.

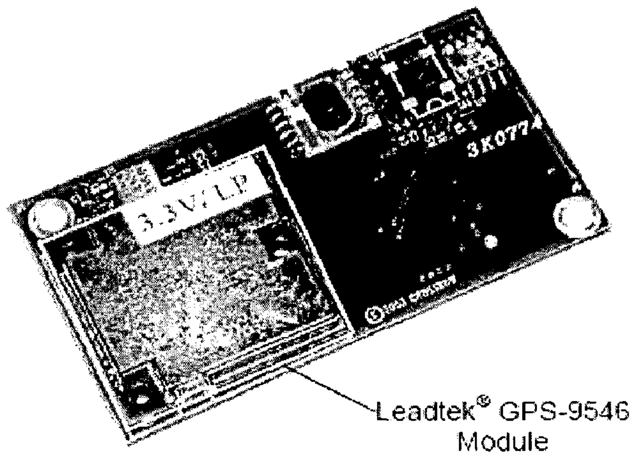


Figure 1-1 Photo of MTS420CA

NOTE: Motes are designed for power efficiency. Hence all the sensors are disconnected from power on the MTS400 and MTS420 sensor boards unless specifically turned on.

1.1 Humidity and Temperature Sensor

The Sensirion (http://www.sensirion.com/) SHT11 is a single-chip humidity and temperature multi sensor module comprising a calibrated digital output. The chip has an internal 14-bit analog-to-digital converter and serial interface. SHT11s are individually calibrated.

Table 1-1. *Summary of the Sensirion® SHT11's Specifications*

Sensor Type	Sensirion SHT11	
Channels	Humidity	Temperature
Range	0 to 100%	-40°C to 80°C
Accuracy	± 3.5% RH (typical)	± 2°C
Operating Range	3.6 to 2.4 volts	
Interface	Digital interface	

This sensor's power is enabled through a programmable switch. The control interface signals are also enabled through a programmable switch. An analog-to-digital converter in the sensor does the conversion from humidity and temperature to digital units.

1.2 Barometric Pressure and Temperature Sensor

The Intersema® (http://www.intersema.ch/) MS55ER is a SMD-hybrid device including a piezoresistive pressure sensor and an ADC interface IC. It provides a 16-bit data word from pressure and temperature measurements. A 3-wire interface is used for all communications.
This sensor's power is enabled through a programmable switch. The control interface signals are also enabled through a programmable switch. An analog-to-digital converter in the sensor does the conversion from pressure and temperature to digital units.

Table 1-2. *Summary of the Intersema® MS55ER's Specifications*

Sensor Type	Intersema MS5534
Channels	Pressure and Temperature
Range	Pressure: 300 to 110 mbar Temperature: -10°C to 60°C
Accuracy	Pressure: ± 3.5% Temperature: ± 2°C
Operating Range	3.6 to 2.2 volts
Interface	Digital interface

1.3 Light Sensor

The TLS2550 is a digital light sensor with a two-wire, SMBus serial interface. It is manufactured by TAOS, Inc (http://www.taosinc.com). It combines two photodiodes and a companding analog-to-digital converter on a single CMOS integrated circuit to provide light measurements over an effective 12-bit dynamic range. Table 4-3 has a summary of the sensor's specifications.

Table 1-3. *Summary of TAOS TSL2550's Specifications*

Sensor Type	Taos TSL2550
Channels	Light
Range	400 – 1000 nm
Operating Range	3.6 to 2.7 volts
Interface	Digital interface

This sensor's power is enabled through a programmable switch. The control interface signals are also enabled through a programmable switch. An analog-to-digital converter in the sensor does the conversion from light to digital units.

1.4 2-Axis Accelerometer

The accelerometer is a MEMS surface micro-machined 2-axis, ± 2 g device. It features very low current draw (< 1mA). The sensor can be used for tilt detection, movement, vibration, and/or seismic measurement. The sensor output's are connected to ADC channels on the Mote's ADC1 and ADC2 channels.

Table 1-4. *Summary of the ADXL202JE's Specifications.*

Sensor Type	Analog Devices ADXL202JE
Channels	X (ADC1), Y (ADC2)
Range	±2 G (1 G = 9.81 m/s2)
Sensitivity	167 mV/G, ±17 %
Resolution	2 mG (0.002 G) RMS
Offset	VBATTERY/2 ±0.4 V
Operating Range	3.6 to 3.0 V
Interface	Analog interface

NOTE: The ADXL202 sensitivity and offset have a wide initial tolerance. A simple calibration using earth's gravitational field can greatly enhance the accuracy of the ADXL202 sensor. By rotating the sensor into a +1 G and a –1 G position, the offset and sensitivity can be calculated to within 1 %.

1.5 GPS (MTS420 only)

The GPS module (Leadtek GPS-9546, http://www.leadtek.com/) is powered via a DC-DC booster, which maintains a constant 3.3 volt input regardless of battery voltage. The booster output is programmably enabled. The output from the GPS module is connected to a serial uart, USART1, interface of the Mote. An active, external, antenna is supplied with the module. The GPS module supplies the antenna power.

Table 1-5. *Summary of the SiRFstarIIe LP's (GPS 9546) Specifications.*

GPS Chipset	SiRFstarIIe LP
Antenna	External active antenna, power supplied by GPS module.
Channels	12
Meters	10 m, 2D
Start Time (sec)	45 Cold; 38 Warm; 8 Hot
Reacquisition Time	0.1 sec (typical, w/o dense foliage)
Protocol	NEMA-0183 and SIRF binary protocol
Current	60 mA at 3.3 V
Interface	Serial interface

NOTE: The GPS module's DC-DC booster can interfere with radio communication. If the GPS module must be continually powered and monitored during radio communication, then 3.3-3.6 volt lithium batteries are recommended to power the Mote. Normal alkaline batteries are not recommended unless the GPS module is powered down during radio communication.

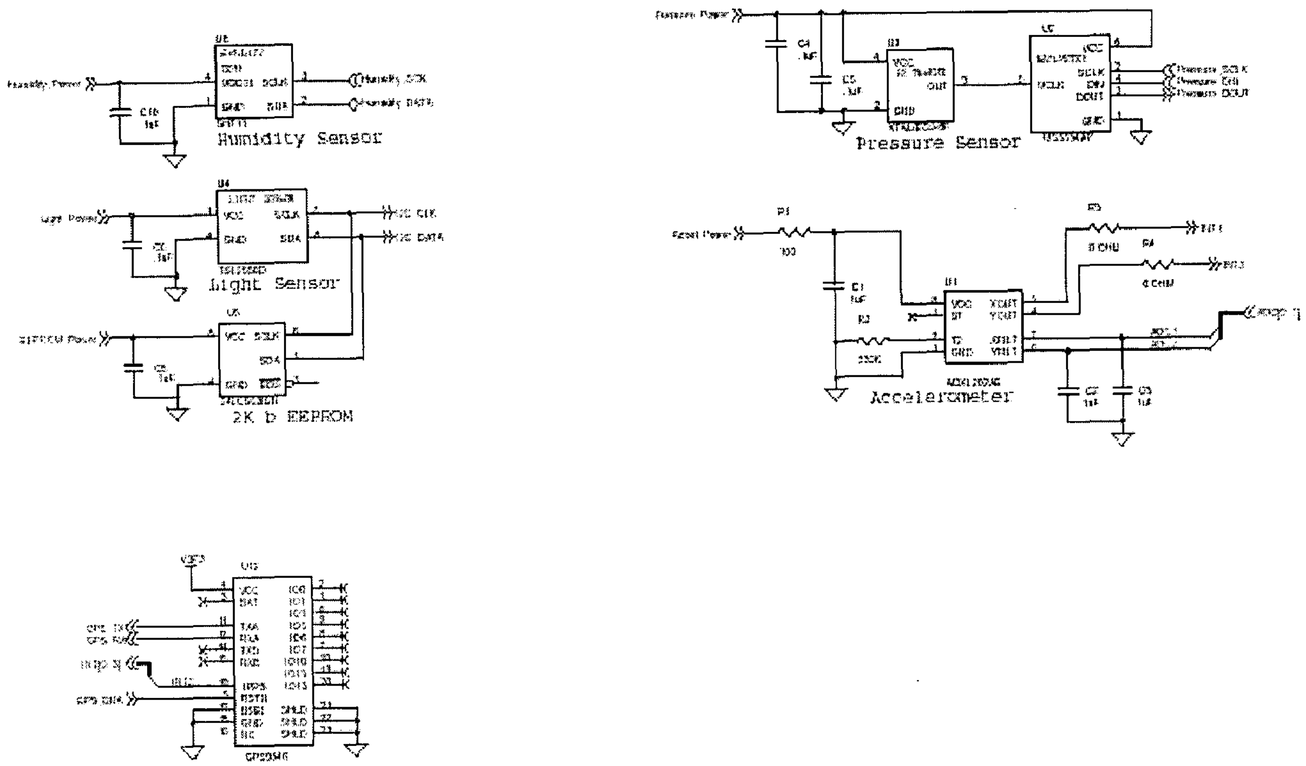
1.6 Turning Sensors On and Off

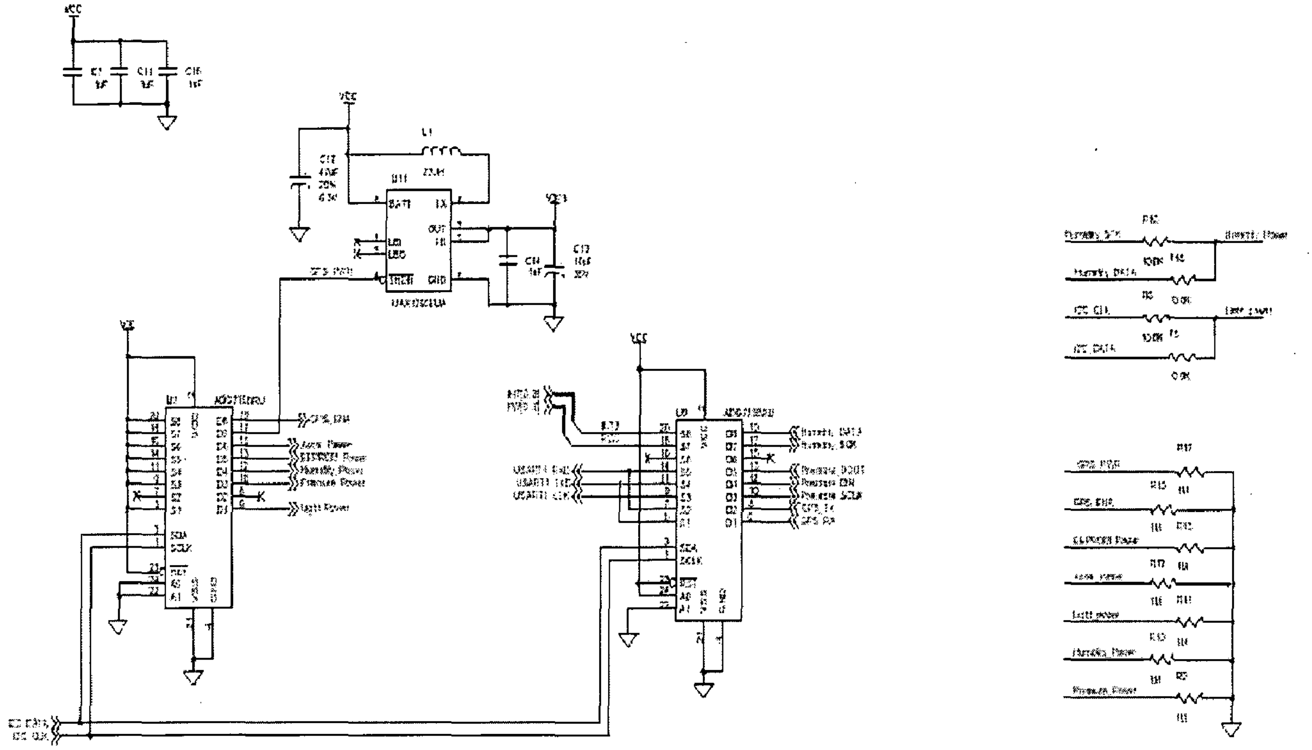
Power for all of the sensors on the MTS400/420 sensor board is controlled through an analog power switch at location U7. It can be programmed enable and disable power to individual sensors. The default condition for the sensors is off. This design helps minimize power draw by the sensor board.

1.7 TinyOS Driver and Test Firmware

A test firmware for the MTS400/420CA and a GUI to view/save the data on a PC is available via MOTE-VIEW interface.

1.8 Schematics of the MTS400CA and MTS420CA





2. MPR2400 (MICAZ)

2.1 Product Summary

The MICAz is the latest generation of Motes from Crossbow Technology. The MPR2400 (2400 MHz to 2483.5 MHz band) uses the Chipcon CC2420, IEEE 802.15.4 compliant, ZigBee ready radio frequency transceiver integrated with an Atmega128L micro-controller. The same MICA2, 51 pin I/O connector, and serial flash memory is used; all MICA2 application software and sensor boards are compatible with the MPR2400.

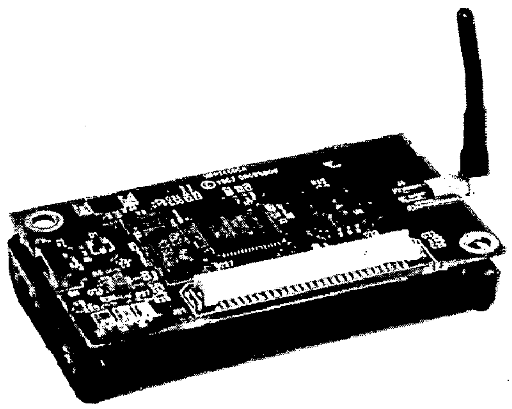


Figure 2-1. Photo of the MPR2400—MICAz with standard antenna.

2.2 Block Diagram and Schematics for the MPR2400 / MICAz

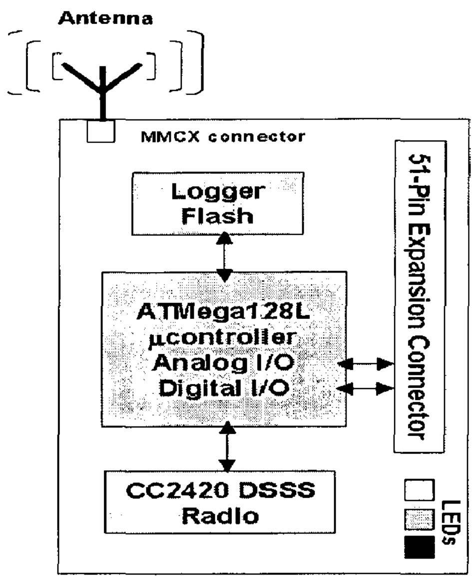
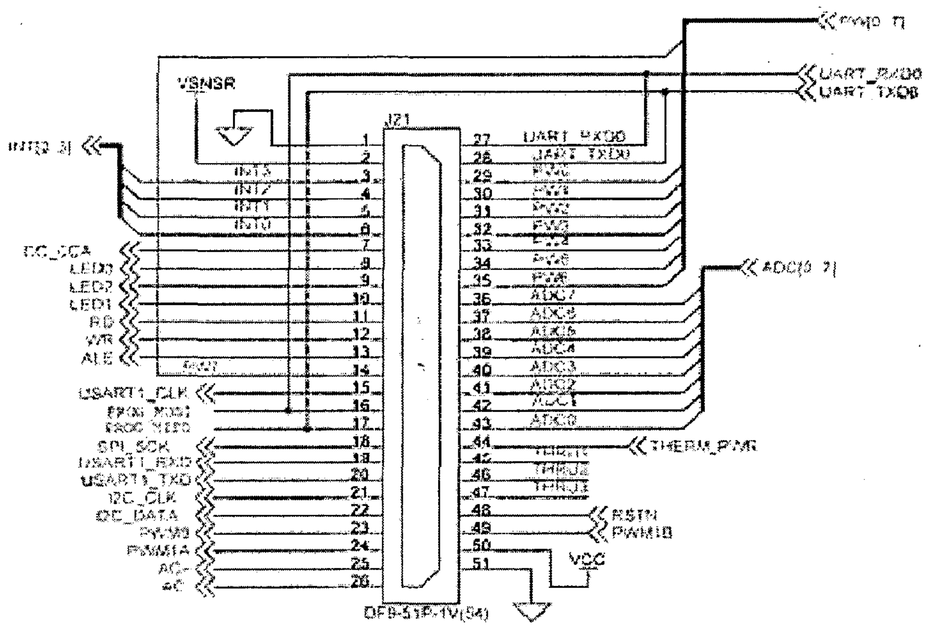
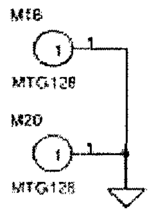


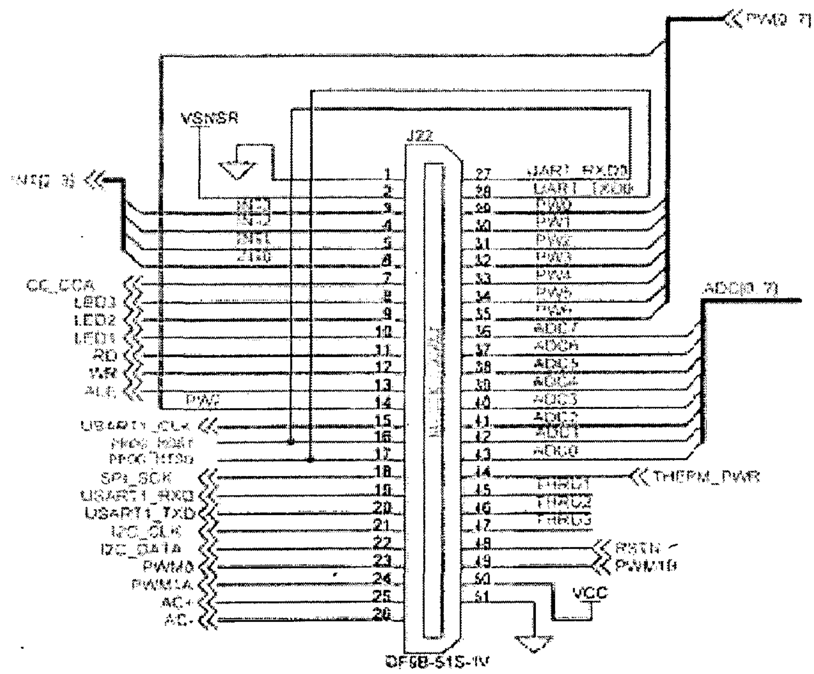
Figure 2-2. Block diagram of the MICA2 and listing of Chapters that discuss the components in

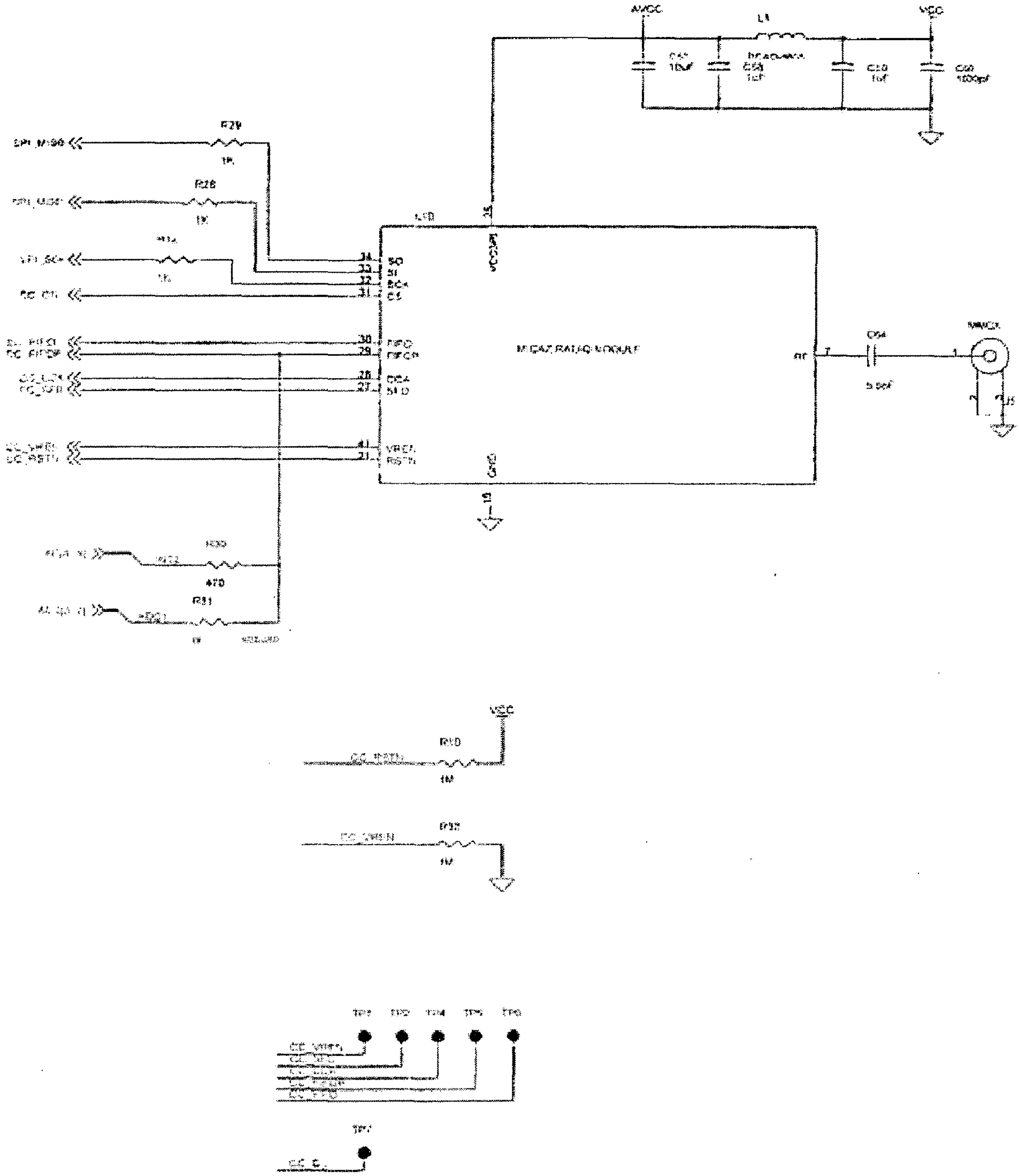
greater detail.

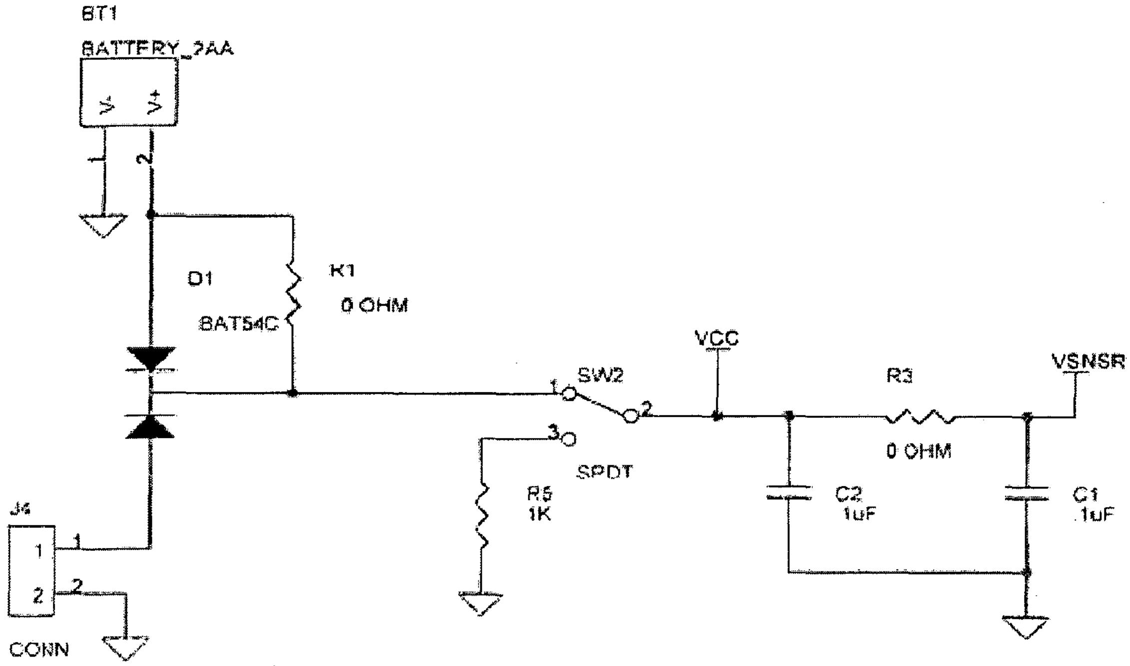
2.2.1 51-pin Expansion Connector 2.2.2 CC2420 Radio 2.2.3 Battery, ADC1



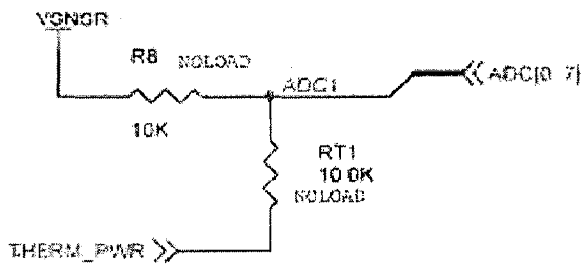





AVCC
L1
VCC
R29
R28
R30
470
R31
SO
SI
SCK
CS
FIFO
FIFOP
CCA
SFD
VREN
RSTN
GND
VCC
R10
1M
R32
1M



BOARD OPTIONS	
R1	INSTALL
R2	NOT INSTALLED
R4	NOT INSTALLED
R8	NOT INSTALLED
RT1	NOT INSTALLED



APPENDIX C: LabVIEW Database Connectivity Toolkit- Connecting to a Database

The LabVIEW Database Connectivity Toolkit allows you to quickly connect to local and remote databases and perform many common database operations without having to know structured query language (SQL) programming. This toolkit greatly simplifies the process of making fast and repeated calls to popular databases, such as Microsoft Access, SQL Server, and Oracle. If you need advanced database functionality and flexibility, the Database Connectivity Toolkit also offers complete SQL capabilities.

There are numerous database formats available from a variety of software vendors. In many cases, you may need to save data to multiple different types of databases. The Database Connectivity Toolkit provides one consistent API for numerous databases to save you the time of learning different APIs. The toolkit can connect to any database with an ADO-compliant OLE DB provider or ODBC driver, including popular databases such as:

Microsoft Access, Microsoft SQL Server, Oracle, Visual FoxPro, dBase, Paradox

Database Terminology:

SQL (Structured Query Language) is a set of character string commands that is a widely supported standard for database access. SQL statements allow you to use a common set of commands to access different databases. SQL statements can be used to store data into a database, query a database for records that match certain criteria, and many other database operations.

At its most basic level, the Database Connectivity Toolkit uses SQL statements to access, modify, and view information in databases. These statements are constructed in the toolkit's VIs and then executed through a Microsoft technology, OLE DB (Object Linking and Embedding Database), that provides a connection between LabVIEW and the database.

Inside LabVIEW, property and invoke Nodes make calls to the Microsoft ActiveX Data Objects (ADO). ADO will then connect to the database through either a Data Source Name or Universal Data Link.

OLE DB is comprised of a set of Microsoft Component Object Model (COM) interfaces that support various DBMS. For instance, OLE DB allows interaction with traditional DBMS such as Microsoft Access and other data storage systems such as Microsoft Excel. OLE DB is a C++ API that allows access to databases through a C++ compiler. OLE DB uses a provider (driver) to talk with the different DBMS.

With OLE DB you can communicate with any DBMS that supplies an ODBC driver or OLE DB provider. OLE DB uses the OLE DB Provider for ODBC as a conversion layer between OLE DB and ODBC if an ODBC driver is used to communicate with a database. However, there are native OLE DB Providers for different DBMS such as SQL Server, Jet (Microsoft Access), and Oracle. These native OLE DB providers are more efficient than the OLE DB Provider for ODBC because they remove the need to convert from OLE DB to ODBC and then to the DBMS.

OLE DB replaced ODBC as the underlying communication technology that allows the Database Connectivity Toolkit to interact with different databases. To change the database that the toolkit is working with, simply change the OLE DB Provider that is selected to communicate between LabVIEW and the DBMS.

CONNECTING TO A DATABASE:

The first step in doing database operations with the Database Connectivity Toolkit is to connect to the database. There are two major types of connections that can be created for LabVIEW to communicate with a database - Data Source Names (DSNs) and Universal Data Links (UDLs). DSNs are used to facilitate ODBC communication, and UDLs are used for OLE DB connections between the DBMS and LabVIEW.

ODBC DSN (Data Source Name)

A Data Source Name uses ODBC for communication between an application and the database. When creating a DSN you specify information such as the name of the data source (database), ODBC driver used for connection, and security information. DSNs are created and configured using the **ODBC Data Source Administrator (Control Panel » Administrative Tools » Data Sources(ODBC)**).

There are three types of DSN you can create:

1. **System DSNs** are contained in the system registry and apply to all system users.

2. **User DSNs** are stored in the registry and allow a single user to access a database.
3. **File DSNs** are files (*.dsn) that allow anyone with access to the file to access the database.

UDL (Universal Data Link)

Universal Data Links use ADO for communication between an application and a database. UDLs contain information about the OLE DB provider that is used for communication, server information, user ID and password, and database. The default OLE DB provider for UDLs is the OLE DB provider for ODBC, but the native providers for the DBMS are more efficient.

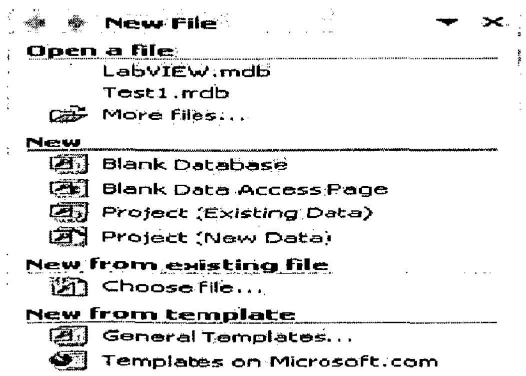
You can create a UDL in three different ways:

1. From within LabVIEW by going to **Tools » Create Data Link.**
2. Using the DB Open Create Connection VI (**All Functions » Database**) which can provide a prompt to create a UDL.
3. From outside LabVIEW by right-clicking on the Desktop or in Windows Explorer and selecting **New » Microsoft Data Link.**

Part 1. Create a Database

In this section you will create a simple database.

1. Open Microsoft Access (**Start » Programs » Microsoft Access**).
2. Create a new **Blank Database** from the **New File** menu, name it **Test Results**, and store it on the Desktop.



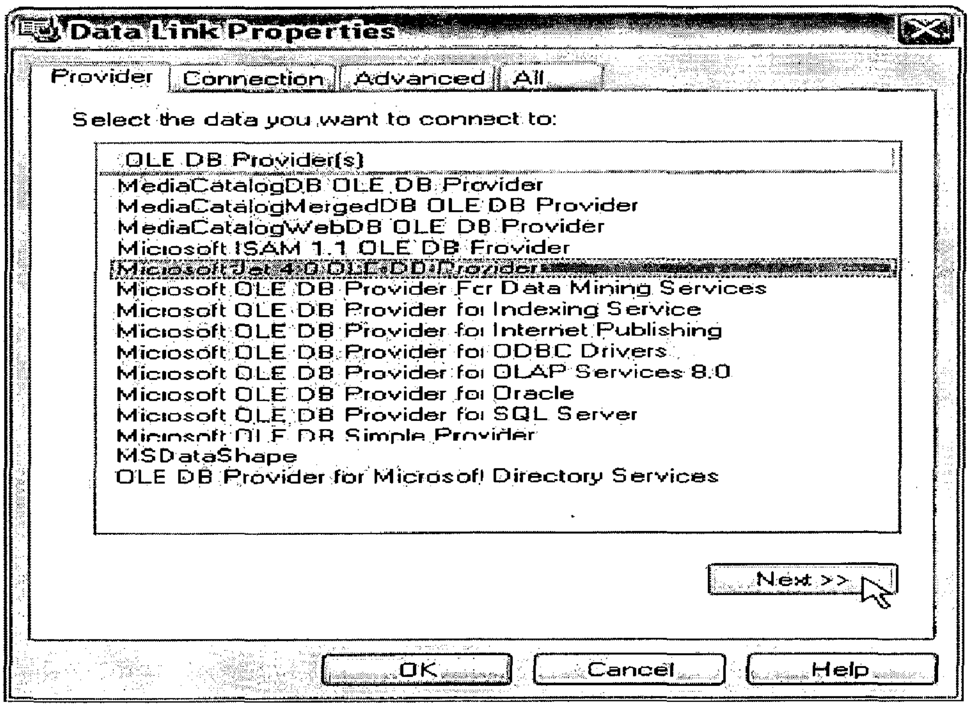
New File Menu in Microsoft Access

3. Save the database and close Microsoft Access. You will add tables and data to the database using the Database Connectivity Toolkit.

Part 2. Create a UDL

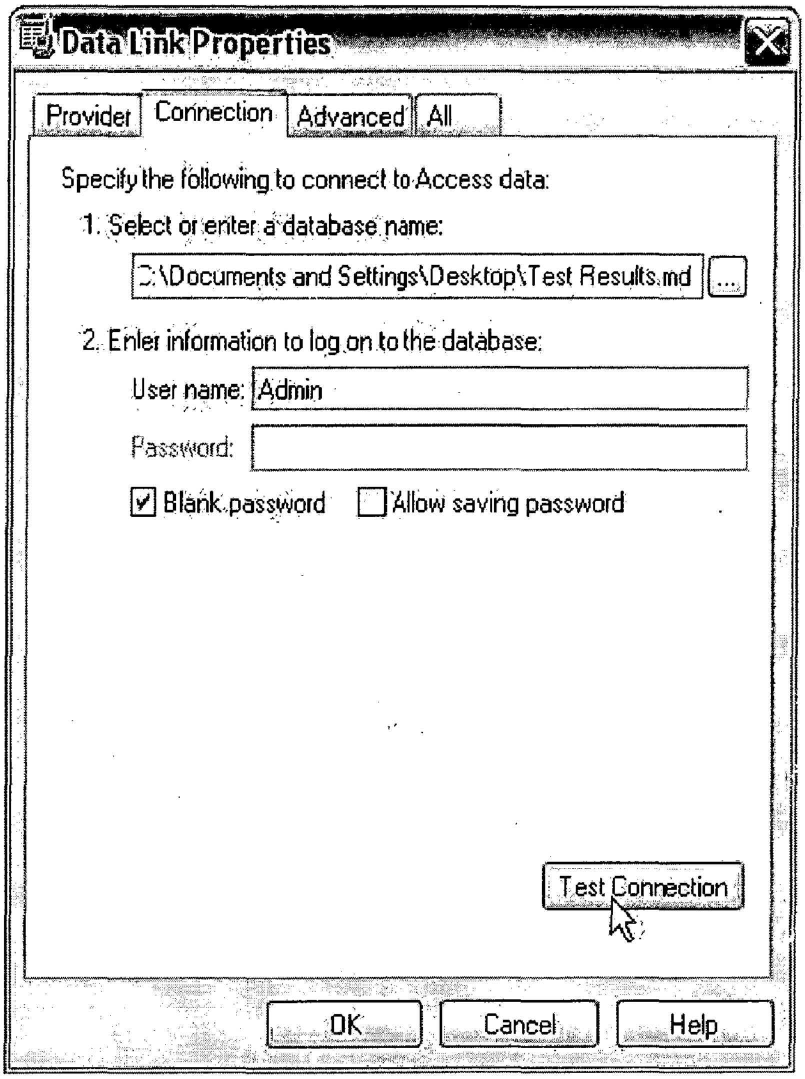
In this step you will create the second type of database connection, a Universal Data Link. You can create a UDL in many different ways. In this exercise you will create a UDL from within LabVIEW.

1. Launch LabVIEW either from **Start »Programs»National Instruments»LabVIEW** or by double-clicking on the LabVIEW short-cut on the Desktop.
2. From a blank VI, select **Tools » Create Data Link** to launch the Data Link Properties window.
3. On the Provider tab, select the provider for the DBMS that you are communicating with. By default this is the Microsoft OLE DB Provider for ODBC Drivers. In this case, select the Microsoft Jet 4.0 OLE DB Provider to communicate with the Microsoft Access database. It is more efficient to use the OLE DB provider for the DBMS if one is provided instead of the OLE DB Provider for ODBC Drivers. After you have selected the provider, click the Next button to move to the next step.



Data Link Properties Provider Page

4. On the Connection tab, browse to and select the Test Results.mdb database you created on the desktop in Step 1. Click the Test Connection button to test the UDL connection.



Data Link Properties Connection Page

5. Click the OK button to complete the setup of the UDL.
6. Save the UDL as TestResultsUDL.udl in the **C:\Program Files\National Instruments\LabVIEW 8.0\Database\data links** folder.