SYSTEM
ANALYSIS REPORT

WARDEN

by Troy

Ali Çetinbulut - 1250133
Fatih Yıldız - 1250935
Tolga Can -1250059
Burak Çiflikli - 1297639

1. INTRODUCTION

1.1 Goals and Objectives

Our new product WARDEN is simply a card based wireless door control system. WARDEN will be developed for the areas where limited people are allowed to enter. This will be provided by a door system that identifies the users having entrance permission. When these door systems are all combined with a master, WARDEN will be generated. Master will have the ability of introducing new users to the system.

System will also keep the log of the events as another security concern. The master will be able to trace the logs of his slave door systems.

1.2 Interviews

The ideas of customer and the potential users give very useful feedback that can be used in understanding system requirements and specifications.

1.2.1 Interview I

- Done by İsmail Öztürk; the hardware technician of the customer.

Q) Why did the department need to establish a card based door security system?

Our concern about security is to prevent the laboratory equipment getting damaged or stolen. So, we established a security system called Keri; not only a card based door system but composed of also a camera system.

Q) Preventing people that are not from our department from entering the laboratories, isn't a security concern for the department?

No actually. It is very easy for a friend of someone from the department to enter the laboratories.

Q) When we come to the door security system what are the main components of the system?

I can mainly divide the system into two; the master computer and the system on the doors.

Q) Can you a little bit explain the system on the door?

There is a reader on the both sides of the doors. When the card is read, the card id and the student number is taken as input. Then the permission for the input is checked locally. Finally, access is confirmed or denied.

Q) So what is the job of the master computer here?

As I said, the permission is checked locally, that is every door has a local user database. This database is updated from the master computer. The access info is also reported to the master computer. For example: "1297639 access-confirmed at 12:34 from inek1". In case of a crash in the system a certain amount of the access info is stored locally also.

Q) As the user database is stored in the door locally, can there be differences between the databases of the doors of different laboratories?

We don't use this property of Keri, but yes it has such a property. We can let only 4th grade students to enter inek laboratories for example.

Q) Would some extra security features be useful such as a double access to a door from the same side will require a punishment?

I don't think so. As I mentioned before; we only concern about the equipment's getting broken or stolen.

Q) Is there any thing that you don't like about Keri?

I don't have enough technical learning to give any details but a better user interface for the master computer could be better.

1.2.2 Interview II

- Done by Emre Güney; software engineer in TÜBİTAK-Bilten. They have a similar security system in their building.

Q) Why is TÜBİTAK in need of a door security system?

TÜBİTAK is the supreme organization put in charge of promoting, developing, organizing and coordinating research and development in the fields of exact sciences in Turkey in line with the national targets of economic development and technical progress. Of course there should be a security system.

Q) Can you give some information about the general working of the system?

There are magnetic readers on the doors that we get our cards read. These readers communicate with the main server through network.

Q) What kind of data is sent or received within the communication between the doors and the server?

When the card is read, if the access is confirmed the user id and the entrance time is sent to the server. Otherwise, that is if the access is denied then, nothing is sent.

Q) Is there any security features like catching double accesses to a door from the same side?

There is no such a directly feature but, when needed it can be obtained by tracing the log files from the server.

Q) Can your card open all the doors in the building?

No. There are some user groups defined. Someone can only enter a door if he or his groups owns the entrance permission for that door.

1.2.3 Interview III

- Done by Özgür Özgür; undergraduate student from Department of Computer Engineering - METU. He is a potential user for our system.

Q) How often do you go to department’s laboratories?

I can say nearly twice a day.

Q) We want to define some user groups for permissions. What will your opinion be about this?

I think such a feature is not really needed. Anyone with a card should be able to enter all the laboratories.

Q) Do you face with any problem about the size of the laboratory entrance card?

My only concern about the size of the card is that it should fit into my wallet. Current cards are okay I think.

Q) Is there anything that you don’t like about the current door security system?

After getting my card read, sometimes I have to wait for a long period of time. It should be faster.

1.3 Comments on Interviews

As a result of this interview we have a general view of key requirements of the system. First of all, as the main security concern of the customer is preventing the laboratory equipment getting damaged or stolen, we don’t have to provide extra security features. Checking user permission will be enough. User permission will be given separately for every door. There should be a feature on the master providing user grouping for permissions.

When the card is read, the validity of the user and card ids should be checked. This will take some time but the user shouldn’t be waited too much. So, clever algorithms should be found for data storing.

The user permissions will be stored locally as this will reduce the waiting time of the user. They will be updated from the master. As the update process will be done through network, the data sent should be as small as possible.

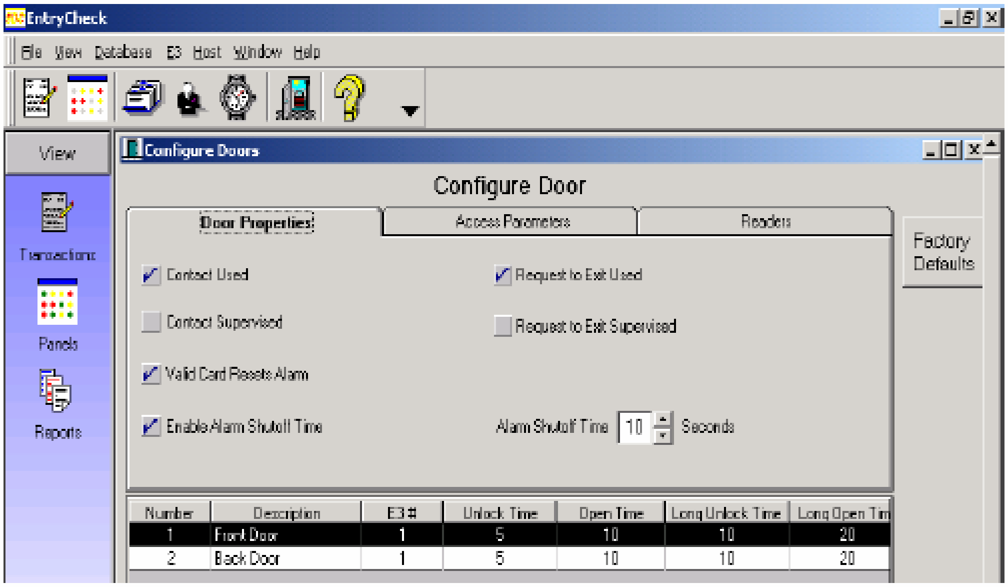
We should also keep the logs of the events on the doors. The master should provide tracing both current and old logs. In case of a crash in the system, a certain amount of log should be kept locally in the door system.

Finally, the software on the master computer should have a friendly and easy to use user interface.

1.4 Literature Surveys

1.4.1. Security Door Controls

The name of the system is E3 card access control [1]. This system has very well formed graphical user interface design. The most interesting properties of this system are that you can setup system with any number of doors and this control system can store the photos of user and also this system can schedule for working hours of the doors.



☑ Contact Used
☑ Request to Exit Used
☐ Contact Supervised
☐ Request to Exit Supervised
☑ Valid Card Resets Alarm
☑ Enable Alarm Shutoff Time
Alarm Shutoff Time 10 Seconds

Number	Description	E3 #	Unlock Time	Open Time	Long Unlock Time	Long Open Tim
1	Front Door	1	5	10	10	20
2	Back Door	1	5	10	10	20

Figure 1 – User Interface of E3

1.4.2 Millennium Entry Electronic Access Control System:

This system [2] can detect and report abnormal events like intrusion attempts, forced entry, attempts to use restricted doors, and integrated systems such as fire, tamper or other hazard alarms. This system allows system admin to update user profiles and schedule events from a central location. And also; every use of every access point is recorded.

Features

- Lock and unlock doors according to preset schedules
- Real-time event monitoring and reporting
- Centralized lockdown capability
- One door or one site at a time up to 100,000 access points
- Instant alarm notification supported by maps, sounds, instructions and reports
- Distributed architecture allows access points to function normally even if communication with the PC interrupted.

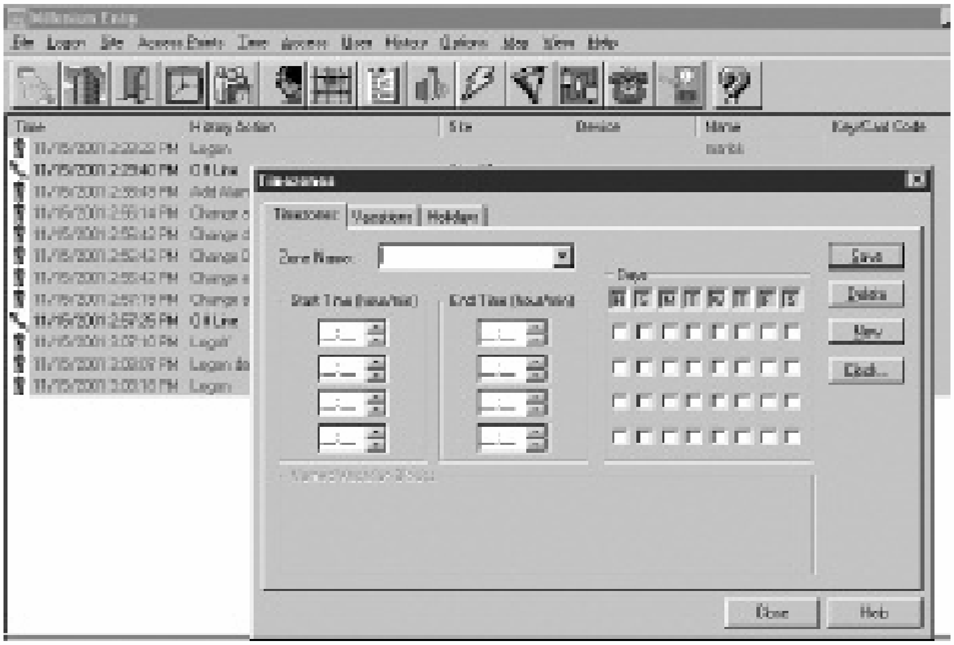


Figure 2 – User Interface of Millennium

1.5 Statement of Scope

WARDEN will be a card based door security system which will be used where entrance of people is limited based on permission. Users will have cards and they will get them read to the card readers on the doors for entrance.

Firstly, the doors and the users will be introduced to the system. The user information will be kept in the master computer. The permissions will also be attached by the master computer. A user may have different permissions for different doors. User grouping will also be provided. To reduce the waiting time of the users, the permissions of the users will also be stored locally. Every door will store its own permission file. The update of permissions will be done from the master computer and the updated files will be sent to the doors. The master will be able to make an update anytime.

The system will also keep the logs of the events on the doors like 'confirmed access', 'not defined user' and 'force attempt'. When a user get is card read, the user id and the card id are sent to the door. They are checked and if the user has permission to enter, it will be reported to the master as a 'confirmed access'. If the card id or the user id is invalid, then the report will be 'user not defined'. There will be a handle on one side of the door in case of an emergency. When this handle is used, it will be reported as a 'forced attempt'. The logs will be reported to the master immediately after an event. In case of a system crash, certain amount of these logs will also be stored locally at the doors. The master will have a *get log* feature, which will be used to get the locally stored logs from the doors. After a crash, when the master I restarted, this feature will be used automatically.

The master will be able to shut down the system. In this situation, he doors will not be opened even if an identified user gets his card read until the system is restarted by the master. If the master gets broken and the system can not be restarted, then a system card will get read to the readers on the doors. This card will make the doors work locally without the master.

The communication between the doors and the master will be established through a wireless network. The risk of a crash in the communication due to external physical factors will be reduced. This will also make introducing new doors to the system very easier.

2. USAGE ANALYSIS

2.1 Usage Areas Definitions

The general usage area of our product is company buildings, military, hospitals, universities (libraries or laboratories) and homes.

COMPANY BUILDINGS

Companies have several departments and several workers. Not all of the workers are allowed to enter all departments. For secure policy, companies restrict entrance permissions. Some workers are allowed to enter all departments and some are not. According to department new user groups are identified. Several user groups can be identified such as admin, user, engineers, managers and others. Each group has different permissions for doors. For example, admin is allowed to pass through parts and engineers are allowed to enter only software department.

MILITARY

Military is one of the most important areas that security is crucial. Entering into military areas must be restricted. People that are not from military must not be allowed to enter military areas. Also some groups must be defined. Some groups must have permission to enter all areas where some has only permission to enter only one area. This restriction is very important to know who is working where and also is there any one that has no permission in military area.

HOSPITALS

In hospitals, there are mainly two kinds of people. First are hospital staffs and second are patients. First of all patients must be restricted to enter laboratories, operating room or services and then hospital staff must be restricted. Doctors can have full permission to enter all departments and laboratory workers can have only permission for entering laboratories. These restrictions can be done by defining new groups and assigning access permissions to these groups.

UNIVERSITIES

In universities, security of laboratories and also libraries is very important. In order to restrict people in these areas security systems are required. For a laboratory of a department only the students of this department are allowed to enter and other students don’t have permission to use these laboratories. This restriction is crucial in case of stolen and broken laboratory or library components. If only a part of the students in the university is allowed to enter these sites, controlling these sites becomes easier.

HOUSES

As time passes, burglary increases. To prevent our homes from burglary some precaution must be taken more than keys. By electronic systems, homes can be protected more easily. If an undefined user is recognized, doors will not be opened and also it reports any force attempts. Also some alarm sounds are very useful to inform other people in case of a burglary. In a home system, there is no need to a lot of groups one group is enough. Reporting force attempts and burglaries are more important.

2.2 User Profiles

WARDEN will have two user categories which are admin and ordinary user.

Admin will be able to use the master computer. He will be responsible of identifying new cards and users to the system. Identified users can be grouped. Admin will arrange the permissions of the ordinary users. He can attach permission for every user separately or attach permission for a group. A user or a group can be updated or deleted anytime. Admin will have the ability of tracing the event logs of the doors. System can be shut down or restarted by the admin also. Lastly, admin will have a system card for the readers on the doors to open or close the system in case of a network connection failure.

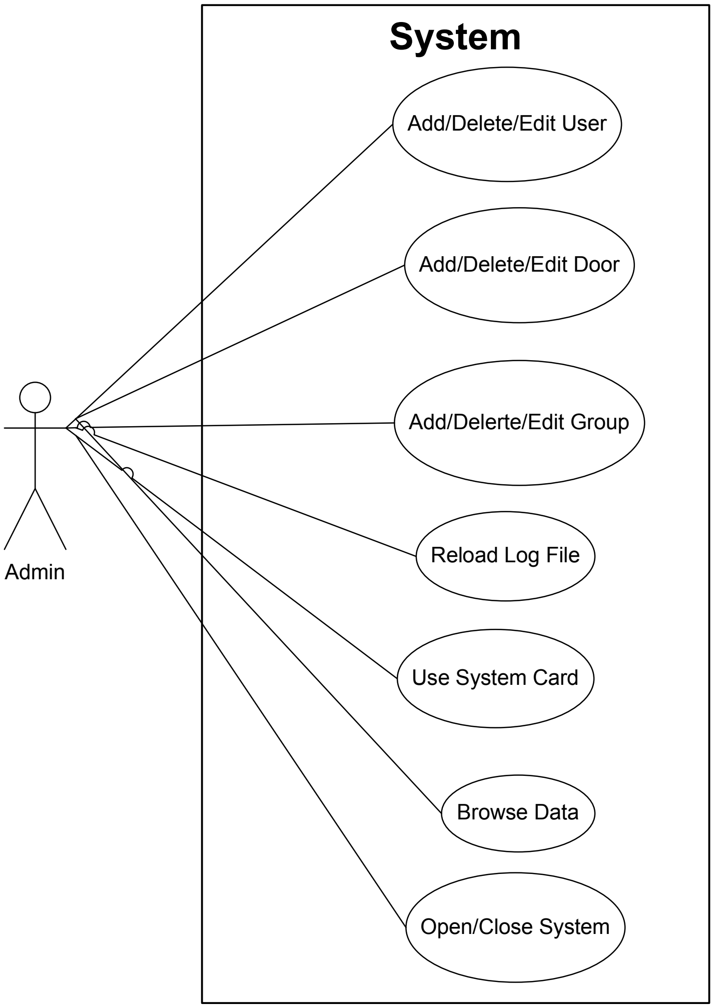


Figure 3 – Use Case Diagram of Admin

Ordinary users will be given cards that will be used to open the doors. User will get this card read to the card reader on the doors to open it.

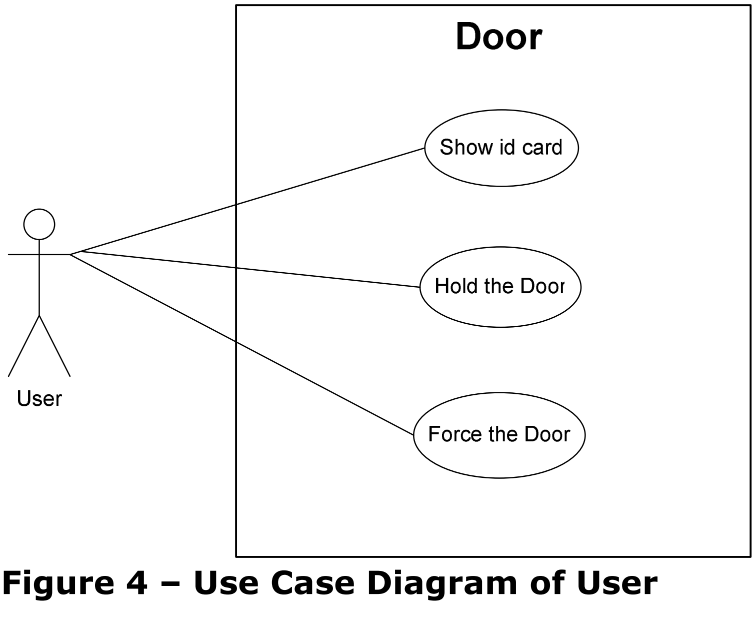


Figure 4 – Use Case Diagram of User

2.3 Usage Scenarios

In our system user can only open door by showing the card, when user shows its card to proximity reader. Card info is controlled by system. If card info is valid door is opened else a warning sound is given.

Most important mission belongs to admin in our system. Admin is able to add, remove and edit doors, user, also he can view logs and their statistics and print the report. Admin can add users to system via master computer graphical user interface. Also, by this interface admin can update users and doors info.

If a new user come to admin and wants card to open doors. Admin chooses the add user menu then fills users info and give permission to user to pass through the doors. When admin adds data to system and updates local data at single computer board, user has access permission to enter the doors.

If a new door is needed to be identified to system, admin choose add door menu and fills doors info and send local data of that door to the door. After this point door allow users to pass through according to permissions.

In case of edit users or doors edit menu is chosen and new data is entered then data at doors and system is updated.

3. DATA ANALYSIS

3.1 Data Storage

We have a file system instead of a database system to increase the speed of system and to decrease used disk space. There are two main file in system, user permissions file and log file. Also there will be other files such as user information file or door information file that are stored in master computer.

User Permissions

This storage unit is on the door locally to and keeps the id of users and their cards which have permission to enter that door. Both the users' and their cards ids' are stored because this provides an extra security precaution. When a card is read, the permission of the user is checked locally from this file. This increases the system speed and reduces the waiting time of the user when compared with doing this checking from the master computer.

As the memory on the door is very limited and speed is a very important performance concern, this storage unit will be a hash file. The student ids will be hashed according to their remainders when divided by 101 (prime number nearest to 100).

Log Store

This storage unit will keep the logs of the events. This database is kept in case of a tracing request from admin. When an event occurs on a door, this is reported to the master computer. This report will include student id (if has), operation, event time and location. The reports from all of the doors will be joined together on the master computer and a log file for the system will be kept. This file will be a linear one. The logs will be ordered according o their event time. Tracing the logs will be provided by observing this file.

In case of a crash in the master computer, every door will keep a certain amount of its own logs. When the master computer is restarted, these files will be loaded from the doors and appended to the log file of the master computer. The files on the doors will have a circular structure. When the maximum amount of logs reached, the incoming log will overwrite the oldest one.

Record example of a Log Store File,

ID	Operation	Door	Time	Date
1250133	F	multimedia	15:33	04.11.2004

Master Data Store

This storage unit keeps the user information, user groups and the doors on the master computer. The user information file will have the information of the identified users and their permissions on the doors. The local user permission files will be updated from this file. Another file will keep the user groups and its members. Lastly, a file will keep the information about the doors.

3.2 Data Flow Model Diagrams (DFDs)

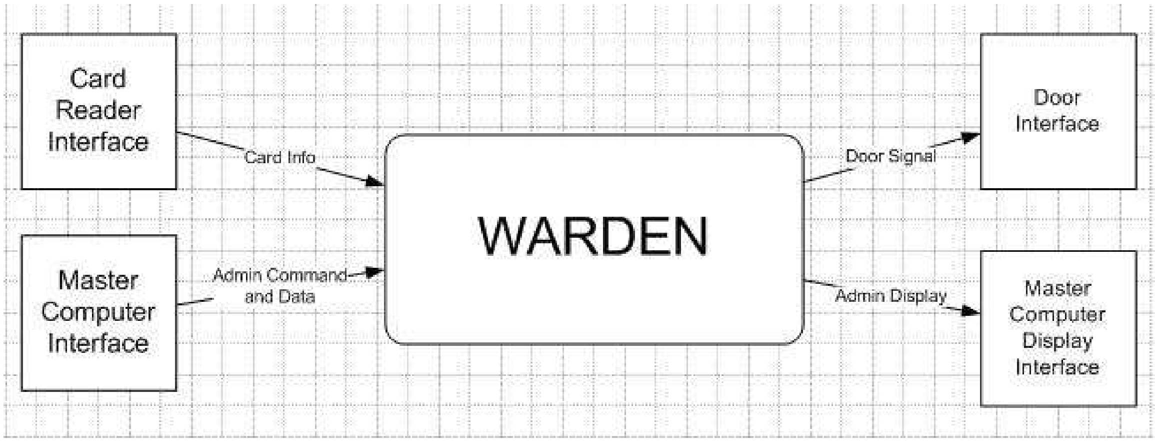


Figure 5 - DFD (Level 0)

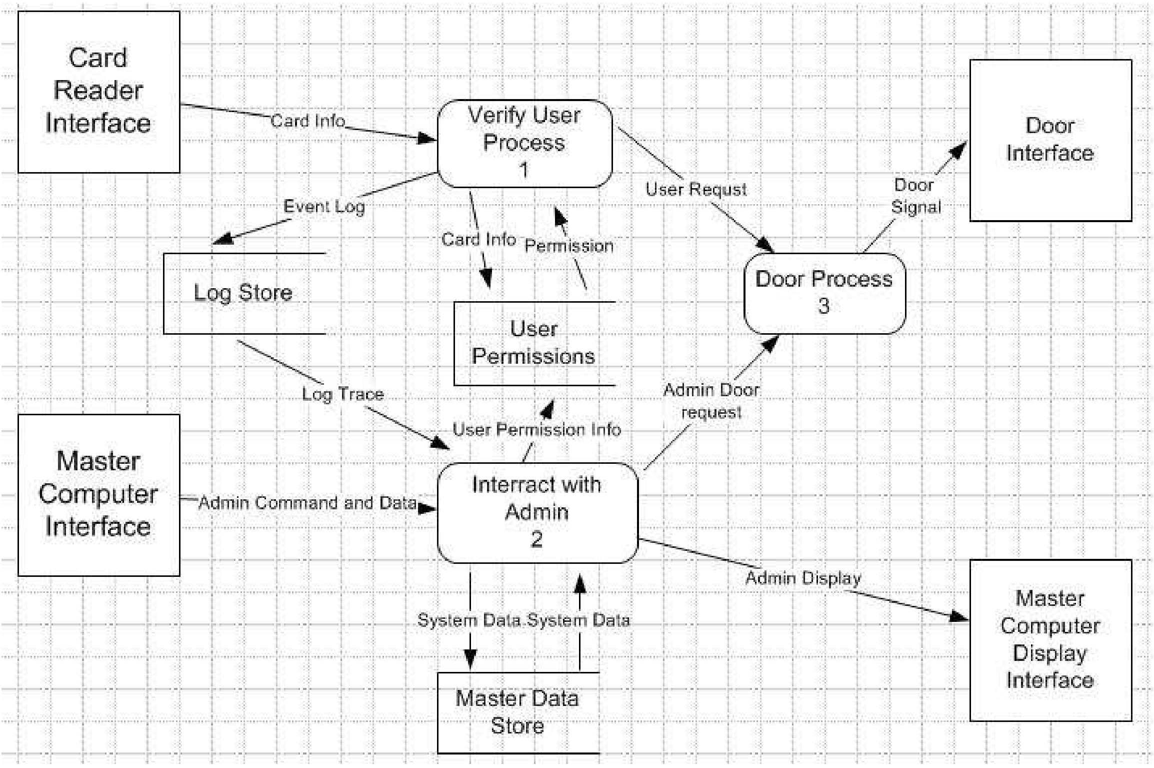


Figure 6 - DFD (Level 1)

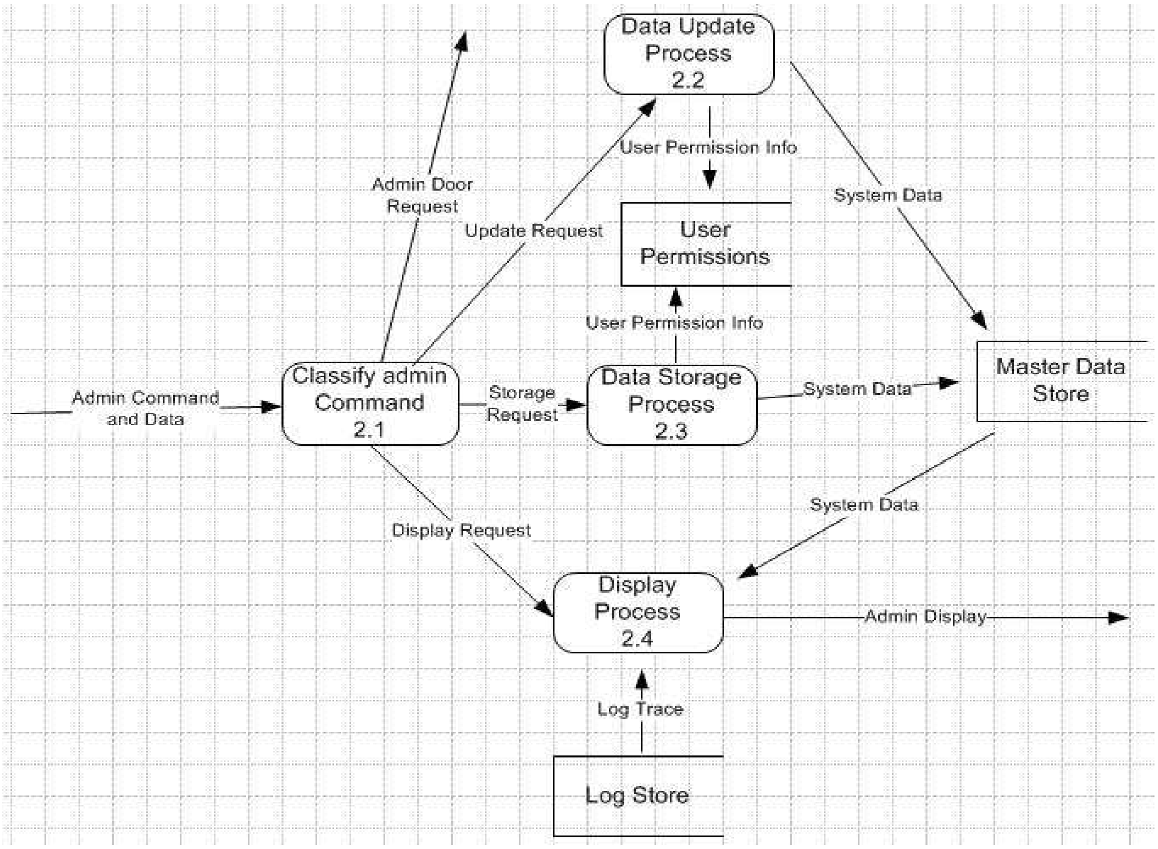


Figure 7 - DFD (Level 2)

3.3 Data Dictionary

Name:	Card Info
Aliases:	none
Where used/how used:	output from - Card Reader Interface input to - Verify User Process 1 output from – Verify User Process1 input to – User Permissions
Description: Card Info will be composed of the card id and user id. The card can be a user card or a system card.	

Name:	User Request
Aliases:	none
Where used/how used:	output from – Verify User Process1 input to – Door Process 3
Description: User request is an output defining the event on the reader. It can be a confirmed access, force attempt or a system card request.	

Name:	Door Signal
Aliases:	none
Where used/how used:	output from – Door Process 3 input to – Door Interface
Description: Door signal tells the door what to do. It can be open, restart, sleep or sound alarm.	

Name:	Event Log
Aliases:	none
Where used/how used:	output from – Verify User Process1 input to – Log Store

Description:

Event log is a sentence telling a current event on the door. It is composed of user id, event time and location.

Name:	Permission
Aliases:	none
Where used/how used:	output from – User Permissions input to – Verify User Process1

Description:

This data includes the entrance permission of the user on the door to which he get his card read.

Name:	Admin Command and Data
Aliases:	none
Where used/how used:	output from – Master Computer Interface input to – Classify Admin Command 2.1

Description:

This data is composed of what the admin wants to and the arguments of his request. In the Classify Admin Command, the request part of this data will be cut and by looking at it the remaining part will be sent to the related process.

Name:	Admin Door Request
Aliases:	none
Where used/how used:	output from–Classify Admin Command 2.1 input to – Door Process 3
Description: This data is defining the request of the admin on the doors. It can be a shutdown or restart request.	

Name:	Update Request
Aliases:	none
Where used/how used:	output from–Classify Admin Command 2.1 input to – Data Update Process 2.2
Description: This data is composed of the data that will be updated and its type. It can update the doors, users or groups.	

Name:	Storage Request
Aliases:	none
Where used/how used:	output from – Data Update Process 2.2 input to – Data Storage Process 2.3
Description: This data is composed of the data that will be stored and its type. It can store new doors, users or groups.	

Name:	Display Request
Aliases:	none
Where used/how used:	output from–Classify Admin Command 2.1 input to – Display Process 2.4
Description: This data is composed of the data that will be displayed and its type. It can display the doors, users or groups.	

Name:	User Permission Info
Aliases:	none
Where used/how used:	output from–Classify Admin Command 2.1 input to – User Permissions
Description: This data is composed of the system users' information and their permissions on the doors.	

Name:	Log Trace
Aliases:	none
Where used/how used:	output from – Log Store input to – Display Process 2.4
Description: This data is composed of event log sentences composed of user id, event time and location.	

Name:	Admin Display
Aliases:	none
Where used/how used:	output from – Display Process 2.4 input to – Master Computer Display Interface
Description: This data is composed of the data that will be displayed to the admin. It can be users, their permissions, doors or groups.	
Name:	System Data
Aliases:	none
Where used/how used:	output from – Data Update Process 2.2 input to – Master Data Store output from – Data Storage Process 2.3 input to – Master Data Store output from – Master Data Store input to – Display Process 2.4
Description: This data can be user information, user permission, user group or information of a door.	

3.4 Process Specification

Verify User Process (1): This process makes a user validation on the doors. The card id and user id are checked from the local database. If the user has the permission to enter, then an *open request* is sent. If the card is the system card, a *restart request* is sent. If the incoming signal reports a force attempt, a *sound alarm* is requested. The log of the event is also stored in the data store.

Classify Admin Command (2.1): The command of the admin is classified here. When an update command is received, incoming update arguments are sent to Data Update Process for instance. The processes that get input from Classify Admin Command are: Data

Update Process, Data Storage Process, Display Process and the Door Process.

Data Update Process (2.2): This process makes updates for user information, user permission, user group or information of a door. The updates for user and door information are done on the master computer’s storage system. Updates for user groups and individual user permission will affect the data storage of both the master computer and the doors. After a group or an individual permission is updated, the user file of the master will be updated first. Then the doors will get their own permission lists to update their local permission files.

Data Storage Process (2.3): This process stores new instances of user, user group and information of the doors. When a new door is installed, the permissions of the users will be updated both on the master and local data stores by adding a new permission for the new door. When new groups are defined, they will be stored in the data store of the master and then user permission stores of both he master and the doors will be rearranged according to the permissions of the new groups. If new users are defined, again user permission stores of both he master and the doors will be rearranged.

Display Process (2.4): This process prepares the corresponding display output for the incoming display request. Any data stored in the system database can be the display output. Log tracing will be provided by this process.

Door Process (3): The requests of the users and the admin for an event on the doors are handled here. According to the incoming request, the suitable signal is sent to the door interface.

4. REQUIREMENT SPECIFICATION

Our project warden is a composed of 6 components.

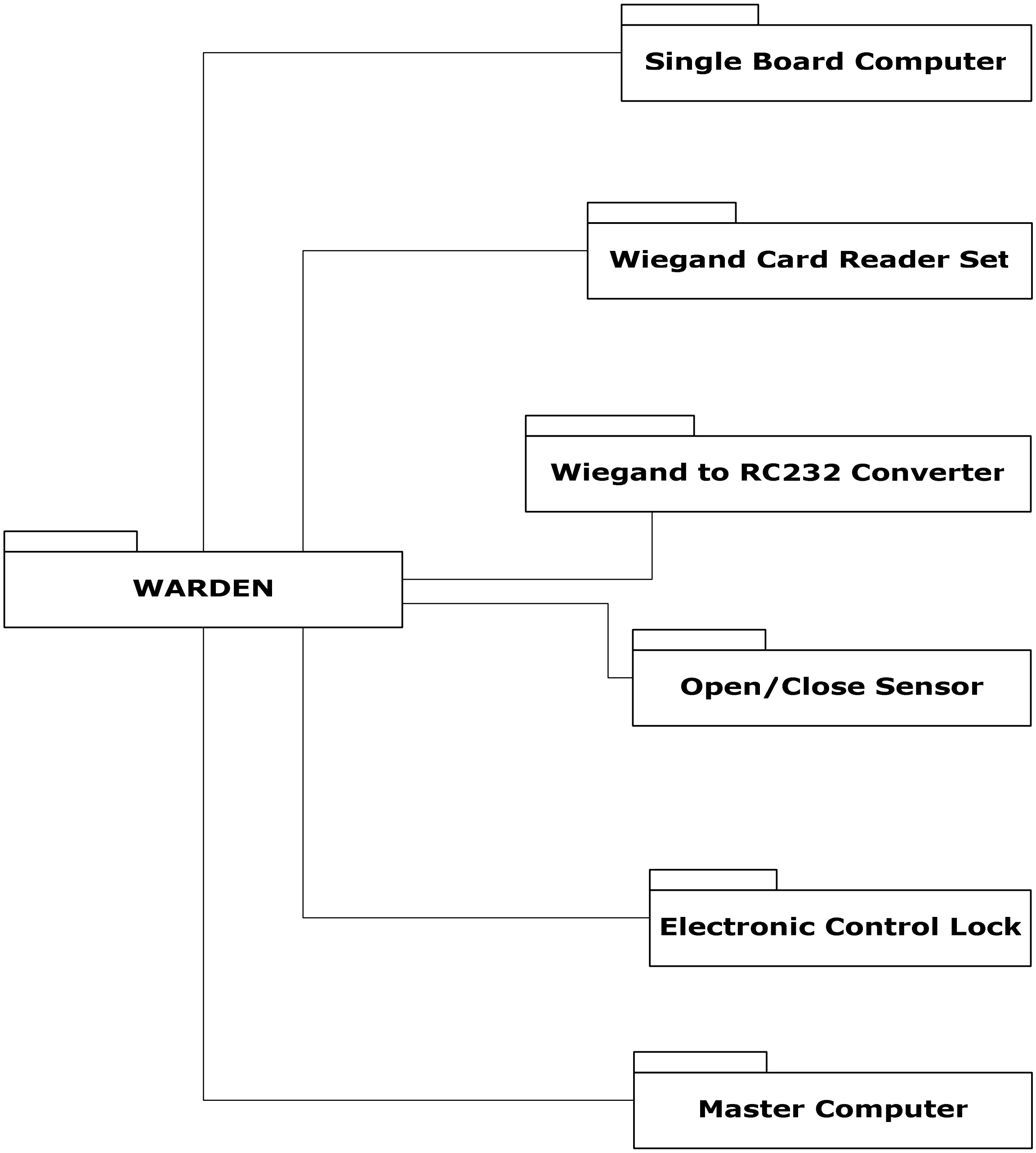


Figure 8 - Component Modelling Diagram

4.1 Single Board Computer

This component is the most important part. It includes a main board and other hardware. The specifications are below:

- VIA ATX Main Board
- Processor
- RAM (128 MB)
- Portable Hard Disk (Flash Disk, etc)
- WiFi Ethernet Card

We are waiting for the hardware parts. The exact cost is not announced, but the estimated cost is 300 $.

The other part of the component is the software. We need an operating system, the driver of the Ethernet card and the embedded program. The operating system will be Linux based, the driver will be chosen for Linux. The embedded application is developed by our company.

4.1.1 Embedded Application

The state chart diagrams of embedded application are below.

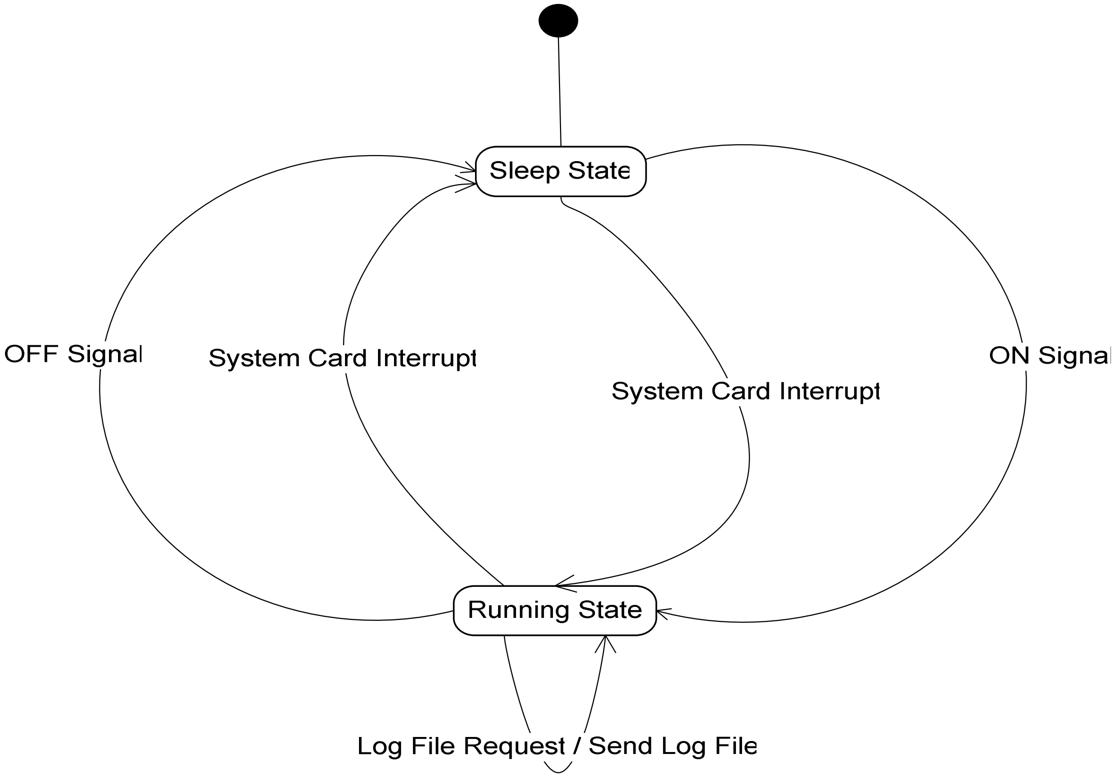


Figure 9 – Main State Chart Diagram

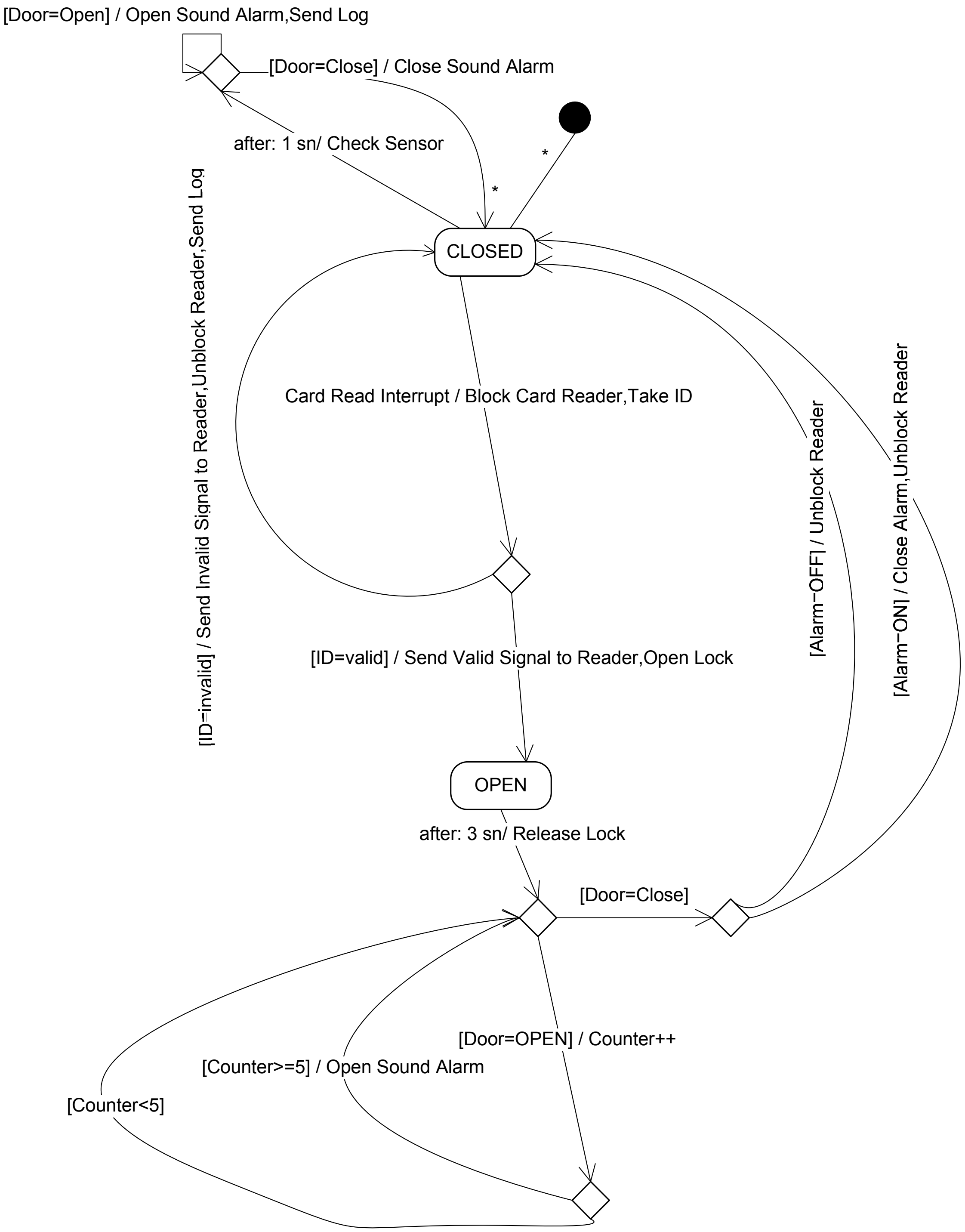

[Door=Open] / Open Sound Alarm,Send Log
[Door=Close] / Close Sound Alarm
after: 1 sn/ Check Sensor
*
*
CLOSED
[ID=invalid] / Send Invalid Signal to Reader,Unblock Reader,Send Log
Card Read Interrupt / Block Card Reader,Take ID
[Alarm=OFF] / Unblock Reader
[Alarm=ON] / Close Alarm,Unblock Reader
[ID=valid] / Send Valid Signal to Reader,Open Lock
OPEN
after: 3 sn/ Release Lock
[Door=Close]
[Door=OPEN] / Counter++
[Counter>=5] / Open Sound Alarm
[Counter<5]

Figure 10 – Running State's State Chart Diagram

4.1.2 Definition of States

SLEEP STATE

In this state, no user is allowed to pass through doors. If master computer sends a OFF Signal, all doors are locked and system starts to wait a signal to restart. System waits for a on signal, that is sent from master computer, or system card, that is defined to computer as full access card. System does not give response to other cards.

RUNNING STATE

This is the state that system works. If an ON Signal is sent to system or a system card is read by card reader in SLEEP STATE, state changes from SLEEP STATE to RUNNING STATE. In this state, system is ready to read all cards and allow users to pass through doors. When system passes to RUNNING STATE, it is in default CLOSE STATE.

CLOSE STATE

In this state, door is closed and card reader is ready to read a card. This state involves two important parts. In the first part, system checks sensor to detect any force attempt. In the second part, system reads a card and check card id to decide whether card is allowed to enter or not. If card ID is not valid then door is not opened else state changes to OPEN STATE.

OPEN STATE

This is the state to allow users to enter through door. In this state door lock is released and waits three seconds to allow user to enter. After opening the door new entry is sent to master computer as log. If door is not closed in five seconds system gives an alarm and warn users to close door to change state to CLOSE STATE.

4.1.3 Control Specification

OFF Signal:

This is the signal that is sent from master computer to doors to disable user entrance through doors. System changes its state from RUNNING STATE to SLEEP STATE by this signal.

ON Signal:

This is the event that occurs when system is restarted after SLEEP STATE. By ON Signal system starts to work again.

System Card Interrupt:

This interrupt is only way of closing or restarting system without master computer. If the system is in SLEEP STATE, it restarts the system and if it is in RUNNING STATE, it closes the system.

Log File Request:

Master computer request a signal to embedded application to send the log file.

Send Log File:

Send the log file to master computer.

Open System Order:

This is the only way of restarting computer from master computer. By Open System Order, an ON Signal is produced and system changed its state to RUNNING STATE from CLOSE STATE.

[Door=Open]:

This is the condition to show that door is open.

Open Sound Alarm:

System gives an alarm to inform users about door situation, whether it is close or not. Open Sound Alarm starts alarm signal to inform users to close door.

Send Log:

Every entry is stored in master computer as a log. By Send Log, user data that enters through a door or exists from one is sent to master computer in order to be stored.

[Door=Close]:

This is the condition to show that door is close.

Close Sound Alarm:

If door is opened and is not closed for a period, system gives an alarm. By Close Sound Alarm, this alarm signal is closed.

After 1 sn:

This is the condition to show waiting 1 second.

Check Sensor:

By Check Sensor, door status is controlled whether someone is trying to open the door without permission or not.

Card Read Interrupt:

In CLOSE STATE, system is always ready to read card. If a card is read, a Card Read Interrupt is produced to inform single board about action.

Block Card Reader:

When a card is read, system never reads a card until unblock. Disabling card reading is done by Block Card Reader.

Take ID:

When a card is recognized, its data must be read to control whether this data is valid or not. Take ID is the process that reads card ID.

[ID=invalid]:

This is the condition to show ID is valid.

Send Invalid Signal to Reader:

If card reader reads an invalid card, it sends invalid signal to reader by Send Invalid Signal to Reader to give an alert and turn back to CLOSE STATE.

Unblock Reader:

When a valid id is read, system does not read any other card until door is closed again. To disable card reading is done by Unblock Reader.

[Alarm=OFF]:

This is the condition to show that alarm is OFF.

[Alarm=ON]:

This is the condition to show that alarm is ON.

Close Alarm:

If alarm is ON, by Close Alarm is closed.

[ID=valid]:

This is the condition to show that id is valid.

Send Valid Signal to Reader:

If card reader reads a valid card, it sends valid signal to reader by Send Invalid Signal to Reader to give an alert and open the door.

Open Lock:

If a valid id is read by reader, system is invoked by Open Lock to open door.

Release Lock:

If system is opened and 3 seconds passes, system releases lock to lock the door when it is closed.

After 3sn:

This is the condition to show waiting 3 second.

Counter++:

Increment counter by one to see how many times it is tried.

Open Sound Alarm:

If door is open for a long time, system gives an alarm by Open Sound Alarm.

[Counter>=5]:

This is the condition to show that counter is equal to or greater than 5.

[Counter<5]:

This is the condition to show that Counter is smaller than 5.

4.2 Wiegand Card Reader Set

This component is the interface of users except administrators. There are Wiegand ID cards and two Wiegand card readers in this set. However, Wiegand is not the most secure technology; we choose it. The reasons are cheap card and reader costs. This set is supplied from a company. The estimated cost is $200.

ID cards hold the users' ID data electronically. By this ID data each user is distinguished form others. One card reader is needed for one side of the door and the other one is for the other side. Both readers have a beep sounder and a led. The card readers have a protocol named Wiegand and must have connection with the single board computer component.

4.2.1 Wiegand Output Protocol

The Wiegand protocol (26 bit mode) itself is made up of a leading even parity bit (for b0 - b11), 24 bits of data (from transponder data) and a trailing odd parity bit (for b12 - b23). The 36 bit mode has the same format except 34 bits are used to form the data sequence.

For example:

```
H4001 tag data (Hex):        04 60 22 12 75
Wiegand 26 bit sequence:   E (b0 --------- b11) (b12 -------- b23) O
                           E (0      4      6      0      2      2) O
                           1 0000  0100  0110  0000  0010 00101
```

Where E is EVEN parity bit for bit 0 to 11 and O is ODD parity bit for bits 12 to 23.The physical Wiegand protocol is asynchronously transmitted as low going 50 mS pulses on the appropriate DATA low or DATA high pins. These pulses are separated by 2mS periods.

4.2.2 Wiegand Protocol Timing Diagram

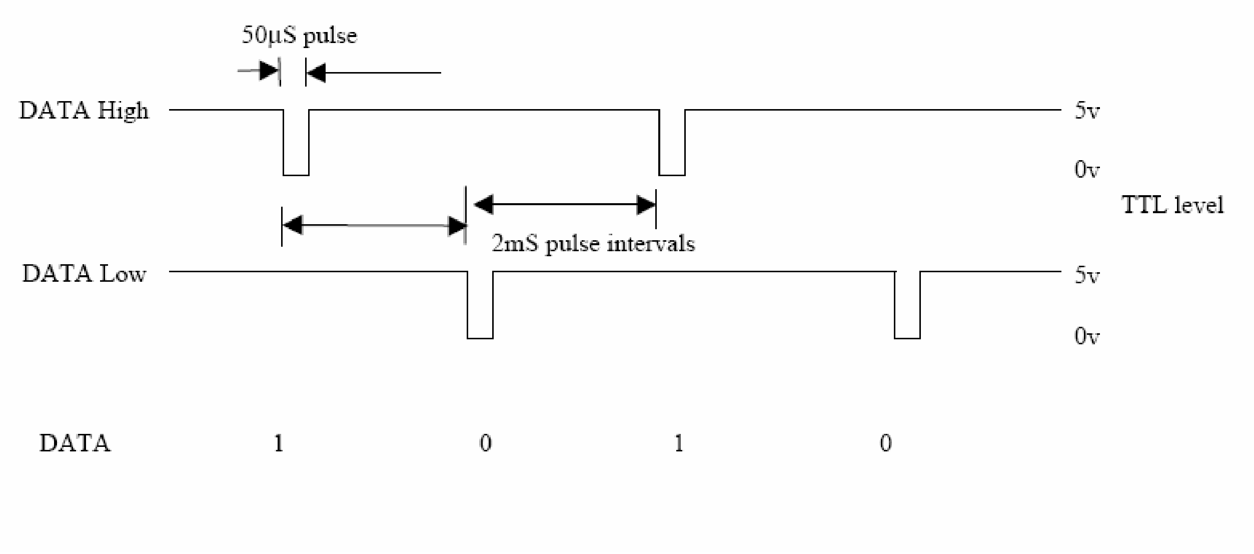


Figure 11 - Timing Diagram

4.3 Wiegand to RS232 Converter

This component is composed from just a circuit. However it seems so simple; it may be the most difficult component for us, because we don’t have a personnel having hardware experience. The aim of this circuit is converting the Wiegand protocol to RS232 data signal.

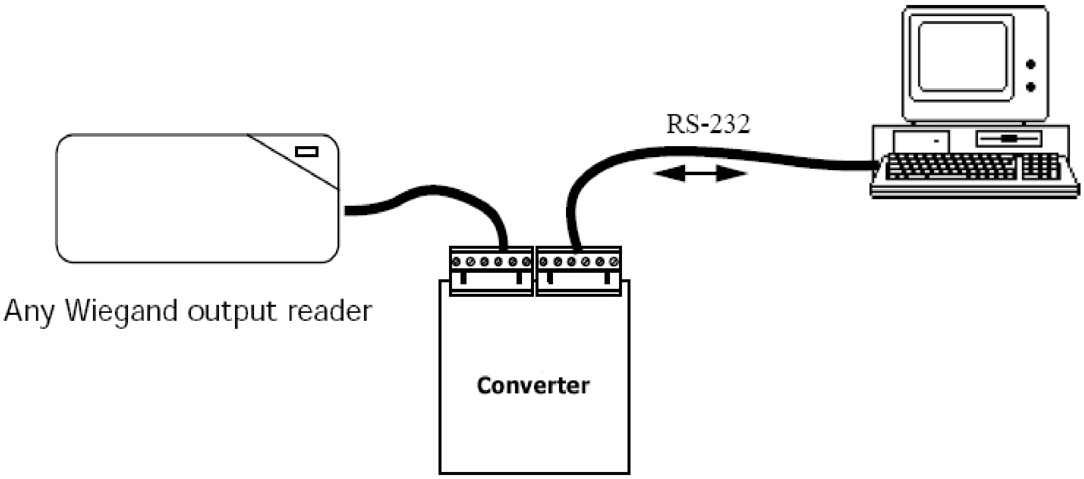


Figure 12 – Role of Converter

4.3.1 RS232 Protocol

RS232 is an asynchronous serial communications protocol, widely used on computers. Asynchronous means it doesn't have any separate synchronizing clock signal, so it has to synchronize itself to the incoming data; it does this by the use of 'START' and 'STOP' signals. The signal itself is slightly unusual for computers, as rather than the normal 0V to 5V range, it uses +12V to -12V.

Current usage of RS232 states that, data is transmitted in groups or characters of 7 or 8 bits. Each character is preceded by a start bit that must be 0 and is followed by at least one stop bit that must be a one. And also we have parity bit and it is optional. The parity may be odd, even or may not be present.

Examples:

1-)

Let’s send “troy” string by rs232. We choose 8 bit data and even parity.

00010101011001001110010111101100101001111011

So, these bits are sent by left to right.

2-)

There is another example with diagram for sending 0100111. As you can see in this example we don’t use parity bit and we choose 7 bits data.

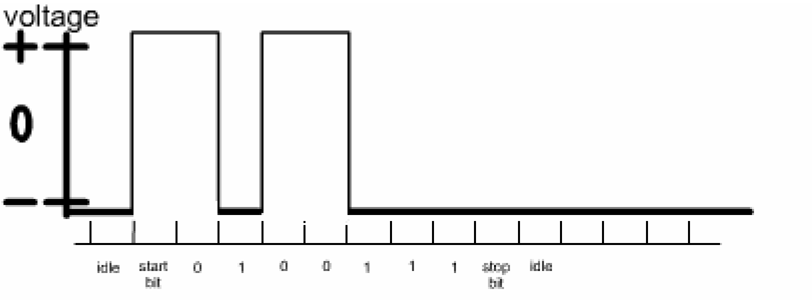


Figure 13 – Bit Sequence of 0100111

4.3.2 General View of Converter

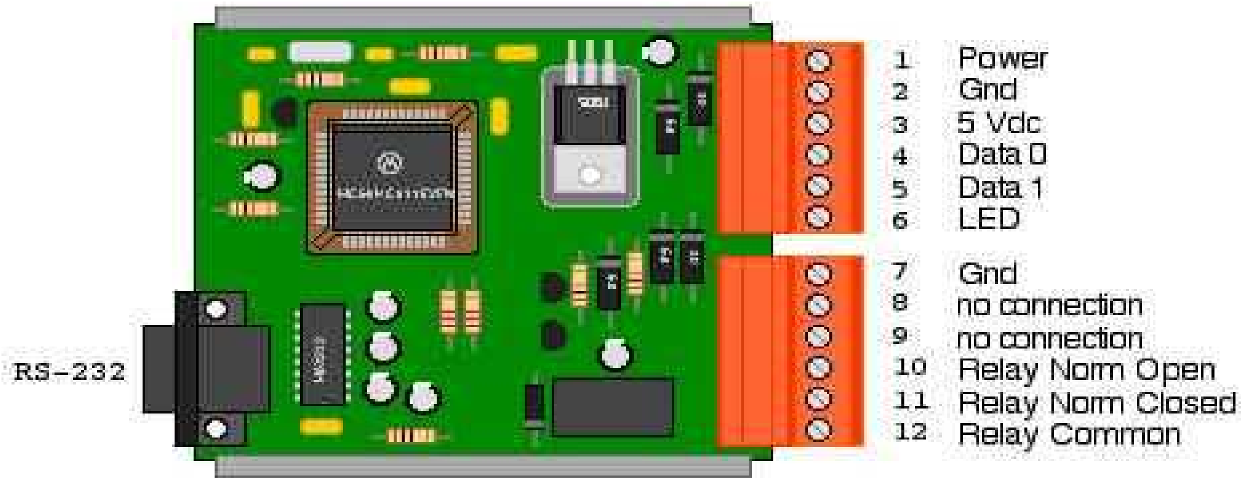


Figure 14 – Converter Circuit Schema

Figure 14 is an example schema of a Wiegand to RC232 converter [3]. Our aim is designing this kind of a circuit which does the job in diagram 2. According to the analysis of the circuit we need the bellows:

- Resistances
- Diodes
- Power transistors
- Transistors
- Capacitors
- Op – amp
- Microprocessors
- RS232 port
- Wiegand data port

Data low and Data high pins of proximity reader are connected to the Data 0 and Data 1 pin of converter circuit schema. Power and 5vdc are connected by power supply. And the out of converter which is the RS232 port is connected to the single board computer.

4.4 Open/Close Sensor

A door sensor can serve two purposes. First is for access control, the door sensor provides an extra level of security, in the following way. If the lock release time is set to, say, 10 seconds, it is quite possible for someone to pass through the door in only two or three seconds after using their card. This leaves seven or eight seconds of 'un–expired' time, during which (if no door sensor was fitted) the door could still be opened. However, if a door sensor is fitted, then as soon as the door opens the lock release is de-energized and the door re–locks as it close.

Second is for access monitoring, having a door sensor fitted means that all occurrences of the door opening and closing can be monitored. Also, a relay can be set to operate – and thereby sound an alarm – if a door opens when it shouldn't (i.e. the access control system had not released the lock), or stays open for too long.

Open/close sensor needs a power connection and must communicate with the single main board. The sensor will be supplied from a company. Its estimated cost is 30$.

4.5 Electronic Control Lock

As magnetic locks are not suitable for our system, electronic lock system will be used for controlling the door. This system needs a power supply and a connection with the single board computer. This component will be supplied from related companies and the estimated cost is 300 $.

4.6 Master Computer

The computer will used for controlling all door systems after installing the software. Master computer must have a connection with all single board computers, so doors. For these connections and to install our software minimum system requirements are:

- PC Pentium 200 Mhz
- 256 MB RAM
- 5GB hard disk space
- VGA monitor
- WiFi Ethernet reader
- Windows 98/ME/NT/2000/XP
- Mouse or tablet
- CDRW or network connection for back up purposes

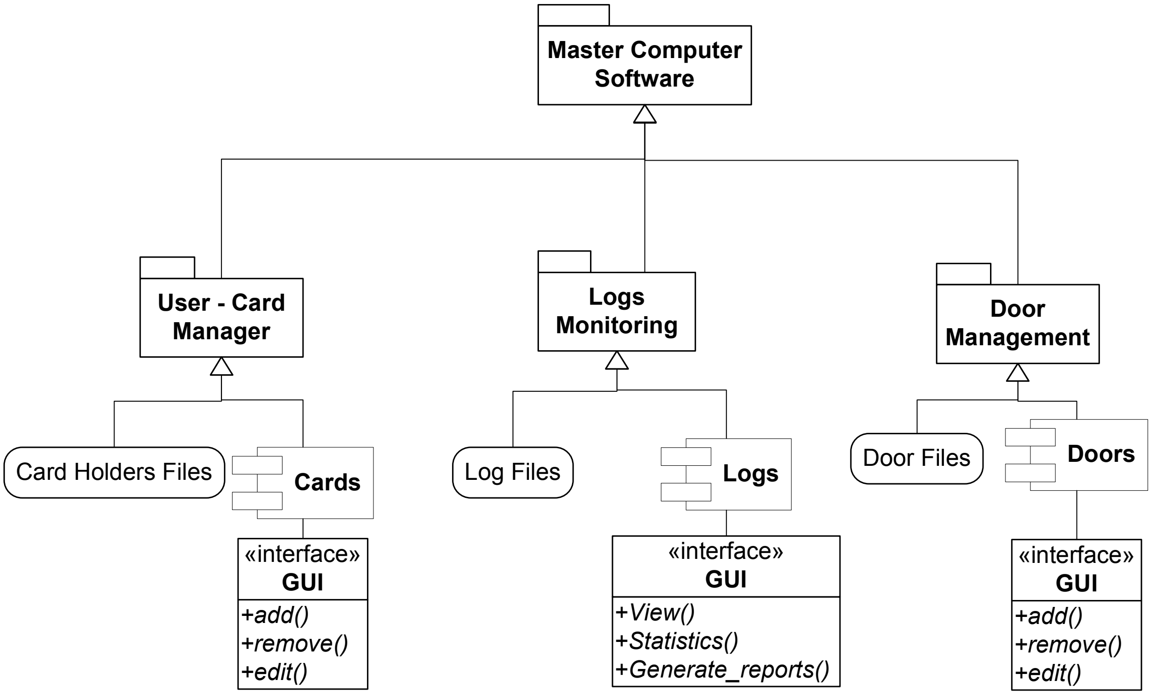


Figure 15 - Component Diagram of Master Computer Software

This diagram shows the component of master computer software. It is used by system admin. There are three packages;

User Card Package: This package is used for managing users. System admin can add user and card information belonging to him by using GUI. System admin can also edit and remove user.

Logs Package: Master computer store the all entrance time, user id, and card id of users by logs. And also this information can be seen by system admin. System admin can view some statistics about logs. For example system admin can view day of time and number of entrance relation diagram. And also system admin can take report about logs.

Doors Package: Warden System can work for any number of doors. So, system admin can add doors to the system by entering door property by using GUI. System admin can choose the number of proximity reader of door. It can be one or two. And system admin can also remove doors and edit door property by using GUI.

5. ESTIMATION

5.1 FP BASED

Information domain value	Opt.	Likely	Pess.	Est. Count	Weight	FP count
# of inputs	7	5	3	5	4	20
# of outputs	3	2	1	2	5	10
# of inquiries	9	6	3	6	5	30
# of files	4	3	2	3	10	30
# of external interfaces	2	1	2	2	7	14
						104

Factor	Value
Backup and recovery	2
Data communications	5
Distributed processing	3
Performance critical	2
Existing operating environment	2
Online data entry	3
Input transaction over multiple screens	0
Master files updated online	0
Information domain values complex	2
Internal processing complex	3
Code design for reuse	1
Conversion /installation in design	2
Multiple installations	0
Application design for change	1
TOTAL	**26**

Complexity adjustment factor = 0.65 + 0.01* TOTAL

= 0.65 + 0.01*26

= 0.91

FPestimated = Count Total * Complexity adjustment factor
= 104 * 0.91
= 94.64

We will use C++ so that LOC/FP is 64.

LOC = 94.64 * 64
= 6056 lines of code
KLOC = 6

We use Kremerer Model.

E=60.62*7.728*10-8 *FP3
=3.97 people per month

5.2 LOC - Based Estimation

We use Bailey-Basili Model

E = 5.5 + 0.73*(KLOC)1.16

= 18.33 person-month

We use Waltson-Felix Model

E = 3.2*(KLOC) 1.05
= 20.99 person-month

5.3 Estimation by Using COnstructive COst MOdel

The estimates for LOC are substituted into the COCOMO formula for effort and duration estimation. The basic COCOMO model is used, for which

Effort E = a $(KLOC)^b$
Duration D = c E^d

We classified our project as an embeded one. As a result the following default values are used;

a = 3.6,

b = 1.2, c = 2.5 and d = 0.32.

E = $3.6(KLOC)^{1.2}$
= $3.6(6)^{1.2}$
31 person-months

D = $2.5*(E)^{0.32}$
= $2.5 *(31)^{0.32}$
= 8 months

N = E/D
=4 people

Since we have a staff number of 4, we can finish this project in 8 months according to these calculations.

5.4 Comments about Calculations

According to COCOMO model we need 4 people and it takes 8 months with this stuff.

5.5 Cost Estimation

Our company is in techno police, so our total rent for 8 months is $25000. For documentation and software equipment we will spend $2500. And our total labour cost for 4 people is about $27500.

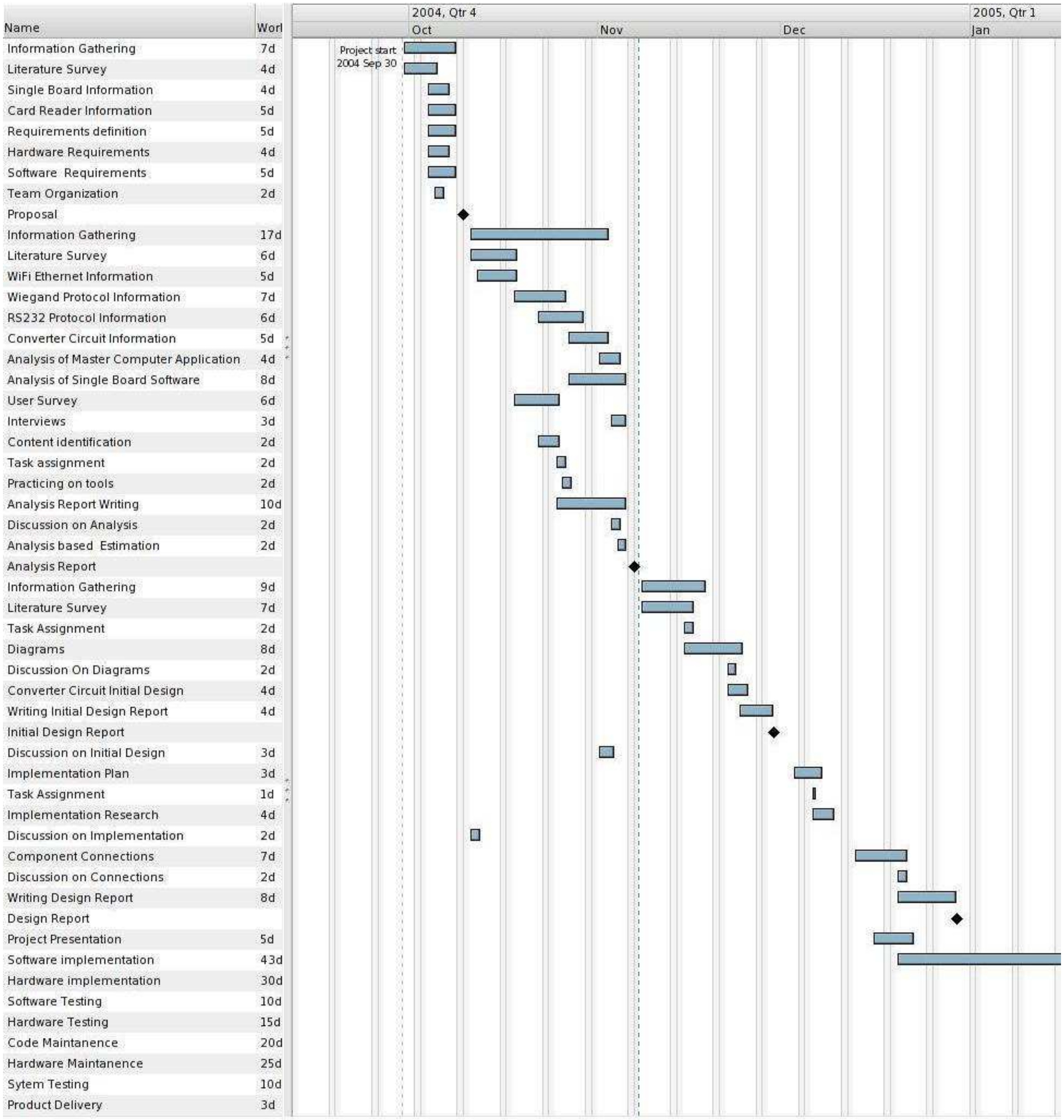
6. PROJECT DECOMPOSITION AND SCHEDULING

The information plotted on gannt chart is shown below;

Information Gathering	Sep 30 – Oct 8
Literature Survey	Sep 30 – Oct 5
Single Board Information	Oct 3 – Oct 7
Card Reader Information	Oct 2 – Oct 8
Requirements definition	Oct 2 – Oct 8
Hardware Requirements	Oct 2 – Oct 7
Software Requirements	Oct 4 - Oct 8
Team Organization	Oct 5 – Oct 6
Milestone	Oct 10 – Oct 10

Information Gathering	Oct 10 – Nov 2
Literature Survey	Oct 10 – Oct 18
WiFi Ethernet Information	Oct 12 - Oct 18
Wiegand Protocol Information	Oct 17 – Oct 26
RS232 Protocol Information	Oct 22 – Oct 29
Converter Circuit Information	Oct 27 - Nov 2
Analysis of Master Computer Application	Nov 1 – Nov 4
Analysis of Single Board Software	Oct 27 – Nov 5
User Survey	Oct 16 – Oct 25
Interviews	Nov 3 – Nov 5
Content identification	Oct 22 – Oct 25
Task assignment	Oct 25 – Oct 26

Practising on tools	Oct 26 – Oct 27
Writing Analysis report	Oct 24 - Nov 5
Discussion on Analysis	Nov 3 - Nov 4
Analysis based estimation	Nov 4 - Nov 5
Milestone	Nov 7 – Nov 7
Information Gathering	Nov 8 – Nov 18
Literature Survey	Nov 8 – Nov 16
Task Assignment	Nov 15 – Nov 16
Diagrams	Nov 14 – Nov 24
Discussion on Diagrams	Nov 22 – Nov 23
Converter Circuit Initial Design	Nov 20 – Nov 25
Initial Design Report	Nov 24- Nov 29
Milestone	Nov 30 – Nov 30
Discussion on Initial Design	Dec 1 – Dec 3
Implementation Plan	Dec 3 –Dec 7
Task Assignment	Dec 5 – Dec 7
Implementation Search	Dec 6 – Dec 9
Discussion on Implementation	Dec 10 – Dec 12
Component Connections	Dec 12 – Dec 21
Discussion on Connections	Dec 19 – Dec 21
Design Report	Dec 20 – Dec 29
Milestone	Dec 29 – Dec 30



Name	Worl
Information Gathering	7d
Literature Survey	4d
Single Board Information	4d
Card Reader Information	5d
Requirements definition	5d
Hardware Requirements	4d
Software Requirements	5d
Team Organization	2d
Proposal	
Information Gathering	17d
Literature Survey	6d
WiFi Ethernet Information	5d
Wiegand Protocol Information	7d
RS232 Protocol Information	6d
Converter Circuit Information	5d
Analysis of Master Computer Application	4d
Analysis of Single Board Software	8d
User Survey	6d
Interviews	3d
Content identification	2d
Task assignment	2d
Practicing on tools	2d
Analysis Report Writing	10d
Discussion on Analysis	2d
Analysis based Estimation	2d
Analysis Report	
Information Gathering	9d
Literature Survey	7d
Task Assignment	2d
Diagrams	8d
Discussion On Diagrams	2d
Converter Circuit Initial Design	4d
Writing Initial Design Report	4d
Initial Design Report	
Discussion on Initial Design	3d
Implementation Plan	3d
Task Assignment	1d
Implementation Research	4d
Discussion on Implementation	2d
Component Connections	7d
Discussion on Connections	2d
Writing Design Report	8d
Design Report	
Project Presentation	5d
Software implementation	43d
Hardware implementation	30d
Software Testing	10d
Hardware Testing	15d
Code Maintanence	20d
Hardware Maintanence	25d
Sytem Testing	10d
Product Delivery	3d

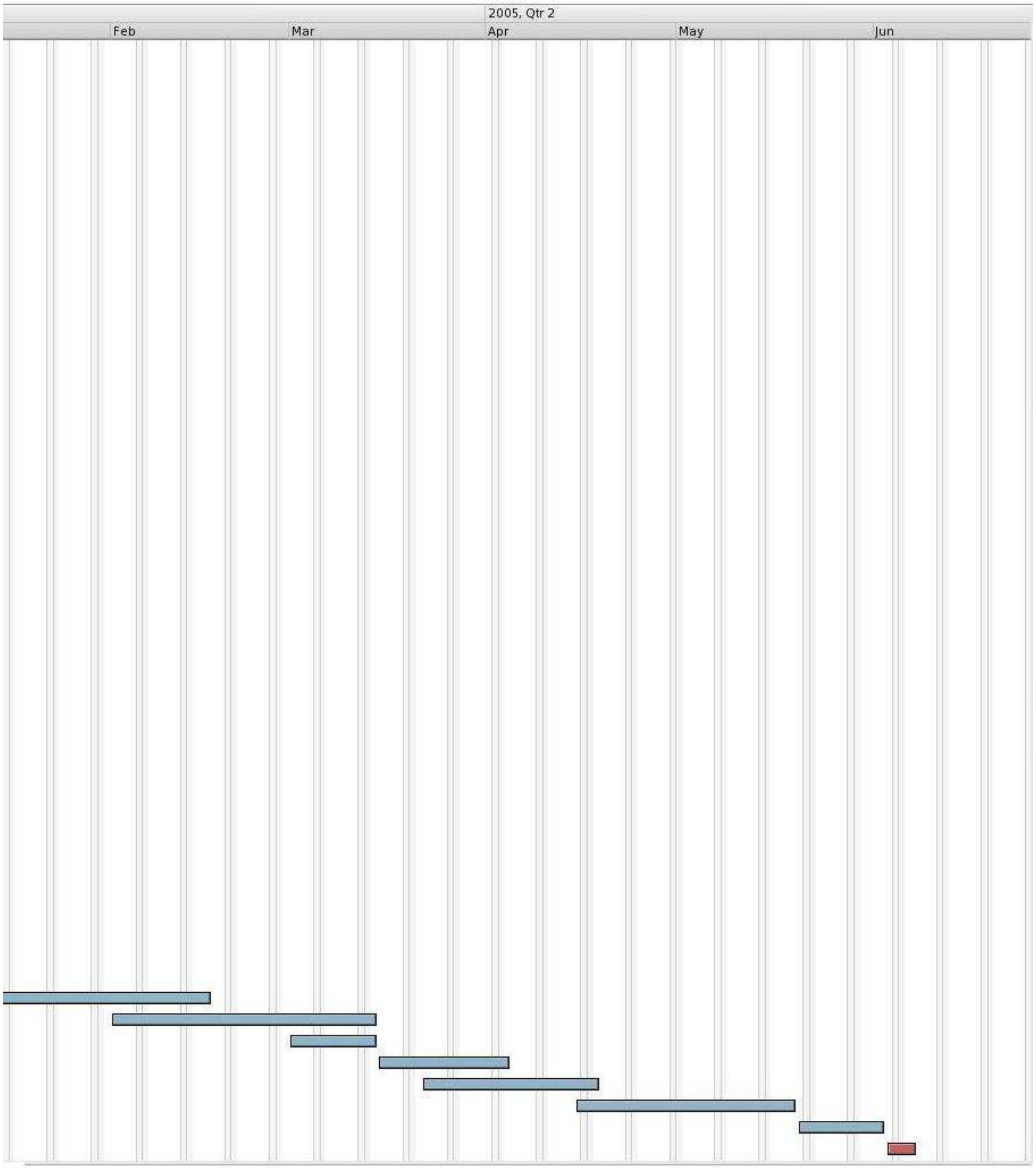


Figure 16 – Gantt chart

7. RESTRICTIONS, LIMITATIONS AND CONSTRAINTS

The system has to use only 128 MB at single board computer. For this reason, system must use as less memory as possible at single board computer.

This system uses wireless network to communicate with master computer and must response user cards as quickly as possible. To response quickly, user data will be hold locally at single board computer and it must be as small as possible because memory of single board computer is not big enough to hold all user data, also user data except user id and card id are useless for deciding user permission.

System can have some problems about communication via wireless network also. Handshaking will be used and in some situations this can produce some unwanted conditions such as can not see master computer or door single board via wireless network.

As project engineers we have some other projects so time management can be a problem some delay some occur.

8. REFERENCES

[1] Security Door Controls (SDC), http://www.sdcsecurity.com

[2] Millennium Entry Electronic Access Control System, http://www.kaba-ilco.com

[3] General Technical Information on the Wiegand to RS-232 Converters, http://www.cypresscom.com/tech/Converters/cvt2xxx.htm