MINISTRY FOR DEVELOPMENT OF INFORMATION TECHNOLOGIES AND COMMUNICATIONS OF THE REPUBLIC OF UZBEKISTAN
TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

Allowed to defense
Head of «IS» Department
Irgasheva D.Y. _____
«___» _____ 2015

Final work

on theme: *"Development of software part of Access Management Control System for interprise"*

Graduate _____ *Barotov X.B*

Supervisor _____ *Karimov M.M.*

Life safety consultant _____ *Borisova Y.A.*

Reviewer _____ *Xasanov X.P.*

Tashkent – 2015

TABLE OF CONTENTS

INTRODUCTION

In conformity with the decree of the President of the Republic of Uzbekistan dated June 27, 2013 DP-1989 "On measures for further development of national information and communication system of the Republic of Uzbekistan". There were approved projects and activities for the development of e-government in the Republic of Uzbekistan in the period from 2013 to 2014, which set in front of public authorities a number of key tasks for the establishment and mutual integration of information systems, automation of government agencies that improve the efficiency and quality performance of their functions [1]. Accordingly, the research paper offers development of the software based on client-server architecture designed security systems that can be used to automate the system of access to classified objects.

One of the areas of information security at the enterprise or organization is an engineering and technical protection, under which is in use card access control. Accordingly, in the majority companies where it is necessary to monitor and limit the access of people in different areas, automated control access systems (CAS) found its wide application. These systems designed to provide authorized passage within protected areas zone. In addition to its core functions of providing access to a resource, access control helps to solve many other tasks. This includes time tracking, rapid determination of the location of employees, management elevators, ventilation, fire alarms and more.

Today, the main focus of monitoring and access control is their intellectualization, the transfer of the maximum possible number of functions the collection, processing of information and decision-making, hardware security systems computers. Liberation of human routine work is especially important in security facilities where the cost of failure and sometimes-elementary carelessness is very high. On the other hand, it is important to provide the operator a full and accurate information on the events taking place at the facility and convenient means for error-free and timely operational decisions [3].

However, the access control system can be used not only to reduce costs of the enterprise in the organization of the security system. They are used and as a marketing automation in hotels, resorts and so on. In this case, access to various premises is regarded as a paid resource that allows us to speak about such a system as an automated marketing management system. A special feature is the implementation of these security systems the mechanism of settlement of system users with its owner with his or her affiliation.

The purpose of current final work is to develop a flexible control system software and control of access to a room or premise for its implementation in enterprise, supports calculation scheme user customers with the owner of CAS. Under the software is understood here the organizational structure of the system namely based on client – server architecture with appropriate specially designed hardware as well, which includes the separation of the system, Communication between these parts, the mechanisms of interaction and basic principles projection system.

Relevance of the topic. The current CAS are too specialized. For example, in some systems, not enough supported functions regarding user records. Therefore, faced with the problem of development of a such user recording system that would comprehensively solves all problems concerning user access to certain premises. Integrated design system will solve all occurring in its implementation security problems.

To achieve this goal it is necessary to solve the following tasks:

– Carry out an analytical study of access control systems, and on its basis carry out the construction of the domain model;

– Develop, implement and server and client software, a set of mechanisms to ensure execution of requirements for system access;

– The architecture of the system modules on the basis of established mechanisms;

– Conduct a comprehensive testing architecture, confirming the possibility of use.

The first chapter reviews the domain problem and reveal basic the concept, structure and principles of work, a classification of CAS. The second chapter devoted to explaining the choice of approaches and tools, as well as the description of the structure developing stages of a software system and domain model.

1. THEORETICAL PART. THE STUDY OF SUBJECT AREA

1.1. The composition of the AMCS

Access control system usually comprise of the AMCS or CAS server - ordinary computers that control attached to them CAS controller. The ***controller*** (control panel) - a specialized highly trusted computer, that stores information about the configuration mode of the system, a list of people who have the right to access the resource, and their access privileges, affiliation to the resource. In ordinary cases the minimum, the controller may be built into the reader, the turnstile or other locking actuator or equipment [3].

The next important link in the security systems are devices such as readers, which can be connected to the controllers. The reader is a device that allows you to read information recorded on the card. Furthermore, its needless to say that apart from reading controller is able to write a data to specified card e.g. tag if specially designed and the majority of card controllers nowadays are designed to do both tasks, reading and writing simultaneously. The information received is transmitted to the controller, which will decide on the admission of human resource. You can configure the controller so that it will request confirmation of the decision taken at the computer. Any reader assumes mate - a key identifier that contains information by which the identification of the person. Each card is assigned a certain level of access, according to which the user is authorized to access a particular resource at certain intervals. The classification keys are presented in §1.2.

To improve the reliability of identification except readers can be connected to the controller keyboard for a set of personal identification number (PIN). Another type of device that can be connected to the controller - a security panel. It is also a specialized controller that monitors the security sensors (sensors on doors, windows, interior motion sensor, etc.). If status of any sensor is changed, the information about the immediately fed to the main controller.

At the control panel can be set relay, through which it controls the actuators electromechanical locks, turnstiles, elevators, automatic doors, etc.

1.2. Methods of identification

There are two different areas in the methods of identification. Its as follows: identification using electronic cards and identification using biometrics person. Currently, the following types of cards, each of which corresponds to a certain type of reader [4]:

– magnetic cards - are read during a particular direction and at a certain speed through the slot. Magnetic stripe with written therein information is applied to one side of a plastic card. Modern magnetic strips made of materials that require strong magnetic fields to write data, and responsible for its destruction, so there is no fear of accidental demagnetization. However, magnetic cards quite sensitive to external influences of another kind - contamination, moisture, scratches. Another drawback associated with the need to refine positioning the reader. The average service life of magnetic cards is about a year, and then the magnetic layer is erased. Therefore, the magnetic card is used, usually in applications where frequent replacement is provided cards, for example, in hotels or in car parks;

– contactless radio frequency (PROXIMITY) card also called RFID tags - the most promising to date, card type. Contactless cards operate at a distance and do not require precise positioning, making them stable performance and easy to use, high throughput. To read information from a contactless card it is simple enough to bring to the reader. Reader generates electromagnetic radiation a certain frequency, and when making a coverage card reader, this radiation through an antenna embedded in the card feeds the chip card. After receiving the necessary energy to work on the card reader sends a unique identification number by means of an electromagnetic pulse defined shape and frequency. This card can be in your pocket or purse.

– wigand Cards - named after the scientist who discovered the alloy with a rectangular hysteresis loop. Inside the card are placed pieces of wire of the alloy, which, when moved past the reading head allows to read information. These cards are more durable than magnetic, but also more too expensive. One disadvantage is that, the code entered into the card during manufacture is forever.

Bar code card - is applied to a bar code. There is a more complicated variant - barcode closed material transparent only infrared light, reading occurs in the infrared region.

Touch-memory - a metal tablet in which the chip is the ROM. Touching tablet reader from the memory is sent to the controller tablets unique identifier code. Cheap enough and comfortable. Biometric identification methods include:

– scan fingerprint - fingerprint scanning is the most convenient method, as used in this device - the cheapest. It is advantageous and reliable fingerprint: unauthorized access is possible in about one in a million, and the denial of access to the authorized user to occur in about 3% of cases and is associated mostly with improper care of the scanner;

– palm geometry and hands - not scanned line, as in the fingerprint and hand geometry: the shape of the palm or wrist, finger length etc... In principle, the reliability of this method is almost as good as the previous one, but such systems take up much more space, making them difficult to use on a PC, and they cost more;

– scan your eyes - there are two types: scanning the iris and retinal scan. The first method is simpler and more convenient, but less reliable. The second is the most reliable but also the most expensive;

– identification of the voice – The advantage is ease of use. But this method has a low reliability as to the person's voice has changed significantly enough to catch a cold;

– signature - a person signs a special device such as a graphics tablet. The computer compares the received information with the written, stored in its

database, and depending on the comparison result gives access or denies it. Very easy to forge a signature, but Modern readers measure also characteristic movements of the hand when writing, which increases the reliability of the method.

1.3. Operating Principles of control access systems

The basis of the system of access control based on the principle comparisons of certain identification features, belonging to a particular person or object with the data laid down in. Each of the employees (or a student for instance) an access card or key fob containing a unique code assigned by the issuance of access cards in the office Pass. The code can be used as the biometric data of the person. When passing through the protected area or protected area data is read from the storage medium through a code reader. Information about the visitor is transferred into the system, which is analyzed and given a signal that adequately responds to the situation: <Access Granted> <Entry prohibited> <Re-run on a single card>, the output signal <Alarm> on the remote guard in violation of the protected area without the appropriate license, etc.

If necessary, the protection intervention in the situation on the computer screen guard post output alarm and instruction, which determines personnel actions in this situation. Moreover, the system can immediately respond to the alarming situation, blocking locks in the protected area and the way of passage of the access points.

For the analysis of the events it is possible to view and print the event log for a certain period of time. To eliminate the misuse of cards and tightening flow regime in particular has a number of important areas functions that allow:

– eliminate the double pass in zone one card (distinguish the possibility of blocking the passage again at a certain time - for systems that are not equipped with card readers at the exit and entrance to the ban on non-contiguous zone for full access control);

– allow access only for the 2nd card (may enter only two people met together and with appropriate powers);

– limit the number of people in the room and the area (if you exceed the threshold controller does not flow into the zone of another person);

– set the <input under duress> (imperceptibly protection an alarm);

– guard given the right to an independent decision on the authorization to proceed visitor (when reading the map is displayed on the monitor guard photograph of the holder, which is compared with the image, issued camera);

– set the meter to use the card (number of card reader on a particular reader is limited);

– establish a hidden control room (sound an alarm to the control of the penetration of the protected area and the absence of the relevant rights, and for an attacker is the discovery unknown).

1.4. AMCS Classification

Consider some important classification systems of access control. Classification by AMCS control method are:

– Independent - to control one or more devices without barring the transfer of information to a central control and without the control of the operator. Usually just the CAS, more electronic locks, which limit access to the premises. The advantages of such systems may also include the ability to easily remove the key from the room volatile memory system when it is lost, so the key finder will never be able to use it. Stand-alone systems have been used, as a rule, small objects (included in the houses, cottages, etc.).

There are also stand-alone access control system with the functions of protection.

– Centralized (network) - to control barring devices through the exchange of information with the central control-to-control (control) by the operator.

Network monitoring systems are used where continuous monitoring of the state of the object, the possibility of rapid interference in the operation of the system and preparation of various statistics about the movement of personnel. Access control in the network system is basically carried out automatically on the basis of different object and temporal access restrictions defined for individual owners of keys and groups the owners allocated on any grounds with a special program. The operator has the opportunity to work with database users to record and edit permissions. When running the program, all events occurring in the system are displayed on a monitor in real-time and logged for subsequent reports for each user. The system provides a complete set of standard reports the movements of staff and keep a record of working time. Communication networks are already protected against intruders' hardware and software. Networked systems are optimal for use in small and medium-sized offices or enterprises (up to 256 measurement points of passage). Universal - including the functions of both standalone and networked systems operating in network mode under the control of the central control and passing in offline mode in the event of failure to network equipment, in the central device or connection is broken.

By the number of controlled access points are distinguished:

- system of small capacity (less than 16 points);
- system of medium capacity (not less than 16 and not more than 64 points);
- system of high capacity (64 points or more).

Classification by type of control objects:

- to control access to the physical environment;
- to control access to information.

1.5. Access Control systems in automation

Currently, there are widespread concept of the "Access Control" as a means of organizing the check mode on enterprise. In these systems, users are understood

as the employees of the company - owner of the ACS, and the most immediate attended to the safe access to areas and facilities. Such use ACS helps to reduce costs on a security organization. Using access control systems as a means of marketing automation pursuing several other goals: making a profit by selling opportunities access to the resource. In this sense, the system access control becomes a specialized system of marketing automation [6].

In such systems, users are understood more broadly - as both businesses and individuals. There is already an enormous importance to the organization of the mechanism of settlement of these users with the owner of ACS, which totally absence in the primary sense of access control systems, where the members were employees.

In the first case group members are claimed only as a means of more convenient access control, then in the automation, it acquires greater significance due to the introduction of the concept bills. One account can be used as a single person or a group of people (the company, the family and so on.), Moreover even a group of teams (teams association), which specifies the possibility of constructing complex hierarchies. In general understanding of the ACS as an automation system can be considered a generalization of the primary concept, as all visitors of the interaction with the system can be interpreted through the mechanism of the accounts.

Automation Systems load additional meaning and various reports generated by ACS, allowing them to produce statistical analyzes based on the demand for a resource in a particular access point. These studies can be used to tune the system to the needs of users. Access Statistics particular user or group allows effectively stimulate the loyal customers through a variety of schemes of discounts and promotions.

Using ACS offers great opportunities for the automation of the various enterprises, and other establishments that sell access to various facilities. For example, Access Control System, automates the hotel can not only reduce the costs of providing security, but also to organize the paid use of services of the company.

1.6. Features of access control systems as real-time system

By their very nature, access control systems are real-time systems (RTS). RTS, as a hardware-software system includes sensors recording events at the site, input-output, transforming sensor data into digital form, suitable for the treatment of these readings on the computer and, finally, a computer program that responds to events occurring at the facility.

Any RTS is focused on processing of external events. Its main task - is to respond in a predictable time, unpredictable flow of external events. This means that the system is supposed react to an event occurring in the facility in a timely manner, i.e. for a time critical for this event. The critical time for each event is determined by the object and the event itself, and can of course be different, but the system's response time reaction have to be predicted (calculated) in establishing the system. Absence of the reaction at the predicted time is considered an error for the real-time systems. On top of that, the system ought to have time to respond to both events. Even if two or more external events occur simultaneously, the system must have time to react to each of them during the time intervals for these critical events. There are real-time system of two types –hard real-time systems and soft real-time systems. Hard real-time systems do not allow any delay system response because [8]:

- results may be useless in case of delay;
- could occur in the event of a disaster response delay;
- cost of delay can be infinitely large.

Soft real-time systems are characterized by the fact that the response delay is permissible, and may even lead to an increase in cost results and reduce overall system performance. ACS refers to this type of systems.

In general, the main difference between the systems of hard and soft real-time can be expressed as follows: hard real-time system is never late with reaction to the event, soft real-time system - cannot be late with the response to the event. Understanding the access control system as a real-time system requires developer use a number of specific mechanisms that have a significant impact on the architecture of the whole system.

1.7. “Client-Server” system architecture preview

In information system **“Client-Server” architecture,** is an architecture of a computer network in which many clients e.g. remote processors request and receive service from a centralized server which is also known as a host computer [9]. The client computers provide an interface to permit a computer user to request services of the server and to display the results the server returns. Servers wait for requests to arrive from clients and then respond to them according to a query. Essentially, a server provides a standardized transparent interface to connected clients so that clients need not be aware of the specifics of the system (i.e., the hardware and software) that the service is providing. Today clients are often situated at workstations or on personal computers, while servers are located elsewhere on the network, usually on more powerful highly trusted machines. Appropriate computing model is especially effective when clients and the server each have distinct tasks that they routinely perform. In ACS data processing, for example, a client controller can be running an application program for entering visitors’ information and their access within a room or organization while the server computer is running another program that manages the database in which the information is permanently stored. Many clients can access the server’s information simultaneously, and, at the same time, a client computer can perform other tasks, such as sending an appropriate message or information as a query to remote or local host machine. Due to that both client and server, computers are considered intelligent devices; the client-server model is very different from the

old mainframe model, which utilized a centralized mainframe computer that performed all the tasks for its associated remote or local terminals. Having said that in information system architecture there actually two approaches are widespread for constructing ***client – server*** design architecture:

1) ***Classical approach***
2) ***Multitier architecture***

Classical approach (see fig.1.1)

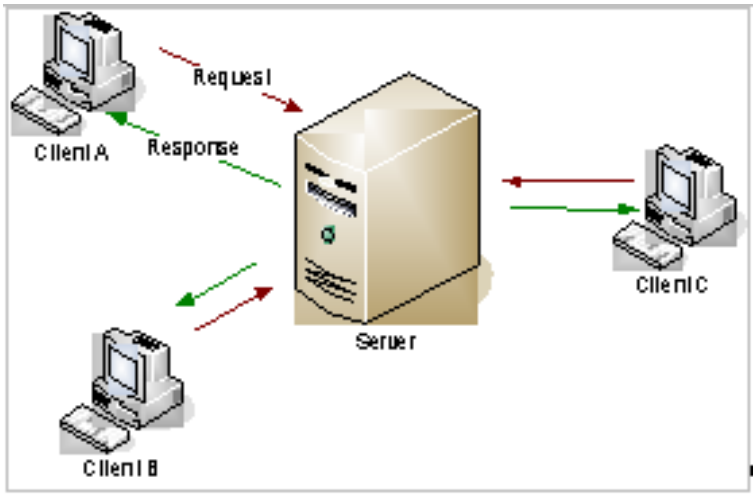

Figure 1.1. Client – Server classical approach.

As it is described in 1.1 figure, classical client-server approaches are based on a single host machine that receives query and responds to them respectively, and the client machines. The interface between the client side application and server is side application is accomplished using the protocol. The paradigm of classic client-server is the database server, in which clients communicate with the server using standardized query language e.g. SQL. However, the classic client - server admittance is not ideal solution in the majority of problem domains, due to their advantages and disadvantages.

The pros of client – server [9]:

– processing of the entire Database System for example is spread out over clients and server.

– in term of DBMS can achieve high performance because it is dedicated to processing transactions (not running applications).

– client Applications can take full advantage of advanced user interfaces such as Graphical User Interfaces.

The cons of client - server:

– implementation is more complex because one needs to deal with middleware and the network;

– It is possible the network is not well suited for client/server communications and may become saturated.

Multitier architecture (see fig. 1.2.)

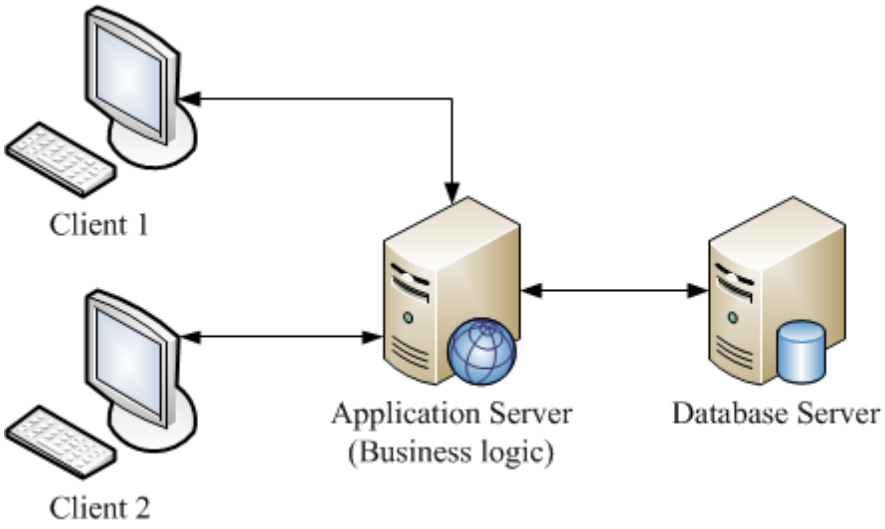

Figure 1.2. Multitier client - server architecture

In software engineering**, *multi-tier architecture*** (often referred to as *n*-tier architecture) is a client–server architecture in which presentation, application processing, and data management functions are physically separated. The most widespread use of multi-tier architecture is the three-tier architecture see figure 1.2.

N-tier application architecture provides a model by which developers can create flexible and reusable applications. By segregating an application into tiers, developers acquire the option of modifying or adding a specific layer, instead of reworking the entire application. A three-tier architecture is typically composed of a *presentation* tier, a *domain logic* tier, and a *data storage* tier.

Presentation layer (also known as client layer) – is a complex interface (usually graphical) components which is provided to the end user. This level should not have a direct connection to the database (for safety requirements and scalability), to be loaded with the basic business logic (requirements for scalability) and store the state of the application (according to the requirements of reliability). On this level usually imposed only simple business logic: Interface authentication encryption, checking for valid input values and compliance with the format simple data operation (sorting, grouping, counting values) already loaded to the terminal.

Domain logic layer (middle layer, adhesive layer) is located on the second level, it contains most of the business logic. Outside it there are only fragments exported to the client (terminals), as well as elements of logic, embedded in the database (stored procedures and triggers). The implementation of this component provides communication software. Application servers are designed in such a way as to add to them additional copies provided scaling performance software package and do not require changes to the application code.

Data storage layer (data layer) provides storage and data to be made on a separate level, is implemented as a rule by means of database management systems, connect to this component is provided solely with the server-level applications.

In the simplest configuration, all the components or some of them may be combined on a single computing node. The productive configurations usually a dedicated compute node to the database server or a cluster of database servers, application servers - selected group of computing nodes which are directly connected clients (terminals).

While the concepts of layer and tier are often used interchangeably, one fairly common point of view is that there is indeed a difference. This view holds that a *layer* is a logical structuring mechanism for the elements that make up the software solution, while a *tier* is a physical structuring mechanism for the system infrastructure.

1.8. Communication protocol in the respective CAS systems

As a data transfer is the major concern in CAS system, there are plenty of approaches to achieve this goal. The first approach relies on hardware chosen for CAS system, because communication is performed by not only client and server sides application but also between controller and RFID (Radio frequency identification) reader as well. Taken in account these criteria, communication protocol between controller and reader (RFID) is constructed in low level, name using SPI protocol.

Serial Peripheral Interface (SPI) is an interface bus commonly used to send data between microcontrollers and small peripherals such as shift registers, sensors, and SD cards. It uses separate clock and data lines, along with a select line to choose the device you wish to talk to [14].

In contrast, a common serial port, the kind with TX and RX lines, is called "asynchronous" (not synchronous) because there is no control over when data is sent or any guarantee that both sides are running at precisely the same rate. Since computers normally rely on everything being synchronized to a single "clock" (the main crystal attached to a computer that drives everything), this can be a problem when two systems with slightly different clocks try to communicate with each other.

To work around this problem, asynchronous serial connections add extra start and stop bits to each byte help the receiver sync up to data as it arrives. Both sides must also agree on the transmission speed (such as 9600 bits per second) in advance. Slight differences in the transmission rate aren't a problem because the receiver re-syncs at the start of each byte.

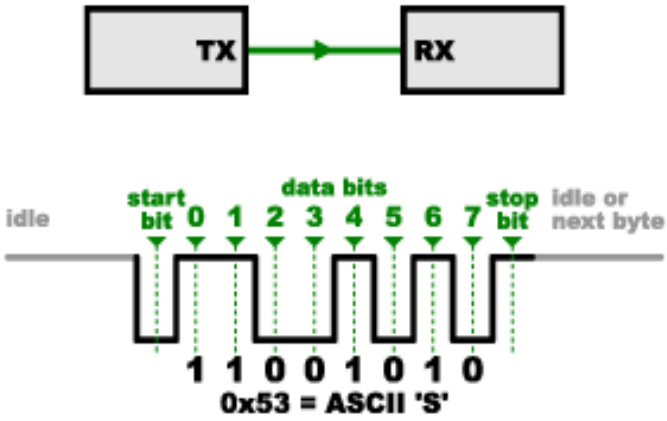

Figure 1.3. Serial port interface bits order

On top of that, as it is noticed that “11001010” does not equal 0x53 in the above diagram detail. Serial protocols will often send the least significant bits first, so the smallest bit is on the far left. The lower nybble is actually 0011 = 0x3, and the upper nybble is 0101 = 0x5.

Asynchronous serial works just fine, but has a lot of overhead in both the extra start and stop bits sent with every byte, and the complex hardware required to send and receive data. Moreover, as you have probably noticed in your own projects, if both sides are not set to the same speed, the received data will be garbage. This is because the receiver is sampling the bits at very specific times (the arrows in the above diagram). If the receiver is looking at the wrong times, it will see the wrong bits.

While, SPI works in a slightly different manner. It is a “synchronous” data bus, which means that it uses separate lines for data and a “clock” that keeps both sides in perfect sync. The clock is an oscillating signal that tells the receiver exactly when to sample the bits on the data line. This could be the rising (low to high) or falling (high to low) edge of the clock signal; the datasheet will specify which one to use. When the receiver detects that edge, it will immediately look at the data line to read the next bit (see the arrows in the below diagram). Because the clock is sent along with the data, specifying the speed isn’t important, although devices will have a top speed at which they can operate.

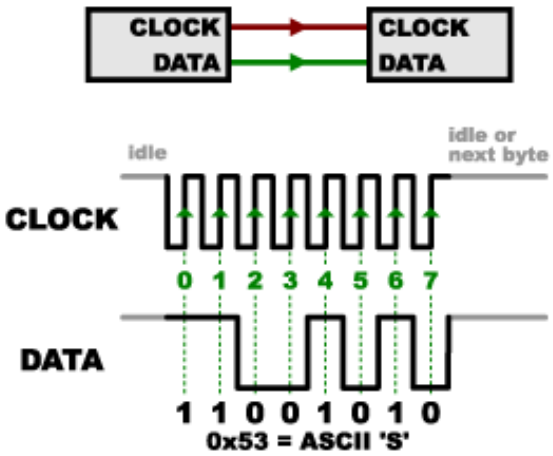

Figure 1.4. SPI interface bits order-using clock and data.

One reason that SPI is so popular is that the receiving hardware can be a simple shift register. This is a much simpler (and cheaper!) piece of hardware than the full-up UART (Universal Asynchronous Receiver / Transmitter) that asynchronous serial requires [14].

In SPI, only one side generates the clock signal (usually called CLK or SCK for Serial Clock). The side that generates the clock is called the “master”, and the other side is called the “slave”. There is always only one master (which is usually microcontroller), but there can be multiple slaves (more on this in a bit).

When data is sent from the master to a slave, it is sent on a data line called MOSI, for “Master Out / Slave In”. If the slave needs to send a response back to the master, the master will continue to generate a prearranged number of clock cycles, and the slave will put the data onto a third data line called MISO, for “Master In / Slave Out”.

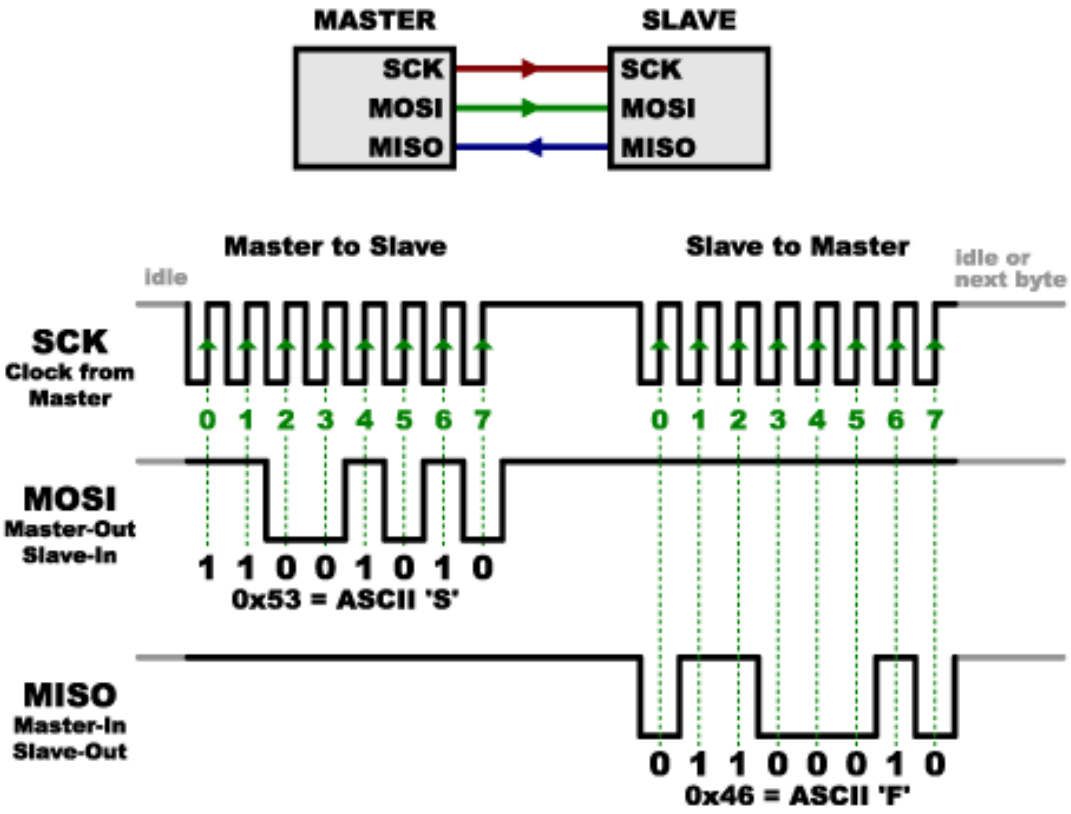

Figure 1.5. SPI master – slave method data transmission

The master always generates the clock signal, that have to known in advance when a slave needs to return data and how much data will be returned. This is very different from asynchronous serial, where random amounts of data can be sent in either direction at any time. In practice, this is not a problem, as SPI is generally used to talk to sensors that have a very specific command structure. For example, if you send the command for “read data” to a device, you know that the device will always send you, for example, two bytes in return. (In cases where you might want to return a variable amount of data, you could always return one or two bytes specifying the length of the data and then have the master retrieve the full amount.)

It is note to mention that SPI is “full duplex” (has separate send and receive lines), and, thus, in certain situations, you can transmit and receive data *at the same time* (for example, requesting a new sensor reading while retrieving the data from the previous one).

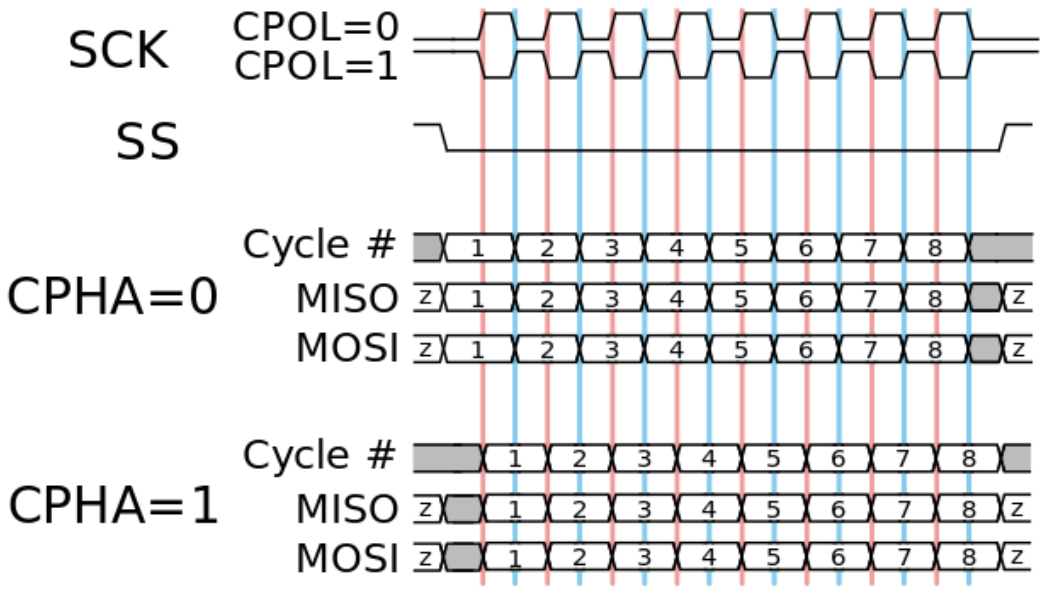

Figure 1.6. SPI clock polarity set

In addition to setting the clock frequency, the master must also configure the clock polarity and phase with respect to the data see figure.1.5. Freescale's SPI Block Guide names these two options as CPOL and CPHA respectively, and most vendors have adopted that convention.

The timing diagram is shown to the right. The timing is further described below and applies to both the master and the slave device.

At CPOL=0 the base value of the clock is zero

For CPHA=0, data are captured on the clock's rising edge (low to high transition) and data is propagated on a falling edge (high to low clock transition).

For CPHA=1, data are captured on the clock's falling edge and data is propagated on a rising edge.

At CPOL=1 the base value of the clock is one (inversion of CPOL=0)

For CPHA=0, data are captured on clock's falling edge and data is propagated on a rising edge.

For CPHA=1, data are captured on clock's rising edge and data is propagated on a falling edge.

That is, CPHA=0 means sample on the leading (first) clock edge, while CPHA=1 means sample on the trailing (second) clock edge, regardless of whether

that clock edge is rising or falling. Note that with CPHA=0, the data must be stable for a half cycle before the first clock cycle.

The MOSI and MISO signals are usually stable (at their reception points) for the half cycle until the next clock transition. SPI master and slave devices may well sample data at different points in that half cycle. This adds more flexibility to the communication channel between the master and slave.

2. MAIN PART. AMCS SOFTWARE DEVELOPMENT

2.1. Approaches and tools

The main goal of any developer of software systems is to write an effective application. Effective in all senses: a reliable, convenient, expandable. Therefore, if convenient and intuitive approach is used, the less developer will make an error, less time will be on writing programs, it will be easier to understand and extend. Today, for writing any program it is often used an object-oriented approach, allowing the developer to ignore the algorithm as a sequence of instructions [12].

Object-oriented approach offers the programmer to represent abstract essence of the program in the form of interacting objects. This approach is closer and understandable to human, as it is most convenient reflects the surrounding real world. Object thinking allows ones to represent and understand the increasingly complex system. In pursuit of further efficiency and reduce development time software systems, the existence of such an approach and the corresponding object-oriented programming languages is not enough. It is necessary to have special tools to help think through the system to model, to avoid fatal errors occurring when a plurality of lines of code already written. It is requisite to have means in order to visually represent objects and their interactions and necessary techniques to consistently find and study the interacting objects, consider the development process and adapt it to changing needs.

Models help to illustrate the structure and behavior of the system. They are necessary for the visualization and control system architecture, minimizing the risks. The models allow a better understanding of systems, which leads to their simplification and reuse. The system can be described from different perspectives, which are used for different models, each of which is semantically meaningful abstraction system. There are structural models representing the system organization, and behavior, reflecting its dynamics.

2.2. Structure of AMCS

As is aforementioned above, the focus of the AMCS is their intellectualization, the maximum number of aggregation functions to collect, process information and make decisions. AMCS systems are capable of automating many processes associated with the organization of access to the resource. These include the registration of subjects (users and staff) and facilities (resources) ACS, a direct access to a resource, organization of control staff, collection and provision of statistics on the operation of the system and more.

The automation and access management control are expanding their capabilities by organizing the system of accounts. AMCS-oriented service a large number of customers usually have a modular structure allows you to organize entrance to specific room. Modular circuit is provided using a client-server architecture. The number of modules and functionality depends on the purpose of the system and manufacturer. For example, the set of modules can be [3]:

"Pass Controller" - the service is responsible for registering new customers, issuing electronic cards, account creation, assignment of access rights to individual users and groups. It is accomplished by hardware installed in the door of premise, where the client software does authentication and identification process.

"Administrator module" where an administrator performs the system's configuration, IDs, registration personnel, see the online state of a controller visually and manage the AMCS controller remotely see fig.2.1.

Modules interact with the central AMCS server (see para. 1), which plays the role of a manager, a processing application requests and event controllers, sensors and actuators. A local area network or the address space of the computer can as a medium of interaction service applications and server security system.

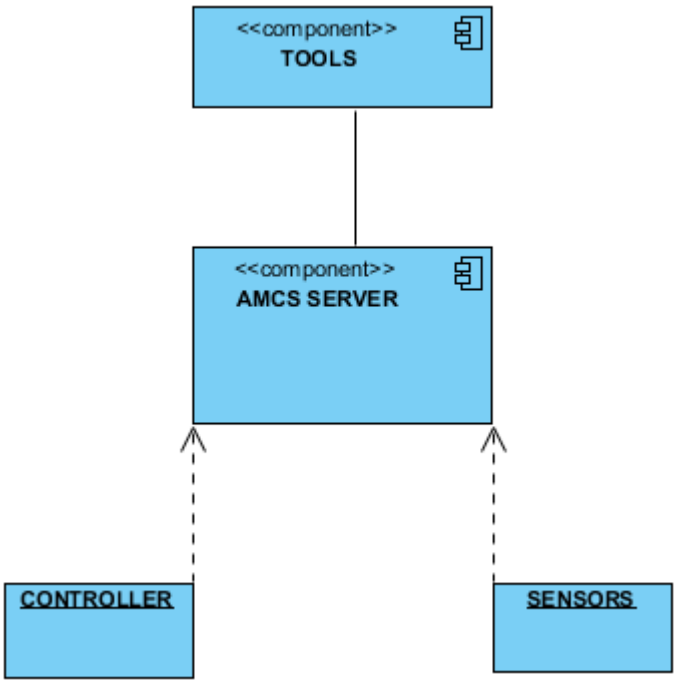

Figure 2.1. AMCS deployment diagram.

2.3. Architectural mechanisms of AMCS developing

The software architecture of AMCS is based on a number of mechanisms, defining the requirements applicable to the system. The handling of AMCS as a real-time system requires the implementation of mechanisms for scheduling, inter-object communication and of work with timers. Parallelism in the handle of external events occurring at the same time should be provided by using of multi-threading. Client-server approach makes the need to implement mechanisms and ways of interaction between the server and applications, and general safety requirements and reliability make choosing special methods of data storage and handling. Some architectural mechanisms used an unusual approach to the creation of objects, requiring the transfer of the string name of the class of object to create. This approach may also be considered as an auxiliary mechanism (a lower level). Furthermore, there have been utilized some design patterns in order to solve tasks that encountered while in the step of development of AMCS client-server software. Namely, "*Singleton*" pattern was used in many part of software development, due to it's flexibility which offers many problems to be solved by virtue of it [12].

Singleton - generating a design pattern that ensures that single-threaded application will be the only instance of the class with the global access point.

In class has only one instance, and it provides him a global point of access. Significantly, it is possible to use an instance of the class, since in many cases it becomes available more functionality. For example, the components described in the class can be accessed via the interface, if available language.

Global "single" object - the object's name and not a set of procedures that are not tied to any object - is needed:

– if you use an existing object-oriented library;

– if there is a chance that one object ever turn to a few;

– If the interface of the object (for example, the game world) is too complex and not worth the litter Main namespace many features;

– if it is, depending on what some conditions and settings, creates one of several objects. For example, depending on whether or not the log is carried out, or this object is created, writing to a file, or "cap", does nothing. Such objects can be created and the initialization of the program.

This can lead to such difficulties. The object is needed already at initialization, it may require before it is created. It happens that the object is not always necessary. In this case, it is possible to create and miss.

Besides, to enable both scalability and reliability in client – server application there have been utilized modular approach. Since, modular approach requires separate and delegate functionalities of to be developing client – server software, therefore, it was used "*Factory*" design pattern to achieve modularity of the system as a whole.

To be more specific, *Factory* - generating a pattern design that provides an interface for creating subclasses instances of a class. At the time of the heirs can determine which class to create. In other words, the creation of factory delegates objects to the heirs of the parent class. This allows the use in the program code than specific classes, and abstract objects manipulated at a higher level.

It defines the interface for creating an object, but leaves the decision on whether subclasses which class to instantiate. Factory Method lets a class delegate the creation of subclasses. It is used when:

– class not known in advance what facilities it is necessary to create subclasses;

– class is designed so that objects that it creates, specify subclasses;

– class delegate their responsibilities to one of several auxiliary subclasses, and planned to localize the knowledge of which class takes these responsibilities themselves.

All the architectural mechanisms described below were implemented on C ++ Qt framework 4.8.6. List of attached files-modules is given in Appendix.

2.4. Server architecture

The current paragraph is dedicated to architecture of server side application. As it is illustrated below server's structure is divided into three main layers (See fig. 2.1.). Kind of structure is well known within web services, due to its flexibility and clarity.

The foundation of the whole server service is the "***Source"*** layer. Server application's source layer takes a part from two blocks, namely "***Network***" and "***Database network***" layer - provides socket connection e.g. server listens the port for incoming client's connections, and the last one is database provider, which is important driver providing network connection with the database server. In this project, connected to MySQL database server and service listens for 5222 system port respectively.

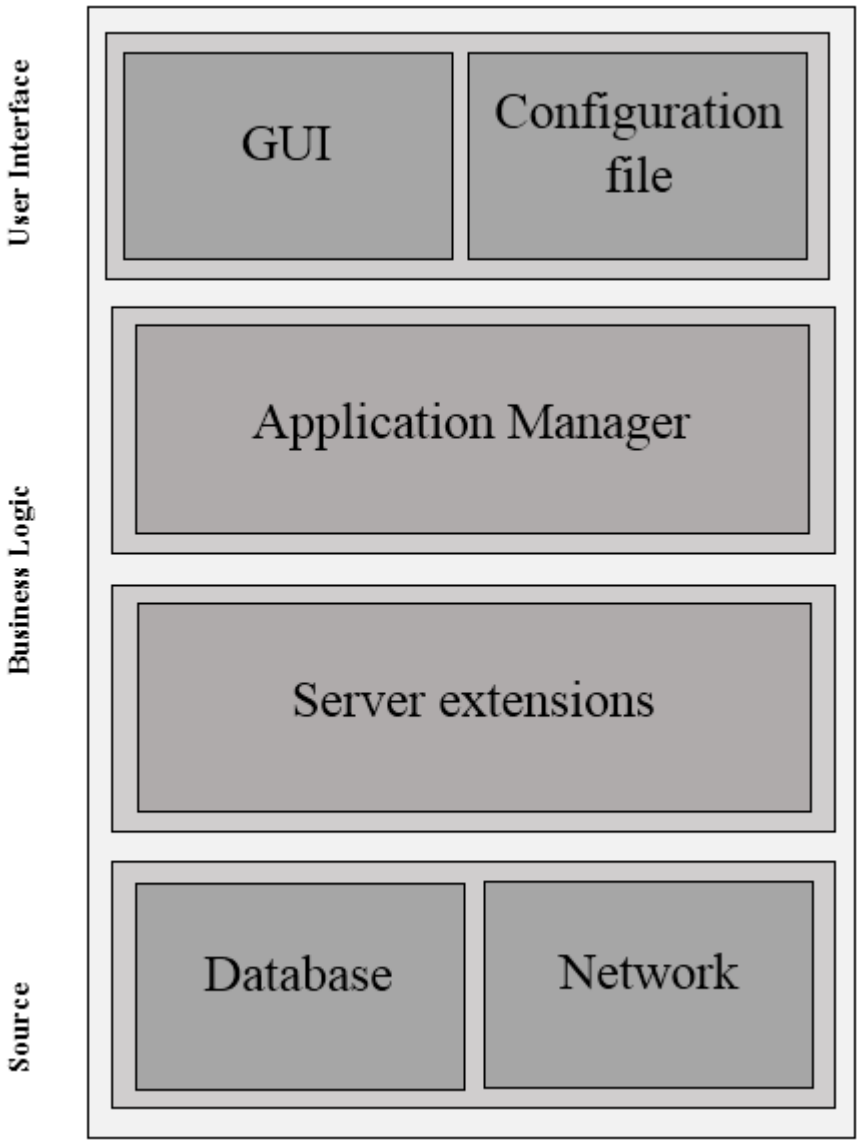

Figure 2.2. Server architecture of AMCS

The second central importance layer is "***Business Logic***". In order to implement it as perfect as possible, the current service part is divided into two interconnected logical parts. The first of them ensures the server to get prerequisite configuration files, for example, port number to listen to, database options to connect etc. On top of that, manages the sessions and connection establishing with appropriate clients connected to the AMCS server. In other words, this (Application Manager) module is also know as the main controller in server. The following module is known as Server Extension modules (see fig. 2.3.), which includes sub-modules in it in it essence. Each module make up new functionality to the server, and also can referred as the plugin manager in the business logic. All

functionality of server comprises of the server extension module and whole business logic is put on this part. Note to mention that each module is separate and in order to provide this there have been created exception block, which in case of a module crash, it catches an error and writes it to Warning.log.

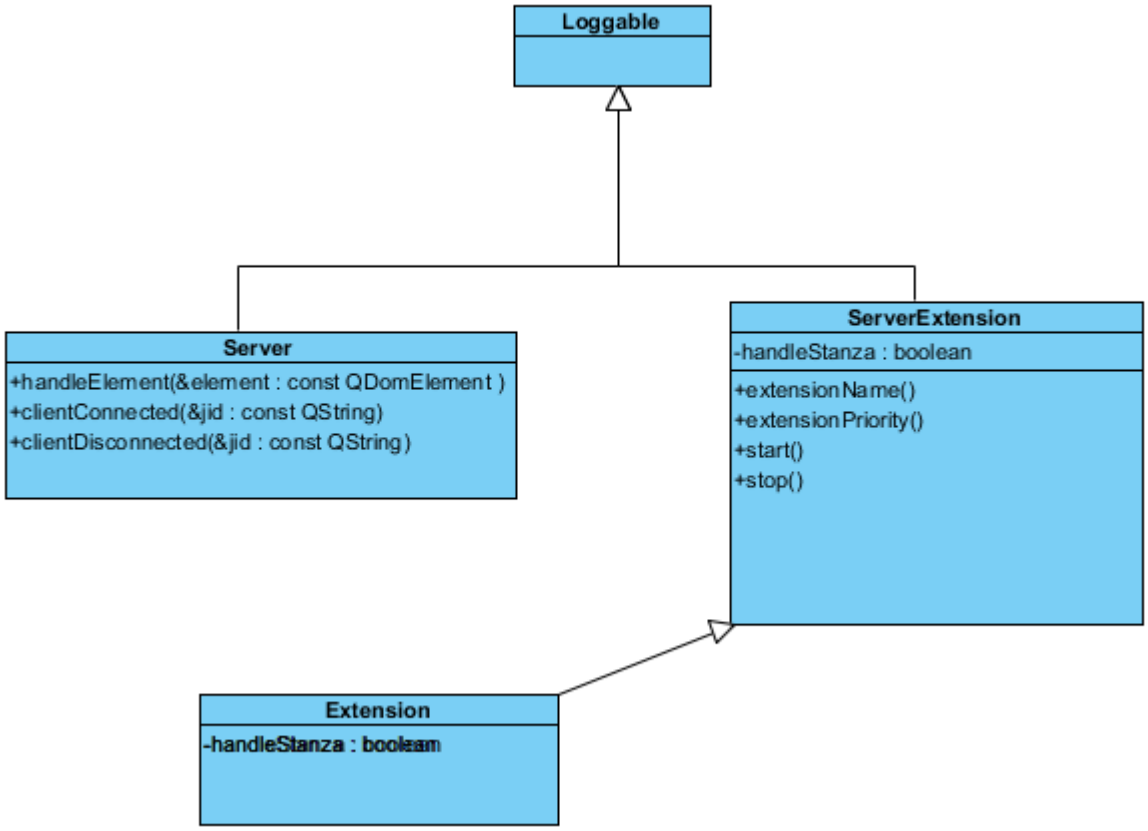

Figure 2.3. Application manager structure in server

All actions in server is logged in a log file and it is done by Logger module in the AMCS server. All concerning modules description are described below by object-oriented class model.

The last layer is known as "***User interface***", which is responsible for server management it's configuration with GUI. Graphical overview of full map where AMCS controller is installed. Graphically add user set him or her access add attach unique Tag with UID, handle AMCS controller. Moderator is able to read the logs and configure the server through GUI.

2.5. Database design of server application

All information is stored in database with relational schema, which performs maintenance and management of the information and is responsible for the integrity and security of data, as well as providing input-output operations when accessing customer information see fig. 2.2. In the current work, the main part of database is demonstrated. There are two table in it, which encompass business logic of a server. As to modularity of server structure and ability to expand functionality, the database structure as well can be also enlarged with relational tables.

As it is shown in the diagrams below, the main logic, comprise of AMCS controller (which installed on the door) and the User Identification of a tag per an employee or a student and the office or institution. There was used only one type of a bond and it is Foreign key bond that hold UID of forbidden tag of an employee or a student.

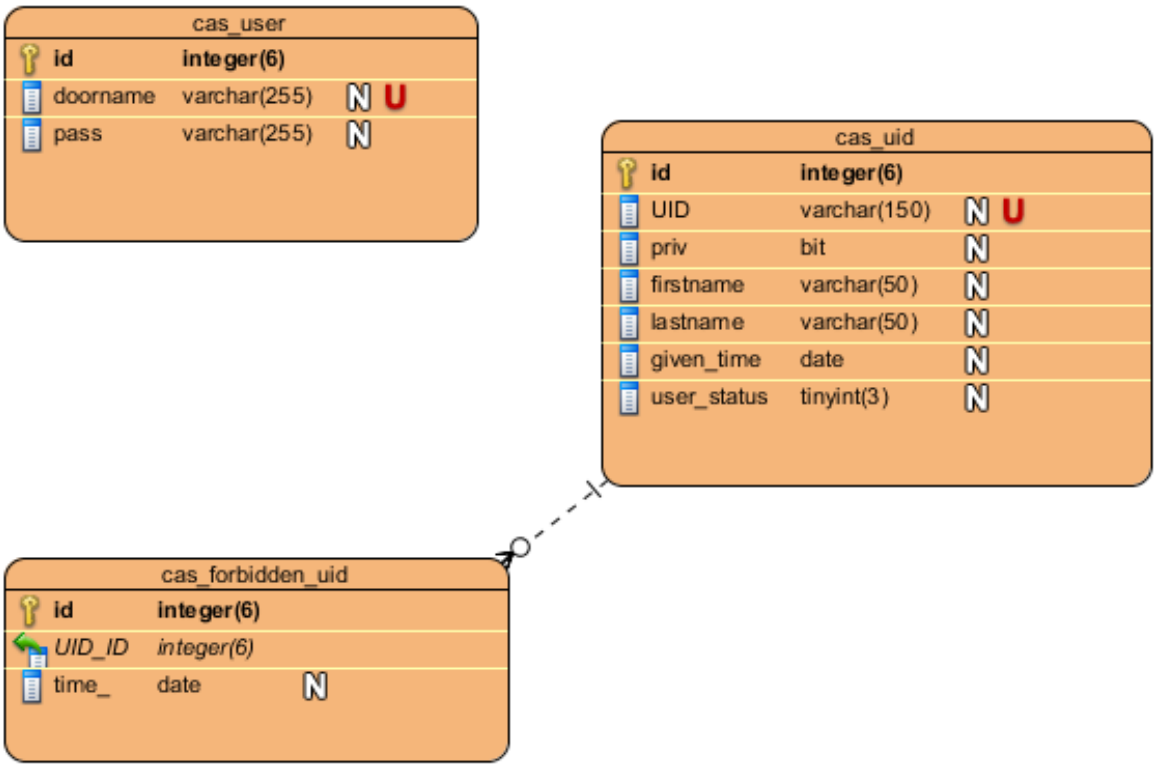

Figure 2.4. Relational scheme of AMCS server side application's database

The biggest priority in business logic is to ensure grand access to tag's owner if he or she has of course or deny, therefore data storing is only done on server side by moderator vie server application GUI. The first relational table name *"cas_user"* is includes in it, all clients which connect with a server, with according it door number in which it is installed and password. In order to ensure that connected client is a reliable source there is also a password for clients to be connected. Each connected client store the UIDs, which is attached to an owner. Moreover, associating UID is also bonded with user's initials e.g. his or her first name, last name, the given time of tags to an user, affiliation or privilege of UID owner, status as well are stored in server database in order to ensure integrity of AMCS. The users with denied permission UID is stored in *"cas_forbidden*" with associating UID that is linked as a foreign key to *"cas_user"* table, by the way, the time when the UID's privilege was restricted is saved as well in the same table respectively.

Table 1. Database schema description of client side application

Table name	**Type of field**	**Denomination in database table**	**Description**
cas_uid			
	INT	id	PRIMARY KEY with AUTO_INCREMENT attribute
	VARCHAR	UID	Given to the user tag's unique ID
	BIT	priv	Privilege of the user (whether GRANTED or DENIED)

Table name	Type of field	Denomination in database table	Description
	VARCHAR	firstname	Firstname of the user
	VARCHAR	lastname	Lastname of the user
	DATE	given_time	The time when the tag was given to a user
cas_user			
	INT	id	PRIMARY KEY with AUTO_INCREMENT attribute
	VARCHAR	doorname	The given name to the AMCS controller name e.g. client to be connected
	VARCHAR	pass	The password of to be connected user
cas_forbidden			
	INT	id	PRIMARY KEY with AUTO_INCREMENT attribute
	VARCHAR	UID	The FOREIGN KEY linking to cas_uids table UID attribute
	DATE	time_	Date when UID was blocked

2.6. Client architecture

Clients' side architecture differs from server side with its additional functionality than of server side application. Apart from modular functionality, that server offers client side is associated with RFID reader hardware that reads tags' UID in it. The business logic in client side is strongly relies on reader functionality and build around it. All functionality blocks as in server application is separated as it is in server side, and run in an isolated thread and all threads communicated within each other through main thread. Reader controller that receives data from Proximity Integrated Circuit Card (PICC) encompass essential role in business logic. As Proximity Coupling Device (PCD) receives data, it then emits signal with data and corresponding threads catch the signal and process it while manipulating with in it is own thread.

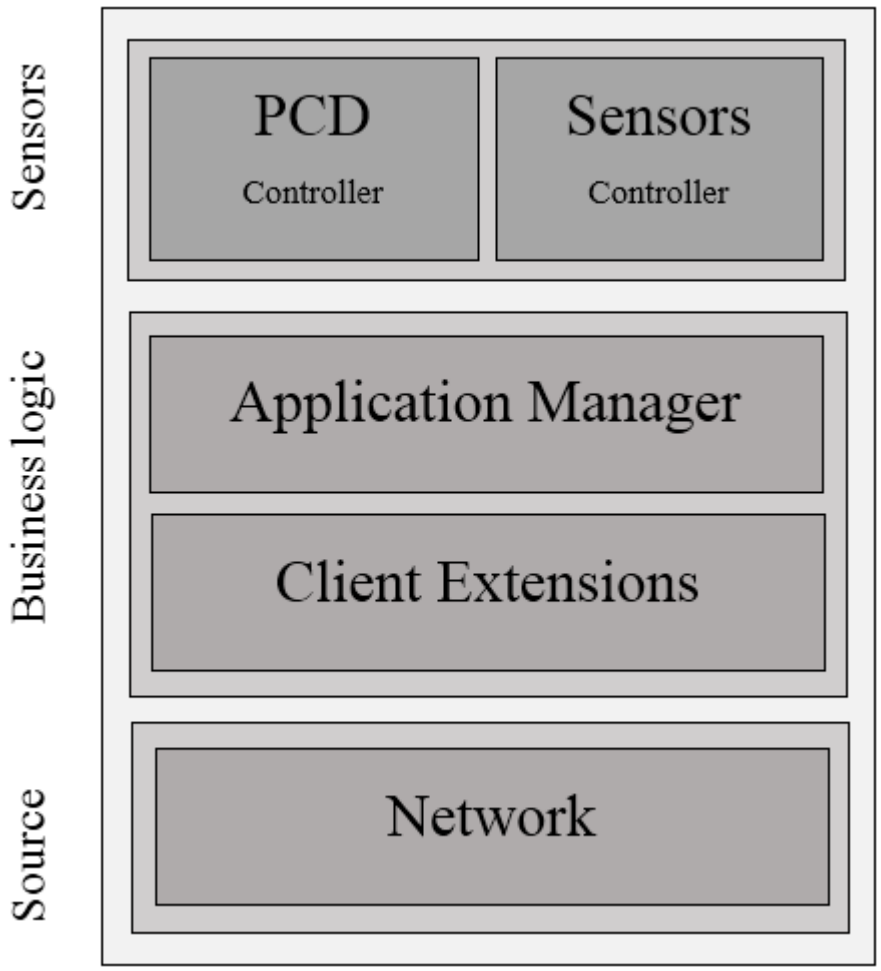

Figure 2.5. Client architecture

As it is represented in the fig. 2.5. the client architecture comprise of three different layers than those on server side. There are: sensors, business logic part and sources and all configuration files are stored in a file. The first commences sensors layer, which includes in it PCD equipment and other sensors used in AMCS. The second as it is noted above business logic with its Application Manager (see fig. 2.5.1) and extensions. Network block in current work represent source layer. Which means every data processed in client-application has it's commence on this layer apart from configuration settings.

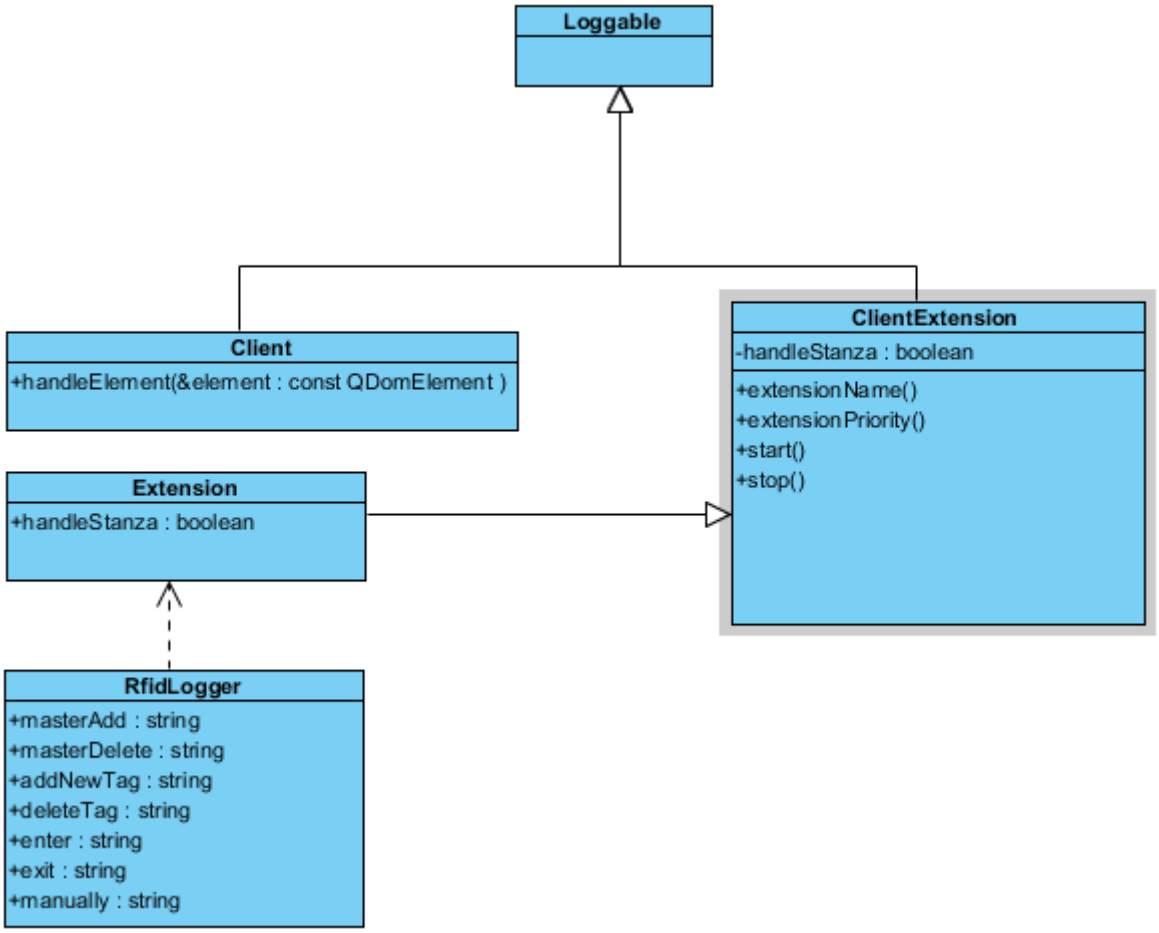

Figure 2.5.1. Client –side application manager

2.7. PCD and PICC communication in AMCS client.

As represented in the figure above sensors played major role in whole client-server architecture of AMCS. Correspondingly, there was a major concern how to adjust RFID reader with remaining business logic of AMCS. Taken into account

all that requirements and communication protocol of RFID reader hardware protocol (this is MIFARE ISO/IEC 14443) there was developed the “RFID” controller module operating in a separate thread in client - side application.

To begin with, The MIFARE name covers proprietary technologies based upon various levels of the ISO/IEC 14443 Type A 13.56 MHz contactless smart card standard. The MIFARE name (derived from the term MIkron FARE Collection System) covers seven different kinds of contactless cards. MIFARE Classic employs a proprietary protocol compliant to parts (but not all) of ISO/IEC 14443-3 Type A, with an NXP proprietary security protocol for authentication and ciphering [15].

The MIFARE Classic card is fundamentally just a memory storage device, where the memory is divided into segments and blocks with simple security mechanisms for access control. They are ASIC-based and have limited computational power. Thanks to their reliability and low cost, those cards are widely used for electronic wallet, access control, corporate ID cards, transportation or stadium ticketing.

The MIFARE Classic 1K offers 1024 bytes of data storage, split into 16 sectors; each sector is protected by two different keys, called A and B. Each key can be programmed to allow operations such as reading, writing, increasing value blocks, etc. MIFARE Classic 4K offers 4096 bytes split into forty sectors, of which 32 are same size as in the 1K with eight more that are quadruple size sectors. MIFARE Classic mini offers 320 bytes split into five sectors.

For each of these card types, 16 bytes per sector are reserved for the keys and access conditions and cannot normally be used for user data. In addition, the very first 16 bytes contain the serial number of the card and certain other manufacturer data and are read only. That brings the net storage capacity of these cards down to 752 bytes for MIFARE Classic 1k, 3440 bytes for MIFARE Classic 4k, and 224 bytes for Mini. It uses an NXP proprietary security protocol (Crypto-1) for authentication and ciphering. The encryption used by the MIFARE Classic card uses a 48-bit key. The Digital Security research group of the Radboud

University Nijmegen made public that they performed a complete reverse engineering and were able to clone and manipulate the contents of an OV-Chipkaart which is a MIFARE Classic card. For demonstration, they used the Proxmark device, a 125 kHz/ 13.56 MHz research instrument.

The MFRC522 is a highly integrated reader/writer IC for contactless communication at 13.56 MHz. The MFRC522 reader supports ISO/IEC 14443 A/MIFARE mode. The MFRC522's internal transmitter is able to drive a reader/writer antenna designed to communicate with ISO/IEC 14443 A/MIFARE cards and transponders without additional active circuitry. The receiver module provides a robust and efficient implementation for demodulating and decoding signals from ISO/IEC 14443 A/MIFARE compatible cards and transponders. The digital module manages the complete ISO/IEC 14443 A framing and error detection (parity and CRC) functionality.

The MFRC522 supports all variants of the MIFARE Mini, MIFARE 1K, MIFARE 4K, MIFARE Ultralight, MIFARE DESFire EV1 and MIFARE plus RF identification protocols. To aid readability throughout this data sheet, the MIFARE Mini, MIFARE 1K, MIFARE 4K, MIFARE Ultralight, MIFARE DESFire EV1 and MIFARE Plus products and protocols have the generic name MIFARE. The following host interfaces are provided:

– serial Peripheral Interface (SPI);

– serial UART (similar to RS232 with voltage levels dependent on pin voltage supply);

– I2C-bus interface.

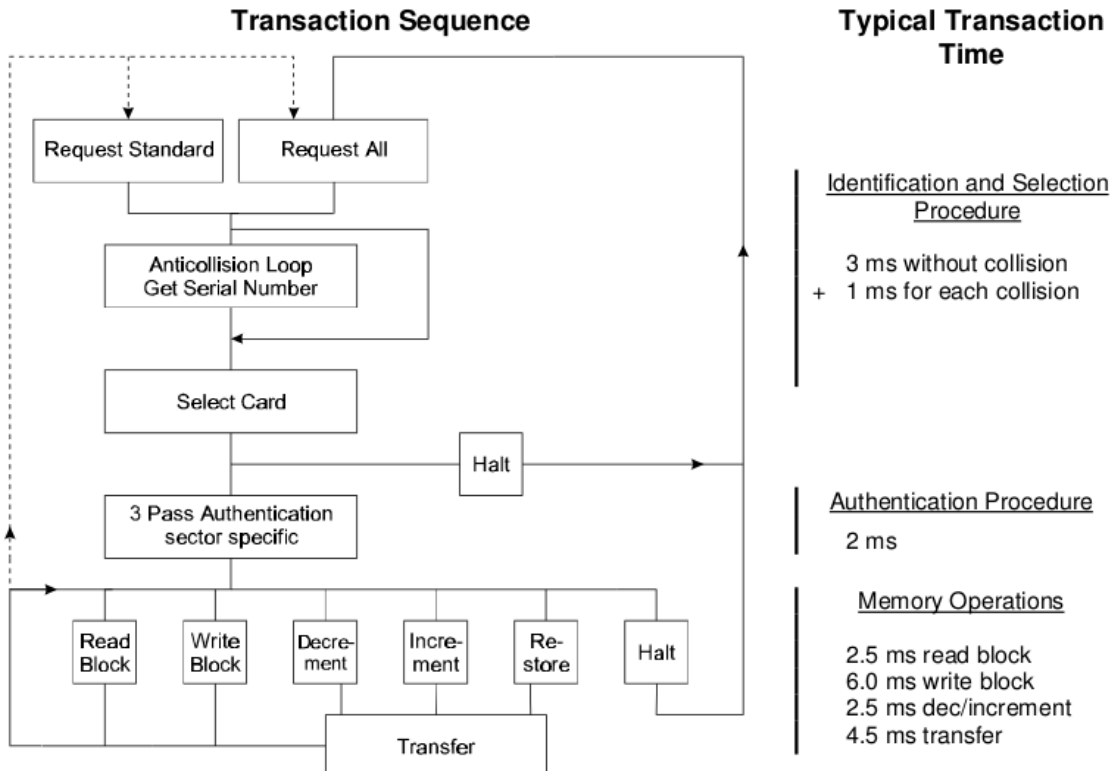

Figure 2.6. RFID reader application communication algorithm with transaction sequence

For PCD to function properly the following modules were developed as a prerequisite:

*Answer to Request.*With the Answer to Request sequence the MIFARE RWD (Read Write Device) requests all MIFARE cards in the antenna field. When a card is in the operating range of a RWD, the RWD continues communication with the appropriate protocol.

Anticollision loop. In the Anticollision loop the serial number of the card is read. If there are several cards in the operating range of a RWD, their different serial numbers can distinguish them and one can be selected (Select card) for further transactions. The unselected cards return to the standby mode and wait for a new Answer to Request and Anti-collision loop.

Select Card. With the Select Card command, the RWD selects one individual card for further authentication and memory related operations. The card returns the Answer to Select (ATS) code, which determines the individual type of the selected card. Access Specification. After identification and selection of one

card the RWD specifies the memory location of the following access [15].

Three Pass Authentication. The appropriate access key for the previously specified access is used for 3 Pass Authentication. Any communication after authentication is automatically encrypted at the sender and decrypted by the receiver. *Read/Write.* After authentication any of the following operations may be performed:

– READ reads one block;

– WRITE writes one block;

– DECREMENT decrements the contents of one block and stores the result in the data-register;

– INCREMENT increments the contents of one block and stores the result in the data-register;

– TRANSFER writes the contents of the data-register to one block;

– RESTORE stores the contents of one block in the data-register;

The MF1ICS50 IC of a Mifare Classic has integrated an 8192-Bit EEPROM, which is split into 16 sectors with four blocks. One block consists of 16 bytes (one Byte = 8 Bit).

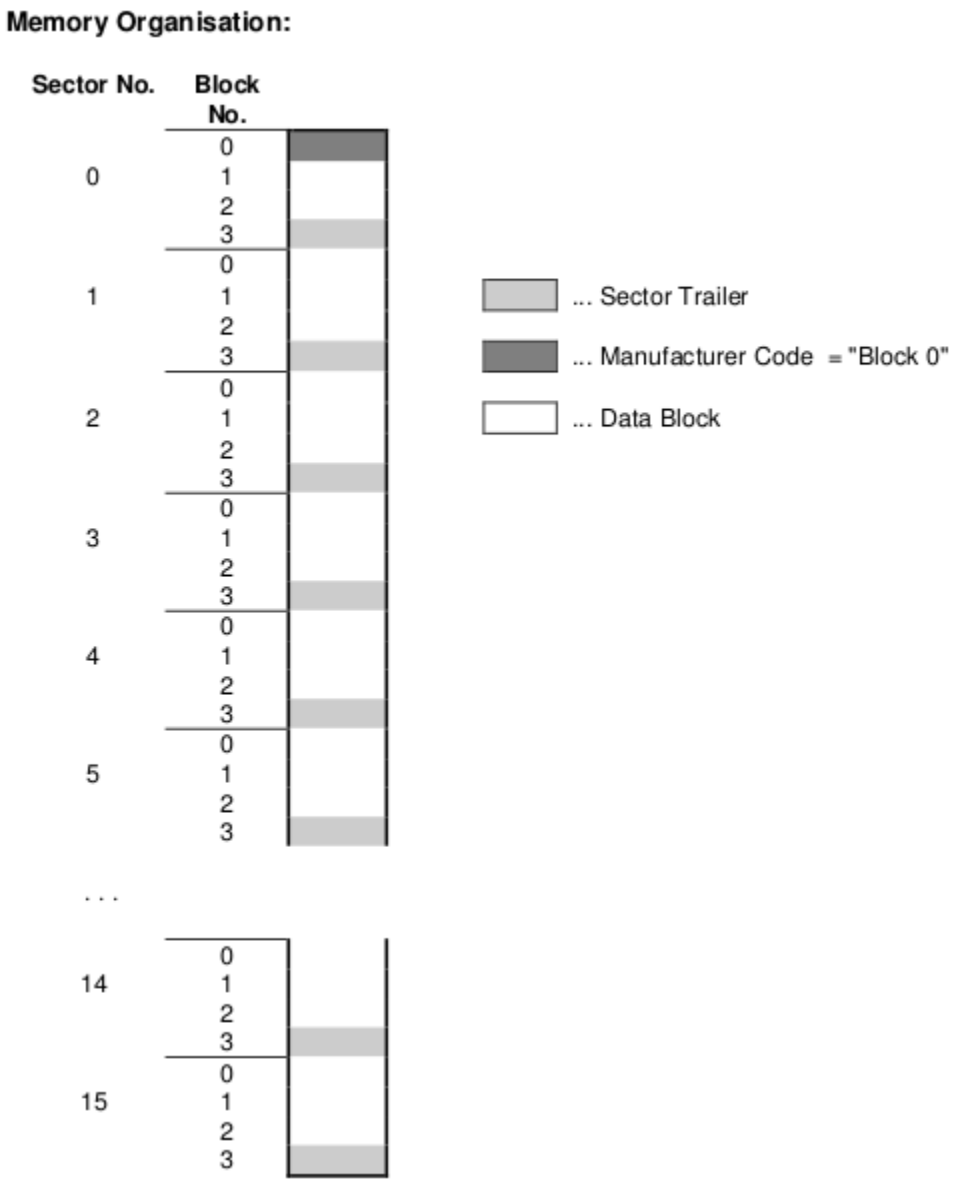

Figure 2.6.1. Mifare Classic Card (PICC) 1K data structure

Manufacturer Code (Block 0 of Sector 0).The first block of the memory is reserved for manufacturer data like 32 bit serial number. This is a read only block. In many documents, it is named "Block 0".

Data Block (Block 0 to 3 except "Block 0"). Access conditions for the Data Blocks are defined in the Sector Trailers. According to these conditions data can be read, written, incremented, decremented, transferred or restored either with Key A, Key B or never.

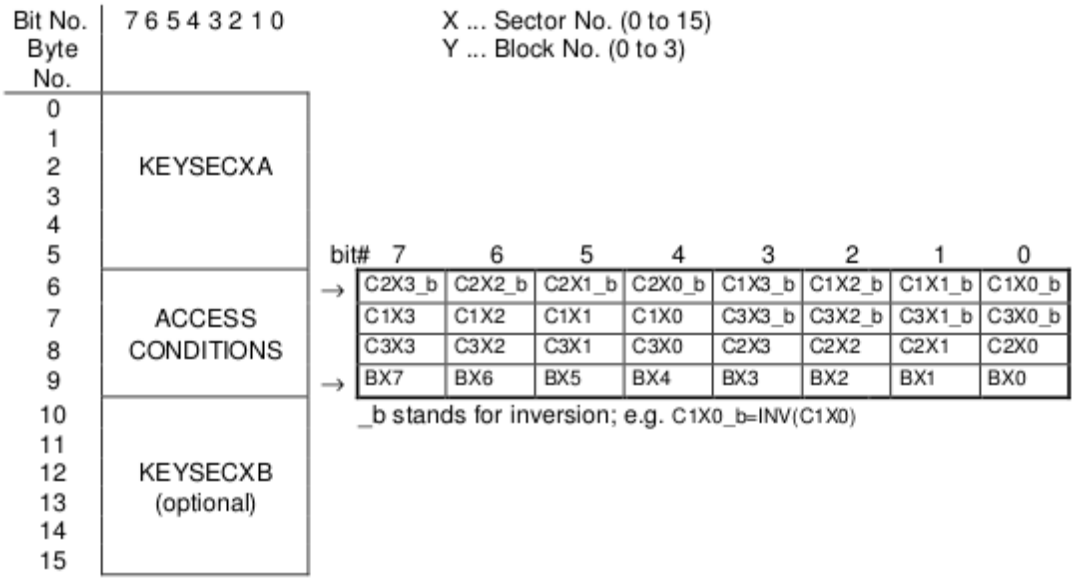

Figure 2.6.2. Sector Trailer description in PICC

The fourth block of any sector is the Sector Trailer. The Sector Trailer contains access Key A (KEYSECXA) an optional Key B (KEYSECXB) and the access conditions for the four blocks of that sector. If Key B is not needed, the last 6 Bytes of block 3 can be used as data bytes. The corresponding access condition settings are marked grey below (see fig 2.8.).

C1XY to C3XY that are stored twice for safety reasons define the access condition independently for the sector's four blocks. The last byte of the access conditions may be used to store some specific application data (e.g. location of the write backup block).

			KEYSECXA		ACCESS COND.		KEYSECXB	
C1X3	C2X3	C3X3	read	write	read	write	read	write
0	0	0	never	key A	key A	never	key A	key A
0	1	0	never	never	key A	never	key A	never
1	0	0	never	key B	key A|B	never	never	key B
1	1	0	never	never	key A|B	never	never	never
0	0	1	never	key A	key A	key A	key A	key A
0	1	1	never	key B	key A|B	key B	never	key B
1	0	1	never	never	key A|B	key B	never	never
1	1	1	never	never	key A|B	never	never	never

incr, decr, transfer, restore : never

Figure 2.6.3. Access condition for sector trailer (Y = 3)

Since the transport access conditions equal to 001, new cards must not be authenticated with Key B.

C1XY	C2XY	C3XY	read	write	incr	decr, transfer, restore
0	0	0	keyA|B[1]	key A|B[1]	key A|B[1]	key A|B[1]
0	1	0	keyA|B[1]	never	never	never
1	0	0	keyA|B[1]	key B[1]	never	never
1	1	0	keyA|B[1]	key B[1]	key B[1]	key A|B[1]
0	0	1	keyA|B[1]	never	never	key A|B[1]
0	1	1	key B[1]	key B[1]	never	never
1	0	1	key B[1]	never	never	never
1	1	1	never	never	never	never

Figure 2.6.4 Access condition for data blocks (Y = 0 to 2)

The process of decrement and increment of a block's data is performed and controlled by the Card – IC. For transportation, the manufacturer predefines KEYSECXA and the access conditions as follows:

C1X0, C2X0, C3X0 = 0 0 0 block 0 (data block)

C1X1, C2X1, C3X1 = 0 0 0 block 1 (data block)

C1X2, C2X2, C3X2 = 0 0 0 block 2 (data block)

C1X3, C2X3, C3X3 = 0 0 1 block 3 (Sector Trailer)

The KEYSECA, secret key, known only by the manufacturer and system integrator.

2.8. AMCS client – server communication basic algorithm

As a rule of thumb, client and server communication ought to be accomplished through mutually excepted protocol. As to this, in the current AMCS client – server software due to the extensibility of the protocol there was used XMPP protocol in order to ensure real – time accessibility of the system and. The protocol known as extensible for messaging and presence, and also open, based on XML, a free to use the protocol for instant communication between client – server entities and presence information in a close to real time. The basic algorithm for communication is described in the figures 2.7. and 2.8.

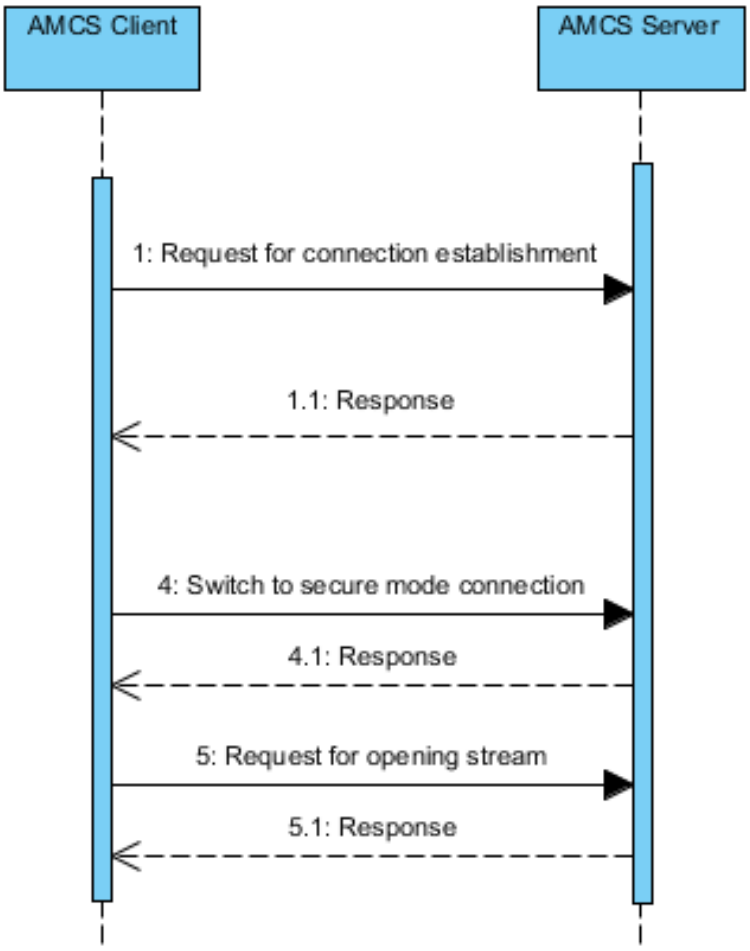

Figure 2.7. AMCS client – server communication principle

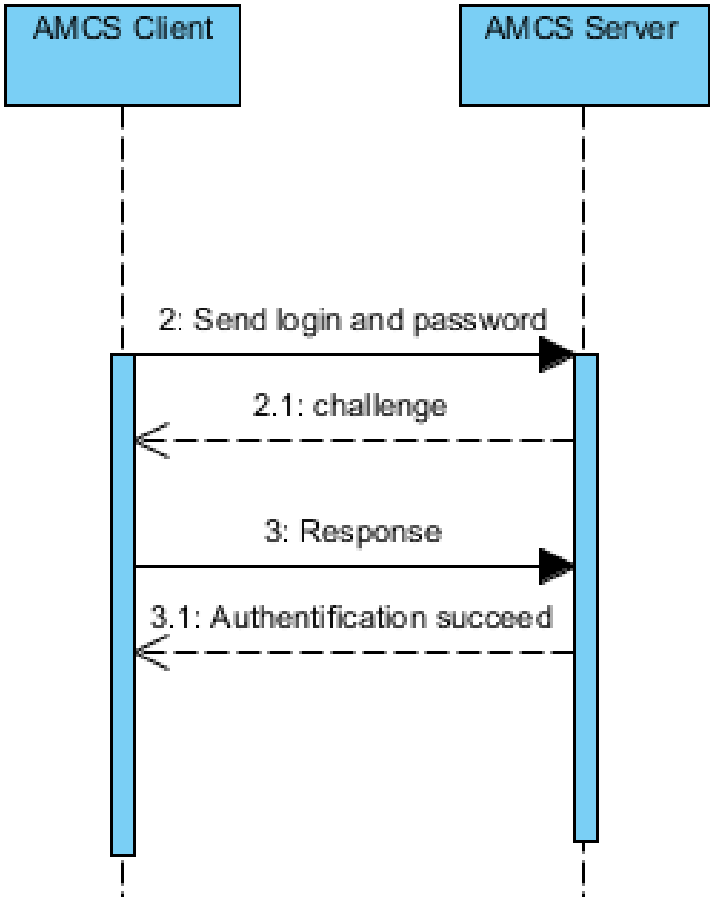

Figure 2.8. Authentication process

1) Here we consider authorization process with sasl-plain mechanism. It means that login (apart from domain) and password will be encrypted.

2) If authorization successful, Server side will response

3) Client again sends negotiation

4) Finally, server service opens for client session and gives permissions to access all available features:

```
<?xml version='1.0'?>
<stream:stream from='gapim.uz' version='1.0'
    xml:lang='en'>
  <stream:features>
  <bind xmlns='urn:ietf:params:xml:ns:xmpp-bind'/>
```

<session xmlns='urn:ietf:params:xml:ns:xmpp-session'/>

</stream:features>

Algorithm of client-server connection establishing. The process between “client” and “server” subsystems goes through several stages and as a result connection establishing creates secure communication channel, which is being kept during the whole session. For channel protection, system uses secure protocol while data transmission over network. That protocol is TLS 1.2 (transport layer security). fig.2.8.

Connection stages of XMPP:

1) XML negotiation after connection to the 5222 port of AMCSserver:
   <?xml version=«1.0»?>
   <stream:stream to=«amcs.uz» xml: lang=«en»>;
2) Response to client after request:
   <?xml version='1.0'?>
   <stream: stream id='3357826913'from=amcs.uz' version='1.0'
   xml:lang='en'>
   <stream:features>
   <starttls xmlns='urn:ietf:params:xml:ns:xmpp-tls'/>
   <compression >
   <method>zlib</method>
   </compression>
   <mechanisms xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
   <mechanism>PLAIN</mechanism>
   </mechanisms>
   </stream:features>

After successful authentication on server side client communicates with server through extended XMPP protocol which was specially designed for AMCS client – server interaction. The protocol is as follows:

```
<iq id="13" to="door_number_1@amcs.uz/rfid" from="amcs.uz" t
ype="result">
<cas xmlns="urn:amcs:cas" >
<MASTER>Master uid for including and excluding tags</MASTER>
        <log>
            <event>EVENT_TYPE_ON_CLIENT</event>
            <uid>UID_OF_A_TAG</uid>
        </log>
        <item>
            <uid>Unique UID of the tag</uid>
            <priv>Access of a user GRANTED or DENIED</priv>
            <first>NAME</first>
            <last>SURNAME</last>
            <given>Given Time</given>
         </item>
        Number of items….
    </cas>
</iq>
```

The above protocol describes and encompass basic communication with client and server. On any event, occurred client sends appropriate XML stanza to server as aforementioned protocol. Server then process the date e.g. parses it then save in log file "*UserLog.log*" on server side and if new item is added on client it's added on server side simultaneously. Event are as follows:

- MasterAdd - when master tag is brought to RFID reader;
- MasterRemove – when master drop tag is brought to nearby RFID reader;
- Add – when new tag is brought to RFID reader;
- Delete – when existing tag or new tag is brought nearby reader;
- Enter – when door is opened;
- Exit – when door is closed;

– EnteredByButton – entrance accomplished by button press;

– ExitedByButton – exit accomplished by button press;

– MasterAlreadyExists – attempt to add new master tag (actually there are two master tags on for including new tag e.g. grant access and the other for excluding tag e.g. deny access of the tag);

– UIDAlreadyExists – endeavor to add existing card;

– UIDAlreadyDeleted – attempt to drop none existing in settings.conf file tag UID;

– AccessGranted – when tags is permitted to enter;

– AccessDenied – access to the tag is blocked e.g. denied;

– Closed – when system shuts down;

– RequestedUIDNotFound – request for unknown to system tag authentication;

– Destroyed – when door is destroyed;

– ConnectedToServer – the state when AMCS client connected to the server;

– UnableToDeleteMaster – attempt to delete or exclude master tag;

– RequestAuthentification – when tag request for authentication;

2.9. AMCS Server UI manual

Having started client software on AMCS controller, client attempts to connect to the server with server host address domain name on port 5222. Meaning while, server listens client on 5222 port while opening a socket for incoming client. When client authenticates successfully and connects to the server on server GUI e.g. on the premises map of blinks transparent red label which means that client connection is established and the door is in *closed* state, see fig. 2.9. When still *disconnected* on server client illustrated as the grey label on the door, see fig. 2.10. In case when the AMCS controller door is *destroyed* or opened by force without tag's authentication the system alarm with red label on the appropriate door on the map, see fig. 2.11. However, when customers bring tag which is granted on the system and opens the door there will prompt opaque green label on the door till it is in *opened* state, see fig. 2.12.

To see logs on client side there ought to be pressed "*L"* button on the door layout, see fig. 2.13. In order to manage client AMCS controller tags affiliation and data concerning users *"M"* button ought to be pressed and to load all users info "*LOAD DATA"* is to be pressed to view all existing users, see fig. 2.14.

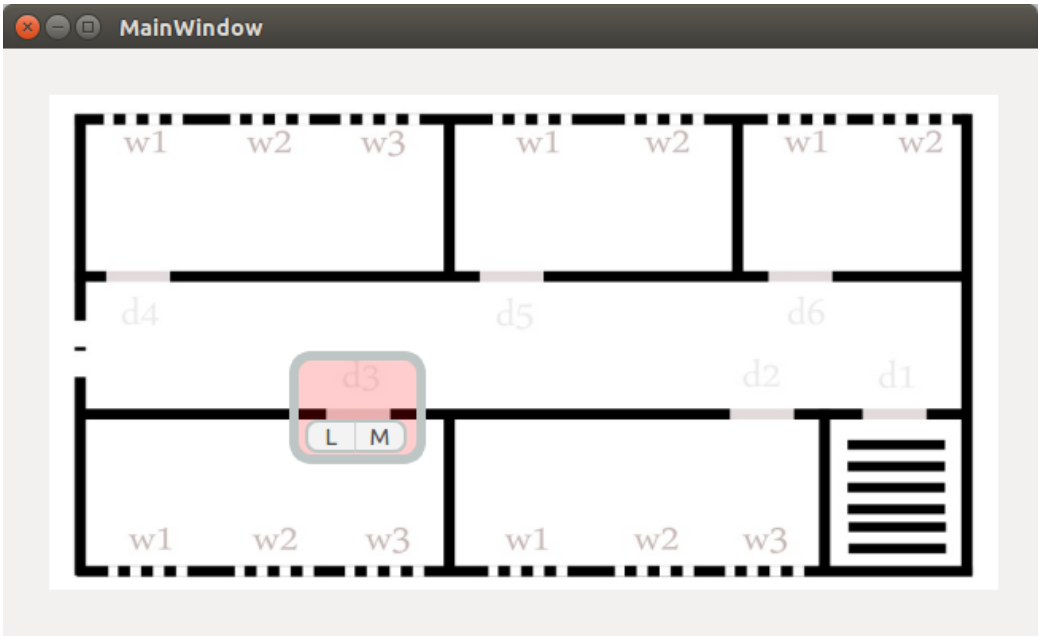

Figure 2.9. AMCS client connected state

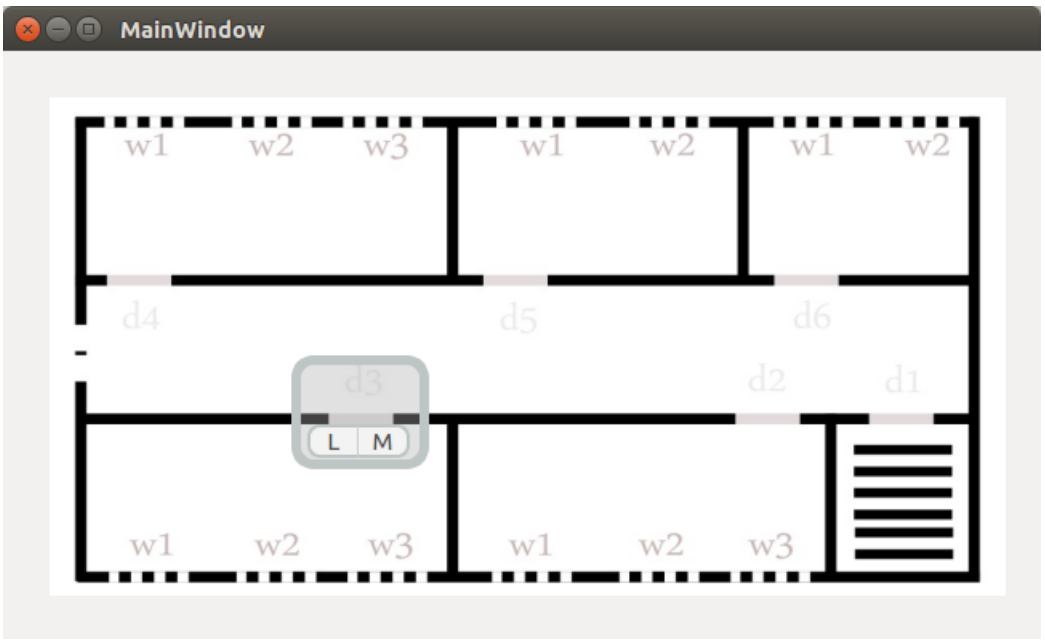

Figure 2.10. AMCS client disconnected and door closed state

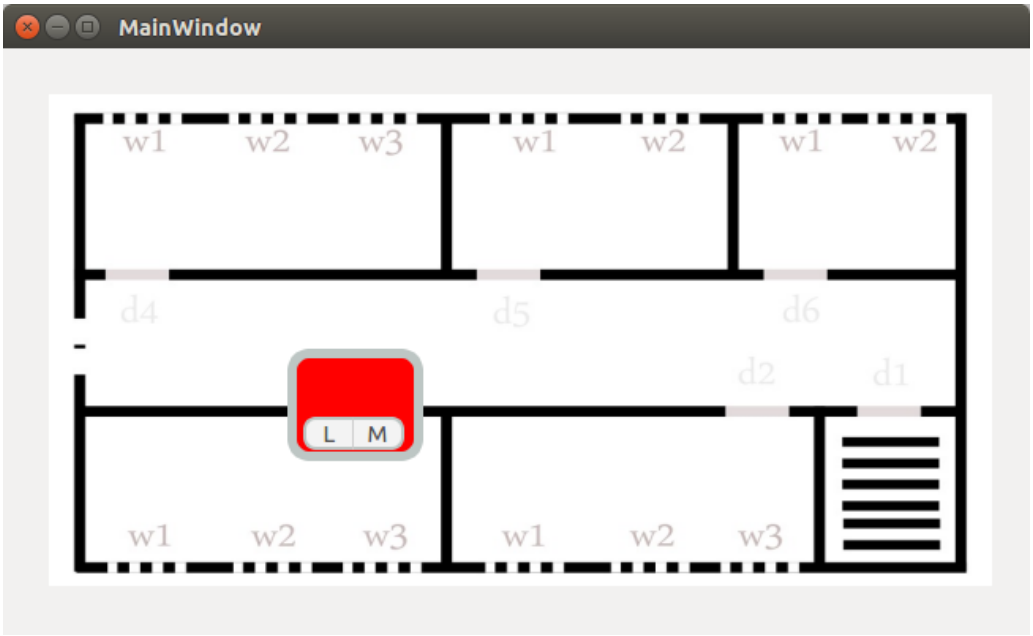

Figure 2.11. AMCS client door destroyed state

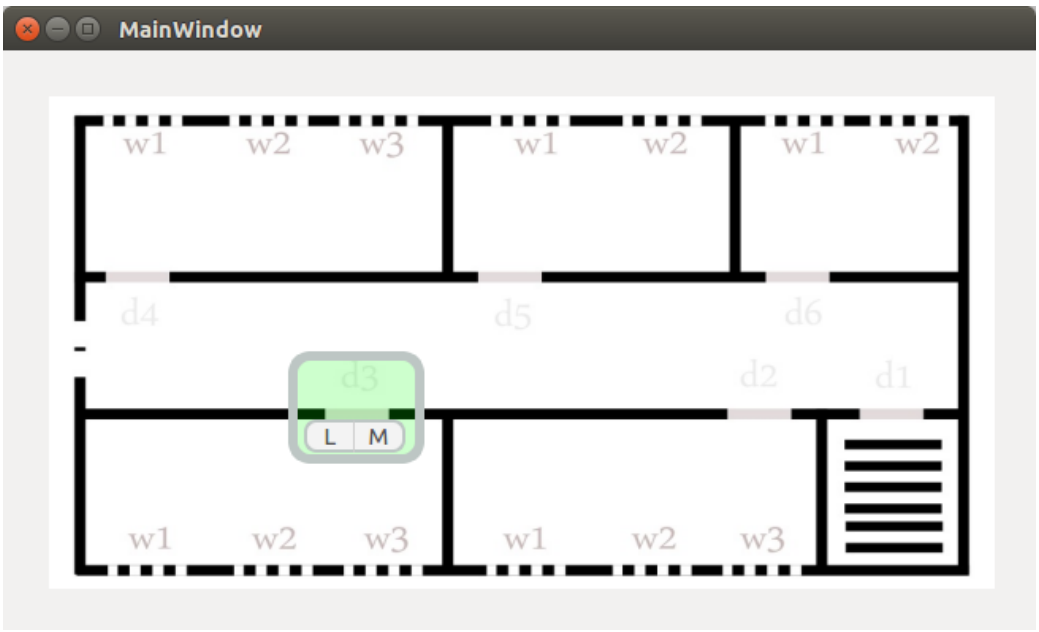

Figure 2.12. AMCS client door opened state

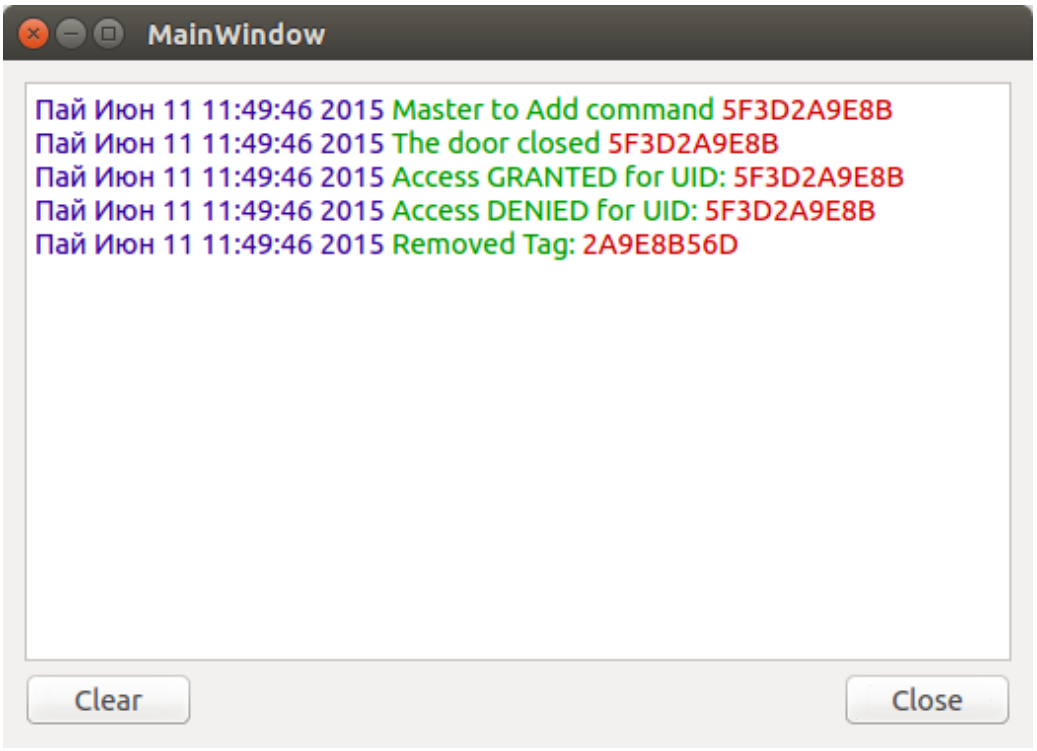

Figure 2.13. AMCS client logs

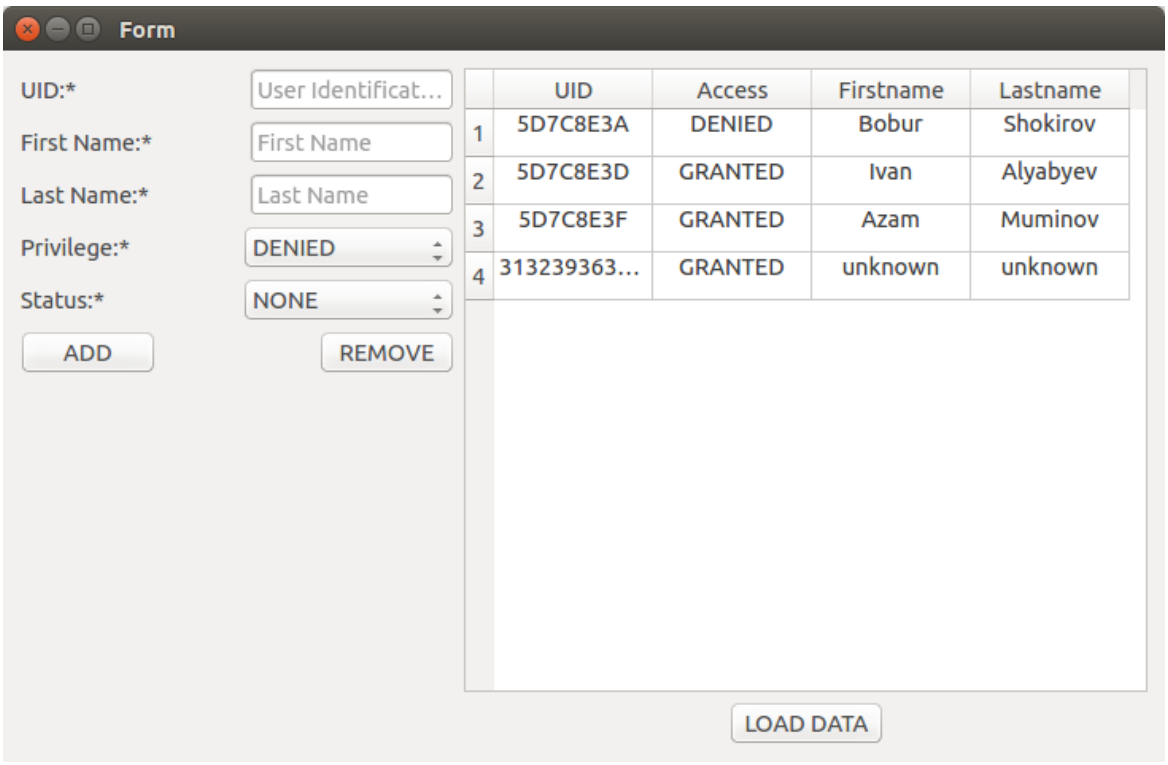

Figure 2.14. AMCS clients information and client management

3. SAFETY OF VITAL ACTIVITY

3.1. Protection from ionizing radiation

Ionizing radiation is widely used in industry, and can present a significant health hazard. It causes microscopic damage to living tissue, which can result in skin burns and radiation sickness at high exposures (known as "tissue effects"), and statistically elevated risks of cancer at low exposures ("stochastic effects").

Radiation protection can be divided into *occupational radiation protection*, which is the protection of workers, *medical radiation protection*, which is the protection of patients, and *public radiation protection*, which is protection of individual members of the public, and of the population as a whole. The types of exposure, as well as government regulations and legal exposure limits are different for each of these groups, so they must be considered separately [13].

There are three factors that control the amount, or dose, of radiation received from a source. Radiation exposure can be managed by a combination of these factors:

– time: Reducing the time of an exposure reduces the effective dose proportionally. An example of reducing radiation doses by reducing the time of exposures might be improving operator training to reduce the time they take to handle a source;

– distance: Increasing distance reduces dose due to the inverse square law. Distance can be as simple as handling a source with forceps rather than fingers;

– shielding: The term 'biological shield' refers to a mass of absorbing material placed around a reactor, or other radioactive source, to reduce the radiation to a level safe for humans. The effectiveness of a material as a biological shield is related to its cross-section for scattering and absorption, and to a first approximation is proportional to the total mass of material per unit area interposed along the line of sight between the radiation source and the region to be protected. Hence, shielding strength or "thickness" is conventionally measured in units of g/cm^2. The radiation that manages to get through falls exponentially with the

thickness of the shield. In x-ray facilities, walls surrounding the room with the x-ray generator may contain lead sheets, or the plaster may contain barium sulfate. Operators view the target through a leaded glass screen, or if they must remain in the same room as the target, wear lead aprons. Almost any material can act as a shield from gamma or x-rays if used in sufficient amounts.

Shielding reduces the intensity of radiation depending on the thickness. This is an exponential relationship with gradually diminishing effect as equal slices of shielding material are added. A quantity known as the halving-thicknesses is used to calculate this. For example, a practical shield in a fallout shelter with ten halving-thicknesses of packed dirt, which is roughly 115 cm (3.8 ft) reduces gamma rays to 1/1024 of their original intensity (1/2 multiplied by itself ten times).

Practical radiation measurement using calibrated radiation protection instruments is essential in evaluating the effectiveness of protection measures, and in assessing the radiation dose likely to be received by individuals. The measuring instruments for radiation protection are both "installed" (in a fixed position) and portable (hand-held or transportable).

Fundamental to radiation protection is the reduction of expected dose and the measurement of human dose uptake. For radiation protection and dosimeter assessment the International Committee on Radiation Protection (ICRP) and International Commission on Radiation Units and Measurements (ICRU) have published recommendations and data which is used to calculate the biological effects on the human body, and set regulatory and guidance limits.

Ionizing radiation’s biological effects appears in the form of primary physical and chemical processes that occur in the molecules of living cells and the surrounding them substrates, and a dysfunction of the whole organism as a consequence of the primary processes.

Because of radiation in living tissue, as in any environment, the energy is absorbed, raises excitation and ionization of atoms irradiated material occurs. Since humans and mammals the main part of body weight makes up water (75%), the primary processes are largely determined by the absorption of radiation by

water cell, ionization of water molecules to form a highly chemically free radicals such as OH or H chain and subsequent catalytic reactions (mainly oxidation these radicals protein molecules). This is an indirect (indirect) effect of radiation through the products of water radiolysis.

Direct exposure to ionizing radiation can cause the splitting of protein molecules break the weakest bonds, radical separation and other processes. Direct ionization and direct transfer of energy the body tissues do not explain the damaging effect of radiation. Thus, when absolutely lethal dose of 6 Gr to the whole body, in 1 cm 3 of tissue formed 10 15 ions that the ionization is one molecule of water from 10 million. Molecules. In the future, under the influence of the primary processes in the cells functional changes occur, obeying the laws of life biological cell. The most important changes in the cells: damage to the mechanism of mitosis (division) and the chromosome apparatus of the irradiated cells; blocking the process of renewal and differentiation of cells; blocking the proliferation and subsequent physiological tissue regeneration. Particularly radiosensitive cells are constantly updated (differentiating) tissues and organs (bone marrow, gonads, spleen, etc.), changes at the cellular level, cell death lead to violations of the functions of individual organs and within organs interconnected processes in the body, and this causes all sorts of effects on the body or lethal repercussion.

Medical evidence shows that the exposure of the human body as a whole and separate organs, leads to varying degrees of destruction. Therefore, to ensure the safety of people there were introduced the concept of a critical body - the part of the body, tissue, organ, under irradiation that causes the greatest damage to the person. In order of decrease, the radio sensitivity of organs referred to as I, II or III groups:

I - the whole body, red bone marrow, gonads;

II - muscles, thyroid gland, adipose tissue, liver, kidney, spleen,

III - skin, bone, hands, forearms, shins and feet.

All the effects which are caused by irradiation of the body are classified into the following groups:

– somatic effects - the degree of damage and the severity increases with dose;

– stochastic effects - effects of the probability of occurrence of tumors in organs, tissues, malignant changes in hematopoietic cells (the threshold for this effect is absent);

– genetic effects - congenital deformities as a result of mutations and other disorders associated with heredity (threshold exposure and is impossible under the influence of small doses).

Irradiation of human in minor doses of radiation, there will not be changes in health. So on Earth natural background radiation at sea level is 0.5 mGy / year. At 1500 meters, it has already 2 times higher at the height of 6000 m (plane flight) which is 5 times higher. For a single irradiation of the whole body, depending on the total absorbed dose of radiation the following biological disorders are:

– from 0.25 Gy (25 rem) - apparent violations there;

– 0.25 - 0.50 Gy (25-50 Baer) - possible changes in the blood;

– 0.50-1.00 Gy (50-100 Baer) • Changes in the blood, the normal state is broken, the ability to work;

– 1.00-2.00 Gy (100-200 Baer) -Easy form of radiation sickness, the latent period of up to 1 month, weakness, headache, nausea, blood recovery after 4 months;

– 2.00-3.00 Gy (200-300 Baer) is the average form of radiation sickness after 2-3 hours of mild symptoms of radiation sickness, indigestion, depression, sleep disturbances, fever, bleeding gums, cramps, bleeding, and recovery after 6 months. Chance of fatality;

– 3.00-5.00 (300-500 Behr) - a severe form of radiation sickness, uncontrollable vomiting within an hour and all the signs of radiation sickness appear sharply: fever, refusal to eat. Death within one month is 50-60% of the exposure. More than 5.00 Gy (500 rem) - is a very severe form of radiation

sickness after 15 minutes. Uncontrollable vomiting blood, loss of consciousness, diarrhea, bowel obstruction. Death occurs within 10 days (100% of the total number of victims).

The irradiation 100-1000 times greater than mortal man dies during irradiation: "death under the ray." Collective protection against ionizing radiation are a variety of devices (sealing, ventilation and air purification, transportation and storage of isotopes, automatic control and alarm systems, remote control) and safety signs, containers for radioactive isotopes and others.

When working with the substance in comply with the rules of personal hygiene, it is advised to use personal protective equipment, organize dosymetric control. On the works of Class I and Class II individual works PPE include coveralls or a suit, socks, footwear, gloves, paper towels and handkerchiefs, disposable, wear respiratory protection. On the works of Class II and Class III separate working papers provide bathrobes, lightweight shoes, gloves, hats and if necessary, wear respiratory protection. Those conducting the cleaning and working with radioactive solutions and powders, except for the basic working clothes and footwear, further provided with arm ruffles of polyvinyl chloride (polyethylene), aprons, rubber or plastic shoes or rubber boots. When necessary, use an insulating hose suits (pressure suits), glasses, plates, hand grips Regulation OSP-72/80 defined a strict order of radiation control, including individual (mandatory for those who work under the terms of the dose may be greater than 0, 3 annual SDA).

3.2. Working conditions

Working conditions - characteristics of the production process and environment that affect the company's employees. Characteristics of the production process are determined by the equipment used, the object and product of labor, technology, system maintenance jobs [11].

The work environment is primarily characterized by sanitary working conditions (temperature, noise, lighting, dust, fumes, vibration, etc.), security,

work, work and rest, as well as the relationship between the employees of the company. The intensity of labor characterizes the amount of labor expended in the unit of time. The main factors affecting the intensity of work include:

– degree of employment the employee during the working day;

– the pace of work;

– the effort required in the performance of works which depend on the weight of transported goods, the equipment features, the organization of work;

– number of serviced facilities (machines, workstations, etc.);

– the size of the objects of labor;

– specialization in the workplace;

– sanitary and hygienic working conditions;

– form relationships in the production teams.

The criteria and classification of working conditions' working conditions are divided into four classes: the optimal permissible, harmful and dangerous. Optimum working conditions (1st class) - conditions under which preserved the health of workers and created the preconditions for maintaining a high level of efficiency.

Acceptable conditions of work (2nd class) - is characterized by such levels of environmental factors and labor process, that does not exceed the hygienic standards for workplaces, and possible changes in the functional state of the organism recovered regulated during breaks or the beginning of the next shift, and should not adversely actions in the near and long term on the health of workers and their offspring. Acceptable working conditions conventionally considered to be safe.

Hazardous working conditions (class 3) - occupational hazards, exceeding hygienic standards and having adverse effects on the body working and his offspring. Hazardous working conditions on the degree of excess hygienic standards and severity of changes in the body are divided into four working degree of harmfulness.

Dangerous (extreme) conditions of work (4th grade) - levels of production factors, the effects of which during the working shift poses a threat to life, a high risk of acute occupational diseases, including severe.

Class working conditions determined by the degree of deviation of the parameters of the working environment and working process of the current hygienic standards in accordance with the identified impact of these deviations on the functional status and health of workers.

Hygienic standards of working conditions (MPC, RC) - is the levels of harmful factors, which in daily (except weekends) work, but not more than 40 hours a week, during the working time should not cause diseases or abnormalities in the health status detected by modern methods of research in the process or in the remote terms of life of present and future generations. Compliance with hygienic standards does not exclude a violation of the state of health in individuals with hypersensitivity (hygienic criteria).

Significant impact on the performance have weather conditions in the room or climate, which depends on thermal characteristics of the process equipment, season, heating and ventilation conditions. The microclimate is determined by the action on the human body combinations of temperature, relative humidity, air velocity and temperature of the surrounding surfaces, the intensity of the thermal radiation.

The main factor is the temperature of the climate - the degree of heated air. The change of air temperature in the premises affected by the heat (the kinetic energy of the molecules) coming from various sources mainly due to thermal radiation from hot surfaces and convection. Humidity - the content of water vapor, it is characterized by the following concepts:

– absolute humidity (water vapor pressure is expressed (Pa) or in weight units in a defined volume of air (g / m3) under certain pressure and temperature);

– maximum humidity (moisture when fully saturated air at a given temperature, g / m3);

– relative humidity (characterizes the degree of saturation of the air with water vapor and is defined as the ratio of the absolute humidity to maximum)%.

For saturated air relative humidity taken as 100%. To determine the relative humidity, there are psychometric tables, graphs and charts, allowing to find the relative humidity depending on the temperature of the dry and wet bulb.

Indoor air mobility is created by convection currents temperature difference between inside and outside, as well as the work of mechanical ventilation. Unit - m / s. The intensity of the heat radiation of the human body is a source of thermal energy per unit body surface, W / m2.

Thermoregulation of the human body. The human body has a constant temperature of 36.6 ° C. To save its persistence on human skin there are two types of analyzers: some react to the cold, while others to heat. Thermal analyzers protect the body from hypothermia and overheating, help to maintain a constant body temperature. The combination of processes of heat and heat transfer occurring in the body, allows you to maintain a constant body temperature, called regulators.

The mechanism of heat release has a chemical thermoregulation and heat irradiation physical thermoregulation. Increased heat release is achieved by increasing the intensity of energy metabolism and the major contribution it makes muscle activity. So resting heat production of 111, 6-125, 5 W, and the intensive muscle work - 313, 6-418, 4 watts.

Along with temperature, humidity and air mobility in industrial premises there effects air ion formula on human activity. Negatively charged air ions, are beneficial to the human body, improve labor productivity. In areas with negative ions decreases the number of microorganisms, reduces the concentration of dust in the air, eliminates electrostatic charges on the surface of the equipment, and neutralizes some gases. Aero-ions air are called light ions. Light air ions, encountered on the way the suspended particles connects with them, telling them their charge. As a result of connection, there generated charged particles, which are called heavy ions that are harmful to health.

Air Ionization - the process of turning neutral atoms and molecules of air in the electrically charged particles (ions). Natural ionization occurs as a result of the impact on the air environment of cosmic radiation and particles emitted by radioactive substances during their decay. Technological ionization - when exposed to the air radioactive environment, X-ray and ultraviolet radiation, thermal emission, the photoelectric effect and ionizing other factors caused the process. Special devices - ionizers, which provide a limited amount of air pollution given certain polarity ion concentration, perform artificial ionization.

In areas of respiration of the personnel in the workplace, where there are sources of electrostatic fields (video display terminals, copiers, televisions), allows the absence of ions of positive polarity.

For the normalization of air ion formula used aero-ionizers, passed sanitary-epidemiological evaluation and with existing sanitary and epidemic conclusion. It is also necessary to use ventilation, the automatic mode of regulation of ion air environment.

Natural lighting and rationing. The lighting in the production areas in the daytime is carried out by natural light source - the firmament. Natural lighting is created in areas with a permanent presence of people. It may not be available in areas with short-term stay of people, and where the presence of light is unacceptable for technological conditions of work.

Types of natural lighting are lateral (through the window), the top (through skylights) and combined. The use of a system of natural light depends on the purpose and size of the room, its location in terms of the building, as well as the light of climate areas.

With a lack of natural light using artificial light, the combination of which is called a combined lighting. The intensity of natural light is estimated by coefficient of natural illumination (CNI), showing how many times the brightness in the room is less than the outer light as per percentage. CNI’s normalized value of building regulations 23-05-95 "Natural and artificial illumination" and building regulations 2.2.1 / 2.1.1.1278-03 "Hygienic requirements for natural, artificial and combined

coverage of residential and public buildings" in view of the nature of visual works, visual discharge operation, type of natural and combined illumination light climate where the building is located, the CNI in the range of 0.1 to 6%.

Artificial lighting by its appointment subdivided into operating, emergency, security and rescue. Task lighting is provided for all premises, buildings for work.

The system of artificial lighting is the general system of local and combined lighting. General lighting is for the common uniform and common localization. General uniform illumination provides the required visibility across the illuminated area because of the uniform arrangement of luminaires at a relatively high altitude under the ceiling. Total localized coverage determined by the location of the equipment.

Combined illumination system is used, where accuracy is required to execute process and general lighting, creates shadows on work surfaces arranged vertically or obliquely. When used combined light besides lamps, the general lighting fixtures with local non-translucent reflectors. The use of local lighting is not permitted. This is because the sharp uneven lighting in the workplace and in the room reduces efficiency and causes fatigue.

Artificial lighting is normalized by building regulations 23-05-95 and 2.2.1 / 2.1.1.1278-03 given the nature of visual work, discharge and subclass of visual work, the contrast of the object with the background, the background characteristics, lighting systems, and is in the range from 5 000 to 20 lux at any monitoring the manufacturing process.

Light sources. For artificial lighting there used incandescent and discharge (fluorescent) lamps. When you select a source of artificial lighting there supposed to be considered electrical, lighting, structural, operational and economic performance.

Lamps placed in the light fixtures (together referred to as lamps), intended for the redistribution of the luminous flux, to protect the eyes from glare and lamps from pollution, provide electricity, explosion and fire safety, protection against moisture.

Important characteristics of the lamp is protective angle and the efficiency of the lamp (CAP). The protective angle is the angle the luminaire, within which the observer's eye is protected from glare lamp and which is formed by the horizontal and a line tangent to the luminous body and the edge of the reflector edge. The smallest angle is 15 degrees.

The efficiency of the luminaire is the ratio of luminous flux luminaire to the luminous flux of lamps in the luminaire. In modern lamps, efficiency is more or less 60-80%.

3.3. Radiation from mobile communication

Radiation from mobile communication or from electromagnetic radiation is practically everywhere. Many believe that the electromagnetic radiation prevails only in installations, but this is not so. Electromagnetic radiation is stalking us everywhere: at home, at work, on the street. The sources of electromagnetic radiation, in addition to the electric networks is practically all appliances, including a variety of electronic devices: television and radio equipment, mobile phones, electronic gadgets and many other electrical appliances [16].

Even on the streets of the city, where, apparently, there is no electromagnetic radiation source itself is electrified transport, power networks, street lighting and others.

Consider the impact these or other sources of electromagnetic radiation on the human body. To begin with this parameter as the maximum permissible dose of electromagnetic radiation for humans - it is 0.2 mT. Now, note the average value of the electromagnetic radiation of various electrical appliances and devices with which people face daily.

Computer - an essential element in the home of each family. In nine out of ten homes have a PC or other computer equipment (laptop, tablet, etc.). This miracle of technology is a source of electromagnetic radiation of up to 100 mT. It is easy to calculate that a person being in close proximity to a computer is exposed to electromagnetic radiation, which is 500 times higher than the permissible value.

Almost the same level of electromagnetic radiation generated by microwave. Even an ordinary desk lamp is a source of electromagnetic radiation, which is 4-5 times higher than the permissible value. In this case, the radiation source is a wire feed tube. It should also be noted adverse effects of mobile phones and other electronic gadgets and devices. Electromagnetic radiation from these machines is 50 mT, which is 250 times greater than the maximum value.

Electrified transport is one of the most powerful sources of electromagnetic radiation. The trip on the tram or trolley accompanied the influence on the human body of electromagnetic radiation value of 150-200 mT. With that, the Metro value of electromagnetic radiation is much higher and it is 300 mT.

Even on vacation, where, apparently, the person is away from sources of electromagnetic radiation, but it is also exposed to electromagnetic radiation. The source of electromagnetic radiation in this case are high-voltage power lines that cross the surrounding countryside along and across.

All instruments and devices that receive power from the mains, in one way or another are a source of electromagnetic radiation. It turns out that people living in modern conditions, are usually exposed to electromagnetic radiation. Therefore, the issue of protecting the body from the effects of electromagnetic radiation in our time is particularly relevant. Consider the basic measures to reduce the negative effects of electromagnetic radiation on the human body.

Methods for protection against electromagnetic radiation

One of the most effective ways to protect against the negative effects of electromagnetic radiation is the use of special devices that allow to neutralize this radiation and the maximum to minimize its negative impact on the human body. The principle of operation of these devices is based on the hover-EMF, which helps to reduce the negative impact on the human body of unwanted electromagnetic radiation.

The maximum reduction in the residence time in the range of the electromagnetic radiation is one of the most effective ways to protect the body from the negative effects of electromagnetic radiation. This is particularly relevant

issue for employees of electric power companies, where maximum levels of electromagnetic radiation.

For example, the staff serving the high-voltage distribution substations. In switchgears, both open and closed, the level of electromagnetic radiation is very large. In installations 110 and above are often the level of electromagnetic radiation reaches values, such that its negative impact on the human body is very strong.

The first symptoms appear almost immediately: headache, fatigue, irritability, depression. In such cases, finding a person in a zone of the electromagnetic radiation without the use of special protective clothing (the screening devices) is unacceptable.

If you find the staff away from the high-voltage equipment, such as substation control, the level of electromagnetic radiation is much smaller, but its meaning is hundreds of times higher than permissible. This is because in this room there are many sources of electromagnetic radiation: computer technology, device protection and automation equipment, low-voltage distribution panels and others.

In such a case, you should, where possible, take breaks and get out of the room, thereby reducing time spent in the area of electromagnetic radiation. Also, do not be amiss to use the above devices that minimize the negative impact of electromagnetic radiation on the human body.

It should also be noted that the degree of influence of electromagnetic radiation on the human body depends not only on the residence time in the zone of its action, but also on the distance from the radiation source. That is the process of using any appliance or electrical device should be possible to increase the distance to the source.

Besides, cell phones have become a major biohazard, almost weapon may equally be deadly as smoking. In order to reduce their negative impact – it is advised to use alternative means of communication (landline) for the appearance of any opportunity. Do not use cell phones for long conversations and think of others - do not keep them on the hook longer than necessary.

It is highly recommended using a headset, or something as simple as a speakerphone. We do not notice it, but we can be really enough situations where it is convenient to use. Children, for the sake of their health, must be fully protected against cell phone use because their developing brains are particularly vulnerable to EMP cell phones, and their skulls are thinner. Experts recommend that children up to 10 years did not use cell phones. Older children also need to comply with strict guidelines on the use of phones.

For example, when working at a computer is recommended to put the monitor no closer than 30 cm from the head. The same goes for TV and various gadgets. When talking on a cell phone is recommended to use the speakerphone or a wired headset. If the mobile phone is not in use, do not need to keep it in your pocket, it is better to put it on the table.

As a rule, instructions for electrical appliances should be mentioned safety measures, in particular the safety distance to this appliance, wherein the level of radiation is minimized. If such data are not available, then for their own safety, these data are better clarified. On the Internet, there are freely available information about it.

Very often, both at home and at work are included in the electrical network, which is not currently used. These electrical appliances include mobile phone chargers, audio, video, TV, etc. Disabling these appliances can significantly reduce the level of electromagnetic radiation and therefore the degree of its negative impact. Furthermore, electrical disconnection reduces total energy consumption.

As mentioned above, the high-voltage power lines are a source of electromagnetic radiation, and the level of radiation is sufficiently high, and the voltage is higher, the radiation level is higher. Therefore, it is necessary to eliminate or reduce as far as possible while staying within range of the electromagnetic field lines.

There is such a thing as a protected zone of power lines - the distance on both sides of the wire lines. The size of the security zone transmission lines varies

depending on the voltage class. For example, a buffer zone of power lines of 35 kV is 15 m, 110 kV - 20 m, 330 kV - 30 m.

In the buffer zone of power lines degree of electromagnetic radiation is much higher than the permissible value. Therefore, this area is not recommended the construction of residential buildings and various structures. If you enjoy gardening, it is necessary to abandon the area, which runs along the power line. As a rule, on a plot spent much of the time, so you will always be exposed to excessive electromagnetic radiation from power lines.

CONCLUSION

With advent of automated systems nowadays in the world, in front of the system developer of organization's information security specialist, there are often set the task to provide protection for employees in certain areas within which the free exchange is possible.

As a rule, such a system can be Access Management Control. System, developed on the basis of sensors. The effective Access management control system, allows to manage the security of an object and control access. This final qualification work was devoted to demonstrate the feasibility of the model based on the client – server of AMCS software compatible analog with RFID reader, which will be much more profitable in commercial terms as compared to the existing industrial analogues.

As a result of work performed, there has been created a flexible system architecture for Access Management Control System, supporting calculation scheme for the use and visit control. Implemented in C ++ Qt framework and tested all application architecture mechanisms. We obtained the following results:

A systematic study of the subject area. On its basis there was corresponding model which is built, taken into account the visit control for customers using the service;

Designed, implemented and tested the basic architectural mechanisms (Inter-object communication, serialization is on the storage, parameterized creation of objects, commands, interaction mechanisms Applications).

The architecture and software modules were created with appropriate structural models of these modules. Implemented applications supporting the viability of both, the architecture as a whole, and the validity of the application the proposed mechanisms. Practical value of work consists of the following:

Access management control system software can be used as the base interface between hardware and customer in automated system control, while ensuring integrity and accessibility.

BIBLIOGRAPHY

1. DP-1989 "On measures for further development of national information and communication system of the Republic of Uzbekistan".
https://www.mf.uz/media/file/egov/egov1.pdf
2. Encyclopedia UML. - Access:
http://ooad.asf.ru/standarts/uml/spr/Architecture.asp, free.
3. The access control system. - Access:
http://www.gamma.kz/gt/sud.html, free.
4. Cards - IDs for access control systems. - Access:
http://www.avtolik.ru/access/systems/identifikotor.htm, free.
5. Davlethanov M. Attention, alien, 2003. - Access:
http://daily.sec.ru/dailypblshow.cfm?rid=5&pid=6637&pos=1&stp=50, free.
6. Working principles of access control systems. - Access:
http://www.secret-c.ru/uphp/default.php?id=41, free.
7. Gilmanov AA, Klimenko AY, Strangul ON, Tarasenko VP Cards
marketing automation technologies. - Tomsk: Publishing YTL, 2000. -380 p.
8. AA Zhdanov The modern view of real-time OS. - Access:
http://asutp.interface.ru/articles/display_topic_threads.asp?ForumID=13&TopicID
=29
9. Client – Server Model.
http://en.wikipedia.org/wiki/Client%E2%80%93server_model
10. Unified Modeling Language. - Access:
http://penguin.photon.ru/doc/uml.shtml, free.
11. Working condition
http://studme.org/1594102414356/bzhd/klassifikatsiya_usloviy_truda
12. E. Gamma, R. Helm, R. Johnson, J. Vlissides. Receptions object
oriented design. Design Patterns - SPb: Peter, 2001.
- 386 p.
13. Protection from ionizing radiation.

http://studme.org/10440708/ekologiya/zaschita_ioniziruyuschih_izlucheniy.
14. SPI protocol review
https://learn.sparkfun.com/tutorials/serial-peripheral-interface-spi/receiving-data
15. MIFARE classic interface
http://www.nxp.com/documents/data_sheet/MF1S503x.pdf.
16. Radiation from mobile communication.
https://sites.google.com/site/stanleyguansite/health/wireless-radiation/radio-frequency-radiation-emissions-of-wireless-communication-devices

APPENDIX