

COMPUTER SCIENCE

**A SIMULATION MODEL FOR MANAGING
PARAMETERS OF INTELLIGENT SECURITY SYSTEM**

Anzor Babunashvili, Nona Kukhianidze
Kutaisi Akaki Tsereteli State University, Georgia

DOI: https://doi.org/10.31435/rsglobal_sr/28022020/6952

ARTICLE INFO

Received 15 December 2019
Accepted 08 February 2020
Published 28 February 2020

KEYWORDS

intelligent security systems,
safety systems, signalling
system, reliability, module,
management.

ABSTRACT

Security systems are the guarantee of stable functioning of the organization, company, office, industry, housing and other types of buildings. For entire security, complex control devices are set on the building which has to be protected, like fire and burglar alarms, video-audio controls and access systems. Intelligent Security Management System is built on Atmel's microcontrollers. This allows the system to be flexible and to modify it easily if needed. The reliability of the security system depends on its uniqueness. This given security system is easily modified and hence its reliability is high. The system can be easily integrated into a variety of external modules, which can further increase the factor of reliability. It's also easy to adopt it to various security management systems. Many of the security and video surveillance systems allow to control the situation of the object from a large distance. From any point of the planet, we can track and manage the security system modes and make easy changes in them, which enable adequate reaction. Digital complexes of video surveillance are one of the variants of defense organization. The main areas of their use are the most important objects and large areas where buildings are located far from each other.

Citation: Anzor Babunashvili, Nona Kukhianidze. (2020) A Simulation Model for Managing Parameters of Intelligent Security System. *Science Review*. 2(29). doi: 10.31435/rsglobal_sr/28022020/6952

Copyright: © 2020 Anzor Babunashvili, Nona Kukhianidze. This is an open-access article distributed under the terms of the **Creative Commons Attribution License (CC BY)**. The use, distribution or reproduction in other forums is permitted, provided the original author(s) or licensor are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

Introduction. The tendencies of developing technologies of security systems has caused the transformation of existed security systems into more serious complexes of various devices, which are designed for the protection of industrial properties [1].

Modern security and video surveillance systems provide a unique opportunity to fully control the situation at the property that has to be protected. This reduces the risk of breaking into the building and gives us an opportunity to react effectively. Many systems of security and video surveillance allow to control the situation at the property. One can monitor and manage the regimes of how the security system works and make some changes in it that allow to react adequately [2].

1. Digital Security Devices.

Digital video surveillance complexes are one of the variants of organizing security. The main areas of their usage are especially important properties and large areas, where the buildings are far from each other. Their distinctive feature is the wide spectrum, as the transmission of information and high quality of image requires special software and additional equipment. Recently, the so-called electronic security systems, that include the means of identification such as password, plastic card, key, etc. are widely used. There are different approaches for using such kind of systems in private properties and large state units [3].

Nowadays password authentication systems are quite widespread, which enables to distinguish between individual users with the help of unique information, which is known only for them. This can be the name of the accounting record or specially generated unique numerical identifiers.

User password – is a secret information which is only known for the individual for the authentication. According to the system realization, the password can be used only once or many times.

Let's discuss some of the recommendations of the password system in case of passwords that are used many times:

1. Minimum length of passwords used in the system complicates the password guessing system. 6-8 characters are recommended.

2. The existence of different groups of symbols in the password – big and small letters, numbers, special characters make it difficult to guess it.

3. Periodical verification of the passwords by the administrator with the imitation of attacks.

4. Determining the maximum and minimum lifecycle of the passwords and using the mechanisms of force alteration of the old ones. When using this way, we need to take into consideration the fact that the users may require additional explanations from the administrator, what does the system require from them.

5. Restricting the number of failed attempts to enter the password. This will protect the system from multiple attempts to identify passwords through the keyboard, but there is a threat that the legal users will have their accounting records blocked due to incorrectly used passwords.

6. Introducing the register of history of passwords, so the users won't reuse old, already compromised passwords due to their force alteration [3].

2. Virtual model of signaling.

Creation of the new security system requires great work and experience, as well as certain level of knowledge of some characteristics, how it will function and what requirements it will have. There is a very good way out of this situation by means of program-simulators, which change the real details and tools by virtual models. They allow to sort out the scheme work without constructing the real device, find errors made at the stage of designing, remove the necessary features and many more... One of these programs is PROTEUS, for which the simulation of elements isn't the only skill. It's the environment of the so-called „penetrating design“, which means that the device can be created from its graphic image by means of controllers at any stage before the device is produced. It's an architecture in which any additional models can be created in any way, most of their types can function without addressing to coding, therefore PROTEUS allows professional engineers to run interactive simulation of real projects and be rewarded by the result, which corresponds to the scheme simulation. If this is not enough, there are number of popular simulation models of microcontrollers, with the help of which it's possible to simulate the whole microcontrollers' system and work out the programs for them without addressing to their physical prototypes.

With the help of PROTEUS I've decided to construct the scheme of signaling system. One of the main device of this scheme is the microcontroller. For reliability of the scheme and its functional perfection I've decided to choose the microcontroller Arduino Mega 2560, which I have chosen because of several advantages:

A) Inexpensive – in comparison to others, Arduino platform is rather cheap. Also, the board drawings and any kind of information are available. A man can construct and make this board work with his own hands.

B) Simple and integrated development environment – the IDE is friendly to all starters and at the same time it is sufficiently powerful for experienced consumers.

C) The base of extensive equipment and the open-source is the core of Arduino – its microprocessor – of Atmel [4] firm, ATMEGA8 and ATMEGA168 microcontroller [5].

D) For minimization of places in the scheme and a big number of the input-output ports, it has got 54 input-output ports, 15 of which works as a source regulating the power, electricity, speed, lighting, additionally 16 analogue ports, that convert the received signals, are used as digital output, with the help of which it's possible to organize a powerful branch, as well as to control the automatic control system from distance and to monitor all of the parameters [4].

The scheme constructed by me can be used for the protection of state units, as well as private buildings and properties. One-time password is used in the scheme to enter but it can be changed. The signal is active for 10 seconds while opening the door. A person should enter a 4-digit PIN number to stop the burglar alarm (1234 in our case). If we press the key B, we will enter the password change menu, after the change, we will be able to stop the alarm only after entering a new password, if the password is entered incorrectly, we will get the message on the display “Try Again”.



Fig. 1. Arduino Mega 2560

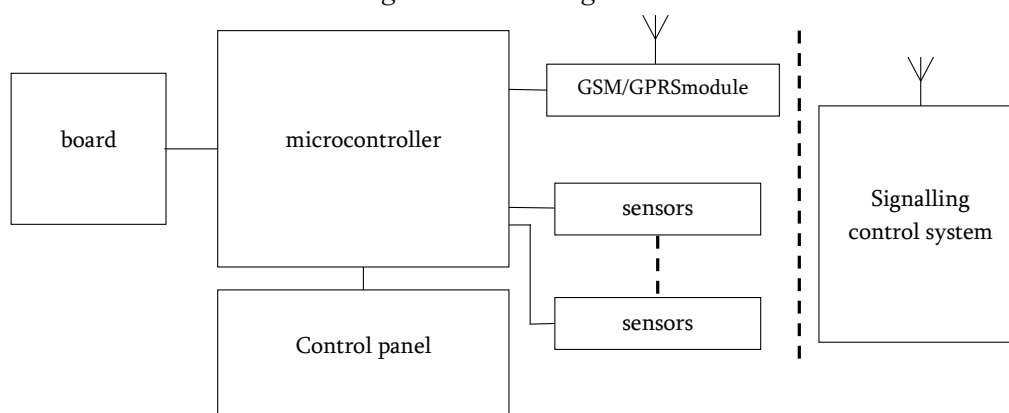


Fig. 2. Scheme of Digital Security System.

The scheme is accompanied by the program. According to the program the initial stage is to initialize the library, enter the initial password, activate an alarm while opening the door and assigning function to the buttons.

Conclusions. Thus, we can say, that:

1. The constructed scheme is one of the possible alternatives of signalling system on certain state unit, which successfully ensures the protection of various types of properties.

2. It is constructed on a microprocessor block and it is a flexible device by means of functional alteration. It's also easy to make.

3. The cost is low, it's reliable and satisfies modern requirements, only slight change in it ensures the protection of different properties at the same time, the system is reliable and secure.

4. It can send SMS and MMS messages, remember them, it is characterized with multi-hour feed autonomy. With a little software and hardware changes, it can be used for a wide range of units.

REFERENCES

1. Рыжова В.А Проектирование и исследование комплексных систем охраны и безопасности. СПб - 2012 г. с. 27-35.
2. Волхонский В.В. Системы охранной сигнализации, 2-ое изд. СПб -2009 г. с. 82-89.
3. Идентификация объектов управления. Самарский государственный технический университет 2009. с. 122-130.
4. Sook-Ling Chua and Stephen Marsland and Hans W. Guesgen" Behaviour Recognition in Smart Homes Sook" Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence 2016. P.45-60.
5. Ia Mosashvili, Salome oniani. Arduino Programming Basics. Georgian Technical University. 2016y. ISBN 978-9941-20-711-2.