ISSN 1330-3651
UDC/UDK 004.056.5

ACCESS CONTROL SYSTEM BASED ON ELECTRONIC KEY

Goran Martinovic, Tibor Kis-Konja, Zoran Kradija

Original scientific paper

Thanks to sufficient memory space, timers, sensors, possibility of communication with other keys and computers, robust design and a reasonable price, electronic keys are devices that enable a significant level of access control referring to space, data and resources in general. Hardware and software possibilities of the developed system of electronic locks which is based on iButton enable rather reliable, precise and simple work as well as user-friendliness in handling and administering access rights, and taking prompt actions in case of unauthorized access. Further improvements and usage of advanced electronic key possibilities might significantly contribute to the level of ambiental intelligence and security of human living environment.

Key words: *access control, ambiental intelligence, electronic key, microcontroller system, security.*

Sustav za nadzor pristupa zasnovan na elektroničkom ključu

Izvorni znanstveni članak

Zahvaljujući posjedovanju dovoljnog memorijskog prostora, vremenskih sklopova, senzora, mogućnošću komunikacije s drugim ključevima i računalima, mehaničkoj otpornosti i prihvatljivoj cijeni, elektronički ključevi su uređaji koji omogućavaju značajnu razinu nadzora pristupa prostoru, podacima i resursima općenito. Sklopovske i programske mogućnosti razvijenog sustava elektroničke brave zasnovane na elektroničkom ključu, omogućavaju značajnu razinu pouzdanosti i točnosti. Također, sustav je jednostavan za upotrebu i pristupačan korisniku, kako s gledišta rukovanja i administriranja prava pristupa, tako i s gledišta poduzimanja hitnih zahvata pri neovlaštenom pristupu. Daljnja poboljšanja i upotreba dodatnih mogućnosti elektroničkog ključa mogu značajno pridonijeti razini inteligentnosti i sigurnosti čovjekove životne sredine.

Ključne riječi: *nadzor pristupa, inteligentnost životne sredine, elektronički ključ, mikroupravljački sustav, sigurnost.*

1 Introduction
Uvod

Access control of space, resources, data and all other resources which are preferred to be placed "behind closed doors", represents part of environment. Depending on the type of resources, limited access to the aforementioned resources is enabled by means of well-known mechanical and electrical locks and keys [3], but also by means of very intelligent systems which include identification by contact and contactless cards as in [4] and [5], as well as by identification of a person accessing some resource by measuring its biometrical features, as in [2] and [10]. One form of a physical key with electronic features is iButton [11].

iButton is an electronic key designed in form of an integrated circuit placed within steel housing. That housing ensures resistance to corrosion and acid, providing stability to the information stored within it. It was launched on the market by the American company Dallas Semiconductor [11]. Owing to robustness, small dimensions and portability, steel iButton might be built-in almost anywhere into a pendant, ring, watch or any other personal item. It might be used on a daily basis; most frequently for the purpose of controlling access to buildings and computers, handling various resources, controlling acquisition in data access and identification.

Due to additional possibilities, it is used in industry and intelligent ambients, as in [1] and [6], for measurement and storage of temperature and humidity.

Electronic keys are autonomous devices. What users see (e.g. from the outside) is a slot for iButton and LED. From the inside, the door is opened by simply pressing the button. For locking a solenoid or a bolt might be used. Serial numbers stored in the key memory might be deleted and refreshed as necessary.

Only two contacts have an electronic key, and communication is carried out through a 1-Wire bus described in [7]. The basic key design consists of a 64-bit identification code, whereas advanced designs have a possibility of measuring temperature or some other physical quantity, additional memory, etc. iButton uses steel housing as a communication interface. Every housing possesses a data contact and a grounding contact. Each contact is connected with the chip which is positioned within the housing. The data contact is placed on top of the housing and it usually covers the whole area, whereas the grounding contact is made up of sides and the bottom part of the housing and it also includes the bed which makes positioning of the key into the slot easier. Contacts are separated by a polypropylene seal.

1-Wire communication uses small data transmission rates, and power supply is carried out through a signal wire. Since the contact is most often temporary, the internal temporary memory is used for writing into the memory, i.e. the so-called scratchpad memory described in [12]. Communication is master-slave, and data transmission is asynchronous. There is a possibility of building a 1-Wire network with one master and more than one slave. This form of communication is most frequently used for communication in inexpensive devices, such as digital thermometers and meteorological instruments.

In addition to showing iButton possibilities and types, from the hardware and software point of view, this paper also presents the system which enables us to use iButton for the purpose of controlling access to space or resources. Section 2 deals with the most common and frequently used key types. Section 3 describes a software and hardware solution of the electronic lock system, whereas Section 4 analyses functionality of the described solution.

2
iButton types
Tipovi iButton ključa

2.1
Most Common Types
Osnovni tipovi

Electronic keys are widely used [9], thus they might be broadly classified into identification keys, memory keys, RTC (Real-Time Clock) keys, sensor [13] and security keys, and data storage keys. All keys must have certain memory capacity; hence, we generally deal with memory keys. Differences among keys mostly refer to additional options, such as the ones having a microprocessor, clock and/or sensor.

Memory keys can be further classified into address keys, EPROM keys, NV (Non-Volatile) RAM keys and EEPROM keys. Each model has a 64-bit ROM, which contains the so-called Family Code, a unique serial number, as well as a CRC (Cyclic Redundancy Check) code for checking proper operation of transmission. It might be applied as a key (for simple access control), as a location identificator for coordination of paths (routes, directions), for checking and maintenance of equipment, etc. NV RAM memories are read/write memories. In addition to RAM memories, there is a lithium battery, which enables data storage for at least 10 years. These keys are manufactured from 1 kb to 64 kb. They are used in such instances where frequent data refreshment is necessary.

EPROM keys have a possibility of writing memory content as a single instance. These keys are also made from 1 kb to 64 kb. They are used for permanent storage of data. EEPROM keys are read/write devices with a memory space between 256 b and 32 kb. They are used in situations when data are to be less frequently rewritten in comparison to NV RAM keys. The number of writings is limited and the manufacturer guarantees at least one million writings. These keys are cheaper than NVRAM keys, but the memory is less recordable.

RTC keys [9] are available in two types. Both of them have a clock/calendar in a binary format. The first type enables counting in seconds, whereas the second one has three separate counters. The difference between them lies also in application. In contrast to the first type, the second type has alarm, planner, software authorization, and timely controlled access.

There is a wide variety of iButton sensor types, the simplest one being a digital thermometer, which operates between -55 °C and +100 °C. A digital hygrometer for measuring humidity is a bit more complex. Sensor characteristic is also closely related to the possibility of data storage.

Security is a problem referring to the whole digital world, which is shown in e.g. [8]. Thus, security keys are made of high-quality material. There are three types i.e. three levels of security keys, whereby each of them is intended for a certain purpose.

2.2
Frequently Used Types
Često korišteni tipovi

The system described in Section 3 functions as an electronic lock which restricts access to some resource or space. Therefore, out of all aforementioned types of electronic keys, three were used. Their joint features are the following: a 64-bit serial number, an 8-bit family code, a 48-bit code, an 8-bit Cyclic Redundancy Check (CRC) code, and a possibility of building a MicroLAN network. Specific characteristics of the types used include:

- **DS1991L** - 1152-bit security NV memory, security memory cannot be decoded without a 64-bit password, memory is divided into three 384-bit blocks, a 64-bit password and ID area for every memory block, a 512-bit 'scratchpad' for data transmission, working temperature ranging from -40 °C to +70 °C, and data storage for up to 10 years.
- **DS1996L** - 65536-bit security NV memory, increasing communication rate up to 142 kbit/s by means of an overdrive mode, a 256-bit 'scratchpad' for data transmission, memory divided into 256-bit blocks, correct data transmission enabled via a strict reading and writing protocol, working temperature ranging from -40 °C to +70 °C, and data storage for up to 10 years.
- **Ds1920 -** a digital temperature sensor measures temperatures from -55 °C to +100 °C within 0,2 s, resolution of 0,5 °C, available internal counters enable improvement of resolution by interpolation, an 8-bit CRC code which enables correct data transmission, a special instruction which enables a user to start measurements simultaneously on all devices connected to the bus, a 2B EEPROM which might trigger the alarm or user memory, as well as search the alarm in order to find the device reporting a too high temperature.

3
Electonic Lock
Elektronička brava

3.1
Hardware Solution
Sklopovsko rješenje

iButton is most frequently used as an electronic lock. In that respect, persons wishing to pass through the door must possess iButton whose code in ROM matches the code in the database. Design and manufacturing of such system can be divided into hardware and software part. In contrast to software, hardware is rather simple, and a block diagram of the system is shown in Fig. 1. Power supply comes from a 5V DC source.

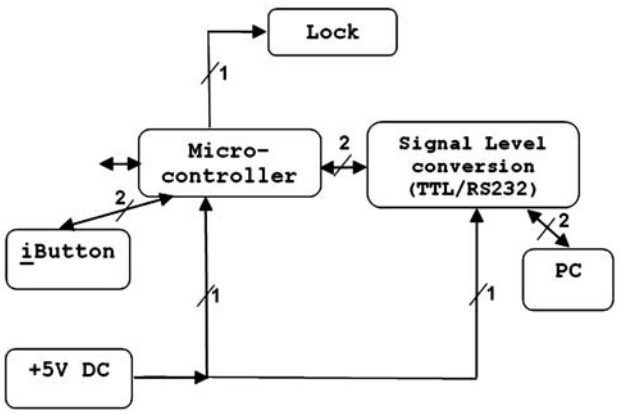

Fig 1. Block diagram of the electronic lock system
Slika 1. Prikaz sustava elektroničke brave

The main role in this system is played by a microcontroller, which ensures a connection between the computer and the iButton device. In addition to conversion of communication protocols, a microcontroller checks regularity of the received data by means of the CRC code, generates a sound signal and controls an electromechanic lock. Within the lock, there is an integrated circuit which transforms the signal level from TTL to RS-232 and vice versa. Only one signal wire is necessary for communication of a microcontroller and a 1-wire device. The other wire is used only in case of heavier current load of devices, such as writing in EEPROM, measuring temperature, etc.

Communication between the software part and the computer is carried out via the RS232 interface. The main reason for such communication lies in the fact that the microcontroller supports a UART (Universal Asynchronous Receive Transmit) protocol, which enables a simple access to the bus. Communication is half-duplex, which means that the microcontroller can both receive and transmit the data, but not simultaneously.

3.2
Software Solution
Programsko rješenje

Similarly to the project in [7], the computer can control hardware by means of the following instructions:

- "OK" - the door is opened (the key exists in the database).
- "DENIED" - the alarm is activated (the key does not exist in the database).
- "DEVICE" - presence of hardware is recognized (compatibility on the string level).

The software for the microcontroller is written in the C programming language. The structure of the main loop of the microcontroller software is shown in Fig. 2.

The software is run on a dead loop. If the key is set, its unique serial number is read, CRC is checked, and if the transmission is successful, a sound signal is generated and a code is transmitted to the computer via the RS-232 interface. After that, the computer tries to find the key code in the database. The instructions received are carried out as an interrupt subroutine shown in Fig. 3. The interrupt is caused by data (ASCII characters) entering through the RS-232 interface. These characters are acquired into a temporary memory, and upon the end of data transmission there follows processing of the received data.

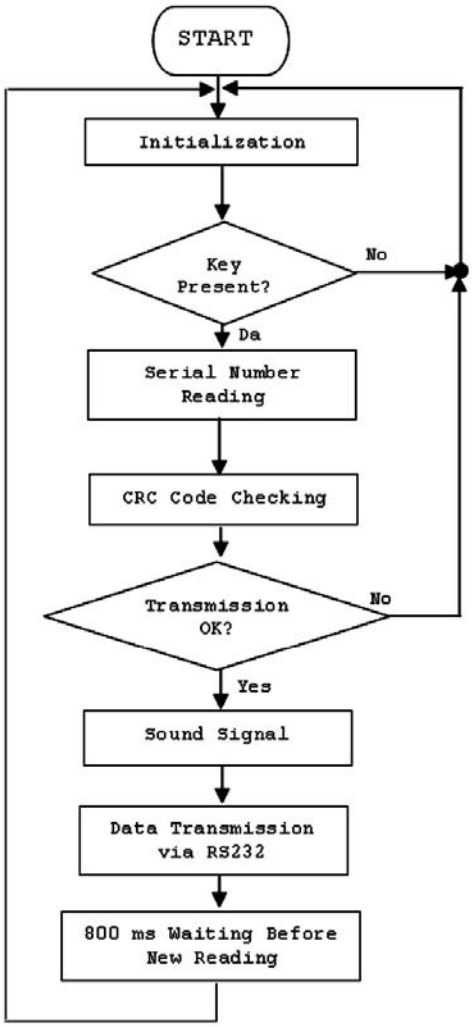

Fig. 2. Main loop of the microcontroller software
Slika 2. Glavna petlja programa mikroupravljača

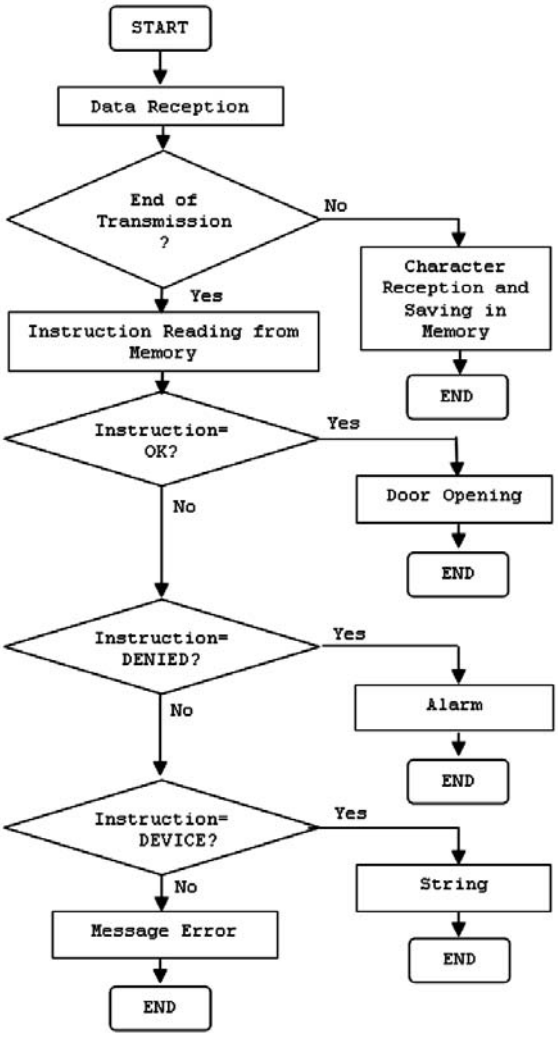

Fig. 3. Microcontroller interrupt subroutine
Slika 3. Prekidna rutina programa mikroupravljača

The second part of software support ensures communication with the database (reading, writing, searching and other necessary operations), and controls system software. This part of the software solution is realized by means of components "Microsoft Comm Control 6" described in [14]. Transmission rate is 9600 bauds, and 8 bits of data without parity and with one stop bit are transmitted. Communication with the database is carried out through basic functions of generating, reading, writing, searching and sorting.

Handling the device is very simple. It consists of selecting and setting access, which can be done either manually or automatically. With respect to the latter, the software opens free accesses and transmits the instruction "DEVICE". If it receives a suitable response, it has found a key reader. Upon starting, hardware application checks in its directory whether there exists a database named "Base.mdb". If it exists, it is opened, otherwise it is created. The database remains opened during application operation. The software has a possibility of entering a new user, whereby personal data are stored. The identification procedure on the basis of the received data (at the key) is shown in Fig. 4. iButton transmits its code by a serial connection and after that the application checks whether the key in question is in the database. If it exists, it transmits the instruction "OK" to the circuit which unlocks the electronic lock. Then the name and family name of the key owner is stored into the .log database. In case the key code is not found in the database, the application transmits the instruction "DENIED" which activates the alarm, whereby the key code is also stored into the .log database.

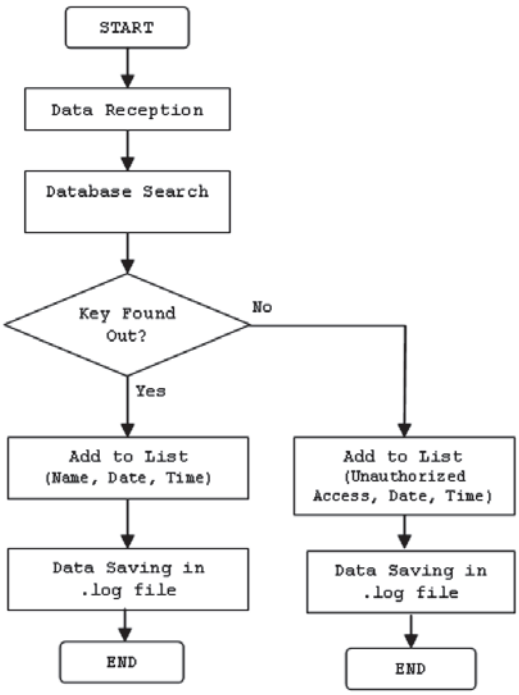

Fig. 4. Key identification procedure
Slika 4. Postupak identifikacije ključa

Fig. 5 shows an electronic lock prototype. This prototype is self-developed and placed on a printed circuit board (PCB).

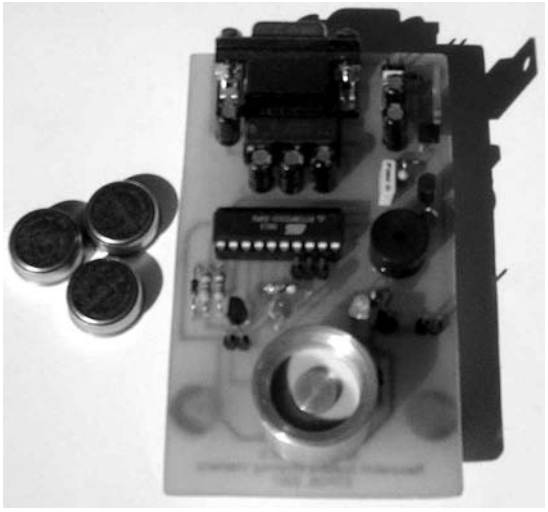

Fig. 5. Prototype of an electronic lock
Slika 5. Prototip elektroničke brave

4
Analysis of System Functionality
Analiza funkcionalnosti sustava

In the image of [8] and [13], the iButton-based developed system of an electronic lock has been used for the purpose of testing functionality in industry aimed at controlling access to spare parts storehouses, but also access to computers with confidential data. Functionality is validated on the basis of statistics referring to proper operation of the system as well as on the basis of indicators showing users' satisfaction within the period of 3 months. The given parameters have been evaluated by scores from 1 to 5, with 5 representing the highest score. Evaluation results are presented in Table 1.

Table 1. Evaluation of the system functionality
Tablica 1. Vrednovanje funkcionalnosti sustava

Parameter	Score
Operation reliability	4,17
System accuracy at key recognition	4,97
Key portability	3,71
User-friendliness of the system	4,56
Simple administration of the system	4,22
Fast discovery of unauthorized access	4,76
Access history logging	4,12
Average	4,36

Since we deal with a prototype, it is not surprising that the system has been occasionally blocked, a problem that has been quickly solved by resetting the microcontroller or the computer. Therefore, system reliability is scored by 4,17. System accuracy at key recognition is graded by a very high score, i.e. 4,97. It has happened that due to a key form and dimension users either loose or forget the key; hence, key portability is scored by 3,71. Users have estimated that the system is user-friendly (4,56), and a little bit more complicated for administration (4,22). Thanks to the alarm, the system enables fast discovery of unauthorized access (4,76), and provides a rather good overview of statistics concerning the history of access to space and resources (4,12). The average score of system functionality is very good 4,36.

5
Conclusion
Zaključak

The developed electronic lock system based on iButton represents an inexpensive and rather simple solution for access control to space, resources and data. Although scored by a relatively high grade, the system definitely requires improvements. They primarily refer to increasing reliability of the end system with respect to the prototype, adjustment of the software solution to a user, especially as to easier administration which is well laid out. Concerning hardware, the system can be improved by using additional options of the given, but also of other iButton types. They can enable a more reliable and faster communication among a greater number of monitoring nodes, as well as timely access control. Electronic key sensor possibilities might significantly improve access control in terms of increasing ambiental intelligence of the human environment.

References
Literatura

[1] Aarts, E. Ambient intelligence: a multimedia perspective, IEEE Multimedia, Vol. 11, No. 1(2004), pp. 12-19.
[2] Andrijchuk, V. A.; Kuritnyk, I. P.; Kasyanchuk, M. M.; Karpinski, M. P. Modern algorithms and methods of the person biometric identification, Proc. of 3rd IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2005), Sept. 5-7, 2005, Sofia, Bulgaria, pp. 403-406.
[3] Blaze, M. Rights amplification in master-keyed mechanical locks, IEEE Security & Privacy Magazine, Vol. 1, No. 2 (2003), pp. 24-32.
[4] Carr, M. R. Smart card technology with case studies, Proc. of 36th Annual 2002 International Carnahan Conference on Security Technology, Atlantic City, NJ, USA, Oct. 20-24 2002, pp. 158-159.
[5] Conti, M.; Di Pietro, R.; Mancini, L. V.; Spognardi, A. RIPP-FS: An RFID identification, privacy preserving protocol with forward secrecy, Proc. of 5th Annual IEEE Int. Conf. on Pervasive Computing and Communications Workshops (PerCom Workshops '07), White Plains, NY, USA, March 19-23, 2007, pp. 229-234.
[6] Doctor, F.; Hagras, H.; Callaghan, V. A fuzzy embedded agent-based approach for realizing ambient intelligence in intelligent inhabited environments, IEEE Transactions on Systems, Man and Cybernetics, Part A, Vol. 35, No. 1(2005), pp. 55-65.
[7] Downs, R. Using 1-Wire I/O for distributed system monitoring, WESCON'98 Conference Proceedings, Anaheim, CA, USA, Sept. 15-17, 1998, pp. iv+366.
[8] Gutiérrez Vela, F. L.; Isla Montes, J. L.; Paderewski Rodríguez, P.; Sánchez Román, M.; Jiménez Valverde, B. An architecture for access control management in collaborative enterprise systems based on organization models, Science of Computer Programming, Vol. 66, No. 1(2007), pp. 44-59.
[9] Henderson, N. J.; White, N. M.; Hartel, P.H. iButton Enrolment and Verification Requirements for the Pressure Sequence Smartcard Biometric, Lecture Notes In Computer Science; Vol. 2140(2001), pp. 124-134.
[10] Kim, H.-S.; Lee, S.-W.; Yoo, K.-Y. ID-based password authentication scheme using smart cards and fingerprints, Vol. 37, No. 4(2003), pp. 32-41.
[11] Maxim Integrated Products, Dallas Semiconductor, What Is an iButton? http://www.maxim-ic.com/products/ibutton/ibuttons
[12] Puaut, I.; Pais, C. Scratchpad memories vs. locked caches in hard real-time systems: a quantitative comparison, Proc. of Conf. on Design, Automation and Test in Europe (DATE'07), Nice, France, April 17-19, 2007, pp. 1484-1489.
[13] Ramamurthy, H.; Prabhu, B. S.; Gadh, R.; Madni, A. M. Wireless Industrial Monitoring and Control Using a Smart Sensor Platform, IEEE Sensors Journal, Vol. 7, No. 5(2007), pp. 611-618.
[14] Ridiko, L.; Lapitskiy, V. iButton Electronic Lock Project, Make: technology on your time, http://www.makezine.com/blog/archive/2006/08/ibutton_electronic_lock_projec.html.

This work was supported by research project grant No. 165-0362980-2002 from the Ministry of Science, Education and Sports of the Republic of Croatia.

Authors' Addresses
Adrese autora

Goran Martinovic, PhD
Faculty of Electrical Engineering
J. J. Strossmayer University of Osijek
Kneza Trpimira 2b, 31000 Osijek, Croatia
Phone: +385 31 224 766, Fax: +385 31 224 605
goran.martinovic@etfos.hr

Tibor Kis-Konja
Faculty of Electrical Engineering
J. J. Strossmayer University of Osijek
Kneza Trpimira 2b, 31000 Osijek, Croatia

Zoran Kradija
Faculty of Electrical Engineering
J. J. Strossmayer University of Osijek
Kneza Trpimira 2b, 31000 Osijek, Croatia