MIKROKRMILNIŠKI SISTEM BREZKONTAKTNE IDENTIFIKACIJE IN NADZORA PRISTOPA

Rajko Svečko, Boris Ratej
Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko, Slovenija

Ključne besede: sistemi nadzorovanja, sistemi identifikacijski, nadzor pristopa, identifikacija oseb, mediji identifikacijski brezkontaktni, mediji identifikacijski pasivni, mikrokrmilniki, protokoli komunikacijski, CAN vodila omrežij krmilnikov področij, postopki identifikacije

Povzetek. V članku opisujemo mikrokrmilniški sistem identifikacije oseb zaradi pristopa v prostore z uporabo brezkontaktnih identifikacijskih medijev. Sistem identifikacije in nadzora sestavljajo nadzorni računalnik, vmesnik med RS232 in CAN vodilom, CAN vodilo in mikrokrmilniški vmesniki, ki upravljajo čitalnike brezkontaktnih identifikacijskih medijev, krmilijo električne ključavnice, tipkovnice, LCD prikazovalnike ter druge svetlobne in zvočne naprave. Poleg identifikacije nudi opisani sistem tudi beleženja delovnega časa in popoln nadzor nad pristopi v posamezne prostore. Omogoča zajemanje podatkov o času prihoda-odhoda, pregled nad pretokom ljudi med prostori in nadzorovan pristop v vsak prostor, ki je vključen v sistem. Vsi dogodki se zapisujejo v podatkovno bazo na nadzornem računalniku, kjer so mogoče različne statistične analize o zasedenosti prostorov, izkoriščenosti opreme, prisotnosti uslužbencev itd.

Microcontroller contactless identification system and access control

Key words: control systems, identification systems, access control, personal identification, contactless identification media, passive identification media, microcontrollers, communication protocols, CAN buses, Controller Area Network buses, identification procedures

Abstract. The basic operations in the access control systems are identifications. They are divided according to identifying instruments on the PIN code, magnet storage media, fingerprint, voice, etc. and by procedures themselves divided into the contact and contactless ones /2/. Since the contactless memory medium has many advantages /5/, the contactless identification system LEGICŇ /8/ is used in the access control system which is described in this paper. This device is a Radio-Frequency Identification (RFID) system that is composed of three components - an interrogator (reader), a passive tag, and a host computer. The tag is composed of an antenna coil and a silicon chip that includes basic modulation circuitry and non-volatile memory. The tag is energized by a time-varying electromagnetic radio frequency (RF) wave (carrier signal) that is transmitted by the reader. A passive RFID tags use the backscatter modulation to send data back to the reader. By repeatedly shunting the tag coil through a transistor, the tag can cause slight fluctuations in the reader's RF carrier amplitude. This amplitude modulation loading of the reader's transmitted field provides a communication path back to the reader. In order to read multiple tags simultaneously, the tag and reader must be designed to detect the condition that more than one tag is active. A number of different methods are in use for preventing collisions.

The computerized admittance control system (Fig. 3) is globally composed of monitoring computer, interface between RS232 and CAN bus, CAN bus and micro controller interface, which manages a tag reader and LCD, controls electric key-lock and other light and acoustic signals (Fig. 4).

By establishing of a successful communication between the card reader and tag, micro controller interface reads the data from the media, redesigns them and sends them to the CAN bus. The interface between CAN and RS232 bus accepts these data, redesigns them in order to transfer them over RS232 to the monitoring computer. As the monitoring computer accepts the data package, it can differentiate between a demand for an access into the area, communication checking or some other package (alarm for example). In case of demanding an access to enter, information is shown from the data package as to who and where to be entered. The monitoring computer checks over the data base if the user has a permission to enter a certain door at that certain time or not. In both cases, it sends the data package as an answer to the microcontroller interface where it is written how to operate with light and acoustic signals and of course electric key-lock (Fig. 6). Program sent two more packets with name of the identified person when access is permitted. Name and other notices are displayed on LCD screen.

For the communication between supervisor computer and microcontroller interface CAN communication bus was used. CAN (Controller Area Network) is high reliable multimaster serial communication protocol which effectively supports distributed supervision. Each microcontroller interface receives and transmits massages with certain priorities. Interface between RS232 and CAN is exception because it receives massages regardless of the priority. Arbitration field is divided to identification (11 bits) and RTR bit (Remote Transmission Request) (Figure 5). We further divide identification field to microcontroller interface address (8 bits) and command code (remain three bits and RTR bit). This partition proved successful because we transmit bytes over RS232 bus. For command code there are only three bits left, which could address eight different commands (Table 1). Because of that command "enlargement" was defined, where real command lies in first data byte and enables expansion to 2^8 commands.

The supervisor computer manages database whit users, microcontroller interfaces, access conditions and all events. New user is added to the database whit his first name, surname and identification number. Identification number is a password for the access with microcontroller interface keyboard, which is also saved to the RFID tag. Database contains for each user access conditions, which must be fulfilled for permitting user access on certain doors. For this purpose concept of writing access conditions was developed which enables defining different access conditions for each day of a week (Table 2). Each access request (permitted or not) is written to events database. There are also all vital parameters written to database which later enables performing search in events database: who request access, on which door, time of request, was request permitted or not. Search is enabled whit one parameter or combination of different parameters.

Besides taking track of the working time, the computerized access control system also offers absolute control over accesses into certain areas (rooms). It enables the data acquisition about the time of arrival-departure, view over the circulation of people between various areas and monitored access into every area that is included in the system. Over the data, which are saved in the monitoring computer, different statistic analyses are possible, for example space occupation, utilization of equipment, presence of employees, etc.

Uvod

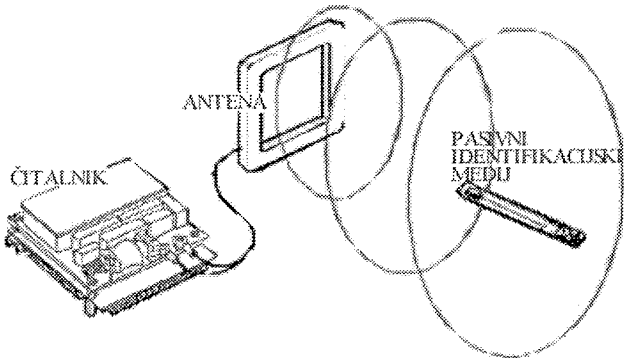
V vsakdanjem življenju se čedalje pogosteje srečujemo s storitvami in napravami, ki preverjajo našo identiteto, ob prihodu v službo, pri bankomatu ali na internetu /1/. Kako se identificiramo, je odvisno od aplikacije, ki od nas zahteva vnos gesla ali PIN kode, bodisi prek tipkovnice bodisi s pomočjo s prenosnega identifikacijskega medija /2/. Čedalje bolj pa se širi tudi uporaba biometrike (prstni odtis, identifikacija obraza itd.) /3, 4/. Pri razvoju in inštalaciji sistema nadzora pristopa je zato prvi korak izbira ustreznega identifikacijskega sistema na osnovi študije varnostnih zahtev. V primeru nadzora pristopa v prostore, je za doseganje srednje stopnje varnosti ustrezna uporaba brezkontaktnih identifikacijskih medijev (smart cards) /5/, ki jo opisujemo v tem prispevku. Naslednji korak je zasnova sistema nadzora, ki poleg beleženja delovnega časa ponujajo tudi popoln nadzor nad pristopi v posamezne prostore. V /5, 6/ je opisan računalniško vodeni sistem, ki omogoča zajemanje podatkov o času prihoda-odhoda, pregled nad pretokom ljudi med prostori in nadzorovan pristop v vsak prostor, ki je vključen v sistem.

Za razliko od znanih rešitev za identifikacijo oseb in nadzora pristopa, smo razvili modularni mrežni sistem, ki temelji na robustnem industrijskem vodilu CAN. Jedro sistema so mikrokrmilniški moduli, ki upravljajo periferne naprave (čitalnik identifikacijskih medijev, LCD prikazovalnik, tipkovnica itd.) in komunicirajo preko CAN vodila z nadzornim računalnikom, ki upravlja s podatkovnimi bazami. Pri podatkih, ki jih shranjujemo v nadzornem računalniku, so mogoče razne statistične analize, kot so na primer zasedenost prostora, izkoriščenost opreme, prisotnost uslužbencev itd.

Identifikacijski postopek

Osnovna in s stališča varnosti najpomembnejša operacija v sistemu nadzora pristopa je identifikacija. Ločimo jo lahko po obliki identifikacijskih sredstev na PIN kodo, magnetni identifikacijski medij, elektronski identifikacijski medij, prstni odtis, glas in podobno ter po samem postopku na kontaktni in brezkontaktni /1, 2, 3/. Ker imajo slednji občutne prednosti, smo v sistemu nadzora, ki ga opisujemo v tem prispevku, uporabili brezkontaktni identifikacijski sistem LEGIC® /8/. To je radio-frekvenčni identifikacijski sistem (RFID) /15/, ki je sestavljen iz čitalnika, pasivnega identifikacijskega medija (TAG) in gostiteljskega računalnika (slika 1).

Pasivni identifikacijski medij (slika 2) je sestavljen iz antene in integriranega vezja, ki vsebuje osnovno modulacijsko vezje in trajni pomnilnik (NV-RAM). Napaja se iz zunanjega spremenljivega elektromagnetnega polja (nosilni val), ki ga oddaja čitalnik. Integrirano vezje v pasivnem identifikacijskem mediju preko iste antene komunicira s čitalnikom tako, da vpliva na amplitudo nosilnega vala. Frekvenci, ki se uporabljata za nosilne valove sta standardizirani 125KHz in 13.56MHz (LEGIC SM100), kjer se izkorišča lastnost medsebojne induktivnosti med anteno oddajnika in anteno pasivnega identifikacijskega medija.

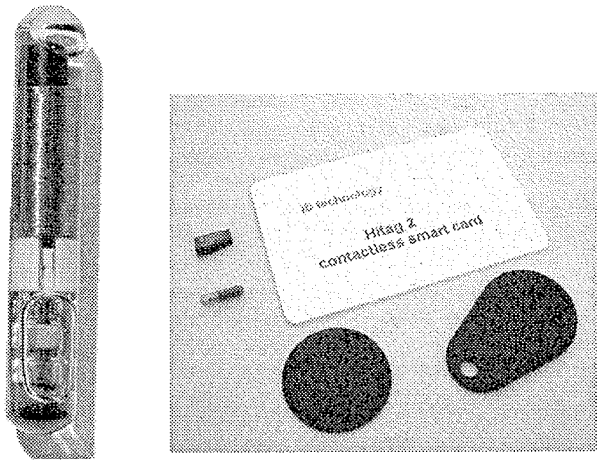


Slika 1: Elementi radio-frekvenčnega identifikacijskega sistema

Elektromagnetno polje čitalnika uporablja pasivni identifikacijski medij v tri namene:

1. V pasivnem identifikacijskem mediju se inducira dovolj veliko napajanje, da lahko integrirano vezje prične delovati. Inducirana napetost je lahko različna (od 200Vpp do 5Vpp) in je odvisna od oddaljenosti medija od antene čitalnika.
2. Večina pasivnih radio-frekvenčnih identifikacijskih medijev deli frekvenco nosilnega vala, da pridobi sinhroniziran urni signal za serijsko oddajanje podatkov čitalniku.

Služi kot nosilni signal za podatke, ki se prenašajo od pasivnega identifikacijskega medija do čitalnika. Povratno vplivanje pasivnega identifikacijskega medija na nosilni val zahteva od čitalnika, da razpozna spremembe na svojem oddajanem nosilnem valu.



a) b)

Slika 2: a) pasivni identifikacijski medij uporabljen kot implantant v projektu Cyborg /16/,
b) različne izvedbe pasivnih identifikacijskih medijev /17/

Tipični potek dogajanj med čitalnikom in pasivnim identifikacijskim medijem se izvaja na naslednji način:

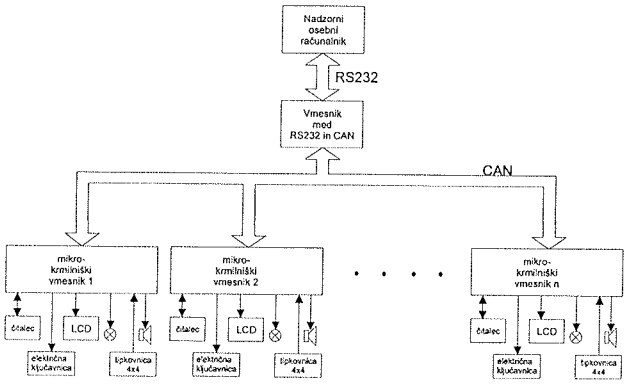
1. Čitalnik neprenehoma oddaja nosilni val in čaka na modulacijo nosilnega vala, ki predstavlja prisotnost medija v elektromagnetnem polju antene čitalnika.
2. Pasivni identifikacijski medij, ki se pojavi v elektromagnetnem polju čitalnika, najprej poskrbi za napajanje integriranega vezja. Ko ima dovolj napajanja, deli frekvenco nosilnega vala da dobi urni signal in prične s serijskim oddajanjem podatkov. Izhodni podatki dejansko krmilijo tranzistor, ki je priključen med oba konca antene pasivnega identifikacijskega medija.
3. Pasivni identifikacijski medij glede na krmilni serijski podatkovni signal preko izhodnega tranzistorja kratko spaja antensko navitje.
4. Kratki spoji na antenskem navitju povzročajo trenutno slabljenje nosilnega vala, ki se kaže v majhnih spremembah amplitude.
5. Čitalnik razpoznava spremembe amplitude nosilnega vala in obdeluje serijski podatkovni tok glede na metodo kodiranja podatkov (NRZ, manchaster) in glede na uporabljeno modulacijsko tehniko (ASK, FSK, PSK).

Postopek identifikacije zagotavlja visoko stopnjo varnosti podatkov, ki so zapisani na pasivnem identifikacijskem mediju, saj čitalnik ne more hkrati komunicirati z več mediji. Kadar je v polju antene čitalnika več kot eden pasivni identifikacijski medij, lahko pride do trkov oziroma do navzkrižnega moduliranja nosilnega signala. Z arbitražnim algoritmom je zagotovljeno, da v določenem trenutku s čitalnikom komunicira le eden. Ob vzpostavitvi komunikacije se čitalnik in pasivni identifikacijski medij dogovorita o ključu, po katerem se bodo kodirali podatki. Ključ se sestavlja iz več delov, med katerimi so tudi naključna števila. Del ključa, ki ga priskrbi medij, je odvisen od podatkov, ki so na njem zapisani, in od predhodnih dostopov do teh podatkov. Vsaka izmenjava podatkov je tako kodirana po drugem ključu. Pasivni identifikacijski medij, ki ga predamo končnemu uporabniku v uporabo moramo ustrezno programirati s sistemskim identifikacijskim medijem in pri tem upoštevati posebna varnostna pravila.

Modularni mrežni sistem nadzora pristopa

Sistem nadzora (slika 3) oblikujejo štirje sklopi: nadzorni osebni računalnik, vmesnik med RS232 in CAN vodilom, CAN vodilo in mikrokrmilniški vmesniki, ki upravljajo čitalnike identifikacijskih medijev, LCD prikazovalnike in tipkovnice, krmilijo električne ključavnice ter druge svetlobne in zvočne naprave.

Nadzorni računalnik krmili delovanje celotnega sistema. Z mikrokrmilniškimi vmesniki komunicira preko CAN vodila, zato je vsakemu mikrokrmilniškemu vmesniku, ki je priključen na CAN vodilo, dodeljen unikatni naslov dolžine enega zloga. Ta naslov je zapisan v programski kodi vmesnika in se med delovanjem ne more spreminjati. Mikrokrmilniški vmesnik ob uspešni vzpostavitvi komunikacije med čitalnikom in identifikacijskim medijem prečita podatke z medija, jih preoblikuje in pošlje po CAN vodilu. Vmesnik med CAN in RS232 vodilom te podatke sprejme, jih preoblikuje in pošlje nadzornemu računalniku. Ko nadzorni računalnik sprejme podatkovni paket, lahko ugotovi, ali gre za zahtevo po pristopu v prostor, za preverjanje komunikacije ali kakšen drugi paket (na primer alarm). V primeru zahteve po odobritvi pristopa se iz podatkovnega paketa razbere informacija o uporabniku in kje (na katerih vratih) želi vstopiti. Nadzorni računalnik preveri v podatkovni bazi, ali ima uporabnik ob tem času na teh vratih dovoljen vstop ali ne. V obeh primerih kot odgovor pošlje mikrokrmilniškemu vmesniku podatkovni paket, v katerem je zapisano, kako naj krmili svetlobne in zvočne izhode ter seveda električno ključavnico in LCD prikazovalnik. Enak postopek se izvede ob vnosu gesla prek tipkovnice.

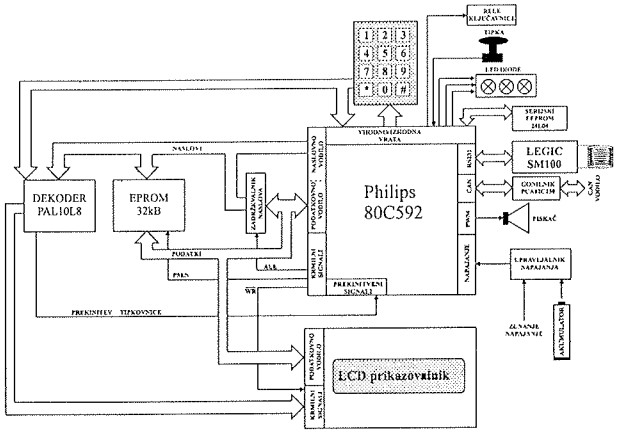


Slika 3: Shematski prikaz sistema za nadzor pristopa

Jedro nadzornega sistema so mikrokrmilniški vmesniki s Philips-ovim mikrokrmilnikom 80C592, ki je izpeljanka zelo razširjenega mikrokrmilnika 80C51 /13/. Zraven jedra, ki ga predstavlja 80C51 ima 80C592 dodana še dodatna vhodno/izhodna vrata, analogno-digitalni pretvornik, pulzno-širinski modulator (PWM) in ostale sklope. V primerjavi z ostalimi izpeljankami mikrokrmilnika 80C51 je za ta tip mikrokrmilnika značilen predvsem vgrajen CAN krmilnik. Mikrokrmilnik 80C592 ima s svojim naslovnim vodilom možnost neposrednega naslavljanja do 64k zunanjega programskega pomnilnika in do 64k zunanjega podatkovnega pomnilnika. Izbiro med programskim in podatkovnim pomnilnikom izvaja s posebnim signalom PSEN (Program Store ENable). Mikrokrmilnik nima ločenega naslovnega prostora za vhodno/izhodne naprave. Vhodno/izhodne naprave, ki jih v sistemu uporabljamo in do katerih bi radi dostopali s podatkovnim vodilom, je potrebno z uporabo ustreznega dekodirnika naslovnega prostora vključiti v zunanji pomnilniški naslovni prostor /14/.

Izdelan mikrokrmilniški vmesnik (slika 4) ima 32kB zunanjega programskega pomnilnika (možnost razširitve na 64kB) iz katerega se izvaja program, nima pa posebej zunanjega podatkovnega pomnilnika. Programske spremenljivke se

shranjujejo v notranji podatkovni pomnilnik mikrokrmilnika 80C592. Nastavitve spremenljivk, ki so ključnega pomena pri identifikaciji posameznega mikrokrmilniškega vmesnika znotraj sistema nadzora in od katerih zahtevamo, da vrednost zadržijo tudi pri morebitnem izpadu napajanja, so shranjene v serijskem EEPROM-u velikosti 512B. Dostop do LCD prikazovalnika se izvaja preko zunanjega podatkovnega naslovnega prostora, z nepopolnim dekodiranjem v naslovnem prostoru do 32k. Za dekodirnik naslovnega prostora se uporablja programabilno logično vezje PAL10L8, ki vsebuje tudi logiko za proženje prekinitve mikrokrmilnika v primeru pritiska tipke uporabniške tipkovnice (matrična tipkovnica 3x4). Mikrokrmilniški vmesnik komunicira s čitalnikom SM100 preko RS232 vmesnika neposredno brez pretvornika nivojev. Na CAN vodilo se CAN krmilnik mikrokrmilnika 80C592 priključi preko gonilnika PCA82C250. Mikrokrmilniški vmesnik vsebuje zraven naštetega tudi nadomestno akumulatorsko napajanje s polnilcem, ki skrbi za napajanje v primeru izpada centralnega oz. lokalnega napajanja. Za komunikacijo med uporabnikom in mikrokrmilniškim vmesnikom služi tipkovnica in LCD prikazovalnik, piskač, ki se krmili s PWM izhodom mikrokrmilnika, ter LED diode, ki so priključene na vhodno/izhodna vrata mikrokrmilnika. Na vhodno/izhodna vrata mikrokrmilnika je priključena tudi tipka, ki je namenjena odpiranju vrat iz notranjosti prostora (odpiranje v primeru, ko nekdo trka na vrata) in krmilni tranzistor releja namenjen krmiljenju elektronske ključavnice.



Slika 4: Blokovna shema mikrokrmilniškega vmesnika

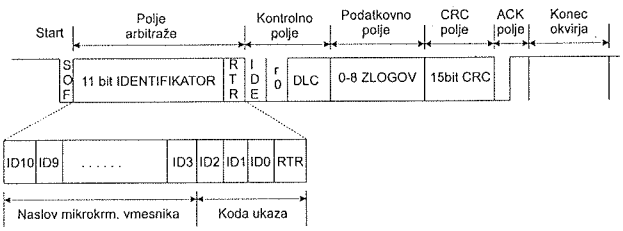
Vmesnik med RS232 in CAN (slika 3) je po konfiguraciji enak mikrokrmilniškemu vmesniku, le da ima vgrajen RS232 pretvornik nivojev, nima pa vgrajenega čitalnika SM100. Program, ki se izvaja na tem vmesniku se razlikuje od programov mikrokrmilniških vmesnikov, ki vsebujejo čitalnike, saj je posebej prirejen za preslikovanje in zajemanje CAN sporočil, ki jih nato preko RS232 povezave posreduje programu nadzorovanja prostorov, ki se izvaja na osebnem računalniku.

Komunikacija na CAN vodilu

Komunikacija med nadzornim računalnikom in mikrokrmilniškimi vmesniki poteka po CAN (Controller Area Network) vodilu. CAN je serijski multimaster komunikacijski protokol, ki z visoko stopnjo varnosti zelo učinkovito podpira porazdeljen nadzor. Je sporočilno naravnan protokol, ki ne vsebuje cilja sporočila, ampak opisuje pomen podatkov /7/.

Naprava, ki želi oddati sporočilo, najprej s tipanjem nivoja linije preveri, ali je vodilo prosto. Če je prosto, prične oddajati sporočilo, v nasprotnem primeru pa si po določenem času zopet poskuša pridobiti vodilo. Vsaka naprava, ki oddaja sporočilo, tudi preverja trenutni nivo podatkovne linije. Če se oddani in otipani nivo razlikujeta, to pomeni, da je izgubila tekmovanje za vodilo, in takoj postane sprejemnik sporočila. V sistemu ima vsaka naprava svoj unikatni naslov, ki je določen z identifikatorjem. Vsak mikrokrmilniški vmesnik sprejema in oddaja samo sporočila ene prioritete. Izjema je vmesnik med RS232 in CAN, ki sprejema vsa sporočila, ne glede na prioriteto.

Vsak okvir se začne s SOF (Start Of Frame) bitom, ki označuje začetek okvirja in sinhronizira sprejemnike z oddajnikom. Polje arbitraže, ki je dolgo 12 bitov, je razdeljeno na identifikator (11 bitov) in RTR bit (Remote Transmission Request) (slika 5). Identifikator smo razdelili naslov mikrokrmilniškega vmesnika (8 bitov) in na kodo ukaza (preostali trije biti identifikatorja in RTR bit). Takšna razdelitev se je izkazala za smiselno, ker prek RS232 vodila prenašamo zloge. Tako imamo naslov v enem zlogu, kodo ukaza pa združimo z biti kontrolnega polja in dobimo drugi zlog. Podatkovno polje je lahko dolgo od 0 do 8 zlogov, kar določimo z vrednostjo, zapisano v DLC (Data Lenght Code). Za podatkovnim poljem sledi CRC (Cyclic Redundancy Check) polje, ki služi preverjanju pravilnosti sprejetih podatkov. Če so podatki pravilno preneseni, potem sprejemnik prepiše en bit v ACK (Acknowledge) polju z dominantnim nivojem in oddajnik tako ve, da je bilo sporočilo pravilno sprejeto. Za ACK poljem je še polje recesivnih bitov, ki označujejo konec okvirja.



Slika 5: Standardni CAN format

Ker so za kodo ukaza ostali le trije biti, ki omogočajo zapis osmih ukazov (tabela 1), smo definirali ukaz Razširitev, kjer se dejanska koda ukaza nahaja v prvem podatkovnem zlogu. S tem je omogočena razširitev še na 28 ukazov.

Koda ukaza (hex)	Ukaz
0	Zahteva po pristopu
2	Preverjanje komunikacije
4	Alarm
6	Reset
8	Postavitev izhodov
A	Razširitev (koda ukaza je v prvem podatkovnem zlogu)
C	Beri iz EEPROM-a
E	Piši v EEPROM

Tabela 1: Nabor ukazov in njihovo kodiranje

Krmiljenje in vizualizacija sistema

Programska oprema na nadzornem računalniku upravlja prek uporabniškega vmesnika s celotnim sistemom /12/. Poleg naloge, da odloča o odobreni oziroma zavrnjeni zahtevi po pristopu, opravlja tudi preverjanje komunikacije za vsak mikrokrmilniški vmesnik posebej. V enakomernih programsko nastavljivih časovnih presledkih naslovi eno od naprav in ji pošlje paket, v katerem je podatek o sistemski uri. Ko naslovljena naprava sprejme paket, obnovi zapis na LCD prikazovalniku in kot odgovor nadzornemu računalniku pošlje svoj status. Če nadzorni računalnik ne sprejme tega paketa v vnaprej predvidenem času, to pomeni, da naprava ne deluje pravilno, in to tudi izpiše na uporabniškem vmesniku.

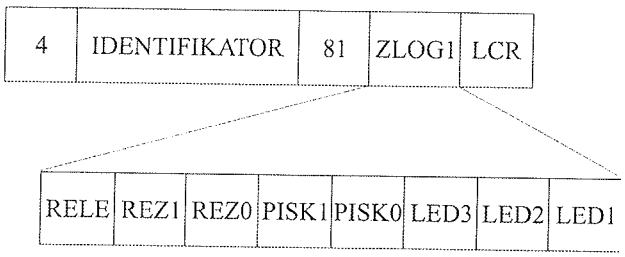
Nadzorni računalnik vodi podatkovno bazo, v kateri so zapisani uporabniki, mikrokrmilniški vmesniki (vrata), pogoji za odobritev pristopov in vsi dogodki. Ko dodajamo novega uporabnika, moramo vnesti njegovo ime in priimek, identifikacijsko številko in vpisno številko. Identifikacijska številka se zapiše na medij, ki ga dobi uporabnik, oziroma je tudi geslo, ki ga lahko vnesemo prek tipkovnice. Vpisna številka pa je dodana kot opcija, če bi se sistem povezoval v druge informacijske sisteme. Ob vnosu novega uporabnika v bazo zapišemo pogoje, ki morajo biti izpolnjeni, da se uporabniku na določenih vratih odobri pristop. Izdelali smo koncept zapisovanja pogojev, da lahko oblikujemo različne pogoje, ki veljajo ob določenih dnevih v tednu. Tabela 2 prikazuje nekaj mogočih oblik pogojev za pristop.

pogoj	omogočen pristop
0	ni dnevnih in časovnih omejitev
tor,00:00,23:59;	torek brez časovnih omejitev
sre,08:30,14:00;	sreda od 8:30 do 14:00
čet,09:15,12:00;čet,13:30,16:30;	četrtek od 9:15 do 12:00 in od 13:30 do 16;30

Tabela 2: Primeri oblikovanja pogojev dostopa

Zaradi modularnosti izvedemo širitev sistema z dodajanjem novih mikrokrmilniških vmesnikov enostavno z zapisom njegovega naslova (ID) v podatkovno bazo.

Ko osebni računalnik sprejme zahtevo po dostopu, preveri, ali obstaja uporabnik z ustrezno identifikacijsko številko. Če takšnega zapisa v podatkovni bazi ne najde, se takoj pošlje podatkovni paket za zavrnitev dostopa. V nasprotnem primeru program pregleda tabelo s pogoji. Glede na zapisan pogoj se sprejme odločitev, ali bo dostop odobren ali ne. Program pošlje ustrezen podatkovni paket za odobren oziroma zavrnjen dostop, z ustrezno postavljenimi biti v zlogu, ki krmili ključavnico ter svetlobno in zvočno signalizacijo (slika 6).



Slika 6: Podatkovni paket odobritve pristopa

V primeru odobritve pristopa pošlje program še dva podatkovna paketa z imenom osebe, ki se je identificirala. Ime se skupaj z ostalimi obvestili izpiše na LCD prikazovalniku.

Vsaka zahteva po pristopu (odobrena ali zavrnjena) se zapiše v podatkovno bazo dogodkov. Zapišejo se vsi vitalni parametri, ki jih kasneje uporabljamo kot kriterije pri poizvedbah v podatkovni bazi dogodkov: kdo je zahteval dostop, na kateri napravi, čas sprejete zahteve in ali je bil dostop odobren ali ne. Poizvedbe so možne s posameznim kriterijem ali s poljubno kombinacijo več kriterijev.

Sklep

Opisani sistem računalniškega nadzora pristopa lahko poleg osnovnega namena (odpiranje vrat, dovolitev ali zavračanje vstopa, beleženje vstopov) uporabljamo še za pridobivanje informacij o zasedenosti prostorov, prisotnosti posameznih oseb v določenem prostoru ali kot alarmni sistem. V ta namen vključimo v sistem čitalnike identifikacijskih medijev s po dvema usmerjenima antenama, ki tako dajeta informacije tudi o izstopih iz prostorov. Tako lahko na nadzornem računalniku vodimo evidence o prisotnosti oseb za posamezni prostor.

V sistem nadzora so vključeni mehanizmi za samopreverjanje delovanja, ki ob izpadu posamezne naprave sprožijo dogovorjene postopke za čim manj moten pristop v prostore. Za primer krajših izpadov električnega toka (do ene ure), je sistem opremljen z inteligentnim sistemom neprekinjenega napajanja.

Literatura

/1/ Security technology, *IEEE Aerospace and Electronics Systems Magazin*, vol. 15, issue 10, pp. 131-136, 2000.

/2/ Sanchez-Reillo, R.: Smart card information and operations using biometric, *IEEE Aerospace and Electronics Systems Magazin*, vol. 16, issue 4, 2001.

/3/ Sanchez-Reillo, R.; Sanchez-Avila, C.; Gonzalez-Marcos, A.: Improving access control security using iris identification, in *Proc. IEEE 2000 Int. Carnahan Conf. On Security Technology*, pp. 56-59, 2000.

/4/ Jain, A.K.; Prabhakar, S.; Lin Hong; Pankanti, S.: FingerCode: a filterbank for fingerprint representation matching, in *Proc. Computer Society Conference on Computer Vision and Pattern Recognition*, vol. 2, 1999.

/5/ Chor L.P.; Chong T.E.: Group accesses with smart card and threshold scheme, in *Proc. TENCOM 99 IEEE Region 10 Conference* , pp. 415-418, 1999.

/6/ Rumble, R.P.; Jong, D.Y.; Kluz, S.M.: The CAIN II access-control system, in *Proc. IEEE 1988 Int. Carnahan Conf. On Security Technology*, pp. 127-132, 1988.

/7/ Cena, G.; Valenzano, J.D.: A distributed mechanism to improve fairness in CAN network, in *Proc. IEEE Int. Workshop on Factory Communication Systems*, pp. 3-11, 1995.

/8/ LEGICŃ Info level 3, Bauer Kaba AG, 1997.

/9/ Philips Semiconductors, *Data sheet PCA82C250 CAN controller interface*, Philips electronics, 1996

/10/ Philips Semiconductors, *Data sheet P8x2C592 8-bit microcontroller with on-chip CAN*, Philips electronics, 1996.

/11/ Schultz, T.W.: *C and the 8051 Programming for Multitasking*, Pretince Hall, New Jersey, 1993.

/12/ Svečko, R.; Čučej, Ž.; Petrič, A.: Računalniški sistem nadzora dostopa v prostore, *Elektrotehniški vestnik*, 1999, letn. 66, št. 3, str. 168-175.

/13/ Philips Semiconductors, *P8xC592 8-bit microcontroller with on-chip CAN*, Data Sheet, 6/1996.

/14/ Ratej, B.: *Diskretna PI in PID regulacija z mikrokrmilniškim sistemom*, diplomsko delo, Fakulteta za elektrotehniko, računalništvo in informatiko, Maribor, 4/1996.

/15/ Passive RFID Basics, *Microchip*, AN680, 1998.

/16/ http://www2.cyber.rdg.ac.uk/implant/IEVersionSmall/index.html

/17/ http://www.ibtechnology.co.uk/cards.htm

Rajko Svečko
Boris Ratej
Univerza v Mariboru, Fakulteta za elektrotehniko, računalništvo in informatiko
Smetanova 17, 2000 Maribor, Slovenija
e-mail: rajko.svecko@uni-mb.si

Prispelo (Arrived): 21.06.2001 *Sprejeto (Accepted): 20.08.2001*