Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Aleš Boštjančič

Vgrajen sistem za obračunavanje porabe vode in električne energije na javnih mestih

diplomsko delo

visokošolski strokovni študijski program prve stopnje
računalništvo in informatika

Mentor: prof. dr. Patricio Bulić

Ljubljana, 2013

Rezultati diplomskega dela so intelektualna lastnina avtorja in Fakultete za računalništvo in informatiko Univerze v Ljubljani. Za objavljanje ali izkoriščanje rezultatov diplomskega dela je potrebno pisno soglasje avtorja, Fakultete za računalništvo in informatiko ter mentorja.

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tržaška 25
1001 Ljubljana, Slovenija
telefon: 01 476 84 11
01 476 83 87
faks: 01 426 46 47
01 476 87 11
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 00295/2012
Datum: 13.04.2012

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **ALEŠ BOŠTJANČIČ**

Naslov: **VGRAJEN SISTEM ZA OBRAČUNAVANJE PORABE VODE IN ELEKTRIČNE ENERGIJE NA JAVNIH MESTIH**

AN EMBEDDED SYSTEM FOR WATER AND ENERGY CONSUMPTION ACCOUNTING IN PUBLIC PLACESS

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija prve stopnje

Tematika naloge:

Načrtujte vgrajen sistem za merjenje porabe vode ter električne energije na javnih mestih, kot so marine, avtokampi ipd. Izvedba naj temelji na sodobnem mikrokrmilniškem sistemu z jedrom ARM in ustreznimi senzorji za zajem podatkov o porabi virov. Sistem naj omogoča individualno beleženje porabe za posameznega odjemalca. Identifikacija uporabnika naj se izvede s pomočjo tehnologije RFID. Poleg vgrajenega sistema razvijte še spletno aplikacijo, ki omogoča pregled ter upravljanje dobroimetja in celotnega sistema.

Mentor:
izr. prof. dr.Patricio Bulić

Dekan:
prof. dr. Nikolaj Zimic

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

Izjava o avtorstvu diplomskega dela

Spodaj podpisani Aleš Boštjančič, z vpisno številko 63090378, sem avtor diplomskega dela z naslovom:

Vgrajen sistem za obračunavanje porabe vode in električne energije na javnih mestih

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom prof. dr. Patricia Bulića,
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela
- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki "Dela FRI".

V Ljubljani, dne 15. januarja 2013 Podpis avtorja:

Zahvala

Zahvaljujem se mentorju prof. dr. Patriciu Buliću za mentorstvo in pomoč pri izdelavi diplomske naloge.

Posebna zahvala gre partnerki Marjani in sinu Roku ter obema družinama, za razumevanje in podpori pri študiju.

Kazalo

Povzetek

Abstract

1 Uvod **1**

2 Računalniška omrežja **3**

2.1 Komunikacijski model ISO/OSI 3

2.2 Komunikacijski model TCP/IP 4

2.3 Ethernet 5

2.4 Naslavljanje MAC 6

2.5 Mehanizem ARP 7

2.6 Protokol IP 8

2.7 Protokol TCP 9

2.8 Protokol HTTP 10

3 Sistem RFID **11**

3.1 Klasifikacija sistemov glede na funkcionalnost 12

3.2 Prenos energije in podatkov med čitalcem ter ključem 15

3.2.1 Induktivno sklopljeni sistem 15

3.2.2 Elektromagnetno sklopljeni sistem 15

3.2.3 Električno sklopljeni sistemi 16

3.3 Prenos podatkov od čitalca na ključ 16

3.4 Varen prenos podatkov 16
3.4.1 Simetrična vzajemna identifikacija 16
3.4.2 Avtentikacija z izpeljanimi ključi 16
3.4.3 Varen prenos podatkov 17
3.5 Standardi RFID 17
3.5.1 Identifikacija živali 17
3.5.2 Brezkontaktne pametne kartice 18
3.5.3 Standard MIFARE 19

4 Terminal ELVO **23**

4.1 Centralno krmilno vezje 25
4.1.1 Jedro ARM 25
4.1.2 Procesorska plošča mbed 26
4.1.3 Napajanje vezja 28
4.1.4 Grafični prikazovalnik ter vmesnik na dotik 28
4.1.5 Identifikacija uporabnika s sistemom RFID 31
4.1.6 Zajem podatkov o porabi vode 32
4.1.7 Zajem podatkov o porabi električne energije 33
4.1.8 Vhodni kanali 34
4.1.9 Izhodni kanali 35
4.1.10 Meritev temperature 36
4.1.11 Vmesnik za omrežje Ethernet 36
4.2 Programska oprema 36
4.2.1 Operacijski sistem SmartX 37
4.2.2 Omrežni sklad TCP/IP – mikroNet 38
4.2.3 Osnovna programska oprema 38
4.2.4 Beleženje podatkov o porabi virov 39
4.2.5 Komunikacija s strežnikom 39

4.2.6 Identifikacija uporabnika s pomočjo RFID 41
4.2.7 Uporabniški grafični vmesnik na terminalu 42
4.2.8 Krmiljenje izhodov 43

5 Strežniška programska oprema **45**

5.1 Spletni strežnik Apache 45
5.2 Skriptni jezik PHP 46
5.3 Podatkovna baza MySQL 46
5.4 Terminalski vmesnik 47
5.4.1 Dokumenti HTML 47
5.4.2 Grafični zapis WBMP 47
5.4.3 Konceptualni model podatkovne baze 48
5.5 Administracijski uporabniški vmesnik 48
5.5.1 Pregled porabe 49
5.5.2 Upravljanje uporabnikov 49
5.5.3 Administracija sistema 50

6 Sklepne ugotovitve **51**

Slike

2.1 Model ISO/OSI 4

2.2 Prehod podatkov med plastmi modela TCP/IP 5

2.3 Sestava naslova MAC [1] 7

2.4 Zapis podatkov v datagramu IP (IPv4) 8

3.1 Klasifikacija sistemov RFID glede na funkcionalnost [35] 13

3.2 Družine pametnih kartic s pripadajočimi standardi [35] 18

4.1 Zgradba priključnega terminala ELVO 24

4.2 Bločna shema centralnega vezja terminala ELVO 24

4.3 Izdelano centralno krmilno vezje (spredaj in zadaj) 26

4.4 Pregled nivojev izvajanja ter pripadajočih registrov jedra ARM7 [36] . . . 27

4.5 Plošča mbed z oznakami priključnih kontaktov [2] 28

4.6 Osnovna priključitev EADOGL-128 prikazovalnika [3] 29

4.7 Krmiljenje signalov serijskega vmesnika SPI [3] 29

4.8 Dimenzijska skica (a) in tehnični podatki folije na dotik (b) [3] 30

4.9 Vodna merilna turbina s pulznim izhodom 33

4.10 Števec porabe električne energije DDS-1L 34

4.11 Vhodno vezje posameznega kanala 35

4.12 Vezje izhodnega kanala 35

4.13 Priključitev senzorja temperature LM75 36

4.14 Logični nivoji na vmesniku UART, pri prenosu enega zloga v formatu 8N1 41

4.15 Pregled možnih stanj (strani) uporabniškega menija 43

5.1 Zgradba celotnega sistema z dvema terminaloma 46

5.2 Konceptualni model podatkovne baze 48

5.3 Pregled porabe po terminalu 49

Tabele

3.1 Pregled frekvenčnih področij RFID [20] 13
3.2 Karakteristike komunikacije po standardu ISO/IEC 14443 [35] 19

4.1 Seznam poznanih ukazov prikazovalnika EADOG [3] 30
4.2 Primer podatkovnega ukaza za branje podatkov ali identifikacije kartice [4] 32
4.3 Karakteristike impulznega izhoda po standardu ISO/IEC 62053-31 33

5.1 Zapis datoteke WBMP 47

Seznam uporabljenih kratic in simbolov

RFID	Radio Frequency Identification
RISC	Reduced Instruction Set Computer
IEEE	Institute of Electrical and Electronics Engineers
FDDI	Fiber Distributed Data Interface
ATM	Asynchronous Transfer Mode
EEPROM	Electrically Erasable Programmable Read-Only Memory
RAM	Random Access Memory
SRAM	Static Random Access Memory
CPU	Central Processing Unit
PHY	Physical Layer
LCD	Liquid Crystal Display
LED	Light Emitting Diode
TFT	Thin Film Transistor
COG	Chip On Glass
USB	Universal Serial Bus
ARM	Advanced RISC Machine
TTL	Transistor-Transistor Logic

FIFO	First In First Out
VIC	Vector Interrupt Controller
DMA	Direct Memory Access
SSP	Synchronous Serial Port
UART	Universal Asynchronous Receiver Transmitter
I^2C	(tudi IIC) Inter-Integrated Circuit
SPI	Serial Peripheral Interface
ADC	Analog to Digital Converter
DAC	Digital to Analog Converter
CAN	Controller Area Network
PLL	Phase Locked Loop
UHF	Ultra High Frequency
ASK	Amplitude Shift Keying
FSK	Frequency Shift Keying
PSK	Phase Shift Keying
CSMA/CD	Carrier sense multiple access with collision detection
CRC	Cyclic Redundancy Check
MAC	Media Access Control
EUI	Extended Unique Identifier
OUI	Organizationally Unique Identifier
NIC	Network Interface Controller
ISO/OSI	International Organization for Standardization / Open Systems Interconnection
TCP/IP	Transmission Control Protocol / Internet Protocol

ARP	Address Resolution Protocol
IP	Internet Protocol
TCP	Transmission Control Protocol
ICMP	Internet Control Message Protocol
SMTP	Simple Mail Transfer Protocol
HTTP	Hyper Text Transfer Protocol
FTP	File Transfer Protocol
HTML	Hyper Text Markup Language
XML	Extensible Markup Language
URL	Uniform Resource Locator
UID	Unique Identification Number
QR	Quick Response code
OTP	One Time Programmable memory
AES	Advanced Encryption Standard
EAS	Electronic Article Surveillance systems
GCC	GNU Compiler Collection
PHP	PHP: Hypertext Preprocessor
SUPB	Sistem za Upravljanje s Podatkovnimi Bazami
PNG	Portable Network Graphics
JPEG	Joint Photographic Experts Group
WBMP	Wireless Bitmap
WAP	Wireless Application Protocol

Povzetek

Diplomska naloga opisuje razvoj vgrajenega sistema za obračunavanje porabe vode in električne energije na javnih mestih. Primeri uporabe so objekti, kot so: marine, komunalni privezi, avtokampi ali podobni infrastrukturni objekti.

Izvedba sistema temelji na sodobnem mikrokrmilniškem sistemu z ustreznimi senzorji za zajem podatkov o porabi virov, obdelavi le-teh ter poročanju stanja centralnemu strežniku. Sistem omogoča individualni dostop le avtoriziranim uporabnikom storitev in tako individualno beleženje porabe za posameznega odjemalca. Identifikacija uporabnika se vrši z uporabo tehnologije RFID. V ta namen vsak uporabnik prejme v uporabo ustrezen identifikacijski ključ RFID, s katerim dostopa do sistema. Upravljanje uporabniškega dobroimetja je omogočeno z namensko razvito spletno aplikacijo, s katero sta možna pregled in upravljanje celotnega sistema tako lokalno (na območju sistema) kot tudi iz oddaljene lokacije, preko interneta.

Ključne besede: tehnologija RFID, sklad mikroNet TCP/IP, mikrokrmilnik ARM7, standard MIFARE, vgrajeni operacijski sistem SmartX, prikazovalnik s tekočimi kristali DOGL-128

Abstract

This thesis focuses on a embedded system for water and energy consumption accounting in public places, such as marinas, municipal mooring berths or camping places.

The system is based on an advanced microcontroller system combined with specific water and electricity consumption sensors. It allows consumption monitoring on an individual basis. As such, is designed to grant access only to authorized users. User identification is performed by using RFID technology. Each user authenticates on the system by using his own RFID key. The system is composed of a central server and one or more user terminals, interconnected by Ethernet. The server authorizes access to any single user based on user authentication, while at the same time providing persistent storage for user's consumption data. There is provision for system administration by implementing a web-based application. As such it can be administered either locally, on the site, or from remote locations by using internet access.

Key words: RFID technology, mikroNet TCP/IP stack, ARM7 microcontroller, MIFARE standard, SmartX embedded operating system, LCD display DOGL-128

Poglavje 1

Uvod

Pri ponudnikih storitev, kot so komunalni privezi, marine ali avtokampi, se pojavlja vprašanje načina zaračunavanja porabe vode in električne energije. Možen je pavšalni obračun stroškov, ki pa ni pravičen do uporabnikov, ki redkeje ali manj uporabljajo omenjene storitve, in po drugi strani privilegira uporabnike, ki te storitve uporabljajo bolj pogosto. S tega vidika je smiselno vzpostaviti način obračunavanja stroškov glede na dejansko porabo vira. Tako je hkrati omogočeno spremljanje statistike porabe in s tem možne optimizacije infrastrukture. V ta namen se je uveljavila uporaba namensko razvitih ter računalniško podprtih t. i. "priključnih terminalov", s pomočjo katerih je možno uporabnikom nuditi obračun stroškov skladno z dejansko porabo vira.

V tej diplomski nalogi bomo opisali razvoj in delovanje takega priključnega terminala. Na začetku diplomske naloge bomo opisali nekaj ključnih tehnologij, ki smo jih uporabili pri izdelavi terminala, nato sledi predstavitev strojne in programske zasnove ter sam opis delovanja.

Sistem je sestavljen iz centralnega strežnika ter ene ali več oddaljenih terminalskih enot, imenovanih "Terminal ELVO". Strežnik je uporabljen kot koordinator delovanja celotnega sistema. Posamezni terminali so z omrežno povezavo neprekinjeno povezani s strežnikom in tako v realnem času posredujejo podatke o stanju terminala, najsi bo to prijava uporabnika z uporabo RFID (angl. *Radio Frequency Identification*), stanje porabe določenega vira ali druge delovne parametre. Terminali izvršujejo tudi aktivacijo ali deaktivacijo posameznega vira glede na prejete ukaze s strežnika. Za izdelavo sistema smo uporabili nekatere že obstoječe rešitve, predvsem na strežniški strani, kot sta spletni strežnik in relacijska podatkovna baza. Nekatere pa smo namenoma razvili za potrebe sistema, med katerimi lahko izpostavimo knjižnico za obdelavo in prikazovanje dokumentov v formatu HTML (angl. *Hyper Text Markup Language*).

Poglavje 2

Računalniška omrežja

2.1 Komunikacijski model ISO/OSI

Komunikacijski model ISO/OSI (angl. *International Organization for Standardization/Open Systems Interconnection*) je bil zasnovan leta 1984 kot referenčni model za računalniške komunikacije [5]. Opredeljuje sedem ločenih plasti, od katerih vsaka plast opravlja določeno funkcijo oz. definira nek nivo modela. Vsaka plast (N) nudi storitve (streže) višji plasti (N + 1) ter zahteva storitve (odjema) nižje plasti (N - 1). Pravila komuniciranja med istoležnima procesoma (entitetni par) imenujemo protokol. Slika 2.1 prikazuje entitetne pare procesov ter posamezne plasti.

Seznam plasti zajema:

1. fizično plast – predpisuje zahteve za prenosni medij, preko katerega se prenašajo podatki, definira nivoje signala, hitrosti prenosa, način kodiranja ter multipleksiranja podatkov;

2. povezavno plast – določa okvirjanje bitov sporočila, načine ugotavljanja in popravljanja napak ter kontrolo pretoka;

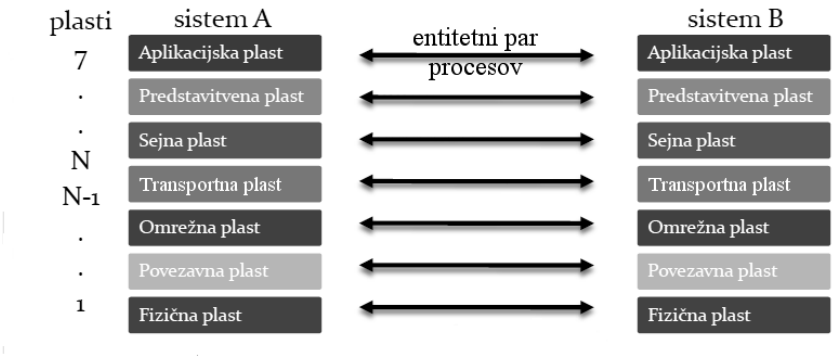
3. omrežno plast – omogoča prenos podatkov višjenivojskih plasti ne glede na tip prenosnega medija ter njegove lastnosti, skrbi za usmerjanje, posredovanje in izogibanje zamašitvam;

4. transportno plast – zagotavlja zanesljivost prenosa podatkov, učinkovitost pošiljanja ter način prenosa večjih paketov podatkov;

5. sejno plast – vzpostavlja in prekinja komunikacijo med enotami, določa vrsto komunikacije (enosmerno, dvosmerno) ter upravlja logično povezovanje procesov znotraj aplikacij (aplikacijsko multipleksiranje);

6. predstavitveno plast – zagotavlja različne načine kodiranja in sintakse sporočil ter njihovo kompresijo;

7. aplikacijsko plast – definira protokole za storitve, kot so npr. SMTP (angl. *Simple Mail Transfer Protocol*), HTTP (angl. *Hyper Text Transfer Protocol*), FTP (angl. *File Transfer Protocol*) in ostali visokonivojski protokoli.



Slika 2.1: Model ISO/OSI

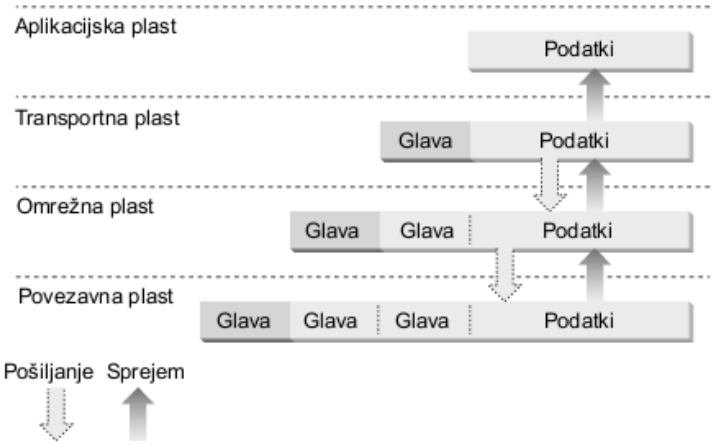
Model ISO/OSI se v praksi ni uveljavil kot samostojen komunikacijski model implementacije, ampak je dobra osnova za izpeljavo drugih komunikacijskih modelov, npr. TCP/IP (angl. *Transmission Control Protocol/Internet Protocol*).

2.2 Komunikacijski model TCP/IP

Komunikacijski model TCP/IP [6] poenostavlja model ISO/OSI. Tako združuje nekatere nivoje oz. plasti ISO/OSI modela in s tem zmanjša skupno število nivojev. Model TCP/IP ni tako sistematičen kot model ISO/OSI, saj se nekatere funkcionalnosti v določeni meri prepletajo med plastmi. Plasti modela TCP/IP so zajete v dokumentu [7].

Model ima štiri nivoje, in sicer:

1. povezavno plast – združuje fizično in povezavno plast modela ISO/OSI, definira nizkonivojske zahteve za omrežja, kot so formati in tipi kodiranja podatkov, kakor tudi nivoji in tip signala za prenos po določenem mediju;



Slika 2.2: Prehod podatkov med plastmi modela TCP/IP

2. internetno ali omrežno plast – definira tip in format naslovov za uporabo v omrežju TCP/IP, skrbi za usmerjanje podatkov glede na izbrano destinacijo in trenutno stanje omrežja (izogibanje zamašitvam);

3. transportno plast – ima enako vlogo kot istoimenska plast v modelu ISO/OSI, regulira potek pošiljanja in količino prenesenih podatkov v določenem času ter popravke napak z uporabo ustreznih metod;

4. aplikacijsko plast – združuje sejno, predstavitveno ter aplikacijsko plast modela ISO/OSI, definira višjenivojske protokole, kot so npr. SMTP, FTP, HTTP, ki služijo komunikaciji med uporabniško aplikacijo ter ustreznim strežnikom. Na tem nivoju se vrši tudi morebitno upravljanje s sejami, kjer je to potrebno.

Osnova prehajanja podatkov med plastmi je uporaba enkapsulacije. Nižjenivojske plasti prevzemajo podatke od višjenivojskih, pri čemer podatke enkapsulirajo v novo enoto podatkov v kateri so dodani specifični podatki posamezne plasti. Slika 2.2 prikazuje enkapsulacijo podatkov na različnih nivojih modela. Model TCP/IP je osnova za omrežje internet.

2.3 Ethernet

Standard Ethernet nosi uradno oznako IEEE-802.3 [8]. Pripada družini standardov IEEE-802 [9]. Pojavil se je v 70. letih prejšnjega stoletja. Izhaja iz omrežij, kot so "Token Ring", FDDI (angl. *Fiber Distributed Data Interface*) in ATM (angl. *Asynchronous Transfer*

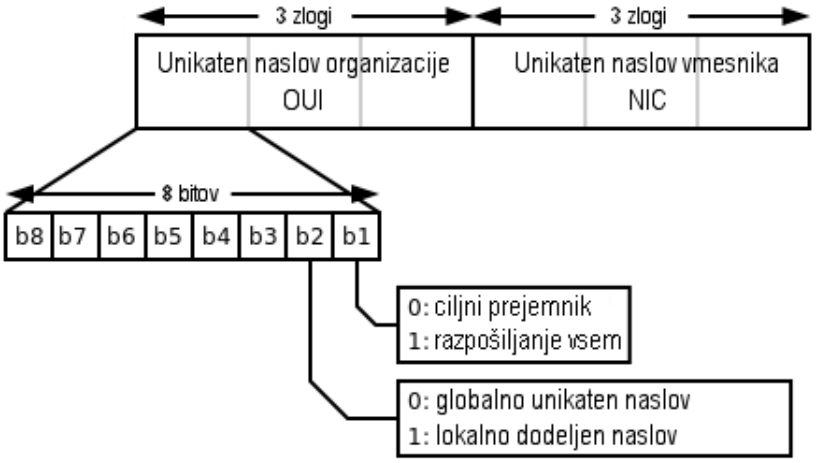
Mode). Razloge za uspeh in prevlado omrežja Ethernet lahko najdemo v omogočanju velikih hitrosti prenosa (danes do 10 Gb/s), enostavnosti ter cenenosti v primerjavi z ostalimi tipi omrežij. Prvotne različice omrežja so uporabljale enotno vodilo (angl. *Bus*) za vsa vozlišča istega omrežja, kar se je s časom izkazalo za neučinkovito, saj je pogosto prihajalo do kolizij med vozlišči ter s tem zmanjševanja skupne prepustnosti omrežja. Okoli leta 2000 se je pojavila nova topologija omrežja, in sicer t. i. zvezdna topologija. V tej topologiji se uporablja centralno stikalo za ločevanje posameznih krakov (vozlišč) omrežja in s tem ločevanje kolizijskih domen. Tako dosežemo bistveno večjo prepustnost omrežja tudi pri velikih obremenitvah. V prvotnih različicah je omrežje Ethernet podpiralo hitrosti do 10 Mbit/s. Novejše različice podpirajo hitrosti od 100 MBit/s do 1 Gbit/s po bakreni parici ter tudi več po optičnih povezavah.

Omrežje uporablja t. i. CSMA/CD (angl. *Carrier sense multiple access with collision detection*) dostop do skupnega medija, kar pride prav predvsem v topologiji enotnega vodila, v določeni meri pa tudi v zvezdni topologiji, ko posamezna vozlišča ne uporabljajo hkratne dvosmerne komunikacije (angl. *Full Duplex*). S CSMA/CD je omogočeno čim manjše prekrivanje oddanih okvirov s strani različnih vozlišč in tako večja prepustnost omrežja. Preverjanje pravilnosti prejema okvira se vrši z uporabo t. i. CRC (angl. *Cyclic Redundancy Check*). Po drugi strani ne predvideva potrjevanja prejema okvirov ter ponovnega pošiljanja in tako ne nudi zanesljivosti prenosa. Te funkcije so prepuščene višjim plastem komunikacijskega modela.

2.4 Naslavljanje MAC

Na povezavni plasti se uporablja naslavljanje MAC (angl. *Media Access Control*) [1, 10]. Obstaja več različic naslovov MAC, označenih s kratico EUI (angl. *Extended Unique Identifier*). Najpogosteje uporabljani sta 48 (EUI-48) in 64 (EUI-64) bitni različici. Omrežje Ethernet uporablja EUI-48 različico naslova MAC. Takšna dolžina naslova omogoča naslavljanje 2^{48} enot (določeni naslovi so rezervirani). Sestava polj v naslovu je podana na sliki 2.3. Prvih 24 bitov, imenovanih tudi OUI (angl. *Organizationally Unique Identifier*) del naslova, je unikatno dodeljenih proizvajalcu opreme s strani organizacije IEEE (*Institute of Electrical and Electronics Engineers*). Proizvajalec lahko zaprosi za dodelitev enega ali več unikatnih OUI. Naslednjih 24 bitov t. i. NIC (angl. *Network Interface Controller*) del naslova, je na razpolago proizvajalcu za unikatno identifikacijo posameznega izdelka. Naslovi MAC morajo biti unikatni, saj v nasprotnem primeru prihaja do kolizij na omrežju in s tem do motenj v delovanju posameznih vozlišč omrežja. Stan-

dardi iz skupine IEEE-802 predvidevajo format zapisa naslova EUI-48 v človeku prijazni obliki in sicer z uporabo šestih heksadecimalnih števil, ločenih z znakoma '-' ali ':', npr. 01:23:45:67:89:AB. Prvi zlog OUI dela naslova vsebuje dva rezervirana bita s posebnim

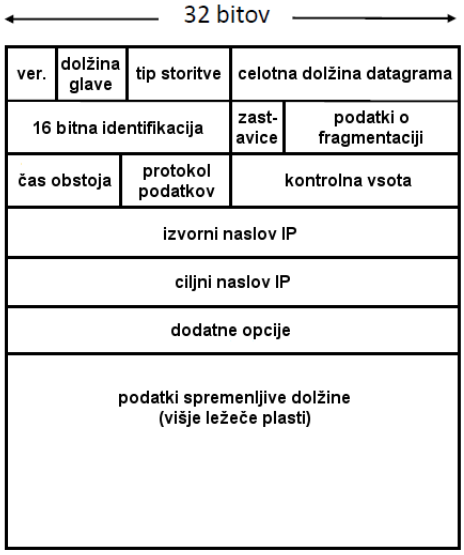


Slika 2.3: Sestava naslova MAC [1]

pomenom. Bit z najmanjšo težo (angl. *least significant bit*) tj. bit 1, je postavljen, ko se v omrežje pošlje okvir podatkov brez točno določenega naslova, kot v primeru pošiljanja več prejemnikom hkrati (angl. *Multicast*) ali vsem udeležencem na omrežju (angl. *Broadcast*). Bit z drugo najmanjšo težo tj. bit 2, pa se uporablja za testne namene, npr. ko nimamo dodeljenega OUI, ali podobnih primerih. V takih primerih je ta bit postavljen na 1, preostanek naslova pa določimo sami.

2.5 Mehanizem ARP

Za pošiljanje podatkovnih paketov IP (angl. *Internet Protocol*) po omrežju Ethernet je potrebno poznati naslov MAC končnega vozlišča. Ker to vnaprej običajno ni znano, je potrebno uporabiti mehanizem za pretvorbo naslova IP v naslov MAC. Ta mehanizem je poznan pod imenom ARP (angl. *Address Resolution Protocol*) [11]. Mehanizem ARP deluje tako, da v primeru pošiljanja okvira vozlišču, za katerega naslov MAC še ni znan, izvorno vozlišče namesto originalnega okvira pošlje zahtevo ARP, v katero vpiše svoja naslova IP in MAC ter naslov IP ciljnega vozlišča. Ta zahteva se v omrežju razpošlje kot nenaslovljeni (angl. *Broadcast*) okvir, s čimer se doseže, da ga sprejmejo vsa vozlišča na istem segmentu omrežja. Vozlišče s ciljnim naslovom IP na to zahtevo odgovori z odgovorom ARP, v katerega vpiše svoj naslov MAC. S tem izvorno vozlišče prejme naslov MAC ciljnega vozlišča in vsled pošlje originalni, čakajoči okvir. Mehanizem se tipično



Slika 2.4: Zapis podatkov v datagramu IP (IPv4)

uporabi le enkrat v seji komunikacije, saj se z namenom izogibanja nepotrebnega prometa na omrežju naslov MAC lokalno shrani ter večkrat uporabi.

2.6 Protokol IP

Protokol IP spada v omrežno plast modela TCP/IP [12]. Podatkovne pakete na tem nivoju imenujemo "datagrami". Najpomembnejša naloga protokola IP je naslavljanje podatkovnih datagramov. Trenutno najbolj razširjena različica protokola IP je različica 4 (IPv4) [13]. Ta različica uporablja naslove dolžine 32 bitov, kar omogoča več kot 4 milijarde unikatnih naslovov. Novejša različica 6 (IPv6), ki pa še ni toliko razširjena, razširja naslovni prostor, saj uporablja naslove dolžine 128 bitov [14]. Ostale naloge protokola IP so še: fragmentacija oz. delitev podatkov velikih datagramov v manjše, primerne za pošiljanje po omrežju, in obraten proces na sprejemu, identifikacija datagrama, preklapljanje datagramov med omrežji, preverjanje časovnega izteka veljavnosti datagramov ter posredovanje (v datagramu vsebujočih) podatkov ustreznim višjim plastem. Slika 2.4 prikazuje sestavo datagrama IP. Z delovanjem protokola IP je tesno povezan protokol ICMP (angl. *Internet Control Message Protocol*) [15, 7]. ICMP skrbi za obveščanje o napakah ali ostalih dogodkih na omrežju, kot je npr. nedosegljivost ciljnega naslovnika ali vmesnih vozlišč.

2.7 Protokol TCP

Protokol TCP (angl. *Transmission Control Protocol*) spada v transportno plast modela TCP/IP in predstavlja logični komunikacijski kanal med aplikacijskimi procesi. TCP je osnova za zanesljiv prenos podatkov med udeleženci, saj zagotavlja, da se poslani podatki pravilno prenesejo ciljnemu udeležencu. Pakete podatkov na tem nivoju imenujemo "segmenti". TCP skrbi za potrjevanje prejema oz. ponovno pošiljanje nepotrjenih segmentov v določenem časovnem intervalu, zagotavlja pravilnost zaporedja prenesenih podatkov in izloča podvojene segmente v primeru večkratnih ponovitev pošiljanja in prejema istih podatkov. Izločevanje podvojenih podatkov se vrši tako, da je vsakemu posameznemu zlogu podatkov dodeljena sekvenčna številka. S tem protokol TCP natančno loči, kateri zlogi so že prejeti, kateri pa še ne. Sekvenčna številka se uporablja tudi kot osnova za potrjevanje prejema podatkov v segmentih. Protokol TCP je povezavni tip protokola, kar pomeni, da se povezava med udeležencema vzdržuje dalj časa, kolikor je potrebno za prenos vseh podatkov znotraj iste seje. V ta namen se ob vzpostavitvi povezave uporablja t. i. trojno rokovanje (angl. *three-way handshake*). V tem postopku si udeleženca izmenjata določene začetne delovne parametre, potrebne za uspešno nadaljnjo komunikacijo. Prav tako se ob zaključku povezave TCP izvede podoben (nekoliko enostavnejši) postopek rokovanja.

TCP omogoča multipleksiranje večjega števila tokov podatkov preko iste točke omrežne plasti. Tako je možno hkrati vzpostaviti veliko število povezav med istimi ali različnimi udeleženci, ne da bi prišlo do mešanja tokov podatkov. Multipleksiranje tokov podatkov temelji na osnovi uporabe številke vrat, ki je dejansko nekakšen naslov procesa znotraj iste naprave. V kombinaciji z izvornim ter ciljnim naslovom IP par številk vrat unikatno določi povezavo med udeležencema. Posamezna številka vrat je lahko večkratno sočasno uporabljena z različnimi udeleženci, v kombinaciji z različnimi ciljnimi vrati ali naslovi IP. Primer takega delovanja je spletni strežnik, ki deluje na vratih s številko 80. Posamezni med seboj neodvisni odjemalci uporabijo svojo številko vrat (in svoj naslov IP), s katero vzpostavijo povezavo na vrata 80 strežnika.

TCP uporablja t. i. vtiče (angl. *Socket*). Vtič je dejansko vmesnik med transportno in aplikacijsko plastjo. Posamezen vtič vsebuje vse podatke o vzpostavljeni povezavi, kot so npr. izvorni in ciljni naslov IP ter številki vrat, prejemne in oddajne sekvence ter stanje potrjenosti prenešenih podatkov. Vtiču je tipično dodeljen tudi podatkovni predpomnilnik, tako za prejete, kakor tudi podatke v postopku pošiljanja oz. čakajoče na potrditev prejema s strani ciljnega naslovnika. S tem je olajšano upravljanje povezave s strani aplikacije, saj aplikaciji ni potrebno skrbeti za potrjevanje prejema in/ali pravočasno

branje prejetih podatkov. Protokol TCP skrbi tudi za kontrolo pretoka in izogibanje zamašitvam glede na stanje povezave med udeležencema ter glede na prejemnikovo hitrost branja prejetih podatkov. V ta namen uporablja t. i. okno povezave.

Protokol TCP je definiran v [16], kasnejši popravki in spremembe so v [7], razširitve pa v [17].

2.8 Protokol HTTP

Protokol HTTP spada v skupino aplikacijske plasti modela TCP/IP. HTTP je protokol namenjen dostopu do vsebin oz. datotek na zahtevo. Tipično se na internetu uporablja za prenašanje večpredstavnih datotek tipa HTML ali podobnih, vendar HTTP omogoča prenašanje kakršnekoli vrste datotek. Aplikacije, ki uporabljajo protokol HTTP, lahko v grobem ločimo na dve skupini. Na eni strani so strežniki, čigar naloga je, da omogočijo dostop do datotek s strani uporabnika oz. v ta namen uporabljenih spletnih brskalnikov, na drugi pa so brskalniki sami. Protokol je zasnovan tako, da se strežnik vedno obnaša kot pasiven udeleženec ter samostojno ne začenja s pošiljanjem podatkov, ampak pošlje podatke le kot odgovor na ustrezne zahteve s strani odjemalca oz. brskalnika.

Protokol HTTP pozna več vrst zahtev, med katerimi so najbolj uporabljene zahteve "GET" in "POST". Zahteva "GET" se uporabi za pridobivanje določene datoteke s strežnika. Odjemalec izda ukaz "GET", v katerem specificira URL (angl. *Uniform Resource Locator*) želene datoteke. Strežnik se na to odzove s pošiljanjem zahtevane datoteke oz. pošlje ustrezno označbo napake v primeru, da zahtevana datoteka ne obstaja. Zahteva "POST" razširja zahtevo "GET" s tem, da omogoča hkratno pošiljanje izbranih podatkov odjemalca, npr. podatke za dostop ali ostale uporabniške podatke, strežniku.

Protokol HTTP je definiran v [18, 19].

Poglavje 3

Sistem RFID

Potreba po identifikaciji se pojavlja na različnih področjih uporabe sodobnih tehnologij. Tako je potreba po identifikaciji uporabljena na področju industrije, logistike, prodaje ter še na kakšnem. Skozi leta uporabe so bile razvite različne vrste tehnologij za identifikacijo. Najenostavnejša med njimi je črtna koda. Obstaja več tipov črtne kode od enostavne 2D-črtne kode, do kompleksnejših kod, kot je npr. koda QR (angl. *Quick Response code*). Naprednejša in kompleksnejša tehnologija so pametne kartice. Poznamo dva tipa pametnih kartic in sicer kartice, v katerih je vgrajen le spomin, tipično je to EEPROM (angl. *Electrically Erasable Programmable Read-Only Memory*), ter kartice, kjer je poleg spomina vgrajena tudi enota CPU (angl. *Central Processing Unit*). Sprva so se na tržišču pojavile kontaktne pametne kartice, kjer se napajanje ter podatki, prenašajo preko mehanskih kontaktov, z vstavitvijo kartice v ustrezen čitalnik. Naprednejša tehnologija je uporaba pametnih kartic, kjer se tako napajanje kot podatki, prenašajo brezžično. Taki sistemi so poznani pod nazivom RFID oz. sistem za brezžično identifikacijo [20, 35].

Sistem RFID je sestavljen iz dveh komponent:

1. pametne kartice oz. ključa, ki vsebuje informacijo o identiteti in/ali ostale podatke za delovanje;

2. čitalca, ki posreduje energijo za napajanje ključa in izvaja prenos podatkov z le-tem. Kljub dejstvu, da se ga je prijelo ime "čitalec", se dejansko uporablja za branje in pisanje na ključ.

Pametni ključ je lahko pasivnega ali aktivnega tipa. Pasivni tip nima vgrajenega vira napajanja, medtem ko ga aktivni ima. Pasivni ključ se napaja s pridobivanjem energije v polju čitalca. Sisteme RFID lahko delimo glede na frekvenco delovanja, način prenosa

energije med čitalcem in ključem ter dometom sistema. Sistem RFID se lahko uporablja na širokem frekvenčnem spektru, in sicer od 120 kHz do 10 GHz. Dosegljiva razdalja med čitalcem in ključem je od nekaj milimetrov do preko 15 m. Prenos energije s čitalca je možen na tri načine in sicer preko magnetnega, električnega ali elektromagnetnega polja.

Sistem kratkega dosega omogoča branje/pisanje ključev do razdalje 1 cm. Uporaben je v primerih, ko je, bolj kot sam doseg, pomembna varnost prenosa podatkov. Tak ključ je potrebno vstaviti oz. položiti na čitalec. Za prenos energije se uporablja električno ali magnetno polje. Pri takem sistemu je možno doseči večjo moč prenesene energije in tako uporabo kompleksnejših kartic z vgrajeno enoto CPU.

Sistemi RFID z dosegom do 1 m so poznani kot sistemi srednjega dosega. Tipično se za prenos energije uporablja induktivni sklop. Obstaja več standardov, ki definirajo tehnične karakteristike ter delovanje standardnih skupin naprav RFID s tega področja, med drugimi sta to: standard ISO/IEC 14443, ki se uporablja za raznovrstne identifikacijske kartice ter ISO/IEC 15693, ki definira področje pametnih nalepk ter v določeni meri tudi identifikacijskih ključev. Tipične nosilne frekvence so $\leq$ 135 kHz ter 13,56 MHz.

Sistemi RFID z dometom večjim od 1 m, so znani kot sistemi dolgega dosega. Delujejo na UHF (angl. *Ultra High Frequency*) ter mikrovalovnem frekvenčnem področju, tipično na 868 MHz v Evropi oz. 915 MHz v ZDA ter 2,5 in 5,8 GHz po celem svetu. Tipični domet je do 3 m z uporabo pasivnega ključa in do 15 m ali več z uporabo aktivnega ključa (z dodatnim virom napajanja). Dodaten vir napajanja služi predvsem za napajanje enote CPU ter ohranjanje spomina in ne za oddajanje podatkov proti čitalcu. Za prenos (oddajanje) podatkov se uporablja energija, pridobljena iz elektromagnetnega polja čitalca z uporabo ustreznega usmerjevalnega vezja.

Obstaja množica standardov ki predpisujejo delovanje sistemov RFID. Razlikujejo se v sami nosilni frekvenci elektromagnetnega valovanja, kakor tudi v protokolu komunikacije. Tabela 3.1 prikazuje pregled frekvenčnih področij uporabe sistema RFID.

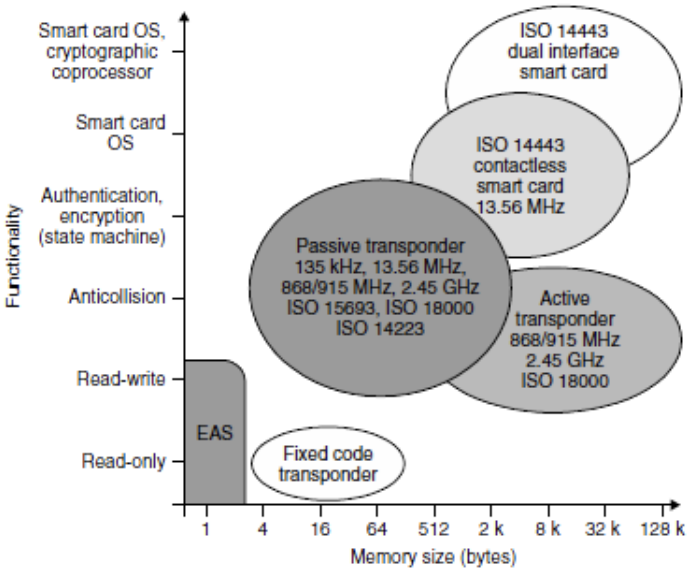
3.1 Klasifikacija sistemov glede na funkcionalnost

Sisteme RFID lahko razdelimo glede na funkcionalnost, ki jo nudijo (slika 3.1). V osnovi jih delimo na tri skupine, in sicer:

1. enostavni sistemi, ki jih delimo na dve podskupini:

Frekvenčno področje	Domet	Prenosna hitrost	Pogosta uporaba
120–150 kHz	10 cm	Nizka	Identifikacija živali, sledenje paketov
13,56 MHz	1 m	Srednje nizka	Pametne kartice
433 MHz	1–100 m	Srednja	Vojaške aplikacije
865–868 MHz (EU) 902–928 MHz (ZDA)	1–2 m	Srednje visoka	Identifikacija izdelkov
2450–5800 MHz	1–2 m	Visoka	Različna uporaba
3,1–10 GHz	200 m	Visoka	Različna uporaba

Tabela 3.1: Pregled frekvenčnih področij RFID [20]



Slika 3.1: Klasifikacija sistemov RFID glede na funkcionalnost [35]

- sistem za elektronski nadzor artiklov – EAS (angl. *Electronic Article Surveillance systems*), kjer je edina funkcionalnost detekcija prisotnosti ključa v polju čitalca. Uporablja se npr. za nadzor artiklov na izhodu iz prodajalne;

- enostavnejše elektronsko vezje, ki omogoča le branje in tipično služi kot unikatna identifikacijska koda, permanentno vpisana s strani proizvajalca. Prednost takega tipa ključev je v enostavni in posledično poceni izdelavi. Zaradi svoje enostavnosti pa omogoča tudi majhno porabo energije in s tem uporabo na večji razdalji. Tipična uporaba obsega identifikacijo palet, embalaže ali jeklenk. To področje zajema standard ISO/IEC 18000. Uporablja se tudi na področju identifikacije živali po standardu ISO/IEC 11785;

2. srednje-kompleksni sistemi:

   Ta skupina sistemov predstavlja največjo razširjenost in raznolikost med sistemi RFID. Večinoma se uporabljajo sistemi, v katerih je predvsem spominska enota, ki jo je možno brati ali v njo pisati. Velikosti spomina so od nekoliko zlogov do preko 100 k-zlogov spomina tipa EEPROM – pasivni ključi ali SRAM (angl. *Static Random Access Memory*) – aktivni ključi. Taki ključi omogočajo dostop z uporabo namenskih ukazov, s katerimi je možen dostop do vgrajenega končnega avtomata. V splošnem imajo vgrajene tudi metode za preprečevanje kolizije in so tako primerni za sočasno uporabo večjega števila ključev v polju istega čitalca. Določene različice vsebujejo algoritme za enkripcijo podatkov in tako povečujejo varnost dostopa do podatkov. Uporabljajo se na vseh frekvenčnih področjih sistemov RFID;

3. kompleksni sistemi:

   Ta segment predstavljajo sistemi z vgrajeno enoto CPU in namenskim vgrajenim operacijskim sistemom. Enota CPU omogoča uporabo bistveno kompleksnejših metod enkripcije in avtentikacije, kot je to možno z uporabo le končnih avtomatov v enostavnejših sistemih. Najnaprednejši tip predstavljajo napredne kartice z dvojnim dostopom. Omogočajo uporabo sistema RFID v aplikacijah z zelo visokimi varnostnimi zahtevami dostopa do podatkov, kot je npr. elektronska denarnica. V tej skupini se skoraj izključno uporablja frekvenčno področje 13,56 MHz. Prevladujoči standard na tem področju je ISO/IEC 14443.

3.2 Prenos energije in podatkov med čitalcem ter ključem

3.2.1 Induktivno sklopljeni sistem

Ključi, ki izkoriščajo prenos energije preko magnetnega polja, imajo poleg elektronskega vezja vgrajeno obsežno navitje. Čitalec z lastnim navitjem ustvari močno izmenično elektromagnetno polje določene (nosilne) frekvence. Frekvence delovanja induktivno sklopljenih sistemov so $\leq$ 135 kHz ter 13,56 MHz. Zaradi relativno nizkih frekvenc in s tem velikih valovnih dolžin se elektromagnetno polje v bližini oddajnika lahko smatra kot izmenično magnetno polje, ki, ko je sprejemnik v bližini čitalca, v tuljavi sprejemnika inducira električno napetost. Sistemi z induktivnim prenosom energije so skoraj vedno pasivni (brez dodatnih virov napajanja). Prenos podatkov od ključa na čitalec (branje) se izvaja na tri načine: 1. z modulacijo bremena, 2. z modulacijo bremena z dodatnim nosilnim signalom ter 3. z uporabo nižjih harmonskih frekvenc nosilnega signala.

Posebna vrsta induktivno sklopljenih sistemov je znana pod imenom "bližnje sklopljeni sistemi". Taki sistemi omogočajo zelo majhno razdaljo delovanja ($\leq$ 1 cm) in zato zahtevajo natančno pozicioniranje ključa ob čitalec. Moč prenosa energije je relativno velika in s tem omogoča uporabo kompleksnejših ključev (z večjo porabo). Prenos podatkov se lahko izvede z modulacijo bremena ali tudi (zaradi zelo majhne razdalje) kapacitivno.

3.2.2 Elektromagnetno sklopljeni sistem

Elektromagnetno sklopljeni sistemi omogočajo večje uporabne razdalje sistema RFID. Prenos energije je v takem načinu delovanja slabši in prenesena moč je zato manjša. Za uporabo teh ključev je potrebno zagotoviti kar se da varčna ter učinkovita vezja z minimalno porabo energije. Uporablja se tako pasivne enote kot tudi enote z dodatnimi viri napajanja. Pri tem je dodaten vir napajanja uporabljen izključno za napajanje vezja in ne za samo komunikacijo s čitalcem. Standard določa uporabo na frekvenčnih področjih 868 MHz v Evropi oz. 915 MHz v ZDA ter 2,5 in 5,8 GHz po celem svetu. Pasivna vezja omogočajo uporabno razdaljo med čitalcem in ključem do razdalje približno 3 m (868 MHz) ter okoli 1 m (2,4 GHz). Prenos podatkov proti čitalcu se vrši izključno z modulacijo odbojne karakteristike antene.

3.2.3 Električno sklopljeni sistemi

V tem načinu prenosa čitalec ustvarja električno polje visoke napetosti, iz katerega je z ustreznimi elektrodami na ključu možno pridobiti dovolj energije za delovanje elektronskega vezja. Prenos podatkov se vrši z modulacijo bremena.

3.3 Prenos podatkov od čitalca na ključ

Za prenos podatkov s čitalca na ključ se ne glede na tip sklopa med čitalcem in ključem uporablja eno izmed najpogostejših tipov digitalnih modulacij [21]. Najosnovnejše poznane digitalne modulacije v uporabi so: amplitudna modulacija – ASK (angl. *Amplitude Shift Keying*), frekvenčna modulacija – FSK (angl. *Frequency Shift Keying*) ter fazna modulacija – PSK (angl. *Phase Shift Keying*). V sistemu RFID se zaradi preproste demodulacije tipično uporablja modulacija ASK.

3.4 Varen prenos podatkov

Za določene aplikacije, kot so npr. dostop do prostorov z omejenim dostopom ali izvršitev plačil določenih storitev, je izjemnega pomena varen prenos podatkov med čitalcem in ključem. V osnovi je potrebno zagotoviti varno branje in spreminjanje podatkov na ključu, preprečevati vdor v sistem z uporabo neavtoriziranih ključev ali snemanjem komunikacije z namenom kasnejšega reproduciranja.

3.4.1 Simetrična vzajemna identifikacija

Simetrična vzajemna identifikacija med čitalcem ter ključem temelji na principu trikoračne vzajemne avtentikacije skladno s standardom ISO/IEC 9798-2 [22]. Vsaka od enot preveri poznavanje skrivnega kriptografskega ključa druge enote. Je simetrična avtentikacija, kar pomeni, da obe enoti uporabljata enak ključ, ki mora biti strogo varovan.

3.4.2 Avtentikacija z izpeljanimi ključi

Slabost avtentikacije, opisane v 3.4.1, je večja verjetnost odkritja skrivnega ključa, predvsem v določenih aplikacijah (npr. vozovnice za javni transport), kjer je v uporabi izjemno

veliko število enot. V takem primeru postane cel sistem nezavarovan in odprt za zlorabe. Temu se je možno izogniti z uporabo procedure, kjer ima vsaka enota RFID svoj lasten kriptografski ključ, izpeljan iz unikatne identifikacijske številke enote. Z uporabo skrivnega algoritma se z uporabo identifikacijske številke enote in dodatnega skrivnega kriptografskega ključa generira nov ključ, ki se ga vpiše na enoto. Tako ima vsaka enota lasten kriptografski ključ, ki se ga uporablja v prihodnje. S tem preprečimo ogrozitev celotnega sistema, tudi če pride do razkritja kriptografskega ključa posameznih enot.

3.4.3 Varen prenos podatkov

Pri branju oz. pisanju na ključ je pomembno, da se zaščiti prenos podatkov in s tem prepreči prestrezanje in tako zlorabo prenesenih podatkov s strani tretjih oseb. Rešitev se ponuja z uporabo enkripcijskih algoritmov, s katerimi pred samim prenašanjem podatke kriptiramo in nato ob sprejemu dekriptiramo. Morebitno prestreženi (kriptirani) podatki so brez poznavanja kriptografskega ključa neuporabni. Za enkripcijo podatkov se v sistemu RFID uporablja simetrični (enak) ključ. Poznamo dva osnovna načina kriptiranja in sicer bločno (enkripcija celega bloka podatkov) ter zaporedno (enkripcija zlog za zlogom). Sistem RFID, zaradi enostavnejših algoritmov, uporablja zaporedno enkripcijo.

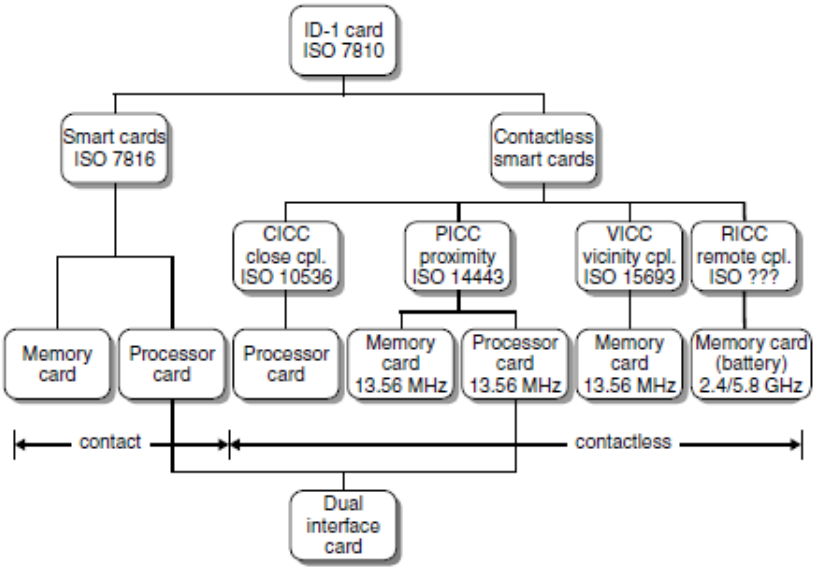
3.5 Standardi RFID

Obstaja množica standardov za sistem RFID. S standardi se določajo fizične lastnosti, prenos energije in podatkov ter samih protokolov komunikacije oz. formata podatkov. Slika 3.2 prikazuje družine pametnih kartic skupaj s pripadajočimi standardi.

3.5.1 Identifikacija živali

Za identifikacijo živali s pomočjo RFID so bili sprejeti naslednji standardi:

- ISO/IEC 11784 – definira format zapisa podatkov,
- ISO/IEC 11785 – definira tehnične zahteve sistema, kot so: frekvenca delovanja, tip prenosa podatkov ter ostali vidiki komunikacije,
- ISO/IEC 14223 – razširja standarda ISO/IEC 11784 in ISO/IEC 11785 z naprednimi funkcijami delovanja ter zapisom dodatnih podatkov na ključe.



Slika 3.2: Družine pametnih kartic s pripadajočimi standardi [35]

3.5.2 Brezkontaktne pametne kartice

Brezkontaktne pametne kartice so različica ključev RFID, kjer je izvedba samih ključev tipičnih dimenzij bančnih ali podobnih kartic. To področje v glavnem zajemajo tri standardi. To so:

- ISO/IEC 10536 – izredno majhen domet ($\leq$ 1 cm),
- ISO/IEC 14443 – bližnji domet ($\leq$ 10 cm),
- ISO/IEC 15693 – Srednje velik domet ($\leq$ 1m).

Med bolj razširjenimi so kartice po standardu ISO/IEC 14443. Standard definira delovanje sistemov z bližnjim dometom do največ 15 cm. Tipično so to kartice z vgrajeno enoto CPU, ki imajo lahko vgrajene električne priključke za žični prenos podatkov. Standard med drugim definira tudi dimenzije kartic RFID in sicer je to: 85,72 mm $\times$ 54,03 mm $\times$ 0,76 mm. Napajanje kartic se vrši z uporabo induktivnega sklopa preko magnetnega polja čitalca z nosilno frekvenco 13,56 MHz. Na kartici se za sprejem energije vgrajuje električna zanka s 3 do 6 ovoji.

V sklopu standarda obstajata dva tipa komunikacijskega protokola med čitalcem in kartico, to sta "Tip A" ter "Tip B". Posamezna pametna kartica je narejena po eni ali drugi različici medtem, ko mora čitalec podpirati obe. Standard definira delovanje sistema, tudi ko je v polju čitalca istočasno več kartic. Tabela 3.2 prikazuje glavne karakteristike komunikacije med čitalcem ter kartico.

	Tip modulacije	Bitno kodiranje	Sinhronizacija	Prenosna hitrost
Čitalec → Kartica Tip A	ASK 100%	Prilagojena "Miller koda"	Oznake začetek / konec bloka (1bit)	106 kBaud
Kartica Tip A → Čitalec	Modulacija bremena z ASK modulacijo harmonika 847 kHz	Kodiranje manchester	Oznake začetek / konec bloka (1bit)	106 kBaud
Čitalec → Kartica Tip B	ASK 10 %	Kodiranje NRZ	1 start, 1 stop bit po zlogu	106 kBaud
Kartica Tip B → Čitalec	Modulacija bremena z BPSK modulacijo harmonika 847 kHz	Kodiranje NRZ	1 start, 1 stop bit po zlogu	106 kBaud

Tabela 3.2: Karakteristike komunikacije po standardu ISO/IEC 14443 [35]

3.5.3 Standard MIFARE

Standard MIFARE je izvedba standarda ISO/IEC 14443 Tip A, z določenimi dodelavami. Prvič se je pojavil leta 1994 z uvedbo kartic tipa "Classic 1K". Zelo hitro se je uveljavil v javnem transportu, za sistem elektronskih vozovnic, pri čemer je še danes vodilni standard. Razvit je bil v podjetju Mikron, ki ga je kasneje kupilo podjetje Philips (danes NXP Semiconductors). Obstaja večje število različic kartic MIFARE, ki razširjajo osnovni standard z izpeljanimi ter dodatnimi rešitvami in zato niso povsem kompatibilne z osnovnim standardom.

3.5.3.1 MIFARE Classic

MIFARE Classic je osnovna različica kartic, združljiva s standardom (vendar ne v celoti) ISO/IEC 14443-3 – Tip A [23]. Podpira enkripcijo podatkov ter vsebuje protokol za avtentikacijo. V osnovi je to le spominska kartica, brez enote CPU ter tako brez naprednih funkcij, ki ji omogoča uporaba le-te.

Glavne lastnosti kartice Classic 1K so:

- 1024 zlogov EEPROM (768 uporabniško dosegljivih zlogov),
- unikatna serijska številka (dolžine 4 oz. 7 zlogov) – UID (angl. *Unique Identification Number*),
- 16 ločenih sektorjev, vsak z lastnima ključema (več aplikacij na isti kartici),
- 4 bloki po sektorju, dolžine 16 zlogov,

- 2×48 bitni ključ po sektorju,
- maksimalno število vpisov posameznega bloka: 100.000,
- hranjenje podatkov: 10 let.

Delitev spomina na ločene sektorje omogoča uporabo iste kartice v ločenih sistemih. Posamezen sektor vsebuje lastne varnostne ključe in tako omogoča dostop do sektorja le ustreznemu sistemu. Sektor je razdeljen na štiri bloke velikosti 16 zlogov. Prvi blok prvega sektorja je rezerviran za podatke proizvajalca. Uporablja se za zapis serijske številke (identifikacije kartice), ki jo zapiše proizvajalec in je ni mogoče spreminjati. Obstajata dve različici serijske številke in sicer različica dolžine 7 zlogov (unikatna) ter dolžine 4 zloge (neunikatna). V istem bloku so vpisani še nekateri podatki o samem proizvajalcu. Tako sta v prvem sektorju le dva bloka na voljo za uporabniške podatke. Sledijo sektorji spomina v katerih so za uporabniške podatke na voljo tri od štirih blokov. Četrti blok v vsakem sektorju je vedno rezerviran za dostopna ključa (A ter B) posameznega sektorja. Posamezen blok se lahko uporablja na dva načina in sicer kot navaden bralno-pisalni spomin ali kot posebni "števni" blok. Za števne bloke lahko uporabljamo posebne ukaze, s katerimi povečujemo ali zmanjšujemo vrednost števca v bloku.

Obstaja različica Classic 4K, ki se od osnovne 1K razlikuje le v večjem številu sektorjev in s tem z večjo kapaciteto spomina.

3.5.3.2 MIFARE Ultralight

Kartica MIFARE Ultralight je namenjena uporabi v nizkocenovnih ter nezahtevnih sistemih (enkratna uporaba), kjer je potreba po spominu zelo majhna. Primeri takih sistemov so npr. vstopnice za prireditve ali športne tekme, kjer je dostop omejen na določen dan in/ali področje, oz. na omejeno število dostopov do neke storitve npr. atrakcije v lunaparku. Zaradi svoje enostavnosti ter majhne količine spomina, je kartica zelo poceni [23].

Karakteristike kartice MIFARE Ultralight so:

- podpira metode za preprečevanje kolizije ob sočasni prisotnosti večjega števila kartic v polju čitalca,
- domet do 10 cm,
- hitrost prenosa podatkov 106 kbit/s,

- unikatna številka dolžine 7 zlogov,
- 32 bitov spomina z enkratnim vpisom – OTP (angl. *One Time Programmable memory*),
- 384 bitov spomina za branje/pisanje uporabniških podatkov,
- uporabniško programabilni bit za zaklepanje posameznih blokov spomina,
- 3DES-varnostni protokol (le na različicah MIFARE Ultralight C in Ultralight DES-Fire).

3.5.3.3 MIFARE DESFire ter MIFARE DESFire EV1

Ti verziji razširjata serijo Classic in tako omogočata uporabo naprednih enkripcijskih algoritmov. [23].

3.5.3.4 MIFARE Plus

Kartica MIFARE Plus, omogoča enostaven prehod iz serije Classic na serijo Plus in s tem varnejši način dostopa do podatkov. Uporablja enkripcijo AES (angl. *Advanced Encryption Standard*) z 128 bitnim ključem. Enkripcija AES se uporablja za vse vidike varovanja dostopa, in sicer za avtentikacijo, zagotavljanje celovitosti podatkov ter zasebnost [23].

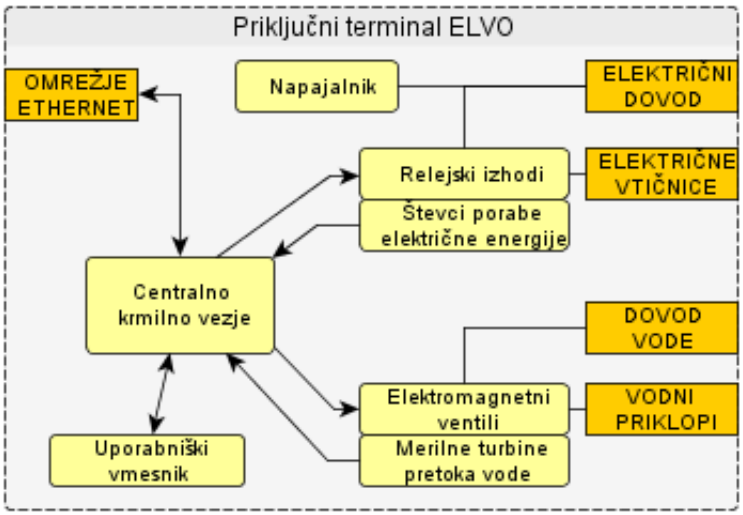
Poglavje 4

Terminal ELVO

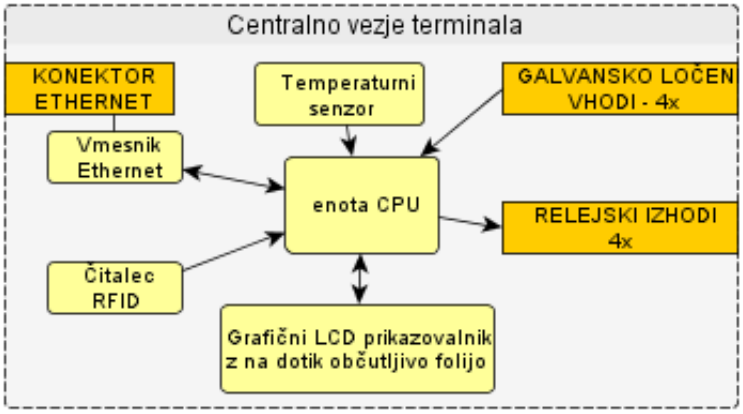
Terminal ELVO je ena izmed glavnih komponent sistema. Omogoča dejanski priklop porabnikov na vodovodno oz. električno omrežje in hkrati tudi popoln nadzor nad samim vklapljanjem ter spremljanjem porabe posameznih virov. Vgrajeni fizični priklopi omogočajo uporabniku priklop na eno ali drugo omrežje. Vklop določenega priključka je možen z uporabo ustreznih aktivatorjev. Za vodo se v ta namen uporablja elektromagnetne ventile, za električno energijo pa ustrezne močnostne releje. Slika 4.1 prikazuje celotno zgradbo terminala. Centralni sestavni del terminala predstavlja namensko razvito elektronsko vezje, ki krmili vse aktivatorje priključkov in hkrati beleži porabo po posameznem priključku.

Z namenom zajema podatkov o porabi virov je na vezju predvidena prisotnost štirih vhodnih kanalov, na katere priključimo ustrezne merilne enote za dejansko izvedbo meritev porabe. Prav tako vezje predvideva štiri izhodne kanale, s katerimi krmilimo aktivatorje. Meritev porabe električne energije se opravlja s števci električne energije, ki nudijo informacijo o porabi z ustreznim pulznim izhodom. Delovanje takega izhoda je definirano s standardom DIN 43864 oz. novejšim ISO/IEC 62053-31. Meritev porabe vode se opravlja z uporabo vodne merilne turbine, ki ima vgrajene potrebne mehanske in elektronske komponente za pridobivanje impulzov skladno s pretokom vode. Kot dodatno funkcijo terminal omogoča meritev temperature v samem ohišju terminala z namenom preprečevanja zamrznitve vode v ceveh.

Terminal ELVO predvideva upravljanje le-tega s strani uporabnikov preko vmesnika z grafičnim prikazovalnikom. Za omogočanje dostopa le avtoriziranim uporabnikom terminal uporablja tehnologijo RFID. Centralno vezje terminala sestavlja sklop komponent, med katerimi je enota CPU iz družine mikrokrmilnikov ARM (angl. *Advanced RISC Machine*). Dodatno so prisotni še vhodni in izhodni vmesniki, vmesnik za omrežno povezavo



Slika 4.1: Zgradba priključnega terminala ELVO



Slika 4.2: Bločna shema centralnega vezja terminala ELVO

Ethernet, čitalec RFID, temperaturni senzor, grafični prikazovalnik s tekočimi kristali – LCD (angl. *Liquid Crystal Display*) ter piskač, s katerim uporabniku posredujemo povratno informacijo ob upravljanju z uporabniškim vmesnikom.

Delovanje terminala je usklajeno s centralnim strežnikom, ki vodi evidenco o avtoriziranih uporabnikih ter dobroimetju na posameznem uporabniškem računu. Centralni strežnik uporabnikom omogoča prijavo v sistem in vklop enega ali več izmed prostih priključkov, prav tako tudi izklop priključkov, ko dobroimetje na računu uporabnika poteče ali na zahtevo uporabnika. Terminal samostojno ne vodi evidence o porabi, ampak strežniku v realnem času poroča o porabi ali drugih dogodkih. Slika 4.2 prikazuje bločno shemo centralnega vezja terminala ELVO.

Aktivacija oz. deaktivacija določenega priključka poteka tako, da se uporabnik identificira s približanjem kartice RFID k vgrajenemu čitalcu, nakar sistem preko grafičnega vmesnika vodi uporabnika skozi postopek aktivacije oz. deaktivacije posameznega priključka. Z ustrezno izbiro uporabnik sproži preklop priključka.

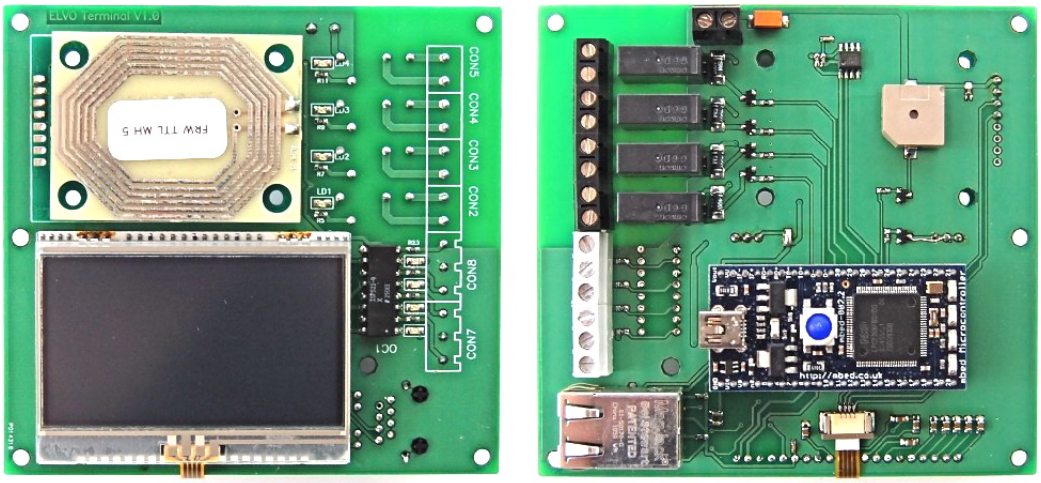
4.1 Centralno krmilno vezje

Centralno krmilno vezje je narejeno z uporabo mikrokrmilnika ARM7. Uporabili smo mikrokrmilnik LPC2368 proizvajalca NXP Semiconductors. Za namenom poenostavitve izvedbe smo uporabili že sestavljeno enoto, ki vsebuje izbrani mikrokrmilnik, napajalni del (stabilizatorje napetosti), vmesnik za povezavo na omrežje Ethernet ter dodatno vezje za priklop na vodilo USB (angl. *Universal Serial Bus*) osebnega računalnika, ki omogoča nalaganje programske opreme na mikrokrmilnik.

Izhodni kanali so realizirani z uporabo miniaturnih relejev, s katerimi je omogočeno krmiljenje porabnikov večjih moči in ki hkrati zagotavljajo galvansko ločitev le-teh od glavnega vezja. Vhodi so galvansko ločeni z uporabo optosklopnikov. S tem se varnost uporabe sistema in zanesljivost delovanja povečata, saj je morebitni vpliv zunanjih motenj na delovanje sistema zmanjšan na minimum. Za identifikacijo uporabnika je uporabljen čitalec RFID, ki podpira kartice, skladne s standardom MIFARE. Pomemben faktor pri izbiri načina interakcije z uporabnikom je izogibanje uporabi navzven dostopnih tipk, saj terminal deluje v oteženih pogojih, kot so izpostavljenost dežju in vlagi. Še posebno ostre pogoje predstavlja uporaba terminala tik ob morju, saj je v primeru slabega vremena možen prenos morske vode na terminal. Odločili smo se za uporabo prikazovalnika, ki omogoča krmiljenje na dotik. S tem je možna montaža krmilnega vezja v zaprto ohišje in tako zmanjšanje morebitnih škodljivih vplivov omenjenih snovi. Slika 4.3 prikazuje izgled izdelanega centralnega krmilnega vezja.

4.1.1 Jedro ARM

CPU-jedro ARM7 je sodobno zasnovano 32-bitno RISC (angl. *Reduced Instruction Set Computer*) mikroprocesorsko jedro [24]. Razvito je v podjetju ARM Ltd. iz Velike Britanije, ki sicer ne izdeluje ali prodaja končnih integriranih vezij, ampak se osredotoča na prodajo licenc za uporabo lastno razvitih jeder. Proizvajalci integriranih vezij, kot so npr. NXP Semiconductors, Motorola, Samsung itd., proizvajajo lastne mikrokrmilnike

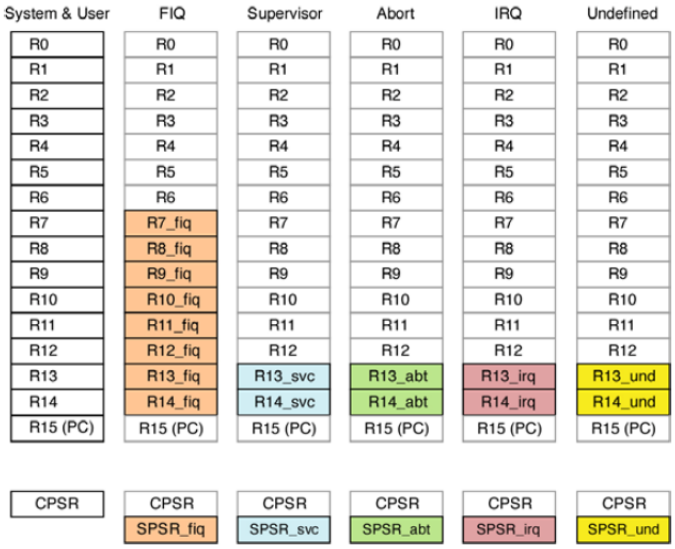


Slika 4.3: Izdelano centralno krmilno vezje (spredaj in zadaj)

po licenci ARM-a, v katere poleg jedra ARM vgradijo dodatno periferijo. Jedro je zasnovano za zmogljivo izvrševanje tako zmogljivih 32 bitnih ukazov, kakor tudi za delovanje v posebnem načinu "Thumb", v katerem jedro izvršuje enostavnejše 16 bitne ukaze. Delovanje v načinu "Thumb" je gledano s performančnega vidika slabše, vendar pride v poštev, ko ima poraba programskega spomina prednost pred hitrostjo izvajanja. Jedro ARM7 omogoča izvajanje programske kode v različnih izvajalskih nivojih, kar je velika prednost za uporabo operacijskega sistema. Vsak od nivojev uporablja lastne kopije statusnega in nekaterih delovnih registrov ter lastni (ločen) sklad. Vsebuje napredni vektorski upravljalnik prekinitev VIC (angl. *Vector Interrupt Controller*) z nastavljivo prioriteto, kar izboljša odzivnost sistema na prekinitve. Dodatno vsebuje t. i. "Hitro prekinitev - FIQ", ki omogoča izjemno hitro odzivnost, saj ima najvišjo prioriteto ter večje število popolnoma ločenih delovnih registrov, s čimer se izognemo zamudnemu shranjevanju vsebine le-teh na sklad ob vstopu v rokovalnik prekinitve. Slika 4.4 prikazuje seznam nivojev izvajanja z označenimi ločenimi delovnimi registri (obarvana polja).

4.1.2 Procesorska plošča mbed

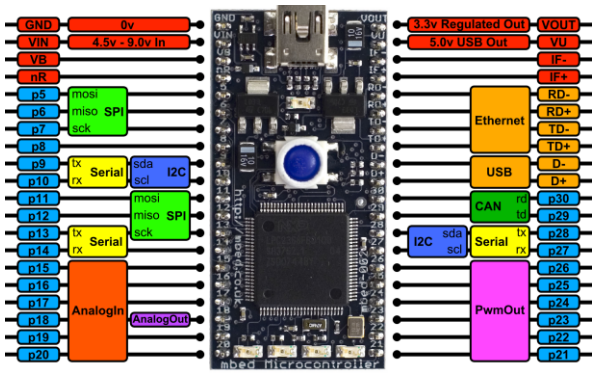
Razvojna procesorska plošča mbed je razvita s strani dveh inženirjev, zaposlenih pri podjetju ARM Holdings. Njen glavni namen je hiter in enostaven razvoj projektov z mikrokrmilnikom ARM. Obstaja več različic plošče mbed. Glavna razlika je v modelu vgrajenega mikrokrmilnika. Za naš projekt smo izbrali procesorsko ploščo mbed z mikrokrmilnikom LPC2368 [2]. Nalaganje programa je možno preko vgrajenega vmesnika USB. Na plošči je vgrajena tudi dodatna periferija, med katero najdemo vmesnik za povezavo na fizični nivo



Slika 4.4: Pregled nivojev izvajanja ter pripadajočih registrov jedra ARM7 [36]

Ethernet omrežja, napajalni del s stabilizatorjem napetosti in vse potrebne generatorje takta. S tem sta uporaba in priklop plošče zelo poenostavljena. Plošča ima 40 priključnih kontaktov, med katerimi so tako napajalne linije kakor namenske ali splošne vhodno-izhodne linije. Slika 4.5 prikazuje procesorsko ploščo mbed in vse priključne kontakte. Uporabljeni mikrokrmilnik ima vgrajene periferne enote, kot so napredni upravljalnik prekinitev – VIC, vmesnik za direkten dostop do spomina – DMA (angl. *Direct Memory Access*), Ethernet MAC, USB, SSP (angl. *Synchronous Serial Port*), UART (angl. *Universal Asynchronous Receiver Transmitter*), I^2C (angl. *Inter-Integrated Circuit*), ADC (angl. *Analog to Digital Converter*), DAC (angl. *Digital to Analog Converter*), CAN (angl. *Controller Area Network*) in še nekatere druge vmesnike [25]. Takt ure je možno nastaviti do 72 MHz z vgrajenim sintetizatorjem PLL (angl. *Phase Locked Loop*). Krmilnik vsebuje 512 kB programskega spomina in 58 kB statičnega delovnega spomina – RAM (angl. *Random Access Memory*).

Za procesorsko ploščo mbed je na voljo obsežna programska knjižnica, ki omogoča enostaven dostop do mikrokrmilniških perifernih enot. Podjetje ponuja tudi prevajalnik za programski jezik C, do katerega je možno dostopati preko spletnega vmesnika. Na ta način je možno uporabiti vse obstoječe ali tudi lastno razvite knjižnice in tako ustvariti programsko kodo za izvajanje v mikrokrmilniku. Alternativa temu je uporaba ločenega prevajalnika po lastni izbiri. Za naš projekt smo se odločili za uporabo samostojnega prevajalnika GCC (*GNU Compiler Collection*) [26], odprtokodnega vgrajenega operacijskega sistema in lastnih namenskih knjižnic.



Slika 4.5: Plošča mbed z oznakami priključnih kontaktov [2]

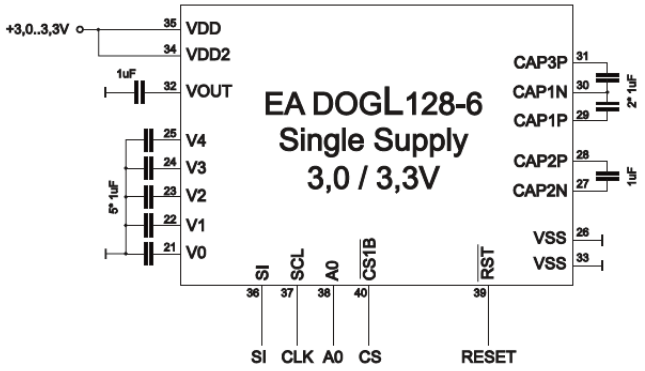
4.1.3 Napajanje vezja

Za napajanje vezja potrebujemo zunanji napajalnik, z izhodno enosmerno napetostjo 5 V in s tokovno zmogljivostjo do 300 mA. Sama procesorska plošča mbed ima vgrajene stabilizatorje napetosti, s pomočjo katerih se napetost ustrezno zniža na 3,3 V, kolikor je potrebno za delovanje mikrokrmilnika. Hkrati to napetost izkoristimo za napajanje prikazovalnika LCD in temperaturnega senzorja. Z napetostjo 5 V napajamo vse ostale dele vezja, med katerimi so: izhodni releji, vezje vhodnih kanalov, čitalnik RFID in piskač. Pri tem nam povezavo med posameznimi perifernimi enotami in samim mikrokrmilnikom olajša dejstvo, da so vhodne nožice mikrokrmilnika tolerantne za napetost 5 V, kar pomeni, da lahko izhod določenega vezja na nivoju 5 V neposredno povežemo na vhod mikrokrmilnika, brez skrbi da vhod uničimo. Potrebno je posvetiti nekoliko pozornosti le pri povezavi mikrokrmilniških izhodnih signalov, saj je maksimalni nivo napetosti v tem primeru 3,3 V, kar lahko v določenem primeru ne zadošča za krmiljenje vezja na izhodu.

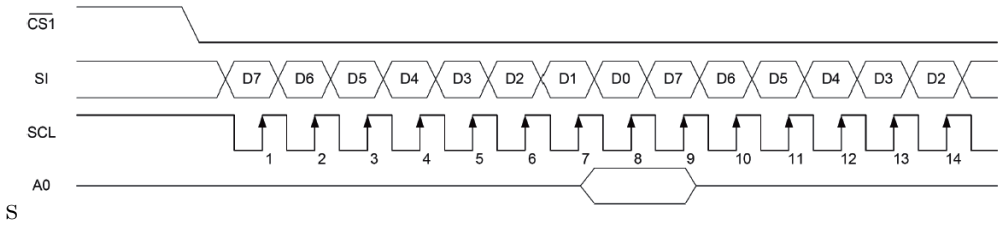
4.1.4 Grafični prikazovalnik ter vmesnik na dotik

Za upravljanje terminala ELVO smo se odločili za enobarvni grafični prikazovalnik na tekoče kristale (LCD) z na dotik občutljivim vmesnikom. Odločili smo se za prikazovalnik nemškega podjetja Electronic Assembly. Podjetje proizvaja množico različnih tipov prikazovalnikov, od najenostavnejših znakovnih do kompleksnih grafičnih barvnih prikazovalnikov v tehnologiji TFT (angl. *Thin Film Transistor*).

Končna izbira je bila za prikazovalnik DOGL-128 [27]. Prikazovalnik omogoča grafično ločljivost 128 × 64 pik, montažo na dotik občutljive folije in izbiro različnih barv dodatne osvetlitve. Prikazovalnik je tipa COG (angl. *Chip On Glass*), kar pomeni, da je krmilna elektronika vgrajena na samo stekleno površino, kjer so električno občutljivi tekoči kri-



Slika 4.6: Osnovna priključitev EADOGL-128 prikazovalnika [3]



Slika 4.7: Krmiljenje signalov serijskega vmesnika SPI [3]

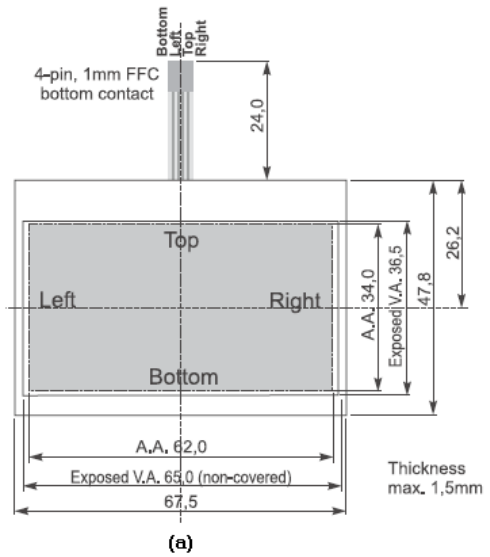
stali. S tem dosežemo visoko stopnjo integracije in relativno majhno število priključnih kontaktov. Za delovanje prikazovalnik potrebuje le napetost 3,3 V iz katere proizvede vse ostale potrebne napetosti z uporabo namenskih pretvornikov DC-DC. Za delovanje potrebuje minimalno število zunanjih komponent in sicer so to v glavnem le gladilni kondenzatorji za pretvornik DC-DC. Na sliki 4.6 je prikazano osnovno vezje priključitve in vse osnovne komponente potrebne za delovanje. Krmiljenje prikazovalnika se upravlja preko zaporednega vmesnika SPI (angl. *Serial Peripheral Interface*). To je zaporedni vmesnik, ki uporablja sinhronizacijo prenesenih podatkov z uporabo signala taktne ure. Ker v prikazovalnik vedno le pišemo, potrebujemo le enosmerno komunikacijo od mikrokrmilnika do prikazovalnika. Dodatno potrebujemo še nekatere krmilne linije, in sicer A0, CS ter linijo RESET. Na sliki 4.7 lahko vidimo zaporedje krmiljenja signalov na zaporednem vmesniku pri vpisu ukaza v prikazovalnik. Prikazovalniku preko vmesnika SPI pošiljamo vrsto ukazov, s katerimi nastavimo parametre delovanja, kakor tudi vpišemo podatke o sami sliki. Seznam poznanih ukazov prikazuje tabela 4.1.

Zaznavanje dotika se opravi z uporabo namenske na dotik občutljive folije, ki deluje na principu uporovnega delilnika napetosti. Sestavljena je iz več plasti, na katere je nanesena snov z določeno ohmsko upornostjo. Vsaka izmed osi ima svojo uporovno plast. V ta namen ima folija štiri priključne kontakte, dva za uporovno plast na x osi, ostala dva pa

Command	Command Code									Function
	A0	D7	D6	D5	D4	D3	D2	D1	D0	
(1) Display ON/OFF	0	1	0	1	0	1	1	1	0 1	LCD display ON/OFF 0: OFF, 1: ON
(2) Display start line set	0	0	1	Display start address						Sets the display RAM display start line address
(3) Page address set	0	1	0	1	1	Page address				Sets the display RAM page address
(4) Column address set upper bit Column address set lower bit	0	0 0	0 0	0 0	1 0	Most significant column address Least significant column address				Sets the most significant 4 bits of the display RAM column address. Sets the least significant 4 bits of the display RAM column address.
(6) Display data write	1	Write data								Writes to the display RAM
(8) ADC select	0	1	0	1	0	0	0	0	0 1	Sets the display RAM address SEG output correspondence 0: normal, 1: reverse
(9) Display normal/ reverse	0	1	0	1	0	0	1	1	0 1	Sets the LCD display normal/ reverse 0: normal, 1: reverse
(10) Display all points ON/OFF	0	1	0	1	0	0	1	0	0 1	Display all points 0: normal display 1: all points ON
(11) LCD bias set	0	1	0	1	0	0	0	1	0 1	Sets the LCD drive voltage bias ratio 0: 1/9 bias, 1: 1/7 bias (ST7565R)
(14) Reset	0	1	1	1	0	0	0	1	0	Internal reset
(15) Common output mode select	0	1	1	0	0	0 1	*	*	*	Select COM output scan direction 0: normal direction 1: reverse direction
(16) Power control set	0	0	0	1	0	1	Operating mode			Select internal power supply operating mode
(17) V_0 voltage regulator internal resistor ratio set	0	0	0	1	0	0	Resistor ratio			Select internal resistor ratio(Rb/Ra) mode
(18) Electronic volume mode set Electronic volume register set	0	1 0	0 0	0	0	0	0 Electronic volume value	0	1	Set the V_0 output voltage electronic volume register
(19) Static indicator ON/OFF Static indicator register set	0	1 0	0 0	1 0	0 0	1 0	1 0	0 0	0 1 Mode	0: OFF, 1: ON Set the flashing mode
(20) Booster ratio set	0	1 0	1 0	1 0	1 0	1 0	0 0	0 step-up value	0	select booster ratio 00: 2x,3x,4x 01: 5x 11: 6x
(21) Power save	0	Display OFF and display all points ON compound command								
(22) NOP	0	1	1	1	0	0	0	1	1	Command for non-operation

Tabela 4.1: Seznam poznanih ukazov prikazovalnika EADOG [3]

za y os. Z dotikom določene točke na foliji se vzpostavi kontakt med uporovnimi plastmi, s tem lahko z meritvijo padca napetosti na delilniku posamezne osi, določimo mesto dotika. Za zaznavanje 2D-pozicije je potrebno opraviti dve meritvi, in sicer po eno za vsako os. Dimenzijska skica in tehnični podatki folije so prikazani na sliki 4.8.



Specification			
Specification	**min**	**max**	**Unit**
Top-Bottom	100	400	Ω
Left-Right	110	410	Ω
Voltage	3	12	V
Current	5	25	mA
Linearity		1,5	%
Force	45	65	g
Contact Bounce	5	10	ms
Op. Temperatur	-20	+60	°C
Stor. Temperatur	-20	+70	°C
Transmission	75	85	%
Life Time	10000		Cycles

(b)

Slika 4.8: Dimenzijska skica (a) in tehnični podatki folije na dotik (b) [3]

Za uporabo takšne folije se tipično uporablja namenska elektronska vezja, ki z določeno periodo opravijo meritev na posamezni osi. V našem sistemu smo se odločili za drugačen pristop, in sicer smo za meritve uporabili na mikrokrmilniku vgrajene pretvornike ADC. Glede na to, da je uporabljena folija uporovnega tipa, lahko z merjenjem napetosti (na poljubni elektrodi) na eni osi zaznamo mesto dotika z drugo osjo. Na posamezno os z določenim intervalom dovedemo napetosti 3,3 in 0 V na posamezna kontakta osi, nakar s pretvornikom ADC izmerimo napetost na enem kontaktu druge osi. Iz tako izmerjene napetosti lahko izračunamo mesto dotika po enačbi $a = \frac{U_i}{U_{3,3}-U_0} * r$, pri čemer je U_i izmerjena napetost, $U_{3,3}$ in U_0 pa priključeni napetosti na merjeno os. Rezultat (a) je skaliran skladno z ločljivostjo osi prikazovalnika (r) in tako predstavlja pozicijo točke med U_0 ter $U_{3,3}$. V naslednjem koraku postopek ponovimo s tem, da sedaj vloge osi med seboj zamenjamo. Ta postopek opravljamo v nedogled s periodo približno 10 ms. V praksi se je izkazalo, da je natančnost zaznave po opisanem postopku popolnoma zadovoljiva za naše zahteve, saj ne potrebujemo izjemno natančne meritve mesta dotika.

4.1.5 Identifikacija uporabnika s sistemom RFID

Pri upravljanju s terminalom se pojavi potreba po identifikaciji uporabnika, saj je višina dobroimetja vezana na le-tega. Sistem mora omogočiti praktično, hitro in zanesljivo identifikacijo oz. prijavo uporabnika. Kot idealen odgovor na te zahteve se ponuja sistem RFID. Za uporabo v našem projektu smo se odločili za tehnologijo MIFARE Classic, saj je enostavno dobavljiva ter cenovno ugodna.

4.1.5.1 Čitalnik RFID – FRW-MH

FRW-MH je enota RFID, ki omogoča uporabo kartic po standardu MIFARE [4]. Podpira različne tipe kartic standarda MIFARE, med katerimi sta Classic ter Ultralight. Čitalec podpira uporabo enkripcijskih ključev za avtentikacijo kartic tipa Classic. Obstajajo tri različice čitalca, ki se razlikujejo glede na tip vhodno-izhodnega vmesnika. Tako so na voljo vmesniki po standardih RS-232, RS-485 in UART s TTL (angl. *Transistor-Transistor Logic*) nivoji signalov.

Za naše vezje smo izbrali tip s TTL-izhodom, saj je tako možno vhode in izhode čitalca povezati neposredno na mikrokrmilnik. Obstajata dve možnosti izbire delovanja čitalca, in sicer avtonomni način delovanja, ki ob detekciji prisotnosti kartice avtomatsko pošlje podatke o kartici na svoj izhod, ali ročni način delovanja, kjer je detekcijo prisotnosti kartice potrebno sprožiti z ustreznim ukazom. Odločili smo se za avtonomni način delovanja.

Polje	Možne vrednosti	Opomba
STX	0x02	
NASLOV ČITALCA	0x00 - 0x7C	Le za verzijo RS-485
DOLŽINA	0x04	
FUNKCIJA	0x04	
FRB	0x00 - 0x3F	Indeks bloka podatkov
ŠT.BLOKOV	0x00 - 0x01	0 - branje ID št. kartice / 1 branje podatkov
BCC	0x00 - 0xFF	Kontrolna vsota

Tabela 4.2: Primer podatkovnega ukaza za branje podatkov ali identifikacije kartice [4]

Vmesnik čitalca (UART) uporablja hitrosti prenosa podatkov 9600 bit/s ter nastavitve 8N1 oz. 8 bitov podatkov, brez bita paritete ter 1 stop bit. Po specifikacijah je čitalnik prilagojen za uporabo kartic do razdalje približno 40 mm. Čitalnik ima osem priključnih kontaktov, od katerih za delovanje potrebujemo le štiri in sicer liniji napajanja 0 in 5 V ter vhodno oz. izhodno linijo.

Komunikacija s čitalcem poteka z uporabo namenskega protokola. Vsak ukaz se prične z zlogom z vrednostjo 0x02, kar predstavlja vrednost za sinhronizacijo podatkov ukaza. V primeru uporabe RS-485-različice čitalca sledi naslov čitalca, v ostalih primerih postavimo to vrednost na 0x00. Sledi dolžina preostalih podatkov v poslanem paketu vključno z upoštevanjem samega polja dolžine. Polje funkcija se razlikuje glede na ukaz oz. povratne podatke. Polje FRB pove indeks želenega bloka podatkov za branje oz. pisanje. Sledi podatek o številu blokov za branje v primeru ukaza oz. sami podatki v primeru odgovora čitalca na ukaz za branje podatkov. Kot zadnje polje se pošlje kontrolna vsota prenesenih podatkov, ki se jo izračuna z uporabo logične operacije XOR nad vsemi zlogi v paketu. Primer ukaza za branje podatkov oz. serijske številke kartice je podan v tabeli 4.2.

4.1.6 Zajem podatkov o porabi vode

Za zajem podatkov o porabi vode smo uporabili namensko vodno turbino za merjenje pretoka z dajalnikom impulzov. Dajalnik impulzov ima fiksno razmerje števila impulzov glede na volumen porabljene vode. V našem projektu smo uporabili turbino z razmerjem 1000 impulzov na liter vode. Impulzni izhod turbine povežemo z vhodom centralnega vezja terminala ELVO in tako omogočimo beleženje porabe vode. Slika 4.9 prikazuje uporabljeno turbino.

Slika 4.9: Vodna merilna turbina s pulznim izhodom

4.1.7 Zajem podatkov o porabi električne energije

Enostaven način za zajem podatkov o porabi električne energije je uporaba namensko izdelanih števcev porabe z vgrajenim impulznim izhodom. Na trgu obstaja množica takih števcev, ki poleg samostojnega prikaza porabe električne energije z ustreznim prikazovalnikom predvidevajo dodatni impulzni izhod. Takšen izhod je natančno opredeljen v standardu DIN 43864 oz. novejšem ISO/IEC 62053-31. Vezje impulznega izhoda uporablja vezavo izhodnega tranzistorja v vezavi odprtega kolektorja (angl. *Open Collector*). Ob posameznem impulzu se tak izhod sklene na potencial mase in s tem omogoči detekcijo impulza z ustreznim vezjem. V tabeli 4.3 so prikazane osnovne karakteristike izhoda po standardu ISO/IEC 62053-31. Obstajata dve vrsti izhodov, in sicer sta to Klasa A (prenos pulzov na daljših povezavah) ter Klasa B (krajše povezave oz. sistemi z varčnim delovanjem).

Parameter	Klasa A	Klasa B
Najvišja napetost na izhodu (enosmerna napetost)	27 V	15 V
Največja tokovna obremenitev (izhod aktiven)	27 mA	15 mA
Najmanjša tokovna obremenitev (izhod aktiven)	10 mA	2 mA
Največja tokovna obremenitev (izhod neaktiven)	2 mA	0,15 mA
Čas trajanja impulza (minimalno)	30 ms	30 ms
Pavza med impulzi (minimalno)	30 ms	30 ms
Čas prehoda nivoja (maksimalno)	5 ms	5 ms

Tabela 4.3: Karakteristike impulznega izhoda po standardu ISO/IEC 62053-31

V našem sistemu smo uporabili električni števec z oznako DDS-1L, ki je prikazan na sliki 4.10. Števec predvideva galvansko ločitev izhoda od omrežja visoke napetosti z uporabo optičnega sklopnika. Izhod števca električne energije povežemo na enega od

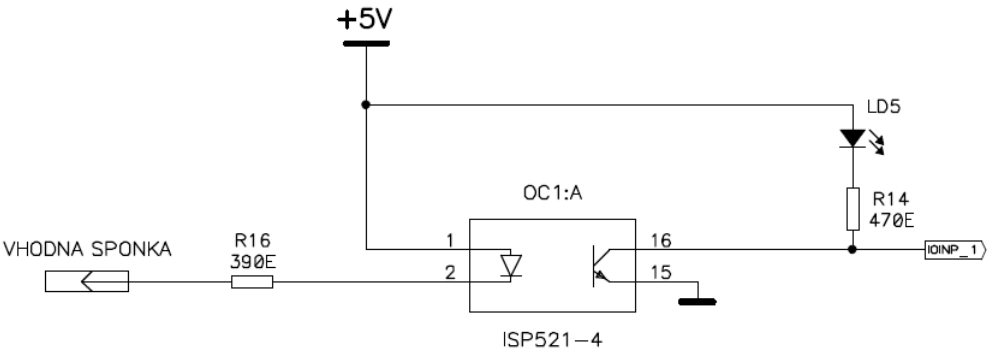
vhodov centralnega vezja terminala in tako omogočimo beleženje števila impulzov in s tem porabljene električne energije.

Slika 4.10: Števec porabe električne energije DDS-1L

Dolžina posameznega impulza števca DDS-1L je tipično okoli 90 ms. Impulzno razmerje je 1000 impulzov na kWh porabljene električne energije oz. 1 impulz na porabljeno Wh energije.

4.1.8 Vhodni kanali

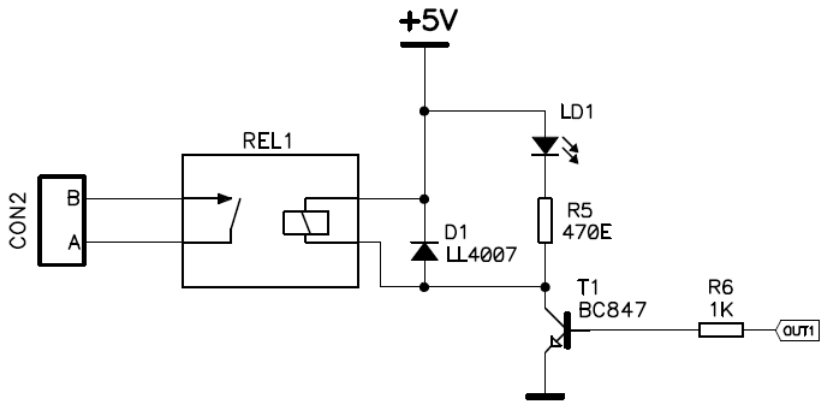
Vhodne kanale smo realizirali z uporabo optosklopnika. S tem zagotovimo dodatno zaščito vezja in samega mikrokrmilniškega vhoda, tako pred motnjami, kakor pred napetostnim sunkom višje napetosti. Aktivacija vhoda se izvede s priključitvijo vhodnega priključka na potencial mase. S tem se v optosklopniku vgrajena svetleča dioda aktivira in s tem aktivira izhodni tranzistor optosklopnika. Izhod optosklopnika je tipa odprti kolektor in kot tak lahko preklopi le v nizko stanje (0 V). Z vezavo upora med izhodom tranzistorja in napajanjem zagotovimo visoko stanje, kadar je izhodni tranzistor neaktiven. V ta namen smo izkoristili vezje za indikacijo vklopa, sestavljeno iz LED (angl. *Light Emitting Diode*) in ustreznega predupora. Slika 4.11 prikazuje shemo vezja enega izmed štirih vhodnih kanalov.



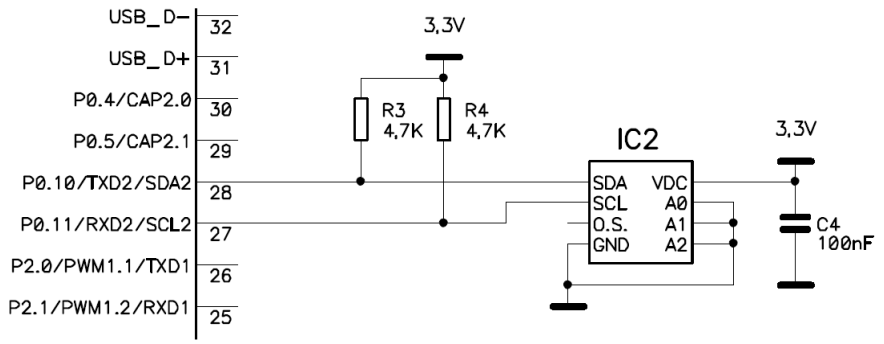
Slika 4.11: Vhodno vezje posameznega kanala

4.1.9 Izhodni kanali

Izhodne kanale smo realizirali z uporabo relejev, kot je prikazano na sliki 4.12. Nazivni tok navitja releja je okoli 40–50 mA, kar je preveč za mikrokrmilniške izhode, saj je tok na posamezni nožici omejen na največ 40 mA. Hkrati je potrebno krmiliti tudi svetlečo diodo, ki porabi približno 10 mA. V tem obziru smo uporabili ojačevalnik z tranzistorjem T1 v vezavi s skupnim emiterjem. S takšno vezavo hkrati zaščitimo morebitne zunanje motnje mikrokrmilnika in tako zagotovimo zanesljivejše delovanje le-tega. Zaščitna dioda D1 služi za kratkostičenje induciranega visokonapetostnega sunka ob izklopu releja. Uporabili smo indikacijo aktivnosti izhoda, ki smo jo realizirali z uporabo svetleče diode (LD1) in ustreznim preduporom za omejitev toka. Z opisanim vezjem in uporabo izbranih relejev lahko (z napetostjo 220 V) krmilimo porabnike do moči 1000 W, kar povsem zadošča za krmiljenje močnostnih izhodnih relejev posameznega priključka terminala ELVO.



Slika 4.12: Vezje izhodnega kanala



Slika 4.13: Priključitev senzorja temperature LM75

4.1.10 Meritev temperature

Z namenom merjenja temperature zraka v samem terminalu smo na vezje vgradili temperaturni senzor z oznako LM75 [28]. Izbrano vezje je samostojen in s strani proizvajalca umerjen senzor temperature. Po specifikacijah proizvajalca je zagotovljena natančnost senzorja ± 2 ^{o}C na celotnem temperaturnem območju delovanja (od –25 do +100 ^{o}C), kar zadošča za potrebe merjenja temperature v terminalu. Branje podatkov s senzorja poteka preko vodila I^{2}C. Shema 4.13 prikazuje povezavo senzorja temperature na mikrokrmilnik.

4.1.11 Vmesnik za omrežje Ethernet

Za priključitev v omrežje Ethernet je potrebno upoštevati zahtevane električne nivoje signala na omrežju. V ta namen obstaja vrsta namenskih integriranih vezij t. i. PHY (angl. *Physical Layer*), ki poskrbijo za pretvorbo med električnimi nivoji na fizičnem omrežju in vmesniki MAC. Uporabljeni mikrokrmilnik vsebuje le vezje MAC, zato je potrebno vgraditi zunanje vezje PHY. Uporabljena mikroprocesorska plošča mbed že vsebuje ustrezno vezje PHY, tako je potrebno dodati le ustrezno vtičnico za priklop mrežnega kabla. Dodatna zahteva priklopa na omrežje Ethernet je uporaba galvanskih ločilnih transformatorjev. Uporabili smo vtičnico, ki že vsebuje potrebne ločilne transformatorje skladno s standardom. Na sami vtičnici sta tudi dve svetleči diodi, ki smo ju uporabili za prikaz stanja omrežne povezave.

4.2 Programska oprema

Terminalska programska oprema je ključni del izdelave terminala. Programsko opremo smo napisali v programskem jeziku C, prevedli pa z uporabo prevajalnika GCC [26].

Osnova programske opreme je vgrajeni operacijski sistem SmartX. SmartX podpira uporabo večnitnosti in tako omogoča navidezno sočasno izvajanje različnih operacij. Za komunikacijo po omrežju Ethernet smo uporabil namensko razviti sklad TCP/IP imenovan mikroNet. Sklad nudi osnovne storitve za uporabo protokolov TCP/IP in povezavo z omrežjem Ethernet. Na osnovi sklada smo razvili implementacijo protokola HTTP, ki ga uporabljamo za povezavo s centralnim strežnikom.

Komunikacija s strežnikom poteka z uporabo protokola HTTP. Za tak pristop smo se odločili ker se tako izognemo dodatnemu razvoju in testiranju strežniških aplikacij, saj obstaja množica tako plačljivih kakor brezplačnih strežnikov HTTP.

S strežnika prenašamo primerno prirejene spletne strani, ki jih prikažemo na prikazovalniku uporabniškega vmesnika. Protokol HTTP uporabljamo tudi za poročanje o porabi virov kot tudi prejema ukazov s strani strežnika. Ena od ključnih nalog programa je beleženje porabe na posameznih vhodih. To je narejeno s štetjem impulzov s strani namenskih zunanjih enot. V programu moramo preštete impulze ustrezno shraniti v določen register in vrednosti le-tega periodično pošiljati strežniku. Branje izmerjene temperature senzorja LM75 se izvaja periodično in avtonomno.

4.2.1 Operacijski sistem SmartX

SmartX je odprtokodni vgrajeni operacijski sistem za mikrokrmilnike [29]. Podpira raznolike družine mikrokrmilnikov, med katerimi so družine ARM, Cortex, AVR ter nekatere ostale.

SmartX omogoča navidezno izvajanje različnih opravil z uporabi večnitnosti. Posamezni niti je možno nastaviti poljubno prioriteto in s tem je možno smiselno razporejanje izvajanja opravil glede na pomembnost samega opravila. Preklapljanje izvajanja niti je operacija ki jo opravlja del jedra operacijskega sistema (angl. *Scheduler*). Možni so različni načini preklopa in sicer skladno z določenim intervalom ali glede na določen dogodek (angl. *preemptive*). Vsaki niti je možno določiti prioriteto izvajanja in s tem ustrezno razporediti izvajanje pomembnejših ter časovno zahtevnejših niti. SmartX ima vgrajene različne osnovne sinhronizacijske elemente, kot so:

- dogodki (angl. *Events*),
- števni semaforji (angl. *Counting Semaphores*),
- poštni predali (angl. *Mailbox*),

- čakalne vrste (angl. *Queues*),
- binarni semaforji oz. ključavnice (angl. *Lock*),
- ekskluzivni zaklep (angl. *Mutex*).

4.2.2 Omrežni sklad TCP/IP – mikroNet

Omrežni sklad mikroNet je namensko razviti sklad TCP/IP, prilagojen za uporabo na sistemih, ki vsebujejo omejeno količino programskega in delovnega spomina. S tem namenom je sklad omejen na najnujnejše in osnovne funkcije, potrebne za delovanje skladno s standardi in tako ne vsebuje določenih naprednih funkcionalnosti oz. kjer le te so, podredi parametre delovanja za navedene sisteme. Vgrajene ima tudi vtičnike TCP ter tako olajša pisanje višjenivojskih plasti in same aplikacije. Kljub omejitvam sklad zagotavlja kompatibilnost s protokoli TCP/IP in kot tak zadostuje potrebam našega sistema.

Pregled osnovnih karakteristik sklada:

- podpira uporabo vmesnika MAC mikrokrmilnika LPC2368,
- pošilja in prejema okvire Ethernet,
- omogoča preslikavo med naslovi MAC in IP z uporabo protokola ARP,
- nudi osnovne funkcionalnosti omrežne plasti (naslavljanje, protokol ICMP),
- omogoča vzpostavljanje povezav TCP z uporabo vtičnikov.

4.2.3 Osnovna programska oprema

Delovanje programske opreme terminala ELVO je razdeljeno na naslednje osnovne operacije:

- zajem in beleženje podatkov o porabi virov,
- komunikacija s strežnikom,
- identifikacija uporabnika s pomočjo sistema RFID,
- upravljanje terminala s strani uporabnika,
- krmiljenje izhodov.

4.2.4 Beleženje podatkov o porabi virov

Beleženje podatkov o porabi vira se opravlja s štetjem impulzov, prejetih od zunanjih naprav, in z beleženjem le-teh v programskih registrih. Za samo izvedbo inkrementiranja smo uporabili mikrokrmilniško zunanjo prekinitev (angl. *External Interrupt*) ob spremembi stanja vhoda. Izbrani mikrokrmilnik omogoča štiri ločene zunanje prekinitve, ki so označene z EINT0 do EINT3. Vsaka od prekinitev uporablja določeno nožico na mikrokrmilniku in ima lasten rokovalnik prekinitve, le prekinitev EINT3 dodatno nudi možnost proženja le-te z uporabo večjega števila nožic mikrokrmilnika [25]. Posebnost pri uporabi tega načina je, da je v rokovalniku prekinitve potrebno programsko preveriti, kateri izmed vhodov je dejansko prožil prekinitev. Za posamezno prekinitev je možno izbrati nivojsko proženje ali proženje ob prehodu logičnega stanja in izbrati aktiven ali neaktiven nivo le-tega. Načrtovano vezje vsebuje štiri vhodne kanale, za kar bi zadoščala uporaba osnovnih zunanjih prekinitev mikrokrmilnika, a v tem primeru ne ostane prostih prekinitev za ostale, v prihodnosti možne potrebe. Odločili smo se za uporabo zunanje prekinitve EINT3 in omenjenega načina delovanja, kar omogoča tudi morebitno razširitev z več vhodnimi kanali. V samem rokovalniku prekinitve EINT3 preverimo, kateri kanal(i) so prekinitev prožili, in tako posodobimo ustrezne programske registre. Uporabili smo proženje ob prehodu logičnega nivoja, in sicer iz logične 1 v logično 0.

4.2.5 Komunikacija s strežnikom

Vsa komunikacija med terminalom in strežnikom poteka preko protokola HTTP. Sam protokol je zastavljen kot odjemalec–strežnik in ne omogoča asinhrone dvosmerne komunikacije. Vsled tega le odjemalec, v našem primeru terminal ELVO, lahko proži in pošlje zahteve strežniku, le-ta pa na zahteve odgovori. Temu je potrebno podrediti sam protokol komunikacije med terminalom in strežnikom.

Zahteve terminala v osnovi delimo v dve skupini:

- zahteve za posredovanje podatkov o porabi,
- zahteve za upravljanje z uporabniškim vmesnikom.

Zahtevo za posredovanje podatkov o porabi uporabljamo za periodično poročanje stanja števcev posameznih kanalov in hkrati za prejem ukazov o vklopu oz. izklopu posameznega vira. Sama zahteva sledi formatu zahteve "GET" protokola HTTP. Zahtevo pošiljamo s periodo 1 s, tudi v primeru ko ni nobeden izmed priključkov aktiven, saj (poleg podatkov

o porabi) hkrati poroča vrednost izmerjene temperature v terminalu. Posamezne informacije zapišemo v sam naslov URL kot parametre, skladno s formatom zahteve "GET". Primer take zahteve je:

```
GET /poraba.php?INPUT1=123&INPUT2=0&INPUT3=30&INPUT4=0&TEMPERATURE=22
```

S to zahtevo strežniku sporočimo podatke o trenutnem stanju posameznega števca vhodnih kanalov in izmerjeno temperaturo. Kot odgovor na navedeno zahtevo strežnik pošlje dokument v formatu XML (angl. *Extensible Markup Language*), v katerem so zapisana zahtevana stanja aktivacije priključkov. S tem terminal prejme informacijo o zahtevanem stanju priključkov in tako reagira na spremembo aktivacije v kolikor je to potrebno. Primer takega dokumenta je:

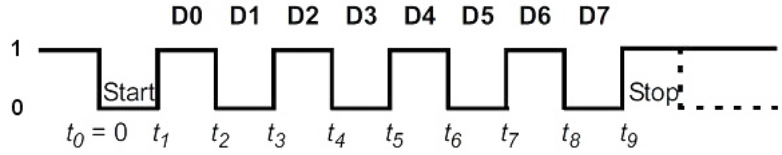
```
<xml>
 <outputs>
  <output id="0" state="1">
  <output id="1" state="0">
  <output id="2" state="0">
  <output id="3" state="0">
 <outputs>
<xml>
```

Druga vrsta zahtev so zahteve za upravljanje z uporabniškim vmesnikom. Na te zahteve strežnik odgovori z dokumentom v obliki HTML, ki se uporabi za prikaz na prikazovalniku terminala. Ob neprijavljenosti uporabnika terminal periodično pošilja zahtevo za začetno stran menija. Primer te zahteve je:

```
GET /idle.php
```

Ob prijavi uporabnika terminal strežniku sporoči identifikacijo uporabnika (oznako UID kartice RFID) z zahtevo za prijavno stran menija. Taka zahteva je:

```
GET /menu.php?userid=12345678
```



Slika 4.14: Logični nivoji na vmesniku UART, pri prenosu enega zloga v formatu 8N1

V kolikor je uporabnik strežniku znan oz. vnesen v bazi avtoriziranih uporabnikov, strežnik le-temu omogoči dostop do začetne strani uporabniškega menija. To stori s pošiljanjem ustreznega dokumenta HTML, v katerega med drugim vpiše podatke o uporabniku in stanje dobroimetja le-tega. Uporabnik ima sedaj možnost izbire vklopa oz. izklopa določenega priključka. V primeru neavtoriziranega uporabnika strežnik odgovori z začetno stranjo menija.

4.2.6 Identifikacija uporabnika s pomočjo RFID

Uporabnik ob prijavi v sistem približa kartico RFID čitalcu, ki po zaporednem vmesniku sporoči prisotnost in oznako kartice (UID). Zaporedni vmesnik je skladen s standardom UART. UART omogoča dvosmerno komunikacijo v asinhronem načinu (sprejem je neodvisen od pošiljanja podatkov). Za komunikacijo s čitalcem uporabimo format podatkov z nastavitvami 8N1 (8 podatkovnih bitov, 1 stop bit in brez paritetnega bita). Slika 4.14 prikazuje potek logičnih nivojev signala (za prenos zloga z vrednostjo 0x55) na vmesniku UART z nastavitvami 8N1. Hitrost vmesnika UART nastavimo na 9600 bitov/s. To naredimo z vpisom ustreznih delilnih faktorjev v registre vmesnika UART, s katerimi delimo osnovno urino frekvenco in tako dosežemo želeno hitrost prenosa [25]. Mikrokrmilnik LPC2368 omogoča deljenje osnovne frekvence z racionalnim številom in tako omogoča izredno natančno nastavitev prenosne hitrosti ne glede na osnovno frekvenco ure. Za izračun prenosne hitrosti uporabimo enačbo 4.1.

$$UART_{baudrate} = \frac{PCLK}{16 * (256 * UDLM + UDLL) * (1 + \frac{Div}{Mul})} \tag{4.1}$$

pri čemer je $PCLK$ osnovna frekvenca ure vmesnika, $UDLM$ in $UDLL$ vrednosti registrov osnovnega delilnika, Div in Mul pa vrednosti racionalnega števila deljenja ure.

Izbrana osnovna frekvenca ure vmesnika UART je 12 MHz. Vsled tega izberemo ustrezne vrednosti registrov in tako lahko izračunamo dobljeno hitrost (enačba 4.2). Izračunana hitrost 9615,38 bit/s od idealne hitrosti 9600 bit/s odstopa manj kot 1 % in je tako v

mejah zanesljivega delovanja vmesnika. V pomoč pri izbiri vrednosti lahko uporabimo tabele, podane v dokumentaciji mikrokrmilnika [25].

$$UART_{baudrate} = \frac{12000000}{16 * (256 * 0 + 48) * (1 + \frac{5}{8})} \tag{4.2}$$

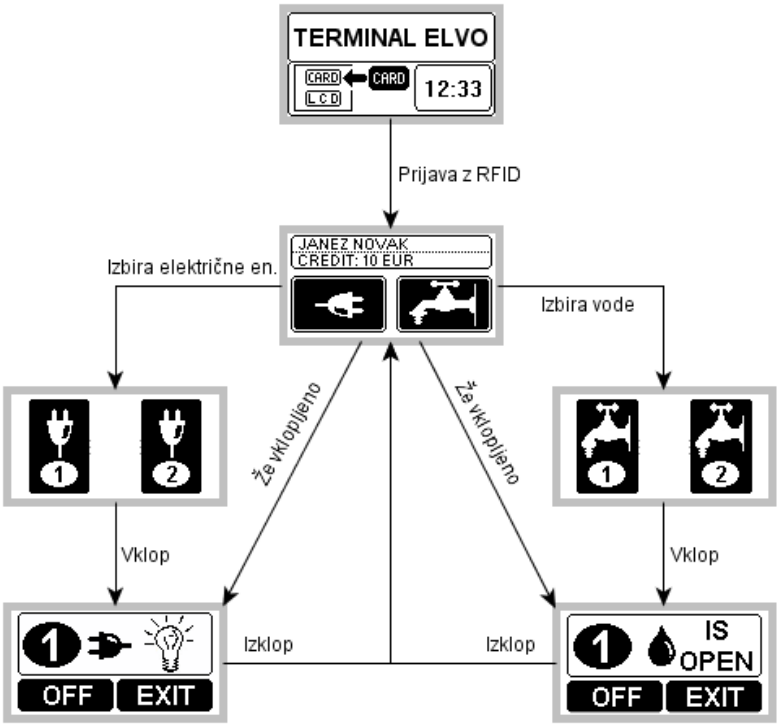
$$UART_{baudrate} = 9615,38 \text{ bit/s} \tag{4.3}$$

Sprejem posameznega zloga je operacija, ki se opravi samostojno (brez izvajanja programa) s strani vmesnika UART. Vmesnik ima vgrajen medpomnilnik FIFO (angl. *First In First Out*), v katerega shranjuje prejete zloge. Ko se medpomnilnik napolni do določene meje, vmesnik pošlje jedru zahtevo za ustrezno prekinitev. V ta namen smo napisali prekinitveni rokovalnik, ki ob izvajanju opravi branje podatkov iz vmesnikovega medpomnilnika in jih shrani v glavni pomnilnik za kasnejšo obdelavo. Ustrezna zanka programa podatke iz pomnilnika prebere in preveri ali je bila informacija o številki kartice (UID) pravilno prejeta ter (v kolikor ustreza) le-to shrani. Ob uspešnem prejemu proži proceduro za prijavo uporabnika na strežnik.

4.2.7 Uporabniški grafični vmesnik na terminalu

Za izdelavo grafičnega uporabniškega vmesnika smo se odločili za uporabo jezika za označevanje nadbesedila (HTML). S strežnika pridobimo ustrezne datoteke HTML, ki jih uporabimo za prikaz na prikazovalniku terminala. S tem je omogočeno pregledno vodenje uporabnika skozi postopek aktivacije posameznega priključka. Na terminalu smo implementirali ustrezno programsko knjižnico za prikazovanje dokumentov HTML.

Uporabniški vmesnik pozna dva osnovna načina delovanja. V primeru ko na terminalu ni prijavljenega uporabnika, vmesnik prikazuje le stran z informacijami o stanju terminala in trenutno uro. Ob prijavi uporabnika preide v stanje prikaza uporabniškega menija, kjer lahko uporabnik preveri stanje lastnega dobroimetja na računu in ima možnost izbire posameznih opcij menija. Meni je zastavljen tako, da vodi uporabnika skozi vse možnosti izbire in aktivacije prostih priključkov. V kolikor ima uporabnik v določeni skupini priključek že aktiviran se v uporabniškem meniju prikaže opcija za izklop le-tega. Slika 4.15 prikazuje možna stanja (strani) uporabniškega menija in prehode med stanji.



Slika 4.15: Pregled možnih stanj (strani) uporabniškega menija

4.2.8 Krmiljenje izhodov

Krmiljenje izhodov se opravi s postavitvijo ustreznega stanja ustrezne nožice mikrokrmilnika in s tem aktivacije ustreznega relejskega izhoda. Izbira stanja posameznih priključkov je povsem v domeni strežnika. Terminal le pasivno izvršuje prejete strežniške ukaze, prejete v odgovoru na zahtevo poročanja stanja števcev.

Poglavje 5

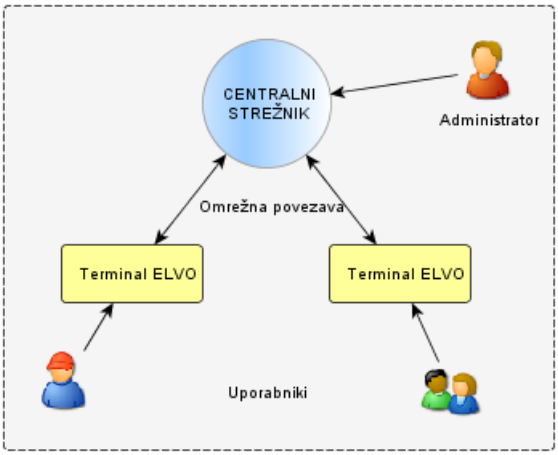
Strežniška programska oprema

Strežnik predstavlja centralni del sistema, saj usklajuje delovanje terminalov, beleži porabo po posameznem terminalu in vodi seznam avtoriziranih uporabnikov sistema. Hkrati smo strežnik izkoristili za omogočanje dostopa pooblaščenim upravljalcem sistema. Izdelali smo ustrezno spletno aplikacijo, s katero sta omogočena upravljanje in nadzor celotnega sistema. Slika 5.1 prikazuje zasnovo sistema v primeru uporabe dveh terminalov.

Pri razvoju strežnika smo se oprli na obstoječe strežniške tehnološke rešitve. Kot osnovno platformo smo uporabili spletni strežnik v povezavi s podatkovno bazo. Spletni strežnik nudi dostop preko protokola HTTP tako terminalom ELVO kot tudi administratorjem sistema. Odločili smo se za uporabo spletnega strežnika Apache s podporo skriptnega jezika PHP (angl. *PHP: Hypertext Preprocessor*) ter podatkovne baze MySQL.

5.1 Spletni strežnik Apache

Spletni strežnik Apache je odprtokodni strežnik za nudenje storitev z uporabo protokola HTTP [30]. Uporaben je kot samostojen strežnik HTTP ali kot platforma za uporabo vstavkov, s katerimi je mogoče izjemno razširiti uporabnost in zmogljivost strežnika. Med vstavki najdemo npr. skriptne jezike za izdelavo dinamičnih spletnih strani in knjižnice za dostop do podatkovne baze. Strežnik Apache ima največji tržni delež med spletnimi strežniki na internetu (okoli 55%), uporablja ga preko 350 milijonov internetnih strani [31]. Strežnik Apache je možno poganjati na različnih operacijskih sistemih, tako na Linux, Windows ali platformah OS-X.



Slika 5.1: Zgradba celotnega sistema z dvema terminaloma

5.2 Skriptni jezik PHP

Skriptni jezik PHP je osnova za izdelavo dinamičnih spletnih strani [32]. Je skupina ukazov (skripta) s katero je možno v realnem času izdelati dokumente HTML in tako prilagoditi izgled dokumenta glede na želene zahteve ali potrebe. PHP omogoča povezavo s podatkovnimi bazami in s tem dostop do podatkov ter matematične ali različne obdelave le-teh. Leta 1994 ga je razvil dansko-kanadski programer Rasmus Lerdorf. Od takrat je bilo narejenih ogromno dodelav in razširitev jezika. Izhaja iz osnov programskega jezika C, ki mu je po sintaksi tudi dokaj podoben. PHP vključimo v spletni strežnih Apache kot vstavek oz. zunanjo knjižnico. Strežnik tako datoteke tipa php obdela z vstavkom PHP ter pošlje odjemalcu.

5.3 Podatkovna baza MySQL

Z namenom trajnega hranjenja podatkov o konfiguraciji sistema in o uporabniškem dobroimetju smo uporabili sistem za upravljanje s podatkovnimi bazami – SUPB (*Sistem za Upravljanje s Podatkovnimi Bazami*). Izbrali smo relacijsko podatkovno bazo MySQL [33]. MySQL je odprtokodni, brezplačni sistem za upravljanje z relacijskimi podatkovnimi bazami. Omogoča uporabo transakcij, kar je izjemnega pomena pri vodenju konsistentnega stanja podatkov o terminalskem sistemu. MySQL deluje po principu strežnik – odjemalec in tako omogoča večuporabniški dostop s strani ločenih odjemalcev. Za dostop do podatkovne baze iz aplikacije smo uporabili ustrezno knjižnico, del jezika PHP.

Ime polja	Dolžina polja	Opis
Tip slike	spremenljiva	Tip slike. 0 - WBMP
Rezervirano	1 zlog	Vrednost 0
Širina	spremenljiva	Širina slike v točkah
Višina	spremenljiva	Višina slike v točkah
Podatki	spremenljiva	Podatki - 1 bit za vsako točko

Tabela 5.1: Zapis datoteke WBMP

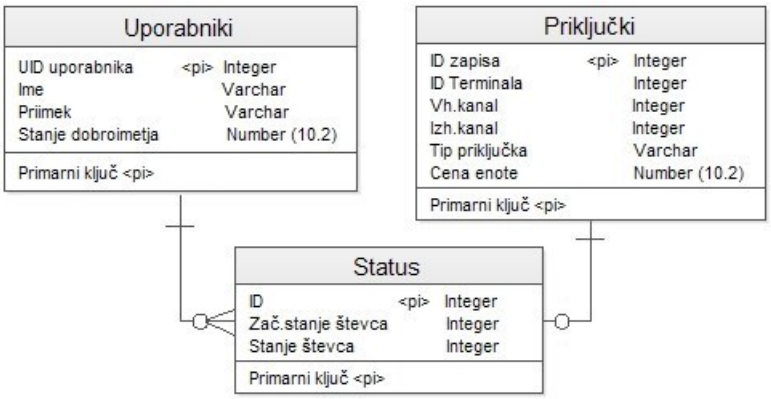
5.4 Terminalski vmesnik

5.4.1 Dokumenti HTML

Terminalski uporabniški vmesnik temelji na prikazu dokumentov HTML, ki jih pošiljamo terminalu skladno z zahtevami in stanjem sistema. V dokumente HTML po potrebi vključimo grafične elemente oz. slikovne datoteke. Dokumenti so ustrezno prilagojeni, skladno z zahtevami in omejitvami terminala. Tako moramo upoštevati ločljivost uporabljenega grafičnega prikazovalnika in omejitve knjižnice za obdelavo dokumentov HTML. Posebna omejitev je nedostopnost knjižnic za uporabo kompleksnih grafičnih zapisov kot npr. PNG (*Portable Network Graphics*), JPEG (angl. *Joint Photographic Experts Group*) ali podobnih. Kot omejitev se postavlja tudi majhna količina spomina terminalskega mikrokrmilnika. Odločili smo se za uporabo izjemno enostavnega grafičnega zapisa WBMP (angl. *Wireless Bitmap*), opisanega v poglavju 5.4.2.

5.4.2 Grafični zapis WBMP

Grafični zapis WBMP je izjemno enostaven zapis grafičnih datotek, ki je bil razvit z namenom uporabe v sistemu WAP (angl. *Wireless Application Protocol*) [34]. Zapis WBMP omogoča definiranje večjega števila tipov slik. Trenutno je definiran le tip 0, uporaben za zapis enobarvnih slik, saj uporablja le en bit za posamezno točko slike. Bit z vrednostjo 0 označuje črno oz. prisotnost barve, bit z vrednostjo 1 pa belo oz. odsotnost barve. Zapis WBMP omogoča uporabo poljubne velikosti slike, saj ne postavlja omejitev glede tega. Podatki o velikosti skupaj s še nekaterimi osnovnimi podatki o sliki se zapišejo v glavo oz. začetek datoteke. Tabela 5.1 prikazuje vsebino zapisa datoteke WBMP.



Slika 5.2: Konceptualni model podatkovne baze

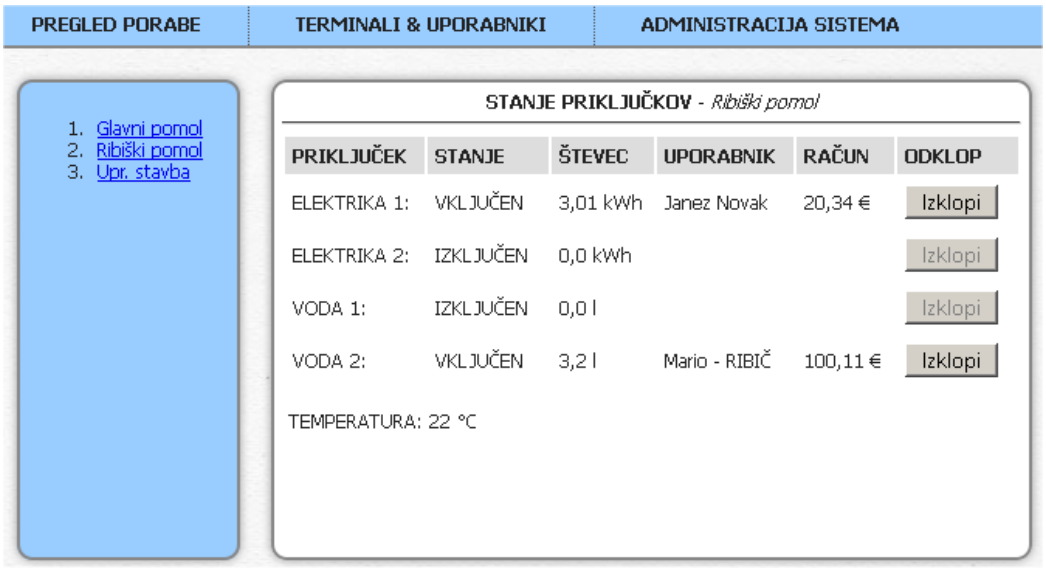
5.4.3 Konceptualni model podatkovne baze

Podatke o trenutnem stanju sistema hranimo v podatkovni bazi. V ta namen smo izdelali konceptualni model baze, prikazan na sliki 5.2. Model lahko v grobem delimo na entitete za hranjenje uporabniških podatkov, entitete za informacije o vseh priključkih po posameznem terminalu in entitete o trenutnem (delovnem) stanju sistema. Entiteto priključkov tipično izpolnimo ob postavitvi ali kasnejšem vzdrževanju sistema. Med rednim delovanjem sistema se teh informacij ne spreminja. Entiteto uporabnikov uporabimo za hranjenje vseh v sistemu avtoriziranih uporabnikov. V to entiteto dodajamo ali iz nje brišemo uporabnike skladno z registracijo uporabnika in izdajanjem identifikacijskih kartic RFID. Entiteta o statusu se tipično dostopa s strani skript aplikacije na strežniku in se uporablja za beleženje tekočega stanja posameznega priključka v sklopu celotnega sistema.

5.5 Administracijski uporabniški vmesnik

Za administracijo celotnega sistema smo zastavili in naredili spletno aplikacijo. Razvili smo administracijski uporabniški portal, ki omogoča dostop do sistema administratorjem ali ustreznim pooblaščenim osebam ter tako pregled in upravljanje le-tega. Uvedli smo dostop do podatkovne baze o informacijah terminalov ter napisali ustrezne skripte za dostop in urejanje posameznih tabel ter izvoz podatkov v dokumente HTML in tako prikaz uporabniku aplikacije. Izgled spletne aplikacije je prikazan na sliki 5.3. Aplikacija omogoča prijavo uporabnikom z uporabo gesla in tako dostop le pooblaščenim osebam.

Spletna aplikacija je razdeljena na tri osnovne dele:



Slika 5.3: Pregled porabe po terminalu

- pregled porabe,
- upravljanje terminalov in uporabnikov,
- administracija sistema.

5.5.1 Pregled porabe

Administracijski vmesnik omogoča pregled trenutnega stanja priključkov posameznega terminala. Za vsak terminal je izpisano stanje vseh priključkov, trenutna porabljena količina vira in informacije o prijavljenem uporabniku. Slika 5.3 prikazuje izgled strani pregleda uporabe. Pooblaščeni osebi je na voljo tudi možnost izključitve aktivnega priključka ne glede na stanje dobroimetja uporabnika (uporabnik lahko pozabi izključiti priključek) in s tem centralno upravljanje priključkov na terminalih.

5.5.2 Upravljanje uporabnikov

V to skupino spadajo operacije tekočega delovanja kot so dodajanje ali brisanje uporabnikov. Možno je dodatki ali odvzeti dobroimetje na računu uporabnika, in/ali uporabnika popolnoma izbrisati iz sistema in mu s tem onemogočiti nadaljnjo uporabo le-tega.

5.5.3 Administracija sistema

Stran za administracijo sistema nudi upravljanje sistema ob začetni postavitvi terminalov ali kasnejšem vzdrževanju le-teh. Vmesnik omogoča nastavljanje količine in tipa priključkov na posameznem terminalu skladno s samo izvedbo terminala. Posameznemu priključku je možno nastaviti naslednje lastnosti: izhodni kanal na krmilnem vezju, vhodni kanal na krmilnem vezju, tip priključka ter cena enote porabe (voda – liter ali električna energija – Wh).

Poglavje 6

Sklepne ugotovitve

V tej diplomski nalogi smo prikazali možno izvedbo vgrajenega sistema za obračunavanje porabe vode in električne energije na javnih mestih. Opisan je bil sistem, ki s pomočjo računalniškega omrežja centralizira nadzor in upravljanje večjega števila priključnih mest. S tem je omogočeno pregledno upravljanje celotne infrastrukture na enem mestu, najsi bo to lokalno na območju sistema ali povsod, od koder je možen dostop preko interneta. Opisani terminali ponujajo omejeno število priključkov na posameznem priključnem mestu, vendar je opisane osnove in principe možno uporabiti tudi za izdelavo zmogljivejših terminalov ter uporabo večjega števila le-teh in s tem pokrivanje široke potrebe ponudnikov storitev. Predstavljen je bil pregled osnovnih uporabljenih tehnologij, vključno z lastno razvitim skladom TCP/IP za vgrajene sisteme in z namensko razvito knjižnico za obdelavo jezika za označevanje nadbesedila – HTML.

Celoten sistem je bil tudi praktično realiziran in s tem je bila dokazana izvedljivost takega sistema v praksi. Izvedba je bila opravljen do faze prototipa. Za serijsko proizvodnjo bi bilo smiselno določene dele sistema optimizirati in s tem zmanjšati stroške same izdelave terminalov ali razširiti funkcionalnost z večjim številom priključkov po enoti.

Literatura

[1] (2012) Media Access Control address. Dostopno na:
http://en.wikipedia.org/wiki/MAC_address

[2] (2012) mbed LPC2368 - Rapid Prototyping with Microcontrollers. Dostopno na:
http://mbed.org/handbook/mbed-NXP-LPC2368

[3] (2012) DOGL Graphic Series. Dostopno na:
http://www.lcd-module.com/eng/pdf/grafik/dogl128-6e.pdf

[4] (2012) FRW 13.56MHz ISO14443A MIFARE READER/WRITER. Dostopno na:
http://www.inoutsrl.it/common/pdffiles/FRW-SER-M.pdf

[5] (2012) Open Systems Interconnection (OSI) model. Dostopno na:
http://en.wikipedia.org/wiki/OSI_model

[6] (2012) Internet protocol suite. Dostopno na:
http://en.wikipedia.org/wiki/TCP/IP_model

[7] (2012) Requirements for Internet Hosts - Communication Layers. Dostopno na:
http://tools.ietf.org/html/rfc1122

[8] (2012) IEEE 802.3 Working Group standards. Dostopno na:
http://www.ieee802.org/3/

[9] (2012) IEEE 802 standards family. Dostopno na:
http://en.wikipedia.org/wiki/IEEE_802

[10] (2012) IANA Considerations and IETF Protocol Usage for IEEE 802 Parameters. Dostopno na:
http://tools.ietf.org/html/rfc5342

[11] (2012) An Ethernet Address Resolution Protocol. Dostopno na:
http://tools.ietf.org/html/rfc826

[12] (2012) Internet Protocol. Dostopno na:
http://tools.ietf.org/html/rfc791

[13] (2012) Internet Protocol Version 4 (IPv4). Dostopno na:
http://en.wikipedia.org/wiki/Ipv4

[14] (2012) Internet Protocol Version 6 (IPv6). Dostopno na:
http://en.wikipedia.org/wiki/IPv6

[15] (2012) Internet Control Message Protocol. Dostopno na:
http://tools.ietf.org/html/rfc792

[16] (2012) Transmission Control Protocol. Dostopno na:
http://tools.ietf.org/html/rfc793

[17] (2012) TCP Extensions for High Performance. Dostopno na:
http://tools.ietf.org/html/rfc1323

[18] (2012) Hypertext Transfer Protocol - HTTP/1.0. Dostopno na:
http://tools.ietf.org/html/rfc1945

[19] (2012) Hypertext Transfer Protocol - HTTP/1.1. Dostopno na:
http://tools.ietf.org/html/rfc2616

[20] (2012) Radio-frequency identification. Dostopno na:
http://en.wikipedia.org/wiki/Radio-frequency_identification

[21] (2012) Quantized radio modulation modes. Dostopno na:
http://en.wikipedia.org/wiki/Category:Quantized_radio_modulation_modes

[22] (2012) Application security. Dostopno na:
http://en.wikipedia.org/wiki/Application_security

[23] (2012) Mifare portal. Dostopno na:
http://mifare.net/

[24] (2012) ARM7 Processor Family. Dostopno na:
http://www.arm.com/products/processors/classic/arm7/index.php

[25] (2012) LPC23XX User Manual. Dostopno na:
http://www.nxp.com/documents/user_manual/UM10211.pdf

[26] (2012) GCC, the GNU Compiler Collection. Dostopno na:
http://gcc.gnu.org/

[27] (2012) LCD DOG series. Dostopno na:
http://www.lcd-module.com/products/dog.html

[28] (2012) Digital Temperature Sensor and Thermal Watchdog with 2-wire Interface. Dostopno na:
http://datasheets.maximintegrated.com/en/ds/LM75.pdf

[29] (2012) SmartX - a preemptive, multitasking, priority based RTOS. Dostopno na:
http://smartx.sourceforge.net/

[30] (2012) The Apache Software Foundation. Dostopno na:
http://www.apache.org/

[31] (2012) Netcraft - Web Server Survey. Dostopno na:
http://news.netcraft.com/archives/2013/01/07/january-2013-web-server-survey-2.html

[32] (2012) PHP: Hypertext Processor. Dostopno na:
http://php.net/

[33] (2012) MySQL Database. Dostopno na:
http://www.mysql.com/

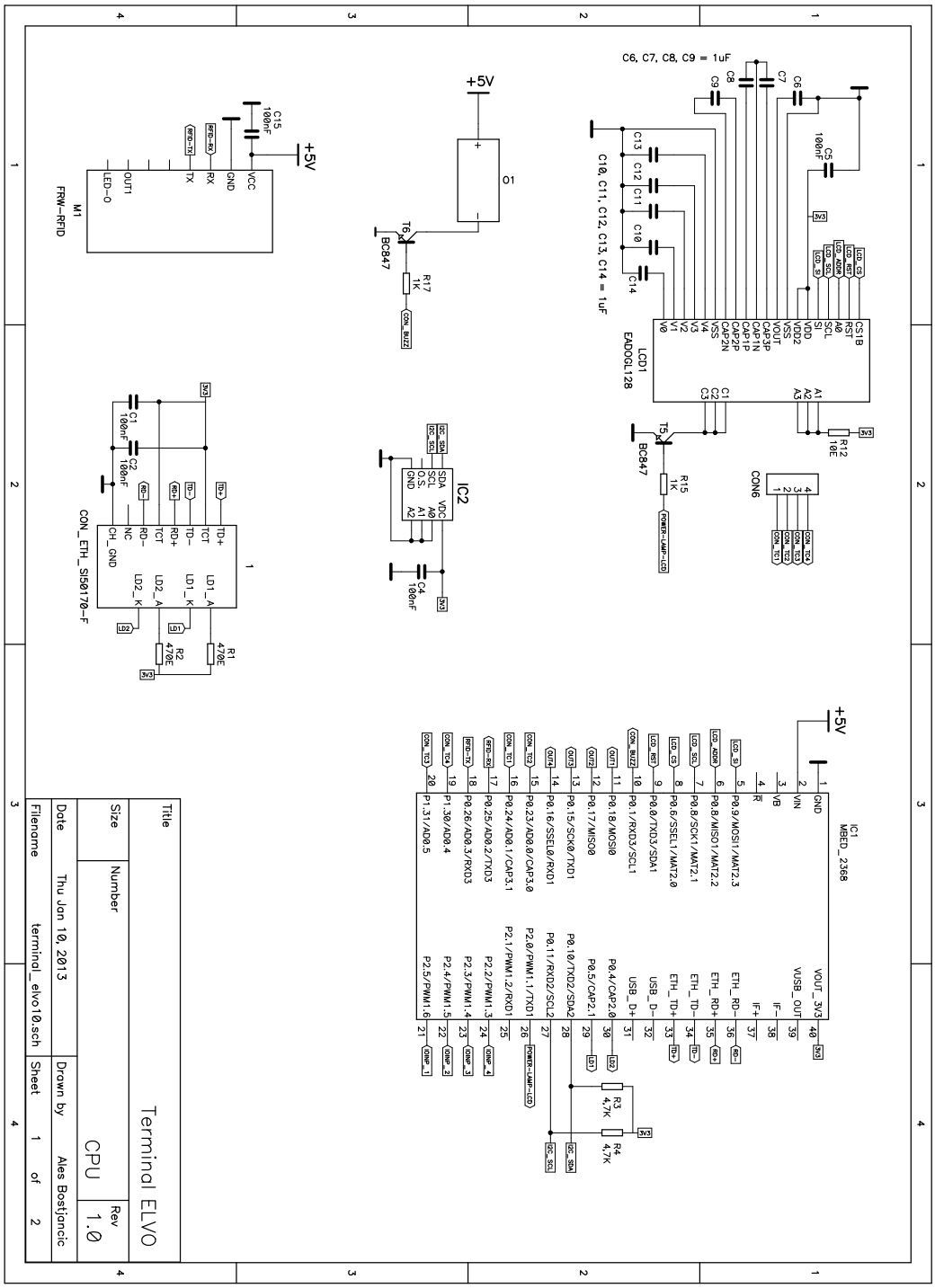
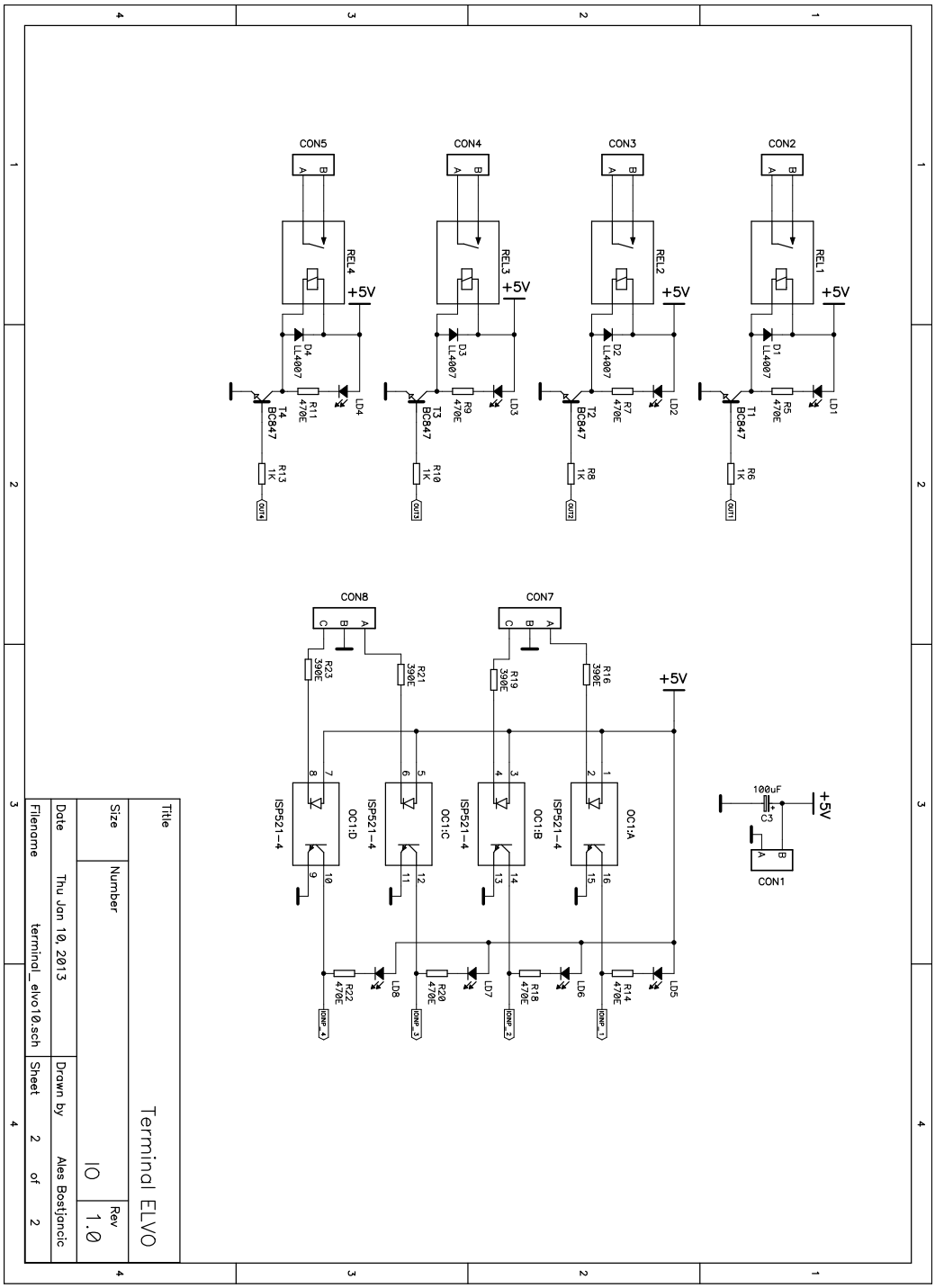
[34] (2012) Wireless Application Protocol Bitmap Format. Dostopno na:
http://en.wikipedia.org/wiki/Wireless_Application_Protocol_Bitmap_Format

[35] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Second Edition*, John Wiley & Sons, 2003

[36] T. Martin, *Introduction to the LPC2000*, Hitex (UK) Ltd., 2006

Priloga A - Električna shema centralnega vezja terminala ELVO

A.1 Mikrokrmilniški del



A.2 Vhodni in izhodni kanali