Prenos alarmnih sporočil preko interneta v sistemu Intervencije.net

Tomaž Dežman[1], Grega Jakus[2]

[1]*Aldia, d.o.o., informacijske storitve, Pot za Brdom 100, 1000 Ljubljana*
[2] *Univerza v Ljubljani, Fakulteta za elektrotehniko, Tržaška 25, Ljubljana, Slovenija*
E-pošta: tomaz.dezman@aldia.si, grega.jakus@fe.uni-lj.si

Transferring alarm messages in Intervencije.net system over internet

Abstract. *Intervencije.net is a system that activates rescue services, like fire departments or emergency medical service teams. The system currently supports collecting information about an incident from various communication channels, including paging system, telephone network, text messages, and forwarding information to members of intervention teams.*

It is now necessary to upgrade the system with internet-based message transfer in the event of an automatic incident detection. Required is a definition of a new protocol, based on TCP protocol and upgraded with client identification and authentication mechanisms, data encryption and communication path availability control.

Clients are simple IoT devices, collecting data from their environment and forwarding alarms to the server. The server part processes alarm data and, when required, notifies the rescue services.

Currently, upgrading of the system is in its testing phase, aimed at discovering errors and troubleshooting as well as establishing, if the system meets the needs of its users. Once the testing phase is concluded, the devices will be introduced into real-world environments. Initially, we plan to install the IntP devices in fire stations and health centres, later however, they will also be offered to individual members of rescue services, so they can stay connected in their flats and houses.

1 Uvod

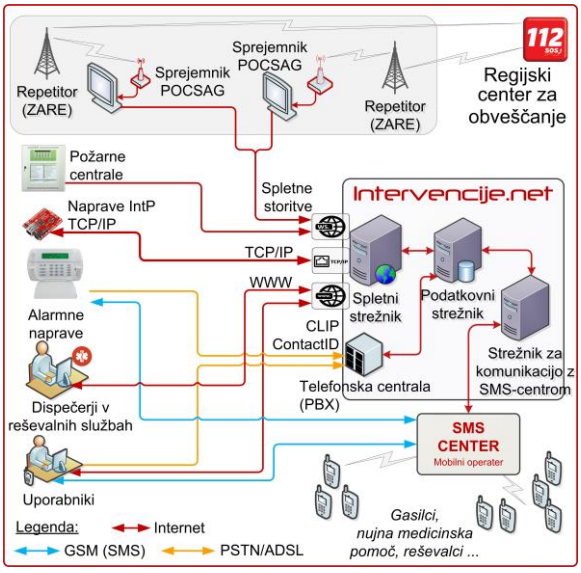
Vpeljava sodobnih informacijsko-komunikacijskih tehnologij na področju zaščite in reševanja pomembno vpliva na učinkovitost reševalnih skupin. S takojšnjim posredovanjem natančnih informacij o nesreči reševalni službi lahko namreč prepolovimo njen odzivni čas, čemur pritrjuje tudi analiza sistema eCall, ki v primeru prometne nesreče samodejno sporoči mesto nesreče pristojnim službam [1]. Poleg tega lahko intervencijo organiziramo učinkoviteje, če imamo informacijo o tem, kdo se je nanjo odzval in kakšno opremo ima na voljo.

V Sloveniji imamo zelo dobro razvite in razvejane službe za zaščito in reševanje. Če bi po zgledu sistema eCall vpeljali samodejno obveščanje pristojnih služb tudi v primeru vseh ostalih nesreč v naravnem in urbanem okolju ter v zasebnih prostorih in javnih ustanovah, bi s tem omilili posledice teh nesreč in tako pomembno pripomogli k zaščiti ljudi in njihovega imetja.

O aktualnosti problematike priča množica projektov, ki so v teku, izmed katerih se večina osredotoča na vodenje intervencij na nacionalni ravni. Primera sta projekta NEXES [2], ki se ukvarja predvsem z geografskim usmerjanjem klicev v regijske centre za obveščanje (112), in 6InACtion [3], ki je namenjen vzpostavitvi intervencijskega prenosnega omrežja v primeru obsežnih naravnih in drugih nesreč.

V Sloveniji sicer od leta 2010 deluje sistem Intervencije.net, ki je za razliko od navedenih sistemov namenjen podpori posameznim (lokalnim) intervencijskim službam. Sistem Intervencije.net je bil razvit z namenom izboljšati obveščanje prostovoljnih gasilcev v primeru intervencije, kmalu po njegovi uvedbi pa se je izkazalo, da je uporaben tudi za druge službe, kot so nujna medicinska pomoč, bolnišnice, zdravstveni domovi, gorska in jamarska reševalna služba, kinološka zveza in druge. V zadnjem času so se v sistem začela vključevati tudi nekatera podjetja, ki imajo organizirane lastne reševalne službe. Danes tako v sistemu Intervencije.net deluje že več kot 930 reševalnih služb z več kot 35 tisoč reševalci.

Čeprav je sistem Intervencije.net namenjen predvsem podpori lokalnih intervencijskih skupin, pa omogoča tudi integracijo s sistemi za vodenje intervencij na nacionalni ravni, saj lahko zanje zbira podatke iz lokalnih okolij.



Slika 1. Arhitektura sistema Intervencije.net [4]

Na Sliki 1 je prikazana arhitektura sistema Intervencije.net. Jedrni del sistema sestavljajo

- *podatkovni strežnik*, ki shranjuje prejeta in poslana sporočila, podatke o uporabnikih itd.,
- *spletni strežnik*; namenjen gostovanju spletnih strani in storitev,
- *strežnik PBX*, ki prestreže klice, jih obdela in posreduje podatkovnemu strežniku, ter
- *strežnik za komunikacijo z SMS-centri* mobilnih operaterjev.

Informacije o nesrečah so zbrane preko

- *spletnih storitev*, namenjenih sprejemanju alarmov iz požarnih central in sporočil, ki jih regijski centri za obveščanje sicer pošiljajo pozivnikom članov reševalnih služb,
- *spleta*, z uporabo katerega lahko obveščanje članov sproži končni uporabnik sistema ali pa dispečer preko spletne strani;
- *klica na predpisano stacionarno telefonsko številko*, pri čemer kombinacija kličoče in klicane številke sproži aktivacijo neke enote;
- *protokola ContactID*, ki ga uporabljajo alarmne naprave za javljanje alarmov varnostno-nadzornim centrom;
- *SMS sporočil*.

Sistem posreduje informacije o nesreči članom reševalnih enot ali drugim napravam preko SMS-sporočil in elektronske pošte. Obveščeni se lahko odzove na intervencijsko sporočilo s klicem na določeno telefonsko številko. Pregled odzivov je dostopen preko spletne strani, tako da je vodja intervencije seznanjen, kdo se je namerava udeležiti.

2 Nadgradnja sistema

Čeprav so Intervencije.net že uveljavljen in preverjeno uporaben sistem, ima ta še vedno nekaj omejitev. Ena izmed njih je zmožnost posredovanja informacij samo o tistih nesrečah, o katerih je nekdo že obvestil center za obveščanje, samodejno obveščanje pa povečini ni mogoče.

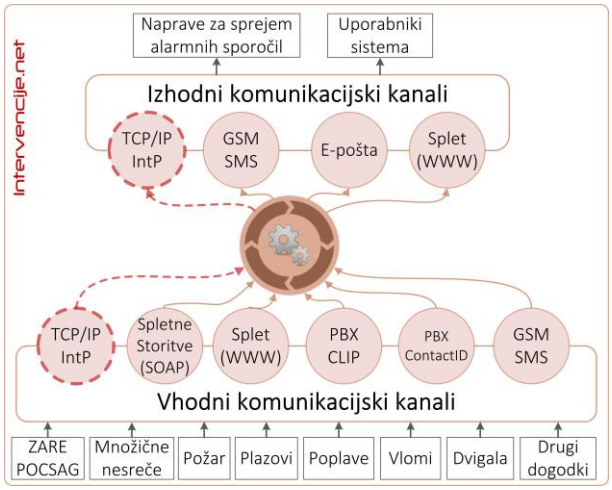
Poleg tega določene reševalne službe niso vključene v sistem tihega alarmiranja (ne uporabljajo pozivnikov), v takih primerih pa je obveščanje lastnega osebja, ko reševalna služba prejme poziv na intervencijo, pogosto zamudno in nepraktično. Takšno obveščanje je trenutno mogoče s prijavo v spletno aplikacijo in vpisom intervencijskega sporočila ali pošiljanjem SMS-sporočila oziroma klicem s točno določene naprave na določeno številko. Obveščanje bi bilo veliko lažje, če bi obstajala naprava, ki bi ob pritisku na tipko samodejno sprožila obveščanje osebja.

Po drugi strani nekatere skupine, na primer gasilci, želijo določeno avtomatizacijo postopkov ob pozivu na intervencijo, kot na primer

- obveščanje članov gasilskega društva z opravljenim strokovnim izpitom iz nudenja prve pomoči, ko je zaznana uporaba samodejnega zunanjega defibrilatorja (AED),
- odpiranje garažnih vrat gasilskega doma in
- obveščanje ljudi v okolici s svetlobnim in zvočnim signalom, da se ti umaknejo gasilcem.

Poleg omenjenega mora biti nadgradnja sistema cenovno sprejemljiva, brez dodatnih stroškov, kot je naročnina pri mobilnem operaterju in tako dosegljiva čim širšemu krogu uporabnikov.

Za izpolnitev omenjenih zahtev smo se odločili za dopolnitev obstoječega sistema z dvosmernim komunikacijskim kanalom, ki bo temeljil na internetnem omrežju in protokolnem skladu TCP/IP (Slika 2, rdeča črtkana črta).



Slika 2. Vhodno-izhodni kanali strežniškega dela sistema

V ta namen smo razvili:

- avtonomno napravo za (samodejno ali ročno) obveščanje strežnika o alarmnih dogodkih in odziv na strežnikove ukaze (za krmiljenje določene naprave, npr. za odpiranje vrat itd.);
- strežnik, ki bo obdeloval podatke z odjemalcev in jih posredoval drugim napravam oziroma uporabnikom sistema Intervencije.net;
- komunikacijski protokol za komunikacijo med odjemalci in strežniki.

Omenjeni elementi so podrobneje opisani v nadaljevanju.

3 Protokol za prenos alarmnih sporočil

Ker zagotavlja zanesljiv prenos, smo protokol za prenos alarmnih sporočil osnovali na transportnem protokolu TCP. Slednjega smo nadgradili z lastnim aplikacijskim protokolom, ki smo ga poimenovali IntP (*Intervencije.net Protocol*). Protokol IntP nadgrajuje protokol TCP z mehanizmi za

- identifikacijo in overjanje odjemalca,
- šifriranje podatkov ter
- nadzor razpoložljivosti komunikacijske poti.

3.1 Identifikacija in overjanje odjemalca

IntP je povezavno naravnan protokol. Vzpostavitev povezave med odjemalcem in strežnikom je namenjena predvsem identifikaciji in overjanju odjemalca.

Prvi korak pri identifikaciji in overjanju odjemalca je preverjanje, če je odjemalčev IP-naslov na seznamu dovoljenih naslovov. Če odjemalčevega naslova ni na omenjenemu seznamu, strežnik odjemalca zavrne.

Identifikacija in overjanje odjemalca se nadaljujeta po različici postopka *izziv in odgovor* (ang. CHAP – Challenge and Response Protocol). Po vzpostavitvi povezave TCP, se odjemalec strežniku predstavi s sporočilom CHAP0, strežnik pa mu odgovori z naključnim besedilom v sporočilu CHAP1. Odjemalec nanj odgovori s sporočilom CHAP2 z izvlečkom prejetega besedila, ki ga ustvari z zgostitveno funkcijo SHA-1 z uporabo lastnega ključa. Strežnik prejeti izvleček primerja z lastno izračunanim izvlečkom. Če se izvlečka ujemata, pošlje odjemalcu sporočilo CHAP3 z vsebino 'OK', v nasprotnem primeru pa 'ERR, wrong HASH'. Ko je odjemalec overjen, strežniški protokolni osebek o tem obvesti svoj uporabniški proces.

3.2 Izmenjava uporabniških sporočil in šifriranje podatkov

Uspelemu overjanju sledi izmenjava podatkovnih sporočil DATA in ukaznih sporočil COMMAND. Obe vrsti sporočil sta sestavljeni iz

- glave, v kateri sta določeni vrsta sporočila ('DA|' za DATA in 'CM|' za COMMAND) in njegova zaporedna številka, ter
- vsebine, ki lahko vključuje
  - alarm, meritev ali ukaz za vklop ali izklop izhoda na odjemalcu pri sporočilih DATA in
  - ukaze za upravljanje strežnika in odjemalca v primeru sporočil COMMAND.

Vsebina obeh vrst sporočil je šifrirana s simetričnim šifrirnim postopkom AES (ang. Advanced Encryption Standard), ki je dovolj enostaven tudi za manj zmogljive mikrokrmilnike.

Obe vrsti sporočil zahtevata potrjevanje sprejema z uporabo pozitivnih potrditev ACK ali negativnih potrditev NACK. Obe potrditveni sporočili vsebujeta glavo ('AY|' oziroma 'AN|') in zaporedno številko sporočila, na katerega se nanašata.

Sporočilo ACK potrjuje, da je sprejemni osebek sporočilo uspešno dešifriral, razbral vsebino, jo obdelal in, na strežniški strani, predal svojemu uporabniškemu procesu. Sporočilo NACK po drugi strani pomeni zavrnitev prejetega sporočila zaradi napake pri enem izmed omenjenih procesov in posredno zahtevo za ponovno pošiljanje sporočila, na katerega se nanaša.

3.3 Nadzor nad komunikacijskim kanalom

Ker protokol TCP nima primernega mehanizma za nadzor razpoložljivosti komunikacijske poti, tega v protokolu IntP zagotavljamo s sporočilom HB (ang. HeartBeat, slov. srčni utrip). Sporočilo HB se lahko prenaša od strežnika k odjemalcu ali v nasprotni smeri. Uspešno prejeto sporočilo HB pomeni prehodno pot in v sprejemnem osebku povzroči ponastavitev časovnikov za preverjanje razpoložljivosti komunikacijske poti do svojega partnerja.

Sporočilo PING in odgovor PONG uporabljamo za ugotavljanje lastnosti prenosne poti in odzivnosti odjemalca oziroma strežnika. S pomočjo omenjenih sporočil lahko strežnik izračuna hitrost odziva posameznega odjemalca in temu primerno prilagaja časovnike za nadzor komunikacijske poti.

4 Odjemalec

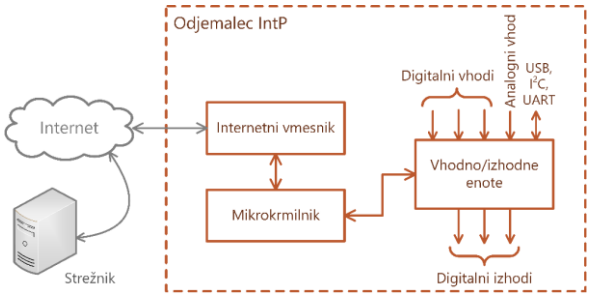
Odjemalec je naprava, ki zaznava izredne dogodke v svoji okolici in jih posreduje strežniku v skladu s protokolom IntP. Tipični dogodki, ki jih odjemalec zaznava, so:

- pritisk na gumb,
- sklenjene vhodne priključne sponke,
- izmerjena vrednost na analognem vhodu,
- podatki s komunikacijskih vodil (npr. I2C ali UART za komunikacijo z drugimi napravami in senzorji, na primer za zaznavanje temperature).

Poleg tega lahko odjemalec alarme in ukaze s strežnika tudi sprejema in nanje reagira. Podatki in ukazi, ki jih odjemalec prejme od strežnika, se lahko posredujejo na odjemalca priključenim napravam preko digitalnih izhodov ali komunikacijskih vodil.

Odjemalec je lahko bistveno preprostejši od strežnika, saj ga lahko izdelamo z uporabo cenovno ugodnega mikrokrmilnika (npr. ESP8266, ESP32 ali ATMEGA328) z dodanim omrežni vmesnikom in vhodno-izhodnimi enotami (Slika 3).

Tudi odjemalčev uporabniški vmesnik je lahko enostaven, saj mora vključevati le gumbe oziroma priključne sponke za proženje alarmov in LED-diode za prikaz stanja odjemalca.



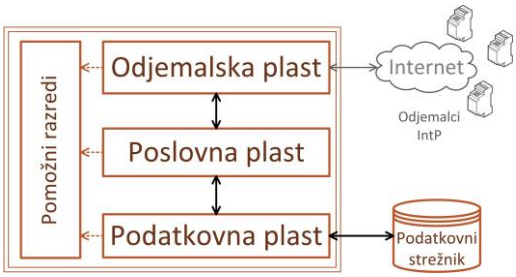
Slika 3. Shema odjemalca IntP

Slika 4. Odjemalec IntP

Na podlagi predstavljene zasnove smo izdelali odjemalca IntP (Slika 4), ki temelji na modulu WEMOS D1 mini [5]. Ta med drugim vključuje mikrokrmilnik ESP8266 z vgrajenim čipom za povezljivost z Wi-Fi omrežji in komunikacijo po protokolnem skladu TCP/IP, anteno WiFi, napetostni stabilizator, 11 vhodno-izhodnih povezav, analogno-digitalni pretvornik ter povezavo USB.

5 Strežnik

IntP strežnik je strežniški proces, ki komunicira z odjemalci: odziva se na njihove zahteve, obdeluje prejete podatke in jih posreduje drugim napravam oziroma komponentam sistema. Zaradi boljše preglednosti in preprostejšega vzdrževanja smo strežniški del izdelali v skladu s tri-nivojsko arhitekturo. Strežniški del tako sestavljajo odjemalska, poslovna in podatkovna plast (Slika 5).



Slika 5. Arhitektura strežnika IntP

Odjemalska plast predstavlja izvedbo protokola IntP na strežniku. Naloge plasti vključujejo

- komunikacijo z odjemalci z uporabo vseh mehanizmov, ki jih predvideva protokol IntP (razdelek 3),
- predajo sporočil iz odjemalcev poslovni plasti,
- sprejem sporočil s poslovne plasti in njihovo pošiljanje odjemalcem.

Poslovna plast je uporabnik protokola IntP, ki izvaja vsebinsko komunikacijo z odjemalci, obenem pa uporablja storitve podatkovne plasti. Naloge poslovne plasti vključujejo

- vodenje zbirke aktivnih odjemalcev,
- sprejem in potrditev sprejema sporočil z odjemalske plasti ter posredovanje prejetih sporočil podatkovni plasti,
- sprejem sporočil iz podatkovne plasti in njihovo posredovanje odjemalski plasti in
- odziv na izredne dogodke, kot je na primer neprehodna povezava do nekega odjemalca.

Naloga *podatkovne plasti* je zagotoviti poenostavljen in centraliziran dostop do podatkov, ki so zapisani v relacijski podatkovni zbirki sistema Intervencije.net.

Strežnik IntP temelji na Microsoftovih tehnologijah .Net Framework (aplikacijski del) in SQL Server (podatkovni del) in se izvaja kot storitev na operacijskem sistemu Windows.

6 Zaključek

Predstavljena nadgradnja sistema Intervencije.net je trenutno v postopku preizkušanja. Prvo fazo preizkusa smo opravili s tremi odjemalci IntP, ki so se povezovali z enim strežnikom. Namen preizkusa v tej fazi je bil predvsem odkrivanje in odpravljanje napak.

Trenutno poteka druga faza preizkušanja, namen katere je ugotoviti, če naprave zadoščajo potrebam uporabnikov, zato preizkusi potekajo v gasilskih domovih. V preizkuse je vključenih deset odjemalcev in dva strežnika.

Opravljenemu preizkušanju bo sledila vpeljava odjemalcev IntP v stvarna okolja. Najprej načrtujemo nameščanje naprav v gasilskih in zdravstvenih domovih, kasneje pa jih bomo ponudili tudi posameznim članom reševalnih služb za priključitev v njihovih stanovanjih in hišah.

Čeprav v okviru dosedanjega preizkušanja nismo odkrili večjih pomanjkljivosti, pa je odjemalce IntP in strežniški del sistema mogoče še izboljšati. Načrtovane so predvsem naslednje izboljšave:

- samodejno posodabljanje programske opreme v odjemalcih, kar je predpogoj za njihovo vpeljavo v stvarna okolja,
- dodajanje rezervnega komunikacijskega kanala, kot so sporočila SMS, če pride do prekinitve internetne povezave,
- izdelava grafičnega uporabniškega vmesnika za lažje upravljanje sistema Intervencije.net,
- vgradnja LED-prikazovalnika v napravo IntP namesto statusnih LED-diod, ki bo omogočal dodatne nastavitve naprave,
- uporaba zmogljivejšega mikrokrmilnika ESP32,
- povečanje števila relejskih izhodov in digitalnih vhodov,
- izdelava spletnega vmesnika, s pomočjo katerega bo lahko uporabnik sam upravljal določene nastavitve naprave.

Ostale funkcionalnosti bomo dodajali postopoma, glede na potrebe prihodnjih uporabnikov.

Literatura

[1] ETSC - Europan Transport Safety Council: New Pan-European Emergency Call System, sep. 2013, http://www.roadsafetyobservatory.com

[2] NEXES - NEXt generation Emergency Services, http://nexes.eu/

[3] Gen 6, 6 in Action – Smart communications solution in emergency situations, http://www.6inaction.net/

[4] Aldia, d.o.o.: Predstavitev sistema Intervencije.net., sep. 2015, https://www.intervencije.net

[5] WEMOS Electronics: D1 mini [WEMOS Electronics], https://wiki.wemos.cc/products:d1:d1_mini