

Varnostno nadzorni centri

Dušan Fefer

Povzetek:

Namen prispevka:

Varnostno-nadzorni center (VNC) je najobčutljivejši in najpomembnejši člen v sistemu tehničnega varovanja. Vanj se stekajo alarmna sporočila iz priklopljenih alarmnih sistemov, tu se jih obdela in shrani ter obvešča ustrezne intervencijske in varnostne službe. Zato je nujno potrebna njegova varnostna brezhibnost, tehnična dovršenost in ne nazadnje organizacijska učinkovitost.

Na pobudo SIST TC EAL je leta 2005 Institut za standardizacijo RS razglasil slovenski prevod BS 5979:2000 za slovenski standard. V tem standardu so priporočila za načrtovanje, izgradnjo in opremo kadrovske zasedenih in nezasedenih VNC-jev, kot tudi za delovanje centrov za sprejem alarma v povezavi s protivlomnimi in protipožarnimi sistemi, video nadzorom, socialnih alarmov, alarmnimi sistemi za varovanje oseb ter ostalimi nadzornimi službami.

VNC so razdeljeni glede na tip alarmnega signala. Iz tega pa sledi namembnost zgradbe, komunikacij, opreme, delovanja in informacij. Postavitev kvalitetnega VNC se začne že pri njegovem načrtovanju. Kot so različni tipi stavb za VNC-je, tako tudi ni mogoče določiti vseh potencialnih rešitev. Zatorej so priporočila poklicnega kodeksa le okvirna.

Zakon o zasebnem varovanju, ki je stopil v veljavo v letu 2004 oz. 2007 [21], uvaja, da so slovenski standardi obvezni v sistemih varovanja, torej tudi standardi, ki urejajo problematiko VNC-jev. Upravljanje z VNC-jem (2. člen tega zakona) je upravljanje in stalen fizičen nadzor nad vgrajenimi tehničnimi sistemi in napravami za varovanje premoženja, območja ali varovane osebe, in nadzor s telekomunikacijskimi potmi prenosa alarmnih signalov, ki se opravlja v VNC-ju.

Metodologija:

Sklep Strokovnega odbora za standarde z dne 26.10.2006: ZRSZV bo v sodelovanju s Fakulteto za elektrotehniko, Univerze v Ljubljani opravila strokovni nadzor pri vseh imetnikih licence za upravljanje z VNC, v skladu z veljavnim standardom SIST BS 5979:2005.

Ugotovitve:

V Sloveniji je bilo 31.3.2008 sedemnajst VNC-jev, ki so pridobili, oziroma so v postopku pridobitve licence za upravljanje z varnostno nadzornim centrom. Pri revizijskem pregledu centrov smo ugotovili, da dvanajst VNC-jev izpolnjuje vse bistvene zahteve SIST BS5979:2005. Tu in tam so sicer obstojajo manjša odstopanja od zahtev standarda, ki pa niso bistvena za delovanje VNC-ja. Pet VNC-jev pa nimajo rezervnega »backup« centra, torej ne izpolnjujejo 8.4 člena standarda SIST BS 5979:2005.

Izvirnost/pomembnost prispevka:

Dvig kvalitete zasebnega varovanja v Sloveniji in s tem dvig ugleda in zaupanja te panoge. Korekcijski ukrepi, ki sledijo vsaki presoji in reviziji, pa skrbijo za izpopolnjevanje sistema kakovosti.

Ključne besede: Tehnično varovanje, varnostno nadzorni centri, standardi.

1 UVOD

Človek je že v samem začetku svojega obstoja oblikoval potrebo po varovanju samega sebe in svoje lastnine. Potreba po varovanju se je večala z razvojem družbe, ki je v skladu z izboljšano kakovostjo življenja pogojevala tudi rast stopnje kriminala.

V zadnjih letih je pomemben delež k področju varovanja prispeval tehnološki razvoj, predvsem razvoj na področjih elektrotehnike ter računalništva. Mikroprocesorska tehnologija je imela za posledico miniaturizacijo sistemov varovanja, njihovo programabilnost, predvsem pa hitrejšo odzivnost ob nastopu dogodkov na varovanih področjih, kar omogoča še hitrejše in pravočasno ukrepanje. Prav tako se, zahvaljujoč hitremu razvoju telekomunikacij, množijo oblike prenašanja alarmnih sporočil preko različnih medijev, kar povečuje uporabnost in prilagodljivost sistemov varovanja.

Namen varovanja je zavarovati in obvarovati premoženje pred odtujitvijo ter varovano območje pred nedovoljenimi vstopi in posegi. Iz namena samega izhaja dejstvo, da je za zagotovitev kvalitetnega varovanja potrebno skrbno in strokovno načrtovanje ter pravilna izbira tehničnih sredstev. To od samega začetka izbire oblike varovanja vključuje tudi dobro projektiranje. Določiti je potrebno stopnjo ogroženosti človeških življenj ter materialnih dobrin, verjetna mesta za morebitne poskuse nepooblaščenih vstopov v objekt, pravilne lokacije javljalnikov ter podobno (Fefer, 2006) [3]. Učinkovitost varovanja je odvisna tudi od hitrega odziva dežurne intervencijske ter servisne službe.

Varovanje za naročnika ne predstavlja samo stroška, temveč tudi dobro ekonomsko potezo. Stroški investicije za tehnično varovanje so namreč precej nižji kot stroški zaposlenih oseb (varnostnikov) ter stroški morebitne škode ob vlomu, kraji, požaru, eksploziji, izlivu strupenih tekočin ter podobnem.

Pomembna je tudi kakovost vgrajenih tehničnih sredstev v sistem varovanja, saj je tako že na začetku zmanjšana verjetnost lažnih alarmov, ki so nezaželeni prav tako pri naročnikih kot pri dežurnih intervencijskih službah, saj po nepotrebnem povečujejo stroške varovanja.

Danes se področje varovanja deli na tri glavna področja:

- fizično varovanje,
- tehnično varovanje, ter
- fizično-tehnično varovanje kot kombinacija obeh.

Sistemi tehničnega varovanja so z uporabo tehničnih sredstev upravičili osnovne razloge in potrebe po varovanju. Tehnična sredstva uporabljamo kot pripomoček varnostnemu osebju, da se zmanjša odvisnost od človeškega faktorja. Varnostno osebje ima pri nadzoru ob sebi zanesljiv sistem, ki ga pravočasno opozarja na različne situacije na varovanih objektih, ob katerih je potrebno ustrezno ukrepati. Pri varovanju večjih kompleksov je število varnostnega osebja manjše, ti pa imajo zato boljši pregled nad stanjem varovanega objekta iz nadzornega centra. S tem se zmanjša ali popolnoma odpravi število obhodov po objektu, reakcije varnostnega osebja ob alarmnih stanjih pa so zato hitrejše. Pomembna razloga za uporabo tehničnih sredstev v sistemih tehničnega varovanja sta tudi preventivno odvrčanje in oteževanje oziroma onemogočanje dostopa morebitnim storilcem do varovanih področij (Fefer, 2004) [2] in [12], [13], [14]. Sistemi tehničnega varovanja zaradi svoje kompleksnosti zahtevajo usposobljeno varnostno osebje, ker je sicer še tako dobra tehnika v rokah neusposobljenega osebja nekoristna.

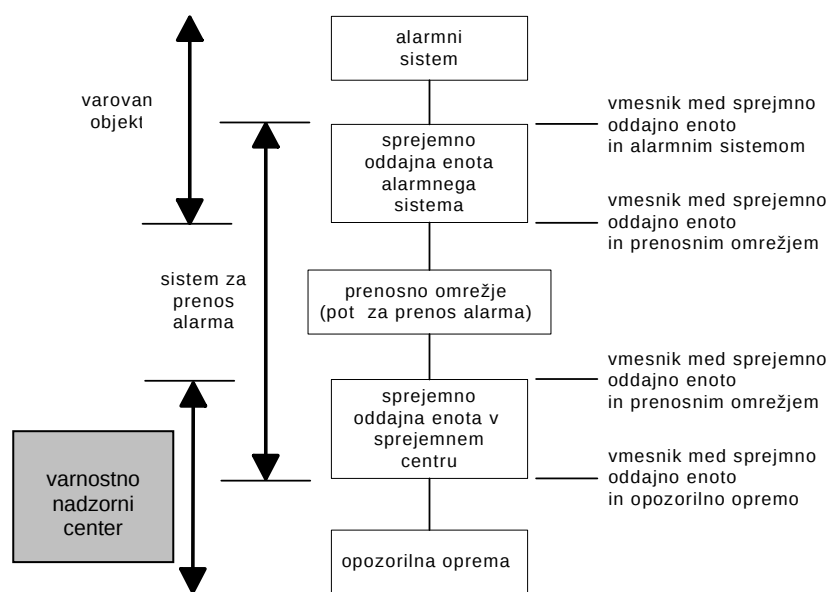
Sistem tehničnega varovanja, ki alarmna sporočila prenaša na daljavo do varnostno nadzornega centra, razdelimo na tri tehnično ločene segmente:

- alarmni sistem varovanega objekta,
- sistem za prenos alarma, ter

- alarmni sprejemni center.

Učinkovit sistem tehničnega varovanja s tremi ločenimi segmenti prikazuje slika 1.

Glavna naloga alarmnega sistema je signaliziranje stanja sistema, ki se lahko vrši lokalno ali pa na daljavo do varnostno nadzornega centra. Pri signalizaciji na daljavo alarmni sistem oddaja alarmna sporočila sistemu za prenos alarma, ki poskrbi za njihov prenos do varnostno nadzornega centra. Vsa sporočila o dogodkih se shranjujejo v notranjem pomnilniku, ki ima vlogo notranjega arhiva alarmne centrale. Zunanji arhiv centrale lahko predstavlja priključen tiskalnik, ki tekoče izpisuje sporočila o vseh dogodkih.

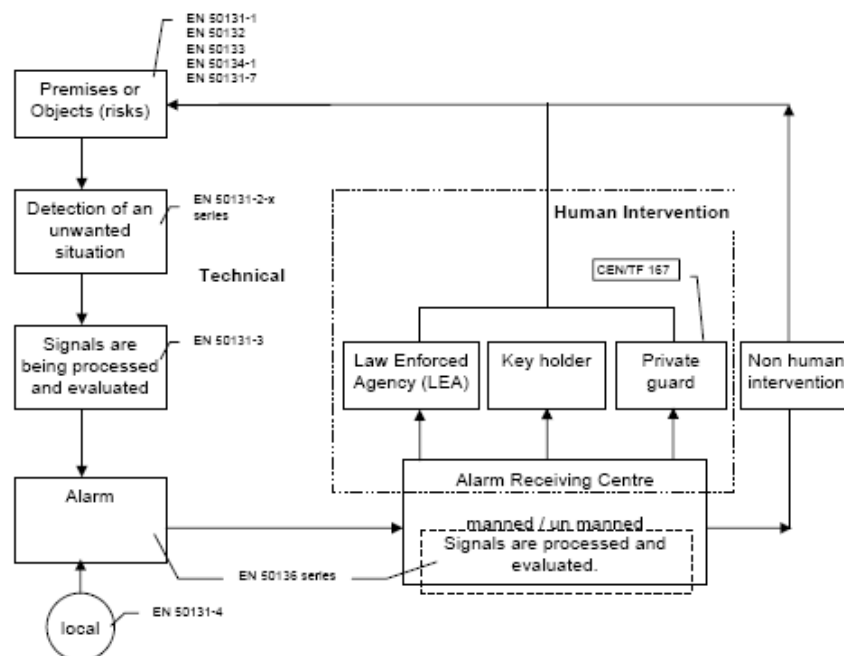


Slika 1: Sistem tehničnega varovanja.

Sistem za prenos alarma (Fefer, 2004) [1] opravlja funkcijo prenosa alarmnih sporočil do oddaljenega varnostno nadzornega centra. Zahteve podaja serija standardov SIST EN 50136 [19], [10], [11]. Pomembni faktorji, ki vplivajo na hitrost prenosa so: hitrost prenosa sistema za prenos alarma, zaščita alarmnih sporočil po prenosnih poteh ter korekcija napak pri prenosu. Podsestav alarmnega prenosnega sistema je prenosno omrežje po katerem se prenašajo alarmna sporočila. Najbolj razširjeno prenosno omrežje je javno telefonsko omrežje, ki nudi več različnih možnosti prenosa.

Varnostno nadzorni center VNC je informacijsko središče sistema tehničnega varovanja. Sprejema alarmna sporočila z vseh objektov in jih v informacijskem smislu obdeluje, prikazuje in arhivira. Osebe v VNC sprejema vse pomembne odločitve v zvezi s prispelimi alarmnimi sporočili, ter o tem obvešča ustrezne intervencijske in dežurne službe za nadaljnje ukrepanje, odgovorne osebe na varovanih objektih in podobno. Na sliki 2 vidimo blok shemo VNC-ja, ki jo določa oSIST prEN 50518-1:2008 [5]. Danes funkcija alarmnih sistemov ni le sprožitev alarma ob ustreznem dogodku na objektu, ampak tudi zaznava vseh ostalih, na videz manj pomembnih dogodkov, kot so npr. vklopi in izklopi alarmnega sistema, različne napake ter ostali dogodki, ki tvorijo celotno podobo o dogajanju na varovanem objektu. Alarmno sporočilo o dogodku bi se moralo kar najhitreje prenesti do VNC [9], ki naj prevzame funkcijo ustreznega ukrepanja. Pomembno je, da so alarmna sporočila ob sprejemu enaka oddanim, da

se ohranja istovetnost sprejetega sporočila z dogodkom na varovanem objektu. Vlogo kvalitetnega prenosa sporočil opravlja prenosni alarmni sistem, fizično izvedbo prenosa pa opravlja prenosno omrežje. V celotni funkciji varovanja ima pomembno vlogo odzivnost sistema tehničnega varovanja, ki mora biti čim hitrejša, da lahko dosežemo osnovni cilj - čim krajši intervencijski čas posredovanja ob dogodku na objektu.



Slika 2: Blok shema VNC-ja, ki jo določa oSIST prEN 50518-1:2008.

2 OPRAVILA VARNOSTNO NADZORNEGA CENTRA

Danes je za zagotavljanje kvalitetnih varnostnih storitev treba zagotoviti hitro odzivnost celotne strukture sistema varovanja, ki se zrcali v hitrem in uspešnem posredovanju intervencijskih skupin na objektih. Tukaj ima najpomembnejšo vlogo VNC [4], ki je informacijsko, komunikacijsko ter operativno središče operativnega dogajanja za sisteme tehničnega varovanja. Alarmni sprejemni center opravlja različne sklope nalog od katerih so najpomembnejše:

- Sprejem, informacijska obdelava, prikaz in arhiviranje prispelih alarmnih sporočil z varovanih objektov in s tem zagotavljanje stalnega nadzora nad varovanimi objekti;
- Sistematičen nadzor nad vsemi prispelimi alarmnimi sporočili;
- Operativno vodenje intervencijskih ekip na terenu;
- Nadzor gibanja posebnih ekip za varovan prevoz denarja ali drugih dragocenosti;
- Obveščanje in koordinacija operativnih ukrepov z drugimi varnostnimi podjetji in državnimi organi (policija, gasilci ter različne reševalne službe);
- Zagotavljanje stalnega informiranja naročnikov varnostnih storitev v smislu organizacijske enote, ki se v varnostnem podjetju prva odziva na želje, zahteve in potrebe uporabnikov varnostnih storitev;
- Kot ključni element nadzornega sistema varnostnega podjetja pomagajo razreševati vse varnostne probleme varnostnikom, ki opravljajo različne oblike fizičnega varovanja na varovanih objektih ali serviserjem, ki opravljajo montažo alarmne tehnike na terenu.

3 STROJNA IN PROGRAMSKA OPREMA

V VNC je montirana strojna in programska oprema. *Strojno opremo* sestavljajo sprejemnik signalov, ki sprejema alarmna sporočila preko prenosnega omrežja, vsa računalniška oprema za sprejem, obdelavo, prikaz in arhiviranje prispelih alarmnih sporočil, svetlobni in zvočni indikatorji ob sprejemu alarmnih sporočil, pomožni viri napajanja, razdelilna telefonska omarica in podobno.

Programsko opremo sestavljajo vse računalniške aplikacije, ki so v teku ter zagotavljajo operativno, komunikacijsko in informacijsko funkcijo alarmnega sprejemnega centra. Programska oprema nam omogoča selektivnost nad sprejetimi alarmnimi sporočili, njihovo dodatno obdelavo, bolj pregledne prikaze sporočil ter dodatne možnosti arhiviranja na različne pomnilniške medije.

3.1 Opozorilna oprema

Opravi alarmnega sprejemnega centra opisujejo slovenski standardi serije SIST EN 50131 [6], [7], [8], [15] ter SIST BS 5979:2005 [4]. Standarda podajata splošne zahteve za opozorilno opremo ter zahteve za zagotavljanje integritete celotnega sistema alarmnega sprejemnega centra.

Oprema v alarmnem sprejemnem centru bi morala biti načrtovana tako, da ne bi prihajalo do izgube alarmnih sporočil v primeru:

- Prezasedenosti alarmnega sprejemnega centra;
- Aktivnosti, ki niso alarmnega značaja (arhiviranje in druga administracijska opravila);
- Posameznih ali predvidljivih napak opozorilne opreme;
- Posameznih oziroma predvidljivih napak ostale opreme (npr. tiskalnikov).

Pri sprejemu alarmnih sporočil je najpomembnejši gradnik alarmnega sprejemnega centra sprejemnik, ki sprejema alarmna sporočila preko sistema za prenos alarma. V praksi je najpogostejši digitalni sprejemnik, ki sprejema alarmna sporočila preko javnega telefonskega omrežja. Nanj je lahko preko linijskih vmesnikov priključenih več telefonskih linij istočasno, kar je pomembno pri ureditvi prometa ter onemogoča prezasedenost ene izmed linij.

Standard definira sprejem alarmnih sporočil, kjer alarmna sporočila deli na več podtipov, in sicer na:

- *Sporočila o alarmih*, ki bi morala biti najavljena operaterju najkasneje v treh sekundah po sprejemu s pomočjo opozorilne opreme. Najava naj bo izvedena s slikovnim prikazom vsebine alarma in z zvočnim opozorilnim signalom;
- *Nujna sporočila*, so vsa ostala sporočila, ki zahtevajo pozornost dežurnega osebja alarmnega sprejemnega centra in ustrezno ukrepanje;
- *Pričakovana sporočila*, so sporočila, ki so vnaprej predvidena za sprejem v določenem časovnem obdobju. Ne potrebujejo pozornosti dežurnega osebja v alarmnem sprejemnem centru, temveč so lahko avtomatsko potrjena ob sprejemu in dodatno obdelana. Zahtevana je časovna evidenca sprejema sporočil. Kadar se pričakovano sporočilo pojavi izven predvidenega časovnega obdobja, bi se moralo obdelati kot nujno sporočilo in v 10 sekundah bi moralo biti prikazano nadzornemu osebju alarmnega sprejemnega centra.

Oprema za zvočno opozarjanje bi morala imeti jakost zvočnega signala, ki ne bi smel presehati 60 dBA, izmerjenih na razdalji enega metra od opozorilne opreme.

3.2 Obdelava sprejetih alarmnih sporočil

Obdelava sprejetih alarmnih sporočil, ki jo določa serija standardov SIST EN50136, je sestavljena iz več zaporednih postopkov, od katerih so najpomembnejši:

- Tvorba vhodne čakalne vrste sprejetih alarmnih sporočil, ki čakajo na obdelavo;
- Beleženje prispelega alarmnega sporočila;
- Nivoji dostopa in avtorizacijske kode ;
- Dodaten vnos podatkov ob obdelavi (dodatna obdelava).

Dodeljevanje prioritet lahko temelji na:

- Identiteti alarmnega sistema varovanega objekta;
- Tipu alarma;
- Tipu sprejetega alarmnega sporočila, ki ni alarm.

3.3 Prikaz informacij alarmnih sporočil

Prikazane informacije o sprejetem alarmnem sporočilu bi morale vsebovati:

- Identifikacijo objekta s katerega prihaja sprejeto alarmno sporočilo;
- Identifikacijo vhoda v sistem za prenos alarmov na strani varovanega objekta, kadar ima sistem za prenos alarma več vhodov;
- Tip alarmnega sporočila, kadar je na voljo več različnih sporočil;
- Datum in čas sprejema alarmnega sporočila v alarmnem sprejemnem centru (s točnostjo ene minute), ter
- Možnost prikaza datuma, časa oziroma zaporedja sporočila, kadar so le ti vsebovani v sprejetem alarmnem sporočilu. Če prikaz ni avtomatski, bi moral operater imeti možnost izbire za prikaz.

Kadar z varovanega objekta prispe več enakih sporočil, alarmni sprejemni center pa omogoča vhodno čakalno vrsto, bi to moralo biti razvidno ob prikazu v VNC.

Standard podaja zahteve za vidljivost prikazanih informacij. Informacija bi morala biti jasno vidna v oddaljenosti 1m od zaslona gledano v smeri normale zaslona. Zorni kot pogleda na zaslon se lahko spreminja do 30 kotnih stopinj v obeh vertikalnih smereh, ter do 60 kotnih stopinj v obeh horizontalnih smereh, glede na normalo zaslona.

3.4 Arhiviranje

Vsa sprejeta alarmna sporočila v alarmnem sprejemnem centru, vključno s sporočili sistema za prenos alarma, bi morala biti zabeležena kar najhitreje po sprejemu. Sporočila bi morala biti zabeležena v izvirno evidenco sporočil, ki bi morala ustrezati zahtevam, ki jih bomo podali v nadaljevanju. Alarmna sporočila se lahko poleg izvirne evidence beležijo v eni ali več sekundarnih evidenc, če so le te omogočene, ker je iz takih evidenc omogočen selektivni dostop do vseh sprejetih sporočil. Primer take evidence v praksi je lahko postavitve ene evidence za posamezni alarmni sistem varovanega objekta.

Evidenca sprejetih sporočil se lahko vodi s pomočjo tiskalniških izpisov ali programskih zapisov v datotečnem sistemu računalniškega sistema.

Za evidenco sporočil so podane naslednje zahteve, ki jih podaja standard:

- Mehanizem evidentiranja (tiskalnik, arhivi, ...);
- Integriteta evidence sporočil (vsakemu sporočilu mora biti prirejena zaporedna številka, čas in datum);
- Opozorilna oprema bi morala imeti vmesni pomnilnik za alarmna sporočila;
- Napaka mehanizma beleženja (izpad tiskalnika, odstranitev diskov, ...);
- Preklic vnosa v evidenco;

- Onemogočanje izpisovanja evidence;

3.5 Ostale funkcije delovanja opozorilne opreme

Evropski standardi v nadaljevanju navajajo še nekaj funkcij delovanja opozorilne opreme [16], [17], [18], [19], od katerih so najpomembnejše:

- Testiranje priključenih alarmnih sistemov (možnost testiranja za priključene alarmne sisteme različnih objektov);
- Nivoji dostopa in avtorizacijske kode (prijava v sistem se vrši s pomočjo uporabniškega imena in gesla);
- Vnos podatkov (ime objekta, naslov, ime odgovorne osebe, ...);
- Nadzor alarmnih vhodov (vsi vhodi, ki sprejemajo alarmna sporočila, morajo biti nadzorovani);
- Arhiviranje podatkov;
- Zahteve za napajanje (potrebno je zagotoviti neprekinjeno napajanje);
- Ostale funkcije sistema (opozorilna oprema lahko vsebuje tudi daljinski nadzor objektov, popravil, ...);
- Razdelitev opozorilne opreme sistemov na več delov (v alarmnem centru je onemogočeno obdelovanje dveh enakih sporočil hkrati s strani dveh operatorjev);
- Priprava programske opreme;
- Za opozorilno opremo, ki je nadzorovana s programi, ki so del programske opreme v alarmnem sprejemnem centru, bi morali biti za zagotavljanje zanesljivosti sistema izvedeni naslednji postopki:
 - o Programi oziroma programska oprema bi morala imeti modularno zgradbo;
 - o Vmesniki za točno in avtomatsko pripravo vhodnih podatkov in operacij bi morali biti pripravljeni, tako da ne bi povzročali nepredvidljivih programskih operacij v primeru nepričakovanih oziroma napačnih vhodnih podatkov ali operacij, ter
 - o Vsi procesi, ki izvajajo prekinitvene procese med procesiranjem, bi morali biti pripravljeni tako, da izključujejo možnost mrtvega teka aplikacij (angl. deadlock).

3.6 Dokumentacija programske opreme

Za vso programsko opremo opozorilne opreme v alarmnem sprejemnem centru je potrebna dokumentacija. Proizvajalčeva dokumentacija programske opreme bi morala obsegati naslednje:

- Funkcionalen opis osnovnega programskega teka;
- Podrobnosti komunikacije med posameznimi programskimi moduli;
- Opis prekinitvenih procesov, ki omogočajo razpoznavo osnovne hierarhije v programu; opis je lahko podan grafično;
- Pregleden prikaz zasedenosti spominskega medija ter logičnih naslovov vhodno izhodnih naprav, ter

podrobnosti o vsakem programskem modulu, ki bi morale vsebovati:

- Ime programskega modula;
- Ime avtorja in ostalo identifikacijo;
- Datum izdelave in številko verzije;
- Razumljiv prikaz vseh funkcij, ki nastopajo v modulu;
- Razlago vmesnikov pri povezavi z ostalimi moduli, vključno s tipi prenosov podatkov, pravih območij vrednosti podatkov in potrjevanja pravilnosti sprejema podatkov, ter

- Izvirni kodni zapis programa, z evidenco vseh lokalnih in globalnih spremenljivk, konstant ter drugih podatkov z uporabo obširnih komentarjev, ki omogočajo enostavno sledenje teka programa.

4 ORGANIZACIJSKI PREDPIS ZA ALARMNI CENTER

Alarmni center je najobčutljivejši in najpomembnejši člen v sistemu tehničnega varovanja. Torej je nujno potrebno, da ima alarmni center svoj organizacijski predpis, v katerem so opisani elementi sistema kakovosti po zahtevah standardov serije ISO 9000, tehnične zahteve pa določajo SIST BS 5979:2005 [4] ter serija standardov SIST EN 50136 [9], [10], [11].

Organizacijski predpis za alarmni center naj bi obsegal naslednja poglavja in podpoglavja:

- Politika kakovosti (izjava o politiki kakovosti, odobritve in potrditve);
- Sistem kakovosti (cilji in oblika sistema kakovosti, organizacijski predpis, vodenje kakovosti, dokumentacija, hišni red);
- Organizacija in vodenje (organizacija, organizacijski diagram, vodenje - vodilno osebje, administrativni postopki, osebje - kvalifikacije in šolanje);
- Presoja in revizija sistema kakovosti (namen, odgovornost, izvajanje: splošna ureditev, načrtovanje in dokumentiranje, sistemi nadzora kakovosti);
- Načrtovanje in izgradnja alarmnega centra (načrtovanje: alarmni center je načrtovan in zgrajen glede na SIST BS 5979:2005) [4], [5];
- Sporazumi so sklenjeni s telekomunikacijskim operaterjem, posameznimi intervencijskimi službami, vzdrževalci, zavarovalnicami;
- Oprema alarmnega centra (oprema za nadzor alarmnega centra, alarmni sistemi za varovanje alarmnega centra, komunikacije, električno napajanje, varnostna oprema, snemalna oprema, oprema za osebje, oprema za nadzor na alarmni center priključenih alarmnih sistemov, zapisi o opremi);
- Delovanje alarmnega centra (dostopi, delovni postopki, veljavnost sistema);
- Minimalni pogoji za priklop na alarmni center (vlomni alarmni sistemi, požarni alarmni sistemi, alarmni sistemi za detekcijo eksplozivnih snovi, alarmni sistemi za varovanje oseb).

Dodatek (izjava tehničnega vodje alarmnega centra, izjava vodje za kakovost alarmnih centrov, izjava člana osebja alarmnega centra, referenčni dokumenti:

- Delovno navodilo za priklop novega objekta/naročnika na alarmni center;
- Delovno navodilo za zagotavljanje veljavnosti alarmnega centra;
- Delovno navodilo za vstop in izstop;
- Delovno navodilo za preverjanje zaposlenega osebja;
- Delovno navodilo o vklopnih in izklopnih časih;
- Delovno navodilo za sprejem napake med prenosom;
- Delovno navodilo za sprejem alarmnega signala;
- Delovno navodilo za ravnanje ob katastrofalnih dogodkih.

Usklajevanje organizacijskega predpisa s posameznimi standardi je zapleten in dolgotrajen postopek, ki lahko traja tudi več let. Pomanjkljivosti se ponavadi pokažejo šele z uporabo predpisa v praksi, njihovo odkritje pa omogočajo predvsem presoje in revizije sistema kakovosti. Korekcijski ukrepi, ki sledijo skoraj vsaki presoji in reviziji, pa skrbijo za izpopolnjevanje sistema kakovosti, zato lahko rečemo, da se izdelava organizacijskega predpisa in pripadajočih dokumentov praktično nikoli ne konča.

5 ZAKLJUČEK

Alarmni center je najobčutljivejši in najpomembnejši člen v sistemu tehničnega varovanja. Vanj se stekajo alarmna sporočila iz priklopljenih alarmnih sistemov, tu se jih obdela in shrani ter obvešča ustrezne intervencijske in varnostne službe. Postavitev kvalitetnega alarmnega centra se začne pri njegovem načrtovanju. To pomeni, da ga naj ne bi namestili v pritličju, kjer je zelo izpostavljen direktnemu napadu s ceste, ali na lokaciji, kjer je obstaja velika verjetnost, da lahko pride do požara, poplav ali česa podobnega. Zagotoviti je treba dovolj velike delovne prostore, vhodni medprostor, ustrezno ventilacijo in razsvetljavo, sanitarije, Posebno pozornost je v fazi načrtovanja treba nameniti tudi mehanski zaščiti alarmnega centra, kot so neprebojna stekla, robustna vrata in stene, zaščita oskrbovalnih in komunikacijskih vodov, ventilacijskih odprtín, tako da je alarmni center popolnoma odporen na napad in požarno odporen vsaj eno uro.

Naslednja faza pri postavitvi alarmnega centra je izvedba tehničnega varovanja le-tega. Namestiti je treba vlomni alarmni sistem [7], [4], [15], požarni alarmni sistem [20], sistem za detekcijo eksplozivnih snovi in video nadzorni sistem [12], [13]. Alarmni signali, sproženi v primeru napada na alarmni center ali v primeru požara v njem, morajo biti prikazani znotraj alarmnega centra ter istočasno poslani drugemu alarmnemu centru ali ustrezni varnostni službi (policija, gasilci, reševalci, ...).

Z vidika električnega napajanja je alarmni center lahko popolnoma samostojna enota. Če pride do izpada električne energije, se mora alarmni center avtomatsko prekloniti na ustrezni alternativni vir električne energije, kot je npr. generator, in to tako, da preklon ne povzroči nobene motnje v delovanju opreme. Zagotavljati mora vsaj 24 urno neprekinjeno delovanje alarmnega centra.

Sistem komunikacij alarmnega centra s priključenimi alarmnimi sistemi, intervencijskimi in varnostnimi službami ter drugimi alarmnimi centri je zelo pomemben in zato vreden premišljenega načrtovanja [5], [9], [10], [11]. Vstopno komunikacijo predstavlja več telefonskih linij, namenjenih izključno za sprejem alarmnih signalov iz priključenih alarmnih sistemov ali satelitov. Za izstopno zvočno komunikacijo morata biti na voljo vsaj dve telefonski liniji, ki sta namenjeni samo alarmnim komunikacijam in zaprti za vstopne klice. S kontrolno sobo ustrezne intervencijske ali varnostne službe morata obstajati dva neodvisna načina komunikacije. Enega od njiju lahko predstavlja radijska zveza, radijske komunikacijske antene pa morajo biti znotraj lupine, sicer pa podvojene in/ali nedostopne in/ali zavarovane pred fizičnim napadom.

Vse telefonske komunikacije, usmerjene v in iz alarmnega centra morajo biti dokumentirane skupaj s časom in datumom njihovega nastanka, shranjene pa morajo biti vsaj 3 mesece in zmožne ponovnega predvajanja [4], [5]. Vse podatkovne komunikacije, usmerjene v in iz alarmnega centra, katere se tičejo nadzorovanih dogodkov, morajo biti dokumentirane skupaj s časom in datumom njihovega nastanka, shranjene pa morajo biti vsaj 3 mesece z možnostjo izpisa in/ali ponovnega prikaza. To omogoča instalirana računalniška strojna in programska oprema, ki je zanesljiva in enostavna za upravljanje.

Strojno opremo sestavljajo digitalni sprejemniki alarmnih signalov, ki sprejemajo alarmna sporočila preko prenosnega omrežja, vsa računalniška oprema za sprejem, obdelavo, prikaz in arhiviranje prispelih alarmnih sporočil, svetlobni in zvočni indikatorji sprejema alarmnih sporočil, telefoni, oprema za radijsko komunikacijo, alternativni viri napajanja, Programsko opremo pa tvorijo vse računalniške aplikacije, katere skrbijo za operativno, komunikacijsko in informacijsko funkcijo alarmnega centra.

Za nemoteno delovanje alarmnega centra morajo biti v delovnih navodilih točno definirani vsi delovni postopki. Vsa delovna navodila pa morajo biti v vsakem trenutku dostopna delovnemu osebju. Vsi podatki o stranki in dodatni sporazumi z njo morajo biti operaterju

enostavno dostopni. Vpeljana morata biti sistem presoj kakovosti alarmnega centra in izpeljava korekcijskih ukrepov.

Delovno osebje mora biti preverjeno in usposobljeno za opravljanje zahtevanih delovnih nalog. V alarmnem centru morata biti stalno prisotni vsaj dve osebi, sposobni izvajanja vseh delovnih postopkov, skupaj z vsaj še enim operaterjem, ki mora biti prav tako stalno prisoten na svojem delovnem mestu. Drugače pa mora biti število stalno prisotnih oseb v skladu z zagotavljanjem predpisanega odzivnega časa.

Vse, do sedaj rečeno, o alarmnem centru, je samo grob oris le-tega. Za točno predstavo o zahtevah in pogojih, katere mora izpolnjevati kvaliteten alarmni center, pa se je treba nasloniti na veljavne standarde, kot je npr. Serija standardov SIST EN 50136, SIST BS 5979: 2005 in serija standardov ISO 9000.

6 LITERATURA

- [1] FEFER, Dušan. Sistem za prenos alarma. V: *Projektiranje javljanja in alarmiranja požara : enodnevni seminar, 19. januar 2004*. [S.l.: s.n.], 2004, str. 114-122. [COBISS.SI-ID [4061780](#)].
- [2] FEFER, Dušan. Uporaba biometričnih tehnologij v sistemih pristopne kontrole. *Varstvoslovje*, jun. 2004, letn. 6, št. 2, str. 148-156, tabele, graf. prikazi. [COBISS.SI-ID [895722](#)].
- [3] FEFER, Dušan. *Osnove sistemov tehničnega varovanja*. Ljubljana: Zbornica Republike Slovenije za zasebno varovanje, 2006. 51 f., ilustr. [COBISS.SI-ID [5190996](#)].
- [4] SIST BS 5979:2005: Pravila ravnanja za sprejemne centre pri sprejemu signalov iz varnostnih sistemov (vključuje popravek št. 1).
- [5] oSIST prEN 50518-1:2008: Nadzorni in sprejemni centri za alarme - 1. del: Zahteve za lokacijo in konstrukcijo.
- [6] kSIST-TS CLC/FprTS 50131-7:2008: Alarmni sistemi - Sistemi za javljanje vloma - 7. del: Navodila za uporabo.
- [7] SIST EN 50131-1:2007: Alarmni sistemi - Sistemi za javljanje vloma in ropa - 1. del: Systemske zahteve.
- [8] SIST EN 50131-1:2006/kFprISA:2008: Alarmni sistemi - Sistemi za javljanje vloma in ropa - 1. del: Systemske zahteve.
- [9] oSIST prEN 50136-1:2008: Alarmni sistemi - Sistemi in oprema za prenos alarma - 1. del: Splošne zahteve za sisteme za prenos alarmov.
- [10] SIST EN 50136-1-1:1999/kprA2:2006: Alarmni sistemi - Sistemi in oprema za prenos alarma - 1-1. del: Splošne zahteve za sisteme za prenos alarmov.
- [11] SIST EN 50136-2-4: 1999, Alarm systems - Alarm transmission systems and equipment, Part 4: Annunciation equipment used in alarm receiving centres.
- [12] SIST EN 50132-5:2001: Alarm systems - CCTV surveillance systems for use in security applications - Part 5: Video transmission.
- [13] oSIST prEN 50132-1:2008: Alarmni sistemi - Nadzorni sistemi CCTV za uporabo v aplikacijah varovanja - 1. del: Systemske zahteve.
- [14] SIST EN 50133-7:2000: Alarm systems - Access control systems for use in security applications - Part 7: Application guidelines.
- [15] kSIST prEN 50131-2-X:2007: Alarmni sistemi - Sistemi za javljanje vloma in ropa - 2-X. del: Zahteve za javljalnike.
- [16] SIST-TS CLC/TS 50131-3:2004: Alarm systems - Intrusion systems -- Part 3: Control and indicating equipment.
- [17] SIST-TS CLC/TS 50131-4:2007: Alarmni sistemi - Sistemi za javljanje vloma - 4. del: Opozorilne naprave.

- [18] SIST-TS CLC/TS 50131-7:2004: Alarm systems - Intrusion systems -- Part 7: Application guidelines.
- [19] SIST EN 50134-7:1997: Alarmni sistemi - Socialni alarmni sistemi - 7.del: Navodila za uporabo.
- [20] SIST EN 54 - 1: Fire detection and fire alarm systems - Part 1: Introduction.
- [21] Zakona o zasebnem varovanju (Uradni list RS, št. 126/03, 16/07 - odločba US in 102/07).

O avtorju:

Dušan Fefer je diplomiral leta 1975 in se 1976 zaposlil kot asistent na Fakulteti za elektrotehniko, Univerze v Ljubljani, kjer je leta 1983 magistriral in 1986 doktoriral. Leta 1996 je bil izvoljen v naziv rednega profesorja. Njegovo pedagoško in raziskovalno delo pokriva področja merilnih sistemov, senzorjev, AC/DC napetostnih referenčnih virov, akustike, magnetike, tehničnega varovanja in vplivov elektromagnetnih polj na biološke sisteme. [/dusan.fefer@fe.uni-lj.si/](mailto:dusan.fefer@fe.uni-lj.si/)