CIVITAS, 2017, 7(1), 65-78
www.civitas.rs

Aleksandar Bošković[1]
Slavko Dubačkić[2]

UDC 621.397:621.311
Stručni rad
Primljen: 12. 04. 2017.
Prihvaćen: 21. 04. 2017.

SISTEM VIDEO-NADZORA I KONTROLE PRISTUPA U ELEKTOENERGETSKIM OBJEKTIMA

Rezime: Kontrola ovlašćenog ili neovlašćenog prisustva, video-nadzor nad elektroenergetskim objektima i detekcija i alarmiranje incidentnih situacija predstavljaju bitan elemenat u obezbeđivanju kvalitetnog i efikasnog funkcionisanja samih elektroenergetskih objekata, kao i celokupnog elektroenergetskog sistema. Stoga je od izuzetnog značaja funkcionisanje tehničkog sistema zaštite, kao i zaštita ovog sistema od visokotehnološkog kriminala. Osnovna namena tehničkog sistema zaštite elektroenergetskih objekata je odvraćanje nepozvanih lica od potencijalnog neovlašćenog pristupa, sprečavanje neadekvatnog i nebezbednog rada na objektima, identifikacija lica i drugih uzročnika alarmnih situacija, detekcija kretanja i ostalih incidentnih situacija u objektu i prepoznavanje osoba u objektu. Pored navedenih osnovnih funkcionalnosti, u tehničkom sistemu zaštite elektroenergetskih objekata potrebno je implementirati i mehanizme kontinuiranog nadzora, arhiviranja podataka, reakcije na incidentne situacije i sl. U radu se prezentuju iskustva autora u razvoju i implementaciji kompanijskog tehničkog sistema zaštite elektroenergetskih objekata na konzumnom području Vojvodine. Prezentuju se tehnička rešenja, organizacioni problemi i ekonomsko-finansijski aspekt.

***Ključne reči*:** tehnički sistem zaštite, elektroenergetski objekti, kontrola pristupa, protivprovalna zaštita, video-nadzor

[1] Fakultet za pravne i poslovne studije dr Lazar Vrkatić, Novi Sad, E-mail: aboskovic@fpps.edu.rs

[2] ODS EPS Distribucija d.o.o, Beograd, E-mail: slavko.dubackic@epsdistribucija.rs

1. Uvod

Tehnički sistem zaštite na konzumnom području Vojvodine je integrisani bezbednosni sistem namenjen za daljinski nadzor elektroenergetskih objekata. Ovaj sistem objedinjuje funkcije:

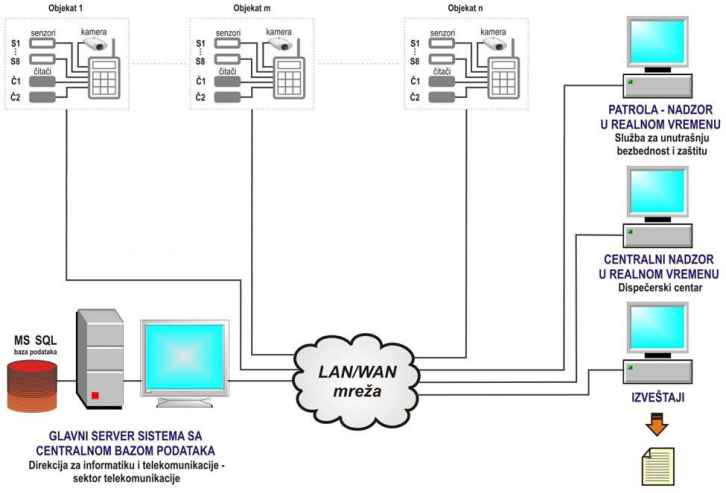
- sistema kontrole pristupa zasnovanog na beskontaktnim identifikacionim karticama;
- sistema alarmnog nadzora zasnovanog na dualnim senzorima za detekciju pokreta i
- sistema video-nadzora zasnovanog na IP kamerama sa internom memorijom.

Izgradnjom tehničkog sistema zaštite nad elektroenergetskim objektima na konzumnom području Vojvodine za potrebe kontrole pristupa lica i alarmnog i video nadzora omogućena je bolja i efikasnija zaštita imovine, kao i nadzor i evidencija prisutnosti lica u objektima preduzeća.

Osnovni ciljevi funkcionisanja ovog sistema su povećanje pouzdanosti rada elektroenergetskog sistema i bezbednost radnika i opreme angažovane na elektroenergetskim objektima. Takođe, cilj je da se i sam sistem obezbedi tako da bude raspoloživ i omogući poverljivost i integritet informacija.

2. Opis sistema

Tehnički sistem zaštite se sastoji od opreme u nadzornim centrima u ograncima preduzeća i opreme na elektoenergetskim objektima. U svim nadzornim centrima instalirani su serveri sistema sa bazom podataka i odgovarajućim softverom. Serveri preuzimaju podatke sa uređaja na elektroenergetskim objektima, upisuju podatke u bazu podataka i omogućuju ovlašćenim korisnicima sistema nadziranje elektroenergetskih objekata i pregledanje arhiviranih događaja (Idejni projekat sistema, 2009).



Slika 1. Principijelna šema tehničkog sistema zaštite

Ovlašćena lica u računarskoj mreži preduzeća, putem nadzorne aplikacije, nadziru određenu grupu ili sve elektroenergetske objekte u sistemu, u skladu sa svojim ovlašćenjima. U nadzornoj aplikaciji prikazana su imena i aktuelni video-prikazi odabranih elektroenergetskih objekata, dok su bojom označeni statusi tih objekata.

Instalirana oprema na elektroenergetskim objektima predviđena je za spoljnu montažu i montirana je na građevinskim objektima i stubnim nosačima uočljive crvene boje, sa vidljivim tekstualnim obaveštenjima i upozorenjima. Mesta montaže opreme posebno su određena za svaki elektroenergetski objekat. Oprema koja je montirana na elektroenergetskim objektima je sledeća:

- uređaj za kontrolu pristupa i alarmni nadzor (terminal);
- beskontaktni čitači identifikacionih kartica za evidentiranje ulaska i izlaska lica;
- alarmni senzori za detekciju pokreta, odnosno prisustva lica;
- IP kamere sa internom memorijom;
- alarmna sirena sa stroboskopskim svetlom i
- rezervno baterijsko napajanje.
-

Po pravilu, na elektroenergetskim objektima oprema je ugrađena na sledeći način:

- Metalni stubni nosači za montažu opreme ugrađeni su kod ulaza i po potrebi kod transformatorskog polja.
- Dva čitača identifikacionih kartica za kontrolu i evidenciju pristupa objektu postavljeni su na metalnom stubnom nosaču za montažu opreme kod ulaza.
- U stubnim nosačima instalisani su uređaj za kontrolu pristupa i alarmni nadzor sa odgovarajućim softverom.
- IP kamere su montirane na stubovima i na građevinskim objektima i usmerene su ka transformatorskom polju, ulazima i ogradi objekata. Kamere su postavljene u odgovarajućem kućištu za spoljnu montažu sa odgovarajućim softverom. Za svaku kameru je obezbeđena memorijska kartica za snimanje.
- Spoljašnji senzori pokreta su postavljeni na građevinskom objektu i na stubnim nosačima tako da pokrivaju prostor oko elektroenergetskog objekta, ulaza i transformatorskog polja.
- Alarmna sirena je instalisana na stubu kod ulaza ili na građevinskom objektu.
- Instalisan je komunikacioni orman sa L2 PoE svičem, FTP razdelnikom, letvom za napajanje i besprekidnim napajanjem.
-

3. Zaštita sistema

Obezbeđivanje samog tehničkog sistema zaštite, kontrole pristupa i alarmnog i video nadzora od eventualnih narušavanja njegovih atributa sigurnosti ostvareno je na više načina (Projekat izvedenog sistema, 2013):

- na samim objektima ugrađena je visokokvalitetna oprema namenjena za rad u svim vremenskim i drugim uslovima karakterističnim za elektroenergetske objekte, smeštena u odgovarajuća kućišta ili ormane;
- postoji kontrola pristupa samim ormanima (tamperi);
- komunikacija od elektroenergetskih objekata do sedišta ogranaka gde se nalaze serveri sistema obezbeđena je kriptovanjem;
- obezbeđen je rad u režimu van mreže;

- sam koncept u kome se serveri ne smeštaju na svakom elektroenergetskom objektu, nego u sedištima ogranaka, što su omogućile kvalitetne telekomunikacione veze, podiže nivo bezbednosti kako operativnog rada, tako i analize arhiviranih podataka;
- restriktivan je odnos ka pravima pristupa sistemu kroz klijentske aplikacije.

Poseban aspekt predstavlja organizacija kompanije, u smislu korišćenja sistema u realnom vremenu, kao i u slučaju *post festum* analize podataka.

U realizaciji ovog sistema primenjuju se svi mehanizmi zaštite koje preduzeće primenjuje i za ostale sisteme u domenu informaciono-komunikacionih tehnologija. Od zaštite *data* centara na fizičkom nivou (zaštita od požara, prenapona, napajanja, neovlašćenog fizičkog pristupa opremi i sl.) do zaštite od napada na sistem kroz informaciono-komunikacionu infrastrukturu.

Normativno uređenje zaštite informaciono-komunikacionog sistema predstavlja posebnu oblast i predmet je aktivnosti države, pravosuđa i upravljačkih i pravnih struktura preduzeća.

Drugi aspekt zaštite informaciono-komunikacionog sistema je projektovanje i uvođenje tehničkih mera za ostvarivanje zaštite celokupnog informacionog sistema. Cilj je da se obezbede atributi sigurnosti sistema (Ross Anderson, 2012):

- *Raspoloživost* – osigurava opstanak servisa i pored napada čiji je cilj da se oni ugroze. Takvi napadi mogu biti pokrenuti sa bilo kog nivoa. Na fizičkom nivou zlonamerni korisnik može npr. da ometa komunikaciju na fizičkim kanalima. Na višem nivou remećenjem rada protokola za rutiranje može se dovesti do raspada mreže.
- *Poverljivost* – osigurava da se neke informacije nikada ne stave na raspolaganje neautorizovanim entitetima. Curenje poverljivih informacija može imati nesagledive posledice.
- *Integritet* – garantuje da poruka nikada neće biti kompromitovana. Poruka može biti kompromitovana zbog bezazlenih kvarova, kao što su smetnje u radio-prenosu ili zbog zlonamernih napada na mrežu.

- *Autentikacija* – omogućava da bilo koji čvor utvrdi identitet čvora sa kojim trenutno komunicira. Bez autentikacije napadač bi mogao da se maskira kao čvor i tako dobije pristup informacijama i resursima, čime bi uticao na rad ostalih čvorova.
- *Neporicanje* – znači da pošiljalac poruke ne može da porekne da ju je poslao. Neporicanje je veoma značajno za otkrivanje i izolaciju kompromitovanih čvorova.

Konačno, namena ovih sistema jeste da se obezbedi kontinuitet poslovnih procesa preduzeća i u tom cilju je i implementiran na skoro svim visokonaponskim elektroenergetskim objektima na konzumnom području Vojvodine sa tendencijom da se proširi i na srednjenaponske elektroenergetske objekte. Da bi se došlo do ovakvog nivoa prihvatanja sistema, kako od strane korisnika, tako i od strane uprave preduzeća, sistem je morao pokazati svoju upotrebnu vrednost, robusnost i stabilnost u radu.

4. Programski moduli sistema

Svi programski moduli mogu da se pokrenu sa bilo kog računara u okviru računarske mreže preduzeća od strane autorizovanog korisnika.

Sistem sadrži sledeće programske module:

- serverski modul,
- nadzornu aplikaciju,
- administrativnu aplikaciju i
- izveštajnu aplikaciju.

Serverski modul je aplikacija pokrenuta na serveru sistema koja proziva sve uređaje sa elektroenergetskih objekata, preuzima podatke i upisuje ih u bazu i pruža podršku svim klijentskim aplikacijama u sistemu.

Nadzorna aplikacija je klijentska aplikacija koju mogu pokrenuti svi autorizovani korisnici da u skladu sa svojim privilegijama vrše nadzor grupe ili svih objekata u sistemu.

Nadzorna aplikacija omogućava:

- uvid u trenutni status svih objekata i pripadajućih alarmnih senzora za detekciju pokreta koje nadgleda ta nadzorna aplikacija;

- nadzor u realnom vremenu alarmnih situacija (vrsta, vreme i mesto alarma i trenutna slika koju daje dodeljena kamera);
- prikaz u realnom vremenu sa kamere koja je nadležna za alarmni senzor za detekciju pokreta koji je aktivirao alarmnu situaciju;
- pretraživanje snimaka po mestu, vremenu i vrsti događaja.

Administrativna aplikacija sadrži sledeće funkcije:

- održavanje podataka o strukturi sistema;
- održavanje podataka o strukturi preduzeća;
- održavanje podataka o zaposlenima;
- održavanje podataka o identifikacionim karticama;
- održavanje podataka o ovlašćenim korisnicima sistema;
- definisanje i održavanje vremenske šeme za aktivaciju, odnosno deaktivaciju senzora.

Izveštajna aplikacija omogućava generisanje sledećih izveštaja:

- hronološki izveštaj o alarmima koji prikazuje i snimke zabeležene kamerom;
- izveštaj o aktivaciji, odnosno deaktivaciji alarmnih senzora za detekciju pokreta;
- pregled snimaka koje je napravila kamera prilikom alarmne situacije;

Svaki od ovih izveštaja se može formirati za izabrani objekat, senzor, organizacionu celinu ili celo preduzeće za željeni vremenski period. Sistem omogućava i izvoz dela ili svih podataka iz generisanih izveštaja na zahtev ovlašćenog lica u bilo kom *Microsoft* podržanom formatu.

5. Način rada sistema

Prilikom ulaska u elektroenergetski objekat pod tehničkim sistemom zaštite lice se identifikuje svojom identifikacionom karticom na beskontaktnom čitaču kartica montiranom na stubnom nosaču i povezanom na terminal. Terminal je montiran unutar stubnog nosača u kutiji za elektronsku opremu.

Podaci o ulasku u elektroenergetski objekat, lokacija, ime, prezime i identifikacioni broj lica i vreme ulaska beleže se u bazu podataka na serveru.

Ukoliko je ovlašćeno lice ušlo u objekat:

- alarmni senzori za detekciju pokreta će se deaktivirati,
- terminal će proslediti informaciju o ovlašćenom prisustvu serveru,
- u nadzornoj aplikaciji prikazanog objekta biće označeni zelenom bojom.

Lica zadužena za nadzor mogu videti koja su lica trenutno prisutna u objektu.

Ukoliko je neovlašćeno lice ušlo u objekat:

- alarmni senzori za detekciju pokreta će se aktivirati,
- alarmna sirena sa stroboskopskim svetlom će se uključiti,
- terminal će proslediti informaciju o neovlašćenom prisustvu serveru,
- u nadzornoj aplikaciji uključiće se zvučna i vizuelna signalizacija,
- u nadzornoj aplikaciji prikazi tog objekta biće označeni trepćućom crvenom bojom.

Ukoliko ovlašćeno lice potvrdi alarm:

- u nadzornoj aplikaciji isključiće se vizuelna i zvučna signalizacija,
- u nadzornoj aplikaciji prikazi tog objekta biće označeni crvenom bojom tokom trajanja alarmne situacije dok je aktivan alarmni senzor za detekciju pokreta na elektroenergetskom objektu.

Podaci o alarmnom situaciji, naziv senzora, naziv objekta, vreme aktivacije i deaktivacije senzora beleže se u bazu podataka na serveru. U svim nadzornim aplikacijama će biti prikazan aktuelni video-prikaz sa tog objekta tako da u nadzornom centru može da se vizuelno nadgleda u realnom vremenu alarmna ili bilo koja druga situacija.

IP kamere snimaju neprekidno bez obzira na to postoji li alarmna situacija i ima li lica na objektu. Video-zapis se neprekidno beleži na serveru, a po aktiviranju detektora pokreta na IP kamerama smešta se i u internu memoriju kamere. U slučaju prekida veze, video-snimak koji je arhiviran u internoj memoriji kamere može se preuzeti lokalno ili daljinski nakon uspostave veze i prebaciti na server. Alarmni sistem, takođe, radi u slučaju gubitka veze u režimu van mreže tako što su podaci o pravima prisustva pohranjeni u terminalu.

6. Osnovne karakteristike sistema

Tehnički sistem zaštite elektroenergetskih objekata na konzumnom području Vojvodine je nezavisan sistem za kontrolu prisustva i alarmni i video nadzor elektroenergetskih objekata koji predstavlja zaokruženu funkcionalnu celinu, ali je i povezan sa drugim identifikacionim sistemima. Korisničke identifikacione kartice za identifikaciju u sistemu za evidenciju radnog vremena i kontrolu pristupa su jedinstvene i koriste se i za autorizaciju u tehničkom sistemu zaštite.

Uređaji za kontrolu pristupa i alarmni nadzor i alarmni senzori za detekciju pokreta zasnovani su na digitalnoj tehnologiji, dok su beskontaktni čitači i identifikacione kartice zasnovani na tehnologiji radiofrekventne identifikacije. Sistem ima mogućnost proširenja brojalica, uređaja i objekata. Svi računari i uređaji povezani su u jedinstvenu računarsku mrežu preduzeća.

Snimanje i obrada podataka su centralizovani u bazi podataka na serveru. Sistem centralizovano prikuplja podatke sa svih elektroenergetskih objekata, a funkcije nadzora u realnom vremenu, administracije i izveštavanja su centralizovane na nivou preduzeća. Alarmiranje putem alarmne sirene sa stroboskopskim svetlom je lokalno, ali se svaka alarmna situacija zvučno oglašava i prikazuje u svim nadzornim aplikacijama koje nadgledaju taj alarmni uređaj.

Terminali komuniciraju sa serverima *Ethernet* vezom (optičkim linkovima ili usmerenim radio-relejnim linkovima). Ukoliko je komunikacija između terminala na elektroenergetskom objektu i servera u prekidu, podaci o pristupu pamte se u internoj memoriji terminala i pri ponovnom uspostavljanju komunikacije prebacuju se na server. Terminal automatski detektuje prekid u komunikaciji i pokušava da se ponovo poveže sve dok ne uspostavi vezu sa serverom.

Sistem podržava rad u sledećim režimima (Idejno rešenje sistema, 2009):

- rad u mreži – kada je uspostavljena komunikacija uređaja sa serverom, svi događaji trenutno se upisuju u bazu podataka, obrađuju i prikazuju na svim nadzornim aplikacijama koje nadgledaju dati uređaj; svi podaci o ovlašćenim prolascima i alarmnim situacijama su raspoloživi kroz preglede i izveštaje;

- rad van mreže – kada je prekinuta komunikacija uređaja sa serverom, putem bafera uređaja koji pamti podatke o registrovanim pristupima i alarmnim situacijama i putem interne memorije uređaja koja čuva naloge za aktivaciju, odnosno deaktivaciju senzora, sistem nesmetano radi. Kada se uspostavi konekcija sa serverom, sistem automatski prelazi u režim rada u mreži i prenosi baferovane podatke u bazu podataka.

Terminal ima osam alarmnih ulaza od kojih su iskorišćena dva do tri za priključivanje alarmnih senzora za detekciju pokreta. Na prvi alarmni ulaz povezani su svi tamper prekidači alarmnih senzora za detekciju pokreta i terminala tako da se u slučaju fizičkog uklanjanja senzora javlja alarmna situacija.

Svi alarmni ulazi su konfigurisani kao bezuslovni alarmi i uključuju se na pobudu od senzora nezavisno od vremenske šeme za aktivaciju, odnosno deaktivaciju senzora. Konfiguracija kao uslovni alarm, u skladu sa unapred definisanom vremenskom šemom aktivacije, odnosno deaktivacije, koristi se prilikom remonta elektroenergetskih objekata. Takođe, svi alarmni ulazi su definisani kao trenutni, izuzev alarmnog ulaza na koji je priključen alarmni senzor za detekciju pokreta na ulazu, odnosno izlazu, koji ima vremensku zadršku od 20 sekundi. Pored toga svi alarmni ulazi su definisani kao čujni i aktiviraju alarmnu sirenu sa stroboskopskim svetlom.

Napajanje terminala, beskontaktnih čitača identifikacionih kartica i alarmnih senzora za detekciju pokreta obezbeđeno je preko rezervnog baterijskog napajanja koje je vezano na invertor elektroenergetskog objekta. Sistem automatski pravi rezervnu kopiju podataka na odabranu lokaciju u okviru sistema datoteka u definisanom vremenu.

7. Implementacija sistema

Prvom i drugom fazom izgradnje obuhvaćeni su visokonaponski elektroenergetski objekti i pojedine poslovne zgrade. U Tabeli 1 dat je pregled elektroenergetskih objekata pod tehničkim sistemom zaštite (Projekat izvedenog sistema, 2013).

ED Novi Sad	**ED Subotica**	**ED Sombor**	**ED Pančevo**	**ED Zrenjanin**	**ED Ruma**	**ED S. Mitrovica**
TS Novi Sad 1	TS Subotica 1	TS Sombor 1	TS Pančevo 3	TS Zrenjanin 1	TS Ruma 1	TS S. Mitrovica 1
TS Novi Sad 2	TS Subotica 2	TS Sombor 2	TS Pančevo 4	TS Zrenjanin 3	TS Ruma 2	TS S. Mitrovica 3
TS Novi Sad 4	TS Subotica 4	TS Apatin	TS Vršac 1	TS Zrenjanin 4	TS Pećinci	TS Šid
TS Novi Sad 5	TS B. Topola 2	TS Odžaci	TS Vršac 2	TS Kikinda 1	TS Inđija 1	
TS Novi Sad 6	TS Bajmok	TS Vrbas 1	TS Kovin	TS Kikinda 2	TS Inđija 2	
TS Novi Sad 7	TS Ada	TS Vrbas 2	TS Alibunar	TS N. Bečej	TS S. Pazova	
TS Novi Sad 9		TS Kula	TS Debeljača	TS Begejci	TS N. Pazova	
TS Futog				TS N. Crnja		
TS Temerin						
TS Žabalj						
TS R. Šančevi						

Tabela 1. Pregled elektroenergetskih objekata pod tehničkim sistemom zaštite

Treća faza izgradnje bi obuhvatila preostalih jedanaest visokonaponskih elektroenergetskih objekata.

U svakom elektroenergetskom objektu se nalazi:

- telekomunikacioni orman gde su na FTP razdelniku terminirani FTP kablovi IP kamera i kontrolera za senzore pokreta, RFID čitače i alarmnu sirenu.
- U telekomunikacionom ormanu se nalazi i Cisco WS-C2960-24PC-L PoE svič i besprekidno napajanje.
- Od tri do sedam IP kamera proizvođača *Axis* modeli P3364-VE i P1354 sa memorijskim karticama. Kamere su montirane na metalnim stubovima, stubovima rasvete ili građevinskom objektu.
- Stubni nosač kod ulaza za montažu opreme.
- Kontroler kontrole pristupa i alarmnog nadzora model SD-100VEB sa neprekidnim napajanjem koji je montiran u metalnom stubu.

- Dva čitača ID kartica model SD25 montirana na metalnom stubu.
- Od osam do četrnaest senzora za detekciju pokreta za spoljašnju montažu proizvođača DSC model LC-171. Detektori su montirani na metalnom stubu, stubovima rasvete ili objektu TS.
- Instalacioni kablovi.

8. Zaključak

Realizacijom tehničkog sistema zaštite elektroenergetskih objekata na konzumnom području Vojvodine, kao integrisanog bezbednosnog sistema kontrole pristupa i alarmnog i video nadzora, omogućena je bolja i efikasnija zaštita imovine preduzeća kroz smanjenje krađa na elektroenergetskim objektima, a postignut je i veći stepen bezbednosti na radu kroz nadzor i evidenciju prisutnosti lica na elektroenergetskim objektima. Sistem u punoj meri ispunjava svoju ulogu u odvraćanju nepozvanih lica od potencijalnog neovlašćenog pristupa, sprečavanju neadekvatnog i nebezbednog rada na objektima, identifikaciji lica i drugih uzročnika alarmnih situacija, detekciji kretanja i ostalih incidentnih situacija u objektu i prepoznavanja osoba u objektu. Implementirani su mehanizmi kontinuiranog nadzora, arhiviranja podataka i reakcije na incidentne situacije. Tehničkim sistemom zaštite obezbeđeno je kvalitetnije i efikasne funkcionisanje samih elektroenergetskih objekata, pouzdaniji rad celokupnog elektroenergetskog sistema i kvalitetnija usluga napajanja potrošača električnom energijom. Stoga je od izuzetnog značaja funkcionisanje tehničkog sistema zaštite elektroenergetskih objekata, kao i zaštita ovog sistema od visokotehnološkog kriminala.

9. Literatura

1. BS 25999-2:2007 Business continuity management. Specification, British Standard, 2007.
2. BS 25999-2:2007 Business continuity management. Specification, British Standard, 2007.
3. Energetski podaci za 2014. godinu, Elektrovojvodina, Novi Sad, 2015.
4. Idejni projekat sistema nadzora i kontrole pristupa u poslovnim i elektroenergetskim objektima na području Elektrovojvodina d.o.o. Novi

Sad, Sveske 1–8, Elektrovojvodina d.o.o. Novi Sad, Institut za bezbednost i sigurnost na radu Novi Sad, 2009.
5. Idejno rešenje integrisanog bezbednosnog sistema za daljinski nadzor Vesta ID, Solutis.
6. ISO/IEC 27001:2005 Information security management systems - Requirements, International Organization for Standardization, 2005.
7. ISO/IEC 27002:2007 Code of practice for information security management, International Organization for Standardization, 2007.
8. ISO/IEC 27005:2008 Information security risk management, International Organization for Standardization, 2008.
9. Jonathan Perks, Jonathan Hyde, Angela Falconer. Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector, AEA Technology plc for European Commission, Directorate-General Justice, Freedom and Security, 2009.
10. JP Elektroprivreda Srbije Beograd, Distributivni elektroenergetski sistem Srbije, Inteligentne mreže u JP EPS, Strategija i razvoj sistema za daljinski nadzor i upravljanje srednjenaponskom distributivnom mrežom u uslovima značajnijeg prisustva distribuirane proizvodnje, Studija, Enerogprojekt Entel a.d. ITEN Engineerig, Beograd, 2014.
11. Projekat izvedenog sistema video nadzora u EEO na konzumnom području Elektrovojvodine, Sveske 1-49, Elektrovojvodina d.o.o. Novi Sad, Solutis d.o.o. Beograd, 2013-2015.
12. Ross Anderson. Measuring the Cost of Cybercrime, University of Cambridge, http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.
13. SONA promises advanced next-generation networks, URL: http://www.networkworld.com/article/2293980/infrastructure-management/cisco--sona-promises-advanced-next-generation-networks.html