PREDLOZI TIPSKIH MODELA ZA REALIZACIJU VISOKO POUZDANIH LOKALNIH KOMUNIKACIONIH MREŽA U ELEKTROENERGETSKIM OKRUŽENJIMA

SUGGESTIONS OF TYPICAL MODELS FOR THE REALIZATION OF HIGHLY RELIABLE LOCAL COMMUNICATION NETWORKS IN POWER DISTRIBUTION ENVIRONMENTS

Slavko DUBAČKIĆ, Elektrodistribucija Srbije d.o.o. Beograd, Ogranak Novi Sad, Serbia
Aleksandar BOŠKOVIĆ, „Fakultet tehničkih nauka“ Novi Sad, Srbija, Serbia
Đorđe VLADISAVLJEVIĆ, Elektrodistribucija Srbije d.o.o. Beograd, Ogranak Novi Sad, Serbia

KRATAK SADRŽAJ

SCADA sistemi su jedni od najvažnijih infastrukturnih sistema u industrijskom i energetskom sektoru, od nafte i gasa do nuklearnih postrojenja ili postrojenja za obradu vode. Oni predstavljaju tipične primere OT (Operational Technology) mreža. Njihova kritična infrastruktura je definisana kao skup fizičkih i IT uređaja, mrežnih servisa, koji, ukoliko budu oštećeni ili uništeni, mogu imati veliki uticaj poslovne i tehničke procese kompanije, bezbednost kompanije, na zdravlje zaposlenih i stanovništva, sigurnost i ekonomsku stabilnost regiona ili države. Imajući sve ovo u vidu, zaštita kritičnih OT sistema i infrastukture postavlja se kao imperativ. Rad daje predloge rešenja i tipske modele za realizaciju visoko pouzdanih lokalnih komunikacionih mreža u industrijskim okruženjima. Rad sadrži funkcionalne opise predloženih rešenja i tipske predloge za realizaciju lokalnih OT mreža sagledavajući zahteve za modernizacijom, povećanjem efikasnosti i bezbednosti ovih objekata. Pri izradi ovog rada posebno se vodilo računa o bezbednosti IKT sistema i sistema daljinskog upravljanja (informacionih i operacionih tehnologija (IT/OT)).

Ključne reči: informatička bezbednost, OT sistemi, elektroenergetski sistemi

SUMMARY

SCADA systems are some of the most important infrastructural systems in the industrial and energy sector, from oil and gas to nuclear plants or water treatment plants. They represent typical examples of OT (Operational Technology) networks. Their critical infrastructure is defined as a set of physical and IT devices, network services, which, if disrupted or destroyed, can have a big effect on the business and technical processes of the company, the company's safety, the health of employees and the population, the security and economic stability of the region or the state. Bearing in mind all this, the protection of critical OT systems and infrastructures is assumed to be imperative. The paper presents suggestions for solutions and typical models for the realization of highly reliable local communication networks in industrial environments. It contains functional descriptions of the proposed solutions and type proposals for the implementation of local OT networks considering the requirements for modernization, increasing the efficiency and safety of these facilities. The paper specifically considers the security of ICT systems and remote management systems (information and operational technologies (IT/OT)).

Key words: Information Security, OT systems, Power Systems

slavko.dubackic@ods.rs
aboskov@uns.ac.rs
djordje.vladisavljevic@ods.rs

UVOD

Šta su OT sistemi?

Operativne tehnologije (OT) čine sistemi namenjeni nadzoru, kontroli i upravljanju uređajima u industrijskim sistemima, transportu, komunalnim sistemima.

IT – OT konvergencija.

Kako fizički uređaji postaju „pametni“, raste trend ka IT – OT konvergenciji. Povezivanje korišćenjem IT tehnologija omogućuje bolje praćenje sistema, mogućnost daljinske kontrole i upravljanja fizičkim uređajima. Stvaraju se mogućnosti za analizu podataka iz OT sistema u realnom vremenu i preduzimanje upravljačkih aktivnosti što olakšava preventivno održavanje i smanjuje vreme neraspoloživosti OT servisa.

Zašto je OT bezbednost važna?

Kako industrijski sistemi postaju sve više povezani, tako postaju i izloženiji napadima. Visoki troškovi industrijske opreme, njihova raznolikost, slaba kompatibilnost, tehnološko nasleđe i drugi faktori mogu uticati na složenost implementacije bezbednosnih mehanizama. Sa druge strane štete koje bi napad mogao da ima na dati OT sistem, ali i na društvo i na ekonomiju mogu biti vrlo velike.

VRSTE PRETNJI U OT SISTEMIMA

Vrste napada na OT sisteme obuhvataju sve one napade koji su karakteristični za IT sisteme (virusi, zlonamerni softveri, DOS napadi i sl.) ali i neke specifične za OT sisteme:

- *Malware* i APT (*Advanced Persistant Threat*)
  Zlonamerni softver dizajniran sa ciljem nanošenja štete računaru, serveru, klijentu ili računarskoj mreži. Može uzeti oblik izvršnog koda, skripta, aktivnog sadržaja ili nekog drugog softvera. U malvere se ubrajaju virusi, crvi, trojanci, ransomware i spyware.
- *Backdoor* napadi preko mrežnog perimetra
  Kao i kod IT sistema i OT mreže poseduju određen broj ranjivosti koje mogu napadaču omogućiti tzv. backdoor kojim može doći do neovlašćenog pristupa. Vrlo često ove ranjivosti su jednostavni nedostaci u arhitekturi perimetra ili neke starije funkcionalnosti koje su zaboravljene, neprimećene ili jednostavno odbačene. Ovi nedostaci takođe mogu biti nesvesno napravljeni na više mesta, ali su, iz očiglednih razloga, na mrežnom perimetru oni od najvećeg značaja.
- OPC/DCOM napadi (*OLE for Process Control/ Distributed Componenet Object Model*)
  Modernizacija OT sistema uvela je nove IT tehnologije kao što su OLE, DCOM i Remote Procedure Call (RPC). Majkrosoftov OLE for Process Control (OPC) je standard za komunikaciju u realnom vremenu za ove servise i sa sobom donosi svu bezbedonosnu problematiku.
- Napadi na bazu podataka i data injection napadi
  Baze podataka su još jedna od kritičnih komponenti svakog OT sistema. Tradicionalni modeli za bezbednost zasnivaju se na potpunoj izolaciji OT sistema i fokusu na zaštiti tačno određene vrste OT sistema. Međutim, često se iste baze koriste za OT sisteme i za neke druge IT sisteme. Jedan od primera su web aplikacije, koje za svoje funkcionisanje koriste baze podataka i SQL.
- *Man-in-the-middle* (MITM) napadi
  Ustaljeni način zaštite industrijskih OT sistema od neovlašćenog pristupa iz IT mreže je takozvani „air gap”, odnosno fizička izolacija celokupne OT mreže. Prirodno, interna komunikacija između uređaja u okviru jedne OT mreže je manje osigurana.
- *Supply Chain* napadi
  Takozvani Supply Chain napad, ili napad preko treće strane, se dešava kada se napadač infiltrira u sistem preko legitimnog proizvođača softvera ili hardvera koji je u upotrebi.
- BYOD napadi (*Bring Your Own Device*)
  Praksa donošenja svojih uređaja je dobar biznis model koji povećava fleksibilnost i produktivnost, s druge strane ima veliki uticaj na IT infrastrukturu. Donošenjem svojih uređaja na radno mesto, korisnici na jednom uređaju mešaju privatne i poslovne podatke što dovodi do bezbednosnih izazova: rizik od curenja podataka, mešanje privatnih i poslovnih podataka, širenje zlonamernog softvera kroz IT infrastrukturu.

ODNOS BEZBEDNOSTI IT I OT SISTEMA

Istorijski gledano, odgovornost za sigurnost industrijskih OT sistema se pripisivala korporativnom IT sektoru, koji je pratio procedure i planove za zaštitu ključnih informacionih resursa. S obzirom na prisutnu IT – OT konvergenciju, potrebno je proširiti IT procedure kako bi odgovarale i OT mrežama. Sa stanovišta sprečavanja napada, postavljanje čiste IT infrastrukture za odbranu u OT mreži ne mora da znači i zaštitu OT mreže. Iako se koriste isti protokoli, sama priroda i funkcionalnost im nisu iste. Neki sektori, kao što je energetski, zahtevaju veoma delikatna podešavanja u realnom vremenu, tako da bilo kakvo kašnjenje ili odlaganje, prouzrokovano konvencionalnim načinima zaštite, ne dolazi u obzir.
U Tabeli 1 prikazane su ključne razlike između korporativne (IT) i industrijske (OT) mreže sa stanovišta sigurnosti mreže.

TABELA 1. PRIORITETI IT I OT SISTEMA

Tema	**Korporativna mreža**	**Industrijska mreža**
Anti-virusni softver	Preporučeno, skoro neophodno	Retko implementirano, često nemoguće za implementaciju
Podrška za određenu tehnologiju	3-5 godina, EoS – EoL	Rešenja su dizajnirana da traju preko 20 godina
Outsourcing	Često se koristi	Retko se koristi
Instalacija zakrpa	Redovna, od mesečnog do reda veličine sekunde.	Ne radi se često, pre svega zbog pouzdanosti sistema
Kritičnost usluga	Odlaganje od par sati ili dana je moguće	Odlaganje je neprihvatljivo
Dostupnost	Nedostupnost je moguća	Nedostupnost je neprihvatljiva
Fizička sigurnost	Veoma osigurane prostorije data centara	Lokacije su udaljene i bez ljudskog prisustva

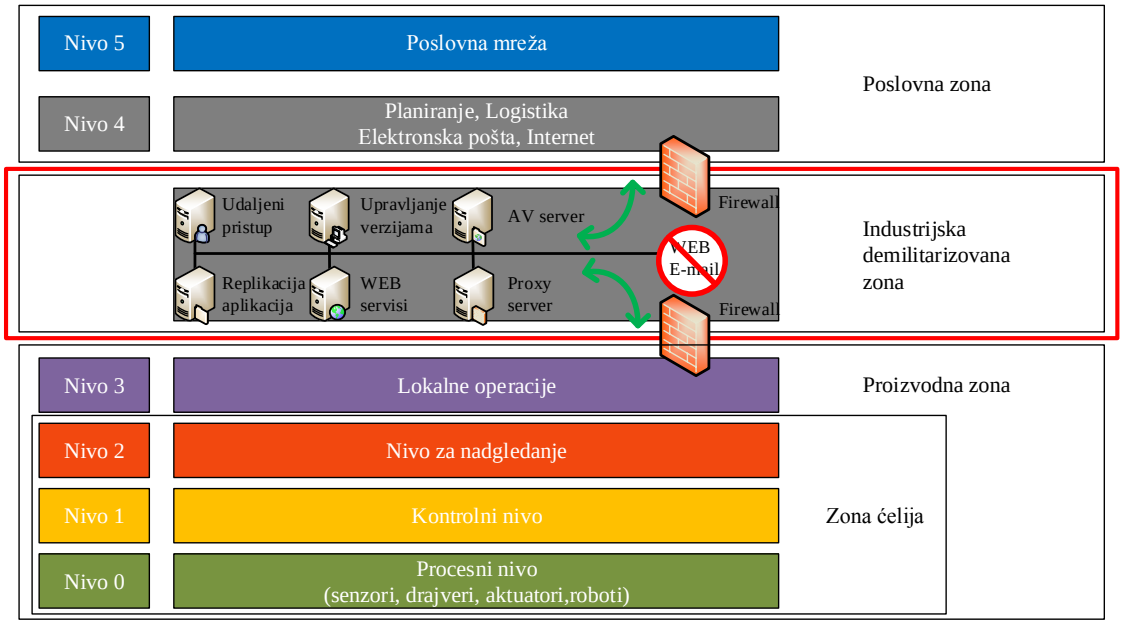
MREŽNA ARHITEKTURA

Dobra vest je da je moguće zaštititi nove ili postojeće industrijske OT mreže čak i bez ometanja tekućeg rada. Koristeći rešenja koja omogućavaju potpunu vidljivost mrežnog kontrolnog saobraćaja i uspostavljanje ispravnih bezbednosnih politika, može se postaviti efikasna strategija OT bezbednosti koja će zaštititi procese, ljude i profit i značajno smanjiti bezbednosne slabosti i incidente.
Osnova odbrane svake OT mreže leži u njenoj pravilnoj arhitekturi. Moderne mreže svoju arhitekturu zasnivaju na *Purdue* modelu. Ovaj model je deo *Purdue Enterprise Reference Architecture* (PERA) modela izrađenog od strane ISA-99 i koji se koriristi kao primer za segmentaciju kontrolnih sistema. U skladu sa *Purdue* modelom potrebno je realizovati OT infrastrukturu. Kada je u pitanju jedno industrijsko okruženje potrebno je izvršiti segmentaciju pojedinih delova i postaviti mehanizme zaštite između njih.

- **Poslovna Zona** je deo mreže gde se nalaze poslovni softveri kao što su ERP i SAP i drugi IT sistemi.
  - Nivo 5: Poslovna mreža
  - Nivo 4: Deo zadužen za planiranje i logistiku.

  Poslovna mreža je na korporativnom nivou i obično se prostire na više lokacija. U ovoj zoni se prikupljaju podaci iz hijerarhisjki niže postavljenih zona.
  Deo zone zadužen za logistiku je deo na kome je većina IT infrastrukture koja stoji iza proizvodnih procesa. Ovaj deo poslovne mreže uglavnom sadrži fajl servere, baze podataka, aplikativne servere, imejl servere, administratorske radne stanice itd.
- **Industrijska Demilitarizovana Zona** je namenjena za odbranu OT mreže.
  Industrijska DMZ (IDMZ) služi kao nivo za razmenu podataka između IT i OT segmenta mreže. Ovim uređenjem se postiže da proizvodni procesi u nižim nivoima nisu direktno izloženi potencijalnim opasnostima iz viših nivoa. Čak i ukoliko dođe do proboja viših nivoa, IDMZ zona može biti privremeno ugašena dok se incident ne razreši, bez remećenja proizvodnih procesa.
  Sistemi koji se obično nalaze u IDMZ su proksi serveri, replikatori baza, domen konroleri itd.
- **Proizvodna Zona** je mesto u kojoj je jezgro sistema. Proizvodna zona se prema *Purdue* modelu deli na četiri nivoa:
  - Nivo 3: Lokalne operacije,
  - Nivo 2: Nadgledanje,
  - Nivo 1: Kontrolni nivo i
  - Nivo 0: Proizvodni procesi.

Lokalne operacije – Nivo na kome se nalaze servisi za kontrolu i praćenje sistema. Na ovom nivou se vrši interakcija operatora (dispečera) u kontrolnim sobama sa sistemom. Takođe, ovde se vrši agregacija podataka sa svih nižih nivoa upravljanja i prosleđuje u DMZ (ili prosleđuje na zahtev, tzv. *Push vs Pull*). Ovaj nivo najčešće uključuje baze podataka, aplikativne servere, fajl servere, domen kontrolere i dispečerske terminale.
Nivo za nadgledanje – ovaj nivo je vrlo sličan prethodnom, uz napomenu da se na ovom nivou prate sistemi mnogo manjih dimenzija. Ovde se vrši kontrola i upravljanje na nivou jedne mašine, prekidača, rastavljača itd.
Kontrolni nivo – na ovom nivou se nalazi sva oprema za kontrolu i upravljanje. Ovde se izvršavaju funkcije kao što su otvaranje i zatvaranje prekidača, pomeranje aktuatora, startovanje motora i sl. Iako se PLC uređaji mogu sresti i na drugom nivou, njihova uloga je drugačija. Na drugom nivou imaju ulogu upravljanja dok na prvom imaju ulogu izvršavanja.
Procesni nivo – ovde se nalazi oprema za monitoring i kontrolu uređaja. Tipično se ovde nalaze motori, senzori, pumpe, ventili, merni transformatori.



SLIKA 1. SEGMENTACIJA OT SISTEMA – *PURDUE* MODEL

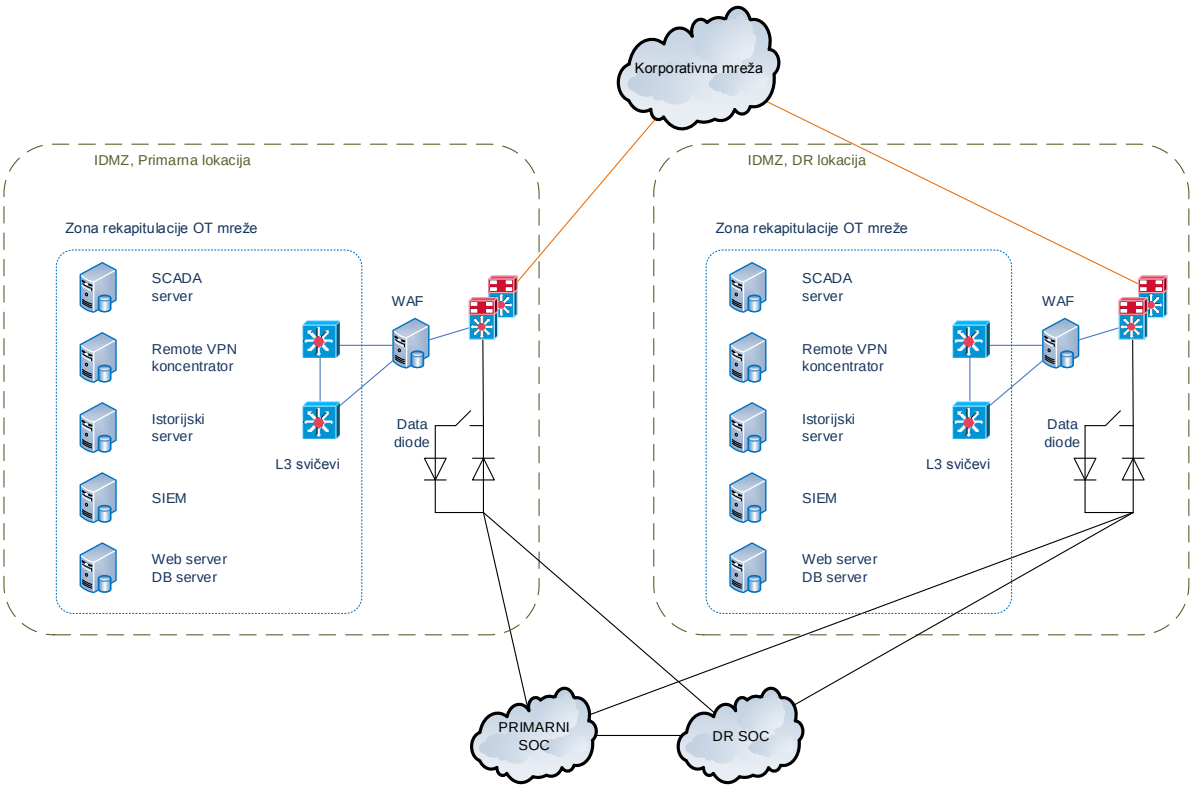
Prikazani *Purdue* model u potpunosti je primenjiv na industrijska okruženja. Poseban bezbedonosni izazov predstavljaju udaljeni objekti. Nekada je bilo bitno da se nekako dođe do njih i da se povežu ali u savremenom okruženju predstavljaju jedan od najznačajnijih segmenata koje treba obezbediti.
Konkretna primena i realizacija predloženog globalnog modela u EPS Distribuciji se ograničila na OT deo Purdue modela. Segmentacija je urađena tako da je sistem podeljen na pet zona:

- Прва зона – Зона EEO,
- Друга зона – Зона DDC,
- Трећа зона – Зона PDC/ODC,
- Четврта зона – Security Operations Center – SOC,
- Пета зона – Industrijska DMZ зона.

Od formiranja EPS Distribucije teži se unifikaciji tehničkih rešenja na celoj teritoriji. U tom smislu se pristupa i ovoj problematici, tj. unifikaciji OT LAN mreža u EEO, kao u VN EEO tako i SN EEO i uređaja.
Prvi korak je bio izrada tehničke dokumentacije koja bi definisala i detaljnije analizirala sve aspekte bezbednosti OT mreža EPS Distribucije. To je urađeno početkom 2019. godine.
Sledi implementacija rešenja. S obzirom na veliki broj EEO i prostornu udaljenost pristupa se faznom rešavanju.
Prva faza obuhvata implementaciju SOC-a u Beogradu, IDMZ-a u DDC/PDC Kraljevo i ODC Raška i zaštitu 5 TS 110/x. Prva faza je realizovana početkom 2020. godine.
Druga faza obuhvata implementaciju IDMZ-a u DDC/PDC Kragujevac i DDC/PDC Kragujevac, zaštitu 15 TS 110/x i povezivanje na SOC u Beogradu. Druga faza se realizuje tokom 2020. godine
Naredne faze će se realizovati u narednom periodu.
Poseban aspekt jeste povezivanje i modifikacija postojećih OT mreža (mreže za VN i SN upravljanje) na SOC u Beogradu i IDMZ po DP.

INDUSTRIJSKA DMZ

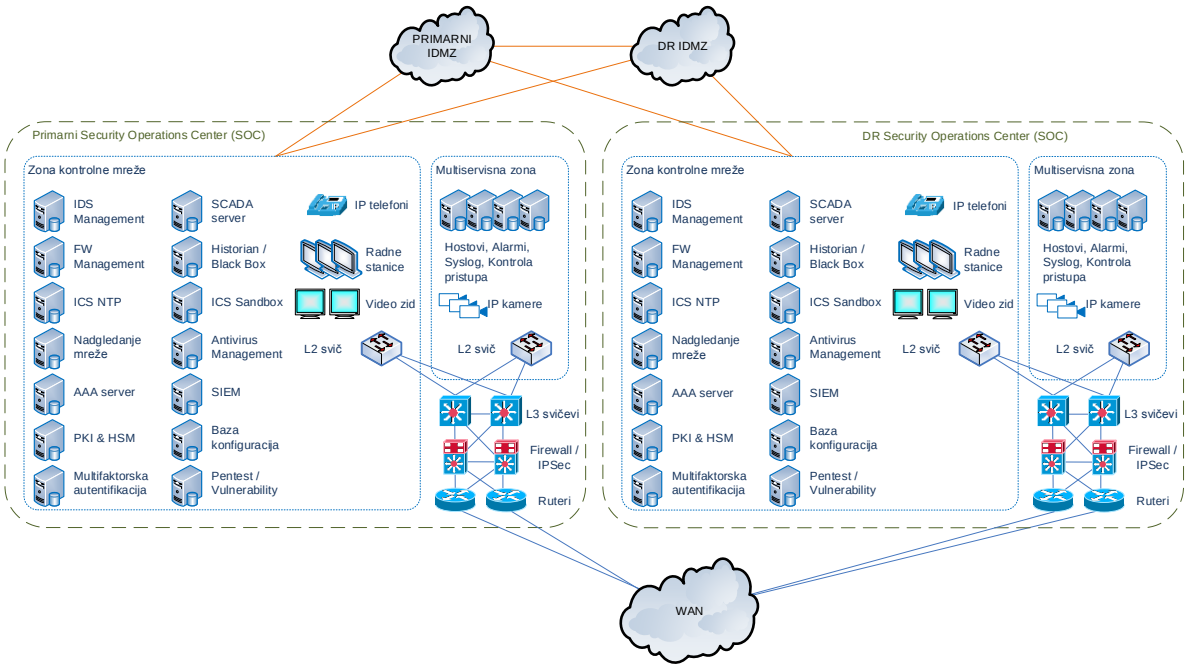
Industrijska DMZ (IDMZ) se nalazi između korporativne poslovne zone i kontrolne OT mreže (proizvodna zona) i čini petu zonu ove segmentacije. Ova zona omogućuje korisnicima iz IT mreže (i iz spoljašnjih mreža) pristup podacima od interesa iz OT mreže koristeći replikaciju podataka iz mreže.
Pristup samoj OT mreži je strogo regulisan i moguć samo uz eksplicitnu dozvolu. Pored replikacije podataka, cilj ove zone je da omogući OT mreži kontrolisan pristup internetu za potrebe preuzimanja sistemskih ažuriranja i zakrpa. U izuzetnim slučajevima, kada za tim postoji potreba, kroz DMZ je moguće napraviti i VPN tunel u OT mrežu koristeći VPN koncentrator. Ova zona može biti iskorišćena kao mesto objavljivanja veb aplikacija ili servisa, i kao mesto implementacije svih sigurnosnih rešenja namenjenih za zaštitu ovih servisa (Load Balancer, Web Application Firewall, Database Firewall, BlackBox). Za samu inspekciju saobraćaja, na ulazu u zonu je predviđen firewall, koji praktično ima ulogu rutera između tri mreže (korporativne, DMZ i OT). S obzirom na to da je ova zona zajednička za ceo sistem zbog redundantnosti sistema, realizacija DMZ zone je predviđena na dve lokacije.



SLIKA 2. INDUSTRIJSKA DMZ

SECURITY OPERATIONS CENTER (SOC)

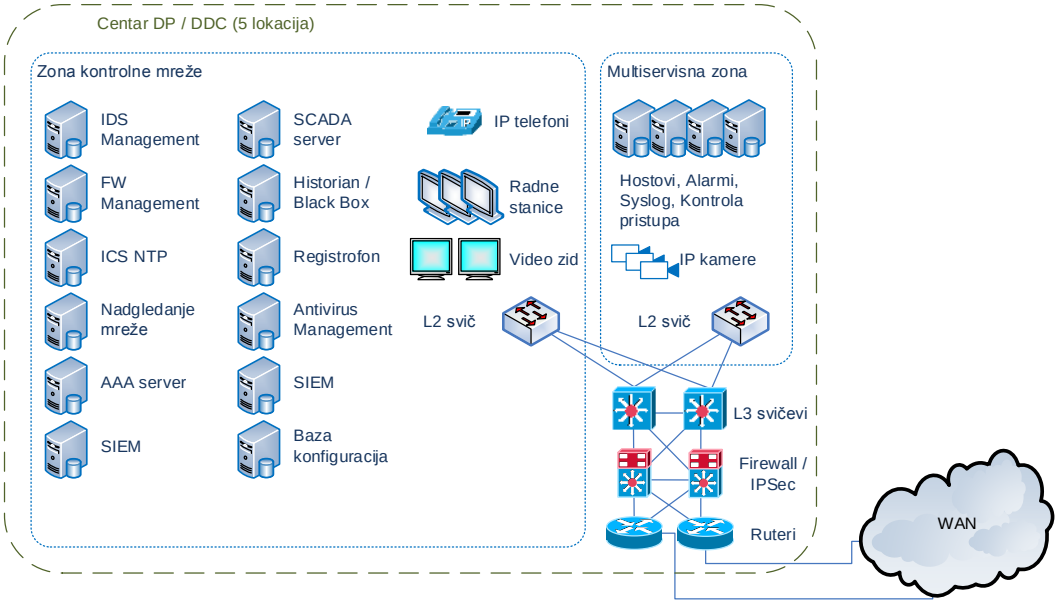
Četvrti nivo segmentacije OT mreže EPS Distribucije je SOC (Security Operations Center). Na ovom nivou se vrši nadgledanje i upravljanje sistemima za zaštitu za celokupan sistem ODS-a. Ovde se nalazi sistem za virtuelizaciju opreme, sistemi za sakupljanje i agregiranje obaveštenja, sistem za upravljanje IDS komponentom sistema, sistem za centralno upravljanje firewall uređajima, centralni delovi sistema za autentifikaciju i autorizaciju, sistem za upravljanje privilegovanim nalozima, PKI, sistem za čuvanje konfiguracija, sistem za praćenje anomalija u mreži, sistem za multifaktorsku autentifikaciju, upravljanje antivirus rešenjem, pentest alat, sistem za enkripciju virtuelizovane opreme, ICS Sandbox, ICS NTP i Historian (Black Box). Zbog potpune redundantnosti sistema, predviđena je i DR lokacija sa identičnom arhitekturom.
Pored komponenti sistema za bezbednost, u SOC-u postoji i multiservisna zona u kojoj se nalaze komponente bitne za fizičku bezbednost kao što su kamere, alarm i fizička kontrola prisutpa.



SLIKA 3. SECURITY OPERATIONS CENTER

NIVO DISTRIBUTIVNOG PODRUČJA / DDC

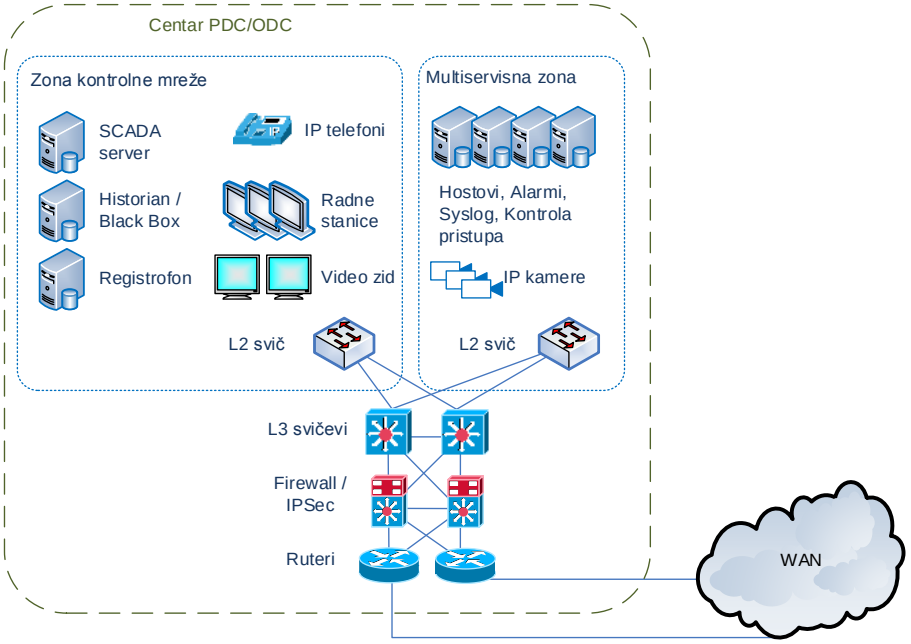
Na nivou centra distributivnog područja (treći nivo) omogućeno je upravljanje određenim komponentama sistema za koje se smatra da predstavljaju opterećenje ukoliko bi se njima upravljalo centralizovano. Ovde se pre svega misli na prava pristupa fizičkim elementima sistema i upravljanje firewall i IDS uređajima koji se nalaze u konkretnom distributivnom području. Na ulazu u mrežu centra distributivnog područja predviđeno je postavljanje firewall uređaja koji će vršiti inspekciju dolaznog i odlaznog mrežnog saobraćaja. Upravljanje firewall uređajima vršiće se na nivou SOC-a.
U svakom centru distributivnog područja je predviđen jedan ovakav centar upravljanja sigurnosnim komponentama sistema.



SLIKA 4. ZAŠTITA NA NIVOU DDC-A

NIVO PDC/ODC

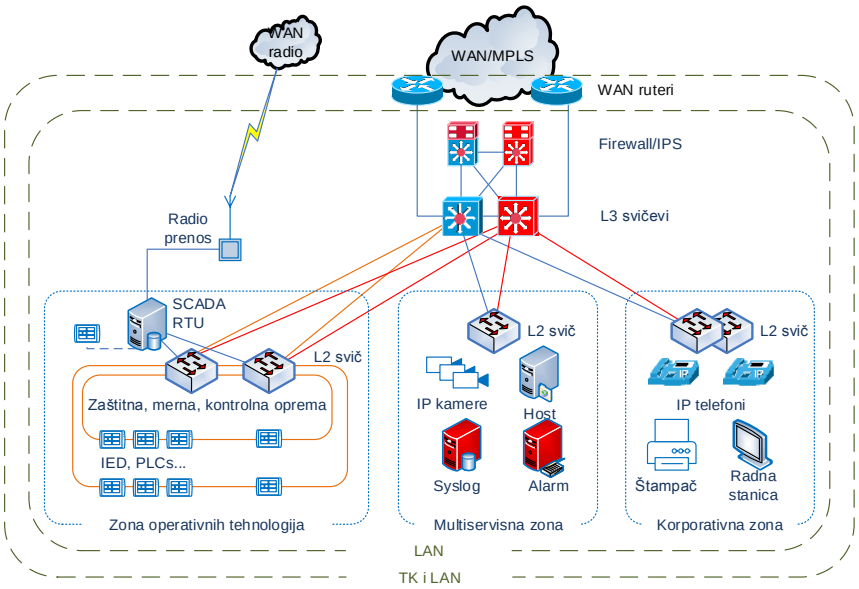
Segmentacija mreže na nivou PDC i ODC predstavlja drugi nivo. Od opreme za zaštitu OT mreže ovde su prisutni samo firewall uređaji koji se nalaze na sam ulaz mrežu PDC-a ili ODC-a a kojima se upravlja sa nivoa iznad. Takođe, na ovom nivou je vrlo važno da postoji i Black Box, kao osiguranje da log-ovi neće biti izmenjeni nakon napada.



SLIKA 4. ZAŠTITA NA NIVOU PDC/ODC

TIPSKA REŠENJA ZAŠTITE EEO

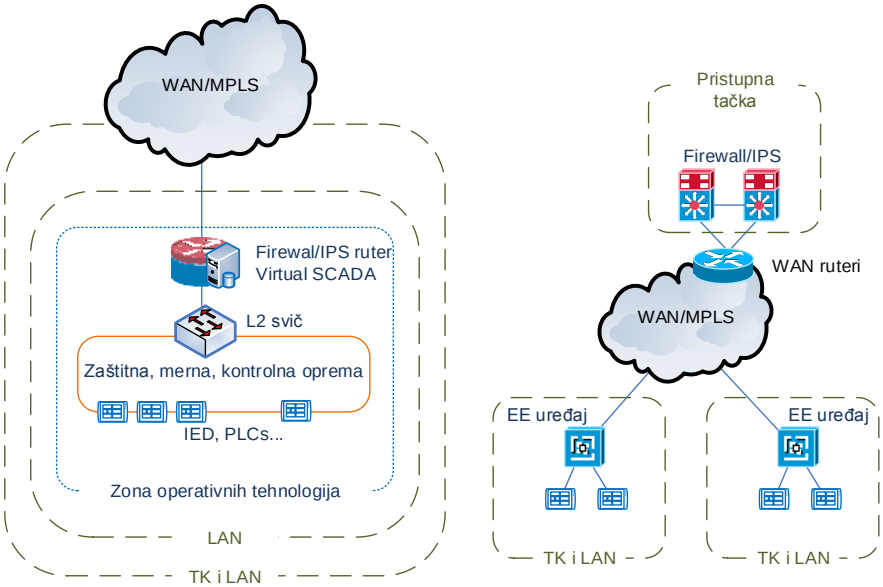
Prvi, najniži nivo segmentacije je nivo samih EEO a kao podvrste ovog nivoa predviđeno je četiri tipa EEO, razvrstano prema prioritetima od najvišeg do najnižeg. U tipu 1, sva oprema u EEO može se svrstati u jednu od tri grupe(zone). Zona Operativnih tehnologija je mesto gde se nalaze uređaji koji su usko vezani za funkcionisanje samog sistema nadzora i daljinskog upravljanja. U Multiservisnoj zoni se nalazi oprema potrebna za funkcionisanje servisa fizičkog obezbeđenja, alarma, kontrole pristupa kamera i servera za skladištenje obaveštenja. Poslednja zona je zona Kontrolne mreže u kojoj se nalaze lokalno upravljačko mesto (ako postoji) i telefonija. Komunikacija između zona je kontrolisana preko firewall uređaja koji su smešteni na sam ulaz u mrežu. Pored ove funkcije, firewall-i će biti zaduženi i za inspekciju saobraćaja kao i za slanje IDS podataka sistemu koji se nalazi u SOC-u.
S obzirom da postoje različiti EEO po svojoj veličini, značaju, nameni, načinu ostvarivanja TK veza izvršena je tipizacija rešenja u skladu sa vrstom EEO. Sama tipizacija rešenja omogućuje da se u praksi primeni jedan od navedenih modela, da se koriste uniformna i usvojena rešenja. Tako se smanjuju greške u implementaciji i na kraju smanjuju se mogućnosti napada na OT sistem.
OT LAN Tip 1 predstavlja složeno industrijsko okruženje koje obuhvata i OT i IT mrežne segmente, sa visokim zahtevima po pitanju dostupnosti, raspoloživosti i drugih bezbednosnih aspekata. Lokalna mreža OT sistema Tip 1 podrazumeva realizaciju visoko dostupne mrežne infrastukture koja obezbeđuje dovoljan broj i tip interfejsa za povezivanje krajnjih uređaja. Ovi objekti obično imaju redundatne veze prema centralnoj lokaciji i više desetina različitih uređaja u lokalnoj mreži.
OT LAN Tip 2 je segmentiran na isti način kao i Objekat Tip 1 samo pojedine komponente nisu realizovane u redundansi (bez crvenih elemenata na Slici 2.). Razlozi za ovo mogu biti od nivoa značaja objekta, nekih tehničkih ograničenja, nasleđene opreme do finansijskih razloga.



SLIKA 5. LOGIČKA ŠEMA VEZA OT LAN TIP 1 I TIP 2

OT LAN Tip 1 i OT LAN Tip 2 su primenjeni u realnim elektroenergetskim okruženjima. Sve VN EEO: TS 110/x, TS 35/x i pojedina razvodna postrojenja modifikujemo kako bismo njihove OT mreže usaglasili sa ovim modelima. Konkretno je tokom 2019. godine rešenje OT LAN Tip 1 primenjeno u 5 TS 110/x u Ogranku Kraljevo a tokom 2020. godine radi se proširenje na u Ograncima Kragujevac i Novi Sad na ukupno 15 TS 110/x.

OT LAN Tip 3 podrazumeva realizaciju jednostavne lokalne mrežne infrastukture koja obezbeđuje dovoljan broj i tip interfejsa za povezivanje krajnjih uređaja. Objekti Tip 3 imaju veze prema centralnoj lokaciji i nekoliko uređaja u lokalnoj mreži.
OT LAN Tip 4 – Objekti sa izmeštenom zaštitom podrazumeva realizaciju vrlo jednostavne lokalne mrežne infrastukture koja obezbeđuje dovoljan broj i tip interfejsa za povezivanje krajnjih uređaja. Objekti Tip 4 imaju veze prema centralnoj lokaciji i nekoliko ili često samo jedan uređaj u lokalnoj mreži.



SLIKA 6. LOGIČKA ŠEMA VEZA OT LAN TIP 3 I OBJEKAT TIP 4

OT LAN Tip 3 i OT LAN Tip 4 su primenjeni u realnim elektroenergetskim okruženjima. SN i NN EEO koji se uvode u sisteme daljinskog upravljanja upravo se realizuju na ovaj način. To su TS 20/0.4, TS 10/0.4, merno razvodna postrojenja, sekcioneri, reklozeri i slični EE uređaji.

ZAKLJUČAK

Umesto zaključka evo sedam preporuka koje bi trebalo primeniti da bi OT sistemi bili spremni za bezbednosne izazove:

1. Uložite u nadogradnju OT mreža.
   „Dobra vest“ je ta da su OT mreže vrlo često tehnološki stare i da minimalnim ulaganjima može se dosta poboljšati bezbednost ovih sistema.
2. Postavite teška pitanja i definišite odgovornost.
   Vrlo često postoje nerešena organizaciona pitanja. Vrlo je važno identifikovati ko je odgovoran za nadgledanje OT mreža. Bez odgovornosti nema ni bezbednosti.
3. Priznajte svoje nedostatke.
   Mnoge kompanije ne znaju šta ne znaju. Odsustvo dokaza nije isto što i dokaz o odsustvu zlonamernih aktera u OT mreži, to što neko ne vidi neke alarme ne znači da problema nema.
4. Proverite da li postoji segmentacija između vaših IT i OT mreža.
   Dobro razgraničavanje IT i OT mreža, postavljanje „crvenih linija“, su od suštinskog značaja.
5. Učinite OT mrežu vidljivom.
   IT timovima i administratorima potrebna je vidljivost OT mreže kako bi se implementirarli bezbednosi mehanizmi i nadzirala mreža. Ne možete se pravilno braniti ako nemate pristup opremi i uređajima.
6. Zaštita OT mreža nije jednokratna vežba.
   Razmislite strateški o tome kako i koliko često ažurirati i revidirati bezbednosne mehannizme, segmentaciju IT i OT mreža. Proverite da li su OT mreže deo plana upravljanja i reagovanja na eventualne incidente.
7. Edukujte rukovodioce o uticaju napada na OT mreže.
   Konačno, rukovodioci moraju da razumeju rizike poslovanja ako su OT mreže narušene i kako ovakvi napadi mogu da se propagiraju i kroz IT i kroz OT mreže. Edukujte ih tako da mogu obezbediti potrebne resurse za proaktivno upravljanje eventualnim incidentima.

LITERATURA

[1] Projekat IT bezbednosti SCADA sistema ODS, EPS Distibucija, – Faza 1, Beograd, Srbija, 2019.

[2] Projekat IT bezbednosti SCADA sistema ODS, EPS Distibucija, – Faza 2 – Predlog tehničkog rešenja Projekta IT bezbednosti SKADA sistema, Beograd, Srbija, 2019.

[3] Projekat IT bezbednosti SCADA sistema ODS, EPS Distibucija, – Faza 3 – Tehničko rešenje IT bezbednosti SKADA sistema Naručioca po tipskim trafo stanicama i vezama (idejni projekat), Beograd, Srbija, 2019.

[4] Tehničke preporuke visoko pouzdane LAN opreme EEO na konzumu ODS, EPS Distribucija, Beograd, Srbija, 2019.

[5] Horwitz L., OT networks and IT networks are closely intertwined, Cisco.com, RSA Conference 2018, San Francisco, USA, 2018.

[6] Odabrani energetski podaci za 2019. godinu, EPS Distribucija, Beograd, Srbija, 2020.