HRVATSKI OGRANAK MEĐUNARODNE
ELEKTRODISTRIBUCIJSKE KONFERENCIJE - HO CIRED
5. (11.) savjetovanje
Osijek, 15. - 18. svibnja 2016.

SO3 - 30

Marijan Petričec, mag. ing. rač.
Končar – Inženjering za energetiku i transport d.d.
marijan.petricec@koncar-ket.hr

Ante Previšić, dipl. ing.
Končar – Inženjering za energetiku i transport d.d.
ante.previsic@koncar-ket.hr

Zoran Budak, dipl. ing.
HEP ODS d.o.o. Elektroslavonija Osijek
zoran.budak@hep.hr

IMPLEMENTACIJA SIGURNOSNIH MEHANIZAMA U SUSTAVU UPRAVLJANJA DCV ELEKTRA ZAGREB I ELEKTROSLAVONIJA OSIJEK

SAŽETAK

Nadogradnjom SCADA (Supervisory Control And Data Acquisition) sustava u DCV Elektra Zagreb i Elektroslavonija Osijek implementiran je središnji upravljački mehanizam za kontrolu korisnika, računala i pristup istima. Jedna od glavnih značajki sustava je korištenje Kerberos protokola za autentifikaciju mrežne komunikacije na temelju sigurnosnih kartica. Isto tako implementirani su mrežni sigurnosni mehanizmi u vidu podjele mreže na logičke segmente, te domenski sigurnosni mehanizmi u vidu grupnih politika koji objedinjuju korisnike i računala na Windows platformama. Na Linux poslužiteljima implementirani su sigurnosni mehanizmi u vidu vatrozid pravila, te kontrole portova i servisa.

Ključne riječi: SCADA, Elektra Zagreb, Elektroslavonija Osijek, nadogradnja, Kerberos

SECURITY CONTROL IMPLEMENTATION IN DCV ELEKTRA ZAGREB AND ELEKTROSLAVONIJA OSIJEK

SUMMARY

With the upgrade of the SCADA system in DCV Elektra Zagreb and Elektroslavonija Osijek came the implementation of a central management system for user access control and computers access control. One of the main characteristics of the system is the Kerberos protocol for authentication of network communication based on security tickets. Also network security systems are implemented providing network distribution through logical segments and domain security controls based on group policies which include users and computers on Windows operating systems. Linux servers have security controls implemented based on firewall rules and control of ports and services.

Key words: SCADA, Elektra Zagreb, Elektroslavonija Osijek, upgrade, Kerberos

1. UVOD

Elektroslavonija Osijek s površinom od 4.152 četvorna kilometra je četvrta prema veličini u HEP Operatoru distribucijskog sustava. Njezinih 766 radnika skrbi o 153.236 kupca električne energije. Organizirana je u šest pogona i šest službi.

Na području Elektroslavonije Osijek izgrađeno je 7.453 kilometara mreža i vodova, sedam trafostanica 110/35(30) kV, tri trafostanice 110/10(20) kV, 25 trafostanica 35(30)/10 kV i 1.486 trafostanica 10/04 kV. Svojim kupcima tijekom 2011. godine prodali su 929.046.000 kWh, maksimalno vršno opterećenje je iznosilo 176 MW, a gubici električne energije iznosili su 9,14 %.

Područje Elektre Zagreb ima posebnu odgovornost u HEP Operatoru distribucijskog sustava, jer električnom energijom opskrbljuje i glavni grad Hrvatske – političko, administracijsko, kulturno i gospodarsko središte Republike Hrvatske.

Elektra Zagreb prostire se na površini od 2.550 četvornih kilometara, a o opskrbi kupaca električnom energijom, osim Pogona u sjedištu Zagreb, brinu i pogoni u Sv. Ivanu Zelina, Samoboru, Velikoj Gorici, Zaprešiću, Dugom Selu te Svetoj Klari.

Elektra Zagreb skrbi o skoro četvrtini kupaca HEP-a, odnosno o skoro pola milijuna kupaca. Vršno opterećenje je 723 MW, a godišnja potrošnja električne energije iznosi 3.772.784 MWh.

Elektra Zagreb upravlja s brojim elektroenergetskim postrojenjima, primjerice:

- 34 kilometra 110 kV zračnih dalekovoda i 6,2 kilometara 110 kV kabelskih vodova,
- 5 TS 110/30 (35) kV i 14 TS 110/10 (20) kV,
- 22 TS 35(30)/10 (20) kV i 867 TS 20/04 kV te
- 3215 TS 10(20)/04 kV i pripadnim vodovima.

Implementaciji sigurnosnih mehanizama pristupilo se zbog sljedećih razloga:

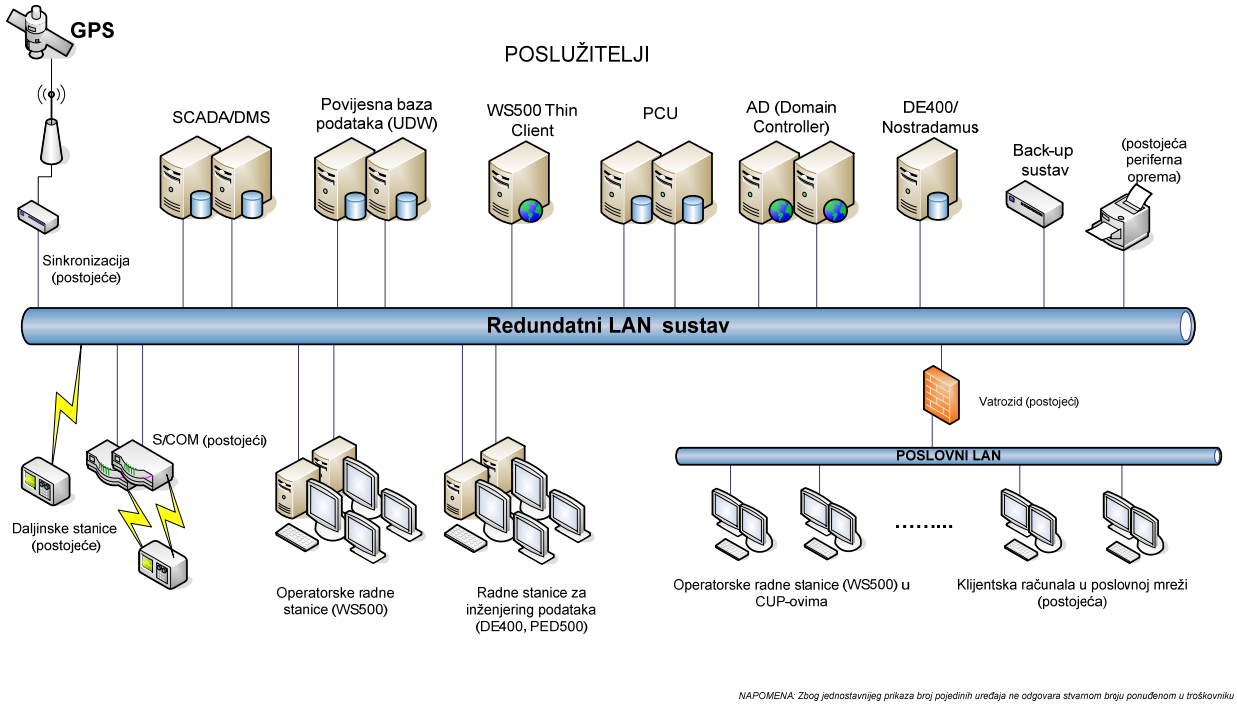
- povećan broj korisnika koji pristupa sustavu,
- povećana kompleksnost sustava upravljanja (broj komponenti sustava upravljanja iz dana u dan raste),
- sve veći broj veza prema sustavu upravljanja od raznih korisnika/aplikacija,
- nova verzija SCADA sustava zahtjeva sigurnosne postavke,
- podizanje razine sigurnosti u sustavima,
- lakša i jednostavnija analiza neočekivanih događaja u sustavu,
- jednostavnija administracija sustava.

2. KONFIGURACIJA SCADA/DMS SUSTAVA

Konfiguracija SCADA/DMS (Distribution management system) sustava se zasniva na poslužitelj/klijent modelu odnosno na distribuiranom modelu sklopovske i programske opreme, uključujući i procesnu bazu podataka. SCADA/DMS sustav se sastoji od sljedećih funkcionalnih komponenata:

- poslužitelji pojedinih procesnih cjelina,
- poslužitelji za realizaciju pojedinih funkcija vođenja EE (Elektroenergetskog) sustava,
- lokalna mreža SCADA/DMS sustava,
- sustav za sigurnost podataka,
- povezivanje s postojećim vanjskim informatičkim sustavima,
- povezivanje na postojeći komunikacijski podsustav,
- način nadzora i upravljanja SCADA/DMS sustavom,
- radne stanice,
- periferna oprema.

Logička shema SCADA/DMS sustava na kojoj se vide pojedine poslužiteljske komponente prikazana je na slici ispod.



Slika 1. Konfiguracija SCADA/DMS sustava

3. MREŽNA ARHITEKTURA SUSTAVA

Mrežna arhitektura procesnog sustava realizirana je kao zasebna cjelina korištenjem suvremenih mrežnih tehnologija, VLAN (Virtual Local Area Network), VRF (Virtual Routing and Forwarding) i GRE (Generic Routing Encapsulation).

Sustav je podijeljen u logičke grupe računala sa pripadajućim VLAN-ovima na sljedeći način:

- AD (Aktivni Direktorij) serveri: VLAN1,
- SCADA serveri: VLAN2,
- UDW (Utility Data Warehouse) serveri: VLAN3,
- PCU (Process Communication Unit) serveri: VLAN4,
- DE (Data Engineering) server i Nostradamus: VLAN5,
- WEB server: VLAN6,
- Operaterske radne stanice: VLAN7,
- Inženjerske radne stanice: VLAN8.

Što omogućava podjelu mreže na zone različitih razina sigurnosti. U zoni najveće sigurnosti nalaze se AD poslužitelji, SCADA poslužitelji, PCU poslužitelji i operatorske radne stanice (budući da su ova računala od kritične važnosti za vođenje elektroenergetskog sustava). U zoni srednje sigurnosti nalaze se UDW poslužitelji, DE poslužitelj i Nostradamus poslužitelj zajedno sa inženjerskim radnim stanicama. I još ostaje WEB poslužitelj prema kojemu je omogućen pristup vanjskim korisnicima iz nezaštićenih zona te se isti nalazi u tzv. demilitariziranoj zoni.

Sklopovska oprema se sastoji od 2 složena layer 2 preklopnika zbog osiguranja redudantnosti i jednog usmjernika. Na usmjerniku se koristi jedan port („router on a stick“). Sva pravila pristupa definiraju se na lokalnom vatrozidu.

4. SIGURNOST KOMUNIKACIJSKIH PROTOKOLA

SCADA/DMS sustav ima implementirane sve potrebne sigurnosne mjere za komunikacijske protokole daljinskog upravljanja. IEC 60870-5-104 i ICCP (Inter-Control Center Communications Protocol) komunikacijski protokoli su osigurani korištenjem preporuka iz IEC 62351 standarda.

Sigurnost navedenih protokola je u skladu s preporukama:

- IEC 62351-3: Data and Communication Security – Profiles Including TCP/IP (ovi sigurnosni standardi pokrivaju profile korištene od ICCP, IEC 60870-5 Part 104, DNP 3.0 over TCP/IP, i IEC 61850 over TCP/IP).
- IEC 62351-4: Data and Communication Security – Profiles Including MMS (ovi sigurnosni standardi pokrivaju profile korištene od ICCP i IEC 61850).
- IEC 62351-5: Data and Communication Security – Security for IEC 60870-5 and Derivatives (i.e. DNP 3.0) (ovi sigurnosni standardi pokrivaju i serijske i mrežne profile korištene u IEC 60870-5 i DNP).

IEC 62351-6: Data and Communication Security – Security for IEC 61850 Peer-to-Peer Profiles (ovi sigurnosni standardi pokrivaju profile korištene u IEC 61850 koji nisu bazirani na TCP/IP).

5. UPRAVLJANJE SIGURNOSNIM MEHANIZMIMA

Središnji sustav za upravljanje sigurnosnim postavkama se sastoji od središnjeg sustava za upravljanje korisničkim računima baziranog na LDAP-u (LightWeight Directory Access Protocol). Sigurnosne i mrežne postavke komunikacijskih centara distribucijskog područja također su nadzirane. Komunikacijski centri na razini distribucijskog područja imaju mogućnost da automatski obave operacije za svoje područje u slučaju prekinutih veza sa središnjim sustavom. Sustav se sastoji od lokalnog sustava za upravljanje računima korisnika baziranog na LDAP-u (Aktivni direktorij).

5.1. AD POSLUŽITELJI

Sve aplikacije ponuđenog SCADA/DMS sustava, uključujući SCADA, DMS podržavaju LDAP tehnologiju te se i autorizacija pojedinačnih korisnika odvija preko središnjeg sustava za upravljanje korisničkim računima. AD sustav omogućava jedinstveno mjesto pristupa (eng. single sign-on - SSO) tako da je korištenje RBAC (Role-Based Access Control) sustava kontrole pristupa baziranog na ulogama ekvivalentan direktnom pristupu.

U sustavu postoje 2 AD (domenska) poslužitelja koji rade u dualnom načinu rada. Sinkronizacija među njima se odvija automatski, tako da se radovi na jednom automatski repliciraju na drugi.

5.2. GRUPNE POLITIKE

Grupne politike su skup pravila konfiguracije korisnika i/ili računala. Korištenjem grupnih pravila uvode se mjere zabrane pregleda pojedinih resursa operativnih sustava, mrežnih resursa, te vanjskih jedinica koje se administriraju na jednom centralnom mjestu.

Na sustavima Elektre Zagreb i Elektroslavonije Osijek implementirane su sljedeće grupne politike:

- instalacija programa gdje se na određena računala, prilikom pokretanja sustava, automatski instaliraju programi predviđeni za rad pojedinih korisnika istih računala. Instalacijski programi dijele se na:
    - programe trećih proizvođača (7-zip, putty, itd…)
    - programe za HMI (Human Machine Interface) sučelje SCADA/DMS sustava.

Grupne politike za instalaciju programa koriste se za instalaciju operatorskih i inženjerskih radnih stanica.

- restrikcija korištenja vanjskih jedinica pohrane podataka (floppy, USB, CD-ROM). Politika obuhvaća cijelu domenu, što znači da svako računalo koje pripada domeni ima onemogućeno korištenje vanjskih jedinica pohrane podataka; navedena grupna politika osigurava sustav od neželjenog prijenosa virusa i ostalog opasnog sadržaja preko vanjskih jedinica
- zabrana vidljivosti i korištenja upravljačke ploče i pripadajućih servisa određenoj grupi korisnika. Politika je instalirana na razini cijele domene, ali su isključenje grupe Administratora i Glavnih Sistem Inženjera; navedena grupna politika osigurava sustav od neželjnih promjena postavki i instalacije/deinstalacije aplikacija koje su neophodne za ispravan rad sustava
- zabrana lokalnog spajanja određenoj grupi korisnika; ova grupna politika osigurava sustav od neovlaštenog pristupa pojedinim resursima

Navedene grupne politike pridjeljuju se organizacijskim jedinicama koje mogu sadržavati računala, korisnike ili kombinaciju istih dok se još finija podjela dobiva korištenjem grupa. Pred definirane grupe korisnika i računala date su u sljedećem pod poglavlju.

5.2.1. GRUPE KORISNIKA I RAČUNALA

Sa stanovišta sigurnosti korisnici su podijeljeni u grupe visoke, srednje i niske sigurnosti. U grupu visoke sigurnosti pripadaju WEB korisnici kojima je omogućen pristup isključivo WEB poslužitelju i niti jednom drugom resursu sustava. U grupu srednje sigurnosti pripadaju VN operateri, SN operateri i CUP korisnici (koji su također operateri), dok grupi niske sigurnosti pripadaju Administratori i Sistem Inženjeri kojima je dozvoljen pristup svim računalima kao i administracija istih. Detaljna razrada grupa i dozvola koje pripadaju istima dana je ispod:

- Administratori - članovi grupe imaju prava pristupa svim računalima u sustavu, bilo lokalno ili daljinski. Nisu u mogućnosti koristiti vanjske jedinice (floppy, USB, CD-ROM). Vidljiva je upravljačka ploča, što ujedno omogućava administraciju i instalaciju novih programa, kao i deinstalaciju istih,
- Glavni sistem inženjeri - članovi grupe imaju prava pristupa svim računalima u sustavu, bilo lokalno ili daljinski, osim AD poslužiteljima, gdje se mogu spojiti daljinski. Nisu u mogućnosti koristiti vanjske jedinice (floppy, USB, CD-ROM). Vidljiva je upravljačka ploča, što ujedno omogućava instalaciju novih programa, kao i deinstalaciju istih,
- Sistem inženjeri - članovi grupe imaju prava pristupa radnim stanicama u sustavu, bilo lokalno ili daljinski i WEB serveru daljinski. Nisu u mogućnosti koristiti vanjske jedinice (floppy, USB, CD-ROM). Nije im vidljiva upravljačka ploča, što ujedno onemogućava administraciju računala i instalaciju novih programa, kao i deinstalaciju istih,
- VN operateri - članovi grupe imaju prava pristupa operatorskim radnim stanicama bilo lokalno i daljinski, te WEB serveru daljinski. Nisu u mogućnosti koristiti vanjske jedinice (floppy, USB, CD-ROM). Nije im vidljiva upravljačka ploča, što ujedno onemogućava instalaciju novih programa, kao i deinstalaciju istih,
- SN operateri - članovi grupe imaju prava pristupa operatorskim radnim stanicama lokalno i daljinski, te WEB serveru daljinski. Nisu u mogućnosti koristiti vanjske jedinice (floppy, USB, CD-ROM). Nije im vidljiva upravljačka ploča, što ujedno onemogućava administraciju računala i instalaciju novih programa, kao i deinstalaciju istih,
- Web korisnici - članovi grupe imaju prava pristupa WEB serveru samo daljinski. Nisu u mogućnosti koristiti vanjske jedinice (floppy, USB, CD-ROM). Nije im vidljiva upravljačka ploča, što ujedno onemogućava administraciju računala i instalaciju novih programa, kao i deinstalaciju istih,
- CUP korisnici - članovi grupe imaju prava pristupa pripadajućim CUP radnim stanicama samo lokalno. Nisu u mogućnosti koristiti vanjske jedinice (floppy, USB, CD-ROM). Nije im vidljiva upravljačka ploča, što ujedno onemogućava administraciju računala i instalaciju novih programa, kao i deinstalaciju istih.

Sa stanovišta sigurnosti i računala su podijeljena u grupe visoke, srednje i niske sigurnosti. U grupu visoke sigurnosti pripadaju svi poslužitelji osim WEB poslužitelja. Računalima u zoni visoke sigurnosti dozvoljen je pristup samo administratorima i sistem inženjerima. U grupu srednje sigurnosti pripadaju operatorske radne stanice i CUP daljinske stanice. Na njima je dozvoljen pristup operatorima, administratorima i sistem inženjerima. U zonu niske sigurnosti pripada WEB poslužitelj. Na WEB poslužitelju je dozvoljen daljinski pristup praktički svim korisnicima. Detaljnija podjela računala prema grupama dana je u sljedećoj listi:

- SCADA poslužitelji – glavni aplikacijski poslužitelji na Linux OS-u u zoni visoke sigurnosti; pristup je dozovljen samo administratorima
- Domenski kontroleri– središnji sustavi za upravljanje sustavom u zoni visoke sigurnosti; pristup je dozovljen samo administratorima,
- Thin client – računalo namijenjena udaljenom pristupu u zoni niske sigurnosti,
- DE poslužitelj – računalo sa Oracle bazom podataka gdje se nalazi alat DE400 dizajniran za efikasno modeliranje, unos i kasnije održavanje podataka u zoni visoke sigurnosti,
- Nostradamus poslužitelj – računalo sa sustavom baziranim na neuronskim mrežama za kratkoročno predviđanje opterećenja u zoni visoke sigurnosti,
- PCU poslužitelji – računala koja se koriste za povezivanje SCADA poslužitelja sa daljinskim stanicama u zoni visoke sigurnosti,
- UDW poslužitelji – računala za spremanje povijesnih podataka podataka, na Linux OS-u u zoni visoke sigurnosti,
- Operatorske radne stanice – pristup svim aplikacijama sustava u zoni srednje sigurnosti,
- Inženjerske radne stanice – pristup svim aplikacijama sustava u zoni srednje sigurnosti,
- CUP – daljinske radne stanice u zoni srednje sigurnosti.

6. UPRAVLJANJE KORISNIČKIM RAČUNIMA

Upravljanje korisničkim računima implementirano je na bazi Aktivnog direktorija na Windows Server 2008 R2 operativnom sustavu. Sustav za upravljanje korisničkim računima pruža sljedeće usluge:

- Autorizaciju,
- Autentifikaciju,
- Sigurnost temeljenu na ulogama.

Sustav za upravljanje računima korisnika uključuje:

- identificiranje tipova računa (npr., individualni , ili sustav),
- dodjeljivanje pripadnih autorizacija.

SCADA/DMS sustav omogućava upravljanje lozinkama korisničkih računa, uključujući:

- odabir duljine lozinke,
- učestalosti promjene,
- postavljanje traženog nivoa kompleksnosti lozinke,
- broj pokušaja spajanja,
- prekidanje neaktivnih sesija,
- zaključavanje ekrana aplikacija,
- sprečavanje uzastopnog korištenja iste lozinke.

Sve navedene postavke usuglašene su sa korisnicima sustava prilikom implementacije istih.

7. KERBEROS PROTOKOL

Siguran, single-sign-on autentikacijski protokol koji izdaje korisnicima „kartice“ koje vrijede 24 sata. Single-sign-on je moguć jer sve aplikacije u sustavu vjeruju centralnom autentikacijskom entitetu (KDC – Key Distribution Center) koji se nalazi na Aktivnom direktoriju.

Sigurna autentikacija Kerberos protokola je dopunjena korištenjem GSSAPI/SSPI (Generic Security Services API/ Security Support Provider Interface) za osiguranje enkripcije/integriteta cjelokupne komunikacije između računala. Komunikacija koja ne koristi Kerberos protokol, kao prijenos podataka, odvija se preko SSL/TLS (Transport Layer Security/Secure Sockets Layer) ili IPSec (Internet Protocol Security) protokola.

Korištenjem Kerberos protokola pojednostavljena je autentikacija korisnika, koji se jednim prijavljivanjem autenticiraju, umjesto da se prijavljuju na svaku aplikaciju posebno.

.

8. SIGURNOSNO REDUCIRANJE

Sigurnosno reduciranje nad računalima je kompleksan i složen proces i prilikom implementacije potreban je biti vrlo pažljiv jer krivim postavkama može doći do degradacije funkcionalnosti sustava. Sigurnosno reduciranje se sastoji od postavljanja dozvoljenih portova u postavkama vatrozida na računalima te gašenjem svih servisa osim onih koji su neophodni za ispravan rad sustava (u oba slučaja radi su o tzv. white listing-u). Tako se, na primjer, na SCADA poslužiteljima gase svi servisi koji nisu neophodni za ispravan rad SCADA aplikacija dok se na PCU poslužiteljima koji služe za komunikaciju prema daljinskim stanicama gase svi servisi osim onih neophodnih za komunikaciju sa daljinskim stanicama i SCADA poslužiteljima. Sve postavke sigurnosnog reduciranja sustava napravljene su prema preporukama proizvođača softvera.

9. SIGURNOSNI ZAPISI (AUDIT TRAIL)

U sustavu su implementirani sigurnosni zapisi na više mjesta. Prvo mjesto su Linux poslužitelji i sigurnosni zapisi na Linux poslužiteljima sastoje se od zapisa vezanih na sam operacijski sustav te zapisa vezanih na SCADA/DMS aplikacije. Što se tiče SCADA/DMS aplikacija bilježe se sve neovlaštene akcije za sve definirane operacije u sustavu. Tako se, na primjer, bilježi svaka neovlaštena komanda (kada operater pokušava poslati komandu na objekt za koji nema nadležnost) i svaki neovlašteni pokušaj otvaranja izvještaja sa prikazom bilo povijesnih bilo podataka u stvarnom vremenu. Bitno je napomenuti da je sustav moguće konfigurirati da se bilježe i sve ovlaštene akcije, ili samo dio njih, u slučaju da se za to ukaže potreba. Osim akcija vezanih na SCADA/DMS aplikacije na Linux poslužiteljima bilježi se i svaka prijava/odjava sa sustava, bilo ovlaštene ili pokušaj neovlaštene, te sva komunikacija između poslužitelja i drugih računala. Drugo mjesto na kojemu se nalaze sigurnosni zapisi su zapisi događaja na Windows mašinama koji se sastoje od događaja vezanih na aplikacije, događaja vezanih na sigurnost, događaja vezanih na postavke sustava te sistemski i proslijeđenih događaja. U navedenim zapisima nalaze se događaji vezani na pokretanje/zaustavljanje servisa na računalu, instalaciji/deinstalacije aplikacija, primjeni grupnih politika, prijavama/odjava sa sustava, itd…. Treće mjesto na kojima se nalaze sigurnosni zapisi su AD poslužitelji na kojima se nalaze zapisi za cijelu domenu, a najbitniji događaji vezani su na prijave/odjave na Windows poslužitelje. Sve navedeno omogućava da administratori sustava na brz i jednostavan način provjere trenutno stanje sustava kao i da naprave analize povijesnih događaja.

10. ZAKLJUČAK

U radu je dan opis implementacije središnjih upravljačkih mehanizama kontrole korisnika i računala te pristupa SCADA sustavima u DCV Elektra Zagreb i Elektroslavonija Osijek. Kao glavna značajka je opisan način autentifikacije korištenjem Kerberos protokola te korištenje središnjeg upravljačkog mehanizma u vidu Aktivnog direktorija. Opisana je i podjela sustava na mrežne logičke cjeline te podjela korisnika i računala radi lakšeg upravljanja SCADA sustavom.

Bitno je naglasiti kako je implementacija AD poslužitelja u velikoj mjeri olakšala nadzor i administraciju cjelokupnog sustava dok je implementacija sigurnosnih mehanizama podigla razinu sigurnosti istog s obzirom na postojeći sustav i stari SCADA/DMS sustav. Zbog svega navedenog, implementirani SCADA/DMS sustav doveo je do podizanja kvalitete svakodnevnog vođenja elektroenergetske mreže distributivnog područja Elektre Zagreb i Elektroslavonije Osijek.

11. LITERATURA

[1] dostupno na poveznici: http://www.hep.hr/ods/dp/osijek/

[2] dostupno na poveznici: http://www.hep.hr/ods/dp/zagreb/

[3] ABB: Function Description – Cyber Security, Release NM6.1, 1KSE001239 Rev. B, November 2013

[4] ABB: Implementation Manual – Cyber Security Installation Guide, Release NM6.4, 1KSE001240 Rev. D, November 2014

[5] Končar-KET d.d.: Nadogradnja SCADA sustava u dispečerskim centrima Elektre Zagreb i Elektroslavonije Osijek, Izjava o radovima, 8340-25-14-0045, 2014.