POZIV NA SEMINAR

HRVATSKOG OGRANKA
MEĐUNARODNE ELEKTRODISTRIBUCIJSKE KONFERENCIJE
i
HRVATSKE KOMORE INŽENJERA ELEKTROTEHNIKE

DIGITALIZACIJA ELEKTROENERGETSKOG SEKTORA I IZAZOVI KIBERNETIČKE SIGURNOSTI

Zagreb, 21. ožujka 2019.

Velika dvorana HEP d.d.
Ulica grada Vukovara 37/ VII, Zagreb

Ožujak, 2019.

Međunarodna elektrodistribucijska konferencija CIRED (akronim od Congrès International des Réseaux Electriques de Distribution; International Conference on Electricity Distribution) je udruga koja okuplja zainteresirane u području elektrodistribucijske djelatnosti: najširi krug stručnjaka iz distribucijskih poduzeća, iz instituta i fakulteta, proizvođače opreme i davatelje usluga, opskrbljivače i potrošače, regulatore. Cilj je CIRED-a, prema Statutu, povećanje stručne kompetencije i sposobnosti, umijeća i znanja, u najširem području elektroprivredne djelatnosti.

Jedan od načina širenja i produbljivanja stručne kompetencije su savjetovanja, tematski seminari, radionice i skupovi. S tim ciljem Hrvatski ogranak Međunarodne elektrodistribucijske konferencije (HO CIRED) organizira ─ u zajednici s Hrvatskom komorom inženjera elektrotehnike (HKIE) ─ seminar:

DIGITALIZACIJA ELEKTROENERGETSKOG SEKTORA I
IZAZOVI KIBERNETIČKE SIGURNOSTI

Sektor energetike pa tako i elektroenergetski sektor prolazi kroz proces značajnih promjena. Obnovljivi izvori energije, decentralizacija proizvodnje, sve složenije značajke sastavnica i pogona mreže, razvoj tržišta, predstavljaju izazove s kojima se elektoenergetski sektor suočava.
Digitalizacija elektroenergetskog sektora sposoban je odgovor mnogim izazovima koje nam promjene elektroenergetskog sustava donose. Upravo zbog toga elektroenergetsko gospodarstvo će bi ti značajan korisnik digitalizacije, ali i njezin pokretač.

S druge strane, digitalizacija elektroenergetskog sektora i korištenje naprednih tehnologija u poslovnim procesima otvaraju pitanje sigurnosti sustava, posebno u domeni informacijske i kibernetičke sigurnosti. Hrvatski sabor je na sjednici održanoj 6. srpnja 2018.g. donio Zakon o kibernetičkoj sigurnosti ključnih usluga i davatelja digitalnih usluga, kojemu je cilj osigurati visoku razinu kibernetičke sigurnosti u pružanju usluga koje su od posebne važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti. Na temelju istog Zakona donesena je i Uredba o kibernetičkoj sigurnosti ključnih usluga i davatelja digitalnih usluga kojom se utvrđuju mjere za postizanje visoke razine kibernetičke sigurnosti operatora ključnih usluga, način njihove provedbe, kriteriji za određivanje incidenata koji imaju znatan učinak na pružanje ključnih usluga, sadržaj obavijesti i druga bitna pitanja za obavješćivanje o incidentima.
Koje izazove u području sigurnosti elektroenergetskog sektora donosi njegova digitalizacija? Kako osigurati visoku razinu kibernetičke sigurnosti, a pri tome omogućiti snažnu digitalizaciju elektroenergetskog sustava i korištenje naprednih mreža? Samo su neka od pitanja na koja će se kroz Seminar o digitalizaciji elektroenergetskog sektora i izazova kibernetičke sigurnosti potražiti odgovori.

Sadržaj Seminara

Pozdravna riječ organizatora i uvod Voditelja seminara

Tema 1:

ELEKTROENERGETSKI SEKTOR U SVIJETLU DIGITALIZACIJE
Ivan Periša, dipl.ing., HEP-Operator distribucijskog sustava d.o.o.

Digitalizacija elektroenergetskog gospodarstva odgovor je mnogim izazovima koje nam promjene EES-a donose. Upravo zbog toga elektroenergetsko gospodarstvo će bi ti značajan korisnik digitalizacije, ali i njezin pokretač. Opredjeljenjem društva za čistom energijom, svijet elektroenergetike ušao je procese promjena. Zaokret prema proizvodnji energije iz obnovljivih izvora energije dovesti će do značajnih promjena u funkcioniranju EES-a. Elektroenergetski sustav od centraliziranog postaje decentraliziran, a elektroenergetska mreža, posebno na razini distribucije, od pasivne postaje aktivna. Sposoban odgovor na glavni izazov/pitanje kako osigurati pouzdanu opskrbu u mreži sa složenim značajkama sastavnica i pogona mogu dati upravo napredne tehnologije u naprednim (distribucijskim) digitaliziranim mrežama.

Tema 2:

KIBERNETIČKA SIGURNOST KAO TEMELJ DIGITALNE TRANSFORMACIJE GOSPODARSTVA

Mario Posavec, dipl. ing., Zavod za sigurnost informacijskih sustava

Digitalna transformacija -> Industrija 4.0
Kibernetička sigurnost u RH
Uloga državnih tijela
Uloga sektorskih nositelja
EU Direktiva o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava 2016/1148 i specifičnosti transpozicije u zakonodavni okvir RH
Trendovi sigurnosne politike u RH

Tema 3:

ZAKON I UREDBA O KIBERNETIČKOJ SIGURNOSTI KLJUČNIH USLUGA I DAVATELJA DIGITALNIH USLUGA

Goran Piškor, dipl. ing., HEP-Operator distribucijskog sustava d.o.o.

Cilj Zakona je osigurati visoku razinu kibernetičke sigurnosti u pružanju usluga koje su od posebne važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti. Zakonom se uređuju postupci i mjere za postizanje tog cilja, nadležnosti i ovlasti nadležnih sektorskih tijela, jedinstvene nacionalne kontaktne točke, tijela nadležnih za prevenciju i zaštitu od incidenata i tehničkog tijela za ocjenu sukladnosti, nadzor provedbe i prekršajne odredbe.

Zakonom i prilozima je definiran identifikacijski postupak operatora ključnih usluga. Ukoliko subjekt pruža neku od identificiranih usluga i udovoljava određenim kriterijima, proglašava se operatorom ključnih usluga.

Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga donesena temeljem Zakona detaljno definira mjere za postizanje visoke razine kibernetičke sigurnosti operatora ključnih usluga (upravljanje sigurnošću mrežnih i informacijskih sustava, upravljanje rizicima, područja zaštite ključnih sustava) i obavezno izvješćivanje o incidentima.

Sektori obuhvaćeni Zakonom su energetika (električna energija, nafta, plin), prijevoz (zračni, željeznički, vodni, cestovni), bankarstvo, infrastrukture financijskog tržišta, zdravstveni sektor, opskrba vodom za piće i njezina distribucija, digitalna infrastruktura, digitalne usluge te poslovne usluge za državna tijela. U skladu s navedenim kriterijima i pragovima, između ostalih, HEP ODS d.o.o je proglašen operatorom ključnih usluga.

Tema 4

Tema 4.1

KIBERNETIČKA SIGURNOST ELEKTROENERGETSKOG SUSTAVA I ULOGA REGULATORA

Marko Poljak, dipl.ing., Hrvatska energetska regulatorna agencija

Korištenje naprednih informacijskih tehnoloških rješenja u elektroenergetskom sustavu otvara prostor brojnim poboljšanjima u vođenju, fleksibilnosti, učinkovitosti, sigurnosti i mjerenju. Napredna mreža i napredna brojila su pojmovi koji se sve češće koriste u izražavanju o budućnosti elektroenergetskog sustava te su na razini EU jedni od glavnih ciljeva u njegovom razvoju. Međutim, sa svim poboljšanjima dolazi i opasnost zlonamjernog iskorištavanja tehnologije u svrhu ostvarenja zarade ili druge koristi pojedinca ili grupe. Odgovoriti će se na pitanja uloge i odgovornosti pojedinih sudionika s naglaskom na ulogu regulatora.

Tema 4.2

KIBERNETIČKA SIGURNOST U RADIO-KOMUNIKACIJSKIM SUSTAVIMA

Rok Strlic, dipl.ing., Motorola Solutions Inc.

Prezentirat će sigurnosne značajke koje implementira kod dizajna radio-komunikacijskih sustava.
Koji su najvažniji sigurnosni izazovi u korištenju radio-komunikacijskih sustava?

Kako se nositi sa svakodnevno promjenjivim i rastućim kibernetičkim prijetnjama?
Zašto evoluirati od pristupa zadovoljavanja regulatornih propisa prema strategiji baziranoj na riziku?
Koje funkcionalnosti ugrađene u TETRA DIMETRA X-Core sustav pomažu korisnicima nositi se sa pitanjima kibernetičke sigurnosti?

Tema 5

Tema 5.1

SIGURNOSNO-TEHNIČKI ASPEKTI ZAKONA O KIBERNETIČKOJ SIGURNOSTI OPERATORA KLJUČNIH USLUGA I DAVATELJA DIGITALNIH USLUGA U ELEKTROENERGETSKIM SUSTAVIMA

Jure Šimundić, dipl.ing., CS – Computer Systems d.o.o.

Procesima informatizacije i umrežavanja, procesna okruženja postupno su se otvorila i povezala s drugim vanjskim procesnim sustavima, poslovnom mrežom i u konačnici s Internetom. Takva otvorenost svakako je olakšala poslovnu djelatnost, ali je ujedno sa sobom donijela i određene IT sigurnosne probleme- prijetnje, ranjivosti i rizike, koji su učinili takva okruženja podložnima sigurnosnoj kompromitaciji i eksploataciji. Stupanjem na snagu Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, procesna okruženja našla su se pred novim izazovima koji uključuju zahtjeve za sustavnijim izmjenama i nadogradnjama postojeće IT infrastrukture. Namjena je ove prezentacije osloviti određene članke Zakona u kontekstu elektroenergetskih okruženja i pružiti primjere tehničkih rješenja, najbolje prakse i načina kako postići sukladnost s njima.

Tema 5.2

PRIMJENA KIBERNETIČKIH INDUSTRIJSKIH NORMI – KLJUČ UPRAVLJANJA SIGURNOŠĆU AUTOMATIZIRANIH POSTROJENJA U ELEKTROENERGETSKOM SUSTAVU?

dr.sc. Stjepan Sučić, KONČAR - Inženjering za energetiku i transport d.d.

Kibernetička sigurnost kritične infrastrukture izravno je vezana uz načine upravljanja i zaštite automatiziranih postrojenja i primjenu načela informacijske sigurnosti na aplikacije namijenjene daljinskom vođenju elektroenergetskog sustava. Primjena otvorenih tehnologija i njihovo korištenje u sustavima daljinskog nadzora i upravljanja omogućila je značajne iskorake u stvaranju novih tehnoloških rješenja za potrebe automatizacije ali ujedno ukazala i na kibernetičke ranjivosti sustava nastale nesustavnom primjenom istih tehnologija. Kako bi stvorili funkcionalni okviri djelovanja namijenjeni razvoju informacijski sigurnih rješenja za automatizaciju postrojenja normizacijska tijela su odredila nekoliko normi namijenjenih rješavanju navedenog izazova. U predavanju su predstavljene ključne standardizacijske aktivnosti na normama kibernetičke sigurnosti i kako ih primijeniti u postojećim i novim sustavima.

Tema 5.3

KIBERNETIČKA SIGURNOST U DIGITALNOJ TRAFOSTANICI

Mario Valčić, dipl.ing., Josip Tošić, dipl.ing.; Siemens d.d.

Danas postoji realna opasnost od „hakiranja“ sustava upravljanja transformatorskom stanicom, što se događa na svim stranama svijeta. Napredni sustavi daljinskog nadzora i upravljanja postaju meta za napade hakerima, interesnim skupinama, istraživačima, profesionalcima koji na bilo koje načine mogu koristi potpuni nestanak napona unutar jedne regije, države ili kontinenta.

Kako bi se spriječili ovakvi neželjeni upadi sigurnost sustava mora biti na visokoj razini, jer sustav je ranjiv onoliko koliko je ranjiva njegova najslabija točka. U ovoj prezentacija pokazati ćemo najnovije tehnologije Siemens-a iz područja kibernetičke sigurnosti u digitalnim trafostanicama.

Tema 5.4

CYBERSECURITY I ZAŠTITA PODATAKA – PRILIKA ILI PRIJETNJA DIGITALNE TRANSFORMACIJE

Ivan Paić, dipl.ing., Schneider Electric d.o.o.

Digitalna transformacija je jedan od glavnih pojmova u gospodarstvu koji svakodnevno pratimo u medijima. Mnogo se pažnje posvećuje benefitima koje svaka kompanija može dobiti uvođenjem novih digitalnih alata, promjene načina tradicionalnog razmišljanja svojih zaposlenika, interne organizacije koje sve više postaju agilne te naposlijetku novih digitalnih poslovnih modela koji ostvaruju dodatni profitabilni rast za kompaniju te omogućuju izlazak na druge vrste tržišta pružajući nove usluge postojećim i novim kupcima. Izazovi u vidu cybersecuritya i zaštite podataka koje pri tome ovakva vrsta transformacije stavlja ispred svake kompanije je nešto o čemu je vrlo bitno više komunicirati kako bi se svima nama približili postojeći rizici, ali i rješenja koja te rizike svode na minimum. Neka od pitanja iz prakse na gore spomenute teme, koja se postavljaju Schneider Electricu, kao jednom od lidera u digitalnoj transformaciji elektroenergetskog sektora, ali i energetike, na koja će se odgovoriti su: Kako mi štitimo sebe i svoje kupce? Koje su garancije da su svi naši proizvodi i rješenja dovoljno sigurni? Što činimo kako bi osigurali zaštitu podataka kupaca i garantirali privatnost tih podataka prilikom korištenja cloud rješenja? Koje usluge pružamo da se unaprijedi i osigura cybersecurity u fazi projektiranja, instalacije, puštanja u pogon i svakodnevne eksploatacije različitih proizvoda i rješenja unutar elektroenergetskog sustava?

Tema 5.5

BLOCKCHAIN U ENERGETICI

Boris Njavro, dipl.ing., Energy Code d.o.o., Boris Golub, dipl.ing., Adnet d.o.o.

Energetska učinkovitost, energetske uštede, smanjenje emisije stakleničkih plinova, proizvodnja energije iz obnovljivih izvora... toliko su danas eksponirani da gotovo svakodnevno dobivamo novi aktivni element u distribucijskom dijelu EES-a. Bilo da je to novi distribuirani izvor (od kojih neki i nisu više mali i zanemarivi), bilo da je to kupac s vlastitom proizvodnjom, vlasnik električnog vozila ili samo napredni uređaj s mogućnošću utjecaja na proizvodnju i potrošnju energije, svi oni mijenjaju način kako se ponaša distribucijska mreža. Svi takvi uređaji potaknuti su željom cjelokupnog društva da izgradimo održivi sustav koji će nam osigurati energetsku samodostatnost i sigurnost opskrbe, kao osnovu daljnjeg razvoja (u prijevodu, želimo udisati čisti zrak i imati što povoljniju energiju uz zadržavanje dosadašnjeg komfora), međutim, do konačnog cilja treba prijeći i nekoliko prepreka na tom putu, Npr. riješiti probleme koje takvi uređaji uzrokuju u distribucijskoj mreži u pogledu regulacije napona, opterećenja dijelova mreže i dinamičnosti proizvodnje i potrošnje, a da ipak svi sudionici u priči imaju koristi i interes, kako društveni, tako i financijski. Uz sve navedeno nije teško predvidjeti korištenje specijalističkih digitalnih platformi za vođenje mreže, trgovanje energijom i uslugama, koje će optimirati tehničke parametre cijelog sustava uz maksimiziranje benefita svih korisnika. S obzirom na prirodu komercijalnih odnosa uključenih strana, platforma mora imati nezavisne mehanizme komunikacije i provjere svih zadanih i realiziranih transakcija pomoću tehnologije koja se odlikuje transparentnošću, decentraliziranošću i nepormijenjivosti podataka, čitaj “Blockchain”.

Kako će platforma(e) izgledati i funkcionirati, čije je vlasništvo i kakva su očekivanja korisnika, pokušat ćemo detaljnije razraditi kroz naslovnu prezentaciju, kao i sam mehanizam Blockchain tehnologije koji bi se mogao koristiti za sigurnost i nezavisnost rada platforme.

Tema 6

Tema 6.1

INFORMACIJSKA SIGURNOST KORPORACIJE I NIS DIREKTIVA

N.N., HEP d.d., Voditelj službe za informacijsku sigurnost

Sveobuhvatan sustav upravljanja informacijskom sigurnošću Hrvatske elektroprivrede između ostaloga podrazumijeva i zaštitu operacijskih (OT) i informacijskih tehnologija (IT) primijenjenih u osnovnim tehnološko proizvodnim te u potpornim poslovnim procesima od kibernetskih prijetnji. Učinkovito i djelotvorno upravljanje informacijskom sigurnošću uvjetuje razlikovanje cilja, fokusa i objekata informacijske i kibernetske sigurnosti u osnovnim proizvodno-tehnološkim i u potpornim poslovnim procesima korporacije.

Uskladba poslovanja korporacije i njenih sastavnica sa Zakonom i Uredbom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga zahtjeva (I) uspostavu učinkovite dostave obavijesti o

incidentima sa znatnim učinkom na ključne sustave te (II) provedbu postupaka i mjera za postizanje visoke zajedničke razine kibernetičke sigurnosti ključnih sustava proizvodnje i distribucije električne energije.

Da li je suvremeni Sigurnosni operativni centar - SOC rješenje korporacijske sigurnosti? Cilj ove prezentacije je ponuditi perspektivan holistički sigurnosni odgovor.

Tema 6.2

PRIMJENA NIS UREDBE U HOPS-u I NETWars VJEŽBA U POLJSKOJ

Andreja Mihalić Milavec, dipl.ing., Bernard Ivančević, dipl.ing.; Hrvatski operator prijenosnog sustava

Metodologija upravljanja rizicima koja definira obuhvat sustava kritične infrastrukture, uloge u procesu upravljanja rizicima, način evaluacije i vrednovanja rizika.

Planovi za uspostavu sustava informacijske sigurnosti na kritičnoj infrastrukturi HOPS-a, te tehnički i organizacijski izazovi s kojima se HOPS mora nositi u tom procesu.

Poljski operator prijenosnog sustava zajedno s partnerima iz SAD-a organizirao je zajedničku vježbu GridEx i NetWars. Partneri koji su sudjelovali na organizaciji vježbe su: SANS, NERC, DOE, ministarstvo obrane Poljske i ministarstvo sigurnosti Poljske. Na vježbu su bili pozvani svi Europski operatori prijenosa. Područja koja su bila obuhvaćena sudjelovanjem na sigurnosnoj vježbi su: kibernetička sigurnost u realnom vremenu i obrana sustava u realnom vremenu. Fokus je bio usmjeren prema zaštiti okoline radnih procesa.

RASPRAVA SUDIONIKA I ZAVRŠNA RIJEČ VODITELJA SEMINARA.

Congrès International des Réseaux Electriques de Distribution

HO CIRED, Zelinska 7, 10000 Zagreb
Telefon/telefaks: (+ 385 1) 617 15 27
www.ho-cired.hr
ho-cired@zg.t-com.hr

Seminar „Digitalizacija elektroenergetskog sektora i izazovi kibernetičke sigurnosti“
HO CIRED i HKIE održat će se

u četvrtak 21. ožujka 2019. u

Velikoj dvorani HEP d.d.
Ulica grada Vukovara 37/ VII, Zagreb

u vremenu od 9 do 17 sati

s jutarnjom stankom i ručkom

Kotizacija za sudjelovanje na ovom seminaru iznosi

1.000 kn neto + 250 kn (PDV) = 1.250 kn bruto

i uključuje materijale seminara, jutarnje osvježenje i ručak.

Kotizaciju uplatiti do 18. ožujka 2019. na IBAN žiro-račun: HR93 2340 0091 1102 5968 2.
Potvrdu o uplati poslati e–poštom na adresu ho-cired@zg.t-com.hr ili telefaksom na broj 01/617 15 27.
.

Broj sudionika je ograničen pa će se njihov konačni broj zaključiti prioritetom uplaćenih kotizacija.

Sudjelovanje na Seminaru vrednuje se u Hrvatskoj komori inženjera elektrotehnike s 8 akademskih sati.

Prijavnica za Seminar ─ kao i obrazac za obveznike stručnog usavršavanja ─ dostupni su na web–stranici www.ho-cired.hr, i šalju se ispunjeni e–poštom na adresu ho-cired@zg.t-com.hr ili telefaksom na broj 01/ 617 15 27.