37. Саветовање CIGRE Србија 2025
СИГУРНОСТ, СТАБИЛНОСТ, ПОУЗДАНОСТ И RESILIENCE ЕЛЕКТРОЕНЕРГЕТСКОГ СИСТЕМА
МУЛТИСЕКТОРСКО ПОВЕЗИВАЊЕ У ЕНЕРГЕТИЦИ И ПРИВРЕДИ
26 - 30. мај 2025, Копаоник

DOI: 10.46793/CIGRE37.B5.18

B5.18

DIGITALIZACIJA VN POSTROJENJA - IDS SISTEMI ZA DETEKCIJU SOFTVERSKIH NAPADA

DIGITALIZATION OF HV SUBSTATIONS - IDS INTRUSION DETECTION SYSTEMS

Srđan Mijušković*

Kratak sadržaj: Visokonaponska (VN) postrojenja čine ključne elemente prenosnog dela elektroenergetskog sistema, omogućavajući povezivanje izvora energije značajnih instalisanih snaga sa raznovrsnim potrošačima električne energije. Energetska tranzicija, podstaknuta globalnim inicijativama za dekarbonizaciju i klimatske akcije poput Pariskog sporazuma i ciljeva *Net Zero*, značajno je uticala na promene u elektroenergetskim sistemima. Digitalizacija putem IEC 61850 standarda nudi konkretna rešenja za navedene izazove, s posebnim fokusom na unapređenje komunikacionih aspekata. Implementacija sofisticiranih komunikacionih sistema, zasnovanih na savremenim digitalnim uređajima i principima računarske bezbednosti, predstavlja izuzetno složen i dinamičan proces. Uspešna realizacija zahteva precizno planiranje, kao i usklađenost sa relevantnim standardima kako bi se osigurala stabilnost, pouzdanost i sigurnost modernih elektroenergetskih sistema. Primena modernih tehnologija, kao što su *Intrusion Detection Systems* (IDS), omogućava proaktivno praćenje mrežnog saobraćaja i detekciju anomalija u realnom vremenu. U radu je prikazana analiza računarske bezbednosti VN postrojenja kroz smernice NIST CSF 2.0 - *National Institute of Standards and Technology Cybersecurity Framework Version 2.0*.

Ključne reči: *IEC 61850, IDS, Računarska bezbednost, NIST CSF 2.0, Mašinsko učenje*

Abstract: High-voltage (HV) substations represent key elements of the transmission part of the power system, enabling the connection of energy sources with significant installed capacities to a diverse range of electricity consumers. The energy transition, driven by global decarbonization initiatives and climate actions such as the Paris Agreement and Net Zero goals, has significantly influenced changes in power systems. Digitalization through the IEC 61850 standard offers concrete solutions to these challenges, with a particular focus on enhancing communication aspects. The implementation of sophisticated communication systems, based on modern digital devices and cybersecurity principles, is an extremely complex and dynamic process. Successful implementation requires precise planning, as well as compliance with relevant standards to ensure the stability, reliability, and security of modern power systems. The application of modern technologies, such as Intrusion Detection Systems (IDS), enables proactive monitoring of network traffic and real-time anomaly detection.

* Srđan Mijušković, Acinel, srdjan.mijuskovic@acinel.com

This paper presents an analysis of cybersecurity in HV substations based on the guidelines of NIST CSF 2.0 - National Institute of Standards and Technology Cybersecurity Framework Version 2.0.

Key words: *Digitalization, IEC 61850, IDS, Cyber Security, NIST CSF 2.0, Machine learning*

1 UVOD

Koncept *Smart Grid*-a moramo razumeti kao kontinualan proces, koji se izuzetno precizno može sagledati kroz razvoj visokonaponskih (VN) postrojenja tokom 21. veka. Budući da se funkcionalno nalaze u samom središtu elektroenergetskih sistema, za očekivati je da promene i unapređenja u povezanim sistemima direktno utiču i na VN postrojenja. Promene se prevashodno odnose na aspekt informaciono-komunikacionih tehnologija (IKT). IKT u industrijskim i energetskim delatnostima nazivamo operacionim OT tehnologijama, za razliku od informacionih IT tehnologija koje povezujemo prvenstveno s poslovnim procesima [1].

Digitalizacija VN postrojenja putem standarda IEC / SRPS EN 61850 „Komunikacione mreže i sistemi za automatiku u elektroenergetskim objektima“ je proces koji bi trebalo da omogući navedene zahteve, posebno komunikacioni aspekt. Često se u brojnim materijalima može videti naglašavanje da se radi o standardu, nikako samo o komunikacionom protokolu. Međutim, možda ni reč standard ne naglašava sveobuhvatnost ove platforme za digitalizaciju elektroenergetskih objekata. Radi se o soluciji koja omogućava da *Smart Grid* postane realan i održiv cilj. Proteklo je više od 20 godina od objavljivanja i početaka praktične upotrebe IEC 61850. U 40-ak različitih dokumenata na više od 8000 strana date su jasne smernice za digitalizaciju elektroenergetskih objekata, inicijalno i prevashodno VN objekata.

VN postrojenja predstavljaju osnovu prenosnog dela elektroenergetskog sistema, omogućavajući stabilan prenos energije između izvora značajnih instalisanih snaga i širokog spektra potrošača. Globalne inicijative, poput Pariskog sporazuma i ciljeva *Net Zero*, ubrzale su energetsku tranziciju, donoseći promene u strukturi proizvodnje i potrošnje električne energije. Sve veće prisustvo obnovljivih izvora energije zasnovanih na inverterima, uz porast decentralizovanih sistema i fleksibilnih potrošača, zahteva modernizaciju postojećih infrastruktura i primenu naprednih tehnologija [2][3].

Koordinacija i upravljanje nepredvidivih i nestalnih izvora obnovljive energije predstavlja izuzetno složen zadatak. S jedne strane su izuzetno raznoliki proizvođači, dok se s druge strane nalaze sve zahtevniji potrošači. Za uspešnu funkcionalnost ovakvih sistema neophodno je prikupljanje i obrada velike količine podataka, često i u realnom vremenu. Razmena tako značajne količine informacija u višestrukim pravcima zahteva robusnu i visokopouzdanu komunikacionu mrežu. S porastom složenosti komunikacionih sistema, digitalizacija donosi nove izazove, posebno u domenu računarske bezbednosti. Postoji više pravaca odgovora na navedene i povezane izazove, stoga je njihovo pravilno razumevanje ključno za sadašnjost i budućnost elektroenergetske mreže [4].

VN postrojenja, kao deo kritične infrastrukture, postaju potencijalna meta za napade koji mogu narušiti stabilnost i sigurnost sistema. Primetan je značajan porast napada na EES, na svetskom nivou, ali više ni region nije pošteđen izuzetno ozbiljnih napada [5][6].

Međutim, računarska bezbednost se može narušiti na više različitih načina, osim hakerskih napada, shodno tome postoji i čitava kategorizacija vrsta ugrožavanja OT sistema [7].

Implementacija sveobuhvatnih okvira, poput *National Institute of Standards and Technology Cybersecurity Framework Version* 2.0 (NIST CSF 2.0), pruža osnovu za identifikaciju, zaštitu, detekciju, odgovor i oporavak od potencijalnih pretnji. Primena modernih tehnologija, kao što su *Intrusion Detection Systems* (IDS), omogućava proaktivno praćenje mrežnog saobraćaja i detekciju anomalija u realnom vremenu.

Moderna istraživanja na ovu temu svakako ukazuju na potencijale, a zbog obimnosti potencijalno ukazuju i na neophodnost uključivanja *Machine Learning* algoritama u cilju unapređenja klasifikacije značajnih količina GOOSE i naročito *Sampled Values* podataka [8][9].

2 DIGITALIZACIJA VN POSTROJENJA

Digitalizacija VN postrojenja putem IEC 61850 standarda je proces koji bi trebalo da omogući navedene *Smart Grid* zahteve, posebno komunikacioni aspekt. Ključne prednosti IEC 61850 jesu dobro poznate i priznate mogućnosti interoperabilnosti, skalabilnosti, tipiziranog inženjeringa i uključivanja u digitalne tendencije u skladu sa principima računarske bezbednosti.

Model zaštitno-upravljačkog sistema koji se najčešće primenjuje u savremenim digitalizovanim VN postrojenjima s pravom se naziva hibridni. Moderni zaštitno-upravljački sistemi primenjuju digitalizovane IED (*Intelligent Electronic Device*) uređaje, redundantne SCADA sisteme i koriste u svojim procesima poruke bazirane na 8-1 delu standarda – MMS i GOOSE, što se smatra digitalizacijom do staničnog nivoa [10]. Shodno definicijama IEC 61850, proces digitalizacije zaštitno-upravljačkih VN sistema bi morao biti zaokružen korišćenjem *Sampled Values* – digitalizovanih merenja ili prema SRPS EN 61850-9-2:2013 - vrednosti uzoraka [11][12].

Potpuno digitalizovani zaštitno-upravljački sistem, iako u potpunosti definisan standardom, idalje nije uobičajen u kreiranju Smart Grid infrastrukture. U međuvremenu, mnoge nove tehnologije (*Virtual Local Area Network* VLAN, *Digital Twin,* Virtuelizacija IED..) su počele da pronalaze svoje pozicije u modernizaciji zaštitno-upravljačkih sistema. Sofisticiranost razlika i složenost preciznog definisanja nivoa digitalizacije postrojenja jasno ilustruje sveobuhvatnu zahtevnost izazova navedenog globalnog procesa [13].

Pored navedenog, potrebno je naglasiti da je IEC 61850 zasnovan na SCL (*Substation Configuration Language*), koji pruža mehanizam za deskripciju funkcionalnosti i strukture elektroenergetskih postrojenja. SCL se opisuje pomoću XSD (*XML Schema Definition*), što omogućava standardizovanu i za mašinski čitljivu strukturu podataka. Navedena karakteristika čini SCL ključnim za primenu naprednih tehnika analize podataka, uključujući mašinsko učenje i razvoj sistema za detekciju upada (IDS - *Intrusion Detection Systems*) [14].

Standard definiše nekoliko tipova konfiguracionih fajlova koji sadrže sve potrebne informacije o radu, topologiji i komunikaciji u postrojenju.

Posebno su zanimljivi sledeći fajlovi u kontekstu detekcije anomalija i unapređenja računarske bezbednosti:

- *IED Capability Description* (ICD) fajl: Sadrži šablone podataka, tipove podataka i logičke čvorove implementirane na svakom uređaju (IED - *Intelligent Electronic Device*).

- *Substation Configuration Description* (SCD) fajl: Sadrži električnu topologiju postrojenja, povezane IED-ove i informacije koje se razmenjuju među njima. Fajl pruža uvid u celokupnu komunikacionu mrežu i međusobne interakcije uređaja.

3 NIST CSF 2.0

National Institute of Standards and Technology Cybersecurity Framework Version 2.0 (NIST CSF 2.0) je sveobuhvatan i fleksibilan okvir koji pomaže organizacijama da unaprede status računarske bezbednosti svog sistema i upravljaju bezbednosnim rizicima. Definisani okvir je strukturiran oko tri osnovne komponente: Osnova (*Core*), Slojevi implementacije (*Implementation Tiers*) i Profili (*Profiles*) [15]. Svaka od ovih komponenti igra ključnu ulogu u kreiranju strategije računarske bezbednosti koja je prilagodljiva specifičnim potrebama organizacija.

3.1 Osnova NIST CSF 2.0

Osnova (*Core*) NIST CSF 2.0 je srž okvira (*framework*) i pruža organizacijama visok nivo strukturiranosti neophodne za upravljanje rizicima računarske bezbednosti.

Sastoji se od pet ključnih funkcija: *Identify* (Identifikacija), *Protect* (Zaštita), *Detect* (Detekcija), *Respond* (Odgovor) i *Recover* (Oporavak). Svaka funkcija je dizajnirana da pomogne organizacijama da sistematski pristupe računarskoj bezbednosti, fokusirajući se na različite aspekte upravljanja rizikom i otpornosti sistema.

Identifikacija (*Identify*)**:** Funkcija Identifikacija pruža organizacijama jasno razumevanje računarskih bezbednosnih rizika. Uključuje identifikaciju ključnih resursa, sistema, podataka i pojedinaca koji zahtevaju zaštitu, kao i razumevanje bezbednosnih rizika ovih resursa. Kroz ovu funkciju, organizacije razvijaju strategiju upravljanja rizicima i strukturu upravljanja, postavljajući temelje za druge aktivnosti vezane za računarsku bezbednost. Ključne aktivnosti uključuju procenu rizika, upravljanje imovinom i procedurama računarske bezbednosti.

Zaštita (*Protect*): Funkcija Zaštita fokusira se na implementaciju neophodnih zaštita kako bi se osiguralo da kritična infrastruktura organizacije bude adekvatno zaštićena od pretnji po računarsku bezbednost. Navedeno podrazumeva obezbeđivanje sistema, mreža i podataka od neovlašćenog pristupa i osiguranje njihove zaštite. Funkcija Zaštita uključuje kategorije poput kontrole pristupa, zaštite podataka, obuke i podizanja svesti, kao i zaštitnih tehnologija.

Detekcija (*Detect*): Funkcija Detekcija fokusira se na otkrivanje i identifikaciju događaja i anomalija koje ukazuju da je računarska bezbednost ugrožena. Organizacije moraju kontinuirano pratiti svoje sisteme i mreže kako bi što ranije otkrile upade ili maliciozne aktivnosti. Rana detekcija pomaže u smanjenju potencijalnog uticaja incidenata. Aktivnosti u ovoj funkciji uključuju implementaciju sistema za detekciju upada, kontinuirano praćenje i analizu događaja kako bi se brzo prepoznale pretnje po računarsku bezbednost.

Odgovor (*Respond*): Kada je sajber događaj detektovan, funkcija Odgovor pruža strukturirani pristup za ublažavanje uticaja događaja. To uključuje uspostavljanje plana odgovora na incidente, analizu događaja, komunikaciju sa relevantnim zainteresovanim stranama i preduzimanje koraka za suzbijanje i minimiziranje štete prouzrokovane napadom. Cilj je da se ograniči ukupni prekid rada organizacije i njenih operacija.

Oporavak (*Recover*): Funkcija Oporavak obezbeđuje da organizacija može da vrati normalne operacije nakon sajber incidenta.

Ovo uključuje oporavak izgubljenih podataka, vraćanje sistema u punu funkcionalnost i učenje iz incidenta kako bi se poboljšala buduća otpornost. Naglašava se značaj otpornosti i kontinuiranog poboljšanja kako bi se organizacija brzo oporavila nakon incidenta. Ključne aktivnosti uključuju planiranje oporavka, implementaciju poboljšanja i komunikaciju statusa oporavka.

U okviru NIST-a je već kroz vizuelni prikaz jasno prikazana kontinuiranost i cikličnost računarske bezbednosti kao procesa. Verzija 2.0 iz februara 2024. donosi značajnu novinu, uvođenjem sveobuhvatne *Govern* funkcije. Cilj ove funkcije je da se skrene pažnja na obavezu vodećih struktura u organizacijama da usklade koncepte računarske bezbednosti sa organizacionim ciljevima, zakonodavnim okvirima i merama za upravljanje rizikom. Na ovaj način, formalno se odgovornost za računarsku bezbednost sistema prenosi na najviši hijerarhijski nivo upravljanja kompanijom. Zadati pristup naglašava potrebu za uspostavljanjem jasnih procedura, procesa i uloga koje svaki deo sistema mora preuzeti u procesu računarske bezbednosti. Podizanjem na najviši hijerarhijski nivo ostvaruje se usklađenost primena mera, uvođenje najboljih praksi i redovna revizija implementiranih sigurnosnih procedura. Povišen nivo praćenja mera podrazumeva i veće oslanjanje na zahteve definisane u IEC 61850, a naročito u standardu IEC 62351 Komunikacione mreže i sistemi za automatiku u elektroenergetskim objektima – Bezbednost.

Do sada je akcenat, a često i prva pomisao na računarsku bezbednost, bio na funkciji *Protect* – zaštiti sistema od mogućih pretnji. U nastavku su prikazani brojni elementi i mehanizmi koji pripadaju navedenoj *Core* funkciji. Očigledno je zašto je navedena komponenta ključna za računarsku bezbednost i nije slučajno da IEC 62351 posvećuje veliku pažnju datim funkcionalnostima:

- *Firewall* – „zaštitni zid“
- Mrežna segmentacija, *Purdue Model*
- *Demilitarized Zones* DMZ - demilitarizovane zone
- *Role-Based Access Control* RBAC - Kontrola pristupa zasnovana na ulogama
- *Secure Remote Access* - Siguran daljinski pristup
- *Data Encryption* - Enkripcija podataka
- *Intrusion Prevention Systems* (IPS) - Sistemi za prevenciju softverskih upada

4 IDENTIFIKACIJA I DETEKCIJA

Zaključak prethodnog poglavlja jasno potvrđuje *Protect* kao ključni aspekt računarske bezbednosti OT sistema. Međutim, sagledavanjem komunikacione arhitekture računarskih sistema VN postrojenja, primetno je da je sistem previše ranjiv iznutra. Ključni zadatak kritične OT infrastrukture se ogleda u „*availibility*“ – neprekidnoj dostupnosti podataka. Očigledno je da bez adekvatnog fokusa na funkcije *Identify* i *Detect*, ukupna otpornost sistema ostaje nedovoljna. Sve ovo se potpuno uklapa u „*Defence in Depth“* koncepta višeslojne zaštite i reagovanja na izazove računarske bezbednosti [16].

Funkcija *Identify* omogućava da se sistematski i proaktivno identifikuju sve potencijalne ranjivosti, rizici i kritične komponente, čime se postavlja osnova za sve ostale sigurnosne aktivnosti. Navedeno uključuje mapiranje resursa, analizu pretnji i procenu rizika, što je od ključnog značaja za složene i digitalizovane sisteme, poput VN postrojenja. Za VN postrojenja „*attack vectors*“ predstavljaju konekcije ka nadređenim centrima i veza sa IT servisima.

Možemo reći da navedeni aspekt uključuje i aktivnu primenu *Asset Monitoring*-a. Kreiranje liste elemenata prisutnih u sistemu znatno je olakšano SCL fajlovima, precizno definisanim IEC 61850-6.

4.1 Intrusion Detection System - IDS

Činjenica da u Švajcarskoj od jula 2024. zakonskom regulativom postaje obavezna upotreba IDS možda najbolje svedoči o realnoj važnosti ovakvih sistema [17]. Svakako da i EU NIS2 (*Network and Information Security Directive* 2) direktiva o mrežnoj i informacionoj bezbednosti, značajno utiče na porast svesti i broja zahteva za ovakvim sistemima širom Evrope. Značajna razlika u pristupu koje OT i IT koncepti računarske bezbednosti imaju izuzetno se dobro sagledava kroz način primene IDS sistema. U IT konceptima koristi se dobropoznata ideja antivirus skenera i kreiranja listi zabranjenih podataka „*deny list*".

Integracija IDS sistema se po pravilu vrši praćenjem mrežnog saobraćaja preko *mirror* portova na eternet *switch*-evima. Naročito su važni portovi koji su vezani za računare sa *gateway* ulogom.

Najčešći problemi na koje se u VN objektima nailazi IDS pretragom predstavljaju:

- Ugroženi IED uređaji
- Rizične TCP/IP konekcije
- Nepotrebne i nepouzdane funkcionalnosti
- Neodgovarajuća segmentacija mreže
- Neodgovarajuća *asset* lista

Izuzetno cenjene karakteristike interoperabilnosti i transparentnosti modelovanja standarda IEC 61850 će verovatno morati da postanu i deo AI (*Artificial Intelligence*) standardizacije i procesa funkcionalnosti, budući da sa povećanjem kompleksnosti algoritama, mogućnost nekompatibilnosti sa realnim zahtevima i očekivanjima neminovno vodi ka gubitku pouzdanosti povratnih informacija [18]. Navedeni izazov je primećen tokom procesa programskog učenja AI servisa u digitalizovanom VN postrojenju za potrebe računarske bezbednosti. Funkcionisanje komunikacionih protokola, njihova frekventnost i odziv prilikom normalnog radnog stanja su klasifikovani i memorisani pomoću markera. Pokazalo se da je takav sistem pušten u paralelan rad sa postojećim, emitovao neočekivano veliki broj neželjenih (*false*) alarma [19].

Plan je nedovoljno pripremljen za veliki broj situacija koje ne pripadaju normalnom radnom režimu. U situacijama poput rutinskih testiranja i kontrolisanih kvarova u mreži, isuviše lako dolazi do pomenutih neželjenih alarma, usled sofisticiranosti semantike komunikacionih protokola u sastavu IEC 61850.

Izazvani alarmi u sebi sadrže složene tehničke detalje, a budući da AI ne spoznaje u celosti fiziku procesa, za njihovo potpuno tumačenje je neophodna stručnost iz IEC 61850 (OT), IT mrežnih i sistema računarske bezbednosti, a najviše - poznavanje implementiranih funkcionalnih logika zaštitno-upravljačkog sistema [20].

Napredak u integraciji IDS sistema moguć je zahvaljujući uniformnosti informacija u VN postrojenjima digitalizovanim prema IEC 61850 standardu. Od velike pomoći je činjenica da u digitalizovanim VN postrojenjima izuzetno visok procenat mrežnog saobraćaja pripada IEC 61850 protokolima.

Značajno je i što od samog starta implementacije i analize SCL fajla, može se sagledati koji su modeli rada i informacije očekivani u komunikaciji. Na taj način se zapravo kreira suprotnost „*deny*“ liste, „*allow*“ lista sa dozvoljenim podacima u analiziranoj mreži. Praćenjem svetskih tehnologija nameće se logična ideja o kreiranju AI *machine learning* sistema koji bi mogli da odgovore na specifičnosti zahteva OT mreže [21].

Svakako treba naglasiti, kako bi bilo koja AI metodologija obrade ovakve količine podataka mogla da se sprovede u realnosti, neophodno je prvenstveno oformiti bazu koja će biti temelj svih planiranih postupaka. Baze podataka moraju biti tačno definisane i sastavljene isključivo od podataka koji sadrže informacije od značaja za monitoring željenih parametara. Datim postupkom omogućavaju se dalje analize i daje sposobnost AI da u perspektivi donosi sve preciznije i upotrebljivije zaključke.

Ključni aspekt unapređenja jeste bolje razumevanje između domena koji do skoro nisu imali toliko dodirnih tačaka, IT i OT sektora u kompanijama [22].

5 ZAKLJUČAK

Složenost procesa digitalizacije VN postrojenja prevazilazi striktno tehničke aspekte. Negativna iskustva u realizaciji ovakvih struktura mogu imati štetan uticaj, ali ne samo na kompanije koje trpe finansijske gubitke. Celokupan tehnološki progres i proces ostvarivanja globalnih inicijativa kao što su *Smart Grid* i *Zero Net* ciljevi postaje ugrožen.

Verovatno najveći izazov u implementaciji digitalnih tehnologija leži u prihvatanju velikih promena u funkcionalnim i strogo definisanim okruženjima. Energetski sektor, kao ključni predstavnik kritične infrastrukture, teško prihvata tranzicione promene jer se suočava s potencijalnom nepouzdanošću digitalnih sistema. Navedeno potvrđuju NIST CSF i drugi relevantni standardi, ističući da apsolutna bezbednost digitalnih sistema nije moguća. Primenom IDS računarska bezbednost VN postrojenja se svakako pospešuje.

Kao što vidimo, izazovi su brojni, ali potencijali koje digitalizacija donosi predstavljaju ključni motiv za nastavak istraživanja i unapređenja u ovom domenu, inspirišući korake ka sigurnijoj i održivoj budućnosti elektroenergetskih sistema.

6 LITERATURA

[1] A. Apostolov, Digitizing the electric power grid, 2023

[2] M. Kanabar, Building the Grid of the Future through Innovations with Digital Transformation, PAC World, 2023

[3] J. Ugwu, Comprehensive Review of Renewable Energy Communication Modeling for Smart Systems, Energies, 2023

[4] P. Bishop, IEC 61850 Principles and Applications to Electric Power Systems, 2023

[5] Fortinet, State of Operational Technology and Cybersecurity Report, 2024

[6] Balkan energy news, *https://balkangreenenergynews.com/serbias-power-utility-eps-under-unprecedented-hacker-attack/*, 2023

[7] Fortinet, 20 Most Common Types Of Cybersecurity Attacks, 2024

[8] JA Lopez, Substation-Aware: An Intrusion Detection System for the IEC 61850 Protocol, 2022

[9] TS Ustun, *Machine Learning-Based Intrusion Detection for Achieving Cybersecurity in Smart Grids Using IEC 61850 GOOSE Messages*, 2021

[10] IEC 61850 *Communication networks and systems for power utility automation* - Part 8-1: *Specific communication service mapping* (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802/3, 2011

[11] IEC 61850-9-2: Specific Communication Service Mapping (SCSM) – Sampled Values over ISO/IEC 8802-3. – First Edition, 2004

[12] SRPS EN 61850-9-2:2013 - *Komunikacione mreže i sistemi za automatizaciju energetskih objekata — Deo 9-2: Specifično preslikavanje komunikacionih servisa (SCSM) — Vrednosti uzoraka prema ISO/IEC 8802-3 – Edicija 2*

[13] S. Mijušković, *Pregled izazova integracije modernih komunikacionih sistema u elektroenergetskim mrežama*, CIRED Crna Gora, 2024

[14] PSRC WG C43 Report, *Practical applications of AI / ML in Power system PAC*, PAC World, 2024

[15] The NIST Cybersecurity Framework (CSF) 2.0, 2024

[16] IEC 62351, *Power systems management and associated information exchange - Data and communications security*, 2023

[17] A.Klien, *Exploring Hidden Flaws in the Power Grid*, PAC World, 2024

[18] A. Apostolov, *Data Sources for AI application*, PAC World, 2024

[19] A.Klien, *New approach for detecting cyber intrusions in IEC 61850 substations*, PAC World, 2019

[20] A. Klien, *Cyber aware Session 6: Digital Substations, White paper and Webinar - Smart Grid Forums*, 2022

[21] K. Park, *Machine Learning Based Cyber System Restoration for IEC 61850 Based Digital Substations*, 2024

[22] F. Cleveland, *Cybersecurity for Power Systems using IEC 61850, Including Distributed Energy Resources (DER)*, 2021