Broj rada: R3-23
DOI:10.46793/CIRED2026.R3-23_140

# SIGURNOSNI ASPEKTI KOMUNIKACIJSKIH SUSTAVA U DIGITALIZIRANIM ELEKTRODISTRIBUTIVNIM MREŽAMA

# SECURITY ASPECTS OF COMMUNICATION SYSTEMS IN DIGITALIZED DISTRIBUTION NETWORKS

Lucija MEDIĆ*, JP „Elektroprivreda HZ HB“ d.d. Mostar, Bosna i Hercegovina
Sonja SUŠAC, JP „Elektroprivreda HZ HB“ d.d. Mostar, Bosna i Hercegovina
Ivan ŠIMOVIĆ, JP „Elektroprivreda HZ HB“ d.d. Mostar, Bosna i Hercegovina
Marin MAJSTOROVIĆ, JP „Elektroprivreda HZ HB“ d.d. Mostar, Bosna i Hercegovina
Mia PREVIŠIĆ, JP „Elektroprivreda HZ HB“ d.d. Mostar, Bosna i Hercegovina

## KRATAK SADRŽAJ

U ovom stručnom radu razmatraju se sigurnosni aspekti komunikacijskih sustava u digitaliziranim distribucijskim mrežama, s posebnim naglaskom na SCADA i sustave automatizacije distribucije (Distribution Automation – DA). U uvodnom dijelu rada analizirani su osnovni razlozi digitalizacije distribucijskih mreža te se ističe povezanost pouzdanog upravljanja mrežom i sigurnosti komunikacijske infrastrukture. Posebna pozornost posvećena je rastu sigurnosnih rizika koji proizlaze iz sve šire primjene otvorenih komunikacijskih protokola i IP-baziranih komunikacijskih mreža. Ovaj rad donosi pregled uloge komunikacijskih sustava u funkcijama upravljanja i zaštite distribucijske mreže, uz opis temeljnih funkcionalnosti SCADA i DA sustava. Nadalje, analizirani su najčešće korišteni komunikacijski protokoli u distribucijskim mrežama, uključujući IEC 60870-5-104, IEC 61850 i DNP3, pri čemu su razmatrane njihove tehničke prednosti, ali i sigurnosni izazovi koji se javljaju u praktičnoj primjeni. Razmatrane su specifičnosti distribucijskih sustava u odnosu na klasične informacijsko-komunikacijske (IT) sustave te identificirane su tipične ranjivosti komunikacijskih sustava, kao što su prisutnost zastarjele opreme, nedovoljna razina enkripcije i korištenje javnih komunikacijskih mreža. Analizirane su moguće posljedice sigurnosnih incidenata, uključujući poremećaje u upravljanju pogonom, smanjenje pouzdanosti opskrbe električnom energijom te potencijalne rizike za sigurnost i stabilnost sustava. U radu se razmatrane i kibernetičke prijetnje SCADA i DA sustavima, uz pregled najčešćih oblika prijetnji, kao što su neovlašteni pristup, manipulacija podacima i uskraćivanje usluge. Nadalje, prikazani su osnovni sigurnosni mehanizmi u komunikacijskim sustavima, uključujući autentifikaciju, enkripciju, segmentaciju mreže te upravljanje korisničkim pravima. Razmatrana je uloga norme IEC 62351 kao temeljnog standarda za unaprjeđenje sigurnosti elektroenergetskih komunikacija te se iznose smjernice za postupnu implementaciju sigurnosnih mjera u distribucijskim mrežama. Zaključno se naglašava važnost kibernetičke sigurnosti kao jednog od ključnih čimbenika pouzdanog i održivog razvoja budućih distribucijskih sustava.

**Ključne reči**: komunikacijski sustavi, kibernetička sigurnost, SCADA sustav, digitalizirane distribucijske mreže

* Lucija Medić, lucija.medic@ephzhb.ba

## ABSTRACT

This technical paper examines the security aspects of communication systems in digitalized distribution networks, with particular emphasis on SCADA and Distribution Automation (DA) systems. The introduction outlines the main drivers of distribution network digitalization and highlights the relationship between reliable network operation and the security of communication infrastructure. Special attention is given to the increasing security risks associated with the widespread adoption of open communication protocols and IP-based communication networks. The paper then discusses the role of communication systems in distribution network control and protection functions and describes the core functionalities of SCADA and DA systems. It further reviews the most commonly used communication protocols in distribution networks, including IEC 60870-5-104, IEC 61850, and DNP3, focusing on their technical advantages as well as the security challenges encountered in practical implementation. The specific characteristics of distribution systems, compared with conventional information and communication technology (ICT) systems, are addressed, and typical vulnerabilities of communication systems are identified, such as the presence of legacy equipment, insufficient levels of encryption, and the use of public communication networks. The paper also examines the potential consequences of security incidents, including disturbances in network operation, reduced reliability of electricity supply, and risks to overall system security and stability. In addition, the paper addresses cyber threats to SCADA and DA systems by outlining the most common threat types, such as unauthorized access, data manipulation, and denial-of-service attacks. It also presents fundamental security mechanisms applied in communication systems, including authentication, encryption, network segmentation, and user access management. Finally, the paper discusses the role of the IEC 62351 standard as a key framework for enhancing the security of power system communications and proposes guidelines for the gradual implementation of security measures in distribution networks. The paper concludes by emphasizing the importance of cybersecurity as a key factor in the reliable and sustainable development of future distribution networks.

**Keywords:** communication systems, cybersecurity, SCADA system, digitalized distribution networks

## 1. UVOD

Digitalizacija elektrodistribucijskih mreža jedan je od najvažnijih razvojnih procesa u suvremenom elektroenergetskom sektoru. Razvoj naprednih funkcija nadzora i upravljanja, široka primjena daljinski upravljanih uređaja, integracija distribuiranih izvora i sve veći zahtjevi za pouzdanošću opskrbe električnom energijom, doveli su do znatnog povećanja uloge komunikacijskih sustava u distribucijskim mrežama. Komunikacijska infrastruktura danas više nije pomoćni dio sustava, nego jedan od ključnih nositelja funkcionalnosti upravljanja i zaštite. U klasičnim distribucijskim mrežama mnoge su funkcije bile lokalne, elektrotehnički definirane i relativno slabo povezane s vanjskim mrežama. U digitaliziranom okruženju stanje je bitno drukčije: mjerenja, upravljačke naredbe, signalizacija, alarmi i procesni podaci neprestano se razmjenjuju između većeg broja međusobno povezanih uređaja i informacijskih sustava. Posljedica toga je da svaka slabost u komunikacijskoj infrastrukturi može neposredno utjecati na raspoloživost, točnost i pravodobnost podataka potrebnih za siguran pogon mreže. Sigurnost komunikacijskih sustava u elektrodistribucijskim mrežama razlikuje se od sigurnosti klasičnih poslovnih informacijskih sustava. U elektroenergetskom kontekstu prioriteti su visoka raspoloživost, vremenska određenost komunikacije, mogućnost kontinuiranog rada i tolerancija

na ograničene prekide održavanja. Uz to, posljedice sigurnosnog incidenta ne zadržavaju se samo u virtualnom prostoru, nego mogu imati vrlo konkretne fizičke posljedice u mreži, uključujući pogrešne sklopne operacije, kašnjenje zaštite, gubitak nadzora nad postrojenjem ili poremećaje u opskrbi.

U ovom radu razmatraju se sigurnosni aspekti komunikacijskih sustava u digitaliziranim elektrodistribucijskim mrežama s naglaskom na SCADA i DA sustave te rastući broj kibernetičkih napada na kritičnu infrastrukturu. Najprije se opisuje uloga komunikacijskih sustava u funkcijama nadzora, upravljanja i zaštite, zatim se analiziraju temeljni komunikacijski protokoli i njihove sigurnosne slabosti, nakon čega se razmatraju tipične prijetnje, posljedice incidenata i osnovne mjere zaštite. Posebno se ističe važnost norme IEC 62351 kao relevantnog standarda za povećanje sigurnosti elektroenergetskih komunikacija [1].

## 2. ULOGA KOMUNIKACIJSKIH SUSTAVA U DISTRIBUCIJSKIM MREŽAMA

Komunikacijska infrastruktura temelj je digitalizirane distribucijske mreže, jer omogućuje razmjenu telemetrijskih podataka, stanja sustava, informacija o kvarovima i upravljačkih naredbi između nadzornog centra i terenskih uređaja. Bez pouzdane komunikacije nije moguće učinkovito upravljanje mrežom ni primjena funkcija automatizacije. Zahtjevi za komunikacijskim performansama izravno ovise o vrsti funkcije. Norma IEC 61850 definira klase performansi prijenosa poruka: GOOSE poruke za brzu zaštitnu signalizaciju zahtijevaju klasu P1 s maksimalnom latencijom od 4 ms, dok funkcije nadzora i upravljanja toleriraju dulje vremenske odzive u okvirima klasa P2 i P3 [5][6]. Funkcije automatizacije distribucije, poput FLISR-a (Fault Location, Isolation and Service Restoration) [18], zahtijevaju pouzdanu komunikaciju s latencijom u rasponu od desetaka do stotinjak milisekundi, ovisno o topologiji mreže i primijenjenom protokolu. Distribucijski sustavi pritom sve češće uključuju heterogene mreže optičkih, bakrenih i bežičnih medija s IP-baziranim arhitekturama, što povećava fleksibilnost, ali svaki komunikacijski segment i prijelaz između protokola uvodi potencijalnu ranjivost.

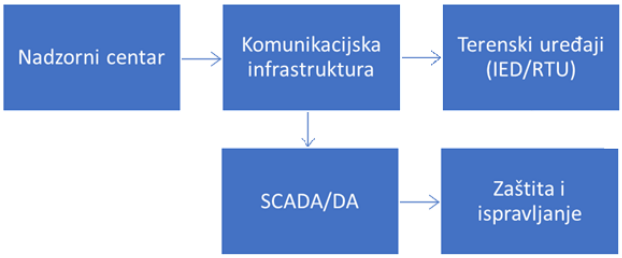
Sigurnost komunikacijske infrastrukture stoga je izravna pretpostavka pogonske pouzdanosti mreže, kompromitirana komunikacija operateru može uskratiti uvid u stvarno stanje postrojenja ili uzrokovati slanje netočnih upravljačkih naredbi, što nosi izravne fizičke posljedice u sustavu [1].

## 3. SCADA I SUSTAVI AUTOMATIZACIJE DISTRIBUCIJE

SCADA sustavi (Supervisory Control and Data Acquisition) predstavljaju osnovu daljinskog nadzora i upravljanja elektroenergetskim postrojenjima. Prikupljaju procesne podatke s terena, prikazuju pogonsko stanje u nadzornom centru i šalju upravljačke naredbe prema udaljenim uređajima. Sustavi automatizacije distribucije (Distribution Automation – DA) nadograđuju SCADA funkcije autonomnom obradom podataka i automatiziranim akcijama poput izolacije kvara, preusmjeravanja napajanja i optimiranja pogonskih stanja. Uspješnost tih funkcija izravno ovisi o dostupnosti i točnosti komunikacije [1].

Za razliku od klasičnih IT sustava, SCADA i DA okruženja temelje se na opremi dugog životnog vijeka, uređajima RTU (Remote Terminal Unit) i IED (Intelligent Electronic Device) starijih generacija koji često nemaju hardversku podršku za kriptografske operacije, što izravno ograničava implementaciju TLS -a (Transport Layer Security) i snažne autentifikacije [2]. Pritom ovi sustavi moraju osigurati kontinuitet rada čak i u degradiranim uvjetima komunikacije, pa sigurnosne mjere ne smiju znatno narušiti vremenski odziv ni raspoloživost

funkcija. Ravnoteža između sigurnosti, pouzdanosti i operativne učinkovitosti jedan je od temeljnih izazova u projektiranju komunikacijskih sustava digitaliziranih distribucijskih mreža. Slika 1 prikazuje arhitekturu digitalizirane distribucijske mreže.




*Slika 1* – Arhitektura digitalizirane distribucijske mreže

### 3.1. Specifičnosti elektroenergetskih sustava u odnosu na IT sustave

Sigurnosni pristup u elektrodistribucijskim mrežama bitno se razlikuje od pristupa u klasičnim poslovnim IT sustavima. Sustavi industrijskog upravljanja, označeni pojmom OT (Operational Technology), primjenjuju AIC (Availability, Integrity, Confidentiality) trijadu kao temeljni sigurnosni okvir, za razliku od CIA (Confidentiality, Integrity, Availability) trijade u IT okruženjima, u OT sustavima dostupnost funkcije ima apsolutni prioritet, slijedi je integritet podataka, dok je povjerljivost relativno manje kritična. Kratkotrajan prekid komunikacije u elektroenergetskom sustavu može imati ozbiljnije pogonske posljedice nego djelomičan gubitak povjerljivosti podataka. SCADA i DA sustavi temelje se na kombinaciji stare i nove opreme, što otežava primjenu jedinstvene sigurnosne politike. Zakrpe i nadogradnje zahtijevaju validaciju, certifikaciju i usklađivanje s pogonskim uvjetima, pa su patch management ciklusi znatno duži nego u IT sustavima; svaka promjena konfiguracije mora proći formalizirani change management proces. Zbog toga je u OT okruženjima posebno važan koncept obrane u dubinu (eng. defense in depth), umjesto oslanjanja na jednu zaštitnu mjeru, sigurnost se postiže više međusobno nadopunjujućih slojeva zaštite.

## 4. KOMUNIKACIJSKI PROTOKOLI U DISTRIBUCIJSKIM MREŽAMA

U distribucijskim mrežama posebno su zastupljeni protokoli IEC 60870-5-104, IEC 61850 i DNP3, koji su nastali s naglaskom na funkcionalnost, interoperabilnost i pouzdan prijenos procesnih podataka. Kako u to doba otvorene IP mreže i sofisticirani kibernetički napadi nisu bili dominantna prijetnja, sigurnosni mehanizmi u tim protokolima uglavnom su naknadno uvedeni, što u suvremenim implementacijama zahtijeva posebnu pozornost.

### 4.1. IEC 60870-5-104

IEC 60870-5-104 mrežna je adaptacija protokola IEC 60870-5-101 kojoj je dodana podrška za TCP/IP (Transmission Control Protocol/Internet Protocol) arhitekturu, čime je omogućena jednostavna integracija u suvremene komunikacijske mreže i veća fleksibilnost u povezivanju udaljenih postrojenja . Oslanjanje na IP okruženje istodobno uvodi izloženost prijetnjama poput prisluškivanja, manipulacije prometom i napada ponavljanjem poruka (replay attack), pa implementacija bez dodatnih sigurnosnih mehanizama poput TLS enkripcije i obostrane autentifikacije predstavlja značajan sigurnosni rizik [7].

## 4.2. IEC 61850

IEC 61850 standard je za komunikaciju u elektroenergetskim postrojenjima s naglaskom na interoperabilnost IED uređaja. Definira tri ključna mehanizma: GOOSE (Generic Object Oriented Substation Event) poruke za brzu zaštitnu signalizaciju (klasa P1, maks. latencija 4 ms), MMS (Multimedia Messaging Service) protokol za upravljačku komunikaciju između IED uređaja i nadzornih sustava te SCL (Substation Configuration Language) format za standardiziranu konfiguraciju postrojenja. Pogrešno konfigurirane SCL datoteke mogu uzrokovati neispravno ponašanje IED uređaja ili otvoriti prostor za neovlašteni pristup, a složenost standarda u distribuiranim okruženjima povećava broj mjesta na kojima se mogu javiti ranjivosti vezane uz autentifikaciju i integritet poruka [5][6].

## 4.3. DNP3

DNP3 (Distributed Network Protocol 3) dugo se primjenjuje u elektroenergetskim i industrijskim upravljačkim sustavima zahvaljujući pouzdanosti prijenosa podataka i dobroj prilagodbi radu na slabijim komunikacijskim kanalima. Izvorne verzije protokola nisu sadržavale kriptografske mehanizme, pa je radi unaprjeđenja sigurnosti razvijena nadogradnja DNP3 Secure Authentication v5 (DNP3 SA v5), standardizirana normom IEEE 1815-2012. Ona uvodi obostranu autentifikaciju između upravljačkog sustava i RTU uređaja i preporučuje se svugdje gdje protokol radi u IP okruženju [13]. U Tabeli I je prikazan usporedni pregled komunikacijskih protokola u distribucijskim mrežama.

*Tabela I* – Usporedni pregled komunikacijskih protokola u distribucijskim mrežama

| Protokol | Tipična primjena | Glavna prednost | Tipičan sigurnosni rizik | Preporučena zaštita |
|---|---|---|---|---|
| **IEC 60870-5-104** | Daljinsko upravljanje i nadzor udaljenih postrojenja | Integracija u TCP/IP mrežne arhitekture | Prisluškivanje, manipulacija prometom, replay napadi | TLS enkripcija, obostrana autentifikacija, mrežna segmentacija |
| **IEC 61850** | Komunikacija unutar postrojenja i između IED uređaja | Standardizirani model podataka i interoperabilnost | Neovlašteni pristup, pogrešna konfiguracija SCL datoteka, kompromitacija integriteta | Kontrola pristupa, sigurna konfiguracija, nadzor prometa |
| **DNP3** | Telemetrijski i industrijski upravljački sustavi | Pouzdan rad i dobra prilagodba različitim komunikacijskim uvjetima | Nedostatak izvorne kriptografije, lažno predstavljanje, izmjena poruka | Sigurna autentifikacija, zaštita cjelovitosti, dodatni sigurnosni slojevi |

# 5. TIPIČNE RANJIVOSTI KOMUNIKACIJSKIH SUSTAVA

Ranjivosti komunikacijskih sustava u distribucijskim mrežama proizlaze iz kombinacije tehničkih, organizacijskih i naslijeđenih čimbenika. Najčešći problemi su: korištenje zastarjele

opreme bez podrške za moderne sigurnosne funkcije, nedostatna autentifikacija te slaba ili nepostojeća enkripcija, što otvara prostor za lažno predstavljanje uređaja, prisluškivanje prometa i napade Man-in-the-Middle (MitM). Oslanjanje na javne ili dijeljene komunikacijske mreže uvodi dodatne rizike manjom kontrolom nad prijenosnim putem i povećanom izloženošću vanjskim napadima.

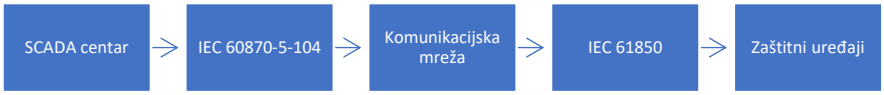
Posebnu kategoriju čini nedostatak nadzora mrežnog prometa. U mnogim OT okruženjima nije implementiran sustav za detekciju upada (IDS – Intrusion Detection System), pa napadačke aktivnosti mogu dulje ostati neotkrivene. RTU i IED uređaji na trafostanicama izloženi su i neautoriziranom fizičkom pristupu, koji može rezultirati manipulacijom konfiguracije ili instalacijom zlonamjernog softvera. Organizacijski čimbenici, nedovoljno definirana prava pristupa, slaba segmentacija mreže i ograničena svijest osoblja, mogu poništiti i tehnički dobro zamišljene zaštitne mehanizme, pa sigurnost komunikacijskog sustava nije samo tehničko, nego i upravljačko pitanje.

### Autentifikacija i upravljanje identitetima

Autentifikacija je temeljni preduvjet za uspostavu povjerenja između uređaja koji komuniciraju putem mreže koja nije pod kontrolom nijednog sudionika. Primjenjuje se infrastruktura javnih ključeva PKI (Public Key Infrastructure) temeljena na X.509 digitalnim certifikatima [11]. Za sve kritične komunikacijske veze između SCADA sustava i terenskih uređaja preporučuje se obostrana autentifikacija (mTLS) umjesto jednosmjerne, a upravljanje certifikatima, uključujući procese izdavanja, obnavljanja i povlačenja, nužan je dio sigurnosne arhitekture svakog OT okruženja.

## 6. KIBERNETIČKE PRIJETNJE SCADA I DA SUSTAVIMA

SCADA i DA sustavi izloženi su širokom rasponu prijetnji, od pokušaja neovlaštenog pristupa do složenih koordiniranih napada na raspoloživost i integritet. Slika 2 prikazuje tijek komunikacije u distribucijskoj mreži.




*Slika 2* – Tijek komunikacije u distribucijskoj mreži

Neovlašteni pristup nastaje iskorištavanjem slabih zaporki, loše konfiguriranih servisa ili ranjivosti u daljinskom pristupu, a napadač može promatrati stanje sustava, mijenjati parametre i slati lažne upravljačke naredbe. Posebno su opasni APT (Advanced Persistent Threat) napadi koji su dugotrajno prikriveni, ciljani i teško detektabilni standardnim mehanizmima. Zlonamjerni softver Industroyer (CrashOverride) iskorišten je 2016. za napad na ukrajinsku elektrodistribucijsku mrežu i uzrokovao stvarne ispade napajanja; prethodni napad 2015. uz pomoć BlackEnergy malwarea prvi je dokumentirani kibernetički napad s fizičkim ispadom električne energije za oko 230.000 korisnika [14][15].

Manipulacija telemetrijskim podacima, alarmima ili statusnim informacijama može pružiti operateru lažnu sliku stanja mreže i dovesti do pogrešnih pogonskih odluka, poput zakašnjelog

reagiranja na kvar ili neispravnog upravljanja sklopnim aparatima. DoS/DDoS (Denial of Service/ Distributed Denial of Service) napadi ograničavaju dostupnost komunikacijskih resursa, a posebno su problematični u IP-baziranim industrijskim mrežama jer ih je teže filtrirati mrežnom opremom ograničenih performansi, poput RTU/IED uređaja. MitM napadi i napadi ponavljanjem poruka (replay attack) iskorištavaju nedovoljno zaštićene komunikacijske kanale, a sve veću prijetnju predstavljaju i napadi na lanac opskrbe (supply chain attack) koji pristižu kroz legitimne kanale, zaražena firmware ažuriranja ili kompromitirani hardver, čime prolaze ispod praga standardnih sigurnosnih provjera.

## 7. POSLJEDICE SIGURNOSNIH INCIDENATA

Sigurnosni incident u komunikacijskom sustavu distribucijske mreže može imati izravne pogonske posljedice, uključujući gubitak komunikacije s uređajima i otežano donošenje operativnih odluka. Posebno kritična je kompromitacija integriteta podataka (npr. naponi, struje, status prekidača), jer može dovesti do pogrešnih upravljačkih akcija. Elektroenergetski sustavi su kiberfizički sustavi (eng. cyber-physical systems – CPS), u kojima su digitalni i fizički sloj izravno povezani, pa kibernetički napad može uzrokovati fizičke posljedice u mreži. Primjeri napada na ukrajinsku elektrodistribucijsku mrežu 2015. i 2016. godine potvrđuju da takvi incidenti mogu izazvati široke ispade napajanja i oštećenja opreme, što naglašava važnost zaštite komunikacijskih sustava u kontekstu otpornosti kritične infrastrukture.

## 8. SIGURNOSNI MEHANIZMI ZA ZAŠTITU KOMUNIKACIJSKIH SUSTAVA

Zaštita komunikacijskih sustava mora se temeljiti na konceptu obrane u dubinu, niti jedna pojedinačna mjera ne može samostalno osigurati zadovoljavajuću razinu zaštite, pa je nužno istodobno primjenjivati komplementarne tehničke, organizacijske i proceduralne mehanizme. Autentifikacija i enkripcija temeljni su tehnički slojevi zaštite. Za TCP/IP komunikacijske veze primjenjuje se TLS 1.2 ili TLS 1.3, definiran kao preporučeni mehanizam u IEC 62351-3 za IEC 60870-5-104 i IEC 62351-4 za IEC 61850 MMS komunikaciju, a kao standardni simetrični algoritam šifriranja koristi se AES-128 ili AES-256. Segmentacija mreže pomoću VLAN (Virtual Local Area Network) tehnologije i vatrozidnih uređaja ograničava lateralno širenje napada; za SCADA okruženja preporučuje se uspostava DMZ (Demilitarized Zone) zone koja fizički i logički odvaja OT mrežu od poslovnih IT mreža i interneta [8][9].

Upravljanje korisničkim pravima i načelo najmanjih privilegija (eng. principle of least privilege) smanjuje mogućnost neovlaštenih radnji u sustavu. Svakom korisniku i uređaju dodjeljuju se isključivo ovlasti neophodne za izvršenje definirane funkcije, a upravljanje ulogama provodi se sukladno modelu RBAC (Role-Based Access Control) definiranom u IEC 62351-8 [11]. Nadzor prometa i detekcija anomalija omogućuju pravodobno otkrivanje sumnjivih aktivnosti. Sustavi za detekciju upada pasivno analiziraju promet i generiraju upozorenja, pri odstupanjima od referentnog ponašanja, dok sustaviza sprječavanje upada (IPS – Intrusion Prevention System) mogu aktivno blokirati sumnjivi promet. Za centraliziranu analizu i korelaciju sigurnosnih događaja iz više izvora primjenjuje se SIEM (Security Information and Event Management) platforma, koja operaterima osigurava cjelovit uvid u sigurnosno stanje sustava.

Zero trust arhitektura predstavlja suvremeni sigurnosni model koji se sve više razmatra i u OT okruženjima. Za razliku od tradicionalnih pristupa koji pretpostavljaju implicitno povjerenje unutar mreže, zero trust načelo polazi od toga da nijedan korisnik, uređaj ni mrežni segment ne smije biti automatski smatran pouzdanim, tj. svaki zahtjev za pristupom mora biti eksplicitno

verificiran, neovisno o lokaciji inicijatora. Primjena ovog modela u elektrodistribucijskim sustavima još je u ranoj fazi, ali predstavlja jedan od strateških pravaca razvoja industrijske kibernetičke sigurnosti.

## 9. ULOGA STANDARDA IEC 62351 I IEC 62443

IEC 62351 temeljni je referentni okvir za sigurnost komunikacijskih sustava u elektroenergetskim mrežama, razvijen upravo zbog toga što industrijski komunikacijski protokoli izvorno nisu sadržavali dostatne sigurnosne funkcije. Za distribucijske mreže posebno su relevantni: IEC 62351-3 (TLS zaštita za TCP/IP protokole, direktno primjenjivo na IEC 60870-5-104) , IEC 62351-4 (sigurnost MMS komunikacije za IEC 61850) , IEC 62351-5 (sigurnost DNP3 i IEC 60870-5 protokola) te IEC 62351-8 (RBAC upravljanje ulogama i pravima pristupa) [11].

Komplementarno, IEC 62443 definira širi organizacijski i tehnički okvir kibernetičke sigurnosti industrijskih upravljačkih sustava, uključujući procjenu rizika i upravljanje životnim ciklusom. Ta dva standarda nadopunjuju se: IEC 62351 adresira sigurnost protokola, IEC 62443 uređuje cjelokupni sigurnosni sustav upravljanja. Za operatore u međunarodnom okruženju primjenjivi su i NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) standardi koji propisuju obvezne mjere zaštite elektroenergetske kritične infrastrukture [12][16].

## 10. IMPLEMENTACIJA SIGURNOSNIH MJERA U ELEKTROENERGETSKIM SUSTAVIMA

Prvi korak u implementaciji sigurnosnih mjera obično uključuje popisivanje komunikacijskih tokova (eng. asset inventory i network traffic baselining), uređaja i protokola te utvrđivanje mjesta na kojima se razmjenjuju najkritičniji podaci i upravljačke naredbe. Nakon toga potrebno je definirati osnovne sigurnosne zone, ograničiti pristupne putove i uvesti strože metode autentifikacije na najosjetljivijim točkama sustava. Sljedeći korak odnosi se na podizanje razine vidljivosti nad komunikacijskom infrastrukturom. To uključuje bilježenje događaja, nadzor prometa, uspostavu postupaka za odgovor na incidente i redovito provjeravanje konfiguracija uređaja. Bez takvih mehanizama operator može imati tehnički implementirane zaštite, ali i dalje ne imati dovoljno uvida u stvarno sigurnosno stanje sustava. Sigurnost komunikacijskih sustava treba biti integrirana u cijeli životni ciklus opreme, od planiranja i nabave do održavanja i zamjene, pri čemu se sigurnosni zahtjevi uključuju u tehničke specifikacije i projektne kriterije. Pri projektiranju i nabavi primjenjuje se načelo Security by Design, gdje su sigurnosne mjere ugrađene od početka, a ne naknadno dodane. U EU kontekstu, operatori distribucijskih mreža obvezni su primjenjivati NIS2 direktivu koja definira upravljanje rizicima, prijavu incidenata i kontinuitet usluga [17].

U elektroenergetskom sektoru Bosne i Hercegovine primjenjuju se osnovna IT/OT mrežna segmentacija te djelomična implementacija IEC 62443 principa kroz IT i OT odvajanje. U Elektroprivredi Hrvatske zajednice Herceg-Bosna koristi se parcijalno upravljanje imovinom i evidencija SCADA/ICS komponenti, dok se komunikacijski protokoli u praksi oslanjaju na IEC 60870-5-104 i Modbus TCP. U dijelu zaštite informacijskih sustava primjenjuju se ISO/IEC 27001 kontrole te pojedini zahtjevi IEC 62443 standarda.

## 11. ZAKLJUČAK

Digitalizacija elektrodistribucijskih mreža donijela je značajne koristi u daljinskom nadzoru, upravljanju i automatizaciji pogona, ali je istodobno uvela nove sigurnosne izazove vezane uz komunikacijsku infrastrukturu. Budući da SCADA i DA sustavi ovise o pouzdanoj i zaštićenoj razmjeni podataka, sigurnost komunikacije temeljni je preduvjet stabilnog rada distribucijske mreže. Ključni izvori rizika su: primjena otvorenih protokola bez adekvatnih zaštitnih mehanizama, zastarjela oprema bez hardverske podrške za kriptografske operacije, nedostatna autentifikacija i ograničena segmentacija mreže. Elektroenergetski sustavi kao kiberfizički sustavi (CPS) pokazuju da kibernetički incidenti mogu imati izravne posljedice na fizički rad mreže, uključujući poremećaje u pogonu i isporuci električne energije.

Zaštita komunikacijskih sustava mora biti višeslojna i prilagođena specifičnostima OT okruženja, u kojemu AIC trijada — dostupnost, integritet i povjerljivost — definira drugačiji redoslijed prioriteta nego u klasičnim IT sustavima. U tom kontekstu primjenjuju se standardizirani tehnički i organizacijski okviri za unaprjeđenje sigurnosti elektroenergetskih komunikacija i industrijskih sustava. U europskom regulatornom okviru, operatori distribucijskih mreža obvezni su primjenjivati mjere upravljanja kibernetičkim rizicima, uključujući prijavljivanje incidenata i osiguranje kontinuiteta usluga. Primjena načela u kojemu su sigurnosni zahtjevi integrirani u svaku fazu životnog ciklusa sustava, od projektiranja i nabave do pogona i zamjene, nužan je uvjet da digitalizacija ne postane izvor novih ranjivosti. Budući razvoj prema pametnim mrežama (smart grid) i integracija naprednih mjernih infrastruktura (AMI – Advanced Metering Infrastructure) dodatno će proširiti napadnu površinu komunikacijskih sustava. To zahtijeva kontinuirano unapređenje sigurnosnih okvira, uključujući primjenu novih metoda detekcije anomalija temeljenih na strojnom učenju i postupno uvođenje zero trust arhitekture u OT okruženja. Samo takav sveobuhvatan i proaktivan pristup može osigurati da digitalizacija doista doprinese većoj pouzdanosti, učinkovitosti i otpornosti budućih elektrodistribucijskih sustava.

## LITERATURA

[1] D. Harinath, M. V. R. Murthy and P. Satyanarayana, „A Review on Security Issues and Attacks in Distributed Systems", *Journal of Advances in Information Technology*, Vol. 8, No. 1, 2017, str. 72–79.
[2] N. Suri, „Distributed Systems Security", *Cyber Security Body of Knowledge (CyBOK)*, Issue 1.0, Lancaster University, 2019.
[3] D. R. Rhead, „Security Considerations in Distributed Systems", *Master's Thesis*, Naval Postgraduate School, Monterey, CA, 1991.
[4] P. Reiher, „Distributed System Security", *Operating Systems: Three Easy Pieces*, Poglavlje 57.
[5] IEC TR 61850-1-1:2026, *Communication networks and systems for power utility automation – Part 1-1: Introduction and overview*, International Electrotechnical Commission (IEC), 2026.
[6] IEC 61850 SER:2026, *Communication networks and systems for power utility automation – ALL PARTS*, International Electrotechnical Commission (IEC), 2026.
[7] IEC 60870-5-104:2006+AMD1:2016, *Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles*, International Electrotechnical Commission (IEC), 2016.

[8] IEC 62351-3:2023, *Power systems management and associated information exchange – Data and communications security – Part 3: Profiles including TCP/IP*, International Electrotechnical Commission (IEC), 2023.
[9] IEC 62351-4:2018+AMD1:2020 CSV, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives*, International Electrotechnical Commission (IEC), 2020.
[10] IEC 62351-5:2023, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*, International Electrotechnical Commission (IEC), 2023.
[11] IEC 62351-8:2026, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control for power systems*, International Electrotechnical Commission (IEC), 2026.
[12] IEC 62443-3-2:2020, *Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design*, International Electrotechnical Commission (IEC), 2020.
[13] IEEE Std 1815-2012, *IEEE Standard for Electric Power Systems Communications – Distributed Network Protocol (DNP3)*, IEEE Power & Energy Society, New York: IEEE, 2012.
[14] Dragos Inc., „CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations", *Dragos Threat Intelligence Report*, June 2017
[15] Electricity Information Sharing and Analysis Center (E-ISAC) and SANS ICS, „Analysis of the Cyber Attack on the Ukrainian Power Grid", *E-ISAC/SANS ICS Report*, March 2016.
[16] NERC CIP Standards CIP-002 through CIP-014, *Critical Infrastructure Protection Standards*, North American Electric Reliability Corporation (NERC), Atlanta, 2023, dostupno na: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx; pristupljeno 2025-06-11.
[17] Directive (EU) 2022/2555, *on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*, European Parliament and Council, *Official Journal of the European Union*, L 333, str. 80–152, 27.12.2022.
[18] IEEE Std 1366-2022, *IEEE Guide for Electric Power Distribution Reliability Indices*, IEEE Power & Energy Society, New York: IEEE, 2022.