SADRŽAJ

1. Uvod

Komunikacijski sustavi u elektroenergetici razvijali su se tijekom vremena, od velikih promjena početkom 20. stoljeća u području telekomunikacija do suvremenih sustava za prikupljanje podataka (engl. *DAS — Data Acquisition Systems*) koji pretvaraju fizikalne veličine u digitalne vrijednosti pogodne za daljnju uporabu. Kvaliteta, pouzdanost i brzina bile su glavne značajke takvih sustava, ali je problem predstavljala propusnost podatka (engl. *bandwidth*), stoga ih je bilo potrebno optimizirati kako bi radili preko slabo propusnih komunikacijskih protokola [6]. Nastankom novih protokola znatno je promijenjen pristup sigurnosti, a važnost pouzdanosti i učinkovitosti sustava dodatno je naglašena procesom liberalizacije tržišta električne energije i troškovima infrastrukturnog održavanja postrojenja [1].

Norma IEC 61850 omogućila je standardizaciju svih procesa u trafostanici. Normom je definiran *Sampled Measured Values* (SMV ili SV) protokol odgovoran za razmjenu digitaliziranih uzorkovanih izmjerenih vrijednosti unutar pametne trafostanice od elektroničkih mjernih transformatora do zaštitnih i upravljačkih releja [3]. Međutim, iako se protokolom prenose kritični podaci, nema ugrađene kriptografske zaštite te ga je lako napasti, mijenjati i lažirati poslane podatke.

Namjera ovog rada je pokazati primjenu norme IEC 61850 i relevantnog protokola u pametnoj trafostanici, odnosno primjer zaštite protokola SMV korištenjem kodova za zaštitu integriteta poruka (engl. *MAC — Message Authentication Code*).

Nakon uvodnog dijela slijedi drugo poglavlje koje donosi povijest razvoja i pregled standarda IEC 61850, strukturu norme i komunikacijske protokole koje definira, te značajke i prednosti koje osiguravaju funkcionalnost i interoperabilnost norme. Treće poglavlje opisuje ulogu norme u trafostanici, te karakteristike, arhitekturu i infrastrukturu pametne trafostanice.

U četvrtom poglavlju razrađena je osnovna tema rada, odnosno korištena je biblioteka *libiec61850* koja implementira normu IEC 61850 i relevantne protokole koji se koriste u trafostanicama. SMV protokol izmijenjen je na način da podržava zaštitu integriteta i autentičnosti poruka, što je ostvareno HMAC algoritmom (engl. *Hash-based*

message authentication code) koji koristi kriptografsku funkciju sažetka SHA256.

Posljednje poglavlje donosi zaključne misli o potrebi informacijske sigurnosti elektroenergetskog sustava, odnosno o važnosti pravovremenih i točnih informacija i čuvanju integriteta elektroenergetskog sustava.

2. IEC 61850

2.1. Povijest razvoja

Ulaskom u digitalno doba dolazi do pojave inteligentnog elektroničkog uređaja (engl. *IED — Intelligent Electronic Device*) koji objedinjuje tisuće analognih i digitalnih pristupnih podatkovnih točaka. IDE-ovi ili moderni zaštitni releji povećali su značaj i važnost informacijske infrastrukture u elektroenergetskom sustavu, ali i potrebu za uvođenjem sigurnosnih normi i boljom učinkovitošću u zaštiti integriteta sustava. Nedostatkom uređaja pokazala se složena konfiguracija i dokumentacija, a ukazala se i potreba za rješavanjem zahtjeva kao što su:

- stalna dostupnost
- podrška sigurnosti
- težnja prema standardu.

Kako bi se zadovoljili spomenuti zahtjevi, američka organizacija za istraživanje i razvoj u energetskoj industriji (engl. *EPRI — Electric Power Research Institute*) započela je rad na njihovom ostvarenju što je proizvelo specifikaciju nazvanu UCA (engl. *Utility Communication Architecture*). Rezultat toga je postao temelj za rad IEC tehničkog odbora broja 57 (engl. *TC57 — Technical Committee Number 57*) radne grupe 10 (engl. *WG10 — Working Group 10*) iz kojeg je 1995. proizašla norma IEC 61850 — *Communication Networks and Systems in Substations* [6]. Sama norma sastoji se od niza dokumenata i doživjela je dosada dva izdanja, izdanje 1.0 (1995.-2004.) koje se sastojalo od 14 dokumenata i izdanje 2.0 (2005.- danas) koje sadrži više od 30 dokumenta.

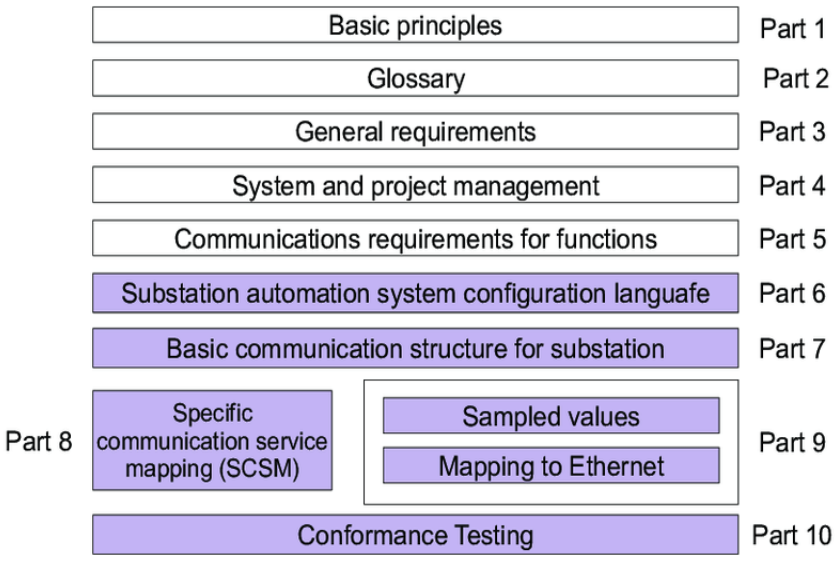
Norma IEC 61850, kao skup komunikacijskih protokola, u početku je razvijena kako bi se koristila u električnim trafostanicama, no njena daljnja primjena i razvoj omogućila je prijelaz na novo rješenje koje se pojavilo u industriji — pametne mreže (engl. *SG — Smart Grids*). SG revolucionarizira tradicionalne elektroenergetske sustave korištenjem stalnog nadzora stanja i protoka podataka [4]. Pametna trafostanica,

koja je dio SG-a, objedinjuje moderne senzore, elektroniku, komunikacijske usluge i programsku podršku (engl. *software*). Unutar trafostanice implementirane su razne napredne mogućnosti kao što su automatizacija kontrole radom trafostanice, distribuirana podjela kontrole te detaljna analiza i pametno donošenje odluka [3]. Norma IEC 61850 standardizira način komunikacije uređaja unutar pametne trafostanice kako bi ostvarili potpunu interoperabilnost [4].

2.2. Pregled norme

2.2.1. Struktura norme

Dokument koji opisuje normu IEC 61850 identificira razne elemente komunikacijske infrastrukture u trafostanici. Sastoji se od 10 poglavlja prikazanih na slici 2.1, pri čemu poglavlja 6 – 10 imaju veću važnost od ostalih. Poglavlja 3, 4 i 5 utvrđuju općenite i specifične funkcionalne zahtjeve u komunikaciji unutar trafostanice [6]. Poglavlje 7 opisuje logički pogled na komunikacijski sustav, kao što je logički model uređaja te apstraktno komunikacijsko uslužno sučelje (engl. *ASCI — Abstract Communication Service Interface*). Kako se ti logički principi implementiraju i koriste u komunikacijskoj mreži objašnjavaju poglavlja 8 i 9 [4], a poglavlje 10 definira metodologiju ispitivanja kako bi se ostvarila usklađenost norme sa raznim protokolima i njihovim ograničenjima [6].

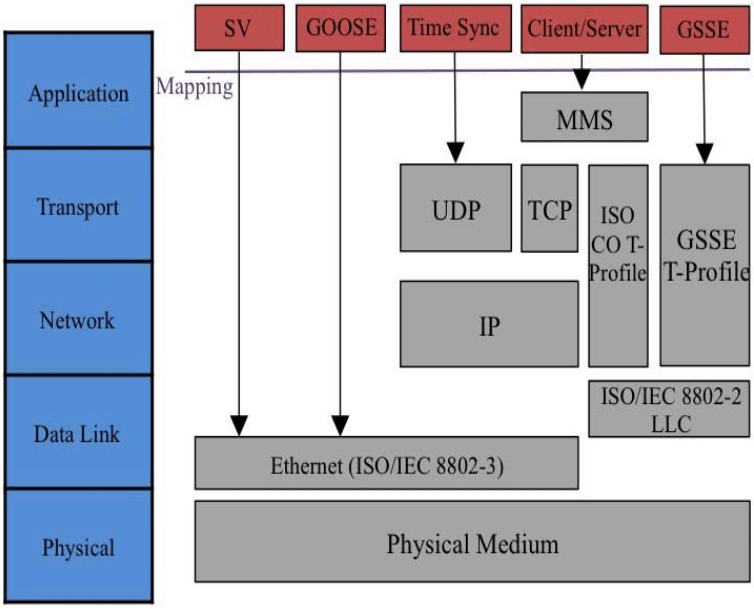


Slika 2.1: Struktura norme IEC 61850

2.2.2. Komunikacijski protokoli

IEC 61850 definira 5 komunikacijskih protokola prikazanih na slici 2.2. SMV i *Generic Object Oriented Substation Event* (GOOSE) su protokoli koji se izravno preslikavaju u sloj podatkovne poveznice (engl. *data link*) kako bi značajno povećali svoje performanse [4]. GOOSE protokol je odgovaran za brz i pouzdan prijenos podataka o događajima kao i signala zaštite i upravljanja preko cijele mreže trafostanice [3]. *Generic Substation State Event* (GSSE) je protokol koji sadrži vlastito preslikavanje prilagođeno njegovim funkcijama. Prethodna tri navedena protokola su vremenski osjetljiva.

Time Sync i *Client/Server* protokoli rješavaju vremensku sinkronizaciju i nadzor uređaja u trafostanici [4]. *Client/Server* protokol koristi *Manufacturing Message Specification* (MMS) koji je zadužen za prijenos vremenskih osjetljivih podataka između uređaja i aplikacija [3]. SMV protokol je detaljno objašnjen u poglavlju 4.2.



Slika 2.2: Komunikacijski protokoli definirani u IEC 61850

2.3. Utjecaj norme

IEC 61850 je stvorena kako bi mogla raditi preko modernih mrežnih tehnologija te pruža ogromnu količinu funkcionalnosti koja smanjuje implementacijske i operacijske troškove u automatizaciji trafostanice. Takvu funkcionalnost tradicionalni komunikacijski protokoli nisu mogli ostvariti jer su bili optimizirani da smanje količinu poslanih

podataka kroz mrežu. Na taj način nisu iskoristili nagli porast propusnosti podataka (engl. *bandwidth*) kojeg omogućuju moderne mrežne tehnologije [6]. Popis važnijih značajki norme donosi poglavlje 2.3.1, a značajnijih prednosti u odnosu na tradicionalni pristup poglavlje 2.3.2.

2.3.1. Značajke

Značajke standarda IEC 61850 su:

1. Objektno orijentirani model podataka

Model sadrži opis samog sebe te tako dopušta usporedbu konfiguracije sustava u skladu s očekivanom konfiguracijom. Logički čvorovi su temeljni gradivni elementi modela. Čvorovi predstavljaju informaciju unutar sustava trafostanice ili informaciju koja je dobivena od vanjskih uređaja. Informacija se sastoji od konfiguracijskih podataka, pločice s imenom i dijagnostičkih podataka [2]. Imena podataka unutar sustava nisu uvjetovana uređajima koji ih koriste ili postavljena od strane korisnika. Definirana su standardom što olakšava otkrivanje značenja tog podatka bez korištenja dodatnih informacija o samom podatku i sustavnim podacima kao što su napon i struja [6].

2. Konfiguracijski jezik

Jezik konfiguracije trafostanice (engl. *SCL — Substation Configuration Language*) je XML temeljen format datoteke koji služi za razmjenu konfiguracijskih informacija između uređaja te konfiguriranje same trafostanice. S obzirom na to da je format datoteke standardiziran može se koristiti i za aplikacije izvan trafostanice [2].

3. Usluge na aplikacijskoj razini

ACSI podržava mnoštvo usluga što daleko nadilazi mogućnosti tradicionalnog pristupa. GOOSE i SMV su samo neki od raznih komunikacijskih protokola [6].

2.3.2. Prednosti

Potreba za jedinstvenim standardom na razini elektroenergetskog postrojenja dovela je do nastanka norme IEC 61850 što je omogućilo interoperabilnost i proširivost sustava s proizvodima različitih proizvođača. Prednosti primjene norme su slijedeće [6]:

1. Uklanjanje dvosmislenosti u nabavi

SCL, uz svoju primarnu svrhu, može poslužiti za definiranje korisničkih zah-

tjeva za trafostanicu i njene uređaje. Korisnici uz pomoć SCL-a mogu detaljno i nedvosmisleno opisati svrhu i ulogu uređaja.

2. Manji troškovi instalacije

IEC 61850 omogućuje uređajima brzu razmjenu podataka i statusa koristeći GOOSE i GSSE preko LAN stanice bez potrebe za spajanjem zasebnih veza za svaki relej, što uvelike smanjuje cijenu ožičenja.

3. Smanjeni troškovi dodavanja proširenja

Nova proširenja se lako dodaju u cjelokupni sustav bez potrebe za mijenjanjem uređaja kojima rad ne ovisi o dodanom proširenju.

4. Niži troškovi integracije

Korištenjem iste tehnologije umrežavanja diljem industrijskog svijeta, troškovi integracije podataka unutar trafostanice znatno su smanjeni. Umjesto ručnog konfiguriranja i održavanja svake pristupne podatkovne točke, IEC 61850 mreže sposobne su isporučivati podatke bez zasebnih komunikacijskih prednjih strana (engl. *front-ends*) i promjene konfiguracije uređaja.

5. Dodavanje novih mogućnosti

Napredne usluge i jedinstvene značajke norme osiguravaju rješenja koja jednostavno nisu moguća u tradicionalnom pristupu. Jedan od takvih primjera su inače preskupe sheme zaštite šireg područja, koje sad postaju izvedive.

3. Pametna trafostanica

Razvojem elektroenergetskog sustava, trafostanice postaju od iznimne važnosti jer omogućuju nadzor i upravljanje radom cijelog sustava. S obzirom na složene pogonske uvjete i pojavu zahtjeva za povećanim korištenjem obnovljive energije, tradicionalne trafostanice više nisu bile konkurente na tržištu, pa dolazi do pojave nove generacije trafostanica, tzv. pametnih trafostanica koje značajno smanjuju troškove izgradnje i održavanja trafostanice [3].

Suvremeni dizajn pametne trafostanice trebao bi težiti standardizaciji te zadovoljiti zahtjeve kao što su interoperabilnost, pouzdanost, sigurnost, prilagodljivost, održivost i smanjen utjecaj na okoliš. Primjenom norme IEC 61850 na pametnu trafostanicu osigurali su se uvjeti za ispunjenje navedenih zahtjeva, pa su pametne trafostanice temeljene na IEC 61850 široko rasprostranjene na svijetu [3].

3.1. Zadaci IEC 61850 u trafostanici

Već je ustanovljeno kako je norma IEC 61850 revolucionarizirala trafostanice. U ovom odjeljku objašnjene su dvije najvažnije uloge norme u trafostanici: kontrola osigurača te mjerenje struje i napona.

3.1.1. Kontrola osigurača

Cjelokupni model kontrole definiran je u IEC 61850–7-2 kao apstraktne usluge i preslikavanje tih usluga u konkretni protokol MMS objašnjeno je u IEC 61850–8-1. Model se sastoji od uređaja kao što su IED i *Human Machine Interface* (HMI) te logičkih čvorova CSWI , XCBR i CILO. Logički čvor CSWI služi za upravljane osiguračem iz kontrolne razine trafostanice, XCBR modelira informaciju dobivenu od osigurača, a CILO predstavlja informaciju o uvjetima blokiranja za otvaranje ili zatvaranje osigurača [2].

IED pristupa osiguraču preko binarnih ulaza i izlaza što kontroliraju otvaranje ili

zatvaranje. Naredbeni lanac ide od HMI-a koji šalje informaciju preko sabirnice stanice (engl. *station bus*) do IED-a. Prije izvršavanja naredbe otvaranja/zatvaranja osigurača IED provjerava trenutne uvjete blokiranja [2].

3.1.2. Mjerenje struje i napona

U trafostanicama struja i napon se mjere u strujnim (engl. *CT — Current Transformer*) i naponskim (engl. *VT — Voltage Transformer*) transformatorima te se kao digitalni uzorci šalju preko komunikacijskog kanala prema IDE-u koji prikuplja te izmjerene vrijednosti. Kod tradicionalnih trafostanica veza između CT/VT-a i IDE-a ostvarivala se analognim signalima, a noviji koncept veze temeljen na slanju digitalnih uzoraka omogućuje SMV protokol [2].

Uređaji koji se koriste izmjerenim vrijednostima moraju povezati izvor sa primljenim digitalnim uzorkom. Stoga CT i VT moraju biti sinkronizirani na način da se digitalnim uzorcima dodaje referenca na vrijeme njihovog odašiljanja [2].

3.2. Model pametne trafostanice

3.2.1. Konfiguracija trafostanice

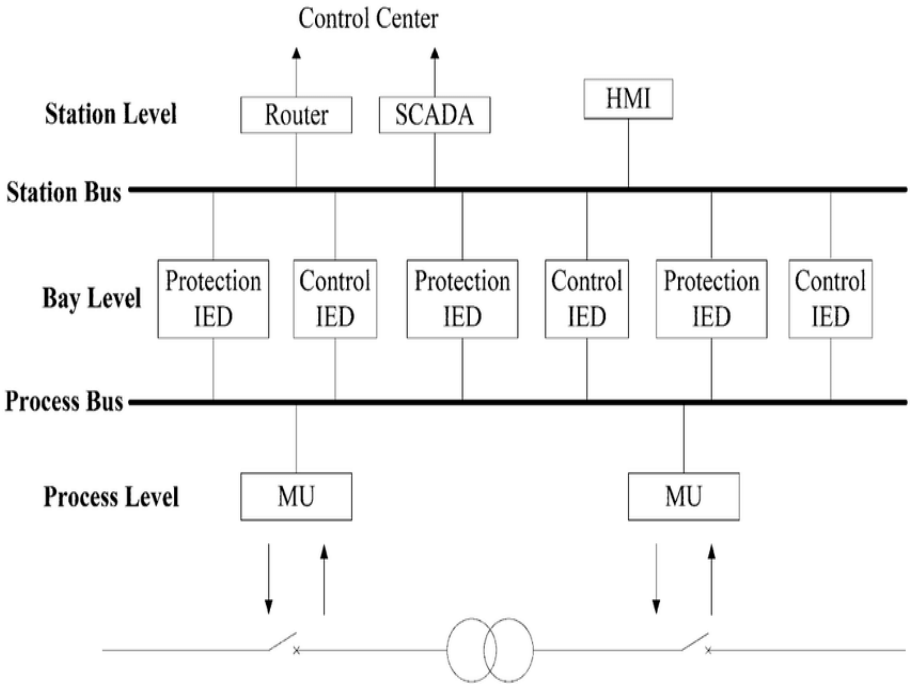
SCL ima veliki utjecaj na projektiranje trafostanice. Cjelokupna konfiguracija sustava i njegov dizajn sadržani su u *Substation Configuration Description* (SCD) datoteci nastaloj iz datoteka — *System Specification Description* (SSD) i *IED Capability Description* (ICD). SSD datoteka sadrži formalnu specifikaciju sustava kao što su različiti dijagrami te funkcionalnost logičkih čvorova, a ICD datoteka detaljan opis sposobnosti i funkcionalnosti IDE-ova unutar trafostanice [2].

U životnom ciklusu trafostanice, SCL se koristi na različite načine, a jedna od uloga SCL-a je i konfiguriranje protoka podataka od IDE-a prema ostalim uređajima. U tu svrhu definiraju se kontrolna izvješća međusobno povezanih skupova podataka [2].

3.2.2. Arhitektura trafostanice

Na slici 3.1 prikazana je arhitektura trafostanice prema standardu IEC 61850. Na procesnoj razini, podaci iz optičkih/elektroničkih senzora napona i struje, kao i informacije o statusu, prikupljat će se i digitalizirati u jedinicama spajanja (engl. *MU — Merging Uint*). Prikupljeni podaci šalju se dalje prema IDE-ima preplaćenima na određene MU-ove fizički smještene na terenu ili unutar trafostanice [6].

Između IDE-ova i uređaja na razini trafostanice (engl. *station level*) nalazi se sabirnica stanice koja podržava 10 – 100 MB *Ethernet* prometa. Sabirnica osigurava povezanost IDE-ova sa uređajima na višoj razini te njihovu međusobnu komunikaciju prema modelu s povratnom vezom (zahtjev za informacijom, zahtjev za konfiguracijom uređaja) ili bez povratne veze (GOOSE poruka). Uređaji i sustavi na razini trafostanice kao što su HMI i *Supervisory Control and Data Acquisition* (SCADA) pružaju funkcije zaštite. kontrole, nadzora i vođenja trafostanice [6].



Slika 3.1: Arhitektura trafostanice prema IEC 61850 standardu

3.2.3. Karakteristike modela

Dva temeljena zahtjeva SG-a su: dinamičko upravljanje stanjem primarne visokonaponske opreme (engl. *HV — High Voltage*) i koordinacija trafostanice sa drugim trafostanicama i kontrolnim centrom više razine. Kako bi ispunila zahtjeve nametnute od strane SG-a, pametna trafostanica ostvaruje svoju funkcionalnost konfiguracijom modularnih komponenti. Karakteristike proizašle iz te funkcionalnosti su [3]:

- digitalizirani podaci, umrežena razmjena informacija, integriranje aplikacija
- prikupljanje i dijeljenje podataka u stvarnom vremenu
- mogućnost interakcije između uređaja radi boljeg rada i održavanja istih
- optimizacija životnog ciklusa sustava na temelju trenutno dobivenih podataka

– poboljšana fleksibilnost, sigurnost i pouzdanost

– ekološki prihvatljiv rad sustava.

3.3. Oslonac pametne trafostanice

Spomenuto je kako je pametna trafostanica nova generacija trafostanica, te su u nastavku analizirane promjene i poboljšanja postojeće opreme koja su dovela do razvoja pametnih trafostanica.

3.3.1. Primarna visokonaponska oprema

Inteligentna oprema kao što je HV unutar pametne trafostanice ima svojstva kao što su digitalno mjerenje, vizualno pamćenje stanja, integrirana funkcionalnost te umrežena kontrola [3].

Nekonvencionalni mjerni transformator (engl. *NCIT — Non-conventional instrument transformers*) i pametni sklopni uređaj (engl. *SSD — Smart switchable device*) su najvažnija inteligentna HV oprema. NCIT je zamijenio konvencionalne elektromagnetske CT-ove i VT-ove te su na taj način izbjegnuti problemi elektromagnetskog zasićenja i kompliciranog sekundarnog ožičenja. Mala veličina, niska cijena, visoka točnost, dug životni vijek i široka propusnost podataka, prednosti su NCIT-a. SSD, za razliku od konvencionalnih sklopnih uređaja, integrira funkcionalnosti praćenja stanja, mjerenja i kontrole, zaštite i komunikacije te zadovoljava zahtjev za integriranim protokom energije i podataka [3].

Pametna primarna HV oprema olakšava obavljanje mnogih naprednih funkcionalnosti kao što su napredno upravljanje imovinom, on-line nadzor i predviđanje kvarova uz smanjenje troškova životnog ciklusa i povećanu pouzdanost trafostanice [3]

3.3.2. Automatizacijski sustav trafostanice

Automatizacija unutar trafostanice je napredovala od udaljene terminalne jedinice do jedinstvene mreže terminalnih jedinica, za što je zaslužan automatizacijski sustav trafostanice (engl. *SAS — Substation Automatization System*). Moderni dizajn SAS-a pomalo napušta klasične funkcije kod tradicionalnih trafostanica kao što su zaštita, nadzor i kontrola primarnog sustava, te se okreće upravljanju i nadzoru dinamičkog dijela sustava, odnosno sabirnica, transformatora i osigurača [3].

Takva mrežna arhitektura uspostavlja hijerarhijsku strukturu i poboljšava cijeli sustav automatizacije kroz manje vrijeme odziva, brži pristup kritičnim podacima te smanjenim vremenom konfiguracije sustava. Primjena SAS-a također omogućava implementiranje novih vrsta zaštite i integriranje obnovljive energije u rad trafostanice [3].

3.3.3. Zaštita

Zaštita u pametnoj trafostanici je orijentirana na cjelokupni sustav, za razliku od tradicionalne zaštite koja primarno štiti opremu. Tako se ranije odvojena zaštita releja, sigurnost mjerenja i upravljanja, integrira u jedinstven digitalni sustav zaštite [3].

Model zaštite je organiziran hijerarhijski, na način da se zaštiti integritet elektromagnetskog sustava i izbjegne kaskadni kvar čak i kod značajnijeg prodora sigurnosti. Razlikujemo lokalni sustav zaštite koji se nalazi u blizini visokonaponske opreme postavljene unutar razvodnog ormara, zaštitu područja postaje i zaštitu šireg područja čime se ostvaruje zaštita na razini sustava. Zaštita područja postaje i šireg područja može se smatrati rezervnom zaštitom u odnosu na lokalnu, kako bi se ubrzalo vrijeme djelovanja za 0.3–0.5 sekundi. Glavna zaštita mora djelovati unutar 20–30 ms, a rezerva do maksimalno 1.2 s da bi se ispunili sigurnosni zahtjevi trafostanice [3].

3.3.4. Mjerenje

Pametna trafostanica garantira pravovremenost, visoku preciznost, pouzdanost i jedinstvenost podataka u procesu mjerenja, za što su većinom zaslužni napredna infrastruktura mjerenja (engl. *AMI — Advanced Metering Infrastructure*) i pametno brojilo (engl. *smart meter*) [3].

Prednosti digitalnog mjernog sustava su brzi prijenos i obrada podataka, visoka sposobnost sprječavanja smetnji, ostvarivanje integriranog i pouzdanog prikupljanja, prijenosa i obrade informacija u stvarnom vremenu te smanjeni troškovi projektiranja. Jedan od nedostataka takvog sustava je moguća velika pogreška mjerenja kada je signal ometan i slabijeg intenziteta [3].

4. Zaštita integriteta SMV protokola

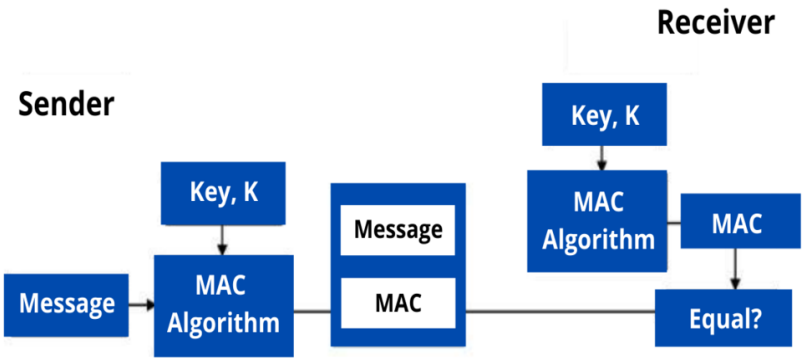
U komunikacijskim protokolima koji se koriste za razmjenu poruka između uređaja unutar trafostanice, šifriranje i dešifriranje poruka uzrokuje dodatna kašnjenja, stoga je zadatak kriptografskih algoritama što efikasnije izvođenje operacija kriptiranja i dekriptiranja kako bi se smanjila dodatna kašnjenja u automatiziranim sustavima i povećala sigurnost i ostvarila povjerljivost podatka [7]. U tu svrhu predložen je cijeli niz kriptografskih algoritama [3], međutim većina se pokazala neupotrebljiva s obzirom na zahtjeve SMV protokola odgovornog za razmjenu digitaliziranih uzorkovanih izmjerenih vrijednosti. Jedini koji je osigurao zahtjeve za integritetom i autentičnošću, te imao zadovoljavajuće performanse je MAC algoritam.

4.1. Kod za zaštitu integriteta poruke

MAC je kod za provjeru autentičnosti i integriteta poruke, poznatiji kao oznaka (engl. *tag*), koji se dodaje na kraj poruke koju se želi zaštiti. Korištenje MAC-a u komunikaciji dvaju entiteta prikazano je na slici 4.1. Pošiljatelj (engl. *sender*) i primatelj (engl. *receiver*) koriste isti ključ za MAC algoritam. Primatelj uspoređuje oznaku primljene poruke sa poslanom oznakom i ukoliko su jednake to je ujedno potvrda da je poruka poslana od točno određenog pošiljatelja zaduženog za njeno slanje te da nije promijenjena.

Sigurni MAC mora spriječiti pokušaje napadača da krivotvori oznake za proizvoljne, odabrane i sve poruke. Bez poznavanja ključa, trebalo bi biti računski nemoguće izračunati oznaku za danu poruku, čak i ako napadač posjeduje cijelu kolekciju poruka i njihovih oznaka [5].

MAC algoritmi mogu se podijeliti na CBC-MAC i HMAC algoritme. CBC-MAC algoritmi kao OMAC i PMAC temelje se na *cipher block chaining* (CBC) procesu enkripcije, a HMAC na kriptografskim funkcijama sažetka (engl. *hash functions*). S obzirom da je HMAC korišten u praktičnom dijelu ovog rada, detaljnije je objašnjen u poglavlju 4.1.1.



Slika 4.1: Princip korištenja MAC-a

4.1.1. HMAC algoritam

HMAC treba funkcionirati s bilo kojom iteriranom kriptografskom funkcijom sažetka i tajnim ključem bilo koje duljine. Primjeri takvih funkcija su dani u tablici 4.1. Pokazalo se da funkcije MD5 i SHA-1 nisu sigurne te da ih ne treba koristiti. Prednosti ovakvog pristupa su: korištenje besplatnih i široko dostupnih (engl. *open-source*) kriptografskih funkcija sažetka, jednostavno korištenje i rukovanje ključevima, omogućena jednostavna zamjena kriptografske funkcije sažetka sa novom, bržom i sigurnijom funkcijom. Sigurnost HMAC-a ovisi o kriptografskoj snazi korištene funkcije sažetka, veličini izlaza te funkcije te veličini i kompleksnosti ključa [5]. Definicija funkcije HMAC je prikazana jednadžbom 4.1.

$$HMAC(K, m) = H((K\ XOR\ opad)\ ||\ (H(K\ XOR\ ipad)\ ||\ m)) \tag{4.1}$$

Korištene oznake:

K ključ

m poruka

H kriptografska funkcija sažetka

B veličina bloka u oktetima kojeg koristi funkcija H

L veličina izlaza funkcije H u oktetima

XOR operacija ekskluzivno ili

opad oktet 0x36 ponovljen B puta

ipad oktet 0x5C ponovljen B puta

|| operacija nadovezivanja

Minimalna duljina ključa trebala bi biti L, a za duljine veće od B ključ se sažme pomoću funkcije H na odgovarajuću duljinu. Duljina ključa veća od L neće znatno poboljšati sigurnost, osim u slučaju kada ključ nije dovoljno nasumičan, odnosno lako je predvidljiv. Povremeno osvježavanje ključa je temeljno za dugoročnu sigurnost [5].

Tablica 4.1: Kriptografske funkcije sažetka

H	B	L
MD5	64	16
SHA-1	64	20
SHA-256	64	32
SHA-512	128	64
SHA3-256	136	32
SHA3-512	72	64

4.2. SMV protokol

Prijenos uzorkovanih vrijednosti vremenski je kritičan, stoga IEC 61850-5 zahtijeva odgodu prijenosa manju od 3ms i mogućnost slanja podataka prema više primatelja. Zbog navedenih zahtijeva SMV protokol ne koristi koncept klijent-poslužitelj (engl. *client-server*) i svih 7 slojeva OSI modela mreža, već koncept objavljivanja-pretplate (engl. *publisher-subscriber*) i uslugu multicast te izravno preslikavanje poruka u *Ethernet* sloj [2]. Entitet koji šalje pakete naziva se *publisher*, a entitet koji prima pakete *subscriber*. Multicast je komunikacijski proces u kojem *publisher* šalje istodobno pakete prema više primatelja, a *subscriber* se preplaćuje na točno određene pakete te koristi podatke koje paket sadrži.

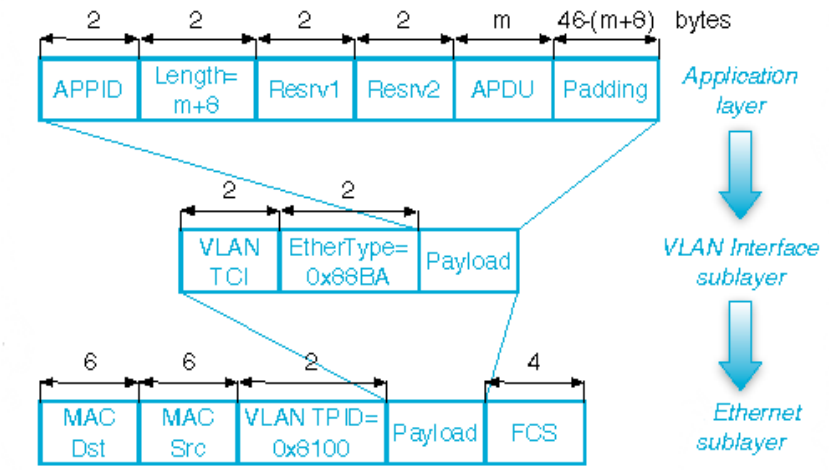
4.2.1. Realizacija protokola u libiec61850

Unutar biblioteke *libiec61850* principi rada SMV protokola implementirani su u dvije datoteke: *sv_publisher.c* i *sv_subscriber.c*. Datoteke su izmijenjene kako bi podržale zaštitu integriteta te je dodana *integrity.c* datoteka koja pruža funkcionalnost kao što su funkcije stvaranja ključa, kreiranje oznake i uspoređivanje dviju oznaka.

Na slici 4.2 prikazana je jedna SMV poruka koja se sastoji od *Ethernet*, VLAN, SMV zaglavlja te polja aplikacijske protokolne jedinice (engl. *APDU — Application Protocol Data Unit*) čija je struktura detaljnije objašnjena u poglavlju 4.2.2. *Ethernet* zaglavlje sastoji se od izvorišne i odredišne adrese, polja *VLAN Tag Protocol Identifier* (VLAN TPID) čija je podrazumijevana vrijednost 0x8100 te *Frame Check Sequence-a* (FCS).

Elementi VLAN zaglavlja su *VLAN Tag Control Information* (TCI) i *EtherType*. TCI se sastoji od polja *Priority*, *Canonical Format Indicator* (CFI) i *VLAN ID*. Polje *Priority* veličine 3 bita koristi se za postavljanje prioriteta poruke koja putuje kroz *Ethernet* mrežu koja podržava prioritetno označavanje, CFI veličine 1 bita označava redoslijed bitova jednog bajta u poruci, a *VLAN ID* je veličine 12 bita sa podrazumijevanom vrijednošću 0x000 i služi sa identificiranje VLAN asocijacije. *EtherType* sa podrazumijevanom vrijednošću 0x88ba jedinstveno identificira korištenje SMV protokola [4].

SMV zaglavlje sastoji se od polja: *APPID*, *Length*, *Resrv1* i *Resrv2*. *APPID* jedinstveno određuje aplikaciju koja koristi SMV protokol te ima podrazumijevanu vrijednost 0x4000. Polje *Length* označava duljinu SMV paketa, što uključuje duljinu zaglavlja i APDU-a u kojem su sadržani podaci za slanje kao što su izmjerene vrijednosti. Stoga, ako je duljina APDU-a m okteta i duljina SMV zaglavlja 8 okteta, polje *Length* ima vrijednost $m + 8$. Polja *Resrv1* i *Resrv2* u izravnoj su vezi sa budućom nadogradnjom protokola i njegovom sigurnošću te su postavljeni na podrazumijevanu vrijednost 0x0000 [4].

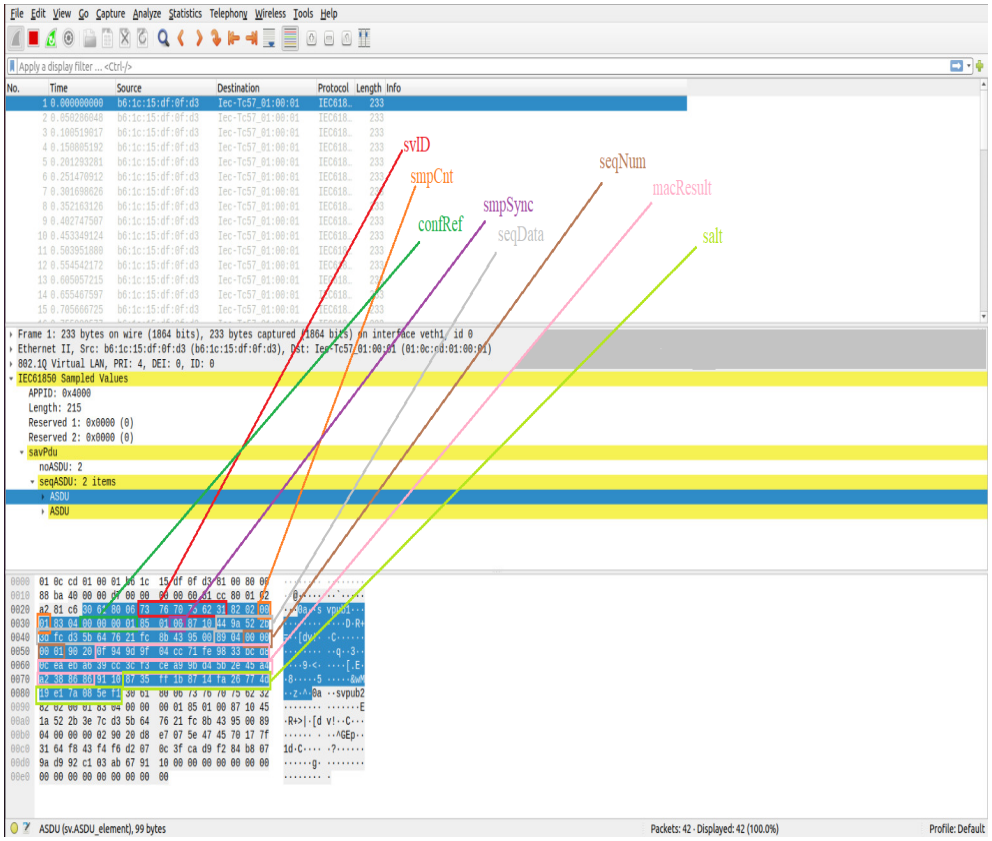


Slika 4.2: Struktura SMV poruke

4.2.2. Aplikacijska protokolna jedinica

Podaci koji se šalju od *publisher-a* prema *subscriber-u* objedinjuju se u aplikacijsku specifičnu jedinicu (engl. *ASDU — Application Specific Data Unit*). APDU se sastoji od nula ili više ASDU-a. Unutar APDU-a se koriste polja *noASDU* i *seqASDU* kako bi se odredio broj i ukupna veličina ASDU-a koji se šalju. ASDU sadrži standardna polja koja predstavljaju informacije o samom ASDU-u i o vrijednostima koje se šalju te polja vezana uz zaštitu integriteta. Nije nužno da ASDU sadrži sva standardna polja, već samo ona potrebna i važna za svrhu korištenja SMV protokola kao što vidimo na primjeru sa slike 4.3 koja prikazuje sadržaj polja ASDU-a uhvaćenog u alatu Wireshark.

Standardna polja definirana normom IEC 61850 su : *svID, datset, smpSynch, smpCnt, confRev, refrTm, smpMod, smpRate, seqData*. Polje *seqData* sadrži izmjerene vrijednosti koje želimo prenositi putem protokola. Kako bi se zaštitio integritet poruke dodano je polje *seqNum*, koje predstavlja redni broj poslanog ASDU-a od strane jednog publisher-a te se ovisno o njegovoj vrijednosti mijenja ključ, polje *macResult* kao oznaka za taj ASDU i polje *salt* koje se koristi kod stvaranja ključa.



Slika 4.3: Struktura ASDU-a

4.3. Zaštita integriteta

4.3.1. Princip rada zaštite

Publisher i *subscriber* koriste isti ključ pri računanju oznake za ASDU, koji se dobiva iz početne lozinke i nasumičnog salt-a te se mijenja kroz vrijeme. Princip zaštite integriteta ostvaren kod *publisher-a* i *subscriber-a* objašnjen je u ovom odlomku.

Algoritam 1 opisuje način rada ostvarene zaštite kod *publisher-a*. Prije slanja ASDU-a preko mreže, *publisher* računa oznaku na temelju podataka koje ASDU sadrži. Istovremeno sa samim ASDU-om šalje se oznaka, korišteni salt te redni broj poslanog ASDU-a na temelju kojeg se osvježava ključ. Kada redni broj dosegne vrijednost N, u ovom slučaju 100 000, ključ se mijenja i broj se resetira, a *publisher* koristi novi ključ za računanje oznake i obavještava *subscriber-a* da se ključ promijenio. Ovaj postupak se ponavlja unedogled, sve dok se zadane postavke ne ponište.

Algorithm 1 Publisher — zaštita integriteta pri slanju jednog SMV APDU-a

Ulaz: $APDU$ – sadrži niz ASDU-a.
asdu := prviAsdu(APDU)
while $asdu \neq null$ **do**
  if $redniBroj(asdu) > N$ **then**
    kljuc := noviKljuc(lozinka, salt)
  end if
  podaci := dohvatiPodatke(asdu)
  oznaka := kreirajOznaku(podaci, kljuc)
  zapisiOznaku(oznaka, asdu)
  asdu := sljedeciAsdu(APDU)
end while
pošalji(APDU)

Zaštita na strani *subscriber-a* opisana je algoritmom 2. *Subscriber* osluškuje na Ethernet sučelju te kada primi paket od *publisher-a* za svaki ASDU sadržan unutar APDU-a izračunava novu oznaku te je uspoređuje sa primljenom oznakom. Ukoliko su oznake jednake, *subscriber* nastavlja s radom. U suprotnome slučaju, otkriva da je integritet narušen te odbija taj ASDU i sve ostale koji će pristići nakon njega. Odbijanje ASDU-a traje sve do trenutka kada je primljena informacija da je *publisher* promijenio ključ, na temelju čega *subscriber* osvježava svoj ključ te nastavlja s radom i prihvaćanjem paketa.

Algorithm 2 Subscriber — zaštita integriteta pri primanju jednog SMV APDU-a

Ulaz: $APDU$ – sadrži niz ASDU-a.
asdu := prviAsdu(APDU)
kljucTrebaPromjenu := false
while $asdu \neq null$ **do**
  if $redniBroj(asdu) > N$ **then**
    kljuc := noviKljuc(lozinka, salt)
    kljucTrebaPromjenu := false
  end if
  if kljucTrebaPromjenu **then**
    continue
  end if
  staraOznaka := ucitajOznaku(asdu)
  podaci := dohvatiPodatke(asdu)
  novaOznaka := kreirajOznaku(podaci, kljuc)
  if $staraOznaka \neq novaOznaka$ **then**
    kljucTrebaPromjenu := true
    continue
  end if
  obradi(asdu)
  asdu := sljedeciAsdu(APDU)
end while

Za stvaranje virtualnih Ethernet sučelja i pokretanje primjera SMV komunikacije potrebno je imati operacijski sustav Linux, a u sklopu ovog rada u tu svrhu korišten je operacijski sustav Ubunutu 20.04 LTS.

4.3.2. Stvaranje virtualnih sučelja

Prije pokretanja primjera koji predstavljaju SMV *publisher-a* i *subscriber-a* nužno je stvoriti virtualna *Ethernet* sučelja preko kojih će *publisher* slati, a *subscriber* primati pakete. U tu svrhu potrebno je otvoriti naredbeni redak i utipkati sljedeće:

1. `$ sudo ip link add veth0 type veth peer name veth1`
2. `$ sudo ip link set veth0 up`
3. `$ sudo ip link set veth1 up`

4. `$ sudo ip link`

Navedenim naredbama napravljena su, povezana i upaljena dva sučelja: *veth0* i *veth1*. Ukoliko je sve izvedeno ispravno, nakon zadnje naredbe ispis bi trebao nalikovati sljedećem:

```
veth1@veth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisc noqueue state UP mode DEFAULT group default qlen 1000
   link/ether d2:3a:ad:ae:ff:d6 brd ff:ff:ff:ff:ff:ff

veth0@veth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
qdisc noqueue state UP mode DEFAULT group default qlen 1000
   link/ether 1a:ce:c8:f4:80:7d brd ff:ff:ff:ff:ff:ff
```

4.3.3. Pokretanje primjera

Potrebno se postaviti unutar mape gdje se nalaze primjeri. Projekt se nalazi na adresi `https://github.com/jurko365/zavrsniRadSMV`. Izvorna mapa projekta je *libiec61850-1.5*. Kako bi se pokrenuo primjer za *subscribera-a*, unutar naredbenog retka (engl. *command prompt*) treba se pozicionirati u izvornu mapu, te zatim utipkati naredbu:

```
$ cd examples/sv_subscriber/
```

Primjer se pokreće naredbom:

```
$ sudo ./sv_subscriber_example veth0 loz12loz123
```

Prvi argument je ime *Ethernet* sučelja a drugi lozinka koja služi za dobivanje ključa. Nakon pokretanja ove naredbe pojavljuje se ispis koji znači da *subscriber* osluškuje na sučelju *veth0* i čeka na primanje paketa:

```
Set interface id: veth0
```

Zatim treba otvoriti novi prozor naredbenog retka te se pozicionirati unutar izvorne mape i utipkati sljedeću naredbu:

```
$ cd examples/sv_publisher/
```

Primjer se pokreće naredbom:

```
$ sudo ./sv_publisher_example veth1 loz12loz123
```

Prvi argument je ime *Ethernet* sučelja a drugi lozinka koja služi za dobivanje ključa, a nakon pokretanja naredbe ispis, koji označava da *publisher* šalje pakete preko sučelja *veth1*, bi trebao izgledati:

```
Using interface veth1
```

Ako je sve napravljeno prema uputama kod *subscriber-a*, koji prima poslane pakete, pojavljuje se ispis nalik sljedećem:

```
.
.
svUpdateListener called
  svID=(svpub1)
  smpCnt: 112
  confRev: 1
   DATA[0]: 1356.665039
   DATA[1]: 11.223457
svUpdateListener called
  svID=(svpub2)
  smpCnt: 112
  confRev: 1
   DATA[0]: 2713.330078
   DATA[1]: 22.446915
svUpdateListener called
  svID=(svpub1)
  smpCnt: 113
  confRev: 1
   DATA[0]: 1357.765015
   DATA[1]: 11.323458
svUpdateListener called
  svID=(svpub2)
  smpCnt: 113
  confRev: 1
   DATA[0]: 2715.530029
   DATA[1]: 22.646915
.
.
```

U slučaju kada je integritet narušen i *subscriber* ustanovi da su podaci unutar ASDU-a kompromitirani, odbacuje taj i sve ASDU-e koji dolaze nakon njega. Poslije promjene ključa, *subscriber* može nastaviti s radom. Navodi se primjer ispisa u ovom slučaju:

```
.
.
svUpdateListener called
  svID=(svpub2)
  smpCnt: 60
  confRev: 1
   DATA[0]: 2598.932617
   DATA[1]: 12.046893
svUpdateListener called
  svID=(svpub1)
  smpCnt: 61
  confRev: 1
   DATA[0]: 1300.566284
   DATA[1]: 6.123446
Data is compromised!!
Waiting for the key to be updated.
svUpdateListener called
  svID=(svpub1)
  smpCnt: 251
  confRev: 1
   DATA[0]: 1509.561646
   DATA[1]: 25.123510
svUpdateListener called
  svID=(svpub2)
  smpCnt: 251
  confRev: 1
   DATA[0]: 3019.123291
   DATA[1]: 50.247021
.
.
```

4.4. Analiza performansi zaštite

Analiza performansi je napravljena na 64-bitnom procesoru *Intel(R) Core(TM) i5-8265U* sa 8 GB RAM-a. U poglavljima 4.4.2 i 4.4.1 je analizirana memorijska i vremenska analiza zaštite za razne kriptografske funkcije sažetka, veličine ključa i *salt-a*. Zbog performansa samog SMV protokola i nužnog zahtijeva na prijenos podataka unutar 4 ms, prednost se daje zaštiti koja ima pogodnije vremenske performanse, osim u slučaju sličnih vremenskih performansi kada se uvažavaju i memorijske performanse korištene zaštite.

4.4.1. Memorijska analiza

U tablici 4.2 je dan pregled memorijskog zauzeća zaštite u ovisnosti o različitim kriptografskim funkcijama sažetka. Polje tablice *ukupno* označava za koliko se okteta veličina ASDU-a povećava u prijenosu preko *Ethernet* mreže kada se koristi zaštita. Odabrana kriptografska funkcija sažetka i veličina *salt-a* koja se koristi u praktičnom dijelu ovog rada se nalazi u osjenčanom retku.

Tablica 4.2: Memorijske performanse zaštite

krpt. funk. saž.	oznaka (okteti)	salt (okteti)	seqNum (okteti)	ukupno (okteti)
SHA224	28	18	4	50
SHA256	32	22	4	58
SHA384	48	38	4	90
SHA512	64	54	4	122

4.4.2. Vremenska analiza

S obzirom da se za zaštitu integriteta koristi HMAC algoritam koji zahtijeva korištenje tajnog ključa za dobivanje oznake, tablica 4.3 prikazuje vremenske performanse stvaranja ključeva različitih veličina. Kako bi se izračunale tražene performanse, stvaranje ključa je ponovljeno 20 puta te je na temelju dobivenih rezultata izračunat prosjek i standardna devijacija . Njihovom analizom odabrano je da minimalna duljina ključa mora biti 32 okteta što je označeno osjenčanim retkom.

U tablici 4.4 je dan prikaz vremenskih performansi stvaranja oznake za jedan ASDU u ovisnosti o različitim kriptografskim funkcijama sažetka i veličini ključa. U tu

svrhu je od strane *publisher-a* poslano 200 uzastopnih APDU-a, koji sadrži 2 ASDU-a, prema *subscriber-u* i za svaki ASDU je izračunano vrijeme stvaranja oznake. Na temelju tih rezultata je dobiven prosjek i standardna devijacija. Iako SHA384 i SHA512 imaju čak i do 4 puta bolje performanse u odnosu na SHA224 i SHA256, zbog zadovoljavajućih vremenskih i boljih memorijskih performansa te dobre sigurnosti same funkcije odabrana je funkcija SHA256 sa minimalnom duljinom ključa od 32 okteta što je označeno osjenčanim retkom.

Tablica 4.5 daje uvid u cjelokupne vremenske performanse zaštite. To obuhvaća vrijeme stvaranja oznaka za ASDU-e sadržane unutar APDU-a na strani *publisher-a*, vrijeme prijenosa APDU-a preko mreže od *publisher-a* prema *subscriber-u*, vrijeme uspoređivanja oznaka i obrade podataka unutar ASDU-a kod *subscriber-a*. Prosjek i standardna devijacija su dobiveni na temelju rezultata slanja 200 uzastopnih ADPU-a, svaki sadrži 2 ASDU-a, kroz mrežu i računanja njihovih pojedinačnih vremena, od kojih jedno i uključuje vrijeme potrebno za promjenu ključa. Upravo korištena zaštita, osjenčani redak, ima najbolje vrijeme.

Tablica 4.3: Vremenske performanse stvaranja ključa

ključ (okteti)	prosjek (ms)	standardna devijacija (ms)
20	0.01060	0.00467
28	0.01190	0.00535
32	0.01280	0.00819
48	0.01340	0.00824
64	0.01710	0.00611
70	0.01820	0.01242

Tablica 4.4: Vremenske performanse stvaranja oznake za ASDU

krpt. funk. saž.	ključ (okteti)	prosjek (ms)	standardna devijacija (ms)
SHA224	20	0.02108	0.01296
SHA224	28	0.02189	0.01238
SHA224	32	0.01945	0.01143
SHA224	48	0.02043	0.01191
SHA224	64	0.02130	0.01341
SHA224	70	0.02048	0.01209
SHA256	20	0.02698	0.00788
SHA256	28	0.02852	0.00825
SHA256	32	0.02692	0.00996
SHA256	48	0.02194	0.01365
SHA256	64	0.02162	0.01267
SHA256	70	0.02367	0.01447
SHA384	20	0.00637	0.00468
SHA384	28	0.00596	0.00439
SHA384	32	0.00657	0.00502
SHA384	48	0.00628	0.00641
SHA384	64	0.00580	0.00419
SHA384	70	0.00688	0.00416
SHA512	20	0.00612	0.00405
SHA512	28	0.00587	0.00397
SHA512	32	0.00656	0.00430
SHA512	48	0.00623	0.00476
SHA512	64	0.00638	0.00481
SHA512	70	0.00765	0.00269

Tablica 4.5: Vremenske performanse zaštite

krpt. funk. saž.	ključ (okteti)	prosjek (ms)	standardna devijacija (ms)
SHA224	20	0.33080	0.17618
SHA224	28	0.33840	0.17551
SHA224	32	0.35147	0.18661
SHA224	48	0.34766	0.17627
SHA224	64	0.33750	0.16402
SHA224	70	0.40671	0.15372
SHA256	20	0.29734	0.13940
SHA256	28	0.19931	0.08833
SHA256	32	0.19425	0.04938
SHA256	48	0.34782	0.18126
SHA256	64	0.31703	0.15521
SHA256	70	0.37638	0.17491

5. Zaključak

Pojava suvremenih inteligentnih elektroničkih uređaja (IED) znatno je poboljšala mogućnosti upravljanja i nadzora elektroenergetskih postrojenja. Nedostatkom se pokazala složena konfiguracija i nekompatibilnost uređaja različitih proizvođača, što je rezultiralo otežanom komunikacijom unutar sustava i potrebom za standardizacijom i zaštitom od različitih sigurnosnih prijetnji. Primjenom norme IEC 61850 i njenih protokola povećana je funkcionalnost i interoperabilnost, a smanjeni troškovi procesa automatizacije postrojenja. Nova i poboljšana sigurnosna rješenja omogućila su stalni nadzor stanja i protoka podataka u elektroenergetskim sustavima.

SMV protokol, koji je dio komunikacijske infrastrukture standarda IEC 61850 i služi za prijenos podataka o uzorkovanim mjerenjima, nema nikakvu zaštitu te se podaci mogu lako mijenjati i na taj način manipulirati radom trafostanice. Primjenom koda za zaštitu integriteta poruke ostvarena je zaštita integriteta protokola, te takva vrsta zaštite ima zadovoljavajuće performanse koje su u skladu sa zahtjevima protokola.

Zaštita integriteta cijelog protokola ostvarena je na način da se zaštiti integritet svakog ASDU-a koji sadrži izmjerene vrijednosti. Prednost takvog pristupa je što se ne odbacuje cijeli APDU ukoliko se ustanovi da je integritet narušen, već samo pojedinačni ASDU-i, čime se u konačnosti smanjuje cjelokupni broj odbačenih ASDU-a. Buduću nadogradnju sustava zaštite moguće je ostvariti na drugačiji način. Takva zaštita bi zaštitila integritet cijelog APDU-a te ako se kompromitiraju podaci makar jednog ASDU-a odbacuje se cjelokupni APDU. Iako prvi pristup radi dobro za APDU koji sadrži malo ASDU-a, potrebno je implementirati drugi pristup te ih međusobno usporediti na puno većim APDU-ima i odabrati bolji.

LITERATURA

[1] Vibor Belašić, Juraj Šimunić, i Branka Dobraš. Substation process information modeling due to technological achievements, standardization and liberalization. *Engineering review : znanstveni časopis za nove tehnologije u strojarstvu, brodogradnji i elektrotehnici*, 30:35–47, 2010. ISSN 1330-9587.

[2] Christoph Brunner. Iec 61850 for power system communication. U *2008 IEEE/PES Transmission and Distribution Conference and Exposition*, stranice 1–6, 2008. doi: 10.1109/TDC.2008.4517287.

[3] Qi Huang, Shi Jing, Jian Li, Dongsheng Cai, Jie Wu, i Wei Zhen. Smart substation: State of the art and future development. *IEEE Transactions on Power Delivery*, 32 (2):1098–1105, 2017. doi: 10.1109/TPWRD.2016.2598572.

[4] Jakub W. Konka, Colin M. Arthur, Francisco J. Garcia, i Robert C. Atkinson. Traffic generation of iec 61850 sampled values. U *2011 IEEE First International Workshop on Smart Grid Modeling and Simulation (SGMS)*, stranice 43–48, 2011. doi: 10.1109/SGMS.2011.6089025.

[5] Dr. Hugo Krawczyk, Mihir Bellare, i Ran Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, Veljača 1997. URL `https://www.rfc-editor.org/info/rfc2104`.

[6] R.E. Mackiewicz. Overview of iec 61850 and benefits. U *2006 IEEE Power Engineering Society General Meeting*, stranice 8 pp.–, 2006. doi: 10.1109/PES.2006.1709546.

[7] Stjepan Sučić i Hrvoje Keserica. Iec 62351 - information security in electrical power systems. stranica 5, 2009.

Zaštita protokola SMV korištenjem kodova za zaštitu integriteta poruka

Sažetak

Potreba za standardizacijom komunikacijskih sustava u elektroenergetici pojavila se sa brzim tehnološkim razvojem, deregulacijom tržišta električne energije i zahtjevima za jednostavnošću i ekonomičnošću. U radu su predočene prednosti primjene norme IEC 61850u razvoju pametne mreže, kao i značaj komunikacijskih protokola u razmjeni informacija između različitih uređaja i sustava unutar trafostanice. Na primjeru je prikazana primjena koda za zaštitu integriteta poruke kako bi se osigurao integritet SMV protokola odgovornog za prijenos uzorkovanih izmjerenih vrijednosti unutar pametne trafostanice. Korištena je poslužiteljska i klijentska biblioteka *libiec61850* koja omogućuje brzu i isplativu implementaciju IEC 61850 protokola. Trend za postizanjem veće učinkovitosti i sigurnosti elektroenergetskih sustava nastavit će s razvojem pametnih mreža i sve složenijih IED-ova različitih proizvođača.

Ključne riječi: IEC 61850, pametna trafostanica, sigurnost komunikacije, IED

Protection of SMV protocol using message authentication codes

Abstract

The need for the standardization of communication systems in the power industry appeared with rapid technological development, deregulation of the electricity market and demands forsimplicity and cost effectiveness. This paper presents the advantages of applying the IEC 61850 standard in the development of a smart grid, as well as the importance of communication protocols in information exchange between different devices and systems within substations. The use of the message authentication code to ensure the integrity of the SMV protocol responsible for the transmission of sampled measured values within a smart substation are shown in the example. The *libiec61850* server and client library was used, which enables fast and cost-effective implementation of the IEC61850 protocol. The trend towards achieving higher efficiency and security of the entire power system will continue with the development of the smart grids and more complex IEDs from different manufacturers.

Keywords: IEC 61850, smart grid, communication security, IED