Osiguravanje komunikacijskog protokola IEC 60870-5-104 koristeći standarde IEC 62351-3 i IEC 62351-5

Cindrić, Ivan

SVEUČILIŠTE U ZAGREBU

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Ivan Cindrić

Osiguravanje komunikacijskog protokola IEC 60870-5-104 koristeći standarde IEC 62351-3 i IEC 62351-5

SPECIJALISTIČKI RAD

Zagreb, 2024.

SVEUČILIŠTE U ZAGREBU

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Ivan Cindrić

Osiguravanje komunikacijskog protokola IEC 60870-5-104 koristeći standarde IEC 62351-3 i IEC 62351-5

SPECIJALISTIČKI RAD

Zagreb, 2024.

UNIVERSITY OF ZAGREB
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING
SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Ivan Cindrić

Securing IEC 60870-5-104 using IEC 62351-3 and IEC 62351-5
Osiguravanje IEC 60870-5-104 koristeći IEC 62351-3 i IEC 62351-5

SPECIALIST THESIS
SPECIJALISTIČKI RAD

Zagreb, 2024.

Specijalistički rad izrađen je na Sveučilištu u Zagrebu Fakultetu elektrotehnike i računarstva u sklopu poslijediplomskog specijalističkog studija informacijske sigurnosti.

Mentor(i): izv. prof. dr. sc. Stjepan Groš

Specijalistički rad ima: 38 stranica

Specijalistički rad br.:_____

Povjerenstvo za ocjenu u sastavu:

1. izv. prof. dr. sc. Marin Vuković – predsjednik
2. izv. prof. dr. sc. Stjepan Groš – mentor
3. prof. dr. sc. Krešimir Grgić, Sveučilište Josipa Jurja Strossmayera u Osijeku Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek - član

Povjerenstvo za obranu u sastavu:

1. izv. prof. dr. sc. Marin Vuković – predsjednik
2. izv. prof. dr. sc. Stjepan Groš – mentor
3. prof. dr. sc. Krešimir Grgić, Sveučilište Josipa Jurja Strossmayera u Osijeku Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek - član

Datum obrane: 9. svibnja 2024.

Summary

This thesis deals with the implementation challenges of securing the communication protocol IEC 60870-5-104 using IEC 62351-3 and IEC 62351-5. In the introduction, the need for such an implementation is briefly described. Then, the family of IEC 62351 standards is described, and the rationale is given for the inclusion of the specific subset of chosen standards. The chosen standards are, as described, IEC 62351-3 and IEC 62351-5, whilst it is noted that some other standards need to at least be aware of. Those two standards are then each described in their own chapters following the same chapter structure. Firstly, the standard is briefly described, then the implementation and the technologies used are presented, and finally, the implementation challenges are touched upon. In the conclusion, the author's view is given on the viability of each of the standards and the way they are formally tested against the standard requirements.

Sažetak

Ovaj rad se bavi implementacijskim izazovima osiguravanja komunikacijskog protokola IEC 60870-5-104 koristeći IEC 62351-3 i IEC 62351-5. U uvodnom poglavlju ukratko je opisana potreba za takvom implementacijom. U idućem poglavlju je opisan IEC 62351, i dano je objašnjenje za odabir specifičnog podskupa dokumenata iz porodice IEC 62351. Odabrani dokumenti, kako je ranije rečeno, su IEC 62351-3 i IEC 62351-5, ali je i napomenuta činjenica da su i drugi dijelovi IEC 62351 barem informativno potrebni. Sljedeća dva poglavlja opisuju ta dva odabrana dokumenta prateći istu strukturu razrade poglavlja. U oba poglavlja je ukratko objašnjen dokument, prezentirane tehnologije i način implementacije, te konačno, opisani problemi na koje se naišlo tijekom implementacije. U zaključku autor daje mišljenja o korisnosti oba dijela IEC 62351 i o načinu formalnog testiranja zahtjeva ta dva dijela IEC 62351.

Sadržaj

1. Uvod

IEC 60870-5-104 protokol (IEC 104) je komunikacijski protokol za udaljenu kontrolu i nadziranje opreme i sustava koristeći mreže temeljene na TCP/IP (engl. *Transmission Control Protocol/Internet Protocol*) protokolu. IEC 104 protokol definira entitete koji se razmjenjuju između upravljane stanice i kontrolne stanice. Ti entiteti su jednaki kao i entiteti u IEC 60870-5-101 (IEC 101). IEC 104 specifikacija kombinira aplikacijski sloj i entitete definirane u IEC 101 s mogućnostima koje nudi TCP/IP. Upravljana stanica je stanica koja se nadzire ili kojom se upravlja, dok je kontrolna stanica iz koje se provodi upravljanje i nadzor. Na kontrolnoj stanici se nalaze SCADA (engl. *Supervisory Control and Data Acquisition*) sustavi [1].

SCADA sustavi se koriste za nadzor i upravljanje stanica u sustavima elektroenergetskog prijenosa i distribucije. Ti sustavi su često od kritične važnosti zbog mogućnosti upravljanja i utjecanja na veliki dio kritične infrastrukture. Zbog tog istog razloga, ti sustavi su često dugotrajni te stoga i zastarjeli. Zastarjeli sustavi često zbog svoje starosti i nemogućnosti popravljanja sadrže ranjivosti koje se mogu iskoristiti. Kao takvi, čine dobru metu za maliciozne napadače. Napadač koji preuzme kontrolu nad SCADA sustavom može negativno utjecati na stabilnost elektroenergetske mreže. Jedan od primjera takvog napada je ruski napad na ukrajinsku elektroenergetsku infrastrukturu 2015. godine, kada je 225 000 ljudi ostalo bez električne energije. Hakeri su preko poslovne mreže uspjeli pristupiti operativnoj mreži i udaljenim pristupom se spojiti na SCADA sustave stanica te ugasiti energiju [2].

Iako je IEC 104 široko korišten u Europi i drugim dijelovima svijeta, činjenica da je stvoren u vrijeme kada informacijska sigurnost nije uzimana u obzir predstavlja problem kada se takav nesiguran protokol koristi u modernom industrijskom okruženju [3].

Protokol ima nesigurne metode autentifikacije te nema propisani način šifriranja komunikacije. Pošto je IEC 104 protokol nesiguran, podložan je raznim ranjivostima. Moguće je mijenjati sadržaj poruka, umetati poruke, prisluškivati poruke, raditi DDoS (engl. *Distributed Denial of Service*) napade, lažno se predstavljati kao izvorišna ili odredišna točka komunikacije i mijenjati odredišta poruka te izvršavati napade poput čovjek-u-sredini (engl. *Man-in-the-middle*) [1].

Ovaj rad opisuje implementaciju zaštitu IEC 104 protokola koristeći IEC 62351. Primarni cilj same implementacije jest izraditi rješenje koje je široko primjenjivo u industriji. Vlastita implementacija šifriranih protokola stoga ne bi bila korisna jer takva implementaciju ne podržavaju uređaji koji su trenutno u tim industrijskim okruženjima. Stoga je odlučeno u obzir uzimati standardizirani način zaštite protokola IEC 104. Grupa WG15 (*engl. Working Group 15*), koja je dio tehničkog odbora TC 57 (*engl. Technical Committee*) komisije IEC (*franc. Commission électrotechnique internationale*) je razvila porodicu normi IEC 62351. Primarni cilj IEC 62351 jest: „Razviti norme za sigurnost komunikacijskih protokola definiranih od IEC TC 57, specifično za IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970 i IEC 61968 seriju protokola. Odnosno, razviti skup normi i/ili tehničkih izvješća koji se bave sigurnošću od jedne krajnje točke do druge krajnje točke. [3]“

Cilj ovog specijalističkog rada je opisati izazove kod implementacije podskupa IEC 62351 normi u kombinaciji s komunikacijskim protokolom IEC 60870-5-104 (IEC 104).

Podskup IEC 62351 normi korištenih u ovoj implementaciji su:

- *IEC 62351-3: Communication network and system security – Profiles including TCP/IP*
- *IEC 62351-5: Security for IEC 60870-5 and derivatives*

Implementirajući IEC 62351-3, zaštićuje se transportni sloj komunikacijskog protokola IEC 104. To se radi šifriranjem poruka transportnog sloja, time osiguravajući da su poruke autentične, tajne i neizmijenjene [3].

Osiguravanjem aplikacijskog sloja pomoću IEC 62351-5 umanjuje se mogućnost dodatnih prijetnji poput utjecaja drugih zaraženih aplikacija na istom računalu koje bi mogle nedopušteno čitati komunikaciju i nesigurnosti komunikacije serijske veze. Povećanjem granuliranosti kontrole pristupa koristeći autentifikacijske mehanizme opisane u IEC 62351-5 također se postiže i veća razina povjerljivosti i autentičnosti podataka [3].

Specijalistički rad je podijeljen u poglavlja koja prate korake pristupa implementaciji. Prvo se opisuje IEC 62351, svi dokumenti koji su sadržani u IEC 62351, kratki opis pojedinih dokumenata, kako su ti dokumenti povezani i razlog za odabir specifičnog podskupa dokumenata iz IEC 62351. Za potrebe implementacije zaštite samo protokola IEC 104 nisu potrebni svi dokumenti iz IEC 62351, jer osim zaštite industrijskih protokola, IEC 62351 opisuje i načine zaštite postrojenja, procedura u postrojenjima, zaštite procesa, dijelova informacijskih sustava, definira mehanizme kontrole pristupa i definira opseg sigurnosnih tema

koje se moraju uzimati u obzir kada se sagledava kibernetička sigurnost elektroenergetskog postrojenja. Pošto se ovaj radi bavi samo implementacijom zaštite IEC 104 komunikacijskog protokola, šira slika koju pruža kompletan IEC 62351 nije potrebna za implementaciju, stoga su odabrani samo IEC 62351-3 i IEC 62351-5 kao dokumenti koji se direktno primjenjuju za implementaciju.

Nakon poglavlja o IEC 62351, opisana je norma IEC 62351-3. Opisuje se proces implementacije IEC 62351-3, način formalnog testiranja implementacije prema zahtjevima dokumenata, testiranje funkcionalnosti te problemi na koje se naišlo tijekom implementacije i testiranja.

Poglavlja koja se odnose na IEC 62351-5 slijede iste korake opisa dokumenta, implementacije, testiranja i opisa problematike.

Testiranje implementacija IEC 62351-3 i IEC 62351-5 se vrši koristeći dokumente IEC TS 62351-100-1 i IEC TS 62351-100-3.

U zaključku se nalazi diskusija o korisnosti dvije opisane norme i o pripadnom načinu testiranja te prijedlozi za unaprjeđenje postojećeg načina procesa implementacije ovih vrsta normi.

Odabrani podskup dokumenata iz skupine normi i tehničkih izvješća IEC 62351 zajedno čini implementaciju zaštite protokola IEC 104, nazvanu „*IEC 104 Secure“*.

Dio implementacije, poput logike komunikacije protokola IEC 104, je javno dostupan kroz radni okvir otvorenog koda (engl. *open-source framework*) zvanog *Hat-Open* [10].

Hat-Open je kolekcija otvorenog koda koja sadrži alate i biblioteke za razvijanje aplikacija koje služe udaljenom nadzoru, kontroli i upravljanju pametnih elektroničkih uređaja poput IoT uređaja, PLC uređaja, uređaja za industrijsku automatizaciju i uređaja za automatizaciju doma. Razvoj *Hat-Open* okvira sponzorira KONČAR Digital [10].

Hat-Open se sastoji od TCP, SSL (TLS) i IEC 104 upravljačkih programa (engl. *driver*), uključujući potrebnu kombinaciju navedenih funkcionalnosti da se stvori sigurna IEC 104 veza. Takvi upravljački programi trebaju na ulazu primiti konfiguracijske parametre poput TCP adresa, vremena čekanja na uspostavljanje veze i postavke TLS veze.

Ulazni konfiguracijski parametri i implementacija ponašanja krajnjih točaka koje obrađuju *IEC 104 Secure* komunikaciju nisu javno dostupni i dio su SCADA sustava zvanog PROZA STATION.

PROZA STATION (PROZA HAT) je napredna SCADA platforma za automatizaciju energetskih sustava i upravljanje kritičnom infrastrukturom. Razvijena je za primjenu u automatiziranom upravljanju distribucijskim sustavima električne energije i transformatorskim stanicama. PROZA STATION potpunu funkcionalnost SCADA sustava za praćenje u stvarnom vremenu i upravljanje primarnom i sekundarnom opremom u distribucijskim podstanicama. Programsko rješenje je razvijeno u Končaru a kao rezultat 40 godina iskustva u razvoju digitalnih rješenja za elektroenergetske sustave i upravljanje elektranama. Ključne značajke uključuju PROZA STATION platforme: [11]

- automatsko čitanje podataka,
- rad na Linux OS-u, u virtualnom okruženju ili na fizičkom računalu,
- sigurnost putem korisničke autorizacije, centraliziranog bilježenja svih događaja u sustavu i sigurnosnih kontrolnih mehanizama,
- jedinstveno rješenje za digitalnu redundanciju u oblaku,
- jednostavna nadogradivost na nove verzije i kompatibilnost s prethodnim verzijama,
- prilagodljivost različitim operacijskim sustavima,
- *open-source* kod,
- grafičko korisničko sučelje temeljeno na web tehnologijmama,
- brza i jednostavna konfiguracija

IEC 104 Secure je implementacija koja pruža sigurnosnu nadogradnju komunikacijskog protokola IEC 104 implementiranog u *Hat-Open*. *IEC 104 Secure* se koristi u PROZA STATION platformi koja je certificirana po IEC 62351-3.

2. Opis porodice normi i tehničkih izvješća IEC 62351

Razlog za definiranje dokumenata koji su dio IEC 62351 jest činjenica da se elektroenergetska industrija sve više oslanja na korištenje informacijskih sustava. U elektroenergetskoj industriji su uvijek bila važna svojstva sigurnosti i pouzdanosti sustava, a kako raste ovisnost o informacijskim sustavima, tako raste i potreba za kibernetičkom sigurnošću. Rastom široke dostupnosti interneta, elektroenergetski sustavi više nisu nepoznate arhitekture napadačima, odnosno, javne informacije o načinu rada protokola, cijelih sustava i infrastrukture tih sustava se mogu naći na internetu što stvara rizik. Industrijski komunikacijski protokoli su najkričniji dio u procesu upravljanja elektroenergetskim sustavima. Industrijskim komunikacijskim protokolima se dohvaćaju informacije i šalju komande uređajima u elektroenergetskim postrojenjima. Iako su od ključne važnosti, dosta takvih protokola nema sigurnosne mehanizme protiv pogrešaka, zatajenja uređaja u postrojenjima, zatajenja komunikacijskih uređaja ili namjerne sabotaže. Porodica normi IEC 62351 pokriva sigurnost komunikacije industrijskih protokola s dokumentima IEC 62351-3, IEC 62351-4, IEC 62351-5 i IEC 62351-6. Međutim, također se uvažava činjenica da je potrebno pružiti i mehanizme zaštite samih krajnjih točaka. Potrebno je omogućiti mehanizme za detekciju upada, provjeru valjanosti sustava, autentifikaciju za pristup kritičnim uređajima i podacima, osiguravanje dostupnosti informacija o kvarovima i greškama, stvoriti mehanizme za sigurnosno kopiranje kritičnih sustava i stvoriti infrastrukturu bilježenja događaja s ciljem omogućavanja lakše istrage u slučaju kritičnih događaja [3].

Opis porodica normi je dan tablično u tablicama numeriranima od 2.1. do 2.9. Norme sa zajedničkim karakteristikama su grupirane zajedno u istu tablicu. Na primjer, svi testni dokumenti su grupiranu u istu tablicu. Opis je dan tablično kako bi se za svaki dokument mogla dati racionalizacija uključivanja ili isključivanja dokumenta iz konačne implementacije *IEC 104 Secure* na uniformiran način. Stupac „Korišteno u implementaciji“ podrobnije opisuje razloge na koji način se dokument koristi u implementaciji *IEC 104 Secure*, ako se koristi. Također, makar se neki dokumenti ne koriste direktno, potrebno je njihovo razumijevanje radi shvaćanja problematike i implementacije sigurnosnih mehanizama nad protokolom IEC 104.

Tablica 2.1. prikazuje prva dva dijela IEC 62351. Prva dva dijela služe kao uvodni dokumenti za opisivanje IEC 62351, problematike, razlog za postojanje IEC 62351 te uvode opće pojmove s kojima čitatelj mora biti upoznat da lakše razumije ostale dijelove IEC 62351.

Tablica 2.1. Uvodni dokumenti koji opisuju IEC 62351.

Ime	Opis	Korišteno u implementaciji
IEC/TS 62351-1: *Introduction*	Daje opis problematike sigurnosti u elektroenergetskom industrijskom okruženju.	Uvod. Nije direktno korišteno u implementaciji, ali potrebno za upoznavanje s problematikom.
IEC/TS 62351-2: *Glossary of Terms*	Uključuje pojmove, definicije i akronime korištene u ostalim IEC 62351 dokumentima.	Nije direktno korišteno u implementaciji, ali potrebno za lakše razumijevanje ostalih IEC 62351 dokumenata.

Fokus trećeg dijela IEC 62351, zvanog *IEC 62351-3: Data and Communication Security – Profiles Including TCP/IP*, jest na sigurnosti transportnog sloja TCP/IP modela. Sigurnost se postiže koristeći protokol TLS (engl. *Transport Layer Security*). IEC 62351-3 je opisan u tablici 2.2.

Tablica 2.2. Dokument koji opisuje sigurnost transportnog sloja

Ime	Opis	Korišteno u implementaciji
IEC 62351-3: *Data and Communication Security – Profiles Including TCP/IP*	Opisuje kako primijeniti zaštitu transportnog sloja s ciljem osiguravanja sigurnosnih zahtjeva povjerljivosti, cjelovitosti i autentičnosti podataka.	**Korišteno u implementaciji.** Glavni dio zaštite implementacije je temeljen na ovom dokumentu.

Dijelovi IEC 62351 četiri, pet i šest se fokusiraju na zaštitu raznih industrijskih komunikacijskih protokola poput porodice protokola IEC 60870-5, DNP3, IEC 61850, MMS, GOOSE i drugih. Ti dijelovi opisuju zaštitu aplikacijskog sloja nudeći mehanizme sigurnosnih proširenja nad pripadajućim protokolima. Pošto je fokus ove implementacije na zaštiti IEC 104 komunikacijskog protokola, odnosno, punim imenom, IEC 60870-5-104, jedan od dokumenata koji ulaze u opseg implementacije jest IEC 62351-5: *Security for IEC 60870-5 and derivatives*. Tablica 2.3. popisuje dijelove IEC 62351 koji se fokusiraju na sigurnost aplikacijskog sloja.

Tablica 2.3. Dokumenti koji opisuju sigurnost aplikacijskog sloja, ovisno o protokolu.

Ime	**Opis**	**Korišteno u implementaciji**
IEC 62351-4: *Data and Communication Security – Profiles Including MMS and Similar Payloads*	Opisuje proces sigurnosne nadogradnje protokola TASE.2 / ICCP, IEC 61850-8-1 i IEC 61850-8-2.	Namijenjeno za druge protokole, a ne za IEC 104. Nije korišteno u implementaciji.
IEC 62351-5: *Data and Communication Security – Security for IEC 60870-5 and Derivatives (i.e., DNP 3.0)*	Opisuje proces sigurnosne nadogradnje protokola porodice IEC 60870- i protokola DNP3.	**Korišteno u implementaciji.** Pruža dodatnu zaštitu specifičnu za IEC 104.
IEC 62351-6: *Data and Communication Security – Security for IEC 61850 Peer-to-Peer Profiles*	Opisuje proces sigurnosne nadogradnje protokola IEC 61850, GOOSE i SV.	Namijenjeno za druge protokole, a ne za IEC 104. Nije korišteno u implementaciji.

Tablica opisuje 2.4. IEC 62351-7. Taj dokument definira apstraktne NSM (engl. *Network System Management*) podatkovne objekte koji se koriste u elektroenergetskom procesnom okruženju u svrhu nadziranja informacijskih sustava.

Tablica 2.4. Dokument koji definira procese mrežnog nadgledanja.

Ime	Opis	Korišteno u implementaciji
IEC 62351-7: *Network and System Management (NSM) of the information infrastructure*	Definira NSM. NSM se koristi za nadziranje mreže, detekciju upada i provjeru performansi i pouzdanosti informacijske infrastrukture.	Fokusira se na mrežno nadgledanje, a ne na sigurnost komunikacije. Nije korišteno u implementaciji.

Tablica opisuje 2.5. opisuje dokumente koji se bave kontrolom pristupa temeljenim na ulogama , načine kako su uloge definirane kroz sustav kriptografskim ključevima i cjelokupan proces životnog ciklusa kriptografskih ključeva i certifikata.

Tablica 2.5. Dokumenti koji opisuju kontrolu pristupa i životni ciklus kriptografskih ključeva.

Ime	Opis	Korišteno u implementaciji
IEC 62351-8: *Role-Based Access Control for Power System Management*	Opisuje procese i korisničke uloge za kontrolu pristupa u elektroenergetskom procesnom okruženju-	Fokusira se na zaštitu krajnjih točaka kontrolom pristupa, a ne na sigurnost komunikacije. Nije korišteno u implementaciji.
IEC 62351-9: *Key Management*	Specificira procese stvaranja, distribuiranja, opozivanja i općenitog rukovanja digitalnim certifikatima i kriptografskim ključevima.	Fokusira se na zaštitu krajnjih točaka, a ne na sigurnost komunikacijskih protokola. Nije korišteno u implementaciji. Međutim, povezano je s IEC 62351-3.

Dokumenti IEC 62351-10, IEC 62351-12 i IEC 62351-13 su dokumenti koji na visokoj apstraktnoj razini preporučaju načine zaštite elektroenergetskog sustava. IEC 62351-10 se fokusira na razne mehanizme sigurnosti koji već postoje i referencira se na druge sigurnosne norme i njihovu interoperabilnost, IEC 62351-12 se fokusira specifično na sigurnost distribuiranih elektroenergetskih sustava, a IEC 62351-13 je općeniti dokument koji definira područja sigurnosti koja moraju biti pokrivena dokumentima koji se bave kibernetičkom sigurnošću u energetici. Tablica 2.6. prikazuje te dokumente i njihovu primjenjivost u implementaciji.

Tablica 2.6. Dokumenti koji opisuju općenite teme sigurnosti u elektroenergetici.

Ime	Opis	Korišteno u implementaciji
IEC 62351-10: *Security Architecture*	Opisuje smjernice za sigurnost elektroenergetskih sustava. Smjernice sigurnosti se temelje na kontrolama i sigurnosnim komponentama te njihovoj međusobnoj interakciji.	Ne koristi se direktno u implementaciji, ali je korisno opisane kontrole imati na umu.
IEC/TR 62351-12: *Resilience for Power Systems with DER Systems*	Opisuje operativne strategije, tehnike i preporuke pomoću kojih se podiže otpornost distribuiranih elektroenergetskih sustava (DER, engl. *Distributed Energy Resources*).	Nije direktno povezano s osiguravanjem općenite vrste komunikacije niti je specifično za IEC 104. Nije korišteno u implementaciji.
IEC 62351-13: *What Security Topics Should Be Covered in Standards and Specifications*	Savjeti o tome koje teme vezane za sigurnost moraju biti pokrivene normama koji su vezani uz područje elektroenergetike.	Ne koristi se direktno u implementaciji, ali je korisno opisane savjete imati na umu.

Tablica 2.7. opisuje IEC 62351-11 koji definira mehanizme osiguravanja XML datoteka. Ako XML datoteke nisu potpisane, mogu biti neovlašteno mijenjane. A ako su potpisane, i dalje mogu biti neovlašteno mijenjane i pristupane. Sigurnosni mehanizmi u ovom dokumentu onemogućuju napade čovjek-u-sredini, povredu integriteta podataka i ponavljanje poruka [4].

Tablica 2.7. Dokument koji opisuje sigurnost XML datoteka.

Ime	Opis	Korišteno u implementaciji
IEC 62351-11: *Security for XML Files*	Definira sigurnosne zahtjeve za razmjenu datoteka u XML formatu. Takve datoteke su korištene u IEC 61970 te i za neke vrste IEC 61850 poruka.	Namijenjeno za druge protokole, a ne za IEC 104. Nije korišteno u implementaciji.

Napade je potrebno uočiti što ranije moguće kako bi se mogle poduzeti obrambene akcije. Kako bi se to omogućilo, potrebno je bilježiti sigurnosno bitne događaje. Proučavanjem tih događaja se može dobiti uvid u potencijalne incidente i saznati njihove uzroke. Tablica 2.8. opsuje IEC 62351-14 koji opisuje kako bilježiti sigurnosne događaje u elektroenergetskom informacijskom sustavu.

Tablica 2.8. Dokument koji opisuje mehanizme bilježenja sigurnosnih događaja.

Ime	Opis	Korišteno u implementaciji
IEC 62351-14: *Cyber Security Event Logging*	Dokument čija je implementacija baziran na *Syslog* sustavu za bilježenje događaja. Sadrži specifikacije o implementaciji bilježenja sigurnosnih zapisa (engl. *Security Logs*)	Ne koristi se direktno u implementaciji jer obuhvaća širu sliku od samo komunikacije. Međutim, IEC 62351-3 i IEC 62351-5 bilježe zapise po strukturi opisanoj ovim dokumentom. Koristi se indirektno.

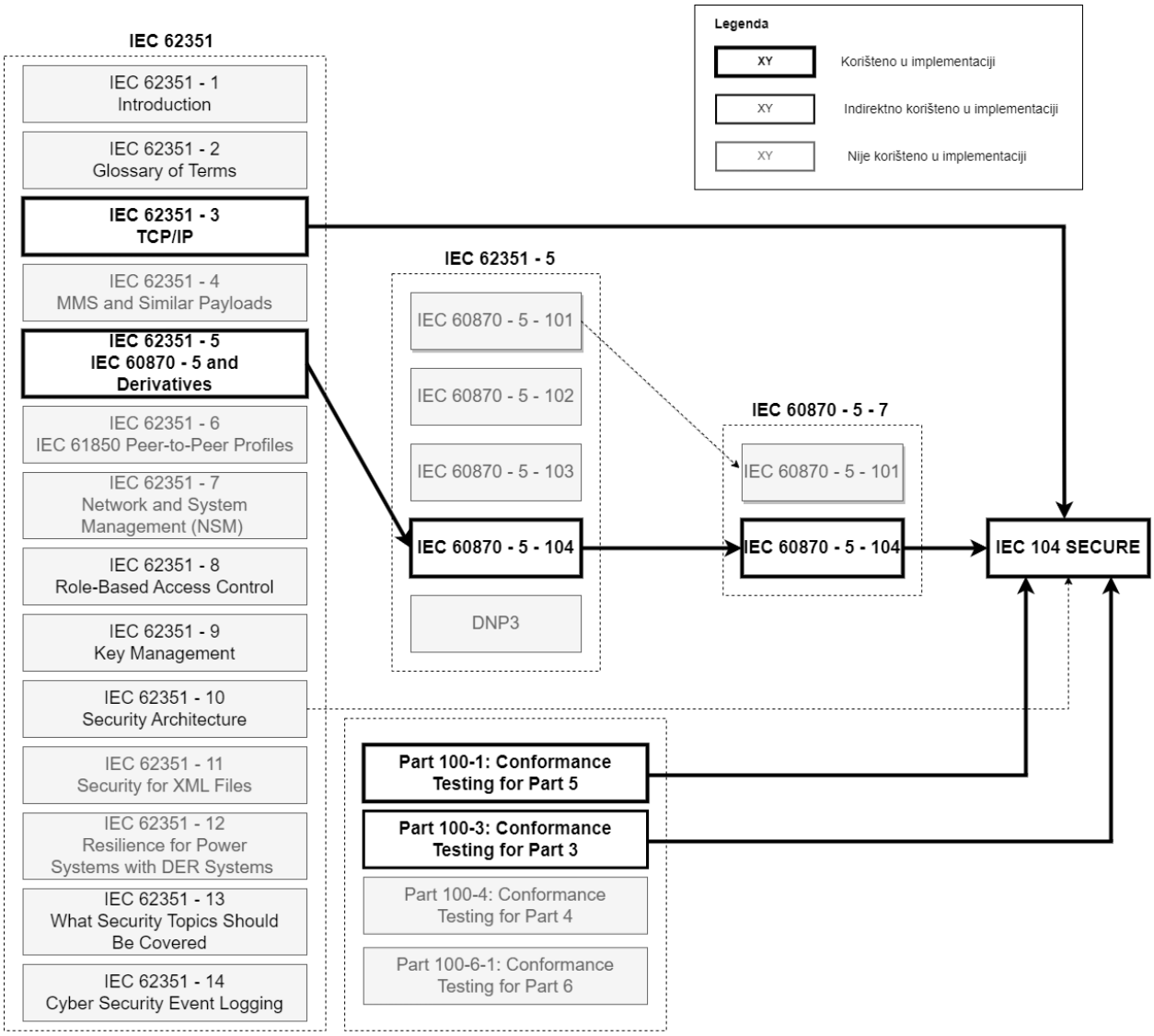
Testovi sukladnosti su definirani za IEC 62351-3, IEC 62351-4, IEC 62351-5 i IEC 62351-6. U implementaciji se radi osiguravanje protokola IEC 104. Osiguravanje tog protokola je definirano kroz IEC 62351-5. IEC 62351-5 zahtjeva da uz osiguravanje aplikacijskog sloja tim dokumentom, potrebno je i osigurati transportni sloj na način opisan u IEC 62351-3. Dakle, za testiranje implementacije se koriste IEC 62351 *Part* 100-1 i IEC 62351 *Part* 100-3. Tablica 2.9. prikazuje dokumente za testiranje sukladnosti.

Tablica 2.9. Dokumenti za testiranje implementacija definiranih u IEC 62351 dokumentima.

Ime	Opis	Korišteno u implementaciji
IEC TS 62351 Part 100-1: *Conformance Testing for Part 5*	Formalan način testiranja implementacija prema zahtjevima dokumenta IEC 62351-5.	**Korišteno u implementaciji.**
IEC TS 62351 *Part 100-3: Conformance Testing for Part 3*	Formalan način testiranja implementacija prema zahtjevima dokumenta IEC 62351-3.	**Korišteno u implementaciji.**
IEC TS 62351 *Part 100-4: Conformance Testing for Part 4*	Formalan način testiranja implementacija prema zahtjevima dokumenta IEC 62351-4.	Namijenjeno za druge protokole, a ne za IEC 104. Nije korišteno u implementaciji.
IEC TS 62351 Part 100-6: Conformance Testing for Part 6	Formalan način testiranja implementacija prema zahtjevima dokumenta IEC 62351-6.	Namijenjeno za druge protokole, a ne za IEC 104. Nije korišteno u implementaciji.

3. Podskup IEC 62351 za implementiranje *IEC 104 Secure*

Nakon što su ukratko objašnjeni svi dijelovi IEC 62351 koristeći tablice, implementacija se može vizualno prikazati. Slika 3.1. prikazuje koji su dijelovi IEC 62351 uključeni u implementaciju te koji su dodatni dokumenti potrebni uz IEC 62351 dokumente. Uz dokumente koji su direktno korišteni, potrebno je i barem površno znanje dokumenata koji su navedeni da su korišteni indirektno radi boljeg razumijevanja implementacije i problematike.



Slika 3.1. Popis dokumenata potrebnih za implementaciju *IEC 104 Secure.*

Iako svi dokumenti porodice IEC 62351 imaju svojih koristi i primjena, glavni fokus ove implementacije je na sigurnosti komunikacije, stoga se odabiru samo dijelovi IEC 62351 koji se bave komunikacijskom sigurnošću i koji se mogu primijeniti na komunikacijski protokol IEC 104. Drugim riječima, u implementaciju ne ulaze svi dijelovi IEC 62351. Sama implementacija se fokusira na IEC 62351-1 i IEC 62351-5.

Međutim, i ostali dokumenti poput IEC 62351-1, IEC 62351-2, IEC 62351-9, IEC 62351-10, IEC 62351-12 i IEC 62351-13 su korišteni indirektno. Implementacija i sami IEC 62351 dokumenti očekuju da uređaji koji koriste IEC 62351-3 i IEC 62351-3 imaju proces rukovanja certifikatima na krajnjim točkama kako je opisano u IEC 62351-9 te da implementacije podržavaju bilježenje sigurnosnih događaja u formatu opisanom IEC 62351-14. Takav sustav bilježenja je korišten u svim ostalim dokumentima porodice IEC 62351 koji imaju potrebu za sigurnosnim porukama. IEC 62351-3 pruža zaštitu transportnog sloja te ga IEC 62351-5 traži kao nužan početni korak. IEC 62351-5 se može primijeniti na druge komunikacijske protokole uz IEC 104, poput IEC 101 i DNP3. Za potrebe ove specifične implementacije se u obzir uzima samo primjena nad komunikacijskim protokolom IEC 104. Implementacija IEC 62351-5 nad komunikacijskim protokolom IEC 104 je opisana dokumentom *IEC 60870-5-7: Transmission protocols - Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)*. IEC 62351 *Part* 100-1 i IEC 62351 *Part* 100-3 služe za formalnu provjeru implementacije prema zahtjevima definiranima u IEC 62351 dokumentima na koje se ti dokumenti odnose.

IEC 104 Secure direktno koristi sljedeće dokumente kako bi se ostvarila implementacija zaštite komunikacijskog protokola IEC 104:

- IEC 62351-3: *Communication network and system security - Profiles including TCP/IP*
- IEC 62351-5: *Security for IEC 60870-5 and derivatives*
- IEC 60870-5-7: *Transmission protocols - Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)*
- IEC TS 62351-100-1: *Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7*
- IEC TS 62351-100-1: *Conformance test cases for IEC 62351-3, the secure communication extension for profiles including TCP/IP*

4. Implementacija norme IEC 62351-3

S obzirom na to da je IEC 62351 kroz godine mijenjan, važno je napomenuti da je specifična verzija korištena za implementaciju rješenja verzija iz 2021. godine, punim imenom IEC TR 62351-3:2021. Ta verzija je u vrijeme implementiranja bila najnovija dostupna.

IEC 62351-3 je dio IEC 62351 koji opisuje kako osigurati povjerljivost, cjelovitost i autentičnost poruka u protokolima koji koriste TCP/IP za prijenos tih poruka. Ti sigurnosni zahtjevi su ispunjeni koristeći TLS (engl. *Transport Layer Security*) protokol preko postojeće nesigurne mreže. To znači da sigurnost aplikacijskog sloja nije dio ovog dokumenta, nego dio drugih dokumenata, poput IEC 62351-5. Međutim upravo zbog razloga što je dokument agnostičan po pitanju aplikacijskog sloja, može se primijeniti u kombinaciji sa svim protokolima pokrivenima IEC 62351, odnosno, u kombinaciji s IEC 62351-4, IEC 62351-5 i IEC 62351-6. Korištenje zaštite transportnog sloja je obavezan zahtjev po IEC 62351-5 i IEC 60870-5-7 [5].

Korištenjem IEC 62351-3 se mogu izbjeći iduće prijetnje i napadi:

- Lažno predstavljanje koje se suzbija korištenjem certifikata koji osiguravaju obostranu autentifikaciju.
- Poruke su šifrirane i sadržaj poruke nije moguće izmijeniti jer se uz poruke šalje i MAC (engl. *Message Authentication Code*) tih poruka pa napad čovjek-u-sredini (engl. *Man-in-the-Middle*) nije moguće izvršiti. Pojam MAC je po funkciji i funkcionalnosti vrlo sličan funkcijama za sažetke (engl. *hash*).
- Ponovno slanje poruka je spriječeno činjenicom da svaka poruka ima redni broj koji se uvećava svakim slanjem. Poruke su, kako je gore navedeno, šifrirane i neizmjenjive, što i taj redni broj čini neizmjenjivim i nečitljivim potencijalnom napadaču.
- Prisluškivanje je također spriječeno činjenicom da je komunikacija šifrirana [6].

Razlog postojanja ovog dokumenta je činjenica da postoje razlike u načinu korištenja TLS-a u klasičnom IT okruženju i u OT industrijskom okruženju, odnosno, u elektroenergetici. Jedna od glavnih razlika je trajanje TCP/IP veze. Očekivano trajanje veze u elektroenergetskom okruženju se mjeri u mjesecima ili čak u godinama. To znači da su veze „vječne“. Zbog tog razloga dokument detaljno propisuje mehanizme obnove sjedničkih ključeva koristeći

postojeće TLS mehanizme. Obnova i ponovno dogovaranje ključeva se moraju izvršavati periodički s ciljem smanjenja mogućnosti otkrivanja sjedničkih ključeva koji bi trajali predugo. Uz trajanje veze, u obzir se mora uzimati i kompatibilnost unatrag. Naime, elektronička oprema korištena u području elektroenergetike je dugog vijeka trajanja, što znači da se u obzir moraju uzimati i starije verzije podržanih protokola i kriptografskih algoritama pošto je moguće da novije verzije nisu podržane. Međutim, svakako se mora uzeti u obzir činjenica da to stvara potencijalne sigurnosne rizike pošto starije verzije TLS-a imaju poznate ranjivosti. Međutim, na umu se mora imati činjenica da je najvažniji sigurnosni zahtjev u takvom OT sustavu, za razliku od IT sustava, dostupnost usluge. To znači da iako napadač može dešifrirati poruke, ako nema potrebe za prisilnim gašenjem sustava ili odbijanjem spajanja, sustav mora raditi unatoč znanim ranjivostima. Dakako, kako je i predviđeno IEC 62351-3, prikladna sigurnosna poruka se mora ispisati u sustavu bilježenja događaja kako je definirano IEC 62351-14.

Dokument IEC 62351-3 opisuje načine nošenja s potencijalnim problemima korištenja TLS-a u elektroenergetskom okruženju prilagođavajući način rada TLS-a da više odgovara takvoj okolini [6].

4.1 Ispitivanje sukladnosti

IEC 104 Secure implementira samo obavezne dijelove IEC 62351-3 i IEC 62351-5 zvane normativni zahtjevni (engl. *Normative requirements*). Razlog za to jest činjenica da ti dokumenti nude više mogućnosti za implementaciju pojedinih mehanizama. Na primjer, prema IEC 62351-3, provjeru opozvanih certifikata je moguće izvesti koristeći CRL (engl. *Certificate Revocation* List) datoteke ili koristeći OCSP (engl. *Online Certificate Status Protocol*). IEC 104 podržava samo CRL mehanizam za provjeru opozvanih certifikata. Za testiranje sukladnosti se koristi dokument *IEC TS 62351-100-3: Conformance test cases for the IEC 62351-3, the secure communication extension for profiles including TCP/IP*. Svrha tog dokumenta je omogućiti formalno testiranje implementacija IEC 62351-3 i osigurati njihovu međusobnu kompatibilnost. Dokument je tabličnog oblika. Sadržaj pojedinog reda je specifični zahtjev, a stupci su obaveznost implementacije zahtjeva, izjava implementacije koja se testira o podršci zahtjeva te komentar ako je potrebno pojašnjenje. Obaveznost zahtjeva se izražava sljedećim oznakama:

- **m** (*mandatory*):
    - Obavezan zahtjev koji mora biti implementiran
    - *Mandatory support. The item shall be implemented.*
- **o** (*optional*):
    - Neobavezan zahtjev koji može biti implementiran
    - *Optional support*. *The item may be implemented.*
- **c** (*conditional*)*:*
    - Uvjetno podržan zahtjev koji može biti implementiran ovisno o uvjetu uz zahtjev
    - *Conditional support. The item shall be implemented as specified by the condition.*
- **x** (*excluded*):
    - Isključen zahtjev koji neće biti podržan
    - *Excluded*. *The item shall not be supported* [7].

Jedan od testova sukladnosti sa IEC 62351-3 po dokumentu IEC 62351-100-3 jest provjera dostupnih verzija protokola TLS, odnosno, SSL. Podrška za protokol SSL mora biti isključena

kako bi implementacija zadovoljavala IEC 62351-3. Prema IEC 62351-3, preporučena i pretpostavljena verzija za uspostavu komunikacije je TLS 1.2., i ta verzija obavezno mora biti podržana. IEC 62351-3 preporuča i podršku za TLS 1.3., kao i mogućnost da krajnje točke uvijek u pregovaranju verzije protokola dogovore najnoviju moguću verziju. Starije verzije protokola ne smiju biti direktno dopuštene, ali mora postojati mogućnost da korisnik dopusti zastarjele verzije protokola zbog ranije spomenute potrebe za kompatibilnošću unatrag. Međutim, kako je propisano IEC 62351-3, u slučaju uspostave komunikacije pomoću zastarjele verzije protokola, mora se ispisati odgovarajuća poruka definira po formatu propisanom IEC 62351-14 [6].

Implementacija dopušta omogućavanje verzija TLS-a 1.0. i 1.1 uz ispisivanje prikladne poruke u *Syslog* sustav za bilježenje događaja. Tablica 4.1. prikazuje strukturu načina na koji se pomoću IEC 62351-100-3 provjerava sukladnost implementacije sa IEC 62351-3.

Tablica 4.1. Podržane TLS verzije u *IEC 104 Secure*.

Zahtjev	Obavezno	Podržano	Komentar
Verzije prije 1.0	x	Ne	Nije podržano. Moderne implementacije protokola TLS ni ne mogu automatski raditi s toliko starim verzijama.
1.0	c	Da*	Kroz konfiguracijske postavke sustava, takvo ponašanje se može omogućiti. Međutim, prema zadanim postavkama, podrška je isključena.
1.1	c	Da*	
1.2	m	Da	Zadana verzija.
1.3	o	Da*	Ova verzija se može dogovoriti tijekom početnog rukovanja, ali pošto je prema IEC 62351-3 podrška za ovu verziju opcionalna, prema zadanim postavkama u *IEC 104 Secure* je ova verzija isključena i korisnik ju mora omogućiti kako bi u početnom rukovanju ova verzija mogla biti dogovorena.

Rukovanje certifikatima je sustav koji je dijelom opisan IEC 62351-3 a dijelom IEC 62351-9. IEC 62351-9 specificira proces rukovanja kriptografskim ključevima i certifikatima, odnosno, kako ih stvarati, distribuirati, opozvati i rukovati njima tijekom cijelog životnog ciklusa ključa [8]. S druge strane, IEC 62351-3 opisuje kako implementacija treba rukovati dostupnim ključevima na krajnjim uređajima. Drugim riječima, IEC 62351-3 zahtjeva da postoji mehanizam provjere opozvanih certifikata, ali ne ulazi u detalje implementacije takvog mehanizma, bilo da se radi o CRL datotekama ili OCSP sustavu. Uz obavezan sustav provjere opozvanih certifikata, IEC 62351-3 također zahtjeva da implementacije pružaju mogućnost podrške za višestruka certifikacijska tijela (CA, engl. *Certificate Authority*) [6].
Tablica 4.2. prikazuje zahtjeve IEC 62351-100-3 koji se tiču rukovanja certifikatima.

Tablica 4.2. Sukladnost *IEC 104* Secure s mehanizmima rukovanja certifikatima.

Zahtjev	Obavezno	Podržano	Komentar
Podrška za više CA-ova.	m	Da	*IEC 104 Secure* koristi sustav za pohranu certifikata od operacijskog sustava.
Certifikati do 8192 okteta.	m	Da	Podrška za certifikate do veličine od 65535 okteta.
Sukladnost sa RFC 5280.	m	Da	Podržano. Kako je opisano IEC 62351-3, očekivani format certifikata je X.509 [5], i takav format *IEC 104 Secure* podržava.
CRL podrška.	m	Da	Podržano. Sustavu je potrebno postaviti putanju do datoteke koja sadrži CRL. Sustav tada prema konfiguriranom periodu provjera promjene u toj datoteci.
OCSP podrška.	o	Ne	Nije podržano.
Autorizacijske liste certifikata, definirane prema IEC 62351-9	o	Ne	Nije podržano.

4.2 Opis implementacije

Funkcionalnost sustava je ostvarena koristeći programski jezik *Python* i *ssl* modul tog jezika uz korištenje mogućnosti korištenja proširenja funkcionalnosti modula kroz programski jezik C. Taj *ssl* modul je *Python* implementacija *OpenSSL* biblioteke. Međutim, *Python* implementacija tog modula ne nudi sve značajke te biblioteke. Neke specifične funkcionalnosti koje nisu podržane modulom su morale biti ručno razvijane za *Python* podršku. Na primjer, u trenu pisanja ovog dokumenta, Python direktno ne podržava upravljanje TLS proširenjem „*renegotiation_info*“ koje prema IEC 62351-3 obavezno mora biti podržano. Zbog toga, koristeći upute koje pruža OpenSSL, vlastita implementacija ponovnog pregovaranja (engl. *Renegotiation*) sjednice je morala biti napisana u programskom jeziku C. Ta implementacija je tada dalje korištena u programskom jeziku *Python*, kako je prikazano u Ispisu 4.1.

```
static PyObject *renegotiate(PyObject *self, PyObject *args) {
   PartialPySSLSocket *sslobj;
   if (!PyArg_ParseTuple(args, "O", &sslobj))
      return NULL;

   // clang-format off
   int result;
   Py_BEGIN_ALLOW_THREADS
   result = SSL_renegotiate(sslobj->ssl);
   Py_END_ALLOW_THREADS

   return PyLong_FromLong(result);
   // clang-format on
}
PyMethodDef methods[] = {{.ml_name = "renegotiate",
                          .ml_meth = (PyCFunction)renegotiate,
                          .ml_flags = METH_VARARGS},
                         {NULL}};

PyModuleDef module_def = {
   .m_base = PyModuleDef_HEAD_INIT, .m_name = "_ssl", .m_methods = methods};


PyMODINIT_FUNC PyInit__ssl() { return PyModule_Create(&module_def); }
```

Ispis 4.1. Implementacija ponovnog pregovaranja.

Sukladnost ponašanja ssl veze s zahtjevima norme je većinski ostvarena prilagođavanjem konteksta ssl veze. SSL kontekst modula ssl služi za detaljno upravljanje postavkama i certifikatima [9].

Koristeći konfiguracijske opcije konteksta i dodatne implementacije u C jeziku, *IEC 104 Secure* je u stanju zadovoljiti sve zahtjeve IEC 62351-3, odnosno, zadovoljiti testiranje prema IEC 62351-100-3. Na primjer, koristeći kontekst, mogu se definirati popisi kriptografskih algoritama koji se smiju koristiti. Ispis 4.2. prikazuje kako se definira dopušten popis kombinacija kriptografskih algoritama (engl. *cypher suites*), kako je definiran IEC 62351-3.

```
ctx.set_ciphers(
        'AES128-SHA256:'
        'DH-RSA-AES128-SHA256:'
        'DH-RSA-AES128-GCM-SHA256:'
        'DHE-RSA-AES128-GCM-SHA256:'
        'DH-RSA-AES128-GCM-SHA256:'
        'ECDHE-RSA-AES128-GCM-SHA256:'
        'ECDHE-RSA-AES256-GCM-SHA384:'
        'TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256:'
        'TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384')
```

Ispis 4.2. Kod definiranja popisa kombinacija kriptografskih algoritama (engl. *cypher suites*).

Jedan od zahtjeva norme, ali i bitno sigurnosno svojstvo same TLS veze jest činjenica da certifikati krajnjih točaka ne smiju biti opozvani. Ispis 4.3. prikazuje kako se provjerava je li certifikat opozvan.

```
def _ext_verify(ssl_object, crl_path):
    cert_bytes = ssl_object.getpeercert(True)
    cert = cryptography.x509.load_der_x509_certificate(cert_bytes)

    crl = cryptography.x509.load_pem_x509_crl(crl_path.read_bytes())

    is_revoked = crl.get_revoked_certificate_by_serial_number(
        cert.serial_number)

    if is_revoked:
        raise Exception('Received endpoint certificate revoked')
```

Ispis 4.3. Provjera statusa opozvanosti certifikata.

Neki zahtjevi poput veličine certifikata, veličine ključeva i valjanost certifikata također se moraju programski provjeravati s ciljem osiguravanja da je komunikacija sukladna sa zahtjevima definiranima u IEC 62351-3. Dio koda koji provjerava veličinu certifikata je prikazan u Ispisu 4.4. *IEC 104 Secure* dozvoljava veličinu certifikata veću od 8192 okteta, ali se zabilježi upozorenje, jer je to traženo normom.

```
def _check_cert(cert_bytes):
    if not cert_bytes:
        raise Exception('peer certificate unavailable')

    if len(cert_bytes) > 8192: // Only a warning, do not stop the program
        mlog.warning('TLS certificate size exceeded')

    cert = cryptography.x509.load_der_x509_certificate(cert_bytes)
    key = cert.public_key()

    if isinstance(key,
                  cryptography.hazmat.primitives.asymmetric.rsa.RSAPublicKey):  # NOQA

        if key.key_size < 2048:
            raise Exception('insufficient RSA key length')

        if key.key_size > 8192:
            mlog.warning('RSA key length greater than 8192')
```

Ispis 4.4. Provjera veličine certifikata i veličine ključa.

Konfiguracija sustava se vrši kombinacijom YAML datoteka i grafičkog sučelja prikazanog na Slici 3.4. Tehnički detalji koji nisu bitni krajnjem korisniku, poput perioda ponovnog pregovaranja i omogućavanja zastarjelih verzija protokola TLS se mogu definirati kroz takvu YAML datoteku.

Međutim, krajnji korisnici su prvenstveno zainteresirani za jednostavno postavljanje komunikacije između IEC 104 uređaja. Zbog toga je većina tehničkih postavki unaprijed definirana kroz YAML konfiguracijske datoteke i krajnji korisnik se ne mora brinuti o njima, dok napredan korisnik ima mogućnost naprednog prilagođavanja sustava.

Jedine postavke koje krajnji korisnik nužno mora definirati su certifikati, odnosno, putanje do certifikata. Te putanje se zadaju kroz grafičko sučelje sustava zvanog PROZA HAT *Editor*, kako je prikazano na Slici 4.1.

Slika 4.1. Postavljanje putanja do datoteka certifikata u programu PROZA HAT *Editor*.

Nakon postavljanja navedenih postavki, sustav se može pokrenuti i komunikacija može započeti. Sigurnosni događaji i drugi događaji bitni za rad sustava se prikupljaju na *syslog* poslužitelju i prikazuju kako je vidljivo na Slici 4.2. *Syslog* poslužitelj kojega koristi PROZA STATION je temeljena na *hat-syslog* implementaciji protokola *Syslog* za bilježenje događaja, a *hat-syslog* je dio radnog okvira *hat-open* [12].

Timestamp filters
From: To:

ID	Timestamp	Severity	Message ID	Message
42658	2023-04-05 11:03:53.792	WARNING	hat.gateway.devices.iec10...	received certificate revoked
42657	2023-04-05 11:03:37.790	WARNING	hat.gateway.devices.iec10...	received certificate revoked
42656	2023-04-05 11:03:21.789	WARNING	hat.gateway.devices.iec10...	received certificate revoked
42655	2023-04-05 11:03:05.786	WARNING	hat.gateway.devices.iec10...	received certificate revoked
42654	2023-04-05 11:02:49.784	WARNING	hat.gateway.devices.iec10...	received certificate revoked
42653	2023-04-05 11:02:35.691	INFORMATIONAL	hat.orchestrator.component	writing stdin for component gui (16617)
42652	2023-04-05 11:02:35.691	INFORMATIONAL	hat.orchestrator.component	component gui (16617) started
42651	2023-04-05 11:02:35.691	INFORMATIONAL	hat.orchestrator.component	writing stdin for component gateway (16615)
42650	2023-04-05 11:02:35.691	INFORMATIONAL	hat.orchestrator.component	component gateway (16615) started
42649	2023-04-05 11:02:35.691	INFORMATIONAL	hat.orchestrator.component	component nginx (16619) started
42648	2023-04-05 11:02:35.691	INFORMATIONAL	hat.orchestrator.component	writing stdin for component event (16602)
42647	2023-04-05 11:02:35.691	INFORMATIONAL	hat.orchestrator.component	component event (16602) started
42646	2023-04-05 11:02:35.690	INFORMATIONAL	hat.orchestrator.component	writing stdin for component monitor (16598)
42645	2023-04-05 11:02:35.690	INFORMATIONAL	hat.orchestrator.component	component monitor (16598) started
42644	2023-04-05 11:02:35.690	INFORMATIONAL	hat.orchestrator.component	writing stdin for component syslog (16596)
42643	2023-04-05 11:02:35.690	INFORMATIONAL	hat.orchestrator.component	component syslog (16596) started
42642	2023-04-05 11:02:35.690	WARNING	hat.eds.license	no license. system running in trial mode for 3 hours, exceeds on 05.04.2023 14:02:30
42641	2023-04-05 11:02:33.782	INFORMATIONAL	hat.gateway.devices.iec10...	TLS session successfully established

Slika 4.2. Grafičko sučelje *hat* sustava *Syslog*.

4.3 Poteškoće s implementacijom IEC 62351-3

U samom IEC dokumentu 62351-3 nisu pronađene pogreške i dokument nedvojbeno opisuje što je potrebno implementirati. Sve funkcionalnosti i proširenja protokola TLS su jasno definirane. Na primjer, za opis implementacije proširenja za ponovno pregovaranje, dokument se referencira na službenu dokumentaciju tog proširenja, RFC 5746 [13]. Takav način opisivanja proširenja jasno definira kako se implementacija IEC 62351-3 mora ponašati. Sva vremena čekanja, veličine ključeva i algoritmi su jasno definirani u zasebnim poglavljima.

Glavni problem na koji se naišlo je tijekom faze implementacije. Naime, tehnologija koja se zbog poslovnih razloga morala koristiti, odnosno, *Python* i *OpenSSL*, ne podržavaju sve potrebne funkcionalnosti da se zadovolje zahtjevi IEC 62351-3. To znači da su se te funkcionalnosti morale razvijati, umjesto da se koriste gotova rješenja, što je produžilo fazu implementacije.

OpenSSL implementacija u programskom jeziku *Python* ne pokriva sve funkcionalnosti potrebne za sukladnost s IEC 62351-3. Ponovno pregovaranje sjednice (engl. *session renegotiation)* i nastavljanje sjednice (engl. *session resumption*) te pripadna proširenja definirana u RFC 5746 i RFC 5246 nisu direktno dostupna kroz *ssl* biblioteku programskog jezika *Python*. Problem jest činjenica da ta proširenja nisu početno omogućena a mora ih se moći omogućiti, što nije moguće kroz *ssl* biblioteku. Iako to nije moguće kroz programski jezik *Python*, nativna implementacija *OpenSSL*-a u programskom jeziku C nudi tu mogućnost. Zbog tog razloga, kako je prije pokazano na Slici 3.1., *Python* funkcija, koja proširuje mogućnost *Python ssl* biblioteke je morala biti implementirana. Također, mora postojati mogućnost provjere prisutnosti tih proširenja, kako je definirano IEC 62351-3:

> „Ako bilo koja strana uoči da *renegotiation_info* proširenje nije prisutno tijekom procesa ponovnog rukovanja, a podrška za to proširenje je naznačeno u početnom rukovanju, podići se sigurnosni događaj *("alarm: secure session renegotiation not supported (renegotiated handshake)").* Sjednica će biti prekinuta. Implementacije koje tvrde da zadovoljavaju IEC 62351-3 će podržavati proširenje definirano u RFC 5746 [6]“.

To znači da, kako je ranije rečeno, mora postojati način provjere postojanja proširenja *renegotiation_info*. Također, isti uvjet se odnosi i na sva ostala proširenja opisana u IEC 62351-3. Ako bilo koje od navedenih proširenja nisu prisutna, primjerena poruka mora biti zabilježena u sustav bilježenja događaja. Zbog toga razloga, potrebno je bilo koristiti još jednu Python biblioteku, zvanu *cryptography* [14].

Cryptography sadrži visoko apstraktne funkcionalnosti, ali i sučelja na niskoj razini za pristup učestalim kriptografskim algoritmima, poput simetričnih i asimetričnih algoritama, funkcije za stvaranje ključeva, funkcije za sažetke poruka. Ti mehanizmi se koriste u TLS komunikacijskim sučeljima [14].

Uzimajući sve to u obzir, završni proizvod je postao kompleksniji nego je bilo očekivano pošto nije bilo moguće ograničiti izradu implementacije na jednu visoko apstraktnu biblioteku. Razlog za korištenje tih specifičnih biblioteka, tehnologija i programskih jezika jest činjenica da su te tehnologije već korištenje u sklopu razvoja PROZA STATION i *hat-open* sustava, a *IEC 104 Secure* je nadogradnja tih sustava.

5. Implementacija norme IEC 62351-5

Ovaj dio porodice IEC 62351 se bavi pitanjem sigurnosti aplikacijskog sloja autentifikacijom poruka koje protokoli šalju. Sigurnost se ostvaruje mehanizmom zvanim „izazov-odgovor“ (engl. *challenge-response*). Kada se primi poruka koja se smatra kritičnom, primatelj na nju može umjesto očekivanog odgovora poslati izazov i čeka odgovor na izazov. Pošiljatelj originalne poruke mora poslati odgovor na izazov prije nego se nastavi normalan tijek komunikacije. Pošiljatelj računa poruku sažetka i šalje tu poruku unutar poruke odgovora na izazov. Primatelj prima odgovor na izazov i uspoređuje poruku sažetka s očekivanim sažetkom. Ako je verifikacija uspješna, originalna poslana poruka se obrađuje. Inače se originalna poruka zanemaruje i bilježi se događaj neuspješnog odgovora na izazov.

Drugi način autentifikacije poruke je takozvani *agresivni način rada*. Ako su oboje strane svjesne da je poruka koja se šalje kritične razine sigurnosti, pošiljatelj može predvidjeti da će se za poruku tražiti odgovor na izazov i uz originalnu poruku automatski šalje i poruku sažetka. Tako se ubrza proces autentifikacije [15].

Važno je napomenuti da je specifična verzija IEC 62351-5 za implementaciju rješenja verzija iz 2013. godine. Za ostvarenje implementacije je potreban i pripadajući dokument koji opisuje implementaciju IEC 62351-5 nad specifičnim protokolom, odnosno, nad IEC 104. To je u ovom slučaju IEC 60870-5-7. Taj dokument postoji samo za verziju IEC 62351-5 iz 2013. godine.

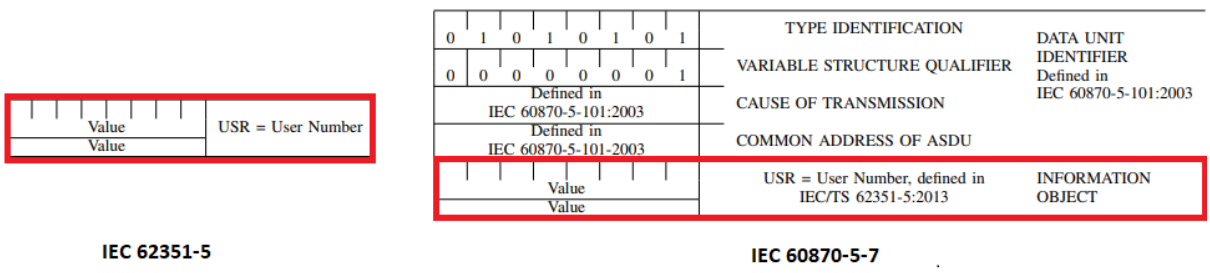
IEC 60870-5-7 opisuje potpunu strukturu poruka, uključujući zaglavlja poruka, za korištenje takvih poruka na način koji je sličan protokolu IEC 104, odnosno, kao nadogradnja na IEC 104 [16].

Izgled poruka definiranih prema IEC 62351-5 i IEC 60870-5-7, implementacija poruka i testiranje implementacije će biti prikazano na primjeru poruke definirane u IEC 62351-5 kao *Key Status Request Message*. U dokumentu IEC 60870-5-7 je definirana poruka s oznakom S_KR_NA_1 koja sadrži dodatne parametre potrebne da se poruka *Key Status Request Message* prenese komunikacijskim protokolom IEC 104.

Na slici 4.1. je prikazana poruka zahtjeva za status ključa sjednice (engl. *key status request message*). IEC 62351-5 definira što takva poruka mora sadržavati na visoko apstraktnoj razini, bez ulaska u to kako pojedini protokoli prenose takve poruke, i što takva poruka mora postići, kao i mjesto takve poruke u slijedu automata stanja.

Kako je opisano u IEC 62351-3, poruka zahtjeva za status ključa sjednice (S_KR_NA_1, *Key Status Request Message*) će indicirati kontrolnoj postaji status tih ključeva i pružit će podatke koje kontrolna postaja mora koristiti za autentifikaciju [15].

Međutim, kako je vidljivo na lijevoj strani Slike 5.1., te informacije nisu dovoljne za slanje takve poruke protokolom IEC 104. Za slanje takve poruke potrebni su i podaci definirani IEC 60870-5-7, prikazani na desnoj strani Slike 5.1. Odnosno, za svaki komunikacijski protokol je način prenošenja poruka definiranih u IEC 62351-5 specifičan. Zbog toga je potreban i dodatan dokument za svaki od tih protokola. U ovom slučaju, radi se o dokumentu IEC 60870-5-7.



Slika 5.1. *Key Status Request Message,* definiran u IEC 62351-5 (lijevo) i IEC 60870-5-7- (desno).

5.1 Ispitivanje sukladnosti

Testiranje sukladnosti provodi se prateći IEC TS 62351-100-1. Cilj ovog dokumenta je omogućiti međusobnu kompatibilnost različitih implementacija IEC 62351-5 pružajući standardiziranu metodu testiranja implementacija protokola kako bi se provjerilo da implementacija ispunjava zahtjeve definirane u IEC 62351-5. Opseg ovog dokumenta je definiranje postupaka i načina testiranja IEC TS 62351-5 i IEC TS 60870-5-7. Definirani testni slučajevi služe za provjeru usklađenosti procedura autentifikacije koje su definirane u IEC TS 62351-5 i detaljnije specificirane u IEC TS 60870-5-7, s ciljem zaštite komunikacije temeljene na IEC 60870-5-101 i IEC 60870-5-104. Međutim, važno je napomenuti, čak i kako je opisano samim dokumentom IEC 62351-100-1, usklađenost s IEC 62351-5 ne jamči kompatibilnost između uređaja koji koriste različite implementacije. Očekuje se da će korištenje ove specifikacije tijekom testiranja minimizirati rizik od nedostatka interoperabilnosti, ali ne i da će ga potpuno ukloniti. Osnovni uvjet za tu kompatibilnost je da obje implementacije prođu testiranje usklađenosti [17].

Dokument obuhvaća testiranje konfiguracijskih parametara, provjeru komunikacije svih očekivanih razmijenjenih poruka i testiranje procedura autentifikacije. Metode autentifikacije uključuju testiranje upravljanjem korisnicima, upravljanje simetričnim ključevima, upravljanje asimetričnim ključevima, upravljanje ključevima sjednice, testiranje mehanizma izazov-odgovor, testiranje agresivnog načina rada.

Cijeli dokument je strukturiran tablično. Svi zahtjevi, odnosno, testni slučajevi su popisani kao redovi tablice. Svaki zahtjev je klasificiran kao obavezan, a za ostale zahtjeve se mora navesti zašto jesu ili nisu uključeni. Također, pošto se razlikuju ponašanja kontrolirajuće i upravljane postaje, dokument nudi mogućnost da se definira za koju stranu komunikacije je implementacija sukladna. Također, neki zahtjevi su specifični samo za kontrolirajuću postaju, a neki zahtjevi su specifični samo za upravljanu postaju.

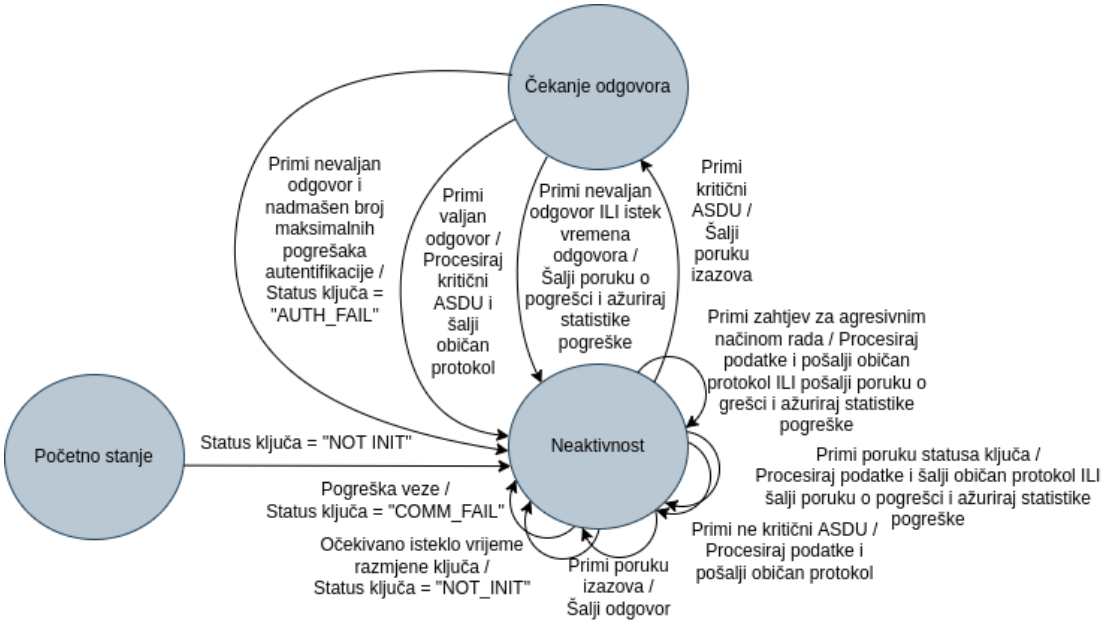
Postupci se testiraju slanjem poruka i provjerom je li primljena poruka očekivana te sadržava li očekivane informacije. Na primjer, navedena poruka za zahtjev statusnog ključa prikazana u slici 4.1 testira se i prikazuje tablično kako je definirano u Tablici 5.1.

Tablica 5.1. Testiranje poruke *Key Status Request Message*(S_KR_NA_1) po IEC 62351-100-1 .

Test	Opis	Referenca	Obaveznost
S_KR_NA_1 ASDU 84 *Session Key Status Request*	VSQ: *Variable Structure Qualifier* SQ = 0 N = 1	IEC TS 60870-5-7:2013, 7.3.4	M (obavezno)
	COT: *Cause of Transmission* *Controlling Station values* = 15 *Controlled Station values* = 44	IEC TS 60870-5-7:2013, 7.3.4	M (obavezno)
	USR: *User Number* *Value range* = <1...65535>	IEC TS 62351-5:2013, 7.2.4.4	M (obavezno)

5.2 Opis implementacije

Proces implementacije je pratio strukturu norme IEC 62351-5. Kao i u IEC 62351-5, prvo su definirane sve poruke i njihovi sadržaji. IEC 62351-5 definira automate stanja, odnosno, očekivane redoslijede poruka. Primjer takvog automata stanja je na Slici 5.2., gdje je dan primjer automata stanja za autentifikaciju upravljane postaje, odnosno, kako se upravljana postaja treba ponašati tijekom procesa autentifikacije. Dakle, postaja je u početnom stanju dok ključ nije iniciran. Kada se ključ inicira, postaja prelazi u stanje neaktivnosti u kojem čeka poruke. Na poruke izazova šalje odgovore, na ne kritične poruke ili poruke o statusu ključa šalje odgovore bez izazova, a na zahtjeve za agresivnim načinom rada šalje poruke na agresivni način. Postaja je u stanju čekanja odgovora kada primi kritičnu poruku i prelazi u stanje neaktivnosti kada primi odgovor ili kada istekne vrijeme čekanja. IEC 62351-5 definira rubne uvjete, bilježenja događaja po IEC 62351-14 te dodatne napomene i završne detalje. Međutim, kako je objašnjeno u poglavlju o problemima implementacije, s implementacijom se stalo tijekom implementacije automata stanja.

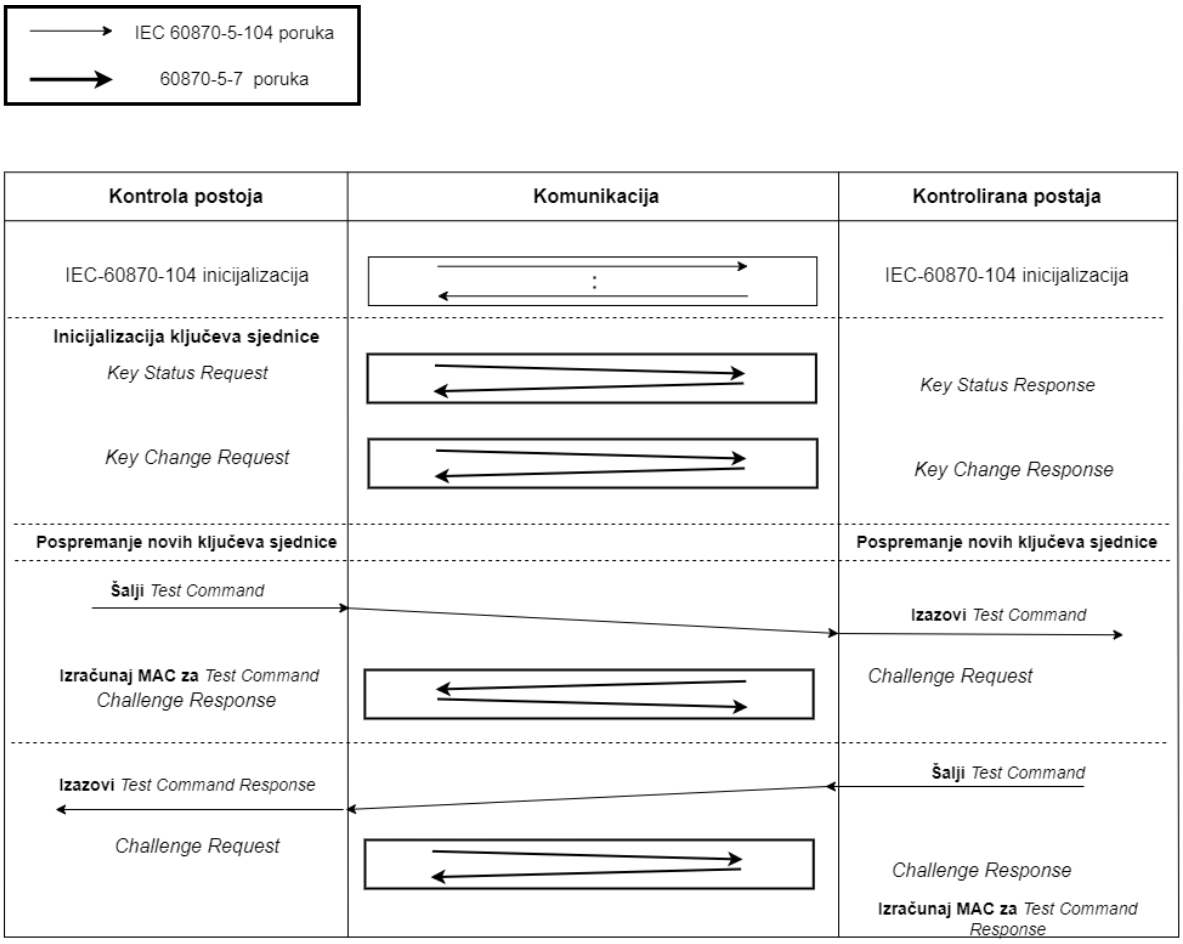


Slika 5.2. Automat stanja za autentifikaciju upravljane postaje

Proces implementacije će biti demonstriran na jednoj poruci. Ta poruka će biti ranije spomenuta *Key Status Request* Message, ili, kako je označena u IEC 60870-5-7, S_KR_NA_1.

Korištena tehnologija, radni okviri, programski jezici i moduli su isti kao za ranije spomenuti dio implementacije prema IEC 62351-3. *Python* implementacija koda je dijelom rađena kao nadogradnja postojećeg IEC 104 *driver* modula radnog okvira *hat-open*. Logika i rukovanje slijedom poruka, kako je opisano u automatu stanja IEC 62351-5, bi bilo implementirano kao IEC 104 *device* u sklopu *hat-gateway* repozitorija.

Slika 5.3. prikazuje kako izgleda inicijalizacija komunikacije po IEC 60870-5-7 i kako se takva inicijalizacija nadograđuje nad postojećom IEC 104 inicijalizacijom. Takav proces inicijalizacije, odnosno, takva slijednost poruka bi bila implementirana u *hat-gateway* repozitoriju. Međutim, zbog razloga objašnjenih u poglavlju o poteškoćama implementacije IEC 62351-5, takva implementacija nikada nije bila dovršena.



Slika 5.3. Klasična IEC 104 inicijalizacija i dodatni koraci definirani u IEC 60870-5-7.

Kako je ranije rečeno, prvi korak implementacije je implementiranje poruka. Svaka poruka je implementirana kao zaseban objekt s atributima koji koreliraju dijelovima poruke definiranima IEC 62351-5. Na primjer, S_KR_NA_1 prema IEC 62351-5 ima samo jedan atribut zvan *user_number* pa je na taj način poruka definirana i u kodu [15].

Ispis 5.1. prikazuje implementaciju poruke S_KR_NA_1 u programskom jeziku *Python*. Sve ostale informacije vezane uz IEC 104 vezane za slanje poruke se automatski procesiraju postojećim *hat-open* IEC 104 *driver*-om.

```
class IoElement_S_KR_NA(typing.NamedTuple):
    user: UserNumber
```

Ispis 5.1. Definicija poruke S_KR_NA u programskom jeziku *Python*.

Kada su sve poruke implementirane, sljedeći korak je pisanje kodera i dekodera poruka za pretvaranje programski definiranih struktura poruka u oktete.

Kako je definirano u IEC 60870-5-7, korisnički broj odnosno *user_number*, u poruci S_KR_NA_1 je veličine dva bajta [17].

Ostali dijelovi poruke nužni za slanje u IEC 104 formatu se automatski procesiraju ranije spomenutim *hat-open* IEC 104 *driver*-om. Dio kodera koji pretvara korisnički broj u podatak od dva bajta je dan u Ispisu 5.2., a pripadajući dekoder koji bajtove s točne pozicije u kodiranoj poruci pretvara u korisnički broj je dan u Ispisu 5.3.

```
elif isinstance(element, common.IoElement_S_KR_NA):
      yield from _encode_int(element.user, 2)
```

Ispis 5.2. Kodiranje poruke S_KR_NA_1.

```
if asdu_type == common.AsduType.S_KR_NA:
    user, rest = _decode_int(io_bytes, 2)

    element = common.IoElement_S_KR_NA(user=user)
    return element, rest
```

Ispis 5.3. Dekodiranje poruke S_KR_NA_1.

Da se testira kodiranje i dekodiranje poruke, napisan je *unit* test. Za svaku pojedinačnu poruku ispitano je par testnih slučajeva. Kodirani bajtovi se uspoređuju s očekivanim bajtovima za pojedinu poruku. Također, dekodirana poruka se uspoređuje s očekivanim formatom poruke. Ispis 5.4. prikazuje testiranje kodiranja i dekodiranja za poruku S_KR_NA_1.

```
@pytest.mark.parametrize(
    'usr_number, cause, asdu_address',
    zip(gen_user_numbers(3),
        gen_causes(3),
        gen_asdu_address(3)))
def test_s_kr_na(usr_number, cause, asdu_address):
    asdu_type = common.AsduType.S_KR_NA

    io_element = common.IoElement_S_KR_NA(user=usr_number)

    assert_encode_decode(asdu_type, cause, asdu_address, io_element)
```

Ispis 5.4. Testiranje kodiranja i dekodiranja poruke S_KR_NA_1.

5.3 Poteškoće s implementacijom IEC 62351-5

Kada su bili implementirani svi koderi i dekoderi za poruke definirane IEC 60870-5-7, ta osnovna implementacija, bez implementiranog automata stanja, je testirana s uređajima koji tvrde da imaju podršku za IEC 62351-5. Napisane su *Python* skripte koje pokušavaju izvršiti inicijalizaciju komunikacije kako je ranije prikazano na Slici 4.2. Testirana su dva mehanizma inicijalizacije. Ranije prikazana implementacija pretpostavlja klasičnu „izazov-odgovor" inicijalizaciju. Druga moguća vrsta inicijalizacije je agresivan način rada, kako je objašnjeno ranije i kako je definirano u IEC 62351-5. Oba način inicijalizacije su testirani s nekoliko uređaja. Utvrđeno je da niti jedan uređaj od testiranih uređaja nije u stanju uspostaviti komunikaciju sigurnim razmjenjivanjem tajnih podataka definiranih u IEC 62351-5 i u IEC 60870-5-7 . Oba dokumenta su veće kompleksnosti od IEC 62351-3, imaju greške te čak u nekim slučajevima i suprotnosti. To ne bi trebao biti slučaj. IEC 60870-5-7 bi trebao dopunjavati sve tvrdnje definirane u IEC 62351-5. Razlog za nekompatibilnost između različitih uređaja i implementacija je činjenica da te greške i nedosljednosti mogu dovesti do različitih interpretacija dokumenata i time do različitih implementacija koje nisu međusobno kompatibilne.

Na primjer, poruka *Session Key Status*, koju šalje kontrolna postaja kao odgovor na prije spomenutu poruku *Key Status Request,* sadrži informacije o valjanosti trenutnog ključa sjednice. Ta informacija, odnosno, status ključa može poprimiti jednu od idućih vrijednosti: OK, NOT INIT, COMM FAIL, AUTH FAIL [15].

Session Key Status poruke sadrže MAC vrijednost, odnosno, izračunati sažetak koji služi za autentifikaciju.

IEC 60870-5-7 navodi da MAC vrijednost je uključena u poruci samo ako je status ključa OK [17].

Međutim, IEC 62351-5 navodi da se MAC vrijednost računa i šalje neovisno o tome smatraju li se ključevi sjednice valjanima. Ako ključevi nisu valjani, pošiljatelj će koristiti zadnje valjane ključeve sjednice. Ako nije bilo prijašnjih ključeva koji su se smatrali valjanima, MAC polje poruke će biti prazno, odnosno, neće biti uključeno u poruku [15].

Te dvije tvrdnje nisu jednake. Po tvrdnji iz IEC 60870-5-7 dalo bi se zaključiti da se MAC šalje samo kada je OK, a po IEC 62351-5 se može zaključiti da se MAC šalje i u slučajevima kada je status COMM FAIL ili AUTH FAIL.

Nadalje, neki dijelovi IEC 62351-5 sadrže greške koje također mogu voditi do netočnog ponašanja implementacije. Poruka S_UC_NA_1 je dva puta definirana s različitim vrijednostima za identifikator tipa. Jednom je definirana s identifikatorom tipa 88, a jednom s identifikatorom tipa 90. Iako se protokol može implementirati da radi usprkos tim greškama, takva vrsta implementacije ne garantira da je i druga strana komunikacije razumjela pogrešku i rukovala s pogreškom na isti način [5].

Također, tijekom pisanja ovog dokumenta, a nakon testiranja implementacije, izašla je nova verzija IEC 62351-5. Ta nova verzija iz 2023. godine zamjenjuje stariju verziju iz 2013. godine i ta starija verzija je sada klasificirana s „*withdrawn*“, odnosno, opozvana je i očekuje se da se koristi novija verzija IEC 62351-5. Međutim, trenutni problem jest činjenica da ta novija verzija znatno mijenja imena poruka, značenja poruka, uklanja neke poruke i potpuno uklanja agresivni način rada te uvodi nove mehanizme autentifikacije. Drugim riječima, ta novija verzija IEC 62351-5 nije kompatibilna s trenutnim IEC 60870-5-7 koji je potreban za implementaciju IEC 62351-5 nad protokolom IEC 104. To znači, ako je želja implementatora da ima novu verziju implementacije IEC 62351-5, morat će pričekati da izađe i nova verzija IEC 60870-5-7. Nadalje, takva implementacija bi trenutno imala i upitnu poslovnu korisnost. Naime, kako je opisano, čak i IEC 62351-5 iz 2013. ima ograničenu podršku nad uređajima koji se koriste u elektroenergetici zbog čega i ta verzija ima upitnu korisnost. Novi IEC 62351-5 iz 2023. godine trenutno nema uređaja koji ga podržavaju.

6. Zaključak

Pošto je IEC 104 komunikacijski protokol stvoren bez fokusa na kibernetičku sigurnost, za rad u modernom okruženju mu je potrebna zaštita.

Primjena IEC 62351-3 za takvu zaštitu protokola IEC 104 ima smisla. IEC 62351-3 opisuje korištenje poznatog i široko podržanog protokola TLS te na poprilično jednostavan način pruža korake kako taj protokol primijeniti u elektroenergetici. Korištenjem ovog protokola se lakše osigurava kompatibilnost između više različitih proizvođača i više različitih implementacija. Kada bi svaki proizvođač radio vlastito rješenje za zaštitu komunikacije, javljao bi se problem međusobne kompatibilnosti.

IEC 62351-5, s druge strane, je poprilično veći dokument koji također zahtjeva i dodatan dokument IEC 60870-5-7 kako bi se implementirala zaštita nad protokolom IEC 104. Zbog takve veće složenosti, javlja se i više problema kod implementacije. Oba dokumenta imaju svoje vlastite greške, bilo manje greške koje se potencijalno daju ispraviti, ili veće greške koje vode do problema kompatibilnosti između različitih implementacija. Također, ta dva dokumenta imaju i kontradikcije koje stvaraju dodatne probleme s razumijevanjem i implementacijom. Također, ustanovljeno je da je IEC 62351-5, za razliku od IEC 62351-3, slabije podržan. Čak i ako se pronađu uređaji koji nominalno podržavaju IEC 62351-5, u praksi se pokazalo da je nemoguće uspostaviti očekivani tijek komunikacije opisan u IEC 62351-5. Nadalje, verzija IEC 62351-5 iz 2013. koju je moguće implementirati jer ima pripadajući opis implementacije za protokol IEC 104, IEC 60870-5-7, je povučena, a nova verzija nema pripadajući IEC 60870-5-7. Zbog toga je za očekivati da broj uređaja koji podržavaju verziju iz 2013. neće rasti. Imajući na umu kompleksnost IEC 62351-5, teškoće implementacije, probleme s kompatibilnošću i činjenicu da je dokument povučen, korisnost ovakvog rješenja je upitna. Iz poslovne perspektive, implementacija IEC 62351-5 nije isplativa.

Zajednički problem koji je pronađen kod implementacije oba dijela IEC 62351 je činjenica da testovi sukladnosti opisani dokumentima IEC TS 62351-100-1 i IEC TS 62351-100-3 ne

garantiraju međusobnu kompatibilnost između uređaja koji tvrde da su sukladni s IEC 62351-3, odnosno, IEC 62351-5 [17] [7].

Iako su dokumenti IEC TS 62351-100-1 i IEC TS 62351-100-3 službeni dokumenti za testiranje pojedinih implementacija prema IEC 62351-5, odnosno, IEC 62351-3, i dalje ne garantiraju potpunu međusobnu kompatibilnost različitih implementacija, i to predstavlja problem.

Koristilo bi kada bi postojao detaljan sustav testiranja, po mogućnosti u programskom obliku, ili u vrlo detaljnom tabličnom obliku, koji bi nedvosmisleno garantirao da je svaka implementacija koja zadovolji takav test ujedno i kompatibilna s ostalim implementacijama koje su zadovoljile isti test.

7. Popis literature

[1] P. Matoušek, "Description and analysis of IEC 104 Protocol, Technical Report," Faculty of Information Technology, Brno University of Technology, Brno, Czech Republic, 2017.

[2] P. S. I. G. E. K. E. P. Panagiotis Radoglou-Grammatikis, "Attacking IEC-60870-5-104 SCADA Systems," *IEEE World Congress on Services,* 2019.

[3] International Electrotechnical Commission, IEC, "62351-1: Introduction and overview".

[4] International Electrotechnical Commission, IEC, "62351-11: Security for XML documents".

[5] I. Cindrić and T. Hadjina, "An analysis of IEC 62351 implementations for securing IEC 60870-5-104 communication," in *Powertech 2023*, Belgrade, 2023.

[6] International Electrotechnical Commission, IEC, "62351-3: Communication network and system security – Profiles including TCP/IP".

[7] International Electrotechnical Commission, IEC, Part 100-3: Conformance test cases for IEC 62351-3, the secure communication extension for profiles including TCP/IP, 2020.

[8] International Electrotechnical Commission, IEC, "62351-9: Power systems management and associated information exchange".

[9] Python Software Foundation, "TLS/SSL wrapper for socket objects," Python, 2023. [Online]. Available: https://docs.python.org/3/library/ssl.html#ssl-contexts.

[10] Koncar Digital, "Hat Open - About," 2023. [Online]. Available: https://hat-open.com/.

[11] KONČAR DIGITAL, "PROZA HAT," KONČAR DIGITAL, 2023. [Online]. Available: https://www.koncar.hr/poslovna-podrucja/digitalna-rjesenja/rjesenja-i-platforme/proza-hat/.

[12] Končar Digital, "hat-syslog - Syslog Server and tools," 2023. [Online]. Available: https://github.com/hat-open/hat-syslog.

[13] Internet Engineering Task Force (IETF) , "Transport Layer Security (TLS) Renegotiation Indication Extension," 2010. [Online]. Available: https://www.rfc-editor.org/rfc/rfc5746.html.

[14] Individual Contributors, "pyca/cryptography," 2023. [Online]. Available: https://cryptography.io/en/latest/.

[15] International Electrotechnical Commission, IEC, "62351-5: Security for IEC 60870-5 and derivatives".

[16] International Electrotechnical Commission, IEC, Part 5-7: Transmission protocols – Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351), 2013.

[17] International Electrotechnical Commission, IEC, 62351-100-1: Conformance test cases for IEC TS 62351-5 and IEC TS 60870-5-7, 2018.

[18] IEC, "SyC Smart Energy," 2023. [Online]. Available: https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62351/.