Kibernetička sigurnost nadzorno upravljačkog sustava cestovnog tunela"

Merkaš, Marko

Professional thesis / Završni specijalistički

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Electrical Engineering and Computing / Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:168:501155

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-07-17**

Repository / Repozitorij:

FER Repository - University of Zagreb Faculty of Electrical Engineering and Computing repozitory

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Marko Merkaš

KIBERNETIČKA SIGURNOST NADZORNO-UPRAVLJAČKOG SUSTAVA CESTOVNOG TUNELA

SPECIJALISTIČKI RAD

Zagreb, 2023.

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

Marko Merkaš

CYBER SECURITY OF A ROAD TUNNEL SURVAILLANCE AND CONTROL SYSTEM

KIBERNETIČKA SIGURNOST NADZORNO-UPRAVLJAČKOG SUSTAVA CESTOVNOG TUNELA

SPECIALIST THESIS
SPECIJALISTIČKI RAD

Zagreb, 2023.

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

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

Specijalistički rad ima: 35 stranica

Specijalistički rad br.:_____.

Povjerenstvo za ocjenu u sastavu:

1. izv. prof. dr. sc. Miljenko Mikuc – predsjednik

2. izv. prof. dr. sc. Stjepan Groš – mentor

3. izv. 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. Miljenko Mikuc – predsjednik

2. izv. prof. dr. sc. Stjepan Groš – mentor

3. izv. prof. dr. sc. Krešimir Grgić, Sveučilište Josipa Jurja Strossmayera u Osijeku Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek - član

Datum obrane: 30. listopada 2023.

Zahvaljujem se mentoru na pomoći u izradi ovog specijalističkog rada. Posebno se zahvaljujem svojoj supruzi na podršci, strpljenju i motivaciji bez koje ovaj rad ne bi bio moguć.

Sažetak

Kibernetička sigurnost upravljačkih sustava od iznimne je važnosti za funkcioniranje kritične infrastrukture, a o njezinoj implementaciji potrebno je voditi računa već kod projektiranja samog sustava. Zbog toga je kod projektiranja sustava za nadzor i upravljanje cestovnim tunelom ključno odabrati arhitekturu koju će biti što je moguće lakše zaštiti od kibernetičkih napada. U radu je odabrana je ISA95 mrežna arhitektura u koju su uključeni svi nadzorni i sigurnosni sustavi u tunelu, a nakon čega je pomoću stabla napada razmatrana sigurnost dobivenog sustava. Zaključeno je da je ISA95 arhitektura primjenjiva u slučaju da se ne koriste IIoT uređaji i da je ključno osigurati vezu između razine 2 – serverske infrastrukture nadzorno-upravljačkog sustava i razine 4 – poslovne mreže tvrtke koja upravlja tunelom. Zaštitu je potrebno provoditi pravilno dizajniranom DMZ zonom.

Summary

Cybersecurity of control systems is of utmost importance for the functioning of critical infrastructure, and its implementation needs to be taken into account during the design phase of the system itself. Therefore, when designing a supervisory and control system for a road tunnel, it is crucial to select an architecture that can be easily protected from cyber attacks. In this paper, the ISA95 network architecture was chosen that includes all the monitoring and security systems in the tunnel. Subsequently, the security of the obtained system was analyzed using attack trees. It was concluded that the ISA95 architecture is applicable if IIoT devices are not used, and it is crucial to secure the connection between Level 2 - server infrastructure of the surveillance and control system and Level 4 - the business network of the company that responsible for the operation of the tunnel. Properly designed DMZ (demilitarized zone) is necessary for implementing all of the needed defense mechanisms.

Sadržaj

1. Uvod 1
2. Kibernetička sigurnost upravljačkih sustava 3
2.1 Mrežna arhitektura IEC 62264 / ISA 95 8
2.2 NIS2 direktiva 11
3. Nadzorno upravljački sustav cestovnog tunela 12
3.1 Datex II 16
3.2 Nadzorno-upravljački sustav cestovnog tunela 16
4. Identifikacija prijetnji 19
4.3 Kibernetički napad na Carmel Tunnels 20
4.4 Potencijalni napadači 21
4.5 Prijetnje 22
5. Sigurnosne mjere 31
6. Zaključak 33
7. Literatura 34

1. Uvod

Cestovni tuneli kao tehnički najkompleksniji dijelovi cestovnog prometa značajno doprinose ubrzanju prometa ljudi i robe. Oni služe kao poveznica inače geografski odijeljenih cjelina i omogućuju da se put između tih geografskih cjelina značajno skrati. Ovisno o njihovoj dužini i prometnom opterećenju zakonski su propisani sigurnosni sustavi koji moraju biti ugrađeni u tunelu kako bi njihova sigurnost bila na zadovoljavajućoj razini. S obzirom na to da su sustavi koji se ugrađuju najčešće umreženi, a čijom se međusobnom integracijom postižu potrebni funkcionalni i sigurnosni zahtjevi potrebno je voditi računa i o njihovoj kibernetičkoj zaštiti pri čemu je osnovna svrha zaštite očuvanje raspoloživosti sustava.

U prosincu 2022. na razini Europske unije donesena je NIS2 direktiva čiji je cilj osiguravanje visoke razine odgovornosti za mjere upravljanja rizicima kibernetičke sigurnosti i obveze izvješćivanja na razini ključnih i važnih subjekata. Među ključnim vertikalama nalazi se i promet, a s čime i sustavi za nadzor i upravljanje tunelima.

Kako bi se omogućila kvalitetna kibernetička zaštita bilo kojeg sustava, uključujući i nadzorno-upravljačkog sustava tunela, potrebno je već u fazi projektiranja tog sustava kibernetičku sigurnost postaviti kao jedan od temeljnih zahtjeva. Vodeći računa o kibernetičkoj sigurnosti sustava od samog početka može se stvoriti arhitektura sustava koja zadovoljava potrebnu funkcionalnost sustava, a istovremeno pruža mogućnost njegove kibernetičke zaštite smanjujući moguće vektore napada. Uz odgovarajuću arhitekturu sustava pri odabiru opreme također je potrebno voditi računa da ona zadovoljava barem minimalne sigurnosne zahtjeve kao što je kontrola pristupa te po mogućnosti sigurne komunikacijske protokole. Odabir protokola kojima će sustavi komunicirati već u fazi projektiranja od velike je važnosti budući da oni svojim sigurnosnim, ali i funkcionalnim ograničenjima značajno mogu utjecati na arhitekturu sustava.

Poznata je činjenica da su kod upravljačkih sustava komunikacijski protokoli često u potpunosti nezaštićeni budući da se jednim dijelom radi o protokolima koji su dizajnirani za u to vrijeme korišteni način komunikacije (npr. serijska komunikacija) i kasnije prilagođeni mrežnoj komunikaciji. Također, budući da je kod upravljačkih sustava izrazito bitno da je komunikacija sa sustavom ili između sustava što bliža komunikaciji u stvarnom vremenu sigurnost je često žrtvovana kako se u komunikaciju ne bi unosilo kašnjenje. Konačno, unošenje sigurnosnih

elemenata u komunikaciju traži veću procesnu moć hardvera, a što dodatno poskupljuje njegovu proizvodnju.

Cilj je rada kreirati model nadzorno-upravljačkog sustava cestovnog tunela, odabrati mrežnu arhitekturu koja će omogućiti potrebnu komunikaciju, odrediti potencijalne ranjivosti dobivenog sustava te predložiti sigurnosne mjere za njihovo uklanjanje ili smanjenje njihovog utjecaja. U fokusu rada je mrežna sigurnost upravljačkog sustava pa će u nastavku ona detaljnije razmatrati.

Rad je strukturiran na sljedeći način. 2. poglavlje daje pregled osnovnih svojstava upravljačkih sustava, navodi zahtjeve na mrežnu arhitekturu te pobliže opisuje IEC 62264 / ISA95 mrežnu arhitekturu. Također, opisana je i NIS2 direktiva koja predstavlja zakonski okvir kibernetičke sigurnosti subjekata koji su na temelju direktive definirani kao ključni ili važni. U 3. poglavlju koristeći postojeće zakonske zahtjeve koji propisuju sustave koji moraju biti implementirani u tunelu kako bi se postigla minimalna razina njegove sigurnosti dobivaju se sastavnice nadzorno-upravljački sustav cestovnog tunela. Dobivene sastavnice nadzorno-upravljačkog sustava zatim se koriste kako bi se dobio model nadzorno upravljačkog sustava prema ISA95 standardu. U 4. poglavlju prvo se daje primjer OT:ICEFALL popisa ranjivosti koji ukazuje na mogućnost postojanja brojnih ranjivosti u korištenim uređajima te primjer napada na Carmel Tunnels koji pokazuje kako kibernetički napad na nadzorno-upravljački sustav cestovnog tunela nije samo teoretska mogućnost. Nadalje u poglavlju se definiraju potencijalni napadači te se koristeći stabla napada pronalaze izloženi dijelovi sustava. 5. poglavlje na temelju detektiranih prijetnji u prethodnom poglavlja predlaže mjere za njihovo ublažavanje što je i krajnji cilj rada. Konačno, u 6. poglavlju prikazani su zaključci ovog rada.

2. Kibernetička sigurnost upravljačkih sustava

Kibernetičkom sigurnošću uobičajeno želimo zaštiti tri temeljna svojstva – tajnost (engl. *confidentiality*), integritet (engl. *integrity*) i raspoloživost (engl. *availability*). Kada govorimo o poslovnoj okolini gdje se koriste informacijske tehnologije (IT) cilj nam je zaštiti tajnost informacija, a potom integritet i raspoloživost. Kod upravljačkih sustava gdje se koriste operacijske tehnologije (OT) najbitnije svojstvo koje želimo očuvati je raspoloživost, a tek nakon toga integritet i tajnost [1]. Operacijske tehnologije sastoje se od raznih programibilnih uređaja koji služe za nadzor i upravljanje fizičkim sustavima. Kod cestovnog tunela primjer takvih uređaja su PLC (engl. *Programmable Logic Controler*) uređaji koji npr. upravljaju ventilacijom u tunelu. U Tablici 1 prikazane su bitne razlike između IT i OT sustava na temelju kojih je vidljivo da se pouzdanost i dostupnost OT sustava ni u kojem slučaju ne smiju ugroziti.

Tablica 1: Razlike IT i OT sustava [2]

Kategorija	**IT**	**OT**
Performanse	Nije u stvarnom vremenu. Odgovor mora biti dosljedan. Zahtijeva se visok propusnost. Interakcija u hitnim situacijama manje je kritična. Strogo ograničena kontrola pristupa može se provoditi u potrebnoj mjeri za sigurnost.	U stvarnom vremenu. Odgovor je vremenski kritičan. Skromna propusnost je prihvatljiva. Visoko kašnjenje i/ili fluktuacije nisu prihvatljivi. Odgovor na interakciju s ljudima i drugim hitnim situacijama je kritičan. Pristup OT-u treba strogo kontrolirati, ali ne smije ometati interakciju između čovjeka i sustava.
Dostupnost	Prihvatljive reakcije uključuju ponovnog pokretanje sustava. Izostanak dostupnosti često se može tolerirati, ovisno o operativnim zahtjevima sustava.	Reakcija poput ponovnog pokretanja možda nije prihvatljiva zbog zahtjeva za dostupnošću procesa. Mogu zahtijevati redundantne sustave. Prekidi moraju biti planirani i zakazani danima/tjednima unaprijed. Visoka dostupnost zahtijeva temeljito testiranje prije implementacije.
Upravljanje rizicima	Upravljanje podacima. Povjerljivost i integritet podataka su ključni. Manja važnost ima otpornost na kvarove - kratkotrajni prekidi nisu veliki rizik. Glavni rizik utječe na kašnjenje poslovnih operacija.	Interakcija sa fizičkim svijetom. Ljudska sigurnost je ključna, a zatim slijedi zaštita procesa. Otpornost na kvarove je bitna; čak i kratkotrajni prekidi možda neće biti prihvatljivi. Glavni rizici utječu na neusklađenost s propisima, utjecaje na okoliš i gubitak života, opreme ili proizvodnje.

Upravljanje sustavom	Sustavi su dizajnirani za korištenje sa tipičnim operacijskim sustavima. Nadogradnje su jednostavne uz dostupnost automatiziranih alata za implementaciju.	Sustavi često koriste različite i moguće proprijetarne operacijske sustave, ponekad bez ugrađenih sigurnosnih mogućnosti. Promjene softvera moraju se pažljivo provoditi, obično od strane dobavljača softvera, zbog specijaliziranih kontrolnih algoritama i potencijalno modificiranog hardvera i softvera.
Ograničenja resursa	Sustavi se specificiraju s dovoljno resursa za podršku dodavanju aplikacija trećih strana poput sigurnosnih rješenja.	Sustavi su dizajnirani kako bi podržali namjeravani industrijski proces i možda nemaju dovoljno memorije i računalnih resursa da bi podržali dodavanje sigurnosnih mogućnosti.
Komunikacija	Standardni komunikacijski protokoli. Primarno žičane mreže s nekim lokaliziranim bežičnim mogućnostima. Tipične IT prakse mrežnog povezivanja.	Razni proprijetarni i standardni komunikacijski protokoli. Koriste se različite vrste komunikacijskih medija, uključujući izolirane žičane i bežične tehnologije Mreže su složene i ponekad zahtijevaju inženjersku stručnost.
Upravljanje promjenama	Promjene u softveru se primjenjuju na vrijeme uz dobru politiku i postupke sigurnosti. Postupci su često automatizirani.	Softverske promjene moraju biti temeljito testirane i primijenjene postupno u cijelom sustavu kako bi se osigurala očuvanost integriteta OT sustava. OT prekidi često se moraju planirati i zakazati nekoliko dana / tjedana unaprijed. OT može koristiti OS-ove koji više nisu podržani.
Održavanje	Dopušteni su raznovrsni načini održavanje.	Održavanje najčešće od jednog dobavljača.
Životni vijek hardvera	Između 3 i 5 godina.	Između 10 i 15 godina.
Smještaj hardvera	Lokalno i lako dostupno.	Izolirane, udaljene i često teško dostupne.

Kibernetička sigurnost upravljačkih sustava od iznimne je važnosti jer se njezinim ugrožavanjem direktno ugrožava zdravlje i sigurnost ljudi, sigurnost okoliša i infrastrukture, no njezina važnost tek od nedavno dolazi u fokus. Razlog za kasno uključivanje kibernetičke sigurnosti u upravljačke sustave je taj što je njezin razvoj, odnosno prihvaćanje novih tehnologija, znatno sporiji u usporedbi s IT sustavima. Dugo vremena upravljački sustavi izvođeni su kao zatvoreni sustavi – bez interakcije s poslovnim sustavom tvrtki, no to se promijenilo te danas IT i OT sustavi sve više konvergiraju. Zatvorenost upravljačkih sustava za posljedicu je imalo i razvoj tehnologija i komunikacijskih protokola koji ne vode računa o kibernetičkog zaštiti. Također, upravljački sustavi znatno su manje podložni promjenama i jednom kada se puste u rad izmjene su veoma rijetke što znači da kada se neka komponenta ugradi u upravljački sustav, ona tamo ostaje dugi niz godina. Iz navedenih značajki upravljačkih sustava može se zaključiti sljedeće:

- kibernetičku sigurnost upravljačkih sustava potrebno je ubrzano razvijati budući da prelazak iz izoliranog sustava u povezani sustav donosi čitav niz do tada nepoznatih prijetnji upravljačkom sustavu,
- kod projektiranja upravljačkog sustava potrebno je posebnu pozornost dati i kibernetičkoj sigurnosti.

Posebno ugrožena skupina upravljačkih sustava su oni sustavi koji su digitalnom transformacijom poslovanja tvrtke povezani s poslovnom mrežom tvrtke, a koji se sastoje od zastarjelih operacijskih tehnologija i protokola koji pružaju male ili nikakve mogućnosti kibernetičke zaštite.

Nadzorno-upravljački sustav tunela koji je predmet ovog rada baziran je na SCADA (engl. *Supervisory Control and Data Acquisition*) sustavu koji se općenito koristi za upravljanje više različitih podsustava, a gdje se očekuje centralizirano prikupljanje podataka kao i upravljanje. Prikupljeni podaci prikazuju se operaterima u grafičkom sučelju koje najčešće topološki ili tlocrtno prikazuje sustav koji se nadzire i upravlja. SCADA sustav sastoji se od centralnog servera, mrežne opreme te upravljačke opreme (RTU, PLC) koja upravlja izvršnim elementima ili prikuplja podatke sa senzora. Uz centralnu SCADA-u promatrani sustav sadrži i PSIM (engl. *Physical security information management*) softver koji se fizički sastoji od centralnog servera, mrežne opreme i sustava koji nadzire te SCADA-e specijalizirane za nadzor elektroenergetskog sustava tunela. PSIM softver i SCADA za energetiku u ovom su slučaju podsustavi nadzorne SCADA-e.

Kod projektiranja bilo kojeg upravljačkog sustava vodi se računa da taj sustav zadovoljava sljedeće osnovne karakteristike [3]:

- dostupnost: sustav i informacije u sustavu moraju biti dostupne autoriziranim korisnicima ili drugim sustavima koji o njima ovise,
- otpornost na greške: sustav mora biti robustan te nastaviti s radom u maksimalnom mogućem opsegu i u slučaju kvara nekog od njegovih dijelova,
- performanse: sustav mora biti učinkovit i izvršavati svoje zadaće točno i na vrijeme,
- sigurnost: sustav mora prepoznati opasna stanja i svojom reakcijom uspostaviti sigurno okruženje.

Osim toga, poželjne su i sljedeće karakteristike:

- održavanje: sustav mora pružiti adekvatne dijagnostičke i kontrolne funkcije kako bi se mogao pravilno održavati,
- otvorenost: potiče se korištenje otvorenih standarda i tehnologija kako bi se povećala interoperabilnost između uređaja različitih sustava i infrastruktura,
- sigurnost: zaštita od najčešćih prijetnji kao što su neautorizirani pristup i manipulacija podacima,
- jednostavnost korištenja: omogućuje korisnicima brzu prilagodbi i kratak period učenja.

Kako bi se uspješno upravljalo kibernetičkom sigurnošću upravljačkog sustav ENISA (engl. *European Union Agency for Network and Information Security*) preporučuje [3]:

1. uključivanje kibernetičke sigurnosti u glavne zahtjeve tijekom dizajna upravljačkog sustava,
2. identificirati i definirati uloge osoba koje koriste upravljački sustav – upravljanje autorizacijama korisnika od iznimne je važnosti,
3. definirati mrežne komunikacijske tehnologije i arhitekturu imajući na umu interoperabilnost sustava – cilj je da se za komunikaciju koriste standardni protokoli čije su sigurnosne značajke poznate, a izbjegavati zatvorene protokole proizvođača koji su se u povijesti često koristili,
4. unutar organizacije uspostaviti komunikaciju u kojoj sudjeluju svi zaposlenici povezani sa upravljačkim sustavom tijekom njegovog životnog ciklusa – korisnici, IT stručnjaci, sigurnosni stručnjaci, uprava, itd.,
5. uključiti nadogradnje uređaja u redovito održavanje upravljačkog sustava,
6. unutar organizacije provoditi periodičke edukacije i kampanje osvještavanja o kibernetičkoj sigurnosti.

Arhitektura današnjih upravljačkih sustava definira se imajući u vidu njezinu potrebu za povezivanjem s poslovnom mrežom tvrtke, no ta veza mora biti strogo kontrolirana i sigurna. Iz tog se razloga upravljački sustav projektira kao neovisan segment koji se u samo jednoj točki povezuje s poslovnom mrežom. U budućnosti se predviđa sve veće korištenje Internet stvari uređaja (IoT, engl. *Internet of things*) u upravljačkim sustavima što će donijeti nove pristupe u njihovoj izgradnji s obzirom da IoT uređaji, najčešće, prikupljene informacije šalju poslužitelju u oblaku, a što podrazumijeva njihovu konstantnu povezanost sa Internetom.

Trenutačno se najboljom praksom u kibernetičkoj zaštiti upravljačkih sustava smatra korištenje strategije obrane u dubinu (engl. *defense-in-depth*) [2] preuzetom iz poslovnih sustava gdje se

također smatra dobrom praksom. Upotrebom takve strategije izbjegava se jedna točka proboja (engl. *single point of failure*) korištenjem više slojeva obrane u sustavu:

1. upravljanje sigurnošću;
2. fizička sigurnost: zaštita perimetra, fizička kontrola pristupa, nadzor, praćenje ljudi i imovine;
3. mrežna sigurnost: segmentacija i izolacija, centralizirano bilježenje dnevničkih zapisa, praćenje mrežnog prometa, zaštita od malicioznog koda;
4. sigurnost hardvera: hardver koji se koristi mora pružati mogućnosti zaštite od neautoriziranog pristupa i zaštite komunikacije, a istovremeno vodeći računa o utjecaju na operativne performanse, sigurnost i mogućnosti;
5. sigurnost softvera: popis dozvoljenog softvera, nadogradnje, korištenje sigurno razvijenog softvera.

Uz strategiju obrane u dubinu sve više u literaturi spominje i preporučuje arhitektura nultog povjerenja (engl. *zero-trust architecture*, ZTA) koja se temelji na kontinuiranoj provjeri autorizacija korisnika [4]. U ZTA mreži ne postoji koncept perimetra koji se štiti od vanjskih napadača i nakon kojeg postoji implicitno povjerenje prema korisniku već se autorizacija korisnika provodi bliže resursima u mreži – točka provjere može na prelasku segmenata mreže ili točno ispred pojedinog resursa. Implementacija ZTA mreže u OT sustavima otežana je ograničenjima mogućnosti uređaja budući da OT komponente često ne podržavaju tehnologije i protokole potrebne za njezinu implementaciju. Također, kontinuirana provjera autorizacija korisnika može dovesti do povećanja latencije u mreži, a što može prouzročiti probleme u radu sustava [2].

Općenito se kod sigurnosti hardvera i softvera preporučuje voditi načelom minimalne funkcionalnosti prema kojem je potrebno definirati minimalan potreban skup funkcionalnosti koje su potrebne da bi sustav radio, a sve ostale je potrebno isključiti.

Budući da je u fokusu rada je mrežna sigurnost upravljačkog sustava u nastavku će se ona detaljnije razmatrati. Za mrežnu arhitekturu upravljačkog sustava preporučuje se sljedeće:

- razdvojiti mrežu u različite zone/segmente,
- kako bi se kontrolirala i nadzirala komunikacija između različitih zona na njihovim granicama potrebno je uključiti sigurnosne uređaje (npr. vatrozid) pri čemu je potrebno voditi računa o specifičnim tehnologijama koje koristi OT,

- za komunikaciju izvan lokalne mreže koju je potrebno uspostaviti preko Interneta potrebno je koristiti sigurnu vezu (npr. VPN, engl. *virtual private network*),
- implementirati demilitariziranu zonu (DMZ, engl. *demilitarized zone*) između poslovne mreže i kontrolnog centra. Servise u DMZ-u potrebno je nadzirati kako bi se spriječilo daljnje prodiranje u mrežu u slučaju incidenta.

U literaturi [2] se spominju razni modeli mrežne arhitekture OT sustava, a odabir odgovarajuće ovisi o njegovoj namjeni, raspodijeljenosti sustava, tehnologijama koje se koriste i slično.

Među raznim arhitekturama koje se spominju u literaturi [2,3] za promatrani sustav odabrana je arhitektura prema IEC 62264 / ISA 95 standardu (u nastavku ISA95).

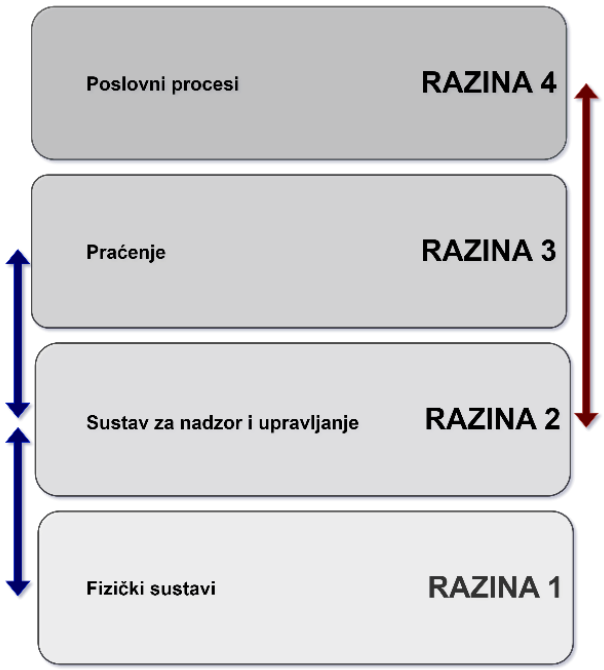
2.1 Mrežna arhitektura IEC 62264 / ISA 95

IEC 62264 / ISA 95 je strukturirana višerazinska mrežna arhitektura u kojoj je svaka razina namijenjena jednom od podsustava upravljačkog sustava. Fokus ISA95 arhitekture je na potrebnim vezama između uređaja, odnosno sustava, pri čemu se oni grupiraju u razine ovisno zadaći sustava. ISA95 definira sljedeće razine [3]:

- Fizički sustavi (razina 1): sadrži sve sustave koji imaju fizičku interakciju s okolinom. Procesi međusobno rijetko komuniciraju, već informacije koje pružaju nakon obrade imaju utjecaja na ostale procese. Najčešće se ovdje nalazi sljedeći hardver: lokalni HMI, PLC, RTU, razni senzori, razni izvršni elementi. Softver na ovoj razini najčešće je specifičan za svakog od proizvođača hardvera koji se rijetko ili nikad ne nadograđuje,
- Nadzor i upravljanje fizičkim sustavima u tunelu (razina 2): svrha elemenata na ovoj razini je osigurati pravilan rad proizvodnih i upravljačkih procesa. Hardver na ovoj razini služi za grafičku prezentaciju informacija s razine 1 i najčešće uključuje: SCADA servere, PSIM server, domenske kontrolere, servere za sinkronizaciju vremena i slično. Softver na ovoj razini služi za nadzor, praćenje i upravljanje u stvarnom vremenu koji se rijetko nadograđuje i često se nalazi na računalima s zastarjelim operacijskim sustavima,
- Upravljanje tunelom (razina 3): na ovoj razini nalaze se sustavi za upravljanje procesima u tunelu, kao što su sustavi za upravljanje ventilacijom, sustavi za praćenje i upravljanje ispušnim plinovima i drugi slični sustavi. Ovi sustavi imaju zadatak upravljati procesima na razini tunela. Hardver na ovoj razini uključuje računala sa instaliranim SCADA softverom koji omogućuje nadzor i upravljanje tunelom. Softver na ovoj razini

ovisi o potrebama funkcije koja se obavlja, ali i ovdje se često radi o zastarjelim i neodržavanim operacijskim sustavima,

- Upravljanje poslovanjem (razina 4): obuhvaća sustave za upravljanje poslovnim procesima tvrtke koja upravlja tunelom, poput upravljanja ljudskim resursima, financijama, nabavom i drugim sličnim sustavima. Sa strane kibernetičke sigurnosti upravljačkog sustava ova razina smatra se nesigurnom budući da sadrži velik broj raznovrsnih sustava i korisnika. Također, ova razina obično ima vezu prema Internetu.



Slika 1: Mrežna arhitektura prema ISA95 standardu

U ISA95 modelu razlikuju se dvije različite vrste komunikacije:

- vertikalna komunikacija: razmjena podataka između uređaja i sustava u različitim razinama,
- horizontalna komunikacija: razmjena podataka između uređaja i sustava u istim razinama.

Vertikalna komunikacija odvija se između:

- razina 1 i 2 (dvosmjerno) kako bi nadzorni sustav dobio mjerene vrijednosti od senzora i po potrebi aktivirao izvršne elemente,
- razina 2 i 3 (dvosmjerno) kako bi podaci dobiveni na razini 1 bili prikazani operaterima na razini 3 te kako bi akcije operatera bile proslijeđene na razinu 1,

- razina 2 i 4 kako bi podaci dobiveni na razini 1 bilo proslijeđeni poslovnim sustavima.

Horizontalna komunikacija odvija se unutar:

- razine 1 gdje se komunikacija odvija između upravljačkih elemenata i senzora te upravljačkih elemenata međusobno,
- razine 2 gdje se komunikacija odvija razmjena informacija između SCADA servera i ostalih servera unutar ove razine – PSIM server, NTP server, itd.,
- razine 4 gdje se odvija uobičajena IT komunikacija između poslovnih sustava.

Kako je već spomenuto, u modernim upravljački sustavima sve se više koriste IoT uređaji koji najčešće sakupljene podatke na obradu šalju u servise koji se nalaze u oblaku (engl. *cloud services*). To podrazumijeva da oni imaju vezu prema Internetu, a kako bi se oni prema ISA95 modelu trebali nalazili na razini 1 za koju je predviđena komunikacija samo s razinom 2 može se zaključiti kako ISA95 ne podržava uključivanje IoT uređaja. S obzirom na to da u tunelu ne postoji potreba za IoT uređajima za ovakvu primjenu ISA95 arhitektura je i dalje odgovarajući izbor.

Centralizirano prikupljanje dnevničkih zapisa sa zaštitnih uređaja (vatrozida), mrežnih preklopnika i usmjerivača, servera, radnih stanica i OT uređaja može pružiti vrijedne informacije o događanjima u sustavu i to za detekciju incidenata, ali i za rekonstrukciju događaja u slučaju incidenta. Ako je moguće preporučuje se upotreba platforme za obradu dnevničkih zapisa za nadzor, analizu i održavanje baze dnevničkih zapisa.

Mrežni promet OT sustava je znatno više deterministički [2] (predvidiv, ponovljiv) od IT komunikacije što može znatno olakšati nadzor i analizu mrežnog prometa te detekciju grešaka i anomalija [2]. Alati za detekciju (engl. *Intrusion Detection System*, IDS) i prevenciju napada (engl. *Intrusion Prevention System*, IPS) učinkoviti su u zaustavljanju dobro poznatih IT napada, a neki su proizvođači IDS/IPS svoje alate dodatno prilagodili korištenju u OT sustavima implementirajući u njih razumijevanje protokola specifičnih za OT kao što su Modbus, DNP3 i ICCP [2,5]. No, potrebno je dobro sagledati koje tehnologije i u kojim dijelovima sustava će se koristiti kako bi se izbjegao utjecaj alata za detekciju i prevenciju napada na performanse i sigurnost sustava – ne smije se dogoditi da akcije alata utječu na rad upravljačkog sustava ako dođe do lažno pozitivne detekcije incidenta ili da se instalacijom alata unesu nove ranjivosti.

2.2 NIS2 direktiva

Direktiva (EU) 2022/2557 Europskog parlamenta i vijeća - NIS2 direktiva (Network and Information Security Directive) Europske Unije za cilj ima povećati ukupnu kibernetičku otpornost kritičnih i važnih subjekata u Europskoj Uniji. Direktivom se utvrđuje osnovna razina mjera upravljanja rizicima kibernetičke sigurnosti i obveze izvješćivanja u svih subjekata koji se smatraju kritičnim ili važnim. U kritične ili važne subjekte ubrajaju se i tvrtke koje su odgovorne za kontrolu upravljanja prometom pa tako i sustav upravljanja tunelom podliježe NIS2 direktivi [6].

Mjere koje direktiva propisuje u poglavlju 4 su sljedeće [6]:

- članovi upravljačkih tijela ključnih i važnih subjekata moraju pohađati osposobljavanja te se ključne i važne subjekti potiču da slično osposobljavanje redovito nude svojim zaposlenicima kako bi stekli dovoljno znanja i vještina za procjenu rizika i upravljanje rizicima kibernetičke sigurnosti te potencijalnim učinkom upravljanja tim rizicima na usluge koje subjekt pruža
- ključni i važni subjekti moraju poduzimati odgovarajuće i razmjerne tehničke, operativne i organizacijske mjere za upravljanje rizicima kojima su izloženi mrežni i informacijski sustavi kojima se ti subjekti služe u svom poslovanju ili u pružanju svojih usluga te za sprečavanje ili smanjivanje na najmanju moguću mjeru učinka incidenata na primatelje njihovih usluga i na druge usluge. Mjere uključuju najmanje sljedeće:
    - analize rizika i sigurnosti informacijskih sustava;
    - obradu incidenata;
    - kontinuitet poslovanja i upravljanje krizama;
    - sigurnost lanca opskrbe, uključujući sigurnosne aspekte u pogledu odnosa između svakog subjekta i njegovih izravnih dobavljača ili pružatelja usluga;
    - sigurnost u nabavi, razvoju i održavanju mrežnih i informacijskih sustava, uključujući rješavanje ranjivosti i njihovo objavljivanje;
    - politike i postupke za procjenu djelotvornosti mjera upravljanja rizicima kibernetičke sigurnosti;
    - prakticiranje osnovne higijene kibernetičke sigurnosti i edukacija o kibernetičkoj sigurnosti;
    - politike i postupke u pogledu kriptografije i, prema potrebi, kriptiranja;
    - sigurnost ljudskih resursa, politike kontrole pristupa i upravljanje imovinom;

- korištenje višefaktorske autentifikacije ili rješenja kontinuirane autentifikacije, zaštićene glasovne, video i tekstualne komunikacije te sigurnih sustava za komunikaciju u hitnim slučajevima

3. Nadzorno upravljački sustav cestovnog tunela

Prema Direktivi 2004/54/EC Europskog parlamenta i Vijeća Europske unije svaki tunel duljine veće do 500 m mora zadovoljiti minimalne sigurnosne građevinske zahtjeve i minimalne sigurnosne zahtjeve za prometnu signalizaciju i opremu u tunelu koji uključuju strukturalne mjere, zahtjeve za rasvjetu, ventilaciju, stanice za hitne slučajeve, vodoopskrbu, cestovne oznake, kontrolni centar, sustave nadzora, opremu za zatvaranje tunela, komunikacijske sustave te opskrbu energijom u nuždi [7].

Minimalni propisani sigurnosni građevinski zahtjevi određuju broj tunelskih cijevi i prometnih traka, geometriju tunela, putove i izlaze u slučaju nužde, pristup za hitne službe, zaustavne površine, odvodnju i otpornost tunela na požar.

Minimalni propisani sigurnosni zahtjevi za prometnu signalizaciju i opremu uključuju rasvjetu, provjetravanje (ventilaciju), stanice za hitne slučajeve, vodoopskrbu, cestovnu prometnu signalizaciju, kontrolni centar i njegove aktivnosti, sustav praćenja (videonadzor), opremu za zatvaranje tunela, komunikacijske sustave, opskrba električnom energijom i strujni krug, otpornost opreme na požar, korištenje tunela, zatvaranje tunela i alternativne pravce, prijevoz opasnih tvari, zabranu pretjecanja teretnim vozilima u tunelu, udaljenosti između vozila i brzinu vozila, informativno-edukativne akcije i kampanje, prometne znakove, signalizaciju i opremu za tunele, radiopostaje, smještaj prometnih znakova i panela, smještaj znaka za tunel, horizontalnu signalizaciju, stanice za hitne slučajeve, zaustavne površine, izlaze u slučaju opasnosti, signale voznih traka i promjenjive prometne znakove.

U promatranom slučaju radi se o tunelu dužine veće od 3000 m koji se sastoji od dvije tunelske cijevi u kojima se odvija jednosmjeran promet iz čega proizlazi da tunel mora biti opremljen minimalno sustavima prikazanim u Tablici 2.

Rasvjeta u unutrašnjosti tunela osigurava primjerenu razinu vidljivosti danju i noći, pri čemu su njezin sastavni dio prilagodne zone na ulazu i izlazu iz tunela. U sklopu sustava rasvjete potrebno je tunel opremiti i sa sigurnosnom rasvjetom koja se aktivira prilikom kvara normalne

rasvjete ili prestanka opskrbe električnom energijom. Također, potrebno je izvesti i protupaničnu rasvjetu za evakuaciju osoba iz tunela.

Kako bi se regulirala koncentracija ispušnih plinova unutar tunela prilikom prometovanja vozila i u slučaju zaustavljanja prometa zbog incidenta ili nesreće te koncentracija dima u slučaju požara tunel je potrebno opremiti mehaničkom ventilacijom. Također, kod tunela duljih od 3000 m potrebno je postaviti pokretne žaluzine za odvod zraka i dima iz tunela te stalno pratiti uzdužnu brzinu zraka te u skladu s njom podešavati proces upravljanja ventilacijom.

Stanice za hitne slučajeve opremaju se telefonom za hitne slučajeve.

Sustav za vodoopskrbu mora osigurati dovoljnu količinu vode putem hidranta ili na drugi odgovarajući način. U slučaju da tunel nema pristup lokalnoj vodovodnoj mreži potrebno je ugraditi rezervoare za vodu, a čija razina popunjenosti se prati u kontrolnom centru.

Cestovna prometna signalizacija i oprema pružaju prometne informacije i upute korisnicima tunela.

Sustav videonadzora operaterima u kontrolnom centru pruža uvid u događanja unutar tunela, a koji pruža i mogućnost detekcije zaustavljenog vozila i pojave dima. Uz sustav videonadzora potrebno je tunel opremiti i sustavom za automatsko otkrivanje prometnih nesreća.

Kako bi se omogućilo zatvaranje tunela prema potrebi na ulazu je potrebno postaviti prometna svjetla te unutar tunela na maksimalnim razmacima od 1000 m prometne znakove te dodatna sredstva kao što su zvučnici, promjenjivi znakovi i slično.

Pravovremena komunikacija osobama koje su se zatekle u tunelu u slučaju izvanrednog događaja od iznimne je važnosti. Iz tog razloga tunel se oprema radio sustavom za reemitiranje te za komunikaciju u s hitnim službama. Također, oprema u tunelu mora omogućiti prekid radio programa kako bi se na istom kanalu emitirale hitne poruke. Ispravnost rada radio sustava potrebno je nadzirati iz kontrolnog centra.

Pouzdana opskrba električnom energijom iznimno je bitna za rad tunela, a u slučaju prekida opskrbe električnom energijom tunel mora imati nužno napajanje kako bi se osigurao rad sigurnosne opreme potrebne za evakuaciju i zatvaranje tunela. Sigurnosni strujni krugovi moraju biti otporni na kvarove na električnoj mreži te kvarove u slučaju požara.

Kontrolni centar preuzima nadzor i upravljanje tunelom ukoliko:

- prometni parametri dosegnu kritične vrijednosti,

- uvjeti u okolišu ugrožavaju sigurnost prometa (slaba vidljivost, visoka koncentracija CO i slično),
- dođe do pojave izvanrednih nepredvidivih ili predvidivih događaja (radovi na cesti, prometna nesreća, požar i slično).

Zadaće kontrolnog centra su:

- prikupljanje prometnih i okolišnih podataka koji se odnose na izvanredne događaje na prilazima i unutar tunela,
- kontrola trenutnog stanja prometa i upravljanje tunelom za vrijeme izvanrednih događaja,
- upravljanje ventilacijom, rasvjetom i nadzor električnog napajanja,
- upravljanje prometom i informiranje korisnika i drugih javnih službi o izvanrednim događajima.

U normalnom radu tunela svi sustavi rade neovisno od kontrolnog centra, a njihove međusobne interakcije programirane su na razini svakog pojedinog sustava.

Kontrolni centar oprema se SCADA sustavom koji u stvarnom vremenu omogućuje prikaz informacija o mjerenjima i trenutnom stanju povezanih sustava, a prema potrebi operateri u kontrolnom centru mogu i upravljati povezanim sustavima.

Budući da videonadzor uobičajeno nije sastavni dio SCADA sustava, u kontrolnom centru instalira se i poseban softver za konfiguraciju, upravljanje i prikaz videonadzora – VMS (engl. *Video Management System*) ili ako postoje još neki od sustava fizičke zaštite PSIM. U promatranom slučaju koristi se PSIM softver koji osim prikaza videonadzora prihvaća informacije iz sustava za automatsku detekciju incidenata koje prikazuje i zatim prosljeđuje SCADA sustavu. Iz SCADA sustava PSIM prima zahtjeve za prikazom kamera povezanih s alarmnim događajima iz ostalih sustava.

Za prikaz navedenih softvera kontrolni centar najčešće se oprema video zidom koji omogućuje jasan prikaz situacije u tunelu kako bi operateri mogli reagirati na incidente koji zahtijevaju njihovu pozornost u što kraćem roku. Primjer video zida prikazan je na Slici 2.

Slika 2: Video zid u kontrolnom centru tunela Učka

Redundantno napajanje tunela najčešće se izvodi pomoću zasebne veze na elektroenergetski sustav sa svake strane tunel pri čemu je zanimljivo da često to znači i da tunel ima vezu prema dvije različite elektroenergetske domene unutar iste države ili čak u dvije različite države. Kako te elektroenergetske domene mogu imati međusoban pomak u fazi od kritične je važnosti osigurati da se one nikad međusobno ne povežu jer bi to moglo dovesti do ozbiljnih problema u opskrbi električnom energijom samog tunela, ali i ostalih subjekata koji koriste električnu energiju iz tih elektroenergetskih domena.

Tablica 2: Minimalna sigurnosna oprema tunela

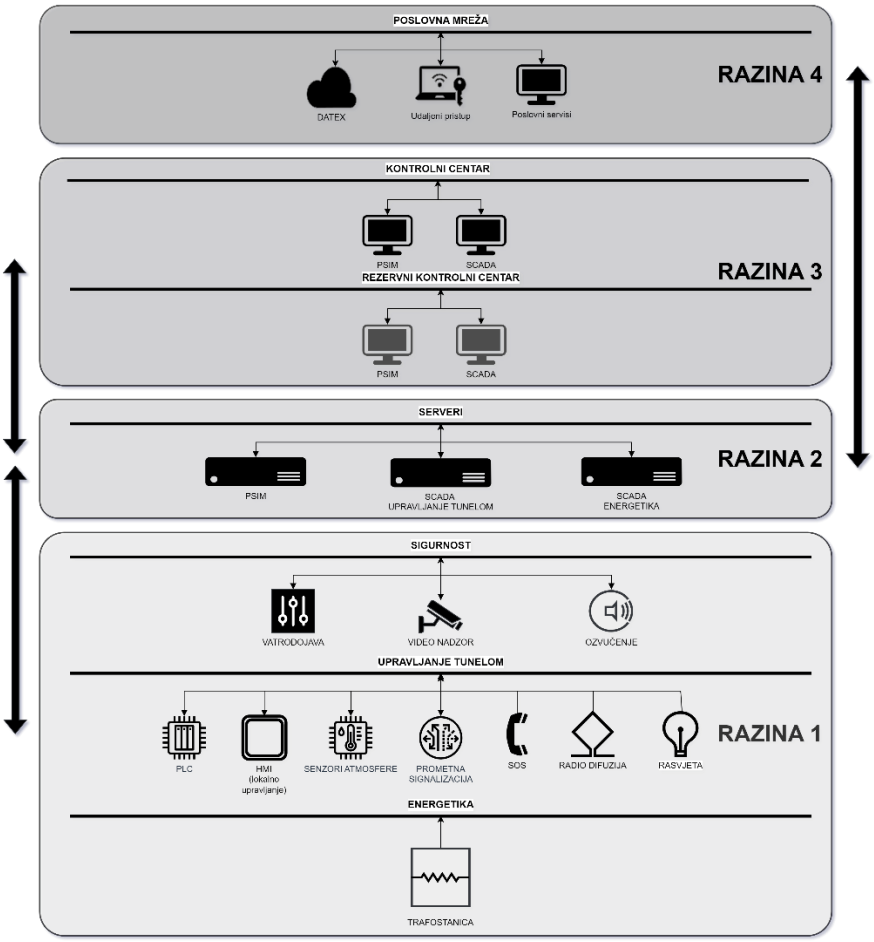
Sustav	**Podsustavi**
Rasvjeta	Normalna rasvjeta Nužna rasvjeta Protupanična rasvjeta za evakuaciju
Ventilacija	Mehanička ventilacija Posebni uređaji za poprečnu ventilaciju
Stanice za hitne slučajeve (najmanje svakih 150 m)	
Vodoopskrba (najmanje svakih 250 m)	
Cestovna prometna signalizacija i oprema	
Kontrolni centar i rezervni kontrolni centar	
Sustavi nadzora	Videonadzor Automatsko otkrivanje incidenata i/ili požara
Oprema za zatvaranje tunela	Prometni signali prije ulaza Prometni signali unutar tunela najmanje svakih 1000 m
Komunikacijski sustavi	Radio emitiranje za hitne službe Hitne radio poruke za korisnike tunela Zvučnici u skloništima i izlazima
Opskrba energijom u nuždi	

3.1 Datex II

DATEX II je standard koji se koristi u Europi za razmjenu informacija o prometu. Razvoj DATEX II započeo je početkom devedesetih godina zbog potrebe za razmjenom informacija između centara za promet operatora autocesta, a nakon čega se pokazala potreba za dijeljenjem prometnih informacija pružateljima usluga povezanih s prometom. DATEX I je bio donekle ograničen za ovu svrhu te je koristio zastarjele tehničke koncepte. Zato je DATEX II razvijen u ranim 2000-tim. Pomoću DATEX II, informacije o prometu i upravljanju prometom distribuiraju se na način koji nije ovisan o jeziku i formatu prikaza. To znači da nema prostora za nesporazume i/ili prijevodne pogreške kod primatelja, ali primatelj može odabrati uključivanje govornog teksta, slike na karti ili integraciju u navigacijski proračun. Na neki način, sličan je prirodnom jeziku, s gramatikom i rječnikom. DATEX II je standard za sektor informacija o prometu i putovanjima kako bi se podaci dijelili i pružila sveobuhvatna informacijska usluga krajnjem korisniku. DATEX II je dizajniran i razvijen kao mehanizam za razmjenu podataka o prometu i putovanjima od strane europske radne skupine koja je osnovana radi standardizacije sučelja između centara za kontrolu i informiranje o prometu.

3.2 Nadzorno-upravljački sustav cestovnog tunela

Kako je ranije navedeno, za upravljački sustav koji ne sadrži IIoT uređaje i funkcionira kao neovisna cjelina u odnosu na poslovni sustav tvrtke kojemu služi samo kao izvor podataka ISA95 mrežna arhitektura smatra se standardom te će se ta ista arhitektura koristiti i za nadzorno-upravljački sustav cestovnog tunela. Kada se nabrojani minimalni sigurnosni zahtjevi za cestovni tunel uključe u ISA95 model, dobijemo sustav prikazan na Slici 3.



Slika 3: Blok shema sustava nadzorno-upravljačkog sustava cestovnog tunela u ISA95 modelu

Smještaj podsustava po razinama je sljedeći:

- razina 1: sustavi za upravljanje i nadzor tunelom. Ovi sustavi ključni su za sigurnost prometa u tunelu i potrebno je osigurati njihov autonoman rad – u najvećem mogućem opsegu oni moraju raditi i ako se prekine veza s višim razinama.
- razina 2: serverske komponente za nadzor i upravljanje sustavima na razini 1
- razina 3: korisničko sučelje za nadzor i upravljanje sustavima u tunelu
- razina 4: komponente koje imaju pristup do nadzorno upravljačkog sustava cestovnog tunela. Nadzor nad ovim komponentama je u nadležnosti IT službe tvrtke koja upravlja tunelom. Ova razinu omogućuje komunikaciju prema DATEX sustavu, udaljeni pristup zaposlenika tvrtke koja upravlja tunelom te vanjskih izvođača kojima je omogućen pristup. Također, ovdje se nalaze poslovni servisi koji prikupljaju podatke iz sustava u tunelu.

U ovako strukturiranom sustavu sa stajališta potencijalnih prijetnji možemo zaključiti da:

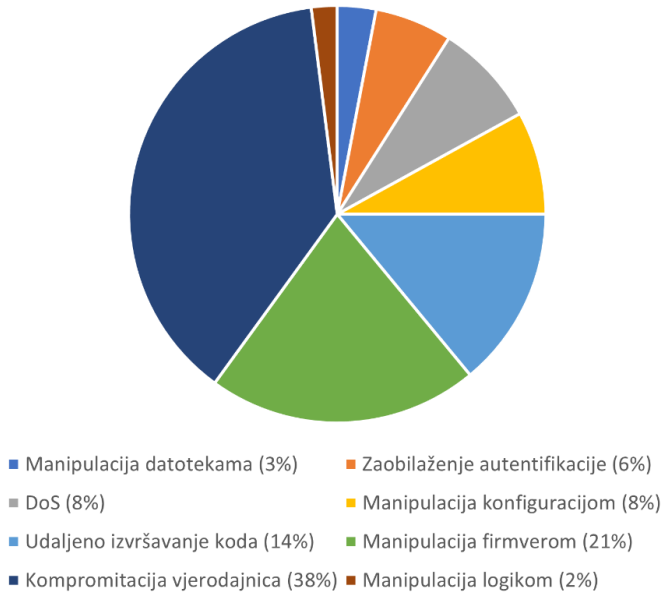
- oprema na razinama 1 i 2 smještena je na fizički zaštićena mjesta gdje pristup ima mali broj autoriziranih korisnika koji zloupotrebom ili nepažnjom predstavljaju najveću prijetnju sustavu. Također, zloupotreba vjerodajnica (kartica, PIN i slično) autoriziranih korisnika od strane zlćudnih pojedinaca prijetnja je koju je potrebno minimizirati odgovarajućim sustavima kontrole pristupa. Mrežno ove razine nemaju direktnu vezu prema vanjskom svijetu,
- na razini 3 nalazi se oprema s kojom interakciju imaju operateri pa na ovoj razini treba osigurati da pristup imaju samo autorizirani korisnici te da ti korisnici poštuju pravila korištenja te opreme. Mrežno ova razina nema direktan pristup vanjskom svijetu,
- razina 4 zapravo je razina IT sustava i oprema ovdje je pod kontrolom IT službe. Ova razina ima direktan pristup vanjskom svijetu što ju čini najmanje sigurnom razinom. S obzirom da zbog raznih poslovnih potreba razina 4 mora imati pristup do razine 3 posebnu pozornost potrebno je usmjeriti na ograničavanje tog pristupa na najmanju moguću razinu. Također, korištenje sigurnih protokola u komunikaciji sa razinom 4 važno je kako bi se minimizirala mogućnost manipulacije podacima u tranzitu ili curenja vjerodajnica.

4. Identifikacija prijetnji

Posljednjih godina primjećuje se porast kibernetičkih napada na upravljačke sustave što je u skladu i s općenitim porastom kibernetičkog kriminala, većim tehničkim znanjem napadača i prelaskom s oportunističkih na ciljane kibernetičke napade [8].

Kako bi bilo koji sustav mogli obraniti od kibernetičkog napada potrebno je najprije identificirati potencijalne napadače, njihovu motivaciju te ranjivosti sustava koji je potrebno obraniti.

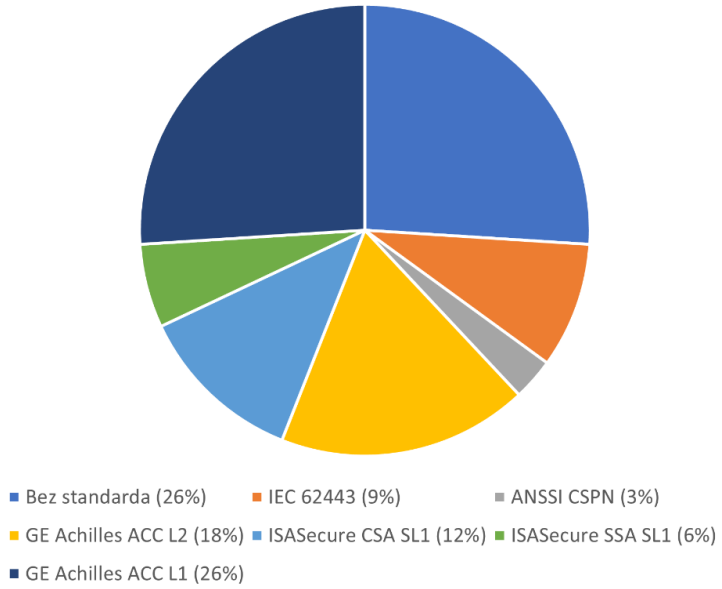
Tvrtka Vedere Labs je provela istraživanje o postojećim ranjivostima u OT uređajima te je do lipnja 2023. u izvještaju nazvanom OT:ICEFALL izdala popis od 61 ranjivosti u opremi 13 različitih proizvođača OT uređaja [9]. Cilj istraživanja bio je osvijestiti zajednicu o postojećim ranjivostima i greškama u dizajnu hardvera i softvera. Ranjivosti su podijeljene u 4 glavne kategorije: nesigurni protokoli, slaba kriptografija ili slomljena autentifikacija, nesigurna nadogradnja firmvera i udaljeno izvršavanje koda korištenjem nativnih funkcionalnosti, a tipovi ranjivosti i njihov udio u ukupnom broju pronađenih ranjivosti prikazan je na Slici 4.



Slika 4: Tipovi ranjivosti objavljeni u izvješću OT:ICEFALL[9]

Veliki dio pogođenih uređaja proizvođači tvrde da su razvijeni vodeći se načelom sigurnosti u dizajnu (engl. „*secure by design*“), pri čemu, kako je prikazano na Slici 5, njih čak 74% posjeduje neku vrstu certifikata da su napravljeni prema određenim sigurnosnim standardima.

Kako bi se dodatno naglasio paradoks ovakve situacije u izvještaju se ti uređaji nazivaju „*insecure by design*“.



Slika 5: Standardi prema kojima su uređaji s ranjivostima certificirani [9]

Vlasnici sustava, kako bi mogli donijeti pravilne odluke oko segmentacija, nadzora i ojačavanja sustava, moraju biti svjesni ranjivosti u hardvera i softveru koji se nalazi u njihovim sustavima i zbog toga su istraživanja i objavljivanja postojećih ranjivosti iznimno važna.

4.3 Kibernetički napad na Carmel Tunnels

Carmel Tunnels je niz od 4 tunela otvorenih 2010. godine ukupne dužine 8,6 kilometara – dva tunela dužine 3,5 km i dva tunela dužine 1,6 km smještenih u gradu Haifa, trećem po veličini grada u Izraelu. Svrha tunela je smanjenje gužve unutar samog grada i povećanje sigurnosti putnika budući su alternativa pravcu koji uključuje putovanje preko planinskog područja. Korištenjem tunela putovanje s jednog kraja grada na drugi smanjeno je s 30-50 minuta na 6 minuta [10].

Tunel je 2013. godine pretrpio napad zloćudnim kodom u obliku trojanskog konja koji je ciljao sustav video nadzora tunela. Posljedica napada bilo je inicijalno zatvaranje tunela u periodu od 20 minuta te naknadno zatvaranje sljedećeg dana u trajanju od 8 sati koje je prouzročilo ogromne gužve i financijske gubitke [11]. Detalji napada nisu nikad objavljeni jer su ti podaci klasificirani kao tajni.

Čak i iz ovakvog šturog opisa događaja vidi se da su napadači uspjeli pristupiti sustavu video nadzora i ubaciti zlćudni kod. Sustav video nadzora spada u OT tehnologije i ne bi trebao biti lako dostupan izvana.

4.4 Potencijalni napadači

Napadači na upravljačke sustave uključuju unutarnje – npr. nezadovoljne zaposlenike i vanjske subjekte – pojedince, haktiviste, kiberkriminalce i državno sponzorirane aktere (engl. *advanced persistent threat,* APT), pri čemu imaju različite ciljeve kao što su financijska dobit, špijunaža, sabotaža ili posljedice na zdravlje i život ljudi.

Unutarnji napadači mogu biti zaposlenici čije radno mjesto ne uključuju potrebu za pristupom nadzorno-upravljačkom sustavu tunela (djelatnici službi koje nisu direktno povezane sa upravljanjem prometom u tunelu, npr. kadrovska služba). Ti zaposlenici sustav mogu napasti fizičkom sabotažom nekog od ključnih dijelova sustav ako uspiju dobiti pristup u prostore gdje se oni nalaze ili kibernetičkim napadom sa razine 4 gdje oni kao zaposlenici imaju pristup. Njihova meta su sustavi na razinama 1, 2 i 3, pri čemu ako pokušaju sabotirati razinu 3 moraju istovremeno izvesti napad i na glavni i na rezervni kontrolni centar što je zahtjevno budući da se oni nalazite na fizički odvojenim lokacijama. Napad na sustave na razini 1 fizičkom sabotažom kompliciran je zbog činjenice da se sustavi fizički nalaze u tunelu, a kibernetički napad traži široko tehničko znanje. Zbog toga su sustavi na razini 2 ipak njihova vjerojatna meta budući da se fizički nalaze izvan tunela i radi se o hardveru i softveru šire primjene (npr. serveri sa Windows operacijskim sustavom) za koje postoje javno dostupne informacije o ranjivostima, a čak i razvijeni napadi. Obrana od ovakve vrste napadača sastoji se od strogih politika fizičkog pristupa ključnim komponentama sa razine 2 i 3, a također kod njihovog projektiranja treba voditi računa o visokoj dostupnosti u slučaju ispada napajanja, mreže i sličnog. Uz to potrebno je zaštiti razine 1, 2 i 3 od neautoriziranog pristupa sa razine 4. Unutarnji napadači koji imaju pristup sustavu (zaposlenici kontrolnog centra ili oni uključeni u njegov rad) vjerojatno će štetu pokušati napraviti kroz korisničko sučelje sustava pa je potrebno osigurati dobru kontrolu nad upravljačkim pravima operatera te svaku akciju operatera zabilježiti u dnevničkim zapisima kako bi se lako mogao detektirati počinitelj. Također, klijentska računala na razini 3 potrebno je zaštititi od prijenosa zlćudnog koda instalacijom odgovarajućih zaštitnih aplikacija te ograničavanjem korisničkih prava (npr. zabrana korištenja prijenosne memorije) ukoliko to poslovni zahtjevi dopuštaju.

S obzirom na kompleksnost i specifičnost sustava u tunelu vanjski napadači moraju imati visoku razinu znanja kako bi prvo uspješno izveli napad na IT sustav tvrtke koja upravlja tunelom, koji ima vezu prema internetu, a zatim uspješno izveli prelazak u domenu nadzorno-upravljačkog sustava gdje ponovno moraju imati visoku razinu znanja da bi mogli dobiti pristup sustavima na razini 2, a još više da bi mogli izvesti napad na sustave na razini 1. Takvu razinu znanja možemo očekivati kod APT skupina čija bi motivacija u slučaju cestovnog tunela najvjerojatnije bila sabotaža sa svrhom onemogućavanja prometa između dvije, prirodno odvojene, teritorijalne cjeline. Također, uz APT skupine potrebna razina znanja mogla bi se naći kod izuzetno sposobnih kiberkriminalaca. Primarni motiv kiberkriminalaca je financijska dobit koju obično dobivaju ucjenom nakon izvedbe napada ucjenjivačkim kodom. Napadi ucjenjivačkim kodom uobičajeno ciljaju IT sustave s obzirom na to da je kod njih vrijednost sadržana u podacima, dok kod ovakvog sustava vrijednost proizlazi iz dostupnosti sustava koju bi ucjenjivački kod morao ugroziti. Kako bi se ugrozila dostupnost sustava ucjenjivački kod bi morao onemogućiti rad sustava na razini 1, a da bi to učinio morao bi biti usko specijaliziran budući da se tamo ne nalaze uređaji koji su općenito u širokoj primjeni. Razvoj takvog ucjenjivačkog koda bio bi zahtjevan i samim time bi tražio značajna financijska ulaganja, a što je u suprotnosti s načelima djelovanja kiberkriminalnaca. Konačno, možemo zaključiti da je najvjerojatniji vanjski napadač APT skupina s motivom sabotaže sustava.

4.5 Prijetnje

Nakon što smo identificirali potencijalne napadače i njihovu motivaciju sljedeći zadatak je identificirati način na koji je moguće izvesti napad. Da bi to učinili potrebno je definirati model prijetnje promatranog sustava. Postoje razni načini za konstrukciju modela prijetnje kao što su [12]: STRIDE, PASTA, stablo napada, OCTAVE. U sklopu rada odlučeno je da će se za modeliranje prijetnji koristiti stabla napada.

Stablo napada (engl. *attack tree*) je metodički način opisa sigurnosti sustava temeljen na mogućim načinima napada [13]. Ono je grafički prikaz mogućih napada na sustav pri čemu korijen stabla predstavlja konačni cilj napadača, a listovi stabla predstavljaju različite načine postizanja tog cilja – podciljeve. Za postizanje konačnog cilja napadač mora zadovoljiti podciljeve pojedine grane, pri čemu oni mogu biti u *ILI* odnosu – samo jedan podcilj mora biti zadovoljen kako bi se napadač približio konačnom cilju ili u *I* odnosu – više podciljeva istovremeno mora biti zadovoljeno kako bi se napadač približio konačnom cilju.

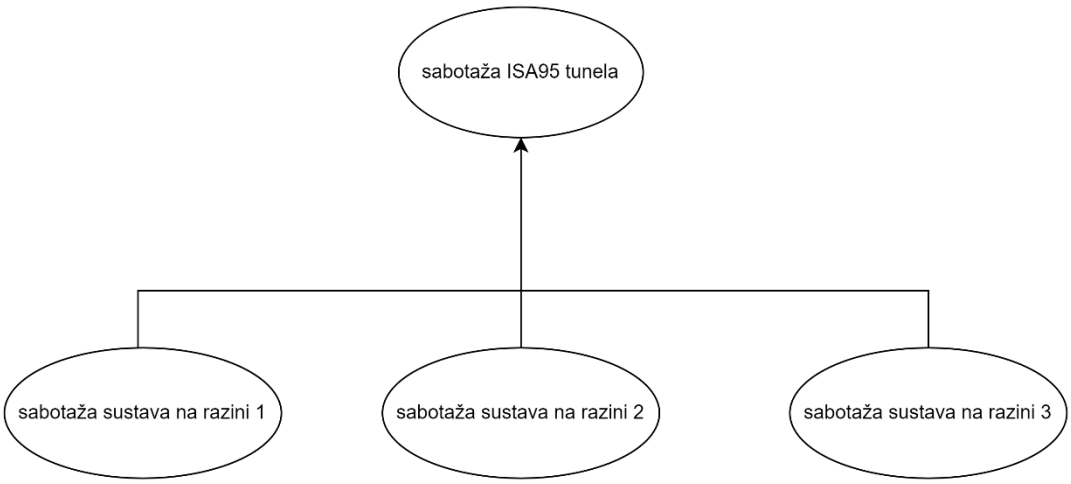
Kod identifikacije potencijalnih napadača zaključili smo kako je najvjerojatniji cilj sabotaža nadzorno-upravljačkog sustava tunela, a s posljedicom zatvaranja tunela. Osim toga, moguća posljedica je i utjecaj na rad elektroenergetskog sustava povezivanjem dviju elektroenergetskih domena.

Sabotažom ćemo smatrati onemogućavanje rada pojedinog sustava. Kod fizičkih sustava koji provode određena mjerenja na temelju kojih se donosi zaključak o mogućem incidentu (npr. vatrodojava) moguće je provesti sabotažu i generiranjem lažnih mjerenja prema SCADA sustavu koji ga nadzire. Budući da se na razini 1 nadzorno-upravljačkog sustava tunela nalaze razni sustava koji koriste različite protokole za komunikaciju sa SCADA sustavom proučavanje mogućnosti iskorištavanja potencijalnih ranjivosti komunikacijskog protokola za generiranje lažnih mjerenja smatra se previše specifičnim za ovaj rad.

Kako je nadzorno-upravljački sustav cestovnog tunela podijeljen u funkcionalne cjeline, razmotrit ćemo prvo utjecaj sabotaže na svaku od razina:

- razina 4: Funkcije iz ove razine nisu od nužnog značaja za rad tunela pa njihova sabotaža nema posljedice na rad tunela,
- razina 3: Kontrolni centar i rezervni kontrolni centar zakonski su preduvjet za funkcioniranje tunela pri čemu da bi sabotaža bila uspješna nužno da se ona odnosni na oba kontrolna centra, a u suprotnom tunel može nastaviti s prometom vozila,
- razina 2: Iako je pri projektiranju sustava cilj osigurati automatizirano izvršavanje odgovora na prometne ili sigurnosne incidente na razini 1, nadzor i upravljanje sustavima na razini 1 koje omogućuju razina 2, a izvršava se na razini 3 zakonski je preduvjet funkcioniranja tunela. Dakle, sabotaža razine 2 ne bi trebala imati utjecaja na rad sustava na razini 1, ali bi onemogućila rad razine 3 i prekid komunikacije s razinom 4. S obzirom na to da je rad razine 3 ključan za rad tunela možemo zaključiti kako bi sabotaža razine 2 dovela do zatvaranja tunela,
- razina 1: Izvršavanje funkcija sustava u tunelu kod detekcije incidenta, kvara i sličnog definira se Prometno informacijskim sustavom (PIS) tunela koji detaljno opisuje interakcije među sustavima. S obzirom na to da je on specifičan za svaki pojedini tunel u svrhu ovog rada pretpostavit ćemo da se tunel zatvara pri onemogućavanju bilo kojeg od sustava iz ove razine.

Slika 6 prikazuje stablo napada na razine tunela koje rezultira zatvaranjem tunela.



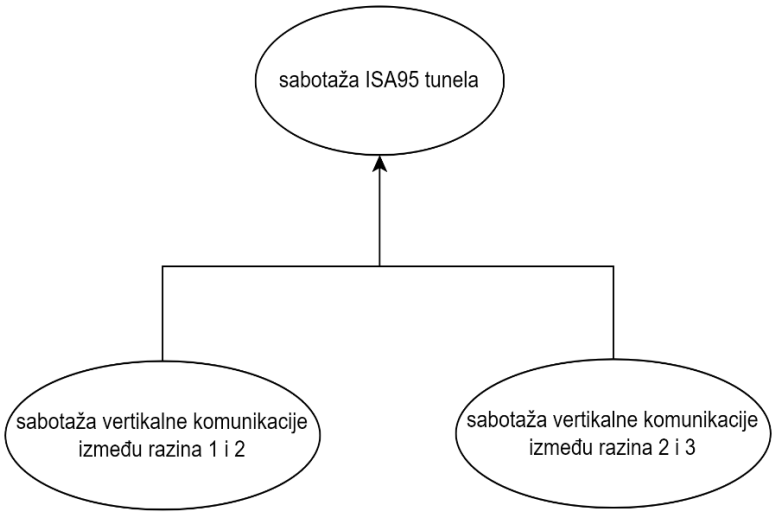
Slika 6: Stablo napada na razine tunela temeljenog na ISA95 arhitekturi

Osim sabotažom samih podsustava tunela njegovo zatvaranje moguće je uzrokovati i sabotažom mrežne komunikacije između (vertikalna komunikacija) ili unutar razina (horizontalna komunikacija).

Vertikalna komunikacija postoji između:

- razina 4 i 2: ova komunikacija nije ključna za funkcionalnost tunela pa se njezinim onemogućavanjem ne postiže željeni cilj,
- razina 2 i 3: ova komunikacija omogućuje rad kontrolnog i rezervnog kontrolnog centra i ključna je za rad tunela pa se njezinim onemogućavanjem također onemogućuje i njihov, a bez čega tunel ne može funkcionirati,
- razina 1 i 2: ova komunikacija omogućuje nadzor i upravljanje sustavima na razini 1 i iako sustavi na razini 1 bez ove komunikacije u nekoj mjeri mogu funkcionirati onemogućava se rad kontrolnog i rezervnog kontrolnog centra, a bez čega tunel ne može funkcionirati.

Slika 7 prikazuje stablo napada za vertikalnu komunikaciju nadzorno-upravljačkog sustava cestovnog tunela.



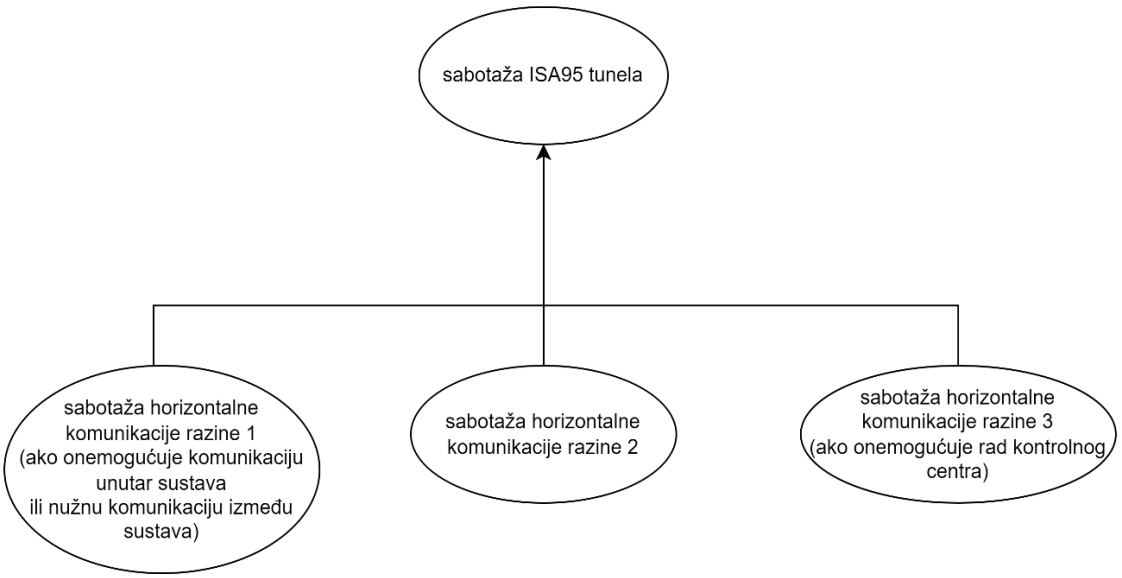
Slika 7: Stablo napada na vertikalnu komunikaciju tunela temeljenog na ISA95 arhitekturi

Horizontalnom su komunikacijom povezane komponente pojedinih sustava te je omogućena komunikacija različitih sustava na istoj razini.

- razina 4: komunikacija sustava u poslovnoj mreži tvrtke koja nije ključna za rad tunela,
- razina 3: komunikacija između komponenti u kontrolnom centru ovisi o implementaciji kontrolnog centra, no za pretpostaviti je kako prekidom komunikacije tih komponenti sustav gubi dio mogućnosti, no ne i nužno one osnovne pa bi on mogao zadržati svoju funkcionalnost, a time i spriječiti zatvaranje tunela. Isto vrijedi i za rezervni kontrolni centar,
- razina 2: na ovoj razini horizontalna komunikacija služi za razmjenu podataka između centralne SCADA-e i SCADA-e za energetiku te PSIM-a. Budući da operateri u kontrolnom centru rade isključivo s centralnom SCADA-om, ova komunikacija iznimno je bitna za rad tunela jer njezinim gubitkom operateri u kontrolnom centru gube sve informacije iz podsustava sigurnosti i energetike. Možemo zaključiti kako je, dođe li do onemogućavanjem ove komunikacije, tunel nužno zatvoriti,
- razina 1: na ovoj razini horizontalna komunikacija ima dvije svrhe – komunikaciju između samih sustava i komunikaciju komponenti unutar pojedinih sustava. Ako sustavi sa svojim komponentama komuniciraju na mrežnoj razini, tada prekid te komunikacije rezultira u potpunom onemogućavanju rada tog sustava, a time i rada tunela. Također, ako je komunikacija između različitih sustava izvedena na mrežnoj

razini, a nužna je u slučaju incidenta (npr. paljenje crvenih svjetala na semaforima u slučaju alarma vatrodojave) tada onemogućavanje te komunikacije rezultira zatvaranjem tunela.

Slika 8 prikazuje stablo napada za horizontalnu komunikaciju nadzorno-upravljačkog sustava cestovnog tunela.

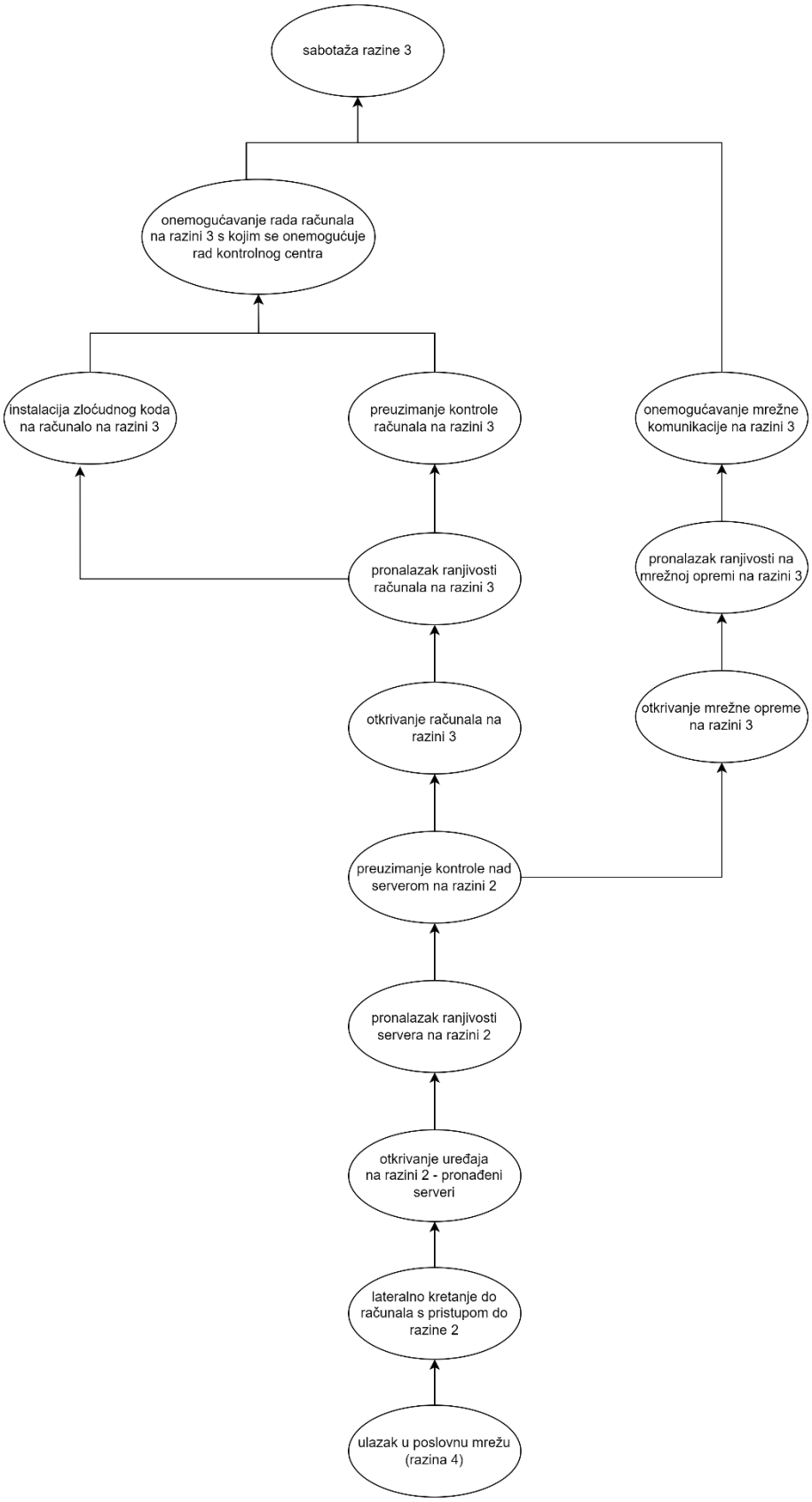


Slika 8: Stablo napada na horizontalnu komunikaciju tunela temeljenog na ISA95 arhitekturi

Vjerojatno je da se onemogućavanjem horizontalne komunikacije na pojedinoj razini onemogućava i vertikalna komunikacija te razine s ostalima. U tom slučaju vrijedi isto što i kod razmatranja prekida vertikalne komunikacije između razina.

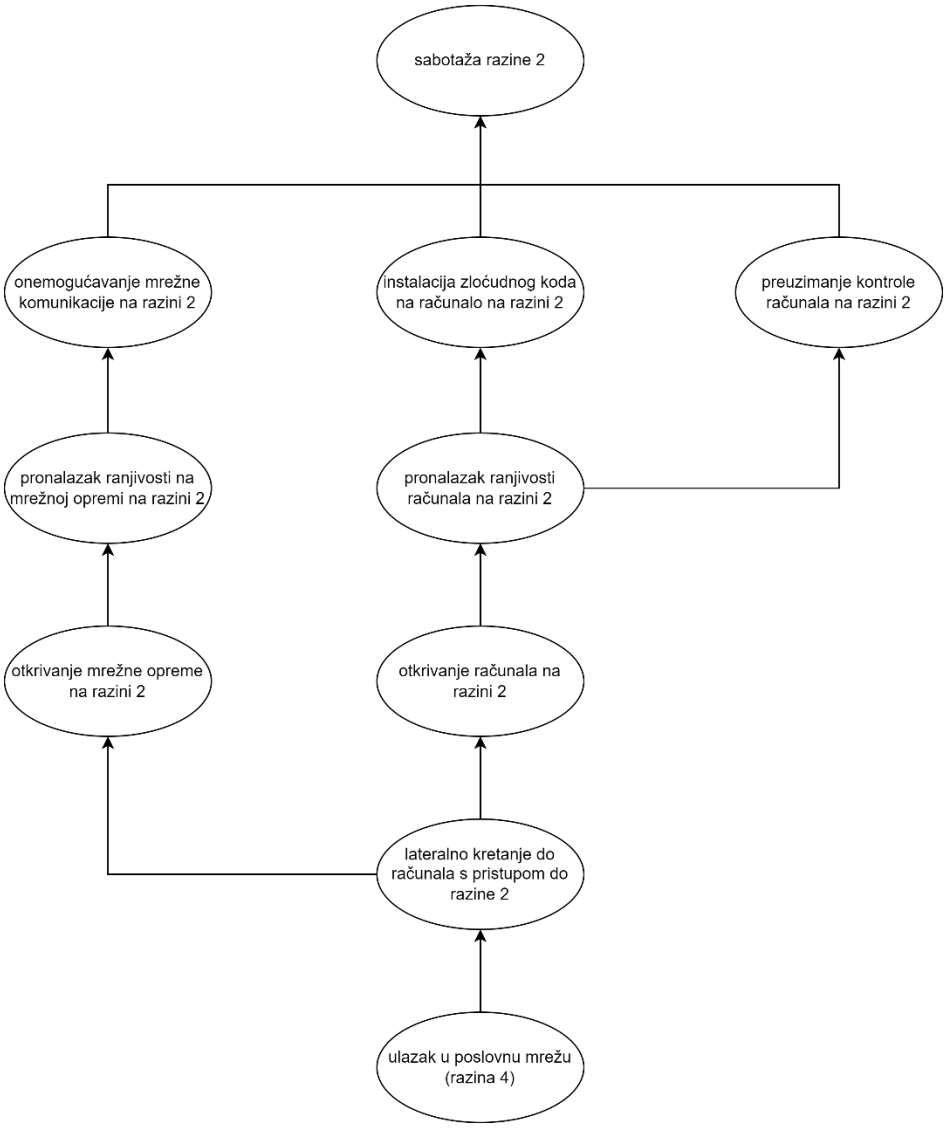
Može se zaključiti kako je zatvaranje tunela moguće postići sabotažom sustava na razinama 1, 2 i 3 te vertikalnom i horizontalnom komunikacijom tih istih razina pa su u nastavku prikazana stabla napada na svaku pojedinu razinu.

Slika 9 prikazuje stablo napada na razinu 3 gdje su prikazani koraci pristupa do razine 3 te načini onemogućavanja rada klijentske opreme koja se koristi za nadzor i upravljanje tunelom ili mrežne opreme koja omogućuje komunikaciju unutar razine 3 kao i s razinom 2.



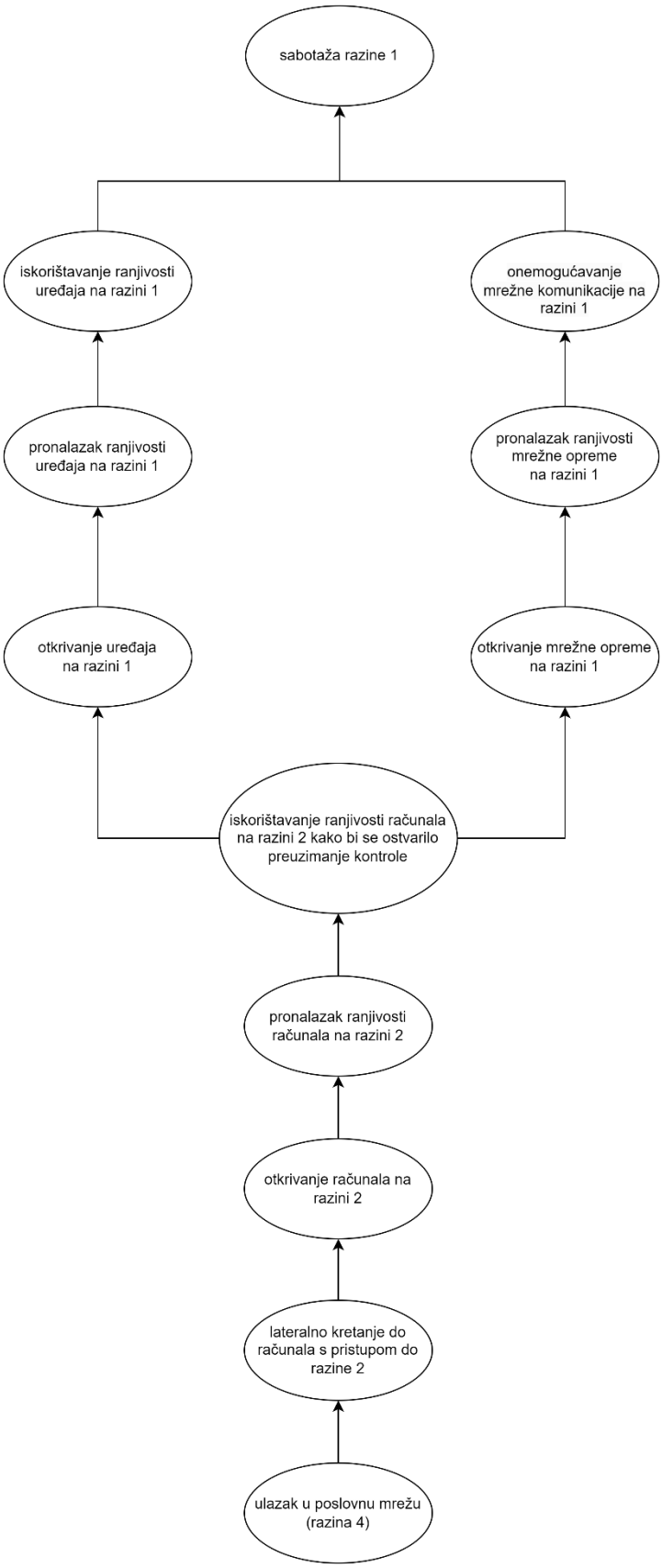
Slika 9: Stablo napada na razinu 3 tunela temeljenog na ISA95 arhitekturi

Slika 10 prikazuje stablo napada na razinu 2 gdje su prikazani koraci pristupa do razine 2 te mogući napadi na servere koji se nalaze na toj razini te mrežnu opremu koja omogućuje komunikaciju unutar razine 2 kao i s razinama 3 i 1 kao i napad na komunikaciju s razinama 3 i 1.



Slika 10: Stablo napada na razinu 2 tunela temeljenog na ISA95 arhitekturi

Slika 11 prikazuje stablo napada na razinu 1 gdje su prikazani koraci pristupa do razine 1 te prikazani mogući napadi na sustave koji mogu prouzročiti prestanak njihovog rada te napadi na mrežnu opremu na ovoj razini.



Slika 11: Stablo napada na razinu 1 tunela temeljenog na ISA95 arhitekturi

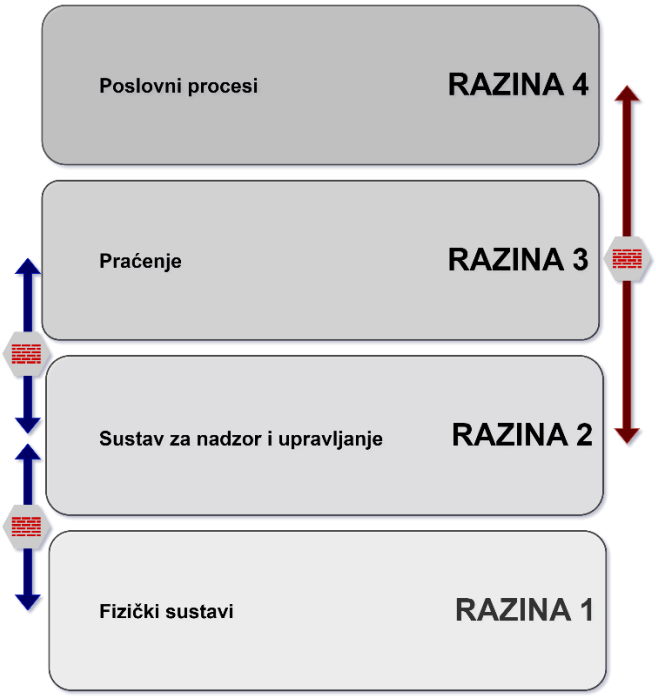
Iz prikazanih stabla napada za razine 3, 2 i 1 vidljivo je da svi napadi kreću iz poslovne mreže, odnosno razine 4 koja ima vezu prema Internetu. Razina 4 jedinu vezu s nadzorno-upravljačkim sustavom tunela ostvaruje preko razine 2, tako da je ona sljedeći korak svakog napada. Kada napadač dospije do razine koja mu je cilj koristi jedan od sljedećih napada kako bi ostvario zadatak:

- instalacija zloćudnog koda (npr. ucjenjivački kod),
- preuzimanje kontrole nad uređajem,
- promjena postavki uređaja,
- napad na dostupnost zauzimanjem dostupnih resursa (engl. *Denial-of-service attack*, DOS) napad,
- izmjena komunikacije između uređaja pozicioniranjem napadača u sredinu komunikacije (engl. *Man-in-the-middle attack*, MITM).

Sa stajališta napadača za očekivati je kako će njegov cilj biti točka sustava koja od njega traži najmanji napor za postizanje željenog krajnjeg cilja – sabotaže rada tunela. Iz stabla napada vidljivo je kako svi napadi za preduvjet imaju pristup na razinu 2, a putem koje se također može provesti željeni cilj. Može se dakle zaključiti da je zaštita pristupa razini 2 najvažniji cilj sigurnosnih mjera koje je potrebno implementirati.

5. Sigurnosne mjere

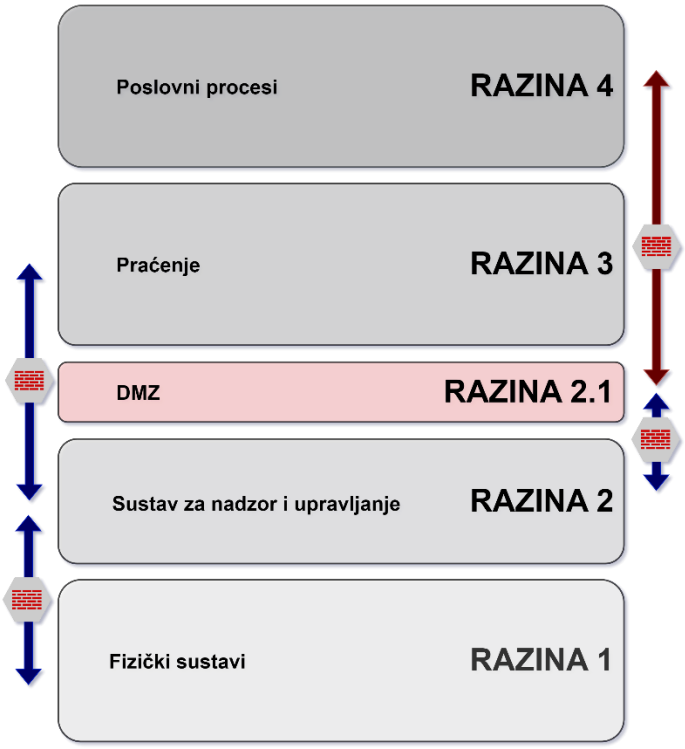
Mrežna arhitektura prema ISA95 standardu svojom podjelom sustava na razine sama po sebi nameće segmentaciju sustava prema potrebnoj mrežnoj komunikaciji što je općenito jedna od minimalnih sigurnosnih mjera koje je moguće implementirati u sustavu. Kako bi omogućili potrebnu komunikaciju između različitih razina potrebno je dobro poznavanje potreba za komunikacijom između uređaja. Budući da je u upravljačkom sustavu komunikacija između mrežnih OT uređaja strogo definirana funkcijom uređaja i većinom se sastoji od komunikacije točno određenim protokolom po točno određenom portu lako se dobije strogo kontrolirana mrežna komunikacija između razina. Može se zaključiti kako je između pojedinih razina jednostavno implementirati vatrozid koji dopušta samo prolaz dobro poznate komunikacije [14] kako je prikazano na Slici 12.



Slika 12: Mrežna arhitektura prema ISA95 standardu s vatrozidom

Kako je utvrđeno u prethodnom poglavlju mogući izvor vanjske prijetnje je razina 4 iz koje je moguće prijeći na razinu 2. Budući da je to i uobičajeni način udaljenog pristupa do sustava za poslove održavanja zadatak je IT službe, koja vodi brigu o sigurnosti poslovne mreže, u najvećoj mogućoj mjeri onemogući lateralno gibanje do računala s pristupom do upravljačke mreže tunela. S obzirom na to da razmjena podataka između poslovnih servisa i upravljačke mreže ne mora uključivati i mogućnost korištenja udaljenog pristupa do upravljačke mreže

potrebno je u konfiguraciji vatrozida između razina 4 i 2 onemogućiti korištenje udaljenog pristupa do računala čime značajno smanjujemo mogućnost prelaska na razinu 2. Također, preporučuje se razinu 2 proširiti demilitariziranom zonom kako je prikazano na Slici 13 u koju se smještaju uređaji sa servisima koji moraju komunicirati s razinom 4 [15]. DMZ zona trebala bi sadržavati i računalo koje služi kao prijelazni domaćin (engl. *jump host*) putem kojeg je jedino moguće pristupiti u DMZ zonu, pri čemu se za autentifikaciju na prijelaznom domaćinu koristi vjerodajnice različite od onih za udaljeni (VPN) pristup. Uz prijelaznog domaćina DMZ zona može sadržavati i mamac (engl. *honeypot*) – računalo koje namjerno sadrži sigurnosne propuste i koje se ne koristi za funkcioniranje sustava nego se pristup njemu nadzire. Svaki pristup mamcu smatra se alarmom.



Slika 13: Mrežna arhitektura prema ISA95 standardu s vatrozidom i DMZ-om

U slučaju da napadač uspije ostvariti prelazak sa razine 4 na razinu 2 i dalje na razine 3 ili 1 potrebno je implementirati sigurnosne mjere koje trebaju spriječiti napade navedene u prethodnom poglavlju, a koje su ovisne o uređaju koji se napada. Općenito, na razini 1 potrebno je voditi računa o zaštiti komunikacije uvođenjem kriptografije budući da su upravljački protokoli većinom nezaštićeni. Također, mnogi upravljački uređaji, npr. PLC, sadrže mogućnosti definiranja popisa IP adresa s kojima je dopuštena komunikacija što svakako treba

ispravno konfigurirati budući da je taj popis unaprijed poznat. Na razinama 2 i 3, gdje se uglavnom nalaze računala, potrebno je redovito instalirati sigurnosne zakrpe kako one ne bi sadržavale poznate ranjivosti, a obavezna je i instalacija antivirusne zaštite.

6. Zaključak

Cestovni tunel sadrži niz kompleksnih tehničkih sustava koji osiguravaju odvijanje prometa na siguran način. Međusobno povezivanje tih sustava te njihovo povezivanje s poslovnom mrežom tvrtke koja upravlja tunelom potrebno je izvesti tako da se osim funkcionalnih zahtjeva zadovolje i zahtjevi za njihovom kibernetičkom sigurnosti. U sklopu ovog rada prikazane su razlike IT i OT sustava te preporuke vezane za kibernetičke zaštitu OT sustava.

Za tunel odabranih parametara na osnovu minimalnih sigurnosnih zahtjeva definiranih zakonom koji propisuje koji se sustavi moraju nalaziti u tunelu prikazana je mrežna arhitektura tunela u kojoj su ti sustavi raspoređeni u razine definirane ISA95 mrežnom arhitekturom.

Pokazano je kako je prikazani sustav vjerojatna meta APT grupa budući da, od mogućih vanjskih napadača, oni jedini imaju znanje, resurse i motivaciju za napad na ovakvu metu. Analizom sustava korištenjem stabla napada zaključeno je kako je najveći napor potrebno uložiti u osiguranje veze nadzorno-upravljačkog sustava s poslovnom mrežom koja u ovakvoj arhitekturi, uz pretpostavku fizičke sigurnosti mrežnih komponenti, jedina može biti izvor prijetnje od vanjskog napadača. Osiguranje veze između poslovne mreže i nadzorno-upravljačkog sustava cestovnog tunela moguće je implementacijom vatrozida koji bi kontrolirao promet na toj vezi. Također, ISA95 mrežnu arhitekturu moguće je proširiti dodatnom sigurnosnom razinom – DMZ zonom u kojoj je moguće implementirati dodatne sigurnosne mehanizme kao što je prijelazni domaćin ili mamac.

7. Literatura

[1] Knapp, E.D., Langill, J.T., „Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems“, Elsevier, 2015.

[2] Stouffer K., Pease M., Tang C., Zimmerman T., Pillitteri V., Lightman S., „NIST 800-82r3 Guide to Operational Technology (OT) Security“, NIST, 2022.

[3] The European Union Agency for Cybersecurity, „Communication network dependencies for ICS/SCADA Systems“, dostupno na: https://www.enisa.europa.eu/publications/ics-scada-dependencies (2.5.2023.)

[4] Garbis, J., Chapman, J.W., „Zero Trust Security: An Enterprise Guide“, Apress, 2021.

[5] Adamiak, M., Baigent, D., Mackiewicz, R., „IEC 61850 communication networks and systems in substations: An overview for users“, The Protection & Control Journal. 1988, str. 61-68.

[6] Europski parlament i Vijeće Europske unije, „Direktiva (EU) 2022/2557 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2)“, dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32022L2555&qid=1695153585142#d1e3309-80-1 (10.5.2023.)

[7] Ministarstvo pomorstva, prometa i infrastrukture, „Pravilnik o minimalnim sigurnosnim zahtjevima za tunele“, dostupno na. https://narodne-novine.nn.hr/clanci/sluzbeni/2013_07_96_2153.html (6.5.2023.)

[8] The European Union Agency for Cybersecurity, „ENISA threat landscape: transport sector“, dostupno na: https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape (10.5.2023.)

[9] Vedere Labs, „OT:ICEFALL The legacy of “insecure by design” and its implications for certifications and risk management“, dostupno na: https://www.forescout.com/resources/ot-icefall-report/ (22.5.2023)

[10] Wikipedia, „Carmel Tunnels“, dostupno na: https://en.wikipedia.org/wiki/Carmel_Tunnels (2.6.2023.)

[11] Esterin D, „Israeli road tunnel hit by cyber-attack“, dostupno na: https://www.timesofisrael.com/israeli-road-tunnel-hit-by-cyber-attack/ (2.6.2023.)

[12] Shevchenko, N., Chick, T.A., O'Riordan, P., Scanlon, T.P., Woody, C.: Threat modeling: a summary of available methods. Tech. rep., Carnegie Mellon University Software Engineering Institute, 2018.

[13] Schneier, B., "Attack trees: Modeling security threats," Dr. Dobb's Journal, December. 1999

[14] Byres, E., Karsch, J., Carter, J., „NISCC good practice guide on firewall deployment for SCADA and process control networks, 2005.

[15] Mathezer, S., „Introduction to ICS Security Part 3, dostupno na: https://www.sans.org/blog/introduction-to-ics-security-part-3 (3.6.2023.)