SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

RAD

Razvoj eksperimentalnog postava industrijskog upravljačkog sustava za ispitivanja kibernetičke sigurnosti

Filip Katulić

Zagreb, 2021.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

RAD

Razvoj eksperimentalnog postava industrijskog upravljačkog sustava za ispitivanja kibernetičke sigurnosti

Filip Katulić

Zagreb, 2021.

Ovaj rad izrađen je na Zavodu za elektrostrojarstvo i automatizaciju na Fakultetu elektrotehnike i računarstva, pod vodstvom prof.dr.sc. Damira Sumine i predan je na natječaj za dodjelu Rektorove nagrade u akademskoj godini 2020/2021.

Skraćenice

ACL	Lista dozvoljenih pristupa (engl. *Access Control List*)
ARP	Protokol za razlučivanje adresa (engl. *Address Resolution Protocol*)
COTP	COTP protokol (engl. *Connection Oriented Transport Protocol*)
CVE	Ranjivosti sustava (engl. *Common Vulnerabilities and Exposures*)
CVSS	Standardni okvir za određivanje razine prijetnje ranjivosti (engl. *Common Vulnerability Scoring System*)
DB	Blok podataka (engl. *Data Block*)
DoS	Onemogućavanje usluge (engl. *Denial of Service*)
FC	Funkcija (engl. *Function*)
GDPR	Opća uredba o zaštiti podataka (engl. *General Data Protection Regulation*)
HIL	Hardver u petlji (engl. *Hardware In the Loop*)
HMI	Sučelje stroj-čovjek (engl. *Human Machine Interface*)
HTTPS	(engl. *HyperText Transfer Protocol over TLS*)
IACS	Industrijski upravljački sustav (engl. *Industrial Automation and Control System*)
IEC	Međunarodna elektrotehnička komisija (engl. *International Electrotechnical Commission*)
IP	Internet protokol (engl. *Internet Protocol*)
ISO	Međunarodna organizacija za normizaciju (engl. *International Organization for Standardization*)
IT	Informacijske tehnologije (engl. *Information Technologies*)
LAD	Ljestvičasti dijagram (engl. *Ladder Diagram*)

LAN	Lokalna mreža (engl. *Local Area Network*)
L2	Oprema na sloju podatkovne poveznice (engl. *Layer 2*)
MAC	MAC adresa (engl. *Media Access Control*)
MiTM	Napadač u komunikacijskom kanalu (engl. *Man in The Middle*)
NDP	Protokol za otkrivanje susjeda (engl. *Neighbor Discovery Protocol*)
NIC	Mrežna kartica (engl. *Network Interface Card*)
Nmap	Nmap (engl. *Network mapper*)
OB	Organizacijski blok (engl. *Organization Block*)
OSI	Referentni model za otvoreno povezivanje sustava (engl. *Open Systems Interconnection*)
PCS	Procesni upravljački sustav (engl. *Process Control System*)
PDU	Protokolna podatkovna jedinica (engl. *Protocol Data Unit*)
PHA	Analiza procesnog hazarda (engl. *Process Hazard Analysis*)
PLC	Programirljivi logički kontroler (engl. *Programmable Logic Controller*)
RT	U stvarnom vremenu (engl. *Real Time*)
SCADA	Sustav za nadzor, mjerenje i dohvat podataka (engl. *Supervisory Control And Data Acquisition*)
TCP	Transmisijski upravljački protokol (engl. *Transmission Control Protocol*).
TLS	Sigurnost transportnog sloja (engl. *Transport Layer Security*)
TPKT	TPKT protokol (engl. *ISO transport services on top of the TCP*)
VLAN	Virtualna lokalna mreža (engl. *Virtual Local Area Network*)
QoS	Kvaliteta usluge (engl. *Quality of Service*)

Sadržaj

1. Uvod 1

2. Hipoteza te ciljevi rada 3

3. Analiza radova o kibernetičkoj sigurnosti industrijskih upravljačkih sustava 4

4. Opis razvijenog eksperimentalnog postava 9

4.1. Model linije za sortiranje 11

4.2. Programirljivi logički kontroler S7-1516-3 PN/DP 13

4.3. Upravljivi preklopnik SCALANCE X308-2 15

4.4. Implementacija upravljačkog algoritma modela 17

4.5. Implementacija HMI sučelja za upravljanje i nadzor modelom linije za sortiranje . 19

5. Istraživanje kibernetičke sigurnosti razvijenog sustava 21

5.1. Industrijski komunikacijski protokol S7CommPlus 22

5.2. Napad u svrhu prikupljanja informacija 25

5.3. Napad u svrhu onemogućavanja komunikacije između uređaja 27

5.4. Preporuke za sprječavanje predstavljenih kibernetičkih napada na eksperimentalni postav 31

6. Zaključak 36

Literatura 38

Sažetak 41

Summary 42

Popis slika

Slika 4.1 Prikaz implementiranog eksperimentalnog postava 9

Slika 4.2 Prikaz mrežne topologije implementiranog eksperimentalnog postava 10

Slika 4.3 Prikaz modela linije za sortiranje 11

Slika 4.4 Prikaz topologije linije za sortiranje [Interni dokument FER-a] 12

Slika 4.5 Prikaz programirljivog logičkog kontrolera S7-1516-3 PN/DP 13

Slika 4.6 Prikaz industrijskog upravljivog preklopnika SCALANCE X308-2 15

Slika 4.7 Prikaz programskog stabla unutar alata TIA Portal 17

Slika 4.8 Dijagram toka upravljačkog algoritma modela linije za sortiranje 18

Slika 4.9 Prikaz zaslona naziva *Odabir rada* 19

Slika 4.10 Prikaz zaslona naziva *Rucni* 20

Slika 4.11 Prikaz zaslona naziva *Automatski* 20

Slika 5.1 Prikaz raspodjele komunikacijskog protokola S7CommPlus prema OSI referentnom modelu 22

Slika 5.2 Struktura komunikacijskih poruka kod industrijskog komunikacijskog protokola S7CommPlus 23

Slika 5.3 Prikaz razmjene podataka unutar industrijske komunikacijske mreže implementiranog eksperimentalnog postava 24

Slika 5.4 Prikaz mrežnog dijagrama postrojenja uslijed odabranog scenarija kibernetičkog napada 25

Slika 5.5 Prikaz dobivenih informacija o PLC-u uslijed skeniranja pomoću alata Nmap 26

Slika 5.6 Prikaz ARP zahtjeva uređaja na komunikacijskoj mreži 28

Slika 5.7 Prikaz ARP odgovora uređaja na mreži 28

Slika 5.8 Prikaz sučelja alata Ettercap 29

Slika 5.9 Prikaz komunikacije između uređaja nakon provedbe postupka ARP trovanja 30

Slika 5.10 Prikaz upravljačkog sučelja alata SINEC PNI 31

Slika 5.11 Prikaz upravljačkog sučelja za autorizaciju korisnika preklopnika SCALANCE X308-2 32

Slika 5.12 Prikaz podešenja MAC ACL tablice upravljivog preklopnika SCALANCE X308-2 33

Slika 5.13 Prikaz pokušaja otkrivanja uređaja na mreži nakon implementacije MAC ACL tablica 34

Slika 5.14 Prikaz izbornika za deaktivaciju priključaka upravljivog preklopnika SCALANCE X308-2 35

Popis tablica

Tablica 3.1 Metrika za određivanje ponašanja sustava u trenutcima provođenja kibernetičkih napada 5

Tablica 3.2 Intervali rezultata analize ranjivosti prema sustavu CVSS v3.1 6

Tablica 4.1 Značajke PLC-a S7-1516-3 PN/DP 14

Tablica 4.2 Značajke industrijskog upravljivog preklopnika SCALANCE X308-2 16

1. Uvod

Kibernetička sigurnost (engl. *Cybersecurity*) predstavlja pojam kojim se opisuju postupci, alati te znanja čijim se provođenjem smanjuje rizik od kibernetičkih incidenata unutar nekog sustava [1]. Osnovna podjela mjera vezanih uz kibernetičku sigurnost jest podjela na tehničke mjere za povećanje sigurnosti te mjere vezane uz politike i procedure unutar organizacije [2]. Kibernetički incidenti mogu biti različiti, ali im je zajedničko to što se ostvarivanjem kibernetičkog incidenta ugrožavaju procesi i vrijednosti koji su bitni za organizaciju koja je napadnuta. Sam pojam vrijednosti i kritičnih procesa definira organizacija temeljem usluga koje pruža, ali i zakonodavstvo – moguć je slučaj da neke informacije nekoj organizaciji ne predstavljaju značajnu vrijednost (npr. lokalni restoran sprema podatke o mobilnim brojevima i adresama kupaca zbog jednostavnijeg provođenja dostave), ali temeljem zakonskih odredbi organizacija je takve informacije dužna štititi – kao primjer navodi se Opća uredba o zaštiti podataka [3] (engl. *General Data Protection Regulation* – GDPR). Jasno, određeni sustavi zahtijevaju veću razinu kibernetičke sigurnosti od drugih, ali sud o razini zahtjeva sigurnosti mora se donijeti temeljem relevantnih sigurnosnih analiza rizika (engl. *Cybersecurity Risk Analysis*). Razina razvoja kibernetičke sigurnosti pojedinih sustava različita je u ovisnosti o vremenskom trenutku od kojeg je krenulo vođenje računa o sigurnosti. Tako se u literaturi [4] navodi da su početci kibernetičke sigurnosti IT sustava (engl. *Information Technology*) krenuli 1970-ih godina unutar projekta ARPANET (engl. *The Advanced Research Projects Agency Network* – ARPANET) koji je zapravo preteča modernog Interneta, dok se o kibernetičkoj sigurnosti industrijskih upravljačkih sustava (engl. *Industrial Automation and Control System* – IACS) krenulo razmišljati tek 2000-ih godina [5]. Razlog tomu leži u činjenici da se fokus kod IACS-ova postavljao na dostupnost podataka, dok se sigurnost u IT sustavima fokusira na integritet i tajnost podataka. Svijest o kibernetičkoj sigurnosti nekog proizvoljnog sustava – industrijskih upravljačkih sustava, financijskih usluga, računalnih sustava te ostalih kritičnih sustava predstavlja pojam odnosno veličinu kojom je moguće modelirati razinu znanja, sposobnosti i metoda za smanjenje kibernetičkog rizika po sustav [6].

Razinu svijesti o sigurnosti nekog sustava moguće je procijeniti analizom politika i procedura poduzeća vezanih uz sigurnost, razgovorom sa zaposlenicima, analizom dokumentacije i povijesti kibernetičkih incidenata unutar poduzeća te u konačnici

ispitivanjem implementiranih metoda za povećanje sigurnosti i opreme unutar nekog sustava. Navedeni koraci analize rizika već se provode i propisani su zakonom u pojedinim granama IT tehnologije (financijski sektor), dok se unutar kritičnih IACS sustava (sustavi koji predstavljaju značajan rizik u slučaju kompromitacije) zakonom i normama još uvijek najčešće provode procesne analize opasnosti (engl. *Process Hazard Analysis* – PHA). Provedba navedenih analiza u ovisnosti o veličini sustava zahtijeva iznimnu razinu znanja, iskustva, vremena te ljudstva, ali kretnje u zakonodavstvu Europske unije [7] pokazuju da će analize kibernetičke sigurnosti i testiranja sigurnosti opreme unutar IACS-ova postati propisane i zahtijevane zakonom i normama. Slijedom navedenih tvrdnji, može se zaključiti da je razvoj svijesti o sigurnosti industrijskih upravljačkih sustava od kritičnog značaja ne samo za vlasnike i zaposlenike navedenih sustava, već i država unutar kojih se kritični sustavi nalaze. U nastavku slijedi istraživački razvoj čiji je zadatak implementacija te istraživanje mogućnosti fizičkih eksperimentalnih postava za ispitivanje kibernetičke sigurnosti industrijskih upravljačkih sustava.

2. Hipoteza te ciljevi rada

Osnovna hipoteza ovog rada jest da se korištenjem modela linije za sortiranje te industrijske opreme koja tvori svako industrijsko postrojenje mogu kvalitativno provoditi ispitivanja metoda za povećanje kibernetičke sigurnosti IACS-ova, vršiti edukacije, ispitivati ranjivosti odabrane opreme te u konačnici razvijati znanje i svijest o razini kibernetičke sigurnosti industrijskih upravljačkih sustava.

Ciljevi ovog rada slijede u nastavku:

- Razviti model postrojenja za sortiranje izradaka, koji će predstavljati stvarno postrojenje.
- Razviti i implementirati algoritam za upravljanje postrojenjem za sortiranje izradaka korištenjem programirljivog logičkog kontrolera (engl. *Programmable Logical Controller*) te jednog od programskih jezika definiranih normom IEC 61131-3.
- Razviti i implementirati sučelje čovjek-stroj (engl. *Human-Machine Interface* – HMI) za upravljanje postrojenjem.
- Analizirati postojeće radove i literaturu o kibernetičkoj sigurnosti industrijskih upravljačkih sustava, s posebnim fokusom na radove koji analiziraju napade na eksperimentalne postave IACS-ova.
- Predstaviti alate te izvršiti odabrane kibernetičke napade na eksperimentalni postav.
- Analizirati daljnje mogućnosti kod proširenja eksperimentalnog postava IACS-a.

3. Analiza radova o kibernetičkoj sigurnosti industrijskih upravljačkih sustava

Kao što je navedeno, kibernetička sigurnost IACS-ova predstavlja temu niza znanstvenih radova te istraživanja, od kojih su za ovaj rad od posebne važnosti istraživanja vezana uz implementaciju eksperimentalnih postava industrijskih upravljačkih sustava za proučavanje kibernetičke sigurnosti.

Prvi rad [8] koji je potrebno istaknuti jest rad unutar kojeg su autori proučavali ponašanje implementiranog eksperimentalnog postava kemijskog postrojenja temeljenog na modelu Tennessee Eastman (TE). Tennessee Eastman model predstavlja jedan od općepoznatih modela procesnih upravljačkih sustava (engl. *Process Control Systems* – PCS) kojim je moguće istraživati sustave regulacije, nadzora parametara procesa, identifikacije topologije sustava i slično [9]. Nakon implementacije eksperimentalnog modela, autori su proveli niz kibernetičkih napada na postrojenje temeljem definiranih napadačkih scenarija. Nakon provedbe kibernetičkih napada, autori su proveli detaljnu analizu napadačkih scenarija te ponudili neka od rješenja za povećanje kibernetičke sigurnosti ugroženog sustava. Uz navedene rezultate ispitivanja eksperimentalnog postava, autori su predstavili različite kvalitativne metrike za određivanje ponašanja različitih tipova sustava (mjerni sustavi, kontinuirani odnosno diskretni upravljački sustavi) u trenutcima provođenja kibernetičkih napada.

Zbog nepostojanja regulacijskih petlji, ponašanje industrijskog postrojenja koje je implementirano i razvijeno u okviru ovog rada moguće je pratiti metrikom za diskretne sustave. Slijedom navedenih tvrdnji, slijedi tablica 3.1 unutar koje je dana metrika za određivanje ponašanja sustava u trenutcima provođenja kibernetičkih napada.

Tablica 3.1 Metrika za određivanje ponašanja sustava u trenutcima provođenja kibernetičkih napada

Mjera	Opis
Kvaliteta izratka	U primjeru modela linije za sortiranje, kvaliteta izratka temelji se na ispravnosti očitane boje odnosno ubacivanja izratka u ispravni spremnik.
Stopa izradaka s manom	U primjeru modela linije za sortiranje, stopa izradaka s manom predstavlja stopu izradaka s manom u odnosu na ukupan broj izradaka.
Broj izradaka s manom po jedinici mjere	U primjeru modela linije za sortiranje, broj izradaka s manom po jedinici mjere predstavlja broj izradaka s manom u odnosu na dogovorenu jedinicu (npr. na 100 izradaka)
Vrijeme odgovora procesa	U primjeru modela linije za sortiranje, vrijeme odgovora procesa predstavlja vrijeme potrebno da model reagira na upravljački signal poslan s HMI-ja.
Vrijeme trajanja procesa	U primjeru modela linije za sortiranje, vrijeme trajanja procesa predstavlja najveće vrijeme potrebno za sortiranje izratka za vrijeme trajanja kibernetičkog napada.

Drugi rad [10] koji je potrebno istaknuti jest rad autora koji proširuju navedeni eksperimentalni postav s kemijskog postrojenja na još tri različita industrijska upravljačka sustava – sustava upravljanja željeznicom (engl. *Rail Transit*), sustava pametne mreže (engl. *Smart Grid*) te u konačnici upravljačkog sustava standardnog za obradu metala. Svaki od sustava implementiran je koristeći opremu različitih proizvođača, time omogućujući analizu ranjivosti opreme različitih proizvođača. Posebno zanimljiv napadački scenarij proveden na implementiranom eksperimentalnom postavu jest napad na sustav pametne mreže koji se provodi temeljem scenarija analognog stvarnom napadu na ukrajinski elektro-opskrbni sustav [11].

Treći rad koji se bavi tematikom sigurnosti jest rad [12] autora koji daju pregled mogućih metoda za otkrivanje ranjivosti industrijskih upravljačkih sustava, pregled postojećih eksperimentalnih postava za analizu kibernetičke sigurnosti IACS-ova te u konačnici metode za povećanje sigurnosti industrijskih sustava. Zanimljivost navedenog rada jest isticanje važnosti implementacije simulacije procesa IACS-ova (engl. *Hardware in the Loop* – HIL) kod kojih je moguće ne destruktivno ispitivati sigurnost sustava. Također, unutar rada navedeni su zahtjevi koje HIL sustav mora ispuniti da bi takvi sustavi bili reprezentativni unutar određenih dijelova svijeta automatizacije.

Kao četvrto istaknuto istraživanje jest rad [13] grupe autora koja je razvila potpuno simuliran model sustava za nadzor i upravljanje (engl. *Supervisory Control And Data Acquisition* – SCADA) elektro-opskrbne mreže za ispitivanje utjecaja kibernetičkih napada na ponašanje komponenti mreže. Zanimljivost istraživanja temelji se na zaključku da je osnovni nedostatak istraživanja nepostojanje fizičkih komponenti (PLC, HMI i slično) unutar sustava. Iz tog razloga, autori navode da rezultati istraživanja provedeni na simulacijskom modelu sustava predstavljaju ranjivosti programa za emulaciju navedenih komponenti, a ne samih komponenti.

Osim znanstvenih istraživanja, za ovaj istraživački rad posebno su zanimljive javne baze podataka o postojećim poznatim ranjivostima opreme u industrijskoj automatizaciji, temeljem kojih je odabran dio komponenti unutar ovog istraživanja. Tako je kao prvu zanimljivu javno dostupnu bazu podataka poznatih ranjivosti opreme potrebno istaknuti bazu podataka naziva CVE (engl. *Common Vulnerabilities and Exposures* – CVE) organizacije MITRE. CVE prikuplja javno otkrivene podatke o ranjivostima fizičke opreme i softvera od proizvođača ugrožene opreme, nacionalnih organizacija za sigurnost i drugih organizacija za praćenje ranjivosti te omogućuje jednostavan prikaz i klasifikaciju ranjivosti prema odabranom sustavu za određivanje razine moguće prijetnje [14]. Tako CVE koristi standardni okvir za određivanje razine prijetnje ranjivosti naziva CVSS v3.1 (engl. *Common Vulnerability Scoring System*) pomoću kojeg je moguće određivanje ozbiljnosti otkrivene ranjivosti prema numeričkom rezultatu dobivenom analizom prema dogovorenoj metrici [15]. Tablicom 3.2 dan je prikaz intervala rezultata analize ranjivosti prema sustavu CVSS v3.1 u odnosu na ozbiljnost ranjivosti.

Tablica 3.2 Intervali rezultata analize ranjivosti prema sustavu CVSS v3.1

Ozbiljnost ranjivosti	**Rezultat analize ranjivosti prema sustavu CVSS**
Nepostojeća	0
Niska	0.1-3.9
Srednja	4.0-6.9
Visoka	7.0-8.9
Kritična	9-10

Tako je istraživanjem i proučavanjem javno dostupnih podataka otkrivena ranjivost CVE-2020-15782 SIMATIC uređaja proizvođača Siemens (unutar kojih pripada i PLC S7-1516-3 PN/DP koji se koristi u ovom istraživačkom radu) koja napadaču omogućuje pristup čitavom memorijskom prostoru PLC-a, time omogućujući zapisivanje i čitanje osjetljivih podataka [16]. Tvrtka koja je otkrila navedenu ranjivost uspjela je pristupiti memorijskom prostoru PLC-a kojem standardno nije dopušteno pristupati te injektirati maliciozni programski kod kojim je instaliran program na razini jezgre operacijskog sustava koji nije moguće detektirati. Jezgra operacijskog sustava (engl. *Kernel*) jest sustav koji predstavlja osnovu svakog operacijskog sustava, a jedna od funkcionalnosti joj je predstavljanje sučelja između fizičke opreme sustava (procesorska jedinica, fizička memorija) i softverskih procesa. Za zlouporabu ranjivosti, napadač mora ostvariti pristup priključku 102 ciljanog SIMATIC uređaja, a pristup može biti fizički odnosno putem Interneta. Ranjivost je prema sustavu CVSS v3.1 klasificirana kao visoka (rezultat 8.1). Nakon objave podataka o ranjivosti, tvrtka Siemens objavila je dokument [17] unutar kojeg su ponuđene moguće mjere za rješavanje otkrivene ranjivosti. Tako je za dio SIMATIC uređaja izdano ažuriranje firmvera kojim se sprječava zlouporaba ranjivosti, dok za dio uređaja (unutar kojih se nalazi PLC koji se koristi unutar ovog rada) ažuriranje firmvera u trenutku pisanja ovog rada nije dostupno. Uz ažuriranje firmvera, unutar dokumenta [17] navodi se niz specifičnih metoda i prijedloga, od kojih se kao jedan od načina za smanjenje kibernetičkog rizika po sustav može primijeniti koncept obrane u dubinu (engl. *Defense in depth*) koji predstavlja standardnu metodu obrane od kibernetičkih ugroza unutar IT sustava [2]. Sam koncept obrane u dubinu oslanja se na implementaciju niza segmentiranih obrambenih sustava za povećanje kibernetičke sigurnosti kod kojih se u slučaju probijanja određenog sloja obrane, sustav još uvijek u potpunosti ne kompromitira. Zbog složenosti provedbe napada koji koristi analiziranu kritičnu ranjivost PLC-a S7-1500, ranjivost CVE-2020-15782 neće se detaljno razmatrati u nastavku ovog istraživanja, ali implementacijom eksperimentalnog postava industrijskog upravljačkog sustava unutar kojeg se nalazi PLC S7-1516-3 PN/DP otvara se mogućnost za nova istraživanja i ispitivanja kibernetičke sigurnosti navedenog uređaja, kao i ostalih uređaja razvijenog eksperimentalnog postava.

Unutar eksperimentalnog postava, moguće je modelirati napadača koji ima fizički pristup priključku 102, što je prema dokumentu [17] jedini zahtjev koji je potrebno ispuniti prije zlouporabe ranjivosti.

Slijedom navedenih radova i istraživanja, donesen je zaključak o smjeru razvoja eksperimentalnog postava industrijskog upravljačkog sustava za provođenje ispitivanja kibernetičke sigurnosti. Vidljivo je iz priloženih radova da razvoj eksperimentalnog sustava u topologiji stvarni model procesa – PLC – HMI ima smisla, ali je potrebno obratiti pozornost na moguće uništenje modela procesa eksperimentalnog postava u slučaju provedbe nekog kibernetičkog napada koji omogućuje uništenje neke komponente modela (npr. kratko spajanje motora trake).

Iz tog razloga, odabran je model linije za sortiranje izradaka prema boji kod kojeg je iznimno zahtjevno postaviti vrijednosti digitalnih izlaza/ulaza PLC-a koji bi izazvali uništenje modela procesa.

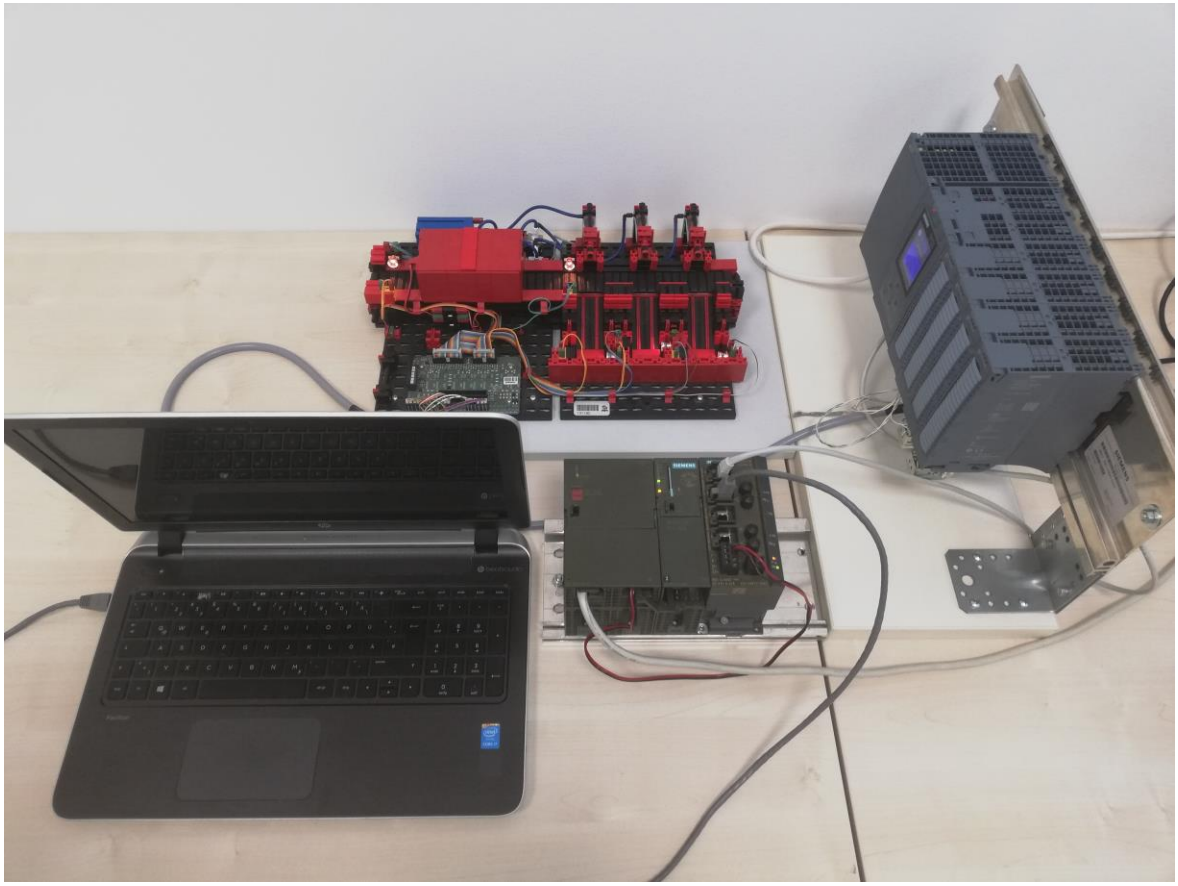
Također, u slučaju nasumičnog pokretanja određenih dijelova linije za sortiranje (npr. istovremeno pokretanje razvodnika koji pokreću pneumatske ventile) nije moguće fizički uništiti model.

Nakon pregleda postojećih radova o eksperimentalnim postavima za analizu kibernetičke sigurnosti industrijskih upravljačkih sustava, slijedi opis razvijenog eksperimentalnog sustava za provođenje ispitivanja kibernetičke sigurnosti.

4. Opis razvijenog eksperimentalnog postava

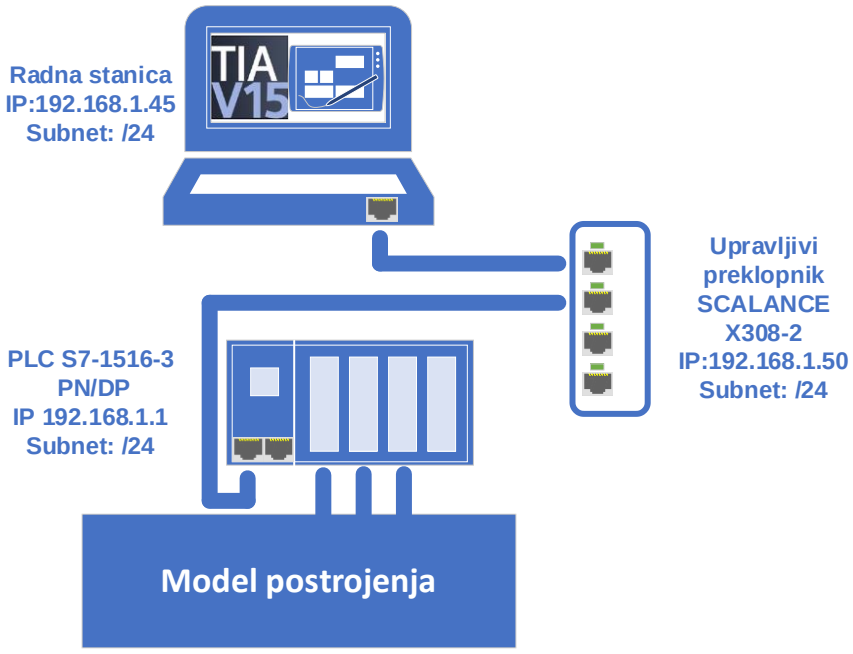
Sustav za ispitivanje kibernetičke sigurnosti eksperimentalnog modela industrijskog upravljačkog sustava sastoji se od odabranih komponenti čije je ranjivosti potrebno utvrditi te ispitati. Sigurnost samog sustava ne ovisi isključivo o opremi, već i o mrežnoj topologiji sustava, politikama unutar poduzeća vezanim uz kibernetičku sigurnost i slično [2].

Slikom 4.1 dan je prikaz implementiranog postava koji se sastoji od modela linije za sortiranje koji predstavlja industrijsko postrojenje, programirljivog logičkog kontrolera S7-1500 proizvođača Siemens, upravljivog industrijskog preklopnika (engl. *Managed switch*) SCALANCE x308-2 proizvođača Siemens te radne stanice (engl. *Work station*) na kojoj je implementirano sučelje čovjek-stroj (engl. *Human Machine Interface* – HMI). Standardno, programirljivi logički kontroler služi za automatizaciju postrojenja i procesa, dok sučelje čovjek-stroj služi za nadzor te interakciju sa sustavom upravljanja.



Slika 4.1 Prikaz implementiranog eksperimentalnog postava

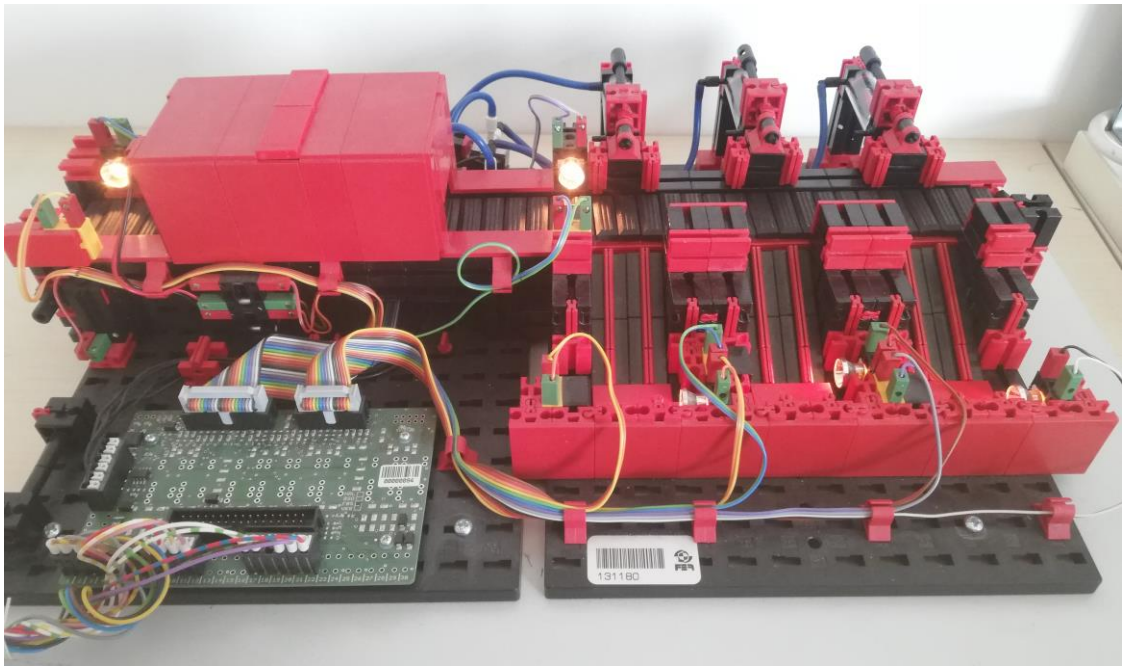
Nakon prikaza implementiranog postava, slijedi slika 4.2 kojom je dan prikaz mrežne topologije eksperimentalnog postava s prikazanim IP (engl. *Internet Protocol*) adresama. Na slici 4.2, vidljivo je da je model postrojenja povezan s programirljivim logičkim kontrolerom koristeći fizičko ožičenje, dok su PLC, radna stanica i upravljivi industrijski preklopnik povezani Ethernet kablom. Općenito, uporaba Ethernet tehnologije u industriji (engl. *Industrial Ethernet*) postala je praksa [2], uz mogućnost korištenja niza industrijskih komunikacijskih protokola kao što su Profinet [18], S7Comm [19], EtherCAT [20], EthernetIP [21], Modbus TCP [22] te mnogi drugi. Unutar ovog rada, odabrani protokol za ostvarivanje komunikacije između PLC-a i HMI-ja jest protokol S7CommPlus koji dolazi iz obitelji komunikacijskih protokola S7 Communication proizvođača Siemens. Protokol S7CommPlus standardno se koristi za povezivanje HMI panela i PLC-ova S7-1200/1500 koje proizvodi tvrtka Siemens [23]. Osnovna razlika između protokola S7Comm i S7CommPlus jest povećanje sigurnosnih mogućnosti (enkripcija, onemogućavanje napada ponavljanja i slično) [23]. Više o samoj analizi mrežnog prometa i protokola u nastavku rada.



Slika 4.2 Prikaz mrežne topologije implementiranog eksperimentalnog postava

4.1. Model linije za sortiranje

Model automatizirane linije za sortiranje izradaka prema boji uzorka predstavlja odabrani primjer industrijskog procesa pomoću kojeg je razvijen eksperimentalni industrijski upravljački sustav. Slikom 4.3 dan je prikaz modela linije za sortiranje. Sam model industrijskog procesa odabran je zbog jednostavnosti implementacije upravljačkog programa pomoću PLC-a – fokus ovog rada nije na zahtjevnosti implementacije upravljačkog algoritma, već na razvoju svijesti o kibernetičkoj sigurnosti u industriji postrojenja i procesa.

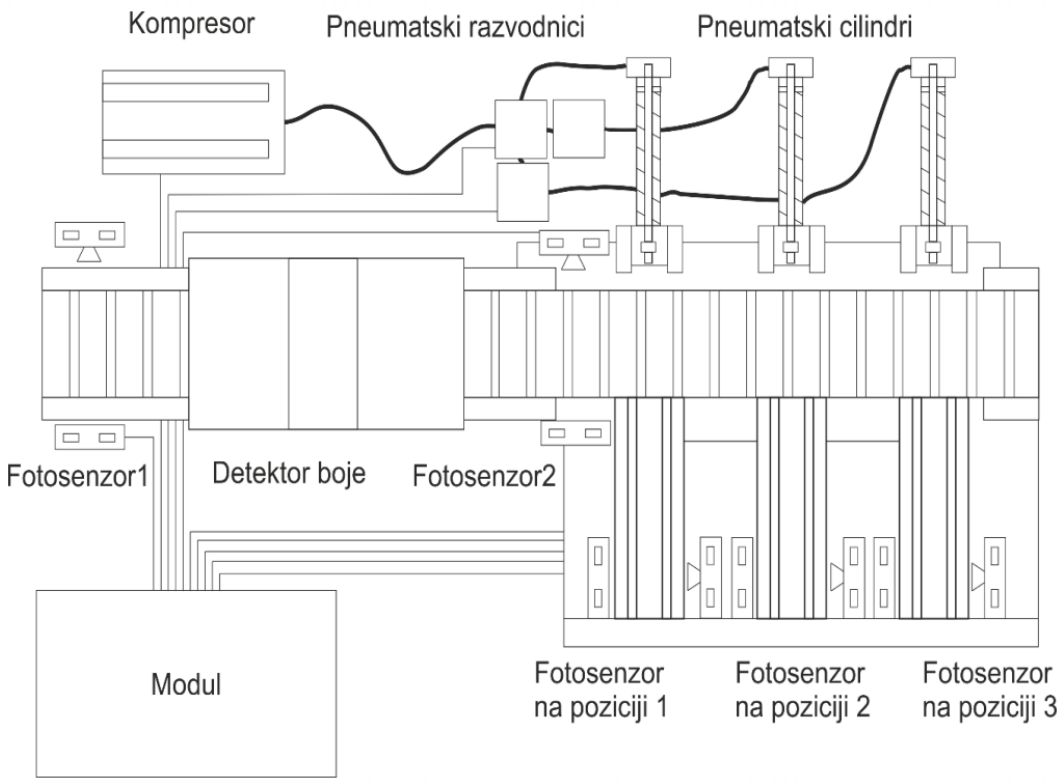


Slika 4.3 Prikaz modela linije za sortiranje

Nakon slike kojom je dan izgled modela sortirnice, slijedi slika 4.4 kojom je dan prikaz topologije modela linije za sortiranje. Gledajući sliku, vidljivo je da se model sastoji od pokretne trake kojom se omogućuje gibanje izradaka, inkrementalnog davača položaja kojim je moguće odrediti trenutni položaj izradaka, optičkih senzora na ulazu i izlazu u komoru unutar koje se nalazi analogni senzor boje izradaka, pneumatskog sustava – kompresora, jednoradnih pneumatskih cilindara za izbacivanje izradaka u ovisnosti o boji te u konačnici 3/1 pneumatskih razvodnika kao aktuatora cilindara. Unutar spremišta nalaze se optički senzori za detektiranje položaja izbačenih izradaka.

Analogni senzor za detekciju boje izradaka radi na principu loma svjetlosti. Senzor unutar sebe sadrži izvor svjetlosti kojom obasjava izradak te u ovisnosti o reflektiranoj svjetlosti daje analognu vrijednost naponskog signala u rasponu od 0-10 volti.

Analogni senzor boje, kao i ostali analogni te digitalni signali priključeni su na programirljivi logički kontroler putem ulazno/izlaznog modula.



Slika 4.4 Prikaz topologije linije za sortiranje [Interni dokument FER-a]

4.2. Programirljivi logički kontroler S7-1516-3 PN/DP

Programirljivi logički kontroler prema literaturi predstavlja „*upravljački sustav koji koristi programirljivu memoriju za pohranjivanje naredbi kojim je moguća implementacija specifičnih funkcija kao što su: aritmetičke operacije, komunikacija, obrada podataka, brojanje, upravljanje ulaznim i izlaznim vrijednostima te implementacija upravljačkih algoritama*“ [24]. Kao što je navedeno, automatizacija modela linije za sortiranje provodi se upotrebom programirljivog logičkog kontrolera S7-1516-3 PN/DP proizvođača Siemens. Odabir PLC-a za implementaciju eksperimentalnog postava za ispitivanje kibernetičke sigurnosti temeljen je na dostupnosti navedenog uređaja unutar laboratorija te značajnoj količini detektiranih ranjivosti [25]. Upravljački algoritam napravljen je upotrebom alata TIA Portal v15.1 (engl. *Totally Integrated Automation Portal* – TIA Portal) pomoću programskog jezika ljestvičasti dijagram (engl. *Ladder Diagram* – LAD). Ljestvičasti dijagram jedan je od programskih jezika za izradu upravljačkih algoritama PLC-ova definiranih unutar norme IEC 61131-3 [26], a prednost implementacije programskih rješenja pomoću jezika definiranih unutar norme jest mogućnost reprogramiranja te implementacije PLC-a nekog drugog proizvođača jednakim programskim rješenjem [26]. Slikom 4.5 dan je prikaz korištenog PLC-a. Gledajući sliku s lijeva na desno, vidljivo je da se PLC sastoji od modula napajanja, procesorske jedinice, modula digitalnih ulaza i izlaza te modula analognih ulaza i izlaza.

Slika 4.5 Prikaz programirljivog logičkog kontrolera S7-1516-3 PN/DP

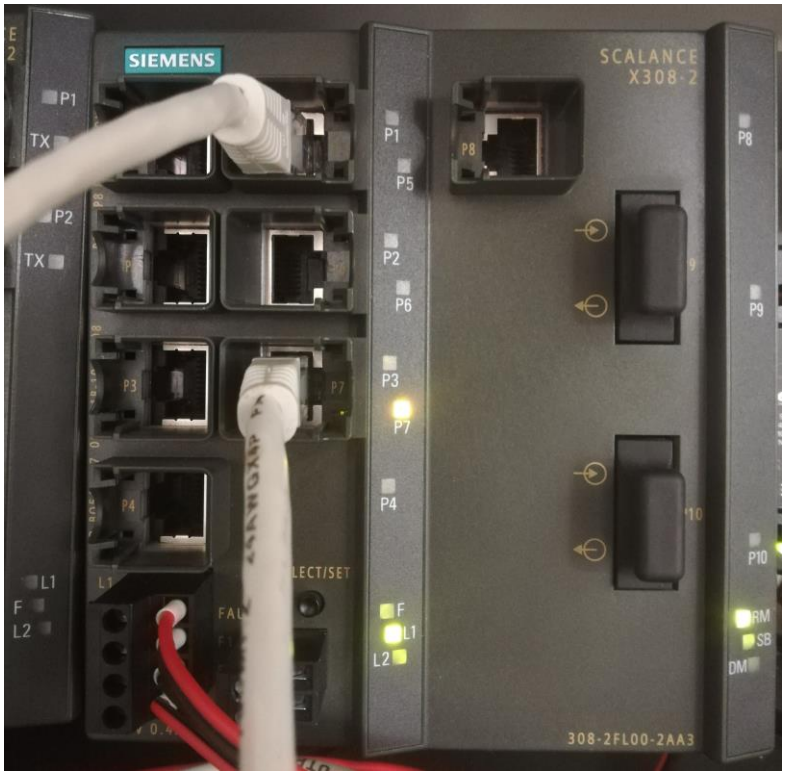
Nakon slike korištenog PLC-a, slijedi tablica 4.1 unutar koje je dan prikaz značajki korištenog PLC-a. Gledajući fizičke značajke, vidljivo je da je korišteni PLC otporniji na ekstremne temperature u odnosu na standardnu opremu koja se ugrađuje u računalne sustave. Razlog tomu leži u činjenici da se oprema u industriji automatizacije postrojenja i procesa projektira i certificira prema zahtjevima koje je moguće očekivati u industrijskim postrojenjima – povećana razina vlage, veći raspon radne temperature, prašina i prljavština te slično. Također, gledajući sigurnosne značajke PLC-a vidljivo je da postoji niz značajki koje je moguće podesiti u svrhu povećanja sigurnosti sustava, ali autori [2] tvrde da se navedene značajke standardno deaktiviraju zbog jednostavnijeg održavanja sustava te uspostave komunikacije između uređaja.

Tablica 4.1 Značajke PLC-a S7-1516-3 PN/DP

Vrste značajki	**Opis**	
Fizičke značajke	Serijski broj: 6ES7 516-3AN00-0AB0 Serijski broj modula digitalnih ulaza/izlaza: 6ES7 521/2-1BL00-0AB0 Serijski broj modula analognih ulaza: 6ES7 531-7KF00-0AB0 Serijski broj modula analognih izlaza: 6ES7 532-5HD00-0AB0 • Maksimalna radna temp: - Horiz. instalacija 60°C - Vert. instalacija 40°C	• Minimalna radna temp: - Horiz. instalacija 0°C - Vert. instalacija 0°C • Dimenzije: - Širina 70 mm - Visina 147 mm - Dubina 129 mm • Težina 845 g •RJ45 komunikacijsko sučelje (100 Mbps); integrirani preklopnik s 2 priključka •RS485 komunikacijsko sučelje (Serijska komunikacija, 12Mbps); •Napon napajanja: 24 V
Komunikacijske značajke	• Podržani Ethernet protokoli - TCP/IP - ISO on TCP - UDP - DHCP - SNMP - DCP - LLDP	• Podržana izokrona komunikacija kod posebnih primjena • S7 Comm • S7 CommPlus • Profinet • Modbus TCP •OPC UA • Mrežni poslužitelj: - HTTP -HTTPS
Sigurnosne značajke	• Zaštita od neovlaštenog pristupa -Zaštita pristupa ekranu zaporkom - Zaštita od čitanja /zapisivanja programa	- Kompletna zaštita od pristupa bez autorizacije - Zaštita od kopiranja programa - Zaštita izmjene programa

4.3. Upravljivi preklopnik SCALANCE X308-2

Industrijski upravljivi preklopnik predstavlja jednu od mrežnih komponenti koja se često koristi unutar industrijskih upravljačkih sustava. Općenito, preklopnici služe za povezivanje uređaja unutar komunikacijske mreže temeljene na Ethernet tehnologiji [2]. Razlika između neupravljivih i upravljivih preklopnika jest povećanje mogućnosti unutar komunikacijske mreže – ovisno o upravljivom preklopniku, moguće je zrcaliti komunikacijski promet na određeni mrežni priključak te ga analizirati koristeći odabrane alate, zatim upravljati postavkama mreže u ovisnosti o različitim mogućim mrežnim topologijama komunikacijskog sustava, upravljati sigurnosnim postavkama sustava i slično [2]. Razlika između industrijskih upravljivih preklopnika te standardnih IT preklopnika temelji se na povećanju fizičke otpornosti opreme prema očekivanoj grubosti radnih uvjeta unutar industrije automatizacije postrojenja i procesa. Unutar ovog istraživačkog rada, koristi se industrijski upravljivi preklopnik SCALANCE X308-2 proizvođača Siemens. Odabir preklopnika temelji se kao i kod odabira PLC-a na dostupnosti opreme unutar istraživačkog laboratorija, ali i znatnim mogućnostima preklopnika vezanih uz kibernetičku sigurnost [27]. Slikom 4.6 dan je prikaz korištenog industrijskog upravljačkog preklopnika.



Slika 4.6 Prikaz industrijskog upravljivog preklopnika SCALANCE X308-2

Nakon pregleda osnovnih informacija o korištenom preklopniku, slijedi tablica 4.2 unutar koje je dan prikaz značajki preklopnika SCALANCE X308-2. Sigurnosne značajke upravljivog preklopnika od posebnog su značaja za ovaj rad te će se detaljnije istraživati u nastavku. Unutar prvog dijela ovog rada, upravljivi preklopnik neće se podešavati. Razlog tomu leži u zahtjevu za što kvalitetnijom simulacijom stanja stvarnih industrijskih upravljačkih sustava kod kojih se značajke za povećanje kibernetičke sigurnosti sustava najčešće ne podešavaju [2]. Nakon provedbe analize sigurnosti razvijenog eksperimentalnog sustava, provest će se odabrani kibernetski napadi prije i nakon podešavanja mogućih značajki za povećanje kibernetičke sigurnosti. Provođenjem napada uz dvije različite konfiguracije preklopnika moguće je verificirati te ispitati implementirane metode za povećanje sigurnosti eksperimentalnog postava.

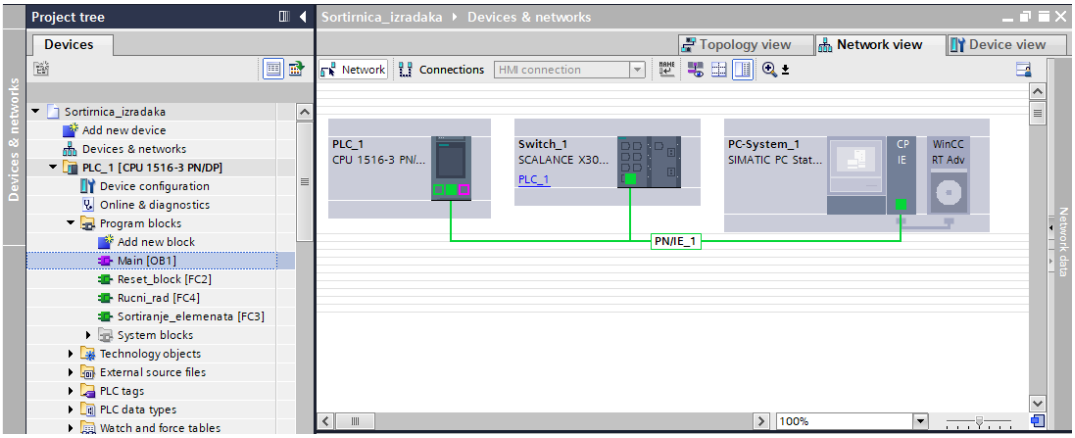
Tablica 4.2 Značajke industrijskog upravljivog preklopnika SCALANCE X308-2

Vrste značajki	**Opis**	
Fizičke značajke	Serijski broj: 6ES7 308-2FL00-2AA3 • Dimenzije: - Širina 120 mm - Visina 125 mm - Dubina 123 mm • Težina 1400 g • Stupanj zaštite IP 30 • DIN šina • Maksimalna vlažnost:95%	• Maksimalna radna temperatura: - Vert. instalacija 60ºC • Minimalna radna temperatura: - Vert. instalacija -10ºC • Maksimalna vlažnost: <95% •7 x RJ45 komunikacijskih priključaka(10/100 Mbps); •1 x RJ45 komunikacijski priključak(10/100/1000 Mbps); •2 x SC Duplex komunikacijski priključak (1000 Mbps) •Napon napajanja: 24 V
Komunikacijske značajke	• Podržani protokoli za pristup upravljačkom sučelju: - HTTP - HTTPS - Telnet - SSH - FTP - LLDP - RADIUS Maksimalan broj naučenih adresa: 8000	• Podržana izokrona komunikacija kod posebnih primjena • Podržane mrežne topologije: - Linearna topologija - Topologija zvijezde - Topologija stabla - Topologija prstena • Mrežni poslužitelj: - HTTP -HTTPS • Dijagnostika Ethernet priključaka i kablova
Sigurnosne značajke	• Podrška VLAN-a • Podrška MAC ACL tablica • Podešavanje QoS svojstava komunikacijske mreže • Zrcaljenje priključaka	• Kompletna zaštita od pristupa bez autorizacije • Mogućnost deaktivacije nekorištenih mrežnih priključaka • SSH te HTTPS pristup mrežnom sučelju • Statistike o komunikacijskim podatcima • Ograničavanje broadcast/unicast slanja podataka

4.4. Implementacija upravljačkog algoritma modela

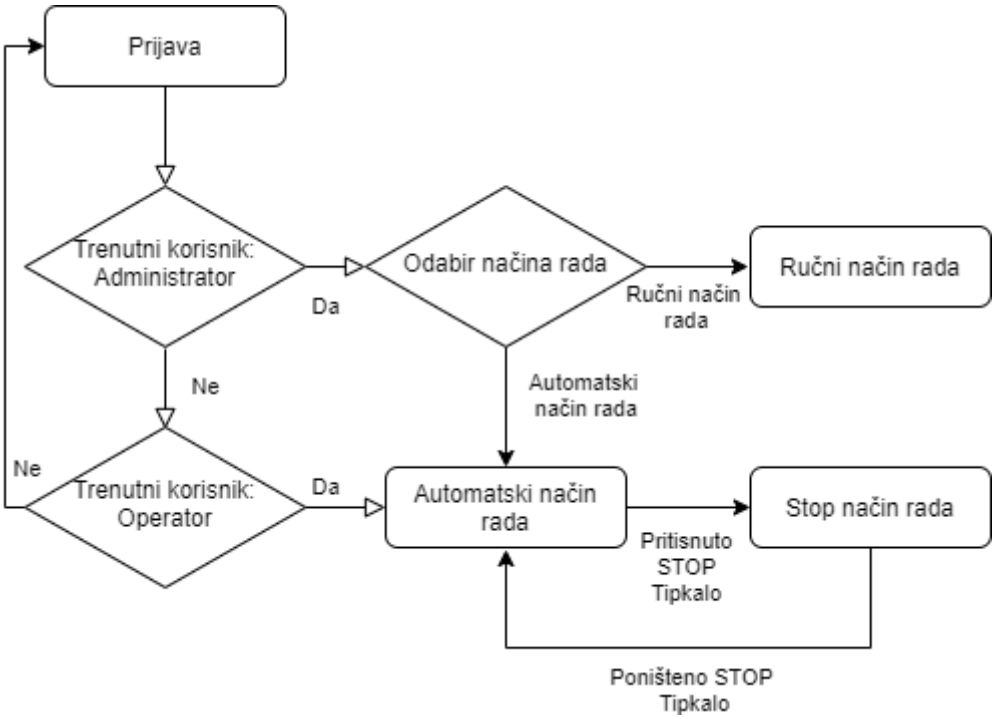
Kao što je navedeno, upravljački algoritam modela linije za sortiranje implementiran je koristeći alat TIA Portal v15.1 te programski jezik LAD. Alat TIA Portal v15.1 predstavlja platformu za izradu upravljačkih algoritama sustava automatizacije, vizualizacijskih sučelja procesa (HMI) i slično [28]. Slikom 4.7 dan je prikaz projektnog stabla napravljenog rješenja za automatizaciju postrojenja te mrežnog dijagrama procesa. Gledajući sliku, vidljivo je da se mrežni dijagram unutar programa sastoji od jednakih komponenti kao i dijagram dan slikom 4.2, dok se mrežno stablo sastoji od tri funkcije (engl. *Function* – FC) te jednog organizacijskog bloka (engl. *Organization Block* – OB) čiji opis slijedi u nastavku:

- Organizacijski blok *Main* [OB1] – Blok čiji se programski kod izvršava ciklički svakih 100 milisekundi. Unutar bloka OB1 pozivaju se funkcije FC2 (*Reset_block*), FC3 (*Sortiranje_elemenata*) te FC4(*Rucni_rad*) u ovisnosti o procesnim uvjetima danim u nastavku teksta.
- Funkcija *Reset_block* [FC2] – Funkcija unutar koje se izvršava resetiranje svih internih vrijednosti odnosno zaustavljanje procesa sortiranja u slučaju pritiska pripadajućih tipki na razvijenom HMI sučelju.
- Funkcija *Sortiranje_elemenata* [FC3] – Funkcija unutar koje se izvodi upravljački algoritam sortiranja izradaka po boji u slučaju aktivnog automatskog režima rada.
- Funkcija *Rucni_rad* [FC4] – Funkcija unutar koje se provodi upravljački algoritam u slučaju aktivnosti ručnog režima rada.



Slika 4.7 Prikaz programskog stabla unutar alata TIA Portal

Slikom 4.8 dan je prikaz dijagrama toka upravljačkog sustava modela za sortiranje izradaka. Gledajući sliku, vidljivo je da je potrebna prijava u sustav u slučaju želje za interakcijom sa sustavom. Samo HMI sučelje prihvaća dva korisnika – korisnika naziva *Administrator* koji ima pristup ručnom i automatskom načinu rada te korisnika *Operator* koji može upravljati linijom za sortiranje isključivo u automatskom načinu rada. Unutar ručnog načina rada moguće je pomicati traku, uključiti odnosno isključiti kompresor te upravljati položajem cilindara pomoću ventila. Unutar automatskog načina rada, moguće je započeti proces sortiranja izradaka, nadzirati stanje unutar sustava – boju posljednjeg sortiranog izratka, broj plavih, bijelih i zelenih izradaka te u konačnici resetirati brojače i zaustaviti proces sortiranja u slučaju sigurnosne ugroze sustava. Više o samim mogućnostima HMI sučelja za upravljanje i nadzor procesa u nastavku rada.



Slika 4.8 Dijagram toka upravljačkog algoritma modela linije za sortiranje

4.5. Implementacija HMI sučelja za upravljanje i nadzor modelom linije za sortiranje

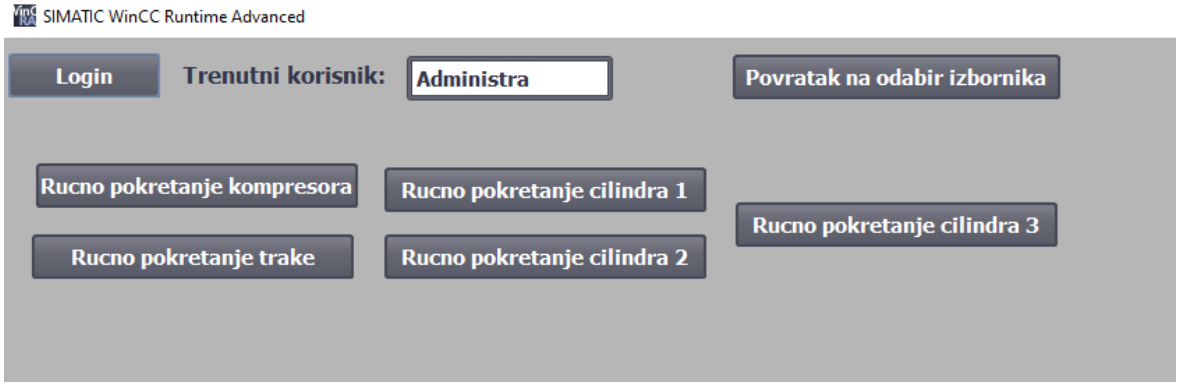
HMI sučelje za upravljanje i nadzor eksperimentalnim postavom napravljeno je koristeći alat WinCC unutar platforme TIA Portal v15.1. Alat WinCC predstavlja alat za izradu HMI sučelja za upravljačke panele proizvođača Siemens [28]. Unutar ovog rada, upravljački HMI panel simulira se na radnoj stanici koja unutar sebe sadrži platformu TIA Portal v15.1 te alat WinCC RT Advanced. Unutar radne stanice simulira se HMI sučelje koje se sastoji od tri različita zaslona:

- Zaslon naziva *Odabir_rada* – Zaslon koji je unutar projekta definiran kao početni zaslon, a unutar njega moguća je autorizacija korisnika te odabir načina rada.
- Zaslon naziva *Automatski* – Zaslon unutar kojeg je napravljeno sučelje za nadzor i upravljanje modelom linije za sortiranje u slučaju odabira automatskog načina rada.
- Zaslon naziva *Rucni* – Zaslon unutar kojeg je napravljeno sučelje za upravljanje modelom linije za sortiranje u slučaju odabira ručnog načina rada.

Slikom 4.9 dan je prikaz zaslona naziva *Odabir_rada*. Gledajući sliku, vidljivo je da se unutar zaslona nalazi prikaz trenutno autoriziranog korisnika te tipka *Login* kojom se otvara prozor za prijavu. Nakon autorizacije, u ovisnosti o trenutno autoriziranom korisniku moguć je odabir između automatskog i ručnog načina rada. U prikazanom primjeru, trenutni korisnik jest *Operator* koji ima moguć pristup isključivo automatskom načinu rada.

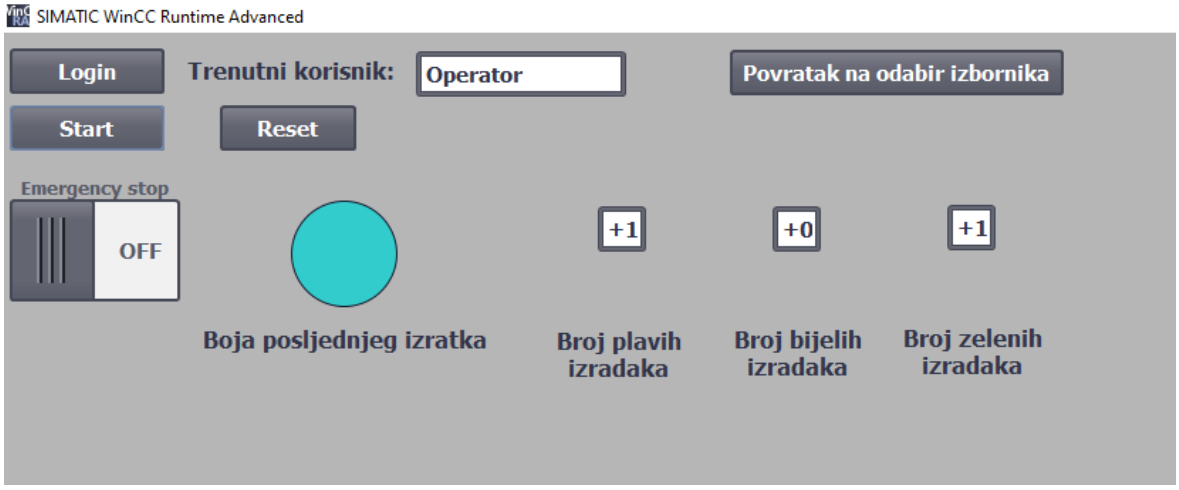
Slika 4.9 Prikaz zaslona naziva *Odabir rada*

U slučaju da je trenutno autorizirani korisnik *Administrator*, pritiskom na tipku *Rucni* otvara se zaslon naziva *Rucni* koji je dan slikom 4.10. Gledajući sliku, vidljivo je da korisnik (*Administrator*) može ručno pokrenuti kompresor, traku te pneumatske cilindre (jasno, uz uključen kompresor). U desnom gornjem dijelu zaslona nalazi se tipka za povratak na odabir izbornika.



Slika 4.10 Prikaz zaslona naziva *Rucni*

I na kraju, slikom 4.11 dan je prikaz zaslona naziva *Automatski*. Gledajući sliku, vidljivo je da je pritiskom na tipku *Start* moguće pokrenuti automatski sustav za sortiranje izradaka, pritiskom na tipku *Emergency Stop* zaustaviti proces sortiranja te tipku *Reset* kojom se resetiraju brojači izradaka. Osim naredbi za upravljanje, unutar zaslona nalaze se brojači plavih, bijelih i zelenih izradaka te indikator boje posljednjeg sortiranog izratka. Kao i kod prethodnih zaslona, u gornjem dijelu zaslona nalaze se podatci vezani uz trenutno autoriziranog korisnika te tipka za povratak na odabir izbornika.



Slika 4.11 Prikaz zaslona naziva *Automatski*

Nakon pregleda implementacije modela IACS-a za sortiranje, slijedi provedba istraživanja kibernetičke sigurnosti razvijenog eksperimentalnog postava te pripadajuće opreme.

5. Istraživanje kibernetičke sigurnosti razvijenog sustava

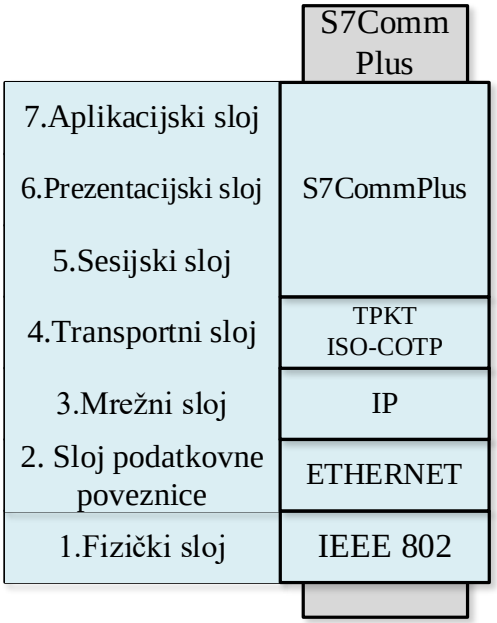
U nastavku poglavlja slijedi analiza industrijskog komunikacijskog protokola S7CommPlus te pregled provedbe odabranih kibernetičkih napada na razvijeni eksperimentalni postav. Tako je kao jedan od mogućih napadačkih scenarija odabran slučaj u kojem se napadač priključuje na neki od slobodnih mrežnih priključaka industrijskog upravljivog preklopnika SCALANCE. U slučaju takvog napadačkog scenarija, napadač ima mogućnost provedbe niza kibernetičkih napada – napadi s ciljem prikupljanja i krađe informacija (engl. *Reconnaissance*), napadi uskraćenja usluge (engl. *Denial of Service* – DOS) te napadi na industrijski komunikacijski protokol unutar mreže [29]. Jasno, uspješnost provedbe navedenih napada ovisi o sposobnosti i motivaciji napadača, ali i o implementiranim sigurnosnim zaštitama unutar sustava. Unutar ovog rada, provest će se odabrani napadi iz prethodno navedenih kategorija.

5.1. Industrijski komunikacijski protokol S7CommPlus

Industrijski komunikacijski protokol S7CommPlus predstavlja unaprijeđenu inačicu protokola S7Comm proizvođača Siemens [30]. U osnovi, S7 uređaji proizvođača Siemens podržavaju niz komunikacijskih protokola, ali se općenito dijele na protokole vezane uz Profinet i protokole iz obitelji S7 Communication. Uz navedenu podjelu, autor [30] tvrdi da su protokoli S7 Communication znatno manje dokumentirani u odnosu na protokole vezane uz Profinet, što se pokazalo i u analizi vezanoj uz ovaj rad. Sam protokol S7CommPlus se kod PLC-a S7-1500 koristi za:

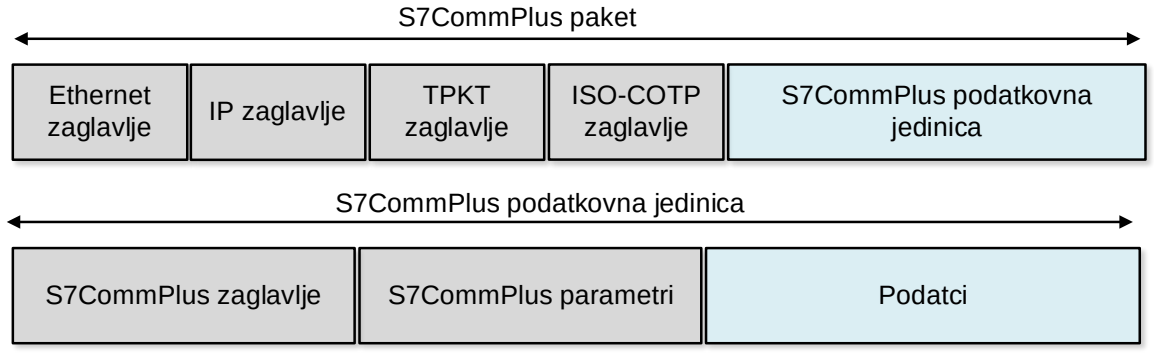
- podešavanje opreme putem alata TIA portal – Mijenjanje načina rada iz START u STOP i obrnuto, prebacivanje programa na PLC s računala i obrnuto, dobivanje dijagnostičkih podataka te podataka vezanih uz alarme,
- razmjenu podataka između PLC-ova S7-1500 te HMI/SCADA sučelja.

Osnovna razlika u odnosu na protokol S7Comm jest implementacija sigurnosnih zaštita vezanih uz onemogućavanje napada ponavljanja (engl. *Replay Attacks*) kod kojih napadač ponavlja promet na industrijskoj komunikacijskoj mreži te enkripcija podatkovnog dijela S7CommPlus paketa [26]. Slikom 5.1 dan je prikaz raspodjele protokola prema OSI (engl. *Open Systems Interconnection* – OSI) modelu [31].



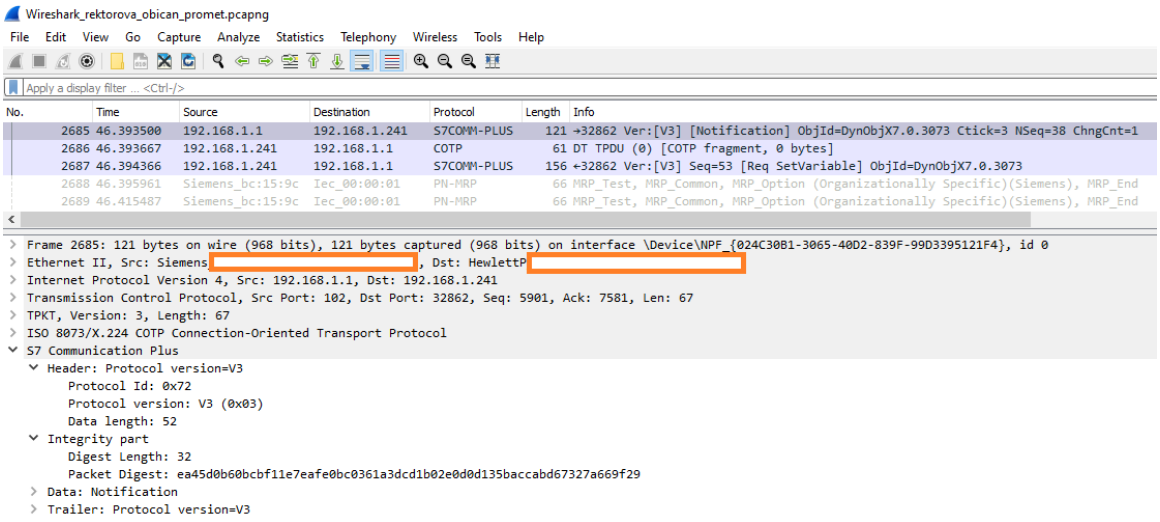
Slika 5.1 Prikaz raspodjele komunikacijskog protokola S7CommPlus prema OSI referentnom modelu

Na slici 5.1, vidljivo je da se za tri najviša apstrakcijska sloja OSI modela koristi S7CommPlus, unutar transportnog sloja koriste se protokol TPKT [32] (engl. *OSI Transport Service on top of the TCP* - TPKT) te protokol COTP [33] (engl. *Connection Oriented Transport Protocol* – COTP, poznat i pod nazivom ISO 8073). Oba navedena protokola služe za omogućavanje prijenosa niza podataka (engl. *Stream*) emulacijom protokola TCP (engl. *Transmission Control Protocol* – TCP). Nakon transportnog sloja, slijedi mrežni sloj kod kojeg S7CommPlus koristi mrežni protokol (IP) za prijenos podataka, dok se kod posljednja dva sloja koriste protokoli vezani uz Ethernet. Nakon pregleda slojeva OSI modela, slijedi pregled strukture komunikacijskih poruka kod protokola S7CommPlus danog slikom 5.2. Na slici 5.2, jasno je vidljivo da se S7CommPlus komunikacijski paket sastoji od Ethernet zaglavlja (sloj 2. OSI modela), IP zaglavlja (sloj 3. OSI modela), TPKT te ISO-COTP zaglavlja (sloj 4. OSI modela) te S7CommPlus podatkovne jedinice (PDU). Unutar S7CommPlus podatkovne jedinice nalazi se S7CommPlus zaglavlje unutar kojeg se nalaze informacije o protokolu i inačici – protokol S7CommPlus ima oznaku 0x72 u odnosu na protokol S7Comm čija je oznaka 0x32. Nakon zaglavlja slijedi dio podatkovne jedinice s parametrima unutar kojeg se nalaze podatci o provjeri integriteta poruke (dio koji onemogućuje napade ponavljanja). U konačnici slijedi dio s podatcima koji je zbog nedostatka izvora literature iznimno zahtjevno sintaksno analizirati te se iz tog razloga neće opisivati. Kako navodi autor u izvoru [30], implementacija simulacije ovog protokola zahtijevala bi poznavanje dijeljenih ključeva (engl. *Shared key*) koji su sadržani unutar koda PLC-a, a jedini način za dobivanje takvih informacija jest razbijanje i rastavljanje postojećeg koda koje je zakonski zabranjeno. Također, bitno je navesti da je za komunikaciju koristeći protokol S7CommPlus definiran priključak (engl. *Port*) 102.



Slika 5.2 Struktura komunikacijskih poruka kod industrijskog komunikacijskog protokola S7CommPlus

Nakon pregleda industrijskog komunikacijskog protokola S7CommPlus po slojevima, slijedi slika 5.3 kojom je dan prikaz razmjene podataka na mreži između PLC-a te HMI-ja. Praćenje podataka na mreži provedeno je koristeći alat Wireshark koji služi za analizu i praćenje prometa i protokola unutar neke komunikacijske mreže [34]. Alat Wireshark podržava niz industrijskih komunikacijskih protokola (Profinet, Ethernet/IP, Modbus TCP, S7Comm), ali protokol S7CommPlus standardno nije podržan zbog nepostojanja javno dostupnog opisa implementacije protokola. Slijedom navedenih okolnosti, unutar ovog rada korišten je analizator protokola S7CommPlus autora [35] čiju je implementaciju moguće ugraditi u alat Wireshark. Jasno, autor analizatora navodi da postoje ograničenja vezana uz samu implementaciju analizatora zbog ograničenosti literature, ali u kontekstu ovog rada čak i uz navedena ograničenja analizator služi svrsi. Gledajući sliku, vidljivo je da alat Wireshark prepoznaje komunikaciju između PLC-a te HMI-ja putem protokola S7CommPlus, ali zbog enkripcije podataka nije moguće odrediti koji se podatci razmjenjuju na mreži.



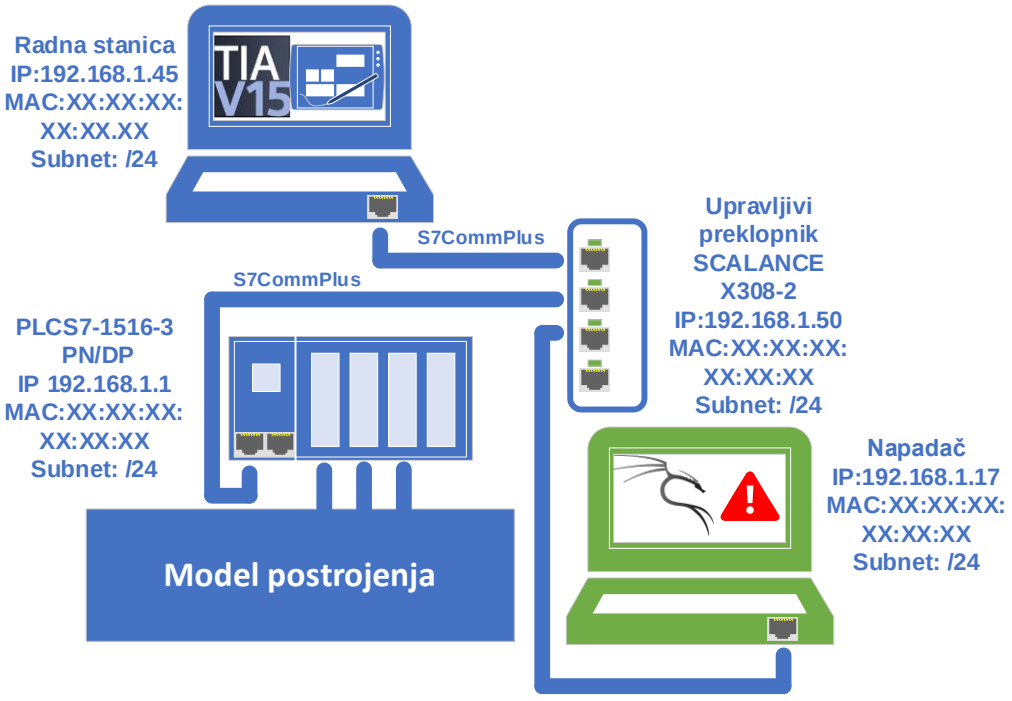
Slika 5.3 Prikaz razmjene podataka unutar industrijske komunikacijske mreže implementiranog eksperimentalnog postava

Nakon prikaza prometa na mreži, slijedi osvrt na sigurnost protokola S7CommPlus. Posebno zanimljiv rad [23] vezan uz kibernetičke napade na protokol S7CommPlus daje informacije o mogućoj krađi sesije između alata TIA portal te proizvoljnog PLC-a na mreži putem ponavljanja S7-ACK paketa. Bez obzira na postojeće radove, u nastavku ovog rada neće biti provođeni napadi na protokol S7CommPlus zbog zakonske osjetljivosti teme, već isključivo napadi u svrhu prikupljanja informacija te napadi uskraćivanja usluge.

5.2. Napad u svrhu prikupljanja informacija

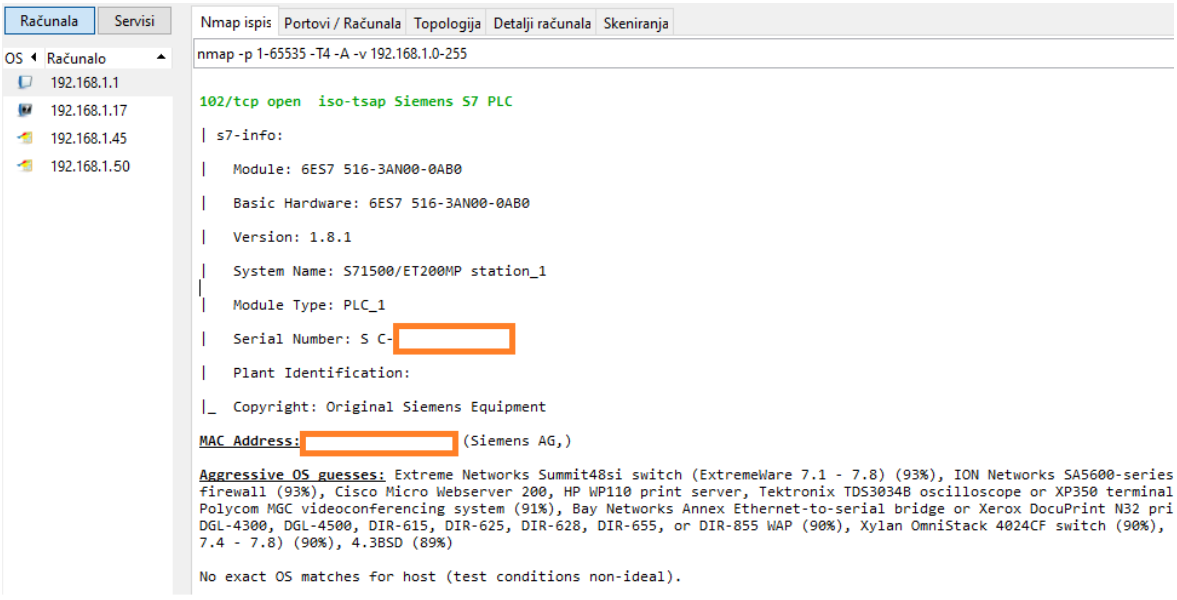
Kao što je navedeno, za provedbu sljedećih napada odabran je napadački scenarij u kojem se napadač priključuje na neki od slobodnih mrežnih priključaka industrijskog upravljivog preklopnika SCALANCE. Također, pretpostavljeno je da napadač razumije ponašanje industrijskih postrojenja, ali i IT sustava. Napadi u svrhu prikupljanja informacija mogu biti razni [36], ali će se u ovom radu fokus postaviti na prikupljanje informacija o uređajima na mreži. Činjenica je da za svaki ozbiljniji kibernetički napad na industrijsku mrežu potrebno provesti neki oblik prikupljanja informacija o uređajima na mreži, inačicama firmvera i slično. Razlog za takvu praksu jest mogućnost pronalaska postojećih ranjivosti određenih komponenti unutar sustava u slučaju neažurnosti inačica softvera i firmvera.

Slikom 5.4 dan je prikaz mrežnog dijagrama IACS-a unutar kojeg je prikazan napadač. Napadač koristi operacijski sustav Windows 10 te virtualni operacijski sustav Kali Linux v2020.4 pomoću alata VMware. Operacijski sustav Kali Linux predstavlja operacijski sustav otvorenog tipa temeljenog na Debian Linux OS-u, a služi za provedbu niza radnji i analiza vezanih uz kibernetičku sigurnost [37]. Unutar sebe sadrži više od 600 različitih penetracijskih alata koji se koriste u ovisnosti o potrebi i zahtjevima analize.



Slika 5.4 Prikaz mrežnog dijagrama postrojenja uslijed odabranog scenarija kibernetičkog napada

Nakon priključenja na mrežu, napadač pokreće postupak detaljne analize komunikacijske mreže pomoću alata Nmap (engl. *Network Mapper* – Nmap). Alat Nmap predstavlja besplatni alat otvorenog tipa koji se koristi za nadzor i analizu uređaja na mreži [38]. Odabrani rezultati analize industrijske komunikacijske mreže dani su slikom 5.5. Na slici 5.5, vidljivo je da skeniranje mreže pomoću alata Nmap daje niz informacija o uređajima na mreži, dok je za demonstraciju specifično odabrana analiza informacija o uređaju s adresom 192.168.1.1. Tako je u primjeru dobivena informacija o vrsti modula te serijskom broju iz kojeg se da iščitati da je riječ o S7-1500 PLC-u. Također, identifikacijski postupak dao je informaciju o inačici firmvera PLC-a, serijskom broju te MAC adresi uređaja. Osim navedenih informacija, alat otkriva koji su sve priključci uređaja otvoreni. Nakon otkrivanja informacija o uređaju, napadač može proučiti javno dostupnu dokumentaciju [25] postojećih ranjivosti uređaja u ovisnosti o inačici firmvera te otvorenosti priključka te planirati daljnje tehnike i metode napada. Osim dokumentacije o ranjivostima uređaja, postoji javno dostupna baza podataka vezana uz ponašanje, tehnike i taktike napadača na industrijske upravljačke sustave naziva ATT&CK for ICS organizacije MITRE [39]. Tako je unutar ATT&CK for ICS baze podataka navedeno i razrađeno 12 različitih faza kibernetičkih napada (od inicijalnog pristupa pa sve do fizičkog utjecaja na IACS). Kod provedbe metoda i alata za povećanje kibernetičke sigurnosti sustava potrebno je voditi računa o mogućim napadačima, ranjivostima i tehnikama napada, a navedena dokumentacija može znatno pomoći zaposlenicima kojima je cilj obrana od kibernetičkih napada [2].



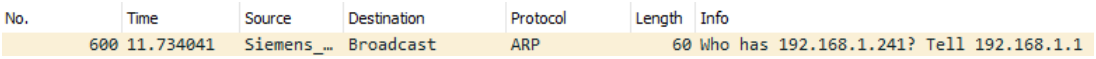
Slika 5.5 Prikaz dobivenih informacija o PLC-u uslijed skeniranja pomoću alata Nmap

5.3. Napad u svrhu onemogućavanja komunikacije između uređaja

Sljedeći odabrani napad na eksperimentalni postav za ispitivanje kibernetičke sigurnosti jest DoS napad. Općenito, DoS napade moguće je podijeliti na mnogo načina, a zajednička karakteristika im je zlouporaba neke od komponenti komunikacijskog sustava – komunikacijskog protokola, operacijskog sustava i slično, odnosno bilo kojeg resursa čijim se iscrpljivanjem narušava dostupnost informacija na mreži [36]. Za ovaj rad odabire se specifični slučaj u kojem napadač presreće komunikaciju između HMI-ja i PLC-a te odbacuje sve pakete na mreži. Onemogućavanjem komunikacije između PLC-a te HMI-ja potencijalno se narušava sigurnost cijelog IACS-a, posebno u slučaju kombinacije navedene metode s drugim oblicima kibernetičkih napada. Preuzimanje komunikacije (engl. *Communication Hijacking*) provodi se zlouporabom ranjivosti svojstvenih protokolu za razlučivanje adresa (engl. *Address Resolution Protocol* – ARP). Opis principa provođenja procesa preuzimanja komunikacije slijedi u nastavku. Postupak ARP trovanja (engl. ARP *Poisoning*; ARP *Spoofing*) predstavlja jednu od metoda za presretanje komunikacije između uređaja na mreži zloupotrebljavajući osnovni princip rada svake mreže temeljenoj na Ethernet tehnologiji.. Bitno je napomenuti da se u kontekstu Ethernet mreža misli na IPv4 komunikacijske mreže, dok se kod IPv6 komunikacijskih mreža koriste drugačiji principi za ostvarivanje komunikacije između uređaja. Svaki uređaj na mreži temeljenoj na Ethernet tehnologiji ima dvije adrese:

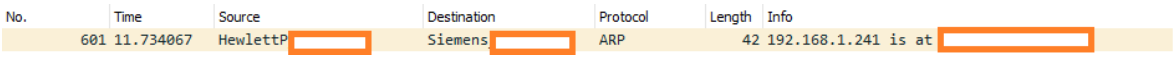
- MAC adresa (engl. *Media Access Control* – MAC) – Predstavlja identifikator veličine 48 bita koji služi za jedinstvenu identifikaciju svake mrežne kartice (engl. *Network Interface Card* – NIC) na drugom sloju OSI referentnog modela (sloj podatkovne poveznice). MAC adrese najčešće dodjeljuju proizvođači opreme.
- IP adresa – Predstavlja identifikator veličine 32 bita koji služi za jedinstvenu identifikaciju uređaja unutar neke komunikacijske mreže na trećem sloju OSI referentnog modela (mrežni sloj). Dio bitova IP adrese odnosi se na adresu mreže, dok se preostali bitovi odnose na adresu mrežnih uređaja. Logička segmentacija mreža izvodi se konceptom podmreža (engl. *Subnetwork*) pomoću kojeg se logičkom operacijom I može odrediti adresa uređaja unutar mreže kao i adresa same mreže. IP adrese dodjeljuju se od strane osoba koje su zadužene za održavanje samog mrežnog sustava unutar neke organizacije.

Kod komunikacije uređaja unutar neke komunikacijske mreže, standardno je da su uređajima poznate IP adrese uređaja s kojima imaju potrebu komunicirati, dok MAC adrese nisu. Kao rješenje za navedeni problem koristi se protokol mrežnog sloja naziva protokol za razlučivanje adresa (ARP) pomoću kojeg je moguće otkriti nepoznatu MAC adresu uređaja s poznatom IP adresom. Princip rada ARP protokola temelji se na odašiljanju paketa ARP zahtjeva (engl. *Broadcasting* ARP *request*) svim uređajima na mreži u obliku danom slikom 5.6.



Slika 5.6 Prikaz ARP zahtjeva uređaja na komunikacijskoj mreži

Svi ostali uređaji na mreži primaju navedenu poruku te u slučaju da se IP adresa unutar zahtjeva podudara s IP adresom uređaja koji je primio zahtjev, uređaj šalje ARP odgovor (engl. *ARP Response*) uređaju koji je odaslao ARP zahtjev. Prikaz ARP odgovora dan je slikom 5.7.



Slika 5.7 Prikaz ARP odgovora uređaja na mreži

U svrhu minimiziranja količine ARP zahtjeva koji se odašilju svim uređajima, uređaji na mreži unutar svoje memorije sadrže tablice povezanih MAC adresa s IP adresama. U slučaju povezivanja postojeće IP adrese unutar tablice s novom MAC adresom, postojeći zapis se briše i sprema se novi zapis. Navedeni mehanizam predstavlja osnovni princip rada ARP protokola [40].

Osnovni problem protokola ARP predstavlja nemogućnost autentifikacije uređaja na mreži (trenutno ne postoji mehanizam za potvrdu identiteta uređaja na mreži) [36]. ARP trovanje temelji se na stvaranju lažiranih ARP odgovora. Slanjem lažiranih ARP odgovora uređajima čiju komunikaciju napadač želi presresti, napadač izmjenjuje legitimne ARP tablice uređaja te povezuje IP adrese komunikacijskih partnera sa svojom MAC adresom.

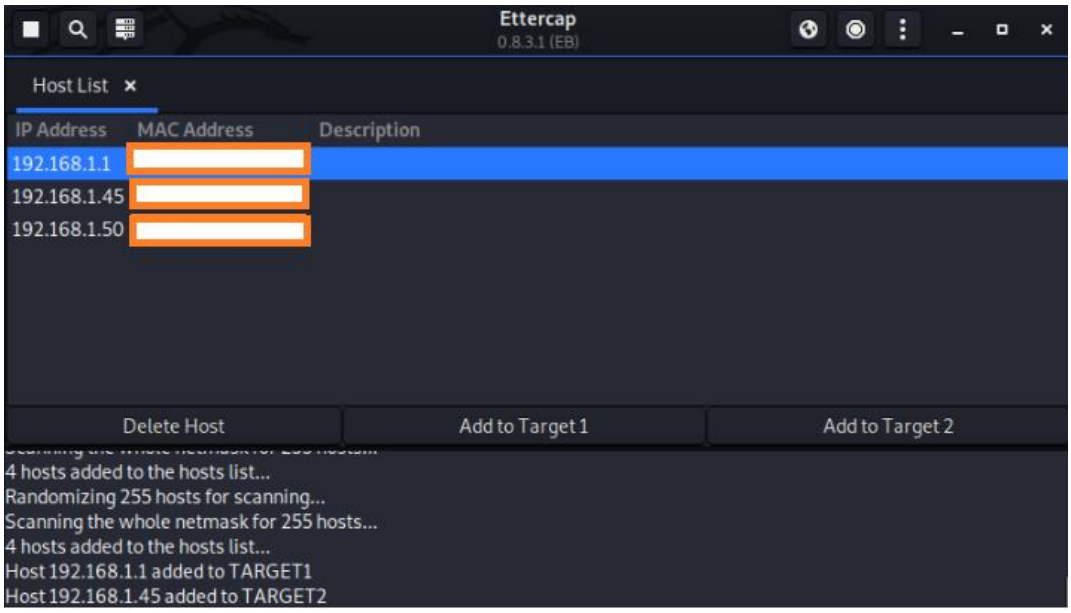
Nakon izmjene legitimnih ARP tablica (engl. *ARP poisoning*) napadač preuzima komunikacijski put i sva komunikacija između uređaja koji komuniciraju prelazi preko njega. ARP trovanje može biti podloga za više vrsta napada, od kojih su neki MiTM (engl. *Man in the Middle* – MITM) napadi, DOS napadi, praćenje komunikacijskog prometa i slično.

U osnovi, univerzalne zaštite od ARP trovanja kod mreža koje koriste IPv4 nema. Tako rad [36] predlaže kao jednu od mogućih metoda za zaštitu implementaciju statičkih ARP tablica unutar uređaja, ali nedostatak takvog rješenja jest nemogućnost automatskog podešavanja mreže u slučaju fizičke izmjene nekih komponenti kod održavanja te gubitak *plug and play* funkcionalnosti. Druga mogućnost jest implementacija upravljivih preklopnika (engl. *Managed Switch*) kod kojih je osim podešavanja statičkih ARP tablica moguće i povezivanje određenog priključka preklopnika s IP i MAC adresom uređaja. Više o prijedlogu metoda za povećanje sigurnosti sustava u nastavku rada.

Kod IPv6 tehnologije ARP protokol više nije podržan, već njegovu funkcionalnost preuzima protokol NDP (engl. *Neighbour Discovery Protocol* – NDP) koji omogućuje veće sigurnosne mogućnosti u usporedbi s ARP protokolom, onemogućujući ARP trovanje.

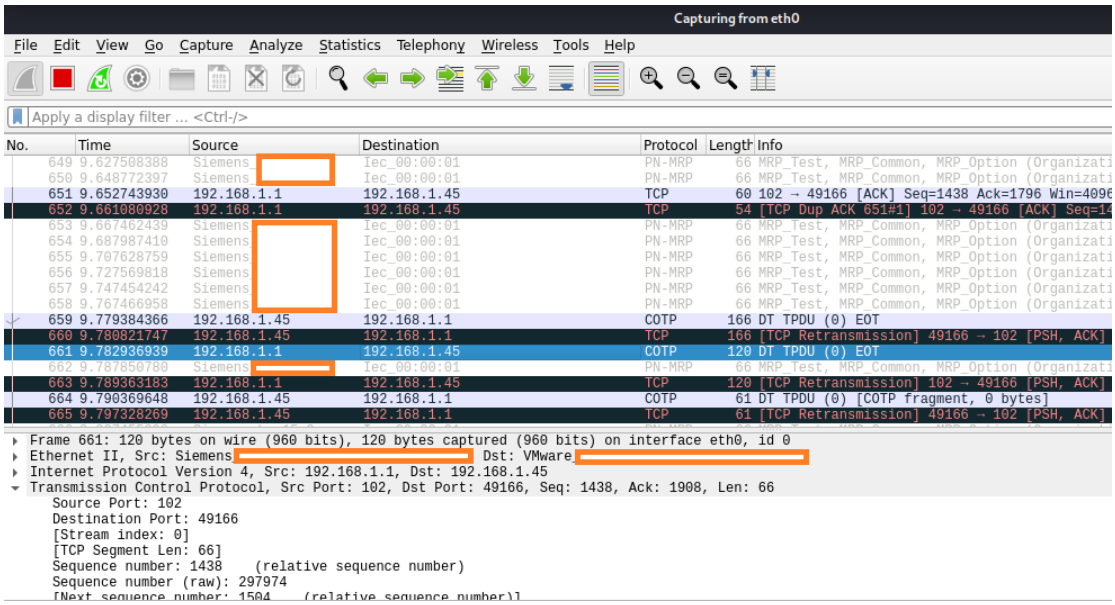
Nakon pregleda teorijske podloge o odabranom napadu uskraćivanja usluge, slijedi pregled provedbe napada. Kao što je navedeno, napadač je priključen na industrijsku komunikacijsku mrežu te koristi operacijski sustav Kali Linux v2020.4. Unutar operacijskog sustava Kali Linux postoji alat naziva Ettercap pomoću kojeg je moguća jednostavna implementacija i provedba određenih MITM odnosno DoS napada [33].

Slikom 5.8 dan je prikaz sučelja alata Ettercap nakon provedbe postupka ARP trovanja. Bez detaljnog objašnjavanja postupka, vidljivo je da su PLC te HMI dodani kao žrtve postupka.



Slika 5.8 Prikaz sučelja alata Ettercap

Provedbom postupka ARP trovanja, sav komunikacijski promet između PLC-a te HMI- ja prolazi preko napadačkog računala. Slikom 5.9 dan je prikaz potvrde navedene tvrdnje analizom mrežnog prometa pomoću alata Wireshark na napadačkom računalu.



Slika 5.9 Prikaz komunikacije između uređaja nakon provedbe postupka ARP trovanja

Implementacijom posebno razvijenog Ettercap filtra pomoću kojeg se odbacuju svi komunikacijski paketi između uređaja, komunikacija između HMI-ja i PLC-a se prekida. Tablicom 5.1 dan je prikaz metrike za određivanje ponašanja sustava u trenutcima provođenja kibernetičkog napada prema radu [19].

Gledajući tablicu, jasno je vidljivo da provedeni napad direktno utječe na vrijeme odgovora procesa (time i na upravljivost), dok ostale kategorije pokazuju zadovoljavajuće ponašanje (u ovisnosti o trenutnom načinu rada).

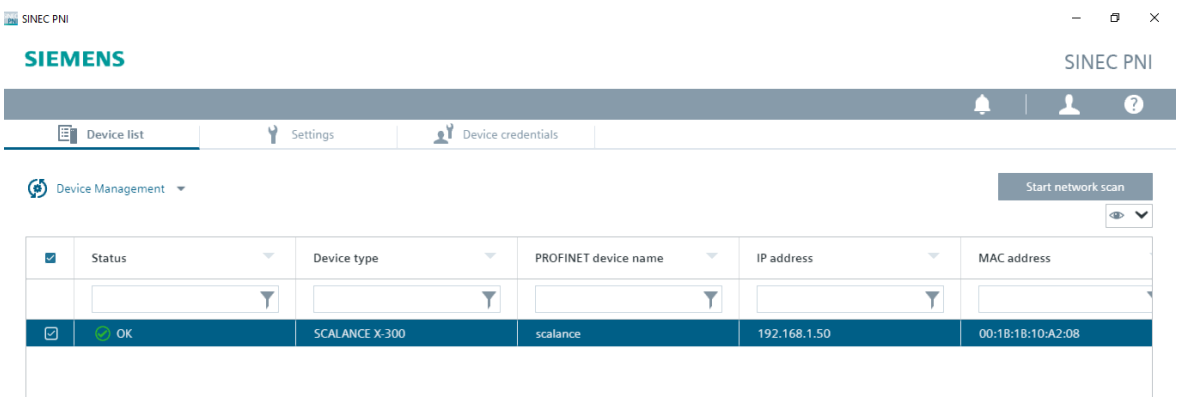
Tablica 5.1 Metrika za određivanje ponašanja sustava za vrijeme provođenja napada odabranog napada u svrhu onemogućavanja komunikacije

Mjera	Opis
Kvaliteta izratka	Zadovoljavajuća – u slučaju da je PLC ostao u automatskom načinu rada prije provedbe napada, sortirnica bi i dalje ispravno sortirala izratke.
Stopa izradaka s manom	Zadovoljavajuća – broj pogrešno sortiranih izradaka ostaje konstantan.
Broj izradaka s manom po jedinici mjere	Zadovoljavajuć – broj pogrešno sortiranih izradaka ostaje konstantan.
Vrijeme odgovora procesa	Beskonačno – komunikacija između HMI-ja te PLC-a ne postoji.
Vrijeme trajanja procesa	Vrijeme trajanja procesa sortiranja jest nepromijenjeno.

5.4. Preporuke za sprječavanje predstavljenih kibernetičkih napada na eksperimentalni postav

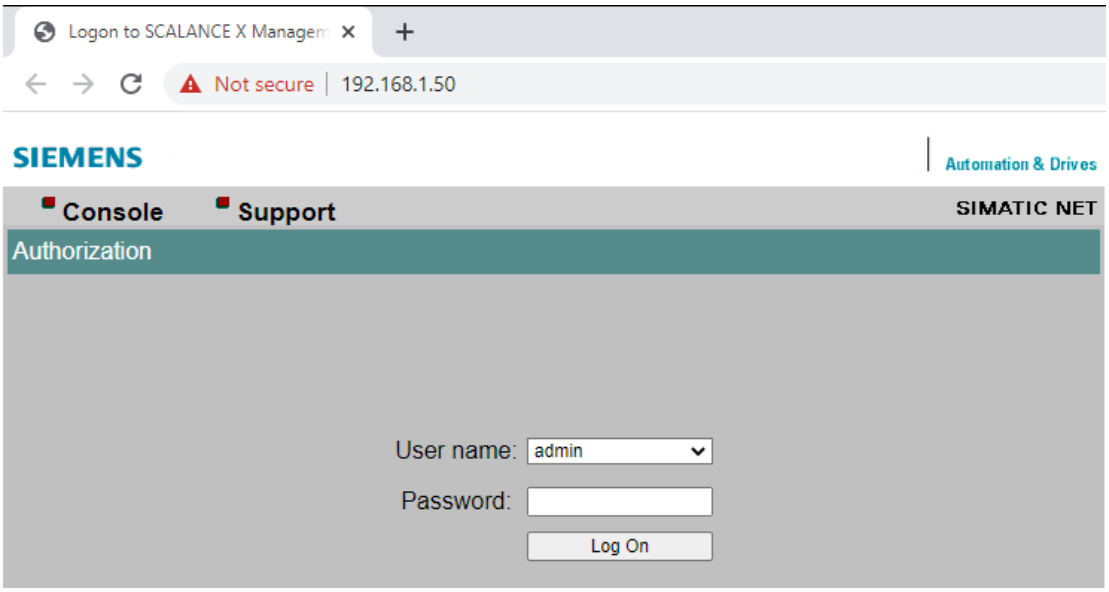
Analizom preporuka unutar analiziranih radova i omjera cijene, zahtjevnosti te standardnog zahtjeva za što manjim izmjenama unutar sustava, donesena je odluka o implementaciji sigurnosnih pravila unutar industrijskog upravljivog preklopnika SCALANCE X308-2. Jasno, SCALANCE X308-2 već se nalazi unutar eksperimentalnog postava, tako da je potrebno isključivo podešavanje preklopnika.

Pristup upravljačkom sučelju preklopnika moguće je ostvariti putem niza protokola, od kojih je zbog sigurnosne važnosti potrebno istaknuti HTTPS te SSH [27]. Inicijalno podešavanje i pristup upravljivom preklopniku moguće je ostvariti koristeći alat SINEC Primary Network Initialization (PNI) proizvođača Siemens. Unutar alata, moguće je podesiti niz parametara samih uređaja – ime, IP adresu, ažurirati firmver, resetirati uređaj na tvorničke postavke, pristupiti upravljačkom sučelju (ovisno o opremi) te u konačnici uspostaviti vezu s opremom [27]. Slikom 5.10 dan je prikaz alata SINEC PNI te otkrivenog SCALANCE upravljivog pretvornika.



Slika 5.10 Prikaz upravljačkog sučelja alata SINEC PNI

Nakon podešavanja imena te IP adrese uređaja, slijedi spajanje na mrežno sučelje preklopnika. Pristup preklopniku ostvaren je unosom mrežne adrese preklopnika unutar odabranog mrežnog preglednika. Slikom 5.11 dan je prikaz sučelja za autorizaciju korisnika.

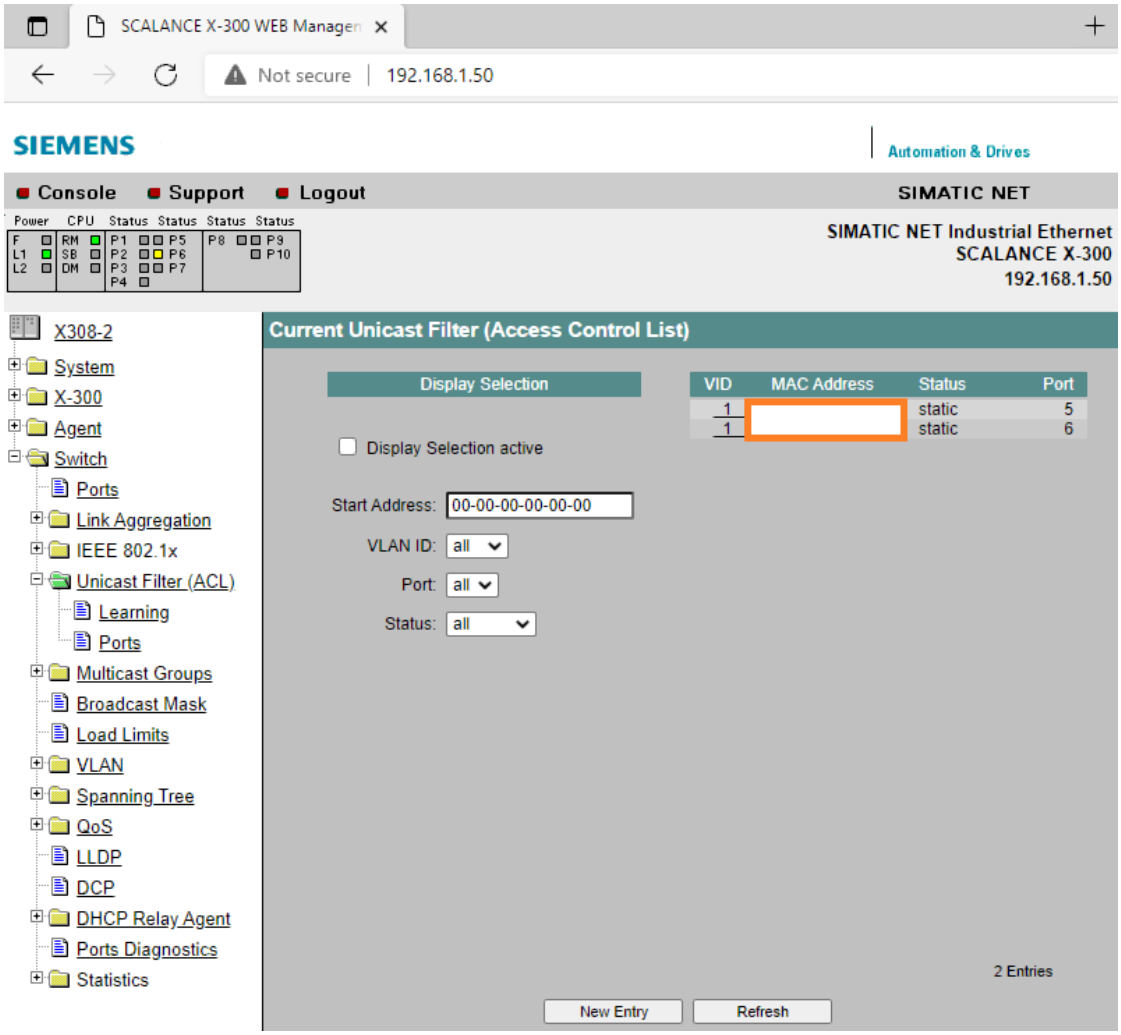


Slika 5.11 Prikaz upravljačkog sučelja za autorizaciju korisnika preklopnika SCALANCE X308-2

Nakon unosa autorizacijskih podataka, korisniku se omogućuje pristup različitim mrežnim postavkama upravljivog preklopnika. Tako je unutar uređaja moguće podešavati postavke vezane uz sustav, priključke, virtualne lokalne mreže (engl. *Virtual Local Area Network* – VLAN), protokole vezane uz razne mrežne topologije te u konačnici postavke vezane uz kibernetičku sigurnost [27]. Od posebnog značaja za ovaj rad jest mogućnost određivanja MAC lista dozvoljenih pristupa (engl. MAC *Access Control List* – ACL) kojim je moguće povezati određeni mrežni priključak i VLAN s jednom odnosno više MAC adresa uređaja. MAC ACL lista predstavlja jednu od metoda koju analizira rad [40] čijom se implementacijom značajno povećava sigurnost samog sustava – otežava se postupak ARP trovanja na način da se napadač mora priključiti na određeni priključak te lažirati svoju MAC adresu. Bez fizičkog priključenja na točno određeni priključak i lažiranja adrese, napadač ne može pristupiti uređajima na mreži.

Slikom 5.12 dan je prikaz podešenja MAC ACL liste upravljivog preklopnika SCALANCE X308-2.

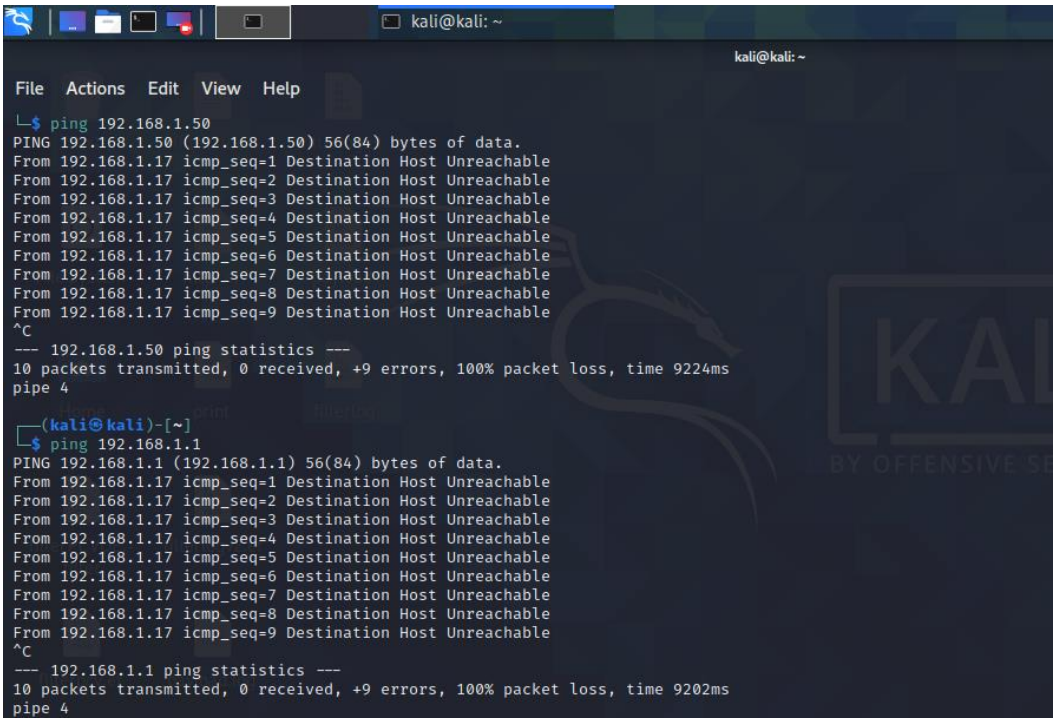
Na slici 5.12, vidljivo je da je prvi uređaj (MAC adrese su maskirane zbog osjetljivosti podataka) povezan s priključkom 5, dok je MAC adresa drugog uređaja priključena na priključak 6. U slučaju priključenja bilo kojeg drugog uređaja na ostale aktivne priključke, navedeni uređaj neće moći komunicirati s PLC-om te HMI-jem.



Slika 5.12 Prikaz podešenja MAC ACL tablice upravljivog preklopnika SCALANCE X308-2

Nakon podešavanja MAC ACL tablica, ponovno je proveden postupak ARP trovanja u svrhu onemogućavanja komunikacije između uređaja, ali ovaj put neuspješno.

Slikom 5.13 dan je prikaz pokušaja detektiranja PLC-a te SCALANCE upravljivog preklopnika pomoću naredbe *ping* u terminalu napadačkog Kali Linux računala.



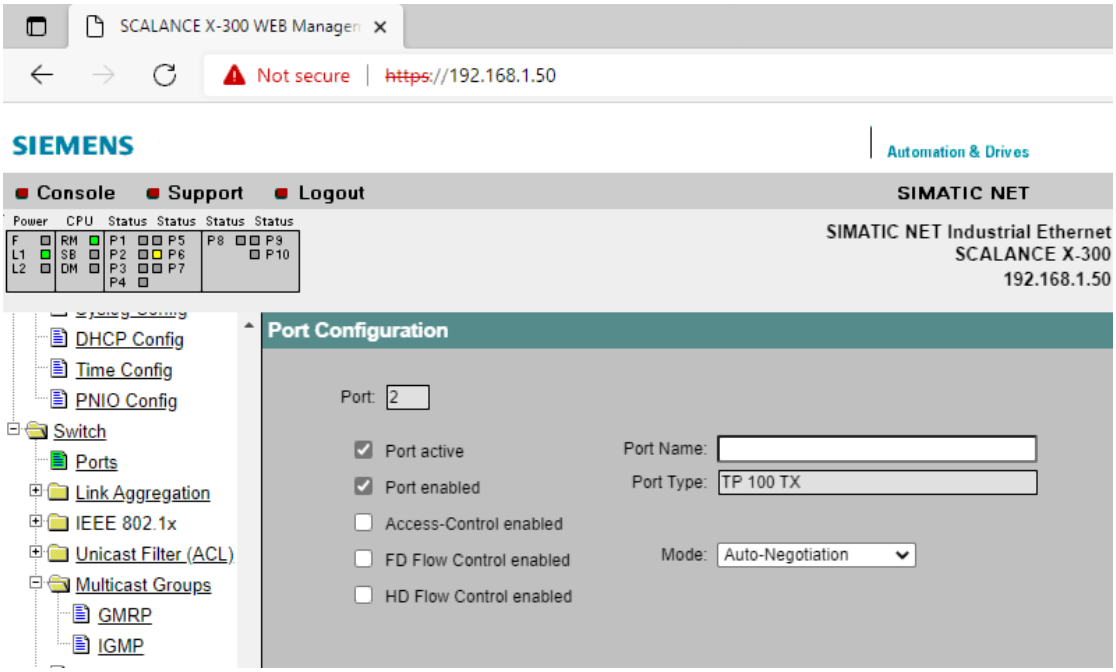
Slika 5.13 Prikaz pokušaja otkrivanja uređaja na mreži nakon implementacije MAC ACL tablica

Na slici 5.13, vidljivo je da su napadačkom uređaju svi drugi uređaji na mreži nedostupni, što je u skladu s očekivanjima. Implementirana metoda onemogućuje oba provedena napada – kod napada u svrhu prikupljanja informacija u potpunosti je onemogućen pristup uređajima, dok kod napada u svrhu onemogućavanja komunikacije između uređaja također nije moguće uspješno provesti napad.

Implementacija MAC ACL tablica zapravo predstavlja jednu od mogućih vrsta segmentacije komunikacijske mreže (engl. *Network Segmentation*), i to specifično na drugom sloju OSI modela (sloj podatkovne poveznice). Sam koncept segmentacije komunikacijske mreže nije nov i dolazi iz IT svijeta [2], a odabir vrste segmentacije i sloja OSI modela na kojem će se segmentacija provesti jest ovisna o sposobnosti opreme i zaposlenika, sigurnosnim zahtjevima te u konačnici dozvoljenim financijskim sredstvima za razvoj kibernetičke sigurnosti unutar sustava. Rizik kod implementacije mjera za povećanje sigurnosti jest dobivanje privida sigurnosti na temelju kojeg netko (potencijalno menadžment) može na trenutak pomisliti da je sustav siguran.

Prestankom praćenja stanja sustava upravljanja kibernetičkom sigurnošću moguće su katastrofalne posljedice po poduzeće – havarije i ekološke katastrofe.

Uz navedenu sigurnosnu preporuku, preporučljivo je deaktivirati sve nekorištene mrežne priključke kako bi se dodatno onemogućio pristup nedozvoljenim uređajima. Korišteni preklopnik podržava i tu mogućnost te se slikom 5.14 prikazuje izbornik unutar kojeg je moguće deaktivirati neaktivne priključke.



Slika 5.14 Prikaz izbornika za deaktivaciju priključaka upravljivog preklopnika SCALANCE X308-2

Jasno, predložene metode za povećanje sigurnosti predstavljaju samo jedan dio metoda koje je moguće implementirati unutar analiziranog sustava, ali su za opseg ovog rada dovoljne. Naime, provedbom ponovljenih napada pokazalo se da navedeni napadi nisu više mogući, ali potpun i cjelovit odgovor o kibernetičkoj sigurnosti sustava nije dobiven. Takav odgovor moguće je dobiti tek u vidu procjene kibernetičkog rizika sustava kod kojeg se provodi niz istraživanja i analiza koje se u ovom radu ne razmatraju, ali bi ih za potpuno razumijevanje sustava bilo nužno provesti.

6. Zaključak

U okviru ovog znanstvenog rada provedeno je istraživanje o mogućnostima eksperimentalnih postava za ispitivanje kibernetičke sigurnosti industrijskih upravljačkih sustava. Nakon provedbe analize postojećih radova, utvrđena je standardna oprema unutar klasičnog industrijskog postrojenja te je provedena implementacija odabranog industrijskog upravljačkog sustava u konfiguraciji: odabrano industrijsko postrojenje – PLC – industrijski upravljivi preklopnik – HMI. Za industrijsko postrojenje u ovom radu odabran je model linije za sortiranje prema boji uzorka, dok su PLC, HMI te industrijski upravljivi preklopnik proizvođača Siemens. Nakon implementacije upravljačkog programa i upravljačkog sučelja procesa, provedena je analiza korištenog S7CommPlus industrijskog komunikacijskog protokola. Po provedbi analize korištenog protokola, provedena su dva odabrana kibernetička napada na postrojenje temeljem napadačkog scenarija u kojem se napadač priključuje na neki od slobodnih mrežnih priključaka unutar industrijskog postrojenja. Prvi odabrani napad jest napad u svrhu prikupljanja informacija, dok je drugi napad proveden u svrhu onemogućavanja komunikacije između uređaja na industrijskoj komunikacijskoj mreži. Oba napada provedena su koristeći javno dostupne alate unutar operacijskog sustava Kali Linux. U konačnici, provedena je analiza mogućih rješenja za povećanje sigurnosti promatranog industrijskog procesa te je naposljetku analizom omjera uloženih resursa u odnosu na povećanje kibernetičke sigurnosti kao metoda za povećanje sigurnosti sustava odabrano podešavanje postojećih sigurnosnih alata u obliku MAC ACL tablica te isključivanja neaktivnih mrežnih priključaka unutar industrijskog preklopnika SCALANCE X308-2. Metode za povećanje sigurnosti sustava verificirane su za oba napada neuspješnim ponavljanjem provedenih kibernetičkih napada unutar sustava.

Nakon pregleda provedenih radnji unutar ovog znanstvenog rada, potrebno je prezentirati zaključke. Rezultati ispitivanja kibernetske sigurnosti implementiranog upravljačkog sustava pokazali su iznimnu ranjivost promatranog sustava, posebno na napade u svrhu prikupljanja informacija. Dodatna otegotna okolnost jest što je za provedbu analiziranih napada potrebna iznimno niska razina znanja i motivacije – oba napada provedena su koristeći javno dostupne alate. Motivirani napadač koji posjeduje veću razinu znanja o IACS-ovima te korištenom komunikacijskom protokolu mogao bi nanijeti znatnu štetu bilo

kojem postrojenju u kojem se nalazi, ako ne postoje alati i metode za povećanje kibernetičke sigurnosti sustava. Jasno, implementirane metode štite sustav od proučavanih napada, ali su navedeni napadi tek djelić mogućih radnji koje napadač može napraviti unutar postrojenja. Također, potrebno je osvrnuti se na nedostatke implementiranog postava. Naime, činjenica je da se fizičkom implementacijom – fizički model industrijskog postrojenja, PLC-a, HMI-ja te upravljivog preklopnika gubi na količini mogućih napadačkih scenarija, zato što su određeni napadački scenariji usko vezani uz kontekst industrijskog postrojenja koje se napada. Tako je model linije za sortiranje odličan i jednostavan primjer IACS-a, ali je za definiranje naprednijih napadačkih scenarija potrebno proširiti kompletan eksperimentalni model – priključiti ga potencijalno na Internet, uspostaviti različite IT usluge unutar postrojenja koje standardno unose nove potencijalne vektore napada te u konačnici definirati kontekst modela linije sortiranje – na primjer, model linije za sortiranje lijekova. Osnovni nedostatak implementiranog postrojenja jest veličina, ali je činjenica da za edukacijske svrhe implementirani postav može predstavljati reprezentativan model IACS-a. Također, ovakav model sustava moguće je koristiti za istraživanje ranjivosti koje su specifične za proizvođače opreme koja se nalazi unutar modela.

Jasno se temeljem navedenih zaključaka može zaključiti da razvijeni eksperimentalni postav potvrđuje hipotezu o kvalitativnom provođenju ispitivanja metoda za povećanje kibernetičke sigurnosti IACS-ova, edukaciji, ispitivanju ranjivosti odabrane opreme te u konačnici razvijanju znanja i svijesti o razini kibernetičke sigurnosti u industrijskim postrojenjima.

Literatura

[1] Diakun-Thibault, N, *Defining Cybersecurity*. Technology Innovation Management Review. 2014.

[2] Knapp E, Langill T, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA and Other Industrial Control Systems* 2. Izdanje, 2015

[3] Europska komisija, *General Data Protection Regulation (GDPR)*, Poveznica: https://www.zakon.hr/z/1023/Zakon-o-provedbi-Op%C4%87e-uredbe-o-za%C5%A1titi-podataka; Pristupljeno 10. svibnja 2021.

[4] Lukasik, S, *Why the Arpanet Was Built*. IEEE Annals of the History of Computing. 2011

[5] McLaughlin, S. et al, *The Cybersecurity Landscape in Industrial Control Systems*. Proceedings of the IEEE. 2016

[6] Tsohou, A, et al, *Investigating Information Security Awareness: Research and Practice Gaps*. Information Security Journal: A Global Perspective. 2008

[7] ENISA. Poveznica: https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services; pristupljeno 10. svibnja

[8] Candell R. et al, *A Cybersecurity Testbed for Industrial Control Systems*, ISA Process Control & Safety Symposium, 2014

[9] Russell E.L. et *al*, *Data-driven Methods for Fault Detection and Diagnosis in Chemical Processes*. Advances in Industrial Control, 2000

[10] Xu, W. et al, *MSICST: Multiple-Scenario Industrial Control System Testbed for Security Research*. Computers, Materials & Continua., 2019

[11] Liang G. et al, *The 2015 ukraine blackaut: implications for false data injection attacks*. IEEE Transactions on Power Systems, 2017

[12] McLaughlin et al, *The Industrial Control Systems Cyber Security Landscape*. Proceedings of the IEEE, 2016

[13] Davis C. M. et al, *SCADA Cyber Security Testbed Development*, Power Symposium, 2006

[14] MITRE organizacija, Poveznica: https://www.cvedetails.com/; Pristupljeno: 10. svibnja 2021.

[15] FIRST organizacija, Poveznica: https://www.first.org/cvss/; Pristupljeno: 10. svibnja 2021.

[16] NIST, Poveznica: https://nvd.nist.gov/vuln/detail/CVE-2020-15782; Pristupljeno: 2. lipnja 2021.

[17] Siemens, Poveznica: https://cert-portal.siemens.com/productcert/pdf/ssa-434534.pdf; Pristupljeno: 2. lipnja 2021.

[18] Profibus & Profinet International (PI), Poveznica: https://www.profibus.com/download/profinet-specification; Pristupljeno 12. svibnja 2021

[19] Wireshark wiki, Poveznica: https://wiki.wireshark.org/S7comm; Pristupljeno 12. svibnja 2021

[20] EtherCAT Technology Group, Poveznica: https://www.tecnical.cat/PDF/OMRON/Vision/Q179-E1-01.pdf; Pristupljeno 13. svibnja 2021

[21] Mohor I, *Ethernet IP Core Specifitation*, Poveznica: http://www.cprover.org/firmware/doc/ethoc/eth_speci.pdf; Pristupljeno 13.svibnja 2021.

[22] Modbus organizacija, Poveznica: https://modbus.org/specs.php; Pristupljeno 14.svibnja 2021

[23] Hui H et al. *Investigating Current PLC Security Issues Regarding Siemens S7 Communications and TIA Portal*. 5th International Symposium for ICS & SCADA Cyber Security Research, 2018

[24] IEEE C37.1-2007 *IEEE Standard for SCADA and Automation Systems*, 2007

[25] MITRE organizacija, Poveznica: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=siemens; Pristupljeno 17. svibnja 2021.

[26] IEC 61131-3:2013 *Programmable controllers – Part 3: Programming languages*, 2013

[27] Siemens, Poveznica: https://cache.industry.siemens.com/dl/files/331/25248331/att_1004652/v1/BA_SCALANCE-X-300_76.pdf; Pristupljeno 20. svibnja 2021.

[28] Siemens, Poveznica; https://new.siemens.com/global/en/products/automation/industry-software/automation-software/tia-portal.html, Pristupljeno 20.svibnja 2021.

[29] Calvo I. et al, *Key Vulnerabilities of Industrial Automation and Control Systems and Recommendations to Prevent Cyber-Attacks*. International Journal of Online Engineering, 2016

[30] Mhiri S. *Analyzing an OT network, what to expect*. Inprosec conference, 2019

[31] Zimmerman H, *OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection*, IEEE Transactions on Communications, vol. 28, no. 4, 1980

[32] Wireshark, Poveznica: https://wiki.wireshark.org/TPKT, Pristupljeno: 25. svibnja 2021.

[33] Wireshark, Poveznica: https://wiki.wireshark.org/COTP, Pristupljeno: 25. svibnja 2021.

[34] Wireshark, Poveznica: https://wiki.wireshark.org/, Pristupljeno: 27. svibnja 2021.

[35] Wiens T, Poveznica https://sourceforge.net/projects/s7commwireshark/, Pristupljeno 30. svibnja 2021.

[36] Yilmaz E.N. et al, *Cyber Security Analysis of DoS and MitM Attacks Against PLCs Used in Smart Grids*, International Istambul Smart Grids and Cities Congress and Fair, 2019

[37] Offensive Security, Poveznica: https://www.kali.org/docs/introduction/, Pristupljeno: 5. lipnja 2021.

[38] Nmap, Poveznica: https://nmap.org/; Pristupljeno: 7.lipnja 2021.

[39] MITRE organizacija, Poveznica: https://collaborate.mitre.org/attackics/index.php/Main_Page; Pristupljeno: 8. lipnja 2021.

[40] Singh J. et al, *A Detailed Survey of ARP Poisoning Detection and Mitigation Techniques*, International Journal of Control Theory and Applications, 2017.

Sažetak

Unutar rada „Razvoj eksperimentalnog postava industrijskog upravljačkog sustava za ispitivanja kibernetičke sigurnosti“ provedena je analiza mogućnosti eksperimentalnih postava za ispitivanje kibernetičke sigurnosti industrijskih upravljačkih sustava. Nakon provedbe analize postojećih znanstvenih radova koji obrađuju sličnu tematiku, utvrđena je standardna oprema unutar klasičnog industrijskog postrojenja te je provedena implementacija odabranog industrijskog upravljačkog sustava u konfiguraciji: odabrano industrijsko postrojenje – PLC – industrijski upravljivi preklopnik – HMI. Za industrijski proces u ovom radu odabran je model linije za sortiranje prema boji uzorka, dok su PLC, HMI te industrijski upravljivi preklopnik proizvođača Siemens. Nakon implementacije upravljačkog programa i upravljačkog sučelja procesa, provedena je analiza korištenog S7CommPlus industrijskog komunikacijskog protokola. Po provedbi analize korištenog protokola, provedena su dva odabrana kibernetička napada na postrojenje temeljem napadačkog scenarija u kojem se napadač priključuje na neki od slobodnih mrežnih priključaka unutar industrijskog postrojenja. Prvi odabrani napad jest napad u svrhu prikupljanja informacija, dok je drugi napad proveden u svrhu onemogućavanja komunikacije između uređaja na industrijskoj komunikacijskoj mreži. Oba napada provedena su koristeći javno dostupne alate unutar operacijskog sustava Kali Linux. U konačnici, provedena je analiza mogućih rješenja za povećanje sigurnosti promatranog industrijskog postrojenja te su predstavljene i verificirane metode pomoću kojih je moguće spriječiti odabrane napadačke scenarije.

Autor rada: Filip Katulić

Ključne riječi: Kibernetička sigurnost industrijskih upravljačkih sustava (IACS-ova), Programirljivi logički kontroler (PLC) S7-1500, Model linije za sortiranje, Eksperimentalni postav za ispitivanje kibernetičke sigurnosti.

Summary

Within the paper "Development of an industrial automation and control system testbed for cybersecurity testing", an analysis of the experimental setup possibilities for industrial control systems cybersecurity testing was conducted. After the analysis of existing scientific papers dealing with similar topics, the standard equipment within the classic industrial plant was determined and selected. Using the standard equipment determined in the previous step, an industrial automation and control system was implemented with the following topology: selected industrial plant - PLC - industrial managed switch - HMI. For the industrial process in this paper, the model of the sorting line with colour detection was chosen, while the PLC, HMI and the industrial managed switch are made by Siemens. After the development and implementation of the automation programme and a user control interface, an analysis of the used S7CommPlus industrial communication protocol was performed. After performing the analysis of the used protocol, two selected cyber attacks on the plant were chosen and performed. The selected cyber attacks were based on the attack scenario in which the attacker obtains physical access to the industrial communication network. The first selected attack is an attack with the aim of information gathering, while the second attack was conducted with the aim of disabling communication between devices on the industrial communication network. Both attacks were carried out using publicly available tools within the Kali Linux operating system. Finally, an analysis of the possible cybersecurity measures was conducted and verified.

Paper author: Filip Katulić

Key words: Industrial automation and control system (IACS) cybersecurity, Programmable logical controller (PLC) S7-1500, Model of the sorting line with colour detection, IACS Cybersecurity testbed.