43. JUPITER KONFERENCIJA
sa međunarodnim učešćem

43rd JUPITER CONFERENCE
with foreign participants

ZBORNIK RADOVA
PROCEEDINGS

UNIVERZITET U BEOGRADU - MAŠINSKI FAKULTET

UNIVERSITY OF BELGRADE
FACULTY OF MECHANICAL ENGINEERING

Beograd, oktobar 2022.

43. JUPITER KONFERENCIJA

ZBORNIK RADOVA

Organizator i izdavač:
UNIVERZITET U BEOGRADU - MAŠINSKI FAKULTET

Adresa:

Kraljice Marije 16, 11120 Beograd, Srbija
Tel: 011/3370341, Fax: 011/3370364
El. pošta: jupiter@mas.bg.ac.rs

Za izdavača: Dekan, dr Vladimir Popović, red. prof.

Štampanje odobrila:
Komisija za izdavačku delatnost Mašinskog fakulteta i Dekan Mašinskog fakulteta

Odlukom br. 27/2022 od 19.09.2022.

Tehnički urednici:

Prof. dr Bojan Babić
Prof. dr Saša Živanović
Prof. dr Mihajlo Popović

Beograd, oktobar 2022.

Tiraž: 100 primeraka
Štampa: **Planeta print**,
11000 Beograd, Igora Vasiljeva 33r, tel.: 011 650 6564

ISBN 978-86-6060-137-9

Spisak svih radova na JUPITER Konferenciji
po prezimenu prvog autora

Jakovljević, Ž., Nedeljković, D.[1)]

SAJBER BEZBEDNOST U KONTINUALNIM SISTEMIMA UPRAVLJANJA – PREGLED REZULTATA U OKVIRU PROJEKTA MISSION4.0[2)]

Rezime

U okviru ovog rada navode se rezultati istraživanja sprovedenih u okviru projekta MISSION4.0 pod nazivom Optimizacioni algoritmi za upravljanje i terminiranje kibernetsko fizičkih sistema u okviru Industrije 4.0 zasnovani na dubokom mašinskom učenju i inteligenciji roja, finansiranog od strane Fonda za nauku Republike Srbije u periodu od 2020-2022. godine. Prikazani rezultati odnose se na oblast sajber bezbednosti u kontinualnim sistemima upravljanja što predstavlja jedan od radnih paketa projekta MISSION4.0. U skladu sa tim, pravci istraživanja odnosili su se na razvoj algoritama za detekciju napada u industrijskim sistemima upravljanja sa centralizovanom i distribuiranom arhitekturom, kao i na primenu otvorene platforme za komunikaciju, u cilju bezbedne razmene podataka između uređaja različitih proizvođača. Pored toga, dobijeni rezultati i njihova integracija u predavanja i laboratorijske vežbe poslužili su kao osnova za edukaciju inženjera u oblastima kibernetsko fizičkih sistema, industrijskog interneta stvari i sajber bezbednosti.

Ključne reči: sajber bezbednost, detekcija napada, OPC-UA, edukacija inženjera

1. UVOD

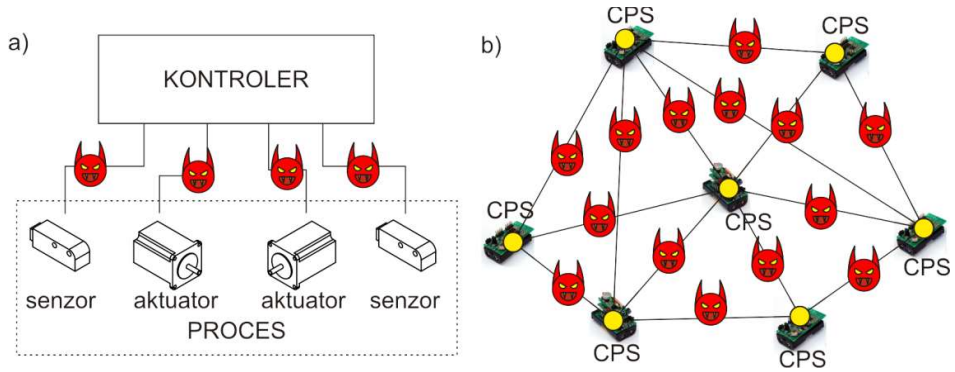
Projekat MISSION4.0 pod nazivom Optimizacioni algoritmi za upravljanje i terminiranje kibernetsko fizičkih sistema u okviru Industrije 4.0 zasnovani na dubokom mašinskom učenju i inteligenciji roja (engl. *Deep Machine Learning and Swarm Intelligence-based Optimization Algorithms for Control and Scheduling of Cyber-Physical Systems in Industry 4.0*) jedan je od dvanaest projekata finansiranih u periodu 2020-2022. godina od strane Fonda za nauku Republike Srbije u okviru Programa za razvoj projekata iz oblasti veštačke inteligencije [1]. Istraživanja u okviru ovog projekta vođena su potrebama proizvodnih kompanija da implementiraju proizvodnu paradigmu pod nazivom Industrija 4.0 čiji je osnovni cilj proizvodnja proizvoda prema zahtevima kupaca. Industrija 4.0 zasnovana je na sveobuhvatnoj digitalizaciji proizvodnih procesa i prikupljanju velike količine podataka iz pogona kako bi se na osnovu njih izvršilo prilagođavanje proizvodnje različitim vrstama proizvoda u skladu sa zahtevima tržišta. Tehničko-tehnološki faktor koji omogućava implementaciju ove paradigme predstavljaju kibernetsko fizički sistemi – CPS (engl. *Cyber-Physical Systems*) i na njima zasnovan industrijski internet stvari – IIoT (engl. *Industrial Internet of Things*) [2]. Zahvaljujući primeni CPS-a u proizvodnim pogonima moguće je ostvariti adaptabilnost proizvodnih sistema kroz njihovu fizičku i funkcionalnu rekonfiguraciju. Sa jedne strane, CPS omogućavaju prikupljanje podataka koji mogu poslužiti za funkcionalno rekonfigurisanje proizvodnih sistema kroz adaptivno planiranje i terminiranje proizvodnje, a s druge strane,oni se u okviru proizvodnih pogona konfigurišu kao sistemi sistema (engl. *Systems of Systems*) gde se CPS manje kompleksnosti (npr. pametni senzori i aktuatori) integrišu u kompleksnije CPS (npr. mašine) sve do nivoa celokupnog kibernetsko fizičkog proizvodnog sistema – CPPS (engl. *Cyber-Physical Production Systems*); ovakav modularan dizajn CPS omogućava brzo i jednostavno fizičko rekonfigurisanje CPPS i njihovih elemenata. Raspoloživost velike količine podataka i modularnost proizvodnih resursa zahteva potpuno nove pristupe upravljanju proizvodnim sistemima i resursima u okviru Industrije 4.0.U skladu sa navedenim, osnovni cilj projekta MISSION4.0 bio je razvoj novih algoritama za

[1)]prof. dr Živana Jakovljević, Univerzitet u Beogradu, Mašinski fakultet, (zjakovljevic@mas.bg.ac.rs), Dušan Nedeljković, mast. inž. maš, asistent, Univerzitet u Beogradu, Mašinski fakultet, (dnedeljkovic@mas.bg.ac.rs)

[2)]U ovom radu, saopštava se pregled dela rezultata istraživanja ostvarenih u okviru naučnog projekta MISSION4.0, ev. broj: 6523109, koji je finansijski podržan od Fonda za nauku Republike Srbije, kao i projekta Univerziteta u Beogradu - Mašinskog fakulteta, ev. broj: 451-03-68/2022-14/200105, finansijski podržanog od Ministarstva prosvete, nauke i tehnološkog razvoja Vlade Republike Srbije.

upravljanje, terminiranje i sajber bezbednost kibernetsko fizičkih proizvodnih sistema.

Uvođenje CPS dovodi do značajnih promena u industrijskim sistemima upravljanja. Naime, uz primenu CPS, sistemi upravljanja distribuirani na pametne uređaje (npr. senzore i aktuatore) sa integrisanim lokalnim kontrolerima najčešće zasnovanim na mikrokontrolerskim platformama polako zamenjuju centralizovane sisteme upravljanja bazirane na tradicionalnoj piramidi automatizacije standardizovanoj kroz IEC 62264 [3]. Pri tom se pojedini elementi zadatka upravljanja distribuiraju na lokalne kontrolere u mreži, a celokupan zadatak upravljanja realizuje se kroz njihovu intenzivnu komunikaciju korišćenjem različitih protokola. I u okviru centralizovanih sistema upravljanja sa pojavom IIoT sve više se koriste pametni uređaji koji sa centralnim kontrolerom razmenjuju podatke takođe korišćenjem komunikacionih protokola. Još jedna od karakteristika Industrije 4.0 je da kompanije, kako bi se što više približile kupcima i što brže odgovorile na njihove potrebe, podatke o statusu proizvodnih procesa stavljaju na raspolaganje svojim kooperantima (dobavljačima, komitentima i sl.). Kao posledica, industrijski sistemi upravljanja nisu više izolovani već su u sve većoj meri povezani na globalnu mrežu, a komunikacioni linkovi u okviru njih postaju izloženi različitim vrstama kibernetskih napada (slika 1).



Slika 1. *Komunikacioni linkovi izloženi kibernetskim napadima u: a) centralizovanim sistemima upravljanja; b) distribuiranim sistemima upravljanja*

U skladu sa navedenim, jedan od radnih paketa u okviru projekta MISSION4.0 odnosio se na sajber bezbednost u kontinualnim sistemima upravljanja. U ovom radnom paketu istraživane su mogućnosti za detekciju napada i bezbedan prenos podataka u okviru centralizovanih i distribuiranih sistema upravljanja proizvodnim resursima. Sprovedena istraživanja se mogu podeliti u tri osnovne grupe: 1) razvoj algoritama za detekciju napada u industrijskim sistemima upravljanja sa centralizovanom i distribuiranom arhitekturom, 2) primena Otvorene platforme za komunikaciju – OPC-UA (engl. *Open Platform Communications – Unified Architecture*) za bezbednu razmenu podataka između uređaja različitih proizvođača, 3) Edukacija inženjera u oblastima CPS, IIoT i sajber bezbednosti. U ovom radu se daje pregled najznačajnijih rezultata projekta MISSION4.0 u navedenim oblastima, a rad je struktuiran upravo u skladu sa njima. Nakon pregleda rezultata, slede zaključne napomene sa pravcima daljih istraživanja.

2. RAZVOJ ALGORITAMA ZA DETEKCIJU NAPADA U INDUSTRIJSKIM SISTEMIMA UPRAVLJANJA

Najveći deo istraživanja u oblasti sajber bezbednosti u okviru projekta MISSION4.0 upravo se odnosio na razvoj algoritama za detekciju napada u industrijskim sistemima upravljanja – ICS (engl. *Industrial Control Systems*). Međutim, pre razvoja samih mehanizama zaštite bilo je neophodno dubinsko poznavanje sistema čija se zaštita vrši kao i specifičnih algoritama koji se koriste za upravljanje resursima u Industriji 4.0. Ovde treba imati u vidu da Industrija 4.0 predstavlja relativno nov koncept i u skladu sa tim za implemetaciju IIoT i na njima zasnovanih distribuiranih sistema u okviru ICS i dalje ne postoje širokoprihvaćene inženjerske metode kao što je to slučaj sa centralizovanim upravljanjem. Kako bi se napravila solidna osnova za razvoj sistema zaštite od kibernetskih napada, određeni napori u okviru projekta su usmerenina metode za distribuciju zadataka upravljanja na pametne uređaje [4, 5], na analizu bezbednosnih izazova u okviru distribuiranih sistema upravljanja [4, 6], kao i na razvoj inteligentnih senzorskih sistema [7], ali je u fokusu istraživanja bio razvoj sistema za detekciju napada na sisteme za kontinualno upravljanje proizvodnim resursima.

ICS po pitanju zahteva koji se postavljaju pred sisteme za detekciju napada imaju određene specifičnosti u odnosu na opšte informacione tehnologije [8]. Kod opštih informacionih tehnologija su poverljivost i integritet

podataka najznačajniji i prihvatljivo ih je obezbediti na račun brzine komunikacije, odnosno raspoloživosti podataka. Kod ICS, s druge strane, od najvećeg značaja je imati podatke na raspolaganju u realnom vremenu kako ne bi došlo do kašnjenja u ostvarivanju upravljačkih zadataka koji su najčešće vremenski ograničeni. Pored toga, u opštim informacionim tehnologijama za implementaciju sistema za zaštitu od napada na raspolaganju je hardver sa relativno visokim proračunskim sposobnostima i mrežnim napajanjem, dok kod ICS kontroleri, posebno u slučaju distribuiranog upravljanja, imaju ograničene proračunske mogućnosti, a često su i napajani baterijama i samim tim energetski ograničeni. Takođe, za razliku od opštih informacionih tehnologija kod kojih su po pravilu u upotrebi operativni sistemi, u okviru ICS najčešće se koriste namenski kreirani softveri i komunikacioni protokoli. Još jedna značajna razlika između opštih informacionih tehnologija i ICS ogleda se u posledicama koje napadi mogu izazvati. Dok su kod opštih informacionih tehnologija posledice napada najčešće ekonomske prirode, kod ICS, pored ekonomskih, posledice mogu biti katastrofalne u smislu značajnih oštećenja opreme, fatalnog uticaja na životnu sredinu i zdravlje čoveka, a u najgorim scenarijima mogu rezultovati gubitkom ljudskih života. U skladu sa navedenim, očigledno je da je u okviru ICS potrebno kreirati namenske, proračunski efikasne algoritme za detekciju napada koji su okarakterisani nultom tolerancijom.

Algoritmi za detekciju napada na kontinualne sisteme upravljanja po pravilu su zasnovani na modeliranju ponašanja sistema u normalnim uslovima (bez napada), a napadi se detektuju na osnovu razlike između modeliranih i ostvarenih vrednosti određenih signala [9]. Modeli mogu biti analitički ili zasnovani na podacima [10]. Imajući u vidu da se u proizvodnom okruženju može pronaći mnoštvo različitih procesa za koje je najčešće izuzetno komplikovano ili nemoguće kreirati analitički model, u okviru projekta MISSION4.0 korišćen je pristup zasnovan na podacima. Kao osnovna tehnika za kreiranje algoritama odabrane su duboke neuronske mreže – DNN (engl. *Deep Neural Networks*) i to:

1. Jednostavne rekurentne neuronske mreže – *Simple* RNN (engl. *Simple Recurrent Neural Networks*),
2. LSTM (engl. *Long Short-Term Memory*) rekurentne neuronske mreže,
3. GRU (engl. *Gated Recurrent Unit*) rekurentne neuronske mreže,
4. CNN (engl. *Convolutional Neural Networks*).

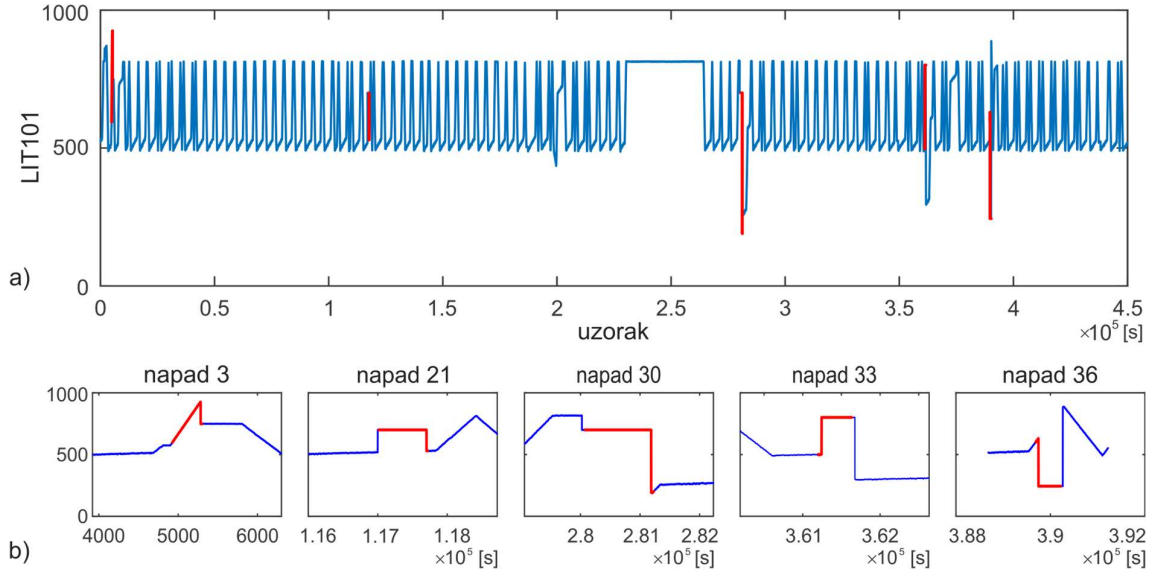
Implementacija DNN zahteva veliku količinu podataka, pa su tokom istraživanja korišćena dva skupa:

1. SWaT (engl. *Secure Water Treatment*) skup podataka i
2. Skup podataka dobijen sa elektropneumatskog sistema za pozicioniranje.

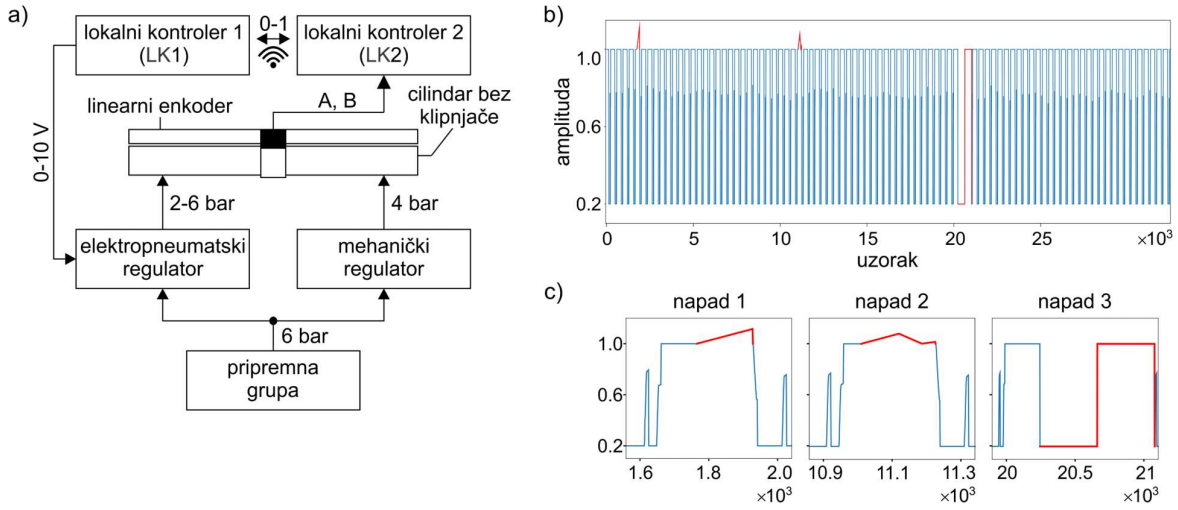
SWaT predstavlja skaliranu verziju industrijskog sistema za prečišćavanje vode kreiranu u svrhu istraživanja u oblasti sajber bezbednosti [11]. Sistem vrši filtriranje vode u šest sektora koji se upravljaju programabilnim kontrolerima i na koje je povezano ukupno 25 senzora i 26 aktuatora. Podaci koji se komuniciraju između kontrolera s jedne i senzora i aktuatora s druge strane se za čitav sistem prikupalju korišćenjem SCADA-e (engl. *Supervisory Control and Data Acquisition*). Akvizicija ovih podataka je vršena ukupno 11 dana od čega je tokom 7 dana sistem funkcionisao u normalnim uslovima, dok je u poslednja 4 dana lansirano ukupno 36 napada na komunikacione linkove sa različitim senzorima i aktuatorima. Na slici 2 prikazan je primer signala sa senzora nivoa vode u rezervoaru – LIT101 koji je prikupljen tokom poslednja 4 dana; delovi signala sa napadima na ovaj senzor (ukupno 5 napada) izdvojeni su i uveličani.

Pošto je, pored razvoja algoritama za detekciju napada na signale, bio cilj dokazati i njihovu primenljivost u realnim uslovima, u okviru projekta MISSION4.0 razvijena je eksperimentalna instalacija – elektropneumatski sistem za pozicioniranje čija je osnovna konfiguracija prikazana na slici 3a. Sistem se sastoji od 1) pametnog cilindra bez klipnjače upravljanog elektropneumatskim regulatorom pritiska sa jedne i mehaničkim regulatorom pritiska sa druge strane koji ima integrisan lokalni kontroler 1 (LK1) i 2) pametnog linearnog enkodera sa integrisanim lokalnim kontrolerom 2 (LK2). Oba lokalna kontrolera zasnovana su na NXP LPC1768 mikrokontroleru i kroz međusobnu komunikaciju ostvaruju zadatu trajektoriju cilindra [12]. Podaci komunicirani između lokalnih kontrolera u okviru ove instalacije prikupljeni su za različite trajektorije cilindra i javno su dostupni na *Zenodo* platformi u skladu sa FAIR (engl. *Findable, Accessible, Interoperable, and Reusable*) principima [13]; deo snimljenog signala sa izdvojenim napadima prikazan je na slikama 3b i 3c.

Prilikom kreiranja sistema za detekciju napada odabran je pristup polunadgledanog obučavanja kod koga su algoritmu za kreiranje IDS na raspolaganju podaci komunicirani između senzora/aktuatora i ostalih elementa sistema upravljanja tokom normalnog rada (bez napada). Korišćenjem ovih podataka i DNN, u okviru MISSION4.0 kreirani su autoregresioni modeli signala kod kojih se trenutna vrednost komuniciranog signala $s(t)$ procenjuje na osnovu bafera njegovih prethodnih z vrednosti - $s(t-z),...,s(t-1)$ (slika 4). Napad na

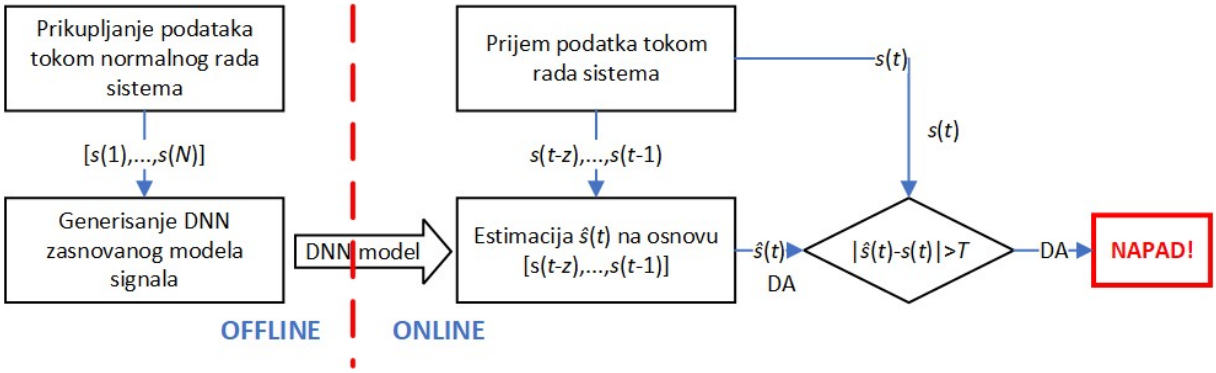


Slika 2. *LIT101 signal sa napadima: a) ceo signal; b) izdvojeni delovi signala za svaki od napada (napadi su označeni crvenom bojom)*



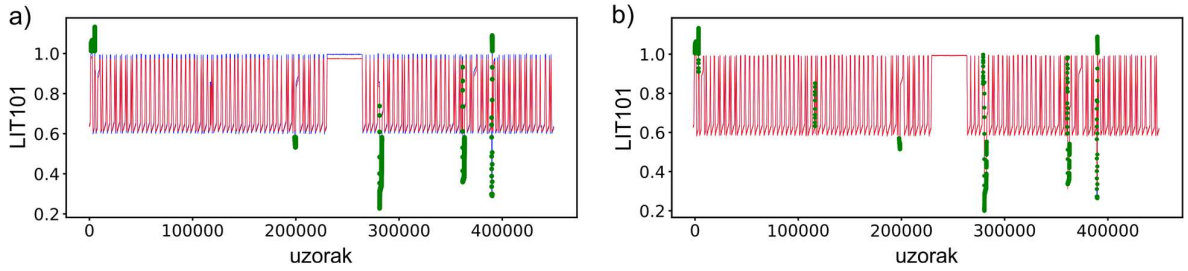
Slika 3. *Elektropneumatski sistem za pozicioniranje: a) skica sistema [12]; b)ceo signal sa napadima; c) izdvojeni delovi signala za svaki od napada (napadi su označeni crvenom bojom)*

komunikacioni link se detektuje kada razlika između primljene $s(t)$ i procenjene $\hat{s}(t)$ vrednosti signala pređe odogovarajući prag - T. Imajući u vidu da su kontrolerima u okviru distribuiranih sistema upravljanja na raspolaganju samo podaci sa pojedinih senzora/aktuatora, odlučeno je da se za detekciju napada na komunikacine linkove koristi univarijantna autoregresija komuniciranih podataka, tj. da se svaki signal modelira zasebno. Kreiranje IDS na osnovu univarijantnog modela je teže u odnosu na multivarijanti model kod koga se jednim modelom obuhvata više signala jer ne uzima u obzir korelaciju između podataka prikupljanih sa senzora i aktuatora. Međutim, IDS zasnovan na univarijantnom modelu je značajno jednostavnije implementirati jer se ne pojavljuju problemi vezani za raspoloživost određenih signala na kontroleru u okviru distriburianih sistema, različitu frekvencu odabiranja pojedinih signala i slično, već se IDS primenjuje odmah nakon prijema vrednosti komunikacionim linkom. Ovde je potrebno naglasiti da univarijantna regresija predstavlja potpuno novi pristup u odnosu na ranije sprovedena istraživanja u oblasti kreiranja IDS na osnovu podataka [14-20] koja čak ne uzimaju u obzir ni mogućnost implementacije algoritama (raspoloživost odgovarajućih signala) na nekom od uređaja u sistemu upravljanja.



Slika 4. *Osnovna arhitektura metode za generisanje IDS u okviru sistema za kontinulano upravljanje proizvodnim resursima*

Rekurentne neuronske mreže su mreže kod kojih trenutna vrednost izlaza zavisi ne samo od trenutne vrednosti ulaza već i od njegovih prethodnih vrednosti reprezentovanih u okviru skrivenih stanja RNN [21, 22] pa je opšteprihvaćen stav da RNN predstavljaju pogodnu tehniku za modeliranje kontinualnih sistema. Polazeći od navedenog, u okviru MISSION4.0 projekta prvobitno je istraživana primena RNN i to *Simple* RNN, LSTM i GRU u kreiranju IDS, a deo rezultata je prezentovan u [23]. Ipak, nastavak istraživanja je pokazao da se bolji rezultati dobijaju uz primenu CNN što je ilustrovanono slici 5 gde su prikazani rezultati primene IDS zasnovane na LSTM RNN i CNN na signalu sa LIT101 senzora iz SWaT skupa podataka. Na ovom signalu LSTM zasnovan IDS je uspeo da detektuje četiri od pet napada na LIT101 signal (napad 21 nije detektovan) i još dva napada na susedne aktuatore, dok je CNN zasnovan IDS bio uspešniji – detektovao je sve napade na LIT101 kao i dva napada na susedne aktuatore; napominje se da su *Simple* RNN i GRU RNN dale lošije rezultate od LSTM RNN.



Slika 5. *Napadi detektovani na LIT101 signalu iz SWaT skupa podataka korišćenjem IDS zasnovane na: a) LSTM RNN; b) CNN; Originalan signal normiran maksimalnom vrednošću signala bez napada prikazan je crvenom linijom, procenjene vrednosti signala plavom linijom, a odbirci na kojima je detektovan napad označeni su zelenim markerom*

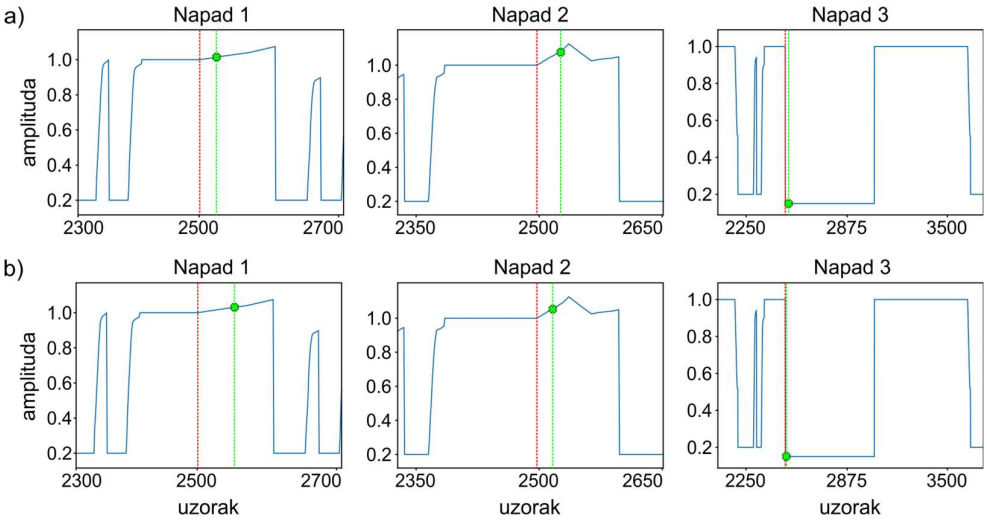
Sprovedena istraživanja su pokazala da je manuelno definisanje DNN arhitekture koja je pogodna za modeliranje signala, definisanje broja podataka z koji će se koristiti pri modeliranju, kao i određivanje praga T za detekciju napada vremenski zahtevno i podložno greškama što naročito dolazi do izražaja prilikom rekonfiguracije proizvodnih resursa kada je IDS potrebno kreirati za svaki novi signal. Iz navedenih razloga, u okviru MISSION4.0 projekta kreiran je metod za automatski izbor DNN, z i T na osnovu svojstava generalizacije različitih DNN modela i njihove sposobnosti da izbegnu prepoznavanje lažno pozitivnih rezultata što je izuzetno značajno u realnim ICS. Ovaj metod je detaljno opisan u radu [9] i zasnovan je na polumrežnoj pretrazi koja za cilj ima pronalaženje DNN sa najmanjim brojem parametara i najmanjom vrednošću z, a koja ispunjava zadate uslove. Naime, broj parametara DNN i veličina bafera z direktno su korelisani sa proračunskom kompleksnošću IDS, a samim tim i sa kašnjenjem koje IDS uzrokuje u algoritmu upravljanja koji radi u realnom vremenu. Ovo se naravno preslikava i na potrošnju energije što je značajno za energetski ograničen hardver.

Potrebno je naglasiti da automatsko definisanje arhitekture mreže i praga za detekciju predstavlja potpuno novi pristup. U prethodnim istraživanjima [17, 18, 24, 25] kreirane su jedinstvene arhitekture mreža, najčešće velike proračunske kompleksnosti, za tačno određene skupove podataka, a pragovi su podešavani ručno [25,

26] ili su zasnovani na primeni signala sa napadima [18, 24] tako da je njihova primenljivost za detekciju napada koji nisu razmatrani pri određivanju pragova upitna.

Pored toga, za razliku od ostalih istraživanja u oblasti koja se nisu bavila implementacijom i eksperimentalnom verifikacijom razvijenih IDS u realnim sistemima, u okviru MISSION4.0 razvijeni IDS su implementirani na opisanom elektropneumatskom sistemu za pozicioniranje [27]. IDS zasnovani na LSTM RNN i CNN su uspešno detektovali lansirane napade kao što je prikazano na slici 6. Iako je po prirodi uvela dodatno kašnjenje u algoritam upravljanja, implementacija IDS nije imala negativne posledice na sveukupan rad sistema.

Iz navedenih razmatranja očigledno je da implementacija DNN u razvoju IDS zahteva veliku količinu podataka dobijenih iz sistema prilikom njegovog normalnog funkcionisanja. Ukoliko se radi o ustaljenim proizvodnim procesima, prikupljanje podataka ne bi trebalo da predstavlja problem, ali u slučaju česte rekonfiguracije sistema ono može predstavljati izazov. Proširivanje podataka (engl. *Data Augmentation*) predstavlja jedan od načina za rešavanje ovog problema. U okviru MISSION4.0 projekta generativne suparničke mreže – GAN (engl. *Generative Adversarial Networks*) su uspešno primenjene za generisanje količine podataka neophodne za razvoj DNN zasnovanih IDS na osnovu relativno malog broja uzoraka na ulazu [28].



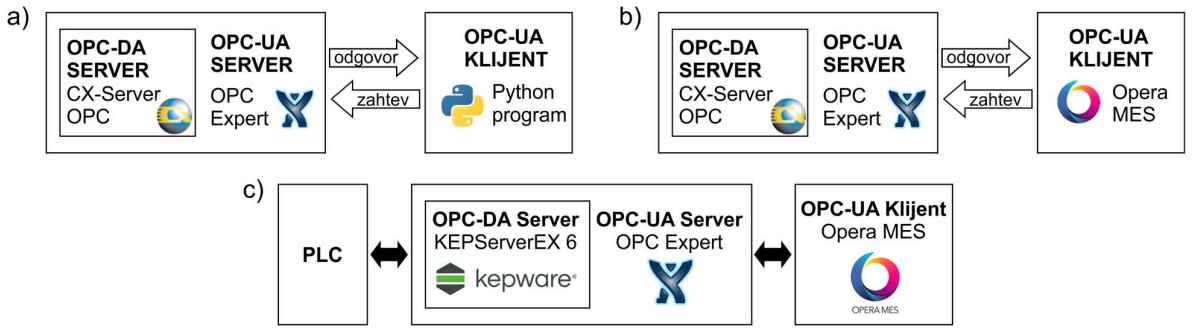
Slika 6. *Napadi detektovani na realnom elektropneumatskom sistemu za pozicioniranje korišćenjem IDS zasnovanog na: a) LSTM RNN; b) CNN; Trenutak napada je označen isprekidanom crvenom, a trenutak njegovog prepoznavanja isprekidanom zelenom linijom*

3. PRIMENA OPC-UA ZA RAZMENU PODATAKA IZMEĐU UREĐAJA U OKVIRU ICS

Jedan od ključnih problema u implementaciji IIoT predstavlja interoperabilnost opreme različitih proizvođača prilikom njenog povezivanja u jedinstven sistem. OPC-UA predstavlja namenski kreiran standard čiji je cilj da obezbedi jednostavnu, pouzdanu i sigurnu komunikaciju između različitih uređaja u okviru ICS [29]. Njega je razvila OPC fondacija koja predstavlja konzorcijum proizvođača i krajnjih korisnika opreme i softvera za industrijsku automatizaciju, a standardizovan je kroz IEC 62541. Razmena poruka u okviru OPC-UA vrši se korišćenjem jednog od dva moguća pristupa – klijent/server (engl. *Client/Server*) ili objava/pretplata (engl. *Publish/Subscribe*). OPC-UA je zasnovan na servisno orijentisanoj arhitekturi u okviru koje server stavlja na raspolaganje klijentu unapred definisan skup servisa. Interoperbilnost se ostvaruje tako što se zajedno sa podacima razmenjuje i njihov meta model koji je definisan u adresnom prostoru servera.

U okviru projekta MISSION4.0 kao osnova za izučavanje kibernetskih napada na njih izvršen je razvoj određenih sistema upravljanja u okviru kojih je komunikacija između uređaja vršena korišćenjem OPC-UA. Jedan od sistema odnosio se na integraciju inteligentnog senzora za određivanje orijentacije dela i manipulatora koji je upravljan programabilim kontrolerom – PLC-om (engl. *Programmable Logic Controller*) *Omron* CP1L-EM40DT-D. Inteligentan senzor zasnovan je na kameri *Cognex Insight* 2000-120 proširenoj kontrolerom *RaspberryPi* Model B. Zadatak upravljanja, koji se odnosio na manipulaciju dela u dva položaja u zavisnosti od njegove orijentacije, distribuiran je između PLC-a i *RaspberryPi* uređaja na sledeći način [30]. Korišćenjem namenskog algoritma zasnovanog na konvolucionim neuronskim mrežama [31] koji

implementiran u okviru programskog jezika *Python*, *RaspberryPi* određuje orijentaciju dela i šalje binarnu informaciju o njoj programabilnom kontroleru koji na odgovarajući način vrši pokretanje manipulatora. Komunikacija između inteligentnog senzora i PLC-a vrši se korišćenjem OPC-UA koji obezbeđuje interoperbilnost uređaja zasnovanih na potpuno različitim hardverskim komponentama. U ovoj konfiguraciji na strani PLC-a je podignut OPC-UA server, dok je u okviru programa za detekciju orijentacije dela realizovanom u *Python*-u uspostavljen OPC-UA klijent. Imajući u vidu da je za korišćeni PLC na raspolaganju bila softverska podrška samo za OPC-DA (engl. *Data Access*) server starije generacije, bilo je potrebno izvršiti njegovo upakivanje korišćenjem OPC-UA *wrapper*-a – u ovom slučaju upotrebljen je OPC *Expert* (slika 7a).



Slika 7. *OPC-UA klijent/server arhitektura za komunikaciju između: a) PLC-a Omron CP1L-EM40DT-D i RaspberryPi [30]; b) PLC-a Omron CPM1-10CDR-A* i *OperaMES [32]; c) PLC-a Mitsubishi iQ-F FX5UC i OperaMES [33]*

Za prikupljanje podataka iz proizvodnih pogona i lansiranje proizvodnje u skladu sa dinamički definisanim planovima koji su bili u fokusu radnog paketa Dinamičko planiranje i terminiranje kibernetsko fizičkih proizvodnih sistema (engl. *Dynamic process planning and scheduling of Cyber-Physical Production Systems*) u okviru projekta MISSION4.0, izuzetno značajnu ulogu imaju sistemi za izvršavanje proizvodnje – MES (engl. *Manufacturing Execution Systems*). Puna implementacija ovih sistema podrazumeva automatsku razmenu podataka između MES i uređaja koji funkcionišu unutar ICS koja se može ostvariti samo uz njihovu potpunu interoperabilnost. U tom kontekstu, u okviru projekta MISSION4.0 izvršene su određene razvojne aktivnosti koje su se odnosile na povezivanje sistema za izvršavanje proizvodnje *OperaMES* sa PLC-ovima korišćenjem OPC-UA. Konkretno, povezani su PLC-ovi *Omron* CPM1-10CDR-A i PLC *Mitsubishi* iQ-F FX5UC korišćenjem klijent/server arhitekture prikazane na slikama 7b i 7c u okviru koje su OPC-UA serveri podignuti na strani PLC-ova, dok je *OperaMES* imala ulogu OPC-UA klijenta. Detalji vezani za ove aktivnosti kao i njihovi rezultati dati su u radovima [32, 33].

4. EDUKACIJA INŽENJERA U OBLASTIMA CPS, IIOT I SAJBER BEZBEDNOSTI

Jedan od izuzetno značajnih elemenata projekta MISSION4.0 predstavljala je diseminacija njegovih rezultata koja je obuhvatala ne samo naučnu i stručnu javnost, već i opštu populaciju. Sajber bezbednost u okviru ICS predstavlja novu naučnoistraživačku i inženjersku oblast koja je zamah dobila tek od 2010. godine nakon Stuxnet napada na iransko nuklearno postrojenje [34]. Imajući u vidu da će implementacija ove oblasti u inženjerskoj praksi tek dobiti zamah u narednom periodu s jedne, kao i posledica do kojih njeno zanemarivanje može dovesti u proizvodnim preduzećima s druge strane, posebna pažnja mora biti usmerena na edukaciju nove generacije inženjera sposobnih da implementiraju bezbednosne mehanizme u okviru ICS. U tom kontekstu, izuzetni napori su usmereni na integraciju rezultata projekta MISSION4.0 u kurikulume odgovarajućih predmeta na master akademskim studijama.

Projekat MISSION4.0 je u tom smislu imao izuzetno povoljnu okolnost – paralelno sa izvršavanjem ovog projekta, na Univerzitetu u Beogradu – Mašinskom fakultetu započeta je implementacija novog Studijskog programa master akademskih studija – Industrija 4.0 [35] na kome je prva generacija studenata upisana školske 2020/21. godine. Kurikulum navedenog studijskog programa obuhvata i predmete Kibernetsko fizički sistemi i Industrijski internet stvari i sajber bezbednost koji su u svojoj osnovi bili pogodni za integraciju rezultata projekta MISSION4.0 i njihovu diseminaciju ka studentskoj populaciji, a dalje, nakon njihovog zapošljavanja, i ka industriji Republike Srbije.

U okviru ovih predmeta uvedene su sledeće nastavne celine:

- Ciljevi sistema za zaštitu od kibernetskih napada,
- Vrste kibernetskih napada u ICS,
- Metode zaštite ICS od kibernetskih napada,
- Koncept dubinske odbrane,
- IDS u okviru sistema sa kontinualnim upravljanjem,
- Otvorena platforma za komunikaciju – OPC-UA standard

u koje su direktno integrisani rezultati projekta MISSION4.0.

Iskustva stečena u razvoju kurikuluma navedenih predmeta i edukaciji studenata podeljena su i sa širom javnosti u okviru rada [36] sa ciljem da se navedene oblasti i rezultati istraživanja u okviru projekta MISSION4.0 što jednostavnije uključe i u kurikulume studijskih programa na drugim visokoškolskim institucijama.

5. ZAKLJUČAK

U ovom radu prikazan je pregled rezultata istraživanja sprovedenih u okviru radnog paketa Sajber bezbednost u kontinualnim sistemima upravljanja na projektu MISSION4.0. Na osnovu datog pregleda može se zaključiti da su najznačajniji rezultati ovog radnog paketa:

1. Razvoj i eksperimentalna verifikacija na realnoj platformi nove metodologije za potpuno automatsko generisanje sistema za detekciju napada na distribuirane sisteme za kontinualno upravljanje proizvodnim resursima koji su zasnovani na metodama dubokog učenja i čije su karakteristike mala proračunska komplesnost, primenljivost na proračunski i energetski ograničenim hardverskim resursima u okviru ICS, visoka efektivnost i rad u realnom vremenu bez značajnih posledica na funkcionalnost sistema u kome su implementirani;
2. Stvaranje preduslova za automatsku implementaciju planova proizvodnje generisanih tehnikama razvijenim u okviru radnog paketa Dinamičko planiranje i terminiranje kibernetsko fizičkih proizvodnih sistema kroz ostvarivanje interoperabilnosti uređaja u okviru ICS korišćenjem OPC-UA;
3. Sveobuhvatna diseminacija rezultata istraživanja ka naučnoj i stručnoj javnosti, kao i edukacija nove generacije inženjera u oblasti sajber bezbednosti u ICS.

Detalji sprovedenih istraživanja mogu se pronaći u objavljenim radovima i to u 5 radova u naučnim časopisima [6, 7, 9, 12, 37], jednom poglavlju u tematskom zborniku vodećeg međunarodnog značaja [36] i devet radova saopštenih na međunarodnim i domaćim konferencijama [4, 23, 27, 28, 30, 31, 32, 33].

U narednom periodu će rezultati i iskustva stečena na ovom projektu poslužiti kao osnova za nastavak istraživanja u oblasti sajber bezbednosti u okviru industrijskih sistema upravljanja pri čemu će umesto kontinualnih sistema upravljanja u fokusu biti neki drugi elementi ICS.

6. LITERATURA

[1] Fond za nauku Republike Srbije, http://fondzanauku.gov.rs, datum pristupa: 19.08.2022.

[2] Kagermann, H., Wahlster, W., Helbig, J.: *Recommendations for Implementing Strategic Initiative INDUSTRIE 4.0*, Acatech, Germany, 2013.

[3] IEC 62264: *Enterprise-control system integration.* International Electrotechnical Commission,2013-2020, https://webstore.iec.ch/publication/59706, datum pristupa: 19.08.2022.

[4] Jakovljević, Ž., Nedeljković, D.: *Distribution of Control Tasks to Smart Devices in Industrial Control Systems: a Case Study*, 8th International Conference on Electrical, Electronics and Computing Engineering (IcETRAN 2021), pp. 585-590, Bijeljina, B&H, 2021.

[5] Jakovljevic, Z., Lesi, V., Pajic, M.: *Attacks on distributed sequential control in manufacturing automation,* IEEE Transactions on Industrial Informatics, Vol. 17, No. 2, pp.775-786, 2020.

[6] Lesi, V., Jakovljevic, Z., Pajic, M.: *Security analysis for distributed IoT-based industrial automation*, IEEE Transactions on Automation Science and Engineering, 2021, doi: 10.1109/TASE.2021.3106335

[7] Markovic, V., Jakovljevic, Z., Budak, I.: *Automatic recognition of cylinders and planes from unstructured point clouds*, The Visual Computer, pp.1-24, 2021, doi: 10.1007/s00371-021-02299-9

[8] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A.: *Guide to industrial control systems (ICS) security*, 2015.

[9] Nedeljkovic, D., Jakovljevic, Z.: *CNN based method for the development of cyber-attacks detection algorithms in industrial control systems*, Computers & Security, Vol. 114, Article 102585, 2022.

[10] Umer, M. A., Mathur, A., Junejo, K. N., Adepu, S.: *Integrating Design and Data Centric Approaches*

to Generate Invariants for Distributed Attack Detection, Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and Privacy, pp. 131–136, ACM, Dallas, USA, 2017.

[11] Goh, J., Adepu, S., Junejo, K.N., Mathur, A.: *A dataset to support research in the design of secure water treatment systems,* International Conference on Critical Information Infrastructures Security, Springer, Paris, France, pp. 88–99, 2016.

[12] Nedeljković, D., Jakovljević, Ž., Miljković, Z., Pajić, M.: *Detection of cyber-attacks in systems with distributed control based on support vector regression*, Telfor Journal, Vol. 12, No. 2, pp. 104-109, 2020.

[13] Nedeljkovic, D., Jakovljevic, Z.: *New datasets obtained from experimental installations with centralized control*, [Data set]. Zenodo, http://doi.org/10.5281/zenodo.5514351, 2021.

[14] Das, T., Adepu, S., Zhou, J.: *Anomaly detection in industrial control systems using logical analysis of data*, Computers & Security, Vol. 96, Article 101935, 2020.

[15] Elnour, M., Meskin, N., Khan, K.: *Hybrid attack detection framework for industrial control systems using 1D-convolutional neural network and isolation forest*, 4th IEEE Conference on Control Technology and Applications (CCTA 2020), pp. 877–884, IEEE, Montreal, Canada, 2020.

[16] Elnour, M., Meskin, N., Khan, K., Jain, R.: *A dual-isolation-forests-based attack detection framework for industrial control systems*, IEEE Access, Vol. 8, pp. 36639-36651, 2020.

[17] Inoue, J., Yamagata, Y., Chen, Y., Poskitt, C. M., Sun, J.:*Anomaly detection for a water treatment system using unsupervised machine learning*, 2017 IEEE International Conference on Data Mining Workshops (ICDMW), pp. 1058-1065, IEEE,New Orleans, USA, 2017.

[18] Kravchik, M., Shabtai, A.: *Efficient cyber attack detection in industrial control systems using lightweight neural networks and pca*, IEEE Transactions on Dependable and Secure Computing, 2021, doi: 10.1109/TDSC.2021.3050101

[19] Priyanga, S., Krithivasan, K., Pravinraj, S., Shankar, S.:*Detection of Cyberattacks in Industrial Control Systems Using Enhanced Principal Component Analysis and Hypergraph-Based Convolution Neural Network (EPCA-HG-CNN)*, IEEE Transactions on Industry Applications, Vol. 56, pp. 4394-4404, 2020.

[20] Sapkota, S., Mehdy, A., Reese, S., Mehrpouyan, H.:*Falcon: Framework for anomaly detection in industrial control systems,* Electronics, Vol. 9, No. 8, pp. 1-20, 2020.

[21] Elman, J.: *Finding Structure in Time*, Cognitive Science, Vol. 14, No. 2,pp. 179-211, 1990.

[22] Hochreiter, S., Schmidhuber, J.: *Long short-term memory*, Neural Computation, Vol. 9, No. 8, pp. 1735–1780, 1997.

[23] Nedeljković, D., Jakovljević, Ž.: *Cyber-attack detection method based on RNN*, 7th International Conference on Electrical, Electronics and Computing Engineering (IcETRAN 2020), pp. 726-731, Belgrade, Serbia, 2020.

[24] Kravchik, M., Shabtai, A.: *Detecting cyber attacks in industrial control systems using convolutional neural networks*, Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy, pp. 72-83, ACM, Toronto, Canada, 2018.

[25] Raman MR, G., Somu, N., Mathur, A.: *A multilayer perceptron model for anomaly detection in water treatment plants*, International Journal of Critical Infrastructure Protection, Vol. 31, Article 100393, 2020.

[26] Goh, J., Adepu, S., Tan, M., Lee, Z. S.: *Anomaly detection in cyber physical systems using recurrent neural networks*, 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE), pp. 140-145, IEEE, Singapore, 2017.

[27] Nedeljković, D., Jakovljević, Ž.: *Implementation of CNN based algorithm for cyber-attacks detection on a real-world control system*, 14th International Scientific Conference MMA 2021 – Flexible Technologies, pp. 119-122, Novi Sad, Serbia, 2021.

[28] Nedeljković, D., Jakovljević, Ž.: *GAN-based Data Augmentation in the Design of Cyber-attack Detection Methods*, 9th International Conference on Electrical, Electronics and Computing Engineering (IcETRAN 2022), pp. 669-674, Novi Pazar, Serbia, 2022.

[29] OPC foundation -The Industrial Interoperability Standard, https://opcfoundation.org/, datum pristupa: 19.08.2022.

[30] Nedeljković, D., Jakovljević, Ž.: *Integration of Smart Vision Sensor into Manipulator Control System using OPC-UA*, 28th Telecommunications Forum (TELFOR 2020), Article 4734, Belgrade, Serbia, 2020.

[31] Nedeljković, D., Jakovljević, Ž., Miljković, Z.: *Klasifikacija slike zasnovana na primeni konvolucionih neuronskih mreža*, 42. JUPITER konferencija, str. 4.13-4.23, Beograd, Srbija, 2020.

[32] Jakovljević, Ž., Nedeljković, D., Ševarlić, F., Puzović, R.: *Komunikacija između proizvodnih resursa korišćenjem OPC-UA standarda*, 42. JUPITER konferencija, str. 4.1-4.12, Beograd, Srbija, 2020.
[33] Nedeljković, D., Stanojević, S., Puzović, R., Jakovljević, Ž.: *Integracija proizvodnih resursa u sistem za izvršavanje proizvodnje korišćenjem OPC-UA*, 13. ETIKUM konferencija, str. 65-68, Novi Sad, Srbija, 2021.
[34] Bakić, B., Milić, M., Antović, I., Savić, D., Stojanović, T.: *10 years since Stuxnet: What have we learned from this mysterious computer software worm?*, 25th International Conference on Information Technology (IT), pp. 1-4, IEEE, Žabljak, Montenegro, 2021.
[35] Master akademske studije INDUSTRIJA 4.0, http://i40.mas.bg.ac.rs/, datum pristupa: 19.08.2022.
[36] Jakovljević, Ž., Nedeljković, D.: *Cyber Physical Systems in Manufacturing Engineers Education*, 11th International Conference on Machine and Industrial Design in Mechanical Engineering, Series Mechanisms and Machine Science - Machine and Industrial Design in Mechanical Engineering (Proceedings of KOD 2021), Springer,2021, doi: 10.1007/978-3-030-88465-9
[37] Lesi, V., Jakovljevic, Z., Pajic, M.: *IoT-Enabled Motion Control: Architectural Design Challenges and Solutions*, IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2022.3202175, 2022

Jakovljević, Ž., Nedeljković, D.

CYBER SECURITY IN CONTINUOUS-TIME CONTROLLED SYSTEMS – OVERVIEW OF THE RESULTS WITHIN THE PROJECT OF MISSION4.0

Abstract: *This paper presents the research results conducted within the project Deep Machine Learning and Swarm Intelligence-based Optimization Algorithms for Control and Scheduling of Cyber-Physical Systems in Industry 4.0, funded by the Science Fund of the Republic of Serbia in the period 2020-2022. The shown results refer to the field of cyber security in continuous-time controlled systems as one of the work packages of the MISSION4.0 project. Accordingly, the research directions were related to developing algorithms for attack detection in Industrial Control Systems with centralized and distributed architecture, as well as the application of an open platform communication to securely exchange the data between the multi-vendor devices. In addition, the achieved results and their integration into lectures and laboratory exercises served as a basis for the education of engineers in cyber-physical systems, Industrial Internet of Things, and cyber security.*
Key words: *cyber security, attack detection, OPC-UA, engineers education*