https://doi.org/10.37528/FTTE/9788673954455/POSTEL.2021.020

DINAMIČKA PROCENA BEZBEDNOSNOG RIZIKA U INDUSTRIJSKIM IoT SISTEMIMA

Mirjana D. Stojanović[1], Jasna D. Marković-Petrović[2]
[1]Univerzitet u Beogradu - Saobraćajni fakultet, m.stojanovic@sf.bg.ac.rs
[2]JP EPS Beograd, jasna.markovic-petrovic@eps.rs

Rezime: *Predmet ovog rada je dinamička procena bezbednosnog rizika u IIoT (Industrial Internet of Things) sistemima. Prikazane su klasifikacije sajber napada na IIoT sisteme, a zatim su opisani principi procene bezbednosnog rizika u industrijskim sistemima daljinskog upravljanja. Sledi prikaz modela i metoda dinamičke procene bezbednosnog rizika u industrijskim IoT sistemima, sa naglaskom na primenljivost metoda mašinskog učenja za tu svrhu.*

Ključne reči: *Bezbednosni rizik, dinamička procena, IIoT, mašinsko učenje*

1. Uvod

Industrijski Internet stvari (*Industrial Internet of Things*, IIoT) je model senzora, aktuatora i drugih industrijskih uređaja, povezanih na Internet i umreženih sa industrijskim aplikacijama. Važno svojstvo IIoT sistema je konvergencija operativnih i informacionih tehnologija, koja se ogleda u umrežavanju operativnih procesa i industrijskih sistema daljinskog upravljanja (*Industrial Control Systems*, ICSs). IIoT podrazumeva potpunu digitalizaciju proizvodnih pogona, visok stepen integracije sistema u smislu automatizacije i optimizacije rada, kao i fleksibilnost lanaca snabdevanja i logistike. IIoT je glavni gradivni blok programa Industrija 4.0, a primenjuje se u energetici, petrohemijskoj industriji, saobraćaju i transportu, poljoprivredi i prehrambenoj industriji, zdravstvu, sistemima specijalne namene, bankarstvu, vladinim ustanovama i dr.

Bezbednost i zaštita privatnosti su kritični faktori za masovnu implementaciju IIoT koncepta, a predmet ovog rada je procena bezbednosnog rizika u IIoT sistemima. Nedavna istraživanja pokazuju da IIoT okruženje zahteva dinamičku procenu bezbednosnog rizika, što znači da se ona vrši *online*, u realnom vremenu [1].

Rad je organizovan na sledeći način. U drugom poglavlju razmatrani su sajber napadi na IIoT sisteme, sa naglaskom na različite klasifikacije napada. Treće poglavlje sadrži prikaz standarda i metodologije za procenu bezbednosnog rizika u industrijskim sistemima daljinskog upravljanja. U četvrtom poglavlju predstavljen je model dinamičke procene bezbednosnog rizika u IIoT sistemima i princip integracije softvera za procenu rizika sa sistemom zaštite. U petom poglavlju prikazani su metodi za dinamičku procenu

bezbednosnog rizika u IIoT sistemima, sa naglaskom na prednosti metoda mašinskog učenja za tu svrhu. Šesto poglavlje sadrži zaključna razmatranja.

2. Sajber napadi na IIoT sisteme

Pored operativnih problema povezanih sa konkretnim industrijskim procesom, sajber napadi na IIoT sistem mogu da privremeno ili trajno ugroze zdravlje i živote ljudi, kao i životnu sredinu i imovinu. Glavni bezbednosni rizici obuhvataju: nedostatak autentifikacije i zaštite u senzorima i drugim sajber-fizičkim uređajima; nebezbedne gejtveje preko kojih se podaci šalju u *cloud*; bezbednosne probleme *cloud* infrastrukture i nebezbedne telekomunikacione protokole.

Specifične pretnje industrijskim IoT sistemima su: napredne perzistentne pretnje (*Advanced Persistent Threats*, APT), odsustvo mehanizama za zaštitu integriteta podataka, MITM (*Man-in-the-Middle*) napadi, krađa identiteta, prisluškivanje (*eavesdropping*), napadi ponavljanjem i različiti oblici napada koji prouzrokuju odbijanje servisa (*Denial of Service*, DoS). U literaturi postoje različite klasifikacije sajber napada na IIoT sisteme, a detaljna analiza napada i različitih načina njihove podele može se pronaći u [2].

Klasifikacija predložena u [3] obuhvata četiri dimenzije: vektor, cilj, uticaj i posledice, koje su podeljene u dve grupe – sajber i fizičke. Ovakvom klasifikacijom omogućena je diferencijacija napada na operativno i informaciono okruženje industrijskog sistema. U [4], napadi na IIoT sisteme klasifikovani su u pet generičkih kategorija: prevara (*phishing*), *ransomware*, napadi na protokole, napadi na lance snabdevanja i sistemski napadi. Takva klasifikacija omogućuje razumevanje bezbednosnih rizika i pridruženih mera za ublažavanje rizika u IIoT okruženju.

Troslojna klasifikacija napada na IIoT, predložena u [5], pretpostavlja da su svakom sloju pridružene određene dimenzije i karakteristike, kao što je prikazano u tabeli 1. Prvi sloj (modus operandi) identifikuje ulazne tačke i metode izvršavanja napada, a napadi su klasifikovani prema tehnici, mehanizmu, načinu izvršavanja i fokusu. Drugi sloj sagledava cilj napada, koje klasifikuje prema ranjivosti sistema i odgovarajućem IIoT sloju. Treći sloj razmatra uticaj realizovanog napada u aspektima obima i posledica.

Tabela 1. Troslojna klasifikacija napada na IIoT sisteme [5]

Sloj	**Dimenzija**	**Karakteristika**
Modus operandi	Tehnika	Fizički/logički
	Mehanizam	Aktivan/pasivan
	Izvršavanje	Samostalan/povezan
	Fokus	Neusmeren/usmeren
Cilj	Ranjivost	Tehnička/socijalna
	IIoT sloj	Fizički/mrežni/aplikacioni
Uticaj	Obim	Sajber/sajber-fizički
	Posledica	Otkrivanje/prevara/prekid/uzurpacija

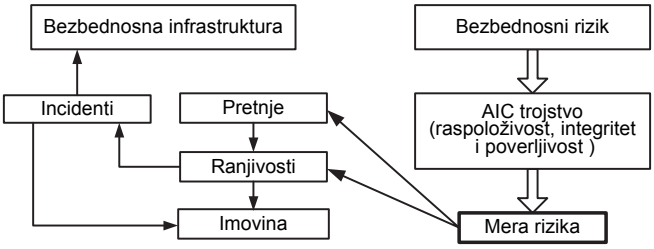
3. Procena bezbednosnog rizika u industrijskim sistemima daljinskog upravljanja

Prema ISO (*International Organization for Standardization*) standardu 31000:2018 [6], procena rizika predstavlja ključni element procesa upravljanja rizikom, a

obuhvata identifikaciju, analizu i evaluaciju rizika. Procena rizika izvršava se u sledećim koracima: (1) identifikacija izvora rizika i mogućih posledica, (2) analiza verovatnoće i uticaja rizika, i (3) evaluacija sa ciljem utvrđivanja akcija koje treba preduzeti za ublažavanje rizika. IEC (*International Electrotechnical Commission*) standard 31010:2019 (zajednički standard sa ISO) sadrži uputstvo za izbor i primenu tehnika za procenu rizika u širokom rasponu različitih situacija [7].

U kontekstu bezbednosti ICS sistema, U.S. NIST (*National Institute of Standards and Technology*) definiše procenu rizika kao „proces identifikacije rizika po proizvodnju, imovinu ili osoblje određivanjem verovatnoće pojave, rezultujućeg uticaja i mehanizama zaštite kojima će taj uticaj biti ublažen“ [8]. Industrijski Internet konzorcijum (IIC) opisuje procenu rizika u kontekstu ukupnih politika i mera zaštite, a naglašava neophodnost adaptacije na kontinuirane promene pretnji i sajber napada, kao i odziva kojim će biti minimiziran uticaj na funkcionisanje IIoT sistema i omogućena kooperacija različitih organizacija sa ciljem rane identifikacije bezbednosnih pretnji [9].

Na slici 1 ilustrovan je proces upravljanja bezbednosnim rizikom ICS sistema. U informacionim i komunikacionim sistemima opšte namene cilj je da se realizuje uravnotežena zaštita poverljivosti, integriteta i raspoloživosti informacija, što je poznato i pod nazivom CIA (*Confidentiality, Integrity, Availability*) trojstvo, u kome poverljivost podataka ima najviši prioritet. Zaštita ICS sistema pretpostavlja isto trojstvo, ali sa obrnutim redosledom prioriteta (AIC), što znači da je najvažnija raspoloživost sistema. Ta razlika je od suštinskog značaja za definisanje bezbednosnih politika i pridruženih mehanizama zaštite, sa prvenstvenim ciljem da se raspoloživost svih sistema koji konstituišu kritičnu infrastrukturu održava po principu 24/7. Bezbednosne pretnje koriste ranjivosti sistema da izazovu incidente, koji mogu da ugroze zdravlje i živote ljudi, da prouzrokuju oštećenje imovine, kao i da utiču na celokupnu bezbednosnu infrastrukturu. Prema tome, mera rizika određuje se kombinovanjem uticaja pretnji, ranjivosti i potencijalnih posledica [10].



Slika 1. Ilustracija procesa procene bezbednosnog rizika u ICS

Određivanje bezbednosnog rizika vrši se kvalitativno i/ili kvantitativno. Kvalitativna mera rizika subjektivno interpretira potencijalne gubitke, na primer nizak, srednji i visok rizik. Primeri metoda za kvalitativnu procenu rizika su: stručna procena, procene rejtinga, kontrolne liste izvora rizika, metod analogija i dr.

Kvantitativna mera rizika dobija se odgovarajućim matematičkim aparatom, pomoću koga se rizik izražava kao numerička vrednost u funkciji verovatnoće i posledica. Uobičajeno je da se mera rizika zasniva na ekonomskim kategorijama, kao što su očekivani godišnji gubitak (*Annualized Loss Expectancy*, ALE) i povrat investicija (*Return on Investment*, ROI). Međutim, investicija u sajber bezbednost po pravilu ne mora da rezultuje

profitom, već se dobitak ogleda u smanjenju rizika koji prete da ugroze određena dobra. Iz tog razloga uvedena je mera povrata investicija u bezbednost (*Return on Security Investment*, ROSI) za kvantifikaciju gubitaka koji su izbegnuti zahvaljujući preventivnim ulaganjima u bezbednost [11]. Kvantitativni metodi za procenu rizika mogu se klasifikovati u tri osnovne kategorije: (1) analitički metodi kao što su: analiza osetljivosti, analiza scenarija, metod diskontnih stopa prilagođenih riziku; (2) probabilistički teorijski metodi koji se zasnivaju na simulaciji, teoriji igara ili konstrukciji stabla, i (3) nekonvencionalni metodi, među kojima su najpoznatiji metodi zasnovani na fazi logici ili na mašinskom učenju [12].

Hibridni metodi kombinuju prethodno opisane pristupe, na primer, stručnu procenu sa nekim od kvantitativnih metoda [13], [14]. Sistematičan pregled metoda za procenu bezbednosnog rizika u ICS sistemima koji koriste tradicionalne Internet tehnologije može se pronaći u [15] i [16].

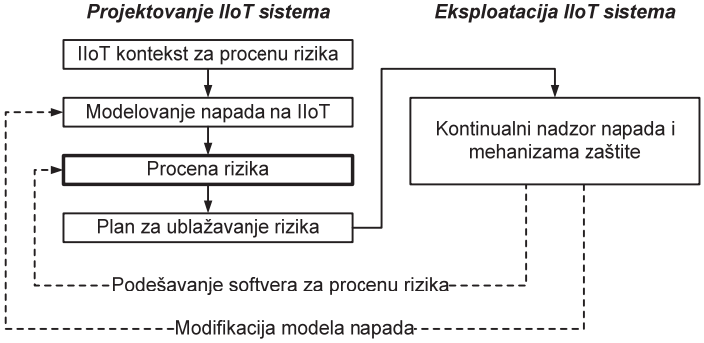
4. Model dinamičke procene bezbednosnog rizika u industrijskim IoT sistemima

Dinamička (kontinualna) procena rizika zasniva se na podacima koji se prikupljaju i procesiraju u realnom vremenu, a obuhvata tri osnovne komponente: upravljanje imovinom, modelovanje napada i proračun rizika [17]. Upravljanje imovinom bavi se vrstama materijalnih dobara (uređaji, komunikacioni linkovi, hardver, softver), njihovim performansama (uključujući i promene, kao što su nadgradnja i ažuriranje) i procenom značaja u smislu uticaja na AIC trojstvo, kritičnost, osetljivost i troškove zaštite. Za modelovanje napada koristi se veliki broj tehnika među kojima se izdvajaju: skriveni Markovljevi modeli, tehnike zasnovane na grafovima, hijerarhijsko modelovanje formiranjem stabla napada, klasterovanje, fazi logika i dr. Proračun rizika uzima u obzir verovatnoću (učestanost) i uticaj svih mogućih napada, a način proračuna može zavisiti od načina modelovanja napada. Ažuriranje mere rizika može se vršiti kontinualno ili periodično (u unapred definisanim intervalima vremena), a mera rizika izražava se kvalitativno ili kvantitativno.

Pri proceni bezbednosnog rizika u IIoT sistemu neophodno je da se prvo identifikuje kontekst, u zavisnosti od „viđenja" rizika i aktera (entiteta) [18]. Postoje različita viđenja rizika za proizvođače senzora i aktuatora; za platforme, aplikacije i ICS sisteme; za korisnike (industrija, zdravstvo, pametni gradovi), ili za integratore sistema, provajdere servisa i krajnje korisnike. Primeri aktera/entiteta su ljudi, hardver, softver, komunikacija i *cloud* infrastruktura, a oni su osnov za određivanje toka podataka. Identifikacija konteksta neophodna je iz dva razloga. Prvo, u IIoT sistemu je moguća multiplikacija tačaka sajber-fizičkog napada usled integracije senzora, aktuatora, platformi, aplikacija i korisnika. To znači da napad izvršen u jednoj ulaznoj tački može uticati na ceo sistem. Drugo, isti objekat može se koristiti u različitim IIoT kontekstima, koji zahtevaju različite nivoe bezbednosti u zavisnosti od konkretnih faktora rizika.

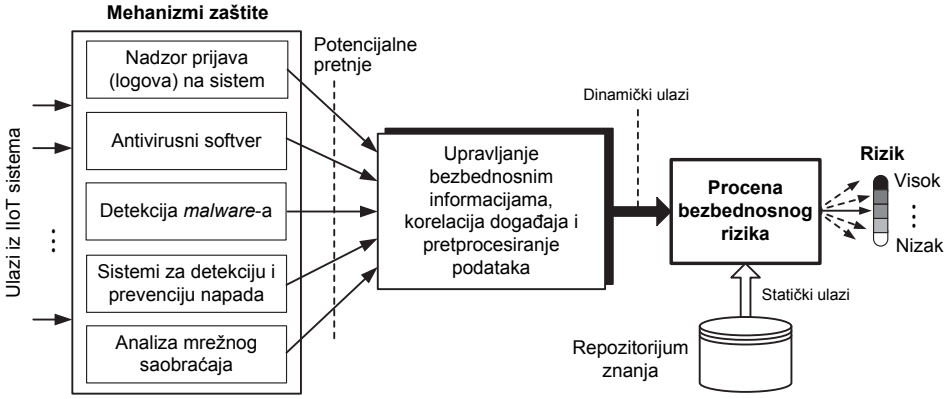
Dinamička procena rizika u IIoT sistemu obuhvata dve faze [19], koje su ilustrovane na slici 2: identifikacija i početna evaluacija rizika u procesu projektovanja sistema, kao i kontinualni nadzor i ponovna procena rizika tokom eksploatacije sistema. Faza projektovanja počinje identifikacijom konteksta za procenu rizika, posle koje se vrši modelovanje napada da bi se obezbedili dinamički ulazi za proces procene rizika. Izlaz tog procesa je kvalitativna ili kvantitativna mera rizika, koja je osnov za definisanje plana za ublažavanje rizika i izbor odgovarajućih mehanizama zaštite. U fazi eksploatacije IIoT

sistema vrši se kontinualan nadzor napada i mehanizama zaštite, koji pruža povratne informacije za modifikaciju modela napada i za podešavanje softvera za procenu rizika.



Slika 2. Model dinamičke procene bezbednosnog rizika u IIoT sistemu

Princip integracije softvera za dinamičku procenu rizika sa sistemom zaštite prikazan je na slici 3. U IIoT sistemu distribuirani su različiti mehanizmi zaštite kao što su: nadzor prijava na sistem, antivirusni softver, softver za detekciju *malware*-a, sistemi za detekciju i prevenciju napada, analizatori mrežnog saobraćaja i dr. Oni, u realnom vremenu, procesiraju ulaze iz IIoT sistema i generišu obaveštenja o potencijalnim pretnjama, anomalijama i sumnjivim događajima. Ta obaveštenja procesiraju se u modulu koji je zadužen za upravljanje bezbednosnim informacijama i korelisanje događaja (*Security Information and Event Management*, SIEM). Ovaj modul vrši pretprocesiranje podataka kako bi generisao dinamičke ulaze za procenu rizika. Pored dinamičkih parametara, modul za procenu rizika uzima u obzir i statičke parametre iz repozitorijuma znanja, a to su politike zaštite, registar imovine, podaci o prethodnim incidentima i dr.



Slika 3. Princip integracije softvera za procenu rizika sa sistemom zaštite

5. Metodi za dinamičku procenu bezbednosnog rizika u IIoT sistemima

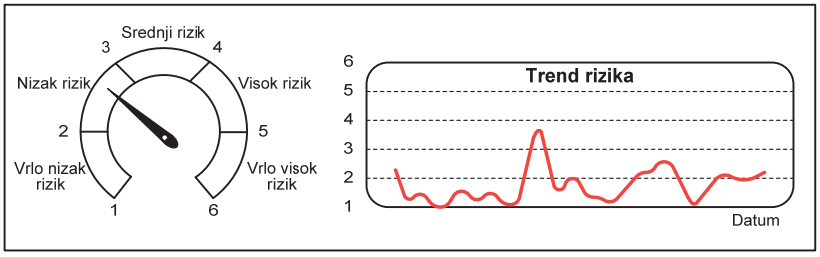
U ovom poglavlju prikazan je pregled tradicionalnih metoda i metoda mašinskog učenja, koji se mogu primeniti za dinamičku procenu bezbednosnog rizika u industrijskim IoT sistemima.

5.1. Pregled tradicionalnih metoda

DRA (*Dynamic Risk Assessment*) metod, opisan u [20], integriše Bajesov metod sa ocenom posledica, a dinamička komponenta ogleda se u analizi incidenata i ažuriranju verovatnoća. Analiza incidenta koristi stablo događaj/otkaz i podatke u realnom vremenu za estimaciju verovatnoća događaja. Zatim se te verovatnoće mogu ažurirati Bajesovim zaključivanjem, korišćenjem svih raspoloživih informacija i novih podataka. Ažurirane verovatnoće se iterativno koriste za ponovnu estimaciju profila rizika. Efikasnost metoda potvrđena je studijama slučaja u rafineriji nafte i podmorskim bušotinama.

DyPASI (*Dynamic Procedure for Atypical Scenarios Identification*) je iterativan metod, predložen u [21], koji obuhvata: identifikaciju incidentnih scenarija pomoću tzv. analize „leptir mašne“ (*bow-tie*), kontinualnu akviziciju i sistematski skrining rizika od neotkrivenih opasnosti, kao i definisanje mera zaštite. Efikasnost metoda verifikovana je na realnim primerima procene rizika u termoelektrani i u petrohemijskoj industriji.

Cilj metoda barometra rizika, predloženog u [22], je kontinuiran nadzor i grafički prikaz rizika kao podrška odlučivanju na dnevnom nivou, a razvijen je za potrebe norveške petrohemijske industrije. Metod uvodi faktore koji utiču na rizik (*Risk Influencing Factors*, RIFs). Zatim se uvode indikatori za dinamičku ocenu stanja RIF faktora, koji se zasnivaju na podacima prikupljenim u realnom vremenu. Na slici 4 prikazana je vizuelizacija rezultata dobijenih metodom barometra rizika.



Slika 4. Primer vizuelizacije rezultata dobijenih metodom barometra rizika

5.2. Metodi zasnovani na mašinskom učenju

Korišćenje veštačke inteligencije i mašinskog učenja pruža niz prednosti za upravljanje rizikom [23]. Prvo, omogućuje efikasnu obradu velike količine strukturiranih i nestrukturiranih podataka, kao i kombinovanje skupova podataka i ažuriranih uzoraka. Drugo, automatizacija procesa upravljanja rizikom doprinosi poboljšanju efikasnosti i redukciji troškova. Treće, omogućuje prediktivno upravljanje rizikom u realnom vremenu, pomoću koga se identifikuju nove pretnje i ranjivosti, poboljšavaju preventivne akcije i postiže brži odziv sistema u kritičnim situacijama. Na kraju, odlučivanje zasnovano na predikciji rizika doprinosi unapređenju poslovanja.

Strukturirani pregledi istraživanja u kojima su metode mašinskog učenja primenjene za procene rizika u inženjerstvu i bezbednosnog rizika prikazani su u radovima [24] i [25], respektivno. Rezultati studija pokazuju da je dominantna metodologija nadgledanog (*supervised*) učenja, zasnovanog na veštačkim neuronskim mrežama (*Artificial Neural Networks*, ANNs). Taj zaključak se ne može generalizovati na IIoT mreže, prvenstveno zbog toga što one zahtevaju distribuirane sisteme za procenu rizika, sa tehnikama koje su pogodne za *edge computing*. U tabeli 2 prikazan je uporedni pregled

osnovnih metoda mašinskog učenja i njihova primena u *edge computing*-u [26]. Nedavno istraživanje dostupnih publikacija o proceni bezbednosnog rizika u IIoT sistemima pokazuje tendenciju primene *deep learning* metoda [27].

Tabela 2. Metodi, algoritmi i primena mašinskog učenja u edge computing-u

Metod	**Algoritmi**	**Primena**	**Prednosti**	**Nedostaci**
Nadgledano učenje	ANN, SVM	Klasifikacija i klasterovanje	Jednostavna i brza implementacija	Osetljivost na podatke, masivni podaci, problem granica performansi
Nenadgledano učenje	ANN, *K-means*			
Deep learning	CNN	Predikcija, detekcija	Učenje *end-to-end* svojstava	Dugotrajan trening sa masivnim podacima
Reinforcement learning	Markovljev proces odlučivanja, *Q-learning*	Odlučivanje	Učenje bez *a priori* znanja o sistemu	Problem dimenzionalnosti
Deep reinforcement learning	DQN	Ekstrakcija svojstava i odlučivanje	*End-to-end reinforcement* učenje	Dugotrajan trening u velikom prostoru diskretnih stanja

Nadgledano učenje pretpostavlja prethodno znanje o izlaznim vrednostima za poznate uzorke ulaznih podataka. Cilj je učenje funkcije koja preslikava ulaz u odgovarajući izlaz, na osnovu poznatih primera parova ulaz-izlaz. Poznati algoritmi su nadgledane ANN i metod potpornih vektora (*Support Vector Machine*, SVM). U [28] je prikazan pristup za dinamičku procenu bezbednosnog rizika u ICS, zasnovan na Bajesovoj mreži sa fazi verovatnoćama, koji je verifikovan na primeru simulacije upravljanja hemijskim reaktorom. Kvantitativni metod za procenu sajber bezbednosnog rizika u infrastrukturi pametnih gradova, zasnovan na ANN pristupu, opisan je u [12].

Nenadgledano učenje ne koristi labelirane izlaze; njegov zadatak je da izvede funkciju koja opisuje strukturu nelabeliranih podataka, a jedan od najrasprostranjenijih algoritama je *K-means*, koji grupiše podatke u više nepovezanih klastera.

Deep learning metodi inspirisani su strukturom i funkcionisanjem ljudskog mozga. Drugim rečima, algoritmi pokušavaju da izvedu slične zaključke kao ljudi, koristeći višeslojnu strukturu neuronskih mreža, npr. konvolucione neuronske mreže (*Convolutional Neural Networks*, CNNs). Na taj način je omogućena automatska ekstrakcija svojstava (iz velike količine podataka) koja su bitna za predikciju i klasifikaciju. *Deep learning* metodi su pogodni za integraciju u *edge-computing* sisteme i mogu se koristiti za predikciju saobraćaja i ponašanja mreže, kao i za detekciju otkaza i incidenata u mreži. Primer primene CNN algoritma za klasifikaciju bezbednosnih rizika u IoT okruženju opisan je u [29]. Sličan pristup, predstavljen u [30], namenjen je za procenu sajber bezbednosnog rizika u zdravstvu. Distribuirani sistem za dinamičku procenu bezbednosnog rizika, zasnovan na politikama upravljanja, predložen je u [31] i namenjen za program Industrija 4.0, lance snabdevanja i inteligentne transportne sisteme.

Reinforcement learning je inspirisan bihevioralnom psihologijom; učenje u interaktivnom okruženju zasniva se na pokušajima i greškama, pri čemu se koriste povratne informacije iz sopstvenih akcija i iskustava. Pri preslikavanju ulaz-izlaz koriste se nagrade i kazne kao indikatori pozitivnog i negativnog ponašanja. Ova klasa metoda pogodna je za automatsko upravljanje i odlučivanje u vrlo dinamičnim okruženjima. Tipični predstavnici su Markovljev proces odlučivanja i *Q-learning* algoritmi.

Deep reinforcement learning (npr. *Deep Q-Network,* DQN) kombinuje ANN sa *reinforcement learning* metodima. Ova klasa tehnika objedinjuje aproksimaciju funkcije i optimizaciju cilja preslikavanjem parova stanje-akcija u očekivane nagrade. To svojstvo čini ove tehnike pogodnim kako za ekstrakciju svojstava, tako i za odlučivanje. DQN algoritam je predložen u [32] za dinamičku ocenu rizika u vetroelektranama.

6. Zaključak

Kompleksnost, dinamičnost i heterogenost IIoT sistema, kao i stalna pojava novih sajber napada i pretnji, uslovljavaju potrebu za definisanjem novih metoda i procedura za procenu bezbednosnog rizika. Dinamička procena rizika obuhvata upravljanje imovinom, modelovanje napada i proračun rizika, zasnovan na brojnim dinamičkim i statičkim parametrima. Permanentan nadzor sajber napada i elemenata bezbednosnog sistema pruža povratne informacije za modifikaciju modela napada i ažuriranje softvera za proračun rizika.

Jedan broj tradicionalnih metoda (Bajesov metod, analiza „leptir mašne“, barometar rizika) može se uspešno primeniti za dinamičku procenu bezbednosnog rizika u IIoT okruženju. Novija istraživanja ukazuju na perspektive primene veštačke inteligencije i mašinskog učenja za tu svrhu, zbog efikasne obrade velike količine podataka, prediktivnog upravljanja rizikom i podrške odlučivanju.

Buduća istraživanja treba da obuhvate definisanje novih modela za dinamičku procenu bezbednosnog rizika, razvoj specijalizovanih algoritama mašinskog učenja, razvoj odgovarajućih okruženja za testiranja i standardizaciju. Posebno je značajan razvoj decentralizovanih modela, zasnovan na većem broju distribuiranih, kooperativnih agenata, u cilju adekvatne procene rizika u različitim delovima IIoT sistema, od perfiferije, preko *cloud* infrastrukture, do aplikacionog sloja. Istraživanje metoda mašinskog učenja odvija se u pravcu *deep learning* i *deep reinforcement learning* algoritama, zbog njihove prilagođenosti *end-to-end* učenju i odlučivanju.

Zahvalnica. Rad je finansiran od strane Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije.

Literatura

[1] C. Adaros Boye, P. Kearney, and M. Josephs, “Cyber-risks in the Industrial Internet of Things (IIoT): Towards a method for continuous assessment”, in L. Chen, M. Manulis, & S. Schneider (Eds.), *Information Security, ISC 2018, LNCS*, vol. 11060, pp. 502-519, Springer, Cham, 2018. DOI: 10.1007/978-3-319-99136-8_27

[2] J. Marković-Petrović i M. Stojanović, “Klasifikacija sajber napada na industrijske IoT sisteme”, *Zbornik radova 19. Simpozijuma CIGRÉ Srbija*, RD2-05, 2020.

[3] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, “Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures”, *Proc. of the IEEE Global Conf. on Wireless Computing and Networking (GCWCN)*, 2018.

[4] K. Tsiknas et al., “Cyber threats to Industrial IoT: A survey on attacks and countermeasures”, *IoT*, vol. 2, no. 1, pp. 163-186, 2021. DOI: 10.3390/iot2010009

[5] S. Berger, O. Burger, and M. Roglinger, "Attacks on the Industrial Internet of Things – Development of a multi-layer taxonomy", *Comput. Secur.*, vol. 93, 101790, 2020. DOI: 10.1016/j.cose.2020.101790
[6] *Risk Management – Guidelines*, ISO Standard 31000:2018, 2018.
[7] *Risk Management – Risk Assessment Techniques*, IEC Standard 31010:2019, 2019.
[8] K. Stouffer et al., *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82 Rev. 2, 2015.
[9] *Industrial Internet of Things Volume G4: Security Framework*, IIC:PUB:G4:V1.0:PB:20160919, 2016.
[10] T. Tsiakis, "Information security expenditures: A techno-economic analysis", *Int. Journal of Computer Science and Network Security*, vol. 10, no. 4, pp. 7-11, 2010.
[11] W. Sonnenreich, J. Albanese, and B. Stout, "Return on security investment (ROSI) – A practical quantitative model", *Journal of Research & Practice in Information Technology*, vol. 38, no. 1, pp. 45-56, 2006.
[12] M. Kalinin, V. Krundyshev, and P. Zegzhda, "Cybersecurity risk assessment in smart city infrastructures", *Machines*, vol. 9, no. 4, article 78, 2021. DOI: 10.3390/machines9040078
[13] J. D. Marković-Petrović, "Procena bezbednosnog rizika u industrijskim sistemima daljinskog upravljanja", doktorska disertacija, Univerzitet u Beogradu – Saobraćajni fakultet, septembar 2018.
[14] J. D. Markovic-Petrovic, M. D. Stojanovic, and S. V. Bostjancic Rakas, "A fuzzy AHP approach for security risk assessment in SCADA networks", *Adv. Electr. Comput. Eng.*, vol. 19, no. 3, pp. 69-74, 2019. DOI: 10.4316/AECE.2019.03008
[15] Y. Cherdantseva et al., "A review of cyber security risk assessment methods for SCADA systems", *Comput. Secur.*, vol. 56, pp. 1-27, 2016. DOI: 10.1016/j.cose.2015.09.009
[16] Q. S. Qassim, et al., "A review of security assessment methodologies in industrial control systems", *Inf. Comput. Secur.*, vol. 27, no. 1, pp. 47-61, 2019. DOI: 10.1108/ICS-04-2018-0048
[17] O. Mirzaei, J. Maria de Fuentes, and L. G. Manzano, "Dynamic risk assessment in IT environments: A decision guide", in Z. Fields (Ed.), *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution*, pp. 234-263, IGI Global, Hershey, PA, 2018. DOI: 10.4018/978-1-5225-4763-1.ch009
[18] E. T. Nakamura and S. L. Ribeiro, "A privacy, security, safety, resilience and reliability focused risk assessment methodology for IIoT systems steps to build and use secure IIoT systems", *Proc. of the Global Internet of Things Summit (GIoTS)*, pp. 1-6, 2018. DOI: 10.1109/GIOTS.2018.8534521
[19] E. Rios et al., "Continuous quantitative risk management in smart grids using attack defense trees", *Sensors*, vol. 20, no. 16, 4404, 2020. DOI: 10.3390/s20164404
[20] M. Kalantarnia, F. I. Khan, and K. Hawboldt, "Dynamic risk assessment using failure assessment and Bayesian theory", *J. Loss Prev. Process Ind.*, vol. 22, no. 5, pp. 600-606, 2009. DOI: 10.1016/j.jlp.2009.04.006
[21] N. Paltrinieri et al., "Dynamic Procedure for Atypical Scenarios Identification (DyPASI): A new systematic HAZID tool", *J. Loss Prev. Process Ind.*, vol. 26, no. 4, pp. 683-695, 2013. DOI:10.1016/j.jlp.2013.01.006

[22] E. H. Okstad, S. Hauge, and R. K. Tinmannsvik, *Proactive Indicators for Managing Major Accident Risk in Integrated Operations*, SINTEF F24087, SINTEF Technology and Society, Trondheim, Norway, 2013.
[23] *Artificial Intelligence Applied to Risk Management*, FERMA, 2019.
[24] J. Hegde and B. Rokseth, "Applications of machine learning methods for engineering risk assessment – A review", *Saf. Sci.*, vol. 122, 104492, 2020. DOI: 10.1016/j.ssci.2019.09.015
[25] G. Erdogan et al., "A systematic mapping study on approaches for AI-supported security risk assessment", *Proc. of the COMPSAC 2021: Intelligent and Resilient Computing for a Collaborative World 45th Anniversary Conference – SEPT Symposium: Security, Privacy & Trust in Computing*, pp. 1-7, 2021.
[26] B. Cao et al., "Intelligent offloading in multi-access edge computing: A state-of-the-art review and framework", *IEEE Commun. Mag.*, vol. 57, no. 3, pp. 56-62, 2019. DOI: 10.1109/MCOM.2019.1800608
[27] M. D. Stojanović and J. D. Marković-Petrović, "Application of machine learning for cyber security risk assessment in Industrial IoT systems: A review", paper submitted to the *7th Virtual Int. Conf. on Science, Technology and Management in Energy – eNergetics 2021.*
[28] Q. Zhang et al., "A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems", *IEEE Trans. Industr. Inform.*, vol. 14, no. 6, pp. 2497-2506, 2018. DOI: 10.1109/TII.2017.2768998
[29] W. Abbass et al., "Classifying IoT Security Risks using Deep Learning Algorithms", *Proc. of the 6th Int. Conf. on Wireless Networks and Mobile Communications (WINCOM)*, 2018. DOI: 10.1109/WINCOM.2018.8629709
[30] M. N. Zakaria et al., "A conceptual model for Internet of Things risk assessment in healthcare domain with deep learning approach", *Int. J. Innov. Comput.*, vol. 10, no. 2, pp. 7-19, 2020. DOI: 10.11113/ijic.v10n2.263
[31] G. Baldini, P. Fröhlich, and E. Gelenbe, "IoT network risk assessment and mitigation: The SerIoT approach", in J. Soldatos (Ed.) *Security Risk Management for the Internet of Things: Technologies and Techniques for IoT Security, Privacy and Data Protection,* pp. 88-104, Now Publishers, Hanover, MA, 2020.
[32] X. Liu, J. Ospina, and C. Konstantinou, "Deep reinforcement learning for cybersecurity assessment of wind integrated power systems", *IEEE Access*, vol. 8, pp. 208378-208394, 2020. DOI:10.1109/ACCESS.2020.3038769

Abstract: *This paper deals with dynamic security risk assessment in IIoT (Industrial Internet of Things) systems. Classifications of cyber attacks against IIoT systems are presented, followed by a brief description of basic principles of security risk assessment in industrial control systems. Models and methods for dynamic security risk assessment have been presented, with emphasis on applicability of different machine learning approaches for that purpose.*

Keywords: *Dynamic assessment, IIoT, machine learning, security risk*

DYNAMIC SECURITY RISK ASSESSMENT IN INDUSTRIAL IoT SYSTEMS
Mirjana D. Stojanović, Jasna D. Marković-Petrović