BEZBEDNOST INDUSTRIJSKIH IoT SISTEMA

Mirjana D. Stojanović[1], Slavica V. Boštjančič Rakas[2], Jasna D. Marković-Petrović[3]
[1]Univerzitet u Beogradu - Saobraćajni fakultet, m.stojanovic@sf.bg.ac.rs
[2] Univerzitet u Beogradu - Institut Mihajlo Pupin, slavica.bostjancic@institutepupin.com
[3]PD "HE Đerdap" - HE "Đerdap 2" Negotin, Jasna.Markovic@djerdap.rs

Rezime: *Predmet ovog rada je bezbednost IIoT (Industrial Internet of Things) sistema, koji predstavljaju temelj budućih kritičnih infrastrukturnih sistema. Opisani su funkcionalni i implementacioni modeli IIoT sistema, a zatim su razmatrani bezbednosni rizici u IIoT sistemima i posledice uspešnih sajber napada. Sledi prikaz rešenja zaštite IIoT sistema koji obuhvata pregled industrijskih standarda, principe zaštite i funkcionalnu arhitekturu zaštite IIoT sistema.*

Ključne reči: *Bezbednost, industrijski sistem, Internet stvari, računarstvo u oblaku*

1. Uvod

Poslednjih godina smo svedoci ubrzanog razvoja Internet tehnologija kao što su: računarstvo u oblaku (*cloud computing*), računarstvo u magli (*fog computing*), Internet stvari (*Internet of Things*, IoT), mobilno računarstvo, obrada i analiza velike količine podataka (*Big Data*). Koncept IoT evoluira u nekoliko pravaca, među kojima se ističu industrijski IoT (*Industrial Internet of Things*, IIoT) [1], Internet energije (*Internet of Energy*, IoE) [2] i heterogeni IoT (HetIoT) [3]. IIoT je model senzora, aktuatora i drugih industrijskih uređaja, povezanih na Internet i umreženih sa industrijskim aplikacijama. To je osnovni gradivni blok programa *Industrija 4.0*, koji podrazumeva potpunu digitalizaciju procesa proizvodnje i primenu tehnologija budućeg Interneta prilikom kreiranja i inženjeringa proizvoda, organizacije i realizacije proizvodnje, kontrole procesa i pružanja industrijskih usluga. Srbija je u junu 2019. godine postala 38. država u svetu koja je usvojila Nacionalni program za Industriju 4.0.

Nove informacione i komunikacione tehnologije neosporno donose industriji niz prednosti u pogledu poboljšanja skalabilnosti, konfigurisanja i održavanja sistema, energetske efikasnosti, kao i unapređenja poslovanja. U radu će biti razmatrana bezbednost industrijskih IoT sistema, kao ključni faktor rizika, koji se mora analizirati u svim fazama razvoja i eksploatacije industrijskog sistema.

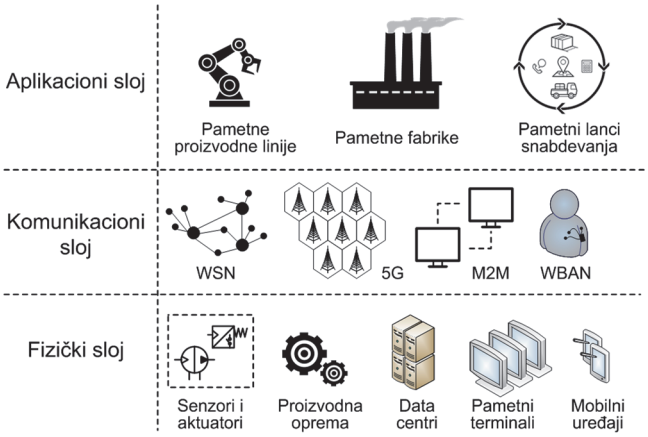
Rad je organizovan na sledeći način. U drugom poglavlju prikazan je funkcionalni model IIoT sistema, kao i tri modela za implementaciju IIoT. U trećem poglavlju opisani su bezbednosni rizici u IIoT sistemima i posledice uspešnih sajber napada. U četvrtom

poglavlju prikazana su moguća rešenja zaštite IIoT sistema. Posle kratkog pregleda industrijskih standarda, razmatrani su ključni principi zaštite i opisan je funkcionalni model zaštite industrijskih IoT sistema. Peto poglavlje obuhvata zaključna razmatranja.

2. Funkcionalni model i implementacija IIoT sistema

Kompleksna arhitektura IIoT sistema uobičajeno se opisuje slojevitom hijerarhijom, na nekoliko načina.

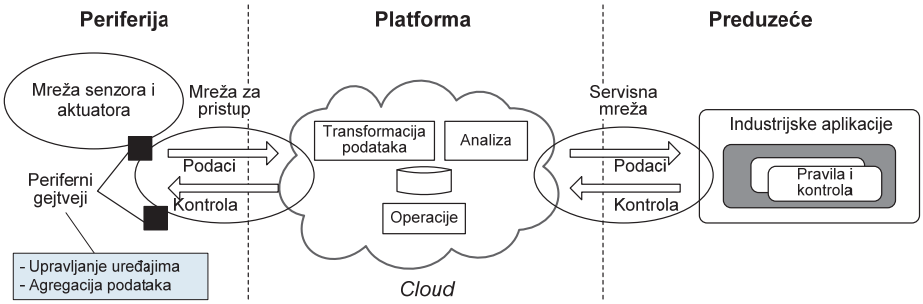
Iz aspekta industrijskih sistema, funkcije IIoT mogu se opisati troslojnim modelom koji čine aplikacioni sloj, komunikacioni sloj i fizički sloj (slika 1) [1]. Aplikacioni sloj čine različite industrijske aplikacije, kao što su pametne proizvodne linije, pametne fabrike, lanci snabdevanja i sl. Takve aplikacije upravljaju velikim brojem senzora i aktuatora na fizičkom sloju. Komunikacioni sloj integriše heterogene mrežne tehnologije kao što su bežične senzorske mreže (*Wireless Sensor Network*, WSN), mobilni sistemi pete generacije (5G), komunikacija između mašina (*Machine to Machine*, M2M), bežične telesne mreže (*Wireless Body Area Network*, WBAN), softverski definisano umrežavanje (*Software Defined Networking*, SDN) i dr. Fizički sloj sačinjavaju senzori, aktuatori, proizvodna oprema, kao i računarski uređaji – *data* centri, pametni terminali i različiti mobilni uređaji.



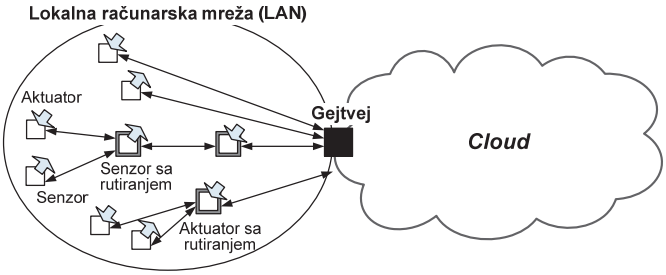
Slika 1. Funkcionalni model IIoT sistema

Industrijski Internet konzorcijum (*Industrial Internet Consortium*, IIC) definiše tri koherentna implementaciona modela za IIoT: troslojni model, povezivanje lokalne mreže preko gejtveja-medijatora i slojevitu magistralu podataka [4].

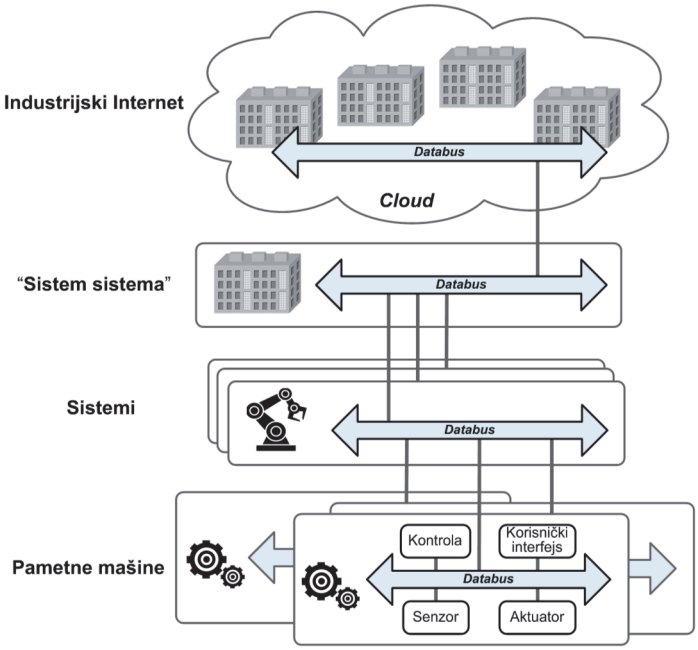
Prvi, troslojni model obuhvata slojeve periferije (*edge*), platforme i preduzeća, kao što je prikazano na slici 2. Sloj periferije prikuplja podatke iz mreže senzora i aktuatora, preko perifernih gejtvej uređaja. Karakteristike ovog sloja, kao što su lokacija, opseg upravljanja, priroda mreže senzora i aktuatora, zavise od specifičnih industrijskih primena. Sloj platforme prihvata kontrolne komande od sloja preduzeća, procesira ih i prosleđuje sloju periferije. Ovaj sloj objedinjuje procese, analizira tokove podataka i



Slika 2. Implementacija IIoT: troslojni model



Slika 3. Implementacija IIoT: povezivanje lokalne mreže preko perifernog gejtveja



Slika 4. Implementacija IIoT: slojevito organizovane magistrale podataka (databus)

upravlja uređajima i ostalom imovinom, a obično se realizuje preko računarstva u oblaku. Sloj preduzeća implementira industrijske aplikacije, sisteme za podršku odlučivanju i specijalizovane interfejse za krajnje korisnike.

U drugom modelu primenjen je koncept povezivanja lokalne računarske mreže na periferiji IIoT sistema sa *cloud* okruženjem preko gejtveja-medijatora, kao što je prikazano na slici 3. Gejtvej funkcioniše kao krajnja tačka oblaka i pri tome izoluje lokalnu mrežu od drugih perifernih čvorova. Ovakva arhitektura omogućuje lokalizaciju operacija i kontrole, čime se poboljšava skalabilnost IIoT sistema, kako u pogledu broja upravljivih objekata tako i u pogledu umrežavanja.

Treći model je zasnovan na slojevito organizovanim magistralama podataka (*databus*), kao što je prikazano na slici 4. Magistrala podataka je logički povezan prostor koji implementira zajednički skup obrazaca (modeli podataka, protokoli, bezbednost) za komunikaciju između krajnjih tačaka. Na najnižem sloju, pametne mašine koriste magistralu podataka za lokalnu kontrolu, automatizaciju i analizu u realnom vremenu. Na drugom sloju su sistemi koji koriste drugu magistralu podataka za nadzor i upravljanje. Udruživanje takvih sistema u "sistem sistema" na trećem sloju omogućuje kreiranje kompleksnih i skalabilnih aplikacija za nadzor, upravljanje i analizu. Najviši sloj ovog modela, industrijski Internet, zasnovan je na računarstvu u oblaku.

3. Bezbednosne pretnje i rizici u IIoT sistemima

Pri rešavanju bezbednosti IIoT sistema polazi se od poređenja IoT i IIoT tehnologija, zbog toga što su u pitanju tehnologije koje se paralelno razvijaju i koriste iste standardizovane protokole, interfejse i inteligenciju. Međutim, ove dve tehnologije imaju različite ciljeve, korisnike, operativne procese i zahteve, iz kojih proističu razlike u rešenjima zaštite.

Ciljevi. Cilj IIoT je da ostvari efikasnost i kontinuitet operacija industrijskog procesa, za razliku od IoT tehnologije koja je usredsređena na optimizaciju potrošnje, lični komfor i kontrolu troškova.

Namena. IIoT je primarno usredsređen na nadzor proizvodnje i parametara životne sredine koji su povezani sa industrijskim procesom, dok se IoT koristi za automatizaciju rutinskih poslova u domaćinstvu.

Zahtevi za kvalitet servisa i radni uslovi. IIoT arhitektura je projektovana tako da ispuni stroge zahteve industrijskih aplikacija koji se odnose na rad u realnom vremenu, sa vrlo visokom raspoloživošću i pouzdanošću. Pored toga, IIoT oprema mora da funkcioniše i u ekstremnim radnim uslovima, kao što su velike varijacije temperature, varijacije pritiska i zapremine gasa, elektromagnetske smetnje i sl.

Višedimenzionalna interoperabilnost. IIoT sistem podrazumeva otvorene standarde koji omogućuju formiranje kooperativnog okruženja sa različitim protokolima, skupovima podataka, sistemima za planiranje resursa preduzeća, ali i integraciju sa postojećim operativnim tehnologijama, kao što su industrijski sistemi daljinskog upravljanja.

Veoma visoka skalabilnost. IIoT mreža obuhvata industrijske kontrolere, robote i drugu automatizovanu opremu, hiljade novih senzora, ali i integraciju sa postojećom opremom koja nema IoT svojstva.

Bezbednost i privatnost. Pored toga što prouzrokuju degradaciju performansi, sajber napadi na IIoT sistem potencijalno ugrožavaju ljude, životnu sredinu i opremu. Osim

toga, podaci prikupljeni tokom industrijske proizvodnje obično su strogo poverljivi. IIoT zahteva robusne mehanizme za zaštitu bezbednosti i privatnosti, kao što su: agilne arhitekture sistema zaštite[1], šifrovanje, specijalizovani čip-setovi, autentifikacija i detekcija napada u realnom vremenu.

Specifične pretnje industrijskim IoT sistemima su: napredne perzistentne pretnje[2] (*advanced persistent threats*, APT), odsustvo mehanizama za zaštitu integriteta podataka, MITM (*man-in-the-middle*) napadi, krađa identiteta, prisluškivanje, napad ponavljanjem paketa (*replay attack*) i različiti oblici napada koji prouzrokuju odbijanje servisa (*Denial of Service*, DoS) [5].

Uzimajući u obzir slojevitu IIoT hijerarhiju, mogu se identifikovati sledeći bezbednosni rizici:

- Lokalne računarske mreže prikupljaju i procesiraju podatke od objekata industrijskog sistema na najnižem sloju. Glavni bezbednosni rizik je odsustvo autentifikacije i drugih bezbednosnih mehanizama u senzorskoj opremi.
- Podaci se prenose do oblaka posredstvom gejtveja. Glavni rizici proističu iz odsustva bezbednosnih mehanizama u komunikacionim protokolima i gejtvejima.
- Podaci se skladište i procesiraju u oblaku, pri čemu se koriste odgovarajuće platforme i specifični algoritmi, npr. za analizu velike količine podataka (*big data*). Glavni problem su nebezbedni podaci.
- Interfejsi između platformi i krajnjih korisnika mogu prouzrokovati probleme zbog nebezbednih komunikacionih protokola.

Bezbednosni rizici koji su posebno relevantni iz aspekta IIoT su: nebezbedni veb, mobilni i *cloud* interfejsi, ugrožavanje privatnosti, loše fizičko obezbeđenje, nebezbedan softver/firmver, slaba autentifikacija i autorizacija, nebezbedne mrežne konekcije, odsustvo enkripcije na transportnom sloju [6].

Posledice uspešnog napada na IIoT sistem manifestuju se nizom problema kao što su: ugrožavanje lične bezbednosti, oštećenje opreme, operativni problemi i regulatorni problemi [6]. Operativni problemi mogu prouzrokovati degradaciju kvaliteta ili uskraćivanje industrijske usluge krajnjim korisnicima. Regulatorni problemi nastaju kada su napadi pokrenuti iz druge države, a tiču se nadležnosti za istragu i pravno sankcionisanje sajber kriminala [7].

4. Bezbednosna rešenja

Bezbednost IIoT sistema je multidisciplinarna oblast koja obuhvata niz rešenja: od sistemskog nivoa (arhitektura zaštite, upravljanje rizikom, implementacija politike zaštite), preko specifičnih bezbednosnih mehanizama (sistemi za detekciju i prevenciju napada, šifrovanje, mehanizmi za autentifikaciju), razvoja specijalizovanih okruženja za testiranje rešenja, do definisanja procedura koje se primenjuju tokom eksploatacije sistema.

---

[1] Agilna arhitektura – pojam koji označava raznovrsnu, evolutivnu i fleksibilnu softversku arhitekturu.

[2] Napredne perzistentne pretnje – napadi kojima se neovlašćeno pristupa računarskoj mreži, a ostaju nedetektovani u dužem vremenskom periodu (obično ih lansiraju organizacije ili grupe pod pokroviteljstvom neke države).

4.1. Pregled standarda

Relevantni standardi obuhvataju: (1) standarde i preporuke za bezbednost informacionih i komunikacionih sistema opšte namene; (2) opšte standarde i smernice za bezbednost IoT i IIoT i (3) specifične smernice koje se tiču rešenja zaštite u pojedinim industrijskim sektorima. Ovde će biti ukazano na standarde, preporuke i druge dokumente koji su neposredno orijentisani ka industrijskom Internetu, a sveobuhvatni pregled relevantnih standarda može se pronaći u literaturi [8], [9].

Industrijski Internet konzorcijum (IIC) osnovan je 2014. godine kao globalna neprofitabilna zajednica industrije, vladinih organizacija i akademskih institucija. Prvenstveni cilj ovog konzorcijuma je da pomogne industrijskim preduzećima u efikasnoj implementaciji industrijskog Interneta putem identifikacije, prikupljanja, testiranja i promocije tzv. najbolje prakse. IIC radna grupa za bezbednost odgovorna je za donošenje opšteg okvira za bezbednost industrijskog Interneta, koji obuhvata model i politiku bezbednosti, zaštitu podataka, zaštitu krajnjih tačaka (periferija – oblak), zaštitu komunikacija i konektivnosti, nadzor i analizu, kao i konfiguraciju i upravljanje zaštitom. Dokument koji opisuje okvir za bezbednost IIoT publikovan je 2016. godine [10].

Međunarodno društvo za automatizaciju (*International Society of Automation*, ISA) osnovalo je radnu grupu zaduženu za sajber bezbednost IIoT – ISA99 *Working Group* 9. Cilj ove radne grupe je da ispita mogućnosti primene poznatog industrijskog standarda IEC 62443 na IIoT sisteme [11].

Rad na bezbednosti IoT u okviru američkog državnog instituta za standarde i tehnologiju (*National Institute of Standards and Technology,* NIST) započet je 2016. godine, a obuhvata definisanje okvira za sajber bezbednost, profile za industriju i proizvodnju, inženjering bezbednosnih sistema, bezbednost računarstva u oblaku i dr. Imajući u vidu da je računarstvo u oblaku integralni deo IIoT, svi aspekti bezbednosti koji se primenjuju na *cloud* okruženje relevantni su i za IIoT [12]-[14].

Međunarodni institut IEEE (*Institute of Electrical and Electronics Engineers*) započeo je, 2019. godine, rad na standardu za digitalnu transformaciju (IEEE P2023), kojim će biti obuhvaćeni aspekti bezbednosti i privatnosti.

4.2. Ključni principi zaštite industrijskih IoT sistema

Zaštita industrijskih IoT sistema obuhvata primenu bezbednosnih mehanizama i alata zasnovanih na standardima i najboljoj praksi [5]. U nastavku su ukratko opisani ključni principi zaštite IIoT.

Zaštita svih delova sistema pre integracije. IIoT aplikacije koriste postojeću opremu od koje "nasleđuju" bezbednosne propuste ili čak odsustvo bezbednosnih mehanizama. Mnogi takvi uređaji ne koriste standardizovane protokole i gejtveje. Najvažniji preduslov za efikasnu zaštitu IIoT sistema je da svi njegovi delovi projektuju, implementiraju i atestiraju zaštitu u svoje komponente i podsisteme, pre integracije u IIoT. Dobra praksa je korišćenje univerzalnih industrijskih protokola kao što je OPC UA (*Open Platform Communications Unified Architecture*). Arhitektura zaštite OPC UA obuhvata poverljivost, integritet i raspoloživost podataka, kao i kontrolu pristupa [15].

Podela mreže na logičke segmente (segregacija). Ovaj metod pretpostavlja podelu velike mreže na nekoliko logičkih mreža, kao i sprovođenje politika za kontrolu komunikacija između specifičnih hostova i servera. Bezbednosni mehanizmi u svakoj logičkoj mreži efikasno izoluju mrežu i nadgledaju aktivnosti u njoj. Primer primene ovog

metoda je implementacioni model zasnovan na slojevito organizovanim magistralama podataka (slika 4).

Kontinuirani nadzor mreže i analiza aktivnosti. Ovaj proces podrazumeva neprekidan nadzor i analizu aktivnosti u mreži, u cilju detekcije i identifikacije anomalija i sumnjivih događaja. Analiza log fajlova značajna je za lociranje i otklanjanje otkaza, detekciju anomalija, mrežnu forenziku. Analiza damp (*dump*) fajlova omogućuje detekciju poznatih i nepoznatih malicioznih aktivnosti prisutnih u RAM memoriji sistema. Analiza mrežnog saobraćaja vrši se u cilju detekcije anomalija u saobraćaju, koje mogu biti indikacija malicioznih aktivnosti. Ona obuhvata analizu "ponašanja" (npr. procedure protokola, intenzitet saobraćaja i dr.) i analizu uzoraka saobraćaja, a može se vršiti na bazi paketa ili na bazi saobraćajnih tokova.

Atribucija napada. Ovaj metod podrazumeva otkrivanje identiteta i/ili lokacije napadača, a posebno je važan kada su napadi izvršeni iz druge države, zbog regulatornih pitanja [7].

Primena alata za detekciju malicioznih aktivnosti i proksi rešenja. Ovi alati obuhvataju "zaštitne zidove" (*firewall*), sisteme za detekciju i prevenciju napada, antivirusni softver i dr. Proksi rešenja kao što su filtriranje paketa i kontrola pristupa koriste se da formiraju zaštitni sloj oko ranjivih ili tehnološki starijih komponenata.

Održavanje sistema. Redovno testiranje ranjivosti sistema neophodno je zbog detektovanja novih i/ili nepoznatih pretnji. Osim toga, obavezna je redovna distribucija ažurnih verzija softvera i softverskih dodataka (*patches*).

4.3. Funkcionalna arhitektura zaštite IIoT sistema

Funkcionalna arhitektura zaštite IIoT sistema prikazana je na slici 5 [10]. Četiri osnovna gradivna bloka su: zaštita krajnjih tačaka, zaštita komunikacija i konektivnosti, nadzor i analiza bezbednosnih mehanizama i upravljanje konfiguracijom bezbednosnih mehanizama.

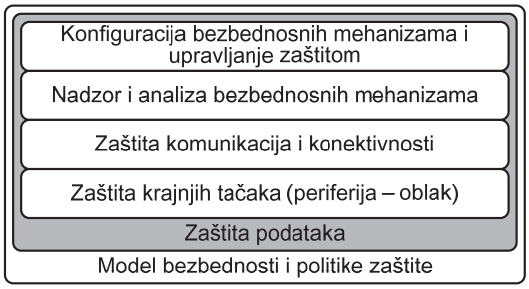
Blok za zaštitu krajnjih tačaka implementira zaštitne mehanizme u uređajima na periferiji i u oblaku. Glavne funkcije su fizička bezbednost uređaja, sajber bezbednost uređaja i upravljanje identitetom.

Blok za zaštitu komunikacija i konektivnosti koristi upravljanje identitetom za implementaciju autentifikacije i autorizacije saobraćaja. Primenjuju se pouzdane kriptografske tehnike za očuvanje integriteta i poverljivosti podataka, kao i tehnike za kontrolu toka informacija.

Kada su krajnje tačke zaštićene i komunikacije obezbeđene, stanje sistema čuva se tokom operativnog ciklusa nadzorom i analizom bezbednosnih mehanizama i kontrolom konfiguracije zaštite svih komponenata sistema.

Zajednička funkcija zaštite podataka pruža podršku za sva četiri prethodno opisana gradivna bloka, a primenjuje se na sve vrste podataka – od neaktivnih podataka (*data-at-rest*), koji se čuvaju u krajnjim tačkama, do podataka koji se procesiraju i prenose u komunikacionom sloju (*data-in-motion*). Ona takođe obuhvata podatke prikupljene u procesima nadzora i analize, kao i konfiguracione i upravljačke podatke.

Model bezbednosti koordinira zajednički rad svih funkcionalnih elemenata i određuje način implementacije zaštite i politika koje garantuju poverljivost, integritet i raspoloživost IIoT sistema tokom operativnog ciklusa.



Slika 5. Gradivni blokovi IIC funkcionalne arhitekture za bezbednost IIoT

Tabela 1. Struktura funkcija zaštite krajnjih tačaka i komunikacija/konektivnosti

Krajnja tačka		**Komunikacije i konektivnost**	
Model bezbednosti i politike	Zaštita podataka (*data-at-rest*) - Fizička bezbednost - *Root of trust* - Identitet - Zaštita integriteta - Kontrola pristupa - Nadzor i analiza - Konfiguracija i upravljanje	Model bezbednosti i politike	Zaštita podataka (*data-in-motion*) - Fizička bezbednost konekcija - Zaštita komunikacije krajnjih tačaka - Kriptografska zaštita - Zaštita toka informacija - Nadzor i analiza mreže - Konfiguracija i upravljanje mrežom

U tabeli 1 predstavljena je detaljna funkcionalna struktura zaštite krajnjih tačaka i zaštite komunikacija i konektivnosti.

Pored fizičkog obezbeđenja, zaštita krajnje tačke obuhvata definisanje komponente od apsolutnog poverenja u kriptografskom sistemu (*root of trust*), definisanje jedinstvenog identiteta krajnje tačke, zaštitu integriteta, kontrolu pristupa, nadzor i analizu, kao i konfiguraciju zaštite i redovno ažuriranje politika zaštite.

Zaštita komunikacija i konektivnosti obuhvata fizičko obezbeđivanje konekcija, zaštitu komunikacija između krajnjih tačaka, kriptografske zaštitne mehanizme, zaštitu informacionih tokova, nadzor i analizu (detekcija napada, kontrola pristupa mreži, analiza protokola, analiza logova), kao i konfiguraciju zaštite i upravljanje mrežom (podela mreže na segmente, kriptografska zaštita parametara komunikacije, konfiguracija gejtveja i zaštitnih zidova).

5. Zaključak

Industrijski IoT sistemi, kao temelj buduće kritične infrastrukture, donose industriji niz prednosti u pogledu energetske efikasnosti, skraćenja proizvodnog ciklusa, efikasnog održavanja opreme, analize velike količine podataka, bržeg i preciznijeg odlučivanja. Međutim, sajber bezbednost je glavni faktor rizika, koji se mora rešavati sa najvećom pažnjom u svim fazama razvoja, implementacije i eksploatacije industrijskog

sistema. U tom svetlu, neophodni su zajednički napori svih relevantnih činilaca – državnih organizacija, industrije, akademskih institucija i tela za standardizaciju. Prvi preduslov za uspešnu zaštitu IIoT je da svi njegovi delovi projektuju, implementiraju i atestiraju zaštitu pre integracije. To se odnosi na senzore, aktuatore, komunikacione podsisteme, gejtveje, ali i na računarstvo u oblaku. Pitanje zaštite IIoT sistema mora se rešavati polazeći od specifične arhitekture zaštite, preko bezbednosnih mehanizama do procedura koje se primenjuju tokom eksploatacije sistema. Među brojnim otvorenim pitanjima za dalja istraživanja ističu se: sistematizacija i atribucija sajber napada na IIoT, metode za procenu bezbednosnog rizika, bezbednosni mehanizmi prilagođeni za IIoT i metodologija testiranja bezbednosnih rešenja.

Zahvalnica. Rad je finansiran od strane Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije (projekat tehnološkog razvoja TR 32025).

Literatura

[1] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on Industrial Internet of Things: A cyber-physical systems perspective", *IEEE Access*, vol. 6, pp. 78238-78259, 2018.

[2] Y. Cao, Q. Li, Y. Tan, Y. Li, Y. Chen, X. Shao, and Y. Zou, "A comprehensive review of Energy Internet: Basic concept, operation and planning methods, and research prospects", *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 3, pp. 399-411, 2018.

[3] T. Qiu, N. Chen, K. Li, M. Atiquzzaman, and W. Zhao, "How can heterogeneous Internet of Things build our future: A survey", *IEEE Communications Surveys and Tutorials*, vol. 20, no. 3, pp. 2011-2027, 2018.

[4] *The Industrial Internet of Things Volume G1: Reference Architecture*, Industrial Internet Consortium, Version 1.9, 2019. [Online]. Available at: https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf

[5] A. Sajid, H. Abbas and K. Saleem, "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges", *IEEE Access*, vol. 4, pp. 1375-1384, 2016.

[6] M. Stojanović and S. Boštjančič Rakas, "Challenges in securing industrial control systems using Future Internet technologies", In M. Stojanović and S. Boštjančič Rakas (Eds.) *Cyber Security of Industrial Control Systems in the Future Internet Environment*. Hershey, PA: IGI Global, 2020. (In press).

[7] A. Cook, A. Nicholson, H. Janicke, L. Maglaras, and R. Smith, "Attribution of cyber attacks on industrial control systems", *EAI Transactions on Industrial Networks and Industrial Systems*, vol. 3, no. 7, pp. 1-15, 2016.

[8] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations", *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702-2733, 2019.

[9] S. Ghosh and S. Sampalli, "A survey of security in SCADA networks: Current issues and future challenges", *IEEE Access*, vol. 7, pp. 135812-135831, 2019.

[10] *Industrial Internet of Things Volume G4: Security Framework*, Industrial Internet Consortium document IIC:PUB:G4:V1.0:PB:20160919, 2016. [Online]. Available at: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf

[11] B. Leander and A. Čaušević, "Applicability of the IEC 62443 standard in Industry 4.0/IIoT", In *Proc. of the 14th International Conference on Availability, Reliability and Security*, Article No. 101, pp. 1-8. Canterbury, UK, August 2019.
[12] P. Ravi Kumar, P. Herbert Rajb, and P. Jelcianac, "Exploring data security issues and solutions in cloud computing", *Procedia Computer Science*, vol. 125, pp. 691-697, 2018.
[13] M. Stojanović, S. Boštjančič Rakas, and J. Marković-Petrović, "SCADA systems in the cloud and fog environments: Migration scenarios and security issues", *FACTA UNIVERSITATIS Series: Electronics and Energetics*, vol. 32, no. 3, pp. 345-358, 2019.
[14] J. Sanders. (2019, August 01). Guide to industry cloud: What businesses need to know. [Online]. Available at: https://www.zdnet.com/article/guide-to-industry-cloud-what-businesses-need-to-know/
[15] *Practical Security Recommendations for Building OPC UA Applications*. (2018). OPC Foundation. [Online]. Available at: https://opcfoundation.org/wp-content/uploads/2017/11/OPC-UA-Security-Advise-EN.pdf

Abstract: *This paper deals with security issues in Industrial Internet of Things (IIoT) systems, which represent a foundation for the future critical infrastructure. Functional and implementation models of IIoT systems have been described, followed by analysis of cyber security risks and consequences of successful cyber attacks on IIoT systems. Subsequently, security solutions are presented, including a brief overview of industrial standards, key principles for securing IIoT and a functional IIoT security architecture.*

Keywords: *Cloud computing, cyber security, industrial system, Internet of Things*

SECURITY ISSUES IN INDUSTRIAL IoT SYSTEMS

Mirjana Stojanović, Slavica Boštjančič Rakas, Jasna Marković-Petrović