Bezbjednost u sajber fizičkim i IoT sistemima

UGLJEŠA D. UROŠEVIĆ, Univerzitet Crne Gore,
Prirodno-matematički fakultet, Podgorica, Crna Gora
MARIJA M. ČUBROVIĆ, Univerzitet Crne Gore
Prirodno-matematički fakultet, Podgorica, Crna Gora

Pregledni rad
UDC: 004.78:004.35
004.056.5
DOI: 10.5937/tehnika2301045U

Bezbjednost sajber-fizičkih sistema (CPS – Cyber-Physical Systems) i IoT (Internet of Things / Internet stvari) sistema je važno pitanje zbog sve veće integracije ovih sistema u kritičnu infrastrukturu, proizvodnju i druga industrijska okruženja, kao i sve veće upotrebe IoT uređaja u različitim sferama života. Stoga je važno razmatrati bezbjednosne izazove u ovim sistemima i raditi na njihovom rješavanju kako bi se održala stabilnost i pouzdanost ovih sistema. U ovom radu se razmatra bezbjednost sajber-fizičkih sistema i IoT sistema, uključujući arhitekturu takvih sistema, bezbjednosne zahtjeve i standarde, kao i specifična pitanja bezbjednosti koja se pojavljuju u oba tipa sistema. Posebno, razmatra se bezbjednost CPS-a kroz fizički interfejs, kontrolni sistem, dostupnost i vremensko ograničenje, dok se bezbjednost IoT sistema razmatra kroz upravljanje povjerenjem, bezbjedne protokole rutiranja, integraciju heterogenih mreža i zaštitu privatnosti.

Ključne riječi: *Internet stvari – IoT, Sajber-fizički sistemi – CPS, bezbjednost*

1. UVOD

Sajber-fizički sistemi, odnose se na integraciju fizičkih i računarskih komponenti, što omogućava integraciju digitalnog i fizičkog svijeta. Ovi sistemi često uključuju integraciju računarskih i kontrolnih mogućnosti u fizičke procese, kao što su proizvodnja, transport ili proizvodnja energije. To su složeni, heterogeni sistemi koji se uglavnom sastoje od velikog broja senzora i aktuatora, koji su povezani sa grupom računarskih čvorova. Pomoću spajanja senzora, računarskih čvorova i aktuatora, koji su povezani putem različitih sredstava komunikacije, CPS-ovi imaju za cilj da uoče i razumiju promjene u fizičkom okruženju, analiziraju uticaj takvih promjena na njihov rad kao i da donose inteligentne odluke kao odgovor na nastale promjene izdavanjem komandi za kontrolu fizičkih objekata u sistemu, čime se na autonoman način utiče na fizičko okruženje. Veza između detekcije i aktivacije kod fizičkog okruženja, između senzora i aktuatora preko jednog ili više (razgranatih) računarskih ili inteligentnih kontrolnih čvorova čini petlju povratne sprege i ima za cilj postizanje željene svrhe ili stabilnog stanja. Ovaj razgranati zatvoreni proces omogućava CPS-u da utiče na daljinu, upravlja, automatizuje i kontroliše mnogo ljudski izrađenih (ali i prirodnih) malih, srednjih i velikih sistema. Zbog operativne prirode CPS-a u većini industrijskih kontrolnih procesa CPS-ovi su poznati i kao sistemi operativne tehnologije (OT sistemi), [1], [2].

IoT se odnosi na međusobno povezanu mrežu fizičkih uređaja i sistema koji su u mogućnosti da prikupljaju i razmjenjuju podatke koristeći internet konekciju. Ovi uređaji, koji mogu uključivati različite potrošačke i industrijske proizvode kao što su pametni termostati, kamere za bezbjednost, senzori i aktuatori, imaju potencijal za unapređenje industrije i poboljšanje efikasnosti kroz automatizaciju i optimizaciju različitih procesa. Međutim, integracija IoT uređaja u različite sisteme takođe uvodi nove rizike vezane za bezbjednost koji treba da se razmotre. Kako broj povezanih uređaja i sistema nastavlja da raste, sve je važnije da proizvođači i korisnici ovih uređaja stave bezbjednost na prvo mesto kako bi se osiguralo sigurno i bezbjedno funkcionisanje IoT sistema.

Masovno usvajanje uređaja sa omogućenim internet protokolom (IP) (tj. IP senzori i aktuatori) u CPS-u i sve veća bežična povezanost su time zamaglili granice između CPS-a i interneta stvari (IoT). Iako neki CPS-ovi mogu biti poznati i kao IoT sistemi sa stanovišta protokola, ako su uređaji za detekciju i

Adresa autora: Uglješa Uroševiić, Univerzitet Crne Gore, Prirodno-matematički fakultet, Podgorica, Džordža Vašingtona bb, Crna Gora
e-mail: ugljesa.urosevic@ucg.ac.me
Rad primljen: 11.01.2023.
Rad prihvaćen: 31.01.2023.

aktiviranje sposobni da koriste IP, primijetimo da postoji mnogo drugih lokalnih CPS-ova koji su još uvijek potpuno odvojeni od globalne IP mreže (što će se s vremenom promijeniti). Ipak, CPS se može posmatrati sa stanovišta funkcionalnosti i može biti poznat kao OT sistem ako se koristi za podršku rada industrijskih kontrolnih procesa. Neke od primjena CPS i IoT sistema uključuju, ali nisu ograničene na: velike ekološke sisteme (npr. upravljanje prirodnim resursima), proizvodnju i distribuciju energije, saobraćajnu infrastrukturu, kućnu automatizaciju, autonomnu vožnju, ličnu zdravstvenu zaštitu, logistiku ili industrijsku proizvodnju, [3]-[4].

Slika 1 – Područja primjene CPS/IOT rješenja

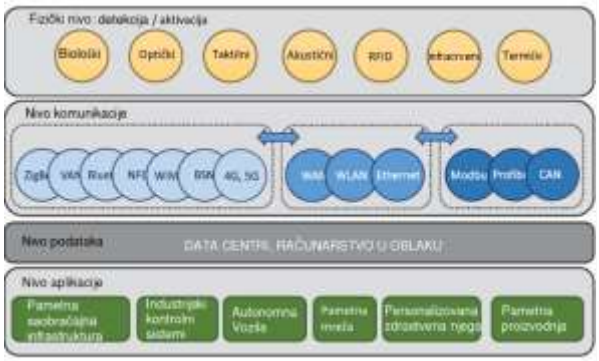
U ovim sistemima dominantno se koristi bežično povezivanje. Razlozi za preferiranje bežičnog povezivanja često su jednostavno smanjeni troškovi instalacije ili želja da se instalacija olakša. Sve veća dostupnost širokog spektra bežičnih tehnologija, optimizovanih za različite komunikacione scenarije i zahtjeve (takođe one koji su posebno relevantni za CPS i IoT) je stoga bila važan pokretač uspjeha i brzog usvajanja CPS-a i IoT-a u našem društvu i ostaće od ključnog značaja za njihovu buduću evoluciju. Nažalost, iako bežična povezanost ima očigledne prednosti, uklanjanje žica takođe donosi brojne teškoće i izazove u pogledu performansi komunikacije (npr. kašnjenje, domet i propusnost), potrošnje energije čvora i bezbjednosti. Zajedno sa zahtjevima CPS-a, ovi problemi određuju izbor pravog bežičnog komunikacijskog standarda i postavljaju osnove za istraživanja o bežičnoj povezanosti CPS-a naredne generacije kroz sve slojeve mrežnog steka.

2. POJEDNOSTAVLJENA ARHITEKTURA CPS/IOT SISTEMA

Arhitektura CPS sistema se sastoji od nekoliko slojeva ili nivoa koji se međusobno povezuju i omogućavaju sistemu da funkcioniše. Ovi nivoi uključuju:

- Fizički nivo: Ovaj nivo uključuje fizičke uređaje i senzore koji čine sistem. Ovi uređaji mogu uključivati senzore, aktuatore i druge hardverske komponente koje interaguju sa fizičkim svijetom.
- Mrežni nivo: Ovaj nivo uključuje komunikacione tehnologije i protokole koji omogućavaju uređajima u sistemu da međusobno komuniciraju. Ovo može uključivati žičane ili bežične komunikacione tehnologije, kao što su WiFi, Bluetooth ili mobilne mreže.
- Nivo podataka: Ovaj nivo uključuje podatke generisane od strane uređaja u sistemu kao i alate i protokole koji se koriste za skladištenje, obradu i analizu ovih podataka. Ovo može uključivati baze podataka, sisteme za skladištenje podataka i alate za analizu.
- Nivo aplikacije: Ovaj nivo uključuje aplikacije i softvere koji interaguju sa sistemom i pružaju funkcionalnost korisniku. Ovo može uključivati korisnički interfejs, sisteme za upravljanje i druge aplikacije koje omogućavaju sistemu da obavlja svoje namijenjene funkcije.
- Nivo bezbjednosti: Ovaj nivo uključuje mjere i protokole bezbjednosti koji su postavljeni da zaštite sistem od hakerskih napada i drugih prijetnji bezbjednosti. Ovo može uključivati enkripciju, autentifikaciju i mjere kontrole pristupa.

Apstraktni prikaz nivoa CPS/IoT prikazan je na slici 2. Nivo za detekciju/aktivaciju omogućen je IoT senzorima i aktuatorima i podržan je slojem transporta/komunikacije povezivanjem čvorova sa slojem aplikacije sistema sa grupom čvorova za obradu podataka i donošenje odluka kako bi se podržale različite vrste OT aplikacija. Različite komponente u ovim slojevima mogu biti povezane kroz različite bežične i žičane komunikacione protokole, uključujući i često spominjanu „Infrastrukturu interneta stvari zasnovanu na IP-u“. Kada takvi sistemi djeluju na fizički svijet kroz integraciju povezanih aktuatora, oni se nazivaju CPS, [5].



Slika 2 – Prikaz nivoa kod Iot/CPS sistema

Dakle, IoT čini osnovu za mnoge moderne složene CPS-ove. Suštinski, CPS-ovi nose svoje ime zbog interakcije sa fizičkim okruženjem kroz senzore i aktuatore.

3. BEZBJEDNOSNI ZAHTJEVI U CPS I IOT SISTEMIMA

Standardne bezbjednosne politike vode se po principima povjerljivosti, integriteta i dostupnosti, poznate i kao CIA (confidentiality, integrity, and availability) trijada. Ove politike se ojačavaju specifičnim bezbjednosnim zahtevima aplikacije i konačno se implementiraju kriptografskim primitivima i bezbjednosnim protokolima.

Istaknuti kriptografski primitivi su:

- Enkripcija simetričnim ključem: ova metoda koristi isti ključ za šifrovanje i dešifrovanje podataka (npr. AES, DES).
- Enkripcija asimetričnim ključem: ova metoda koristi različite ključeve za šifrovanje i dešifrovanje podataka (npr. RSA, ECC).
- Hash funkcije: ova metoda generiše kratak niz bita koji se koriste za provjeru integriteta i autentičnosti podataka (npr. SHA-256, MD5).
- Digitalni potpisi: ova metoda se koristi za potpisivanje podataka i provjeru potpisa (npr. DSA, ECDSA).
- Pseudonimizacija: ova metoda omogućava anonimizaciju podataka tako da se koriste pseudonimi umjesto stvarnih identiteta.
- Tokenizacija: ova metoda omogućava zamjenu ličnih podataka sa tokenima, što smanjuje rizik od curenja podataka.

Neki od najčešće korišćenih bezbjednosnih protokola su:

- Protokoli kriptografije: korišćenje šifrovanih komunikacija (SSL/TLS, AES, RSA, ECC) za zaštitu podataka prilikom prenosa.
- Protokoli za autentifikaciju: korišćenje metoda (OAuth, OpenID Connect, SAML, RADIUS) za provjeru istinitosti identiteta uređaja i korisnika.
- Protokoli za dostupnost: korišćenje metoda (CoAP, MQTT, DDS) za osiguravanje dostupnosti uređaja i sistema.
- Protokoli za razmjenu informacija: korišćenje standardizovanih protokola (JSON, XML, CBOR) za razmjenu podataka između uređaja i sistema.
- Protokoli za upravljanje bezbjednošću: korišćenje metoda (TLS, DTLS, IPSec) za upravljanje bezbjednošću uređaja i sistema, uključujući i ažuriranja i dijagnostiku.

Međutim, korišćenje kriptografskih primitiva i bezbjednosnih protokola ne garantuje potpunu sigurnost. CPS i IoT sistemi su skloni različitim vrstama napada, stoga je važno kontinuirano pratiti i poboljšavati sigurnost CPS i IoT sistema kako bi se osigurala što veća zaštita od napada.

Alternativni pristup bezbjednosnom dizajnu je modelovanje potencijalnih prijetnji. Microsoft je predložio model klasifikacije prijetnji zasnovan na sledećih šest kategorija:

- Lažiranje korisničkog identiteta.
- Neovlašćeno mijenjanje uskladištenih ili prenesenih podataka.
- Nepopravljivost, odnosno negiranje izvršenih radnji kada drugi korisnici ne mogu dokazati suprotno.
- Otkrivanje informacija ili kršenje povjerljivosti.
- Onemogućavanje usluga (DoS - Denial of service) koje čini mrežu/server nedostupnim.
- Povećanje privilegija za korisnika da izvrši neovlašćene radnje.

U savremenim CPS i IoT sistemima, ovaj model prijetnje se razmatra zajedno sa takozvanim površinama napada. Površina napada pruža ulaznu tačku za napadača da stekne kontrolu ili izvlači informacije iz ciljnog sistema. Pogrešno projektovani protokoli često podliježu jednostavnim napadima i predstavljaju nepredviđene površine napada, kao što je ilustrovano sledećim primjerom.

Primjer 1: Bežični standard 802.11b je podložan raznim DoS napadima [6]. Tamo, klijent bežične mreže može poslati poruku o prekidu povezivanja stanici za oslobađanje resursa nakon što je upotreba mreže za klijenta završena. Međutim, ova poruka se šalje bez ikakve autentifikacije, što u suštini omogućava bilo kojem korisniku da pošalje ovu poruku u ime drugog. Na taj način napadač može spriječiti drugog korisnika da se poveže na mrežu. U kontekstu CPS-a, ovaj DoS se može manifestovati kao ozbiljan problem dostupnosti, na primjer, ometanjem mreže ili MITM (man-in-the-middle – čovjek-u-sredini) napadima [7].

3.1. Bezbjednosni standardi

Standardizacija je česta metoda za donošenje politika za sprovođenje prakse, gdje domen bezbjednosti nije izuzetak. Osnovni standardi za sigurnost informacija, poput ISO/IEC 27002, se koriste kao šablon, a zatim se prilagođavaju i dodatno proširuju za potrebe aplikacije. U domenu CPS-ova, postoje napori standardizacije koji se posebno fokusiraju na sigurnost, npr. za zaštitu kritične infrastrukture, poput termoelektrana, elektroenergetskih mreža ili sistema upravljanja saobraćajem. ISA/IEC-62443 definiše skup standarda/preporuka za implementaciju industrijske automatizacije i kontrolnih sistema.

Poštovanje ovog standarda se reguliše od strane Instituta za bezbjednosnu usklađenost ISCI (ISA Security Compliance Institute). Perspektiva sigurnosti CPS-a na visokom nivou, nedavno je predstavljena kroz niz preporuka Nacionalnog instituta za standarde

i tehnologiju (NIST- National Institute of Standards and Technology) kako bi se upozorilo na sve veći broj slučajeva IoT napada. Međutim, treba napomenuti da, za razliku od Standarda za bezbjednost podataka industrije platnih kartica (PCI DSS - Payment Card Industry Data Security Standard) ili Federalnog standarda za obradu informacija (FIPS - Federal Information Processing Standard), standardizacija bezbjednosti u CPS/-IoT sistemima i njihova usklađenost su tek u početnoj fazi. Činjenica je da je u Senatu SAD-a nedavno predložen zakon o poboljšanju sajber bezbjednosti IoT uređaja, dok u Evropskoj uniji postoji konsolidovani napor od strane Evropske agencije za mrežnu i informacionu bezbjednost (ENISA - European Union Agency for Network and Information Security) da se postigne zajednički standard za sve članice [8].

Važno je napomenuti da i pored primjene ovih standarda, nije jednostavno obuhvatiti cijeli protokol složenog CPS-a i zaštititi ga od suptilnih ranjivosti. To se odražava u eksperimentalnim studijama napada na relativno nove CPS-ove, kao što su (polu)autonomna vozila [9], kao i na napade na sisteme, kao što su proizvodna postrojenja. Može se tvrditi da je zadatak standardizacije težak zbog: 1) pojave novih scenarija primjene koji kombinuju CPS/IoT; 2) povećanja obima domena koji se kreću od proizvodnje preko IT-a do bežične mreže; 3) povećanja uloge autonomnih agenata u ovim sistemima; 4) spajanja principa OT sigurnosti i IT sigurnosti. Ovu situaciju ilustrujemo sljedećim primjerom.

Primjer 2: U trenutnim pametnim telefonima zasnovanim na Androidu, mnoštvo internih senzora pruža precizne podatke o kretanju, gravitaciji, pozicioniranju, okruženju i orijentaciji telefona, između ostalog. Pristup ovim senzorima je neograničen i njime se ne upravlja. U nedavnom napadu [10], pokazano je da je tajnim prijavljivanjem (logovanjem) u senzorske podatke i korišćenjem ovih podataka moguće zaključiti ključne riječi koje je ukucao korisnik, na primjer, pin ili bilo koji drugi osjetljivi podatak, sa razumnom tačnošću.

U suštini, standardi se često usvajaju/unapređuju nakon napada i stoga mogu pružiti samo otpor prvog nivoa. Sve veći prodor pametnih komponenti u naš svakodnevni život može enormno povećati rizik od bezbjednosnog incidenta. Ova pitanja, na koja znatno utiče nemogućnost proizvođača CPS-ova da se suoče sa bezbjednosnim izazovima, dovela su do komplementarnog pravnog razvoja paralelno sa CPS/IoT bezbjednosnim standardima. Na primjer, nedavno je objavljeno izuzeće od zaštite autorskih prava za softver koji se izvršava na komponenti CPS/IoT. Ovo omogućava korisniku da ispita softver u elektronskoj kontrolnoj jedinici (ECU - electronic control unit) ili programabilnom logičkom kontroleru (PLC - programmable logic controller) CPS-a, kako bi otkrio nedostatke i uklonio ih, ako se identifikuju, nezavisno. Takav pristup omogućava sigurnosnu reviziju, sa eventualnim rastom sigurnosti kao usluge u CPS-u. Na isti način, američka administracija za hranu i lijekove U.S. FDA (U.S. Food and Drug Administration) objavila je upustva za upravljanje uređajima u slučaju prijetnje sajber sigurnosti [11].

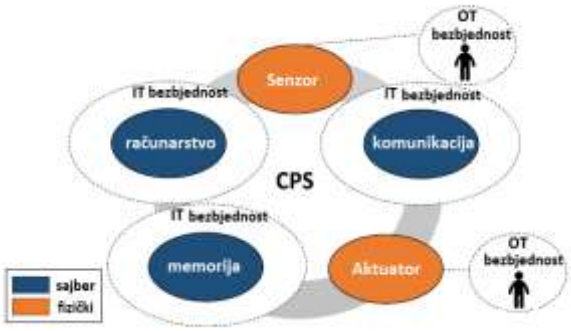
3.2 CPS bezbjednost

Sajber-fizički sistemi (CPS) odnose se na integraciju fizičkih i računarskih komponenti, što omogućava integraciju digitalnog i fizičkog svijeta. Ovi sistemi imaju potencijal da unaprijede industriju i poboljšaju efikasnost, ali predstavljaju i specifične izazove u pogledu bezbjednosti.

Jedan od glavnih izazova zaštite CPS-a je često to što oni rade u realnom vremenu i kontrolišu kritičnu infrastrukturu, kao što su sistemi transporta, elektromreže i proizvodne fabrike. Uspješan hakerski napad na CPS može imati ozbiljne posledice, kao što su gubitak života ili oštećenje kritične infrastrukture.

Još jedan izazov je to što CPS-ovi često imaju veliku površinu napada, sa mnogim različitim komponentama i interfejsima koji mogu biti meta napadača. Osim toga, CPS-ovi često imaju višestruke nivoe kompleksnosti, što otežava identifikaciju i rješavanje ranjivosti.

Opseg CPS-ova nadilazi tradicionalne informacione i komunikacione tehnologije i ulazi u oblast operativnih tehnologija (OT) prikazanih na slici 3, koje se obično nalaze u sistemima za kontrolu industrijskih procesa, kao što su: industrijski sistem za kontrolu ICS (industrial control system), distribuirani sistem za kontrolu DCS (distributed control system) i sistem za nadzornu kontrolu i prikupljanje podataka (SCADA – supervisory control and data acquisition).



Slika 3 – CPS-ovi: IT i OT bezbjednost

U tipičnoj OT implementaciji komponente mreže igraju ključnu ulogu u povezivanju uređaja (kao što su senzori i aktuatori) i računarskih sistema kako bi se olakšale funkcije nadzora i kontrole industrijskih operacija. Senzori i aktuatori u takvim sistemima su potrebni za nadzor nekih fizičkih karakteristika

industrijskih operacija koje su kritične za upravljačke sisteme da donesu pravovremene i efikasne odluke kroz neke nadzorne i kontrolne interfejse, kao što je SCADA.

Za razliku od tradicionalnog IT sistema, kompromitacija sigurnosti u CPS-u često dovodi do katastrofalnih posledica. Razlike u odnosu na tradicionalne IoT sisteme su detaljno opisane u nastavku:

- Fizički interfejs: Interfejsi senzora i aktuatora kod CPS-a dovode do novih površina napada, što čini razliku u odnosu na bezbjednost kod IT sistema. Napadač može iskoristiti fizički interfejs da oslabi bezbjednost CPS-a, bez potrebe da pregazi mehanizam kontrole pristupa koji je uspostavljen u OT modelu bezbjednosti. U tradicionalnoj bezbjednosti IT sistema, to bi se moglo dogoditi samo ako se podaci prenose kroz otvorenu mrežu.
- Kontrolni sistem: CPS-ovi u velikoj mjeri zavise od jedne ili više osnovnih kontrolnih mreža, koje su često integrisane sa fizičkim senzorima/aktuatorima, kao što je npr. implantabilni medicinski uređaj koji prikuplja korisničke podatke i pokreće radnje u slučaju abnormalnih vitalnih parametara. SCADA sistemi su sastavni dio modernih industrijskih CPS-ova, koji se suočavaju s velikim bezbjednosnim izazovima, još više zbog SCADA sistema povezanih na internet, [12]. Mnoge takve kontrolne mreže i komunikacijski protokoli su projektovani imajući na umu samo OT bezbjednost, te se stoga suočavaju s poteškoćama u upravljanju bezbjednošću putem sistema povezanog na internet.
- Dostupnost: Ozbiljnost prekida dostupnosti u CPS-ovima je mnogo veća nego u standalone digitalnom sistemu. Primjer takvog napada je napad na elektroenergetsku mrežu izveden 2015. godine, [13]. Treba imati na umu da za industrijske upravljačke sisteme bilo koji napad na dostupnost povećava ekonomski uticaj napada proporcionalno trajanju nedostupnosti.
- Vremensko ograničenje: Različiti skupovi ograničenja u realnom vremenu čine integralni aspekt CPS-a. Vrijeme izvršenja između događaja i njemu odgovarajućeg odgovora često je definisano strogo određenim rokom, koji, ako se propusti, može dovesti do neuspjeha kompletnog toka kontrole. Na primjer, sistemi za praćenje pametne energije raspoređuju prekidače koji izvršavaju isključenje izvoda u slučaju kvara. U slučaju kašnjenja u otkrivanju naglog povećanja struje, mreža može biti fizički oštećena, što na kraju može dovesti do neuspjeha cijelog sistema.
- Sociotehnički model: Tradicionalna IT bezbjednost čini samo dio veće sociotehničke bezbjednosti sistema. Za CPS, posebno industrijskih sistema, nije dovoljno samo definisati kontrolu pristupa već i društvene i ekonomske posledice prekida bezbjednosti. Ovaj problem se manje manifestuje u klasičnoj informacijsko bezbjednosnoj paradigmi zbog ograničenog izlaganja fizičkim interfejsima i ograničenjima. Međutim, za CPS-ove ovo postaje posebno važno zbog mogućnosti životno opasnih situacija ili takozvanih kinetičkih napada. Kinetički napadi su napadi na CPS sisteme koji izazivaju fizičke posledice ili štete na sistemu ili okruženju. To može uključivati napade na fizičke komponente sistema, kao što su senzori ili aktuatori, ili napade na kontrolne procese u sistemu koji izazivaju neželjene posledice u fizičkom svijetu. Primjeri kinetičkih napada mogu uključivati sabotiranje elektroenergetske mreže ili napad na proizvodnu liniju u industriji koja dovodi do fizičkog oštećenja ili prekida rada.

3.3. IoT Bezbjednost

Jedan od glavnih izazova zaštite IoT uređaja je u tome što se mnogi od njih proizvode sa ciljem uštede novca, što često znači da bezbjednost nije na vrhu liste prioriteta. Kao rezultat toga, ovi uređaji mogu imati slabe lozinke, mogu nedostajati odgovarajuća šifrovanja ili imati zastarjeli softver. Još jedan izazov je u tome što je IoT uređaje često teško patch-ovati i ažurirati, što otežava otklanjanje ranjivosti kada se otkriju. Osim toga, zbog toga što IoT uređaji često imaju duži vijek trajanja od tradicionalnih računarskih uređaja, teško je osigurati da su ažurirani sa najnovijim bezbjednosnim mjerama.

Za razliku od CPS-a, fokus IoT sistema je na povezivanju i, shodno tome, na upravljanju pouzdanim uređajima koji međusobno komuniciraju. U IOT mreži često imamo nove članove i stoga je od posebnog značaja uspostavljati sigurne kanale komunikacije. U nastavku je sažeto nekoliko karakteristika koje razlikujemo kada govorimo o IoT bezbjednosti:

- Upravljanje povjerenjem: glavni scenario upotrebe IoT uređaja su ad hoc senzorske mreže koje pronalaze primjenu u V2V (vehicle-to-vehicle/-vozilo-do-vozila) i V2I (vehicle-to-infrastructure/-vozilo-do-infrastrukture) komunikacijama, na primjer. U takvim mrežama, prihvatanje novog čvora i otkrivanje zlonamjernih čvorova su važni preduslovi za održavanje sigurnosnih politika netaknutima. Bilo je dosta studija o protokolima za upravljanje ključevima za bežične senzorske mreže, npr. putem preddistribucije ključeva, enkripcije zasnovane na identitetu, sertifikacijskih tijela i protokola za razmjenu ključeva. Uopšteno govoreći, ove studije spadaju u opštu temu upravljanja povjerenjem, što je posebno izazovno za

uređaje niske klase zbog opterećenja performansi sigurnog skladištenja ključeva ili atestiranja dinamičkog koda.

- Protokol bezbjednog rutiranja: IoT sistemi se kritički oslanjaju na statičke/dinamičke protokole rutiranja, koji mogu biti podvrgnuti različitim oblicima napada. Tipične protivmjere za napade protokola rutiranja zavise od: 1) pouzdane bazne stanice koja omogućava autentifikaciju i enkripciju; 2) višestrukog rutiranja; 3) bezbjednih protokola geografskog rutiranja.
- Integracija heterogenih mreža: IoT mreže obično su povezane s heterogenom mješavinom bežičnih komunikacionih mreža, od kojih svaka dolazi sa svojim sopstvenim protokolima bezbjednosti. Njihova međusobna kompatibilnost može zahtijevati konverziju formata podataka, što je teško preduzeti bez djelimičnog poznavanja korisnog dijela poruke. Osim toga, mogućnost i često neotkrivena prisutnost različitih kanala informacija ostaje stalna prijetnja [14].
- Zaštita privatnosti: IoT čvorovi mogu zahtijevati da se održi privatnost podataka/lokacije kao i anonimnosti dok učestvuju u mreži. Ovo se može osigurati pomoću bezbjednosti senzora, npr. RFID-/NFC privatnost ili privatnost opštih ugrađenih senzora, [15]. Anonimnost je očuvana, na primjer, generisanjem sličnih količina saobraćaja za određeni broj čvorova koji okružuju čvor za skupljanje podaka ili usvajanjem fraktalne propagacije koja uključuje širenje lažnih poruka na međučvorovima. Primjer: U nedavnoj demonstraciji napada na povezane IoT uređaje, istraživači su preuzeli kontrolu nad svim sijalicama koje su se nalazile u neposrednoj blizini, tako što su prvo zarazili sijalicu zlonamjernim firmverom. Napad je iskoristio ZigBee protokol i nepostojanje bilo kakve kriptografije asimetričnog ključa za uspostavljanje sigurnih kanala komunikacije kako bi se dobila mogućnost bežičnog ažuriranja drugih sijalica.

4. ZAKLJUČAK

Bezbjednost IoT i CPS sistema predstavlja značajan izazov zbog njihove složenosti i interakcije sa fizičkim svijetom. Potrebno je uzeti u obzir mnogobrojne faktore, uključujući integraciju heterogenih mreža, korišćenje sigurnih protokola komunikacije, implementaciju mjera za kontrolu pristupa i osiguravanje privatnosti i anonimnosti podataka i uređaja, vremenska ograničenja i sociotehnički model, kako bi se obezbijedile adekvatne mjere zaštite.

Bezbjednost IoT i CPS sistema predstavlja stalni izazov koji zahtijeva pažljivo razmatranje i proaktivne mjere kako bi se osigurao integritet i pouzdanost ovih sistema. Pored toga, neophodno je razvijati nove pristupe i tehnologije kako bi se mogle ispratiti brze promjene u ovom dinamičnom okruženju. Najaktuelniji pravci budućih istraživanja svakako mogu biti predlozi novih rješenja koja dodatno smanjuju kompleksnost procesa obrade podataka, sa aspekta bezbjednosti, u masivnim IoT uređajima, što produžava vijek trajanja baterije i u skladu je sa 6G zahtjevima. Takođe, svako rješenje koje dodatno smanji kašnjenje usled obrade u okviru bezbjednosnih algoritama doprinijeće razvoju kritičnih IoT sistema. Manja kompleksnost, veća energetska efikasnost, manje kašnjenje, primjena novih bezbjednosnih rješenja na fizičkom nivou i sl. biće zasigurno dalji pravci.

LITERATURA

[1] S. Kim, A Survey on Network Security for Cyber–Physical Systems: From Threats to Resilient Design, in *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1534 - 1573, June 2022.

[2] R. Patil, Medical Cyber–Physical Systems in Society 5.0: Are We Ready, in *IEEE Transactions on Technology and Society*, vol. 3, no. 3, pp. 189 - 198, June 2022.

[3] Available at: https://xymbot.com/en_gb/cyber-physical-systems-and-internet-of-things-where-are-we-going-to/

[4] H. Wang, Survey on Unmanned Aerial Vehicle Networks: A Cyber Physical System Perspective, in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1027 - 1070, Dec. 2019.

[5] S. S. Xu, A Networked Multirobot CPS With Artificial Immune Fuzzy Optimization for Distributed Formation Control of Embedded Mobile Robots, in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 414 - 422, Jan. 2020.

[6] K. Cao, A Survey on Edge and Edge-Cloud Computing Assisted Cyber-Physical Systems, in *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7806 - 7819, Nov. 2021.

[7] K. Huang, L. Yang, R. Fu, S. Zhou and Z. Hong, HASN: A hierarchical attack surface network for system security analysis, in *China Communications*, vol. 16, no. 5, pp. 137-157, May 2019.

[8] 8ENISA: Cybersecurity Standards and Certification. [Online]. Available: https://www.enisa.europa.eu-/topics/standards

[9] Á. Török, Z. Szalay and B. Sághi, New Aspects of Integrity Levels in Automotive Industry-Cybersecurity of Automated Vehicles, in *IEEE Transactions*

on Intelligent Transportation Systems, vol. 23, no. 1, pp. 383-391, Jan. 2022.

[10] M. Zhou *et al*, PressPIN: Enabling Secure PIN Authentication on Mobile Devices via Structure-Borne Sounds, in *IEEE Transactions on Dependable and Secure Computing*, Feb. 2022.

[11] Postmarket Management of Cybersecurity in Medical Devices. [Online]. Available: http://www.fda.-gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf

[12] A. Ajmal, Last Line of Defense: Reliability Through Inducing Cyber Threat Hunting With Deception in SCADA Networks, in *IEEE Access*, vol. 9, pp. 126789 - 126800, Sept. 2021.

[13] Analysis of the cyber attack on the Ukrainian power grid, EISAC, 2016. [Online]. Available: https://ics.-sans. org/media/E-ISAC_SANS_Ukraine_ DUC_-5.pdf

[14] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, Anatomy of Threats to the Internet of Things, in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1636-1675, Secondquarter 2019.

[15] Y. Luo, K. Fan, X. Wang, H. Li and Y. Yang, RUAP: Random rearrangement block matrix-based ultra-lightweight RFID authentication protocol for end-edge-cloud collaborative environment, in *China Communications*, vol. 19, no. 7, pp. 197-213, July 2022.

SUMMARY

SECURITY IN CYBER-PHYSICAL AND IOT SYSTEMS

The security of Cyber-Physical Systems (CPS) and the Internet of Things (IoT) is a significant issue due to the increasing integration of these systems into critical infrastructure, production and other industrial environments, as well as the growing use of IoT devices in various areas of life. It is therefore important to consider the security challenges in these systems and work on their resolution in order to maintain the stability and reliability of these systems. This paper discusses the security of CPS and IoT systems, including the architecture of such systems, security requirements and standards, as well as specific security issues that arise in both types of systems. In particular, CPS security is considered through the physical interface, control system, availability and time constraints, while IoT security is considered through trust management, secure routing protocols, integration of heterogeneous networks and privacy protection.

Key Words: *Internet of Things - IoT, Cyber-Physical Systems - CPS, security*