



KIBERNETIČKA SIGURNOST INDUSTRIJSKIH SUSTAVA

Mato Galović¹, Ivan Matasović², Mato Kokanović³, Zoran Crnac⁴

¹ Tehnička škola, Eugena Kumičića 55, Slavonski Brod 35000, Republika Hrvatska, mgalovic@unib.hr

² Tehnička škola, Eugena Kumičića 55, Slavonski Brod 35000, Republika Hrvatska, imatasovic@unib.hr

³ Tehnička škola, Eugena Kumičića 55, Slavonski Brod 35000, Republika Hrvatska, mkokanovic@unib.hr

⁴ Tehnička škola, Eugena Kumičića 55, Slavonski Brod 35000, Republika Hrvatska, zcrnac@unib.hr

Sažetak: Koncept Industrije 4.0 se temelji na inteligentnom umrežavanju strojeva i drugih proizvodnih sustava koristeći napredne informacijsko – komunikacijske tehnologije. Korištenjem napredne informacijsko – komunikacijske tehnologije tvornice postaju sve više izložene kibernetičkim napadima i prijetnjama, koji imaju za cilj gubitak podataka neophodnih za odvijanje proizvodnih procesa, a posredno i usporavanje procesa proizvodnje, dok u nekim slučajevima rezultiraju oštećenjem opreme koja se koristi. Analizom utjecaja na informacijsko – komunikacijske tehnologije moguće je razviti preventivni sustav kibernetičkih utjecaja i time osigurati određenu zaštitu procesa.

Cilj ovog rada je upoznavanje sa osnovnim aktivnostima i tehnologijama kibernetičke sigurnosti u provođenju koncepta Industrije 4.0. U radu je provedena analiza Europskog izvješća o kibernetičkoj sigurnosti, kao i predložena rješenja zaštite od kibernetičkih napada u industriji. Detaljnije su objašnjeni oblici kibernetičkih prijetnji, te načini njihovog sprječavanja korištenjem industrijskih sigurnosnih standarda koji preciziraju načine i metode kibernetičke zaštite u različitim sferama djelovanja.

Ključne riječi: Industrija 4.0, informatičko – komunikacijske tehnologije, kibernetička sigurnost, sigurnosni standardi

1. Uvod

Glavno obilježje četvrte industrijske revolucije je umrežavanje pametnih digitalnih uređaja bežičnim putem, pri čemu međusobna povezanost proizvodnih sustava omogućava veći stupanj umjetne inteligencije, kvalitetniju komunikaciju pametnih uređaja međusobno kao i njihovu komunikaciju sa sudionicima proizvodnog procesa. U zahtijevanoj komunikaciji razmjenjuju se bitni podaci za odvijanje proizvodnih procesa koji moraju očuvati svoj integritet kako bi se osigurala pouzdana kvaliteta industrijske proizvodnje.

Zbog toga je kibernetička sigurnost industrijskih sustava ključna za zaštitu kritične infrastrukture i industrijskih pogona od digitalnih prijetnji. Sigurnost i pouzdanost korištenja informacijske tehnologije (IT) odnosi se na zaštitu podataka, sustava i mreža od prijetnji te osiguravanje kontinuiranog i nesmetanog rada IT infrastrukture. Zaštita podataka je bitna iz dva osnovna razloga:

- krađa i neovlašteno korištenje podataka;
- utjecaj na podatke koji može štetno djelovati na njihovo korištenje;

- Razvojem IT tehnologije u cilju unapređenja industrijske proizvodnje, kibernetički napadi postaju sve sofisticiraniji, te je potrebna kontinuirana aktivnost u cilju njihovog otkrivanja, te sprječavanja utjecaja na odvijanje proizvodnje.
- Prema izvješću Agencije Europske unije za kibernetičku sigurnost (ENISA), postoji nekoliko glavnih kibernetičkih prijetnji (2022.) (Europski parlament 2023)
- ucjenjivački softver (ransomware). Prema podacima ENISA-e, iznos otkupnine je porastao s 13 milijuna eura u 2019. na 62 milijuna u 2021., a prosječna pojedinačna otkupnina se udvostručila sa 71 tisuće eura u 2019. na 150 tisuća eura u 2020. Procjenjuje se da je ucjenjivački softver u 2021. na globalnoj razini izazvao 18 milijardi eura štete, što je čak 57 puta više nego 2015. (Europski parlament 2023);
- zlonamjerni softver (malware) koji trajno ili privremeno oštećuje sustav, omogućava neovlašteni pristup, ometa rad sustava ili mreže, sve do krađe podataka. Prema podacima ENISA-e, u prvoj polovici 2022. se dogodilo više napada vezanih za Internet stvari nego u prethodne četiri godine;
- društveni inženjering koji se manifestira kroz iskorištavanje ljudske pogreške otvaranjem zlonamjernih dokumenata, nesigurne e-pošte ili posjećivanjem sigurnosno neprovjerenih web stranica;
- prijetnje podacima kroz povredu podataka ili njihovo objavljivanje bez dopuštenja vlasnika;
- prijetnje dostupnosti ili uskraćivanja pristupa podacima i uslugama. Jedan od najčešćih oblika ove vrste prijetnji je preopterećenje mrežne infrastrukture u cilju nedostupnosti potrebnih podataka;

- Internetska dostupnost. Sprječavanje dostupnosti interneta bitno smanjuje komunikaciju u cilju prikupljanja potrebnih informacija, a time i mogućnost njihovog korištenja;

Kibernetički napadi na industrijske sustave mogu uzrokovati zastoj i kvarove u proizvodnji, gubitak podataka za rad automatiziranih upravljačkih sustava (PLC, SCADA), a u određenoj mjeri mogu utjecati na sigurnost ljudi i okoliša.

Izvješće Nozomi Network Labs, koji proučava utjecaj kibernetičkih napada na industrijske sustave bilježi da je tijekom prve polovice 2024. godine broj kibernetičkih prijetnji bio najveći u sektoru proizvodnje, slijedi sektor energetike, komunikacija i transportnih sustava (IoT Cyber Security 2025)

Istraživanja Agencije Europske unije za kibernetičku sigurnost pokazalo je da je razina kibernetičkih prijetnji tijekom jednogodišnjeg razdoblja (srpanj 2023. do lipanj 2024.) u značajnom porastu. U svom izvješću o stanju kibernetičke sigurnosti u Europskoj uniji za 2024. godinu definirana je količina incidenata prema vrsti prijetnje u navedenom vremenskom razdoblju (Izvješće 2024).

Najviše incidenata je uzrokovano Dos/Ddos/Rdos prijetnjama koje za posljedicu imaju uskraćivanje usluga korištenja potrebnih podataka iz jednog zlonamjernog izvora (Dos) kako bi se oslabila pozicija korisnika, više njih (Ddos) ili uskraćivanja usluga u cilju iznude otkupnine.

Značajan broj incidenata je vezan za ransomware prijetnje. Nakon zaraze *ransomware* može šifrirati datoteke ili onemogućiti njihovo korištenje. Od korisnika čije je računalo zaraženo traži se otkupnina u zamjenu za daljnje normalno korištenje računala. (CARNet 2025)

Jednako tako je značajan zlonamjerni utjecaj na podatke u prijenosu koji se

manifestira kroz krađu podataka, sprječavanje njihovog korištenja ili aktivnosti usmjerene na izmjenu podataka.

Uz sve ostale evidentirane prijetnje, kao i činjenice da razvoj novih kibernetičkih prijetnji prati razvoj informacijskih tehnologija, potrebno je posebnu pažnju posvetiti kibernetičkoj sigurnosti.

Osnivanjem stručnih organizacija na globalnoj razini, kao što je Agencija Europske unije za kibernetičku sigurnost (ENISA), ili onih na razini država, kao što je Nacionalni centar za kibernetičku sigurnost (NCSC – HR), razvijaju se regulativni okviri za razvoj i praćenje provedbe kibernetičke sigurnosti. Jedan od njih je i industrijski sigurnosni standard ISA/IEC 62443.

ISA/IEC 62443 je međunarodni niz standarda koje je razvila Međunarodna elektrotehnička komisija (IEC) za kibernetičku sigurnost u industrijskoj automatizaciji i upravljačkim sustavima (IACS). Primarna svrha norme IEC 62443 je zaštita industrijskih okruženja od rastućih kibernetičkih prijetnji. Serija standarda ISA/IEC 62443 definira zahtjeve i procese za implementaciju i održavanje elektronički sigurnih industrijskih automatizacijskih i upravljačkih sustava (IACS). (ISA 2025)

2. Materijali i metode

Usporedno sa ubrzanim razvojem informacijskih tehnologija koje omogućavaju kvalitetnu i nesmetanu komunikaciju komponenti procesnih sustava Industrije 4.0, razvijaju se i različite vrste računalnih napada koji imaju za cilj nanijeti štetu ili osigurati pristup, a samim time i steći kontrolu nad važnim dokumentima vezanim za odvijanje procesa.

Kako je cilj implementacije i razvoja Industrije 4.0 povećanje učinkovitosti proizvodnje, a to se postiže prilagodbom novim tehnologijama i tehnologijama u razvoju, potrebno je osigurati zaštitu

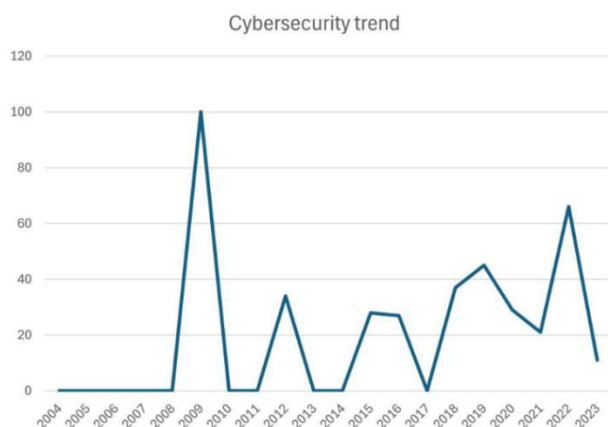
podataka koji su bitni za relevantno funkcioniranje koncepta Industrije 4.0. Prvi i osnovni zadatak je osigurati pouzdano korištenje i prijenos podataka, što podrazumijeva ostvarenje adekvatne kibernetičke sigurnosti.

Jedna od glavnih briga u kontekstu kibernetičke sigurnosti Industrije 4.0 jest mogućnost da kibernetički napadi poremete proizvodni proces. U proizvodnom okruženju, čak i manji poremećaj može imati značajne posljedice, uključujući kašnjenja i financijske gubitke. Osim toga, integracija umjetne inteligencije i strojnog učenja u proizvodne procese znači da postoji mogućnost da zlonamjerni akteri manipuliraju ili poremete te sustave, što dovodi do neispravnih ili čak opasnih proizvoda (Teixiera, Asencio 2025).

Prema definiciji, kibernetička sigurnost je umijeće zaštite mreža, uređaja i podataka od neovlaštenog pristupa ili kriminalne upotrebe te praksa osiguranja povjerljivosti, integriteta i dostupnosti informacija (Pochmara, Sietlicka 2024).

Prema J. Pochmara i A. Swietlicka (Pochmara, Sietlicka 2024), interes za kibernetičku sigurnost u kontekstu Industrije 4.0 doživio značajan porast počevši oko 2009. godine, s vrhuncem u 2022. godini. Interes je ostao relativno nizak od 2004. do 2008. godine, postupno se povećavajući u 2009. godini, a zatim ima promjenjivi trend u sljedećim godinama. Postoje povremeni skokovi interesa, kao što su bili 2012., 2015., 2016., 2018. i 2019. godine, ali najznačajniji vrhunac događa se 2022. godine, što ukazuje na pojačan fokus na kibernetičku sigurnost unutar Industrije 4.0 tijekom tog razdoblja.

Prema slici 1, vrijednost 100 označava najveći interes za kibernetičku sigurnost, dok vrijednost 50 znači da je interes upola manji. Vrijednost 0 označava da nema dovoljno dostupnih podataka za zadani pojam.



Slika 1. Trend kibernetičke sigurnosti na temelju Google Trendsa (Pochmara, Sietlicka 2024)

2.1. Vrste kibernetičkih prijetnji

Prema Oumaima El Kouari, Saïida Lazaar i Tarik Achoughi, najčešći tipovi prijetnji vezanih za Industrijski Internet (IIoT) [8] su:

- napadi s naprednim trajnim prijetnjama (*Advanced Persistent Threat - APT*);
- napadi uskraćivanja usluge (*Denial of Service - DoS*);
- napadi tipa "čovjek u sredini" (*Man In The Middle - MitM*);
- malware softver;
- *phishing* napadi;
- napadi autentifikacije;

2.2. Sigurnost i pouzdanost korištenja informacijske tehnologije

Sigurnost i pouzdanost korištenja informacijske tehnologije (IT) odnosi se na zaštitu podataka, sustava i mreža od prijetnji, te osiguravanje kontinuiranog i nesmetanog rada IT infrastrukture. U suvremenim organizacijama i društvu, IT sustavi igraju ključnu ulogu u poslovanju, zbog čega je važno implementirati sveobuhvatan pristup za osiguranje njihovog ispravnog i sigurnog rada.

Industrijska informacijska tehnologija (IIT) funkcionira kao veza između područja informacijske tehnologije (IT) i područja operativne tehnologije (OT) (Kouari, Lazaar 2025). Pomaže u

prikupljanju podataka iz OT područja i njihovom prijenosu u IT područje. Ovi podaci nisu izravno povezani s upravljanjem strojevima i sustavima, ali su ključni za kontrolu i optimizaciju procesa, praćenje kvalitete, logistiku i protok materijala. Stoga se koncept sigurnosti i pouzdanosti informacijske tehnologije općenito primjenjuje i na industrijsku informacijsku tehnologiju koju koriste sustavi Industrije 4.0.

Ključni koncepti sigurnosti informacijske tehnologije su pokazani slikom 2.



Slika 2. Koncepti sigurnosti i pouzdanosti informacijske tehnologije

Sigurnost informacija odnosi se na praksu zaštite informacija od neovlaštenog pristupa, otkrivanja ili izmjene i uništenja informacija. Sigurnost mreže ima za cilj zaštititi mreže od neovlaštenog pristupa, što omogućuje krađu podataka i izvođenje zlonamjernih napada.

Fizička sigurnost interneta odnosi se na zaštitu fizičke infrastrukture koja omogućuje funkcioniranje internetske mreže.

Malware zaštita - Zlonamjerni program općenito je poznat malware, namjerno je dizajniran da uzrokuje probleme u mrežama i šteti na razne načine. Primarni cilj malwarea je poremetiti

normalno izvršavanje ili dobiti neovlašteni pristup (Gupta et al 2025). U ovisnosti o načinu na koji zlonamjerni softver napada podatke, i rezultatu njegovog djelovanja postoje različite vrste prema kojim se posljedično određuje i način zaštite od njihovog djelovanja. Upravljanje identitetom i pristupom (Identity and access management - IAM) je složen i ključan proces identificiranja, pažljivog praćenja, učinkovite kontrole. Obuhvaća sveobuhvatan raspon aktivnosti koje omogućuju nesmetano funkcioniranje sustava kontrole pristupa, diktirajući i regulirajući dozvole za dopušteni i ograničeni pristup (Ghadge 2024).

Backup podataka (sigurnosna kopija podataka) je proces izrade kopije podataka kako bi se osigurala njihova dostupnost i zaštita u slučaju gubitka podataka, oštećenja, tehničkog kvara, prirodnih katastrofa ili drugih problema. Backup je ključan dio svake strategije za oporavak od katastrofa (Disaster Recovery) i osigurava kontinuitet poslovanja.

Enkripcija (ili šifriranje) je kodiranje informacija tako da im neovlaštene osobe ne mogu pristupiti. Ako se podaci u šifriranom obliku izgube ili ukradu, postoji minimalan rizik od otkrivanja jer napadač neće imati ključ za dešifriranje (ESET 2025).

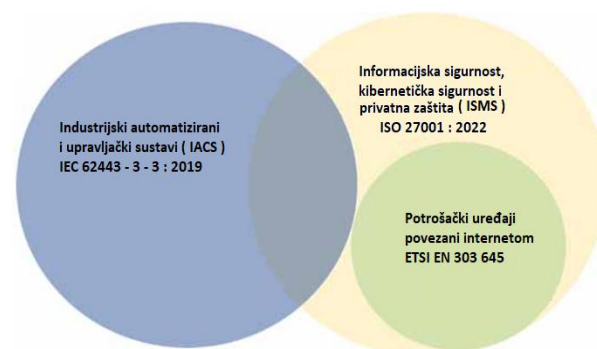
Ažuriranje softvera odnosi se na proces nadogradnje postojećih programa i operativnih sustava kako bi se poboljšala njihova funkcionalnost, sigurnost, stabilnost i performanse. Ažuriranja mogu uključivati ispravke grešaka, sigurnosne zakrpe, nove značajke i optimizacije.

Praćenje i nadzor sustava (eng. Monitoring) je proces kontinuiranog praćenja rada i performansi računalnih sustava, mreža, aplikacija i drugih IT resursa kako bi se osiguralo njihovo optimalno funkcioniranje, sigurnost i dostupnost.

Edukacija korisnika je bitna iz razloga sigurnosti korištenja IT tehnologije. Također, kao posljedica brzog razvoja IT sustava, potrebno je provoditi kontinuiranu edukaciju sa ciljem stjecanja kompetencija vezanih za nove situacije.

3. Rezultati i rasprava

Standardi kibernetičke sigurnosti pružaju strukturirani pristup upravljanju i procjeni rizika kibernetičke sigurnosti. Oni su primarni izvor sigurnosnih zahtjeva i kontrola koje organizacije koriste za smanjenje vjerojatnosti i utjecaja kibernetičkih napada. Postoji velik broj sigurnosnih standarda. Na primjer, samo serija ISO/IEC 27000 obuhvaća preko 60 standarda koji se bave širokim spektrom problema sigurnosti informacija (Džebar, Nordstorm, 2023). Iako su standardi kibernetičke sigurnosti, ISO/IEC 27001, ETSI EN 303 645 i ISA/IEC 62443-3-3, izvorno dizajnirani za različita okruženja, oni dijele brojne zajedničke i generičke zahtjeve kibernetičke sigurnosti koji su valjani i primjenjivi u različitim industrijama i ICT okruženjima (Džebar, Nordstorm, 2023).



Slika 3. Povezanost standarda kibernetičke sigurnosti (Džebar, Nordstorm, 2023)

3.1. Standard ISO/IEC 27001

Standard ISO/IEC 27001 predstavlja se kao standard koji specificira zahtjeve za uspostavljanje, provedbu, održavanje i kontinuirani razvoj strategije sigurnosti informacija. Osim toga, uključuje

potrebne okolnosti koje su prilagođene kako bi ispunile očekivanja tvrtke za procjenu i upravljanje prijetnjama sigurnosti podataka. Ovi preduvjeti su bitni za osiguravanje učinkovitog ublažavanja rizika sigurnosti informacija. Uvjeti navedeni u ISO/IEC 27001 nisu specifični, što znači da se očekuje da će se primjenjivati na sve organizacije, bez obzira na vrstu, veličinu ili prirodu poslovanja (Kitsios, Chatzidimitriou, Kamariotou, 2025).

Norma ISO 27001 osigurava povjerljivost, integritet i dostupnost, što su glavni sigurnosni ciljevi ove norme. Povjerljivost je namijenjena osiguravanju da su informacije dostupne samo ovlaštenim osobama primjenom mehanizama šifriranja i kontrole pristupa. Integritet osigurava da se podaci mijenjaju samo na ovlaštene načine, što štiti organizaciju od napadača koji pokušavaju promijeniti informacije, a također štiti od nenamjernih tehničkih pogrešaka. Dostupnost osigurava da su informacije dostupne sustavu ili ovlaštenim osobama kad god su potrebne (Junaid, 2025).

Analizirajući ciljeve standarada ISO/IEC 27001, njegova učinkovitost se pokazuje kroz smanjenje utjecaja kibernetičkih napada, te osiguranje integriteta svih relevantnih podataka bitnih za organizaciju koja ga provodi. Posredno, standard omogućava veću učinkovitost i ekonomičnost proizvodnje te smanjenje tehnoloških rizika u odvijanju proizvodnih procesa.

Standard ETSI EN 303 645 definira osnovne sigurnosne zahtjeve, takozvane odredbe, za potrošačke IoT uređaje. Prema uvodu u normu ETSI EN 303 645, norma sa svojim osnovnim sigurnosnim zahtjevima „nije namijenjena rješavanju svih sigurnosnih izazova povezanih s potrošačkim IoT-om. Također se ne usredotočuje na zaštitu od napada koji su dugotrajni/sofisticirani ili koji zahtijevaju trajni fizički pristup uređaju. Umjesto toga, fokus je na tehničkim

kontrolama i organizacijskim politikama koje su najvažnije u rješavanju najznačajnijih i najraširenijih sigurnosnih nedostataka“ (Körner et al 2025). Korištenje norme ETSI EN 303 645 omogućuje proizvođačima da osiguraju niz značajki u IoT uređajima za zaštitu osobnih podataka korisnika, kao što je na primjer davanje potrošačima jasnih i transparentnih informacija o tome koji se osobni podaci obrađuju, kako se koriste, od koga i u koje svrhe.

3.2. Industrijski sigurnosni standard ISA/IEC 62443

Standard ISA/IEC 62443 (serija standarda) definira zahtjeve i procese za implementaciju i održavanje elektronički sigurnih industrijskih automatizacijskih i upravljačkih sustava (IACS). ISA/IEC standardi postavljaju standarde kibernetičke sigurnosti u svim industrijskim sektorima koji koriste IACS, uključujući automatizaciju zgrada, proizvodnju i distribuciju električne energije, medicinske uređaje, transport i procesne industrije poput kemikalija te nafte i plina (ISA, 2025).

Temeljno načelo standarda ISA/IEC 62443 je koncept zajedničke odgovornosti kao ključnog elementa kibernetičke sigurnosti u području automatizacije. Ključne skupine dionika moraju se uskladiti kako bi osigurale sigurnost, integritet, pouzdanost i zaštitu upravljačkih sustava. Standardi definiraju zahtjeve za ključne skupine dionika koje su uključene u kibernetičku sigurnost upravljačkih sustava. Serija ISA/IEC 62443 bavi se sigurnošću industrijskih automatizacijskih i upravljačkih sustava (IACS) tijekom cijelog njihovog životnog ciklusa (što se odnosi na sve automatizacijske i upravljačke sustave, ne samo industrijske) (ISA, 2025).

Standardi ISA/IEC 62443 pružaju smjernice koje uključuju:

- Definiranje zajedničkih pojmova, koncepata i modela koje mogu koristiti svi dionici odgovorni za kibernetičku sigurnost kontrolnih sustava;

- Pomaganje vlasnicima imovine u određivanju razine sigurnosti potrebne za zadovoljavanje njihovih jedinstvenih poslovnih potreba i potreba u vezi s rizikom;
- Uspostavljanje zajedničkog skupa zahtjeva i metodologije životnog ciklusa kibernetičke sigurnosti za razvojne programere proizvoda, uključujući mehanizam za certificiranje proizvoda i procesa razvoja dobavljača;
- Definiranje procesa procjene rizika koji su ključni za zaštitu kontrolnih sustava (ISA, 2025);

Serijski standardi ISA/IEC 62443 raspoređeni su u četiri osnovne skupine koje odgovaraju fokusu njihove primjene (ISA, 2025):

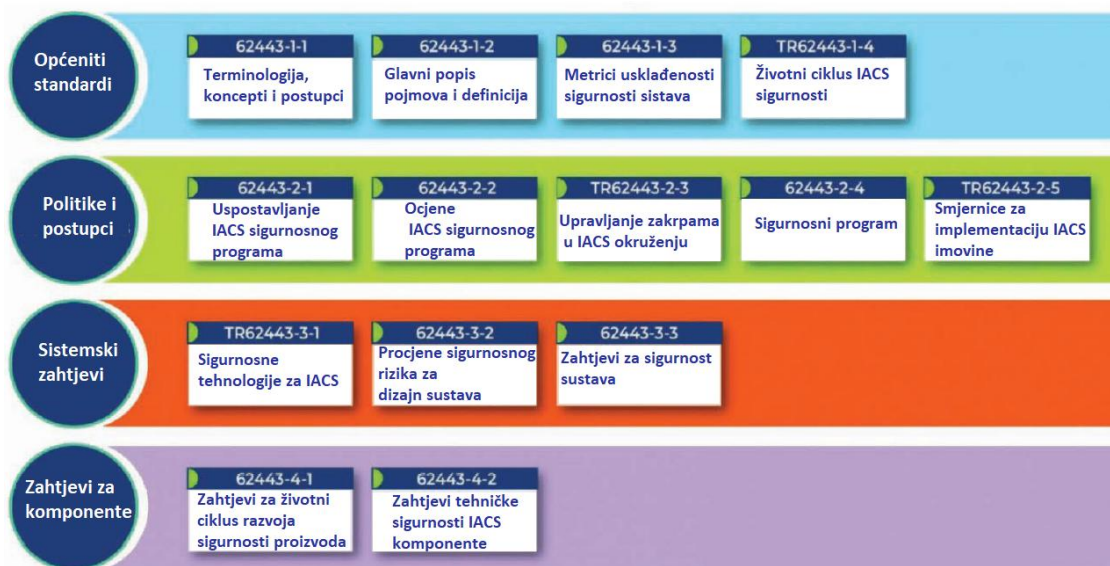
1. skupina – Općeniti standardi koji obuhvaćaju dokumente koji su zajednički za cijelu seriju standarda.

2. skupina – Politike i postupci sadrži dokumente koji su usmjereni na politike i postupke povezane sa sigurnošću IACS-a.

3. skupina – Sistemski zahtjevi sadrže dokumente vezane za zahtjeve na razini sustava

4. skupina – Zahtjevi za komponente – sadrže dokumente koji daju informacije o specifičnim i detaljnim zahtjevima povezanim s razvojem IACS proizvoda. ISA/IEC 62433 je ključan za industrijsku kibernetičku sigurnost jer pruža sveobuhvatan okvir za rješavanje rizika od kibernetičkih napada. Obuhvaća procjenu rizika, dizajn sustava, siguran razvoj i uloge dionika sustava, pomažući industrijskim organizacijama da poboljšaju svoju sigurnost i održe kontinuitet rada.

Detaljni prikaz politike pojedinih skupina je pokazan na slici 4.



Slika 4. Serija ISA/IEC 62334 standarda (ISA, 2025).

4. Zaključak

U radu se analiziraju aktivnosti i tehnologije kibernetičke sigurnosti sustava u konceptu Industrije 4.0. Bitan naglasak je stavljen na kibernetiku informacijsko-komunikacijskih tehnologija. Ranjivost ovih sustava je uzrokovana zlonamjernim aktivnostima u cilju krađe i neovlašteno korištenje podataka, te utjecaja na podatke koji

može štetno djelovati na njihovo korištenje. Kako je razvoj sustava za zlonamjerno djelovanja proporcionalan razvoju sustava industrijske proizvodnje, potreban je kontinuirani i svrsishodan mehanizam zaštite. Koncepti sigurnosti i pouzdanosti informacijske tehnologije su definirani standardima kibernetičke sigurnosti koji pružaju strukturirani pristup upravljanju i procjeni rizika kibernetičke sigurnosti.

Oni definiraju razinu sigurnosnih zahtjeva i kontrola koje je potrebno koristiti za smanjenje vjerojatnosti i utjecaja kibernetičkih napada. Primjenom navedenih standarda uz kontinuirano praćenje i edukaciju u području kibernetičke sigurnosti, omogućuje se kvalitetan okvir za nesmetan razvoj i provođenje aktivnosti Industrije 4.0.

5. Literatura

Europski parlament, Cybersigurnost: glavne i rastuće prijetnje, <https://www.europarl.europa.eu/topics/hr/article/20220120STO21428/kibersigurnost-glavne-i-rastuce-prijetnje> (21. ožujka 2023.)

<https://www.nozominetworks.com/ot-iot-cybersecurity-trends-insights-february-2025> (veljača 2025.)

Izviješće o stanju kibernetičke sigurnosti u Uniji za 2024. – sažeta verzija .pdf <https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union> (3. prosinac 2024.)

Hrvatska akademska i istraživačka mreža CARNET - <https://www.cert.hr/19795-2/ransomware/> (veljača 2025.)

Međunarodno društvo za automatizaciju (ISA) <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards> (veljača 2025.)

Henrique Teixeira, Claudia Asencao, Joao Goncalves, ergio Francisco Sargo Ferreira Lopes - Kibernetička sigurnost u Industriji 4.0. i IoT : Izazovi i prilike https://www.researchgate.net/publication/381349261_Cybersecurity_in_Industry_40_and_Internet_of_Things_Challenges_and_Opportunities (svibanj 2025.)

Janusz Pochmara i Aleksandra Swietlicka : Kibernetička sigurnost industrijskih sustava – izvješće za 2023. godinu (25.

ožujak 2024.)
<https://www.mdpi.com/2079-9292/13/7/1191>

Oumaima El Kouari, Saïda Lazaar i Tarik Achoughi : Jačanje industrijske kibernetičke sigurnosti: nova arhitektura industrijskog interneta stvari poboljšana integracijom honeypota , Međunarodni časopis za elektrotehniku i računarstvo (IJECE) Svezak 15, br. 1, veljača 2025., str. 1089 – 1098, <https://ijece.iaescore.com/index.php/IJECE/article/view/36124>

Nikhil Ghadge - Poboljšanje otkrivanja prijetnji u sustavima upravljanja identitetom i pristupom (IAM), Međunarodni arhiv časopisa za znanost i istraživanje, 2024., 11(02), 2050–2057, travanj 2024.

Ketan Gupta ; Nasmin Jiwani ; Md Haris Uddin Sharif ; Ripon Datta ; Neda Afreen - Pristup neuronskih mreža za klasifikaciju zlonamjernog softvera, <https://ieeexplore.ieee.org/abstract/document/10037653> (svibanj 2025.)

<https://ijsra.net/content/enhancing-threat-detection-identity-and-access-management-iam-systems> (svibanj 2025.)

ESET korisnička aplikacija, <https://help.eset.com/glossary/hr-HR/encryption.html> (svibanj 2025.)

Fatiha Džebbar, Kim Nordström - Komparativna analiza standarda industrijske kibernetičke sigurnosti, Objavljeno u: IEEE Access (Svezak: 11), kolovoz 2023. <https://ieeexplore.ieee.org/abstract/document/10210561> (svibanj 2025.)

Fotis Kitsios, Elpiniki Chatzidimitriou i Maria Kamariotou - Standard upravljanja sigurnošću informacija ISO/IEC 27001: Kako izvući vrijednost iz podataka u IT sektoru, izdanje Upravljanje kvalitetom i održivost <https://ideas.repec.org/a/gam/jsusta/v>

15y2023i7p5828-d1108964.html
(svibanj 2025.)

Ta-Seen Junaid - ISO 27001:
Upravljanje sigurnošću informacija,
Fakultet računalnih znanosti i
inženjerstva Sveučilište primijenjenih
znanosti Frankfurt Frankfurt na Majni,
Njemačka
https://www.researchgate.net/profile/Ta-Seen-Junaid/publication/367166657_ISO_27001_Information_Security_Management_Systems/links/63c4e6536fe15d6a5722c964/ISO-27001-Information-Security-Management-Systems.pdf
(svibanj 2025.)

Felix Körner, Pascal Schäfer, Holger Zwingmann, Bettina Schnor, Samim Ahmadi - Trenutni izazovi implementacije ETSI EN-a 303 645 kao osnovni sigurnosni standard za certifikaciju sigurnosti potrošačkog IoT-a, Institut za računalne znanosti, Sveučilište u Potsdamu, Njemačka
<https://www.techrxiv.org/doi/full/10.36227/techrxiv.24711672> (svibanj 2025.)

Međunarodno društvo za automatizaciju (ISA), <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>

Međunarodno društvo za automatizaciju (ISA), Sigurnost industrijskih automatizacijskih i upravljačkih sustava Pregled standarda ISA/IEC 62443
<https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/ISAGCA%20Quick%20Start%20Guide%20FINAL.pdf> (svibanj 2025.)

CYBER SECURITY OF INDUSTRIAL SYSTEMS

Summary: The concept of Industry 4.0 is based on intelligent networking of machines and other production systems using advanced information and communication technologies. Through the use of advanced information and communication technology, factories become increasingly exposed to cyber attacks and threats, which aim at the loss of data necessary for the development of production processes, and indirectly also the slowing down of the production process, while in some cases it results in damage to the equipment being used. By analyzing the impact on information and communication technologies, it is possible to develop a preventive system of cybernetic influences and thereby ensure a certain protection of the process.

The aim of this paper is to familiarize with the basic activities and technologies of cyber security in the implementation of the concept of Industry 4.0. The paper contains an analysis of the European report on cyber security, as well as proposed solutions for protection against cyber attacks in the industry.

The forms of cyber threats and the ways of their use are explained in more detail using industrial security standards that specify the ways and methods of cyber protection in different spheres of activity.

Keywords: Industry 4.0, IT - communication technologies, cyber security, security standards