37. Саветовање CIGRE Србија 2025
СИГУРНОСТ, СТАБИЛНОСТ, ПОУЗДАНОСТ И RESILIENCE ЕЛЕКТРОЕНЕРГЕТСКОГ СИСТЕМА
МУЛТИСЕКТОРСКО ПОВЕЗИВАЊЕ У ЕНЕРГЕТИЦИ И ПРИВРЕДИ
26 - 30. мај 2025, Копаоник

DOI: 10.46793/CIGRE37.D2.09

D2.09

UNAPREĐENJE BEZBEDNOSTI SCADA INFRASTRUKTURE U ELEKTROENERGETSKOM PRENOSU KROZ IMPLEMENTACIJU REŠENJA ZA ZAŠTITU INDUSTRIJSKIH SISTEMA

IMPROVING THE SECURITY OF SCADA INFRASTRUCTURE IN THE ELECTRIC POWER TRANSMISSION THROUGH THE IMPLEMENTATION OF INDUSTRIAL SYSTEM PROTECTION SOLUTIONS

Nina Đuričić, Jovana Đukić, Neven Nikolić, Mladen Dragićević, Suzana Mladenović*

Kratak sadržaj: Razvoj i digitalizacija elektroenergetskog prenosa značajno su unapredili nadzor i kontrolu sistema, ali su istovremeno povećali izloženost SCADA (Supervisory Control and Data Acquisition) sistema kao i celokupne OT (Operational Technology) infrastrukture sajber pretnjama. Napadi iz prakse, poput Stuxnet-a, Industroyer-a i BlackEnergy-a, pokazali su koliko su i industrijski sistemi zapravo ranjivi iako nisu, ili ne bi trebalo da budu, izloženi Internetu, pri čemu bi kompromitacija SCADA infrastrukture mogla imati ozbiljne posledice po stabilnost i kontinuitet rada elektroenergetskih sistema. Tradicionalna IT bezbednosna rešenja nisu prilagođena specifičnostima OT okruženja, što zahteva primenu specijalizovanih sigurnosnih tehnologija. Rad obuhvata analizu najčešćih sajber pretnji u OT infrastrukturi elektroenergetskog prenosa, kao što su neovlašćeni pristup komponentama SCADA sistema, kompromitacija industrijskih uređaja i lateralno kretanje napadača kroz mrežu. Poseban fokus stavljen je na uticaj različitih komponenti KICS (Kaspersky Industrial CyberSecurity) sistema koji je implementiran kao unapređenje bezbednosti sistema, uključujući detekciju anomalija, zaštitu krajnjih tačaka i analizu mrežnog saobraćaja, pri čemu se vodi računa o očuvanju neometanog rada operativnih procesa unutar elektroenergetskih postrojenja. U okviru unapređenja bezbednosti kritičnih sistema unutar Elektromreža Srbije, KICS platforma je već implementirana u lokalnim trafostanicama, regionalnim dispečerskim centrima, a uskoro će biti integrisana i u Nacionalni dispečerski centar, čime se uspostavlja jedinstven i centralizovan sistem zaštite OT infrastrukture. KICS platforma omogućava proaktivnu zaštitu kritične infrastrukture, smanjenje rizika od sajber napada i efikasnije upravljanje bezbednosnim incidentima, što značajno povećava otpornost industrijske mreže na savremene sajber pretnje.

Ključne reči: *SCADA, OT infrastruktura, KICS, sajber pretnje, industrijska sajber bezbednost, zaštita kritične infrastrukture.*

* Nina Đuričić, Elektromreža Srbije, nina.djuricic@ems.rs
Jovana Đukić, Elektromreža Srbije, jovana.djukic@ems.rs
Neven Nikolić, Elektromreža Srbije, neven.p.nikolic@ems.rs
Mladen Dragićević, Elektromreža Srbije, mladen.dragicevic@ems.rs
Suzana Mladenović, Elektromreža Srbije, suzana.mladenovic@ems.rs

Abstract: The development and digitalization of electric power transmission have significantly improved the monitoring and control of systems, but have also increased the exposure of SCADA (Supervisory Control and Data Acquisition) systems and the entire OT (Operational Technology) infrastructure to cyber threats. Real-world attacks, such as Stuxnet, Industroyer, and BlackEnergy, have demonstrated how vulnerable industrial systems can be, even though they are not, or should not be, exposed to the Internet. A compromise of the SCADA infrastructure could have serious consequences for the stability and continuity of electricity grid operations. Traditional IT security solutions are not tailored to the specifics of the OT environment, which requires the implementation of specialized security technologies. This paper includes an analysis of the most common cyber threats in the OT infrastructure of electric power transmission, such as unauthorized access to SCADA system components, compromise of industrial devices, and lateral movement of attackers within the network. Special focus is placed on the impact of various components of the KICS (Kaspersky Industrial Cyber Security) system, which has been implemented as a security enhancement for the system, including anomaly detection, endpoint protection, and network traffic analysis, while ensuring the uninterrupted operation of operational processes within the power plants. As part of the security improvements for critical systems within Elektromreža Srbije, the KICS platform has already been implemented in local substations, regional dispatch centers, and will soon be integrated into the national dispatch center, establishing a unified and centralized OT infrastructure protection system. The KICS platform enables proactive protection of critical infrastructure, reduces the risk of cyberattacks, and facilitates more efficient management of security incidents, significantly increasing the resilience of the industrial network to modern cyber threats.

Key words: *SCADA, OT infrastructure, KICS, cyber threats, industrial cybersecurity, critical infrastructure protection*

1 UVOD

U savremenim elektroenergetskim sistemima, stabilnost i pouzdanost prenosa električne energije sve više zavise od digitalnih tehnologija i automatizovanih rešenja. U tom kontekstu, SCADA/EMS sistemi predstavljaju srž upravljačke i nadzorne infrastrukture u prenosu električne energije, omogućavajući pravovremeno donošenje operativnih odluka i upravljanje kompleksnim mrežnim strukturama.

Međutim, paralelno sa digitalizacijom, raste i izloženost ovih sistema raznovrsnim sajber pretnjama. Iskustva iz prakse pokazuju da kompromitacija čak i izolovanih industrijskih mreža može imati ozbiljne posledice, ne samo po tehničko-funkcionalni aspekt rada sistema, već i po bezbednost ljudi i stabilnost čitave energetske mreže. Poseban izazov predstavlja činjenica da tradicionalni IT bezbednosni mehanizmi nisu adekvatni za primenu u OT okruženjima, koja zahtevaju neprekidan rad i visoku pouzdanost.

U skladu sa globalnim trendovima u domenu sajber bezbednosti, Elektromreža Srbije je prepoznala potrebu za specijalizovanim pristupom zaštiti SCADA infrastrukture. Ovaj rad ima za cilj da prikaže analizu najčešćih bezbednosnih izazova u OT mrežama, kao i da predstavi konkretne korake koji su preduzeti kroz implementaciju KICS sistema – savremenog rešenja namenjenog unapređenju zaštite kritične infrastrukture.

2 SAJBER PRETNJE I NAPADI NA OT INFRASTRUKTURU SCADA SISTEMA

U kontekstu SCADA sistema i šire OT infrastrukture, sajber bezbednost predstavlja kompleksan i specifičan izazov koji se značajno razlikuje od tradicionalnog IT okruženja. Osnovna razlika leži u prioritetima bezbednosti – dok se u IT sistemima fokus stavlja na poverljivost podataka, integritet i dostupnost , u OT sistemima redosled prioriteta se menja, pri čemu dostupnost i kontinuitet rada procesa zauzimaju primarno mesto. Ova razlika proističe iz činjenice da OT sistemi upravljaju stvarnim fizičkim procesima, kao što su prenos električne energije, regulacija napona, upravljanje zatvaračima, prekidačima i drugim elektroenergetskim komponentama.

Za razliku od IT sistema koji mogu biti privremeno isključeni radi bezbednosnih ažuriranja ili reagovanja na incident, OT sistemi u elektroenergetskom sektoru zahtevaju neprekidan rad, jer svaki prekid može izazvati destabilizaciju mreže, prekid snabdevanja potrošača ili čak ozbiljne havarije. Napadi koji bi u IT okruženju imali ograničen domet – kao što su DoS (Denial of Service), zaraza malverom ili neautorizovan pristup – u OT mreži mogu dovesti do katastrofalnih posledica, uključujući fizičko uništenje opreme, prekide u radu elektrana i trafostanica, pa čak i ugrožavanje ljudskih života, naročito u sistemima gde su automatizovani sigurnosni mehanizmi direktno povezani sa SCADA komponentama.

Pored toga, tehnička ograničenja u OT okruženju dodatno komplikuju implementaciju klasičnih bezbednosnih mehanizama. Na primer, mnogi industrijski uređaji koriste zastarele operativne sisteme, hardver sa ograničenim resursima ili specifične industrijske protokole bez podrške za šifrovanje i autentifikaciju. Zbog dugog životnog ciklusa opreme (često i više od 20 godina), mnoge komponente nisu dizajnirane sa sajber bezbednošću u vidu, a mogućnosti za njihovu zamenu ili nadogradnju su ograničene iz tehničkih i budžetskih razloga.

Još jedan značajan izazov predstavlja to što su SCADA sistemi sve češće povezani sa poslovnim IT mrežama (takozvana IT-OT konvergencija), što otvara dodatne vektore napada. Na primer, ukoliko napadač uspe da kompromituje korisnički uređaj unutar IT mreže, postoji realna mogućnost da se kroz neadekvatno segmentiranu mrežnu arhitekturu infiltrira i u OT deo sistema, što dovodi do lateralnog kretanja i eskalacije napada.

Zbog svega navedenog, jasno je da bezbednost OT sistema mora biti tretirana kao zaseban domen unutar šire oblasti sajber bezbednosti, sa posebnim pristupom, alatima i strategijama koji su prilagođeni realnom vremenu, determinističkom ponašanju i zahtevima visoke pouzdanosti koji definišu industrijska okruženja.

2.1 Najčešće ranjivosti SCADA i OT sistema

OT i SCADA sistemi koji čine okosnicu upravljanja i nadzora u elektroenergetskim mrežama, u svojoj osnovi nisu projektovani sa primarnim fokusom na sajber bezbednost. Njihova arhitektura, funkcionalni zahtevi i dug radni vek uslovili su da bezbednost ostane u drugom planu, što ih danas, u kontekstu sve prisutnijih sajber pretnji, čini izuzetno ranjivim.

Zastarela infrastruktura i dug životni ciklus sistema predstavljaju jednu od ključnih ranjivosti. Mnogi SCADA sistemi i prateći uređaji (kao što su PLC-ovi, RTU jedinice i IED-ovi) koriste operativne sisteme i firmware koji su prestali da se ažuriraju i podržavaju od strane proizvođača. Na primer, prisustvo Windows XP ili Windows 7 sistema u upravljačkim stanicama nije retkost, a upotreba starijih verzija Linux distribucija je uobičajena u ugrađenim sistemima.

U takvom okruženju, bez mogućnosti za pravovremeno ažuriranje bezbednosnih nadogradnji i bez podrške za savremene bezbednosne mehanizme, čak i poznate ranjivosti ostaju otvorene i eksploatabilne.

Neadekvatni komunikacioni protokoli dodatno komplikuju bezbednosnu situaciju. Industrijski protokoli koji se koriste za komunikaciju između kontrolera i SCADA servera – poput Modbus, DNP3, IEC 60870-5-104 ili IEC 61850 – uglavnom nisu dizajnirani sa ugrađenim mehanizmima autentifikacije, enkripcije ili kontrole integriteta. Ovi protokoli funkcionišu po principu implicitnog poverenja, što omogućava napadaču da, uz minimalne tehničke prepreke, izvrši komandne manipulacije, presretne saobraćaj ili potpuno preuzme nadzor nad uređajem.

Fizička dostupnost uređaja predstavlja još jedan često zanemaren aspekt sajber bezbednosti. SCADA komponente su često locirane na geografski udaljenim i slabije zaštićenim lokacijama, kao što su trafostanice, komunikacioni čvorovi ili pomoćni objekti, čime se otvara mogućnost direktnog fizičkog pristupa. U slučajevima kada fizička bezbednost nije na zadovoljavajućem nivou, rizik od sabotaže, neautorizovanog povezivanja uređaja ili unošenja zlonamernog koda postaje znatno veći.

Nezaštićeni udaljeni pristupi sve češće predstavljaju kritičnu tačku napada. Upotreba RDP konekcija, VPN tunela i daljinskih administrativnih alata bez višefaktorske autentifikacije, uz često korišćenje fabričkih lozinki i loše konfigurisanih pristupnih prava, čini infrastrukturu izuzetno ranjivom. Napadači veoma često ciljaju upravo te udaljene pristupne tačke kao „ulazna vrata“ u SCADA sisteme.

Slaba segmentacija mreže i nedostatak nadzora takođe doprinose povećanju rizika. U mnogim slučajevima, IT i OT mreže su delimično ili potpuno integrisane bez jasno definisanih sigurnosnih zona (zone-based security), što omogućava napadačima da, nakon kompromitacije jednog IT resursa, neometano nastave kretanje ka industrijskim kontrolnim sistemima. Nedostatak mehanizama za nadzor saobraćaja, logovanje aktivnosti i otkrivanje anomalija dodatno smanjuje mogućnost za rano otkrivanje napada.

Na sve navedeno se nadovezuje i **ljudski faktor**, uključujući nedovoljnu edukaciju operatera, slab nivo svesti o sajber rizicima u OT sektoru, kao i oslanjanje na zastarele operativne procedure koje ne uključuju moderne bezbednosne zahteve i sajber higijenu.

Uzimajući u obzir specifičnosti SCADA i OT sistema, jasno je da konvencionalna IT rešenja nisu dovoljna za zaštitu ovakve infrastrukture. Potrebna su ciljana, industrijski optimizovana rešenja koja ne samo da adresiraju postojeće tehničke ranjivosti, već i omogućavaju očuvanje kontinuiteta procesa, što je ključna vrednost u elektroenergetskom sektoru.

2.2 Najčešći oblici i primeri sajber napada na SCADA i OT sisteme

Uprkos tome što su SCADA i OT sistemi najčešće fizički odvojeni od interneta i poslovnih IT mreža, njihova složenost, dug radni vek i sveprisutna potreba za daljinskim upravljanjem i održavanjem čine ih potencijalnom metom za napredne sajber napade. U nastavku su predstavljeni najkarakterističniji oblici napada koji ugrožavaju SCADA infrastrukturu, ilustrovani primerima iz realnog sektora.

a) Malveri usmereni na industrijske kontrolne sisteme

Jedna od najopasnijih formi napada na SCADA sisteme jeste upotreba specijalizovanih malvera razvijenih upravo za manipulaciju ili sabotažu industrijskih kontrolnih uređaja. Ovi napadi su često visoko ciljani sa detaljnim poznavanjem infrastrukture sistema koji se napada.

Najpoznatiji primer je **Stuxnet**, prvi malver koji je uspešno doveo do fizičkog oštećenja opreme u realnom industrijskom okruženju. Ovaj napad iz 2010. godine koristio je niz prethodno nepoznatih ranjivosti u Windows operativnim sistemima da bi kompromitovao Siemens PLC kontrolere i izmenio rad gasnih centrifuga u iranskom nuklearnom postrojenju i sve to bez ikakvog vidljivog znaka za operatere.

Još jedan važan primer je **Industroyer** (poznat i kao CrashOverride), koji je 2016. godine korišćen za napad na elektrodistributivnu mrežu Ukrajine. Malver je bio sposoban da koristi više industrijskih protokola uključujući IEC 60870-5-101/104 i IEC 61850 za direktno slanje komandi ka prekidačima i relejima. Za razliku od Stuxnet-a, čiji je cilj bila sabotaža kroz prikrivenu manipulaciju, Industroyer je imao otvoreno destruktivan karakter sa namerom izazivanja nestanka struje.

Sličnu prirodu imao je i **Triton** (poznat i kao Trisis), otkriven u petrohemijskom postrojenju na Bliskom Istoku. Njegova meta bili su sigurnosni sistemi (Safety Instrumented Systems – SIS), čija je funkcija da zaštite ljude i opremu od havarija. Onemogućavanjem rada SIS sistema, Triton je otvorio mogućnost katastrofalnog incidenta.

b) Ransomver napadi u energetskom sektoru

Iako ransomver predstavlja pretnju prepoznatljivu prvenstveno u IT okruženju, sve češće napada i kompanije u oblasti kritične infrastrukture, uključujući elektroenergetski sektor.

Napad na **Colonial Pipeline** 2021. godine izazvao je paniku i nestašicu goriva u Sjedinjenim Američkim Državama. Iako operativni sistemi zaduženi za transport goriva nisu direktno pogođeni, kompanija je iz predostrožnosti zaustavila rad celog sistema, što je pokazalo koliki uticaj kompromitacija IT dela može imati na OT operacije.

Slično tome, **Norsk Hydro**, jedan od najvećih proizvođača aluminijuma, pogođen je 2019. godine ransomware-om "LockerGoga", što je izazvalo zastoj u više od 170 postrojenja širom sveta. Gubici su procenjeni na desetine miliona dolara.

Ovi primeri pokazuju da ransomver napadi više nisu ograničeni samo na enkripciju podataka, već sve češće služe kao poluga za pritisak na organizacije koje upravljaju sistemima od javnog značaja.

c) APT napadi na elektroenergetske sisteme

Napredne trajne pretnje (APT – Advanced Persistent Threats) predstavljaju jedan od najsloženijih i najopasnijih oblika sajber napada, karakterisan dugotrajnim i pažljivo koordinisanim infiltracijama u ciljani sistem. APT napadi se često povezuju sa geopolitičkim ciljevima i njihove mete su uglavnom sektori od kritičnog značaja za funkcionisanje društva i države. APT operacije su posebno opasne jer mogu ostati neprimećene mesecima, pa čak i godinama. Napadači u ovim slučajevima ne izvršavaju napad odmah, već najpre proučavaju mrežu, arhitekturu sistema i rutine operatera, pripremajući precizno sinhronizovanu akciju sa maksimalnim efektom.

3 KASPERSKY REŠENJA ZA ZAŠTITU OT INFRASTRUKTURE SCADA SISTEMA

KICS predstavlja jedno od najsveobuhvatnijih i najnaprednijih rešenja za zaštitu industrijskih sistema od savremenih sajber pretnji. Razvijen od strane kompanije Kaspersky, jednog od globalnih lidera u oblasti sajber bezbednosti, KICS je specijalno dizajniran da odgovori na jedinstvene izazove koji se javljaju u okviru OT i ICS (Industrial Control Systems) okruženjima, uključujući SCADA i DCS sisteme, kao i infrastrukturu u energetici, transportu, vodoprivredi, proizvodnji i drugim kritičnim sektorima.

Za razliku od tradicionalnih IT bezbednosnih rešenja, koja su prvenstveno fokusirana na zaštitu podataka i informacionih sistema, KICS je koncipiran da pruži stabilnu, neprekidnu i kontekstualno svesnu zaštitu u okruženjima u kojima prekid rada može imati ozbiljne posledice, uključujući ugrožavanje ljudskih života, fizičku štetu na postrojenjima i prekid snabdevanja osnovnim uslugama.

U kontekstu industrijskih sistema, ključni izazov je u tome što su mnogi OT sistemi prvobitno projektovani bez ikakvog aspekta sajber bezbednosti i često koriste nestandardizovane, zastarele protokole, uređaje bez mogućnosti za nadogradnju, kao i operativne sisteme koji su odavno van podrške. Ovakvi sistemi su do nedavno funkcionisali u izolovanim mrežama, ali savremeni zahtevi za daljinskim nadzorom, integracijom sa IT infrastrukturama i centralizovanim upravljanjem, doveli su do značajnog povećanja napadnih vektora. KICS je razvijen upravo da adresira ove slabosti na način koji je kompatibilan sa ograničenjima i specifičnostima OT okruženja.

Ono što KICS izdvaja od konkurentskih rešenja jeste njegov višeslojni, modularni pristup, koji omogućava organizacijama da postepeno uvode komponente sistema u skladu sa sopstvenim kapacitetima, bez potrebe za velikim prekidima u radu. Pored toga, KICS je osmišljen tako da ne narušava normalan tok industrijskih procesa – koristi pasivne metode praćenja, ne oslanja se na učestale nadogradnje i ne opterećuje resurse industrijskih uređaja.

KICS ne samo da detektuje napade i anomalije, već pruža i kontekstualnu analitiku, uzimajući u obzir prirodu industrijskih procesa. Na taj način se smanjuje broj lažnih pozitivnih rezultata, što je od izuzetne važnosti u SCADA sistemima u kojima greške u tumačenju mogu dovesti do pogrešnog odlučivanja operatera.

Osim zaštite krajnjih tačaka i nadzora mreže, KICS omogućava centralizovano upravljanje bezbednošću kroz KICS Security Center, čime se obezbeđuje vidljivost nad svim delovima OT infrastrukture, brza reakcija na incidente i jednostavno upravljanje politikama zaštite. Ova centralizacija je posebno značajna u velikim sistemima, gde se SCADA i DCS komponente nalaze na više geografski udaljenih lokacija.

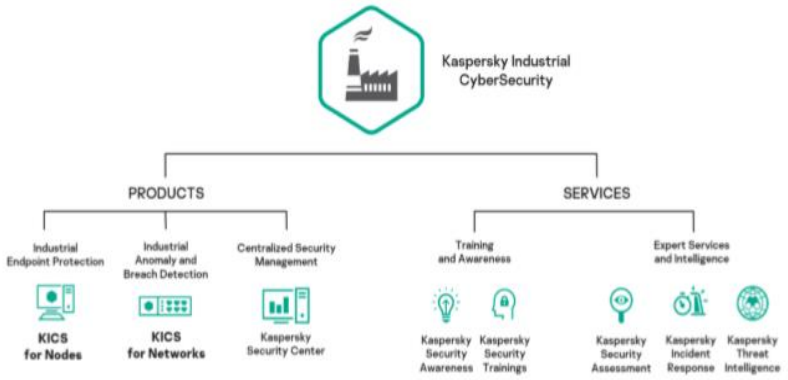
U širem kontekstu, KICS pomaže organizacijama da se usklade sa međunarodnim bezbednosnim standardima, kao što su IEC 62443, ISO/IEC 27001, kao i nacionalnim regulatornim zahtevima. Uvođenje ovakvog rešenja predstavlja ne samo tehničku investiciju, već i strateški korak ka jačanju otpornosti organizacije na sajber pretnje u 21. veku.

U narednim podpoglavljima biće detaljno predstavljeni svi ključni moduli ovog rešenja – KICS for Nodes, KICS for Networks i KICS Security Center – kao i njihove funkcije, međusobna integracija i uloga u izgradnji sveobuhvatnog industrijskog bezbednosnog okruženja.

3.1 Arhitektura i komponente sistema

Modularna arhitektura KICS rešenja omogućava fleksibilnu primenu u različitim industrijskim scenarijima, od lokalnih kontrolnih centara i postrojenja do distribuiranih nacionalnih infrastruktura. Svaka komponenta sistema ima jasno definisanu ulogu u okviru višeslojnog modela zaštite i dizajnirana je tako da ne narušava operativne tokove, već da se nenametljivo integriše u postojeće okruženje.

KICS funkcioniše kroz tri osnovna i međusobno povezana modula: **KICS for Nodes**, **KICS for Networks** i **KICS Security Center**. Zajedno, oni omogućavaju zaštitu celokupne OT arhitekture, od krajnjih tačaka, preko komunikacionih slojeva, do centralizovanog nadzora i upravljanja bezbednosnim politikama.



Slika 1: Arhitektura KICS sistema

a) KICS for Nodes

Komponenta KICS for Nodes je zadužena za zaštitu krajnjih tačaka SCADA sistema, uključujući radne stanice operatera, serverske jedinice, inženjerske konzole i druge računarske uređaje unutar OT okruženja. Ova komponenta implementira višestruke slojeve zaštite u realnom vremenu, pri čemu je akcenat na stabilnosti i minimalnom uticaju na rad industrijskih aplikacija.

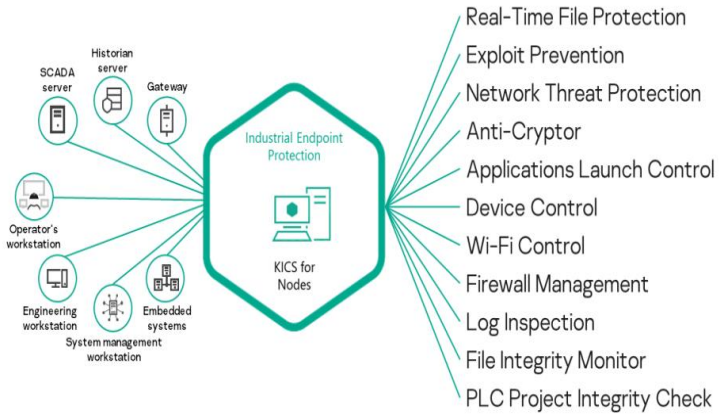
Ključne funkcionalnosti uključuju:

- **Kontrolu pokretanja aplikacija (Application Launch Control):** omogućava precizno definisanje koje aplikacije mogu biti izvršene na uređaju, čime se sprečava pokretanje neautorizovanog softvera.
- **Kontrolu uređaja (Device Control):** omogućava administraciju perifernih uređaja (USB, Wi-Fi, Bluetooth), čime se smanjuje rizik od unosa zlonamernog koda putem fizičkih medija.
- **Zaštitu fajl sistema u realnom vremenu (Real-Time File Protection):** pruža efikasnu detekciju i blokiranje zlonamernog softvera uz kontinuirano skeniranje ključnih direktorijuma i procesa.

- **Prevenciju eksploatacije (Exploit Prevention):** štiti ranjive aplikacije i operativne sisteme od poznatih tehnika eksploatacije, čak i kada zakrpe nisu dostupne ili nisu primenjene.

- **Upravljanje mrežnim pravilima (Firewall Management):** omogućava detaljnu kontrolu mrežnog saobraćaja na nivou svakog uređaja.

Posebna prednost ove komponente je njena optimizacija za rad u starijim i ograničenim sistemskim okruženjima, uključujući operativne sisteme koji su van podrške, ali i dalje u aktivnoj upotrebi u industriji, kao što su Windows XP ili Windows 7.



Slika 2: Funkcionalna struktura KICS for Nodes

b) KICS for Networks

Komponenta KICS for Networks omogućava pasivno, nenametljivo praćenje komunikacije između uređaja u OT mreži. Korišćenjem tehnologije *port mirroring* na upravljivim svičevima, sistem presreće i analizira mrežni saobraćaj bez ikakvog uticaja na tokove podataka i bez rizika po dostupnost sistema.

Osnovne funkcionalnosti ove komponente uključuju:

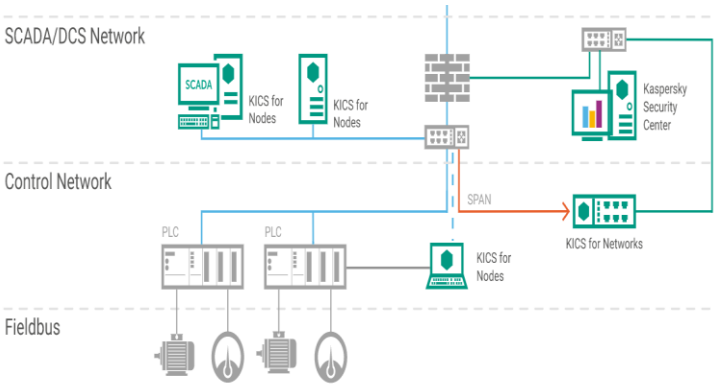
- **Analizu industrijskih protokola** kao što su Modbus, DNP3, OPC Classic/UA, IEC 60870-5-104 i IEC 61850, uz mogućnost otkrivanja netipičnih i potencijalno zlonamernih komandi.

- **Detekciju neautorizovane komunikacije**, kao i pokušaje slanja komandi koje nisu u skladu sa definisanim operativnim obrascima.

- **Identifikaciju anomalija u saobraćaju**, uključujući netipična vremena odgovora, odstupanja u frekvenciji komunikacije, kao i sumnjive tokove između uređaja koji ne komuniciraju u normalnim uslovima.

- **Mapiranje mreže i otkrivanje uređaja**, čime se automatski kreira pregled fizičke i logičke OT topologije.

Ova komponenta posebno je važna za otkrivanje pokušaja lateralnog kretanja napadača unutar mreže, što predstavlja jednu od najčešćih tehnika napada na SCADA sisteme.



Slika 3: Funkcionalna struktura KICS for Networks

c) KICS Security Center

KICS Security Center predstavlja centralnu upravljačku platformu unutar KICS okruženja, dizajniranu da objedini sve informacije, funkcionalnosti i bezbednosne mehanizme u jedan koordinisani sistem. Ova komponenta omogućava punu vidljivost, upravljanje i analizu sajber bezbednosnih događaja u realnom vremenu, čime značajno olakšava operativni nadzor i unapređuje sposobnost reagovanja na potencijalne incidente.

Za razliku od tradicionalnih rešenja, koja često funkcionišu fragmentisano i zahtevaju angažovanje više alata i interfejsa, KICS Security Center integriše nadzor nad krajnjim tačkama, mrežnim komponentama i komunikacionim protokolima u jedinstveni interfejs prilagođen potrebama OT sektora. Ovo omogućava bezbednosnim timovima i operaterima da brzo donose odluke zasnovane na kompletnim i korelisanim podacima iz čitavog sistema.

Ključne funkcionalnosti obuhvataju:

- **Prikaz bezbednosnih incidenata u realnom vremenu:** Sistem kontinuirano prikuplja i prikazuje podatke o detektovanim pretnjama, incidentima, pokušajima kompromitacije i neautorizovanom ponašanju. Prikaz se automatski ažurira i omogućava vizuelnu kategorizaciju događaja po stepenu rizika i tipu pretnje (npr. mrežni napad, pokušaj pokretanja neautorizovane aplikacije, eksploatacija ranjivosti i sl.).

- **Korelaciju i prioritetizaciju događaja:** KICS Security Center poseduje mehanizme za automatsko povezivanje povezanih incidenata u šire bezbednosne scenarije, čime se izbegava delimično tumačenje pojedinačnih događaja. Takođe, primenjuje se prioritetizacija na osnovu poslovnog i operativnog konteksta, što omogućava timovima da usmere pažnju na najkritičnije incidente.

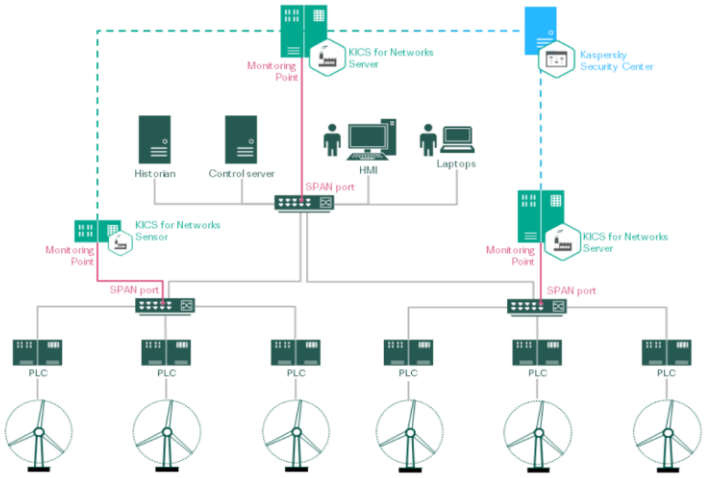
- **Vizuelizaciju OT mrežne topologije:** Interfejs omogućava grafički prikaz mrežnih odnosa, uređaja, veza i komunikacionih tokova između SCADA kontrolera, PLC jedinica, IED-ova, servera i krajnjih tačaka. Vizuelni prikaz pomaže operatorima da uoče potencijalne ranjivosti, neautorizovane uređaje ili promene u ponašanju sistema koje mogu ukazivati na napad.

- **Upravljanje politikama zaštite i agentima:** Platforma omogućava centralizovano konfigurisanje pravila pristupa, ažuriranja i bezbednosnih politika, kao i **upravljanje** softverskim agentima instaliranim na zaštićenim uređajima. Sve promene se mogu sprovoditi daljinski, bez potrebe za fizičkim pristupom terenskim lokacijama.

- **Forenzičku analizu i automatsko generisanje izveštaja:** KICS Security Center vodi detaljne logove svih aktivnosti, omogućavajući detaljnu retrospektivnu analizu svakog incidenta. Sistem generiše audit tragove koji mogu poslužiti u pravnim i regulatornim postupcima, kao i standardizovane i prilagođene izveštaje koji se mogu koristiti za izveštavanje rukovodstva, tehničkih timova i eksternih tela.

- **Integraciju sa SIEM rešenjima i eksternim sistemima:** KICS je projektovan da bude interoperabilan sa drugim bezbednosnim alatima, pre svega sistemima za upravljanje bezbednosnim informacijama i događajima (SIEM), čime se omogućava konsolidacija OT i IT bezbednosnih podataka u jedinstvenu platformu. Time se dodatno unapređuje korelacija između industrijskih i korporativnih pretnji, kao i sveobuhvatna analiza rizika.

Zahvaljujući ovakvom centralizovanom pristupu, KICS Security Center ne samo da omogućava tehnički nadzor, već igra ključnu ulogu u uspostavljanju organizacione kontrole nad celokupnim OT bezbednosnim okruženjem. U uslovima sve složenijih sajber pretnji i regulatornih zahteva, ova komponenta postaje osnovni alat za operativno upravljanje sajber rizicima u SCADA sistemima, uz očuvanje efikasnosti, dostupnosti i sigurnosti ključnih industrijskih procesa.



Slika 4: Kaspersky Security Centar

4 IMPLEMENTACIJA KICS REŠENJA U ELEKTROMREŽI SRBIJE

U svetlu dinamičnih tehnoloških promena i sve naprednijih sajber pretnji koje ugrožavaju bezbednost kritične infrastrukture, Elektromreža Srbije je preduzela strateški iskorak u pravcu modernizacije i jačanja sajber otpornosti svojih SCADA i OT sistema. S obzirom na to da elektroenergetski sektor predstavlja jedan od stubova nacionalne bezbednosti i ekonomskog razvoja, bilo kakva kompromitacija sistema za nadzor, upravljanje i prenos električne energije može imati velike posledice, ne samo tehničke, već i društveno-ekonomske.

EMS je, kao operator prenosnog sistema u Republici Srbiji, odgovoran za održavanje stabilnosti, kontinuiteta i bezbednosti u funkcionisanju elektroenergetske mreže. U tom kontekstu, doneta je odluka da se izvrši implementacija specijalizovanog rešenja koje je u stanju da adresira specifične izazove OT bezbednosti, kako na tehničkom, tako i na organizacionom nivou.

Nakon detaljne analize tržišnih opcija, internog stanja sistema, preporuka iz bezbednosnih izveštaja i konsultacija sa ekspertskim timovima, opredelilo se za platformu KICS. Rešenje je odabrano zbog svoje sposobnosti da se efikasno integriše u postojeće SCADA okruženje, bez narušavanja procesa u realnom vremenu i zbog dokazane uspešnosti u zaštiti industrijskih i energetskih sistema na globalnom nivou.

KICS je odabran kao ključna komponenta nove sajber bezbednosne arhitekture, upravo zato što je razvijen imajući u vidu sve specifičnosti operativne tehnologije, uključujući dug radni vek opreme, zahtev za neprekidnim radom, prisustvo nasleđenih sistema i ograničene mogućnosti za intervenciju u produkcionom okruženju.

4.1 Ciljevi i motivacija implementacije

S obzirom na rastući broj naprednih sajber incidenata usmerenih ka kritičnoj infrastrukturi širom sveta, prepoznata je neophodnost redefinisanja postojećeg pristupa zaštiti SCADA i OT sistema. Posebno je postalo jasno da tradicionalni IT bezbednosni alati i modeli nisu dovoljno efikasni u OT okruženju koje karakterišu dug radni vek sistema, real-time zahtevi i visoka operativna osetljivost.

Jedan od glavnih pokretača inicijative bilo je reagovanje na nalaze bezbednosnih revizija i inspekcija, koje su ukazale na potencijalne ranjivosti unutar industrijskog sistema nadzora i upravljanja. Identifikovani su nedostaci u vidljivosti OT mreže, ograničenja u detekciji pretnji i nedostatak integrisanog pristupa incident menadžmentu. U tom smislu, implementacija KICS rešenja viđena je kao najefikasniji način da se ovi izazovi adresiraju sistemski i dugoročno.

Pored toga, sve češći napadi na energetski sektor na globalnom nivou, uključujući slučajeve Stuxnet, Industroyer i Colonial Pipeline, pokazali su da ni zatvoreni sistemi nisu imuni na ciljane sajber operacije, posebno one koje koriste APT taktike, socijalni inženjering, lateralno kretanje kroz mreže i iskorišćavanje nevidljivih ranjivosti.

Cilj nije bio samo zaštita infrastrukture od pojedinačnih incidenata, već i uspostavljanje stabilnog, održivog i skalabilnog bezbednosnog sistema koji će biti u stanju da se razvija u skladu sa budućim tehnološkim izazovima i regulatornim obavezama. Obezbeđenje kontinuiteta rada čak i u uslovima kompromitacije sistema postavljeno je kao strateški prioritet, jer u elektroenergetici i minimalan prekid može izazvati domino efekat i značajne posledice po nacionalnu bezbednost i privredu.

Posebno važan aspekt motivacije predstavljalo je usklađivanje sa međunarodnim standardima i okvirima. EMS kao članica ENTSO-E i entitet od strateškog značaja na evropskoj energetskoj mapi ima obavezu da se pridržava smernica koje proističu iz:

- **IEC 62443** – standarda za bezbednost industrijskih kontrolnih sistema,
- **ISO/IEC 27001** – međunarodnog okvira za upravljanje informacionom bezbednošću,

- **ENTSO-E preporuka** koje definišu strukturu tzv. Generic Security Plan i očekivane funkcionalnosti sistema za zaštitu od sajber pretnji u elektroenergetici.

Shodno tome, bilo je od ključne važnosti da se odabere rešenje koje je kompatibilno sa postojećom SCADA infrastrukturoe i koje ne zahteva značajne izmene u arhitekturi sistema, ne ugrožava stabilnost operativnih procesa, ali istovremeno pruža:

- visoku vidljivost u realnom vremenu nad OT mrežom i uređajima,
- mogućnost ranog otkrivanja anomalija i incidenata,
- centralizovano upravljanje i forenzičku analizu,
- i kompatibilnost sa regulatornim i internim politikama bezbednosti.

Ovim pristupom, postavljen je temelj za moderni bezbednosni sistem u kojem sajber otpornost postaje sastavni deo celokupnog procesa upravljanja prenosom električne energije, a ne samo izdvojena tehnička funkcija.

4.2 Faze implementacije

Implementacija KICS rešenja u EMS-u predstavljala je složen, ali pažljivo strukturisan proces, realizovan kroz više uzastopnih faza. Svaka etapa projekta osmišljena je tako da minimalno utiče na postojeći režim rada SCADA sistema, uz postepenu izgradnju kapaciteta za nadzor, detekciju i centralizovano upravljanje sajber bezbednošću u OT okruženju. Projekat je sproveden u saradnji sa internim inženjerskim timovima EMS-a, tehničkim partnerima i eksternim konsultantima iz oblasti industrijske bezbednosti, kao i uz koordinaciju sa proizvođačima SCADA softverskih rešenja radi očuvanja kompatibilnosti i stabilnosti sistema.

U prvoj fazi sprovedene su ključne pripreme u okviru OT infrastrukture. Ova faza uključivala je temeljnu analizu postojećeg mrežnog sloja i njegov redizajn u cilju uspostavljanja tehničkih uslova za pasivni nadzor mrežnog saobraćaja. Centralni cilj bio je da se omogući “mirror” pristup komunikaciji između industrijskih uređaja bez narušavanja postojećih funkcionalnosti i bez dodirivanja produkcionih SCADA komponenti. U skladu sa tim, u regionalnim dispečerskim centrima i na lokalnim trafostanicama širom Srbije, izvršena je instalacija upravljivih mrežnih svičeva, kao i segmentacija OT mreže koja je omogućila precizno usmeravanje mrežnog saobraćaja ka nadzornim tačkama bez prekida u radu sistema. Posebna pažnja posvećena je odabiru opreme kompatibilne sa režimom rada u realnom vremenu, uz poštovanje svih bezbednosnih i operativnih zahteva.

U drugoj fazi započeta je fizička instalacija infrastrukture neophodne za rad KICS for Networks komponente. Na predviđenim lokacijama postavljeni su namenski serveri za obradu i skladištenje bezbednosnih događaja, na koje su zatim povezani portovi za pasivno nadgledanje. Paralelno sa infrastrukturnom instalacijom, izvršena je detaljna konfiguracija *port mirroring* funkcionalnosti na upravljivim svičevima, čime je omogućeno presretanje mrežnog saobraćaja u realnom vremenu bez umetanja u sam protokol komunikacije. Time su obezbeđeni svi tehnički preduslovi za početak kontinuiranog nadzora saobraćaja između SCADA servera, RTU, IED i drugih uređaja u OT mreži.

Treća faza bila je posvećena instalaciji softverskih komponenti KICS for Nodes, čime je započela implementacija zaštite na nivou krajnjih tačaka.

Na radne stanice i serverske jedinice u okviru SCADA okruženja, prvenstveno u regionalnim dispečerskim centrima, pa zatim i lokalnim trafostanicama, instalirani su agenti koji omogućavaju nadzor i zaštitu datoteka, kontrolu pristupa, monitoring pokrenutih procesa, kao i upravljanje perifernim uređajima poput USB i Wi-Fi adaptera. Pre svake instalacije, izvršena je detaljna provera kompatibilnosti sa postojećim aplikacijama, posebno sa softverima domaće proizvodnje, poput SCADA rešenja Instituta „Mihajlo Pupin“, kako bi se osiguralo da funkcionalnost sistema ostane neometana. Konfiguracija agenata podešena je tako da bude maksimalno optimizovana u pogledu resursne potrošnje, uz isključenje nepotrebnih modula i prioritizaciju ključnih bezbednosnih funkcija.

Četvrta faza obuhvatila je centralizaciju bezbednosnog nadzora kroz implementaciju KICS Security Center platforme u okviru Nacionalnog dispečerskog centra (NDC). Ova platforma je integrisana sa svim prethodno postavljenim KICS komponentama, omogućivši objedinjeni prikaz bezbednosnih događaja sa više lokacija. Uspostavljen je centralni sistem za nadzor i upravljanje, koji omogućava operaterima u NDC-u da u realnom vremenu vizualizuju OT topologiju, identifikuju anomalije u mrežnom saobraćaju, analiziraju potencijalne incidente i donose operativne odluke u skladu sa unapred definisanim procedurama reagovanja. Pored toga, omogućena je i automatizacija kreiranja izveštaja, kao i pravovremena distribucija informacija relevantnim timovima.

U završnoj, petoj fazi, realizovano je testiranje sistema, evaluacija performansi i edukacija zaposlenih. Tokom testnog perioda sprovedene su simulacije napada, analizirana tačnost detekcionih mehanizama i optimizovane politike zaštite u skladu sa specifičnostima SCADA infrastrukture EMS-a. Na osnovu rezultata testiranja izrađeni su bezbednosni scenariji i incident response protokoli koji su usklađeni sa unutrašnjim procedurama i međunarodnim preporukama. Istovremeno, sprovedene su praktične obuke za operatere i administratore, sa ciljem osposobljavanja za samostalan rad u KICS okruženju, kako u domenu operativnog nadzora, tako i u analizi bezbednosnih incidenata i forenzičkim ispitivanjima.

Ovakav fazni i pažljivo kontrolisan pristup omogućio je EMS-u da sprovede jednu od najznačajnijih modernizacija sajber bezbednosti u okviru nacionalne elektroenergetske infrastrukture, bez kompromitovanja pouzdanosti, dostupnosti i kontinuiteta rada sistema.

4.3 Tehničke i operativne specifičnosti implementacije

Jedan od ključnih faktora uspešne implementacije KICS rešenja u okviru Elektromreže Srbije bio je pažljiv i kontekstualno prilagođen pristup tehničkim i operativnim specifičnostima koje karakterišu infrastrukturu. Za razliku od „generičkih“ bezbednosnih modela koji se često oslanjaju na uniformna IT rešenja, projektovanje sajber zaštite u elektroenergetskom okruženju zahtevalo je temeljno razumevanje SCADA arhitekture, mrežnih ograničenja, softverske kompatibilnosti i organizacionih pravila rada u realnom vremenu.

Jedan od najvažnijih izazova u procesu implementacije odnosio se na kompatibilnost sa postojećim SCADA sistemima, pri čemu je posebno pažljivo analizirana saradnja sa rešenjima domaće proizvodnje, kao što su sistemi razvijeni u Institutu „Mihajlo Pupin“. Budući da SCADA aplikacije koje se koriste u EMS-u sadrže specifične protokole komunikacije i softversku logiku razvijanu i održavanu tokom više decenija, bilo je od suštinske važnosti da se implementacija KICS modula sprovodi bez zadiranja u aplikativni sloj sistema. Ovim pristupom omogućena je besprekidna integracija KICS rešenja bez potrebe za rekonstrukcijom ili prilagođavanjem poslovno-kritičnih SCADA aplikacija, što je značajno doprinelo stabilnosti i bezbednosti produkcionog okruženja.

Pored toga, tehnički timovi su morali da odgovore na izazov ograničenih mrežnih resursa na pojedinim lokacijama, naročito u udaljenim trafostanicama i regionalnim centrima sa infrastrukturom koja nije prvobitno bila projektovana za visokoopterećene nadzorne sisteme. U tim uslovima bilo je neophodno pažljivo optimizovati konfiguraciju port mirroring režima, kako bi se izbeglo zagušenje mrežnog saobraćaja i obezbedila stabilna komunikacija između ključnih SCADA komponenti. Inženjerski timovi EMS-a su, uz podršku bezbednosnih stručnjaka, izvršili precizno balansiranje između obima podataka neophodnih za kvalitetnu detekciju anomalija i tehničkih kapaciteta mrežne infrastrukture.

Poseban kvalitet implementacije ogleda se i u sprovedenoj logičkoj segmentaciji OT mreže, koja je omogućila jasno razgraničenje između funkcionalnih zona, kao i identifikaciju bezbednosno osetljivih delova sistema. Ova segmentacija nije bila samo mrežno-tehničke prirode, već je bila utemeljena na analizama funkcionalne povezanosti uređaja, operativnim procedurama i potencijalnim vektorima napada. Kao rezultat, senzori i KICS agenti su pozicionirani strateški, na mestima od najvećeg značaja za otkrivanje anomalija i neautorizovanih aktivnosti, bez ugrožavanja osnovne komunikacije između industrijskih uređaja.

Još jedna važna komponenta uspeha ovog projekta bila je prilagođavanje softverske politike lokalnim operativnim procedurama i kulturi rada EMS-a. S obzirom na specifičnu strukturu odgovornosti i višedecenijsku praksu u upravljanju elektroenergetskim sistemima, bilo je ključno da se bezbednosne funkcije ne nameću previše striktno, već da se uvode postepeno i u skladu sa realnim operativnim potrebama. Prvo su aktivirane pasivne komponente sistema, poput nadzora saobraćaja i generisanja upozorenja, dok su funkcionalnosti koje podrazumevaju aktivnu zaštitu, kontrolu aplikacija ili ograničavanje komunikacija uvodile sukcesivno, nakon temeljne evaluacije i obuka zaposlenih. Ovakav pristup obezbedio je visok nivo prihvatanja sistema među korisnicima, kao i operativnu stabilnost tokom svih faza primene.

Kao celina, tehnički i organizacioni aspekti implementacije KICS rešenja u EMS-u pokazuju da uspešna primena napredne bezbednosne tehnologije u industrijskom okruženju ne zavisi samo od funkcionalnosti samog alata, već i od sposobnosti da se on prilagodi postojećem sistemu, mreži, procesima i ljudima. Upravo ta prilagodljivost i strateški pristup doprineli su tome da ovaj projekat postane primer dobre prakse u oblasti zaštite nacionalne elektroenergetske infrastrukture.

4.4 Rezultati i dalji planovi

Implementacijom KICS rešenja, EMS je napravio značajan korak ka uspostavljanju modernog, skalabilnog i kontekstualno svesnog sistema za zaštitu OT infrastrukture. Projekat nije samo unapredio tehničke kapacitete za nadzor i detekciju, već je doveo do sistemske transformacije načina na koji se u EMS-u percipira i upravlja sajber bezbednošću industrijskih sistema.

Jedan od najvažnijih rezultata projekta jeste uspostavljanje centralizovane i sveobuhvatne vidljivosti nad OT infrastrukturom. Po prvi put, timovi za bezbednost i operativni nadzor imaju uvid u bezbednosna dešavanja u realnom vremenu na nivou regionalnih dispečerskih centara i ključnih objekata prenosne mreže. Do sada je KICS rešenje uspešno implementirano u svih pet regionalnih dispečerskih centra i na 34 trafostanice koje čine deo osnovne elektroenergetske infrastrukture Srbije. Ovim je obuhvaćen značajan deo SCADA mreže, čime je postignuta operativna pokrivenost sistema koja omogućava identifikaciju potencijalnih pretnji u najkritičnijim tačkama mreže.

Zahvaljujući modularnoj i pasivnoj prirodi KICS rešenja, ostvarena je precizna detekcija anomalija i potencijalnih bezbednosnih incidenata, pri čemu nije došlo do narušavanja stabilnosti sistema ni u jednoj fazi implementacije. Sistem je u stanju da identifikuje sumnjive obrasce ponašanja, pokušaje neautorizovane komunikacije i odstupanja u radu protokola i sve to uz minimalan uticaj na performanse infrastrukture. Detekcije koje su ranije bile moguće isključivo kroz ručne kontrole ili reaktivne analize, sada se odvijaju u realnom vremenu, sa mogućnošću momentalne reakcije operatera.

Kao rezultat implementacije, EMS je takođe postavio čvrst temelj za dalji razvoj sajber bezbednosne arhitekture, sa jasnom strategijom proširenja sistema. U narednim fazama planirano je da se KICS rešenje implementira i u Nacionalnom dispečerskom centru (NDC), koji predstavlja centralnu tačku za nadzor nad prenosnom mrežom i koordinaciju sa operatorima susednih sistema. Integracija NDC-a u KICS sistem ne samo da će obezbediti objedinjeni uvid u čitavu OT infrastrukturu EMS-a, već će omogućiti i centralizovano upravljanje incidentima sa najvišeg nivoa odlučivanja.

Takođe, strateški pravac daljeg razvoja uključuje i integraciju sa IT bezbednosnim sistemima EMS-a putem SIEM rešenja, čime bi se omogućila potpuna korelacija između IT i OT bezbednosnih događaja, uz bolji uvid u međuzavisnosti i zajedničke vektore napada.

Na kraju, jedan od ključnih ciljeva za budućnost jeste uspostavljanje automatizovanih mehanizama detekcije i reakcije (SOAR – Security Orchestration, Automation and Response). Uvođenjem ovakvih sistema EMS planira da dodatno skrati vreme između detekcije i reakcije, smanji zavisnost od ručne analize i obezbedi konzistentan odgovor na sve tipove incidenata, od najjednostavnijih pokušaja neautorizovanog pristupa, do naprednijih višefaznih napada.

U celini, rezultati postignuti implementacijom KICS rešenja predstavljaju značajan korak u evoluciji sajber bezbednosti u EMS-u. Ovaj projekat ne samo da je tehnički unapredio zaštitu infrastrukture, već je postavio i nove organizacione, proceduralne i strateške standarde u pristupu bezbednosti OT sistema, koji će služiti kao osnova za sve buduće aktivnosti u ovoj oblasti.

5 ZAKLJUČAK

Sprovedeni rad ukazuje na rastuću potrebu za sistemskim pristupom zaštiti operativne tehnologije u elektroenergetskom sektoru, posebno imajući u vidu sve naprednije sajber pretnje koje ciljno pogađaju SCADA infrastrukture i sisteme od vitalnog značaja. Istraživanjem je pokazano da efikasna zaštita ovih sistema zahteva specijalizovana rešenja koja su projektovana u skladu sa specifičnostima industrijskog okruženja, kako u tehničkom, tako i u operativnom i organizacionom smislu.

Implementacija KICS platforme u okviru Elektromreže Srbije potvrđuje da je moguće postići visok nivo bezbednosti bez narušavanja funkcionalnosti i pouzdanosti industrijskih procesa. Postignuti rezultati, kao što su unapređena mrežna vidljivost, bolja kontrola nad potencijalnim incidentima i usklađenost sa međunarodnim standardima, ukazuju na praktične koristi i dugoročnu održivost ovakvog pristupa. Kroz pažljivo planiranu faznu realizaciju, omogućena je integracija bez zastoja u radu, što je od izuzetnog značaja za infrastrukturu koja mora funkcionisati neprekidno.

Značaj rada ogleda se u tome što prikazuje jedan od prvih primera na regionalnom nivou gde je specijalizovana platforma za industrijsku sajber bezbednost primenjena na nacionalnoj energetskoj mreži, uz očuvanje lokalnog znanja, resursa i procesa. Time je postavljen temelj ne samo za tehnički napredak, već i za razvoj modela saradnje između inženjerskog sektora, IT bezbednosti i upravljačkih struktura.

Moguća dalja istraživanja trebalo bi da budu usmerena na automatizaciju odgovora na incidente kroz upotrebu SOAR tehnologija, kao i na razvoj domaćih standarda i politika bezbednosti u OT domenu koji bi bili prilagođeni specifičnim uslovima rada domaće infrastrukture. Poseban izazov predstavlja i integracija sa sistemima za veštačku inteligenciju i mašinsko učenje u cilju prediktivne detekcije anomalija, što bi dodatno povećalo otpornost elektroenergetskog sistema u budućnosti.

Rad ujedno otvara mogućnost da se razvije jedinstven nacionalni okvir za zaštitu OT sistema, koji bi mogao poslužiti kao model za druge sektore kritične infrastrukture, poput vodoprivrede, saobraćaja ili industrijske proizvodnje.

6 LITERATURA

[1] International Electrotechnical Commission (IEC). (2018). IEC 62443 – Industrial communication networks – Network and system security. Geneva: IEC

[2] International Organization for Standardization (ISO). (2013). ISO/IEC 27001: Information Security Management Systems – Requirements. Geneva: ISO.

[3] European Network of Transmission System Operators for Electricity (ENTSO-E). (2021). Cybersecurity Framework for the Electricity Sector. Brussels: ENTSO-E.

[4] Kaspersky Lab. (2021). Kaspersky Industrial CyberSecurity – Technical Overview.

[5] Kaspersky Lab. (2023). KICS for Nodes and Networks – Deployment and Configuration Guide.

[6] Radivojević, M. i Ristić, S. (2022). Industrijska sajber bezbednost u SCADA sistemima: izazovi i rešenja. Elektrotehnički fakultet, Univerzitet u Beogradu.

[7] Stojković, M. (2021). Bezbednosni aspekti upravljanja elektroenergetskim sistemima. Zbornik radova sa konferencije INFOTEH-JAHORINA.

[8] US Department of Homeland Security – ICS-CERT. (2020). Recommended Practices for Industrial Control Systems.

[9] Institute "Mihajlo Pupin". (2020). SCADA rešenja za elektroenergetski prenos i distribuciju – tehnički vodič.