METOD PROCENE BEZBEDNOSNOG RIZIKA U SISTEMIMA ZA UPRAVLJANJE TRANSPORTOM PRIRODNOG GASA

Jasna D. Marković-Petrović[1], Mirjana D. Stojanović[2]
[1]JP EPS – Ogranak HE Đerdap, jasna.markovic@djerdap.rs
[2]Univerzitet u Beogradu – Saobraćajni fakultet, m.stojanovic@sf.bg.ac.rs

Sadržaj: *U radu je prvo prikazana opšta konfiguracija SCADA (Supervisory Control and Data Acquisition) sistema, a zatim je razmatrana ranjivost ovih sistema i degradacija performansi operativnog servisa daljinskog upravljanja u uslovima sajber napada. U nastavku je prikazan predlog metoda za procenu bezbednosnog rizika od distribuiranih DoS (Denial of Service) napada na infrastrukturu industrijskih sistema daljinskog upravljanja. Simulacija primene metoda procene rizika je ilustrovana u studiji slučaja modelovanog SCADA sistema u transportnom sistemu prirodnog gasa.*

Ključne reči: *detekcija i prevencija napada, odbijanje servisa, procena rizika, SCADA.*

1. Uvod

SCADA (*Supervisory Control and Data Acquisition*) sistemi predstavljaju pravac razvoja i modernizacije velikih industrijskih pogona sa ciljem nadzora i upravljanja u realnom vremenu i kao takvi danas su od vitalnog značaja za funkcionisanje industrijskih sektora na kojima se zasniva kritična infrastruktura države. Tokom poslednjih decenija, povećali su se broj i vrste konekcija na SCADA sisteme, kao i korišćenje tehnologija zasnovanih na Internetu. Za razliku od prvobitno korišćenih, namenskih, danas su u upotrebi standardizovani protokoli u SCADA sistemima. Iz tih razloga se povećava broj i raznovrsnost napada na telekomunikacione mreže sistema daljinskog upravljanja. Kao posledica, SCADA sistemi su danas u mnogo većoj meri izloženi pretnjama, što potvrđuju registrovani sajber napadi na ove sisteme.

S obzirom na neophodnost implementacije specifičnih mehanizama zaštite u mreži SCADA sistema, važno je da se pri projektovanju sistema izvrši procena bezbednosnog rizika, sa ciljem da se odredi racionalan nivo ulaganja. Procena rizika treba da omogući usvajanje strategije o postupanju sa rizikom, donošenje odluke o investicijama u mehanizme zaštite i definisanje prihvatljivog rizika. Cilj rada je predstavljanje metoda za procenu bezbednosnog rizika i ilustracija primene metoda u slučaju SCADA sistema magistralnog gasovoda.

Rad je organizovan na sledeći način. U drugom poglavlju prikazana je koncepcija SCADA sistema sa akcentom na bezbednost. U trećem poglavlju je prikazan

hibridni metod za procenu bezbednosnog rizika u SCADA sistemima. Četvrto poglavlje sadrži simulaciju primene metoda procene bezbednosnog rizika u studiji slučaja koja je zasnovana na modelovanom sistemu za transport prirodnog gasa. Peto poglavlje obuhvata zaključna razmatranja.

2. Bezbednost SCADA sistema

Kritična infrastruktura obuhvata objekte od vitalnog značaja za svaku državu čije oštećenje ili uništenje dovodi do prekida isporuke neke usluge. Karakteristično za više od polovine sektora koji čine kritičnu infrastrukturu je da ključnu ulogu u upravljanju procesima u realnom vremenu imaju SCADA sistemi. Struktura ovih sistema obuhvata tri celine:

1. Podsistem udaljenih stanica (RTU – *Remote Terminal Units*) preko kojih se prikupljaju podaci o procesu i izdaju upravljačke komande;
2. Upravljački centar koji obuhvata SCADA server (MTU – *Master Terminal Unit*) i aplikativne servere, i
3. Komunikacioni podsistem koji povezuje centar upravljanja sa podsistemom daljinskih stanica, obezbeđuje pouzdan prenos informacija i omogućuje udaljeni pristup operaterima za intervenciju u slučaju otkaza. Detaljni pregled karakteristika SCADA sistema može se naći u [1].

U svetu je zabeležen veći broj uspešnih sajber napada na SCADA sisteme [2]. Do povećanja ranjivosti SCADA sistema došlo je usled usvajanja otvorenih standarda sa poznatim propustima, povezanosti sistema daljinskog upravljanja sa drugim mrežama, ograničenja u postojećim tehnologijama zaštite, daljinskog pristupa i dostupnosti tehničkih informacija o SCADA sistemima. Tipične pretnje savremenim SCADA sistemima su zlonamerni programi, unutrašnji i spoljašnji napadi. Primeri unutrašnjih napada na SCADA sisteme obuhvataju zlonamernu modifikaciju programabilnih fajlova za RTU i instalaciju zlonamerne aplikacije, koja može da isključi aktivne alarme i izda lažne komande uređajima povezanim RTU. Direktni napadi na RTU opremu zahtevaju fizički pristup komunikacionim kanalima (mreži). Klasifikacija napada na SCADA sisteme prikazana je u tabeli 1.

Tabela 1. Napadi specifični za SCADA sisteme [3]

Tip napada	**Opis**
Replay	„Hvatanje“ poruke i prosleđivanje sa kašnjenjem jednom/više puta
Spoofing	„Imitiranje“ MTU ili RTU
Denial of Service	Slanje velike količine lažnih poruka tako da RTU nije u mogućnosti da ispuni validne zahteve
Modifikacija kontrolne poruke	„Hvatanje“ zahteva, modifikacija nekih parametara i slanje ka RTU
Upis u MTU	Dodavanje ili promena fajlova na MTU
Izmena odgovora RTU-a	„Hvatanje“ odgovora, modifikacija nekih parametara i slanje ka MTU
Upis u RTU	Dodavanje ili promena vrednosti na RTU

U radu je posebna pažnja usmerena na DoS (*Denial of Service*) napad u kome napadač falsifikuje adresu izvora saobraćaja i koristi infrastrukturu mreže da uputi veliki intenzitet saobraćaja odredištu koje predstavlja metu napada. Efekat napada se uvećava ako se koriste distribuirani napadači, koji istovremeno napadaju ciljni server. Cilj DDoS (*Distributed DoS*) napada je blokiranje glavnih resursa žrtve ili iskorišćenje raspoloživog mrežnog propusnog opsega što za posledicu ima odbijanje servisa. Ovakvi napadi potencijalno ugrožavaju vitalne funkcije industrijskog procesa [4]. S obzirom da za ovu vrstu napada ne postoje apsolutno pouzdani mehanizmi zaštite, ograničeni su mehanizmi za smanjenje rizika od ove vrste. To su razlozi zbog kojih ova vrsta napada predstavlja ozbiljnu pretnju infrastrukturi savremenih telekomunikacionih mreža u industriji.

3. Metod procene bezbednosnog rizika u SCADA sistemima

Metod procene bezbednosnog rizika zasniva se na činjenici da je rizik srazmeran gubicima koji su posledica sajber napada na infrastrukturu SCADA sistema. Ukupni gubici nastali usled realizovanog napada se mogu klasifikovati u dve grupe: **direktni gubici**, koji su posledica prekinutog proizvodnog procesa i **indireketni gubici** koji obuhvataju gubitke oporavka sistema i druge gubitke, kao što su penali zbog neispunjenja ugovornih obaveza, nepovratni gubici resursa, šteta naneta životnoj sredini i slično. Predloženi metod se izvršava u sledećim koracima:

1. definisanje konfiguracije sistema i scenarija otkaza;
2. identifikovanje i proračun direktnih gubitaka;
3. identifikovanje indirektnih gubitaka i određivanje vrednosti težinskih faktora;
4. određivanje mere rizika i očekivanog godišnjeg gubitka;
5. odabir mehanizma zaštite i proračun investicije uložene u zaštitu;
6. određivanje povrata investicije i optimalnog praga ulaganja u mehanizme zaštite.

U prvom koraku je potrebno da se izvrši analiza SCADA sistema i da se formira model u kome su označeni putevi napada i komponente koje su podložne napadu. Kroz scenario otkaza treba da se ukaže na degradaciju performansi SCADA sistema i uticaj napada na funkcionalnost industrijskog sistema.

U drugom koraku je potrebno da se identifikuju ukupni gubici koji su posledica narušenog proizvodnog procesa. Skaliranje pretpostavljenih maksimalnih direktnih gubitaka u slučaju napada najvećeg intenziteta i najgoreg scenarija otkaza postiže se uvođenjem težinskog faktora $\boldsymbol{W_A} \leq 1$.

Indirektne posledice napada se mogu klasifikovati u nekoliko grupa (zaštita životne sredine, bezbednost i zdravlje na radu, reputacija i zakonodavstvo). Težina posledice zavisi od uslova u kojima se dogodio napad. Svaki pojedinačni indirektni gubitak se može predstaviti u funkciji maksimalnog direktnog gubitka, a kvantifikacija se postiže uvođenjem težinskih faktora $\boldsymbol{W_k} \geq 1$. Broj težinskih faktora jednak je broju uslova koji imaju uticaj na indirektne gubitke. Proizvod svih težinskih faktora W_k uvećava ukupne gubitke usled realizovanog napada.

Izbor težinskih faktora je delikatan proces i zavisi od brojnih tehnničkih i ekonomskih uslova u konkretnom SCADA sistemu. U cilju merenja uticaja sajber napada na performanse, poželjno je da kompanija definiše svoje ključne pokazatelje učinka (KPIs – *Key Performance Indicators*). KPI su definisani u skladu sa ključnim ciljevima

poslovanja kompanije (produktivnost, raspoloživost, pouzdanost, bezbednost, smanjenje uticaja otkaza mreže, integritet, vreme zastoja i slično) koji bi trebalo da podrže ispunjavanje poslovnih ciljeva kao što su profit, smanjenje troškova, poboljšanje kvaliteta proizvoda i zadovoljstva korisnika, ispunjenje regulativa, redukovanje potrošnje resursa i slično [5].

Nakon izbora vrste težinskih faktora određuju se njihove vrednosti, u dve faze. Prva faza obuhvata analizu relevantnih arhiviranih podataka kako bi se odredila verovatnoća nastanka uslova koji utiču na indirektne gubitke. Ovim postupkom se dobija **objektivna** vrednost težinskih faktora. U drugoj fazi u proces procene bezbednosnog rizika se uključuju stručnjaci koji treba da budu iz različitih oblasti: poslovodstvo, informacione i komunikacione tehnologije (IKT), implementacija i održavanje SCADA sistema, operativno osoblje i naučno-istraživačka delatnost. **Subjektivna** komponenta vrednosti težinskih faktora se dobija anketiranjem stručnjaka i ocenom njihove kompetentnosti primenom AHP (*Analytical Hierarchical Process*) metoda [6]. Konačne vrednosti težinskih faktora se određuju upoređivanjem objektivne i subjektivne komponente, na osnovu procene kvaliteta svake faze. Ukoliko arhive podataka nisu raspoložive, ostaje kao mogućnost da se sprovede samo anketa među stručnjacima. Tada težinski faktori imaju samo subjektivnu komponentu.

Za određivanje vrednosti težinskog faktora W_A koji skalira napad najvećeg intenziteta treba uzeti u razmatranje statističke podatke o infrastrukturnim napadima na industrijske sisteme daljinskog upravljanja, interne ili iz dostupnih svetskih izvora. Postupak je isti kao i za određivanje težinskih faktora koji kvantifikuju indirektne gubitke. Ukoliko ovi podaci nisu raspoloživi, preporuka je da se procena vrši za najgori slučaj, kada je $W_A = 1$.

U četvrtom koraku izražava se mera rizika na dva načina: kvalitativno i monetarno. Množenjem svih težinskih faktora određenim u prethodnom koraku dobija se bezdimenziona veličina koja predstavlja meru rizika R. U cilju **kvalitativnog** izražavanja mere rizika potrebno je da se usvoji relacija koja povezuje opsege vrednosti R sa stepenom (nivoom) rizika. Množenjem mere rizika sa maksimalnim direktnim gubicima dobija se **monetarno** izraženi rizik. Izbor kvalitativne ili monetarne predstave rizika zavisi od konkretnog sistema i namene metoda procene rizika.

Očekivani godišnji gubitak (*ALE – Annual Loss Expectancy*) se dobija modifikacijom osnovne formule koja predsatavlja proizvod očekivanih gubitaka i verovatnoće nastanka incidenta u toku godine (*ARO – Annual Rate of Occurrence*) [7].

U petom koraku se, u skladu sa vrstom napada, bira odgovarajuća zaštita. Pažnja je usmerena na infrastrukturne napade kao što je DDoS, a preporučena zaštita je IDPS (*Intrusion Detection and Prevention Systems*). Radi procene vrednosti investicije u mehanizme zaštite, neophodno je da se posmatra duži vremenski period s obzirom da je inicijalna investicija u mehanizme zaštite mnogo veća od kasnijih troškova održavanja.

Na osnovu proračunate vrednosti *ALE* i očekivanih ulaganja u mehanizme zaštite moguće je odrediti povrat investicije u bezbednost IKT infrastrukture, *ROSI* - *Return on Security Investment*. *ROSI* predstavlja odnos ušteda usled ublažavanja rizika koje su ostvarene sprečavanjem sajber napada i cene implementirane zaštite. Definisanje prihvatljivog praga za povrat investicija u zaštitu omogućuje donošenje odluke o racionalnom ulaganju u povećanje bezbednosti SCADA sistema.

Detaljan pregled metoda, algoritmi i formule mogu se naći u [7] i [8].

4. Simulacija primene metoda u gasovodu

Transport i distribucija gasa je deo kritične infrastrukture, a pripada sektoru transporta. U Sjedinjenim Američkim Državama (SAD) sistem cevovoda obuhvata više od četiri miliona kilometara cevi koje prolaze kroz državu i distribuiraju skoro čitav nacionalni prirodni gas i oko 65% opasnih tečnosti, kao i razne hemikalije. Transportni sistem ima ulogu da gas iz sabirnih stanica transportuje do distributivne mreže u kojoj se vrši isporuka krajnjim korisnicima, industriji, proizvodnji električne energije, kao i domaćinstvima. Deo sistema čija je uloga transport gasa se naziva magistralni gasovod.

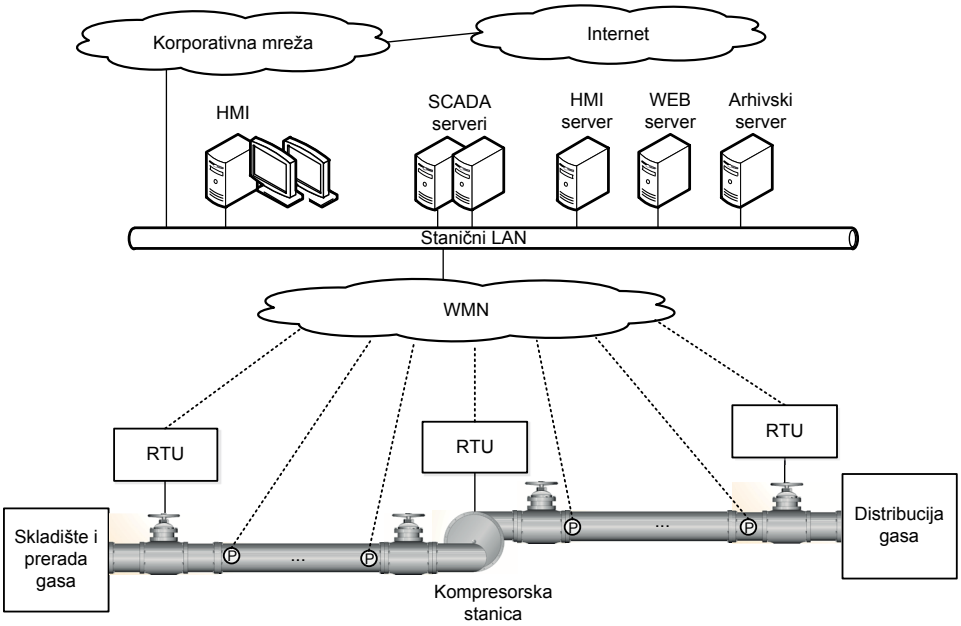
U ovim sistemima se fizičko-tehnički i informacioni deo posmatraju kao jedna celina. Fizičko-tehnički deo obuhvata cevovod, kompresorske stanice, ventile i senzore. Cevovod je deo sistema koji služi za transport gasa, kompresorske stanice se postavljaju na rastojanjima od oko 100 km, a uloga im je da održavaju potreban pritisak gasa duž cele trase. Ventilima se reguliše tok gasa. Senzorima se meri pritisak, protok i druge potrebne fizičke veličine duž cele trase cevovoda. Informacioni deo je zapravo SCADA sistem. Prvi deo SCADA sistema čine RTU-ovi u kompresorskim stanicama. Na njima je implementiran lokalni algoritam upravljanja. U drugom delu – centru upravljanja je SCADA server na kome je implementiran globalni algoritam upravljanja. Treći deo arhitekture SCADA sistema čini komunikacioni podsistem. Algoritmi upravljanja se izvršavaju na osnovu podataka dobijenih sa senzora, a na rad kompresora se utiče postavljanjem *set-point* veličine iz komandnog centra ili lokalnim algortimom. Veza senzora sa RTU, kao i njihova sa komandnim centrom je pretežno zasnovana na bežičnim tehnologijama, prvenstveno zbog geografske razuđenosti, a zatim i zbog razloga što se žičana ili optička mreža može fizički prekinuti namernim ili slučajnim dejstvom, a u topologiji magistrale jedan prekid prouzrokuje gubitak komunikacije sa većim brojem tačaka. U literaturi [9] može se naći pregled nekih uspešnih sajber napada na SCADA sisteme gasovoda i naftovoda.

Metod procene bezbednosnog rizika od infrastrukturnog napada na sistem daljinskog upravljanja u gasovodu testiran je na modelu gasovoda i odgovarajućeg SCADA sistema koji je predložen u [10]. Pretpostavljeno je da se proces upravljanja bezbednosnim rizikom primenjuje u fazi projektovanja sistema kada arhive sa relevantnim veličinama nisu dostupne. Iz tih razloga simulirana je procena bezbednosnog rizika u fazi koja je zasnovana na subjektivnoj oceni stručnjaka.

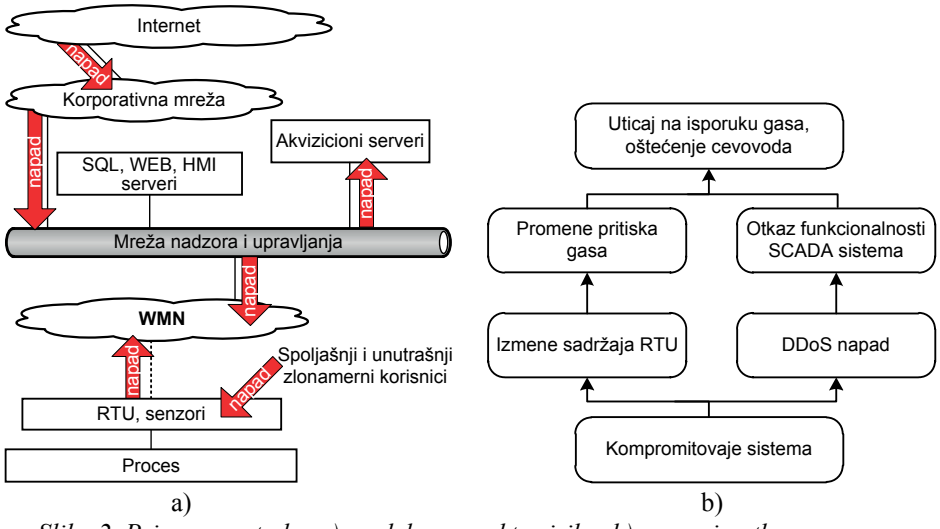
Analiziran je model magistralnog gasovoda koji transportuje prirodni gas od izvora do odredišta koji su udaljeni 257 km. Pritisak u gasovodu treba da bude 6,2 MPa, a kompresorska stanica koja je udaljena 155 km od izvora treba da podigne pritisak na 8,2 MPa da bi na mestu isporuke gas imao željeni pritisak. Maksimalni operativni nivo pritiska je 8,3 MPa. Porast pritiska gasa iznad ovog maksimalnog operativnog nivoa može da prouzrukuje oštećenje unutrašnjeg sloja cevovoda, zatvaranje ventila, curenje gasa ili eksploziju. Na slici 1 prikazani su model gasovoda i arhitektura SCADA sistema. SCADA sistem čine serveri i HMI (*Human Machine Interface*) računari u komandnom centru i RTU-ovi sa senzorima na udaljenim lokacijama čija je uloga da prate stanje procesa i upravljaju kompresorskom stanicom i ventilima. Komunikacioni podsistem čini bežična *mesh* mreža (WMN – *Wireless Mesh Network*).

Posmatrani model magistralnog gasovoda i pripadajućeg SCADA sistema, modelovan sa aspekta rizika od infrastrukturnog napada, prikazan je na slici 2 (a). Na

istoj slici ukazano je na moguće puteve upada u mrežu SCADA sistema i izvršenje infrastrukturnog napada. U studiji slučaja pretpostavljen je napad reprogramiranjem RTU-ova, kako bi bile prikazane pogrešne vrednosti pritiska gasa, što dovodi do pogrešnih instrukcija kompresorskoj stanici. Ovaj napad se kombinuje sa DDoS napadom, što za posledicu ima usporen odgovor sistema. Scenario ovakvog otkaza dat je na slici 2 (b).



Slika 1. Model gasovoda i arhitektura sistema daljinskog upravljanja



Slika 2. Primena metoda: a) model sa aspekta rizika, b) scenario otkaza

Posledice ovakvog napada mogu da budu gubitak u prenosu gasa usled prekida transporta, gubitak rezervi gasa usled potencijalnog curenja gasa i oštećenje cevovoda. U [10] je realizovana simulacija ovakvog napada pri čemu je za model korišćena realna situacija napada na infrastukturu SCADA sistema gasovoda.

Na primeru gasovoda analizirane su moguće posledice kombinovanog napada sa aspekta nadzora, upravljanja i transporta prirodnog gasa, i posledično dve vrste troškova, direktnih i indirektnih. Direktni troškovi nastaju usled prekida transporta gasa usled automatskog zatvaranja ventila zbog razlike u pritiscima gasa u pokazivanjima dva susedna RTU.

Direktni troškovi su srazmerni:

- trajanju napada (t_A);
- vremenu potrebnom za oporavak sistema (t_R);
- maksimalnom protoku gasovoda (Q);
- jediničnoj ceni prirodnog gasa (c_G).

Skaliranje ove vrednosti se postiže faktorom koji izražava intenzitet napada W_A.

Pretpostavlja se da je vreme oporavka proporcionalno maksimalnom vremenu oporavka nakon napada najvećeg intenziteta (t_{Rmax}), a za faktor proporcionalnosti se uzima W_A težinski faktor.

Indirektni troškovi koji se pretpostavljaju u simulaciji nastaju zbog:

- penala usled neispunjenih obaveza ugovorene isporuke prirodnog gasa;
- gubitka rezervi usled curenja gasa;
- oštećenja cevovoda.

Indirektni troškovi se kvantifikuju težinskim faktorima W_P, W_R i W_C, respektivno. Primenom ovih pretpostavki na tradicionalnu formulu za *ALE* dobija se sledeći izraz za proračun očekivanih godišnjih gubitaka:

$$ALE = W_A W_P W_R W_C Q(t_A + W_A t_{R\max}) c_G \times ARO. \quad (1)$$

Za određivanje vrednosti težinskih faktora W_P, W_R i W_C (koji reflektuju subjektivnu ocenu stručnjaka) kreirane su tri ankete. U simulaciji primene metoda procene bezbednosnog rizika analizira se slučaj projektovanja sistema daljinskog upravljanja novog gasovoda. U anketi koja je formirana radi određivanja težinskih faktora kojim se kvantifikuju indirektni troškovi anketirani su učesnici:

- dispečer iz službe planiranja u gasovodu koji ima sličnu infrastrukturu;
- predstavnik poslovodstva gasovoda koji ima sličnu infrastrukturu;
- stručnjak iz oblasti transportnih sistema.

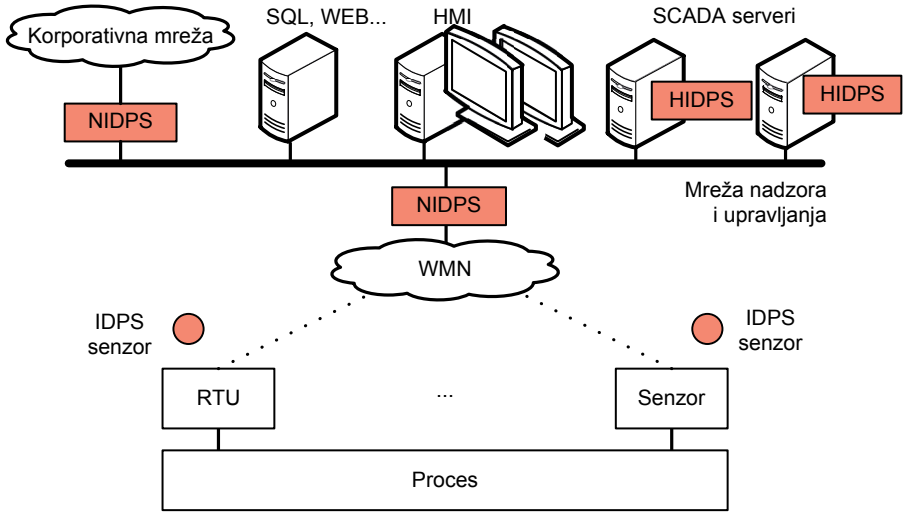
Kompetentnost svakog ankentiranog učesnika je određena AHP metodom na osnovu kriterijuma: (1) radno iskustvo; (2) stepen stručne spreme; (3) vrsta struke i (4) radno mesto.

Konačno, dobijene su sledeće vrednosti težinskih faktora: W_A = 0,204; W_P = 2,84; W_R = 1,17 i W_C = 2,96. Na osnovu dobijenih vrednosti težinskih faktora izračunata je mera rizika R = 2,54.

Unapređenje bezbednosti sistema daljinskog upravljanja u gasovodu postiže se implementacijom algoritama za otkrivanje napada i usvajanjem strategije održavanja funkcionalnosti sistema u uslovima infrastukturnog napada primenom specifičnih algoritama koji vrše prevenciju otkrivenog napada. Sa tim ciljem razmatrana je zaštita mreže komandnog centra i WMN mreže. Za mrežu komandnog centra od interesa je zaštita od DDoS napada i pretpostavljena je implementacija četiri IDPS i to:

- dva mrežna IDPS, prvi sistem prema korporativnoj mreži i drugi sistem prema senzorskoj mreži i
- dva IDPS u hostu na udvojenim SCADA serverima.

Za WMN pretpostavljena je implementacija bežičnih IDPS senzora za spoljašnju montažu (*outdoor*) u zoni RTU-ova i senzora. Na slici 3 prikazan je model analiziranog SCADA sistema nakon implementacije mehanizama zaštite.

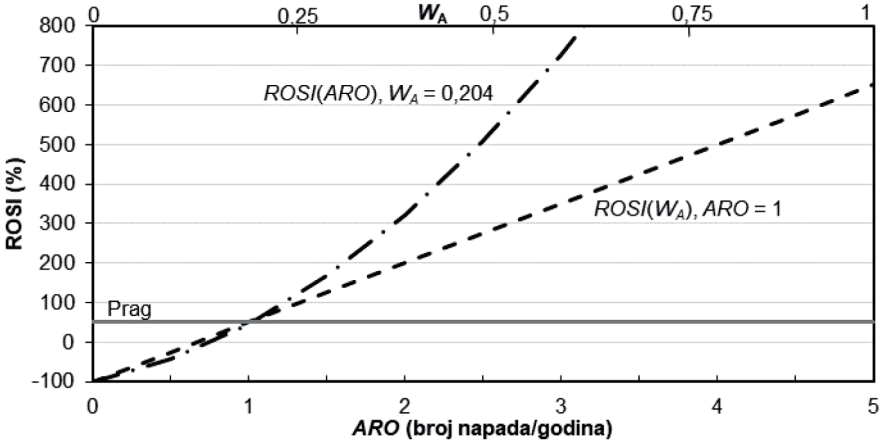


Slika 3. Arhitektura SCADA u gasovodu sistema sa implementiranim IDPS

Na osnovu [11] verovatnoća detektovanih napada od strane IDS sistema kreće se u opsegu 61,5% do 86,2%. U SCADA sistemu su karakteristike legitimnog saobraćaja poznate i predvidljive, pa je verovatnoća detekcije/prevencije napada veća. Iz tog razloga je u analizi pretpostavljeno da verovatnoća detekcije napada iznosi 90%. Prema istraživanju [12] srednje vreme otkaza usled DDoS napada iznosi 30 minuta, a za vreme oporavka u slučaju napada najvećeg intenziteta uzima se t_{Rmax} = 120 minuta. Na osnovu ovih pretpostavki, izračunate *ALE* i vrednosti investicije u zaštitu određen je *ROSI*. Zavisnost *ROSI* od učestanosti napada u toku godine, kao i u funkciji težinskog faktora W_A grafički je prikazana na slici 4.

Za odluku o isplativosti investicije u mehanizam zaštite značajno je da se odredi prag za *ROSI*. Pri definisanju praga moraju se uzeti u obzir značaj konkretnog SCADA sistema i posledice na društvenu zajednicu u slučaju odbijanja servisa daljinskog upravljanja. Za prag označen na slici 4 uočava se pozitivna vrednost *ROSI*, koja ukazuje

da se prihvata investicija za procenjen broj od jednog napada godišnje. U ovom slučaju, investicija u unapređenje bezbednosti IKT infrastrukture je isplativa ako se pretpostavi da bi napad imao intenzitet kvantifikovan težinskim faktorom W_A =0,204. Ukoliko se usvoji pretpostvka o učestanosti napada ARO = 1, isplativost investicije u bezbednost ($ROSI > 0$) postiže se za vrednost težinskog faktora W_A = 0,153.



Slika 4. Zavisnost ROSI od W_A i ARO

5. Zaključak

U radu je prikazan metod procene bezbednosnog rizika u kome se akcenat stavlja na posledice infrastrukturnih napada na telekomunikacionu mrežu SCADA sistema i identifikovanje uslova koji utiču na stepen rizika. Posebna pažnja je usmerena na izbor parametara koji kvantifikuju gubitke nastale usled sajber napada i na određivanje njihovih vrednosti. Vrednosti kvantitativnih parametara određuju se na osnovu statističke analize arhiviranih veličina i subjektivnog mišljenja stručnjaka. Posebna prednost ovog metoda je u tome što se može primenjivati i u fazi projektovanja SCADA sistema, kada arhivski podaci nisu dostupni. U zavisnosti od primene metoda predložena su dva načina izražavanja mere rizika, kvalitativno i monetarno. Metod omogućuje *cost/benefit* analizu, a definisanje prihvatljivog praga za povrat investicija u zaštitu omogućuje donošenje odluke o racionalnom ulaganju u bezbednost SCADA sistema. Primena metoda ilustrovana je za SCADA sistem u magistralnom gasovodu.

Literatura

[1] K. Stouffer, J. Falco and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security", NIST Special Publication 800-82 Rev 2, May 2015.

[2] R. I. Ogie, "Cyber Security Incidents on Critical Infrastructure and Industrial Networks", *in Proc. of the 9th International Conference on Computer and Automation Engineering*, 2017.

[3] S. Patel and J. Zaveri, "A Risk-Assessment Model for Cyber Attacks on Information Systems", *Journal of Computers*, vol. 5, no. 3, pp. 352-359, 2010.

[4] J. Markovic-Petrovic and M. Stojanovic, "Analysis of SCADA System Vulnerabilities to DDoS Attacks", *in Proc. of the 2013 11th International Conference on Telecommunications in Modern Satellite Cable and Broadcasting Services - TELSIKS 2013*, Nis, October 2013.
[5] ITU-T Recommendation E 419, "Business Oriented Key Performance Indicators for Management of Networks and Services", ITU-T, 2006.
[6] T. Saaty, "Decision Making With the Analytic Hierarchy Process", *International Journal of Services Sciences*, vol. 1, no. 1, pp. 83-98, 2008.
[7] J. Markovic-Petrovic and M. Stojanovic, "An Improved Risk Assessment Method for SCADA Information Security," *Elektronika ir Elektrotechnika*, vol. 20, no. 7, pp. 69-72, 2014.
[8] J. Markovic-Petrovic and M. Stojanovic, "A Hybrid Security Risk Assessment Method for SCADA Networks", *in Proc. of 6th International Symposium on Industrial Engineering*, Belgrade, 24 and 25 September 2015.
[9] J. R. Dancy and V. A. Dancy, "Terrorism and Oil & Gas Pipeline Infrastructure: Vulnerability and Potential Liability for Cybersecurity Attacks", *ONE J*, vol. 2, no. 6, pp. 579, 2017.
[10] Y. Wadhawan and C. Neuman, "Evaluating Resilience of Gas Pipeline Systems Under Cyber-Physical Attacks: A Function-Based Methodology", *in Proc. of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy (ACM)*, 2016.
[11] C. Iheagwara, A. Blyth and M. Singhal, "Cost Effective Management Frameworks for Intrusion Detection Systems", *Journal of Computer Security*, vol. 12, no. 5, pp. 777-798, 2004.
[12] J. Pescatore, "DDoS Attacks Advancing and Enduring: A SANS Survey", SANS Tehnical Report, 2014.

Abstract: *The paper presents the general configuration of the Supervisory Control and Data Acquisition (SCADA) system, and then the vulnerabilities of these systems and the degradation of the performances of the remote control service in cyber-attack conditions. We further propose information security risk assessment method for Distributed Denial of Service (DDoS) attacks to the infrastructure of industrial control systems. Simulation of the use of risk assessment method is illustrated in a case study of the modeled SCADA system in natural gas transport.*

Keywords: *intrusion detection and prevention, denial of service, risk assessment, SCADA*

INFORMATION SECURITY RISK ASSESSMENT METHOD IN NATURAL GAS TRANSPORT CONTROL SYSTEMS

Jasna Marković-Petrović, Mirjana Stojanović