UNIVERZITET U BEOGRADU

SAOBRAĆAJNI FAKULTET

Jasna D. Marković-Petrović

PROCENA BEZBEDNOSNOG RIZIKA U INDUSTRIJSKIM SISTEMIMA DALJINSKOG UPRAVLJANJA

Doktorska disertacija

Beograd, 2018

UNIVERSITY OF BELGRADE

FACULTY OF TRANSPORT AND TRAFFIC ENGINEERING

Jasna D. Marković-Petrović

SECURITY RISK ASSESSMENT IN INDUSTRIAL CONTROL SYSTEMS

Doctoral Dissertation

Belgrade, 2018

Mentor: Dr **Mirjana Stojanović,** redovni profesor,
Univerzitet u Beogradu - Saobraćajni fakultet

Članovi komisije: Dr **Miodrag Bakmaz**, redovni profesor
Univerzitet u Beogradu - Saobraćajni fakultet

Dr **Valentina Radojičić**, redovni profesor
Univerzitet u Beogradu - Saobraćajni fakultet

Dr **Andreja Samčović**, redovni profesor
Univerzitet u Beogradu - Saobraćajni fakultet

Dr **Ninel Čukalevski**, naučni savetnik
Univerzitet u Beogradu - Institut „Mihajlo Pupin“

Datum odbrane:

Zahvalnica

Najveću zahvalnost dugujem mentoru dr Mirjani Stojanović koja me je svojim znanjem, profesionalnim iskustvom i višegodišnjim strpljenjem uvela u svet nauke. Bez njene nesebične pomoći i podrške ova disertacija ne bi bila završena.

Zahvaljujem se svim članovima komisije na uloženom vremenu i na sugestijama koje su doprinele konačnom izgledu disertacije.

Posebnu zahvlanost dugujem svojoj porodici na podršci i razumevanju.

PROCENA BEZBEDNOSNOG RIZIKA U INDUSTRIJSKIM SISTEMIMA DALJINSKOG UPRAVLJANJA

Rezime:

Funkcija daljinskog upravljanja industrijskim sistemom postavlja specifične zahteve za informacionu i komunikacionu infrastrukturu, koja treba da obezbedi procesiranje i siguran prenos heterogenih informacija sa različitim zahtevima za kvalitet servisa. Komunikacija se ostvaruje između centra upravljanja i objekata industrijskog sistema, kao i između distribuiranih centara upravljanja. Usvajanje otvorenih komunikacionih standarda, korišćenje otvorenih softverskih platformi, povezanost sistema upravljanja sa drugim mrežama, daljinski pristup i dostupnost tehničkih informacija su razlozi zbog kojih je informaciona i komunikaciona infrastruktura savremenih industrijskih sistema daljinskog upravljnja, a posebno SCADA (*Supervisory Control and Data Acquisition*) sistema podložna različitim vrstama napada.

Uzimajući u obzir evidentnu potrebu za implementacijom specifičnih mehanizama zaštite u mreži industrijskih sistema daljinskog upravljanja, poželjno je da se, pri projektovanju bezbednosnih sistema i kasnije u toku eksploatacije, izvrši procena bezbednosnog rizika, sa ciljem da se odredi racionalan nivo ulaganja u zaštitu.

U disertaciji je prvo utvrđen stepen degradacije ključnih performansi telekomunikacione mreže SCADA sistema, simulacijom različitih uslova distribuiranih napada kao što je napad koji prouzrokuje odbijanje servisa (DDoS – *Distributed Denial of Service*). Zatim su predložena dva nova metoda procene bezbednosnog rizika u slučaju DDoS napada na infrastrukturu SCADA sistema. Prvi, osnovni metod, zasniva se na analizi arhivskih podataka, a pretpostavlja proračun povrata investicija u zaštitu pomoću skupa težinskih faktora, koji kvantifikuju uslove u kojima se dogodio napad. Drugi, hibridni metod, pored analize arhivskih podataka, uzima u obzir subjektivnu ocenu stručnjaka dobijenu na osnovu odgovarajućih anketa. U zavisnosti od primene metoda predložena su dva načina izražavanja mere rizika, kvalitativno i monetarno. Na kraju su predloženi postupci *cost/benefit* analize za preporučenu primenu IDPS (*Intrusion Detection and Prevention System*) mehanizama zaštite na osnovu procenjene mere rizika. Definisanje prihvatljivog praga za povrat investicija u zaštitu omogućuje donošenje odluke o racionalnom ulaganju u bezbednost SCADA sistema.

Za testiranje predloženih metoda definisane su dve studije slučaja: studija slučaja u realnom okruženju protočne hidroelektrane i studija slučaja SCADA sistema u modelovanom magistralnom gasovodu. Rezultati studija slučaja su pokazali da su metodi pogodni za identifikaciju ranjivosti (*vulnerability*) sistema, praktični i primenljivi u različitim industrijskim sektorima. Pored toga, pokazalo se da su metodi efikasni u proceni mere bezbednosnog rizika od infrastukturnog napada i proceni isplativosti ulaganja u poboljšanje bezbednosti infrastrukture SCADA mreža. Studija slučaja u magistralnom gasovodu pokazala je da je drugi metod primenljiv i u fazi projektovanja sistema, kada arhive sa relevantnim podacima nisu dostupne.

Na kraju disertacije, na bazi rezultata istraživanja, predložene su mere za ograničavanje bezbednosnog rizika u industrijskim sistemima daljinskog upravljanja.

Ključne reči: Industrijski sistem daljinskog upravljanja, Internet protokol, bezbednost informacija, bezbednosni rizik, upravljanje rizikom, procena rizika, odbijanje servisa, detekcija napada, prevencija napada

Naučna oblast: Saobraćajno inženjerstvo

Uža naučna oblast: Informaciono-komunikacione tehnologije

UDK broj: 621.39(043.3)

SECURITY RISK ASSESSMENT IN INDUSTRIAL CONTROL SYSTEMS

Abstract:

Remote control of industrial system poses specific requirements for information and communication infrastructure, which has to provide processing and secure transmission of heterogeneous information with different requirements for Quality of Service. Communication takes place between control center and industrial system devices, as well as among distributed control centers. Information and communication infrastructure of modern Supervisory Control and Data Acquisition (SCADA) systems is particularly vulnerable to different cyber security threats due to following reasons: adoption of open communication standards, use of open software platforms, connectivity with other networks, remote access, and availability of technical information.

There is an evident need to implement specific security mechanisms in industrial control networks; hence, in order to determine a cost-effective level of investment, it is desirable to assess security risk during network design phase, as well as during network operation.

In this thesis, we first investigate the level of network performance degradation in SCADA systems by simulation of different conditions of distributed attacks such as Distributed Denial of Service (DDoS). Further, two novel methods for security risk assessment are proposed for the case of DDoS attack on the SCADA system infrastructure. The first, basic method relies on the analysis of historical data, and assumes calculating return on security investment as a function of the set of weighting factors that quantify the attack conditions. The second, hybrid method takes into account both hictorical data and subjective assessment of experts, provided by appropriate questionnaires. Depending on method application two ways (qualitative and monetary) for expressing the risk measure are proposed. Finally, techniques of cost/benefit analysis are also proposed for recommended application of intrusion detection and prevention system, based on the assessed risk measure. Definition of acceptable threshold for return on security investment allows making decision about cost-effective level of investment in security of SCADA system.

For testing of proposed risk assessment methods, two case studies are defined: the first one considers real environment of a run-off-river hydropower plant, and the second one investigates the SCADA system in a simulated main pipeline. The results of case studies have shown that proposed methods are suitable for identification of system's vulnerability, useful and applicable in different industrial sectors. Besides, proposed methods are efficient in security risk assessment regarding infrastructure attacks as well as in analysis of investment feasibility regarding enhancement of the SCADA network infrastructure security. Case study of the main pipeline also shows that the second method is applicable in the system design phase when relevant historical data are not available.

Finally, a set of measures for limitation and mitigation of security risk in industrial control systems are proposed and discussed.

Key words: industrial control system, Internet protocol, information security, security risk, risk management, risk assessment, denial of service, intrusion detection, intrusion prevention

Scientific field: Traffic Engineering

Scientific subfield: Information and Communications Technologies

UDC number: 621.39(043.3)

SADRŽAJ

SPISAK SKRAĆENICA

I Stručni izrazi

ACT	Attack Countermeasure Tree
ADVISE	ADversary VIew Security Evaluation
AEG	Attack Execution Graph
AHP	Analytical Hierarchical Process
ALE	Annual Loss Expectancy
ARO	Annual Rate of Occurrence
AV	Asset Value
BDMP	Boolean Logic Driven Markov Proces
CC	Consistency Check
CIA	Confidentiality, Integrity, Availability
COBIT	Control Objectives for Information and Related Technology
CPU	Central Processing Unit
CRAMM	CCTA Risk Analysis and Management Method
CTM	Cascading Threat Multiplier
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DL	Direct Loss
DMZ	Demilitarized Zone
DNP3	Distributed Network Protocol
DNS	Domain Name System
DNSSEC	Domain Name System SECurity extensions
DoS	Denial of Service
DPF	Distributed Packet Filtering
DV	Distance Vector
EF	Exposure Factor
FA	False Alarm
FMECA	Failure Mode and Effect Criticality Analysis
FN	False Negative
FP	False Positive
FTA	Fault Tree Analysis
FTP	File Transfer Protocol
HART	Highway Addressable Remote Transducer Protocol
HazOP	HAZard and Operability study

HHM	Hierarchial Holographic Modelling
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
ICCP	Inter-Control Center Communications Protocol
ICS	Industrial Control System
IDPS	Intrusion Detection and Prevention Systems
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IRC	Internet Relay Chat
ISRAM	Information Security Risk Analysis Method
IT	Information Technology
KPI	Key Performance Indicator
LAN	Local Area Network
LS	Link State
MAC	Medium Access Control
MTU	Master Terminal Unit
NBA	Network Behavior Analysis
NSRM	Network Security Risk Model
OPGW	Optical Ground Wire
OPNET	Optimized Network Engineering Tool
PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
RAIM	Real-time monitoring, Anomaly detection, Impact analysis and Mitigation strategies
RAT	Remote Access Tool
ROI	Return on Investment
ROSI	Return on Security Investment
RTU	Remote Terminal Unit
SAN	Stochastic Activity Networks
SCADA	Supervisory Control and Data Acquisition
SCP	Secure Copy
SFTP	Secure FTP
SLE	Single Loss Expectancy

SSH	Secure Shell
SWN	Stochastic Well-formed Network
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TN	True Negative
ToS	Type of Service
TP	True Positive
UDP	User Datagram Protocol
UML	Unified Modelling Language
VNC	Virtual Network Computing
VPN	Virtual Private Network
WFQ	Weighted Fair Queuing
WMN	Wireless Mesh Network
ACT	Attack Countermeasure Tree
ADVISE	ADversary VIew Security Evaluation

II Nazivi organizacija i standarda

AGA	American Gas Association
API	American Petroleum Institute
AS/NZS	Australian/New Zealand Standard
BS	British Standards
CIGRÉ	Conseil International des Grands Réseaux Électriques
DoE	U.S. Department of Energy
ENISA	European Network and Information Security Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISA	International Society of Automation
ISO	International Organization for Standardization
ITU	International Telecommunication Union
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
RISI	Repository of Industrial Security Incidents

SPISAK SLIKA

SPISAK TABELA

1. UVOD

Industrijski sistemi daljinskog upravljanja predstavljaju pravac razvoja i modernizacije velikih industrijskih pogona sa ciljem višeparametarskog nadzora i upravljanja industrijskih ciklusa i kao takvi danas su od vitalnog značaja za funkcionisanje industrijskih sektora na kojima se zasniva kritična infrastruktura države. SCADA (*Supervisory Control and Data Acquisition*) sistemi nadziru i upravljaju u realnom vremenu procesnom opremom smeštenom na većem broju geografski distribuiranih lokacija, kada je centralizovano prikupljanje i upravljanje podacima od suštinskog značaja za funkcionisanje procesa. Oni su u širokoj upotrebi u industrijskom sektoru, prvenstveno u proizvodnji, prenosu i distribuciji električne energije, industriji nafte i gasa, vodoprivredi, kao i u saobraćaju i transportu. Otkazi i neispravan rad takvih sistema mogu prouzrokovati ozbiljne posledice zbog njihovog strateškog značaja za kritičnu infrastrukturu svake države.

Razvoj SCADA sistema je počeo pre upotrebe Interneta, u periodu kada se potreba za bezbednošću informacija uglavnom sastojala od zaštite fizičkog pristupa računarima sistema. Tokom poslednjih dvadeset godina, 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. Ova tendencija će se sigurno nastaviti s obzirom na potrebu standardizacije sistema, pre svega sa aspekta pristupa, prikupljanja i obrade podataka. Ovaj pravac razvoja dodatno se ubrzava sve češćom primenom koncepcije pametnih mreža (*smart grid*), uvođenjem koncepta veštačke inteligencije i složenih sistema daljinskog nadzora, sve većeg broja udaljenih korisnika, pojave novih mobilnih uređaja i korišćenja javnih i privatnih *cloud computing* servisa. 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 industrijske sisteme daljinskog upravljanja. Primena konvencionalnih mehanizama zaštite nije uvek dobro rešenje za SCADA sisteme, jer se zahtevi u aspektima pouzdanosti, kvaliteta servisa i primenjenih

informacionih i komunikacionih tehnologija razlikuju za poslovne informacione i SCADA sisteme.

1.1. Predmet i cilj istraživanja

S obzirom na neophodnost implementacije specifičnih mehanizama zaštite u mreži industrijskih sistema daljinskog upravljanja, važno je da se pri projektovanju sistema izvrši procena bezbednosnog rizika, sa ciljem da se odredi racionalan nivo ulaganja. Upravljanje rizikom je kontinualan proces, a svi koraci se ciklično ponavljaju, kako zbog preostalog rizika tako i zbog stalnog unapređenja, proširenja sistema i potencijalne pojave novih ranjivosti i pretnji. Procena rizika treba da omogući usvajanje strategije o postupanju sa rizikom, odlučivanje o investicijama u bezbednosni sistem industrijskih sistema daljinskog upravljanja u strategiji smanjenja rizika i definisanje prihvatljivog rizika.

Pokazalo se da opšti kvantitativni metodi procene rizika u informacionim i komunikacionim sistemima, zasnovani isključivo na ekonomskim kategorijama, nisu adekvatni za industrijske sisteme daljinskog upravljanja, zbog toga što ne uzimaju u obzir specifičnosti u aspektima pouzdanosti, zahteva za kvalitet servisa i primenjenih protokola.

Rezultati studije [1] pokazuju nedostatak referentnog metoda procene bezbednosnog rizika u industriji i potvrđuju potrebu za definisanjem metodologije koja integriše upravljanje i procenu bezbednosnog rizika operativnih i poslovnih infrastuktura. Poželjno je da ovakva metodologija bude prihvaćena od strane većine industrijskih sistema i da objedini njihove specifičnosti.

U distertaciji su predloženi metodi procene bezbednosnog rizika u slučaju distribuiranog odbijanja servisa usled napada na infrastrukturu SCADA sistema i postupak *cost/benefit* analize za preporučenu primenu mehanizama zaštite pomoću sistema za detekciju i prevenciju napada (IDPS – *Intrusion Detection and Prevention System*). U DoS (*Denial of Service)* napadu, 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 da se blokiraju glavni resursi žrtve ili da se iscrpi raspoloživi mrežni propusni opseg što za posledicu ima odbijanje servisa.

Metodi procene bezbednosnog rizika, predloženi u disertaciji, pretpostavljaju kombinaciju kvantitativnog i kvalitativnog pristupa. Procena rizika se zasniva na matematičkom pristupu i ekonomskim parametrima, a obuhvata proračun očekivanog godišnjeg gubitka i povrata investicija u zaštitu. Kvalitativni pristup se ogleda u definisanju težinskih faktora, koji kvantifikuju uslove u kojima se dogodio napad, a zavise od brojnih tehno-ekonomskih faktora. Predloženi metod definiše preduslove za određivanje ovih faktora, a to su analiza statističkih podataka, definisanje ključnih indikatora performansi u skladu sa zahtevanim performansama koje obezbeđuju ostvarenje poslovnih ciljeva i uzimanje u obzir subjektivnog mišljenja stručnjaka koji su relevantni za proces upravljanja i eksploatacije u predmetnom industrijskom sistemu daljinskog upravljanja. Definisanje prihvatljivog praga za povrat investicija u zaštitu omogućuje donošenje odluke o racionalnom ulaganju u zaštitu SCADA sistema.

Primarni cilj metoda za procenu bezbednosnog rizika koji su predloženi u disertaciji je identifikovanje ranjivosti sistema, procena mere bezbednosnog rizika od infrastukturnog napada, predlog adekvatnih mehanizama zaštite i procena isplativosti ulaganja u poboljšanje bezbednosti informacione infrastrukture industrijskog sistema daljinskog upravljanja. Pored toga, cilj je da metodi budu sveobuhvatni, praktični, jednostavni za učenje i lako primenljivi, otvoreni za proveru, zasnovani na eksplicitnim pretpostavkama i premisama, primenljivi u različitim sektorima i industrijama i da su inovativni, a pre svega da su efikasni u ispunjenju primarnog cilja.

1.2. Polazne hipoteze i naučni metodi istraživanja

Polazne hipoteze u istraživanju su:

- Napadi na informacione i komunikacione sisteme za podršku daljinskog upravljanja potencijalno ugrožavaju vitalne funkcije industrijskog sistema. Zbog toga je, pri projektovanju i eksploataciji, neophodno kontinuirano upravljanje bezbednosnim rizikom, kao i razvoj novih metoda procene rizika.

- Razmatraju se sistemi za prevenciju napada i sistemi za detekciju napada.
- Tradicionalni kvantitativni metodi procene bezbednosnog rizika, zasnovani isključivo na ekonomskim kategorijama (očekivani godišnji gubitak, povrat investicija), nisu adekvatni za industrijske sisteme daljinskog upravljanja, zbog toga što ne uzimaju u obzir specifičnosti ovih sistema u aspektima pouzdanosti, kvaliteta servisa i primenjenih informacionih i komunikacionih tehnologija.
- Definisanjem i izborom adekvatnog metoda procene rizika moguće je odrediti racionalan nivo ulaganja u mehanizme zaštite industrijskih sistema daljinskog upravljanja, sa prvenstvenim ciljem prevencije napada.
- Pretpostavlja se definisanje različitih nivoa prihvatljivog rizika.

Pri izradi doktorske disertacije, pored opštih metoda naučnog istraživanja korišćeni su sledeći metodi:

- Klasični metodi prikupljanja, sistematizacije i komparativne analize pri pregledu i klasifikaciji do sada formulisanih i u praksi primenjenih rezultata.
- Matematičko modelovanje, numerička analiza i računarska simulacija.

1.3. Struktura doktorske disertacije

Disertacija je organizovana u osam poglavlja.

U drugom poglavlju analizirana je bezbednost industrijskih sistema daljinskog upravljanja, i to onih koji su deo kritične infrastrukture. Prvo su prikazane osnovne karakteristike i struktura SCADA sistema, a zatim analiza ranjivosti i razlozi za ugroženu bezbednost ovih sistema. U nastavku je prikazana klasifikacija napada na infrastrukturu informacionih i komunikacionih sistema. Posebna pažnja je usmerena na napade koji su specifični za SCADA sisteme i dat je pregled nekih uspešno izvedenih napada na infrastrukturu SCADA sistema. S obzirom da je u disertaciji pažnja usmerena na infrastukturne DDoS napade, preporučen je mehanizam zaštite implementacijom sistema za detekciju i prevenciju napada. Tehnologije ovih sistema, sa posebno istaknutim specifičnostima primene u industrijskim sistemima daljinskog upravljanja prikazane su na kraju poglavlja.

Treće poglavlje sadrži pregled procesa upravljanja bezbednosnim rizikom sa akcentom na postupak procene rizika. U nastavku poglavlja dat je pregled literature i analiza aktuelnih problema istraživanja. Prvo su prikazani standardi i preporuke za upravljanje bezbednosnim rizikom koji su relevantni za SCADA sisteme. Zatim je dat pregled opštih i komercijalnih metoda procene rizika u informacionim sistemima i analiza njihove primenljivosti u industrijskim sistemima daljinskog upravljanja. Na kraju je dat pregled i uporedna analiza metoda namenjenih za procenu bezbednosnog rizika SCADA sistema.

Četvrto poglavlje prikazuje simulacionu analizu performansi sistema daljinskog upravljanja u uslovima simultanih, distribuiranih napada na infrastrukturu mreže zasnovane na tehnologiji Internet protokola (IP – *Internet Protocol*). Simuliran je napad na infrastrukturu SCADA sistema u hidroelektrani. Razvijen je simulacioni model i analizirane su performanse operativnog servisa daljinskog upravljanja u uslovima DDoS napada. Rezultati simulacije ukazuju na degradaciju performansi (raspoloživost, kašnjenje, procenat izgubljenih paketa, opterećenje procesorskih resursa) i uskraćivanje usluga operativnog servisa daljinskog upravljanja.

U petom poglavlju predložen je način izbora kvantitativnih parametara za procenu gubitaka koji su posledica sajber napada na infrastrukturu industrijskog sistema daljinskog upravljanja i metoda procene bezbednosnog rizika u industrijskim SCADA sistemima. Predloženi metodi su zasnovani na činjenici da je rizik srazmeran gubicima koji su posledica sajber napada na infrastrukturu industrijskog sistema daljinskog upravljanja. Metod uključuje niz aktivnosti u cilju analize i procene bezbednosnog rizika. Predložena su dva metoda: (1) osnovni metod u kome se kvantitativni parametari određuju na osnovu statističke analize relevantnih arhiviranih mernih veličina u SCADA sistemu i (2) hibridni metod u kome se kvantitativni parametri osim statističkom analizom arhiva određuju i na osnovu mišljenja relevantnih stručnjaka. U zavisnosti od primene metoda predložena su dva načina izražavanja mere rizika, kvalitativno i monetarno. Završna faza metoda je odabir mehanizama zaštite i *cost/benefit* analiza implementacije kontrolnih mera na osnovu procenjene mere rizika.

U šestom poglavlju su prikazani rezultati verifikacije predloženih metoda. Prvi slučaj je primena metoda u protočnoj hidroelektrani. Analizirana je primena osnovnog metoda, a

na osnovu dobijenih parametara određena je mera rizika i sprovedena *cost/benefit* analiza za predložene mehanizme zaštite. Na istom primeru primenjen je i hibridni metod. Uticaj subjektivne komponente kvalitativnih parametara je analiziran komparativnom analizom rezultata oba metoda. U drugom slučaju je prezentovana simulacija primene metoda procene rizika u transportnom sistemu prirodnog gasa, čiji je model dat u stručnoj literaturi. Simulirana je primena metoda u fazi projektovanja sistema za daljinsko upravljanje, kada arhive relevantnih parametara nisu raspoložive. Iz tog razloga se primenjuje hibridni metod, i to faza u kojoj se kvalitativni parametri određuju na osnovu mišljenja stručnjaka.

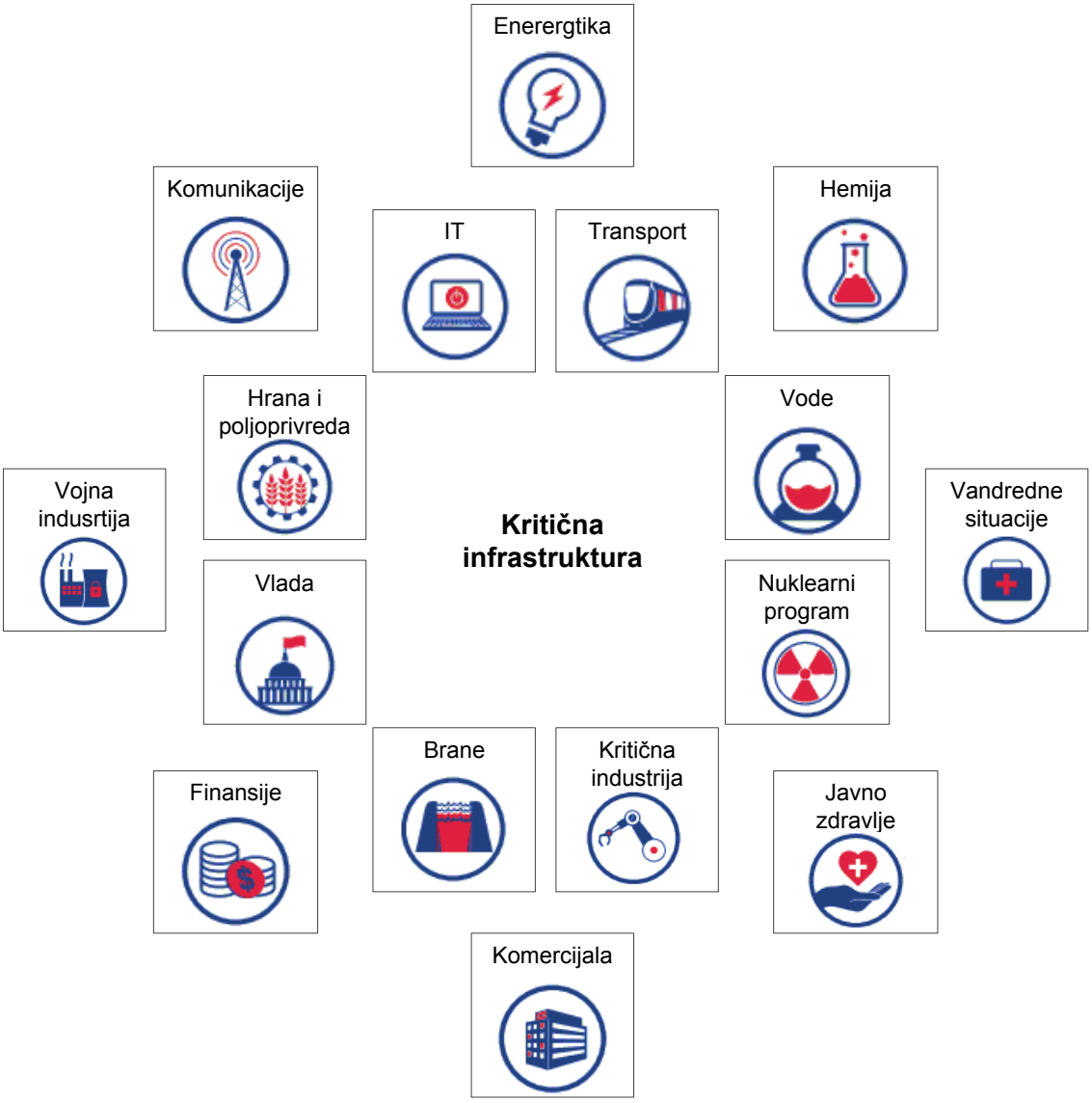
U sedmom poglavlju je prikazana arhitektura industrijskih sistema daljinskog upravljanja sa aspekta bezbednosti u skladu sa *Defense-in-Depth* startegijom, a zatim su predložene mere za ograničenje bezbednosnog rizika.

Osmo poglavlje obuhvata zaključna razmatranja.

2. BEZBEDNOST INDUSTRIJSKIH SISTEMA DALJINSKOG UPRAVLJANJA

Kritična infrastruktura obuhvata objekte od vitalnog značaja za svaku državu čije oštećenje ili uništenje dovodi do prekida isporuke neke usluge. U Sjedinjenim Američkim Državama je nakon terorističkog napada 11. septembra 2001. godine formirano Ministarstvo državne bezbednosti u čijoj je nadležnosti bezbednost kritične infrastrukture, a koju čini 16 sektora (slika 2.1): sektor komunikacija, energetika, informacione tehnologije, transport, sistemi vodosnabdevanja i prerade otpadnih voda, hemijski sektor, brane, nuklearni reaktori, radioaktivni materijali i otpad, javno zdravlje, poljoprivreda i hrana, hitne službe, industrija u službi odbrane, kritična industrija (metalska, auto, avio, mašinska, elektroindustrija), vlada, finansije i komercijalni sektor. Među ovim sektorima postoji međuzavisnost. Karakteristično za više od polovine sektora je da ključnu ulogu u upravljanju kritičnim procesima imaju industrijski sistemi daljinskog upravljanja. Industrijski sistem daljinskog upravljanja (ICS – *Industrial Control System*) je opšti pojam koji obuhvata više tipova upravljačkih sistema. To su prvenstveno SCADA sistemi (koje karakteriše geografska razuđenost tipična za transportnu i distributivnu industriju), distribuirani upravljački sistemi (DCS – *Distributed Control System*) koji su karakteristični za upravljanje lokalnim procesima i programabilni logički kontroleri (PLC – *Programmable Logic Controller*) koji se mogu implementirati u manjim sistemima, bez kontrolnog centra, kada se upravljanje procesom izvršava automatski [2]. Sa aspekta bezbednosti SCADA sistemi su najpodložniji infrastrukturnim napadima pa će se u nastavku disertacije izrazi industrijski sistemi daljinskog upravljanja i SCADA sistemi koristiti ravnopravno.

Za razliku od javnih i korporativnih informacionih sistema, u kojima je bezbednost informacija i infrastrukture dostigla određeni nivo zrelosti, u industrijskim sistemima ne mogu se pravolinijski uvesti ista rešenja, već su u većini slučajeva potrebna nova rešenja zaštite koja su prilagođena kontrolnom okruženju industrijske celine. Ova rešenja često moraju da uzmu u obzir posebnosti koje su posledice različitih tehnologija i industrijskih procesa i nažalost, ne mogu se generalizovati.



Slika 2.1. Kritična infrastruktura po sektorima.

U ovom poglavlju analizirana je bezbednost industrijskih sistema daljinskog upravljanja kao dela kritične infrastrukture.

2.1. Osnovne karakteristike SCADA sistema

SCADA sistemi upravljaju u realnom vremenu procesnom opremom različite generacije, vrste i namene (motori, ventili, pumpe i releji) i koja je smeštena na većem broju geografski distribuiranih lokacija. Centralizovano prikupljanje i upravljanje podacima su od suštinskog značaja za funkcionisanje procesa. SCADA sistem se može

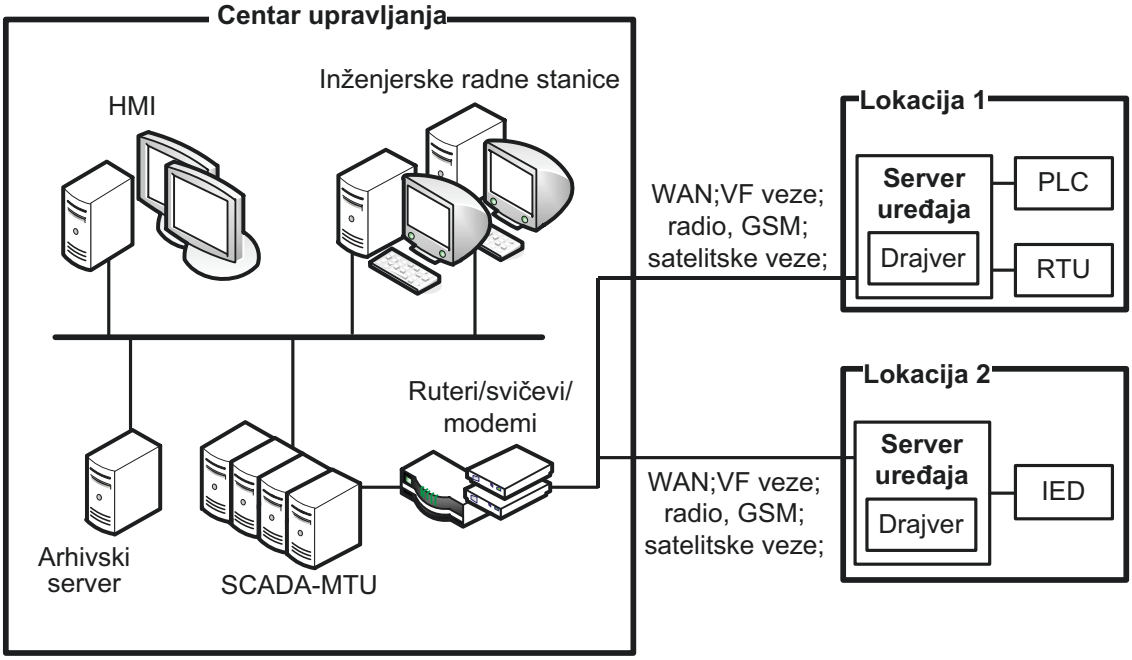
sastojati od stotina, hiljada do desetine hiljada kontrolnih tačaka kojim se upravlja daljinski u realnom vremenu. Sve ovo uslovljava da industrijski sistemi daljinskog upravljanja imaju složenu infrastukturu.

SCADA sistemi su u širokoj upotrebi u industrijskom sektoru, prvenstveno u proizvodnji, prenosu i distribuciji električne energije, industriji nafte i gasa, vodoprivredi, preradi otpadnih voda, kao i u saobraćaju i transportu. Njihov glavni zadatak je da operaterima obezbedi sredstvo i način upravljanja visoko automatizovanim procesima. Neophodan je pregled celokupnog sistema sa lako dostupnim relevantnim informacijama o stanju svakog, ili bar velikog broja, procesa kako bi se omogućila pravovremena akcija operatera. Otkazi i neispravan rad takvih sistema mogu prouzrokovati ozbiljne posledice zbog njihovog strateškog značaja za kritičnu infrastrukturu svake države.

Na slici 2.2 prikazana je opšta blok šema SCADA sistema na kojoj su predstavljeni sledeći podsistemi:

- Podsistem daljinskih telemetrijskih jedinica (RTUs – *Remote Terminal Units*), programabilnih logičkih kontrolera i inteligentnih elektronskih uređaja (IEDs – *Intelligent Electronic Devices*). U njemu se vrši lokalna kontrola mernih pretvarača i nadzor senzora, preko kojih se vrši prikupljanje analognih i digitalnih veličina, kao i izdavanje upravljačkih naloga procesu u vidu digitalnih komandi ili zadavanjem analognih vrednosti neke veličine.
- Centralni podsistem, koji čini lokalna mreža u centru upravljanja koja povezuje SCADA server, arhivski server, server sa softverom za vizuelizaciju, npr. VNC (*Virtual Network Computing*), HMI (*Human Machine Interface*) server i konzole, kao i rutere i/ili svičeve za komunikaciju sa daljinskim stanicama. Centar upravljanja prikuplja i analizira informacije od daljinskih stanica (na različitim lokacijama), prezentuje ih na HMI i generiše akcije na osnovu detektovanih događaja. Centar upravljanja je odgovoran i za opšte alarme, analizu trendova i generisanje izveštaja.
- Komunikacioni podsistem povezuje centar upravljanja sa podsistemom daljinskih stanica i omogućuje operateru daljinski pristup stanicama preko *fieldbus*-ova za potrebe dijagnostike i otklanjanja otkaza.

Većinu savremenih SCADA sistema karakteriše formiranje posebne podmreže, povezane sa korporativnom mrežom preduzeća. Operaterska mesta mogu se implementirati i u klijentima poslovne mreže, posredstvom veb aplikacija.



Slika 2.2. Opšta blok šema SCADA sistema [2].

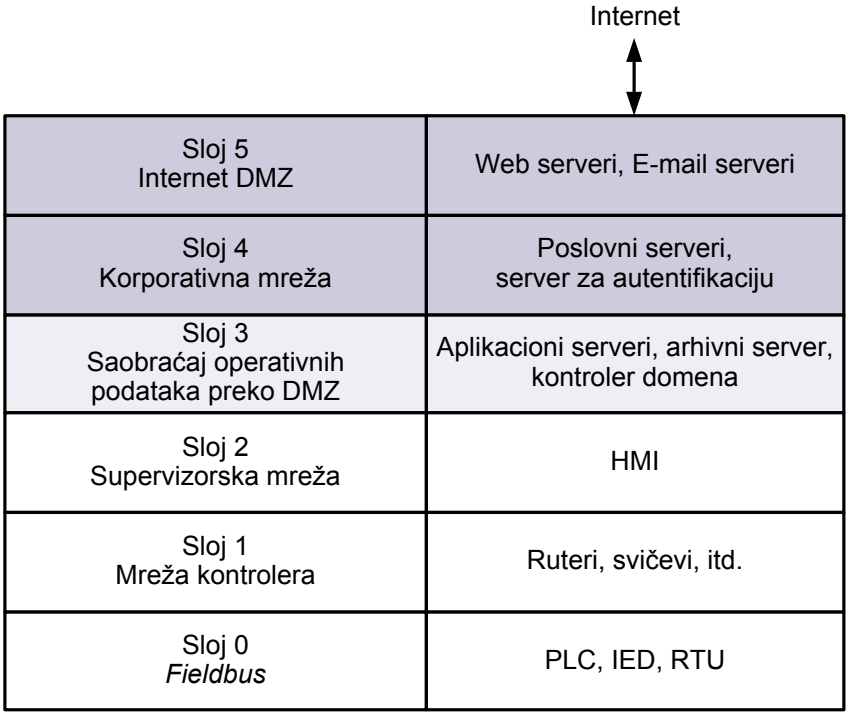
Komunikacioni podsistem treba da obezbedi pouzdan prenos i razmenu informacija između daljinskih telemetrijskih stanica i centra upravljanja, koristeći telekomunikacione tehnologije visokih performansi. On ima mogućnost rada u modu ciklične prozivke, kada centar upravljanja periodično proziva i prikuplja podatke od konektovanih daljinskih jedinica, kao i u modu komunikacije na zahtev, koja se inicira registrovanjem unapred definisanih događaja od strane daljinske jedinice. Komunikacija između daljinskih jedinica i centra upravljanja može se obavljati radio-linkovima, iznajmljenim telefonskim linijama ili posredstvom optičkih vlakana postavljenih unutar zaštitne užadi po dalekovodima (OPGW – *Optical Ground Wire*) karakterističnih za elektroprivredu.

Telekomunikacioni podsistemi savremenih SCADA sistema zasnovani su na otvorenim komunikacionim standardima kao što su Eternet, TCP/IP (*Transmission Control Protocol/Internet Protocol*) skup protokola i bežični standardi (IEEE 802.x, *Zigbee*,

Bluetooth, *WirelessHART*). Tendencija umrežavanja nastavlja se ka okruženjima kao što je *cloud* računarstvo.

Za komunikaciju centra upravljanja sa periferijama se koriste standardni ili namenski protokoli, preko veza tipa tačka-tačka ili širokopojasne IP-bazirane mreže. Postoji veći broj standardnih i specijalizovanih SCADA komunikacionih protokola među kojima su najrasprostranjeniji Modbus, DNP3 (*Distributed Network Protocol*), IEC protokoli serije 60870-5 i IEC standard 61850 namenjen za transformatorske stanice u električnoj mreži. Većina protokola projektovana je ili prilagođena za rad u TCP/IP mreži. Pored toga, najveći broj savremenih *fieldbus* protokola zasnovan je na Eternet tehnologiji. Sistematizovan pregled SCADA protokola može se pronaći u literaturi [3], [4].

Industrijski sistemi daljinskog upravljanja karakterišu se slojevitom i funkcionalno odvojenom hijerarhijom sa različitim protokolima i fizičkim standardima [3], [5]. Slojevita hijerarhija SCADA sistema definiše se u skladu sa međusobnom vezom njegovih komponenata, kao i načinom povezivanja sa eksternim mrežama, kao što je ilustrovano na slici 2.3.



Slika 2.3. Slojevita struktura SCADA sistema.

Najniži sloj (sloj 0) predstavlja fizičke uređaje, koji su u direktnoj interakciji sa fizičkim hardverom, a međusobno su povezani preko *fieldbus*-a. Sloj 1 se sastoji od kontrolera, koji procesiraju signale sa *field* uređaja i generišu odgovarajuće komande za te uređaje. Rezultati procesiranja se prosleđuju sloju 2 na dalju analizu i kontrolu odziva. Sloj 3 tipično predstavlja demilitarizovanu zonu (DMZ) u kojoj su smešteni aplikacioni serveri, arhivski server i kontroleri domena. Viši slojevi odgovaraju korporativnoj IT (*Information Technology*) mreži, koja je povezana na Internet.

2.2. SCADA sa aspekta bezbednosti

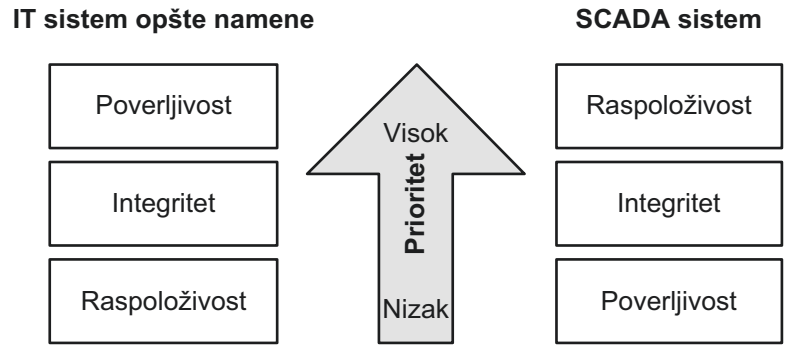
Strateška uloga kritične infrastrukture i tehnološki napredak uslovljavaju potrebu za savremenim informacionim i komunikacionim sistemom. Od ovih sistema se očekuje da obezbede visoku pouzdanost, raspoloživost i prenos ispravnih i pravovremenih informacija u cilju planiranja proizvodnje, efikasnog iskorišćenja resursa, daljinskog upravljanja proizvodnim pogonima, izveštavanja i uspešnog poslovanja industrijskog sistema.

Savremene industrijske telekomunikacione mreže se zasnivaju na koncepciji multiservisnih mreža pri čemu je IP tehnologija prihvaćena kao osnov za integraciju operativnih i poslovnih servisa. Ovako koncipirane mreže imaju propuste i ranjivosti koje su poznate zlonamernim korisnicima. U svetu je zabeleženo više napada na industrijske sisteme [6], [7], [8], [9]. Zbog toga se javlja potreba za stalnim unapređenjem zaštite telekomunikacione mreže. Posebno treba imati u vidu potencijalnu migraciju SCADA sistema ka *cloud* okruženju. Takva realizacija doprinosi smanjenju troškova i poboljšanju efikasnosti poslovanja, ali postavlja dodatne zahteve za bezbednost [10].

Upravljanje zaštitom je trajan proces, a treba da obezbedi bezbedan pristup informacijama i resursima u mreži, i to obezbeđenjem poverljivosti i integriteta informacija, autentifikacije korisnika, kontrole pristupa, raspoloživosti usluga i neporecivosti akcija. Za infrastrukture opšte namene usvojen je princip bezbednosti CIA (*Confidentiality, Integrity, Availability*), „trojka“ koja prioritet daje poverljivosti, zatim integritetu i na poslednjem mestu raspoloživosti podataka. Za infrastrukturu

industrijskih sistema daljinskog upravljanja usvojena je ista „trojka“, ali sa obrnutim redosledom prioriteta, gde je najvažnija raspoloživost, a zatim slede integritet i poverljivost podataka (slika 2.4). Ova razlika je značajna sa aspekta politike bezbednosti i pravaca u primeni mehanizama zaštite gde je najvažnije očuvanje raspoloživosti svih sistema koji su značajni za kritičnu infrastrukturu 24 sata 7 dana u nedelji (24/7).

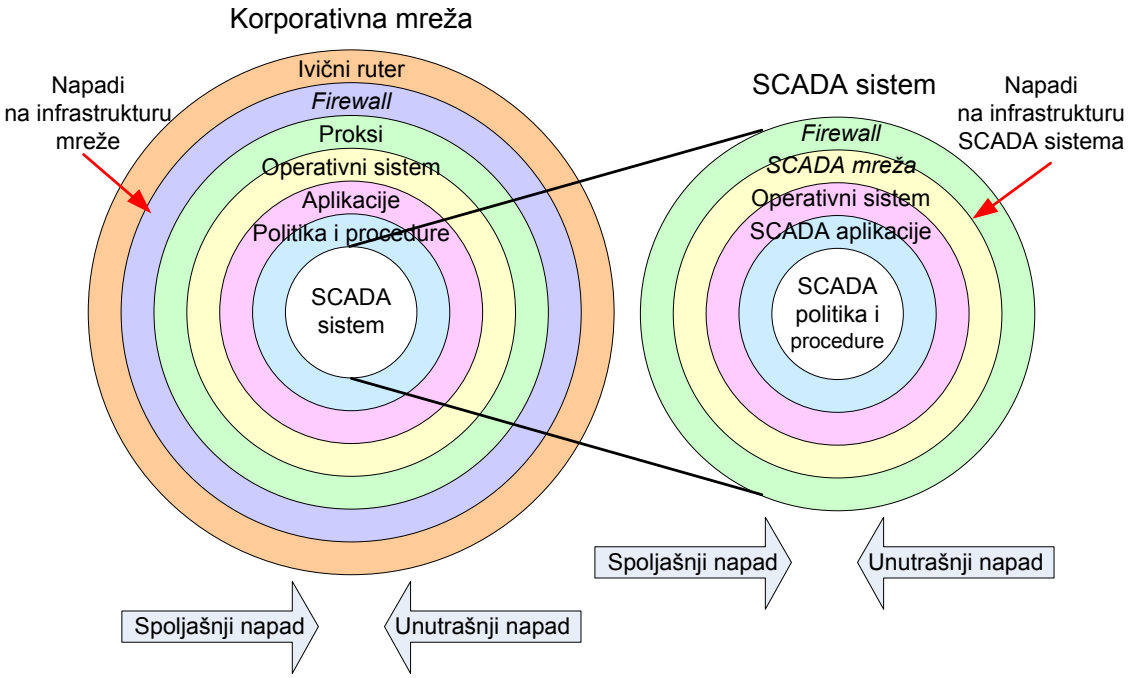
Zaštita mreže se sastoji od prevencije, detekcije i odgovora na napad. Upravljanje zaštitom informacionih i komunikacionih sistema podrazumeva definisanje politike zaštite i izbor odgovarajućih mehanizama zaštite. Pri tome je potrebno da se sprovede analiza ranjivosti sistema, analiza i procena rizika, izbor i implementacija mehanizama zaštite i praćenje njene efikasnosti [11].



Slika 2.4. Principi bezbednosti u IT sistemima i industrijskim sistemima daljinskog upravljanja.

Industrijski informacioni i komunikacioni sistemi se projektuju tako da pružaju operativne i poslovne servise. Ovi servisi postavljaju određeni broj specifičnih zahteva, u pogledu performansi i tehničkih karakteristika. Pod ovim se podrazumeva kašnjenje između krajnjih tačaka, raspoloživost, propusni opseg, tolerancija bitske greške, džiter i dr. Mehanizmi zaštite telekomunikacione mreže se planiraju i primenjuju u procesu projektovanja i implementacije, kao i tokom njenog životnog veka i to na fizičkom, softverskom i organizacionom nivou. Politikom zaštite definišu se ciljevi, pravila, formalne procedure poslovnog procesa, uloge zaposlenih, dozvoljene aktivnosti, akcije, procesi i sl. Pravilima se definiše način obezbeđivanja integriteta informacija, određuje se poverljivost informacija, određuju vrste i nivoi privilegija u pristupu podacima, kao i pravo korišćenja resursa i aplikacija.

Jedna od glavnih specifičnosti poslovnih informacionih i komunikacionih sistema u industriji je integracija sa sistemom za daljinski nadzor i upravljanje industrijskim postrojenjima. Na slici 2.5 prikazani su „prsteni zaštite“ korporativne i SCADA mreže. Napadi na SCADA sistem mogu budu spoljni, preko Interneta kroz korporativnu mrežu, ili unutrašnji koji mogu poticati iz korporativne mreže ili mreže SCADA sistema (sa nivoa RTU ili nivoa aplikacije).



Slika 2.5. Odnos između korporativne i SCADA telekomunikacione mreže.

Razvoj odgovarajuće strategije zaštite podrazumeva analizu višestrukih slojeva arhitekture korporativne mreže i SCADA sistema (koje obuhvataju *firewall*-ove, proksi servere, operativne sisteme, aplikacije, komunikacije i politiku i procedure zaštite).

Povećanje ranjivosti SCADA sistema uslovljeno je sledećim faktorima [12]:

- usvajanje otvorenih standarda sa poznatim propustima;
- povezanost sistema daljinskog upravljanja sa drugim mrežama;
- ograničenja u postojećim tehnologijama zaštite;
- daljinski pristup;
- dostupnost tehničkih informacija o sistemima daljinskog upravljanja.

Tipične pretnje savremenim SCADA sistemima su zlonamerni programi, unutrašnji i spoljašnji napadi. Zlonamerni korisnici koriste poznate ranjivosti informacionih i komunikacionih sistema, ali i specifične nedostatke u mehanizmima zaštite SCADA sistema [11] kao što su:

- propusti u operativnom sistemu;
- često zanemarena autentifikacija;
- udaljeni pristup kojim je omogućena konfiguracija sistema;
- povezanost sa drugim mrežama;
- primena bežičnih veza;
- izostanak primene antivirusnih softvera u cilju racionalnog korišćenja procesorskih resursa zbog rada u realnom vremenu;
- odsustvo sistema za detekciju i prevenciju napada (IDPS);
- nedovoljno iskustvo zaposlenih lica;
- nedovoljno fizičko obezbeđenje lokacija na kojima se nalaze uređaji SCADA sistema, a koji su veome često geografski razuđeni i bez posade.

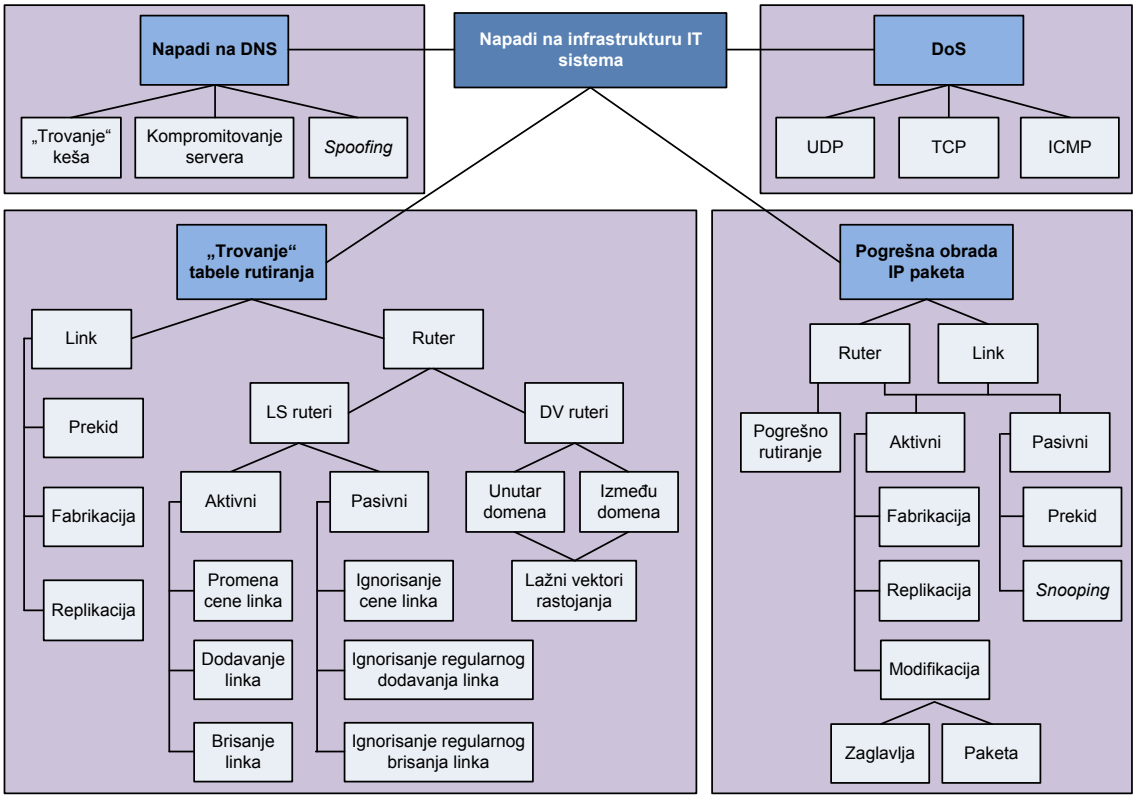
2.3. Sistematizacija napada na infrastrukturu informacionih i komunikacionih sistema

S obzirom da su telekomunikacione mreže u industriji zasnovane na IP tehnologiji [13], dobra osnova za analizu bezednosnog rizika ovih mreža je pregled različitih vrsta napada na infrastrukturu globalnog Interneta i mogućih pravaca zaštite. Sistematizacija napada obuhvata četiri osnovne kategorije [14], [15], [16]:

- napadi na DNS (*Domain Name System*) servere;
- „trovanje“ tabela rutiranja;
- pogrešna obrada IP paketa;
- odbijanje servisa DoS.

Na slici 2.6 je data je klasifikacija napada na infrastrukturu informacionog i komunikacionog sistema.

Napadi na DNS ukazuju na nedostatke autentifikacije i integriteta podataka u okviru DNS i protokola koji se koriste kod kontrole pristupa. Posledice ovih napada mogu biti DoS, „maskiranje“ zlonamernih korisnika, „curenje“ informacija i krađa domena. U cilju rešavanja DNS napada, međunarodna organizacija IETF uvela je proširenje DNS mehanizmima zaštite, poznato kao DNSSEC (*Domain Name System Security Extensions*).



Slika 2.6. Klasifikacija napada na infrastrukturu informacionog i komunikacionog sistema [14].

„Trovanje“ tabela rutiranja se vrši unošenjem lažnih informacija u kontrolne pakete koje razmenjuju ruteri, na osnovu kojih se obavlja ažuriranje tabela rutiranja. Posledice takvih napada mogu biti: rutiranje po putanjama koje nisu optimalne, kreiranje veštačkih particija koje su izolovane od ostatka mreže, formiranje petlji, DoS, zagušenje segmenta mreže koje se ne može otkloniti tradicionalnim mehanizmima kontrole zagušenja, otkrivanje sadržaja informacija i drugo. Mehanizmi zaštite od spoljnih napada, koji sprečavaju pristup mrežnim linkovima, su primena tehnika digitalnog potpisa i obeležavanje kontrolnih poruka rednim brojevima ili vremenskim pečatima. Zaštita od unutrašnjih napada na rutere u kojima je implementiran neki od LS (*Link*

State) protokola može se vršiti pomoću centralizovanog sistema za otkrivanje napadača ili zaštitnim mehanizmima predviđenim u protokolu. Za rutere u kojima je implementiran neki od DV (*Distance Vector*) protokola predloženi su različiti mehanizmi, među kojima je najpoznatija procedura za proveru konzistentnosti (CC – *Consistency Check*) [14].

Pogrešna obrada IP paketa prouzrokuje neadekvatno opsluživanje paketa u čvorovima mreže. Posledice ovih napada mogu biti zagušenje segmenta mreže, DoS i snižavanje korisnog protoka. Zaštita od napada na linkove u tradicionalnim IP mrežama obavlja se pomoću IPSec (*Internet Protocol Security*) standarda. Zaštita od replikacije paketa obavlja se numerisanjem paketa i implementacijom brojača paketa na predajnoj strani i mehanizma pomičnog prozora u prijemniku.

U DoS napadu vrši se ispravno rutiranje IP paketa, a napadač falsifikuje IP adresu izvora saobraćaja i koristi infrastrukturu mreže da uputi velike količine saobraćaja odredištu koje predstavlja metu. Efekat napada se uvećava ako se koriste distribuirani napadači (DDoS), koji istovremeno napadaju ciljni server, što može potpuno da spreči pristup jednom broju korisnika mreži. Moguće tehnike zaštite mogu se svrstati u preventivne i reaktivne. Preventivne tehnike zasnivaju se na filtriranju u cilju sprečavanja napada, kao na primer DPF (*Distributed Packet Filtering*). Cilj reaktivnih tehnika zaštite je da identifikuju napadača kada je napad već izvršen. Moguća rešenja obuhvataju testiranje linkova, IP *Traceback* i dr.

2.4. Pregled napada na SCADA sisteme

Pre nekoliko decenija, u vreme kada je započela primena industrijskih sistema za daljinsko upravljanje, nije bilo mnogo razloga za brigu o bezbednosti ovih sistema. Međutim, od momenta kada su ovi sistemi počeli da se povezuju sa Internetom ili lokalnom mrežom (LAN – *Local Area Network*), bilo je samo pitanje vremena kada će briga o njihovoj bezbednosti doći na dnevni red.

Primeri unutrašnjih napada na SCADA sisteme, obuhvataju zlonamernu modifikaciju programabilnih fajlova za RTU i PLC i instalaciju zlonamerne aplikacije, koja može da isključi aktivne alarme i izda lažne komande uređajima povezanim na *fieldbus* [16].

Direktni napadi na RTU i PLC opremu zahtevaju fizički pristup komunikacionim kanalima (mreži). Unutrašnji napadi se mogu pojaviti i kao posledica „trovanja“ operativnih sistema, npr. usled neovlašćene instalacije nelicenciranog softvera opšte namene na radnoj stanici sistema. Klasifikacija napada na SCADA sisteme prikazana je u tabeli 2.1.

Tabela 2.1. Napadi specifični za SCADA sisteme [17]

Tip napada	**Opis**
Replay	„Hvatanje“ pouke i prosleđivanje sa kašnjenjem jednom ili 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 cilju prikupljanja informacija o učestanosti i verovatnoći napada koriste se *honeypot* arhitekture. *Honeypot* je mrežni uređaj čija je jedina uloga da predstavlja žrtvu napada. To zapravo znači da je gotovo svaka interakcija s tim uređajem neautorizovana ili zlonamerna aktivnost. U studiji, čiji su rezultati objavljeni u [18], kompanija *Trend Micro* je postavila tri *honeypot* sistema, koji oponašaju SCADA uređaje sa ranjivostima koje se uobičajeno nalaze na sličnim sistemima. Jedan *honeypot* je simulirao sistem vodosnabdevanja sa povezanim pumpama i sistemima za prečišćavanje vode. Drugi je simulirao PLC za kontrolu sistema grejanja i ventilacije, a treći je simulirao SCADA server sa povezanim PLC i HMI. Zatim su ovi sistemi učinjeni dostupnim na Internetu preko obične *Google* pretrage, kao što je i inače slučaj sa mnogim od tih sistema. *Trend Micro*-ov *honeypot* se našao na meti i automatizovanih i ciljanih napada, a prvi takav napad zabeležen je već posle 18 sati. U toku eksperimenta koji je trajao 28 dana registrovano je 39 napada, od kojih je 12 bilo ciljanih, a 13 napada istraživači su okarakterisali kao ciljane i/ili automatizovane. Ovakva istraživanja, pokazuju da industrijski sistemi daljinskog upravljanja nisu bezbedni, a rezultati se mogu koristiti kao pomoć u proceni verovatnoće pretnji ovim sistemima. Sa druge strane, podaci o

učestanosti napada se ne mogu uzeti kao referentni, zbog njihove stohastike. U svakom slučaju, zaključak je da se verovatnoća uspešnih napada menja tokom vremena zavisno od evolucije metoda, povećanja znanja o kontroli i zaštitnih mehanizama.

Potencijalni napadači se mogu prepoznati, odnosno klasifikovati u različite grupe, pri čemu oni mogu imati širok spektar sposobnosti, resursa, organizacione podrške i motivacije. U tabeli 2.2 prikazana je klasifikacija potencijalnih napadača na industrijske sisteme daljinskog upravljanja, njihovih sposobnosti, resursa i motiva za iniciranje napada.

Tabela 2.2. Klasifikacija potencijalnih napadača: resursi i motivi [19]

Napadač	**Sposobnosti / resursi**	**Motivi za napad**
Hakeri	Hardverski resursi, slobodno vreme, predanost	Zabava, izazov, slava
Zaposleni	Poznavanje infrastrukture sistema, lak pristup sistemu	Nenamerno usled obavljanja posla bez poznavanja ranjivosti sistema, izazov, eksperimentisanje, nezadovoljstvo, profit
Insajderi, izvođači, konkurentska firma	Pristup sistemu, posedovanje poverljivih informacija, znanja o procesu i podrazumevanim lozinkama	Osveta, nezadovoljstvo, profit
Berzanski posrednici	Računarska znanja i veštine	Finansijska dobit
Strane vlade	Srtučnjaci, kriptografi, obaveštajne agencije, finansije, vojska, veliki računari	Nanošenje strateške, vojne i/ili ekonomske štete
Organizovani kriminal	Informaciona, komunikaciona, računarska znanja	Finansijska dobit
Ekstremističke grupe	Informaciona, komunikaciona, računarska znanja, posvećenost	Nanošenje štete suprotstavljenim grupacijama
Teroristi	Informaciona, komunikaciona, računarska znanja, mogućnost špijunaže, finansije, dobra organizovanost	Terorizam, ekonomska šteta
Udruživanje nekih od prethodnih grupa	Kombinovani izvori prethodno navedenih grupa	Zajednički interes u cilju postizanja sopstvenog interesa

U poslednjoj deceniji je zabeleženo više uspešnih napada na industrijske kontrolne sisteme u svetu [6], [8], [9], [20], [21]. U studiji [22] ukazano je na problem evidentiranja bezbednosnih incidenata u industrijskim sistemima daljinskog upravljanja.

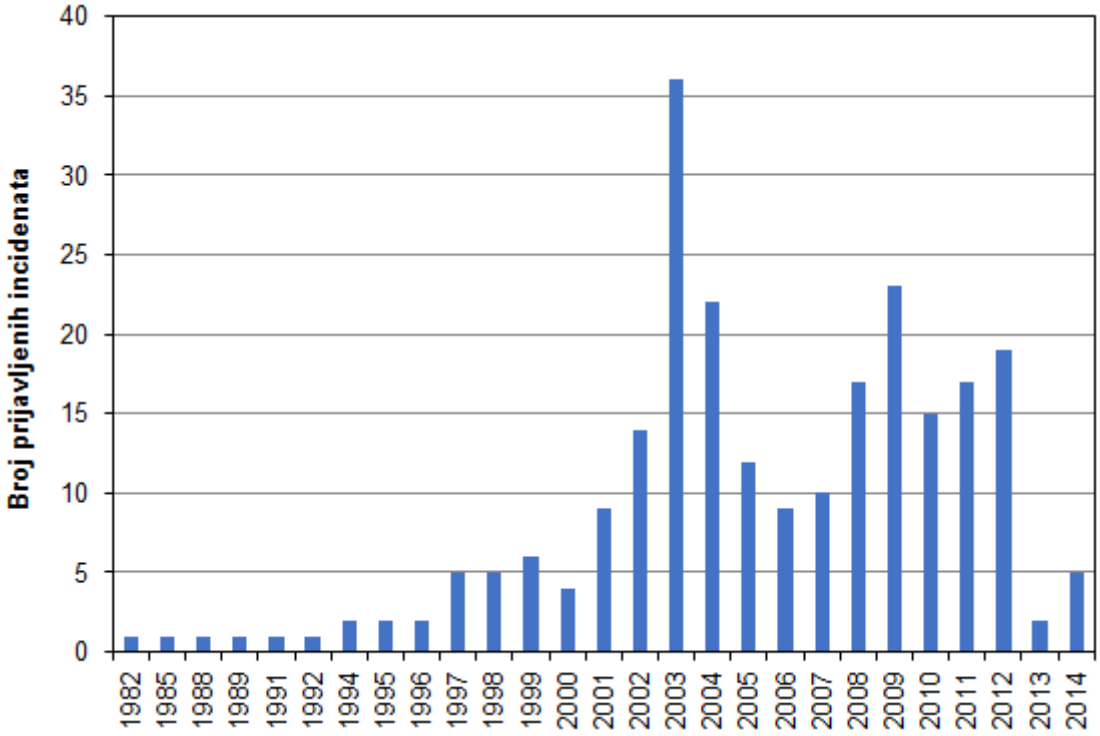
Razlozi za to mogu biti dvostruki: prvo, ukoliko napad na infrastrukturu nije identifikovan ili drugo, ukoliko podaci o napadu nisu objavljeni da se ne bi narušila reputacija kompanije. Istraživanja sprovedena u [22] o broju narušavanja bezbednosti informacione i komunikacione infrastrukture koje su učesnici studije registrovali u toku jedne godine ukazuje na tendenciju pada broja ispitanika koji nisu svesni napada (sa 28% u 2016. godini na 18% u 2017. godini).

Ukoliko je narušavanje bezbednosti prouzrokovalo posledice koje su se osetile van granica kompanije, tada nije moguće prikrivanje sajber napada. S obzirom da upravljanje bezbednosnim rizikom podrazumeva analizu rizika, u ovoj fazi su od velikog značaja iskustva koja dele kompanije koje su iskusile narušavanje bezbednosti informacione i komunikacione infrastrukture. To je bio jedan od motiva za formiranje RISI (*Repository of Industrial Security Incidents*), baze koja sadrži podatke o narušavanjima sajber bezbednosti u industrijskim sistemima daljinskog upravljanja [23]. U bazi su sadržani podaci o incidentima u periodu 1982 – 2014. godine i baza poseduje 242 zapisa. Na slici 2.7 grafički je prikazan broj incidenata po godinama i po grani industrije. Distribucija napada prema nameri, izvršiocu i metodu prikazana je na slici 2.8.

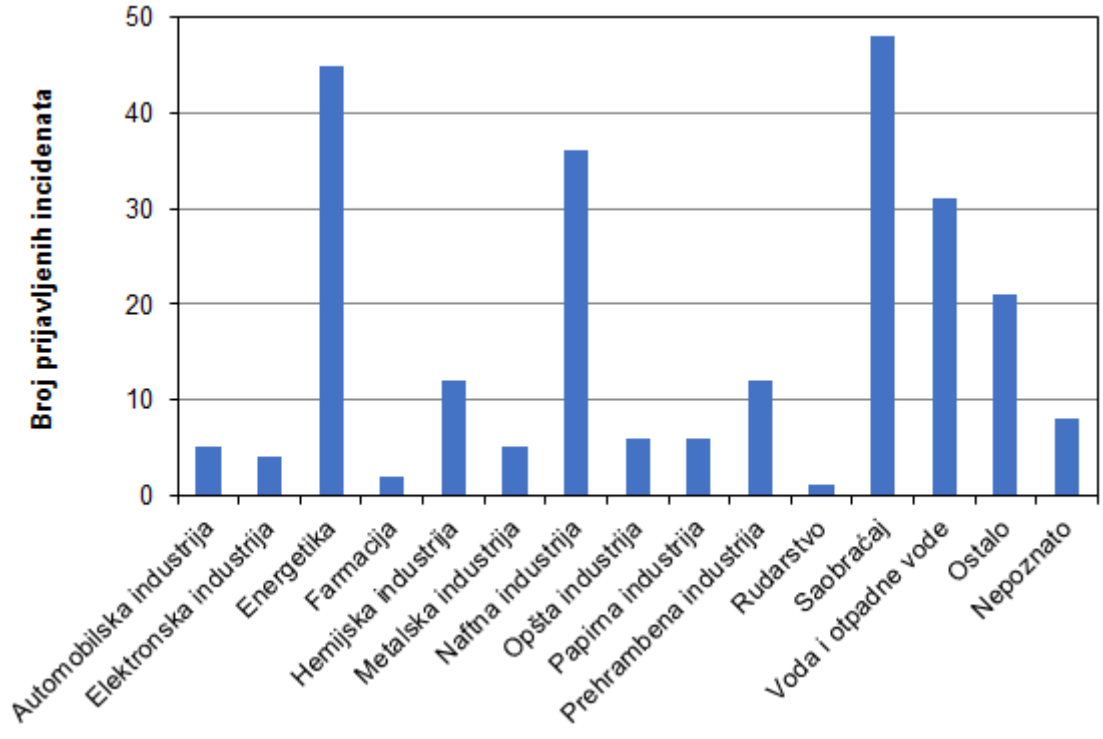
U nastavku su navedeni neki od mnogobrojnih napada na industrijske sisteme daljinskog upravljanja kroz godine, a njihova sistematizacija je prikazana u tabeli 2.3.

Prvi napad na kritičnu infrastrukukturu zabeležen je 1982. godine na Transsibirskom gasovodu. Usled napada na SCADA sistem koji je upravljao gasovodom pritisak u cevima je udvostručen što je dovelo do eksplozije koja je bila vidljiva iz svemira.

Otpušteni radnik kompanije koja se bavi prerađivanjem vode izveo je napad 2000. godine u Kvinslendu, u Australiji. On je iskoristio ukradene delove aparata za radio-signalizaciju u cilju neovlašćenog pristupa SCADA sistemu preko Interneta. Upućivanjem kompromitovanih komandi u sistem koji kontroliše kanalizacione pumpe, otpustio je milion litara otpadnih voda u reke i lokalne parkove. Motiv ovog napada bila je osveta.

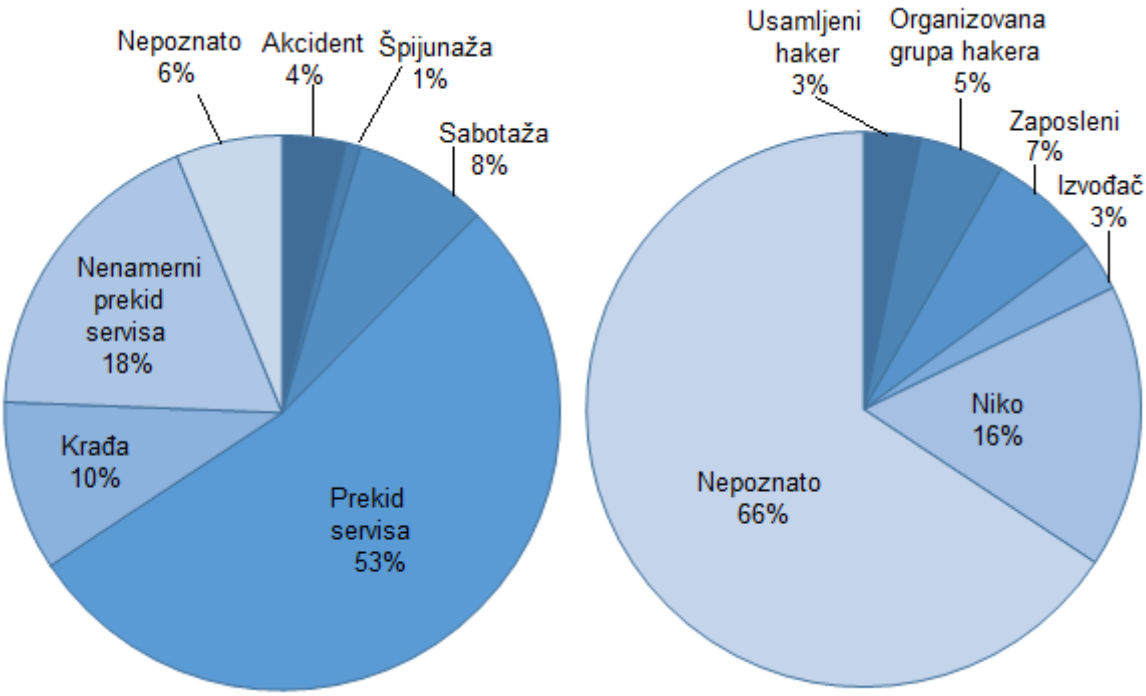


a)

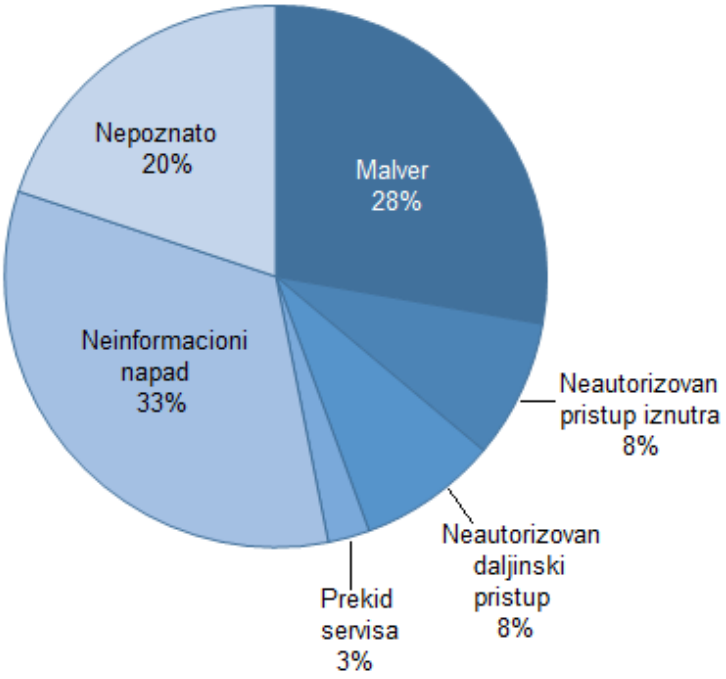


b)

Slika 2.7. Broj narušavanja sajber bezbednosti po a) godinama; b) grani industrije [24].



a) b)



c)

Slika 2.8. Distribucija napada prema a) nameri, b) izvršiocu i c) metodu [24].

Slammer „crv“ se 2003. godine raširio iz računara jednog zaposlenog u korporativnu mrežu, a odatle u procesnu mrežu nuklearne elektrane *Davis-Besse* što je prouzrokovalo pad sistema za prikaz parametara. Prošao je kroz nekoliko *firewall*-ova. Srećom, nuklearna elektrana u tom periodu nije bila u pogonu, tako da nije bilo ozbiljnih posledica.

Iste godine je došlo do zastoja u putničkom i teretnom železničkom saobraćaju na istočnoj obali SAD, uključujući i jutarnji poslovni voz u području Vašingtona. Usled zaraze *Sobig* virusom došlo je do otkaza telekomunikacione mreže i operativnih dispečerskih servisa i servisa za signalizaciju.

Još jedan napad u saobraćajnoj infrastrukturi dogodio se 2006. godine u Los Anđelesu kada su dva saobraćajna inženjera u znak protesta, za vreme štrajka, upala u sistem koji kontroliše semaforsku signalizaciju i reprogramirala sistem tako da su semafori na prometnim raskrsnicama imali crveni signal duže od uobičajenog vremena. Iako nije bilo saobraćajnih nesreća prouzrokovani su veliki zastoji u saobraćaju.

U analizi sajber incidenata na industrijske sisteme daljinskog upravljanja značajna je 2010. godina. Tada se dogodio prvi zabeležen napad „crvom“ *Stuxnet* koji je namenski kreiran za SCADA sisteme. „Crv“ se širio preko inficiranih USB memorijskih uređaja, a koristio je podrazumevane lozinke za pristup *Windows* operativnim sistemima koji pokreću WinCC i PCS7 softver za programiranje PLC uređaja proizvođača *Siemens*. Napad je izveden na iransko nuklearno postrojenje za obogaćivanje uranijuma. Brzina centrifuga se naglo menjala, bez objave kvara. Sistem je bio van funkcije sedam dana.

Sledeći maliciozni softver koji je namenski kreiran za SCADA sisteme je malver *Havex* grupe *Dragonfly*. Malver je tipa RAT (*Remote Access Tool*) koji omogućuje napadačima daljinski pristup i kontrolu nad zaraženim računarima. Ova grupa, koja je aktivna od 2011. godine, odgovorna je za sajber špijunažu kompanija iz energetskog sektora koje se nalaze u SAD i zapadnoj Evropi. Prilikom napada korišćen je *Watering Hole Attack* koji je karakterističan po tome da napadač zarazi veb sajt koji žrtva napada najčešće posećuje. Ova grupa je kompromitovala veb sajtove koji su povezani sa energetikom. Napadi su otkriveni u junu 2014. godine.

Tabela 2.3. Pregled sajber napada na infrastukturu industrijskih sistema daljinskog upravljanja

Godina	Država	Meta napada	Metod napada	Izvšilac
1982.	SSSR	Transsibirski gasovod	Trojanac	Sabotaža
2000.	Australija	Sistem za preradu otpadnih voda	Neovlašćeni pristup	Nezadovoljni bivši zaposlen
2003.	SAD	*Davis-Besse* nuklearna elektrana	„Crv“ *Slammer*	Nenamerni incident
2003.	SAD	Železnica Vašington	Virus *Sobig*	Nenamerni incident
2006.	SAD	Semaforska signalizacija u Los Anđelesu	Neovlašćeni pristup	Protest zaposlenih
2010.	Iran	Nuklearno postrojenje	„Crv“ *Stuxnet*	Sabotaža
2014.	SAD i zapadna Evropa	Energetski sistemi	RAT malver	Industrijska špijunaža

Prekid usluga je cilj više od polovine svih sajber napada na kritičnu infrastrukturu i industrijske sisteme daljinskog upravljanja (slika 2.8 a).

Napadači mogu primeniti različite metode kao što je malver (npr. „crvi“, trojanci, virusi), neautorizovani pristup i DoS da bi izazvali prekid usluge. Elektromagnetske smetnje su jedan od načina prekida usluga u sistemima kritične infrastrukture. Mnogi napadi na industrijske sisteme daljinskog upravljanja započinju tako što napadač prvo obezbeđuje pristup korporativnoj mreži, pre upada u mrežu SCADA sistema. Neovlašćeni pristup se može realizovati kao neautorizovani daljinski pristup ili neautorizovani pristup iznutra (zaposleni, dobavljači i izvođači). Rezultati (slika 2.8 c) su pokazali da je broj udaljenih pristupa (8,68%) i pristupa iznutra (8,26%) približno jednak. Adekvatne bezbednosne politike i kontrolne mere moraju biti uspostavljene kako bi se sprečio neovlašćeni pristup računarskim resursima iznutra. Na istoj slici je prikazano da za 20% bezbednosnih incidenata metod nije poznat. Ovo je značajno, jer se bez dobrog poznavanja metoda koje primenjuju napadači, smanjuje mogućnost za impelementaciju odgovarajućih mehanizama zaštite.

Napad na infrastrukturu industrijskog sistema daljinskog upravljanja može nastati iz više izvora što otežava donošenje odluke o primeni mehanizama zaštite. Približno 5% bezbednosnih incidenata u industrijskim sistemima daljinskog upravljanja je rezultat aktivnosti organizovanih hakerskih grupa (slika 2.8 b). Na istoj slici se vidi da je oko

66% bezbednosnih incidenata u industrijskim sistemima daljinskog upravljanja posledica nepoznatih počinilaca, dok za 16% incidenata koji su registrovani u ovoj bazi nema počinioca. Sigurnosni incidenti koji nisu posledica ljudske aktivnosti su najčešće posledica narušavanja bezbednosti koja nije sajber napad, i njihov broj čini približno 33% bezbednosnih incidenata u industrijskim sistemima daljinskog upravljanja.

Tipični primeri faktora incidenata koji nisu posledica namerne ljudske aktivnosti uključuju udare groma, neadekvatnu primenu bezbednosne politike (npr. instaliranje nekompatibilnog antivirusnog softvera i softverskih dodataka – *patches* u SCADA sistemima, neželjene posledice testiranja sajber napada i slično), nekorektna mrežna konfiguracija, neadekvatno održavanje hardvera i softvera SCADA sistema, nedovoljna obučenost zaposlenih, i slično. Ovakvi incidenti nisu relevantni za razmatranje u ovoj disertaciji. Ovi faktori su neki od razloga za veliki broj nenamenskog prekida servisa (18%) kao što je prikazano na slici 2.8 a.

Uobičajene ranjivosti koje su iskorišćene u mnogim prijavljenim sajber incidentima su: neinstalirani ili zastareli antivirusni programi, neadekvatna *firewall* zaštita, korišćenje slabe ili podrazumevane lozinke, neadekvatne bezbednosne politike, loše upravljanje *backdoor*-ima, ranjivosti SCADA proizvoda, zaposleni (npr. upotreba socijalnog inženjeringa kao i unošenje malvera povezivanjem prenosnih računara i USB memorija), loše osigurani VPN (*Virtual Private Network*) pristup i druge poznate ranjivosti koje su često povezane sa veb uslugama i *Windows* operativnim sistemima.

2.5. IDPS tehnologije u industrijskim sistemima daljinskog upravljanja

Posebna pažnja u istraživanju je usmerena na infrastrukturne napade i preporučen mehanizam zaštite implementacijom sistema za detekciju napada (IDS – *Intrusion Detecion System*) i sistema za prevenciju napada (IPS – *Intrusion Prevention System*). Ovi sistemi imaju mnogo zajedničkih svojstava, a administratori najčešće mogu da blokiraju preventivna svojstva IPS proizvoda, čime se njihova funkcionalnost svodi na IDS. Zbog toga se u literaturi obično sreće zajednički naziv – sistemi za detekciju i prevenciju napada (IDPS).

IDPS tehnologije razlikuju se prvenstveno po tipu događaja koje prepoznaju i po metodologiji koju koriste za identifikaciju incidenata [15], [25]. Osim nadzora i analize događaja, IDPS tipično obuhvata i snimanje informacija o događajima, obaveštavanje administratora o važnim događajima putem upozorenja (alarma) i generisanje izveštaja.

Klasifikacija po tipu događaja obuhvata sledeće četiri grupe:

- mrežni IDPS – nadgleda saobraćaj u pojedinim segmentima mreže i analizira aktivnosti mrežnih i aplikacionih protokola u cilju identifikacije sumnjivih aktivnosti (slika 2.9);
- IDPS u hostu – nadgleda karakteristike jednog hosta i događaja u njemu u cilju detekcije incidenata (slika 2.10);
- bežični IDPS – nadgleda saobraćaj u bežičnoj mreži i analizira odgovarajuće MAC (*Medium Access Control*) protokole (slika 2.11);
- IDPS za analizu ponašanja mreže (NBA – *Network Behavior Analysis*) – analizira mrežni saobraćaj sa ciljem identifikacije pretnji koje generišu neuobičajeni saobraćajni tokovi, kao što su DDoS napadi, neke forme malicioznog softvera ili narušavanje bezbednosnih politika (slika 2.12).

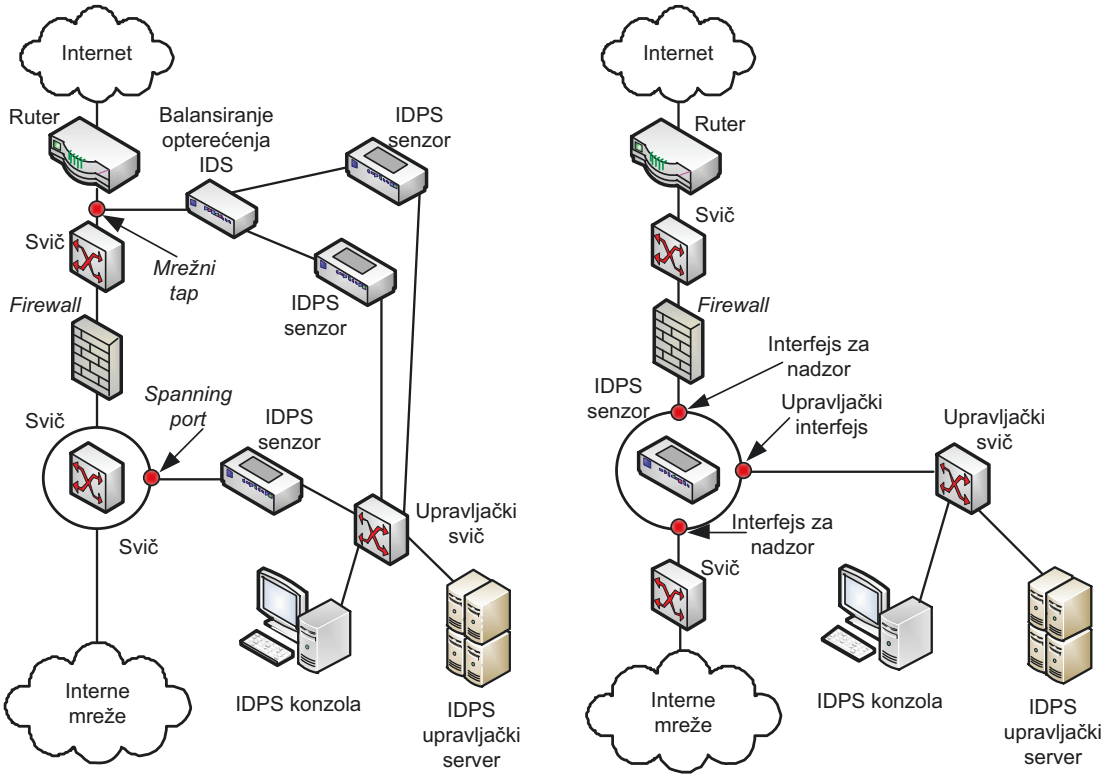
Metodologije za detekciju incidenata mogu biti:

- zasnovane na detekciji potpisa (*signature-based*);
- zasnovane na detekciji anomalija (*anomaly-based*);
- zasnovane na specifikaciji protokola (*specification-based*)[1].

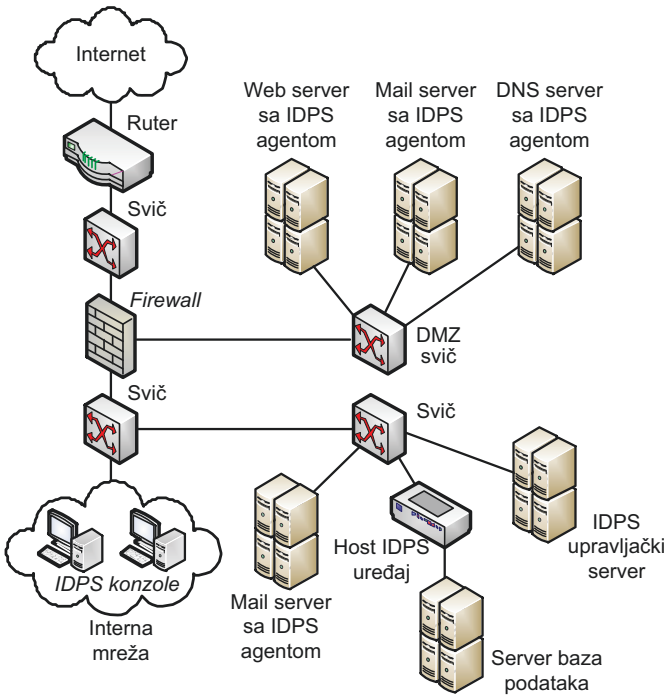
Najveći broj IDPS tehnologija koristi više metodologija detekcije, zasebnih ili integrisanih, u cilju što tačnije detekcije širokog spektra napada.

Metodi zasnovani na detekciji potpisa porede nadgledane događaje sa potpisima (uzorcima koji odgovaraju poznatoj pretnji) u cilju identifikacije mogućih incidenata. Ovi metodi su vrlo efikasni u detekciji poznatih pretnji, ali i potpuno neefikasni u uslovima novih ili nepoznatih pretnji, kao i modifikovanih napada.

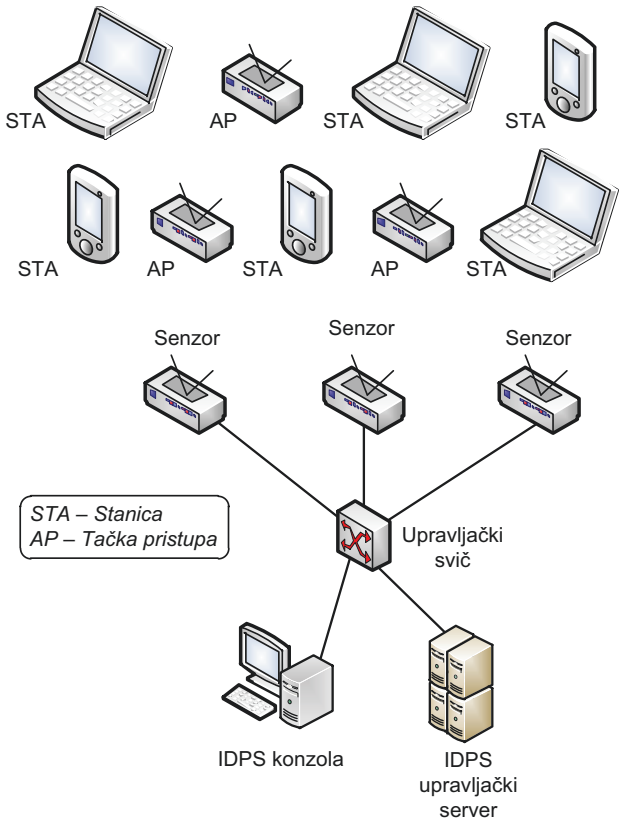
[1] poznati i pod nazivom *stateful protocol analysis* (analiza stanja protokola)



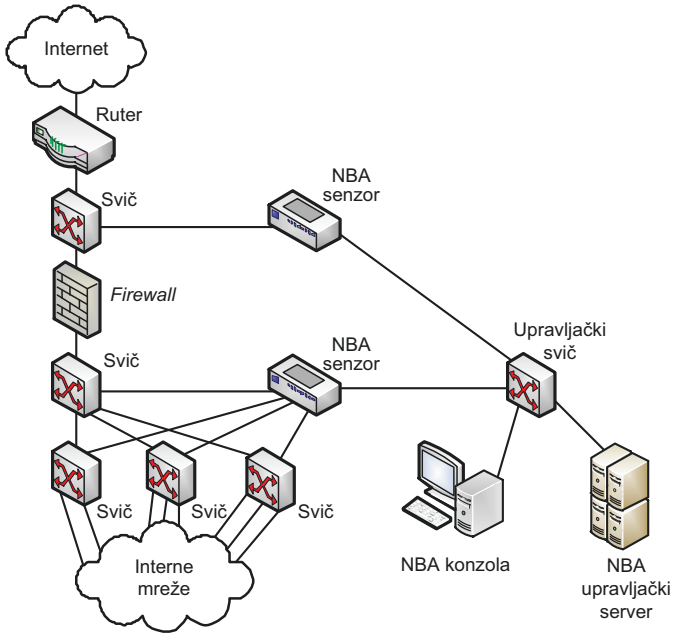
Slika 2.9. Arhitektura mrežnog IDPS a) pasivni, b) *inline* [25].



Slika 2.10. Arhitektura IDPS u hostu [25].



Slika 2.11. Arhitektura bežičnog IDPS [25].



Slika 2.12. Arhitektura IDPS za analizu ponašanja mreže [25].

Metodi zasnovani na detekciji anomalija zasnivaju se na upoređivanju nadgledanih događaja sa listom aktivnosti koje su unapred definisane kao normalne, u cilju identifikacije značajnijih odstupanja. IDPS ima statičke ili dinamičke profile koji reprezentuju normalno ponašanje korisnika, hostova, mrežnih konekcija, ili aplikacija. Inicijalni profil generiše se tokom perioda treninga, koji obično traje nekoliko dana ili nedelja. Razvijen je veliki broj metoda za detekciju anomalija, koji mogu biti: statistički, zasnovani na *data mining*-u, zasnovani na znanju i zasnovani na mašinskom učenju [26]. Glavna prednost metoda zasnovanih na detekciji anomalija je visoki stepen efikasnosti detekcije nepoznatih pretnji. Međutim, pogrešno uključivanje malicioznih aktivnosti u profile je tipičan problem ovih metoda. Drugi problem pri generisanju profila je pitanje tačnosti, a posledica je kompleksnih aktivnosti u mreži.

Metodi zasnovani na specifikaciji protokola upoređuju nadgledane događaje sa unapred određenim profilima, generisanim na osnovu definicija aktivnosti protokola za svako stanje protokol-automata. Drugim rečima, oni koriste univerzalne profile koje definišu organizacije za standarde i/ili proizvođači softvera. Ovi metodi mogu da identifikuju neregularne nizove poruka, kao što je ponavljanje iste komande, ili zadavanje komande kojoj nije prethodila komanda predviđena specifikacijom protokola. Njihov glavni nedostatak je intenzivno korišćenje procesorskih i memorijskih resursa zbog snimanja stanja velikog broja istovremenih sesija i složene analize tih stanja.

IDPS tehnologije ne obezbeđuju potpuno tačnu detekciju napada. Stepen tačnosti sistema opisuje se pomoću više parametara:

- broj malicioznih aktivnosti koje je IDS uspešno detektovao TP (*True Positive*);
- broj normalnih aktivnosti koje je IDS uspešno obeležio kao nemaliciozne TN (*True Negative*);
- broj malicioznih aktivnosti koje nisu detektovane, već su smatrane normalnim FN (*False Negative*);
- broj normalnih aktivnosti koje su detektovane kao maliciozne FP (*False Positive*) ili FA (*False Alarm*).

Na osnovu navedenih parametara izvedene su različite mere za evaluaciju ovih sistema [27], [28]. IDS sistem je utoliko tačniji ukoliko su vrednosti FP i FN manje (u idealnom sistemu je FP=0 i FN=0). U većini IDPS sistema, redukcija FN povećava FP i obrnuto.

Često se usvaja bezbednosna politika kojom se smanjuje FN, na račun potencijalnog povećanja FP. To znači da će biti detektovan veći broj malicioznih događaja, ali i da su potrebni dodatni analitički resursi da se izvrši diferencijacija FP od malicioznih događaja. Podešavanje tačnosti IDPS sistema vrši se promenljivim konfiguracionim parametrima.

Prevencija napada je odziv na detektovane pretnje pokušajem da se spreči njihova relizacija. Postoji nekoliko tehnika odziva:

- IDPS zaustavlja napad raskidom mrežne konekcije ili korisničke sesije koja se koristi za napad, blokiranjem pristupa meti napada sa naloga ili IP adrese koja pripada napadaču, ili blokiranjem svih pristupa meti napada;
- IDPS teži da poremeti napad promenom konfiguracije, promenom kontrolnih parametara ili generisanjem dodataka za softver uređaja;
- IDPS menja sadržaj napada, uklanjanjem ili zamenom malicioznih delova.

Prikaz karakterističnih arhitektura IDPS projektovanih za mreže industrijskih sistema daljinskog upravljanja može se pronaći u literaturi [29].

2.5.1. Specifičnosti industrijskih sistemima daljinskog upravljanja relevantne za IDPS

Vremenska kritičnost industrijskih sistema daljinskog upravljanja je posledica zahteva da se pravovremeno reaguje na određene događaje i paralelnog izvršavanja različitih funkcija, jer se radi o distribuiranim sistemima sa geografski dislociranim komponentama u kojima se paralelno odvija veći broj procesa u realnom vremenu.

Specifični sistemi za detekciju i prevenciju napada na industrijske sisteme daljinskog upravljanja razmatrani su u radovima [30] i [31]. Za ove sisteme ne postoje posebno razvijene mere za evaluaciju, već se koriste opšte tehnike koje su razvijene za IDS u poslovnim sistemima.

Problem bezbednosti kontinualnog sistema koji radi u realnom vremenu zahteva sveobuhvatno razmatranje i holističko razumevanje bezbednosti mreže, teorije upravljanja i fizičkih sistema [32], [33]. Konačni cilj je da se ostvare zahtevane performanse u realnom vremenu tokom 7 dana / 24 časa, u realističnom okruženju u

kome regularno ponašanje koegzistira sa otkazima sistema, uslovima okruženja, ljudskim greškama, ali i sajber napadima.

Aspekti relevantni za projektovanje IDPS su: vreme odziva sistema, pravovremena isporuka svih bitnih podataka i ažurnost podataka (podaci su validni samo u određenom intervalu vremena). Važan je i redosled ažuriranja podataka sa senzora, posebno ako oni vrše nadzor istog procesa ili korelisanih procesa. Redosled dolaska podataka u centar upravljanja ima značajnu ulogu u prezentaciji dinamike procesa i utiče na donošenje ispravnih odluka, bilo da se radi o algoritmu upravljanja (softveru) ili o operateru koji nadgleda industrijski proces. Dodatnu složenost u pogledu vremenskih resursa predstavlja i činjenica da neki od industrijskih procesa jednog te istog sistema mogu biti definisani sa velikim brojem parametara koji se brzo menjaju u vremenu, a koji mogu generisati iste alarme.

Saobraćaj u mrežama SCADA sistema karakteriše se pravilnim uzorcima i relativno ograničenim skupom protokola. Ta svojstva su inherentno pogodna za razvoj i primenu tehnika zasnovanih na detekciji anomalija. U nastavku su navedena osnovna svojstva saobraćaja u mrežama SCADA sistema:

- **Koristan protok.** Stabilnost protoka je karakteristična za mreže SCADA sistema. Promene protoka mogu da budu indikacija događaja koji zahtevaju visok intenzitet saobraćaja (skeniranje, DoS napad, otkazi/greške u radu industrijskog procesa).
- **IP adrese i brojevi portova.** U mrežama SCADA sistema koje koriste statičko dodeljivanje adresa, očekuje se da soketi (parovi „IP adresa:Port“) budu konstantni. Pojava novog soketa ukazuje na aktiviranje novog servisa, ali i na potencijalni napad.
- **Prosečna dužina paketa.** Većina sistema na nivou *fieldbus*-a generiše pakete poznate dužine, sa jasnom statistikom prosečne dužine. Zbog toga, prosečna dužina paketa predstavlja dobar pokazatelj normalnog ponašanja ili anomalije.
- **Merenje vremena.** Vreme prenosa i intervali međudolazaka paketa iz svih mrežnih čvorova su sadržajni podaci za detekciju napada u mrežama SCADA sistema. To proističe iz strogih zahteva za rad u realnom vremenu, posebno na nivou *fieldbus*-a. Vremenske karakteristike saobraćaja i pridružena statistika

pokazuju pravilnosti i ujedno se razlikuju od saobraćaja tipičnih aplikacija u korporativnim mrežama i mrežama provajdera.

- **Smer toka podataka.** Smer toka podataka pokazuje koji sistem inicira konekciju. U tipičnoj operaciji, poznato je koji sistem inicira uspostavu veze. Kada se veza uspostavi, količina podataka koju jedan sistem šalje drugom je predvidljiva, sa velikom verovatnoćom, posebno kada je u pitanju poznat servis. Odstupanje od takvog ponašanja obično ukazuje na anomaliju.
- **Trajanje konekcije.** Trajanje konekcije je tipično za TCP protokol. S obzirom na ograničen broj servisa u mreži SCADA sistema, trajanje konekcija ima veoma malu varijansu.
- **Format i sadržaj korisnog segmenta.** Korisni segmenti (*payloads*) paketa koji potiču od SCADA aplikacija su najčešće precizno definisani. Promene formata korisnog segmenta ukazuju na moguće anomalije u ponašanju sistema. Isto tako, uočene anomalije u sadržaju korisnog segmenta mogu da budu indikatori za detekciju pogrešne konfiguracije sistema ili malicioznih aktivnosti.
- **Preslikavanje MAC adresa u IP adrese.** Preslikavanje MAC adresa u IP adrese vrši se u svakom LAN-u u cilju detekcije promena hardverskih komponenata. Pojava nove MAC adrese ukazuje na instalaciju novog hardvera u mreži. S obzirom da se i MAC adrese mogu falsifikovati, korisne su za detekciju lažnog predstavljanja. One takođe pomažu administratoru da vodi evidenciju o legitimnom hardveru u sistemu.
- **Tipovi i konfiguracija protokola.** Protokoli koji se koriste u mreži SCADA sistema su precizno definisani i ograničeni. Prisustvo novih protokola u saobraćaju ukazuje na ozbiljne promene u mreži. Konfiguracija protokola je najčešće statička, a bira se tako da garantuje najbolje performanse mreže. Nadzor konfiguracionih parametara protokola omogućuje da se detektuju loše konfigurisani servisi i maliciozne aktivnosti.
- **Konektivnost.** Broj konekcija u mreži SCADA sistema je uglavnom permanentan, a konektivnost pojedinih čvorova zavisi od njihove uloge u mreži. Varijacije konektivnosti čvorova, srednje vrednosti konektivnosti (na nivou mreže) i raspodele konektivnosti mogu da budu indikatori malicioznih aktivnosti.

3. PREGLED LITERATURE I ANALIZA AKTUELNIH PROBLEMA ISTRAŽIVANJA

Najvažniji deo procesa upravljanja rizikom je procena rizika, a to je ujedno i oblast upravljanja rizikom koja je najpodložnija greškama. U literaturi se mogu naći različiti pristupi, metodi i alati za procenu bezbednosnog rizika, koji se mogu klasifikovati u kvalitativne i kvantitativne [34], [35]. Kvalitativna procena pretpostavlja metode koje izražavaju gubitke kao subjektivnu meru, npr. stepen rizika procenjuje se kao nizak, srednji ili visok. Metodi iz ove grupe su jednostavni, nije neophodno da se odrede vrednosti troškova, kao ni učestanost potencijalnih pretnji, ali zato ne pružaju mogućnost *cost/benefit* analize. S obzirom da se kvalitativna procena rizika izrazito oslanja na subjektivnu procenu, podložna je greškama. Kvantitativna procena zasniva se na matematičkom pristupu (numerička analiza, statističke metode) pomoću koga se rizik izražava numeričkim vrednostima određenih veličina. Za primenu ovih metoda neophodno je prikupljanje velikog broja informacija, a proračuni su složeni. Zbog toga se kod procene rizika u informacionim sistemima preporučuje kombinacija kvalitativnog i kvantitativnog pristupa. Komparativna analiza različitih pristupa procene rizika se može naći u [35].

Upravljanje rizikom podrazumeva i donošenje odluke kako postupiti sa rizikom. U cilju olakšanja donošenja odluke o isplativosti investicije u smanjenje bezbednosnog rizika koncept povrata od investicije (ROI – *Return on Investment*) se primenjuje na investicije u mehanizme zaštite informacionog i komunikacionog sistema proračunom povrata od investicije u sajber bezbednost (ROSI – *Return on Security Investment*) [36], [37].

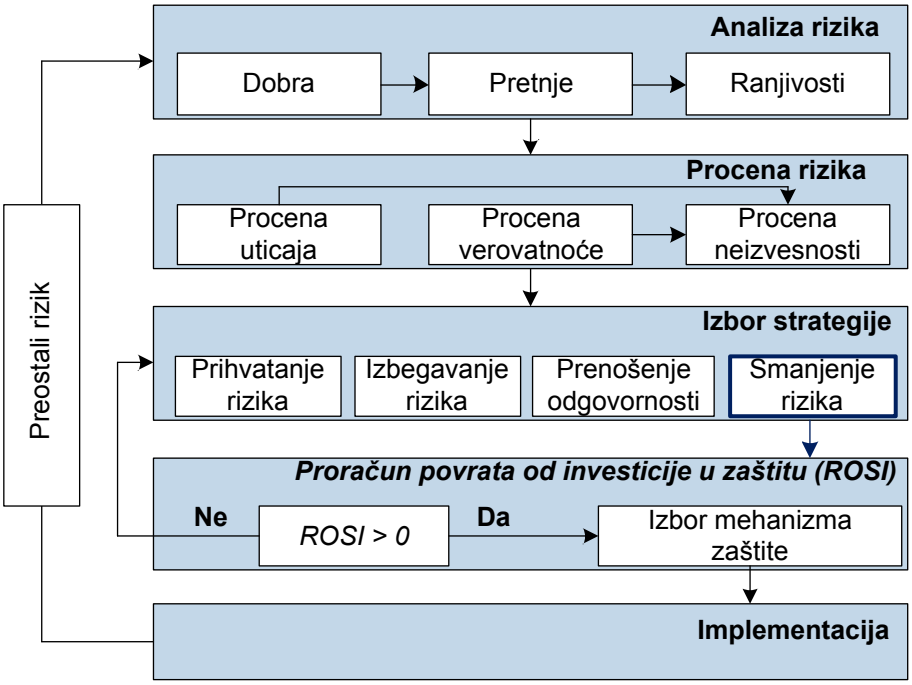
U ovom poglavlju prikazan je proces upravljanja bezbednosnim rizikom i postupak procene rizika. U nastavku poglavlja prikazani su standardi i preporuke za upravljanje bezbednosnim rizikom, a zatim je dat pregled opštih metoda procene bezbednosnog rizika i analiza njihove primenljivosti u SCADA sistemima. Na kraju je dat pregled i uporedna analiza metoda namenjenih za procenu bezbednosnog rizika SCADA sistema.

3.1. Proces upravljanja bezbednosnim rizikom

Rizik je funkcija verovatnoće da određeni izvor pretnje iskoristi potencijalne ranjivosti sistema, što rezultuje određenim štetnim i neželjenim uticajem na poslovanje. Upravljanje rizikom je kontinualan proces i svi koraci se ciklično ponavljaju (slika 3.1) kako zbog preostalog rizika tako i zbog stalnog unapređenja i proširenja sistema, ali i zbog potencijalne pojave novih ranjivosti i pretnji.

Proces upravljanja bezbednosnim rizikom počinje identifikacijom sistema i komponenti sistema i određivanjem bezbednosnih ciljeva, a obuhvata više koraka:

- analiza rizika kroz identifikaciju dobara, ranjivosti i pretnji;
- procena rizika;
- donošenje odluke o postupanju sa rizikom i o nivou prihvatljivog rizika;
- izbor korektivne mere i *cost/benefit* analiza proračunom *ROSI*;
- implementacija mera za snižavanje nivoa rizika.



Slika 3.1. Proces upravljanja bezbednosnim rizikom.

Analiza i procena rizika treba da obezbede informacije koje su ključne za proces upravljanja rizikom. Na osnovu ovih informacija se donose odluke o postupanju sa

rizikom, i kasnije se na osnovu te odluke bira strategija i mehanizmi koje tu odluku podržavaju.

Prema [38] proces procene rizika je skup logičkih, sistemskih i dobro definisanih aktivnosti koje obezbeđuju identifikaciju, kvantifikaciju i meru rizika i na kraju procenu koliko je rizik povezan sa određenim prirodnim fenomenom ili aktivnostima ljudi (namernim ili nenamernim). Procena rizika se može izvoditi kao inicijalna ili ponovljena. Inicijalna procena rizika je osnovna procena kada se identifikuju pretnje, ranjivosti i uticaji na operativnost i dobra, ljudstvo, druge organizacije i društvenu zajednicu u celini. Tada se identifikuju faktori rizika koje treba pratiti tokom vremena u procesu upravljanja rizikim. Ova ponovljena procena rizika treba da odgovori na pitanje kakve uticaje na procenu rizika imaju novootkrivene ranjivosti sistema, uspostavljanje novih konekcija, angažovanje spoljnih saradnika, izvođača i konsultanata, usvajanje nove tehnologije, promena u hardveru, softveru, promene u kontrolnim merama, procesu ili infrastrukturi. Razlozi za ponavljanje procene rizika mogu biti i registrovani incidenti u sistemu.

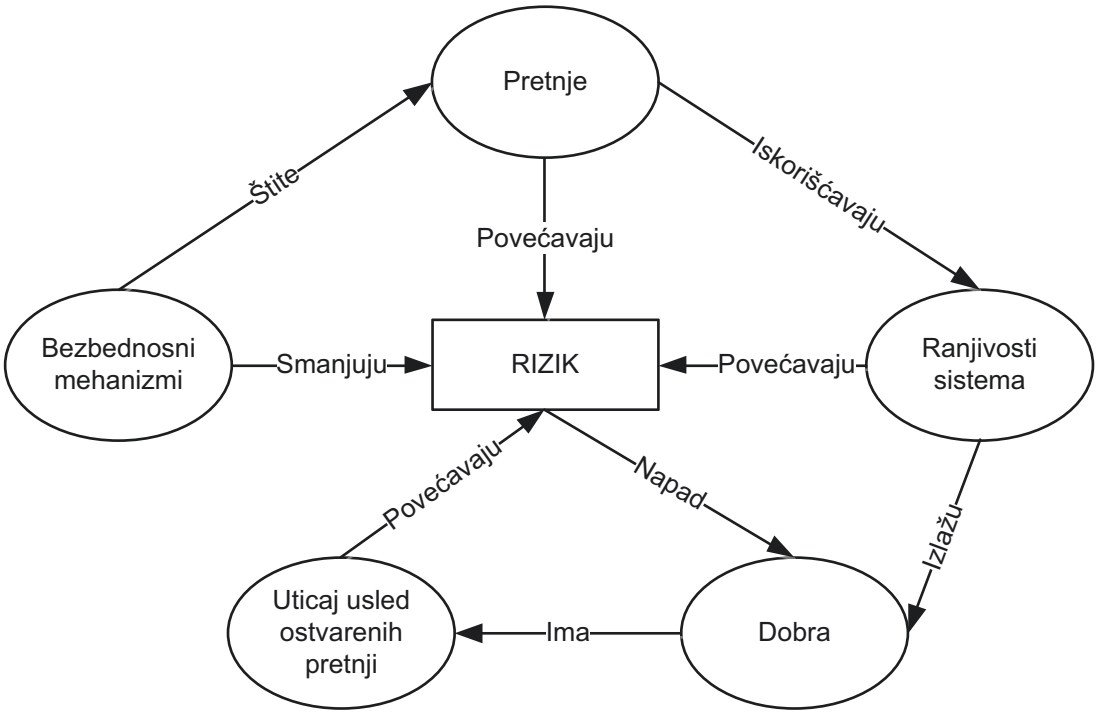
Pre početka analize i procene rizika potrebno je utvrditi granice informacionog sistema i infrastukture u okviru kojih se vrši procena. Time se definiše i raspoloživost podataka koji učestvuju u proceni kao i vremenski okvir validnosti informacija. Na osnovu ovih podataka se određuje i validnost rezultata procene rizika.

Proces procene rizika ima dve vrste ograničenja. Prvu najčešće postavlja poslovodstvo u smislu ograničenih finansijskih sredstava za sprovođenje procene i ograničenih ljudskih resursa. Drugu vrstu ograničenja diktira raspoloživost informacija koji su ulazni parametri procesa procene bezbednosnog rizika.

Polazne pretpostavke procene bezbednosnog rizika se najčešće odnose na izvore pretnji, vrste pretnji, mogući uticaj realizacije pretnje i ranjivosti sistema. Od ovih pretpostavki potiče neizvesnost koja se javlja i u konačnoj proceni rizika, a u velikoj meri utiče na kvalitet procene i toleranciju rizika. Izlazna veličina procesa procene rizika je nivo rizika, a tokom procesa upravljanja rizikom potrebno je da se definiše nivo prihvatljivog rizika.

Informacije potrebne za analizu rizika raspoložive su u dokumentaciji tehničko-informacionog sistema, planu poslovnog kontinuiteta, izveštajima procena rizika relevantnih organizacija i infrastruktura. U obzir se uzimaju sve komponente sistema u prethodno definisanim granicama. Važno je da se uzmu u obzir primenjene tehnologije, veze i zavisnosti od drugih sistema i da li postoji zajednička infrastruktura sa drugim sistemima. Informacije o pretnjama i ranjivostima sistema su dostupne iz internih dokumenata (izveštaji o incidentima, otkazima, propustima), ali su raspoloživi i eksterni izvori u bazama podataka, izveštajima i studijama [39].

Analizi rizika se može pristupiti sa aspekta pretnje, ranjivosti sistema ili uticaja realizovane pretnje na sistem. U zavisnosti od izabranog pristupa izrađuje se model rizika. Za sprovođenje analize rizika važno je da se identifikuju, definišu i procene: (1) dobra; (2) ranjivisti sistema; (3) pretnje; (4) uticaji usled ostvarenih pretnji i (5) mehanizmi zaštite. Elementi modela rizika grafički su prikazani na slici 3.2.



Slika 3.2. Elementi modela rizika.

Za analizu pretnji potrebna je identifikacija izvora pretnji. U širem smislu tu se ubrajaju zlonamerni korisnici, zaposleni koji slučajnom greškom u izvršenju radnih aktivnosti izazovu incident, infrastrukturni izvori u vidu implementiranog hardvera za procesnu i

komunikacionu podršku, stanje okoline, elementarne nepogode i slično. U ovoj disertaciji je pažnja usmerena na infrastrukturne napade i izvori pretnji se nalaze među zlonamernim korisnicima koji su detaljno klasifikovani u tabeli 2.2. U ovom slučaju pretnje su posledice njihovih aktivnosti, a neke od njih su nabrojane u tabeli 2.1. Ranjivosti sistema se mogu identifikovati u arhitekturi sistema, korišćenim komunikacionim protokolima, mobilnim korisnicima, udaljenom pristupu, standardnim komponentama i drugo. U postupku analize rizika potrebno je da se za konkretan slučaj identifikuju izvori pretnji, pretnje i ranjivosti sistema. U obzir treba da se uzmu i implementirani mehanizmi zaštite. Specifičnosti zaštite informacione i komunikacione infrastrukture industrijskih sistema daljinskog upravljanja moraju se uzeti u obzir pri analizi bezbednosnog rizika [40], [41].

Prema [39] procena bezbednosnog rizika SCADA sistema obuhvata sledeće korake:

- karakterizacija sistema kroz identifikaciju dobara i određivanje granica sistema;
- identifikacija pretnji i ranjivosti na pretnje;
- analiza postojećih i planiranih kontrolnih aktivnosti;
- određivanje verovatnoće da bi ranjivost SCADA sistema mogla biti zloupotrebljena;
- analiza uticaja uspešne pretnje;
- određivanje nivoa rizika;
- preporuke za ublažavanje rizika;
- rezultujuća dokumentacija.

Procena bezbednosnog rizika vrši se pri projektovanju zaštite informacione i komunikacione infrastrukture sistema daljinskog upravljanja, a zatim periodično ponavlja (delimično ili u celini) tokom eksploatacije i nadgradnje sistema. Postavlja se pitanje tačnosti ponovljenih procena u uslovima dinamičnog razvoja informacionog i komunikacionog sistema. U radu [42] je razmatran metod inkrementalne procene rizika, zasnovane na formalnim definicijama različitih profila rizika. Proračun profila rizika vrši se distribuirano i nezavisno u različitim komponentama sistema.

Proces upavljanja bezbednosnim rizikom podrazumeva donošenje odluke o postupanju sa rizikom. Veliki uticaj na donošenje odluke ima rezultat prethodne faze upravljanja rizikom - procena rizika. Izbor pri donošenju odluke u strategiji je:

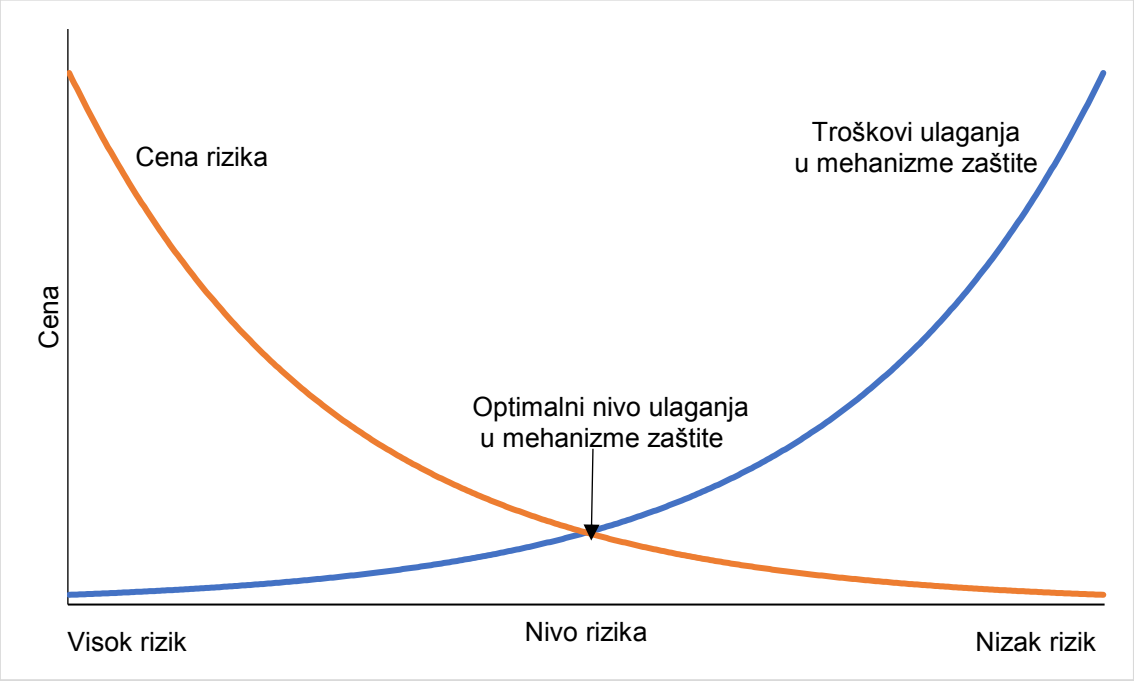
- prihvatanje rizika;
- izbegavanje rizika;
- prenošenje odgovornosti;
- smanjenje rizika.

Prihvatanje rizika predstavlja svesno prihvatanje posledica koje izaziva rizik nakon uspešne realizacije pretnje. **Izbegavanje rizika** predstavlja eliminaciju potencijalne pretnje otklanjanjem njenog uzroka. **Prenošenje odgovornosti** je transfer posledica rizika na neko treće lice, na primer osiguravajuće društvo osiguravanjem dobara, poslovanja i finansijsko obezbeđenje u slučaju štete od realizacije pretnje informacionom sistemu. **Smanjenje rizika** podrazumeva implementaciju mehanizama zaštite koje sprečavaju realizaciju pretnje i smanjivanje uticaja rizičnih događaja tako što se smanjuje verovatnoća njegovog pojavljivanja. Prilikom donošenja odluke o postupanju sa rizikom pažnju treba usmeriti sa izbegavanja na smanjenje rizika. U disertaciji je pažnja usmerena na presretanje infrastrukturnih napada implementacijom IDPS sistema.

Cilj ulaganja u informacionu zaštitu je povećanje bezbednosti informacionih dobara od bilo koje vrste pretnje. Ulaganja u zaštitu se mogu finansijski iskazati, ali ne i korist od investicija zbog umanjenja potencijalnog gubitka. Pitanja na koja treba odgovoriti su: (1) kada je jedan sistem dovoljno bezbedan i (2) koja je cena takve zaštite, jer veća ulaganja u zaštitu ne znače obavezno i viši nivo bezbednosti. Očekivani rezultat procesa upravljanja bezbednosnim rizikom je kvantitativna vrednost dodeljena svakom riziku, koja se može koristiti za rangiranje svih rizika uz definisanje kritičnih nivoa i prioriteta, procenu opravdanosti ulaganja u zaštitu, kao i pripremu za nepredviđene troškove.

Sistem sa nultim rizikom ne postoji, a cena takvog rešenja bi verovatno bila veća od vrednosti dobara koja se štiti ili gubitaka prouzrokovanih ostvarenjem rizika. Optimalni nivo bezbednosti u jednoj informacionoj i komunikacionoj infrastrukturi, sa ekonomske tačke gledišta, nalazi se u situaciji kada je vrednost ulaganja u dodatne mehanizme

zaštite jednaka šteti koja bi nastala kao posledica realizacije pretnje koju je implementirani mehanizam zaštite sprečio (slika 3.3)



Slika 3.3. Odnos ulaganja u mehanizme zaštite i uštede usled sprečavanja realizacije napada.

Ekonomski aspekti zaštite informacionog i komunikacionog sistema od simultanih, distribuiranih napada razmatrani su u [43] sa ciljem da se odredi optimalni nivo ulaganja na osnovu maksimiziranja dobiti. U radu [44] predložen je slojeviti model odlučivanja zasnovan na kombinovanju metoda procene bezbednosnog rizika, modela troškova poslovanja i tehnika *cost/benefit* analize. Kritička evaluacija rešenja zaštite poslovno-informacionih sistema zasnovanih na otvorenim softverskim platformama data je u [45].

3.2. Pregled standarda i preporuka

Važnost zaštite kritične infrastrukture ogleda se i u intenzivnim naporima organizacija za standarde da usvoje preporuke i smernice za poboljšanje bezbednosti industrijskih sistema. Relevantni standardi i preporuke obuhvataju opšte standarde o sajber bezbednosti, zajedničke standarde i uputstva za zaštitu SCADA i industrijskih sistema

daljinskog upravljanja, kao i specifične direktive koje se odnose na pojedine industrijske sektore. Detaljan pregled bezbednosnih standarda i preporuka za SCADA sisteme može se pronaći u literaturi [2], [4], [46].

Potreba za upravljanjem bezbednošću informacija u industriji je prepoznata, kako među članicama specifičnih grana kritične infrastrukture, tako i u međunarodnim regulatornim telima i organizacijama za standardizaciju [46]. Brojne organizacije su objavile dokumenta koja se bave zaštitom SCADA sistema, u okviru kojih je razmatran i proces upravljanja rizikom. U odnosu na infrastrukturu SCADA sistema standardi se mogu klasifikovati u tri grupe:

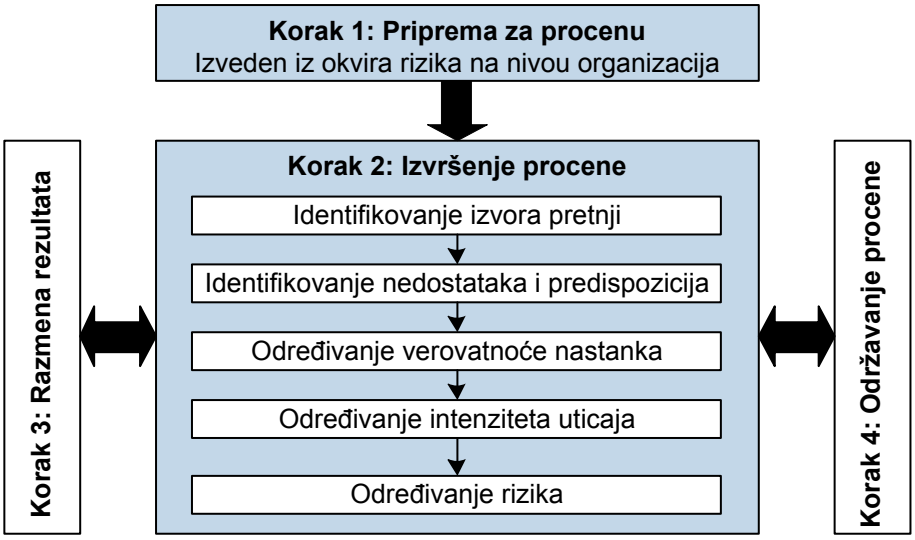
- opšti standardi o sajber bezbednosti (BS, ISO/IEC, ITU);
- opšte smernice za zaštitu SCADA sistema (ISA, DoE, NIST);
- smernice za zaštitu SCADA sistema u specifičnim granama industrije (NERC, IEC, AGA, API, CIGRÉ).

Standardi definišu politiku, procedure, zahteve i smernice za proces upravljanja rizikom. Većina standarda kao zahtev postavlja procenu bezbednosnog rizika [46], pri čemu standardi ne definišu samu metodologiju već daju njene okvire.

Iako standardi iz grupe ISO/IEC 27000 nisu orijentisani na SCADA sisteme, to je uobičajeno korišćen standard za upravljanje bezbednošću informacijama u elektroprivredi [46]. Namenjeni su širokoj grupi korisnika, pre svega za poslovne informacione sisteme [47]. Poređenje ovog standarda sa standardima koji su usmereni na bezbednost informacione i komunikacione infrastrukture SCADA sistema, u aspektima prepoznatih pretnji i preporučenih mehanizama zaštite, može se naći u [46]. Tehnički izveštaj ISO/IEC 27019 dopunjuje skup kontrola sadržanih u ISO/IEC 27000 standardu i obezbeđuje smernice za sprovođenje kontrolnih mera u skladu sa specifičnim zahtevima energetskog sektora.

Specifičnosti rizika telekomunikacionih mreža i upravljanje rizikom prikazano je u ITU-T preporuci X.1055 [48]. Ova preporuka se koristi se za procenu bezbednosnih zahteva i rizika identifikovanih u pružanju telekomunikacionih usluga, sa ciljem da olakša izbor, primenu, održavanje i ažuriranje odgovarajućih mera za smanjenje bezbednosnog rizika i upravljanje bezbednošću informacija.

Organizacija NIST izdala je više dokumenata koji se odnose na bezbednost informacija, a detaljno se bave pojedinim aspektima ovog složenog procesa. Procedure i metode su usklađene sa zatevima grupe standarda ISO/IEC 27000, a oblast bezbednosti industrijskih sistema daljinskog upravljanja je razmatrana u [2]. Ovim dokumentom su obuhvaćeni svi koraci procesa upravljanja bezbednosnim rizikom, sa posebnom pažnjom na preporučene mere zaštite, a novinu predstavlja specifikacija potencijalnih ranjivosti i pretnji. Procena bezbednosnog rizika je jedna od četiri celine procesa upravljanja rizikom koje definiše ovaj dokument (kreiranje konteksta upravljanja, procena rizika, donošenje odluke o postupanju sa rizikom i praćenje rizika). Preporučuje se procena rizika na tri sloja: organizacionom, poslovnom i na nivou informacionog sistema. Proces procene bezbednosnog rizika čine četiri koraka: priprema za procenu, izvršenje procene, razmena rezultata i održavanje procene, kao što je prikazano na slici 3.4.



Slika 3.4. Proces procene bezbednosnog rizika NIST [39].

Dokument [2] sadrži smernice za sprovođenje svakog koraka procesa procene rizika, uz posebne napomene koje se odnose na industrijske sisteme daljinskog upravljanja. Predložen je postupak analize uticaja sajber incidenata u ovim sistemima na:

- šire okruženje (bezbednost ljudi, uticaj na životnu sredinu, uticaj na druge proizvodne i kritične procese koji zavise od procesa industrijskog sistema daljinskog upravljanja koji je meta napada);

- proces koji se kontroliše;
- na industrijski sistem daljinskog upravljanja.

U [2] se ukazuje na nedostatke zbog kojih sajber napad može ugroziti redundantnost koja je opšteprihvaćena praksa u industrijskim sistemima daljinskog upravljanja i to iz razloga što su redundantni delovi sistema jednako podložni napadu. Iako neki sistemi imaju alternativne metode nadzora i kontrole, u vidu analognih instrumenata i uređaja, kao i mogućnosti manuelnog upravljanja, u postupku procene bezbednosnog rizika potrebno je uzeti u obzir duže vreme nadzora i upravljanja koje zahtevaju ovakvi sistemi, naročito na geografski udaljenim lokacijama bez posade. Na kraju, postupak procene bezbednosnog rizika mora da uzme u obzir mogućnost širenja incidenta na povezane sisteme daljinskog upravljanja.

Postojeći standardi, koji su orijentisani na SCADA sisteme, usmereni su prvenstveno na mehanizme zaštite, a manje uzimaju u obzir potencijalne pretnje. U poređenju sa njima, grupa standarda ISO/IEC 27000 je više orijentisana na upravljanje i organizaciona pitanja, a manje se bavi tehničkim aspektima. Industrijski sistemi koji isključivo koriste standarde kao što je ISO/IEC 27000 moraju da se prilagode bezbednosnim zahtevima koji su specifični za SCADA sisteme. Proces procene bezbednosnog rizika bi trebalo da se ponovi nakon značajne promene informacionog sistema, ili ako se pretpostavi pojava nove pretnje i/ili ranjivosti sistema.

3.3. Pregled i analiza metoda za procenu rizika

Tradicionalni metod procene rizika podrazumeva proračun očekivanih gubitaka (*SLE – Single Loss Expectancy*) kao proizvoda funkcije vrednosti dobara (AV – *Asset Value*) i faktora izloženosti pretnjama (EF – *Exposure Factor*) koji predstavlja procenat gubitka dobara u određenom incidentu. Na osnovu verovatnoće nastanka incidenta u toku godine (*ARO – Annual Rate of Occurrence*) može se dobiti vrednost očekivanog godišnjeg gubitka (*ALE – Annual Loss Expectancy*) [35]:

$$ALE = SLE \times ARO = AV \times EF \times ARO. \quad (3.1)$$

Praksa pokazuje da ovakav pristup, kod koga se vrednost informacionih i komunikacionih resursa uglavnom opisuje njihovom knjigovodstvenom vrednošću, iako objektivan, često nije adekvatan. Za primenu ovih metoda neophodno je prikupljanje velikog broja informacija, a proračuni su složeni. Zbog toga se kod procene bezbednosnog rizika preporučuje kombinacija kvalitativnog i kvantitativnog pristupa.

Standardi daju preporuke i okvire za proces procene rizika. Na osnovu njih je izrađeno više metoda, koje su u većini slučajeva podržane softverskim alatima. Sa stanovišta procene bezbednosnog rizika u SCADA sistemima mogu se analizirati metodi za procenu bezbednosnog rizika razvijeni za opšte informacione sisteme i oni koji su namenjeni proceni bezbednosnog rizika u industrijskim sistemima daljinskog upravljanja. Posebno je interesantna analiza moguće primene opštih metoda za procenu bezbednosnog rizika na SCADA sisteme.

Aktuelnost procesa upravljanja i procene bezbednosnog rizika u informacionim i komunikacionim sistemima uslovila je definisanje mnogih metoda i alata za procenu bezbednosnog rizika zasnovanih na preporukama i standardima [49]. Agencija ENISA u svom popisu sadrži sedamnaest metoda i trideset alata za upravljanje i procenu bezbednosnog rizika [50]. Alati su uglavnom komercijalni sa različitim načinima licenciranja.

Ovi metodi i alati su razvijeni za primenu u poslovnim informacionim sistemima, a njihova primena nije uvek jednostavna i moguća za procenu bezbednosnog rizika operativnih informacionih sistema u industriji. Zato su u međunarodnoj organizaciji CIGRÉ uloženi napori za definisanje okvira procesa upravljanja bezbednosnim rizikom SCADA sistema [1], [51]. Rezultati istraživanja radne grupe CIGRÉ ukazuju na razlike u praksi koja se primenjuje u različitim elektroprivrednim preduzećima u oblasti procene bezbednosnog rizika. Ukazano je na neophodnost definisanja metodologije koja bi integrisala procenu bezbednosnog rizika operativnih i poslovnih infrastruktura.

U pregledu i analizi metoda za procenu bezbednosnog rizika prvo će biti prikazan jedan broj metoda namenjenih informacionim sistemima opšte namene, zatim primeri primene ovih metoda u SCADA sistemima, a na kraju će pažnja biti usmerena na metode koji su namenski razvijeni za primenu u SCADA sistemima.

U radu [52] je predložen kvantitativni metod procene bezbednosnog rizika u informacionim sistemima koja uzima u obzir verovatnoću i posledice napada. ISRAM (*Information Security Risk Analysis Method*) se sastoji iz sedam koraka i obezbeđuje vodič kroz proces procene rizika koji razmatra verovatnoću realizacije bezbednosnog rizika kao i posledice koje su rezultat ovog rizika.

U radu [53] je predložen model rizika zasnovan na Bajesovim mrežama koji omogućuje određivanje verovatnoće kompromitovanja telekomunikacione mreže usled različitih nivoa napada i utvrđivanje uzročno-posledičnih veza između stanja mreže. Na osnovu toga se razvija plan upravljanja i definiše strategija za ublažavanje rizika.

Autori rada [54] su predstavili model koji uvodi CTM (*Cascading Threat Multiplier*), multiplikativne faktore koji se uključuju u proširenu definiciju *SLE*. Ovi faktori unose subjektivnost i uvode se sa ciljem dobijanja šire i kompleksnije slike u postupku analize pretnji određenim informacionim dobrima.

Kvantitativni metod analize bezbednosnog rizika zasnovan na poslovnom modelu predložen je u [55]. Metod uzima u obzir kontinuitet poslovanja i utvrđuje vrednost ulaganja u zaštitu informacione i komunikacione opreme na osnovu značaja različitih poslovnih funkcija i nivoa neophodnosti konkretnih zaštitnih mera.

Rezultati istraživanja, koje je sprovela radna grupa CIGRÉ [1] pokazuju da mali broj elektroprivrednih organizacija koristi neki od alata za procenu bezbednosnog rizika. Jedan od metoda namenjen poslovnim informacionim sistemima koji je primenjen u elektroprivredi prema [1] je CRAMM (*CCTA Risk Analysis and Management Method*). Reč je o kvalitativnom metodu za čiju su primenu razvijeni odgovarajući alati. Ceo proces se sastoji iz tri karakteristične faze: (1) identifikacije dobara; (2) identifikacije i procene ranjivosti i pretnji, i (3) predloga mera zaštite. Procena rizika se vrši u prve dve faze. Na kraju svake faze se dobijaju opsežni izveštaji koji predstavljaju polazne parametre za sledeću fazu. Sastavni deo alata je bogata biblioteka potencijalnih ranjivosti, pretnji i mera zaštite koje mogu biti primenjene [56]. Iskustva u primeni ovog alata u elektroprivredi ukazuju da on nije adekvatan za primenu u industrijskim sistemima daljinskog upravljanja zbog nedovoljne fleksibilnosti alata za primenu u SCADA sistemima i kompleksne identifikacije informacionih dobara, što uslovljava

potrebu za aproksimacijama da bi se ovaj metod primenio na specifične arhitekture SCADA sistema.

U istraživanju [1] ukazano je i na primenu CORAS metoda za procenu i upravljanje rizikom u elektroprivredi. CORAS je metod procene rizika zasnovan na izradi modela, a namenjen je sistemima sa visokim bezbednosnim zahtevima. Zasniva se na ISO/IEC 31000 standardu. Kreiran je za generalnu procenu rizika, ali sa posebnom pažnjom usmerenom na bezbednost informacione i komunikacione infrastrukture. Ovaj metod pokriva sve faze upravljanja rizikom, a zasnovan je na modelima koji se kreiraju pomoću UML (*Unified Modelling Language*). CORAS je zasnovan na pet metoda procene rizika HazOP (*HAZard and Operability study*), FTA (*Fault Tree Analysis*), FMECA (*Failure Mode and Effect Criticality Analysis*), Markovljevoj analizi i CRAMM. Ovaj metod obuhvata osam faza koje su dokumentovane dijagramima, a podržan je odgovarajućim softverskim alatom [57].

Modelovanje rizika za prototip industrijskog sistema daljinskog upravljanja pomoću CORAS metoda prezentovano je u [58]. Prvi korak je identifikacija dobara i dodeljivanje nivoa značaja sa aspekta bezbednosti informacione i komunikacione infrastrukture. Zatim su identifikovane pretnje i ranjivosti sistema. Korišćenjem CORAS metoda modelovan je dijagram pretnji. U [58] su prikazani samo preliminarni rezultati, a izveden je zaključak da je CORAS pogodan za primenu u SCADA sistemima.

Procena bezbednosnog rizika u industrijskim sistemima daljinskog upravljanja podrazumeva definisanje parametara rizika na osnovu verovatnoće napada i njegovog uticaja na raspoloživost i kvalitet funkcionisanja industrijskog procesa [59], [60]. U nastavku je prikazano 28 metoda koji su namenjeni proceni bezbednosnog rizika u industrijskim sistemima daljinskog upravljanja. Načelno, metodi se mogu klasifikovati po više osnova, prvo na kvalitativne i kvantitativne, zatim prema načinu modelovanja rizika na one sa matematičkim ili sa grafičkim pristupom, prema izvoru informacija koje su ulazni parametri za procenu rizika (arhive ili stručnjaci), prema tome da li imaju razvijen softverski alat koji olakšava i automatizuje postupak procene, prema oblasti industrije kojoj je namenjen, i drugim [21], [61]. U ovom radu je za osnovnu klasifikaciju, u smislu redosleda prikazivanja odabranih metoda, odabran način

modelovanja rizika. Prvo su predstavljeni metodi koji rizik modeluju matematički i u čijem postupku se koristi formula za obračun rizika [17], [59], [62], [63], [64] i [65], a nakon toga su predstavljeni metodi sa grafičkom predstavom rizika u kojoj se izdvajaju različiti varijeteti: stablo napada (*attack tree*) [66], [67], [68], [69] i njegove modifikacije [70], [71], [72], stablo ranjivosti (*vulnerabilty tree*) [73], Petrijeve mreže [74], [75], [76], infrastrukturni graf [77], [78], [79], teorija igara [80], HHM (*Hierarchial Holographic Modelling*) [81], Bajesove mreže [82]. Na kraju su prikazani metodi za koje odabrana klasifikacija nije bila moguća [60], [83], [84], [85] i [86].

Za procenu ranjivosti sajber bezbednosti u elektroenergetskom sistemu autori rada [62] predlažu dva metoda. Probabilistički kvantitativni metod uzima u obzir verovatnoću kompromitujućeg događaja, uslovnu verovatnoću incidenta nakon neželjenog događaja i težinu posledičnog incidenta. U drugom, integrisanom metodu procene rizika, vrši se kategorizacija rizika u pet grupa i definiše se matrica rizika koju čine procentualna zastupljenost svakog nivoa rizika kao i njihove posledične verovatnoće incidenta i uticaji na sistem. Indeks ranjivosti sistema se računa na osnovu ovih informacija.

Smernice za procenu bezbednosnog rizika u kojima se u obzir uzimaju arhivski podaci i mišljenje stručnjaka predložene su u [63]. Stručnjaci su podeljeni u tri grupe. Prvu grupu čine stručnjaci koji dobro poznaje industrijski proces i bezbednosne zhteve. Njihova uloga je u izradi modela sistema. Pogonski inženjeri, u drugoj grupi, identifikuju ranjivosti i pretnje i odgovarajuće reakcije ljudstva i opreme. IT stručnjaci, koji čine treću grupu, definišu verovatnoću i moguće puteve napada. Proces procene rizika se zasniva na izradi scenarija napada, a izvodi se u deset koraka.

U radu [17] opisan je metod koji se može koristiti za procenu rizika, *cost/benefit* analizu i za proračun premija za osuguravajuća društva. Metod je proveren na prototipu hemijskog postrojenja. U radu je definisano sedam vrsta napada i pet vrsta gubitaka usled realizovanog napada (gubitak kontrole, gubitak u proizvodnji, gubitak vremena osoblja, oštećenje opreme, troškovi prevencije). Gubici zavise od vrste napada. Ulazni parametri su verovatnoće svakog tipa napada i procenjeni finansijski gubici za svaki tip gubitka. Primena ovog metoda obezbeđuje procenu ukupnih gubitaka koji su posledica svih vrsta napada.

Istraživanje o bezbednosnim rizicima predstavljeno u radu [59] ima za cilj da definiše metod i alat koji će zaposleni u elektroenergetskim mrežama koristiti pri odabiru mehanizama zaštite infrastrukture SCADA sistema. Istraživanje dokazuje da se simulacije na test platformama mogu koristiti za generisanje statističkih podataka o postojanju i nivou ozbiljnosti ranjivosti SCADA sistema, kao i o nivou uspešnosti realizacije infrastrukturnog napada. Uticaj pretnje se ocenjuje na osnovu indeksa bezbednosnog rizika koji uključuje verovatnoću postojanja ranjivosti sistema, verovatnoću pojavljivanja pretnje i verovatnoću uspeha sajber napada.

Efikasna detekcija napada na informacionu i komunikacionu infrastrukturu koji menjaju ponašanje ciljnog sistema daljinskog upravljanja moguća je samo uz uključivanje znanja o fizičkom sistemu kojim se upravlja. U radu [64] prikazan je metod procene rizika usled napada na senzore u industrijskom kontrolnom sistemu. Senzori mere procesne veličine i formiraju ulazne podatke koji su neophodni za upravljanje procesom. Metod obuhvata detekciju napada i odgovor na napad. Cilj metoda je da se odredi koji su senzori prioritetni u smislu dodatnih ulaganja u mehanizme zaštite. Polazi se od standardne formule za proračun rizika u kojoj se rizik računa kao proizvod troškova usled realizovanog napada i verovatnoće da napad bude realizovan. Za detektovanje anomalije koristi se linearni model kao aproksimacija ponašanja fizičkog sistema. Kada je detektovana anomalija aktivira se alarm i čeka akcija osoblja. Simuliran je sajber napad na hemijski reaktor u modelu industrijskog kontrolnog sistema. Eksperimenti su pokazali da je predloženi metod ispunio postavljeni cilj.

Metod za kvantitativnu procenu bezbednosnog rizika u SCADA sistemima zasnovan na praćenju toka energije sa ciljem proračuna očekivane štete prikazan je u [65]. Razmatra se petnaest vrsti pretnji i četiri komponente SCADA sistema (EMS server, SCADA server, RTU i komunikacioni podsistem). U postupku procene potrebno je kvantifikovati ranjivost sistema i pretnje. Za potrebe kvantifikacije ranjivosti definišu se indeksi ranjivosti komponenata sistema na svaku vrstu pretnje. Indeksi su zasnovani na arhivskim podacima, ako su dostupni, i bezbednosnim karakteristikama komponenti. Za kvantifikaciju pretnji uzima se u obzir primenljivost pretnje na komponentu, indeks ranjivosti komponente i procena moguće štete koju pretnja nanosi komponenti. Rizik se izračunava u novčanoj vrednosti kao proizvod svih verovatnoća pretnji, ranjivosti i vrednosti dobara. Vrednost dobara je srazmerna troškovima usled otkaza.

Stablo napada se koristi u nekoliko metoda procene rizika u SCADA sistemima. Stablo napada je graf koji opisuje korake procesa napada, čvorovi grafa su stanja napada, a veze su putanja napada kroz sistem.

U [66] je pokazano kako se metodologija stabla napada može primeniti na procenu ranjivosti specifikacije i primene Modbus ili Modbus/TCP protokola u SCADA sistemima. Autori su predložili metod za proračun karakteristika najverovatnijeg napada. Stablo napada čine čvorovi sa identifikovanim ciljevima potencijalnog napadača, svaki sa nivoom mogućnosti realizacije, potencijalnog uticaja na sistem i verovatnoće detekcije. Svi identifikatori su definisani na kvalitativnoj skali. U radu je definisano jedanaest osnovnih i četiri pomoćna cilja, i na ovim primerima je realizovano stablo napada.

Metod za kvantitativnu procenu smanjenja bezbednosnog rizika nakon implementacije mehanizama zaštite predložen je u [67]. Metod predlaže deset koraka koje treba ponoviti za sistem pre i nakon unapređenja, a zatim upoređivanje rezultata i procenu smanjenja rizika. Za obe varijante sistema se kreira stablo napada u kojima su čvorovi potencijalno stanje napada za svaki uređaj u mreži. Veze između čvorova predstavljaju prelaske između stanja napada i njima je pridruženo procenjeno vreme potrebno za prelazak između dva stanja. Izračunava se dominantni put u kome je vreme do kompromitovanja sistema najkraće. Ovo vreme je glavni indikator bezbednosti sistema, a umanjenje rizika nakon implementacije mehanizama zaštite se meri stepenom produženja ovog vremena. Metod je verifikovan na realnom SCADA sistemu za dve vreste napada: DoS i preuzimanje kontrole nad RTU.

Metod opisan u [68] se sastoji iz četiri modula: (1) monitoring u realnom vremenu; (2) detekcija anomalija; (3) analiza uticaja i (4) strategija zaštite. Ovi moduli čine RAIM (*Real-time monitoring, Anomaly detection, Impact analysis and Mitigation strategies*). Prva dva modula se zasnivaju na kontinuiranom praćenju sistemskih logova i prikupljaju podatke koji su potrebni za sledeći modul, analizu uticaja. Ovaj modul je odgovoran za prepoznavanje napada. Primena ovog metoda je demonstrirana na prototipu mreže u elektroprivredi.

U [69] predstavljen je okvir za procenu rizika koji je zasnovan na merenjima fazora u prenosnoj mreži (PMU – *Phasor Measurement Unit*). Metod obuhvata konfiguraciju

sistema, identifikaciju i kvantifikovanje ranjivosti i kreiranje stabla napada koje se koristi za određivanje scenarija i verovatnoće napada. U radu je predstavljen i sistem za nadgledanje u realnom vremenu koji automatski aktivira mehanizme zaštite u slučaju detekcije napada.

Stablo protivmera napadu (ACT – *Attack Countermeasure Tree*) se koristi za analizu rizika i proračun povrata ulaganja u zaštitu ili povrata ulaganja u napad [70]. U stablu se razlikuju tri vrste čvorova: napad, detekcija napada i sprečavanje napada. Mehanizmi zaštite se mogu primeniti u svakom čvoru stabla. Dodatne informacije koje mogu biti uključene u stablo su vrednost implementiranih mehanizama zaštite i troškovi nastali usled realizovanog napada. Primena metoda omogućuje kreiranje scenarija napada, kvalitativnu procenu bezbednosnog rizika, kao i izbor optimalnog mehanizma zaštite.

ADVISE (*ADversary VIew Security Evaluation*) metod je predstavljen u [71], a ima za cilj da generiše simulaciju napada i obezbedi proračun verovatnoće uspešnog napada. Za modelovanje napada koristi se stablo napada (AEG – *Attack Execution Graph*) koje je prošireno različitim karakteristikama napadača. U suštini, na celokupnu bezbednost sistema ne utiče samo sposobnost sistema da odgovori na pokušaj napada, već i sposobnosti napadača i njegovo viđenje sistema. Model se sastoji iz AEG stabla napada i profila napadača. Stablo napada čini nekoliko vrsta čvorova: znanja i veštine napadača, mogućnost pristupa mreži, stanje napada i krajnji cilj. Profil napadača definišu dve grupe promenljivih. Prvu grupu čine promenljive koje ne zavise od sistema koji je meta napada: težina napada i nivo veštine napadača. U drugu grupu se ubrajaju tri promenljive koje zavise od sistema: cilj napada, pristup sistemu i sistemsko znanje. Nakon kreiranja profila napadača, opisivanja sistema i definisanja metrike, može se kreirati stablo napada koje omogućuje stvaranje izvršnih modela za kvantitativnu analizu. Metod je automatizovan softverskim alatom, a verifikovan je na dva primera opšte arhitekture SCADA sistema koji su opisani u [2].

Modelovanje napada kombinacijom Markovljevog procesa i Bulove logike (BDMP – *Boolean Logic Driven Markov Proces*) prikazano je u [72]. Primena ovog metoda obezbeđuje kvantifikovanje mogućih posledica napada. Proces procene počinje kreiranjem modela sistema od čvorova, logičkih kola i međusobnih veza. Čvorove karakteriše verovatnoća uspeha napada. Za razliku od klasičnih stabala napada za

BDMP je karkteristično korišćenje dinamičkih „okidača“, veza koje se koristite u situacijama kada jedan događaj aktivira drugi, i veza koje definišu realizaciju odgovarajućih mehanizama zaštite. Metod je testiran modelovanjem *Stuxnet* napada.

Grafička prezentacija ranjivosti sistema korišćenjem stabla ranjivosti zasnovana je na istim principima koji se koriste u stablima napada, sa razlikom što čvorovi grafa predstavljaju bezbednosne propuste i ranjivosti sistema koje može da zloupotrebi zlonamerni korisnik.

Cilj metoda prikazanog u [73] je pomoć menadžerima u donošenju odluka o implementaciji mehanizama zaštite. Rizik se izražava numerički na osnovu dva indeksa i stabla ranjivosti. Prvi indeks se odnosi na finansijske efekte ugroženosti sistema, a drugi na ranjivost sistema u odnosu na sajber napade. Stablo ranjivosti se razvija na osnovu analiza napada iz prošlosti. Finansijski gubici prouzrokovani napadom su procenjeni na osnovu intervjua sa inženjerima, poslovodstvom, operaterima i finansijskim stručnjacima. Verovatnoće napada su identifikovane na osnovu arhivskih podataka. Upoređivanjem indeksa za različita bezbednosna rešenja, menadžeri mogu izabrati mehanizme u skladu sa njihovom efikasnošću, napraviti najbolji izbor i opravdati troškove ulaganja u bezbednost. Metod je testiran na laboratorijskom modelu SCADA sistema.

Petrijeve mreže su alat za grafičko i matematičko modelovanje dinamičkog sistema, a relativno često se primenjuju za modelovanje informacionih sistema. Petrijeve mreže su po stukturi usmereni grafovi koji imaju dve vrste čvorova, čvor stanja i čvor prelaza.

S obzirom da je za procenu bezbednosnog rizika neophodna analiza ranjivosti SCADA sistema na različite vrste napada, kao i posledica napada na funkcionisanje sistema, u radu [74] analizirani su različiti tipovi napada i odgovarajući mehanizmi zaštite. Autori su predožili metod za procenu ranjivosti na nivou sistema, scenarija i pristupnih tačaka. Ovo istraživanje koristi probabilističke metode koje se baziraju na Petrijevim mrežama i stablu napada kako bi se identifikovale ranjivosti u centru upravljanja i podstanicama. Pažnja je usmerena na napade na mrežu kontrolnog centra do koje se dolazi ili preko korporativne mreže ili preko mreže podstanica. Metod se može koristiti za identifikaciju gubitka i kao alat koji identifikuje bezbednosna uska grla u sistemu u kojima bi primena zaštitnih mehanizama bila najefikasnija.

U radu [75] prikazan je metod procene rizika od infrastukturnog napada na mrežu industrijskog kontrolnog sistema koji je zasnovan na Petrijevim mrežama. Ovaj metod kvantifikuje operativne posledice otkaza svakog dela sa aspekta vlasnika procesa. Cilj je identifikacija stanja napada sa teškim posledicama. Rizik se izražava u funkciji resursa kojima pristupa napadač. Metod je primenjen u sistemu za upravljanje opasnim tečnostima. U svrhu analize identifikovane su moguće greške u sistemu sa odgovarajućim posledicama i resursi potrebni za izvršenje napada. Kreirane su tri Petrijeve mreže koje modeluju: (1) industrijski proces, (2) SCADA sistem i (3) topologiju ranjivosti. Resursi koji su potrebni napadaču formiraju preduslove za otkaz SCADA sistema koji može prouzrokovati jednu ili više grešaka u procesu. U radu je dat primer gubitaka u proizvodnji ili zagađenja životne sredine, a ozbiljnost uticaja se meri brojem povreda na radu usled ispada sistema. Ovaj metod ne omogućuje procenu uticaja rizika na druge elemente infrastrukture.

Pristup modelovanju i kvantifikaciji međusobnih zavisnosti električne i informacione infrastrukture sistema za daljinski nadzor elektroenergetskih objekata razmatran je u [76]. Integrisan metod zasnovan na Petrijevim mrežama kombinuje SAN (*Stochastic Activity Networks*) i SWN (*Stochastic Well-formed Network*) mreže u cilju kvantifikacije posledica otkaza infrastrukture. Pristup je verifikovan simulacijom otkaza pojedinih delova komunikacione infrastrukture usled DoS napada.

U radu [77] predložena je strategija upravljanja rizicima za otkrivanje složenih napada, kao i za podršku ublažavanju rizika. Metod je zasnovan na dva grafa. Prvi je infrastrukturni graf koji opisuje stanje komponenti sistema i njihovu međuzavisnost. Sistem je dekomponovan na manje složene delove koje je lakše predstaviti i analizirati. Drugi je graf evolucije koji opisuje napade na sistem. Složeni napadi su predstavljeni nizom jednostavnih napada. Graf evolucije može predstavljati složene napade koji opisuju put od prvog do poslednjeg jednostavnog napada. Ovaj graf se redukuje u cilju eliminisanja napada male verovatnoće. Pretpostavlja se da mehanizmi zaštite mogu zaustaviti ili ublažiti jednostavne napade prekidajući puteve kojim bi se realizovao složeni napad. Izvor za modelovanje napada su arhivski podaci. Za primenu metoda razvijen je softverski alat. Procena rizika obuhvata i preporuku implementacije mehanizama zaštite.

Upotreba grafa za procenu bezbednosnog rizika je primenjena i u modelu rizika u mreži - NSRM (*Network Security Risk Model*) koji je predstavljen u [78]. Clij metoda je odabir optimalne bezbednosne strategije i mehanizama zaštite, kao i procena poboljšanja bezbednosti nakon implementacije. Metod obuhvata osam koraka. Prvo se identifikuje rizik i modeluje infrastruktura. Zatim se identifikuju mogući otkazi u procesu i njihove posledice. Sledeći koraci su specifikacija procesa i kreiranje scenarija napada u kome se definišu ciljevi i pristupne tačke napada. Na kraju se opisuje bezbednosna struktura procesne mreže i identifikuje politika napadača. Čvorovi grafa su komponente sistema, a veze su potencijalni uticaji među komponentama. Metod je testiran u postrojenju naftnih pumpi. Zbog nedostatka statističkih podataka i specifičnosti sistema, stručnjaci moraju da budu uključeni u procenu parametara neophodnih za proračun.

U radu [79] je prikazan metod za procenu rizika zasnovan na probabilističkom pristupu procene rizika. Testiran je u laboratorijskim uslovima na prototipu destilerije. Dijagnoza otkaza je demonstrirana na scenariju u kom haker vrši napad na korporativnu mrežu i preko nje ubacuje SCADA DNP3 saobraćaj sa zlonamernim kodom. Metod se zasniva na modelu koji je kreiran pomoću usmerenog grafa. Model obezbeđuje formalno predstavljanje strukture i ponašanja SCADA sistema i može se koristiti za procenu rizika i dijagnozu otkaza. Čvorovi usmerenog grafa su komponente sistema, a direkcione veze povezuju čvorove ukoliko postoji mogućnost propagacije rizika sa jednog čvora na drugi. Pomoću grafa moguće je identifikovati izvor otkaza.

Primena teorije igara u cilju analize bezbednosnog rizika u *smart grid* SCADA sistemima prikazana je u [80]. Odnos između sistem administratora SCADA sistema i napadača je modelovan kao sekvencijalna igra sa dva igrača. Posmatra se uticaj akcije igrača na poverljivost, integritet i raspoloživost preko odgovarajućih težinskih koeficienata koji se određuju na osnovu stručnog mišljenja i arhivskih podataka. Prikazana je studija slučaja u SCADA sistemu senzorske mreže.

U radu [81] prikazan je metod koji koristi HHM modelovanje za identifikaciju izvora rizika SCADA sistema u železničkom sektoru. HHM olakšava procenu rizika pojedinih delova sistema i njihovo učešće u ukupnom riziku celog sistema. Metod polazi od kompleksne strukture SCADA sistema u kojoj se izdvajaju tri ključna dela: (1) hardver i

softver, (2) osoblje i (3) okruženje u kome SCADA sistem funkcioniše. Autori ovog metoda preporučuju da se u proces procene uključe iskusni stručnjaci koji poznaju sistem u celini i korišćenje COBIT (*Control Objectives for Information and Related Technology*) koji olakšava identifikaciju rizika.

Procena bezbednosnog rizika primenom Bajesovih mreža koja je zasnovana na analizi podataka predložena je u radu [82]. U grafu kojim je predstavljena Bajesova mreža razlikuju se dve vrste čvorova. Prva vrsta predstavlja ranjivost sistema, a koriste se poznate ranjivosti koje su identifikovane u javno dostupnoj bazi podataka. Druga grupa čvorova predstavlja komponente sistema koje su podložne napadu. Uslovne verovatnoće za Bajesovu mrežu se određuju iz arhivskih podataka, a povećanje tačnosti metoda procene bezbednosnog rizika se postiže primenom mašinskog učenja. Metod je proveren na SCADA sistemu hemijskog postrojenja, primenom Matlab-a.

Autori rada [83] su kao rezultat istraživanja na modelu SCADA sistema identifikovali brojne ranjivosti. Cilj metoda koji je prikazan u [83] je procena ranjivosti sistema. Predložen je postupak koji obuhvata razvoj plana procene, konfiguraciju okruženja i procenu ranjivosti koja se izvodi kroz test napada na sistem. Bezbednost SCADA sistema se izražava kvantitativno.

U radu [84] prikazan je metod koji obezbeđuje okvir za kontinualan proces procene bezbednosnog rizika u sistemu daljinskog upravljanja u elektroprivredi. U okviru metoda su definisane tri faze. Cilj prve faze je upoznavanje sa sistemom i definisanje okvira analize, sa rezultujućom definicijom podsistema i međusobnih odnosa čime se definiše topologija sistema, sa putanjama kroz koje se može proširiti ranjivost i pretnja. Ove putanje definišu lanac otkaza servisa. Druga faza obuhvata procenu ranjivosti i pretnji. Metod predviđa da se prvo izvrši procena ranjivosti u svim delovima sistema, a kao rezultat ove faze metod daje profil ranjivosti sistema. Analiza pretnji se vrši u skladu se profilom ranjivosti sistema. Metod preporučuje da se za pretnju definišu dva atributa: verovatnoća pojave i ozbiljnost pretnje. Atributi imaju kvalitativnu skalu (npr. nizak, srednji, visok). Kombinacija ova dva atributa daje relevantnost pretnje. Za dalju analizu se uzimaju samo one pretnje čija je relevantnost iznad definisanog praga, a rezultat je dobijeni profil izloženosti sistema. Završni deo druge faze je kombinovanje dva profila, ranjivosti i izloženosti pretnjama. U trećoj fazi se vrši procena napada, kroz

razvoj modela napada, i procena rizika čiji je rezultat narušavanje bezbednosti sistema. Autori naglašavaju da je neophodno sagledavanje posledica koje bi ostvarenje rizika imalo na ceo elektroenergetski sistem. Na osnovu indeksa rizika se predlažu mere zaštite i ponavlja proces procene rizika nakon primene predloženih mera.

U [85] su date smernice za upravljanje rizikom od sajber terorizma u SCADA sistemima u Australiji sa ciljem da se izvrši procena rizika i unapredi zaštita ovih sistema. Metod je verifikovan od strane tima koga čini pet stručnjaka u oblasti SCADA industrijskih sistema. Smernice obuhvataju tri faze: procenu rizika kroz izradu modela rizika, izrada modela procene sposobnosti terorista i preporuka mehanizama zaštite. Prva faza se sprovodi primenom standarda za upravljanje rizikom (AS/NZS 4360:2004), a treća primenom standarda za upravljanje bezbednošću informacija (AS/NZS 27002:2006). Da bi se procenila sposobnost terorističkih grupa predložen je metod u kome se ocenjuje politička motivacija i sposobnosti sa aspekta nivoa znanja o informacionim tehnologijama i SCADA sistemima, finansijske podrške, regrutovanja zaposlenih u organizaciji. Ova faza se sprovodi kroz anketu koja sadrži osam pitanja.

Autori rada [60] ističu da je sajber bezbednost korporativnih sistema važna, ali da ona u potpunosti ne rešava sigurnost SCADA sistema. Na ovaj način se ne ostvaruje zaštita sistema kada napad potiče iz SCADA mreže. Pažnja se mora usmeriti na zaštitu krajnjih uređaja SCADA sistema kao što je RTU. U radu je predložen kvalitativan metod procene rizika koji se sastoji iz osam koraka. Procena počinje opisivanjem arhitekture sistema nakon čega sledi identifikovanje pretnji i njihovog uticaja na sistem, procene rizika i ranjivosti sistema čiji je krajnji cilj određivanje nivoa rizika i mehanizama zaštite. Određivanjem prioriteta zaštite i konačnog pristupa u implementaciji kontrolnih mera počinje proces procene preostalog rizika i eventualnog ponavljanja postupka dok se ne zadovolji zahtevani nivo bezbednosti. Nivo rizika se određuje na osnovu verovatnoće realizacije i težine posledica realizovanog napada. Za svaki nivo rizika su preporučeni mehanizmi zaštite. Postupak se sprovodi za svaku komponentu sistema. Metod se zasniva na zajedničkom radu tima stručnjaka različitih oblasti.

Metod procene bezbednosnog rizika koji se može implementirati u procesu projektovanja kontrolnih sistema u nuklearnim elektranama je prikazan u [86]. Postupak obuhvata šest faza: (1) identifikacija sistema i modelovanje bezbednosti informacione i

komunikacione infrastrukture; (2) analiza dobara i uticaja; (3) analiza pretnji; (4) analiza ranjivosti; (5) projektovanje mehanizama zaštite i (6) testiranje napada na sistem. U radu je dat pregled potencijalnih scenarija napada za potrebe testiranja. Na osnovu rezultata primene metoda dobijaju se pregled ranjivosti sistema i preporučene bezbednosne mere.

Uporedna analiza metoda za procenu rizika u informacionim sistemima opšte namene se može naći u [49], [87] i [88]. U nastavku poglavlja pažnja će biti usmerena na metode procene bezbednosnog rizika u industrijskim sistemima daljinskog upravljanja.

U tabeli 3.1 dati su opšti podaci analiziranih metoda.

Tabela 3.1. Pregled analiziranih metoda: opšti podaci

Lit.	Godina	Naziv	Država
[62]	2006	Procena ranjivosti sajber bezbednosti u elektroenergetskom sektoru	Kina
[63]	2006	Analiza bezbednosnog rizika zasnovana na scenariju	SAD
[17]	2010	Model procene rizika u uslovima sajber napada na informacione sisteme	SAD
[59]	2011	Procena sajber bezbednosnog rizika u elektroenergetskim sistemima zasnovana na modelima napada	Italija
[64]	2011	Napadi na sisteme za kontrolu procesa: procena rizika, otkrivanje i odgovor	SAD
[65]	2014	Kvantitativni metod za procenu sajber bezbednosnog rizika SCADA sistema	Južna Koreja
[66]	2004	Korišćenje stabla napada za procenu ranjivosti SCADA sistema	Kanada
[67]	2006	Kvantitativni metod procene smanjenja bezbednosnog rizika za mali SCADA sistem	SAD
[68]	2010	Sajber bezbednost kritične infrastrukture: Modelovanje napada i ogovora na napad	Irska
[69]	2013	Procena rizika u elektroenergetskim sistemima zasnovana na merenjima fazora	SAD
[70]	2010	Analiza sajber bezbednosti primenom stabla mehanizama zaštite	SAD
[71]	2010	Procena bezbednosti sistema zasnovana na karakteristikama napada	SAD
[72]	2012	Modelovanje *Stuxnet* napada kombinacijom Markovljevog procesa i Bulove logike	Francuska
[73]	2008	Kvantitativna procena ranjivosti kritičnih informacionih sistema: Novi metod za procenu poboljšanja bezbednosti	SAD

Tabela 3.1. (nastavak) Pregled analiziranih metoda: opšti podaci

Lit.	Godina	Naziv	Država
[74]	2008	Procena ranjivosti bezbednosti SCADA sistema	SAD
[75]	2009	Procena rizika od sajber napada na SCADA sisteme pomoću Petrijevih mreža i primena na upravljanje opasnim tečnostima	SAD
[76]	2012	Kvantifikacija zavisnosti između električne i informacione infrastrukture	Italija
[77]	2009	Hijerarhijski model upravljanja rizikom kritičnih infrastruktura	Italija
[78]	2009	Sveobuhvatni model bezbednosnog rizika za sisteme za kontrolu procesa	SAD
[79]	2011	Model usmerenih grafova za identifikaciju i upravljanje rizikom u SCADA sistemima	SAD
[80]	2014	Analiza sajber bezbednosti SCADA sisema primenom teorije igara	SAD
[81]	2004	Rizici od terorizma za informacione tehnologije i kritične infrastrukture	SAD
[82]	2017	Primena Bajesovih mreža na procenu bezbednosnog rizika u SCADA sistemima	Kina
[83]	2005	Metodi procene sajber bezbednosti u SCADA sistemima	SAD
[84]	2006	Ključna pitanja i metodologije za analizu i procenu bezbednosnog rizika u elektroenergetskom sistemima	Italija
[85]	2009	Zaštita Australije od sajber terorizma: Upravljanje rizikom od sajber terorizma u SCADA sistemima	Australija
[60]	2011	Analiza rizika zasnovana na raspoloživosti SCADA sistema	SAD
[86]	2012	Procena bezbednosnog rizika za proces projektovanja kontrolnih sistema u nuklearnim elektranama	Južna Koreja

U tabeli 3.2 prikazano je kvalitativno poređenje analiziranih metoda za procenu bezbednosnog rizika u industrijskim sistemima daljinskog upravljanja. Struktura tabele ukazuje na relacije koje postoje između predloženih metoda sa aspekta modelovanog rizika, predloženih kontrolnih mera za ograničavanje rizika, oblasti primene i evaluacije metoda.

Tabela 3.2. Pregled i klasifikacija analiziranih metoda: kvalitativno poređenje

Literatura	Tip		Model rizika		Probabilistički metod	Izvor informacija		Razvijen softverski alat	Predložena kontrolna mera	Sektor primene	Način evaluacije metoda
	Kvalitativan	Kvanitativan	Matematički	Grafički		Arhive	Stručnjaci				
[62]		✓	✓		✓					Energetski	Ne
[63]		✓	✓		✓	✓	✓			Nuklearni	Opšti primer
[17]		✓	✓		✓		✓	✓		Hemijski	Realni sistem
[59]		✓	✓		✓					Energetski	Test platforma
[64]		✓	✓					✓	✓	Hemijski	Laboratorijsko okruženje
[65]		✓	✓			✓	✓	✓		*Smart grid*	Realni sistem
[66]	✓			✓			✓			Energetski	Laboratorijsko okruženje
[67]		✓		✓	✓		✓		✓	Mali SCADA sistem	Realni sistem
[68]		✓		✓	✓	✓		✓	✓	Energetski	Podmreža za testiranje
[69]		✓		✓	✓				✓	Energetski	Simulacija
[70]		✓		✓	✓			✓	✓	Opšta SCADA	Opšti primer
[71]		✓		✓	✓		✓			Energetski	Primer iz literature
[72]		✓		✓	✓		✓	✓		Model Stuxnet napada	Model Stuxnet napada
[73]		✓		✓	✓	✓	✓		✓	Hemijski	Test platforma
[74]		✓		✓	✓	✓			✓	Energetski	Primer iz literature
[75]		✓		✓						Postrojenje sa opasnim tečnostima	Primer iz literature
[76]		✓		✓	✓					Energetski	Primer iz literature
[77]		✓		✓	✓	✓		✓	✓	Opšta SCADA	Opšti primer
[78]		✓		✓	✓	✓	✓		✓	Naftna industrija	Uprošćena verzija SCADA sistema
[79]		✓		✓						Hemijski	Laboratorijsko okruženje
[80]		✓		✓	✓	✓	✓		✓	*Smart grid*	Realni sistem

Tabela 3.2. (nastavak) Pregled analiziranih metoda: kvalitativno poređenje

Literatura	Tip		Model rizika		Probabilistički metod	Izvor informacija		Razvijen softverski alat	Predložena kontrolna mera	Sektor primene	Način evaluacije metoda
	Kvalitativan	Kvanitativan	Matematički	Grafički		Arhive	Stručnjaci				
[81]	✓			✓					✓	Železnica	Ne
[82]		✓		✓	✓	✓				Hemijski	Realni sistem
[83]		✓								Energetski	Ne
[84]	✓						✓	✓	✓	Energetski	Laboratorijsko okruženje
[85]	✓								✓	Opšti SCADA sistem	Evaluacija 5 stručnjaka
[60]		✓			✓		✓		✓	Opšti SCADA sistem	Ne
[86]	✓								✓	Nuklearni	Laboratorijsko okruženje

Analizirani metodi su pretežno kvantitativni. Od 28 prikazanih metoda, 5 metoda je kvalitativno (17,9%), a 23 metoda je kvantitativno (82,1%). Probabilistička procena rizika određuje rizik na osnovu verovatnoće realizacije neželjenog događaja i na osnovu težina potencijalnih posledica. Uprkos nepostojanju pouzdanih podataka na osnovu kojih može da se proračuna verovatnoća koja se uključuje u procenu rizika, metodi koji su zasnovani ovom principu su dominantni. Nedostatak arhivskih podataka o sajber incidentima u SCADA sistemima otežava procenu rizika. Iako je nekada teško odrediti ove verovatnoće, čak 18 metoda pripada ovoj grupi, a svi su kvantitativni, što čini da je 78,3% kvantitativnih metoda probabilističko. Takođe, većina metoda (17) je zasnovana na grafičkom modelu rizika, a procena rizika matematičkom formulom zastupljena je u 6 metoda. Sedam metoda je zasnovano na modelu u kojima dominira pristup izrade stabla napada. Kao izvor informacija u 7 metoda su to stručnjaci, u 4 su arhivski podaci, a u 5 metoda se uzimaju oba izvora informacija. U jednom broju primera (8 radova) je razvijen softverski alat koji automatizuje proces procene rizika. Verifikacija metoda se retko vrši u realnim sistemima. Od analiziranih metoda je to u pet slučajeva, dok se

često koriste opšti primeri i primeri iz literature (7), laboratorijske i test platforme (8). U četiri slučaja nije vršena evaluacija metoda. Kao mera rizika uzima se monetarna vrednost (7), kao i indeks ili nivo rizika (6). U specifičnim slučajevima rizik se meri brojem povreda na radu, izgubljenom proizvodnjom ili nestabilnošću napona u mreži u energetskom sektoru. Međutim, u 10 radova nije eksplicitno navedeno kako se rizik izražava.

Uporedna analiza literature u kojoj je predložena metodologija procene rizika u industrijskim sistemima daljinskog upravljanja ukazuje na sledeće činjenice:

- Nedovoljno je zastupljena detaljna analiza SCADA sistema, njegovih komponenti, njihovih međusobnih zavisnosti i uticaja koje na njih mogu imati spoljašnji faktori.
- Veoma su zastupljeni metodi zasnovani na proračunu verovatnoće, ali su podaci o incidentima često nedostupni. Jedno od rešenja za nedostatak arhivskih podataka je korišćenje SCADA test platformi za prikupljanje eksperimentalnih podataka o pretnjama i ranjivostima. Sa druge strane, simulacije zasnovane na adekvatnim modelima mogu značajno da upotpune statistiku o ranjivosti sistema na napade. U literaturi nisu značajnije zastupljene studije sa simulacionom analizom uticaja pretnji na performanse SCADA sistema.
- U nedostatku arhivskih podataka značajno je subjektivno mišljenje stručnjaka, koje je u mnogim slučajevima dostupnije, pa i vrednije od statističkih analiza arhivskih podataka.

Na osnovu analize relevantne literature, u disertaciji su predložena i ispitana dva metoda koja polaze od analize arhitekture SCADA sistema, a posebna pažnja je usmerena na veze sa drugim informacionim i tehničkim sistemima, kao i na analizu ranjivih delova infrastrukture koja je podložna napadima. Zatim je razvijen simulacioni model kojim se može uvrditi stepen degradacije ključnih performansi (raspoloživost, kašnjenje, procenat izgubljenih paketa, opterećenje procesorskih resursa) u različitim uslovima distribuiranih napada na informacioni i komunikacioni sistem za podršku sistema daljinskog upravljanja. U drugom predloženom metodu primenjen je hibridni pristup u kome se u zavisnosti od raspoloživih izvora koriste arhivski podaci i/ili mišljenja stručnjaka sa preporukom kako da se ta mišljenja formalizuju i kvantifikuju.

Kao opšti zaključak ovog poglavlja, može se reći da je potvrđena potreba za unapređenjem sistema zaštite industrijskih sistema daljinskog upravljanja, a deo tog procesa treba da bude i procena bezbednosnog rizika. Analiza metoda sa aspekta prilagođenosti SCADA sistemima treba da doprinese donošenju odluke o primeni ili razvoju adekvatnog metoda u industriji.

4. ANALIZA PERFORMANSI SISTEMA DALJINSKOG UPRAVLJANJA U USLOVIMA SIMULTANIH, DISTRIBUIRANIH NAPADA NA INFRASTRUKTURU IP MREŽE

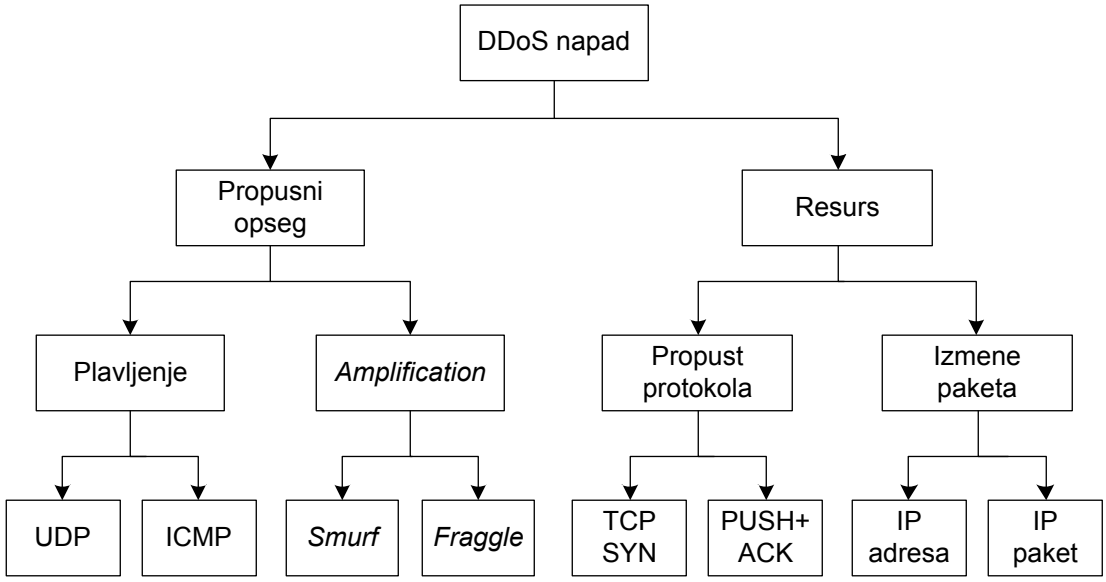
Arhitektura savremenih telekomunikacionih mreža u industriji podrazumeva povezanost korporativne mreže i mreže sistema za daljinsko upravljanje. Dizajn ovih mreža treba da omogući pružanje operativnih i poslovnih telekomunikacionih servisa uz ispunjenje određenog broja zahteva u pogledu performansi i tehničkih karakteristika. Operativni servisi (daljinsko upravljanje, telezaštita, operativna telefonija i operativni video) su direktno vezani za tehnološko funkcionisanje industrijskih sistema. Za njih su karakteristični strogi zahtevi za pouzdanost, raspoloživost i kašnjenje. Operativni servisi ne generišu promenljiv i nepredvidljiv intenzitet saobraćaja. Poslovni servisi (prenos poslovnih podataka, poslovna telefonija, multimedijalni servisi) vezuju se za poslovno funkcionisanje kompanije. Zahtevi, kao što su kašnjenje, pouzdanost i raspoloživost su daleko blaži, a dominantna komponenta postaje zahtev za dovoljno velikim propusnim opsegom.

Napadi kao što je odbijanje servisa (DoS) potencijalno ugrožavaju vitalne funkcije industrijskog procesa. Ovaj tip napada može se vršiti u različitim formama na bilo kom sloju protokol steka. Posebno je teško otkriti i sprečiti distribuirane napade DDoS u kojima više napadača istovremeno napada metu (npr. vitalni mrežni server).

U ovom poglavlju su analizirane performanse (raspoloživost, kašnjenje, procenat izgubljenih paketa, opterećenje procesorskih resursa) operativnog servisa daljinskog upravljanja u uslovima DDoS napada. U nastavku je dat pregled karakteristika ovog napada, a zatim su prikazani rezultati simulacije u kojoj je na modelu elektroprivredne telekomunikacione mreže simuliran DDoS napad. Rezultati istraživanja publikovani su u radu [89].

4.1. DDoS napad

Cilj DDoS napada je da se blokiraju glavni resursi objekta napada ili da se iscrpi raspoloživi mrežni propusni opseg što za posledicu ima odbijanje servisa. U prvom slučaju, kada intenzitet dolaznog saobraćaja postane veliki, resursi žrtve napada, npr. CPU (*Central Processing Unit*) i memorija, bivaju zauzeti, nastaje odbacivanje paketa što izvoru saobraćaja ukazuje da treba da smanji brzinu slanja paketa. Legitimni korisnici će to prihvatiti, ali će napadač povećati intenzitet nelegitimnog saobraćaja. U drugoj grupi napada neželjeni tok saobraćaja dominira na komunikacionom pravcu ka žrtvi i legitimni tokovi saobraćaja bivaju blokirani. Na taj način dolazi do otkazivanja servisa i na drugim serverima koji se nalaze na napadnutom linku. Paketi koji pripadaju legitimnom saobraćaju će biti odbačeni ako ne postoje mehanizmi kojima će se razlikovati legitimni od zlonamernog saobraćaja. Na slici 4.1 je prikazana kategorizacija DDoS napada, a karakteristike jednog napada se mogu svrstati u više kategorija [90].

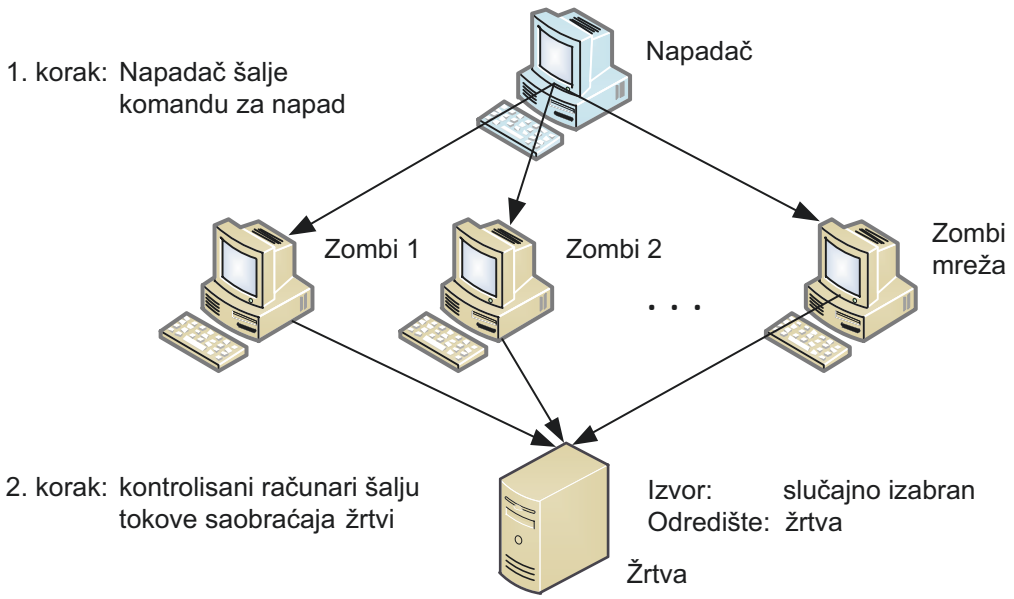


Slika 4.1. Klasifikacija DDoS napada [90].

Napad se može realizovati na više načina, preko napada na operativni sistem, do napada na mrežne servise. Ove napade je veoma lako generisati, ali se veoma teško otkrivaju i zato predstavljaju interesantno oružje potencijalnim napadačima. Napadi koji koriste propuste u softveru se mogu sprečiti blagovremenom instalacijom softverskih dodataka. Druga vrsta napada, u kojoj se koristi veliki intenzitet zlonamernog saobraćaja, ne može

se jednostavno sprečiti. U nastavku će biti razmatrana ova vrsta napada, pri čemu je mreža u kojoj se nalazi napadnuti server povezana na Internet.

DoS napad se zasniva na intenzitetu generisanog saobraćaja, a ne na njegovom sadržaju, tako da napadač može da generiše saobraćaj koji je sličan legitimnom saobraćaju što otežava rad mehanizama odbrane. Da bi napad bio uspešan potrebno je da bude generisan veliki intenzitet saobraćaja. Korišćenjem višestrukih izvora u DDoS napadu povećava se intenzitet napada i neophodni su složeni mehanizmi odbrane. U tipičnom DDoS napadu razlikuju se dve faze, kako je prikazano na slici 4.2 [91]. U prvoj fazi napadač koristi propuste i ranjivosti njemu dostupnih sistema i preuzima nad njima kontrolu pri čemu ih pretvara u „zombije“. U drugoj fazi napadač slanjem komande diriguje napad na žrtvu, pri čemu napadač falsifikuje IP adresu izvora saobraćaja i time onemogućava identifikaciju izvora napada. Broj distribuirano kontrolisanih izvora saobraćaja se može kretati od desetine do stotinu ili čak više hiljada kompromitovanih klijenata.



Slika 4.2. Struktura tipičnog DDoS napada.

Za potrebe izvođenja DDoS napada „zombi“ računari se organizuju u *BotNet* – „zombi“ mrežu koju je moguće daljinski kontrolisati. Napadi su kontrolisani automatizovanim softverom tako da broj kompromitovanih računara može biti uvećan u kratkom vremenskom periodu, na primer, preuzimanje kontrole instalacijom zlonamernog

softvera koji se kasnije aktivira prema potrebi. Osnovni cilj je da „kontrola“ ostane nevidljiva za korisnika, zbog čega se često koristi komunikacija putem IRC (*Internet Relay Chat*) kanala [91], [92]. Komponenta zlonamernog softvera se povremeno priključuje na neki javni IRC kanal sa koga dobija dalje instrukcije. Ovo nije jedini način kontrole, suština je da komponenta zlonamernog softvera pokrene konekciju ka nekom uobičajenom servisu i tako ostane neprimećena i odobrena od *firewall*-a.

Intenzitet DDoS napada ogleda se u tome da [91]:

- intenzitet generisanog zlonamernog saobraćaja može lako zauzeti resurse jedne mreže i prevazići korisni protok većine uređaja;
- paketi koji predstavljaju napad mogu doći sa različitih geografskih lokacija što dodatno otežava pronalaženje izvora napada;
- za postizanje snažnog napada saobraćaj koji se generiše na svakom od „zobmija“ može delovati kao legitiman saobraćaj što otežava filtriranje i selekciju neželjenog od legitimnog saobraćaja.

Intenzitet napada se definiše kao nivo zauzetosti resursa koji je posledica napada i sastoji se iz dva parametra: intenziteta saobraćaja koji je predstavljen brojem paketa u periodu vremena i zauzeća resursa po paketu koje može biti predstavljeno procesorskim vremenom ili memorijom potrebnom za opsluživanje paketa.

Trenutno ne postoji sveobuhvatni metod zaštite od svih poznatih oblika DDoS napada. Moguća rešenja zaštite se mogu svrstati u [14], [90]:

- preventivne, koja se zasnivaju na filtriranju u cilju sprečavanja napada;
- reaktivne, čiji je cilj da identifikuju napadača kada je napad već izvršen;
- mehanizme nakon izvršenog napada koji uključuju primenu forenzičke analize telekomunikacione mreže.

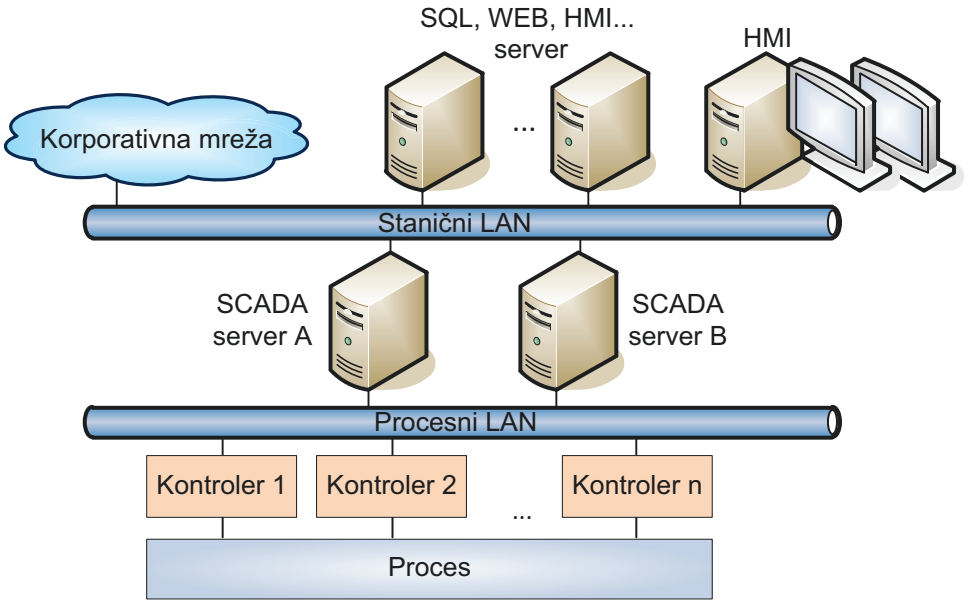
Postojeće tehnike zaštite ne pružaju dovoljnu bezbednost od DDoS napada, tako da ova vrsta napada na infrastrukturu telekomunikacione mreže predstavlja najozbiljniju pretnju savremenim IP mrežama, ujedno i telekomunikacionim mrežama u industrijskim sistemima daljinskog upravljanja.

4.2. Simulacioni model i rezultati simulacije

Strategije simulacije i modelovanja mogu se koristi za otkrivanje ranjivosti sistema daljinskog upravljanja i za određivanje stepena zaštite od mogućeg napada [93], [94]. Detaljna analiza metoda simulacije koji su primenjeni u stručnoj literaturi za određivanje efikasnosti sistema protiv sajber napada može se naći u [94].

U analizi koja je ovde prezentovana korišćen je programski alat OPNET (*Optimized Network Engineering Tool*) *IT Guru Academic Edition* koji predstavlja virtuelno mrežno okruženje za modelovanje, simulaciju i analizu različitih mrežnih topologija, uz izbor odgovarajućih mrežnih uređaja, linkova, protokola i aplikacija. OPNET obezbeđuje simulaciju karakteristika modelovane mreže, prikupljanje odgovarajuće statistike kao i grafički prikaz dobijenih rezultata.

Na slici 4.3 je šematski prikazana koncepcija arhitekture SCADA sistema u jednoj elektrani koja je poslužila za modelovanje topologije mreže u simulacionom modelu [95]. U modelu omogućena je integracija SCADA mreže u korporativnu telekomunikacionu mrežu. Na taj način se operaterska mesta mogu implementirati i na klijentima poslovne mreže korišćenjem, na primer, veb aplikacija [96]. Treba napomenuti da je korporativna mreža povezana na Internet.



Slika 4.3. Arhitektura SCADA sistema.

Simulacija je izvedena kroz dva scenarija:

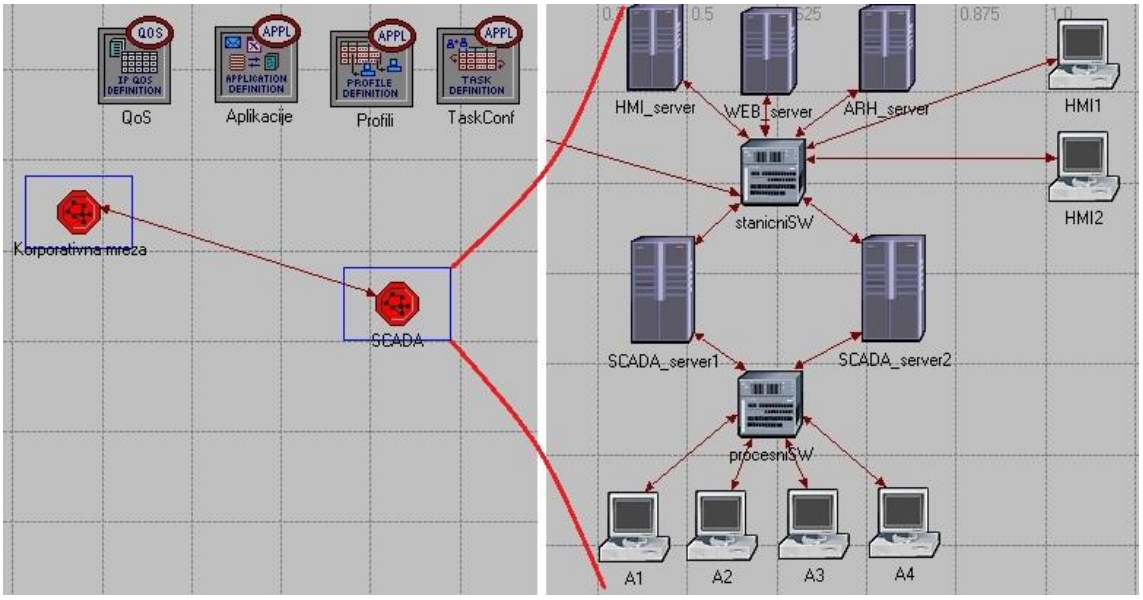
- model bez napada na infrastrukturu mreže;
- model u uslovima DDoS napada.

U prvom scenariju simulacioni model je kreiran definisanjem topologije mreže i modela saobraćaja koji postoji u uslovima bez napada. Drugi scenario je nastao kopiranjem prvog pri čemu je simulacioni model saobraćaja proširen saobraćajnim profilom koji simulira DDoS napad. Pretpostavka je da je zlonamerni korisnik već preuzeo kontrolu nad „zombi“ mrežom računara koji se nalaze u korporativnoj mreži. U oba scenarija simulacija traje 150 s, pri čemu je u drugom scenariju pretpostavljeno da DDoS napad počinje u 100-toj sekundi od početka simulacije.

Topologiju mreže čine čvorovi međusobno povezani linkovima. Model ima dve podmreže. Prvu čine čvorovi korporativne mreže, a drugu čvorovi sistema za daljinski nadzor i upravljanje elektranom. Telekomunikaciona mreža SCADA sistema je modelovana bez agregacije i čine je stanični deo mreže sa serverima i računarima za vizuelizaciju procesa i procesni deo mreže sa daljinskim stanicama za upravljanje agregatima i pomoćnim sistemima elektrane. SCADA serveri imaju dva mrežna interfejsa (simulacioni objekat je kreiran korišćenjem *Device Creator* opcije OPNET alata). Na slici 4.4 je prikazan deo topološkog modela kojim je modelovan sistem za nadzor i upravljanje u elektrani. Korporativni deo mreže čini 50 klijenata od kojih 20 predstavlja *BotNet* mrežu.

Operativni servis daljinskog upravljanja karakteriše prenos pogonskih podataka u realnom i van realnog vremena za potrebe izveštavanja. U simulacionom modelu se ističu tri toka saobraćaja:

- unutar mreže sistema za daljinski nadzor i upravljanje;
- između korporativne mreže i SCADA sistema;
- saobraćaj koji je rezultat DDoS napada.



Slika 4.4. Topologija dela mreže za daljinski nadzor i upravljanje u simulacionom modelu.

Za SCADA saobraćaj su definisana tri profila zasnovana na FTP (*File Transfer Protocol*) aplikaciji koja koristi pouzdan transportni servis, realizovan posredstvom TCP protokola:

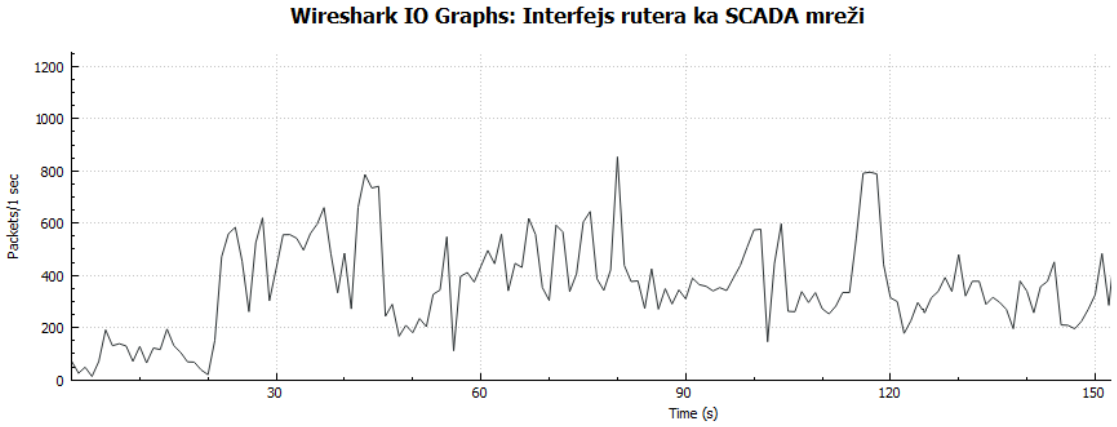
- slanje rezultata merenja iz pogona ka dispečerskom centru: vreme ponavljanja događaja je konstantan kratak period, a količina podataka odgovara uniformnoj raspodeli u opsegu manjih vrednosti;
- razmena signala alarma i komandi između dispečerskog centra i pogona: saobraćaj se generiše u skladu sa Poasonovom raspodelom;
- razmena izveštaja između SCADA sistema: vreme ponavljanja je konstantan duži period, a količina podataka odgovara uniformnoj raspodeli u opsegu većih vrednosti.

U drugoj grupi saobraćaja karakteristične su:

- veb aplikacije pomoću kojih se na klijentima korporativne mreže dobija vizuelni prikaz procesa i potrebni izveštaji;
- prenos podataka ka nadređenim i drugim centrima daljinskog nadzora;
- pristup serverima za potrebe konfigurisanja sa klijenata korporativne mreže.

Saobraćaj je modelovan korišćenjem standardnih aplikacija (*Database*, FTP, Web) u sedam različitih profila.

U čvoru realne mreže je izvršeno snimanje saobraćaja pomoću mrežnog analizatora *Wireshark*. Ovaj slobodno dostupan program prvenstveno služi za snimanje paketa koji se prenose kroz mrežu sa dovoljno detalja koji omogućuju kasniju analizu. Program pruža mogućnost filtriranja paketa po različitim kriterijumima, analizu i dobijanje statističkih podataka [97]. Analiziran je saobraćaj na interfejsu rutera u elektrani kako bi se na osnovu njega modelovao legitimni saobraćaj. Na slici 4.5 je prikazan deo rezultata dobijen mrežnim analizatorom.



Slika 4.5. Rezultati snimanja saobraćaja na interfejsu rutera.

Za DDoS napad je izabrana varijanta UDP (*User Datagram Protocol*) „plavljenja“, a zlonamerni saobraćaj je modelovan pomoću korisnički definisane aplikacije. Za tu namenu je definisan zadatak korišćenjem objekta *Task Configuration*, pri čemu tok saobraćaja postoji samo od izvora ka odredištu i zasnovan je na UDP transportnom protokolu. Za metu napada je izabran SCADA server.

U multiservisnim mrežama se primenjuje disciplina opsluživanja paketa kao jedna od tehnika kojom se postiže kontrola zagušenja. To je mehanizam zadužen za multipleksiranje paketa iz više tokova ili klasa saobraćaja po zajedničkom izlaznom linku i za kontrolu čekanja paketa u izlaznom redu rutera, pre prosleđivanja sledećem elementu mreže. U simulacionom modelu je pretpostavljeno da se primenjuje WFQ (*Weighted Fair Queuing*) disciplina [98], a saobraćaj u korisničkoj ravni je klasifikovan

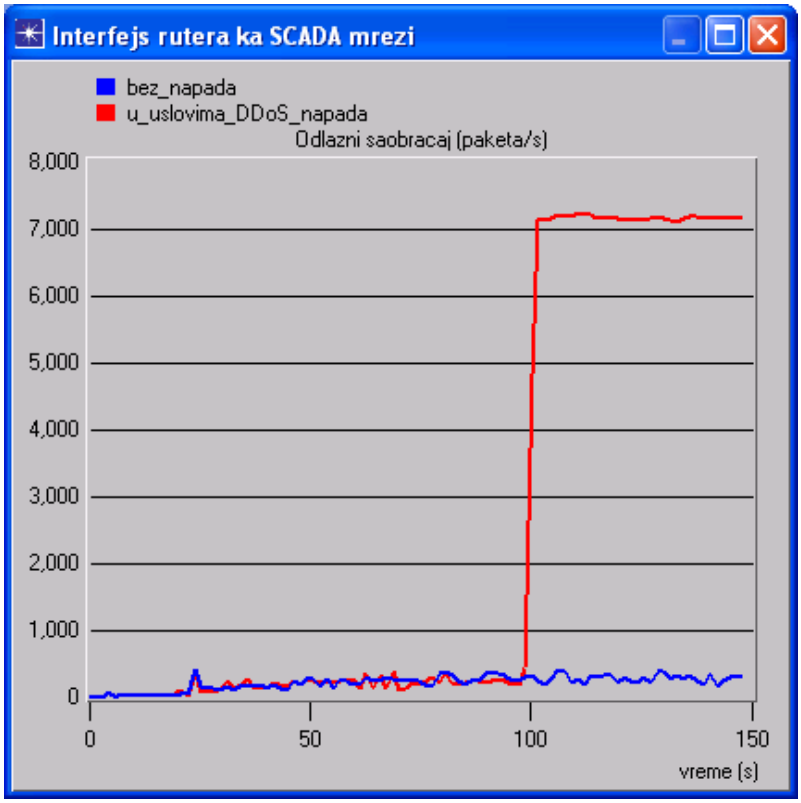
u četiri klase prioriteta, prema vrednosti polja ToS (*Type of Service*), pri čemu je operativnom servisu daljinskog upravljanja pridružen najviši prioritet.

Ovako definisan simulacioni model pruža mogućnosti iscrpne analize performansi telekomunikacione mreže. Servis daljinskog upravljanja postavlja određene zahteve za performanse u telekomunikacionoj mreži. Ovo nije vremenski kritičan servis jer je dozvoljeno kašnjenje do 1s, ali postavlja stroge zahteve za raspoloživost servisa koja treba da bude veća od 99,98% [99].

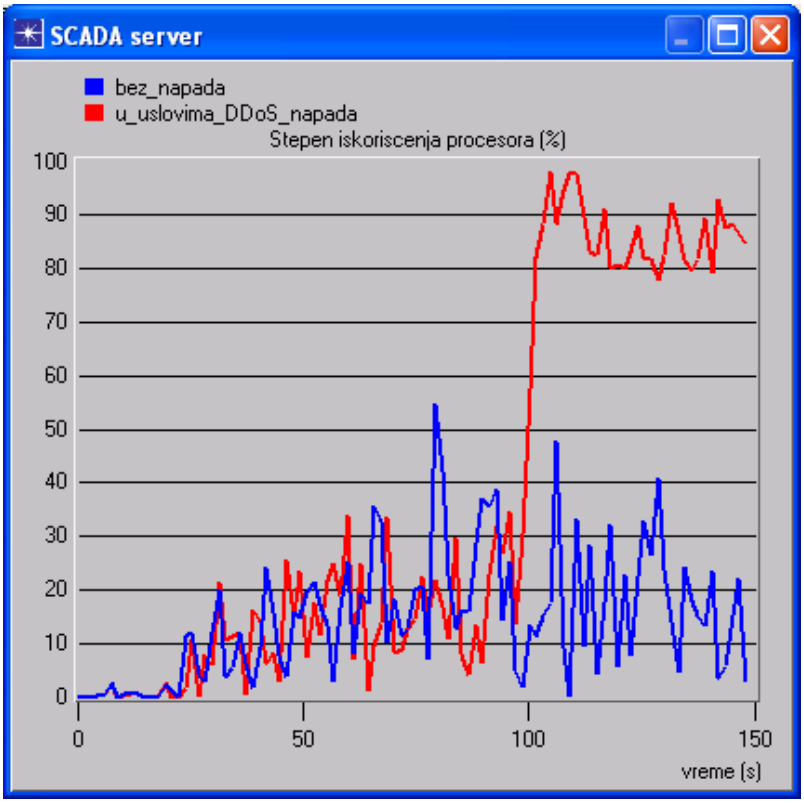
Grafički prikaz rezultata simulacije je dat u nastavku. Na slici 4.6 je dat grafički prikaz odlaznog saobraćaja na interfejsu rutera ka SCADA mreži, a na slici 4.7 stepen iskorišćenja procesora mete napada. Na grafičkim prikazima se vidi trenutak početka DDoS napada.

Uticaj napada na operativni servis daljinskog upravljanja je ilustrovan na slikama 4.8 i 4.9 na kojima je dat grafički prikaz stepena odbacivanja paketa u redu čekanja u kome se opslužuje operativni servis daljinskog upravljanja i kašnjenja TCP paketa na SCADA serveru, respektivno.

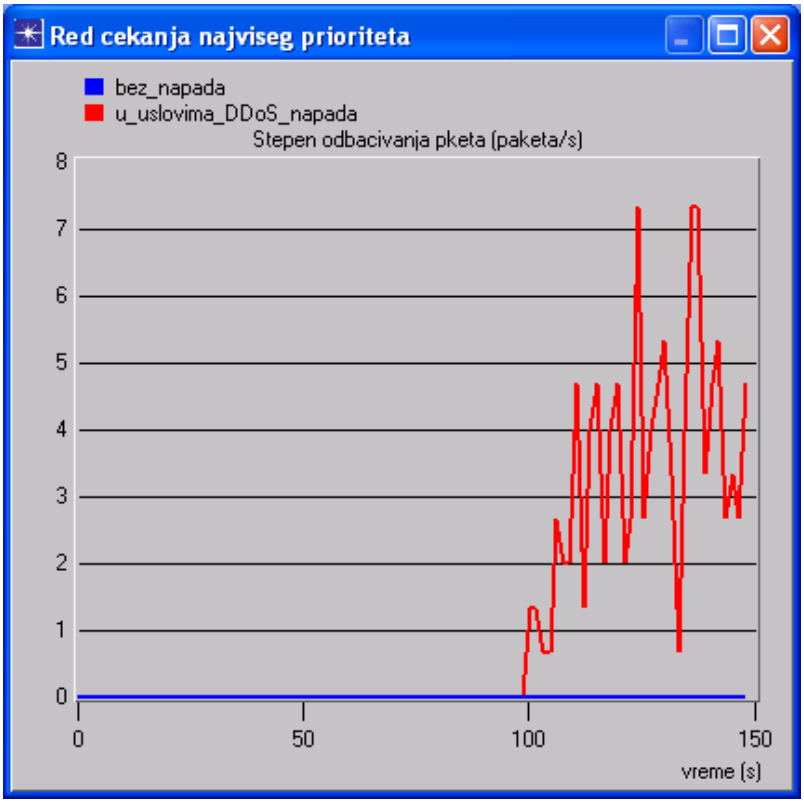
Analizom rezultata se zaključuje da je veliki intenzitet dolaznog zlonamenog saobraćaja prouzrokovao blokadu resursa SCADA servera koji je predstavljao žrtvu napada, što se vidi kroz zauzetost procesorskog vremena preko 80%. U trenutku početka napada, usled zagušenja, počinje odbacivanje paketa na interfejsu rutera ka delu mreže u kojoj se nalazi meta napada, pa se stepen odbačenih paketa koji pripadaju saobraćajnom toku operativnog servisa daljinskog upravljanja povećava i iznosi oko 3,6 % u odnosu na ukupan saobraćaj u redu najvišeg prioriteta. Istovremeno se povećava i kašnjenje u obradi zahteva legitimnog saobraćaja.



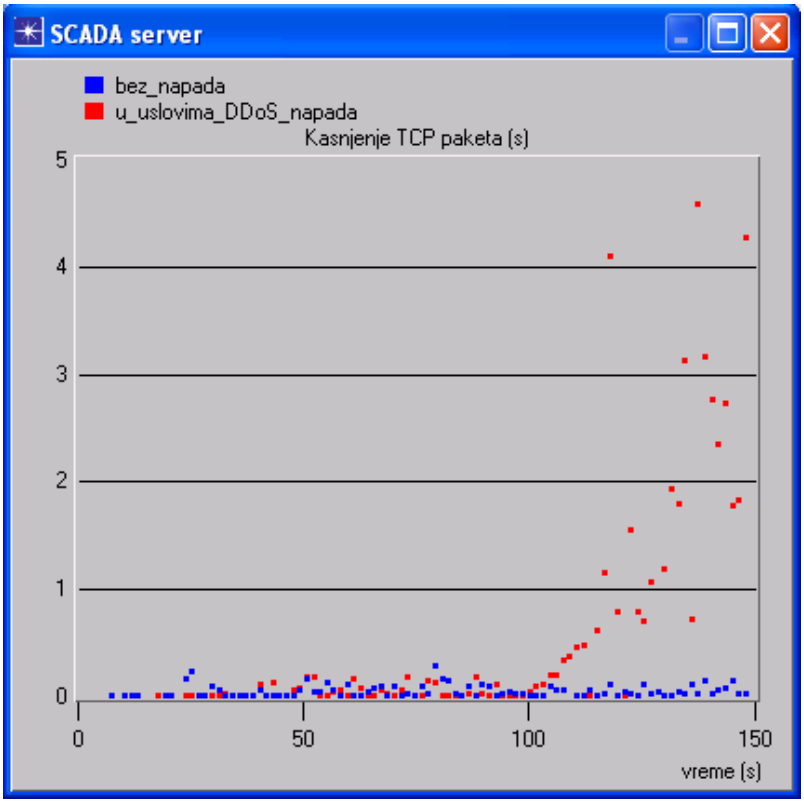
Slika 4.6. Odlazni saobraćaj ka SCADA mreži.



Slika 4.7. Stepen iskorišćenja procesora mete napada.



Slika 4.8. Stepen odbacivanja paketa servisa daljinskog upravljanja.



Slika 4.9. Kašnjenje TCP paketa u čvoru žrtve napada.

5. PREDLOG KVANTITATIVNIH PARAMETARA I METODA PROCENE BEZBEDNOSNOG RIZIKA U INDUSTRIJSKIM SISTEMIMA DALJINSKOG UPRAVLJANJA

U ovom poglavlju predloženi su metodi procene bezbednosnog rizika i način izbora parametara za kvantifikaciju gubitaka koji su posledica sajber napada na infrastrukturu industrijskog sistema daljinskog upravljanja. Predložena su dva metoda: (1) osnovni metod u kome se kvantitativni parametri određuju na osnovu statističke analize relevantnih arhiviranih veličina i (2) hibridni metod u kome se kvantitativni parametri osim statističkom analizom arhiva određuju i na osnovu mišljenja relevantnih stručnjaka. U zavisnosti od primene metoda predložena su dva načina izražavanja mere rizika, kvalitativno i monetarno. Završna faza metoda je odabir mehanizama zaštite i *cost/benefit* analiza implementacije preventivnih mera na osnovu procenjene mere rizika. Rezultati istraživanja publikovani su u radovima [100] i [101].

5.1. Predlog metoda procene bezbednosnog rizika zasnovanog na analizi arhivskih podataka

Predložen metod [100] zasniva se na činjenici da je rizik srazmeran gubicima koji su posledica sajber napada na infrastrukturu industrijskog sistema daljinskog upravljanja.

Ukupni gubici nastali usled realizovanog napada se mogu klasifikovati u dve grupe:

- direktni gubici, (*DL – Direct Loss*), koji su posledica prekinutog proizvodnog procesa;
- indirketni 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.

Metod polazi od osnovne formule (3.1) za godišnji očekivani gubitak *ALE*. Na osnovu dobijene vrednosti i očekivanih ulaganja u mehanizme zaštite moguće je odrediti povrat

investicije u bezbednost informacione i komunikacione infrastrukture *ROSI* i donošenje odluke o optimalnoj zaštiti.

Predloženi metod se izvršava u sledećim koracima:

- definisanje konfiguracije sistema i scenarija otkaza;
- identifikovanje i proračun direktnih gubitaka;
- identifikovanje indirektnih gubitaka i određivanje vrednosti težinskih faktora;
- određivanje mere rizika i *ALE*;
- odabir mehanizma zaštite i proračun investicije uložene u zaštitu;
- određivanje *ROSI* i optimalnog praga ulaganja u mehanizme zaštite.

5.1.1. Definisanje konfiguracije sistema i scenarija otkaza

U ovom koraku je potrebno da se izvrši analiza industrijskog sistema daljinskog upravljanja za koji se vrši procena rizika. Cilj ovog koraka je da se dobije pojednostavljen model sistema, njegovih komponenti koje su podložne sajber napadu kao i međusobnim vezama i putevima kojima se napad može propagirati. S obzirom da posmatran sistem ima veze sa drugim sistemima, kako industrijskim sistemima daljinskog upravljanja, tako i korporativnim informacionim sistemima i Internetom, važno je da model prikaže sve veze sa okruženjem. Značajno je i da se identifikuju i označe potencijalne ranjivosti sistema.

Redundantnost sistema sa aspekta sajber napada ne pruža povećanu bezbednost, jer su sve komponente podjednako podložne napadu, te ih u modelu treba izostaviti. Potrebno je da se u model unesu postojeći mehanizmi zaštite.

Model treba da pruži odgovore na sledeća pitanja:

- Koje su komponente podložne sajber napadu?
- Koji su potencijalni ulazi za napad?

Scenario otkaza treba da pruži odgovore na sledeća pitanja:

- Kako je ugrožena primarna funkcija fizičkog procesa kojim se upravlja?
- Koliki je stepen uticaja komponente na otkaz?

5.1.2. Identifikovanje i proračun direktnih gubitaka

Gubitak koji nastaje prilikom realizacije sajber napada se, prema osnovnoj formuli za očekivani godišnji gubitak računa kao proizvod vrednosti dobara i faktora izloženosti riziku. U slučaju sajber napada na infrastrukturu industrijskog sistema daljinskog upravljanja vrednost koja je izložena riziku se oslikava kroz funkcionisanje sistema. Iz prethodno navedenog, sledi da se za vrednost gubitaka može uzeti gubitak u proizvodnom procesu (u konkretnom primeru to je proizvedena električna energija u proizvodnom elektroenergetskom postrojenju, preneta električna energija u slučaju elektroenergetskog preduzeća za prenos, isporučena energija u slučaju distributivnog preduzeća, preneta i isporučena količina gasa preduzeća za prenos i dietribuciju gasa, isporučena količina vode za vodovod, i slično). Ovi gubici se mogu izraziti monetarno, pa se oni uzimaju za osnovni činilac pri proračunu očekivanog godišnjeg gubitka.

Pretpostavlja se da ovakvih direktnih gubitaka može biti više vrsta. Cilj ovog koraka je da se identifikuju svi direktni gubici koji nastaju usled prekida ili ometanja proizvodnog procesa. Ukupni direktni gubici, usled smanjenog ili prekinutog procesa kojim upravlja industrijski sistem daljinskog upravljanja koji je meta sajber napada, se definišu kao suma pojedinačnih direknih gubitaka DL_j kojih može biti M:

$$DL = \sum_{j=1}^{M} DL_j. \tag{5.1}$$

Da bi se odredio gubitak nastao usled infrastukturnog sajber napada na industrijski sistem daljinskog upravljanja uzimaju se maksimalni direktni gubici koji nastaju u slučaju napada najvećeg intenziteta.

Skaliranje pretpostavljenih maksimalnih direktnih gubitaka u slučaju napada najvećeg intenziteta i najgoreg scenarija otkaza postiže se uvođenjem težinskog faktora $W_A \leq 1$. Metodologija proračuna vrednosti ovog faktora prikazana je u sledećem poglavlju u kome se opisuje određivanje vrednosti težinskih faktora.

5.1.3. Identifikovanje indirektnih gubitaka i određivanje vrednosti težinskih faktora

Značajni gubici koji su posledica napada na infrastrukturu industrijskog sistema daljinskog upravljanja su indirektni gubici. Posledice napada se mogu klasifikovati u nekoliko grupa, kako je to prikazano u tabeli 5.1.

Tabela 5.1. Klasifikacija indirektnih posledica napada na infrastrukturu industrijskog sistema daljinskog upravljanja

Grupa	**Opis posledice**
Operativnost	Uskraćivanje usluge većem ili manjem broju korisnika.
Zaštita životne sredine	Trajne ili privremene posledice koje ugrožavaju životnu sredinu i zdravlje ljudi.
Bezbednost i zdravlje na radu	Povrede sa smrtnim ishodom ili trajnim invaliditetom; stres; duža ili privremena sprečenost za rad; povrede koje zahtevaju ukazivanje medicinske pomoći.
Reputacija	Zastupljenost u medijima; gubitak podrške javnosti; bruka državnih organa; zahtevi javnog mnjenja za ostavkom ogovornih lica; prigovori korisnika.
Zakonodavstvo	Gubitak licence; pravni postupci i sudske presude protiv odgovornih lica; administrativne mere i upozorenja od strane nadležnih institucija i regulatornih tela.

Posledice, bez obzira kojoj grupi pripadaju, prouzrokuju određene finansijske gubitke, sa razlikom što su gubici za neke grupe merljivi, a za neke se ne mogu izmeriti i prikazati monetarnom vrednošću. Posledice koje se ne mogu monetarno izmeriti su često pogubnije i imaju veću težinu za privrednu organizaciju čiji je sistem bio meta napada, ali i šire jer su ovi sistemi deo kritične infrastukture.

Svakoj od posledica se može pridružiti stepen značaja, na primer: beznačajna, mala, srednja, velika ili katastrofalna posledica.

Ovo su indirektni gubici koji mogu biti posledica nekog od razloga koji su klasifikovani u tabeli 5.1, a nisu direktna posledica prekida proizvodnog procesa. Primer takvih troškova su plaćanja po merama zakonodavca zbog nedostavljanja izveštaja državnim službama, a posledica je zaštite (izolovanja) kontrolne mreže u uslovima infrastrukturnog napada. Težina posledice zavisi od uslova u kojima se dogodio napad. Uslova, koji mogu dovesti do indirektnih gubitaka, može biti N. Svaki pojedinačni indirektni gubitak se može predstaviti u funkciji maksimalnog direktnog gubitka. Potrebno je da se odredi težinski faktor $W_k \geq 1$, koji kvantifikuje indirektan gubitak koji

je posledica uzroka k, (k = 1, 2, …, N).. 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 [102].

Nakon izbora vrste težinskih faktora potrebno je odrediti njihove vrednosti. Ovo obuhvata analizu arhiviranih podataka kako bi se dobile statističke vrednosti i da bi se odredila verovatnoća nastanka uslova koji utiču na indirektne gubitke i verovatnoća pojave napada. Oslanjajući se na te rezultate, trebalo bi predvideti efekte napada na ukupne gubitke (direktne i indirektne). Ovim postupkom se dobija objektivna vrednost težinskih faktora.

Postupak podrazumeva prvo identifikaciju veličina koje se mere i arhiviraju, i na osnovu kojih se može opisati stanje procesa sa aspekta ugroženosti od sajber napada. Izabrane veličine treba da obezbede procenu stepena ugroženosti u uslovima koji doprinose povećanju indirektnog troška čiji se težinski faktor određuje. Drugi korak podrazumeva određivanje broja stepena ugroženosti (S) i graničnih vrednosti za izabranu veličinu koje definišu stepene ugroženosti.

Ukoliko više veličina određuje jedan težinski faktor, postupak određivanja opsega za stepen ugroženosti se sprovodi za svaku veličinu i određuje se pripadnost opsezima za svaku veličinu nezavisno. Zatim se definišu uzročno-posledična pravila koja povezuju više veličina i definišu grupnu pripadnost stepenu ugroženosti. Primer definisanja uzročno posledičnih pravila prikazan je u tabeli 5.2.

Tabela 5.2. Primer definisanja uzročno posledičnih pravila

Druga veličina \ Prva veličina		Mali	Srednji	Veliki
		Stepen ugroženosti		
Stepen ugroženosti	Mali	Zanemarljiv	Mali	Srednji
	Srednji	Mali	Srednji	Veliki
	Veliki	Srednji	Veliki	Veoma veliki

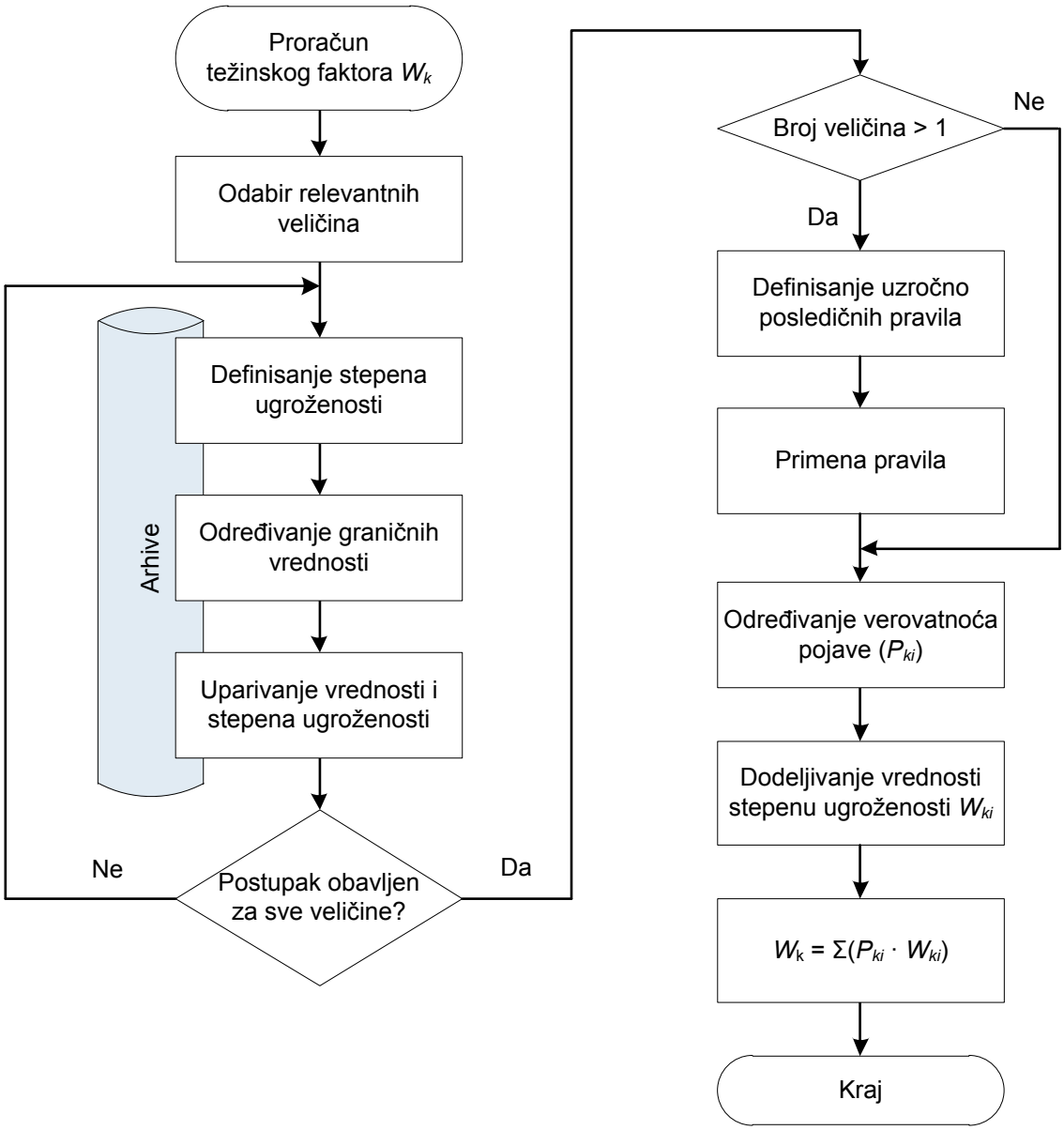
Sledeći korak je određivanje raspodele verovatnoće da veličina uzme vrednost koja pripada određenom opsegu, a rezultat je niz verovatnoća P_{ki}, (i = 1, 2, …, S). To je verovatnoća da veličina koja određuje težinski faktor W_k uzme vrednost iz i-tog opsega. Za svaki stepen ugroženosti se definiše koliki je težinski faktor W_{ki} (i = 1, 2, …, S) u skladu sa minimalnim i maksimalnim indirektnim troškovima koji su posledica konkretnog uslova u kojima se realizuje napad na infrastrukturu.

Konačna vrednost težinskog faktora W_k dobija se na sledeći način:

$$W_k = \sum_{i=1}^{S} (P_{ki} \times W_{ki}). \tag{5.2}$$

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.

Dijagram toka određivanja vrednosti jednog težinskog faktora prikazan je na slici 5.1.



Slika 5.1. Dijagram toka određivanja vrednosti težinskog faktora W_k.

5.1.4. Određivanje mere rizika i ALE

U literaturi je čest slučaj da se rizik iskazuje kvalitativno, na primer kao nizak, srednji ili visok. U skladu sa nivoom rizika preporučuju se adekvatne aktivnosti sprovođenja mera i implementacije mehanizama zaštite. Sa druge strane, u cilju *cost/benefit* analize rizik je potrebno izraziti monetarno. U predloženom metodu, mera rizika se prvo

izražava samo na osnovu vrednosti težinskih faktora, a nakon toga se izračunavaju i očekivani pojedinačni i godišnji gubici.

Množenjem svih težinskih faktora određenim u prethodnom koraku dobija se bezdimenziona veličina koja predstavlja meru rizika *R*:

$$R = W_A \prod_{k=1}^{N} W_k \,. \tag{5.3}$$

U cilju kvalitativnog izražavanja mere rizika potrebno je da se usvoji relacija koja povezuje opsege vrednosti *R* sa stepenom rizika (tabela 5.3).

Tabela 5.3. Primer relacije za kvalitativnu predstavu nivoa rizika

Stepen rizika	**Vrednost mere rizika**
Veoma nizak	$R \leq 1$
Nizak	$1 < R \leq 1{,}5$
Srednji	$1{,}5 < R \leq 3$
Visok	$3 < R \leq 5$
Veoma visok	$R > 5$

Na kraju, u cilju monetarne predstave rizika primenjuje se sledeća formula za obračun pojedinačnih gubitaka *SLE*:

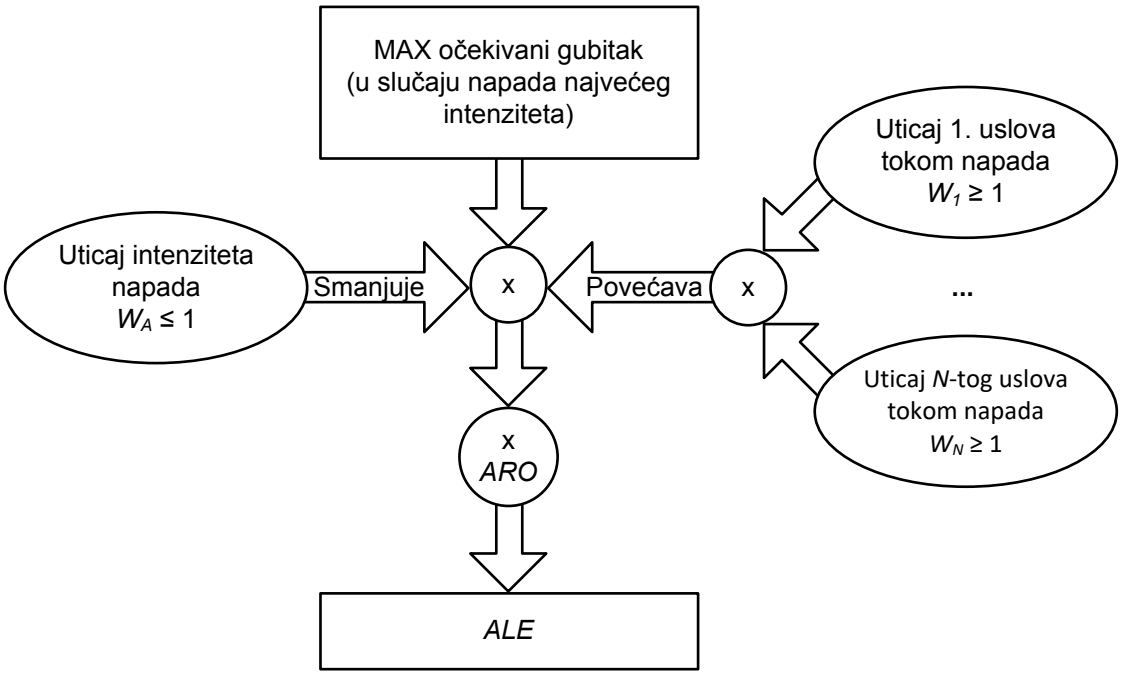
$$SLE = R \times DL = R \times (\sum_{j=1}^{M} DL_j) = W_A \prod_{k=1}^{N} W_k \, (\sum_{j=1}^{M} DL_j). \tag{5.4}$$

Pojedinačni gubitak je srazmeran sumi maksimalnih direknih troškova *DL*. Formula se modifikuje težinskim faktorima koji kvantifikuju indirektne troškove (W_k) i težinskim faktorom W_A čija je uloga da skalira maksimalne direktne troškove u funkciji intenziteta napada, odnosno merom rizika *R*.

Primenom formule (3.1) izračunava se očekivani godišnji gubitak *ALE* usled infrastukturnog sajber napada:

$$ALE = SLE \times ARO = W_A \prod_{k=1}^{N} W_k \, (\sum_{j=1}^{M} DL_j) \times ARO. \tag{5.5}$$

Na slici 5.2 dat je šematski prikaz toka proračuna.



Slika 5.2. Faktori *ALE* u SCADA sistemima.

Izbor kvalitativne ili monetarne predstave rizika zavisi od konkretnog sistema i namene metoda procene rizika.

5.1.5. Odabir mehanizma zaštite i proračun investicije u zaštitu

U skladu sa vrstom napada koji se posmatra bira se odgovarajuća zaštita. U ovom istraživanju pažnja je usmerena na infrastrukturne napade kao što je DDoS, a preporučena zaštita je IDPS.

Radi procene vrednosti investicije u mehanizme zaštite, neophodno je da se posmatra duži vremenski period. Naime, investicija u mehanizme zaštite C_S sastoji se iz jednokratne početne investicije u impelementaciju mehanizma zaštite C_I i godišnjeg održavanja sistema zaštite koje obuhvata ažuriranje sistema i tehničku podršku C_M. S obzirom da je inicijalna investicija mnogo veća od troškova održavanja u narednim godinama, za vrednost ulaganja u mehanizme zaštite koristi se srednja vrednost investiranja u toku Y godina, počevši od prve godine investicije u zaštitu:

$$C_S = \frac{C_I + \sum_{i=1}^{Y} C_{Mi}}{Y}. \tag{5.6}$$

Ovako procenjena vrednost investicije u mehanizme zaštite je jedan od ulaznih parametara za sledeći korak, *cost/benefit* analizu.

5.1.6. Određivanje ROSI i optimalnog praga

Proračunata vrednost očekivanog godišnjeg gubitka omogućuje *cost/benefit* analizu. U tom cilju se koristi parametar *ROSI*. Ovaj pokazatelj efektivnosti investicije u mehanizme zaštite predstavlja odnos ušteda usled ublažavanja rizika (*Mitigated Risk*) koje su ostvarene sprečavanjem sajber napada i cene implementirane zaštite C_S:

$$ROSI = \frac{ALE \times \%MitigatedRisk - C_S}{C_S}. \quad (5.7)$$

Definisanje prihvatljivog praga za povrat investicija u zaštitu omogućuje donošenje odluke o racionalnom ulaganju u povećanje bezbednosti industrijskog sistema daljinskog upravljanja.

5.2. Predlog hibridnog metoda procene bezbednosnog rizika zasnovanog na analizi arhivskih podataka i subjektivnoj oceni stručnjaka

Ovaj metod se zasniva na metodu opisanom u poglavlju 5.1., pri čemu se u proces procene bezbednosnog rizika uključuju stručnjaci i njihovo iskustvo [101]. Potreba za definisanjem hibridnog metoda se ukazala iz dva razloga, prvo što u nekim slučajevima arhive nisu raspoložive i drugo, što je prepoznata korist od korišćenja iskustva koje imaju stručnjaci raznih oblasti koji su suštinski povezani sa predmetnim industrijskim sistemom daljinskog upravljanja. Stručnjaci treba da budu iz različitih oblasti:

- poslovodstvo;
- informacione i komunikacione tehnologije;
- implementacija i održavanje sistema daljinskog upravljanja;
- operativno osoblje;
- naučno-istraživačka delatnost.

Ovim metodom se pored objektivne komponente, koja se dobija analizom arhivskih podataka, formira subjektivna komponenta vrednosti težinskih faktora uzimajući u obzir iskustvo i stav stručnjaka iz različitih oblasti, a koji dobro poznaju industrijski sistem daljinskog upravljanja.

Ukoliko arhive podataka nisu raspoložive, ostaje kao mogućnost da se sprovede samo anketa među stručnjacima. Tada težinski faktori imaju samo subjektivnu komponentu. Ukoliko postoje uslovi da se sprovedu obe faze, konačne vrednosti težinskih faktora se određuju upoređivanjem objektivne i subjektivne komponente, na osnovu procene kvaliteta svake faze.

Algoritam kojim je opisan postupak određivanja vrednosti težinskih faktora prikazan je na slici 5.3. Algoritam se sprovodi za svaki od težinskih faktora u dve faze. U prvoj fazi se određuje objektivna vrednost težinskog faktora W_{kO} na osnovu podataka iz raspoloživih arhiva zavisno od uslova koji je uzet za indirektni gubitak, kao što je opisano u poglavlju 5.1. Na osnovu arhiviranih vrednosti proračunava se verovatnoća raspodele pojave uslova u kojima bi realizovani infrastrukturni napad prouzrokovao indirektne troškove.

U drugoj fazi se anketiraju stručnjaci iz različitih oblasti. Anketa može imati jedno ili više pitanja (broj pitanja je označen sa Q). Lista pitanja se formira za konkretni SCADA sistem, pri čemu se definiše težinski faktor W_{qj} za svako pitanje, uz uslov $\Sigma W_{qj} = 1$, ($j = 1, 2, \ldots, Q$). Anketa je koncipirana tako da je za svako pitanje ponuđen konačan skup odgovora (npr. veoma malo, malo, srednje, veliko, veoma veliko) ili je ponuđen izbor na skali (npr. 1-5, 0-100%). Kvantifikacijom dobijenih odgovora (A_j) dobija se po jedan faktor W_{ki} za svakog stručnjaka:

$$W_{ki} = \sum_{j=1}^{Q} W_{qj} \times A_j, \left(\sum_{j=1}^{Q} W_{qj} = 1 \right). \tag{5.8}$$

Na osnovu anketa ukupno E stručnjaka dobija se niz težinskih faktora W_{ki}, ($i = 1, 2, \ldots, E$). Konačna, subjektivna, vrednost težinskog faktora W_{kS} određuje se na osnovu kompetentnosti svakog stručnjaka C_i :

$$W_{kS} = \sum_{i=1}^{E} C_i \times W_{ki}, \left(\sum_{i=1}^{E} C_i = 1 \right). \quad (5.9)$$

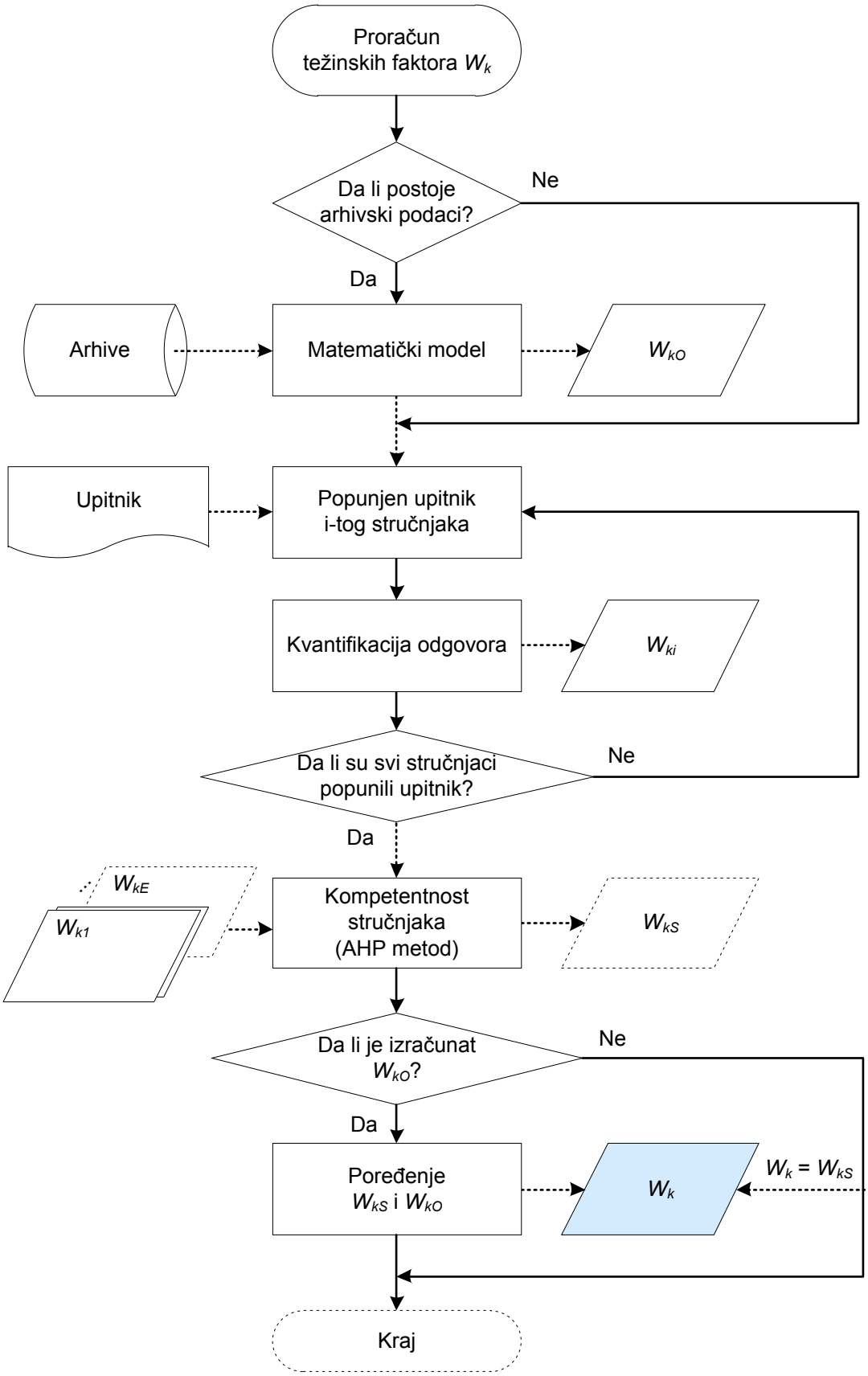
Određivanje kompetentnosti se vrši korišćenjem metoda AHP (*Analytical Hierarchical Process*) [103]. To je višekriterijumska procedura za donošenje odluka u kojoj se hijerarhijski predstavljaju kriterijumi i vrši rangiranje mogućih alternativa korišćenjem serija poređenja dva elementa unutar skale intenziteta odnosa (može imati 9 nivoa). Ovaj metod je pogodan zbog toga što je krajnji rezultat numerička ocena alternative (u ovom slučaju su to stručnjaci).

Dobijeni težinski faktor W_{kS} ima dva aspekta subjektivnosti: (1) izbor pitanja pri formiranju ankete i (2) iskustvo stručnjaka.

Na kraju se vrši poređenje i ocenjivanje faktora koji su dobijeni u dve faze, uz određivanje konačnog težinskog faktora W_k koji je matematička funkcija faktora W_{kO} i W_{kS}. Matematička funkcija dobija se nakon ocene kvaliteta svake faze. Za meru kvaliteta objektivne faze K_O relevantni su količina i kvalitet raspoloživih podataka u arhivi. Kvalitet podataka se procenjuje na osnovu izvora podataka, validnosti i tačnosti mernih metoda i dr. Kvalitet subjektivne faze K_S se procenjuje na osnovu iskustva stručnjaka koji su učestvovali u anketi, kao i na osnovu stepena sličnosti odgovora stručnjaka. U slučaju velike razlike u odgovorima, kvalitet dobijenog subjektivnog faktora je manji. Suma koeficijenata za ocenu kvaliteta faze je jednaka 1. Na kraju se konačna vrednost dobija na sledeći način:

$$W_k = K_O W_{kO} + K_s W_{kS}, (K_O + K_S = 1). \quad (5.10)$$

U slučaju da je sprovedena samo jedna faza, konačna vrednost težinskog faktora jednaka je vrednosti koja je dobijena u sprovedenoj fazi, objektivnoj ili subjektivnoj.



Slika 5.3. Algoritam za određivanje vrednosti težinskih faktora.

6. VERIFIKACIJA PREDLOŽENIH METODA

Problematika bezbednosti SCADA sistema u kritičnoj infrastrukturi je takva da sprovođenje javnih anketa radi prikupljanja podataka o prethodnim bezbednosnim incidentima i iskustvima o bezbednosnoj politici i praksi nije uobičajeno, pre svega zbog poverljivosti ovih informacija i čuvanja poslovne tajne. Informacije ovog tipa u informacionim sistemima opšte namene su dostupnije i korisnici često učestvuju u anketama koje sprovode istraživači ili kompanije koje pružaju usluge. Podaci koji se odnose na bezbednost industrijskih sistema daljinskog upravljanja su često nedostupni i u toku naučno-istraživačkog rada je teško doći do njih. Poznato je da nema dovoljno konkretnih primera primene i verifikacije brojnih metoda procene bezbednosnog rizika u kritičnoj infrastrukturi. Ovo je razlog što se provera metoda u praksi često sprovodi simulacijama i u okruženju formiranom radi testiranja [64], [69], [75], [77], [79].

U ovom poglavlju je prikazana verifikacija predloženih metoda za procenu bezbednosnog rizika. Za testiranje metoda definisane su dve studije slučaja:

- studija slučaja u realnom okruženju protočne hidroelektrane i
- studija slučaja SCADA sistema u magistralnom gasovodu.

6.1. Polazne pretpostavke

U obe studije slučaja korišćene su iste polazne pretpostavke koje se odnose na DDoS napad. U literaturi [54] se navodi da se verovatnoća detektovanih napada od strane IDS sistema kreće u opsegu 61,5% do 86,2%. Kao što je istaknuto u poglavlju 2.5.1, 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 istraživanjima [104], [105] srednje vreme otkaza usled DDoS napada iznosi 30 minuta.

6.2. Studija slučaja u realnom okruženju protočne hidroelektrane

6.2.1. Konfiguracija sistema i scenario otkaza

Posmatrana je hidroelektrana ukupne instalisane snage 270 MW. Proizvodnja električne energije se obavlja sa deset jednakih hidroagregata, pri čemu je instalisana snaga generatora 27 MW.

Infrastrukturu SCADA mreže čine dve celine:

- mreža nadzora i upravljanja u kojoj su ključni serveri i operatorske stanice;
- procesna mreža u kojoj su kontroleri za nadzor i upravljanje agregatima i pomoćnim sistemima elektrane.

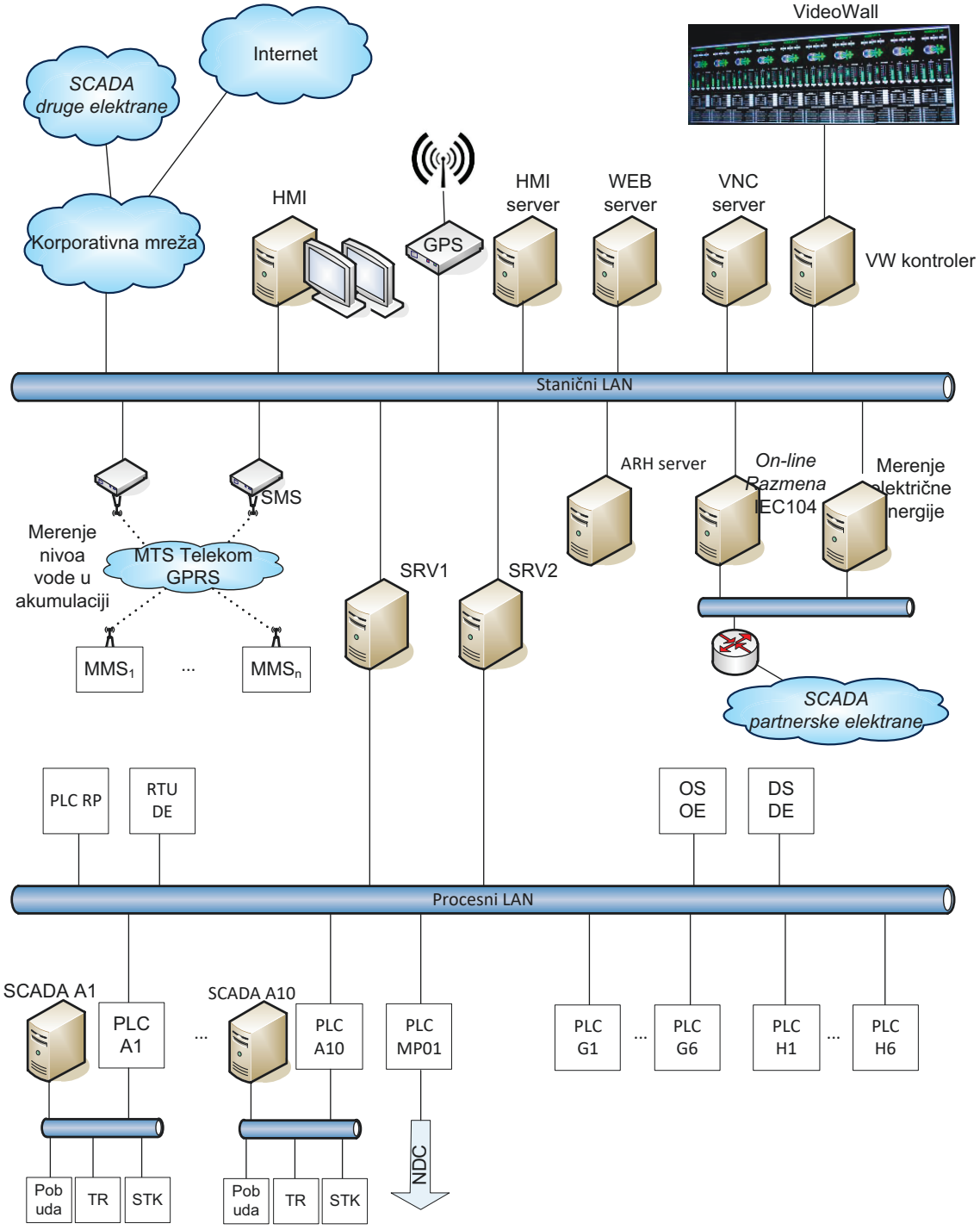
Mreža nadzora i upravljanja je povezana na korporativnu mrežu, koja ima vezu sa Internetom. Na slici 6.1 je prikazana arhitektura industrijskog sistema daljinskog upravljanja [106].

Prvi korak je da se izradi model sistema na osnovu arhitekture i analize rizika od infrastrukturnog napada, kao što je prikazano na slici 6.2. Segmenti mreže nadzora i upravljanja, kao i procesne mreže, nisu izolovani od korporativne mreže, niti od SCADA mreže partnerske elektrane. U uslovima infrastrukturnog napada veliki uticaj na upravljanje procesom bi imalo iskorišćenje resursa akvizicionih servera, kontrolera i mrežnih komponenti u procesnoj mreži.

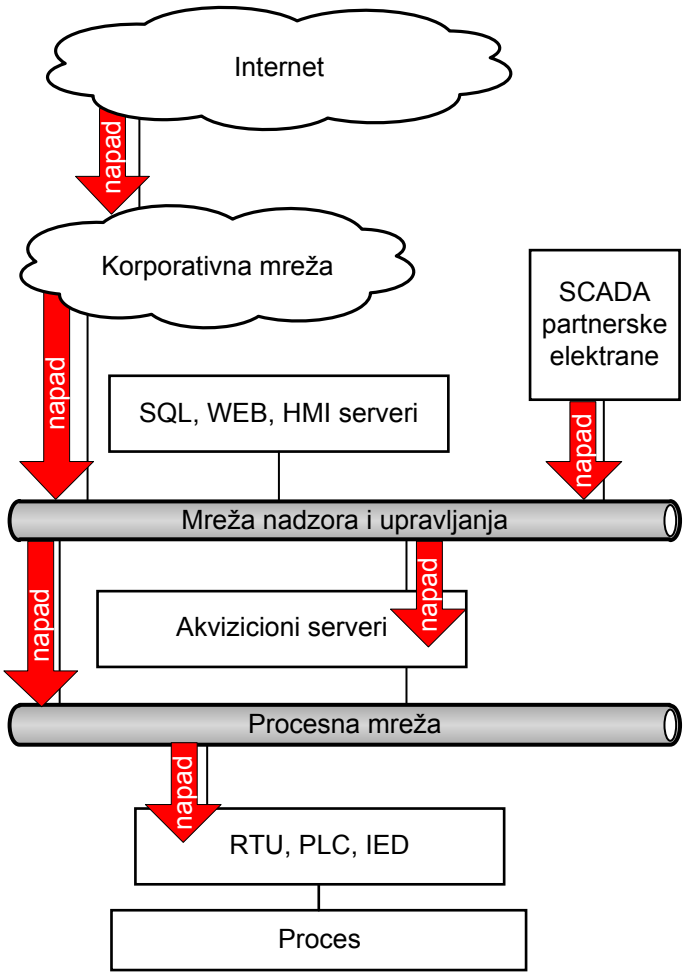
Scenario otkaza je prikazan na slici 6.3. Prvi nivo scenarija je faza kompromitovanja mreže u kojoj zlonamerni korisnik ostvaruje pristup klijentu korporativne mreže preko kojeg inicira DDoS napad koji može biti usmeren na akvizicione servere ili na kontrolere u procesnoj mreži. Posledice napada se mogu klasifikovati u više grupa:

- onemogućen nadzor i upravljanje iz nadređenog centra bez posledica na lokalno upravljanje i proizvodnju;
- onemogućen nadzor i upravljanje iz nadređenog i lokalnog upravljačkog centra bez prekida proizvodnje;
- uskraćeni svi servisi nadzora i upravljanja sa manjim uticajem na proizvodni proces;

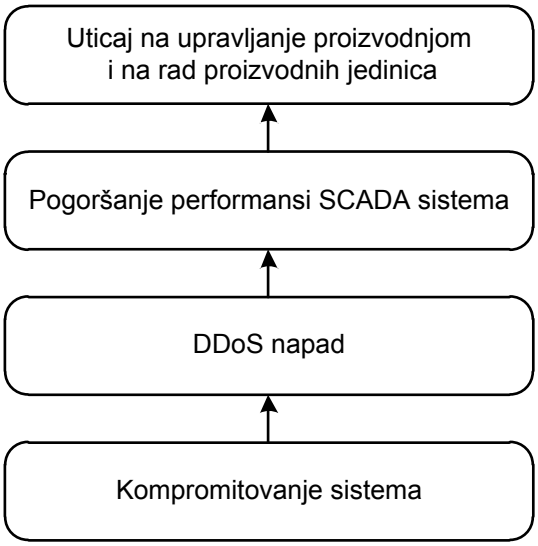
- uskraćeni svi servisi nadzora i upravljanja sa značajnim uticajem na proizvodni proces.



Slika 6.1. Arhitektura sistema za daljinsko upravljanje u hidroelektrani.



Slika 6.2. Model sistema za daljinsko upravljanje u hidroelektani sa aspekta rizika.



Slika 6.3. Scenario otkaza za slučaj hidroelektrane.

6.2.2. Primena metoda procene bezbednosnog rizika zasnovanog na analizi arhivskih podataka

Direktni i indirektni gubici

Analizirane su moguće posledice DDoS napada sa aspekta nadzora, upravljanja i proizvodnje električne energije, i posledično dve vrste troškova: direktnih i indirektnih. Direktni troškovi su posledica smanjene proizvodnje električne energije zbog:

- ispada proizvodne jedinice, ako je meta napada kontroler agregata;
- nemogućnosti regulacije snage usled otkaza servisa daljinskog upravljanja.

Direktni troškovi su srazmerni:

- trajanju napada (t_A);
- vremenu potrebnom za oporavak sistema (t_R);
- instalisanoj snazi elektrane (P);
- jediničnoj ceni električne energije (c_E).

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

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

Indirektni troškovi nastaju zbog:

- penala usled neispunjenih obaveza isporuke električne energije;
- gubitak hidropotencijala ukoliko je napad realizovan u vreme visokih dotoka.

Indirektni troškovi se kvantifikuju težinskim faktorima W_E i W_H, respektivno.

Primenom ovih pretpostavki na formulu (5.5) dobija se sledeći izraz za proračun godišnjih očekivanih gubitaka:

$$ALE = W_A\, W_E\, W_H\, P\, (t_A + W_A\, t_{Rmax})\, c_E \times ARO. \tag{6.1}$$

Napad se može dogoditi u bilo koje doba dana ili godine, zbog čega nije jednostavno unapred odrediti kakve bi efekte imao. Na primer, može se oceniti koliko bi se uvećali troškovi ukoliko bi, usled uskraćivanja servisa daljinskog upravljanja, došlo do prelivanja viška hidropotencijala. Prelivanje viška vode se, inženjerski i tehnološki,

smatra čistim gubitkom vodenog resursa i uvek se teži da se u takvim situacijama koriste maksimalni proizvodni kapaciteti kako bi se umanjila šteta.

Određivanje vrednosti težinskih faktora analizom arhivskih podataka

U ovom slučaju razmatrane su objektivne vrednosti dobijene statističkom analizom arhiviranih podataka o proizvodnji i dotocima. Za primenu metoda uzete su arhive za jednu referentnu godinu. Odabrane su sledeće veličine:

- dnevna proizvodnja električne energije za određivanje težinskog faktora W_E i
- dotok za određivanje težinskog faktora W_H.

Za oba slučaja definisano je po pet stepena ugroženosti, kao i odgovarajuće granične vrednosti opsega relevantnih veličina (tabela 6.1).

Tabela 6.1. Stepen ugroženosti usled napada

Grafički prikaz	**Stepen ugroženosti**	**Granične vrednosti za dnevnu proizvodnju (MWh)**	**Granične vrednosti za dotok (m^3/s)**
	Veoma mala ugroženost	< 3200	< 3100
	Mala ugroženost	3200 – 4200	3100 – 3500
	Srednja ugroženost	4200 – 4300	3500 – 4500
	Velika ugroženost	4300 – 5000	4500 – 5500
	Veoma velika ugroženost	> 5000	> 5500

Grafički prikaz relevantnih arhiviranih veličina dat je na slikama 6.4 i 6.5. Na grafičkim prikazima, bojama (prema tabeli 6.1) su označeni periodi sa različitim uticajima napada na infrastrukturu sistema za daljinsko upravljanje, u skladu sa stepenom ugroženosti.

Slika 6.4. Dnevna proizvodnja električne energije u referentnoj godini (MWh).

Slika 6.5. Dotok u referentnoj godini (m^3/s).

Na osnovu arhiva, određene su verovatnoće pojave uslova za dva faktora indirektnih gubitaka. Ovako dobijene verovatnoće i njima pridružene vrednosti faktora po stepenu ugroženosti prikazane su u tabeli 6.2.

Tabela 6.2. Težinski faktori indirektnih gubitaka hidroelektrane

Uticaj		**Veoma mali uticaj**	**Mali uticaj**	**Srednji uticaj**	**Veliki uticaj**	**Veoma veliki uticaj**
W_E	**Verovatnoća pojave (%)**	4,7	21,9	38,6	18,6	16,2
	Vrednost faktora	1,0	1,2	2,0	2,5	4,0
W_H	**Verovatnoća pojave (%)**	0,3	2,2	20,3	22,5	54,7
	Vrednost faktora	1,0	1,1	1,2	2,0	3,0

Na osnovu raspodele verovatnoće i dodeljenih vrednosti za težinske faktore, konačne vrednosti faktora W_E i W_H određene su na osnovu formule (5.2) i prikazane u tabeli 6.3.

Tabela 6.3. Konačna vrednost težinskih faktora indirektnih gubitaka hidroelektrane

Faktor	W_E	W_H
Vrednost	2,2	2,9

U tabeli 6.4 prikazana je raspodela verovatnoće i vrednost faktora W_A koji skalira intenzitet napada. U konkretnom primeru pretpostavljena je najveća verovatnoća napada manjeg intenziteta. Raspodela verovatnoća i vrednost težinskog koeficijenta definisana je uzimajući u obzir rezultate izveštaja [107].

Tabela 6.4. Faktor za skaliranje intenziteta napada

Intenzitet		**Veoma mali intenzitet**	**Mali intenzitet**	**Srednji intenzitet**	**Veliki intenzitet**	**Veoma veliki intenzitet**
W_A	**Verovatnoća pojave (%)**	40,00	25,00	20,00	10,00	5,00
	Vrednost faktora	0,01	0,20	0,25	0,50	1,00

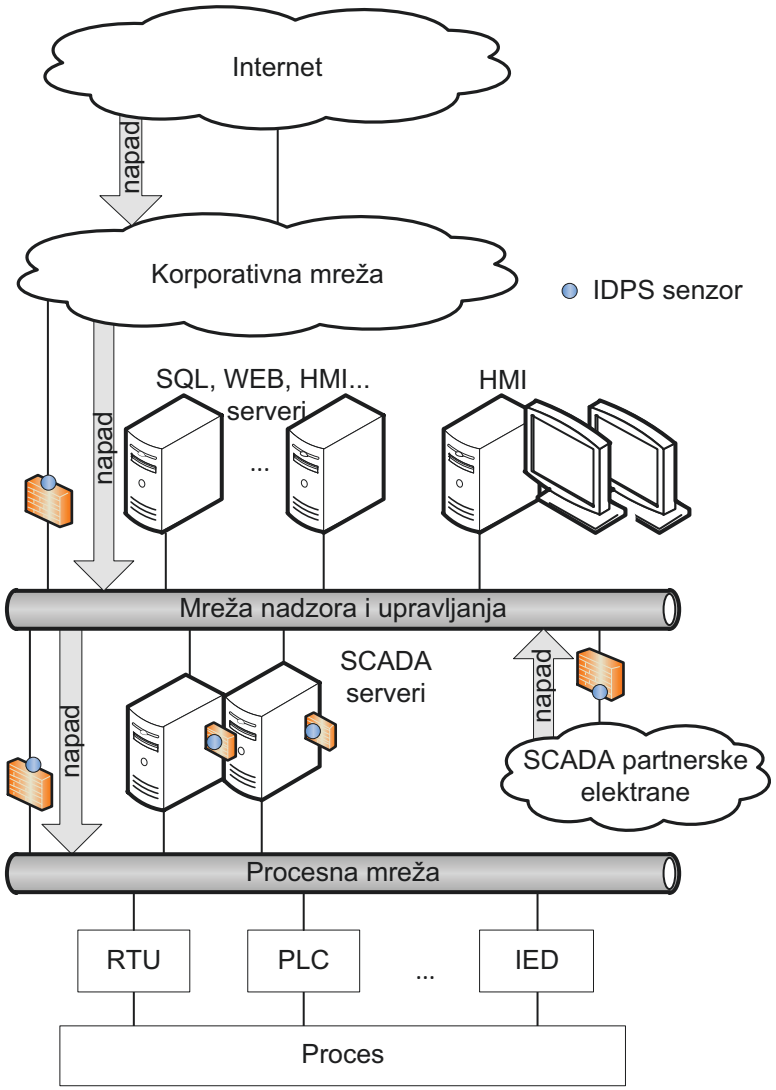
Na osnovu raspodele verovatnoće i vrednosti za težinski faktor, primenom formule (5.2) određena je konačna vrednost $W_A = 0{,}204$.

Analiza rezultata

Pretpostavljena je implementacija pet IDPS sistema i to:

- tri mrežna IDPS, prvi sistem prema korporativnoj mreži, drugi sistem prema procesnoj mreži i treći sistem prema SCADA mreži partnerske elektrane i
- dva IDPS u hostovima na udvojenim SCADA serverima.

Na slici 6.6 prikazan je model analiziranog SCADA sistema nakon implementacije mehanizama zaštite.



Slika 6.6. Model SCADA sistema u hidroelektrani sa implementiranim IDPS.

Pretpostavlja se da je vreme oporavka srazmerno intenzitetu napada. Za vreme oporavka u slučaju napada najveće snage uzima se t_{Rmax} = 120 minuta [105]. Vreme oporavka se dobija kao proizvod težinskog faktora za skaliranje intenziteta napada W_A i vremena oporavka nakon napada najvećeg intenziteta t_{Rmax}.

Težinski faktor W_A koji skalira intenzitet napada će se u daljoj analizi uzimati ili sa vrednošću koja je određena u tabeli 6.4 ili kao promenljiva veličina da bi se u funkciji ovog parametra analizirala vrednost *ROSI*.

Na osnovu dobijenih vrednosti težinskih faktora i formule (5.3) izračunata je mera rizika R = 1,31. Primenom kvalitativne klasifikacije mere rizika iz tabele 5.3 ocenjuje se da je nivo rizika nizak.

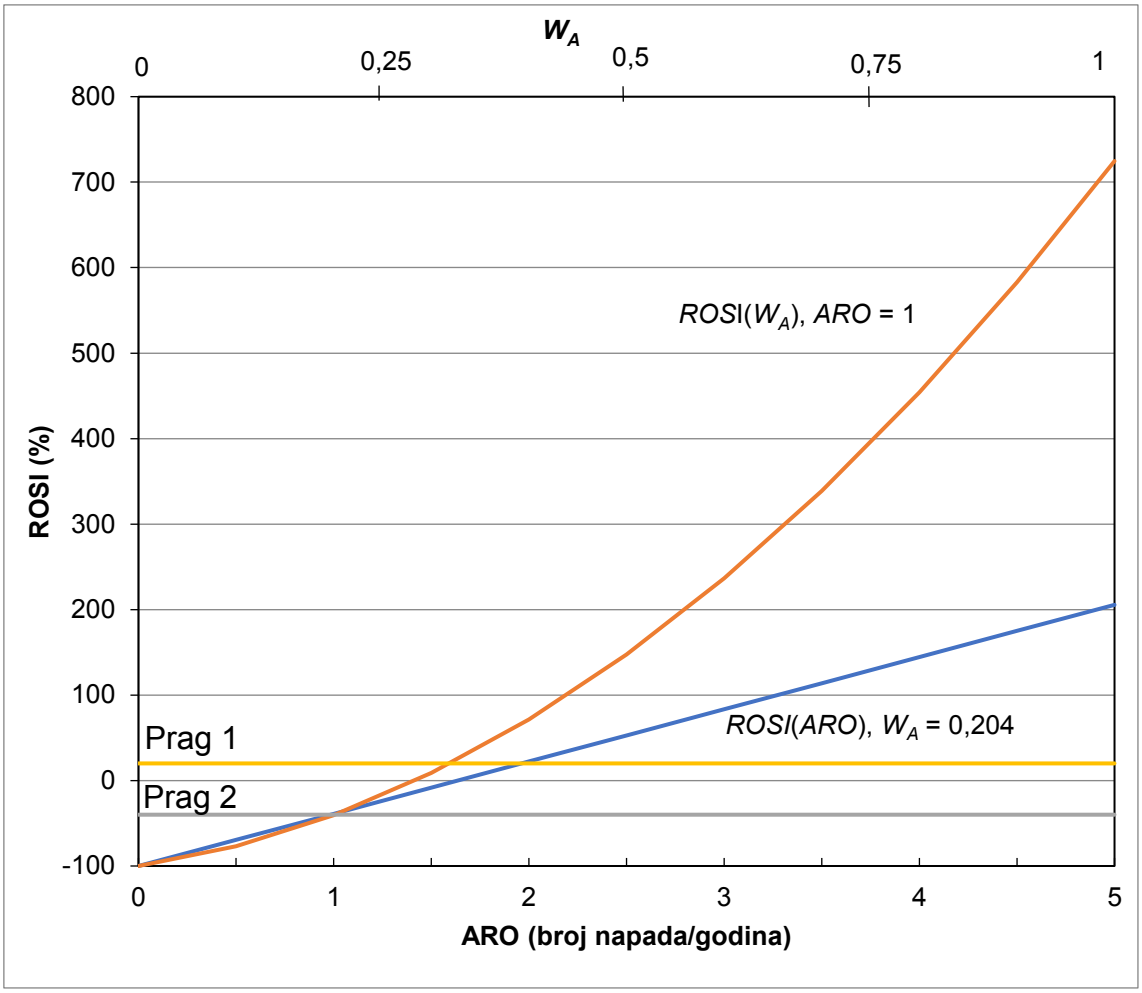
Monetarne vrednosti izražene su odgovarajućom monetarnom jedinicom (MU). Primena formule (5.5) za obračun očekivanih godišnjih gubitaka daje ALE = 16 MU × ARO.

Obračun troškova investicije u mehanizme zaštite izvršen je za procenjeni period od pet godina, srazmerno vrednosti investicije čija je implementacija prezentovana u [108]. Tako dobijena vrednost C_S = 13 MU.

Vrednost *ROSI* određena je na osnovu formule (5.7), izračunatih vrednosti ALE i C_S, i polaznih pretpostavki iz poglavlja 6.1. Zavisnost *ROSI* od učestanosti napada u toku godine, kao i u funkciji težinskog faktora W_A grafički je prikazana na slici 6.7.

Vrednost *ROSI* zavisi od procenjenog broja napada u toku jedne godine, a u konkretnom primeru se dobija pozitivna vrednost ako ima više od jednog napada. Na istom grafičkom prikazu data je zavisnost *ROSI* od težinskog faktora W_A, kojim se kvantifikuje intenzitet napada.

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. Iz tih razloga, na slici 6.7 prikazane su dve vrednosti za prag *ROSI*. Uočava se negativna vrednost za Prag 2, koja označava da se prihvata investicija čak i za procenjen broj od jednog napada godišnje.



Slika 6.7. Zavisnost *ROSI* od W_A i *ARO* u hidroelektrani.

6.2.3. *Primena hibridnog metoda procene bezbednosnog rizika zasnovanog na analizi arhivskih podataka i subjektivnoj oceni stručnjaka*

Objektivna faza

Objektivna faza pretpostavlja analizu arhivskih podataka, koja je identična kao u poglavlju 6.2.2.

Subjektivna faza

Za određivanje vrednosti težinskih faktora W_E i W_H (koji reflektuju subjektivnu ocenu stručnjaka) kreirane su dve ankete koje sadrže tri i četiri pitanja, respektivno. U tabelama 6.5. i 6.6. prikazane su ankete i legenda ponuđenih odgovora.

Tabela 6.5. Ankete za određivenje težinskih faktora za slučaj hidroelektrane

Redni broj	Težinski faktor pitanja	Tekst pitanja	Ponuđeni odgovori					
Određivanje težinskog faktora W_E								
1.	0,3	Koliki je uticaj ispada jednog agregata na ispunjenje zahteva za proizvodnjom?	0	1	2	3	4	5
2.	0,2	Koliki je uticaj nemogućnosti zadavanja snage iz kontrolnog centra na ispunjenje zahteva za proizvodnjom?	0	1	2	3	4	5
3.	0,5	Kakve su posledice neispunjenja zahtevane proizvodnje?	0	1	2	3	4	5
Određivanje težinskog faktora W_H								
1.	0,2	Koliki je uticaj ispada jednog agregata na prelivanje?	0	1	2	3	4	5
2.	0,1	Koliki je uticaj nemogućnosti zadavanja snage iz kontrolnog centra na prelivanje?	0	1	2	3	4	5
3.	0,5	Kakve su posledice prelivanja usled gubitka proizvodnog kapaciteta?	0	1	2	3	4	5
4.	0,2	Kakve su posledice nemogućnosti daljinskog upravljanja prelivnom branom?	0	1	2	3	4	5

Tabela 6.6. Legenda za ponuđene odgovore za ankete u tabeli 6.5

0	Nema uticaja
1	Veoma mali uticaj
2	Mali uticaj
3	Srednji uticaj
4	Veliki uticaj
5	Veoma veliki uticaj

U anketi koja je formirana radi određivanja težinskog faktora W_E kojim se kvantifikuju indirektni troškovi usled neispunjenja obaveze isporuke električne energije anketirani su:

- dispečer iz službe planiranja (E1);
- rukovalac centralne komande (E2);
- rukovodilac u službi eksploatacije (E3);
- predstavnik poslovodstva (E4).

Kompetentnost svakog ankentiranog učesnika je određena AHP metodom na osnovu kriterijuma:

- radno iskustvo;
- stepen stručne spreme;
- vrsta struke.

U tabelama 6.7 – 6.9 prikazan je postupak određivanja kompetentnosti stručnjaka. Prvo je određena težina svakog od kriterijuma (tabela 6.7), a zatim težinski faktori po ovim kriterijumima za svakog učesnika u anketi (tabela 6.8). U tabeli 6.9 je prikazano dobijanje konačnog težinskog faktora kojim se kvantifikuje odgovor svakog stručnjaka.

Tabela 6.7. Primena AHP metoda za određivanje vektora prioriteta za slučaj hidroelektrane

	Radno iskustvo	**Stepen stručne spreme**	**Vrsta struke**	**Vektor prioriteta**
Radno iskustvo	1,00	4,00	2,00	0,60
Stepen stručne spreme	0,25	1,00	1,00	0,19
Vrsta struke	0,50	1,00	1,00	0,21

Tabela 6.8. Matrice za određivanje kompetentnosti prema usvojenim kriterijumima u tabeli 6.7

Radno Iskustvo	**Prioritet**	**0,60**				
	E1	**E2**	**E3**	**E4**		
E1	1,00	7,00	0,33	5,00	0,32	0,19
E2	0,14	1,00	0,11	0,20	0,04	0,02
E3	3,00	9,00	1,00	7,00	0,49	0,29
E4	0,20	5,00	0,14	1,00	0,15	0,09
Stepen stručne spreme	**Prioritet**	**0,19**				
	E1	**E2**	**E3**	**E4**		
E1	1,00	5,00	0,33	1,00	0,24	0,05
E2	0,20	1,00	0,14	0,20	0,05	0,01
E3	3,00	7,00	1,00	3,00	0,47	0,09
E4	1,00	5,00	0,33	1,00	0,24	0,05

Vrsta struke	Prioritet	0,21				
	E1	E2	E3	E4		
E1	1,00	2,00	1,00	7,00	0,36	0,08
E2	0,50	1,00	0,50	5,00	0,23	0,05
E3	1,00	2,00	1,00	7,00	0,36	0,08
E4	0,14	0,20	0,14	1,00	0,05	0,01

Tabela 6.9. Težinski faktor kompetentnosti stručnjaka u hidroelektrani

	Radno iskustvo	Stepen stručne spreme	Vrsta struke	*Ci*
E1	0,19	0,05	0,08	0,31
E2	0,02	0,01	0,05	0,08
E3	0,29	0,09	0,08	0,46
E4	0,09	0,05	0,01	0,15

Ovako dobijenim težinskim faktorima kompetentnosti se skaliraju odgovori u anketi kako bi se dobio konačan težinski faktor W_E (tabela 6.10).

Tabela 6.10. Težinski faktor W_E

	Faktor	E1	E2	E3	E4
Pitanje 1	0,3	4	3	4	1
Pitanje 2	0,2	1	1	0	2
Pitanje 3	0,5	1	0	3	4
$\Sigma (W_{qi} \times A_{ij})$		1,9	1,1	2,7	2,7
Kompetentnost		0,31	0,08	0,46	0,15
W_{Ei}		0,60	0,09	1,24	0,39
W_E		2,32			

Postupak za izračunavanje težinskog faktora W_H je u osnovi isti kao za težinski faktor W_E. Konačna vrednost težinskog faktora W_H je 4,23.

Završna faza

Poslednji korak predstavlja upoređivanje vrednosti iz objektivne i subjektivne faze, kao i određivanje konačne vrednosti faktora W_k.

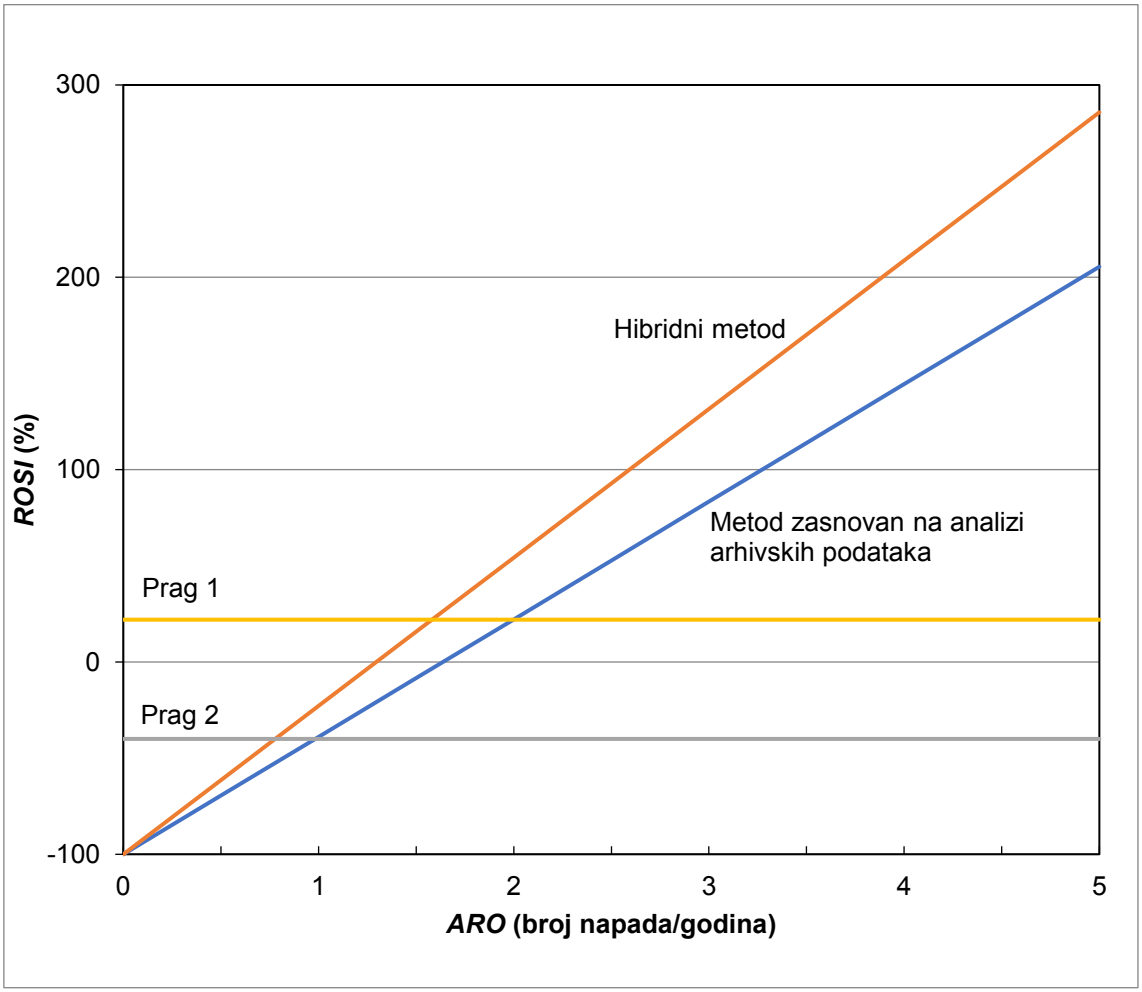
U ovom primeru usvojeno je da su koeficijenti K_O i K_S jednaki, pa su na osnovu formule (5.10) dobijene vrednosti za težinske faktore prikazane u tabeli 6.11. Za ovako dobijene

težinske faktore i usvojenu vrednost težinskog faktora W_A iz objektivne faze dobija se mera rizika R = 1,64. Prema kvalitativnoj klasifikaciji mere rizika iz tabele 5.3 dobija se da je nivo rizika srednji. Dobijeni rezultat pokazuje da je uvođenjem subjektivne komponente procenjena veća mera rizika.

Tabela 6.11. Konačna vrednost faktora u hidroelektrani

Faktor	W_E	W_H
Vrednost	2,26	3,57

Na slici 6.8 su grafički prikazane vrednosti *ROSI* u funkciji *ARO* dobijene primenom oba predložena metoda procene rizika.



Slika 6.8. Poređenje zavisnosti *ROSI* od *ARO* u dva metoda u hidroelektrani.

Težinski faktori dobijeni primenom hibridnog metoda za procenu rizika povećavaju vrednost *ROSI*. Uticaj je veći za učestalije napade i viši nivo postavljenog praga.

Dobijeni rezultat pokazuje da predložena kvantifikacija subjektivne procene rizika menja konačnu procenu o isplativosti investicije u bezbednosni mehanizam.

6.3. Studija slučaja SCADA sistema u magistralnom gasovodu

Transport i distribucija gasa je deo kritične infrastrukture, a pripada sektoru transporta. U Sjedinjenim Američkim Državama sistem cevovoda se sastoji od više od četiri miliona kilometara cevi koji prolazi kroz državu i distribuira skoro čitav nacionalni prirodni gas i oko 65 procenata 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, 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 PLC-ovi i 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. PLC utiče na rad kompresora postavljanjem *set-point* veličine iz komandnog centra ili lokalnim algortimom. Veza senzora sa RTU i PLC, 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 [109] može se naći pregled nekih uspešnih sajber napada na SCADA sisteme gasovoda i naftovoda.

6.3.1. Konfiguracija sistema i scenario otkaza

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 [110]. 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 hibridnim metodom, i to samo u fazi koja je zasnovana subjektivnoj oceni stručnjaka.

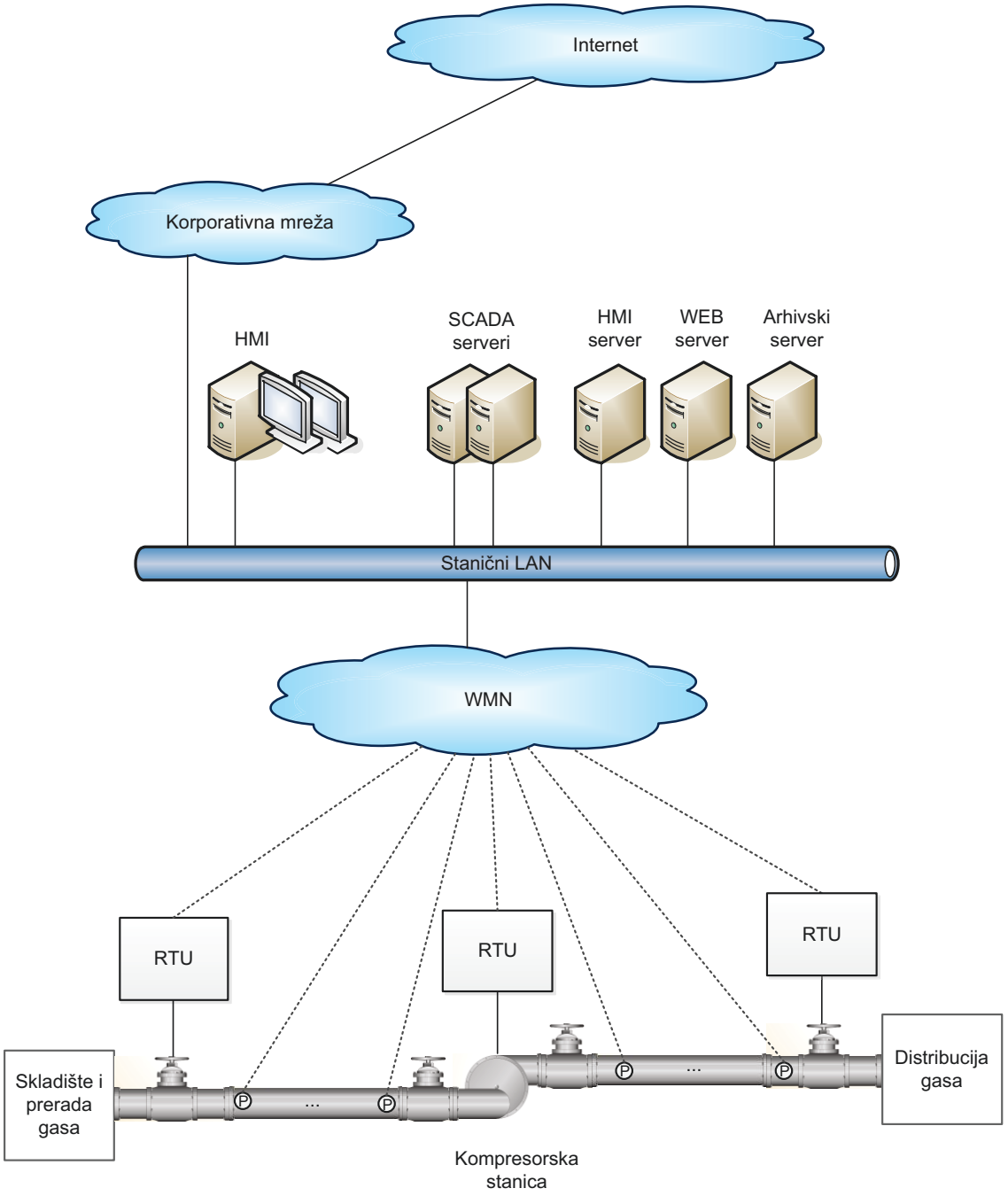
Na slici 6.9 prikazan je model magistralnog gasovoda koji transportuje prirodni gas od izvora do odredišta koji su udaljeni 257 km. Pritisak u gasovodu treba da bude 6,2 MPa, a kompresorska stanica koja je udaljena 155 km od izvora treba da podigne pritisak na 8,2 MPa da bi na mestu isporuke gas imao 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 6.9 prikazani su model gasovoda i arhitektura SCADA sistema. SCADA sistem čine serveri i HMI 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 6.10. Na istoj slici ukazano je na moguće puteve upada u mrežu SCADA sistema i izvršenje infrastrukturnog napada.

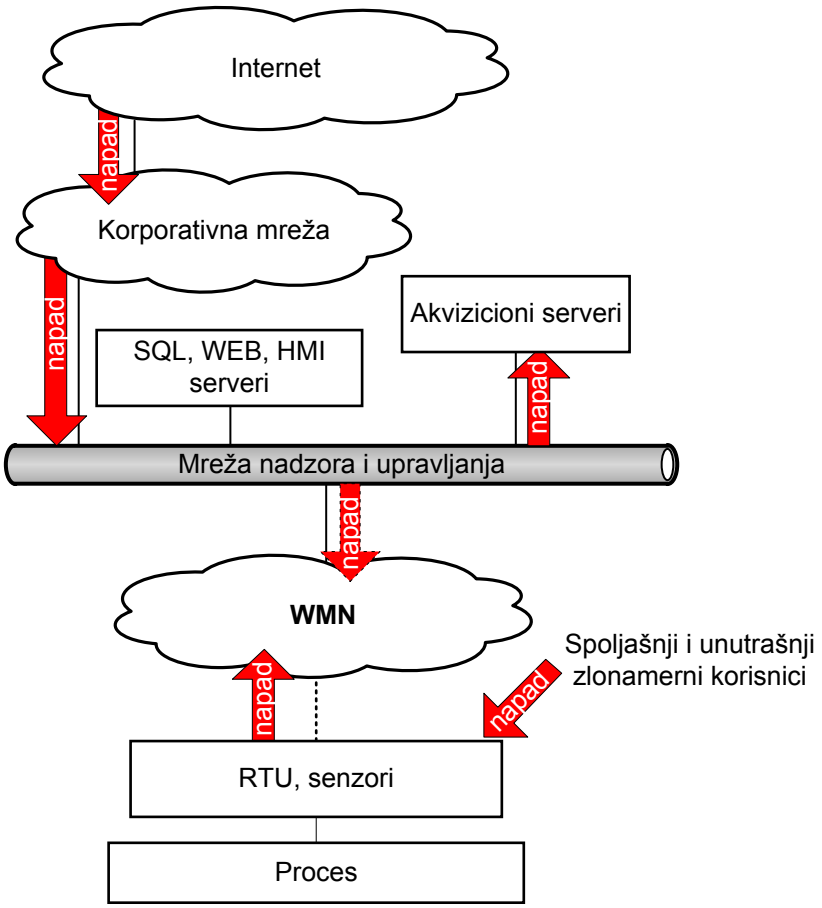
U studiji slučaja pretpostavljen je napad reprogramiranjem RTU-ova, kako bi bile prikazane pogrešne vrednosti pritiska gasa, što dovodi do pogrešnih instrukcija kompresorskoj stanici. Ovaj napad se kombinuje sa DDoS napadom, što za posledicu ima usporen odgovor sistema. Scenario ovakvog otkaza je prikazan na slici 6.11.

Posledice ovakvog napada mogu da budu gubitak u prenosu gasa usled prekida transporta, gubitak rezervi gasa usled potencijalnog curenja gasa i oštećenje cevovoda.

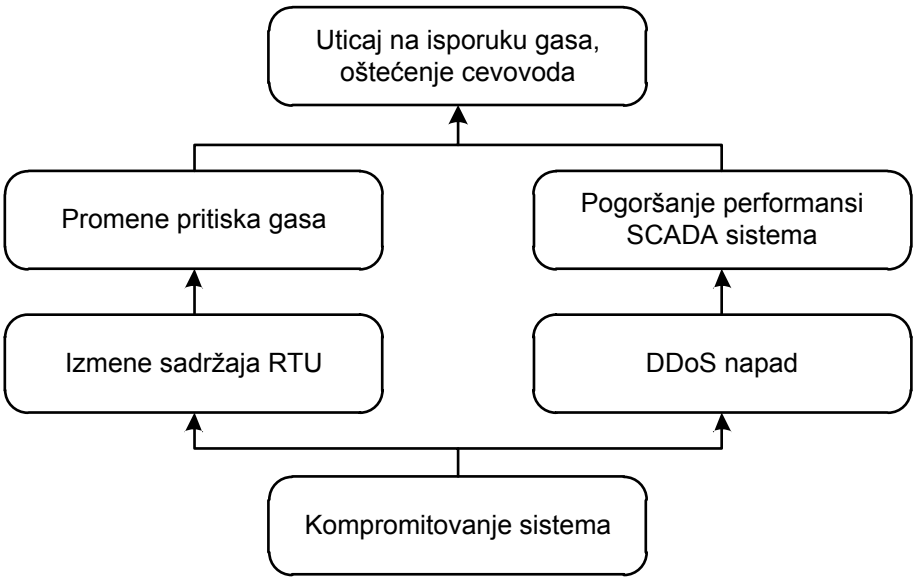
U [110] je realizovana simulacija ovakvog napada pri čemu je za model korišćena realna situacija napada na infrastukturu SCADA sistema gasovoda.



Slika 6.9. Model gasovoda i arhitektura sistema daljinskog upravljanja.



Slika 6.10. Model sistema za daljinsko upravljanje sa aspekta rizika u gasovodu.



Slika 6.11. Scenario otkaza u gasovodu.

6.3.2. Primena metoda procene bezbednosnog rizika zasnovanog na subjektivnoj oceni stručnjaka

Direktni i indirektni gubici

Na primeru gasovoda analizirane su moguće posledice kombinovanog napada izmenama sadržaja RTU i DDoS 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 snagu napada W_A.

Kao i u prethodno obrađenom slučaju (koji se odnosi na hidroelektranu) 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.

Primer indirektnih troškova koji se pretpostavljaju u simulaciji nastaju zbog:

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

Indirektni troškovi se kvantifikuju težinskim faktorima W_P, W_R i W_C, respektivno.

Primenom ovih pretpostavki na formulu (5.5) dobija se sledeći izraz za proračun godišnjih očekivanih gubitaka:

$$ALE = W_A\, W_P\, W_R\, W_C\, Q\, (t_A + W_A\, t_{Rmax})\, c_G \times ARO. \qquad (6.2)$$

Određivanje vrednosti težinskih faktora koji reflektuju subjektivnu ocenu stručnjaka

Za određivanje vrednosti težinskih faktora W_P, W_R i W_C (koji reflektuju subjektivnu ocenu stručnjaka) kreirane su tri ankete prikazane u tabeli 6.12, dok je u tabeli 6.13 prikazana legenda ponuđenih odgovora.

Tabela 6.12. Ankete za određivanje težinskih faktora za slučaj gasovoda

Redni broj	**Težinski faktor piatanja**	**Tekst pitanja**	**Ponuđeni odgovori**					
Određivanje težinskog faktora W_P								
1.1.	0,3	Koliki je odziv ekipe za ručno upravljanje?	0	1	2	3	4	5
1.2.	0,3	Koliko utiče otkaz daljinskog upravljanja iz komandnog centra na isporuku gasa?	0	1	2	3	4	5
1.3.	0,4	Kakve su posledice neispunjenja zahtevane isporuke gasa?	0	1	2	3	4	5
Određivanje težinskog faktora W_R								
2.1.	0,3	Koliki je uticaj gubitaka rezervi gasa na životnu sredinu?	0	1	2	3	4	5
2.2.	0,2	Koliki je uticaj gubitaka rezervi gasa na cenu gasa?	0	1	2	3	4	5
2.3.	0,5	Koliki uticaj ima povišeni pritisak gasa na oštećenja cevovoda?	0	1	2	3	4	5
Određivanje težinskog faktora W_C								
3.1.	0,3	Koliki je uticaj oštećenja cevovoda na kontinualnu isporuku gasa?	0	1	2	3	4	5
3.2.	0,2	Koliki su troškovi sanacije oštećenja?	0	1	2	3	4	5
3.3.	0,5	Koliki uticaj ima povišeni pritisak gasa na oštećenja cevovoda?	0	1	2	3	4	5

Tabela 6.13. Legenda za ponuđene odgovore za ankete u tabeli 6.12

	Pitanje	
	1.1.	**1.2, 1.3, 2.1., 2.2, 2.3, 3.1, 3.3, 3.2**
0	Odličan	Nema
1	Veoma dobar	Veoma mali
2	Dobar	Mali
3	Srednji	Srednji
4	Loš	Veliki
5	Veoma lošš	Veoma veliki

S obzirom da se procena bezbednosnog rizika vrši u fazi projektovanja sistema, izbor stručnjaka koji će biti anketirani je specifičan. Ukoliko se projekat radi za postojeći fizičko-tehnički sistem u cilju modernizacije sistema, ciljna grupa su zaposleni u toj organizaciji. Slično kao i u slučaju procene bezbednosnog rizika u protočnoj hidroelektrani, treba odabrati iskusne operatere u komandnom centru, zaposlene u procesu planiranja isporuke gasa i održavanja, kao i relevantne predstavnike poslovodstva. Ukoliko se projektuje sistem daljinskog upravljanja za gasovod koji je u izgradnji, tada se anketiraju stručnjaci koji su zaposleni u organizacijama slične infrastrukture i stručni timovi relevantnih naučnih institucija. U simulaciji primene metoda procene bezbednosnog rizika analizira se slučaj projektovanja sistema daljinskog upravljanja novog gasovoda, pa su u anketi koja je formirana radi određivanja težinskih faktora kojim se kvantifikuju indirektni troškovi usled neispunjenja obaveze isporuke prirodnog gasa anketirani:

- dispečer iz službe planiranja u gasovodu koji ima sličnu infrastrukturu (E1);
- predstavnik poslovodstva gasovoda koja ima sličnu infrastrukturu (E2);
- stručnjak iz oblasti transportnih sistema (E3).

Kompetentnost svakog ankentiranog učesnika je određena AHP metodom na osnovu kriterijuma:

- radno iskustvo;
- stepen stručne spreme;
- vrsta struke;
- radno mesto.

U tabelama 6.14 – 6.16 prikazan je postupak određivanja kompetentnosti stručnjaka. Prvo je određena težina svakog od kriterijuma (tabela 6.14), a zatim težinski faktori po ovim kriterijumima za svakog učesnika u anketi (tabela 6.15). U tabeli 6.16 prikazan je postupak dobijanja konačnog težinskog faktora kojim se kvantifikuje odgovor svakog stručnjaka.

Tabela 6.14. Primena AHP metoda za određivanje vektora prioriteta za slučaj gasovoda

	Radno iskustvo	Stepen stručne spreme	Vrsta struke	Radno mesto	Vektor prioriteta
Radno iskustvo	1,00	2,00	3,00	3,00	0,33
Stepen stručne spreme	0,50	1,00	0,33	0,17	0,70
Vrsta struke	0,33	3,00	1,00	0,25	0,17
Radno mesto	0,33	6,00	4,00	1,00	0,42

Tabela 6.15. Matrice za određivanje kompetentnosti prema usvojenim kriterijumima u tabeli 6.14

Radno iskustvo	**Prioritet**	**0,33**			
	E1	**E2**	**E3**		
E1	1,00	3,00	0,50	0,25	0,08
E2	0,33	1,00	0,11	0,08	0,03
E3	2,00	9,00	1,00	0,67	0,22
Stepen stručne spreme	**Prioritet**	**0,07**			
	E1	**E2**	**E3**		
E1	1,00	0,50	0,11	0,07	0,01
E2	2,00	1,00	0,14	0,14	0,01
E3	9,00	7,00	1,00	0,78	0,06
Vrsta struke	**Prioritet**	**0,17**			
	E1	**E2**	**E3**		
E1	1,00	2,00	1,00	0,40	0,07
E2	0,50	1,00	0,50	0,20	0,03
E3	1,00	2,00	1,00	0,40	0,07
Radno mesto	**Prioritet**	**0,38**			
	E1	**E2**	**E3**		
E1	1,00	0,50	0,25	0,12	0,05
E2	2,00	1,00	0,20	0,21	0,09
E3	4,00	5,00	1,00	0,67	0,28

Tabela 6.16. Težinski faktor kompetentnosti

	Radno iskustvo	Stepen stručne spreme	Vrsta struke	Radno mesto	*Ci*
E1	0,08	0,01	0,07	0,05	0,21
E2	0,03	0,01	0,03	0,09	0,16
E3	0,22	0,06	0,07	0,28	0,63

Ovako dobijenim težinskim faktorima kompetentnosti se skaliraju odgovori u anketi kako bi se dobio konačan težinski faktor W_P (tabela 6.17).

Tabela 6.17. Težinski faktor kompetentnosti stručnjaka za gasovod

	Faktor	E1	E2	E3
Pitanje 1	0,30	2,00	1,00	2,00
Pitanje 2	0,30	2,00	3,00	4,00
Pitanje 3	0,40	3,00	4,00	3,00
Σ ($W_{qi} \times A_{ij}$)		2,40	2,80	3,00
Kompetentnost		0,21	0,16	0,63
W_{Pi}		0,50	0,45	1,89
W_P		**2,84**		

Postupak za izračunavanje težinskih faktora W_R i W_C je u osnovi isti kao za težinski faktor W_P. Konačne vrednosti težinskih faktora W_R i W_C su 1,17 i 2,96, respektivno.

Usvojena je ista vrednost faktora za skaliranje intenziteta napada W_A kao u studiji slučaja protočne hidroelektrane (tabela 6.4), uz realnu pretpostavku da je uticaj intenziteta napada sličan u oba analizirana slučaja.

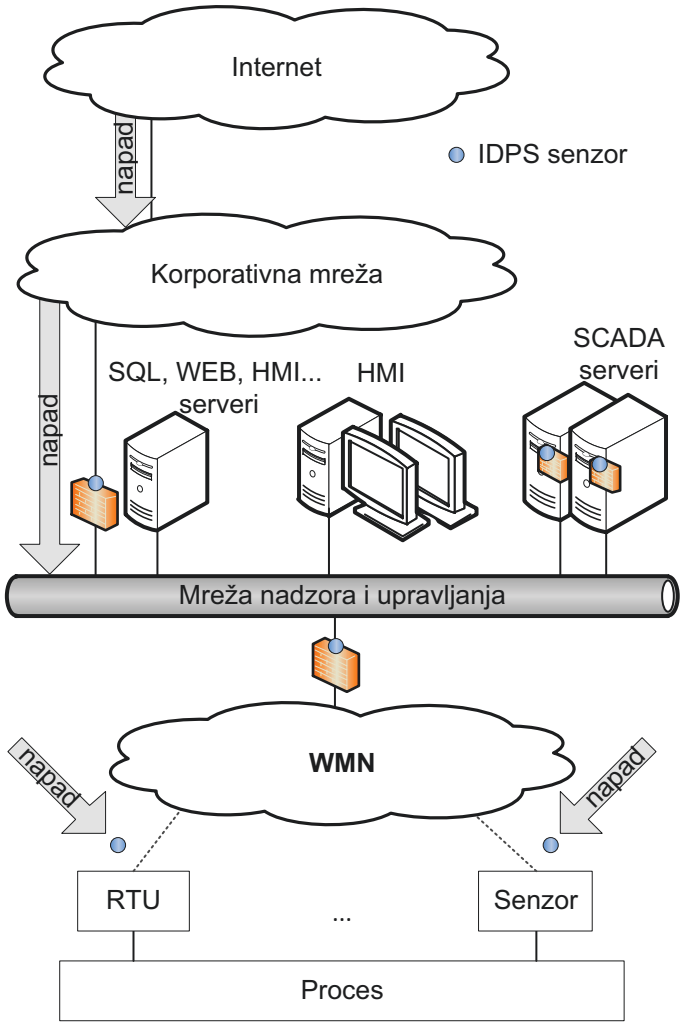
Analiza rezultata

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 hostovima na udvojenim SCADA serverima.

Za WMN pretpostavljena je implementacija bežičnih IDPS senzora za spoljašnju montažu (*outdoor*) u zoni RTU-ova i senzora.

Na slici 6.12 prikazan je model analiziranog SCADA sistema nakon implementacije mehanizama zaštite.



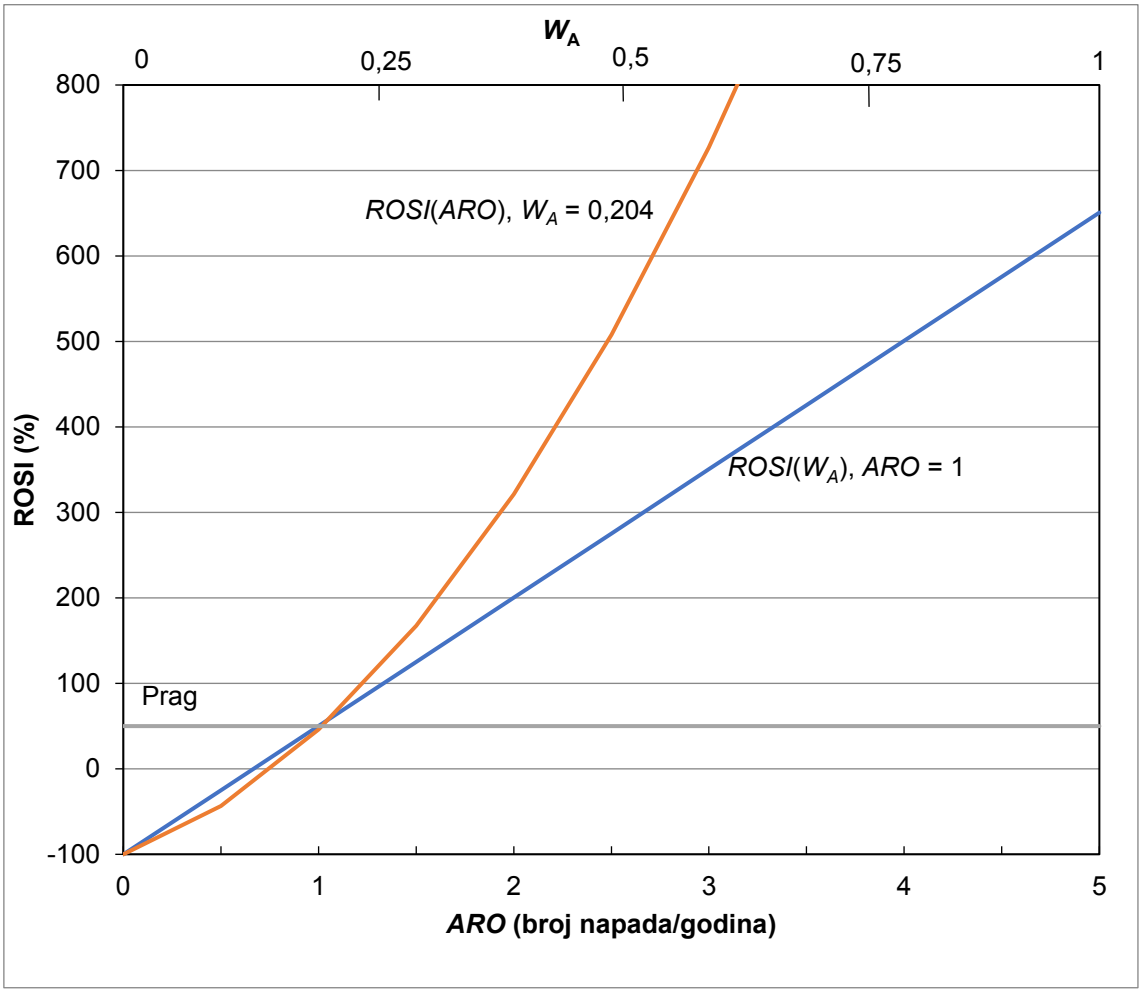
Slika 6.12. Arhitektura SCADA u gasovodu sistema sa implementiranim IDPS.

Analiza rezultata procene bezbednosnog rizika i *cost/benefit* analiza ie izvršena za iste pretpostavljene cene implementiranih mehanizama zaštite i vremena oporavka kao za slučaj protočne hidroelektrane koji je razmatran u poglavlju 6.2.

Na osnovu dobijenih vrednosti težinskih faktora i formule (5.3) izračunata je mera rizika $R = 2{,}54$. Primenom kvalitativne klasifikacije mere rizika iz tabele 5.3 ocenjuje se da je nivo rizika visok.

Primena formule (5.5) za obračun očekivanih godišnjih gubitaka daje $ALE = 68 \times ARO$ MU. Vrednost investicije u mehanizme zaštite za procenjeni period od pet godina je $C_S = 41$ MU.

Vrednost *ROSI* određena je na osnovu formule (5.7), izračunatih vrednosti *ALE* i C_S, i polaznih pretpostavki iz poglavlja 6.1. Zavisnost *ROSI* od učestanosti napada u toku godine, kao i u funkciji težinskog faktora W_A grafički je prikazana na slici 6.13.



Slika 6.13. Zavisnost *ROSI* od W_A i *ARO* u gasovodu.

Vrednost *ROSI* zavisi od procenjenog broja napada u toku jedne godine, a u konkretnom primeru se dobija pozitivna vrednost ako ima više od jednog napada. Na

istom grafičkom prikazu data je zavisnost *ROSI* od težinskog faktora W_A, kojim se kvantifikuje intenzitet napada.

I u ovom slučaju je značajno da se odredi prag za *ROSI* na osnovu kojeg se može doneti odluka o isplativosti investicije u mehanizme zaštite. Na slici 6.13 prikazana je vrednost za prag *ROSI*. Uočava se pozitivna vrednost, koja označava da se prihvata investicija za procenjen broj od jednog napada. U ovom slučaju, investicija u unapređenje bezbednosti informacione i komunikacione 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 $W_A = 0{,}153$.

7. PREDLOG MERA ZA OGRANIČAVANJE BEZBEDNOSNOG RIZIKA

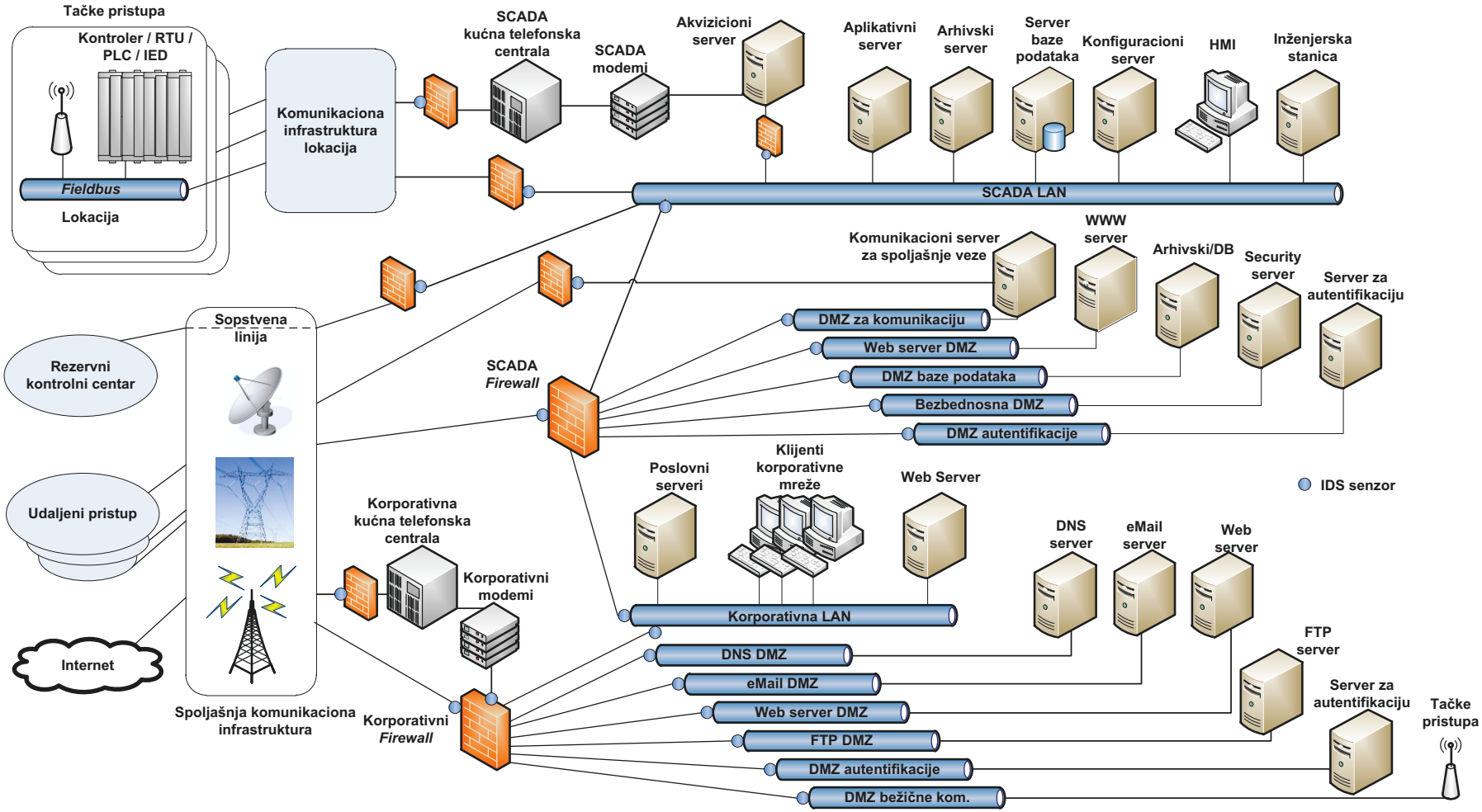
U cilju ograničenja bezbednosnog rizika potrebno je preduzeti opsežne i sveobuhvatne mere koje podrazumevaju usvajanje politike bezbednosti informacione infrastukture, informisanje i obuku zaposlenih o politici, uspostavljanje sistema bezbednosti informacione infrastrukture i kontinualno upravljanje bezbednosnim rizikom.

7.1. Arhitektura industrijskih sistema daljinskog upravljanja sa aspekta bezbednosti

Za zaštitu mreže industrijskog sistema daljinskog upravljanja preporuka je da se primenjuje *Defense-in-Depth* model [2] koji predstavlja koncept bezbednosti zasnovan na zaštiti u više slojeva. Ovako koncipirana zaštita obezbeđuje redundantnost i višestruku zaštitu po dubini. Na svakom sloju se primenjuju adekvatne mere i mehanizmi zaštite koje uključuju upotrebu *firewall*-ova, stvaranje DMZ, implementaciju mehanizama za otkrivanja napada, instaliranje softverskih dodataka, primenu procedura i politike zaštite.

Na slici 7.1 prikazana je arhitektura mreže industrijskog sistema daljinskog upravljanja koja podržava *Defense-in-Depth* strategiju.

Telekomunikaciona mreža industrijskih sistema daljinskog upravljanja treba da bude odvojena od korporativne mreže. Zbog potrebe izveštavanja, analize događaja na klijentima korporativne mreže i praćenja nekih procesnih veličina često postoji potreba za povezivanjem ove dve mreže. Ukoliko postoji takav zahtev važno je da se broj veza minimizuje i da se veza ostvari uz obezbeđenje *firewall*-a i IDPS tehnologija. Serveri kojima se pristupa iz korporativne mreže treba da budu izdvojeni u DMZ. Ukoliko se dozvoli udaljeni pristup mreži za potrebe konfigurisanja i održavanja neophodno je da se to dozvoli isključivo otvaranjem samo porta za adekvatni servis.



Slika 7.1. *Defense-in-Depth* arhitektura industrijskog sistema za daljinsko upravljanje [41].

U okviru ove strategije preporučuje se razdvajanje mreže u mrežne segmente, kojima su dodeljena različita prava pristupa. Na ovaj način se obezbeđuje nezavisna administracija i korišćenje podataka sa različitih uređaja u mreži. Segmentacija mreže se obavlja na logičkom ili fizičkom nivou. Definisanje pravila komunikacije između segmenata pre svega treba da poštuje tehnološki proces u smislu da li komunikacija treba da postoji, a zatim da omogući samo neophodne tokove saobraćaja koji su autentifikovani i autorizovani.

U ovako definisanoj arhitekturi značajno je da se dozvoli komunikacija samo bezbednim protokolima koji imaju implementirane zaštitne mehanizme, a da se protokoli bez zaštite zabrane. Primer je upotreba SSH (*Secure Shell*) umesto *Telnet*, SFTP (*Secure* FTP) i SCP (*Secure Copy*) umesto FTP i TFTP (*Trivial File Transfer Protocol*), HTTPS (HTTP *Secure*) umesto HTTP (*Hypertext Transfer Protocol*) protokola.

SCADA i industrijski protokoli, kao što su Modbus/TCP, Eternet, IEC 61850, ICCP (*Inter-Control Center Communications Protocol*) i DNP3, su kritični za komunikaciju. Nažalost, ovi protokoli su većinom dizajnirani bez ugrađene zaštite i obično ne zahtevaju autentifikaciju za daljinsko upravljanje. Ove protokole treba koristiti samo u okvirima kontrolne mreže, a zabraniti njihovo korišćenje iz korporativne mreže.

7.2. Preporučeni mehanizmi zaštite u industrijskim sistemima daljinskog upravljanja

Osnovni preduslov za uspešnu primenu mehanizama zaštite, odnosno za ograničenje bezbednosnog rizika je analiza dnevnih aktivnosti zaposlenih. Sam mehanizam praćenja podrazumeva prikupljanje podataka o aktivnostima zaposlenih u realnom vremenu što može pružiti jasan uvid u rad sistema kroz neko vremensko razdoblje. Na osnovu toga se može dobiti procena nedostataka zaštite infrastrukture sistema ili odrediti uzrok nekih nepredviđenih događaja.

Zaštita telekomunikacione mreže SCADA sistema zasniva se na mehanizmima koji se mogu svrstati u četiri osnovne kategorije: (1) kontrola pristupa, (2) detekcija/prevencija

napada, (3) otkrivanje i eliminacija zlonamernih aplikativnih programa, i (4) definisanje opštih mera zaštite, kao što je prikazano na slici 7.2.

Slika 7.2. Preporučeni mehanizmi zaštite.

Kontrola pristupa podrazumeva dodeljivanje privilegija za pristup pojedinim segmentima mreže, aplikacijama i podacima, ali i obezbeđenje kontrole fizičkog pristupa lokacijama sistema daljinskog upravljanja. U kontekstu mehanizama zaštite posebno su značajni upravljanje lozinkama i biometrija. Upravljanje lozinkama je diktirano višim stepenom upravljanja kada se postavljaju zahtevi za složenijim lozinkama i mehanizmima autorizacije. U slučajevima kada se lozinke prenose preko mrežne infrastrukture potrebno je primeniti postupke šifrovanja. Biometrija podrazumeva metode jedinstvenog prepoznavanja pojedinaca preko jedne ili više fizičkih karakteristika. Primena ove tehnologije je sve rasprostranjenija kod savremenih mehanizama autentifikacije u SCADA sistemima.

Za detekciju i prevenciju napada koriste se različite tehnike i tehnologije (pojedinačno ili kombinovano):

- *Firewall*-ovi se mogu koristiti za filtriranje saobraćaja između poslovnih IT sistema i SCADA mreža. Neki od problema koji se mogu javiti kod primene *firewall*-a u SCADA sistemima su povremena kašnjenja u prenosu upravljačkih informacija, složenost održavanja i nedostatak *firewall*-ova razvijenih za rad sa specifičnim protokolima koji se primenjuju u SCADA sistemima.
- Kao što je ranije istaknuto u poglavlju 2.5, preporučuje se primena specifičnih IDPS tehnologija koje su namenski razvijene za SCADA sisteme.

- Virtuelne privatne mreže omogućuju korisnicima na udaljenim lokacijama da preko javne mreže jednostavno održavaju zaštićenu komunikaciju.
- Primena *honeypot* uređaja omogućuje identifikovanje neautorizovanih ili zlonamernih aktivnosti.

Otkrivanje zlonamernih programa i njihova eliminacija u SCADA sistemima su od izuzetnog značaja za bezbednost, ali često predstavljaju problem zbog velikih procesorskih zahteva koji usporavaju rad sistema. Aktivnosti poput pokretanja antivirusne programske podrške, osvežavanja baza podataka s definicijama pojedinih virusa, skeniranja sistema u potrazi za zlonamernim kodom i slične akcije zahtevaju procesorske resurse koji često nisu dostupni svim komponentama SCADA sistema.

Definisanje opštih mera zaštite obuhvata aktivnosti kao što su:

- Usvajanje politike kontinuiteta u kojoj je detaljno definisana procedura u slučaju otkaza vitalne funkcije sistema daljinskog upravljanja. Preporučuje se formiranje rezervnog kontrolnog centra, kao i drugih redundantnih mera zavisno od specifičnog sistema.
- Informisanje i kontinualna edukacija zaposlenih o politici zaštite sistema i mehanizmima zaštite, jer ponekad i nenamerne greške zbog nestručnosti ili neinformisanosti mogu imati ozbiljne posledice.
- Kontinualna interna i povremena eksterna provera o pravilnoj primeni usvojenih i implementiranih kontrolnih mera sa ciljem da se obezbedi usklađenost sa utvrđenom politikom i procedurama, i radi preporuke potencijalnih unapređenja mera za ograničenje bezbednosnog rizika.

Na kraju, treba naglasiti da je za uspešno ograničenje bezbednosnog rizika važno ponavljanje procene rizika nakon proširenja i/ili unapređenja sistema i periodično zbog potencijalne pojave novih ranjivosti i pretnji.

8. ZAKLJUČNA RAZMATRANJA

Evolucija arhitekture savremenih industrijskih sistema daljinskog upravljanja uslovila je ranjivost ovih sistema na sajber napade. U poslednjim decenijama bezbednost SCADA sistema je postala značajan problem. Šire posmatrano, bezbednost ovih sistema je od velikog značaja zbog njihove nezamenljive uloge u svetskoj privredi. Iz tog razloga zaštita industrijskih sistema daljinskog upravljanja je aktuelna oblast istraživanja u kojoj se očekuju konkretna i unapređena rešenja procesa upravljanja bezbednosnim rizikom.

Napadi kao što je DDoS potencijalno ugrožavaju vitalne funkcije industrijskog procesa. S obzirom da za ovu vrstu napada ne postoje apsolutno pouzdani mehanizmi zaštite i mehanizmi za smanjenje rizika od ove vrste napada su ograničeni. Ovo su razlozi zbog kojih ova vrsta napada predstavlja ozbiljnu pretnju infrastrukturi savremenih telekomunikacionih mreža u industriji. U istraživanju je analizirana ranjivost industrijskih sistema za daljinsko upravljanje na infrastrukturne napade. Za te potrebe razvijen je simulacioni model SCADA sistema i simuliran DDoS napad. U simulaciji su analizirane performanse ključnih komponenti sistema u uslovima napada. Razvoj simulacionog modela je pružio mogućnost analize performansi operativnog servisa daljinskog upravljanja u uslovima DDoS napada. Rezultati simulacije ukazuju na degradaciju performansi i uskraćivanje usluga operativnog servisa daljinskog upravljanja sa željenim kvalitetom, što potvrđuje da je SCADA sistem ranjiv na ovu vrstu napada. U uslovima degradiranih performansi onemogućeno je pružanje operativnog servisa daljinskog upravljanja. Moguće rešenje zaštite se zasniva na filtriranju saobraćaja u cilju sprečavanja napada. Zato je u istraživanju posebna pažnja usmerena na sisteme za detekciju i prevenciju napada. U disertaciji su prikazane karakteristike i specifičnosti IDPS tehnologija koje se primenjuju u SCADA sistemima.

Proces upravljanja bezbednosnim rizikom obuhvata analizu rizika, metodologiju procene rizika, izbor mehanizama zaštite i donošenje odluke o implementaciji odgovarajućih mehanizama. Najvažniji deo procesa upravljanja rizikom je procena rizika, a to je ujedno i oblast upravljanja rizikom koja je najpodložnija greškama. U disertaciji su predložena dva nova metoda procene bezbednosnog rizika u kojima se

akcenat stavlja na posledice napada i identifikovanje uslova koji utiču na stepen rizika. Posebna pažnja je usmerena na izbor parametara koji kvantifikuju gubitke koji su posledica sajber napada i na određivanje njihovih vrednosti. Preduslov za određivanje ovih faktora je definisanje ključnih indikatora performansi u skladu sa zahtevanim poslovnim ciljevima.

Prvi, osnovni metod, predlaže da se vrednosti kvantitativnih parametara određuju na osnovu statističke analize relevantnih arhiviranih veličina. Drugi, hibridni metod, osim analize arhivskih podataka predlaže uzimanje u obzir subjektivnog mišljenja stručnjaka koji su relevantni za proces upravljanja i eksploatacije u predmetnom industrijskom sistemu daljinskog upravljanja. Predložen je AHP metod za kvantifikovanje mišljenja pojedinih stručnajka uzimajući u obzir njihovu stručnost, radno iskustvo, sferu rada i drugih parametara. Posebna prednost ovog metoda je u tome što se može primenjivati i u fazi projektovanja sistema za daljinsko upravljanje, kada arhivski podaci nisu dostupni. U takvim slučajevima se procena rizika obavlja samo na osnovu subjektivnog mišljenja stručnjaka, izostavlja se faza analize arhiva.

U zavisnosti od primene metoda predložena su dva načina izražavanja mere rizika, kvalitativno i monetarno. Oba metoda omogućuju *cost/benefit* analizu i izbor optimalnih mehanizama zaštite. Definisanje prihvatljivog praga za povrat investicija u zaštitu omogućuje donošenje odluke o racionalnom ulaganju u zaštitu SCADA sistema.

Verifikacija predloženih metoda za procenu bezbednosnog rizika i testiranje metoda obavljeno je u dve studije slučaja. Prva studija slučaja je u realnom okruženju protočne hidroelektrane, a druga studija slučaja je definisana za SCADA sistem u magistralnom gasovodu. Rezultati studija slučaja su pokazali da su metodi pogodni za identifikaciju ranjivosti sistema i da su praktični i primenljivi u različitim sektorima i industrijama. Na kraju, pokazalo se da su metodi efikasni u proceni mere bezbednosnog rizika od infrastukturnog napada i proceni isplativosti ulaganja u poboljšanje bezbednosti informacione infrastrukture posmatranog SCADA sistema. Studija slučaja u magistralnom gasovodu pokazala je da je metod primenljiv u fazi projektovanja sistema, kada arhive sa relevantnim podacima nisu dostupne.

U disertaciji su na kraju razmatrane mere za ograničenje bezbednosnog rizika. Predložena je arhitektura sistema u skladu sa *Defense-in-Depth* strategijom i adekvatni mehanizmi zaštite.

Naučni doprinosi sprovedenih istraživanja, koja predstavljaju predmet ove disertacije su:

- utvrđivanje stepena degradacije ključnih performansi (raspoloživost, kašnjenje, procenat izgubljenih paketa, opterećenje procesorskih resursa) u različitim uslovima distribuiranih napada na informacioni i komunikacioni sistem za podršku daljinskog upravljanja;
- definisanje novih parametara bezbednosnog rizika, zasnovanih na učestanosti distribuiranih napada i njihovom uticaju na ključne performanse sistema;
- predlog i evaluacija dva originalna metoda procene bezbednosnog rizika u industrijskim sistemima daljinskog upravljanja, zasnovanog na prethodno definisanim kvantitativnim parametrima rizika.

Mogući pravci daljeg istraživanja su unapređenje metoda u tri pravca: (1) analiza rizika u uslovima drugih vrsta napada, (2) primena fazi logike (*Fuzzy Logic*) u domenu kvantifikovanja rezultata analize arhivskih podataka i stručnih znanja i (3) prilagođenje metoda za primenu u uslovima migracije SCADA sistema u *cloud* okruženje.

LITERATURA

[1] CIGRÉ Technical Brochure TB 419, "Treatment of Information Security for Electric Power Utilities (EPUs)," CIGRÉ WGD2 22, 2010.

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

[3] B. Galloway and G. P. Hancke, "Introduction to Industrial Control Networks," *IEEE Communications Surveys and Tutorials,* vol. 15, no. 2, pp. 86-880, 2013.

[4] J. Gao, J. Liu, B. Rajan, R. Nori, B. Fu, Y. Xiao, W. Liang and P. C. Chen, "SCADA Communication and Security Issues," *Security and Communication Networks,* vol. 7, no. 1, pp. 175-194, 2014.

[5] I. Ahmed, S. Obermeier, M. Naedele and G. G. Richard III, "SCADA Systems: Challenges for Forensic Investigators," *Computer,* vol. 42, no. 12, pp. 44-51, 2012.

[6] B. Zhu, A. Joseph and S. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," in *Proceedings of the 2011 International Conference on the Internet of Things and the 4th International Conference on Cyber, Physical, and Social Computing*, Dalian, China, October 2011.

[7] E. Byres and J. Lowe, "The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems," in *Proceedings of the VDE 2004 Congress*, Berlin, Germany, October 2004.

[8] B. Miller and D. Rowe, "A Survey SCADA of and Critical Infrastructure Incidents," in *Proceedings of the 1st Annual Conference on Research in Information Technology*, Calgary, AB, Canada, October 2012.

[9] A. Nicholson, S. Webber, S. Dyer, T. Patel and H. Janicke, "SCADA Security in the Light of Cyber-Warfare," *Computers & Security,* vol. 31, no. 4, pp. 418-436, 2012.

[10] M. Stojanović, S. Boštjančič Rakas / J. Marković-Petrović, „SCADA sistemi u *cloud* okruženju,“ u *Zborniku radova 35. Simpozijuma PosTel 2017*, Beograd, 5 i 6 decembar 2017.

[11] R. L. Krutz, Securing SCADA Systems, Wiley Publishing Inc, 2006.

[12] W. T. Shaw, "SCADA System Vulnerabilities to Cyber Attack," *Electric Energy T&D Magazine,* vol. 8, no. 6, pp. 62-65, September/October 2004.

[13] M. Stojanović / J. Marković-Petrović, „Principi realizacije IP mreža za podršku daljinskog upravljanja elektroenergetskim objektima,“ u *Zborniku radova 31. Simpozijuma PosTel 2013*, Beograd, 3 i 4 decembar 2013.

[14] A. Chakrabarti and G. Manimaran, "Internet Infrastructure Security: A Taxonomy," *IEEE Network,* vol. 16, no. 6, pp. 13-21, November/December 2002.

[15] R. C. Newman, Computer Security: Protecting Digital Resources, Jones & Bartlett Learning, 2009.

[16] M. Stojanović / V. Aćimović-Raspopović, „Zaštita infrastrukture elektroprivrednih telekomunikacionih mreža sa tehnologijom Internet protokola," u *Zborniku radova 27. Savetovanja JUKO CIGRÉ, RD2–09*, Zlatibor, maj 2005.

[17] 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.

[18] K. Wilhoit, "Who's Really Attacking Your ICS Equipment," Trend Micro Incorporated, 2013.

[19] G. Ericsson, "Managing Information Security in an Electric Utility," *Electra Magazine-Cigré,* no. 216, 2004.

[20] S. Karnouskos, "Stuxnet Worm Impact on Industrial Cyber-Physical System Security," in *Proceedings of the IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society*, Melbourne, Australia, November 2011.

[21] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby and K. Stoddart, "A Review of Cyber Security Risk Assessment Methods for SCADA Systems," *Computers & Security,* vol. 56, pp. 1-27, 2016.

[22] B. Gregory-Brown, "Securing Industrial Control Systems-2017," A SANS Survey. SANS Institute, 2017. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/securing-industrial-control-systems-2017-37860.

[23] "The Repository of Industrial Security Incidents," [Online]. Available: http://www.risidata.com/Database.

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

[25] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94, February 2007.

[26] V. Jyothsna, V. V. Rama Prasad and K. Munivara Prasad, "A Review of Anomaly Based Intrusion Detection Systems," *International Journal of Computer Applications,* vol. 28, no. 7, pp. 26-35, 2011.

[27] M. H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools," *IEEE Communications Surveys and Tutorials,* vol. 16, no. 1, pp. 303-336, 2014.

[28] G. Gu, P. Fogla, D. Dagon, W. Lee and B. Skoric, "Measuring Intrusion Detection Capability: An Information-Theoretic Approach," in *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security (ASIACCS '06)*, Taipei, Taiwan, 2006.

[29] M. Stojanović / J. Marković-Petrović, „IDPS tehnologije u industrijskim sistemima daljinskog upravljanja," u *Zborniku radova 32. Simpozijuma PosTel 2014*, Beograd, 2 i 3 decembar 2014.

[30] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner and A. Valdes, "Using Model-based Intrusion Detection for SCADA Networks," in *Proceedings of the SCADA Security Scientific Symposium*, Miami Beach, FL, USA, January 2007.

[31] A. Skorobogatjko, P. Dorogovs and A. Romanovs, "The Use of Intrusion Detection Systems Based on the Network Behaviour Analysis in SCADA Networks," *Information Technology and Management Science,* vol. 12, no. 1, pp. 171-175, 2012.

[32] B. Zhu and S. Shankar, "SCADA-specific Intrusion Detection/Prevention Systems: A Survey and Taxonomy," in *Proceedings of the 1st Workshop on Secure Control Systems (SCS)*, Stockholm, Sweden, 2010.

[33] M. Mantere, M. Sailio and S. Noponen, "Network Traffic Features for Anomaly Detection in Specific Industrial Control System Network," *Future Internet,* vol. 5, no. 4, pp. 460-473, 2013.

[34] A. Rot, "IT Risk Assessment: Quantitative and Qualitative Approach," in *Proceedings of the World Congress on Engineering and Computer Science, WCECS 2008*, October 2008.

[35] T. Tsiakis, "Information Security Expenditures: A Techno-Economic Analysis," *International Journal of Computer Science and Network Security,* vol. 10, no. 4, pp. 7-11, 2010.

[36] C. Iheagwara, "The Effect of Intrusion Detection Management Methods on the Return on Investment," *Computers & Security,* vol. 23, no. 3, pp. 213-228, 2004.

[37] W. Sonnenreich, J. Albanese and B. Stout, "Return on Security Investment (ROSI) - A Practical Quantitative Model," *Journal of Research and Practice in Information Technology,* vol. 38, no. 1, pp. 45-56, 2006.

[38] Y. Y. Haimes, Risk Modeling, Assessment and Management, John Wiley & Sons, 2004.

[39] R. S. Ross, "Guide for Conducting Risk Assessments," NIST Special Publication 800-30 Rev 1, 2012.

[40] G. N. Ericsson, "Information Security for Electric Power Utilities (EPUs)—CIGRÉ Developments on Frameworks, Risk Assessment, and Technology," *IEEE Transactions on Power Delivery,* vol. 24, no. 3, pp. 1174-1181, 2009.

[41] C. C. Huang, K. J. Farn and F. Y. S. Lin, "A Study on Implementations of Information Security Risk Assessment: Application to Chlorine Processing Systems of Water Treatment Plants," *International Journal of Network Security,* vol. 16, no. 4, pp. 241-248, 2014.

[42] H. Chivers, J. A. Clark and P.-C. Cheng, "Risk Profiles and Distributed Risk Assessment," *Computers & Security,* vol. 28, no. 7, pp. 521-535, 2009.

[43] C. D. Huang, Q. Hu and R. S. Behra, "Economics of Information Security Investment in the Case of Simultaneous Attacks," in *Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS 2006)*, Cambridge, England, June 2006.

[44] H. Wei, J. Alves-Fross and T. Soule, "A Layered Decision Model for Cost-Effective System Security," *International Journal of Information and Computer Security,* vol. 2, no. 3, p. 308–335, 2008.

[45] M. Stojanovic, V. Acimovic-Raspopovic and S. Bostjancic Rakas, "Security Management Issues for Open Source ERP in the NGN Environment," in *Free and Open Source Enterprise Resource Planning: Systems and Strategies*, New York, IGI Global, 2011, pp. 165-181.

[46] T. Sommestad, G. N. Ericsson and J. Nordlander, "SCADA System Cyber Security: A Comparison of Standards," in *Proceedings of the IEEE Power and Energy Society General Meeting*, 25-29 July 2010.

[47] "ISO/IEC 27005: Information Technology – Security Techniques – Information Security Risk Management," ISO/IEC, 2011.

[48] ITU-T Recommendation X 1055, "Risk Management and Risk Profile Guidelines for Telecommunication Organizations," ITU-T, 2008.

[49] A. Behnia, R. A. Rashid and J. A. Chaudhry, "A Survey of Information Security Risk Analysis Methods," *Smart Computing Review,* vol. 2, no. 1, pp. 79-93, 2012.

[50] "Inventory of Risk Management / Risk Assessment Methods and Tools," [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory.

[51] CIGRÉ Technical Brochure TB 317, "Security for Information Systems and Intranets in Electric Power Systems," CIGRÉ JWGD2/B2/C2, 2007.

[52] B. Karabacak and I. Sogukpinar, "ISRAM: Information Security Risk Analysis Method," *Computers & Security,* vol. 24, no. 2, pp. 147-159, 2005.

[53] N. Poolsappasit, R. Dewri and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs," *IEEE Transactions on Dependable and Secure Computing,* vol. 9, no. 1, pp. 61-74, 2012.

[54] 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.

[55] B. Suh and I. Han, "The IS Risk Analysis Based on a Business Model," *Information & Management,* vol. 41, no. 2, pp. 149-158, 2003.

[56] Z. Yazar, "A Qualitative Risk Analysis and Management Tool – CRAMM," SANS Institute, 2002.

[57] "The CORAS Project," [Online]. Available: http://coras.sourceforge.net/.

[58] G. Francia III, D. Thornton and J. Dawson, "Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems," in *Proceedings of the International Conference on Security and Management (SAM), The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp)*, 2012.

[59] G. Dondossola, F. Garrone and J. Szanto, "Cyber Risk Assessment of Power Control Systems – A Metrics Weighed by Attack Experiments," in *Proceedings of the 2011 IEEE Power and Energy Society General Meeting (CD)*, San Diego, CA, 2011.

[60] S. M. Papa, W. D. Casper and S. Nair, "Availability Based Risk Analysis for SCADA Embedded Computer Systems," in *Proceedings of the 2011 World Congress in Computer Science, Computer Engineering, and Applied Computing (WorldComp11)*, Las Vegas, NV, July 2011.

[61] J. Marković-Petrović / M. Stojanović, „Analiza metoda za procenu bezbednosnog rizika SCADA sistema," u *Zborniku radova 16. Simpozijuma UPRAVLJANJE I TELEKOMUNIKACIJE U EES, CIGRÉ Srbija, RD2–14*, Kladovo, 2014.

[62] J. Yu, A. Mao and Z. Guo, "Vulnerability Assessment of Cyber Security in Power Industry," in *Proceedings of the Power Systems Conference and Exposition (PSCE), IEEE*, 2006.

[63] D. I. Gertman, R. Folkers and J. Roberts, "Scenario-Based Approach to Risk Analysis in Support of Cyber Security," in *Proceedings of the 5th International Topical Meeting on Nuclear Plant Instrumentation Controls, and Human Machine Interface Technology*, 2006.

[64] A. A. Cárdenas, S. Amin, Z. S. Lin, Y. L. Huang, C. Y. Huang and S. Sastry, "Attacks Against Process Control Systems: Risk Assessment, Detection, and Response," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, Hong Kong, China, March 2011.

[65] P. S. Woo and B. H. Kim, "A Study on Quantitative Methodology to Assess Cyber Security Risk of SCADA Systems," *Advanced Materials Research,* Vols. 960-961, pp. 1602-1611, 2014.

[66] E. Byres, M. Franz and D. Miller, "The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems," in *Proceedings of the International Infrastructure Survivability*

Workshop, 2004.

[67] M. Mcqueen, W. Boyer, M. Flynn and G. Beitel, "A Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System," in *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (ACM)*, 2006.

[68] C.-W. Ten, G. Manimaran and C.-C. Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans,* vol. 40, no. 4, pp. 853-865, 2010.

[69] J. Yan, M. Govindarasu, C.-C. Liu and U. Vaidya, "A PMU-Based Risk Assessment Framework for Power Control Systems," in *Proceedings of the Power and Energy Society General Meeting (PES), IEEE*, 2013.

[70] A. Roy, D. S. Kim and K. S. Trivedi, "Cyber Security Analysis using Attack Countermeasure Trees," in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (ACM)*, 2010.

[71] E. Lemay, W. Unkenholz, D. Parks, C. Muehrcke, K. Keefe and W. H. Sanders, "Adversary-Driven State-Based System Security Evaluation," in *Proceedings of the 6th International Workshop on Security Measurements and Metrics (ACM)*, 2010.

[72] S. Kriaa, M. Bouissou and L. Piétre-Cambacédés, "Modeling the Stuxnet Attack with BDMP: Towards More Formal Risk Assessments," in *Proceedings of the 7th International Conference on Risk and Security of Internet and Systems (CRiSIS), IEEE*, 2012.

[73] S. Patel, J. Graham and P. Ralston, "Quantitatively Assessing the Vulnerability of Critical Information Systems: A New Method for Evaluating Security Enhancements," *International Journal of Information Management,* vol. 28, no. 6, p. 483–491, 2008.

[74] C.-W. Ten, C.-C. Liu and G. Manimaran, "Vulnerability Assessment of Cybersecurity for SCADA Systems," *IEEE Transactions on Power Systems,* vol. 23, no. 4, pp. 1836-1846, 2008.

[75] M. H. Henry, R. M. Layer, K. Z. Snow and D. R. Zaret, "Evaluating the Risk of Cyber Attacks on SCADA Systems via Petri Net Analysis with Application to Hazardous Liquid Loading Operations," in *Proceedings of the IEEE Conference on Technologies for Homeland Security*, 2009.

[76] M. Beccuti, S. Chiaradonna, F. Di Giandomenico, S. Donatelli, G. Dondossola and G. Franceschinis, "Quantification of Dependencies Between Electrical and Information Infrastructures," *International Journal of Critical Infrastructure Protection,* vol. 5, no. 1, pp. 14-27, 2012.

[77] F. Baiardi, C. Telmon and D. Sgandurra, "Hierarchical, Model-Based Risk Management of Critical Infrastructures," *Reliability Engineering & System Safety,* vol. 94, no. 9, pp. 1403-1415, 2009.

[78] M. Henry and Y. Haimes, "A Comprehensive Network Security Risk Model for Process Control Networks," *Risk Analysis,* vol. 29, no. 2, pp. 223-248, 2009.

[79] J. Guan, J. Graham and J. A. Hieb, "Digraph Model for Risk Identification and Management in SCADA Systems," in *Proceedings of the 2011 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2011.

[80] R. Hewett, S. Rudrapattana and P. Kijsanayothin, "Cyber-Security Analysis of Smart Grid SCADA Systems with Game Models," in *Proceedings of the 9th Annual Cyber and Information Security Research Conference (ACM)*, 2014.

[81] C. Chittester and Y. Y. Haimes, "Risks of Terrorism to Information Technology and to Critical Interdependent Infrastructures," *Journal of Homeland Security and Emergency Management,* vol. 1, no. 4, 2004.

[82] K. Huang, C. Zhou, Y. C. Tian, W. Tu and Y. Peng, "Application of Bayesian Network to Data-Driven Cyber-Security Risk Assessment in SCADA Networks," in *Proceedings of the 27th International Telecommunication Networks and Applications Conference (ITNAC), IEEE*, Melburne, Australia, 2017.

[83] M. R. Permann and K. Rhode, "Cyber Assessment Methods for SCADA Security," in *Proceedings of the 15th Annual Joint ISA POWID/EPRI Controls and Instrumentation Conference*, Nashville, TN, 2005.

[84] G. Dondossola, O. Lamquet and A. Torkilseng, "Key Issues and Related Methodologies in the Security Risk Analysis and Evaluation of Electric Power Control Systems," in *Proceedings of the CIGRÉ 2006 session*, Paris, France, 2006.

[85] C. Beggs and M. Warren, "Safeguarding Australia from Cyber-terrorism: A Proposed Cyber-terrorism SCADA Risk Framework for Industry Adoption," in *Proceedings of the Australian Information Warfare and Security Conference*, December 2009.

[86] J. Song, J. Lee, C. Lee, K. Kwon and D. Lee, "A Cyber Security Risk Assessment for the Design of I&C Systems in Nuclear Power Plants," *Nuclear Engineering and Technology,* vol. 44, no. 8, pp. 919-928, 2012.

[87] A. Shameli-Sendi, R. Aghababaei-Barzegar and M. Cheriet, "Taxonomy of Information Security Risk Assessment (ISRA)," *Computers & Security,* vol. 57, pp. 14-30, 2016.

[88] S. K. Pandey, "A Comparative Study of Risk Assessment Methodologies for Information Systems," *Bulletin of Electrical Engineering and Informatics,* vol. 1, no. 2, pp. 111-122, 2012.

[89] J. Markovic-Petrovic and M. Stojanovic, "Analysis of SCADA System Vulnerabilities to DDoS Attacks," in *Proceedings of the 2013 11th International Conference on Telecommunications in Modern Satellite Cable and Broadcasting Services - TELSIKS 2013*, Nis, October 2013.

[90] S. M. Specht and R. B. Lee, "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures," in *Proceedings of International Workshop on Security in Parallel and Distributed Systems*, 2004.

[91] T. Peng, C. Leckie and K. Ramamohanarao, "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems," *ACM Computing Surveys,* vol. 39, no. 1, 2007.

[92] E. Alomari, S. Manickam, B. B. Gupta, S. Karuppayah and R. Alfaris, "Botnetbased Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art," *International Journal of Computer Applications,* vol. 49, no. 7, pp. 24-32, July 2012.

[93] M. Guizani, A. Rayes, B. Khan and A. Al-Fuqaha, Network Modeling and Simulation: A Practical Perspective, John Wiley & Sons, 2010.

[94] S. Nazir, S. Patel and D. Patel, "Assessing and Augmenting SCADA Cyber Security: A Survey of Techniques," *Computers & Security,* vol. 70, pp. 436-454, 2017.

[95] J. Marković-Petrović / M. Stojanović, „Performanse operativnog servisa daljinskog upravljanja u uslovima DDoS napada," u *Zborniku radova 31. Savetovanja CIGRÉ Srbija, RD2–13*, Zlatibor, 2013.

[96] J. Marković-Petrović / M. Stojanović, „Zaštita telekomunikaciono-informacionog sistema u Elektroprivredi," u *Zborniku radova 15. Simpozijuma UPRAVLJANJE I TELEKOMUNIKACIJE U EES, CIGRÉ Srbija, RD2–03*, Donji Milanovac, oktobar 2012.

[97] U. Lamping, R. Sharpe and E. Warnicke, "Wireshark User's Guide for Wireshark 1.7," [Online]. Available: www.wireshark.org/download/docs/user–guide–a4.pdf.

[98] M. Stojanović / V. Aćimović-Raspopović, Savremene IP mreže: arhitekture, tehnologije i protokoli, Beograd: Akademska misao, 2012.

[99] CIGRÉ Technical Brochure TB 249, "Integrated Service Networks for Utilities," CIGRÉ WGD2 07, 2004.

[100] 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.

[101] J. Markovic-Petrovic and M. Stojanovic, "A Hybrid Security Risk Assessment Method for SCADA Networks," in *Proceedings of 6th International Symposium on Industrial Engineering*, Belgrade, 24 and 25 September 2015.

[102] ITU-T Recommendation E 419, "Business Oriented Key Performance Indicators for Management of Networks and Services," ITU-T, 2006.

[103] T. Saaty, "Decision Making With the Analytic Hierarchy Process," *International Journal of Services Sciences,* vol. 1, no. 1, pp. 83-98, 2008.

[104] "Cyber Security on the Offense: A Study of IT Security Experts," Ponemon Institute, 2012.

[105] J. Pescatore, "DDoS Attacks Advancing and Enduring: A SANS Survey," SANS Tehnical Report, 2014.

[106] J. Marković-Petrović, Z. Živković, A. Car, N. Jemuović / I. Ćirić, „Modernizacija sistema daljinskog nadzora i upravljanja u HE „Đerdap 2“,“ u *Zborniku radova 31. Savetovanja CIGRÉ Srbija, RD2–01*, Zlatibor, maj 2013.

[107] S. A. Baker, S. Waterman and G. Ivanov, "Critical Infrastructure in the Age of Cyber War," McAfee, Incorporated, 2009.

[108] N. Jevtović, N. Panjevac, J. Marković-Petrović / Z. Živković, „Implementacija bezbednosnog mehanizma u sistem daljinskog nadzora i upravljanja HE „Đerdap 2“,“ u *Zborniku radova 32. Savetovanja CIGRÉ Srbija, RD2–11*, Zlatibor, maj 2015.

[109] 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, p. 579, 2017.

[110] Y. Wadhawan and C. Neuman, "Evaluating Resilience of Gas Pipeline Systems Under Cyber-Physical Attacks: A Function-Based Methodology," in *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy (ACM)*, 2016.

BIOGRAFIJA AUTORA

Jasna D. Marković-Petrović je rođena 4. jula 1968. godine u Negotinu. Osnovnu školu završila je u Negotinu, a gimnaziju u Beogradu. Elektrotehnički fakultet Univerziteta u Beogradu upisala je 1987. godine. Diplomirala je na Profilu Elektronika i telekomunikacije sa prosečnom ocenom 9,26. Diplomski rad, sa temom „Primena viših programskih jezika u telekomunikacijama“, odbranila je decembra 1992. godine, sa ocenom 10. Poslediplomske studije na Elektrotehničkom fakultetu Univerziteta u Beogradu, smer Digitalni prenos podataka, upisala je 1993. godine. Položila je ispite predviđene nastavnim planom i programom sa prosečnom ocenom 10. Magistarsku tezu, pod nazivom „Principi projektovanja multiservisnih IP mreža u elektroprivredi“, odbranila je septembra 2011. godine.

Zaposlena je u JP EPS, u Ogranku HE Đerdap. Rukovodila je razvojem i modernizacijom više telekomunikacionih, informacionih, mernih i kontrolno-upravljačkih sistema, koji su od interesa za proizvodnju električne energije: implementacija i održavanje sistema za daljinski nadzor i upravljanje; uspostavljanje Tehničkog sistema upravljanja; uspostavljanje i održavanje sistema za merenje električne energije; izgradnja i održavanje telekomunikacione mreže; implementacija poslovnog informacionog sistema; implementacija i održavanje sistema za kontrolu pristupa i evidenciju prisustva zaposlenih; rukovođenje realizacijom projekta modernizacije sistema za daljinski nadzor i upravljanje i centralne komande; rukovođenje realizacijom projekta telekomunikacionog povezivanja elektrana HE „Đerdap 2“ i Portile de Fier II (Rumunija).

Član je Studijskog komiteta D2 (Informacioni sistemi i telekomunikacije) u srpskom nacionalnom komitetu CIGRÉ – „CIGRÉ Srbija“.

Изјава о ауторству

Име и презиме аутора **Јасна Марковић-Петровић**

Број индекса _____

Изјављујем

да је докторска дисертација под насловом

Процена безбедносног ризика у индустријским системима даљинског управљања

- резултат сопственог истраживачког рада;
- да дисертација у целини ни у деловима није била предложена за стицање друге дипломе према студијским програмима других високошколских установа;
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио/ла интелектуалну својину других лица.

Потпис аутора

У Београду, 4. 6. 2018.

_____

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора Јасна Марковић-Петровић

Број индекса _____

Студијски програм _____

Наслов рада Процена безбедносног ризика у индустријским системима даљинског управљања

Ментор проф. др Мирјана Стојановић

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла ради похрањена у **Дигиталном репозиторијуму Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског назива доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис аутора

У Београду, 4. 6. 2018.

_____

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

Процена безбедносног ризика у индустријским системима даљинског управљања

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигиталном репозиторијуму Универзитета у Београду и доступну у отвореном приступу могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство (CC BY)
2. Ауторство – некомерцијално (CC BY-NC)
3. Ауторство – некомерцијално – без прерада (CC BY-NC-ND)
4. Ауторство – некомерцијално – делити под истим условима (CC BY-NC-SA)
5. Ауторство – без прерада (CC BY-ND)
6. Ауторство – делити под истим условима (CC BY-SA)

(Молимо да заокружите само једну од шест понуђених лиценци.
Кратак опис лиценци је саставни део ове изјаве).

Потпис аутора

У Београду, 4. 6. 2018.

1. Ауторство - Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце, чак и у комерцијалне сврхе. Ово је најслободнија од свих лиценци.

2. Ауторство – некомерцијално. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела.

3. Ауторство - некомерцијално – без прераде. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела. У односу на све остале лиценце, овом лиценцом се ограничава највећи обим права коришћења дела.

4. Ауторство - некомерцијално – делити под истим условима. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца не дозвољава комерцијалну употребу дела и прерада.

5. Ауторство – без прераде. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца дозвољава комерцијалну употребу дела.

6. Ауторство - делити под истим условима. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца дозвољава комерцијалну употребу дела и прерада. Слична је софтверским лиценцама, односно лиценцама отвореног кода.