

**НАСТАВНО-НАУЧНОМ ВЕЋУ**

**Предмет:** Подобност теме и кандидата **мр Јасне Д. Марковић-Петровић** за израду докторске дисертације

Одлуком Наставно-научног већа Саобраћајног факултета у Београду бр. 25/3 од 19. фебруара 2014. године, именовани смо за чланове Комисије за оцену подобности теме и кандидата мр Јасне Д. Марковић-Петровић за израду докторске дисертације и научне заснованости теме под називом:

**„Процена сигурносног ризика у индустријским системима даљинског управљања“.**

На основу материјала приложеног уз Захтев кандидата, Комисија подноси следећи

**РЕФЕРАТ**

**1. Подаци о кандидату**

**1.1. Биографски подаци**

Јасна Д. Марковић-Петровић је рођена 4. јула 1968. године у Неготину. Основну школу завршила је у Неготину, а гимназију у Београду. Носилац је Вукових диплома на нижем и средњем нивоу образовања.

Електротехнички факултет Универзитета у Београду уписала је 1987. године. Дипломирала је на Профилу Електроника и телекомуникације са просечном оценом 9,26. Дипломски рад, са темом „Примена виших програмских језика у телекомуникацијама“, одбранила је 9. децембра 1992. године, са оценом 10.

Последипломске студије на Електротехничком факултету Универзитета у Београду, смер Дигитални пренос података, уписала је 1993. године. Положила је испите предвиђене наставним планом и програмом са просечном оценом 10. Магистарску тезу, под називом „Принципи пројектовања мултисервисних IP мрежа у електропривреди“, одбранила је 21. септембра 2011. године.

Пријавила је тему докторске дисертације под називом „Процена сигурносног ризика у индустријским системима даљинског управљања“ на Саобраћајном факултету у Београду, 13. јануара 2014. године.

Као аутор или коаутор објавила је више научних радова на скуповима националног и међународног значаја.

Прво запослење Јасне Марковић-Петровић било је у институту ИРИТЕЛ, 1993. године, на пословима развоја оперативног система за чворну телефонску централу.

Од јуна 1993. године запослена је у ЈП Електропривреда Србије, у ПД „Хидроелектране Ђердап“, огранак ХЕ „Ђердап 2“. У периоду 1993–2007. године била је распоређена на радна места: Инжењер за информатику, Самостални инжењер за информатику и Водећи инжењер за информатику, а затим на радна места: Руководилац Техничке службе (2007–2009. године) и Заменик директора ХЕ „Ђердап 2“ за производњу (2009–2013. године). Тренутно обавља послове Водећег инжењера за информатику.

Руководила је развојем и модернизацијом више телекомуникационих, информационих, мерних и контролно-управљачких система, који су од интереса за производњу електричне енергије:

- имплементација и одржавање система за даљински надзор и управљање (SCADA);
- успостављање Техничког система управљања (ТСУ);
- успостављање и одржавање система за мерење електричне енергије;
- изградња и одржавање телекомуникационе мреже;
- имплементација пословног информационог система;
- имплементација и одржавање система за контролу приступа и евиденцију присуства запослених;
- израда програма за обраду оскултационих мерења бране;
- руковођење реализацијом пројекта модернизације система за даљински надзор и управљање и централне команде;
- руковођење реализацијом пројекта телекомуникационог повезивања електрана ХЕ „Ђердап 2“ и Portile de Fier II (Румунија).

Јасна Марковић-Петровић је председник Тима за опоравак пословног континуитета у ХЕ „Ђердап 2“, у оквиру система за управљање безбедношћу информација. Учествовала је у раду тима за дефинисање Производно техничког информационог система у ЈП Електропривреда Србије (ПРОТИС), а тренутно је члан главног тима за имплементацију модула ПРОТИС-а. Такође је била члан више Стручних савета, формираних у ЈП Електропривреда Србије и ПД „Хидроелектране Ђердап“.

Јасна Марковић-Петровић је члан Студијског комитета D2 (Информациони системи и телекомуникације) у српском националном комитету CIGRÉ (Conseil International des Grands Réseaux Électriques) – „CIGRÉ Србија“. Похађала је бројне специјалистичке курсеве, који се односе на базе података, програмирање и процесно управљање.

## 1.2. Стечено научноистраживачко искуство

Кандидат Јасна Марковић-Петровић одбранила је магистарску тезу под називом „Принципи пројектовања мултисервисних IP мрежа у електропривреди“ на Електротехничком факултету у Београду, 21. септембра 2011. године. Ментор магистарске тезе била је др Мирјана Стојановић (у звању доцента Електротехничког факултета у Београду). Тема магистарске тезе припада научној области „Телекомуникације“.

У магистарској тези предложени су принципи моделовања и пројектовања мултисервисних телекомуникационих мрежа у електропривредним системима. Карактеристика ових мрежа је делимична или потпуна интеграција хетерогених телекомуникационих сервиса (оперативних и пословних), који су директно повезани са технолошким функционисањем електропривредног система. Мреже су засноване на технологији Интернет протокола (IP), при чему се претпоставља могућност примене различитих технологија комутације и преноса. Представљени су резултати исцрпне симулационе студије о интеграцији хетерогених сервиса (даљинско управљање, IP телефонија, видео-конференција и основни Интернет сервиси), принципима класификације телекомуникационог саобраћаја и избору оптималне дисциплине опслуживања пакета у циљу подршке различитих захтеваних нивоа квалитета сервиса.

Магистарска теза је написана на 90 страница и организована у седам поглавља. Прва три поглавља садрже увод у проблематику истраживања, приказ основних карактеристика телекомуникационих сервиса и теоријски основ пројектовања телекомуникационих мрежа у електропривреди. У четвртом поглављу истакнут је значај симулације у поступку пројектовања телекомуникационе мреже, а затим су укратко описани карактеристични мрежни симулатори. У петом поглављу приказани су принципи рада и структура мрежног симулатора OPNET, фазе процеса симулације, као и принципи дефинисања елемената мреже, топологије, извора саобраћаја, матрице саобраћаја и сценарија симулације. У шестом поглављу дефинисан је симулациони модел електропривредне телекомуникационе мреже, анализиран је избор оптималне дисциплине опслуживања саобраћаја у циљу подршке различитих нивоа квалитета сервиса и испитан је утицај интеграције новог сервиса на перформансе мреже. Седмо поглавље обухвата закључна разматрања.

Најважнији доприноси магистарске тезе су: (1) предлог поступка пројектовања мултисервисне електропривредне мреже засноване на технологији Интернет протокола и (2) развој симулационог модела електропривредне телекомуникационе мреже, на основу кога су извршена два примера анализе перформанси, која су указала на оптималне начине примене метода симулације у процесу пројектовања телекомуникационих мрежа у електропривреди.

После одбране магистарске тезе, научно-истраживачки рад Јасне Марковић-Петровић усмерен је ка проблематици заштите информационо-комуникационе инфраструктуре система даљинског управљања. Остварила је запажене резултате у истраживању и анализи система за детекцију и превенцију симултаних дистрибуираних инфраструктурних напада на системе даљинског управљања у електропривреди.

У наставку је дат списак референци кандидата Јасне Марковић-Петровић.

*Саопштење са међународног скупа штампано у целини (M33)*

1. **Marković–Petrović, J.**, Stojanović, M.: *Analysis of SCADA System Vulnerabilities to DDoS Attacks*, - Proceedings of the 2013 11th International Conference on Telecommunications in Modern Satellite Cable and Broadcasting Services - TELSIKS 2013, Niš, October 2013, Vol. 2, pp. 591-594.
2. **Marković–Petrović, J.**, Stojanović, M.: *Analiza servisa daljinskog upravljanja u telekomunikacionim mrežama u elektroprivredi*, -Zbornik radova 19. Telekomunikacionog foruma TELFOR, Beograd, novembar 2011, str. 270-273.
3. Srećković, M., Tomić, Ž., Fidanovski, Z., Polić-Radovanović, S., Bugarinović, A., **Marković–Petrović, J.**, Lukić, L., Krčum, D.: *Analitički i numerički prilaz optičkim sistemima za koherentno i nekoherentno zračenje*, -Zbornik radova naučno-stručnog Simpozijuma INFOTEH-JAHORINA 2011, Jahorina, mart 2011, Vol. 10, Ref. B-II-13, str. 186-190.
4. **Marković–Petrović, J.**, Stojanović, M.: *Principi projektovanja multiservisnih IP mreža u elektroprivredi*, -Zbornik radova 18. Telekomunikacionog foruma TELFOR, Beograd, novembar 2010, str. 294–297.

*Предавање по позиву са скупа националног значаја штампано у целини (M61)*

5. Stojanović, M., **Marković–Petrović, J.**: *Principi realizacije IP mreža za podršku daljinskog upravljanja elektroenergetskim objektima*, -Zbornik radova 31. Simpozijuma PosTel 2013, Beograd, decembar 2013, str. 323-332.

*Саопштење са скупа националног значаја штампано у целини (M63)*

6. **Marković–Petrović, J.**, Stojanović, M.: *Performanse operativnog servisa daljinskog upravljanja u uslovima DDoS napada*, -Zbornik radova 31. Savetovanja CIGRE Srbija, Zlatibor, maj 2013, RD2–13, str. 1-8.
7. **Marković-Petrović, J.**, Živković, Z., Car, A., Jemuović, N., Ćirić, I.: *Modernizacija sistema daljinskog nadzora i upravljanja u HE „Đerdap 2“*, -Zbornik radova 31. Savetovanja CIGRE Srbija, Zlatibor, maj 2013, RD2–01, str. 1-8.

8. **Marković–Petrović, J.**, Stojanović, M.: *Zaštita telekomunikaciono-informacionog sistema u Elektroprivredi*, -Zbornik radova 15. Simpozijuma UPRAVLJANJE I TELEKOMUNIKACIJE U EES, CIGRÉ Srbija, Donji Milanovac, oktobar 2012, RD2–03, str.1-8. (Проглашен за најзапаженији рад у Студијском комитету D2).
9. Milić, S., Miladinović, N., **Marković–Petrović, J.**: *Računarsko-merni i komunikacioni sistemi u daljinskom nadzoru i dijagnostici*, -Zbornik radova 30. Savetovanja CIGRÉ Srbija, Zlatibor, maj–jun 2011, RD2–12, str. 1-8.
10. Milić, S., Srećković, M., Karanović, N., Kršenković, Z., **Marković–Petrović, J.**: *On–line Remote Monitoring of Generators and Transformers in Energy Power Systems*, -Zbornik radova konferencije Elektrane 2010 (Power Plants 2010), Vrnjačka Banja, oktobar 2010. Zbornik radova izdat na CD-u.
11. Tomić, Ž., **Marković, J.**: *Sistemska radno mesto u najavnom i posredovanom sistemu (NIPS)*, -Zbornik radova XXXVII konferencije ETAN, Beograd, 1993, sveska IV, str. 343-348.

### *Студије и пројекти*

1. *Главни пројекат: Смештај и инсталација телекомуникационе опреме за изградњу оптичког система преноса по брани и приводних оптичких система*, Енергопројект ЕНТЕЛ, Инвеститор ЈП ЕПС, 2011. – Учешће у реализацији пројекта.
2. *Главни пројекат адаптације за DV 110kV br.1209 РП Ђердап 2 – граница – Румунија, замена заштитног ужета ужетом са оптичким влакнима (OPGW)*, Електроисток – пројектни биро, Инвеститор ЈП ЕПС, 2011. – Учешће у реализацији пројекта.
3. *Извођачки пројекат реконструкције и модернизације централне команде „ХЕ Ђердап 2“, ознака ТП.100.130, рег. број 100.368.*, Институт Михајло Пупин, Инвеститор ПД „ХЕ Ђердап“, 2011. – Учешће у реализацији пројекта.
4. *ХЕ „Ђердап II“ Додатна електрана са монтажним блоком - проширење централне команде*, Енергопројект Хидроинжењеринг, Инвеститор Електропривреда Србије – ЈП Ђердап – Кладово, 2001. – Учешће у реализацији пројекта.
5. *Главни пројекат и повезивање крајње станице RTU-AT32 - Објекат 40203/ХЕ 110kV Ђердап 2/РП*, Институт „Михајло Пупин“, Инвеститор Електропривреда Србије, Центар за интегрални информациони систем, 1994. – Учешће у реализацији пројекта.
6. *Главни пројекат и повезивање крајње станице RTU-AT32 - Објекат 40203/ХЕ 110kV Ђердап 2/ЦК*, Институт „Михајло Пупин“, Инвеститор Електропривреда Србије, Центар за интегрални информациони систем, 1994. – Учешће у реализацији пројекта.
7. *Припрема хидроелектрана ЕПС-а за укључење у технички систем управљања – књига IV: Ђердап II*, Енергопројект Хидроинжењеринг, Инвеститор Електропривреда Србије, Дирекција за инвестиције, 1993. – Учешће у реализацији пројекта.

### 1.3. Оцена подобности кандидата за рад на предложеној теми

Мр Јасна Марковић-Петровић је својим досадашњим истраживачким активностима испољила квалитет, заинтересованост и стручност за научни и истраживачки рад. Досадашњи стручни рад и истраживачка делатност су суштински повезани са темом докторске дисертације и квалификују мр Јасну Марковић-Петровић за успешан рад на предложеној теми. На основу биографских података, научних и стручних активности, одбрањене магистарске тезе, као и објављених радова, Комисија сматра да је кандидат мр Јасна Марковић-Петровић подобра за рад на предложеној теми докторске дисертације.

## **2. Предмет и циљ истраживања**

Функција даљинског управљања индустријским системом поставља специфичне захтеве за информационо-комуникациону инфраструктуру, која треба да обезбеди процесирање и поуздан пренос хетерогених информација са различитим захтевима за квалитет сервиса.

Комуникација се остварује између центра управљања и објекта индустријског система, као и између дистрибуираних центара управљања. SCADA (*Supervisory Control and Data Acquisition*) је дистрибуирани систем даљинског надзора и управљања, који прикупља и анализира информације у реалном времену о индустријском процесу и стању погона. Архитектуру SCADA система сачињавају:

- подсистем систем даљинских телеметријских јединица и програмабилних логичких контролера, повезаних на мерне претварааче и сензоре у процесу и
- информационо-комуникациона инфраструктура, која се састоји од следећих подсистема: (1) комуникациони подсистем, који обезбеђује везу између централне станице и удаљених терминала са једне стране и корисника са друге стране; (2) централни подсистем, који обухвата скуп сервера са базама података, апликативним софтвером и софтвером за визуелизацију; (3) интерфејс између оператера и система, који омогућује графички приказ и контролу процеса и (4) подсистем за обраду и архивирање података, креирање и дистрибуцију потребних извештаја.

Савремени информационо-комуникациони системи за подршку даљинског управљања засновани су на технологијама Интернет протокола (IP) и Ethernet локалних рачунарских мрежа. Даљинско управљање карактерише се као некритичан сервис у реалном времену, што значи да се телекомуникациони захтеви могу реализовати у заједничкој IP мрежи, у коју су интегрисани и други телекомуникациони сервиси за оперативне и пословне потребе. При томе треба да буду испуњени следећи предуслови: диференцијација квалитета сервиса по класама, изолација SCADA саобраћаја од осталих типова саобраћаја у мрежи и заштита информација. Протоколи специфични за даљинско управљање развијају се на апликационом слоју (укључујући моделе и презентацију података) и користе Интернет протокол стек.

Усвајање отворених комуникационих стандарда, коришћење отворених софтверских платформи, повезаност система управљања са другим мрежама, даљински приступ и доступност техничких информација су разлози због којих је информационо-комуникациона инфраструктура савремених SCADA система подложна различитим врстама напада. Примена већине стандардних техника заштите утиче на деградацију перформанси SCADA система због значајних процесорских захтева који успоравају рад, а поједини механизми заштите захтевају процесорске ресурсе који често нису доступни у свим компонентама система. Посебан проблем представља сложеност одржавања и некомпатибилност механизма заштите са специфичним протоколима апликационог слоја.

При пројектовању система заштите, као и током његове експлоатације, потребно је да се изврши анализа безбедносног ризика. За спровођење анализе ризика важно је да се познају, процене и дефинишу: добра (*assets*), потенцијалне претње, подложност нападима, последице напада и механизми заштите.

**Предмет истраживања** у предложеној докторској дисертацији је заштита информационо-комуникационе инфраструктуре индустријских система даљинског управљања. Нагласак је на управљању безбедносним ризиком, које обухвата: анализу безбедносног ризика, методологију процене безбедносног ризика, избор механизма заштите и доношење одлуке о имплементацији одговарајућих механизма.

У оквиру предложене дисертације прво ће бити анализирани познате концепције и архитектуре информационо-комуникационих система за подршку индустријских SCADA система. Истраживањем ће бити обухваћена анализа деградације перформанси SCADA система у условима симултаних, дистрибуираних напада (*Distributed Denial of Service, DDoS*). Затим ће бити извршена систематизација до сада научно формулисаних или у пракси примењених метода управљања безбедносним ризиком. На основу тога ће бити предложен и испитан нови метод процене безбедносног ризика.

**Циљ истраживања**, чији ће резултати бити приказани у овој докторској дисертацији, је да се предложи и испита оригиналан метод процене безбедносног ризика информационо-

комуникационе инфраструктуре SCADA система, у коме се ризик квантификује у зависности од типа напада, учестаности напада и њиховог утицаја на квалитет сервиса, односно расположивост и континуитет индустријског процеса. Предложени метод треба да буде: (1) генералан, у смислу могућности примене у различитим индустријским системима даљинског управљања; (2) ефикасан у условима појаве нових типова напада и (3) прилагођен динамичном развоју информационо-комуникационе инфраструктуре система даљинског управљања.

### Осврт на релевантне библиографске изворе

У литератури су дефинисани квалитативни и квантитативни методи процене безбедносног ризика у информационо-комуникационим системима [18], [24]. Квалитативна анализа претпоставља методе који изражавају ризик као субјективну меру, нпр. степен ризика процењује се као низак, средњи или висок. Квантитативна анализа заснива се на математичком приступу (нумеричка анализа, статистички методи) помоћу кога се ризик изражава нумеричким вредностима одређених величина. То су најчешће економске категорије, као што су очекивани годишњи губитак (*Annualized Loss Expectancy*, ALE) и поврат инвестиција (*Return on Investment*, ROI). Дефиниција очекиваних губитака проширена је мултипликативним фактором узастопних напада у моделу разматраном у [10]. Прилагођењем концепта ROI на инвестиције у систем заштите информационо-комуникационе инфраструктуре добија се ROSI (*Return on Security Investment*) [11], [20].

Економски аспекти заштите информационо-комуникационог система од симултаних, дистрибуираних напада разматрани су у [9], са циљем да се одреди оптимални ниво улагања на основу максимизирања добити. У раду [25] предложен је слојевити модел одлучивања заснован на комбиновању метода процене безбедносног ризика, модела трошкова пословања и техника „cost-benefit“ анализе. Критичка евалуација решења заштите пословно-информационих система, заснованих на отвореним софтверским платформама, дата је у [21]. У раду [12] је предложен квантитативни метод процене безбедносног ризика која узима у обзир вероватноћу догађања напада, као и последице напада. Квантитативни метод анализе безбедносног ризика заснован на пословном моделу предложен је у [22]. Метод узима у обзир континуитет пословања и утврђује вредност улагања у заштиту информационо-комуникационог система, на основу значаја различитих пословних функција и нивоа неопходности конкретних заштитних мера.

Специфичности заштите информационо-комуникационе инфраструктуре индустријских система даљинског управљања морају се узети у обзир при анализи безбедносног ризика [6], [8]. Ефикасна детекција напада на информационо-комуникациону инфраструктуру, који мењају понашање циљног система даљинског управљања, могућа је само уз укључивање знања о физичком систему којим се управља [2].

У циљу процене безбедносног ризика неопходна је анализа осетљивости SCADA система на различите врсте напада, као и последица напада на функционисање система. У радовима [13], [16] и [23] анализирани су различити типови напада и одговарајући механизми заштите. Напади као што је одбијање сервиса (DoS) потенцијално угрожавају виталне функције индустријског процеса. Овај тип напада може се вршити у различитим формама на било ком слоју протокол стека. Посебно је тешко открити и спречити дистрибуиране нападе (DDoS), у којима више нападача истовремено напада мету (нпр. витални мрежни сервер). У раду [14] анализиран је утицај DDoS напада на перформансе SCADA система у електропривреди. Специфични системи за детекцију и превенцију напада на индустријске системе даљинског управљања разматрани су у радовима [3] и [19].

Процена безбедносног ризика у индустријским системима даљинског управљања подразумева дефинисање параметара ризика на основу вероватноће догађања напада и њиховог утицаја на расположивост и квалитет функционисања индустријског процеса [5],

[15]. Приступ моделовању и квантификацији међусобних зависности електричне и информационе инфраструктуре система за даљински надзор електроенергетских објеката разматран је у [1]. Приступ је верификован симулацијом отказа појединих делова комуникационе инфраструктуре услед DoS напада.

У раду [17] је предложен модел ризика заснован на Бајесовим мрежама који омогућује одређивање вероватноће компромитовања телекомуникационе мреже услед различитих нивоа напада и утврђивање узрочно-последичних веза између стања мреже. На основу тога се развија план управљања и дефинише стратегија за ублажавање ризика. Бајесов модел примењен је и у раду [7] за процену безбедносног ризика у информационо-комуникационом систему електропривреде.

Процена безбедносног ризика врши се при пројектовању заштите информационо-комуникационе инфраструктуре система даљинског управљања, а затим периодично понавља (делимично или у целини) током експлоатације и надградње система. Поставља се питање тачности поновљених процена у условима динамичног развоја информационо-комуникационог система. У раду [4] је разматран метод инкременталне процене ризика, засноване на формалним дефиницијама различитих профила ризика. Прорачун профила ризика врши се дистрибуирано и независно у различитим компонентама система.

На основу изложеног може се закључити да је проблематика процене безбедносног ризика у информационо-комуникационим системима веома актуелна и недовољно истражена у аспектима дефинисања квантитативних параметара ризика и одговарајућих метода, прилагођених специфичностима индустријских система даљинског управљања.

#### Списак основне литературе која ће бити коришћена при изради теме

- [1] Beccuti, M., Chiaradonna, S., Di Giandomenico, F., Donatelli, S., Dondossola, G., Franceschinis, G.: *Quantification of Dependencies between Electrical and Information Infrastructures*, -International Journal of Critical Infrastructure Protection, Vol. 5, No. 1, 2012, pp. 14-27.
- [2] Cárdenas, A. A., Amin, S., Lin, Z. S., Huang, Y. L., Huang, C. Y., Sastry, S.: *Attacks Against Process Control Systems: Risk Assessment, Detection, and Response*, -Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, March 2011, pp. 355-366.
- [3] Cheung, S., Dutertre, B., Fong, M., Lindqvist, U., Skinner, K., Valdes, A.: *Using Model-based Intrusion Detection for SCADA Networks*, -Proceedings of the SCADA Security Scientific Symposium, Miami Beach, FL, January 2007, pp. 1-12.
- [4] Chivers H., Clark J. A., Cheng, P-C.: *Risk Profiles and Distributed Risk Assessment*, -Computers & Security, Vol. 28, No. 7, 2009, pp. 521-535.
- [5] Dondossola, G., Garrone, F., Szanto, J.: *Cyber Risk Assessment of Power Control Systems – A Metrics Weighed by Attack Experiments*, -Proceedings of the 2011 IEEE Power and Energy Society General Meeting (CD), San Diego, CA, July 2011.
- [6] Ericsson, G. N.: *Information Security for Electric Power Utilities (EPUs)—CIGRÉ Developments on Frameworks, Risk Assessment, and Technology*, -IEEE Transactions on Power Delivery, Vol. 24, No. 3, 2009, pp. 1174-1181.
- [7] Guo, J., Shen, X.: *The Application of Bayesian Model for Power Enterprise Security Risk Management*, -Proceedings of the 2010 IEEE 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Chendgu, China, August 2010, Vol. 1, pp. 531-533.
- [8] Huang, C. C., Farn, K. J., Lin, F. Y. S.: *A Study on Implementations of Information Security Risk Assessment: Application to Chlorine Processing Systems of Water Treatment Plants*, -International Journal of Network Security, to appear in: Vol. 16, No. 4, 2014, pp. 241-248.
- [9] Huang, C. D., Hu, Q., Behara, R. S.: *Economics of Information Security Investment in the Case of Simultaneous Attacks*, -Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS 2006), Cambridge, England, June 2006, pp. 1-33.

- [10] Iheagwara, C., Blyth, A., Singhal, M.: *Cost Effective Management Frameworks for Intrusion Detection Systems*, -Journal of Computer Security, Vol. 12, No. 5, 2004, pp. 777-798.
- [11] Iheagwara, C.: *The Effect of Intrusion Detection Management Methods on the Return on Investment*, -Computers & Security, Vol. 23, No. 3, 2004, pp. 213-228.
- [12] Karabacak, B., Sogukpinar, I.: *ISRAM: Information Security Risk Analysis Method*, -Computers & Security, Vol. 24, No. 2, 2005, pp. 147-159.
- [13] Karnouskos, S.: *Stuxnet Worm Impact on Industrial Cyber-Physical System Security*, - Proceedings of the IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society, Melbourne, November 2011, pp. 4490-4494.
- [14] Marković-Petrović, J., Stojanović, M.: *Analysis of SCADA System Vulnerabilities to DDoS Attacks*, - Proceedings of the 2013 11th International Conference on Telecommunications in Modern Satellite Cable and Broadcasting Services - TELSIKS 2013, Niš, October 2013, Vol. 2, pp. 591-594.
- [15] Papa, S. M., Casper, W. D., Nair, S.: *Availability Based Risk Analysis for SCADA Embedded Computer Systems*, -Proceedings of the 2011 World Congress in Computer Science, Computer Engineering, and Applied Computing (WorldComp11), Las Vegas, NV, July 2011, pp. 541-547.
- [16] Peng, T., Leckie, C., Ramamohanarao, K.: *Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems*, -ACM Computing Surveys, Vol. 39, No. 1, article 3, 2007.
- [17] Poolsappasit, N., Dewri, R., Ray, I.: *Dynamic Security Risk Management Using Bayesian Attack Graphs*, -IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 1, 2012, pp. 61-74.
- [18] Rot, A.: *IT Risk Assessment: Quantitative and Qualitative Approach*, -Proceedings of the World Congress on Engineering and Computer Science, WCECS 2008, October 2008, San Francisco, CA.
- [19] Skorobogatjko, A., Dorogovs, P., Romanovs, A.: *The Use of Intrusion Detection Systems Based on the Network Behaviour Analysis in SCADA Networks*, -Information Technology and Management Science, Vol. 15, No. 1, 2012, pp. 171-175.
- [20] Sonnenreich, W., Albanese, J., Stout, B.: *Return on Security Investment (ROSI) - A Practical Quantitative Model*, -Journal of Research and Practice in Information Technology, Vol. 38, No. 1, 2006, pp. 45-56.
- [21] Stojanović, M., Aćimović-Raspopović, V., Boštjančič Rakas, S.: *Security Management Issues for Open Source ERP in the NGN Environment*, -Free and Open Source Enterprise Resource Planning: Systems and Strategies, R. Atem de Carvalho and B. Johansson (Eds.), pp. 165-181, IGI Global, New York, 2011.
- [22] Suh, B., Han, I.: *The IS Risk Analysis Based on a Business Model*, -Information & Management, Vol. 41, No. 2, 2003, pp. 149-158.
- [23] Ten, C-W., Liu, C-C., Manimaran, G., *Vulnerability Assessment of Cybersecurity for SCADA Systems*, - IEEE Transactions on Power Systems, Vol. 23, No. 4, 2008, pp. 1836-1846.
- [24] Tsiakis, T.: *Information Security Expenditures: A Techno-Economic Analysis*, -International Journal of Computer Science and Network Security, Vol. 10, No. 4, 2010, pp. 7-11.
- [25] Wei, H., Alves-Foss, J., Soule, T.: *A Layered Decision Model for Cost-Effective System Security*, - International Journal of Information and Computer Security, Vol. 2, No. 3, 2008, pp. 308-335.

Поред основне литературе, у изради дисертације биће коришћени и следећи библиографски извори:

- Agbinya, J. I.: *IP Communications and Services for NGN*, Auerbach Publications, Taylor & Francis Group, 2010.
- CIGRÉ Technical Brochure TB 317: *Security for Information Systems and Intranets in Electric Power Systems*, JWGD2/B2/C2.01, CIGRÉ, 2007.
- CIGRÉ Technical Brochure TB 419: *Treatment of Information Security for Electric Power Utilities (EPUs)*, WGD2.22, CIGRÉ, 2010.
- Guizani, M., Rayes, A., Khan, B., Al-Fuqaha, A.: *Network Modeling and Simulation (A Practical Perspective)*, John Wiley & Sons, 2010.

- Haimes, Y. Y.: *Risk Modeling, Assessment and Management*, John Wiley & Sons, 2004.
- ISO/IEC 27005: *Information Technology – Security Techniques – Information Security Risk Management*, ISO/IEC, 2011.
- ITU-T Recommendation E.802: *Framework and Methodologies for the Determination and Application of QoS Parameters*, ITU-T, 2007.
- ITU-T Recommendation X.1055: *Risk Management and Risk Profile Guidelines for Telecommunication Organizations*, ITU-T, 2008.
- Krutz, R. L.: *Securing SCADA Systems*, Wiley Publishing Inc., 2006.
- NIST Special Publication 800-30 Rev.1: *Guide for Conducting Risk Assessments*, 2012.
- NIST Special Publication 800-82 Rev.1: *Guide to Industrial Control Systems (ICS) Security*, 2013.
- Paul, S., Pan, J., Jain, R.: *Architectures for the Future Networks and the Next Generation Internet: A Survey*, -Computer Communications, Vol. 34, No. 1, 2011, pp. 2–42.
- Stojanović, M., Aćimović-Raspopović, V.: *Savremene IP mreže: arhitekture, tehnologije i protokoli*, Akademska misao, Beograd, 2012.
- Stojanović, M., Boštjančič Rakas, S., Aćimović-Raspopović, V.: *End-to-End Quality of Service Specification and Mapping: The Third Party Approach*, -Computer Communications, Vol. 33, No. 11, 2010, pp. 1354-1368.
- Zhu, B., Joseph, A., Sastry, S.: *A Taxonomy of Cyber Attacks on SCADA Systems*, -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, pp. 380-388.

### 3. Полазне хипотезе

При изради дисертације полази се од следећих хипотеза:

- Напади на информационо-комуникационе системе за подршку даљинског управљања потенцијално угрожавају виталне функције индустријског система. Због тога је, при пројектовању и експлоатацији, неопходно континуирано управљање безбедносним ризиком, као и развој нових метода процене ризика.
- Разматрају се системи за превенцију напада (*Intrusion Prevention Systems*) и системи за детекцију напада (*Intrusion Detection Systems*).
- Традиционални квантитативни методи процене безбедносног ризика, засновани искључиво на економским категоријама (очекивани годишњи губитак, поврат инвестиција), нису адекватни за индустријске системе даљинског управљања, због тога што не узимају у обзир специфичности ових система у аспектима поузданости, квалитета сервиса и примењених информационо-комуникационих технологија.
- Дефинисањем и избором адекватног метода процене ризика могуће је одредити оптимални ниво улагања у механизме заштите индустријских система даљинског управљања, са првенственим циљем превенције напада.
- Претпоставља се дефинисање различитих нивоа прихватљивог ризика.

### 4. Научне методе истраживања

У предложеном истраживању биће коришћени следећи методи:

- Класични методи прикупљања, систематизације и компаративне анализе при прегледу и класификацији до сада формулисаних и у пракси примењених резултата.
- Математичко моделовање, нумеричка анализа и рачунарска симулација.

## 5. Очекивани научни допринос

Очекивани резултати и најважнији научни доприноси спроведених истраживања, која представљају предмет ове дисертације су:

- Утврђивање степена деградације кључних перформанси (расположивост, кашњење, проценат изгубљених пакета, оптерећење процесорских ресурса) у различитим условима дистрибуираних напада на информационо-комуникациони систем за подршку даљинског управљања.
- Дефинисање нових параметара безбедносног ризика, заснованих на учестаности дистрибуираних напада и њиховом утицају на кључне перформансе система.
- Предлог и евалуација оригиналног метода процене безбедносног ризика у индустријским системима даљинског управљања, заснованог на претходно дефинисаним квантитативним параметрима ризика.

Предложени начин решавања проблема има потенцијалну практичну примену у пројектовању и експлоатацији решења заштите информационо-комуникационе инфраструктуре индустријских система даљинског управљања.

## 6. План истраживања и структура рада

Планирано истраживање у оквиру докторске дисертације би било реализовано у четири фазе, дефинисане у складу са предметом, циљем и полазним хипотезама истраживања.

Фаза 1: Преглед литературе и анализа основних праваца истраживања проблема. Анализа концепције IP базиране информационо-комуникационе инфраструктуре у индустријским системима даљинског управљања.

Фаза 2: Анализа и систематизација потенцијалних напада на индустријске SCADA системе. Анализа механизма заштите информационо-комуникационе инфраструктуре од потенцијалних напада. Истраживање метода управљања безбедносним ризиком.

Фаза 3: Анализа утицаја симултаних, дистрибуираних напада на перформансе SCADA система. Развој симулационог модела реалног индустријског SCADA система. Симулација дистрибуираног DoS напада. Анализа резултата симулације.

Фаза 4: Предлог новог начина квантификације безбедносног ризика. Предлог и евалуација новог метода процене безбедносног ризика информационо-комуникационе инфраструктуре индустријских SCADA система. Разматрање мера за ограничавање ризика. Закључна разматрања.

### Структура рада:

- Увод: опис проблема, предмет и циљ истраживања, методологија истраживања.
- Преглед литературе и анализа актуелних проблема истраживања.
- Приказ и анализа напада на информационо-комуникациону инфраструктуру индустријских система даљинског управљања, као и одговарајућих решења заштите.
- Симулациона анализа перформанси система даљинског управљања у условима симултаних, дистрибуираних напада на инфраструктуру IP мреже.
- Процес управљања безбедносним ризиком.
- Предлог квантитативних параметара и новог метода процене безбедносног ризика у индустријским SCADA системима.
- Симулациона анализа перформанси предложеног метода.
- Предлог мера за ограничавање безбедносног ризика.
- Закључна разматрања.

## 7. Закључак и предлог

На основу увида у пријаву теме докторске дисертације, Комисија сматра да је предложена тема научно заснована, релевантна и актуелна у области савремених информационо-комуникационих технологија.

Мр Јасна Д. Марковић-Петровић дипломирала је и магистрирала на Електротехничком факултету Универзитета у Београду. Објавила је радове и учествовала у реализацији пројеката из области из које пријављује тему. Комисија сматра да мр Јасна Д. Марковић-Петровић испуњава формалне и суштинске услове за пријаву теме докторске дисертације, као и да је компетентна да реализује предвиђене циљеве истраживања.

Комисија је, на основу образложења теме и у разговору са кандидатом, закључила да назив теме треба да гласи: „ПРОЦЕНА БЕЗБЕДНОСНОГ РИЗИКА У ИНДУСТРИЈСКИМ СИСТЕМИМА ДАЉИНСКОГ УПРАВЉАЊА“.

Комисија предлаже Наставно-научном већу Саобраћајног факултета Универзитета у Београду да прихвати тему докторске дисертације кандидата мр Јасне Д. Марковић-Петровић, под називом „**ПРОЦЕНА БЕЗБЕДНОСНОГ РИЗИКА У ИНДУСТРИЈСКИМ СИСТЕМИМА ДАЉИНСКОГ УПРАВЉАЊА**“ и да је проследи Већу научних области техничких наука Универзитета у Београду на даљи поступак. Предложена тема докторске дисертације припада ужој научној области „Информационо-комуникационе технологије“, за коју је Саобраћајни факултет у Београду матичан.

За ментора се предлаже др Мирјана Стојановић, дипл. инж. ел., ванредни професор Саобраћајног факултета у Београду.

У Београду, 12.03.2014. године

### ЧЛАНОВИ КОМИСИЈЕ

.....  
Др Мирјана Стојановић, ванредни професор  
Универзитет у Београду, Саобраћајни факултет

.....  
Др Миодраг Бакмаз, редовни професор  
Универзитет у Београду, Саобраћајни факултет

.....  
Др Валентина Радојичић, редовни професор  
Универзитет у Београду, Саобраћајни факултет

.....  
Др Андреја Самчовић, ванредни професор  
Универзитет у Београду, Саобраћајни факултет

.....  
Др Нинел Чукалевски, научни саветник  
Универзитет у Београду, Институт „Михајло Пупин“