

ИЗВЕШТАЈ О ОЦЕНИ ПОДОБНОСТИ ТЕМЕ, КАНДИДАТА И МЕНТОРА ЗА
ИЗРАДУ ДОКТОРСКЕ ДИСЕРТАЦИЈЕ

I ПОДАЦИ О КОМИСИЈИ

Орган који је именовао комисију: Декан Факултета техничких наука

Датум именовања комисије: 02.07.2026.

Састав комисије именоване у складу са *Правилима докторских студија Универзитета у Новом Саду*:

- | | | |
|---|-------------------|---|
| 1. др Гордана Остојић | редовни професор | Мехатроника, роботика, аутоматизација и интегрисани системи |
| презиме и име | звање | ужа научна област |
| Факултет техничких наука Нови Сад | | председник комисије |
| установа у којој је запослен-а | | функција у комисији |
| 2. др Ивана Шенк | ванредни професор | Мехатроника, роботика, аутоматизација и интегрисани системи |
| презиме и име | звање | ужа научна област |
| Факултет техничких наука Нови Сад | | члан |
| установа у којој је запослен-а | | функција у комисији |
| 3. др Срђан Тегелтија | ванредни професор | Мехатроника, роботика, аутоматизација и интегрисани системи |
| презиме и име | звање | ужа научна област |
| Факултет техничких наука Нови Сад | | члан |
| установа у којој је запослен-а | | функција у комисији |
| 4. др Емил Вег | редовни професор | Теорија механизма и машина, Инжењерско цртање са нацртном геометријом |
| презиме и име | звање | ужа научна област |
| Машински факултет Универзитета у Београду | | члан |
| установа у којој је запослен-а | | функција у комисији |
| 5. др Дејан Ранчић | редовни професор | Електротехника и рачунарство |
| презиме и име | звање | ужа научна област |
| Електронски факултет Универзитета у Нишу | | члан |
| установа у којој је запослен-а | | функција у комисији |

II ПОДАЦИ О КАНДИДАТУ

1. Име, име једног родитеља, презиме: Милош, Зоран, Станојевић
2. Датум рођења: 29.09.1994. Место и држава рођења: Нови Сад, Србија

II.1 Основне или интегрисане студије

Година уписа: Година завршетка: Просечна оцена током студија:

Универзитет: Универзитет у Новом Саду

Факултет: Факултет техничких наука

Студијски програм: Мехатроника

Стечено звање: дипломирани инжењер мехатронике

II.2 Мастер или магистарске студије

Година уписа: Година завршетка: Просечна оцена током студија:

Универзитет: Универзитет у Новом Саду

Факултет: Факултет техничких наука

Студијски програм: Мехатроника

Стечено звање: мастер инжењер мехатронике

Научна област: мехатроника, роботика и аутоматизација

Наслов завршног рада: Примена електричних цилиндара код паркинг баријера

II.3 Докторске студије

Година уписа:

Универзитет: Универзитет у Новом Саду

Факултет: Факултет техничких наука

Студијски програм: Мехатроника

Број ЕСПБ до сада остварених: Просечна оцена током студија:

II.4 Приказ научних и стручних радова кандидата

Р. бр.	аутори, наслов рада, часопис, волумен (година) странице од-до, DOI или ISBN/ISSN	категорија
1.	Stanojević M. , Ostojić G., Skorić T., Popović N., Lale S., Kukrić N, Cyber security risk in pervasive environments of unobtrusive cECG-monitoring system during driving, In International Symposium INFOTEH-JAHORINA, Vol. 24 (2025) pp. 1-5, 10.1109/INFOTEH64129.2025.10959206.	M33
Рад припада проблематици докторске дисертације: ☒ ДА ☐ НЕ ☐ ДЕЛИМИЧНО		

Р. бр.	аутори, наслов рада, часопис, волумен (година) странице од-до, DOI или ISBN/ISSN	категорија
2.	Baranovski I., Stankovski S., Ostojić G., Nikolić V., Simonović M., Stanojević M. Toward a smart ecosystem with automated services. In facta Universitatis, Series: Mechanical Engineering, (2022), 0.22190/FUME220525033B	M21
Рад припада проблематици докторске дисертације: ☐ ДА ☒ НЕ ☐ ДЕЛИМИЧНО		

Р. бр.	аутори, наслов рада, часопис, волумен (година) странице од-до, DOI или ISBN/ISSN	категорија
3.	Babić M., Stanojević M. , Ostojić G., Tegeltija S., Stankovski S., Industrial Cyber Security Aspects in ICS Applications, DAAAM International Symposium on Intelligent Manufacturing and Automation, Vol. 33 (2022), pp. 326-33, 10.2507/33rd.daaam.proceedings.045	M33
Рад припада проблематици докторске дисертације: ☒ ДА ☐ НЕ ☐ ДЕЛИМИЧНО		

Р. бр.	аутори, наслов рада, часопис, волумен (година) странице од-до, DOI или ISBN/ISSN	категорија
4.	Tarjan L., Šenk I., Stanojević M. , Babić M., Jovanović D., Rikić D., Tegeltija S., Simulation of the traffic light optimization algorithm based on the current traffic frequency. In International Symposium INFOTEH-JAHORINA, Vol. 22 (2023), pp. 1-5, https://ieeexplore.ieee.org/xpl/conhome/10094039/proceeding	M33
Рад припада проблематици докторске дисертације: ☐ ДА ☒ НЕ ☐ ДЕЛИМИЧНО		

Р. бр.	аутори, наслов рада, часопис, волумен (година) странице од-до, DOI или ISBN/ISSN	категорија
5.	Šenk I., Tarjan L., Tegeltija S., Reljić B., Babić M., Stanojević M. , Development of an IIOT-Ready Conveyor System, International Scientific Conference on INDUSTRIAL SYSTEMS – IS, Vol. 19 (2023), pp. 66-71, 978-86-6022-623-7	M33
Рад припада проблематици докторске дисертације: ☐ ДА ☒ НЕ ☐ ДЕЛИМИЧНО		

Р. бр.	аутори, наслов рада, часопис, волумен (година) странице од-до, DOI или ISBN/ISSN	категорија
6.	Stankovski S., Ostojić G., Šaponjić M., Stanojević M. , Babić M., Using micro/mini PLC/PAC in the Edge Computing Architecture, In International Symposium INFOTEH-JAHORINA, Vol. 19 (2020), pp. 1-4, 10.1109/INFOTEH48170.2020.9066309	M33
Рад припада проблематици докторске дисертације: ☐ ДА ☒ НЕ ☐ ДЕЛИМИЧНО		

Р. бр.	аутори, наслов рада, часопис, волумен (година) странице од-до, DOI или ISBN/ISSN	категорија
7.	Stanojević M. , Babić M., Vekić A., Tarjan L., Tegeltija S., Improvement of Smart Parking Barrier Autonomy Using Battery Supply, DAAAM International Symposium on Intelligent Manufacturing and Automation, Vol. 30 (2019), pp.	M33

1084-1090, 10.2507/30th.daaam.proceedings.151		
Рад припада проблематици докторске дисертације:	ДА	НЕ ДЕЛИМИЧНО

III ОЦЕНА ПОДОБНОСТИ ТЕМЕ

Оцена:

III.1 формулације наслова тезе

Наслов „Заштитни механизми од сајбер напада и њихов утицај на перформансе индустријских управљачких система” (енг: „Cyberattack protection mechanisms and their impact on performance in industrial control systems”) се сматра адекватним насловом за докторску тезу.

Предложени наслов тезе је подобан?

ДА

НЕ

III.2 предмета (проблема) истраживања

Предмет истраживања докторске дисертације обухвата пројектовање и имплементацију безбедне комуникације између рачунарског система за надзор и управљање и програмабилно логичког контролера (PLC) у оквиру индустријских управљачких система. Посебан фокус је стављен на комуникацију засновану на Modbus TCP протоколу, који је широко заступљен у индустријској пракси, али не поседује уграђене безбедносне механизме. У оквиру истраживања анализираће се понашање система у условима различитих сајбер напада, укључујући напад ускраћивањем услуга (DoS), напад путем посредника (MitM) и Replay напад. Такође, предмет истраживања ће обухватати имплементацију додатних безбедносних механизма, као што су VPN тунел и друга програмска решења са циљем унапређења безбедности комуникације између рачунара и PLC. Поред безбедносног аспекта, истраживање обухвата и анализу утицаја уведених механизма заштите на перформансе система, са посебним освртом на време одзива и ефикасност комуникације.

Савремени индустријски управљачки системи доживљавају значајну трансформацију услед убрзане дигитализације и интеграције са информационим технологијама. Системи који су некада били изоловани и радили у затвореним мрежним окружењима данас су све чешће повезани са корпоративним мрежама, па чак и са интернетом. Оваква интеграција омогућава већу флексибилност, даљински надзор и управљање процесима, као и ефикасније доношење одлука, али истовремено значајно повећава изложеност ових система сајбер претњама.

За разлику од класичних информационих система, индустријски управљачки системи управљају физичким процесима који су често од критичног значаја. То могу бити енергетски системи, производни погони, системи за водоснабдевање, транспортни системи и други инфраструктурни објекти. Свако нарушавање њиховог рада може имати озбиљне последице, не само у економском смислу, већ и по безбедност људи и животне средине. Управо због тога, поузданост и безбедност ових система представља кључни фактор њиховог исправног функционисања.

Посебан проблем представља чињеница да велики број индустријских система спада у категорију такозваних legacy система. Ови системи су развијани у време када безбедност није била приоритет, већ је фокус био на функционалности и поузданости. Као резултат тога, многи индустријски протоколи попут Modbus TCP не поседују уграђене механизме за аутентификацију, енкрипцију нити заштиту интегритета података. Иако су овакви системи и даље широко заступљени у индустрији, њихова модернизација кроз потпуну замену хардвера и софтвера често није изводљива због високих трошкова, сложености имплементације и потребе за континуираним радом система без прекида.

Због наведених ограничења, постоји потреба за развојем решења која омогућавају унапређење безбедности постојећих система без њихове потпуне реконструкције. У том контексту, посебно су значајни приступи који се заснивају на увођењу додатних безбедносних слојева, као што су заштита на мрежном нивоу и апликациони механизми заштите. Овакви приступи омогућавају повећање безбедности уз минималне измене постојећег система, што их чини практично применљивим у реалним индустријским системима.

Додатну потврду значаја ове области дају и бројни познати инциденти у индустријским системима. Један од најпознатијих примера представља Stuxnet напад, који је показао да сајбер напади могу имати директне физичке последице по индустријске процесе. Овај напад је циљао индустријске контролере и демонстрирао могућност манипулације њиховим радом без знања оператера. Након овог инцидента постало је јасно да индустријски системи више не могу бити посматрани као изоловани и безбедни, већ као потенцијалне мете софистицираних сајбер напада.

Предмет истраживања је подобан?

ДА

НЕ

III.3 познавања проблематике на основу изабране литературе са списком литературе

Попис литературе наведен приликом пријаве теме докторске дисертације одговара предмету истраживања докторске дисертације и указује на детаљно извршену анализу литературе. За предмет докторске дисертације посебно су значајни следећи извори:

- [1] Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. *computers & security*, 89, 101677.
- [2] Ahmadian, M. M., Shajari, M., & Shafiee, M. A. (2020). Industrial control system security taxonomic framework with application to a comprehensive incidents survey. *International Journal of Critical Infrastructure Protection*, 29, 100356.
- [3] Canonico, R., & Sperli, G. (2023). Industrial cyber-physical systems protection: A methodological review. *Computers & Security*, 135, 103531.
- [4] Cui, H., Hong, J., & Loudon, R. (2024). An overview of the security of programmable logic controllers in industrial control systems. *Encyclopedia*, 4(2), 874-887.
- [5] Morris, T. H., & Gao, W. (2013, September). Industrial control system cyber attacks. In *1st international symposium for ICS & SCADA cyber security research 2013 (ICS-CSR 2013)*. BCS Learning & Development.
- [6] Goldenberg, N., & Wool, A. (2013). Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. *international journal of critical infrastructure protection*, 6(2), 63-75.
- [7] Le, X., Li, J., Zhao, Y., & Fan, Z. (2025). A Security-Enhanced Scheme for ModBus TCP Protocol Based on Lightweight Cryptographic Algorithm. *Electronics*, 14(18), 3674.
- [8] Amer, E., Al-rimy, B. A. S., & El-Sappagh, S. (2025). Strengthening ICS defense: Modbus-NFA behavior model for enhanced anomaly detection. *Journal of Information Security and Applications*, 89, 103990.
- [9] Koay, A. M., Ko, R. K. L., Hettrema, H., & Radke, K. (2023). Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges. *Journal of Intelligent Information Systems*, 60(2), 377-405.
- [10] Pochmara, J., & Świetlicka, A. (2024). Cybersecurity of industrial systems—A 2023 report. *Electronics*, 13(7), 1191.
- [11] Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection*, 9, 52-80.
- [12] Cheminod, M., Durante, L., & Valenzano, A. (2012). Review of security issues in industrial networks. *IEEE transactions on industrial informatics*, 9(1), 277-293.
- [13] Maynard, P., McLaughlin, K., & Haberler, B. (2014, September). Towards understanding man-in-the-middle attacks on iec 60870-5-104 scada networks. In *2nd International Symposium for ICS & SCADA Cyber Security Research 2014 (ICS-CSR 2014)*. BCS Learning & Development.
- [14] Ylmaz, E. N., Ciylan, B., Gönen, S., Sindiren, E., & Karacayılmaz, G. (2018, April). Cyber security in industrial control systems: Analysis of DoS attacks against PLCs and the insider effect. In *2018 6th international istanbul smart grids and cities congress and fair (icsg)* (pp. 81-85). IEEE.
- [15] Eigner, O., Kreimel, P., & Tavolato, P. (2016, August). Detection of man-in-the-middle attacks on industrial control networks. In *2016 International Conference on Software Security and Assurance (ICSSA)* (pp. 64-69). IEEE.
- [16] Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE security & privacy*, 9(3), 49-51.
- [17] Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. *White paper, symantec corp.*,

security response, 5(6), 29.

- [18] Kozak, P., Klaban, I., & Šlajs, T. (2023, May). Industroyer cyber-attacks on Ukraine's critical infrastructure. In *2023 International Conference on Military Technologies (ICMT)* (pp. 1-6). IEEE.
- [19] Di Pinto, A., Dragoni, Y., & Carcano, A. (2018). TRITON: The first ICS cyber attack on safety instrument systems. *Proc. Black Hat USA, 2018*, 1-26.
- [20] Knapp, E. D. (2024). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Elsevier.
- [21] Katulić, F., Sumina, D., Groš, S., & Erceg, I. (2023). Protecting modbus/TCP-based industrial automation and control systems using message authentication codes. *IEEE access*, 11, 47007-47023.
- [22] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. D., & Hahn, A. L. (2015). *Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)*. US Department of Commerce, National Institute of Standards and Technology.
- [23] Kent, S. (2005). *IP encapsulating security payload (ESP)* (No. rfc4303).
- [24] Needham, R. M., & Schroeder, M. D. (1978). Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12), 993-999.
- [25] Denning, D. E., & Sacco, G. M. (1981). Timestamps in key distribution protocols. *Communications of the ACM*, 24(8), 533-536.

Избор литературе је одговарајући?

ДА

НЕ

III.4 циљева истраживања

Циљ истраживања је развој и евалуација модела безбедне комуникације између рачунарског система за надзор и управљање и програмабилно логичког контролера у индустријским управљачким системима. Истраживање ће бити усмерено на анализу рањивости комуникације засноване на Modbus TCP протоколу, као и на испитивање утицаја различитих типова сајбер напада укључујући DoS, MitM и Replay напад. Такође, циљ рада ће бити имплементација и анализа ефикасности додатних безбедносних механизма у циљу унапређења заштите комуникације. Истраживање ће обухватати и експерименталну евалуацију утицаја уведених механизма на перформансе система, са фокусом на време одзива и поузданост комуникације. Крајњи циљ је утврђивање компромиса између повећања безбедности и евентуалног смањења перформанси система. Очекује се да резултати истраживања потврде постојање значајних безбедносних рањивости у комуникацији између рачунарског система и PLC када се користи Modbus TCP протокол без додатних механизма заштите. Након успешне имплементације безбедносних механизма, са аспекта перформанси се очекује да ће се појавити благо повећање времена одзива комуникације услед додатних корака у процесу размене података. Поред тога, претпоставља се да ће то повећање остати у границама које не угрожавају функционалност система.

Циљеви истраживања су одговарајући?

ДА

НЕ

III.5 очекиваних резултата (хипотезе)

Хипотеза 1:

Индустријски комуникациони системи засновани на Modbus TCP протоколу показују значајну рањивост на напад ускраћивањем услуга, на напад путем посредника као и на Replay напад у одсуству додатних безбедносних механизма.

Хипотеза 2:

Комбинована примена више безбедносних механизма обезбеђује виши ниво заштите система уз минималан утицај на његову функционалност и стабилност.

Хипотеза 3:

Имплементација безбедносних механизма доводи до повећања времена одзива комуникације, али то повећање остаје у прихватљивим границама за индустријске системе.

Очекивани резултати представљају значајан научни допринос?

ДА

НЕ

III.6 плана рада (на основу фаза истраживања и оријентационог садржаја дисертације из Обрасца 1)

1. Фаза 1 – Теоријске основе
 - a. Прикупљање литературе
 - b. Анализа постојеће литературе
 - c. Анализа стања у области
2. Фаза 2 – Дефинисање архитектуре система и креирање исте
 - a. Одабир компоненти система
 - b. Одабир комуникационог протокола и дефинисање структуре порука које ће се размењивати између компоненти система
 - c. Повезивање компоненти система и имплементација комуникације
3. Фаза 3 – Креирање модела претњи
 - a. Креирање модела претњи за изабрану мрежну архитектуру
 - b. Анализа и груписање претњи
4. Фаза 4 – Анализа утицаја изабраних претњи на постављено експериментално окружење
 - a. Одабир три типа напада који су највише релевантни за индустријске системе
 - b. Експериментална реализација сваког типа напада
 - c. Анализа резултата напада
5. Фаза 5 – Имплементација безбедносних механизма
 - a. Увођење безбедносних механизма
 - b. Експериментална анализа безбедности система након примене безбедносних механизма
6. Фаза 6 – Анализа утицаја безбедносних механизма на перформансе система
 - a. Мерење перформанси система без уведених заштита
 - b. Мерење перформанси система са уведеним безбедносним механизмима
 - c. Поређење добијених резултата и доношење закључака
7. Фаза 7 – Израда докторске дисертације

Оквирни садржај докторске дисертације ће бити следећи:

- Увод који обухвата актуелно стање у области, дефинисање хипотезе дисертације, давање методологије истраживања, циљеви, резултати као и структура самог рада,
- Индустријски управљачки системи и комуникационе мреже,
- Опис безбедности у индустријским системима и анализа претњи над њима,
- Предлог и примена безбедносних мера,
- Експериментална евалуација безбедности система,
- Дискусија резултата,
- Закључак, и
- Литература.

План рада је одговарајући?

ДА

НЕ

III.7 метода и узорака истраживања

Методе које ће бити примењене у истраживању су следеће:

1. Преглед литературе и постојећих решења
2. Истраживање комуникационих протокола у ICS
3. Креирање лабораторијског окружења
4. Истраживање алата за анализу рањивости система
5. Реализација изабраних напада на систем
6. Имплементација заштите од напада
7. Тестирање

Метод и узорак су одговарајући?

ДА

НЕ

III.8 места, лабораторије и опреме за истраживачки рад

Током истраживања биће коришћене лабораторије Факултета техничких наука Универзитета у Новом Саду опремљене одговарајућим хардвером, софтвером и подацима.

Услови за истраживачки рад су одговарајући?

ДА

НЕ

III.9 методе статистичке обраде података и осталих релевантних података

Место експерименталне провере резултата истраживања ће такође бити лабораторије Факултета техничких наука, Универзитета у Новом Саду, а провера ће се извршити током 2026. године. Истраживање не садржи статистичке обраде података.

Комисија сматра да је овакав метод обраде података адекватан, те да одговара потребама докторске дисертације.

Предложене методе су одговарајуће?

ДА

НЕ

IV ОЦЕНА ПОДОБНОСТИ КАНДИДАТА

Услови дефинисани за кандидата студијским програмом:

Студент стиче право да пријави докторску дисертацију, односно докторски уметнички пројекат када испуни услове предвиђене студијским програмом докторских академских студија. Према Правилнику о упису, студирању на докторским академским студијама и стицању звања доктора наука, односно, доктора уметности, усвојеног на 81. седници Наставно-научног већа Факултета техничких наука Универзитета у Новом Саду, дана 29/30. 9. 2021. године, студент, који је положио све испите одређене студијским програмом и одбранио теоријске основе докторске дисертације, односно уметничког пројекта, стиче право да пријави тему докторске дисертације, односно докторског уметничког пројекта. Докторска дисертација, односно докторски уметнички пројекат, се пријављује из научне, односно уметничке области акредитованог студијског програма.

Образложење:

Према подацима којима располаже студентска служба, кандидат Милош Станојевић је положио све испите предвиђене планом и програмом докторских академских студија студијског програма Мехатроника, укључујући теоријске основе докторске дисертације, чиме је стекао све услове за пријаву теме докторске дисертације.

Да ли кандидат испуњава дефинисане услове?

ДА

НЕ

V ОЦЕНА ПОДОБНОСТИ ПРЕДЛОЖЕНОГ МЕНТОРА

V.1 Биографија ментора (до 500 речи):

Стеван Станковски је рођен 24.10.1962. године у Новом Саду. Дипломирао је 1987. године на Факултету техничких наука на одсеку за електротехнику, смеру за рачунарску технику и аутоматику, Универзитета у Новом Саду, као први студент у генерацији. Магистарску тезу одбранио је 1991., а докторску дисертацију 1994. године, на Електротехничком факултету Универзитета у Београду.

Након дипломирања, запошљава се као асистент у научном раду на Институту за индустријске системе Факултета техничких наука. У асистентским звањима је до 1995. године, када је изабран у звање доцента. У звање редовног професора је изабран је 2005. године.

Свој научни и стручни рад је публикувао у преко 350 наслова, који су објављени у међународним часописима и монографијама, домаћим часописима и монографијама, као и на међународним и домаћим конференцијама. Подаци о цитираности његових радова у јулу 2026. године показују да има преко 2400 цитата и *h*-индекс 28 према Google Scholar бази и преко 1200 цитата и *h*-индекс 20 према Scopus бази. Поседује пет патената и више десетина техничких решења. Руководилац је великог броја пројеката финансираних од стране Министарства за науку и технолошки развој и Покрајинског секретаријата за науку и технолошки развој. Поред руковођења домаћим научним пројектима, руководио је са више међународних пројекта укључујући пројекте из позива FP7, COST, H2020 Horizon Europe. Као члан тима учествовао је на пројектима из позива FP7, COST, IPA и H2020. Добитник је више награда, укључујући: Никола Тесла за иновације, Капетан Миша Анастасијевић за свој научни и стручни рад, Светске организације за заштиту интелектуалне својине за 2015. годину. Победник је такмичења за најбољу технолошку иновацију у Србији за 2015. годину. Своје научно и стручно усавршавање је у више наврата остварио на универзитетима у Аустрији, Немачкој, Енглеској, Холандији, Кини, Португалији, Мађарској и Словенији. Стални је члан IEEE. Члан је уредништва у следећим часописима: Facta Universitates - Series Automatic Control and Robotics, Facta Universitates - Mechanical Series, International Journal of Industrial Engineering and Management и Journal of Mechatronics, Automation and Identification Technology. Поред уређивања ових часописа, рецензент је најугледнијих научних часописа у области, као што су Mechatronics, International Journal of Advanced Manufacturing Technology, Assembly Automations, Computers and Electronics in Agriculture, Knowledge-Based Systems, Journal of Network and Computer Applications, као и других. Гостујући је професор на неколико европских

и кинеских универзитета. Био је ангажован као рецензент научних и иновационих пројеката у Канади, Кини, Словенији, Србији и Хонг-Конгу. Говори и пише на енглеском језику, а служи се немачким, руским и мађарским језиком.

У свом стручном раду је реализовао преко 300 управљачких система на разним машинама и технолошким линијама. Пројектовао је и реализовао неколико специјализованих машина, манипулатора и информационих система. Стални је стручни консултант из области управљања и електронике за компанију ФЕСТО из Штутгарта, Немачка. За потребе ФЕСТО Дидактичког центра у Новом Саду, одржао је преко 200 семинара из области: програмабилни логички контролери, електропнеуматике и система за надзор и управљање.

Један је од иницијатора и оснивача стварања студијских програма Мехатроника и Биомедицинско инжењерство. Од 2009. до 2018. године био је и руководиоца студијског програма Мехатроника на основном и мастер нивоу. Од 2009. до 2013. године био је директор Департамента за индустријско инжењерство и менаџмент. У звању проректора за науку Универзитета у Новом Саду био је у периоду од 2018. до 2021. године. Председник стручног већа за техничко–технолошке науке на Универзитета у Новом Саду био је у периоду 2015.-2018. година. Председник је Српске асоцијације за промоцију теорију машина и механизма. Био је ментор на 7 докторских дисертација и преко 170 дипломских и мастер радова. Стално је запослен у звању редовног професора на Факултету техничких наука у Новом Саду, Универзитета у Новом Саду.

V.2 Референце ментора из научне области којој припада тема докторске дисертације:

Р. бр.	аутори, наслов, часопис, волумен (година) број страница од-до, DOI или ISBN/ISSN	категорија
1.	Prodanović R., Sarang S., Rančić D., Vulić I., Stojanović G., Stankovski S. , Ostojić G., Baranovski I., Maksović D.: Trustworthy Wireless Sensor Networks for Monitoring Humidity and Moisture Environments (https://doi.org/10.3390/s21113636), Sensors, 2021, Vol. 21, No. 3636, pp. 1-24, ISSN 1424-8220	M21
2.	Baranovski I., Stankovski S. , Ostojić G., Nikolić V., Simonović M., Stanojević M. Toward a smart ecosystem with automated services. In facta Universitatis, Series: Mechanical Engineering, (2022), 0.22190/FUME220525033B	M21
3.	Vulić I., Borisov M., Prodanović R., Rančić D., Petrović V., Stankovski S. , Ostojić G.: Protection of Digital Elevation Model—One Approach (https://doi.org/10.3390/app12199898), Applied Sciences, 2022, Vol. 12, No. 19, ISSN 2076-3417	M21
4.	Antić V., Protić D., Stanković M., Prodanović R., Manić M., Ostojić G., Stankovski S. , Kučević D.: Protecting Data at Risk of Unintentional Electromagnetic Emanation: TEMPEST Profiling, Applied Sciences, 2024, Vol. 14, No. 11, ISSN 2076-3417	M22
5.	Arsenijević D., Arsenijević J., Tegeltija S., Zhang X., Ostojić G., Stankovski S. : Assessing Internet of Things Readiness on University Campuses: A Smart Campus-Oriented Approach, IoT, 2026, Vol. 7, No. 39, pp. 1-21, ISSN 2624-831X	M22

V.3 Услови дефинисани за ментора у складу са *Правилима докторских студија Универзитета у Новом Саду* за област којој припада докторска дисертација:

На основу Закона о високом образовању, као и у складу са *Правилима докторских студија Универзитета у Новом Саду* усвојеним на седници Сената Универзитета у Новом Саду одржаној 25.2.2021, која су ступила на снагу 5. 3. 2021., а примењују се од 1. 4. 2021. године (Измене и допуне: 27. 10. 2022. године; 30. 3. 2023. године; 28. 3. 2024. и 30. 9. 2025. године) за ментора за израду докторске дисертације, односно докторског уметничког пројекта може бити именован наставник Универзитета, односно факултета који је у радном односу на факултету који реализује студијски програм докторских студија, као и наставник који је у радном односу на другом универзитету, односно факултету или научној установи, а који има потребну научну, односно уметничку способност из области теме докторске дисертације, односно докторског уметничког пројекта. Ментор мора имати референце из научне, односно уметничке области којој припада тема

докторске дисертације, односно докторског уметничког пројекта и испуњавати друге услове из Стандарда. За поље техничко-технолошких наука ментор мора имати најмање пет радова објављених у претходних десет година у часописима са импакт фактором са SCI листе, односно SCIE листе.

Образложење:

Проф. др Стеван Станковски задовољава услове дефинисане стандардима за акредитацију и има најмање пет радова из категорије M21, M22 односно M23.

Да ли ментор испуњава услове?

ДА

НЕ

VI ЗАКЉУЧАК

Тема је подобна		ДА	НЕ
Кандидат је подобан		ДА	НЕ
Ментор је подобан		ДА	НЕ

Образложење о подобности теме, кандидата и ментора (до 500 речи):

Комисија је након детаљне анализе целокупне документације закључила следеће:

- Предложена тема је актуелна и адекватна за докторску дисертацију.
- Милош Станојевић испуњава услове за израду предложене докторске дисертације.
- Проф. др Стеван Станковски испуњава услове за ментора предложене докторске дисертације.

Комисија закључује да су испуњени сви неопходни услови односно да су кандидат, тема и ментор подобни за предложену докторску дисертацију.

Комисија предлаже Наставно-научном већу Факултета техничких наука, Универзитета у Новом Саду да прихвати тему докторске дисертације „Заштитни механизми од сајбер напада и њихов утицај на перформансе индустријских управљачких система“ (енг. „Cyberattack protection mechanisms and their impact on performance in industrial control systems“), те да кандидату Станојевић Милошу одобри израду ове дисертације, а проф. др Стевана Станковског именује за ментора.

Место и датум: Нови Сад, 17.7.2026.

др Гордана Остојић, редовни професор, председник

др Ивана Шенк, ванредни професор, члан

др Срђан Тегелтија, ванредни професор, члан

др Емил Вег, редовни професор, члан

др Дејан Ранчић, редовни професор, члан

НАПОМЕНА: Члан комисије који не жели да потпише извештај јер се не слаже са мишљењем већине чланова комисије, дужан је да унесе у извештај образложење односно разлоге због којих не жели да потпише извештај и да исти потпише.