УНИВЕРЗИТЕТ У НОВОМ САДУ

ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА

МЕТОДОЛОГИЈА ЗА БЕЗБЕДНУ ПРИМЕНУ РАЧУНАРСТВА У ОБЛАКУ У НАДЗОРУ И УПРАВЉАЊУ ПАМЕТНИМ ЕЛЕКТРОЕНЕРГЕТСКИМ СИСТЕМИМА

ДОКТОРСКА ДИСЕРТАЦИЈА

Ментор:
Проф. др Имре Лендак

Кандидат:
Бојан Јелачић

Нови Сад, 2022. године

УНИВЕРЗИТЕТ У НОВОМ САДУ **ОБРАЗАЦ – 5а**

ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА

КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА[1]

Врста рада:	Докторска дисертација
Име и презиме аутора:	Бојан Јелачић
Ментор (титула, име, презиме, звање, институција)	Проф. др Имре Лендак, ванредни професор, Факултет техничких наука, Универзитет у Новом Саду
Наслов рада:	Методологија за безбедну примену рачунарства у облаку у надзору и управљању паметним електроенергетским системима
Језик публикације (писмо):	Српски (ћирилица)
Физички опис рада:	Унети број: Страница 132 Поглавља 9 Референци 138 Табела 47 Слика 33 Графикона 0 Прилога 1
Научна област:	Електротехничко и рачунарско инжењерство
Ужа научна област (научна дисциплина):	Примењени софтверски инжењеринг
Кључне речи / предметна одредница:	Паметне мреже, рачунарство у облаку, сигурност, безбедност

[1] Аутор докторске дисертације потписао је и приложио следеће Обрасце:
5б – Изјава о ауторству;
5в – Изјава о истоветности штампане и електронске верзије и о личним подацима;
5г – Изјава о коришћењу.
Ове Изјаве се чувају на факултету у штампаном и електронском облику и не кориче се са тезом.

Резиме на језику рада:	Хакерски напади на различите критичне инфраструктуре у периоду 2000-2020 су показали да није довољна примена адекватних мера физичке безбедности, већ је неопходно обезбедити заштиту и од напада у сајбер простору. Последице таквих инцидената могу бити финансијски значајне, доводе до губитка поверења корисника у компанију, и у екстремним ситуацијама могу да угрозе животну средину или доведу до људских жртава. Употребом рачунарства у облаку (енг. cloud computing) одржавање и надоградња рачунарског хардвера и софтвера се делегира трећем лицу. Предузећа за управљање електроенергетским системима су за сада већином скептична у погледу спајања паметних мрежа са рачунарством у облаку, углавном због велике количине осетљивих података и великог броја критичних процеса који су од јавног значаја. Предмет истраживања ове докторске дисертације је методологија процене безбедносних ризика примене најновијих достигнућа у домену рачунарства у облаку у контексту надзора и управљања паметним електроенергетским системима (EEC). Овде је важно нагласити постојање значајних разлика између подсистема за надзор и управљања (енг. Supervisory Control and Data Acquisition – SCADA), који се у научној и стручној литератури често назива „оперативним подсистемом“ (енг. Operational Technology – OT), односно пословног подсистема који се у релевантној литератури често наводи под називом „информационе технологије“ (енг. Information Technology – IT). У овом раду ће фокус бити на анализи безбедносних ризика у OT подсистему. Ова тема је значајна, јер њена темељна анализа може охрабрити власнике паметних EEC да се одлуче на корак прихватања решења из домена рачунарства у облаку уз очување високог нивоа сигурности и безбедности.
Датум прихватања теме од стране надлежног већа:	29.04.2021.
Датум одбране: (Попуњава одговарајућа служба)	
Чланови комисије: (титула, име, презиме, звање, институција)	Председник: др Срђан Вукмировић, редовни професор, Факултет техничких наука, Нови Сад Члан: др Игор Тартаља, ванредни професор, Електротехнички факултет, Београд Члан: др Горан Сладић, редовни професор, Факултет техничких наука, Нови Сад Члан: др Немања Недић, доцент, Факултет техничких наука, Нови Сад Члан, ментор: др Имре Лендак, ванредни професор, Факултет техничких наука, Нови Сад
Напомена:	

UNIVERSITY OF NOVI SAD

FACULTY OF TECHNICAL SCIENCES

KEY WORD DOCUMENTATION[2]

Document type:	Doctoral dissertation
Author:	Bojan Jelačić
Supervisor (title, first name, last name, position, institution)	Imre Lendak, Phd, Associate Professor, Faculty of Technical Sciences, University of Novi Sad
Thesis title:	Methodology for secure using cloud computing in the monitoring and management of smart power systems.
Language of text (script):	Serbian language Cyrillic script
Physical description:	Number of: Pages 132 Chapters 9 References 138 Tables 47 Illustrations 33 Graphs 0 Appendices 1
Scientific field:	Electrical and computer engineering
Scientific subfield (scientific discipline):	Applied software engineering
Subject, Key words:	Smart Grid, cloud, security, safety

[2] The author of doctoral dissertation has signed the following Statements:
5б – Statement on the authority,
5в – Statement that the printed and e-version of doctoral dissertation are identical and about personal data,
5г – Statement on copyright licenses.
The paper and e-versions of Statements are held at he faculty and are not included into the printed thesis.

Abstract in English language:	Hacker attacks on various critical infrastructures in the period 2000-2020 have shown that the application of adequate physical security measures is not enough, but it is necessary to provide protection against attacks in cyberspace. The consequences of such incidents can be financially significant, lead to a loss of customer confidence in the company, and in extreme situations can endanger the environment or lead to human casualties. Using cloud computing, the maintenance and upgrade of computer hardware and software are delegated to a third party. Power system management companies are currently mostly skeptical about connecting smart grids to cloud computing, mainly due to a large amount of sensitive data and a large number of critical processes of public importance. The subject of research of this doctoral dissertation is the methodology of security risk assessment of the application of the latest achievements in the field of cloud computing in the context of monitoring and management of smart power systems (EES). Here it is important to emphasize the existence of significant differences between the Supervisory Control and Data Acquisition (SCADA) subsystem, which in the scientific and professional literature is often called the "operational subsystem" (Operational Technology - OT), or business subsystem which is often referred to in the relevant literature as "information technology" (IT). In this paper, the focus will be on the analysis of security risks in the OT subsystem. This topic is important because its thorough analysis can encourage smart power system owners to decide on the step of adopting solutions in the field of cloud computing while maintaining a high level of security and safety.
Accepted on Scientific Board on:	29.04.2021.
Defended: (Filled by the faculty service)	
Thesis Defend Board: (title, first name, last name, position, institution)	President: PhD Srđan Vukmirović, Professor, Faculty of Technical Sciences, Novi Sad Member: PhD Igor Tartalja, Associate Professor, Faculty of Elecrical Engineering, Belgrade Member: PhD Goran Sladić, Professor, Faculty of Technical Sciences, Novi Sad Member: PhD Nemanja Nedić, Assistant Professor, Faculty of Technical Sciences, Novi Sad Member, Mentor: PhD Imre Lendak, Associate Professor, Faculty of Technical Sciences, Novi Sad
Note:	

Захвалница

Сину Урошу и супрузи Раденки на топлини, љубави, пожртвовању и разумевању, јер без њих ова докторска дисертација не би била написана.

Мојим родитељима, Невенки и Петру који су ме научили како да живим и како да креирам своју будућност и своју судбину. На драгоценим саветима и на томе што су ме постакли да кренем у правом смеру.

Брату Јовану и његовој породици на безрезевној подршци.

Ментору проф. Др Имрету Лендаку на помоћи и смерницама током писања докторске дисертације.

Колегама и пријатељима који су били уз мене током свих година школовања.

Бојан

САДРЖАЈ

СПИСАК КОРИШЋЕНИХ СКРАЋЕНИЦА

Скраћеница	**Пуни назив**
IT	*Information Technology*
OT	*Operational Technology*
DSO	*Dystribution System Operator*
IEC	*International Electrotechnical Commision*
IEE	*Institute of Electrical and Electronics Engineers*
NIST	*National Institute for Standards and Techology*
EES	Elektroenergetski sistem
DoS	*Denial of Service*
SCADA	*Supervisory control and data acquisition*
IKT	Informacione i komunikacione tehnologije
INL	*Idaho National Labaratory*
VPN	*Virtual Private Network*
OMS	*Outage Management System*
SSM	*Switching Sequence Management*
ICS	*Industrial Control System*
GIS	*Geographic Information System*
CIA	*Confidentaly, Integrity, Avaliability*
NERC CIP	*North American Electric Reliability Corporation – Critical Information Protection*
MDM	*Meter Data Management*
ENISA	*Advanced Metering Infrastructure*
RTU	*Remote Terminal Unit*
ENISA	*Europen Union Agency for Cybersecurity*
NRM	*Network Risk Management*

TVRA	*Threat Vulnerability and Risk Analysis*
ETSI	*European Telecommunications Standard Institute*
ISO/IEC	*International Organization for Standardization*
SbD	*Security by Design*
FIPS	*Federal Information Processing Standards*
DDoS	*Distribution Denial of Service*
IED	*Intelligent Electronic Device*
CPNI	*Centre for the Protection of National Infrastructure*
CEN	*European Committee for Standardization*
CENELEC	*European Committee for Electrotechnical Standardization*
IaaS	*Infrastructure as a Service*
PaaS	*Platform as a Service*
SaaS	*Infrastructure as a Service*
IP	*Internet Protocol*
CSP	*Cloud Service Provider*
GDPR	*General Data Protection Regulation*
CSPM	*Cloud Security and Privacy Model*
RPN	*Risk Priority Number*
OWASP	*Open Web Application Security Project*
CSA	*Cloud Security Aliance*
STRIDE	*Spoofing, Tampering, Repudiation, Information Disclosure, Denail of Service, Elevation of Privilege*
DMS	*Dystribution Management System*
EMS	*Energy Management System*
OMS	*Outage Management System*
DMZ	*Demilitarized Zone*
SIEM	*Security Information and Event Management*
DNP3	*Distributed Network Protocol*
APT	*Advanced Persistent Threats*
ACL	*Access Control List*
RAM	*Remote Access Memory*
HDD	*Hard Disk Drive*
CPU	*Central Processing Unit*

CR	*Computer Resources*
R	*Risk*
PII	*Personal Identifiable Information*
OpenSSL	*Open Secure Sockets Layer*
PLC	*Program Logic Controller*
DMSR	*Dystribution Management System Real-Time Instance*
FEP	*Front End Processor*
DR	Disaster Recovery

СПИСАК СЛИКА

СПИСАК ТАБЕЛА

1. УВОД

У оквиру паметних електроенергетских система (ЕЕС) се тежи осавремењавању инфраструктуре, замене људи, оператера, аутоматизованим рачунарским системима и увођење дигиталне револуције у производњу, пренос, дистрибуцију и потрошњу електричне енергије. Ослањањем на комуникационе мреже и интегрисањем великог броја подсистема које одликује разноликост у погледу функционалности и коришћених технологија знатно се усложњава информациона инфраструктура електроенергетског система, а тиме повећава и његова рањивост из сајбер простора.

Последњих година енергетска индустрија се суочила са различитим проблемима узрокованим информационо-безбедносним пропустима чије последице могу имати велике размере, од прекидања свакодневних активности и наношења значајне економске штете, губитка поверења корисника према компанији и штете за репутацију компаније, па све све до проузроковања катастрофа које би угрозиле животну средину или довеле до људских жртава. Није се више довољно заштити само од физичких напада, већ је неопходно обезбедити заштиту од напада у сајбер простору, односно обезбедити заштиту информационих система и мрежа (енг. *cyber security*). Онај ко има контролу над подсистемом за надзор и управљање паметног електроенергетског система може да промени начин његовог функционисања. Ако се то злоупотреби, доводи до озбиљних хаварија, финансијских губитака, нарушавања угледа компаније и као најгори сценарио до губитка људских живота.

Ако је у причу укључено и рачунарство у облаку (енг. *cloud computing*) као један од тренутно најатрактивних појмова у сфери информационих технологија (енг. *Information Technology*) IT, акценат на сајбер безбедност се додатно повећава што представља главни разлог због чега паметне мреже у рачунарском облаку нису заступњене у оној мери у којој би требале бити.

Овај рад настоји да охрабри власнике паметних електроенергетских система да се одлуче на прихватање решења из домена рачунарства у облаку уз очување високог нивоа сајбер безбедности. У ту сврху биће имплементирана методологија за безбедну примену рачунарства у облаку у надзору и управљању паметним електроенергетским системима.

Битно је напоменути да допринос ове дисертације није уско везан за енергетику, већ ће се предложена методологија моћи прилагодити (енг. *Operational Techology*) OT подсистемима других инфраструктурних и индустријских система спрам потреба потенцијалних корисника.

1.1 Предмет и потребе истраживања

Од почетка 21. века енергетска индустрија се суочила са различитим проблемима узрокованим информационо-безбедносним пропустима. Последице таквих инцидената могу бити финансијски значајне, доводе до губитка поверења корисника у компанију, и у екстремним ситуацијама могу да угрозе животну средину или доведу до људских жртава. Хакерски напади на различите критичне инфраструктуре у периоду 2000.-2020. године су показали да није довољна примена адекватних мера физичке безбедности, већ је неопходно обезбедити заштиту и од напада у сајбер простору.

Можда најпознатији примери таквих напада, који уједно добро илуструју домете штете која може да настане као последица напада чији је извор у сајбер простору, а ефекти се осећају у физичком окружењу су следећи:

1. Stuxnet напад 2010. године који је представљао саботажу над нуклеарним постројењем у Ирану где је уз помоћ посебно дизајнираног злонамерног софтвера (енг. *malware*) преузета контрола над индустријским контролним системом и нанета штета у физичком простору.
2. *Malware* Duqu, откривен 2011. године, дизајниран да компромитује индустријске системе са циљем прикупљања информација из контролних система за будућу експлоатацију.
3. Хакерски напад у децембру 2015. године на Украјинске компаније у електроенергетском сектору услед којих је преко 200.000 потрошача остало без електричне енергије у трајању од више сати.
4. Један од највећих цевовода у Америци, који пречишћава бензин и млазно гориво од Тексаса до Њујорка, био је присиљен да се затвори током хакерског напада у мају 2021. године.

Више информација о самим нападима ће бити прикзано у поглављу о теоријским основама и прегледу литературе ове докторске дисертације.

Осим малициозних напада који могу да угрозе правилно функционисање система, велики изазов представља и очување приватности корисника, са обзиром да су различите информације о потрошачима сада доступне како у пословним информационим, тако и у ОТ подсистемима.

Употребом рачунарства у облаку одржавање и надоградња рачунарског хардвера, решавање потенцијалних проблема на оперативном систему и других се делегира трећем лицу. Предузећа за управљање електроенергетским системима су за сада већином скептична у погледу спајања паметних мрежа са рачунарством у облаку, углавном због велике количине осетљивих података и великог броја критичних процеса који су од јавног значаја. Предмет истраживања ове докторске дисертације је методологија за безбедну примену рачунарства у облаку у надзору и управљању паметним електроенергетским системима. Ова тема је значајна, јер њена темељна анализа може охрабрити власнике паметних ЕЕС да се одлуче на корак прихватања решења из домена рачунарства у облаку уз очување високог нивоа сајбер безбедности.

Као потребе истраживања намећу се следећи аспекти:

1. Предлог сигурних и безбедних решења уз максималну искористивост моћи најновијих технологија као што је рачунарство у облаку
2. Заузимање позиције у односу на конкуренцију пратећи најновије трендове
3. Охрабривање предузећа да ОТ компоненте своје паметне мреже мигрирају на рачунарски облак
4. Заштита осетљивих података
5. Смањење укупних трошкова
6. Повећање перформанси софтвера
7. Поверење корисника

1.2 Циљ истраживања и очекивани резултати

Миграција паметних мрежа, као и осталих критичних инфраструктура на рачунарски облак је у повоју. Главни разлог одлагања миграције је сајбер безбедност и неповерење у чињеницу да ће осетљиви ресурси бити препуштени на чување трећој страни.

Циљ истраживања је развој методологије за безбедну примену рачунарства у облаку у надзору и управљању паметним електроенергетским системима. Као што је речено, ова методологија није уско везана за паметне ЕЕС-е, већ је планирано да њена употреба буде могућа и у случају ОТ подсистема других инфраструктура (нпр. гас, вода и отпадне воде), односно индустријских контролних система.

У циљу анализе и верификације развијене методологија за безбедну примену рачунарства у облаку у ОТ подсистемима паметних ЕЕС биће изабрани конкретни примери базирани на захтевима реалних пројеката (реалне корисничке улоге, реални пословни процеси). Методологију ћемо тестирати на две студије случаја, на великом оператеру дистрибутивног система (енг. *Distribution System Operator*) DSO, са сложеним ОТ окружењем и могућношћу опоравка од катастрофе (енг. *Disaster Recovery*); и малом DSO са ограниченим могућностима ОТ подсистема, буџетом и IT особљем а све уз одржавање одговарајућег нивоа сајбер безбедности

Резултат истраживања ће бити презентован кроз прототип обрасца који ће представљати акумулирану процену ризика, затим кроз детаљну анализу потребе за рачунарским ресурсима сваке од компоненти датог DSO-а, као и кроз јасно дефинисану миграциону стратегију на основу чега ће се креирати неколико примера миграције ОТ подсистема на рачунарски облак. Предност методологије је што добијамо више различитих варијанти миграције, од оних са већим нивоом толеранције ризика (већа искористивост услуга рачунарског облака на уштрб сајбер безбедности) до оних оптималних у смислу да смо задовољили како аспекте потребе за рачунарским ресурса тако и задовољавајући ниво сајбер безбедности.

Циљ истраживања ће се састојати из следећих целина:

1. Реализација методологије за безбедну примену рачунарства у облаку у надзору и управљању паметним електроенергетским системима
2. Тестирање и доказивање корисности методологије

1.3 Хипотезе

Хипотезе од којих се у истраживању полази су:

1. **Хипотеза 1**: Могуће је развити методологија за безбедну примену рачунарства у облаку у надзору и управљању паметним електроенергетским системима
2. **Хипотеза 2**: Развијена методологија може бити применљива у контексту ЕЕС различите сложености.

1.4 Методе истраживања

За потребе истраживања биће примењене следеће методе:

1. Анализа стања у области кроз систематично прикупљање и преглед релевантне литературе
2. Развој прототипа
3. Експерименти

Почетна фаза ове дисертације је прикупљање релевантне литературе и њена детаљна анализа. На основу дате литературе можемо видети јасну слику актуелног стања у области, као и нове трендове и правце развоја. На овај начин показујемо где смо ми у односу на друге. Уколико више адекватних истраживања укаже на исте позитивне и негативне правце, на основу тога свакако можемо донети одлуку којим путем да наставимо, а који приступ да избегавамо. У области критичних инфраструктурних система, рачунарства у облаку, а поготово сајбер безбедности постоји велики број усвојених стандарда на које ћемо се позивати.

Систематичан преглед литературе ће бити спроведен у три фазе:

1. Планирање
2. Спровођење
3. Извештавање

Фаза планирања обухвата следеће области:

1. Сајбер безбедност у паметним електроенергетским системима
2. Анализа ризика у паметним електроенергетским системима
3. Преглед најзначајнијих стандарда у области информационе безбедности паметних електроенергетских система
4. Сајбер безбедност у рачунарском облаку
5. Анализа ризика у рачунарском облаку
6. Преглед најзначајнијих стандарда у области информационе безбедности рачунарског облака
7. Анализа постојећих методологија за процену безбедносних ризика примене рачунарства у облаку у контексту паметних електроенергетским система

У току фазе планирања, неопходно је за сваку од области истраживања пронаћи одговарајуће радове. Потребно је да се обради целокупни научни доказ из области, како

би јасно видели где се налазимо и шта је до сада истражено а шта не. У фази спровођења систематичног прегледа литературе вршиће се селекција радова на основу више критеријума као што су година објављивања, цитираност и многи други. На крају ће се у фази извештавања изабрати најрелевантније радове. Објаснићe се важност сваког од њих у оквиру израде тезе и на који начин је послужио као основа за даље истраживање.

На основу систематичног прегледа литературе и истраживања, креира се прототип архитектуре ОТ подсистема. Развијени прототип омогућава извођење експеримената у циљу провере применљивости методологије.

У фази експериментисања ћемо верификовати развијену методологију на претходно споменутом прототипу архитектуре ОТ подсистема. Опсези експеримената ће зависити од хипотеза које требају да потврде. Током анализе добијених резултата тестираћемо хипотезе експеримената, тачније да ли резултати задовољавају претпоставке хипотези. Применљивост предложене методологије ће бити испитана на основу случајева коришћења који су дефинисани према захтевима реалних пројеката на којима је аутор учествовао.

1.5 Приказ дисертација по поглављима

1. Увод
    1. Предмет и потребе истраживања
    2. Циљ истраживања и очекивани резултати
    3. Хипотезе
    4. Методе истраживања
    5. Приказ дисертације по поглављима
2. Теоријске основе и преглед литературе
    1. Сајбер безбедност у паметним електроенергетским системима
    2. Анализа ризика у паметним електроенергетским системима
    3. Преглед најзначајнијих стандарда у области информационе безбедности паметних електроенергетских система
    4. Сајбер безбедност у рачунарском облаку
    5. Анализа ризика у рачунарском облаку
    6. Преглед најзначајнијих стандарда у области информационе безбедности рачунарског облака
    7. Анализа постојећих методологија за процену безбедносних ризика примене рачунарства у облаку у контексту паметних електроенергетским система
3. Прототип архитектуре ОТ подсистема
    1. ОТ подсистем
    2. ОТ DMZ подсистем
    3. ИТ подсистем
4. Методологија за процену ризика у паметним електроенергетским мрежама
    1. Претње и извори претњи
    2. Вероватноћа реализације претњи
    3. Утицај који се проузрокује потенцијалним реализовањем одговарајуће претње
    4. Матрица ризика

2. ПРЕГЛЕД АКТУЕЛНОГ СТАЊА У ОБЛАСТИ

Живимо у ери великог технолошког напретка. Оно што нам се данас чини као иделано решење, већ сутра може да буде застарело и превазиђено. Добар пример за то су рачунари, уређаји са којима смо свакодневно у контакту, па смо сведоци њиховог убрзаног развоја и велике експанзије задњих година. Ако се вратимо само деценију или две уназад, и упоредимо могућности ових уређаја и система заснованих на њима са данашњим, једино што преостаје је да се запитамо шта можемо очекивати у будућности. Велики број светски признатих играча из ове области се утркује да узме што већи дио колача на тржишту. Управо ова трка и настојање да се надмаши конкуренција представља главног кривца за горе поменуту експанзију. Рачунари су ушли у све сфере данашњег доба и модерни живот је тешко замислити без њих.

Оно без чега рачунари не би могли да функционишу, без чега не би ни постојали је електрична енергија. Изум електричне енрегије представља један од најзначајнијих тренутака у нашој цивилизацији. Производња, пренос и дистрибуција електричне енергије се током свога живота нису пуно мењале, док на другој страни, рачунари и рачунарски системи који су настали много касније и за чији настанак је било потребно да се прво појави управо електрична енергија доживљавају невероватну експанзију.

У данашње време пораст броја потрошача електричне енергије је свеприсутан, и тај тренд се наставља из дана у дан. Традиционални електроенергетски системи без великих улагања тешко се могу изборити са овим, те се због тога тежи осавремењавању електроенергетске инфраструктуре, замене људи, оператера, аутоматизованим рачунарским системима и увођење револуције у производњу, пренос, дистрибуцију и само коришћење електричне енергије. Ово представља основни концепт паметних мрежа. Паметни електроенергетски системи представљају бољу интеграцију обновљивих извора у електроенергетску мрежу и уводе одређене технолошке иновације које омогућавају да мрежа функционише на другачији начин од садашњег. Њиховим коришћењем отвара се пут према "зеленој енергетици", тј. да се користи што више обновљивих извора енергије. Улога потрошача више није само да троше електричну енергију, већ и да је производе уз помоћ ветра и соларних панела. Рачунари су кључни елементи паметних електроенергетских система, где обављају многобројне улоге, од надзора и управљања, преко извршавања алгоритама за анализу понашања система, па све до наплате услуга, тј. коришћења електричне енергије.

Ако ћемо причати о револуцијама у ИТ свету, рачунарство у облаку свакако заслужује нашу пажњу. То је дио рачунарства који је у великој експанзији. Његов основни циљ је да понуђачи своје апликације сместе у рачунарски облак, где би користиле хардверску подршку и остале ресурсе самих провајдера. Употреба тих ресурса се наплаћује на основу потрошње. Овај принцип наплате услуга је сличан начину на који се данас плаћају струја,

вода, телефон и многе друге услуге. Оно чему се тежи као крајњем циљу је да се корисници претплате код власника апликација, како би добили окружење у коме би се дата апликација извршавала, а да при томе не брину о проблемима који се могу десити на хардверу, оперативном систему и низу других проблема који данас мучи већину корисника.

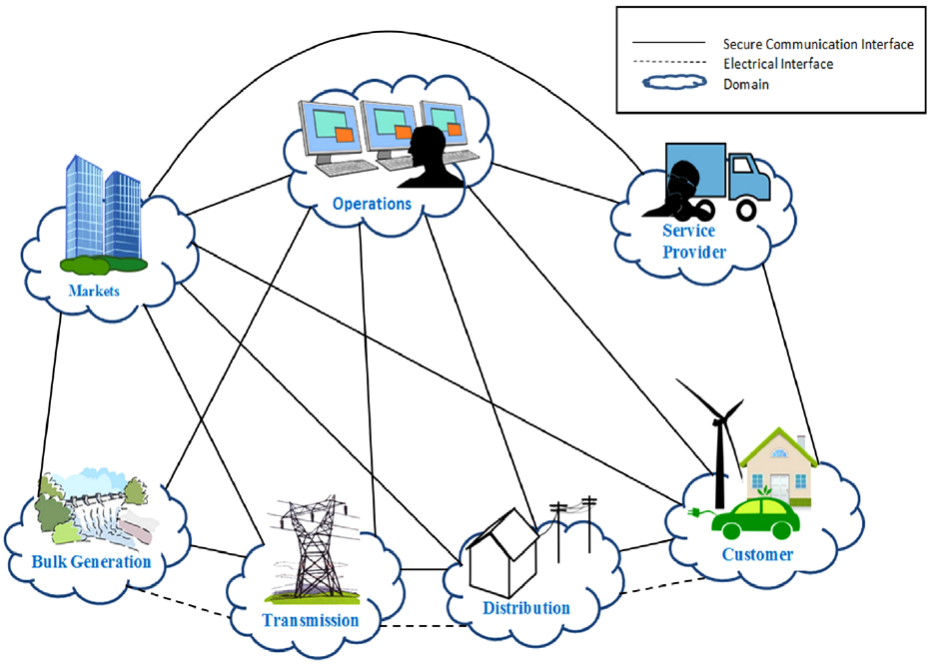
Са обзиром да се паметним електроенергетским системима управља уз помоћ савремених информационих и комуникационих технологија, њихова миграција на рачунарски облак се намеће као велики изазов.

Електроенергетски системи спадају у групу критичних инфраструктурних система те је због тога неопходно њихово константно усавршавање и надоградња. Увођењем рачунарства и информационих система у овај домен добијамо паметне електроенергетске системе. Можемо их дефинисати као савремене енергетске инфраструктуре које подразумевају интеграцију традиционалних енергетских система за производњу, пренос и дистрибуцију енергената (електрична енергија, гас, вода) са информационим и комуникационим технологијама (ИКТ) у циљу повећања поузданости, ефикасности и безбедности система критичних за свакодневно функционисање модерног друштва. Примена најновијих достигнућа у домену ИКТ повећава флексибилност, приступачност, поузданост и економичност ових система [1][2][3][4][5].

Додатно, паметни електроенергетски системи треба да омогуће потпуну контролу над мрежом од стране оператера предузећа, велики број аутоматских радњи под којима се између осталог мисли на самостално поправљање и отпорност на различите аномалије, као и интеграцију свих елемента мреже у једну логичку целину.

Не постоји јединствена дефиниција паметне мреже. Једне од најтачнијих дефиниција су [3]:

1. Америчко Министарство енергетике: “Паметна мрежа користи дигиталну технологију за побољшање поузданости, сајбер безбедности и ефикасности (како економске, тако и енергетске) електроенергетског система почевши од производње, преко система за испоруку потрошачима електричне енергије и све већег броја дистрибуираних извора производње и складиштења “.
2. Међународна електротехничка комисија: (енг. *International Electrotechnical Commission - IEC*): “Паметна мрежа је мрежа далековода, опреме, контрола и нових технологија у развоју које заједно функионишу како би одмах одговориле на нашу потражњу за електричном енергијом у 21. веку.“
3. Институт инжењера електротехнике и електронике (енг. *Institute of Electrical and Electronics Engineers - IEEE*): „Паметна мрежа је револуционарни подухват који укључује нове комуникационе и управљачке способности, изворе енергије, моделе производње и придржавање вишеструких регулаторних структура надлежности.“
4. Национални институт за стандарде и технологију (енг. *National Institute for Standards and Technology - NIST*): “Паметна мрежа је мрежни систем који интегрише многе врсте дигиталних рачунарских и комуникационих технологија и услуга у инфраструктуру електроенергетског система.



Слика 1 - Основни концепт паметног електроенергетског система [1]

Једна од значајнијих предности које доносе паметни електроенергетски системи је могућност складиштења електричне енергије. Енергија се складишти у случајевима када је производња већа од потрошње, а као таква се користи када је потрошња већа од производње или у интервалима када је цена електричне енергије висока. Због ове могућности производња електричне енергије се не треба драстично повећавати и смањивати према захтевима потрошње, већ се одржава на равномерном нивоу. Овакво одржавање производње знатно смањује потрошњу необновљивих извора енергије, повећава енергетску ефикасност, што је и један од циљева увођења паметних ЕЕС. Тренутно, не постоји начин да се врши складиштење велике количине енергије, већ се она смешта у адекватно направљене батерије за ту сврху.

Све предности паметних електроенергетских система у односу на традиционалне су приказане у следећој табели.

Табела 1- Предности паметних ЕЕС у односу на традиционалне [1]

Традиционални ЕЕС	**Паметни ЕЕС**
Механизација	Дигитализација
Једносмерна комуникација	Двосмерна "*real-time*" комуникација
Централизована производња електричне енерије	Дистрибуирана производња електричне енергије
Радијална електроенергетска мрежа	"*Dispersed*" електроенергетска мрежа
Мали број сензора	Велики број сензора и монитора

Мало или без аутоматског надгледања	Напредно аутоматско надгледање
Мануелна контрола и опоравак	Аутоматска контрола и опоравак
Мале бриге о сајбер безбедности	Склоне сигурносним и безбедносим проблемима
Константна пажња људи на поремећаје система	Адаптивна заштита
Истовремена прозводња и потрошња електричне енергије	Складиштење електричне енергије
Лимитирана контрола	Широк систем за контролу
Спор одзив на хитне случајеве	Брз одзив на хитне случајеве
Мали избор корисника	Велики избор корисника

Паметни електроенргетски системи се деле на информационе технологије и операционе технологије. Основна разлика између ова два подсистема се огледа у томе што ИТ управља протоком дигиталних података у оквиру пословног домена, док ОТ представља подсистем у оквиру кога се врши надзор и управљање физичким процесима и машинама. Једне од најтачнијих дефиниција ова два система су следеће:

1. ОТ је хардвер и софтвер који откривају или изазивају промену директним надгледањем и/или контролом физичких уређаја, процеса и догађаја у систему. [6]
2. ИТ је уобичајени термин за читав спектар технологија за обраду информација, укључујући софтвер, хардвер, комуникационе технологије и сродне услуге. [7]

Иако су ови подсистеми традиционално радили као засебни ентитети, најновији трендови показују да је потребна њихова дубља интеграција у транзицији ка правим паметним ЕЕС [2][8][9].

Интеграција ИТ и ОТ система пружа многе бенефите. Палета технолошких предности повезаних са интеграцијом ова два подсистема укључује [1]:

1. Трошкови прикупљања и преношења оперативних података се смањују.
2. Софтвер који стоји у основи многих ОТ подсистема користи стандардне ИТ рачунарске платформе, што омогућава спајање ресурса. Постоје и опције за коришћење рачунарског облака који доноси могућност обраде података са већим опсегом рачунарских капацитета.
3. Повезивања и интегрисање различитих скупова података над којима се могу радити напредне анализе.
4. Приступ оперативним подацима у реалном времену од стране теренских посада (користећи мобилни телефон или таблет) знатно мења дистрибутивне активности као што су оптимизација ресурса на терену, брзина реаговања на разне кварове, праћење залиха и многе друге.
5. Стандарди интероперабилности су развијени и примењени, мада је даље сазревање таквих стандарда пресудно за активирање даље интеграције ИТ/ОТ. Неколико организација, укључујући и међународну комисију за електротехнику IEC и институт за инжењере

електротехнике и електронике, IEEE, развијају стандарде интероперабилности паметних мрежа.

У овом истраживању фокусираћемо се на ОТ подсистем паметне мреже, тачније на његов део за контролу и надзор.

2.1 Сајбер безбедност у паметним електроенергетским системима

Као што можемо видети из *Табела 1*, поред свих позитивних особина, паметне мреже носе са собом и један веома важан недостатак, а то су значајни безбедносни ризици [4][5][9][10]. Традиционални приступ безбедности индустријских контролних система који се ослања на физичку изолованост и принцип затворености (енг. *security-by-obscurity*) [12][13] није више довољан за поуздан и сигуран рад савремених електроенергетских система. Анкета [14] која је спроведена у 18 земаља над више од 200 индустријских контролних система показала је да 90% њих имало проблема са (енг. *Denail of Service*) DoS нападима што је инпозантна бројка и један од индикатора колико су заправо ове врсте система атрактивне за потенцијалне нападаче.

Увођење стандардних ИКТ решења у ОТ подсистем он постаје све отворенији и повећава се површина напада [15][16]. Док је раније ИТ подситем био атрактиван за потенцијалне нападаче, сада све више тај примат преузима ОТ [14]. За разлику од напада на ИТ подсистеме, сајбер напади на ОТ имају за циљ да прекину напајање, оштете високо специјализовану опрему и на крају угрозе здравље, сигурност и животе људи. Заштита сајбер безбедности ОТ подистема [8][11][15] се фокусира на одржавање поверљивости, интегритета и доступности података. Међутим, безбедност се мора фокусирати и на факторе окружења, регулацију, међузависности и профитабилност физичког процеса зато што подсистем мора радити у реалном времену и често су присутни веома високи захтеви за расположивост. Оператор такође мора да се брине о регулаторним захтевима, утицајима на животну средину и међузависностима које ОТ подсистем има на друге системе и инфраструктуре [8].

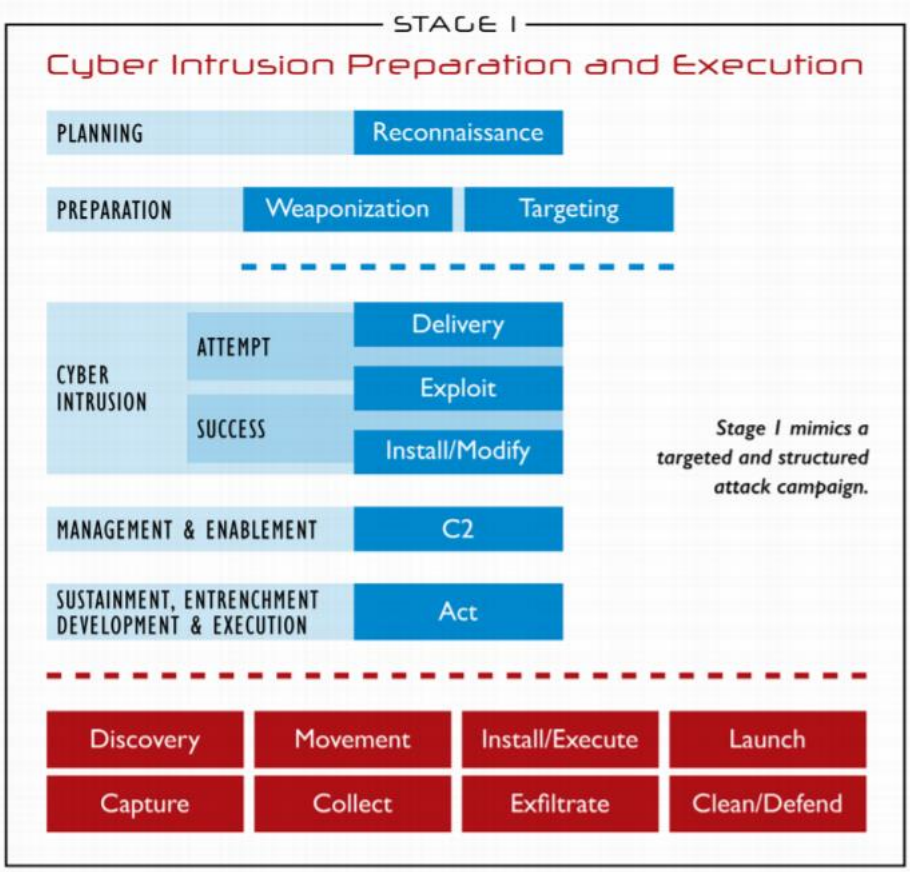
Сајбер безбедност ОТ подсистема је често главни приоритет, те се због тога многи поступци и политике унутар њега преиспитују са великом пажњом. У последње две деценије сведоци смо различитих врста напада на индустријске контролне системе који су имали озбиљне последице, па чак у неким случајевима су резултоване и смртним исходом. Напади на паметне мреже се могу класификовати на физичке, сајбер и хибридне. Неки од најпознатијих су:

1. *Stuxnet* напад који представља саботажу над нуклеарним постројењима у Ирану појаснио је шта се може урадити из сајбер простора [17]. Метод напада је био посебно развијен *malware* дизајниран да искористи рањивост оперативног система и индустријског контролног система са циљем преузимања контроле над ОТ подсистемом и издавања команди актуаторима који су довели до кварова опреме која се користила за обогаћивање нуклеарног горива. Причињена штета је била значајна и у одређеној мери је утицала на успорење Иранског нуклеарног програма [18].

2. Сложени *malware Duqu* откривен 2011. године дизајниран је да компромитује индустријске системе са циљем прикупљања информација из контролних система за будућу експлоатацију [18].
3. Напади у Украјини 2015. и 2016. године против одабраних елемената државног електроенергетског система показали су да такви напади на сајбер-физички систем могу имати значајне последице у облику нестанка струје, који су у 2015. трајали 1 до 6 сати и афектовали око 225.000 потрошача [19].
4. Догађај у националној лабораторији (енг. *Idaho National Laboratory*) INL [20] показао је како напад на електричну мрежу може физички да оштети генераторе. Нападнут је заштитни релеј који је затим коришћен за стално затварање и отварање прекидача који повезује генератор на мрежу [20]. Стално затварање прекидача када генератор није био синхронизован са решетком узроковало је уништење генератора [20].
5. Интересантан је и пример [14] напада на систем за надзор безбедности нуклеарног система у Охају 2003. године када је дошло до паралисања система на 5 часова. *Malware* је стигао путем рачунара једног од извођача који је био конектован на систем и на тај начин заобишао заштитини зид [14]. Срећом електрана је била затворена због редовног одржавања, али се *malware* путем интернета успио пробити и заразити 75 хиљада корисника у року од 10 минута, као и путем виртуалне приватне мреже (енг. *Virtual Private Network - VPN*) заразити систем контроле електроенергетских компанија и још два интегрисана предузећа [14]. Штета је била преко један билион долара.
6. Иако не припада домену електроенергетских система, догађај [21] је пример где је услед недоступности (енг. *Supervisory Control And Data Acquisition*) SCADA система дошло до експлозије у којој су погинуле три особе, осам особа је повређено и нанета је немерљива штета околини и животној средини. Сви ови догађаја несумњиво говоре о катастрофалним последицама које се дешавају услед неадекватне заштите критичних инфраструктурних система, па и ОТ подистема као његовог дела.
7. *Malware Xavex* [22] који се проширио компромитујући инсталационе датотеке популарних софтверских производа за даљински приступ који се користе у ОТ окружењима. Када су корисници инсталирали оно што су мислили да је оригиналан софтвер, они су несвесно инсталирали и дати злонамеран код који је проузроковао значајну штету.

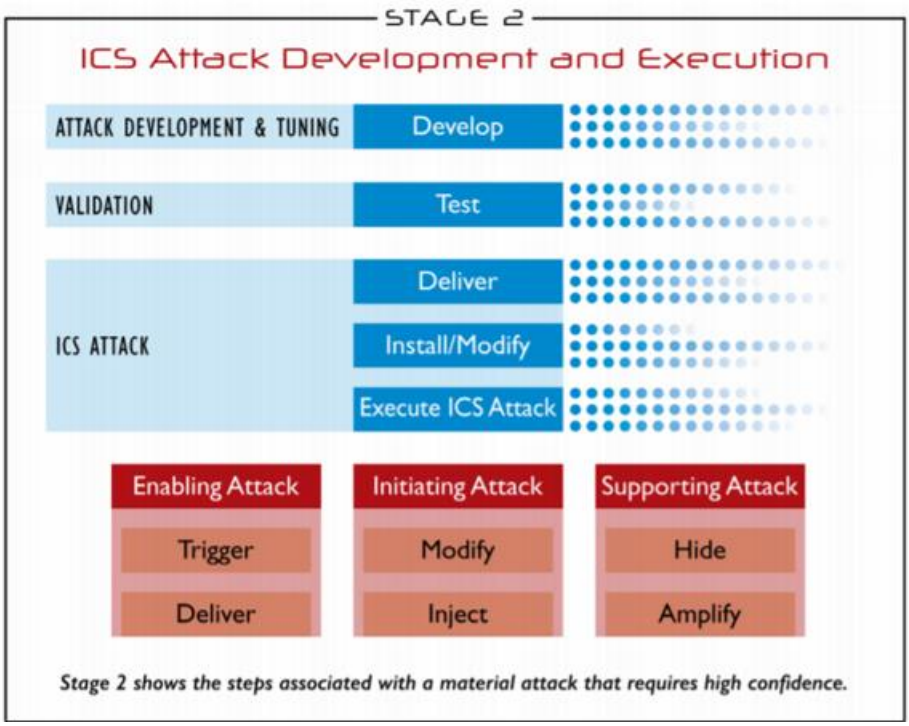
Сајбер напади на индустријске контролне системе разликују се по утицају на основу низа фактора, укључујући намеру противника, њихову софистицираност, способност, као и њихово упознавање са индустријским контролним системом (енг. *Industrial Control Systems - ICS*) и аутоматизованим процесима. Они уводе концепт ICS Cyber Kill Chain са циљем да помогне да се разуме кампања сајбер напада. [23]

Овај концепт се дели на два велика корака, са више фаза у оквиру сваког од њих. Први се састоји од припреме и извршења напада и често се класификује као шпијунажа или обавештајна операција. Током њега се покушава добити што више информација о самом систему и његовом функционисању како би се касније, у другом кораку те информације искористиле.



Слика 2 - Припрема и извршење напада [23]

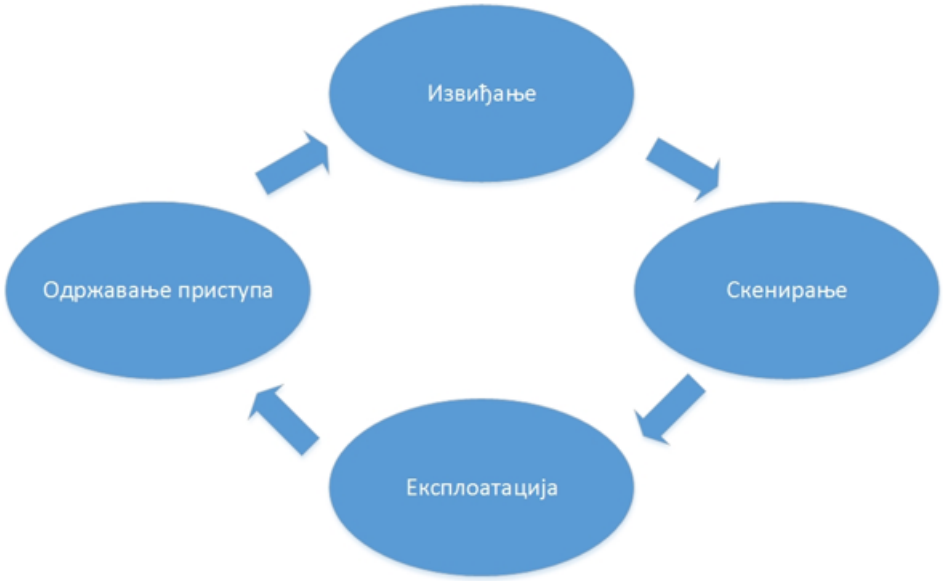
Као што је речено, на основу знања стеченог у првом кораку, потенцијални нападач развија и користи алате помоћу којих може да изазове значајну штету индустријским контролним системима.



Слика 3 - Развој и реализација напада на ICS [23]

Према [23], иако постоје различити начини за напад на ICS окружење, најчешћи методи за постизање функционалног утицаја су губитак приказа и контроле над мрежом, манипулација приказом и контролом, као и манипулација сензорима и осталом опремом.

Слични кораци који доводе до експлоатације система су описани у [24] и приказани на *Слика 4*. Овде злонамерни хакери користе четири корака за напад и контролу над системом, наиме извиђање, скенирање, експлоатација и одржавање приступа. Током првог корака, извиђања, нападач прикупља информације о свом циљу. У другом кораку, скенирањем, нападач покушава да идентификује потенцијалне рањивости које могу бити повезане са софтвером, особљем итд. Током корака експлоатације, покушава да направи компромис и стекне потпуну контролу над циљем. Када нападач има административни приступ циљу, прелази на последњи корак који је представља одржавање приступа. Овај корак се постиже инсталирањем скривеног програма како би се касније могао лако вратити у циљни систем.



Слика 4 - Четири корака за добијање контроле над системом од стране хакера

Да би осигурали информациону безбедност у оквиру ОТ подсистема неопходно је применити низ мера да се осигура (енг. *Confidentaly, Integrity, Avaliability*) CIA тријада, поверљивост, интегритет и расположивост података и информационих система [14][15][25]. Поверљивост информација (енг. *Confidentiality*) се односи на заштиту од неовлашћеног приступа или откривања података. Циљ је да се приступ подацима дозволи само ауторизованим странама како би се заштитили подаци о потрошњи и потрошачима. У контексту индустријских и инфраструктурних система нарушавање поверљивости представља мање ризичан сценарио од нарушавања интегритета (енг. *Integrity*) и расположивости (енг. *Availability*) [4][5][15][25][26][27][28][29]. Крађа информација (енг. *theft of information*) су напади који могу проузроковати откривање поверљивих информација [30]. Интегритет података се односи на заштиту информација од неовлашћеног брисања или измена. Циљ очувања интегритета података је обезбеђивање веродостојности, целовитости и тачности информација, односно да подаци буду ажурни и валидни. Очување интегритета података и сервиса је веома важно у ОТ подсистемима) [4][5][15][25][26][27][28][29]. Једна од главних категорија напада који могу довести до нарушавања интегритета је манипулација сервиса (енг. *manipulation of service*) [30]. Са аспекта функционисања паметних мрежа ниво расположивости података и сервиса је најзначајнији безбедносни циљ [11][12][30]. Док се кашњење у преносу података толерише у пословном подсистему, нормалан рад ОТ подсистема подразумева јасно дефинисана максимална кашњења у преносу [4][5][15][25][26][27][28][29]. За индустријске контролне системе се често захтева 4–5 поновних операција [8] или да су доступни 99.99% времена, што значи да могу бити спуштени само 5 до 50 мин током године. Овај прекид рада мора бити предвиђен да укључи и непредвиђене прекиде, као и многе функције одржавања система [8]. Најчешћи напад који има за циљ да преоптерети комуникациону мрежу и на тај начин доведе до кашњења и губитка података је ускраћивање услуге DoS напад [11][12][30].

Препоруке [8] су да се сигурносне процене и ревизије система требају редовно извршавати разним активностима (нпр. тестирање продора, процене рањивости) како би обезбедили да систем буде заштићен од рањивости, погрешних провера и разних видова

напада. Нажалост, многе технике које се користе за обављање ових процена, попут скенирања портова и скенирања рањивости, могу погоршати перформансе система или проузроковати његов потпуни пад [8].

Сајбер безбедност у паметним мрежама анализирана је систематском студијом од тридесет шест публикација на ову тему [31]. Неке од ових публикација нису стандарди у строгом значењу ове речи. Првобитно су били приказани као смернице, технички извештаји, да би временом дефакто постали стандарди. Аутори референце [32] тврде да би напади на електроенергетску мрежу могли резултирати значајним штетама и описују приступ заштити сајбер безбедности који би помогао у дизајнирању и имплементацији система заштите електроенергетских мрежа. Према (енг. *North American Electric Reliability Corporation - Critical Infrastructure Protection*) NERC CIP, оквири усаглашености са високим приоритетом и прописима захтевају да IT особље и особље OT раде заједно на новим и иновативним начинима за размену документације и сарадњи на јачању безбедности у паметним електроенергетским системима [33][34].

2.2 Анализа ризика у паметним електроенергетским системима

Оно што се намеће као недостатак када причамо о сајбер безбедности OT подсистема је недовољно информација о обиму потенцијалних претњи и утицаја који те претње могу да изазову ако би се реализовале. Све до сада наведено показује са колико широким проблемом се паметни електроенергетски системи свакодневно сусрећу када причамо о аспекту сајбер безбедности и колико то омета њихов свакодневни рад. Свакако охрабрује чињеница [35] да је у енергетском сектору Европе 2019. године направљен значајан помак према заштити критичне инфраструктуре од сајбер претњи и то што је овај вид претње постао предмет од националног значаја. Сличног мишљења су и у америчком енергетском сектору. Они наводе [36] да растућа учесталост, софистицираност и ефикасност сајбер напада током последње деценије означавају прекретницу и сама држава мора са већим фокусом да се укључи овај проблем јер дефинитивно он постаје веома важан.

Широка употреба информационих и комуникационих технологија у оквиру OT подсистема је кључни фактор за пружање одговарајућих услуга корисницима. Пружање и одрживост ових услуга за паметне мреже има висок ниво сложености који доноси повећан ризик од безбедносних претњи које је потребно правилно евидентирати и њима управљати. Ризици настају услед губитка поверљивости, интегритета или доступности информација или информационих система и представљају потенцијалне штетне утицаје на мисију, функције, имиџ или углед [4][5][8][11][15][37].

Према NIST-у, ризик се може сматрати било којим неизвесним догађајем који може имати штетни утицај [37][38]. Дефиниција ризика може се прецизирати у зависности од домена у којем се анализира. У домену индустријских контролних система ризик се дефинише као "вероватноћа да ће одређена претња искористити одређену рањивост система" [39].

Анализа ризика [38][39] је једна од најкритичнијих компоненти оквира за управљање ризицима коју треба спровести да би се идентификовале, анализирале и процениле потенцијалне претње и рањивости у паметним мрежама које могу имати негативан утицај на њене оперативне перформансе. Овај поступак [37] треба изводити методолошки и то континуирано, а не једнократно. Даље, у зависности од временског оквира, сложености

методологије и критичности података, треба размотрити појединачни или вишеструки приступ процени ризика [39].

Један најзначајнијих стандарда за процену ризика, NIST [38], наводи да је анализа ризика веома важан корак и да се у оквиру ње сагледавају потенцијални негативни утицаји на организационо пословање и имовину, појединце, друге организације и економске и националне безбедносне интересе који проистичу из рада и употребе информационих система и информација које они обрађују, чувају и преносе.

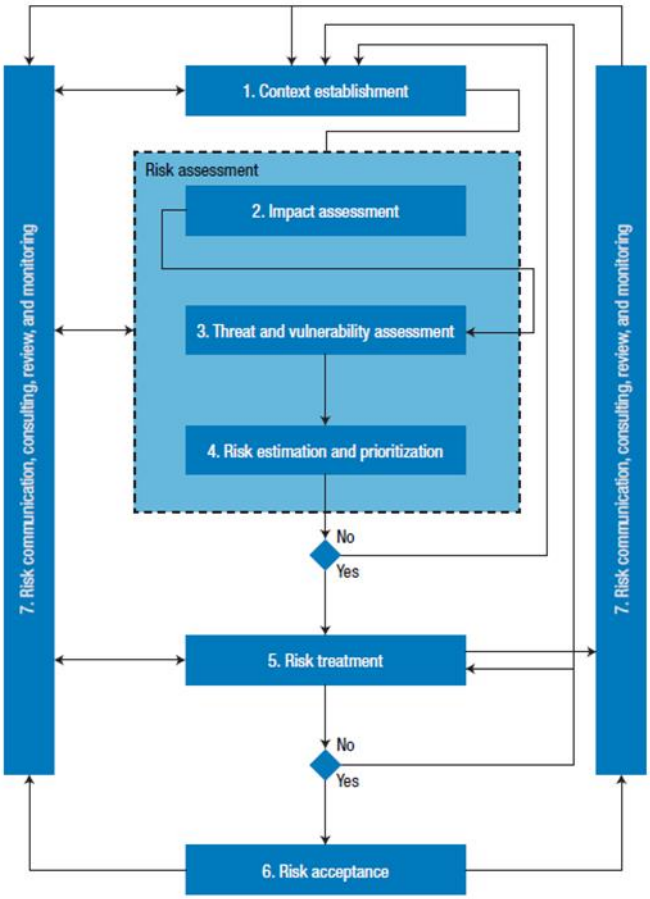
Европска агенција за сајбер безбедност (енг. *European Union Agency for Cybersecurity*) ENISA, слично као и NIST дефинише анализу ризика. Према њој [29] анализа ризика је процес идентификовања, квантификације и управљања ризицима са којима се организација суочава; то је процес који има за циљ постизање ефикасне равнотеже између остваривања могућности за добитке и минимизирања рањивости и губитака. Као саставни део праксе управљања и суштински елемент доброг управљања, управљање ризиком треба да буде периодично, а не једнократно. ENISA доприноси анализи ризицима тако што прикупља, анализира и класификује информације у области нових и тренутних ризика и окружења претњи које се развија.

Анлиза ризика је процес који је и раније имао велику улогу, али све више добија на знчају када причамо о сајбер простору. Све релевантне стране слично приступају овој анализи, па се ни приступ NERC CIP [33] не разликује у односу на већ споменуте NIST и ENISA-у.

Са обзиром на значај и потребу да се се у оквиру паметних мрежа ризик адекватно процени и адресира креиране су различите методологије. Једна од њих је (енг. *SEGRID Risk Management Methodology*) SRMM методологија која побољшава постојеће методе процене ризика из 2012. године [40] на три начина [41]:

1. Проширење методом (енг. *Network Risk Management*) NRM, управљања мрежним ризиком како би укључили међузависност заинтересованих страна и ширење ризика кроз ланце заинтересованих страна.
2. Укључивање практичног приступа за процену друштвеног утицаја у случају нестанка струје изазваног сајбер нападима. Дистрибутивна предузећа морају бити у стању да анализирају ризике у томе контексту.
3. Будући да су они који желе да угрозе паметну мрежу углавном вештији од просечног нападача, *SRMM* примењује побољшану верзију (енг. *Threat Vulnerability and Risk Analysis*) TVRA методе угрожености и анализе ризика Европског института за телекомуникационе стандарде (енг. *European Telecommunications Standards Institute's*) ETSI's), која додаје процену способности и мотивације нападача у фазу процене ризика.

Поред ових побољшања, аутори методологије [41] су укључили оквир за управљање ризицима дат у (енг. *International Organization for Standardization and the International Electrotechnical Commission - ISO/IEC 27005:2011*) ISO/IEC и истичу да су повратне информације DSO-а који су учествовали у евалуацији методе биле кључне за развој ове методологије која је приказана на слици испод.

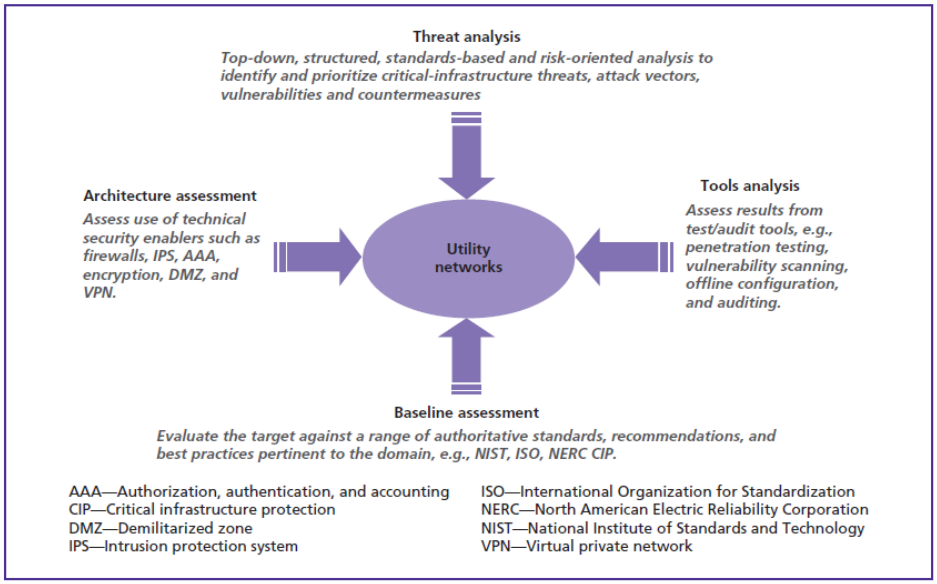


Слика 5 - SRMM методологија [41]

Методологија за процену сајбер безебдности паметних мрежа развијена од стране Белових лабараторија [42] (енг. *Security by Design - SbD*) SbD се састоји од анализе претњи, стандарда процене ризика, анализе алата и процене архитектуре паметне мреже. Аутори наводе да је сврха анализе претњи идентификација потенцијалних рањивости и идентификација потенцијалних противмера за те рањивости, те да је анализа претњи структурирана полуформална процена одозго према доле заснована на стандардима.

Активности и резултати анализе претњи укључују [42]:

1. Дефинисање пословног ризика (у смислу приоритетног низа пословних претњи).
2. Утврђивање критичне имовине производа
3. Разумевање којим претњама је изложена критична имовина
4. Препознавање потенцијалних рањивости и потврђивање познатих рањивости.
5. Приоритетизација рањивостима на основу ризика.
6. Утврђивање контрамера потребних за ублажавање рањивости.



Слика 6 - SbD методологија [42]

На основу изложености претњама, према ауторима дате методологије следећи корак је процена могућих напада на имовину у циљу реализације претње. У циљу извођења анализе ризика проценитељ мора размотрити циљ из перспективе потенцијалног нападача. Уколико је нападач мотивисан да искористи рањивост паметне мреже ризик се повећава што може бити повезано са потенцијалном наградом, геополитичком или војним значајем циља, вредности информације и интересовање шире јавности за дате информације [42]. Анализа ризика [42] се врши ради хитности примене контрамера користећи факторе као што су атрактивност циља, лакоћа напада и утицај успешног напада. Лакоћу напада аутори дефинишу као ниво уложеног труда да се циљ оствари, што повезују са постојањем готових алата, нивоом техничке стручности, као и могућношћу нападача да дође до циља са обзиром на његову потенцијалну изолованост. Утицај успешног напада према овој методологији узима у обзир трошак или износ штете која је резултат успешног напада, укључујући потенцијални утицај на приход, регулаторни утицај, утицај на репутацију код купаца, као и утицај на однос са пословним партнерима, тј. на само пословање. Следећи корак дате методологије је предлагање противмера на основу претходне анализе, али то није тема ове докторске дисертације.

FIPS 199 (енг. *Federal Information Processing Standards - FIPS 199*) [43] је успоставио три безбедносне категорије информација и информационих система, заснованих на потенцијалном утицају (енг. *Impact*) (низак, умерен и висок) на организацију уколико се реализују одређене претње. Веома важно је анализирати и вероватноћу реализације неког ризика (енг. *Likelihood*) која има велики значај приликом процене нивоа ризика.

Категорије за процену и квантификовање утицаја у оквиру паметних мрежа предложене од законодавства енергетске заједнице Европске Уније су [35]:

1. Људски утицаји (обично се мере бројевима)
2. Економски утицаји и утицаји на животну средину (обично се мере у еврима)
3. Политички/социјални утицаји

Утицаји су углавном мапирани на полуквантитативне скале које су сличне код различитих анализа [35] и које у пресеку представљају нивое:

1. Катастрофалан
2. Значајан/веома озбиљан
3. Умерен/озбиљан
4. Мањи/значајни

Према извештају [35] о сајбер безбедности у енергетском сектору Европске Уније критеријуми за оцењивање утицаја су:

1. Критеријум жртава (процењује се у смислу потенцијалног броја смртних случајева или повреда)
2. Критеријум економских ефеката (процењен у смислу значаја економских губитака укључујући потенцијалне ефекте на животну средину)
3. Критеријум јавних ефеката (процењује се у смислу утицаја на поверење јавности, физичку патњу и нарушавање свакодневног живота, укључујући губитак основних услуга).
4. Критеријум губитка имовине (процењен у смислу утицаја на употребљивост имовине и/или деградацију производа или услуге, укључујући губитак основних услуга).

Вероватноћа реализације претње процењена на основу релевантних анализа националне безбедности енергетског сектора Европске Уније у пресеку је подељена у неколико нивоа [35]:

1. Скоро сигурно - учесник је свакодневно изложен овој претњи. Уобичајене претње (нпр. злонамерни код).
2. Вероватно - учесник је изложен овој претњи неколико пута годишње. Инциденти засновани на овој претњи редовно се дешавају у земљи (нпр. на месечном нивоу).

3. Могуће - учесник је изложен овој претњи на годишњем нивоу. Инциденти засновани на овој претњи дешавају се у земљи редовно (нпр. неколико пута годишње). Овакви догађаји се дешавају у региону на месечном нивоу.
4. Ретко - Учесник је изложен овој претњи, инциденти засновани на ова претња се догодила у земљи; такви догађаји су се догодили у региону последњих година

У односу на претходну методологију процене ризика, која користи четири нивоа приликом одређивања утицаја који може да проузрокује дата претња уколико се реализује и вероватноће да ће се то десити, NIST [38][44] и ENISA [29] користе већи ниво гранулације, тј. пет нивоа:

1. Веома висок (енг. *Very High*)
2. Висок (енг. *High*)
3. Умерен (енг. *Moderate*)
4. Низак (енг. *Low*)
5. Веома низак (енг. *Very Low*)

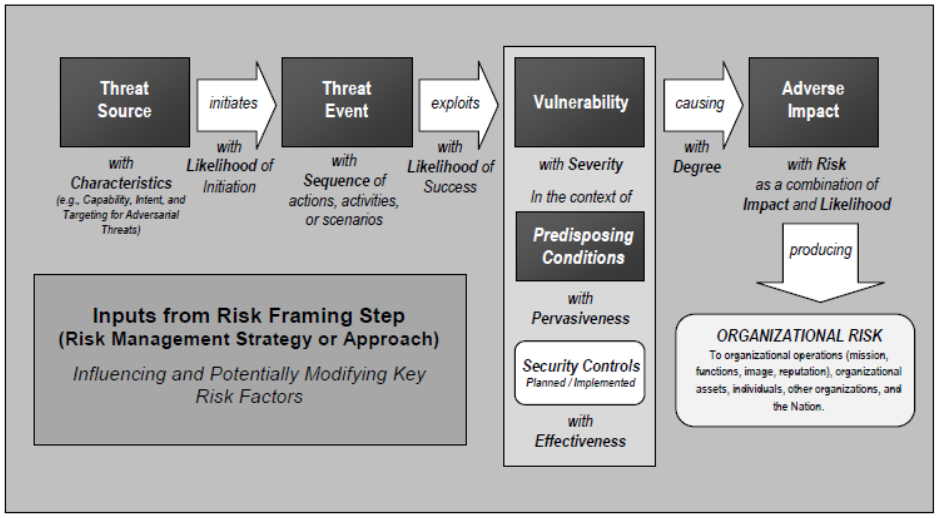
Следећи корак је да се на основу нивоа утицаја и вероватноће уз коришћење матрице ризика одреди ниво процењеног ризика. Према NIST [38], матрица ризика такође има 5 нивоа, са импактом на једној, а вероватноћом на другој оси:

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Слика 7 - Матрица ризика према NIST-у [38]

Погледом на дату матрицу, видимо да се лако на основу утицаја и вероватноће долази до процењеног ризика. Нпр. за веома висок утицај и умерену вероватноћу ризик је процењен високим нивоом.

Вероватноћа да ће претња користећи рањивост да нанесе штету ствара ризик. Према NIST-у генерички модел ризика је приказан на слици испод.



Слика 8 - Генерички модел процене ризика [38]

Приликом процене ризика велику пажњу је потребно усмерити на особље ОТ подсистема и њихову обученост. Лажно представљање у форми *phishing*-а чини 91% успешних вектора напада на ОТ подсистеме [45]. На основу овога је јасно да су људи често најслабија карика у адекватној заштити од потенцијалних сајбер напада [46]. У раду [47] аутори тврде да су претње и познате рањивости подложне променама, па је важно да се процене ризика често преиспитају и ажурирају. Метод описан у [47] има за циљ да упозори особље које води бригу о безбедности у системима базираним на (енг. *Industrial Internet of Things*) IIoT на значајне промене процењене изложености ризику како би се олакшале рационалне и благовремене одлуке.

Аутори [48] представљају више метода процене ризика чији је циљ да приликом развоја помогну инжењерима да имплементирају безбедан систем. Њихова методологија је уско везана за (енг. *Advanced Metering Infrastructure*) AMI инфраструктуру за рад са паметним бројилима. Поред помоћи инжењерима безбедности да имплементирају функционалност која омогућава достизање жељеног нивоа безбедности, аутори тврде да ова методологија може помоћи и регулаторним телима за сертификацију различитих сложених инфраструктурних система. У раду [49] се тврди да комуникација базирана на (енг. *Internet Protocol*) IP мрежама у паметним мрежама повећава вероватноћу мрежних напада, као што су лажирање (енг. *spoofing*) и DDoS напад. Аутори су представили методологију за процену безбедносних ризика унутар паметне мреже фокусирајући се на сигурносне ризике од DDoS напада на интелигентне електронске уређаје (енг. *Intelligent Electronic Device*) IED.

Као што видимо, анализа ризика је један обиман процес коме се мора приступити са великом пажњом, јер последице неадекватне анализе могу бити значајне. Анализирали смо више методологија за процену ризика и видели да све оне подсећају једна на другу, али исто тако свака има неки свој јединствен печат.

2.3 Преглед најзначајнијих стандарда у области информационе безбедности паметних електроенергетских система

Са обзиром да паметни електроенергетски системи спадају у групу критичних инфраструктурних система где је поузданост у сваком смислу веома важна, где се важни подаци размењују без преседана, морају да се стандардизују комуникациони протоколи, софтверске и хардверске компоненте како би се осигурала ефикасност, поузданост и продуктивност датих система.

У овом моменту нама су од интереса стандарди у области информационе безбедности ових система. Безбедносни захтеви информационих система и података у паметној мрежи, њихова приоритетизација, као и категоризација ризика у зависности од природе информационих система су дефинисани одговарајућим техничким стандардима.

Најзначајнији стандарди који покривају техничке аспекте сајбер безбедности ИТ и ОТ подсистема паметних електроенергетских мрежа су [14][33]:

1. (енг. *National Institute of Standards and Technology Interagency Report*) NIST IR 7628, NERC CIP,
2. (енг. *European Union Agency for Cybersecurity*) ENISA,
3. (енг. *Centre for the Protection of National Infrastructure*) CPNI,
4. (енг. *Industrial Automation&Control Sys Security*) ISA99,
5. (енг. *International Organization for Standards*) ISO27K,
6. IEC 62351-3,
7. IEC 62443,

8. IEC 62443,
9. IEC 62351,
10. IEEE P1686,
11. ISO/IEC 27000.

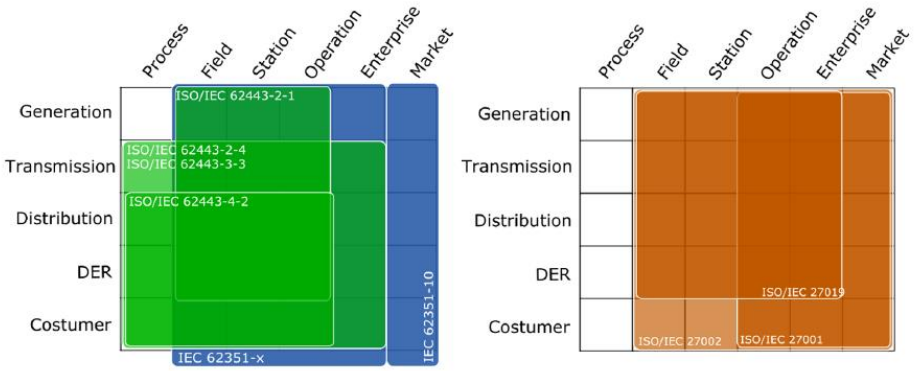
Паметни електроенергетски системи се са аспекта сајбер безбедности дизајнирају на основу IEC 62443 стандарда. IEC 62443 3-3 се односи на безбедност у оквиру самог система, док је IEC 62443 2-4 усмерен на интеграцију са другим системима.

Користећи овај стандард утврђују се захтеви за:

1. дефинисање система који се разматра
2. подела система на зоне и комуникационе канале
3. процена ризика за сваку зону и комуникациони канал
4. успостављање циљног нивоа безбедности за сваку зону и комуникациони канал
5. документовање безбедносних захтева

Спроведено је истраживање [50][51] због идентификовања свих стандарда који дефинишу карактеристике, особине или функције које морају бити присутне у паметном ЕЕС како би се осигурала његова сајбер безбедност.

Поред претходне, анализа стандарда у оквиру паметних електроенергетских система, приказана на *Слика 7*, је урађена је од стране Европског комитета за стандардизацију (енг. *European Committee for Standardization)* CEN, (енг. *European Committee for Electrotechnical Standardization)* CENELEC и *(*енг. *European Telecommunications Standards Institute*) ETSI [52].



Слика 9 - Анализа стандарда за паметни ЕЕС урађена од стране CEN-CENELEC-ETSI [52]

2.4 Сајбер безбедност у рачунарском облаку

Потенцијални безбедносни ризици који су саставни део паметних мрежа добијају једну нову димензију ако се у причу уведе тренутно једна од најизазовнијих области у

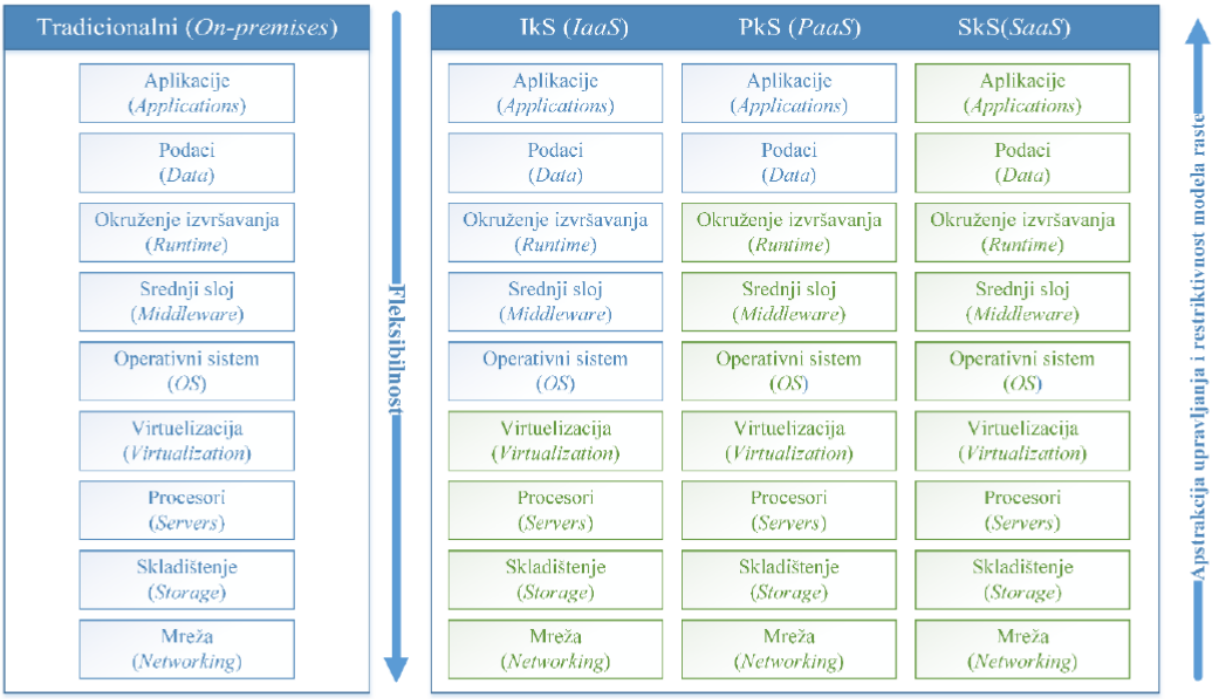
рачунарском свету, а то је рачунарство у облаку. Баланс искористивости могућности које нуди овај вид рачунарства и очувања сајбер безбедности је велики изазов. Рачунарство у облаку представља испоручивање рачунарских ресурса (процесорске моћи, меморије, простора за складиштење итд.) путем Интернета [53][54][55]. Његов основни циљ је да понуђачи своје апликације сместе у "облак", где би користиле хардверску подршку и остале ресурсе самих провајдера. Употреба тих ресурса се наплаћује на основу мерења потрошње, нпр. колико времена је коришћена одређена конфигурација процесора или простора за складиштење. Овај принцип наплате услуга је сличан начину на који се данас плаћају струја, вода, телефон и многе друге услуге. Оно чему се тежи као крајњем циљу је да се корисници претплате код власника апликација, тј. да трећем лицу дају на одржавање и надоградњу хардвера, како би добили окружење у коме би се дата апликација извршавала, а да при томе не брину о проблемима који се могу десити на хардверу, оперативном систему итд.

NIST [53] је дефинисао пет основних карактеристика које разликују рачунарски облак од осталих технологије: самопослуживање на захтев, широк приступ мрежи, удруживање ресурса, брза еластичност и мерење услуга.

Рачунарски облак се намеће као одлично решење за паметне електроенергетске системе [3] са обзиром на његову флексибилност и скалабилне карактеристике што у многоме помаже током складиштења и преноса велике количине података, захтевних рачунарских операција и на крају уштеде енергије, новца и радне снаге. Оператор у рачунарском облаку одговоран за контролу и управљање његове инфраструктуре. Одговорност варира у односу на то да ли облак пружа услуге:

1. инфраструктуре (енг. *Infrastructure as a Service***)** IaaS
2. платформе (енг. *Platform as a Service***)** PaaS
3. софтвера (енг. *Software as a Service*) SaaS

PaaS пружа рачунарску платформу за развој апликација на којој корисник може да развије, тестира и примени апликацију помоћу провајдера рачунарског облака (енг. *Cloud Service Provider*) CSP. У IaaS, CSP пружа инфраструктуру у облику сервера, складиштених и рачунарских ресурса за потрошаче. Предност овога је што корисник не мора инвестирати у скупу ИТ инфраструктуру, сервиси су скалабилни и користе се на захтев, и што је веома важно корисник плаћа само оне ресурсе које потроши. У SaaS-у, CSP пружа апликације преко Интернета за употребу од стране купца. У суштини то су апликације за које је кориснику довољан приступ интернету. [53][54][55][56]



Слика 10 - Услуге рачунарства у облаку [57]

Национални институт за стандарде и технологију [51][58][59] дефинише четири модела испоруке облака: јавни облаци (енг. *public cloud*) доступни јавности, приватни облаци (енг. *private cloud*) искључиво за једну организацију, облаци које дели специфична заједница (енг. *community cloud*), као и хибридни облаци (енг. *hybrid cloud*) који су композиција два или више од горе наведена три модела.

Сва четири типа рачунарског облака имају своје специфичности по чему се издвајају у односу на друге типове. Према ауторима [54]:

1. најсигурнији тип рачунарског облака је приватни и његове главне карактеристике су приватност, сајбер безбедност и контрола. Међутим једна од главних мана је скалабилност.
2. Јавни облаци нису изоловани као приватни, одликују се великом скалабилношћу, перформансама, али као две главне мане наводе се њихова неадекватна сајбер безбедност због тога што ресурсе дијеле са другим корисницима и немогућност кастомизације која директно произилази из претходне чињенице.
3. Облак заједнице користе специфичне групе, као нпр. факултети на једном универзитету, и њихова платформа за учење и истраживање.

Аутори [60] тврде да ће за скоро свако дистрибутивно предузеће крајњи резултат коришћења рачунарског облака бити јединствена комбинација физичких сервера, приватног и јавног облака, тј. хибридно окружење дизајнирано да се мења како се захтеви за ресурсима буду мењали.

Гартнеров циклус промоције (енгл. *Gartner Hype Cycle*) [57] пружа графичку анализу зрелости и усвајања промовисаних нових технологија за одређени временски период који

обично обухвата пар година пре и до десет година након датума када се извештај објављује. У августу 2009. године, према Гартнеру, може се рећи да је рачунарски облак био на врхунцу ишчекиваних технологија [57]. У 2012. години је објављен последњи Гартнеров циклус што се тиче промоције рачунарског облака. Другим речима, може се сматрати да је основна понуда рачунарског облака ушла у фазу пуне продуктивности око 2012. године – јасна временска граница наравно не постоји [57]. Од тада, бележен је глобални раст у погледу захтева за овим технологијама што подиже важност развоју апликација које користе платформу рачунарског облака. [57]

Истраживања [61] тврде да ће организације агресивно инвестирати у стратегије и архитектуре засноване на рачунарском облаку. Препорука је да се што пре крене у израду стратегије његовог усвајања, јер је трансформација тешка и захтева време, али и због чињенице да ће 2022. године, 24% целокупног ИТ маркета бити рачунарски облак [57][61]. Такође, процењује се да ће се годишња стопа раста конзумирања ових сервиса у наредним годинама задржати на око 22% [61][62]. Из разлога све већег прихватања, компаније морају бити спремне на притисак тржишта и да се суоче са решењима заснованим на рачунарском облаку и пословним моделима.

Према [62] структурне карактеристике рачунарског окружења у облаку су главни узроци безбедносних проблема јер је због разноликости технологија тешко контролисати овакво окружење. Поред тога провајдер рачунарског облака има ризик од откривања приватности у процесу преноса, обраде и складиште. Један од главних изазова у ширем усвајању било ког модела испоруке рачунарства у облаку је информациона безбедност. Овај изазов је додатно у фокусу када се ради о националној сигурности где је критичност доступности услуга повећана [62]. У задње време је све актуелнија тема заштите приватних података, тако да не чуди велики број радова на ту тему [63][64][65][66] где аутори скрећу пажњу на значај заштите ових података у рачунарском облаку, анализирају безбедносне ризике и предлажу различита решења заштите приватности. Сајбер безбедност у рачунарском облаку је важна тема која је заступљена у међународним законима о приватности као што је европски (енг. *General Data Protection Regulation*) GDPR [66]

Забринути због честог нарушавања тајности података, заједно са недавно надограђеним законским захтевима, попут опште уредбе о заштити података Европске уније, аутори [66] саветују да се незаштићени осетљиви подаци не би требали чувати у јавним облацима.

Од компанија се тражи да осигурају своје системе и податке на одговарајућем нивоу. То доводи до различитих безбедносних мера и безбедносних решења у различитим компанијама и индустријама. Аутори [67] тврде да сајбер безбедност представља велику препреку у усвајању рачунарског облака. Они су се бавили сигурносним проблемима у рачунарском облаку и показали како да се ти проблеми могу решити користећи квантитативни модел процене безбедносног ризика (енг. *Multidimensional Mean Failure Cost*) MMFC. Аутори [68][69][70] извештавају о детаљној анализи и категоризацији различитих безбедносних претњи у рачунарском облаку. Безбедносна алијанса је представила 12 највећих претњи у облаку које уколико се реализују могу да анулирају све предности остварене преласком на ову технологију [71]. Истраживање спроведено анкетирањем менаџера из ове области показало је да су економичност и сигурност података два главна аспекта приликом усвајања рачунарског облака [72]. Према[73] најважнији изазови које треба решити пре него што организације и појединци добију

поверење да своје апликације мигрирају у облак су безбедност, приватност, ефикасност напајања, усаглашеност и интегритет.

У случају напада на рачунарски облак [74] лакше је поново осигурати доступност и перформансе услуга у облаку него да се поново осигура доступност података са потпуним интегритетом и поверљивости. Аутори [74][75] такође тврде да су провајдери рачунарског облака одговорни за осигуравање доступности услуга у облаку. Међутим, према њима осигуравање сајбер безбедности у облаку је како на провајдерима, тако и на клијентима у зависности од врсте услуге.

Недавно су урађена истраживања [74][75] како би се идентификовали и класификовали проблеми у облаку везани за сигуност и приватност. Безбедносна питања су подељена у пет категорија: безбедносни стандарди, мрежа, контрола приступа, инфраструктура и подаци.

Аутори [74] представљају модел безбедности и приватности у рачунарском облаку (енг. *Cloud Security and Privacy Model*) CSPM. Он је слојевит модел који је подељен у пет безбедосних слојева и то:

1. Физички слој безбедности - процеси и политике које су усвојили провајдери рачунарског облака да би заштитили своје објекте од неовлашћеног физичког приступа, оштећења итд. [76][77]
2. Безбедност инфраструктуре рачунарског облака - Укључује сигурносна питања специфична за инфраструктуру облака (IaaS, PaaS и SaaS). [75][77]
3. Безбедност мреже - односи се на медијуме путем којих се корисници повезују са услугама, прегледаче, мрежне везе итд. [75][77]
4. Безбедност података - поверљивост, интегритет, приватност и губитак података.
   4.1.1. Повезаност података: осигурава да подаци остану поверљиви и невидљиви чак и за провајдера рачунарског облака, па чак и ако је нападнут центар података добављача, подаци о купцима не могу се украсти нити поново користити. [76][78]
   4.1.2. Интегритет података: Одржавање података у исправном облику. То значи да систем мора спречити непримерене модификације информација. [76][77][78]
   4.1.3. Приватност података и губитак података: провајдери рачунарског облака су наметнули ограничења у раду са подацима. Сви покушаји злоупотребе се брзо откривају и пријављују. [76][77]
5. Ниво контроле и управљање привилегијама - Политике и процес који осигуравају да потрошачи добију одговарајуће привилегије да могу да користе или мењају податке. Укључује идентификацију, питања аутентификације и ауторизације. [75][76][77]

Предности CSPM -а су [74]:

1. Може помоћи да се идентификују и класификују различита питања сајбер безбедности и приватности у облаку.
2. Може да помогне за идентификацију и дефинисање разлика између различитих извора претњи у облаку.

3. Може да помогне приликом усвајања противмера (систем за откривање упада или/и спречавање упада у систем) неопходних за сваки слој, како би се осигурали доступност и сајбер безбедносне услуге рачунарског облака.
4. Може да олакша надзор безбедности услуга у рачунарском облаку.

2.5 Анализа ризика у рачунарском облаку

Процену ризика NIST [38] дефинише као процес идентификовања, процене и приоритетизације ризика што захтева пажљиву анализу претњи како би се утврдило у којој мери околности или догађаји могу негативно утицати на организацију и која је вероватноћа да ће се такве околности или догађаји реализовати. Након процене ризика следећи корак је ублажавање или уклањање ризика кроз имплементацију различитих контрола. Безбедносни проблеми су свакако веома важан фактор за усвајање било које технологије, па тако и рачунарства у облаку. Анализа ризика у рачунарском облаку је веома важна основа за истраживање његове безбедности.

Аутори [78] наводе да постоји неколико метода процене ризика [79][80] које су нам доступне у ИТ свету, али да су оне опште и нису уско везане за рачунарство у облаку. Рачунарство у облаку је једна сложена рачунарска платформа и то аутори наводе као главни разлог због чега ове методе не могу ефиаксно да покрију ту област. Они представљају квантитативну методологију [78] за процену ризика која је испод детаљније објашњена.

Табела 2 - Пример квантитативне процене ризика [78]

Претња	Утицај	Учесталост појављивања претње	Ниво откривања ризика	Приоритетни број ризика
Капацитет ресурса	10	6	6	360
Недоступност меморије	9	3	8	216
Флуктуација у времену преноса података	8	8	9	576

Прва колона садржи потенцијалну претњу или догађај који може довести до компромитовања одређеног дела система. У наредне три колоне су приказани утицај, учесталост појављивања претње/догађаја и ниво откривања ризика, чије вредности су аутори одредили да буду у распону од 1-10.

Производ од ове три категорије је приоритетни број ризика (енг. *Risk Priority Number*) RPN што је забележено у петој колони.

$$RPN = I \times O \times D$$

RPN узима вредност у опсегу 1 - 1000. Вредност RPN-а одређује озбиљност ризика, и то тако што је већа вредност RPN-а значај ризика је већи.

Референтна архитектура NIST [53] рачунарства у облаку класификује политике безбедности и приватности под одговорност провајдера рачунарског облака и контроле безбедности су исте за све моделе испоруке.

Упркос главним предностима рачунарства у облаку, постоје бројне бриге [81] о безбедности које обухвата многе технологије, укључујући мреже, базе података, оперативне системе и виртуелизацију. Према [81], више од 70% (енг. *Chief Technology Officers*) CTO показали су своју забринутост због сигурносних проблема у рачунарству у облаку. На основу анкете [82] коју је спровео водећи SaaS провајдер, RightScale, један од главних изазова у усвајању рачунарства у облаку је сајбер безбедност.

Аутори [81] представљају референтни модел за безбедносне захтеве и разматрање у рачунарству у облаку. Циљ предложеног модела је обезбеђивање различитих сигурносних слојева слојева три главне услуге у облаку (SaaS, IaaS и PaaS) са становишта клијената и провајдера.

Исцрпан извештај који описује безбедносне ризике у рачунарском облаку је објавила ENISA [83][84], на основу кога су ризици груписани у три важне групе.

1. Политички и организациони ризици
2. Технички ризици
3. Правни ризици

Према њима ниво ризика се процјењује на основу вероватноће да дође до инцидента, мапирано у односу на процењени негативан утицај. У многим случајевима процена вероватноће у великој мери зависи од модела облака или архитектуре. Резултујући ризик се мери на скали од 0-8, па тако имамо да је:

1. Низак ризик: 0-2
2. Средњи ризик: 3-5
3. Висок ризик: 6-8

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Слика 11 - ENISA матрица ризика [83]

За анализу ризика у рачунарском облаку могуће је искористити и методологије приказане у поглављу *2.2*.

Десет највећих ризика у рачунарском облаку према (енг. *Open Web Application Security Project*) OWASP [81][85] су:

1. Одговорност и власништво над подацима
2. Федерација идентитета корисника
3. Усклађеност са прописима
4. Континуитет и еластичност пословања
5. Приватност корисника и секундарна употреба података
6. Услуга и интеграција података
7. Физичка сигурност
8. Анализа инцидента и форензичка подршка
9. Безбедност инфраструктуре
10. Изложеност непроизводном окружењу

Једну иницијативу у процени безбедносних ризика предузима (енг. *Cloud Security Aliance*) CSA. CSA предводи низ текућих истраживачких иницијатива кроз које пружа техничке књиге, алате и извештаје који помажу компанијама и провајдерима да осигурају услуге рачунарства у облаку. Објављене су и смернице о различитим безбедносним питањима везаним за рачунарство у облаку. Међу CSA препорукама, велики акценат је стављен на дефинисање метрике и стандарда за мерење перформанси информационе безбедности, које треба проценити и документовати уговорима. Поред тога, CSA нуди пакет управљања, ризика и усклађености [30] као сет алата за процену приватних и јавних облака према најбољим праксама које је утврдила индустрија.

Недавно је спроведено неколико студија за побољшање традиционалних техника процене безбедности и представљање нових парадигми за анализу и процену безбедносних ризика у окружењу облака. Методе процене ризика засноване на облаку класификоване су у пет категорија ризика, као што је приказано на слици испод [86].

Табела 3 - Класификација методологија за процену ризика у рачунарском облаку [86]

Methods	Risk Modeling	Stakeholders
Assessment As a Services	Cloud service model	Cloud customer
Qualitative/Quantitative Analysis	Textual language model	Cloud provider
	Threat and vulnerability analysis	Cloud customer and provider
Graph Analsis	Attack Defence Trees (ADT)	Cloud provider
	Decision Tree Analysis (DTA)	Cloud customer

	Graph mathematical model	Cloud provider
Hierarchical Assessment	Risk Breakdown Structure (RBS)	Cloud customer
	Analytic Hierarchy Process (AHP)	Cloud customer and provider
	Hierarchical assessment Indicator system	Cloud customer
Security Matrix	Trust Matrix	Cloud customer
	Cloud Control Matrix (CCM)	Cloud customer and provider
	Trust and Assurance Registry (STAR)	Cloud customer

Моделирање претњи је такође важан корак у процени ризика и омогућава нам да идентификујемо и оценимо претње повезане са системом. Може се имплементирати користећи један од следећа три приступа: усмерено на имовину (енг. *asset-centric*), усмерено на софтвер (енг. *software-centric*) и усмерено на нападача (енг. *attacker-centric*).

2.6 Преглед најзначајнијих стандарда у области информационе безбедности рачунарског облака

Безбедносни захтеви информационих система и података у рачунарском облаку, њихова приоритетизација, као и категоризација ризика у зависности од природе информационих система морају бити дефинисани одговарајућим техничким стандардима.

Иако су решења заснована на облаку атрактивна због своје брзе уштеде трошкова и других предности, приватност и сајбер безбедност у облаку и даље забрињавају већину потрошача и представљају кључну препрека у усвајању рачунарског облака [87]. Последњих година безбедносне стандарде развијају тела за стандардизацију попут CSA [87], међународне организација за стандарде ISO [87], национални институт за стандарде и технологију NIST [87][88], итд.

Security Category	Standard	Standard Developer Organization
Authentication and Authorization	RFC 3820: X.509	IETF
	ISO/IEC 9594-8	ISO/IEC
	FIPS 181	NIST
	ISO/IEC 29115	ISO/IEC
	RFC 5849	IETF
Confidentiality	RFC 5246	IETF
	FIPS 140-2	NIST
	FIPS 188	NIST
	XML Encryption	W3C
Integrity	XMLDSig	W3C
	FIPS 180-4	NIST
	FIPS 186-4	NIST
	FIPS 198-1	NIST
Identity Management	X.idmcc	ITU-T
	FIPS 201-1	NIST
	SAML	OASIS
	SPML	OASIS
Security Monitoring and Incident Response	ISO/IEC 18180	ISO/IEC
	X.1500	ITU-T
	X.1520	ITU-T
	X.1521	ITU-T
Security Controls	CCM V 3.1	CSA
	ISO/IEC 27001	ISO/IEC
Security Policy Management	FIPS 199	NIST
	FIPS 200	NIST
	ISO/IEC 27002	ISO/IEC
Availability	ATIS-02000009	ATIS
	ISO/PAS 22399	ISO

Слика 12 - Стандарди за сајбер безбедност у рачунарском облаку [81]

Аутори [89] наводе да све већи акценат на сајбер безбедност у рачунарском облаку приморава владе држава и све заинтересоване стране да се фокусирају на ову тему. Према њима увођење нових стандарда као што су (енг. *Federal Risk and Authorization Management Program*) FedRAM који је основала Америчка влада за процену ризика, ауторизацију и константанто надгледање, као и (енг. *Cloud Computing Compliance Criteria Catalogue*) C5 који је развила савезна канцеларија за безбедност у Њемачој и који има за циљ подизање нивоа заштите и претњи јединствених за рачунарски облак не доносе радикалну промену на пољу сертификата, већ напротив да се и даље више верује старијим, консолидованим стандардима као што је ISO/IEC 27001.

У овој докторској дисертацији смо фокусирани на однос ОТ подистема паметних електроенергетских система и рачунарства у облаку. Као што смо рекли, тежимо датој интеграцији због многих бенефита које нам пружа рачунарство у облаку, а о којима смо већ писали у претходним поглављима. Према ауторима [90] повезивање индустријских контролних система са рачунарством у облаку угрожава тајност, интегритет и доступност и због тога су ове сигурносне бриге веома важне. У ту сврху су предложени [90] различити сигурносни стандарди у контексту критичних инфраструктурних система повезаних са рачунарством у облаку, а то су ISA-62443-1-1, IEC-62443-3-3 и IEC-62443-2-4 на које је потребно обратити пажњу. Више о овим стандардима је презентовано у поглављу *2.3*.

2.7 Анализа постојећих методологија за процену безбедносних ризика примене рачунарства у облаку у контексту паметних електроенергетским система

Као што смо видели у претходној анализи актуелног стања у области, постоје различите методологије за процену ризика у оквиру паметних електроенергетских система, као и у рачунарству у облаку. Међутим, иста та анализа је показала да је дефицитарно истраживање на тему процене безбедносног ризика примене рачунарства у облаку у контексту паметних електроенергетских система. У наставку смо елаборирали радове које смо издвојили као значајне и који су на путањи која нам је од интереса.

Аутори [91][92][93][94] који су радили на миграцији SCADA подсистема у рачунарски облак тврде да је управљање сигурносним ризиком циклични процес који обухвата неколико фаза и који не одступа од стандардне процене ризика:

1. анализа ризика кроз идентификацију рањивости и претњи
2. процена ризика
3. доношење одлука о прихватљивом нивоу ризика
4. избор и примена мера за ублажавање ризика

Њихов став је да су потребни напори да би се решило питање процене ризика миграције паметних мрежа у рачунарски облак, као и да се нађе компромис између укупних трошкова и ризика приликом дате миграције. Према њима, процена ризика је најважнија фаза у процесу управљања ризиком, али је и подложна грешкама.

У нашој методологији, нећемо се директно бавити трошковима, али ипак на неки начин ћемо их разматрати. Методологија која се развија у оквиру ове докторске дисертације ће бити заснована на компромису потребе за рачунарским ресурсима и потенцијалног ризика сваке од компоненти DSO-а, што на неки начин утиче и на саме трошкове јер за веће ресурсе потребан је и адкеватан буџет .

Миграција SCADA подсистема у рачунарски облак није непознаница јер овакви подсистеми су критични за индустријске процесе и захтевају високо поуздан хардвер. Прилагођавање новим технологијама као што је рачунарство у облаку представља велики изазов за индустријске контролне системе. Аутори [95] су анализирали миграцију на *IaaS* платформу са аспекта цене, перформанси и свих предности које доноси рачунарски облак и закључили да ова миграција представља изазов али и да свакако доноси велике бенефите у смислу трошкова, поузданости и перформанси. Аутори нису обухватили аспект сајбер безбедности што је област интересовања ове докторске дисертације, али свакако својим резултатима су показали да се крећемо у добром смеру.

У раду [4] аутори предлажу софтверски усмерену стратегију миграције паметне мреже на облак базирану на Мајкрософтовој (енг. *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege*) STRIDE методологији.

У радовима [73][96] процењују се различити технички аспекти миграције паметне мреже у рачунарски облак. Већина студија о паметним мрежама у домену рачунарства у облаку заснива се на анализи перформанси и/или трошкова. Рачунарски облак може значајно побољшати оперативне перформансе електроенергетских система [97]. У [98] се приказује методологија за распоређивање монолитног напредног система за управљање

дистрибуцијом у облаку без утицаја на његове оперативне перформансе. Аутори [99] су развили платформу за трансформацију софтверских решења паметних електроенергетских мрежа на рачунарски облак, али њихово истраживање, као и претходно не пружа анализу са аспекта безбедности. О предностима које нуди рачунарски облак али без осврtања на безбедност аутори [99] предстаљају ову платофрму као одлично решење за паметне еектроенергетске мреже у смислу скалабилности и високих перформанси. Према [99] миграција оваквог система са критичном мисијом, треба да уважи и додатне захтеве за отпорношћу на отказе као и потенцијалне регулаторне захтеве. Због тога, резултујући процес миграције има следећа четири главна циља:

1. Минимизација броја физичких рачунара,
2. Обезбеђивање отпорности у случају отказа поједине рачунарске компоненте,
3. Минимизација капацитета резервисане физичке меморије и броја процесорских језгара,
4. Уважавање захтева за физичком сегрегацијом система, смањење површине напада и омогућење уважавање стандарда из области безбедности и поузданости

Постоје различити приступи [100] у којима аутори анализирају и дефинишу миграционе процесе или препоручују водиче за прелазак на рачунарство у облаку.

Референца [101] дефинише скуп тачака које треба размотрити приликом доношења одлуке о миграцији паметних мрежа у рачунарски облак, а то су:

1. Потражите одговарајућег провајдера са адекватним референцама
2. Да ли пројекат заиста треба мигрирати
3. Размотрити сигурност података
4. Анализирати начин преноса података
5. Складиштење података и локација
6. Скалирање
7. Гаранције
8. Надоградње и одржавање
9. Архитектура софтвера
10. Консултовати адекватна правна лица

У раду [102] описан је виртуализовани SCADA систем развијен у рачунарском облаку. Имплементација платформе за симулацију рада паметне мреже у рачунарском облаку, укључујући анализу и оптимизацију трошкова развијена је у [103]. Облачни орјентисан систем за аналитику заснована на подацима који служе за динамичку оптимизацију потрошње енергије је описан у раду [104], док је систем за контролу уређаја паметне мреже заснован на рачунарском облаку представљен у [105]. Према [99], дати радови нуде идејни опис система апликације за рад у реалном времену, али су приказани само симулациони или експериментални системи са малом количином података који се обрађују.

Према [57], најискуснији и најзрелији на овом подручију је Амазон, који је први објавио своју методологију за усвајање рачунарског обалка (енг. *Cloud Adoption Framework*) [106]. Такође, *Microsoft* је објавио књигу која је практично методологија за трансформацију [107].

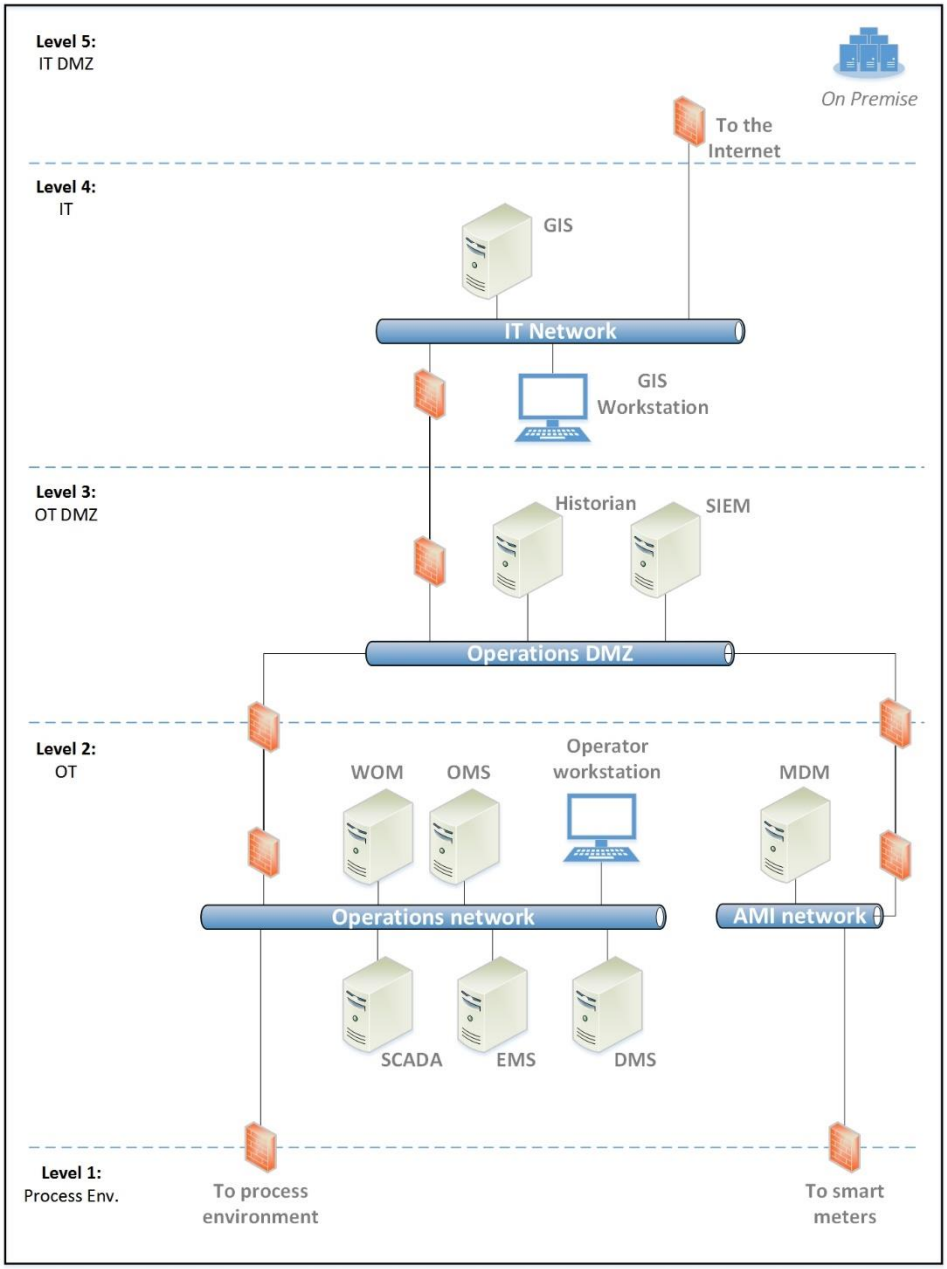
Миграција на рачунарски облак не зависи само од технолошких карактеристика већ и од спремности организације која развија софтвер и пословног модела [57][108][109][110][111][112][113][114][115].

На основу анализе радова можемо закључити да је троструки пресек: рачунарски облак, паметни електроенергетски системи и информациона безбедност само делимично истражен и да не постоје студије засноване на процени ризика које би се систематично бавиле проблемом примене рачунарства у облаку као подршке ОТ услугама паметних ЕЕС-а. То је простор смо почели да испуњавамо кроз публикације [4][5] кроз које смо приказали елементе нове методологије коју може користити било који власник/оператор паметне мреже који треба да осмисли оптималну стратегију примене рачунарства у облаку у контексту индустријских контролних система. Наша препорука је да се као основа за креирање сваке нове методологије користе анализе ризика приказане у поглављу *2.2*.

3. ПРОТОТИП АРХИТЕКТУРЕ ОТ ПОДСИСТЕМА

Архитектура паметне мреже се састоји од подсистема: информационе технологије (ИТ) и операционе технологије (ОТ); са задатком да се баве пословима и операцијама у реалном времену. Основна разлика између ова два подсистема се огледа у томе што ИТ управља подацима у оквиру пословног домена (комерцијално доношење одлука, планирање, управљање пословним процесима и доделу ресурса) док ОТ представља подсистем у оквиру кога се врши управљање физичким процесима и машинама које се користе за њихово извршавање. Иако су ови подсистеми традиционално радили као засебни ентитети, најновији трендови показују да се зближавају [4][5][8]. Ова ИТ-ОТ интеграција сматра се виталним кораком према успешној паметној мрежи.

Ако неко намерава да пресели ОТ или пратеће услуге у рачунарски облак, први корак је идентификација свих релевантних сервиса. Да би се позабавили овим проблемом, развили смо поједностављену архитектуру ОТ управљачког подсистема приказану на *Слика 13*. Формирана је на основу искуства аутора стеченог на више међународних пројеката, као и на основу релевантних научних радова и стручне литература [4][5][28][116][117], а у складу са IEC-62443 моделом сигурносних зона [118].



Слика 13 - Архитектура великог DSO подсистема

У складу са IEC-62443 моделом, архитектура паметног електроенергетског система је подељена у следећих пет нивоа:

1. Ниво 1: Процесно окружење (енг. *Process Environment*) - садржи процесни подсистем, нпр. трансформаторске станице, удаљене терминалне јединице (енг. *Remote Terminal Units*) RTU, итд. Детаљан приказ овог нивоа није представљен на *Слика 13* због тога што његову миграцију у рачунарски облак нећемо разматрати. Више информација о овој одлуци биће у наставку поглавља.
2. Ниво 2: OT подсистем - састоји се од компоненти које власницима/ операторима система омогућавају даљинско праћење и контролу паметне мреже из контролног центра. Подскуп таквих компоненти представља: SCADA, (енг. *Energy/Distribution Management System*) EMS/DMS, (енг. *Switching Sequence*

Management) SSM, (енг. *Outage Management System*) OMS и (енг. *Meter Data Management*) MDM. MDM своју комуникациону инфраструктуру обично не дели са SCADA-ом.

3. Ниво 3: OT (енг. *Demilitarized Zone*) DMZ – је главна веза између OT и ИТ домена, омогућава проток података на строго контролисан начин између ове две зоне. У нашој, поједностављеној архитектури система паметних мрежа садржи (само) компоненту за рад са историјским подацима (енг. *Historical*) и (енг. *Security Information and Event Management*) SIEM компоненту. SIEM је позиционирана овде, између 2. и 4. нивоа, како би била свесна оба нивоа и имала могућност прикупљања податка са обе стране.
4. Ниво 4: IT подсистем - Већина ИТ услуга се налази у овом окружењу. У овој дисертацији ће бити разматран само (енг. *Geographic Information System*) GIS, јер је он често главни извор мрежног модела, тј. информације о мрежи се из GIS -а импортују у различите OT услуге, нпр. SCADA, EMS, DMS, OMS, чије се деловање ослања на приступ ажурном мрежном моделу електроенергетског система.
5. Ниво 5: IT DMZ - обично садржи услуге доступне са Интернета и/или међусобно повезане информационе системе које одржавају други актери паметне мреже, нпр. суседни системи за производњу, пренос или дистрибуцију.

У овој докторској дисертацији биће заузет мало футуристички приступ и размотриће се ИТ подсистем (тј. нивои 4 и 5) као да је већ пресељен у рачунарски облак при чему је GIS једини запажен изузетак, јер је то обично извор мрежног модела. Анализа ће се фокусирати на OT и OT DMZ подсистеме (тј. нивое 2 и 3). Подсистем за контролу процеса (тј. ниво 1) није обухваћен анализом, јер садржи разноврсну опрему на терену (и хардвер и софтвер), чија миграција у рачунски облак технички није изводљива.

У наставку су дати кратки описи OT, OT DMZ и ИТ подситема релевантних за нашу анализу.

3.1 OT Подсистем

SCADA системи су инсталирани у различитим индустријским контролним системима (нпр. вода, нафта/гас и енергија) [4][5][119]. SCADA омогућава оператерима да надгледају и контролишу паметну мрежу прикупљањем података и слањем наредби на интелигентне електронске уређаје (енг. *Intelligence Electrical Devices*) IDE у процесном окружењу. SCADA је временски критични подсистем. Комуникација унутар SCADA подсистема заснива се на многим индустријским протоколима, укључујући дистрибуирани мрежни протокол v3.0 (енг. *Distributed Network Protocol 3*) DNP3, (енг. *Modicon communication bus*) ModBus, IEC 104 и IEC 61850 [15].

Компонента за управљање прекидима (OMS) је средишњи систем за извршавање планираних радова и руковање непланираним прекидима у паметној електроенергетској мрежи. Услед различитих, најчешће временских непогода долази до престанка функционисања одређеног дела мреже. Када се то деси OMS аутоматски креира инцидент. Диспечер управља решавањем тог инцидента уз помоћ радника који уз радне налоге креиране уз помоћ SSM сервиса излазе на терен и отклањају проблеме. Удаљене команде током радова диспечер издаје преко SCADA-е. OMS мора да испуњава строге захтеве за

перформансама, али они су обично повезани са способношћу да прихвате велике количине долазних позива од потрошача који пријављују и траже информације о кваровима. Ова компонента делује као централна тачка информација о прекидима и служи између осталог DSO- у да обавести купце прекидима и статусу рестаурације [4][5][120]. Циљ увођење OMS-а је повећање поузданости мреже откривањем испада и спречавањем прекида на основу идентификације нестабилности и неравнотеже [4][5][121].

Компонента за управљање секвенцом прекидача (SSM) одржава ажурне информације о теренским посадама, задацима које раде, статусима тих задатака и тачним локацијама теренских посада. На овај начин диспечер увијек има ажурне све потребне информације. За било коју акцију на терену у оквиру ове компоненте се праве радни налози са свим потребним информацијама неопходним да би посада на терену на адекватан и безбедан начин интервенисала и отклонила кварове.

Један од задатака EMS компоненте је да извршава различите анализе (нпр. процена стања, проток оптерећења, анализа у непредвиђеним ситуацијама, прорачун кратког споја итд.) над целим или делом подсистема за пренос и производњу електричне енергије [4][5][119]. У последње време преко подсистема за пренос врши се и трговина електричном енергијом. Пребацује се енергија на велике удаљености па су и напонски нивои високи, највиши напонски нивои иду до 750 kV и више у изузетним ситуацијама. У подсистему за производњу електричне енергије су заступљене разне врсте електрана, нуклеарне, хидро и темоелектране, електране на гас и све врсте електрана на обновљиве изворе енергије. EMS на улазу очекује опис мрежног модела (GIS) и тренутне вредности расклопа и мерења из SCADA-е [15]. Често се део мрежног модела и динамичких података добија од EMS "суседних" система за пренос због веза државних подсистема за пренос електричне енергије. EMC углавном ради са мањим моделом од DMS-а, али је покривеност са SCADA тачкама значајно виша, као и ниво редундансе у систему. Основни и најчешће коришћени прорачуни који се обављају након што се изврши основна функција тополошке анализе су естимација стања, токови снага, прорачун кратких спојева (тј. налажење "слабих карика" система у случају кратког споја), итд.

Сервис DMS извршава разне аналитичке прорачуне над подсистемом за дистрибуцију електричне енергије. Он се наслања на GIS тако што од њега преузима статички модел мреже, а са SCADA компоненте преузима тренутне вредности динамичких података, тј. ажурно стање расклопне опреме и мерења. На основу тако прикупљених података је у стању да над интерним моделом изврши основну функцију тополошке анализе. Након урађене тополошке анализе врше се разни прорачуни попут прорачуна токова снага, естимације стања, волт - вар оптимизација и други. Према [4][5][120] DMS поред комуникације са GIS-ом може бити уско повезан са OMS компонентом јер се након решавања инцидента покрећу различите врсте DMS прорачуна како би се мрежа вратила у употребљиво стање.

Сервис MDM прикупља и чува велике податке примљене од (паметних) бројила за мерење и извештавање о потрошњи електричне енергије и преносі те информације одељењу за наплату. Обично не дели комуникациону инфраструктуру са SCADA-ом. Поред MDM-а, AMI комуникациону мрежу чине паметна бројила и локални агрегатори података [4][5][119]. Комуникација између паметних бројила, кућних апарата и AMI главне станице дефинисана је кроз неколико комуникационих протокола попут Z-wave and Zigbee [15].

3.2 OT DMZ подсистем

Подсистем OT DMZ (тј. ниво 3 на *Слика 13*) садржи елементе система који повезују ИТ и ОТ компоненте паметне електроенергетске мреже. Иако овај подсистем може садржати много различитих компоненти и решења, нашу анализу ограничавамо на SIEM и Historical компоненте. У зависности од архитектуре они могу бити позиционирани у различитим деловима система, међутим OT DMZ је логичан избор јер им омогућује прикупљање података из ОТ и ИТ подсистема. У добро дизајнираним системским архитектурама SIEM такође има сакупљаче у процесном окружењу, што омогућава безбедносним аналитичарима да правовремено идентификују аномалије и реагују на инциденте. SIEM решења прикупљају велике количине података, омогућавајући операторима паметних електроенергетских система да открију чак и најнапредније претње (енг. *Advanced Persistent Threats*) APT у сајбер простору. NIST-ов водич за евиденцију рачунарске безбедности [123] говори о најсавременијем SIEM систему и његовим могућностима за обављање функција попут складиштење, анализа и праћење важних логова, те да представља алат коме се даје предност над конвенционалним системима ове врсте.

У идеалном случају све промене статуса и мерења, као и наредбе које су рачунари и/или људи издали у оквиру паметног EEC-а чувају се у историјској бази података ради усклађености са прописима и транспарентности. На основу свих долазних и одлазних порука снимљених на централној локацији, могуће је анализирати прошле догађаје, нпр. ванредни прекид и начин на који је функционисао систем и њиме управљали његови оператери. Historical чува оне поруке које пролазе кроз паметни EEC. Позициониран је на трећем нивоу да би омогућио корисницима у ИТ подсистема да приступе и користе историјске податке, нпр. за потребе планирања.

3.3 ИТ подсистем

На *Слика 13* ИТ подсистем се дели на ИТ и ИТ DMZ део. Иако оба могу садржавати бројне и разнолике услуге усмерене према Интернету (нпр. web, email и proxy сервиси), нашу анализу ограничавамо на GIS компоненту смештену на четвртом нивоу. Према [123] GIS је систем дизајниран за чување, манипулисање, анализу, управљање и представљање свих врста просторних или географских података. Одржава модел мреже и њених делова. Садржи један или више записа о сваком делу паметне мреже са додељеним једним или више географских положаја. GIS је релевантан за нашу анализу, јер се често користи као главни извор мрежног модела. Информације о опреми се експортују из GIS-а и импортују у SCADA, EMS, OMS, DMS и друге компоненте чије се пословање ослања на приступ ажурном мрежном моделу електроенергетског система.

4. МЕТОДОЛОГИЈА ЗА ПРОЦЕНУ РИЗИКА У ПАМЕТНИМ ЕЛЕКТРОЕНЕРГЕТСКИМ МРЕЖАМА

У овом поглављу описујемо виталне елементе методологије за безбедну примену рачунарства у облаку у надзору и управљању паметним електроенергетским системима. Примена дате методологије треба да омогући да оператори паметних ЕЕС изаберу адекватно решење са стране безбедности, уз максимално искоришћење предности које пружа рачунарство у облаку.

Опсези методологија ове врсте су различити, те је због тога неопходно јасно нагласити на који дио паметног ЕЕС ће она бити усмерена. Предмет овог рада је развој методологије за миграцију елемената ОТ подсистема ЕЕС у рачунарски облак. Миграција ИТ подсистема, односно измене веза између ИТ и ОТ подсистема током миграције у рачунарски облак нису елементи овог истраживања.

Методологија ће почети квантитативном анализом ризика која се састоји од:

1. идентификације свих нежељених догађаја или претњи (енг. *threats*),
2. вероватноће реализације датих претњи (енг. *likelihood*),
3. вредност потенцијалних губитака повезаних са датом претњом (енг. *impact*)
4. дефинисања матрице ризика на основу вероватноће реализације и утицаја потенцијалних претњи
5. креирања прототипа обрасца акумулиране процене ризика
6. дефинисања нивоа потребе за одговарајућим рачунарским ресурсима
7. дефинисања стратегија миграције

Попуњавање прототипа обрасца акумулиране процене ризика представља први дио дате методологије. На основу вероватноће реализације одговарајуће претње и утицаја који она може проузроковати, као и уз коришћење матрице ризика недвосмислено се одређује потенцијални ризик за сваку од компоненти датог система и као такав се уноси у образац.

Након што смо припремили све неопходно да се дефинише потенцијални ризик за сваку од компоненти, неопходно је да се одреде и нивои њихове потребе за рачунарским ресурсима. Одређивање ових нивоа за сваку од компоненти ћемо урадити на основу природе паметних електроенергетских система.

После одређивања потенцијалног ризика и потреба за рачунарским ресурсима, прибегавамо основној стратегији миграције. Оно што издваја ову методологију у односу на друге је што смо оставили слободу будућем кориснику да на веома лак начин прилагоди методологију својим пословним потребама и циљевима и на тако одреди колики ризик

може да толерише, као и да смањује или повећава значај рачунарских ресурса за сваку од компоненти.

У следећем поглављу примена дате методологија ће се спровести над компонентама ОТ подсистема. Резултат коришћења методологије ће бити предложена/не архитектура/е паметног ЕЕС заснованог на рачунарском облаку.

4.1 Претње и извори претњи

Почетна тачка методологије је идентификација и јасно дефинисање потенцијалних претњи. Са обзиром да је спектар претњи у електроенергетским системима широк [33][38][83][123][124] ми ћемо се усмерити на оне претње чија би реализација највише угрозила елементе CIA тријаде. У контексту инфраструктурних система нарушавање поверљивости представља мање ризичан сценарио од нарушавања интегритета и расположивости и тиме ћемо се водити приликом процене ризика и одлучивања о миграционој стратегији [4][5][25][26][27][28][29].

Моделовање претњи је важан корак у процени ризика, кроз који се ради њихова идентификација и оцењивање. Може се имплементирати користећи један од следећа три приступа [4][5]: усмерено на имовину (енг. *asset-centric*), усмерено на софтвер (енг. *software-centric*) и усмерено на нападача (енг. *attacker-centric*). Извори претњи као што су бомбашки напади, поплаве, вандализми и разни други примери саботажа су усмерени на имовину и припадају asset-centric домену, те их као такве нећемо моделовати. У овој дисертацији ћемо се усмерити на *software-centric* приступ и моделовати само оне претње које су усмерене на софтвер који се користи у паметним електроенергетским системима.

На основу искуства у овој области и литературе [4][5][14][33][34][35][36][38][42][83][120][124][125][126][127][128] креирали смо листу највероватнијих претњи по ОТ подсистем паметне мреже на основу тога који би елемент CIA тријаде могао да буде највише погођен ако се реализују. Дате претње су приказане табели испод.

Табела 4 - Идентификоване ретње у паметним ЕЕС

Редни број	Претња
П1	Злоупотреба недостатка свести и нередовних тренинга запослених у ОТ подсистему о безбедности
П2	Злоупотреба недостатка свести и нередовних тренинга оператера о безбедности
П3	Инсајдерска претња од запослених, бивших запослених, консултаната, екстерних експерата. Злонамјерни инсајдери, запослени који праве грешке и занемарују политике, инфилтратори који добију легитимни спољни приступ без одобрења.
П4	Злоупотреба недостатка процедура за пријављивање сигурносних слабости
П5	Крађа корисничких креденцијала и њихова злоупотреба
П6	Коришћење неадекватног помоћног софтвера

П7	Злоупотреба неадекватне имплементације безбедносних мера између пословног ИТ подсистема и ОТ подисистема
П8	Злоупотреба безбедносних пропуста у архитектури софтвера
П9	Злоупотреба критичних грешки у софтверу, нпр. прекорачење бафера (енг. Buffer overflow)
П10	Неауторизовано брисање фајлова (нпр. dll, .exe)
П11	Безбедносне претње проузроковане због недовољног тестирање приликом примене нових закрпа (енг. patches) или софтверске грешке након испорученог софтвера.
П12	Злоупотреба безбедносних недостатака у новим закрпама софтвера
П13	Злоупотреба недостатка безбедбносних закрпа за оперативни систем
П14	Нарушавање поверљивости конфигурационих података
П15	Нарушавање доступности конфигурационих података
П16	Нарушавање интегритета конфигурационих података
П17	Нарушавање поверљивости логованих података
П18	Нарушавање доступности логованих података
П19	Нарушавање интегритета логованих података
П20	Непоречивост акција у оквиру ОТ подсистема
П21	Нарушавање поверљивости операционих података
П22	Нарушавање доступности операционих података
П23	Нарушавање интегритета операционих података
П24	Безбеднсоне претње проуроковане неисправношћу опреме, нпр. лажна мерења сензора
П25	Нарушавање поверљивости личних података
П26	Нарушавање доступности личних података
П27	Нарушавање интегритета личних података
П28	Безбедносне претње проузроковане DoS/DDoS нападима на позадинске сервисе и комуникациону мрежу
П29	Безбедносне претње настале услед прекида рада мреже нпр. отказом рутера
П30	Безбедносне претње настале услед намерног оптерећење мреже манипулацијом потрашачких уређаја
П31	DoS/DDoS напади на human-machine interface

4.2 Вероватноћа реализације претњи

Након јасног дефинисања претњи наредни корак методологије је одређивање вероватноће њихове реализације. Са обзиром на природу и архитектуру инфраструктурних система реализација одређене претње може проузроковати значајне последице, међутим ниво вероватноће да ће се она реализовати значајно утиче на сам ризик. Уколико је веома мала вероватноћа реализације неке озбиљне претње, потенцијални ризик губи на тежини. Узмимо за пример колико озбиљне последице би се

проузроковале ако би потенцијални нападач ушао у оператерску собу и преузео контролу над софтвером тако што седне на радно место диспечера и отме му сесију, и још у детаље зна како сам софтвер функционише и на крају има све креденцијале потребне за свој злонамерни поход. Међутим, са друге стране која је вероватноћа да се тако нешто деси? Веома мала, јер свака озбиљна компанија која користи критичне индустријске контролне системе има и озбиљне физичке контроле приступа. Поред тога познавање софтвера и преузимање потребних креденцијала је још мање вероватно. Управо због овога, иако је потенцијални утицај који се може проурроковати веома висок, због мале вероватноће да до тога дође долазимо до ниског ризика.

NIST [38] и ENISA [83] предлажу пет нивоа вероватноће да ће се одређена претња реализовати:

1. Веома висок (енг. *Very High*)
2. Висок (енг. *High*)
3. Умерен (енг. *Moderate*)
4. Низак (енг. *Low*)
5. Веома низак (енг. *Very Low*)

Највећи ниво (*Very High*) представља чињеницу да је готово сигурно да ће се дата претња реализовати, док према најмањем (*Very Low*) нивоу или скоро да не постоји.

На основу разматрања у поглављу *2.2*, вероватноће реализације одређене претње видимо да сви приступи личе један на други са једном главном разликом а то је гранулација нивоа саме вероватноће.

У нашој методологији предлажемо гранулацију од пет нивоа, као и у случају NIST [38] и ENISA [83], које сматрамо референтним за америчко, односно европско тржиште. Током рада на [4][5] приметили смо да управо приликом одређивања вероватноће реализације појединих претњи, нивоа утицаја, а и касније током коришћења матрице ризика недостаје већа грануларност. Са обзиром да ћемо на крају ове методологије имати ситуацију где на основу нивоа ризика и потребе за рачунарским ресурсима треба одредити позицију сваке од компоненти у новој архитектури паметног електроенергетског система заснованог на рачунарском облаку већа гранулација ће нам свакако помоћи да јасно и недвосмислено позиционирамо сваку од компоненти.

Класификација вероватноће орјентисана ка будућој паметној мрежи која ће бити делимично у рачунарском облаку је креирана на основу претходно анализираних методологија [4][5][33][35][38][83]. Она ће бити усмерена на познате рањивости у инфраструктури и архитектури паметних мрежа, квалитет сегментације ИТ/ОТ, лојалност и обуку са аспекта безбедности особља, квалитет безбедносне архитектуре рачунарског облака итд.:

1. Постојање рањивости у сервисима или инфраструктури паметних мрежа/рачунарског облака, у распону од озбиљних до оних слабих.
2. Постојање рањивости у оперативном систему који се користи на рачунарима у оквиру електродистрибутивног предузећа (енг. *on-premise*) и рачунарском облаку

3. Позната могућа искористивост и ниво могућности да се изврше на даљину, физичким приступом и/или стицањем повишених привилегија.
4. Лојалност запослених и оператера у ОТ подсистему, као и код провајдера рачунарског облака (под особљем провајдера подразмевамо (и у наставку текста) које на директан/индиректан начин може да утиче на правилно функционисање паметне мреже).
5. Постојање способних извора претњи и ниво њихове мотивације за извршавање напада.
6. Ниво обуке запослених за сајбер безбедност у ОТ одељењима и код провајдера рачунарског облака.
7. Ниво и квалитет сегментације ИТ/ОТ система у сигурносним зонама.
8. Ниво и квалитет безбедносне архитектуре рачунарског облака.

Табела 5 - Вероватноћа реализације претњи

Вероватноћа	Карактеристике система асоциране са приказаном вероватноћом
Веома висока	Озбиљни сигурносни пропусти у сервисима и/или паметне мреже/рачунарског облака
	Озбиљни сигурносни пропусти у оперативном систему
	Познате експлоатације могу се покренути са Интернета, полу-поузданих или непоузданих мрежа
	Нелојалност оператера и осталих запослених у ОТ подсистему, као и код провајдера рачунарског облака
Висока	Високо мотивисани и способни извори претњи
	Високо интегрисани ИТ-ОТ подсистеми који излажу ОТ подсистем
	Потенцијални пропусти у безбедбосној архитектури рачунарског облака
	ОТ запослени, оператери и особље провајдера рачунарског облака без одговарајућих тренинга из сајбер безбедносни
	Неадекватно надгледање инсајдерских претњи у ОТ подсистему и рачунарском облаку
Умерена	Лимитирани сигурносни пропусти у сервисима паметне мреже/рачунарског облака
	Лимитирано надгледање инсајдерских претњи
	Нередовни тренинзи из бедбедности за оператере, ОТ запослене и особље провајдера рачунарског облака
	Лимитирна мотивација извора претњи због неатрактивног финансијског или политичког утицаја који би проузроковала дата претња
	Познати подвизи који се могу покренути само уколико постоји физички приступ датом систему. На пример уколико потенцијални нападач уместо RTU уређаја у пољу прикључи свој лаптоп и крене да генерише велики број података усмерених на SCADA компоненету.
Ниска	Напредно надгледање инсајдерских претњи

	Лојалност запослених код провајдера рачунарског облака
	Лојалност оператера и осталих ОТ запослених
	Немотивисани извори претњи због минималног финансијског или политичког утицаја ако се дата претња реализује
	Добро обучени запослени код провајдера рачунарског облака са аспекта безбедности
	Добро обучени оператери и остали ОТ запослени са аспекта безбедности
	Неизложеност ОТ подсистема услед добре ИТ-ОТ сегментације
Веома ниска	Изостанак сигурносних пропуста у сервисима паметне мреже и инфраструктури
	Постојање (енг. *Access Control List*) листе контроле приступа
	Нема познатих експлоатација, злонамерним корисницима је потребан физички приступ и повишене привилегије у циљном систему

У овој докторској дисертацији водићемо се чињеницом да провајдери рачунарског облака имају адекватно обучено особље са аспекта безбедности, инфраструктуру без безбедосних пропуста, напредно надгледање инсајдерских претњи итд. Дате информације ћемо оставити у претходној табели како би будући корисници методологије могли да их искористе и директно уврсте у анализу у случају да немају поверење у одређену услугу рачунарског облака.

4.3 Утицај који се проузрокује потенцијалним реализовањем одговарајуће претње

Цела методологија има за циљ да идентификује потенцијалне ризике , како би њен корисник касније уз адекватну имплементацију контрола смањио могућност да се одређене претње реализују. На томе путу, ниво утицаја (енг. *Impact*) који се може проузроковати реализацијом одређених претњи, тј. колико штете може да се проузрокује, је веома важна ставка којој је потребно посветити посебну пажњу. У критичним инфраструктурним системима та штета може да буде неприметна, али исто тако може да доведе до неупотребљивости делова система, финансијских издатака и у најгорем случају људских жртава.

Према NIST [38] и ENISA [83] типови утицаја реализације претњи се деле на оне усмерене на правилно функционисање система, финансијске губитке, казне од стране регулаторних агенција, оштећења инфраструктуре, утицај на друге организације, репутацију компаније, откривање личних података, и на крају повреде људи и губитак људских живота.

У зависности од претходно представљених утицаја, NIST [38] и ENISA [83] предлажу следеће квалитативне нивое утицаја:

1. Веома висок (енг. *Very High*)
2. Висок (енг. *High*)
3. Умерен (енг. *Moderate*)
4. Низак (енг. *Low*)
5. Веома низак (енг. *Very Low*)

Да би се објаснила претходна подела по нивоима, *веома висок* ниво представља озбиљне или катастрофалне штетне ефекте на организацију, инфраструктуру, запослене, друге организације и саму нацију. Последњи ниво представља занемариве утицаје, док остали нивои у смеру од најнижег према већем утицају имају префикс лимитирано, озбиљно и тешко.

На основу методологија [4][5][33][35][38][83] анализираних у поглављу 2.2, а у циљу да и као код вероватноће реализације претњи останемо на гранулацији од пет нивоа предлажемо класификацију утицаја претњи на паметну мрежу која ће бити делимично у рачунарском облаку, засновану на теоријски могућем утицају (1) исправан рад паметне мреже, (2) јавни имиџ оперативне компаније, (3) неоштећење инфраструктуре, (4) финансијски губици и (5) угрожавање или губитак људских живота.

1. Утицаји веома високог нивоа који укључују губитак људских живота или озбиљне повреде запослених или купаца. Такође, дуготрајни прекиди испоруке електричне енергије и уништавање вредне имовине као што су трансформаторске станице са вредношћу већом од милион еура. Комплетна неупотребљивост софтвера и недоступност критичних инфраструктурних система ове врсте може директно да доведе и до значајних економских и јавних ефеката у смислу економског губитка једне државе, утицаја на животну средину итд.
2. Утицаји високог нивоа доводе до распрострањених краткотрајних прекида напајања електричном енергијом, озбиљних оштећења инфраструктуре, директних финансијске трошкове и критичних кварова у сервису (нпр. продужен прекид рада SCADA-е). Такође, овде спада веома осетљива тема а то је губитак личних и/или осетљивих података корисника, затим високе казне од регулаторних тела и неповерење корисника. Све ово доводи до неповерења јавности, поремећаја свакодневног живота, укључујући губитак основних услуга за живот у 21. веку.
3. Утицаји умереног нивоа укључују откривање осетљивих пословних података, података о опреми, ограничене прекиде у напајању, казне од регулаторних агенција и утицај на друге организације и друга електродистрибутивна предузећа. Такође, укључују губитак доступности некритичних услуга (нпр. GIS или EMS), лимитирану штету на инфраструктури, нарушавање интегритета некритичних компоненти и откривање података на основу којих је могуће припремити потенцијални додатни напад.
4. Утицаји ниског нивоа узрокују кашњења у некритичним услугама или објављивању информација које немају директан пословни утицај, али могу довести до рањивости, као и цурење информација без директног финансијског утицаја или утицаја на углед компаније.
5. Утицаји веома ниског нивоа доводе до потенцијалних проблема у софтверу, ниског приоритета који не нарушавају његово свакодневно коришћење.

Горе наведени могући утицаји сажети су у табели испод.

Табела 6 - Ниво утицаја услед реализације потенцијалне претње

Утицај	Опис утицаја
Веома висок	Озбиљне повреде или губитак људских живота
	Дуготрајни прекиди испоруке електричне енергије (енг. *Blackout*)
	Уништавање вредне имовине
	Неупотребљивост софтвера и недоступност система
Висок	Распрострањени краткотрајни прекиди у напајању електричном енергијом
	Недоступност критичних сервиса
	Озбиљна оштећења опреме (e.g. оштећење трансформатора високог напона)
	Директни финансијски трошкови и критични кварови у сервису (нпр. продужен прекид рада SCADA-е).
	Откривање личних и/или осетљивих података корисника
	Високе казне од стране регулаторних агенција
	Губитак поверења корисника
Умерен	Откривање осетљивих пословних података
	Откривање података о опреми
	Умерене казне од регулаторних агенција
	Незадовољство потрошача
	Утицај на друге организације и друга електродистрибутивна предузећа
	Ограничени прекиди у напајању
	Лимитирана штета на инфраструктури
	Губитак доступности некритичних сервиса
	Откривање података на основу којих се може урадити припрема за потенцијални напад
	Нарушавање интегритета некритичних сервиса
Низак	Ограничена недоступност некритичних сервиса
	Цурење информација без директног финансијског утицаја или утицаја на углед компаније
Веома низак	Потенцијални проблеми у софтверу, ниског приоритета који не нарушавају његово свакодневно коришћење

4.4 Матрица ризика

Са обзиром да смо се приликом дефинисања вероватноће и утицаја определили за гранулацију од пет нивоа, очекивано је и да сама матрица ризика буде тих димнезија. На водоравној оси је приказан утицај реализације потенцијланих претњи нивоима:

1. Веома висок
2. Висок
3. Умерен
4. Низак
5. Веома низак

док је на вертикалној оси вероватноћа реализације датих претњи приказана нивоима:

1. Веома висока
2. Висока
3. Умерена
4. Ниска
5. Веома ниска

Заобљени правугаоници у средини (*Слика* 14) једнозначно одређују нивое ризика у зависности од вертикалне и хоризонталне осе. На пример уколико је утицај који се проузрокује потенцијалним реализовањем одговарајуће претње на веома високом нивоу, а вероватноћа да дође до те реализације веома ниска, на основу слике испод можемо закључити да ће процењени ризик бити на ниском нивоу.

Слика 14 - Матрица ризика

Матрица ризика углавном садржи пет нивоа што можемо да видимо и у случају NIST [33] и ENISA [83], које смо узимали као рефрентне као у случају процене вероватноће и потенцијалног утицаја. Постоје и матрице ризика са мање нивоа, као у случају [4][5][38], међутим у радовима [4][5] смо увидели да када се анализирају ризици у оваквим типовима критичних инфраструктурних система често долазимо у ситуацију

да се двоумимо коме нивоу припада анализирана компонента. Уз већу гранулацију је свакако много лакше адекватно позиционирати сваку од компоненти.

Сходно нивоима вероватноће и утицаја који може да се проузрокује ако се нека од претњи реализује, логичним следом долазимо и до нивоа ризика у нашој методологији:

1. Веома висок
2. Висок
3. Умерен
4. Низак
5. Веома низак

Дескриптивна анализа матрице ризика (*Слика 14*), креирана на основу *Табела 5* и *Табела 6* је приказана испод. Ради лакшег читања ових табела ниво ризика из прве колоне ће се манифестовати уколико се на основу рањивости из друге колоне асоцираних са процењеном вероватноћом реализују сценарији из треће колоне и на тај начин изазову дати утицај на систем.

Табела 7 - Илустративни приказ ризика веома високог нивоа

Ниво ризика	Вероватноћа	Утицај
Веома висок	Озбиљни сигурносни пропусти у сервисима паметне мреже Озбиљни сигурносни пропусти у оперативном систему Познате експлоатације могу се покренути са Интернета, полу-поузданих или непоузданих мрежа Нелојалност оператера и осталих запослених у ОТ подсистему	Повреде људи и у најгорем случају губитак људских живота Распрострањени дугорочни прекиди напајања електричном енергијом Значајно оштећење опреме Губитак личних података корисника
	Високо мотивисани и способни извори претњи Високо интегрисани ИТ-ОТ подсистеми који излажу ОТ подсистем ОТ запослени и оператери без одговарајућих тренинга из сајбер безбедносни	

	Неадекватно надгледање инсајдерских претњи у ОТ подсистему	

Табела 8 - Илустративни приказ ризика високог нивоа

Ниво ризика	Вероватноћа	Утицај
Висок	Озбиљни сигурносни пропусти у сервисима паметне мреже Озбиљни сигурносни пропусти у оперативном систему Познате експлоатације могу се покренути са Интернета, полу-поузданих или непоузданих мрежа Нелојалност оператера и осталих запослених у ОТ подсистему	Распрострањени краткотрајни прекиди у напајању електричном енергијом Недоступност критичних сервиса Озбиљна оштећења опреме (e.g. оштећење трансформатора високог напона) Директни финансијски трошкови и критични кварови у сервису (нпр. продужен прекид рада SCADA-е). Откривање личних и/или осетљивих података корисника Високе казне од стране регулаторних агенција Губитак поверења корисника
	Високо мотивисани и способни извори претњи Високо интегрисани ИТ-ОТ подсистеми који излажу ОТ подсистем ОТ запослени и оператери без одговарајућих тренинга из сајбер безбедносни Неадекватно надгледање инсајдерских претњи у ОТ подсистему	
	Лимитирани сигурносни пропусти у сервисима паметне мреже Лимитирано надгледање инсајдерских претњи	Повреде људи и у најгорем случају губитак људских живота Распрострањени дугорочни прекиди напајања електричном енергијом

	Нередовни тренинзи из бедбедности за оператере и остале ОТ запослене Лимитирна мотивација извора претњи због неатрактивног финансијског или политичког утицаја Познати подвизи који се могу покренути само уколико постоји физички приступ датом систему	Значајно оштећење опреме Губитак личних података корисника

Табела 9 - Илустративни приказ ризика умереног нивоа

Ниво ризика	Вероватноћа	Утицај
Умерен	Озбиљни сигурносни пропусти у сервисима паметне мреже Озбиљни сигурносни пропусти у оперативном систему Познате експлоатације могу се покренути са Интернета, полу-поузданих или непоузданих мрежа Нелојалност оператера и осталих запослених у ОТ подсистему	Откривање осетљивих пословних података Откривање података о опреми Умерене казне од регулаторних агенција Незадовољство потрошача Утицај на друге организације и друга електродистрибутивна предузећа Ограничени прекиди у напајању Лимитирана штета на инфраструктури Губитак доступности некритичних сервиса Откривање података на основу којих се може урадити припрема за потенцијални напад
	Високо мотивисани и способни извори претњи Високо интегрисани ИТ-ОТ подсистеми који излажу ОТ подсистем ОТ запослени и оператери без одговарајућих тренинга из сајбер безбедносни	

	Неадекватно надгледање инсајдерских претњи у ОТ подсистему	Нарушавање интегритета некритичних сервиса
	Лимитирани сигурносни пропусти у сервисима паметне мреже Лимитирано надгледање инсајдерских претњи Нередовни тренинзи из бедбедности за оператере и остале ОТ запослене Лимитирна мотивација извора претњи због неатрактивног финансијског или политичког утицаја Познати подвизи који се могу покренути само уколико постоји физички приступ датом систему	Распрострањени краткотрајни прекиди у напајању електричном енергијом Недоступност критичних сервиса Озбиљна оштећења опреме (e.g. оштећење трансформатора високог напона) Директни финансијски трошкови и критични кварови у сервису (нпр. продужен прекид рада SCADA-е). Откривање личних и/или осетљивих података корисника Високе казне од стране регулаторних агенција Губитак поверења корисника
	Напредно надгледање инсајдерских претњи Лојалност оператора и осталих ОТ запослених Немотивисани извори претњи због минималног финансијског или политичког утицаја Добро обучени запослени оператери и остали ОТ запослени са аспекта безбедности	Повреде људи и у најгорем случају губитак људских живота Распрострањени дугорочни прекиди напајања електричном енергијом Значајно оштећење опреме Губитак личних података корисника

	Неизложеност ОТ подсистема услед добре ИТ-ОТ сегментације	

Табела 10 - Илустративни приказ ризика ниског нивоа

Ниво ризика	Вероватноћа	Утицај
Низак	Озбиљни сигурносни пропусти у сервисима паметне мреже Озбиљни сигурносни пропусти у оперативном систему Познате експлоатације могу се покренути са Интернета, полу-поузданих или непоузданих мрежа Нелојалност оператера и осталих запослених у ОТ подсистему	Ограничена недоступност некритичних сервиса Цурење информација без директног финансијског утицаја или утицаја на углед компаније
	Високо мотивисани и способни извори претњи Високо интегрисани ИТ-ОТ подсистеми који излажу ОТ подсистем ОТ запослени и оператери без одговарајућих тренинга из сајбер безбедносни Неадекватно надгледање инсајдерских претњи у ОТ подсистему	
	Лимитирани сигурносни пропусти у сервисима паметне мреже Лимитирано надгледање инсајдерских претњи	

	Нередовни тренинзи из бедбедности за оператере и остале ОТ запослене Лимитирна мотивација извора претњи због неатрактивног финансијског или политичког утицаја Познати подвизи који се могу покренути само уколико постоји физички приступ датом систему	
	Напредно надгледање инсајдерских претњи Лојалност оператера и осталих ОТ запослених Немотивисани извори претњи због минималног финансијског или политичког утицаја Добро обучени запослени оператери и остали ОТ запослени са аспекта безбедности Неизложеност ОТ подсистема услед добре ИТ-ОТ сегментације	Откривање осетљивих пословних података Откривање података о опреми Умерене казне од регулаторних агенција Незадовољство потрошача Утицај на друге организације и друга електродистрибутивна предузећа Ограничени прекиди у напајању Лимитирана штета на инфраструктури Губитак доступности некритичних сервиса Откривање података на основу којих се може урадити припрема за потенцијални напад Нарушавање интегритета некритичних сервиса

	Непознати сигурносни пропусти у сервисима паметне мреже и инфраструктури Постојање (енг. Access Control List) ACL-а Нема познатих експлоатација, злонамерним корисницима је потребан физички приступ и повишене привилегије у циљном систему	Распрострањени краткотрајни прекиди у напајању електричном енергијом Недоступност критичних сервиса Озбиљна оштећења опреме (e.g. оштећење трансформатора високог напона) Директни финансијски трошкови и критични кварови у сервису (нпр. продужен прекид рада SCADA-е). Откривање личних и/или осетљивих података корисника Високе казне од стране регулаторних агенција Губитак поверења корисника
		Повреде људи и у најгорем случају губитак људских живота Распрострањени дугорочни прекиди напајања електричном енергијом Значајно оштећење опреме Губитак личних података корисника

Табела 11 - Илустративни приказ ризика веома ниског нивоа

Ниво ризика	**Вероватноћа**	**Утицај**
Веома низак	Озбиљни сигурносни пропусти у сервисима паметне мреже	Потенцијални проблеми у софтверу, ниског приоритета

	Озбиљни сигурносни пропусти у оперативном систему Познате експлоатације могу се покренути са Интернета, полу-поузданих или непоузданих мрежа Нелојалност оператера и осталих запослених у ОТ подсистему	који не нарушавају његово свакодневно коришћење
	Високо мотивисани и способни извори претњи Високо интегрисани ИТ-ОТ подсистеми који излажу ОТ подсистем ОТ запослени и оператери без одговарајућих тренинга из сајбер безбедносни Неадекватно надгледање инсајдерских претњи у ОТ подсистему	
	Лимитирани сигурносни пропусти у сервисима паметне мреже Лимитирано надгледање инсајдерских претњи Нередовни тренинзи из бедбедности за оператере и остале ОТ запослене Лимитирна мотивација извора претњи због неатрактивног финансијског или политичког утицаја Познати подвизи који се могу покренути само уколико постоји физички приступ датом систему	

	Напредно надгледање инсајдерских претњи Лојалност оператера и осталих ОТ запослених Немотивисани извори претњи због минималног финансијског или политичког утицаја Добро обучени запослени оператери и остали ОТ запослени са аспекта безбедности Неизложеност ОТ подсистема услед добре ИТ-ОТ сегментације	
		Ограничена недоступност некритичних сервиса Цурење информација без директног финансијског утицаја или утицаја на углед компаније
	Непознати сигурносни пропусти у сервисима паметне мреже и инфраструктури Постојање (енг. Access Control List) ACL-а Нема познатих експлоатација, злонамерним корисницима је потребан физички приступ и повишене привилегије у циљном систему	Откривање осетљивих пословних података Откривање података о опреми Умерене казне од регулаторних агенција Незадовољство потрошача Утицај на друге организације и друга електродистрибутивна предузећа Ограничени прекиди у напајању Лимитирана штета на инфраструктури

		Губитак доступности некритичних сервиса Откривање података на основу којих се може урадити припрема за потенцијални напад Нарушавање интегритета некритичних сервиса

4.5 Креирање прототипа обрасца акумулиране процене ризика

На основу дефинисаног скупа претњи (*Табела 4*), вероватноће њихове реализације (*Табела 5*) и утицаја који могу да проузрокују на систем (*Табела 6*) направили смо образац акумулиране процене ризика, који власници/оператори могу да користе за процену ризика својих паметних мрежа. За сваку идентификовану претњу додат је један ред, а свака компонента из ОТ подсистема представља један стубац.

Попуњавање датог обрасца се своди на одређивање вероватноће и утицаја за сваку од претњи и уношења тих информација у заглавље ступаца. Кумулативни ризик се одређује на основу матрице ризика приказане на *Слика 14*, те се након тога уноси у доње делове ћелија са три елемента, тачније у ћелије са тамнијим позадинама.

Евидентно је да ће услед великог броја идентификованих претњи дати образац бити комплексан и са много информација. Због тога предлажемо да се само ризици највећег нивоа по компоненти обоје одговарајућом бојом. На пример ако за компоненту 1 имамо десет процењених нивоа ризика (један по претњи) од којих је највећи умерени ниво који се појављује два пута (нпр. у случају претње 1 и претње 7), онда ћемо само ћелије са тим нивоом обојити у адекватну боју. На овај корак смо се одлучили јер је битно идентификовати највећи процењени ризик по свакој компоненти.

Претходно описани образац који уједно представља резултат првог дела методологије и полазну тачку за креирање стратегија миграције је приказан у табели испод.

Табела 12 - Прототип обрасца акумулиране процене ризика

Претња / Компонента	**ОТ компонента #1**		**…**		**ОТ компонента #N**	
	Утицај	Вероватноћа			Утицај	Вероватноћа
Претња #1						
Претња #2						
…						
Претња # N						

Важно је напоменути да се овај образац за процену ризика може генерализовати, јер се и листа претњи у редовима, као и листа ОТ компоненти у његовим колонама могу прилагодити и ускладити са специфичним архитектурама паметних електроенергетских система. Такође, овај образац на енглеском језику је представљен у *Табела 47*, са циљем да би био доступан и коришћен и ван српског говорног подручија.

Као што је речено, ова методологија није уско везана за паметне ЕЕС-е, већ је планирано да њена употреба буде могућа и у случају ОТ подсистемима других инфраструктура (нпр. гас, вода и отпадне воде). Ако погледамо листу дефинисаних претњи (*Табела 4*), вероватноћу њихове реализације (*Табела 5*), утицај који се проузрокује потенцијалним реализовањем одговарајуће претње (*Табела 7*), као и сам прототип обрасца акумулиране процене ризика (*Табела 12*) видећемо да су оне креиране за потребе различитих критичних инфраструктурних система, и да се нисмо уско везали за ЕЕС.

5. ОСНОВНА СТРАТЕГИЈА МИГРАЦИЈЕ

Јасно дефинисање потенцијалних претњи, вероватноће и утицаја њихове реализације, и на крају дефинисање матрице ризика су кораци који воде до креирања обрасца акумулиране процене ризика што представља последњи аспект првог дела наше методологије. Након што се процени потенцијални ризик за сваку од компоненти попуњавањем датог обраца, следећи корак је одређивање потребе за рачунарским ресурсима, те на основу ове две информације можемо експлицитно одредити позицију сваке од компоненти у новој архитектури паметног електроенергетског система заснованој на рачунарству у облаку. Предности рачунарства у облаку као што су трошкови, минимизација броја физичких рачунара, обезбеђивање отпорности у случају отказа поједине рачунарске компоненте итд., нећемо узимати у обзир приликом миграције, већ ћемо их оставити за нека будућа истраживања.

Генералне препоруке којима ћемо се водити током миграције компоненти паметног електроенергетског система у рачунарски облак су:

1. Услуге сместити у *on-premise* делу ако се директно повезују на физичку опрему.
2. Радне станице сместити у контролни центар, тако да оператери надгледају и контролишу паметну мрежу са физички обезбеђене локације.
3. Пратити методологију и уважавати њене резултате приликом одређивања позиције за сваку од компоненти у хибридном решењу
4. Опције за избор облака у хибридном решењу су приватни облак и облак заједнице.

Очито је да горња правила могу бити прилагођена различитој перцепцији сајбер безбедности од стране власника/оператора паметних мрежа, тј. усклађена с њиховом спремношћу да прихвате одређене нивое ризика.

Сви потенцијални корисници наше методологије ће имати другачије захтеве и потребе за рачунарским ресурсима. Постоје различите архитектуре ових сиситема, које контролишу електроенергетске мреже различите комплексности и опслужују већи или мањи број потрошача.

Доступност рачунарских ресурса на захтев и перформансе су свакако један од аспеката због кога смо се и одлучили да покушамо представити рачунарство у облаку као одлично решење за будућност паметних ЕЕС, па њихово фигурисање у самој методологији је логичан след. У оквиру критичних инфраструктурних система, неопходно је обезбедити довољно адекватних ресурса који директно утичу на перформантност саме апликације. Постоји већи скуп ресурса овога типа, али они који

играју главну улогу, и на којима ће бити акценат у овој докторској дисертацији и који могу директно довести до повећања перформанси апликације су:

1. Потрошња оперативне меморије (енг. *Remote Access Memory - RAM*)
2. Брзина уписа и читања, као и капацитет чврстог диска (енг. *Hard Disk Drive - HDD*)
3. Искоришћење процесора (енг. *Central Processing Unit - CPU*)
4. Проток рачунарске мреже (енг. *Networking Bandwith*)

Када причамо о овим ресурсима, велика предност рачунарског облака је што се они врло лако и брзо могу повећати по потреби и што се провајдери труде да понуде увијек њихову најновију генерацију и на тај начин утичу на перформантност апликације. Употребом рачунарства у облаку перформансе система могу да се повећају до 27 % [129] или чак до 32% [57] у односу на исто рењење инсталирано у оквиру електродистрибутивног предузећа.

Према модерним истраживањама [99], може се закључити да су паметне мреже уско повезане са рачунарством високих перформанси [130], да су облачне платформе примењиве у рачунарству високих перформанси [131] и представљају корисну технику за превазилажење изазова у традиционалном управљању електроенергетских система [132].

Математичка формулација стратегије миграције ће бити дводимензионална са потребом за рачунарским ресурсима (енг. *Computer resources - Cr*) приказаним на апциси, док ће потенцијални ризик (енг. *Risk - R*) бити приказан на ординати.

Свесни смо да ће неки корисници методологије хтети да иду према значајним рачунарским ресурсима и високим перформансама, а на уштруб безбедности, те ћемо због тога дату формулацију проширити са њеним асимптотама *aR* и *aCr*. Асимптота *aR* представља хоризонтално померање, где у случају њене позитивне вредности померање ће бити у десно. Са друге стране, *aCr* је вертикално померање које ће бити у смеру према горе уколико вредност ове асимптоте буде позитивна. Да би лакше разумели, другачије речено, што је већа вредност помоћне променљиве *aR*, добијамо решење са већим нивоом толеранције ризика, док са већом вредношћу променљиве *aP* смањујемо потребу за коришћењем рачунарских ресурса у облаку.

Са обзиром да процењени ризик и потреба за рачунарским ресурсима не могу бити негативни, потребно је посматрати дату функцију само у првом квадранту.

$$\boldsymbol{Cr = f(R, aR, aCr)}$$

$$\boldsymbol{0 \leq R, Cr, aR, aCr}$$

Предност ове методологије је да померање не иде искључиво по једној оси, већ је кориснику методологије препуштено да сам бира однос према ризику и према потреби за рачунарским ресурсима. Они мењају помоћне променљиве истовремено доводећи их до њима прихватљивог нивоа.

6. ПРИМЕНА МЕТОДОЛОГИЈЕ

У овом поглављу ћемо се фокусирати на примену претходно имплементиране методологије за процену ризика у паметним електроенергетским системима на конкретне примере. У ту сврху ћемо као улаз у представљену методологију искористити прототип архитектуре ОТ подсистема (*Слика 13*).

У представљеној методологији имамо промењљиве параметре у оквиру математичке формулације, па ћемо имати више потенцијалних резултата, тј. више предложених архитектура. Потенцијалном кориснику је остављено да изабере који ниво толеранције ризика жели. Постоје корисници којима је акценат на рачунарским ресурсима, а сајбер безбедност решења им није у првом плану, као и обратно. Да не буде забуне, непходно је да се улаже и у сајбер безбедност и у рачунарске ресурсе, међутим често недовољан буџет буде препрека јер нпр. мали DSO нема новца за адекватну заштиту од одређених врста сајбер напада.

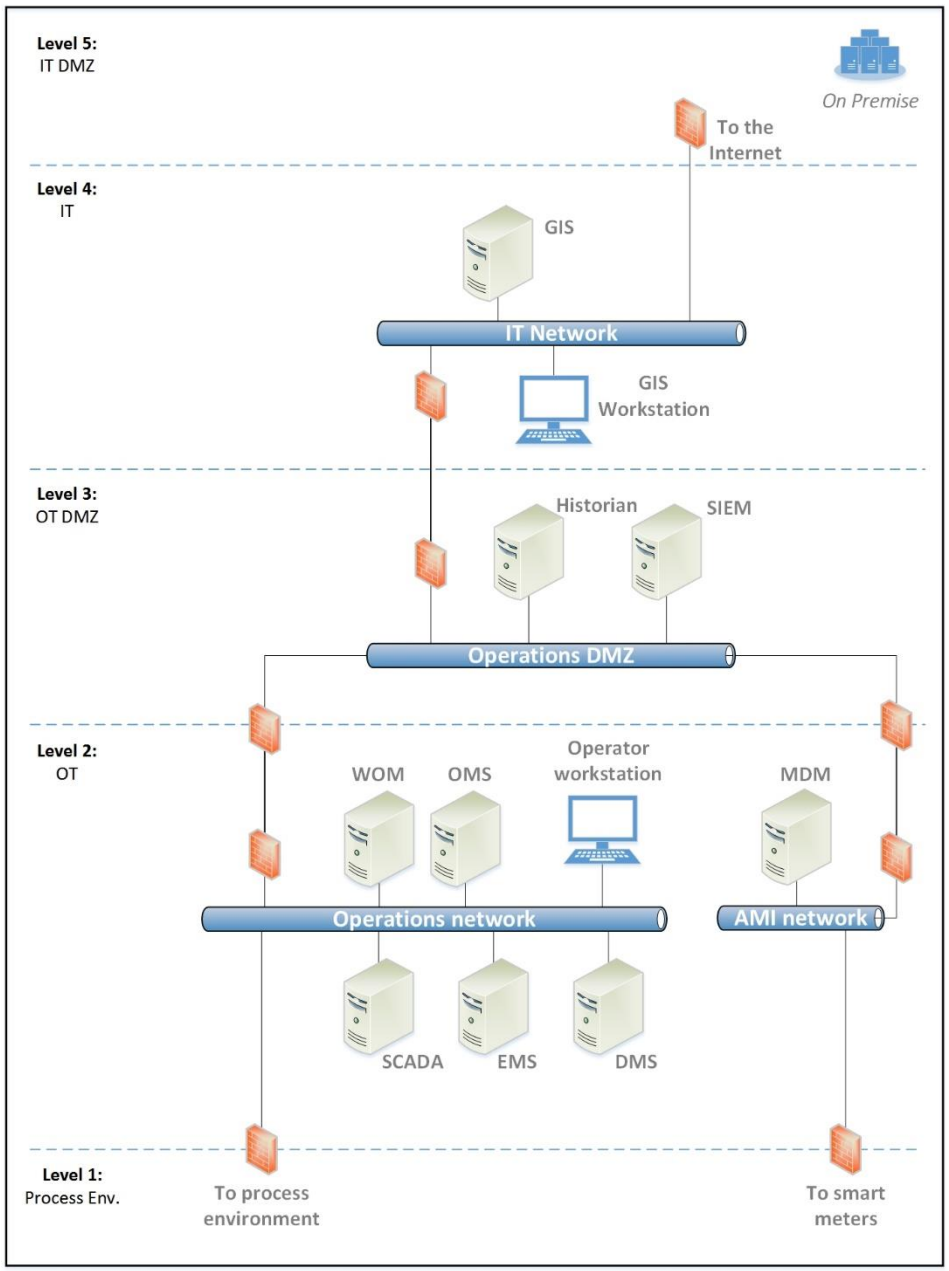
Бићемо усмерени на две значајно различите студије случаја у којима две различите врсте дистрибутивних система (DSO) мигрирају делове својих ОТ подсистема у рачунарски облак.

У првој студији случаја урадићемо процену ризика на основу које ћемо предложити архитектуру углавном засновану на облаку за велики, мултидржавни и/или међународни DSO. Поред тога, анализираћемо и мали DSO који ће се састојати од мањег броја компоненти из предложеног прототипа.

У наставку ћемо приказати најрелевантније карактеристике ове две врсте система. Затим, уз помоћ претходно креиране методологије урадићемо анализу ризика и потребе за рачунарским ресурсима, и на крају као резултат представити више потенцијалних архитектура паметног електроенергетског система заснованог на рачунарству у облаку.

6.1 Процена ризика

Први корак наше методологије је процена ризика за сваку од компоненти претходно описаног великог DSO система. Као што је већ приказано, то су компоненте: SCADA, DMS, EMS, SSM, MDM, SIEM, Historian, OMS и GIS.



Слика 15 - Архитектура великог DSO подсистема

У ту сврху попунићемо образац акумулиране процене ризика (*Табела 12*), задржавајући идентификоване претње паметног ЕЕС-а у редовима и све компоненте као ступце. За сваку комбинацију компоненти и претњи потребно је одредити ниво утицаја (*Табела 5*), као и ниво вероватноће реализације датих претњи (*Табела 6*). На основу ова два нивоа једноставним коришћењем матрице ризика (*Слика 14*) долазимо до процењеног потенцијалног ризика. Укупан ризик за одређену компоненту ће бити једнак највећем процењеном ризику за ту компоненту током анализе свих потенцијалних претњи. Под овим мислимо, да ако током анализе свих потенцијалних претњи које смо идентификовали као релевантне за ову врсту система закључимо да је процењени ризик на веома ниском нивоу, а само у случају једне претње на веома високом нивоу, ми укупан ризик за ту компоненту морамо да означимо као веома висок јер постоји начин да буде компромитована.

Због широког опсега претњи и великог броја компоненти паметног ЕЕС које се анализирају, а све услед боље прегледности груписаћемо и анализирати сличне претње и попуњавати делове прототипа акумулиране процене ризика. Без оваквог приступа би тешко било испратити цели процес јер би на почетку имали дескриптиван текст са много чињеница, а тек на крају анализе би приложили визуелни приказ. Читалац би морао веома често да се са текста референцира на прототип акумулиране процене ризика и обратно. Поред парцијалне анализе, на крају поглавља ћемо приказати и попуњен образац акумулиране процене ризика за све компоненте на једном месту.

6.1.1 Злоупотреба намерних/ненамерних људских грешака са аспекта безбедности

6.1.1.1 Претња 1 (П1): Злоупотреба недостатка свести и нередовних тренинга запослених у ОТ подсистему о безбедности

Конкретно у случају свих компоненти недовољна свест запослених у ОТ подсистему о безбедности може да доведе до откривања информација трећој страни. Баналан пример, а то се односи на сваку компоненту коју ћемо анализирати је да потенцијални нападач позове телефоном некога од запослених и лажно се представи тражећи податке о инцидентима, локацији опреме и опреми, потрошачима, потрошњи итд. Губитком поверљивости оперативних података OMS-а и MDM-а могу процурити лични подаци потрошача (енг. *Personally Identifiable Information – PII*). Други пример како се може искористити недовољна свест запослених о безбедности је *phishing* напад, слање малициозног садржаја на електронску пошту запослених који када се активира може проузроковати значајне штете од већ споменутог цурења информација до тоталног паралисања система услед недоступности компоненти. Лажно представљање у форми *phishing*-а чини 91% успешних вектора напада на ОТ подсистеме [45]. *Stuxnet* напад који представља саботажу над нуклеарним постројењима у Ирану појаснио је шта се може урадити из сајбер простора [17]. Метод напада је био посебно развијен злонамеран *malware* дизајниран да искористи рањивост оперативног система и индустријског контролног система са циљем преузимања контроле над ОТ подсистемом и издавања команди актуаторима који су довели до кварова опреме која се користила за обогаћивање нуклеарног горива. Сложени *malware, Duqu* је откривен 2011. године и дизајниран је да компромитује индустријске системе са циљем прикупљања информација из контролних система за будућу експлоатацију [18]. Потребно је велико доменско знање да се направи *malware* који би нарушио интегритет у оквиру оваквих типова система, али преузимање информација, онеспособљавање сервера и на тај начин нарушавање датих компоненти је један од главних циљева њихових креатора.

6.1.1.1.1 Утицај

Приликом одређивања утицаја узмимо за чињеницу претходно наведено, где услед грешке запослених и неадекватне имплементације безбедности у најгорем случају може доћи до недоступности сваке компоненте, као и нарушавања поверљивости. Ниво штете зависи свакако од мотивисаности нападача, као и од квалитета злонамерног софтвера. Утицај који могу овакве претње да изазову ако се реализују је *веома висок* за SCADA-у. Услед њене недоступности значајан део система је недоступан и неупотребљив. Угрожавање DMS и EMS компоненти може проузроковати *висок* утицај јер нећемо имати основне електроенергетске функције, које припадају домену критичних сервиса (*Табела 6*). Недоступност OMS компоненте може да доведе до временски неприхватљивих испада, што проузрокује високе финансијске трошкове и губитак

угледа, те поред горе споменутог потенцијалног цурења информација, утицај код ове компоненте оцењујемо као *висок* (*Табела 6*). Утицај на MDM компоненту, такође због аспекта цурења информација оцењујемо са *високим* нивоом (*Табела 6*). Са друге стране MDM компонента није критична са аспекта недоступности, али претходно споменуто цурење личних података је заслужно за *висок* ниво утицаја који може да се проузрокује уколико би се дате претње реализовале.

Недоступност SSM и GIS компоненти није критична, јер без SSM компоненте радови на терену се могу изводити на традиционалан начин, са добро обученом посадом, док се подаци о опреми и мрежни модел из GIS компоненте могу ручно унети. Управо због овога, утицај на SSM компоненту можемо сматрати као *умерен* (*Табела 6*), док ћемо и утицај на GIS оценити *умереним* нивоом (*Табела 6*) због потенцијалног цурења информација о самој опреми.

Утицај код SIEM и Historian компоненти ћемо да оценимо *умереним* према препорукама о утицају у оквиру наше методологије (*Табела 6*), јер оне не представљају критичне инфраструктурне системе, а и не постоји ризик да процуре важне информације, осим оних које би потенцијалном нападачу биле од помоћи да припреми напад. Умерен утицај је и због потенцијалних казни од стране регулаторних агенција због непотпуности информација у датим компонентама услед њихове недоступности (*Табела 6*). Регулаторне агенције ове податке користе за различите врсте извештаја.

6.1.1.1.2 Вероватноћа

Иако смо сведоци да су се слични инциденти већ дешавали, вероватноћу да се реализује дата претња за било коју компоненту оцењујемо као *ниску* (*Табела 5*) јер сматрамо да корисници наше методологије улажу и новац и време у потребне тренинге и да имају обучену радну снагу. Такође, сматрамо да је архитектура система адекватно имплементирана са аспекта безбедности како се не би потенцијални *malware* од запослених у ОТ подсистему пропагирао даље кроз њега.

6.1.1.2 Претња 2 (П2): Злоупотреба недостатка свести и нередовних тренинга оператера о безбедности

6.1.1.2.1 Утицај

Утицај који се може манифестовати грешком оператера услед недостатка свести и нередовних тренинга о безбедности је исти као и код претходне претње. Необучен оператер може да открије поверљиве информације, услед слабе концентрације прекине напајање великом броју потрошача, оптерети и онеспособи претходно споменуте компоненте итд.

6.1.1.2.2 Вероватноћа

Претходна анализа је више била усмерена на ОТ запослене и вероватноћу и утицај смо оцењивали на основу њих. Међутим, ако посматрамо оператере, они су неко ко је свакодневно уз софтвер и где су безбедносне обуке чешће и опширније. Свест о потенцијалним проблемима који се могу проузроковати је велика, те због тога вероватноћу да ће они погрешити и на тај начин проузроковати претходно наведене проблеме оцењујемо као *веома ниску* (*Табела 5*).

Табела 13 - Акумулирана процена ризика за претње 1 и 2

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П1	V V	N	V	N	V	N	V	N	U	N	V	N	U	N	U	N	U	N
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	
П2	V V	V N	V	V N	V	V N	V	V N	U	V N	V	V N	U	V N	U	V N	U	V N
	N		**N**		**N**		**N**		**VN**		**N**		**VN**		**VN**		**VN**	

6.1.1.3 Претња 3 (П3): Инсајдерска претња од запослених, бивших запослених, консултаната, екстерних експерата. Злонамјерни инсајдери, запослени који праве грешке и занемарују политике, инфилтратори који добију легитимни спољни приступ без одобрења.

Једна од најопаснијих претњи која је у директној вези са недостатком процедура за пријављивање сигурносних слабости су инсајдерске претње од запослених, бивших запослених, консултаната, екстерних експерата. Злонамерни инсајдери, запослени који праве грешке и занемарују политике, инфилтратори који добију легитимни спољни приступ без одобрења представљају директну опасност чији утицај може бити дефинитивно највећег нивоа. Можемо само да замислимо шта је у стању да уради револтирани оператер који је добио отказ, а услед неадекватних безбедносних процедура задржао све потребне картице и креденцијале које је до јуче имао као регуларно запослен. Интересантан је пример [14] напада на систем за надзор безбедности нуклеарног система у Охају 2003. године када је дошло до паралисања система на 5 часова. *Malware* је стигао путем рачунара једног од извођача који је био конектован на систем и на тај начин заобишао заштитини зид [14]. Срећом електрана је била затворена због редовног одржавања, али се *malware* путем интернета успио пробити и заразити 75 хиљада корисника у року од 10 минута, као и путем *VPN-a* заразити систем контроле електроенергетских компанија и још два интегрисана предузећа [14]. Штета је била преко један билион долара.

6.1.1.3.1 Утицај

Утицај може да буде највећег могућег нивоа на сваку од компоненти, па тако и на целокупни систем. Важно је истакнути да онај ко преузме контролу над целим софтвером, има зле намере, а да при томе зна како софтвер функционише, може и да причини велику материјалну штету и да угрози животе људи. Намерним манипулацијама мрежом и нарушавањем интегритета компоненти SCADA, OMS, EMS, DMS и SSM може да дође до губитка људских живота што поставља утицај на *веома висок* ниво (*Табела 6*). Уколико се наруши интегритет SCADA, EMS и DMS компоненти добијамо систем коме не можемо веровати и на тај начин неискусна посада на терену може да угрози свој живот. Слична ситуација је и код OMS и SSM компоненти, где услед невалидних информација у инциденту и радним налозима последице могу да буду значајне. Такође, са сличном намером осетљиви подаци из MDM компоненте се могу открити, па на тај начин утицај подижемо на *висок ниво* (*Табела 6*). Злонамеран инсајдер, може GIS компоненту довести до стања недоступности, модификације података у оквиру ње и

откривања пословних података што је смешта на *умерени ниво* са аспекта утицаја (*Табела 6*). Брисањем свих акција у систему и читаве историје кроз SIEM и Historical компоненте, корисници од стране регулаторних тела могу да очекују казне. Према *Табела 6*, утицај који се може на овај начин произвести на ове две компоненте је *умереног нивоа*.

6.1.1.3.2 Вероватноћа

Вероватноћа да се реализује дата претња је *ниска*, са обзиром да компаније посвећују пажњу датим ситуацијама ситуацијама кроз безбедносне обуке запослених, сигурносну и физичку изолованост делова компаније и укидање свих креденцијала бившим запосленим (*Табела 5*). Познати напади ове [14][17] врсте су одиграли велику улогу да се вероватноћа реализације сличних напада у будућности сведу на минимум.

Табела 14 - Акумулирана процена ризика за претњу 3

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П3	V V	N	V V	N	V V	N	V V	N	V V	N	V	V N	U	N	U	N	U	N
	U		**U**		**U**		**U**		**U**		**N**		**N**		**N**		**N**	

6.1.1.4 Претња 4 (П4): Злоупотреба недостатка процедура за пријављивање сигурносних слабости

Безбедносне претње проузроковане недостатком процедура за пријављивање сигурносних слабости у директној су вези са свести о безбедости оператера и запослених. У свакој компанији морају да постоје јасне процедуре за пријаву оваквих пропуста.

6.1.1.4.1 Утицај

Утицај који може да настане се не разликује од оног који је процењен у случају недевољне свести и нередовних тренинга оператера и осталих ОТ запослених у *Табела 13*.

6.1.1.4.2 Вероватноћа

Вероватноћа да се реализује дата претња је *ниска* (*Табела 5*). Сматрамо као и у анализи претходних претњи да је сваки запослени у компанији обучен са аспекта безбедности, и да ће пријавити потенцијални проблем.

Табела 15 - Акумулирана процена ризика за претњу 4

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П4	V V	N	V	N	V	N	V	N	U	N	V	N	U	N	U	N	U	N
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	

6.1.1.5 Претња 5 (П5): Крађа корисничких креденцијала и њихова злоупотреба

Претње проузроковане крађом корисничких креденцијала и интерних лозинки спадају у претње са значајним утицајем. Током анализе инсајдерских претњи (*6.1.1.3*) објаснили смо које све злоупотребе могу настати на тај начин, али овде ћемо се осврнути на губитак екстерних лозинки, тј. особља које нема директан приступ операторској соби, али су запослени у ОТ подсистему.

6.1.1.5.1 Утицај

До крађе корисничких креденцијала најчешће долази услед грешке запослених и њихове недовољне безбедносне обуке. Уколико потенцијални нападач дође у посед креденцијала запослених, без *phishing* напада може да компромитује компоненте ЕЕС-а на начин како је описано у случају претње 1 (*6.1.1.1*). Због тога су и нивои утицај исти као код дате претње. Он такође може имати приступ приватној мрежи компаније јер као што је наведено у [133], фирме користе јавну мрежу за приступ приватној како би запослени могли да раде ван канцеларија, те је самим тим обука запослених од изузетне важности.

6.1.1.5.2 Вероватноћа

Верватноћа да се реализује дата претња постоји, али услед правилног коришћења више-факторске аутентификације, тренинга и безбедносних мера, као што су честа потреба за променом лозинке, није висока. Сведоци смо да током *Covid 19* пандемије велики број запослених ради од куће, те да ће се овакав тренд наставити и након пандемије, и да за тај рад користи различите интернет провајдере. Ово свакако повећава вероватноћу да високо мотивисан нападач дође у посед шифре. Један од начина је да ако запослени своје пословне задатке обавља нпр. поред прозора, у стану, ресторану, високо мотивисан нападач може да користи камеру високе резолуције и да сними унос шифре. Такође, уколико запослени не користи неки од алата за безбедно чување лозинки, већ их чува као *plaintext*, оне могу бити компромитоване. Управо због овога вероватноћу да се нешто овако деси не оцењујемо најнижим нивоом, већ *ниским* (*Табела 5*). Чињеница је да компаније константно спроводе обуке запослених где се овакве ситуације истичу и на тај начин образују своје запослене са аспекта безбедности.

Табела 16 - Акумулирана процена ризика за претњу 5

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П5	VV	N	V	N	V	N	V	N	U	N	V	N	U	N	U	N	U	N
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	

6.1.1.6 Претња 6 (П6): Коришћења неадекватног помоћног софтвера

Тема која у последње време иде упоредно са политиком безбедности је свакако коришћење помоћног софтвера као дела целокупног решења и неовлашћене инсталације појединих помоћних алата. Ако помоћни софтвер представља саставни дио неког решења, неопходно је да се инсистира на његовој безбедности. Без обзира колико сигурно решење испоручујете кроз ваш софтвер, помоћни софтвер који користите и који није у вашем власништву представља потенцијалну рањивост и простор за различите врсте злоупотреба. У [134] можемо да видимо који ниво утицаја је проузроковао пропуст у (енг. *Open Secure Sockets Layer*) *OpenSSL*-у, познатији као *Heartbleed* грешка. *OpenSSL* је стандард за безбедну комуникацију на интернету, кога сви користимо, па и критични инфраструктурни системи. Овај пропуст у њему је постојао 3 године и случајно је откривен. Животни циклус безбедног развоја је процес за увођење безбедности у развој производа. Једно од првих питања које треба да се постави креаторима помоћног софтвера је како они обављају ову активност. Компаније са документованим датим процесом смањују ризик од критичних рањивости за 80% [134].

Поред помоћног софтвера који је саставни дио решења, често запослени прибегну коришћењу различитих врста софтвера као помоћ у свакодневном раду. Препорука је да се користе само они софтвери и алати који имају сигурну безбедносну политику и који су одобрени од стране администратора у вашој компанији.

6.1.1.6.1 Утицај

Са обзиром да у овом случају зависимо од грешке запосленог који непажњом може да активира нежељени садржај преузимањем неовлашћеног софтвера на свој рачунар или од пропуста у оквиру помоћног софтвера који је саставни дио решења за управљање паметним ЕЕС, утицај оцењујемо као у случају претње 1 (*Табела 13*). На оба начина је могуће злонамеран *malware* унети и пропагирати кроз систем.

6.1.1.6.2 Вероватноћа

Вероватноћа да се реализује дата претња је *ниска* (*Табела 5*), јер се комапније уз помоћ правних ресурса адекватно заштите у случају нежељених инцидената и неће пристати да користе дати софтвер ако није направљен по свим неопходним безбедносним стандардима. Такође, преузимање неовлаштеног софтвера са интернета је строго забрањено и сматрамо да су запослени адекватно обучени са овог аспекта.

Табела 17 - Акумулирана процена ризика за претњу 6

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П6	VV	N	V	N	V	N	V	N	U	N	V	N	U	N	U	N	U	N
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	

6.1.2 Злоупотреба неадекватно имплементиране безбедносне архитектуре система и софтвера

Основни постулат је да се од самог старта, приликом дизајнирања архитектуре за било који софтвер, а поготово онај који управља критичним инфраструктурним системима треба размишљати о безбедности. Такође, исто важи и за ИКТ инфраструктуру на коју се инсталира дати софтвер. Чест случај је да се на већ готов софтвер и ИКТ инфраструктуру, који се пуштени у продукцију, накнадно решавају озбиљни архитектурални проблеми у вези сајбер безбедности. То као резултат даје неадекватно имплементиране контроле, јер се оне од старта нису узимале у разматрање.

6.1.2.1 Претња 7 (П7): Злоупотреба неадекватне имплементација безбедносних мера између пословног ИТ подсистема и ОТ подисистема

Безбедносне претње проузроковане због неадекватне имплементације безбедносних мера између ИТ подсистема и ОТ подисистема, као и у оквиру самог ОТ подсистема могу да проузрокују значајну штету. ИТ подситем је изложен потенцијалним нападима, док је ОТ подсистем углавном у високој мери изолован. Међутим, уз неадекватну имплементацију мера безбедности између ове две зоне потенцијални *malware* може да се пропагира из пословног подсистема у ОТ подсистем [14][17][18][19] Овде би издвојили Black Energy 3 *malware* [19] који није директно могао да наштети ОТ подсистему, али је извршио прикупљање критичних ОТ системских информација које су на крају омогућиле да се приступи ОТ контролном центру и покрене напад који је довео до нестанка струје код 250 000 потрошача. Овде ћемо се држати става да је зонски модел имплеметиран и да је ОТ подсистем у високој мери изолован. Довољан је један напад на особље путем електронске поруке, да уз интеграцију ИТ и ОТ подсистема са неадекватним мерама безбедности дође до проблема.

6.1.2.1.1 Утицај

Утицај који могу да проузорукује оваква претња је значајан и ми га процењујемо слично као у случају претње која се односи на недостатак и нередовне тренинге запослених о безбедности. На основу тога, сама анализа се не разликује од анализе везане за претњу 1 (*Табела 13*) јер главни начин како се може пропагирати неки потенцијални *malware* је путем *phishing* напада, кроз грешке у дизајну и пропусте у примени одговарајућих мера безбедности.

6.1.2.1.2 Вероватноћа

Вероватноћа да се реализује дата претња је на *ниском* нивоу (*Табела 5*) јер обученост особља и овакве пропусте свака озбиљна компанија мора да реши, што смо и написали током анализе претходних претњи. Поред тога, нисмо изабрали најмањи ниво управо због тога што сматрамо да велики број компанија своју политику безбедности је макар једним делом накнадно имплементирао у односу на инцијалну архитектуру и у таквим случајевима увек постоји ризик да се деси безбедносни проблем. Основни безбедносни постулат код ове врсте система су нивои изолованости.

Табела 18 - Акумулирана процена ризика за претњу 7

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П7	VV	N	V	N	V	N	V	N	U	N	U	N	U	N	U	N	U	N
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	

6.1.2.2 Претња 8 (П8): Злоупотреба безбедносних пропуста у архитектури софтвера

Код великог броја сложених софтверских система у оквиру ЕЕС-а који имају дугачак животни век због трошкова софтвера, обуке и слично, у самом старту инжењери нису имали развијену свест о значају информационе безбедности. Ово је још један од фактора на који би корисници методологије требали обратити пажњу. Због тога безбедност као концепт је додавана накнадно, али то представља погрешан приступ са обзиром да не належе на адекватну инфраструктуру као што би то би случај да се од почетка узела у разматрање. Оваква накнадна имплементација је неадекватна и са мноштвом потенцијалних рањивости. Није редак пример да се многе безбедносне мере накнадно имплементирају са обзиром на природу галопирајућег раста сајбер претњи и безбедности. *Malware Xavex* [22] се проширио компромитујући инсталационе датотеке популарних софтверских производа за даљински приступ који се користе у ОТ окружењима. Када су корисници инсталирали оно што су мислили да је оригиналан софтвер, они су несвесно инсталирали и дати злонамеран код који је проузроковао значајну штету.

6.1.2.2.1 Утицај

Неадекватна иницијална безбедносна архитектура свакако има велики утицај на сам систем, јер је несумљиво простор за различите злоупотребе. Спектар злоупотреба је широк, тако да ви било немогуће навести све потенцијалне утицаје који могу настати као резултат овога пропуста, али морамо издвојити неке. Због тога, утицај ћемо проценити исто као у случају претње 1 (*Табела 13*).

6.1.2.2.2 Вероватноћа

Ниво вероватноће да се испоручи софтвер са неадекватном безбедносном архитектуром је као и у претходном примеру *низак* према *Табела 5*.

Табела 19 - Акумулирана процена ризика за претњу 8

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L

П8	V V	N	V	N	V	N	V	N	U	N	U	N	U	N	U	N	U	N
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	

6.1.2.3 Претња 9 (П9): Злоупотреба критичних грешки у софтверу, нпр. Buffer overflow

Последице *Buffer overflow* напада зависе и од тога који од програмских језика се користи. C и C++ су доста подложнији, док конкретно C# има сигурносне механизме који смањују вероватноћу уноса слабости ове врсте. Приликом развоја апликације, поред ових заштитних механизама, инжењери често користе и као заштиту рандомизацију меморијског простора, насумично се крећући по локацијама адресног простора. Да би се извршио овај напад, нападачи морају знати локацију извршног кода, а насумично постављање адресних простора то чини готово немогућим.

Нападачи користе проблеме са преливањем бафера преписивањем меморије апликације. Ово мења путању извршења програма, покрећући злонамерни код. На пример, нападач може да уведе додатни код, шаљући нова упутства апликацији за добијање приступа или издавање команди.

6.1.2.3.1 Утицај

Овде може доћи до откривања личних података и недоступности свих компоненти [133] те ћемо утицај оценити као у случају претње 1 (*Табела 13*).

6.1.2.3.2 Вероватноћа

Са обзиром да је ОТ подсистем у високој мери изолован и велики број потребних информација да би се извршио овај напад, вероватноћа да се на овај начин компромитују компоненте и систем је *ниска* (*Табела 5*).

Табела 20 - Акумулирана процена ризика за претњу 9

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П9	V V	N	V	N	V	N	V	N	U	N	U	N	U	N	U	N	U	N
	U		**N**		**N**		**N**		**VN**		**VN**		**VN**		**VN**		**VN**	

6.1.2.4 Претња 10 (П10): Неауторизовано брисање фајлова (нпр. dll, .exe)

Неауторизовано брисање фајлова може довести до делимичне недоступности система. Оно што је важно напоменути да кроз овај напад не долази до нарушавања интегритета или откривања осетљивих података.

6.1.2.4.1 Утицај

Утицај који могу овакве претње да изазову ако се реализују је *веома висок* за SCADA-у. Услед њене недоступности систем је значајно афектован (*Табела 6*). Угрожавање DMS и EMS компоненти може проузроковати *висок* утицај јер нећемо

имати основне електроенергетске функције, које припадају домену критичних сервиса (*Табела 6*). Недоступност OMS компоненте може да доведе до временски неприхватљивих испада, што проузрокује високе финансијске трошкове и губитак угледа, те утицај код ове компоненте оцењујемо као *висок* (*Табела 6*). Остале компоненте не спадају у домен критичних, те њихова недоступност према табели *Табела 6* проузрокује *умерен* ниво утицаја.

6.1.2.4.2 Вероватноћа

Вероватноћа да се реализује ова претња је *ниска* (*Табела 5*), са обзиром на изолованост локације на којој се налазе фајлови и чињенице да је прва и основна контрола која се користи у овим случајвима листа контроле приступа, јер је једноставна, а веома ефикасна.

Табела 21 - Акумулирана процена ризика за претњу 10

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П10	VV	N	V	N	V	N	V	N	U	N	U	N	U	N	U	N	U	N
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	

6.1.3 Злоупотреба неадекватних закрпа за софтвер и оперативни систем

Закрпе у овом типу софтвера (енг. *Patches*) нису ретка појава са обзиром да се ради о веома комплексном решењу које захтева константна унапређења. Слично је и са оперативним системима, све чешће добијамо нотификације да је пристигла закрпа коју треба ажурирати.

6.1.3.1 Претња 11 (П11): Безбедносне претње проузроковане недовољним тестирањем приликом примене нових закрпа (енг. patches) или софтверске грешке након испорученог софтвера.

Сваки инжењер који ради на развоју софтвера, а поготово оног који управља критичним инфраструктурним системима, зна колико често се од њега захтева решавање грешака у софтверу у што краћем року са обзиром на природу таквих система и потребу за њиховом готово константном доступношћу. Фирме које развијају софтвер управо због овога улажу значајне ресурсе на функционално и регресионо тестирање. Решење се тестира у оквиру самог тима, приликом развоја, затим у посебно специјализованим тимовима за ту сврху и на крају код самог корисника се прво инсталира и тестира на тест систему клијента, па тек када је верификовано кроз разне сценарије, примењује се у продукцији. Уколико се открије потенцијални проблем што раније на овој путањи, његово сређивање ће бити јефтиније и мање фрустрирајуће за корисника.

6.1.3.1.1 Утицај

У зависности од безбедносног проблема који је унесен утицај може да се креће од *веома ниског* до *веома високог* нивоа. Разлика у односу на већину претходних претњи, је

што овде инжењер услед грешке може да доведе компромитовања осетљивих информација као што су логови, историјски подаци, персонални подаци, подаци о радним налозима или радницима на терену, подаци о инцидентима, подаци о опреми и тд. Да не би појединачно за сваку компоненту анализирали скуп потенцијалних безбедносних пропуста, узећемо и сценарио где услед безбедносних пропуста може доћи до недоступности сваке од компоненти, нарушавања интегритета, високих казни од стране регулаторних агенција и на крају до губитка поверења од стране корисника. Регулаторна тела посебну пажњу посвећују безбедности, а и поверење корисника се лакше губи услед безбедносних пропуста. Према *Табела 6* недвосмислено можемо рећи да је ниво утицаја веома *висок* код SCADA, DMS, EMS, SSM и OMS компоненти јер спадају у домен критичних и чињенице колико су доступност и интегритет таквих компоненти важни за критичне инфраструктурне системе. Уколико се наруши интегритет SCADA, EMS и DMS компоненти добијамо систем коме не можемо веровати и на тај начин неискусна посада на терену може да угрози свој живот. Слична ситуација је и код OMS и SSM компоненти, где услед невалидних информација о инциденту и радним налозима последице могу да буду катастрофалне. MDM због осетљивих личних података се налази на нивоу високог утицаја, док су остале компоненте на умереном нивоу. Злонамеран инсајдер, може GIS компоненту довести до стања недоступности, модификације података у оквиру ње и откривања пословних података што је смешта на *умерени ниво* са аспекта утицаја. Брисањем свих акција у систему и читаве историје кроз SIEM и Historical компоненте, корисници од стране регулаторних тела могу да очекују казне.

6.1.3.1.2 Вероватноћа

Поред свих претходно споменутих провера, вероватноћа да се ова претња реализује је *ниска* за сваку од компоненти (*Табела 5*). Нисмо одабрали најмањи ниво вероватноће због комплексности датог система и постојања ризика да се због много афектованих делова софтвера нешто не истестира до краја.

6.1.3.2 Претња 12 (П12): Злоупотреба безбедносних недостатака у новим закрпама софтвера

Препоруке [8] су да се сигурносне процене и ревизије система требају редовно извршавати разним активностима (нпр. тестирање продора, процене рањивости) како би обезбедили да систем буде заштићен од рањивости, погрешних провера и разних видова напада.

Слично као и у претходној претњи где смо били усмерени на функсионалне пропусте, безбедносни пропуст је у директној вези за недовољним тестирањем софтвера. Као што сам већ напоменуо, због природе и комплексности система некада велики број тестних корака и провера кроз више нивоа не може да открије потенцијални проблем.

6.1.3.2.1 Утицај

Овакав вид анализе између осталог користимо јер за сваку од компоненти постоји више различитих врста потенцијалних проблема, па због тога узимамо сценарио са највећим ризиком. Управо због тога ћемо анализу усмерити на то какав би утицај проузроковала недоступност или неадекватан рад свих компоненти као у случају претходне претње.

6.1.3.2.2 Вероватноћа

Вероватноћа реализације ове претње сматрамо да је *ниска* са обзиром на висок акценат који се ставља на тестирање овог типа система (*Табела 5*).

Табела 22 - Акумулирана процена ризика за претње 11 и 12

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П11	VV	N	VV	N	VV	N	VV	N	VV	N	V	N	U	N	U	N	U	N
	U		**U**		**U**		**U**		**U**		**N**		**N**		**N**		**N**	
П12	VV	N	VV	N	VV	N	VV	N	VV	N	V	N	U	N	U	N	U	N
	U		**U**		**U**		**U**		**U**		**N**		**N**		**N**		**N**	

6.1.3.3 Претња 13 (П13): Злоупотреба дугорочних недостатака безбедносних закрпа за оперативни систем

Поред безбедносних закрпа које су намењене за софтвер постоје и оне које се односе на оперативни систем. Сведоци смо да са времена на време добијемо обавештење да инсталирамо нове безбедносне закрпе за оперативни систем и веома је важно да се пробуди свест код корисника да се те исте закрпе редовно примењују. Високо обучени нападачи овакве пропусте могу да искористе да наруше нормално функционисање целокупног паметног ЕЕС-а. Један од најпознатијих напада који је искористио рањивост оперативног система је *Stuxnet* [17] да би се проширио пронашао инжењерски софтвер *Siemens STEP7*. Када је пронашао овај пакет, заменио је комуникационе библиотеке система тако што је подметнуо своје пројектне датотеке. Ово је омогућило вирусу да суптилно промени програм који ради на одређеним *Siemens* (енг. *Program Logic Controller*) PLC-ма, док је промене сакрио од оператера. Да је изводљиво и са коликим утицајем искористити пропусте због застарелих закрпа оперативног система показује и напад *WannaCry Ransomware* [133] током кога је 12.05.2017. заражено више од 200 000 рачунара чији подаци су криптовани и од валсника је тражен њихов откуп. Уколико се форензичком анализом утврди да је проблем заиста услед грешке у самом оперативном систему, незадовољство корисника и репутација компаније могу се ублажити чињеницом да проблем није настао услед грешке у софтверу.

6.1.3.3.1 Утицај

Утицаји који се на овај начин могу манифестовати,тј. компромитујући оперативни систем су усмерени на откривање информација и нарушавање недоступности паметног електроенергетског система. Сходно томе, ниво утицаја је као у случају претње 1 (*Табела 13*).

6.1.3.3.2 Вероватноћа

Вероватноћа да се нешто овако деси за већину компоненти је на *умереном* нивоу управо због све учесталијих ситуација са безбедносним недостацаима оперативних система [17][19][133]. Мања је вероватноћа да ће циљ напада бити усмерен на компоненте као што су GIS, SIEM и Historian, те због њихове неатрактивности из угла потенцијалног нападача према *Табела 5* ниво вероватноће оцењујемо као низак.

Табела 23 - Акумулирана процена ризика за претњу 13

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П13	V V	U	V	U	V	U	V	U	U	U	V	N	U	N	U	U	N	U
	V		U		U		U		U		U		N		N		N	

6.1.4 Злоупотреба конфигурационих података у оквиру ОТ подсистема

Под конфигурационим подацима подразумевамо почетне вредности одређених параметара у оквиру компоненти паметног електроенергетског система.

6.1.4.1 Претња 14 (П14): Нарушавање поверљивости конфигурационих података

Поверљивост представља ставку *CIA* тријаде која у последње време добија на значају. У оквиру критичних инфраструктурних система концентрација ових података је углавном у оквиру ИТ подсистема, међутим треба бити пажљив и приликом анализе и података из ОТ дела, јер и у њима постоје подаци чије откривање може имати значајан утицај на незадовољство корисника, имиџ компаније и финансијксе губитке у виду великих казни од стране регулаторних тела. Утицај у виду оштећења опреме, повреда и губитака људских живота није реално да настане као експлоатација ових података.

6.1.4.1.1 Утицај

Почећемо од нарушавања поверљивости конфигурационих података. Када би потенцијални нападач имао увид у конфигурационе фајлове, без опције да их брише и модификује, већ само да их чита у већини компоненти не би дошао до осетљивих података које би могао искористити, те је због тога утицај на *веома ниском* нивоу (*Табела 6*) Изузетак су MDM и GIS компоненте, где постоји ризик да се ови подаци злоупотрбе јер се у њима могу наћи информације о потрошачима и опреми. Нпр. информација о каталозима паметних бројила, регијама, идентификационим бројевима паметних бројила, и низ других информација. Због свега наведеног, утицај који се може проузроковати на MDM и GIS је на *умереном* нивоу.

6.1.4.1.2 Вероватноћа

Вероватноћа да се приступим овим фајловима и открију подаци је *ниска* (*Табела 5*) из разлога што се налазе у изолованим зонама и минимално су заштићени листама за контролу приступа. Често имају додатну заштиту у виду потребних креденцијала да би им се приступило.

6.1.4.2 Претња 15 (П15): Нарушавање доступности конфигурационих података

Доступност конфигурационих подататака је важна, али и уколико они постану недоступни премостива је, јер се ова недоступност може лако надокнадити директним

уписивањем вредности за ове податке коришћењем помоћних алата или резервних копија.

6.1.4.2.1 Утицај

Наиме, као што је речено ови подаци су већином почетне вредности за различите промењљиве које се због перформанси учитају у интерну меморију која касније служи као основа за различите прорачуне. Недоступност ове меморије би био велики проблем, али самих конфигурационих података није. Наравно, све зависи како је софтвер имплементиран и шта се све од података чува у датим фајловима. У неким случајевима, када сам софтвер много зависи од саме конфигурације свакако да њена недоступност јесте проблем, али водићемо се тиме да је решење имплементирано на адекватан начин и рећи да је утицај максимално на *умереном* нивоу, и то у случају SCADA-е, где уколико дође до макар малог кашњења, па макар то и био проблем са овим фајловима може да се одрази на целокупни систем. Код осталих компоненети сматрамо да је утицај на *ниском* нивоу (*Табела 6*).

6.1.4.2.2 Вероватноћа

Вероватноћа да се приступим овим фајловима је *ниска* из разлога што се налазе у изолованим зонама и минимално су заштићени листама за контролу приступа. Често имају додатну заштиту у виду потребних креденцијала да би им се приступило.

6.1.4.3 Претња 16 (П16): Нарушавање интегритета конфигурационих података

6.1.4.3.1 Утицај

Од свих аспеката CIA тријаде у контексту конфигурационих фајлова, нарушавање интегритета делује као најризичнији сценарио. Замислимо сценарио где се неке почетне вредности на SCADA-и модификују на тај начин да када крене процесирање изазову неочекиване резултате или недоступност. Сличним приступом и код осталих компоненти је могуће доћи до њихове недоступности и невалидних резултата што представља утицај на нивоу претње 1 (*Табела 13*).

6.1.4.3.2 Вероватноћа

Вероватноћа да се приступим овим фајловима и модификују подаци је *ниска* (*Табела 5*) као у случају претходне две претње, из разлога што се налазе у изолованим зонама и минимално су заштићени листама за контролу приступа. Често имају додатну заштиту у виду потребних креденцијала да би им се приступило.

Табела 24 - Акумулирана процена ризика за претње 14, 15 и 16

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П14	V N	N	V N	N	V N	N	V N	N	V N	N	U	N	U	N	V N	N	V N	N
	VN		**VN**		**VN**		**VN**		**VN**		**N**		**N**		**VN**		**VN**	
П15	U	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
	N		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	

П16	V V	N	V	N	V	N	V	N	U	N	V	N	U	N	U	N	U	N
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	

6.1.5 Злоупотреба логованих података у оквиру ОТ подсистема

Слично као код конфигурационих података, свака компонента има свој фајл у који се уписују акције које се дешавају у оквиру ње. Поред појединачних фајлова, постоје и они заједнички у којима се записују важне поруке током рада самог система. Разлог за постојање оваквих порука је вишеструк, од тога да регулаторна тела инсистирају на постојању ових информација због потенцијалних форензичких анализа и реконструкције рада самог система, те због помоћи инжењерима да лакше репродукују пријављене проблеме [126][135]. Са овим подацима треба бити обазрив из два разлога. Први је да се мора водити свест о безбедности и само логовати оно што је заиста неопходно, без откривања осетљивих информација, док са друге стране не смемо да претерамо са количином ових информација јер то може да наруши перформансе самог система. Да би избегли превелики број логованих података у овим фајловима, углавном се уводе нивои логовања, где се у зависности од активног нивоа логују информације одређеног нивоа критичности (нпр. критична грешка, грешка, информација). На овај начин се подаци који су неопходни за разне реконструкције могу ставити у нивое који нису аутоматски укључени, већ се у циљу поновне репродукције проблема укључују.

6.1.5.1 Претња 17 (П17): Нарушавање поверљивости логованих података

Уколико се у логовима морају наћи осетљиви лични или пословни подаци, препорука је да се ради анонимизација тих података тако да буду нечитљиви за злонамерног нападача уколико би дошао у њихов посед.

6.1.5.1.1 Утицај

Оно што се дефинитивно може прочитати из овог типа фајлова је понашање система, и ове информације се могу искористити за припрему потенцијалних напада. Ово се углавном односи на критичне компоненте са аспекта рада у реалном времену, као што су SCADA, DMS, EMS, те због тога код њих утицај процењујемо као умерен (*Табела 6*). Код осталих компоненти је утицај који би се проузроковао њиховим откривањем на *ниском* нивоу (*Табела 6*) са обзиром да адекватно обучени инжењери са аспекта безбедности неће у ове фајлове уписати осетљиве податке о потрошачима или опреми.

SIEM компонента представља све присутнији модул у оквиру паметних електроенергетских система. Њена улога је вишеструка, али примарна је свакако да води бригу о идентификацији потенцијалних проблема у оквиру система. Она надгледа саме логове и на основу њихове модификације и неуобичајног логовања, догађаја, аларма идентификује потенцијалне проблеме и нападе. Њена позиција је често између пословног и ОТ подсистема, али може да буде по једна SIEM компонента у оба подситема. Може бити атрактивна за потенцијалног нападача да је онеспособи пре било каквог напада.

6.1.5.1.2 Вероватноћа

Вероватноћа да се приступим овим фајловима и открију подаци је *ниска* (*Табела 5*) из разлога што се налазе у изолованим зонама и минимално су заштићени листама за

контролу приступа. Често имају додатну заштиту у виду потребних креденцијала да би им се приступило.

6.1.5.2 Претња 18 (П18): Нарушавање доступности логованих података

6.1.5.2.1 Утицај

Нарушавање доступности логова не може да угрози људске животе, доведе до оштећења опреме и имовине, али недвосмислено имају утицај на потенцијалне казне од стране регулаторних тела, па самим тим и нарушавање имица компаније. Услед недоступности логова, изгубиће се подаци који би у томе моменту били логовани, што значи да сами логови неће бити потпуни. Регулаторне агенције свакако неће бити благонаклоне на ово и због тога утицај за све компоненте је на *умереном* нивоу (*Табела 6).*

6.1.5.2.2 Вероватноћа

Вероватноћа да се приступим овим фајловима је *ниска* (*Табела 5*) из разлога што се налазе у изолованим зонама и минимално су заштићени листама за контролу приступа. Често имају додатну заштиту у виду потребних креденцијала да би им се приступило.

6.1.5.3 Претња 19 (П19): Нарушавање интегритета логованих података

6.1.5.3.1 Утицај

Слично као у случају недоступности, нарушавање интегритета логова не може да угрози људске животе, доведе до оштећења опреме и имовине, али се могу очекивати казне од стране регулаторних тела због невалидних логова којима се не може веровати, па самим тим долази и до нарушавање имица компаније. Регулаторне агенције свакако неће бити благонаклоне на ово и због тога утицај за све компоненте је на *умереном* нивоу (*Табела 6*).

6.1.5.3.2 Вероватноћа

Вероватноћа да се приступим овим фајловима и модификују подаци је *ниска* (*Табела 5*) из разлога што се налазе у изолованим зонама и минимално су заштићени листама за контролу приступа. Често имају додатну заштиту у виду потребних креденцијала да би им се приступило.

Табела 25 - Акумулирана процена ризика за претње 17, 18 и 19

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П17	U	N	U	N	U	N	N	N	U	N	N	N	N	N	N	N	N	N
	N		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	
П18	U	N	U	N	U	N	U	N	U	N	U	N	U	N	U	N	U	N
	N		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	
П19	U	N	U	N	U	N	U	N	U	N	U	N	U	N	U	N	U	N
	N		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	

6.1.5.4 Претња 20 (П20): Безбедносне претње проузроковане непорецивости акција у оквиру ОТ подсистема

Ова претња је у директној вези са претходно две анализиране претње које се односе на недоступност и модификацију логованих података. На оба начина може доћи до непотпуних и невалидно записаних акција у оквиру система и то директно омогућава порецивост коју овде разматрамо.

6.1.5.4.1 Утицај

Безбедносне претње проузроковане услед непорецивости акција у оквиру компоненти, а самим тим и система могу да имају значајан утицај јер регулаторна тела током контрола раде форензику записаних акција у систему и ако су такви подаци неадекватни то може да доведе до казни и финансијских губитака, те је због тога утицај *умереног* нивоа (*Табела 6*) код свих компоненти.

6.1.5.4.2 Вероватноћа

Вероватноћа да се овако нешто деси је *ниска* (*Табела 5*) из разлога што је потенцијалном нападачу примарно да се фокусира на сам напад, а не на прикривање трагова. Такође, сваки траг се налази у фајловима где се чувају логови који служе за праћење рада система и они су заштићени листама за контролу приступа као и често додатном заштиту у виду неопходних креденцијала да би им се приступило.

Табела 26 - Акумулирана процена ризика за претњу 20

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П20	U	N	U	N	U	N	U	N	U	N	U	N	U	N	U	N	U	N
	N		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	

6.1.6 Злоупотреба операционих података у оквиру ОТ подсистема

Оно што је специфично за операционе податке јесте да је пут до њиховог експлоатисања веома тежак, зато што су то углавном динамички подаци смештени у RAM меморији. Оперативни подаци могу бити вредности напона, струјна оптерећења трансформатора, локације кварова, статус прекидача, информације о алармима и догађајима у систему [99][133]. Такође, они захтевају висок ниво безбедности за заштиту паметне мреже да не би дошло до нестанка струје и других нежељених утицаја [133].

6.1.6.1 Претња 21 (П21): Нарушавање поверљивости операционих података

Операциони подаци се користе углавном за различите електроенергетске прорачуне и код већине компоненти не садрже осетљиве податке.

6.1.6.1.1 Утицај

Подаци овог типа који се користе у оквиру SCADA компоненете садрже информације о статусима различитих врста мерења са терена и као такви не користе много потенцијалном нападачу. Према *Табела 6* утицај је на ниском *нивоу* јер нема бојазни од финансијских издатака уколико се открију. Слична ситуација је у случају DMS, EMS, OMS и SSM компоненти. Прве две компоненте на почетку свога рада учитавају целокупни мрежни модел, али је веома тешко наћи релације између тих података па су практично неупотребљиви. OMS и SSM операциони подаци могу у траговима да садрже информације о опреми, посади на терену, инцидентима, али такође због њихове релације у оквиру интерне меморије нису претерано од значаја.

За разлику од претходних компоненти, GIS и MDM могу пронаћи информације о потрошачима и опреми те на основу *Табела 6* утицај оцењујемо као *умерен*.

Исти ниво утицаја имају SIEM и Historian компоненте. SIEM садржи осетљиве пословне податке о различитим активностима у оквиру система као што су аларми и догађаји, док операциони подаци Historian компоненте представљају податке спремне за архиву који не могу директно да утичу на функционисање система, али су осетљиви пословни подаци.

6.1.6.1.2 Вероватноћа

Вероватноћа да дође до нарушавања тајности ове врсте података је *ниска* (*Табела 5*) јер се подаци налазе у оперативној меморији компоненти које су адекватно изоловане. Такође, и ако би потенцијални нападач дошао у посед ових података тешко би могао да направи релацију између њих и конструише праву слику.

6.1.6.2 Претња 22 (П22): Нарушавање доступности операционих података

Иако не припада домену електроенергетских система, догађај [24] је пример где је услед недоступности SCADA система дошло до експлозије у којој су погинуле три особе, осам особа је повређено и нанета је немерљива штета околини и животној средини. Сви ови догађаја несумњиво говоре о значајним последицама које се дешавају услед неадекватне заштите критичних инфраструктурних система, па и OT подистема као његовог дела.

6.1.6.2.1 Утицај

Нарушавање доступности ових података је значајније у односу на њихово откривање. Услед недоступности операционих података и компоненте постају недоступне. Видели смо кроз анализу претње 1 (*Табела 13*) и сличних који утицај на целокупан систем може да буде на основу недоступности компоненти и такав утицај ћемо усвојити и случају ове претње.

6.1.6.2.2 Вероватноћа

Вероватноћа да дође до нарушавања доступности ове врсте података је *ниска* (Табела 5) јер се подаци налазе у оперативној меморији компоненти које су адекватно изоловане и због обучености особља и адекватне безбедносне архитектуре тешко да може да се кроз мрежу пропагира злонамеран код који би довео до недоступности ових података.

6.1.6.3 Претња 23 (П23): Нарушавање интегритета операционих података

6.1.6.3.1 Утицај

Дефинитивно, највећи утицај у случају операционих података ће бити уколико се наруши њихов интегритет. До повреде, или губитка људских живота може да дође у случају невалидних прорачуна на основу SCADA мерења, која директно утичу на EMS и DMS прорачуне и невалидне резултате. Овде се прави низ неадекватних резултата који и у оквиру самог OMS-а могу да предложе невалидне кораке за повратак енергизације што директно угрожава живот радника. Уколико се модификују подаци у радним и безбедносним налозима SSM компоненте, те уколико неадекватно обучена особа крене у поправку мреже на основу тих упустава директно угрожава свој живот. Утицај на све ове компоненте и самим тим на целокупан систем је на *веома високом* нивоу (*Табела 6*). Модификација података у оквиру MDM компоненте не може угрозити људске животе, али може довести до незадовољства потрошача што представља *умерени* утицај (*Табела 6*).

Нарушавањем интегритета GIS компоненте може довести до недоступности ове компоненте и невалидних података што представља такође *умерени* утицај (*Табела 6*). Брисањем свих акција у систему и читаве историје кроз SIEM и Historical компоненте, власници DSO од стране регулаторних тела могу да очекују казне. Према *Табела 6*, утицај који се може на овај начин произвести на ове две компоненте је *умереног нивоа*.

6.1.6.3.2 Вероватноћа

Вероватноћа да дође до нарушавања интегритета ове врсте података је *ниска* (*Табела 5*) јер се подаци налазе у оперативној меморији компоненти које су адекватно изоловане и због обучености особља и адекватне безбедносне архитектуре тешко да може да се кроз мрежу пропагира злонамеран код који би довео до недоступности ових података.

Табела 27 - Акумулирана процена ризика за претње 21, 22 и 23

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П21	N	N	N	N	N	N	N	N	N	N	U	N	U	N	U	N	U	N
	N		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	
П22	V V	N	V	N	V	N	V	N	U	N	V	N	U	N	U	N	U	N
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	
П23	V V	N	V V	N	V V	N	V V	N	V V	N	U	N	U	N	U	N	U	N
	U		**U**		**U**		**U**		**U**		**N**		**N**		**N**		**N**	

6.1.6.4 Претња 24 (П24): Безбедносне претње проузроковане неисправношћу опреме, нпр. лажна мерења сензора

Наредна претња није директно везана за софтвер, већ за опрему. Важно је напоменути да постоји вероватноћа да почну стизати лажна мерења са појединих уређаја, међутим, исто тако на SCADA компоненти постоје детекције невалидних података.

6.1.6.4.1 Утицај

У случају да нема ове детекције, анализа би се усмерила на нарушавање интегритета SCADA, DMS, OMS, EMS, SSM компоненти што на основу претходно анализиране претње представља веома висок утицај. Услед неисправности опреме везане за AMI инфраструктуру, може доћи и до невалидних података у самој MDM компоненти, али пошто ти подаци могу само да проузрокују незадовоство потрошача услед невалидних рачуна за електричну енергију, према *Табела 6* је *умереног* нивоа. Неисправност опреме не утиче директно на функционисање GIS, SIEM и Historical компоненти, па због тога је потенцијални утицај код њих *веома ниског* нивоа.

6.1.6.4.2 Вероватноћа

Због постојања различитих врста детектора ових појава и валидатора мерења пристиглих са поља [99], вероватноћу реализације дате претње оцењујемо *ниским* нивоом према *Табела 5*.

Табела 28 - Акумулирана процена ризика за претњу 24

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П24	V V	N	V V	N	V V	N	V V	N	V V	N	U	N	V N	N	V N	N	V N	N
	U		U		U		U		U		N		VN		VN		VN	

6.1.7 Злоупотреба личних података у оквиру ОТ подсистема

Чување личних података је увек било високоприотитетно, а сведоци смо да се у последње време овом изазову даје на значају [38][83].

6.1.7.1 Претња 25 (П25): Нарушавање поверљивости личних података

У скоро свим врстама софтвера значајан утицај може да се поузрокује уколико неко дође у посед осетљивих личних података корисника. Не треба посебно објашњавати колико незадовољство потрошача и нарушавање имиџа компаније ово може да проузрокује.

6.1.7.1.1 Утицај

Када причамо о критичним инфраструктурним системима, лични подаци су углавном смештени у пословни подсистем који није у фокусу у овој докторској дисертацији. Међутим компонетне као што су OMS и MDM предњаче по броју оваквих података у самом ОТ подсистему, јер садрже осетљиве податке о потрошачима, те код њих утицај

оцењујемо као *веома висок* (*Табела 6*). Утицај код свих осталих компоненти је на *веома ниском* нивоу, без обзира да ли се ради о откривању, недоступности или модификацији, јер у њима, као што је речено не постоје лични подаци који би могли бити компромитовани.

6.1.7.1.2 Вероватноћа

Ови подаци се могу наћи у RAM меморији, или диску, али са обзиром да је због изолованости OT подсистема и низа контрола које мора да има имплементиране свака озбиљна компанија ово практично немогуће, вероватноћу да се они открију оцењујемо као *ниску* (*Табела 5*).

6.1.7.2 Претња 26 (П26): Нарушавање доступности личних података

6.1.7.2.1 Утицај

Недоступност и модификација личних података не утиче на функционисање OMS и MDM компоненте, јер се они не користе за директне прорачуне, већ су више информативног карактера, па тако можемо рећи да је утицај и за њих у овом случају на *веома ниском* нивоу (*Табела 5*).

6.1.7.2.2 Вероватноћа

Ови подаци се могу наћи у оперативној меморији, или диску, али са обзиром да је због изолованости OT подсистема и низа контрола које мора да има имплементиране свака озбиљна компанија ово практично немогуће, вероватноћу да се они учине недоступним оцењујемо као *ниску* (*Табела 5*).

6.1.7.3 Претња 27 (П27): Нарушавање интегритета личних података

6.1.7.3.1 Утицај

Модификација личних података у оквиру OMS и MDM компоненте може да проузорокује проблеме у пословном делу приликом креирања рачуна за потрошњу што директно утиче на задовољство потрошача. Због тога према *Табела 6* утицај оцењујемо као *умерен*.

6.1.7.3.2 Вероватноћа

Ови подаци се могу наћи у оперативној меморији, или диску, али са обзиром да је због изолованости OT подсистема и низа контрола које мора да има имплементиране свака озбиљна компанија ово практично немогуће, вероватноћу да се они модификују оцењујемо као *ниску* (*Табела 5*).

Табела 29 - Акумулирана процена ризика за претње 25, 26 и 27

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П25	VN	N	VN	N	VN	N	VV	N	VN	N	VV	N	VN	N	VN	N	VN	N
	VN		**VN**		**VN**		**U**		**VN**		**U**		**VN**		**VN**		**VN**	

П26	V N	N	V N	N	V N	N	V N	N	V N	N	V N	N	V N	N	V N	N	V N	N
	VN		**VN**		**VN**		**VN**		**VN**		**VN**		**VN**		**VN**		**VN**	
П27	V N	N	V N	N	V N	N	U	N	V N	N	U	N	V N	N	V N	N	V N	N
	VN		**VN**		**VN**		**N**		**VN**		**N**		**VN**		**VN**		**VN**	

6.1.8 Напади усмерени на комуникациону мрежу у оквиру OT подсистема

6.1.8.1 Претња 28 (П28): Безбедносне претње проузроковане DoS/DDoS нападима на комуникациону мрежу и позадинске сервисе

Једна од најраспрострањенијих претњи за нарушавање доступности компоненти паметног ЕЕС-а је DoS, односно DDoS напад [14]. Ако изађемо из оквира критичних инфраструктурних система и анализирамо начин како се извршава DDoS напад, долазимо до тога да је први корак прављење бот мреже од рачунара различитих заражених корисника, који су потенцијални *malware* унели у свој рачунар путем електронске поште или на неки други начин. Након што се направи бот мрежа, креће велики број захтева на одговарајућу компоненту. Са обзиром да се ради о OT подсистему који је у високој мери изолован, и у продукцији нема излаз на интернет овако нешто у овом обиму је неизводљиво.

6.1.8.1.1 Утицај

Ипак, постоји начин да се изврше ови напади, али у мањем обиму. Конкретно за SCADA-у, могуће је извршити DoS напад [137], али да неко физички приступи RTU уређају у пољу, прикључи свој лаптоп или други уређај и крене да шаље велики број података. Уколико се компромитује већи број RTU-ова онда то можемо сматрати DDoS нападом. Утицај би био да се SCADA сервис онеспособи и то би имало висок утицај на целокупни систем. Ово је физички изводљиво и мотивација потенцијалног нападача је велика. Такође је могуће извести овај напад на MDM компоненту [136] и на тај начин поремтити рад мреже, опертера и трећих страна којима су ови подаци потребни. Са обзиром да услед ове врсте напада може да дође до недоступности компоненти утицај за сваку од њих оцењујемо као у случају претње 1 (*Табела 13*).

6.1.8.1.2 Вероватноћа

Ипак, вероватноћу да се деси овако нешто оцењујемо као *умерену* у случају SCADA и MDM компоненте, због тога што постоје познати подвизи које је могуће покренути уколико имамо физички приступ систему (*Табела 5*). Што се тиче осталих компоненти и њихових сериса вероватноћа да се реализује ова врста напада је *ниска*, са обзира на изолованост.

Табела 30 - Акумулирана процена ризика за претњу 28

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L

П28	V V	U	V	N	V	N	V	N	U	N	U	U	U	N	U	N	U	N
	V		**N**		**N**		**N**		**N**		**U**		**N**		**N**		**N**	

6.1.8.2 Претња 29 (П29): Безбедносне претње настале услед прекида рада мреже нпр. отказом рутера

6.1.8.2.1 Утицај

Паметни електроенергетски системи се базирају на непрекидној комуникацији у реалном времену. Услед престанка рада мреже, софтвер не може да фунцкионише на прави начин и да дође до кратотрајног прекида у напајању, што је према *Табела 6* утицај на SCADA, DMS, EMS, OMS компоненту је *умереног* нивоа. Утицај на остале компоненте ће бити *ниског* нивоа, јер ће се систем врло брзо након опоравка мреже или преласка на резервну варијанту вратити у првобитно стање.

6.1.8.2.2 Вероватноћа

Вероватноћа је *ниска* (*Табела 5*), пошто се зна који се проблем може проузроковати па зато се мрежи и посвећује посебна пажња и углавном постоје резервне комуникационе варијанте, најчешће дупла мрежа. Пошто ово зависи од хардвера код кога постоји ризик да се деси проблем, вероватноћа није на најмањем могућем нивоу, већ ћемо је оценити са нивоом *низак*.

Табела 31 - Акумулирана процена ризика за претњу 29

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П29	U	N	U	N	U	N	U	N	N	N	N	N	N	N	N	N	N	N
	N		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	

6.1.8.3 Претња 30 (П30): Безбедносне претње настале услед намерног оптерећење мреже манипулацијом потрашачких уређаја

Манипулација потрошачким уређајима је уз физички приступ или удаљено. Манипулација овим уређајима може да доведе до оптерећења система и представља један вид DoS/DDoS напада. Пандам овоме би било понашање система у случају олуја и неверемена када се генерише велики број различитих догађаја. Пре пуштања у продукцију врши се тестирање софтвера у овом моду и ту постоје предефинисани догађаји који могу да се десе током олује. Догађај у националној лабораторији (енг. *Idaho National Laboratory*) INL [20] показао је како напад на електричну мрежу може физички да оштети генераторе и има импакт на систем. Нападнут је заштитни релеј који је затим коришћен за стално затварање и отварање прекидача који повезује генератор на мрежу[20]. Стално затварање прекидача када генератор није био синхронизован са решетком узроковало је оптерећење мреже и уништење генератора [20].

6.1.8.3.1 Утицај

Овакав сценарио може проузроковати креирање великог броја инцидената у оквиру OMS компоненте и на тај начин је значајно оптеретити. Даље, повећава се и број радних налога на SSM-у, оптерећују DMS и EMS компоненте које морају одговорити на новокреиране инциденте покретањем електроенергетских прорачуна како би се околина инцидента довела на прихватљив ниво. SCADA компонента је прва изложена подацима који стижу са различитих уређаја, па тако може доћи до њене недоступности као што је приказано у [137]. Са обзиром да MDM спада у некритичне сервисе, његова недоступност има *умерен* утицај, док је утицај на остале споменуте компоненте сличан као код претње 1 (*Табела 13*).

6.1.8.3.2 Вероватноћа

Са обзиром да постоји жеља код потенцијалног нападача за оваквим типом напада, али због детектора и валидатора мерења из поља [99] вероватноћу према *Табела 5* оцењујемо као *ниску*.

Табела 32 - Акумулирана процена ризика за претњу 30

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П30	VV	N	V	N	V	N	V	N	U	N	U	N	U	N	U	N	U	N
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	

6.1.8.4 Претња 31 (П31): DoS/DDoS напади на интерфејс човек – машина (енг. *human-machine interface*)

Malware BlackEnergy2 [138] је садржао посебну компоненту која је користила рањивости у интерфејсима човек машина и омогућавала реализацију ове врсте напада.

6.1.8.4.1 Утицај

Углавном оператори у контролним станицама користе ове интерфејсе за манипулисање мрежом, па самим тим реализација дате претње може афектовати њихов рад. Такође, на овај начин се може оптеретити свака компонента и доћи до њене недоступности или рушења. Процењени утицаји ће бити као у случају претње 1 (*Табела 13*).

6.1.8.4.2 Вероватноћа

Безбедносне претње проузроковане DoS/DDoS нападима на интерфејс човек-машина су значајне, али тешко изводљиве са обзиром на изоловност OT подсистема, а самим тим и клијнтских машина. Вероватноћу на основу овога можемо оценити као *ниску* према *Табела 5*.

Табела 33 - Акумулирана процена ризика за претњу 31

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П31	VV	N	V	N	V	N	V	N	U	N	V	N	U	N	U	N	U	N
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	

6.2 Попуњавање прототипа обрасца акумулиране процене ризика

Након детаљне процене ризика за сваку од компоненти прототипа паметног електроенергетског система која је урађена у претходном поглављу, следећи и уједно последњи корак анализе ризика у оквиру наше методолгије је попуњавање прототипа обрасца акумулиране процене ризика представљеног у *Табела 12*.

Овај образац је креиран на основу дефинисаног скупа претњи (*Табела 4*), вероватноће њихове реализације (*Табела 5*) и утицаја који могу да проузрокују на систем (*Табела 6*). За сваку идентификовану претњу додат је један ред, а свака компонента из ОТ подсистема представља један стубац. Попуњавање датог обрасца се своди на одређивање вероватноће и утицаја за сваку од претњи и уношења тих информација у заглавље ступаца. Кумулативни ризик се одређује на основу матрице ризика приказане на *Слика 14,* те се након тога уноси у доње делове ћелија са три елемента, тачније у ћелије са тамнијим позадинама.

Погледом на попуњен дати образац који се налази испод, можемо приметити мноштво информација. Како би поједноставили читљивост, по препоруци из поглавља *4.5* смо само ризике највећег нивоа по компоненти обојили одговарајућом бојом. На пример ако погледамо компоненту DMS, видићемо да је највећи процењени ризик у њеном случају оцењен као *умерен* и то за претње 3, 11, 12, 23 и 24. На овај корак смо се одлучили јер је битно идентификовати највећи процењени ризик по свакој компоненти, са обзиром да је довољно да се један такав манифестује како би се дата компонента компромитовала.

Табела 34 - Акумулирана процена ризика

	SCADA		DMS		EMS		OMS		SSM		MDM		GIS		HIS		SIEM	
	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L
П1	VV	N	V	N	V	N	V	N	U	N	V	N	U	N	U	N	U	N
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	
П2	VV	VN	V	VN	V	VN	V	VN	U	VN	V	VN	U	VN	U	VN	U	VN

	N		**N**		**N**		**N**		**VN**		**N**		**VN**		**VN**		**VN**					
П3	V V	N	V V	N	V V	N	V V	N	V V	N	V	V N	U	N	U	N	U	N				
	U		**U**		**U**		**U**		**U**		**N**		**N**		**N**		**N**					
П4	V V	N	V	N	V	N	V	N	U	N	V	N	U	N	U	N	U	N				
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**					
П5	V V	N	V	N	V	N	V	N	U	N	V	N	U	N	U	N	U	N				
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**					
П6	V V	N	V	N	V	N	V	N	U	N	V	N	U	N	U	N	U	N				
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**					
П7	V V	N	V	N	V	N	V	N	U	N	U	N	U	N	U	N	U	N				
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**					
П8	V V	N	V	N	V	N	V	N	U	N	U	N	U	N	U	N	U	N				
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**					
П9	V V	N	V	N	V	N	V	N	U	N	U	N	U	N	U	N	U	N				
	U		**N**		**N**		**N**		**VN**		**VN**		**VN**		**VN**		**VN**					
П10	V V	N	V	N	V	N	V	N	U	N	U	N	U	N	U	N	U	N				
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**					
П11	V V	N	V V	N	V V	N	V V	N	V V	N	V	N	U	N	U	N	U	N				
	U		**U**		**U**		**U**		**U**		**N**		**N**		**N**		**N**					
П12	V V	N	V V	N	V V	N	V V	N	V V	N	V	N	U	N	U	N	U	N				
	U		**U**		**U**		**U**		**U**		**N**		**N**		**N**		**N**					
П13	V V	U	V	U	V	U	V	U	U	U	V	U	U	N	U	N	U	N				
	V		**U**		**U**		**U**		**U**		**U**		**N**		**N**		**N**					
П14	V N	N	V N	N	V N	N	V N	N	V N	N	U	N	U	N	V N	N	V N	N				
	VN		**VN**		**VN**		**VN**		**VN**		**N**		**N**		**VN**		**VN**					
П15	U	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N				
	N		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**					
П16	V V	N	V	N	V	N	V	N	U	N	V	N	U	N	U	N	U	N				
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**					
П17	U	N	U	N	U	N	N	N	U	N	N	N	N	N	N	N	N	N				
	N		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**					
П18	U	N	U	N	U	N	U	N	U	N	U	N	U	N	U	N	U	N				
	N		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**					
П19	U	N	U	N	U	N	U	N	U	N	U	N	U	N	U	N	U	N				
	N		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**					
П20	U	N	U	N	U	N	U	N	U	N	U	N	U	N	U	N	U	N				
	N		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**					
П21	N	N	N	N	N	N	N	N	N	N	U	N	U	N	U	N	U	N				
	N		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**					
П22	V V	N	V	N	V	N	V	N	U	N	V	N	U	N	U	N	U	N				
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**					

П23	V	N	V	N	V	N	V	N	V	N	U	N	U	N	U	N	U	N
	V		V		V		V		V									
	U		**U**		**U**		**U**		**U**		**N**		**N**		**N**		**N**	
П24	V	N	V	N	V	N	V	N	V	N	U	N	V	N	V	N	V	N
	V		V		V		V		V				N		N		N	
	U		**U**		**U**		**U**		**U**		**N**		**VN**		**VN**		**VN**	
П25	V	N	V	N	V	N	V	N	V	N	V	N	V	N	V	N	V	N
	N		N		N		V		N		V		N		N		N	
	VN		**VN**		**VN**		**U**		**VN**		**U**		**VN**		**VN**		**VN**	
П26	V	N	V	N	V	N	V	N	V	N	V	N	V	N	V	N	V	N
	N		N		N		N		N		N		N		N		N	
	VN		**VN**		**VN**		**VN**		**VN**		**VN**		**VN**		**VN**		**VN**	
П27	V	N	V	N	V	N	U	N	V	N	U	N	V	N	V	N	V	N
	N		N		N				N				N		N		N	
	VN		**VN**		**VN**		**N**		**VN**		**N**		**VN**		**VN**		**VN**	
П28	V	U	V	N	V	N	V	N	U	N	U	U	U	N	U	N	U	N
	V																	
	V		**N**		**N**		**N**		**N**		**U**		**N**		**N**		**N**	
П29	U	N	U	N	U	N	U	N	N	N	N	N	N	N	N	N	N	N
	N		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	
П30	V	N	V	N	V	N	V	N	U	N	U	N	U	N	U	N	U	N
	V																	
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	
П31	V	N	V	N	V	N	V	N	U	N	V	N	U	N	U	N	U	N
	V																	
	U		**N**		**N**		**N**		**N**		**N**		**N**		**N**		**N**	

У случају SCADA компоненте која има велики број процењених ризика *умереног* нивоа, највећи је ипак код претњи 13 и 28 оцењен је као *висок*. Претња 13 је везана за безбедносне пропусте у оквиру оперативног система. Сведоци смо да са времена на време добијемо обавештење да инсталирамо нове безбедносне закрпе за оперативни систем и веома је важно да се пробуди свест код корисника да се те исте закрпе редовно примењују. Високо обучени нападачи овакве пропусте могу да искористе да наруше нормално функционисање целокупног паметног ЕЕС-а. Један од најпознатијих напада који је искористио рањивост оперативног система је *Stuxnet* [17] да би се проширио пронашао инжењерски софтвер *Siemens STEP7*. Када је пронашао овај пакет, заменио је комуникационе библиотеке система тако што је подметнуо своје пројектне датотеке. Ово је омогућило вирусу да суптилно промени програм који ради на одређеним *Siemens* (енг. *Program Logic Controller*) PLC-ма, док је промене сакрио од оператера. Да је изводљиво и са коликим утицајем искористити пропусте због застарелих закрпа оперативног система показује и напад *WannaCry Ransomware* [133] током кога је 12.05.2017. заражено више од 200 000 рачунара чији подаци су криптовани и од валсника је тражен њихов откуп. У случају претње 28 ради се о DoS/DDoS нападу на позадинске сервисе паметног електроенергетског система. Иако је у питању ОТ подсистем који је у високој мери изолован, и у продукцији нема излаз на интернет, ипак постоји начин да се изврше ови напади. Конкретно за SCADA-у, могуће је извршити DoS напад [137], али да неко физички приступи RTU уређају у пољу, прикључи свој лаптоп или други уређај и крене да шаље велики број података. Уколико се компромитује већи број RTU-ова онда можемо то подвести под неку верзију DDoS напада. Циљ би био да се SCADA сервис онеспособи и то би имало висок утицај на целокпни систем. Ово је физички изводљиво и мотивација потенцијалног нападача је велика.

Највећи процењени ниво ризика код OMS компоненте је *умерен* и то у случају реализације претњи 3, 11, 12, 23, 24 и 25. Овде је ризик усмерен на недоступност дате компоненте што између осталог може проузроковати значајна кашњења током решавања инцидената и тако се одразити на дуготрајне прекиде у напајању електричном енергијом, оштећење опреме итд.

Што се тиче компоненти DMS, EMS и SSM, видимо да је највећи ниво процењног ризика код њих *умерен* и да се он скоро за све три манифестује у случају *Претњи 3, 11, 12, 23* и *24*. Заједничко за све ове претње је што могу довести до неупотребљивости система кроз нарушавање доступности и интегритета који представљају веома важне особине критичних инфраструктурних система. Међутим због ниске вероватноће да се овако нешто деси процењени ризик није већег нивоа.

Умрен ризик је процењен код MDM компоненете у случају претње 28. Анализом смо показали да је могуће извести DDoS напад на ову компоненту [136], довести је у стање недоступности и на тај начин поремтити рад мреже, опертера и трећих страна којима су ови подаци потребни.

Низак ниво процењеног ризика оцењен је као највећи код компоненти GIS, HIS и SIEM. Као што је кроз ову докторску дисертацију више пута споменуто, дате компоненте нису критичне са аспекта правилног функционисања једног паметног ЕЕС, не садрже личне податке те на основу тога ова процена је и логичан след догађаја.

6.3 Процена потребе за рачунарским ресурсима

Доступност рачунарских ресурса на захтев и перформансе су свакако један од аспеката због кога смо се и одлучили да покушамо представити рачунарство у облаку као одлично решење за будућност паметних ЕЕС, па њихово фигурисање у самој методологији је логичан след. У оквиру критичних инфраструктурних система, неопходно је обезбедити довољно адекватних ресурса који директно утичу на перформантност саме апликације. Постоји већи скуп ресурса овога типа, али они који играју главну улогу, и на којима ће бити акценат у овој докторској дисертацији и који могу директно довести до повећања перформасни апликације су:

1. Потрошња оперативне меморије (енг. *Remote Access Memory - RAM*)
2. Брзина уписа и читања, као и капацитет чврстог диска (енг. *Hard Disk Drive - HDD*)
3. Искоришћење процесора (енг. *Central Processing Unit - CPU*)
4. Проток рачунарске мреже (енг. *Networking Bandwith*)

Процењени ризик смо представили на скали од пет нивоа. Како би били конзистентни, неопходно да наведемо исти број нивоа потребе и за рачунарским ресурсима и да објаснимо њихово значење, тј. шта значи чињеница да је потреба на одређеном нивоу. Сваки од наведена четири типа претходно споменутих ресурса посматраћемо исто, тј. да имају исту важност.

Као основу анализе потребе за перформанса у овој докторској дисертацији, искористићемо практично истраживање и тестирање извршено у оквиру [99]. За сврху тестирања [99] је направљен је приватни кластер у рачунарском облаку који се састоји од физичких сервера распоређених у две шасије смештене у два ормара и спојена на две

сталне меморије. Сваки од физичких сервера садржи четири осмо-језгарна Интел Хеон процесора са 64 GB оперативне меморије, 292 GB диском, 10G мрежом и оптичким каналом. Уважавајући захтеве за високом доступношћу, сви физички сервери имају две мрежне картице, напајања, комуникациону опрему и дискове у редундантном низу независних дискова, В нивоа, конфигурације 3+1 (на свака 3 диска иде један редундантан). У следећој табели је приказана детаљна спецификацију рачунарских компоненти:

Табела 35 - Спецификација рачунарских компоненти

Компонента	Опис (енг.)
Рачунар	*Model: HP BL 660c Gen.8* *Processor: 4 x E5-4620v2 (2.6GHz/8core/20MB95W)* *Memory: 32 x 16GB (PC3 -149000R)* *Network: 2 x HP Ethernet 10Gb 2P 560M Adapter* *Network: 2 x HP Flex Fabric 10Gb 2 port 554FLB* *Storage: 2 x 146GB 6G SAS 15k*
Шасија	*HP Blc 7000* *4 x HP 6120XG Blade Switch* *2 x HP Blc Flex Fabric 10GB/24port Flex fabric with 2 x FC 8Gb and 2 x RJ45 SFP modules* *2 x HP 32A PDU*
Менаџмент сервер	*Model: HP BL 420c Gen.8* *Processor: 2 x E5- 2403* *Memory: 2 x 8GB PC3-12800R* *Network: HP Flex Fabric 10Gb 2 port 554FLB*
Ормар	*HP 642 1075mm* *PDU: HP 2 7x C13*
Оптички кабал	*2 x HP 8/24 Base 16 port enabled switch* *HP Premier Flex LC/LC 2m cables* *HP 8Gb SW SFP pack*
Стална меморија	*HP 3PAR StoreServ 7200 2-N (Dual Controller)* *3PAR M6710 300GB 6G SAS15k Hard disk*

Такође, према [99] веома важну улогу игра и величина електродистрибутивног предузећа и као таква директно утиче на добијене резултате на начин да се повећањем броја напајаних потрошача повећавају и потребни ресурси. Електродистрибутивна предузећа се могу категорисати на више начина у зависности од броја напајаних корисника (величине електродистрибутивне мреже), нивоа припремљености модела електродистрибутивне мреже и листе функционалности (која зависи од нивоа

припремљености података али и пословних циљева предузећа). Аутор [99] их категорише на: мала, средња и велика, у зависности од броја напајаних потрошача као што је приказано наредној табели:

Табела 36 - Категоризација електродистрибутивних предузећа

Категорија	Број напајаних потрошача
Мала	< 500 000
Средња	500 000 – 1 000 000
Велика	>1 000 000

Како величина шеме електродистрибутивне мреже може зависити од великог броја параметара у [99] је претпостављено да комплексност шеме зависи од броја напајаних потрошача. Као полазну основу за ово тестирање користили су замишљену шему која представља електродистрибутивну мрежу од 78390 потрошача. Међутим, да би се уклопили у вредности приказане у претходној табели урађено је умножавање иницијалне шеме, и то 4 пута да би се добила мала ~300 000 потрошача и 32 пута како би добили велику електродистрибутивну мрежу од ~2 500 000 потрошача.

Природа рада електродистрибутивног система је променљива. Због тога се у [99] анализирају два сценарија:

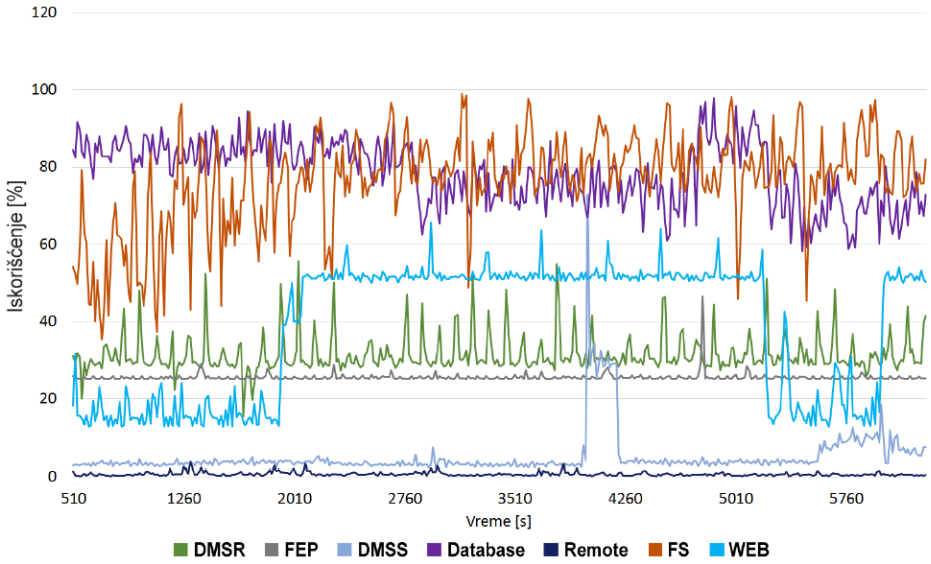
1. Стабилно стање (енг. *Steady Sate*)
2. Стање високе активности (енг. *High Activity*)

Према [99] сценарио стабилног стања подразумева уобичајно понашање мреже у којем се на сваких 5 минута промени 50% аналогних вредности и 10% дискретних вредности, док сценарио високе активности подразумева промену 100% аналогних вредности и 20% дискретних вредности на сваких 5 минута. Током тестирања, дискретне вредности су мењане кроз разна стања док су аналогне вредности осциловале 10%.

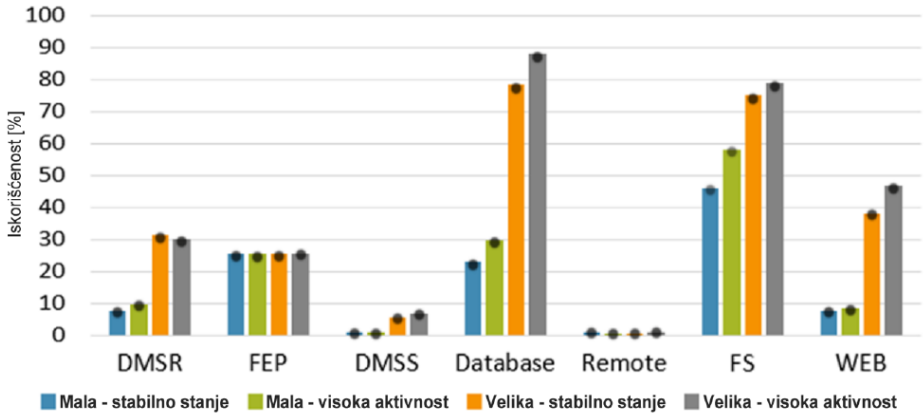
На сликама са амплитудама које следе можемо да видимо графички приказ искоришћености сваког од разматраних ресурса током рада у стабилном стању на великој шеми. Графици ступцима који представљају просечно исришћење приказују шири опсег резултата у зависности од величине електродистрибутивне шеме и сценарија стања рада датог система. У односу на наше компоненте паметног електроенргетског система овде је скоро цели ОТ подсистем моделован као DMSR (енг. *Distribuiton Management System Real-Time Instance*), док су SCADA и *Historian* моделовани као FEP (енг. *Front End Processor*), односно *Database*. На основу природе компоненти у оквиру нашег ОТ подсистема претпоставићемо која од њих је у којој мери одговорна за доле приказане резултате у овкиру DMSR-а.

Ако погледамо прву слику видећемо да су активности у случају Historian компоненте веома високе, тако да у неким моментима досежу и до скоро 100% заузећа процесора, док је просечна вредност у случају велике шеме и високе активности на граници са 90%. Ово аутори оправдавају чињеницом да се значајна количина података

смешта у ову компоненту што редовним путем, што током репликације података. Занимљиво је да величина шеме и ниво активности не утичу на искоришћеност процесора па је он прилично константан на нивоу од 25% заузећа. У оквиру остатка ОТ подсистема (DMSR) средње искоришћење је на нивоу 30%, док је примерно да се икоришћење пење и до 60% у неким случајевима. Због комплексних електроенергетских прорачуна који се одвијају у оквиру DMS и EMS компоненте можемо сматрати да су њих две заслужне за овај ниво процента, док OMS и SSM су са значајној мањим комплексним прорачунима на средњем нивоу, а остале компоненте свакако испод њега. Због природе да чува мрежни модел у оквиру себе, без додатних захтевних прорачуна, сматрамо да је GIS компонента на најнижем нивоу.



Слика 16 - Искоришћење процесора [99]



Слика 17 - Просечно искоришћење процесора [99]

Скалирањем претходно анализираних вредности ћемо да одредимо потребне нивое. Такође, за обзиром да су претходно приказани резултати добијени у рачунарству у облаку, морамо узети у обзир и чињеницу да облак повећава перформансе до 27 % према [129]. Од интереса нам је стање високе активности јер је у оквиру њега потреба за перформансама значајнија. Такође, анализираћемо обе шеме пошто ћемо у наставку нашу методологију применити на мали и велики DSO.

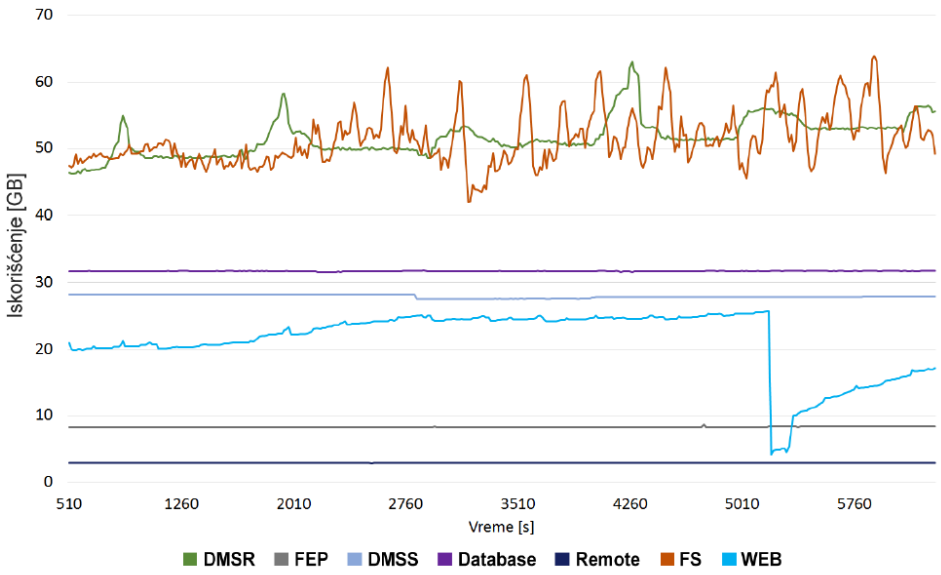
Табела 37 - Ниво искоришћења процесора - велика шема и висока активност

Искоришћење процесора	Компоненте
Веома високо	Historian
Високо	DMS, EMS
Умерено	SCADA, OMS, SSM
Ниско	MDM, SIEM
Веома ниско	GIS

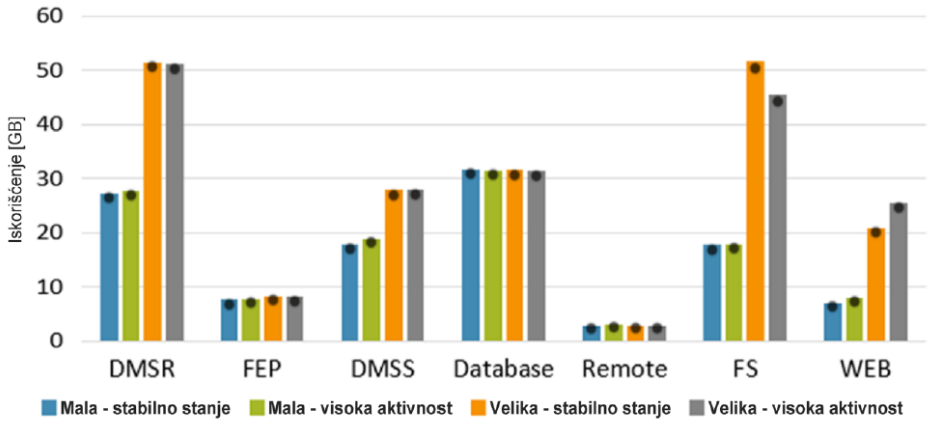
Табела 38 - Ниво искоришћења процесора - мала шема и висока активност

Искоришћење процесора	Компоненте
Веома високо	-
Високо	-
Умерено	SCADA, Historian
Ниско	
Веома ниско	OMS, SSM, GIS, MDM, SIEM

Потрошња оперативне меморије током смештања података у *Historian* компоненту је прилично константа, на неких 30 GB. Код SCADA компоненте је она још мања и видимо да овај ресурс не игра битну улогу. Међутим, у случају остатка OT подсистема је израженија са средњом вредношћу на 50 GB, док највећа амплитуда пребацује 60 GB.



Слика 18 - Искоришћење оперативне меморије [99]



Слика 19 - Просечно искоришћење оперативне меморије [99]

Из истих разлога као у случају искоришћености процесора сматрамо да су овде доминантни првенствено DMS и EMS због тога што извршавају комплексне електроенергетске прорачуне над моделом мреже и симултано одговарају на захтеве оператера, затим OMS и SSM и на крају остале компоненте. Из истог разлога као и у претходном случају сматрамо да је GIS компонента на *веома ниском* нивоу.

Табела 39 - Ниво искоришћења оперативне меморије - велика шема и висока активност

Искоришћење оперативне меморије	Компоненте
Веома високо	-
Високо	DMS, EMS
Умерено	OMS, SSM
Ниско	MDM, SIEM, Historian
Веома ниско	SCADA, GIS

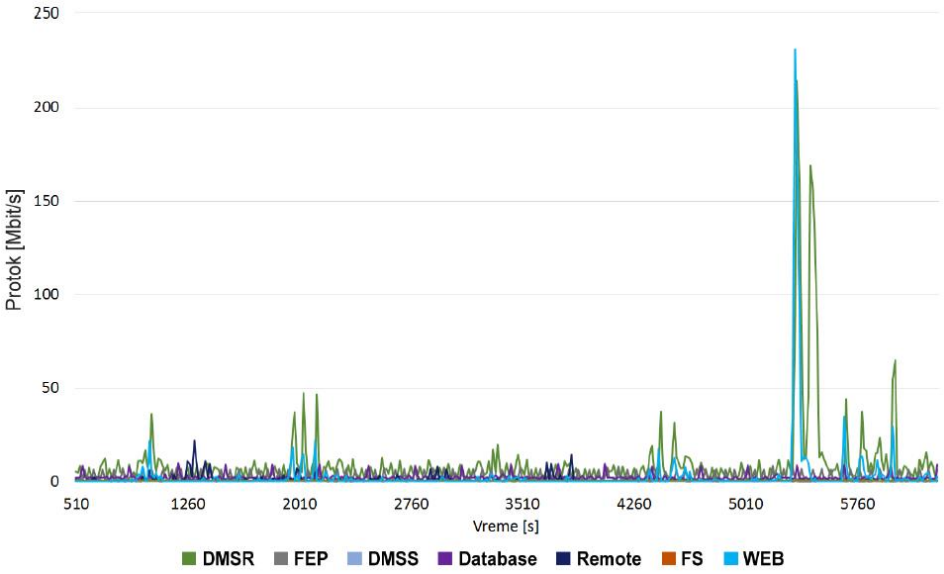
Табела 40 - Ниво искоришћења оперативне меморије - мала шема и висока активност

Искоришћење оперативне меморије	Компоненте
Веома високо	-
Високо	-
Умерено	DMS, EMS
Ниско	MDM, SIEM, Historian, OMS, SSM
Веома ниско	SCADA, GIS

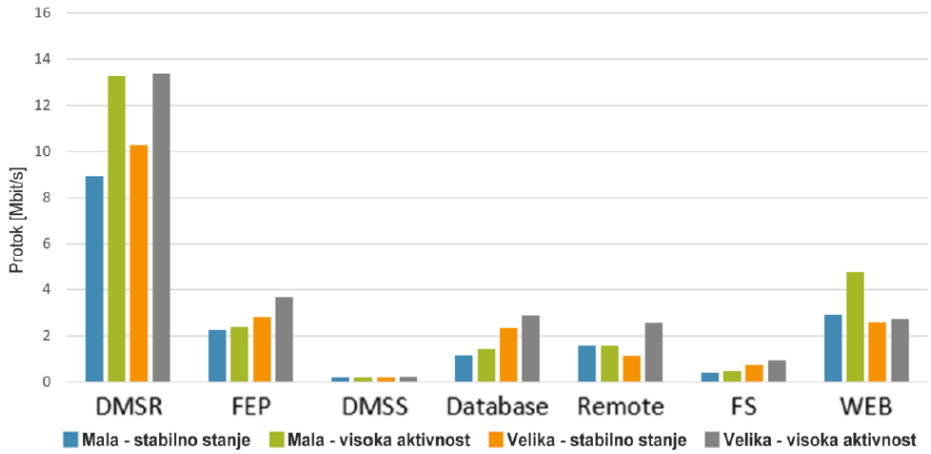
Адекватна пропусност мреже код SCADA компоненте важна, пошто се цела њена логика заснива на константној комуникацији са уређајима у пољу, па брзина којом долазе те информације до система има директни утицај на целокупне перформансе. Сва мерења која стижу са уређаја у пољу не задржавају се пуно у овој компоненти, те SCADA представља на неки начин прокси између уређаја и осатка система. До Historian

компоненте константно стиже значајан број података који требају да се архивирају те је због тога пропусност мреже незанемарива.

Међутим у случају DMS и EMS је најважнија јер ове компоненте повлаче целокупан модел мреже из GIS компоненте који чувају код себе, над њим извршавају различите прорачуне и комуницирају са осталим компонентама у оквиру OT подсистема што се може видети и на следећим графицима.



Слика 20 - Искоришћење мреже [99]



Слика 21 - Просечно искоришћење мреже [99]

У случају нивоа искоришћености мреже можемо да видимо да величина шеме не игра значајну улогу.

Табела 41 - Ниво искоришћења мреже - велика шема и висока активност

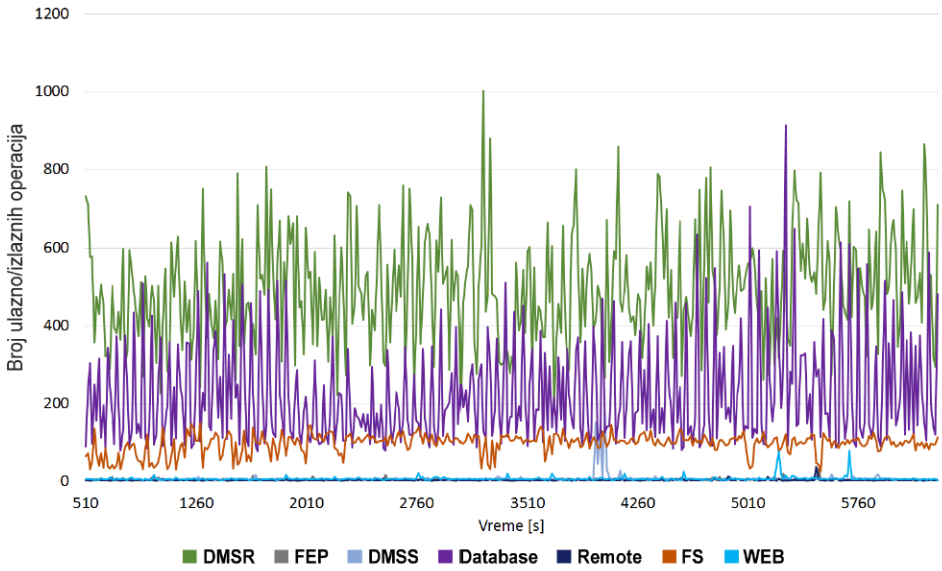
Искоришћење мреже	Компоненте

Веома високо	DMS, EMS
Високо	-
Умерено	SCADA, Historian, OMS, SSM
Ниско	MDM, SIEM
Веома ниско	GIS

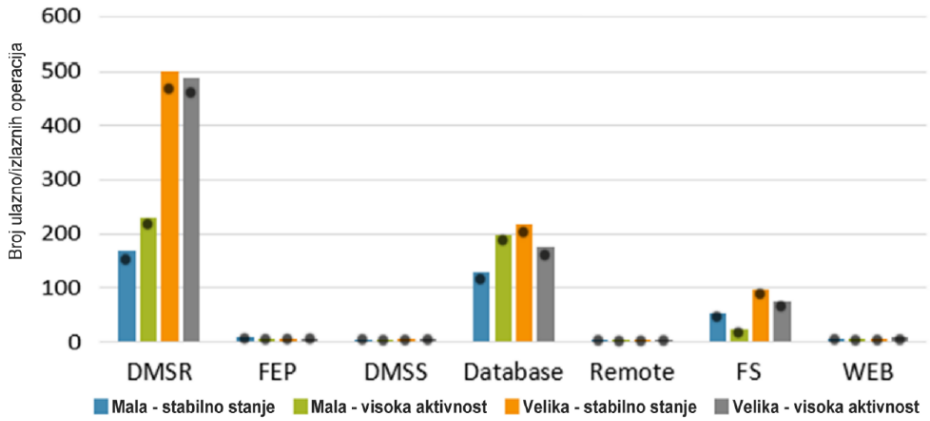
Табела 42 - Ниво искоришћења мреже - мала шема и висока активност

Искоришћење мреже	**Компоненте**
Веома високо	DMS, EMS
Високо	-
Умерено	SCADA, Historian, OMS, SSM
Ниско	MDM, SIEM
Веома ниско	GIS

Логично је да компонента Historian има велики број улазно излазних операција јер она преузима секвенце временских података и догађаја у систему. Приметне су значајне осцилације, са највећом ампчитудом на 900 операција. Код SCADA компоненте овај број је занемарив, док је у оквиру остатка OT подсистема као што видимо значајан. Сматрамо да овде највећи утицај има SIEM компонента која све акције у систему као што су логови, догађаји, аларми и друге важне информације уписује на диск. Не заостају ни DMS, EMS, OMS и SSM који током рада записују велику количину логова и података. GIS компонента чува модел мреже на диску, те због тога захтева значајан ниво потребе за овим ресурсима. Интезитет уписа ових података у случају MDM најмањи пошто интезитет његове активности није висок због чињенице да представља проточни бојлер између поља и ИТ подсистема.



Слика 22 - Број улазно/излазних операција сталне меморије [99]



Слика 23 - просечни број улазно/излазних операција сталне меморије [99]

Табела 43 - Ниво искоришћења сталне меморије - велика шема и висока активност

Искоришћење сталне меморије	Компоненте
Веома високо	SIEM
Високо	DMS, EMS, Historian, GIS
Умерено	OMS, SSM
Ниско	MDM
Веома ниско	SCADA

Табела 44 - Ниво искоришћења сталне меморије - мала шема и висока активност

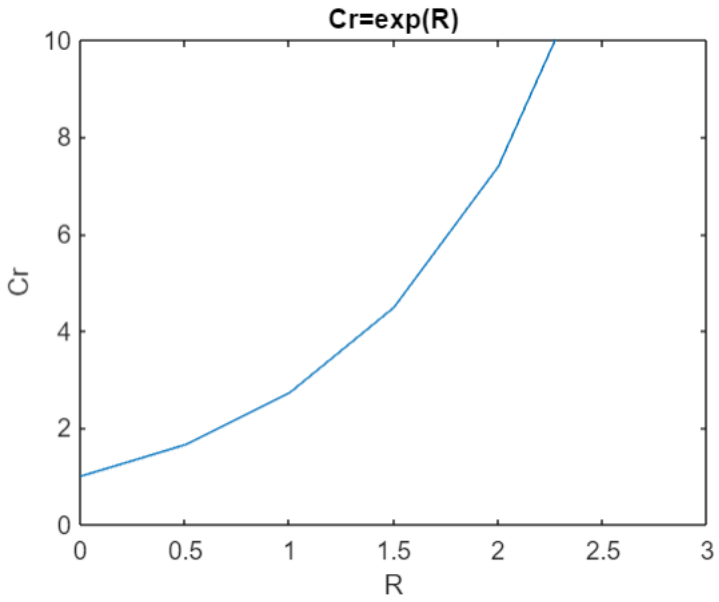
Искоришћење сталне меморије	Компоненте
Веома високо	-
Високо	-
Умерено	SIEM, Historian, GIS
Ниско	DMS, EMS, MDM, OMS, SSM
Веома ниско	SCADA

7. МИГРАЦИЈА

Математичка формулација миграционе стратегије представља дводимензиналну функција са потребом за рачунарским ресурсима (енг. *Computer resources* - *Cr*) приказаним на апциси, док ће потенцијални ризик (енг. *Risk* - *R*) бити приказан на ординати. Основа за нашу математичку формулацију стратегије миграције је ескпоненцијална функција:

$$\boldsymbol{Cr = e^{R}}$$

чији је график приказан на следећој слици.



Слика 24 - Основна функција за математичку формулацију стратегије миграције

Експоненцијална функција је као што можемо видети по природи монотоно растућа порастом независне променљиве, односно у нашем случају *R*, где се брзина раста, односно вредност *Cr* повећава како расте *R*. Управо овом динамиком раста директно сугеришемо да приликом предлагања решења у хибридном облаку већи значај дајемо нивоу процењеног ризика, него потреби за рачунарским ресурсима. Такође, дата функција је и у старту благу предност дала процењеном ризику, са обзиром да не креће из нуле, већ је померена по ординати. Све оне компоентне које припадају самој функцији или се налазе испод ње су кандидати за приватни облак док они који су изнад фунцкије

према нашој методлогији треба да се сместе у облак заједнице. На овај модел смо се одлучили због свеобухватне анализе у поглављима *2.1, 2.2, 2.3* и *2.5* која истиче важност безбедности у контексту рачунарства у облаку. На претходном графику се такође види да без обзира на потребу за рачунарским ресурсима одређене компоненте, уколико је процењени ризик довољно висок, добијамо кандидата за приватни облак.

Свесни смо да ће неки корисници методологије хтети да иду према значајним рачунарским ресурсима и високим перформансама, а на уштруб безбедности, те због тога експоененцијалну функцију проширујемо са њеним асимптотама *aR* и *aCr*. Асимптота *aR* представља хоризонтално померање, где у случају њене позитивне вредности померање ће бити у десно. Са друге стране, *aCr* је вертикално померање које ће бити у смеру према горе уколико вредност ове асимптоте буде позитивна. Да би лакше разумели, другачије речено, што је већа вредност помоћне променљиве *aR*, добијамо решење са већим нивоом толеранције ризика, док са већом вредношћу променљиве *aP* смањујемо потребу за коришћењем рачунарских ресурса у облаку.

Са обзиром да процењени ризик и потреба за рачунарским ресурсима не могу бити негативни, потребно је посматрати дату функцију само у првом квадранту.

$$\boldsymbol{Cr = e^{R-\,\mathrm{a}R} + \mathrm{a}Cr}$$

$$\boldsymbol{0 \leq R, Cr, aR, aCr}$$

Предност ове методологије је да померање не иде искључиво по једној оси, већ је кориснику методологије препуштено да сам бира однос према ризику и према потреби за рачунарским ресурсима. Они мењају помоћне променљиве истовремено доводећи их до њима прихватљивог нивоа.

7.1 Студија случаја #1: Велики DSO

Велики DSO је компанија за дистрибуцију електричне енергије која опскрбљује значајан број потрошача било у густо насељеном, било на великом географском подручју. Један од могућих критеријума за идентификовање великог оператора дистрибутивних система је у зависности од броја напајаних корисника (величине електродистрибутивне мреже), нивоа припремљености модела електродистрибутивне мреже и листе функционалности (која зависи од нивоа припремљености података али и пословних циљева предузећа). Према [99] велики DSO има више од 2 500 000 потрошача. Оваква електродистрибутивна предузећа имају адекватне ИТ буџете за хардвер, ИТ особље као и за сајбер безбедност. *Слика 13* приказује дијаграм системске архитектуре великог DSO-а.

У оваквим системима значајан број ИТ и ОТ услуга је распоређен у властитом контролном/дата центру DSO-а. Најистакнутије предности таквих система су следеће:

1. Аутоматизација и даљинско управљање (SCADA)
2. Управљање инцидентима (OMS)
3. Аналитичке могућности (EMS, DMS)
4. Сигурносни надзор, свест и ревизија (SIEM и Historical)
5. Постоји центар за опоравак од катастрофе (енг. *Disaster Recovery*) DR.

Цена ове врсте система је значајна, јер велики DSO има веома велика капитална улагања у своје сложене (индустријске контроле) системе и мора их периодично надограђивати. Ове надоградње обично укључују дуг процес јавних набавки и пројекти подсистема обично заостају по плану и изнад буџета. Хардвер се обично недовољно користи (нпр. CPU, меморија и складиштење) а и потребно је знатно ИТ-ОТ особље за редовно одржавање и подршку.

7.1.1 Стратегија миграције

Као што је и речено, користићемо математичку функцију и њен график, како би јасно визуализовали предлоге решења.

$$\boldsymbol{Cr} = \boldsymbol{e}^{\boldsymbol{R}-\mathrm{a}\boldsymbol{R}} + \mathrm{a}\boldsymbol{Cr}$$

$$\boldsymbol{0 \leq R, Cr, aR, aCr \leq 2.5}$$

Такође, низ обе осе ћемо се кретати променом вредности асимптота $\boldsymbol{aR}$ и $\boldsymbol{aCr}$ са кораком од 0.5, почевши од 0, па до 2.5:

1. 0.5 – Веома ниско
2. 1.0 – Ниско
3. 1.5 – Умерено
4. 2.0 – Високо
5. 2.5 – Веома високо

На овај корак смо се одлучили да би нивое процењеног ризика и потребе за рачунарским ресурсима лако и интуитивно означили на графику. На ординати вредност 1.5 значи да је ризик на умереном нивоу, док иста вредност на апциси показује да је потреба за рачунарским ресурсима на датом нивоу.

Прво је потребно да се за сваку компоненту датог DSO-а на ординату унесе ниво процењеног ризика који смо идентификовали помоћу наше методологије и приказали у *Табела 34*. Након тога следи унос на апцису ниво потребе за рачунарским ресурсима, такође по компонентама, који је процењен и приказан у *Табела 37*, *Табела 39*, *Табела 41* и *Табела 43*.

Следећа табела садржи управо ове информације – име компоненте, ниво процењеног ризика, као и потребу за рачунарским ресурсима, како би на једном месту имали све неопходне податке.

Табела 45 - Акумулирана процена ризика и потребе за рачунарским ресурсима великог DSO

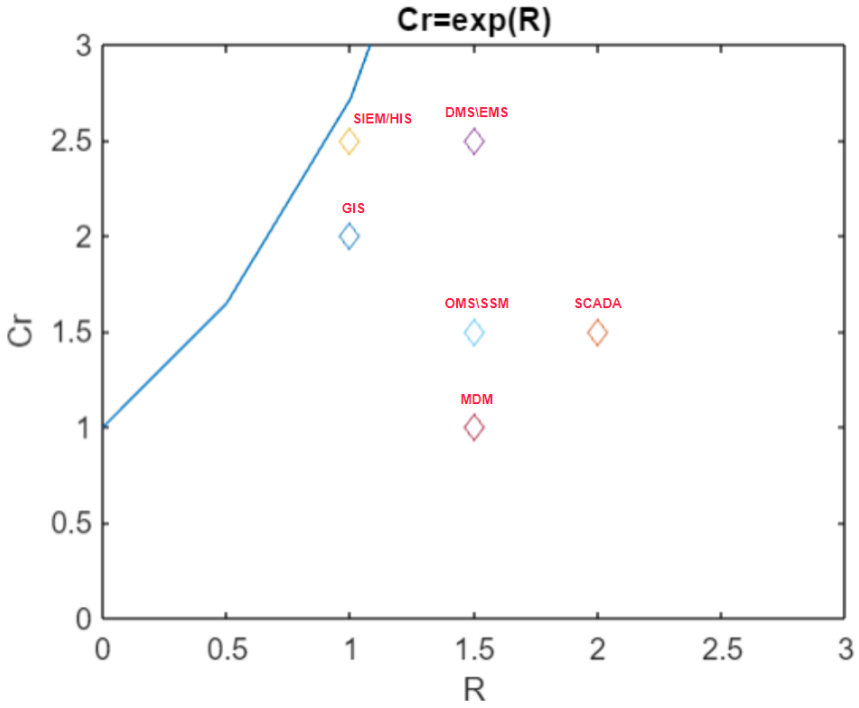
	Ризик	CPU	RAM	Network	I/O HDD
SCADA	V	U	VN	U	VN
DMS	U	V	V	VV	V
EMS	U	V	V	VV	V
OMS	U	U	U	U	U
SSM	U	U	U	U	U
MDM	U	N	N	N	N

GIS	N	VN	VN	VN	V
SIEM	N	N	N	N	VV
Historian	N	VV	N	U	V

Слично као што смо у случају процене ризика узимали највећи процењени за укупни, тако ћемо и овде. Коначан процењени ниво потребе за рачунарским ресурсима одређене компоненте ће бити једнак нивоу највећеног појединачног ресурса.

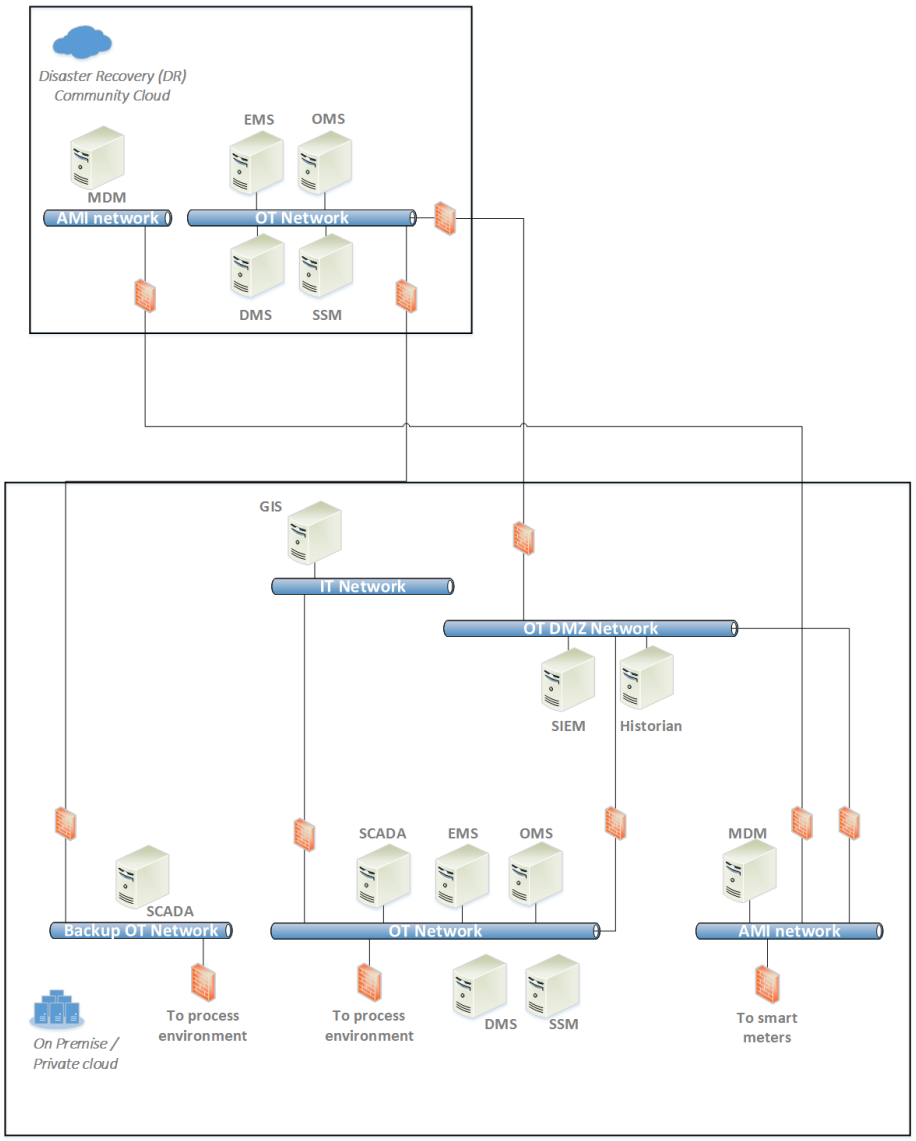
Све компоненте паметног ЕЕС-а чија је позиција на самом графику или изнад њега су кандидати за облак заједнице, док за оне које се налазе испод графика функције препорука је да се сместе у приватни облак.

На следећој слици видимо резултат основне функције миграционе стратегије. Све компоненте се налазе испод графика и пратећи претходне препоруке закључујемо да су оне кандидати за приватни облак. Овакав резултат образложемо чињеницом да је основна функција миграционе стратегије са асимптотом нула и самим тим представља најпесимистичнији приступ са аспекта безбедности.



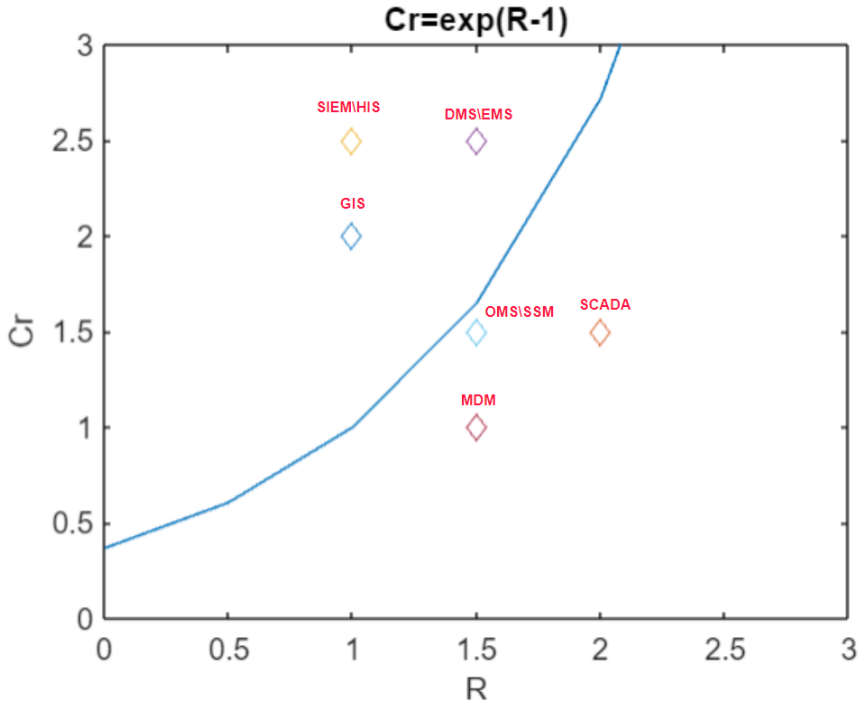
Слика 25 - Резултат основне функције миграционе стратегије (*Cr=exp(R)*) – велики DSO

На основу претходних резултата представљамо архитектуру великог DSO-а у рачунарском облаку.



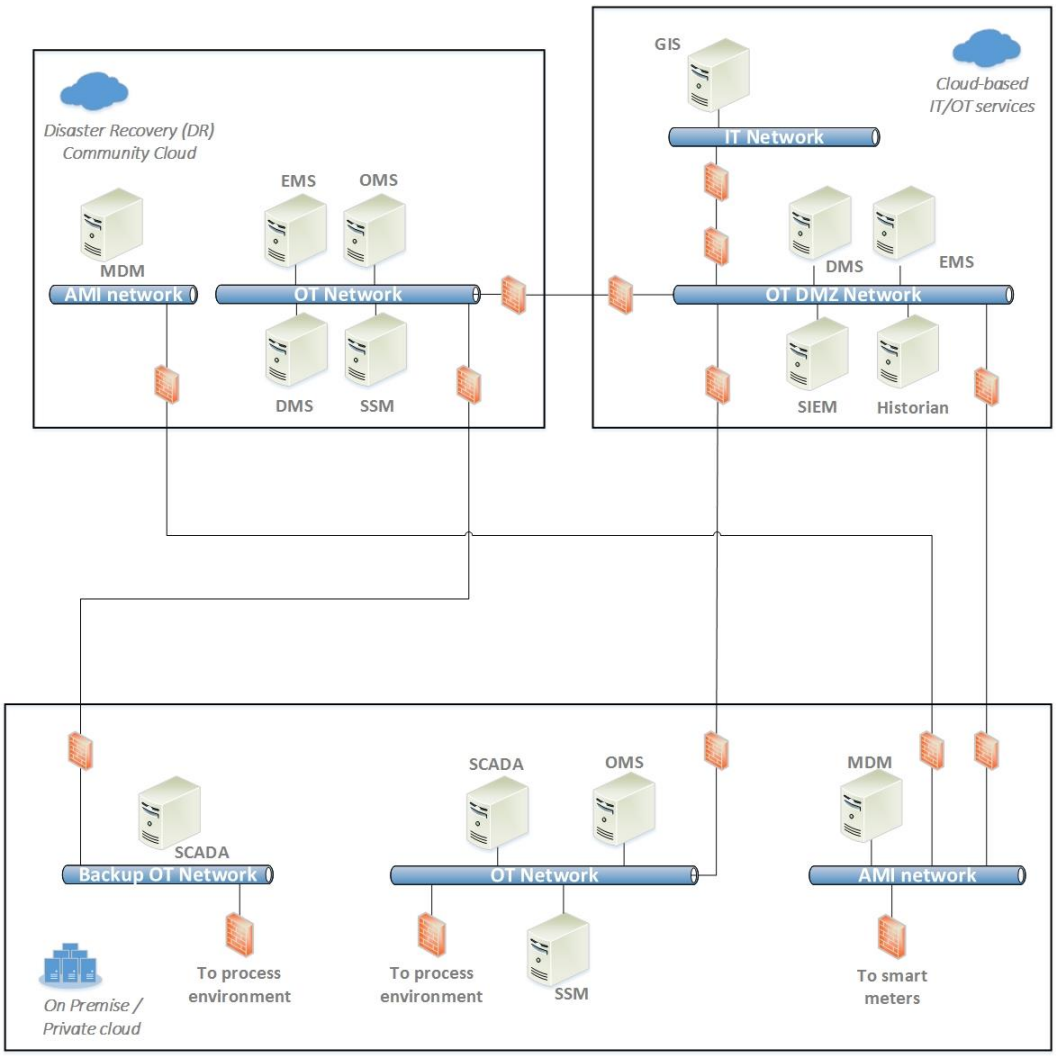
Слика 26 - Архитектура великог DSO као резултат основне функције (*Cr=exp(R)*) мирационе стратегије

Наредна слика представља резултат оптимистичније миграционе стратегије. Изменили смо основну функцију тако што смо се померели по ординати за један (*Cr=exp(R - 1)*), односно у формулу додали асимптоту *aR = 1*. На овај начин смо заначајно смањили ниво процењеног ризика и то је одмах резултовало са првим кандидатима у облаку заједнице. На следећој слици можемо видети да су у облаку заједнице своје место нашле компоненте који имају јако велику потребу за рачунарским ресурсима као што су DMS и EMS (веома висок ниво потребе за рачунарским ресурсима и умерен процењени ризик), SIEM и Historian (веома висок ниво потребе за рачунарским ресурсима и низак процењени ризик), и на крају GIS (висок ниво потребе за рачунарским ресурсима и низак процењени ризик).



Слика 27 - Резултат функције миграционе стратегије (*Cr=exp(R -1)*) – велики DSO

Могли смо и са мањим кораком смањити значај нивоа процењеног ризика, али такође и са већим. Предност ове методологије је да померање не иде искључиво по једној оси, већ је кориснику методологије препуштено да сам бира однос према ризику и према потреби за рачунарским ресурсима. Они мењају помоћне променљиве истовремено доводећи их до њима прихватљивог нивоа.



Слика 28 - Архитектура великог DSO као резултат основне функције (*Cr=exp(R-1)*) мирационе стратегије

На претходно илустрованој миграционој стратегији паметног ЕЕС у рачунарски облак видимо да су OMS, MDM, SSM и SCADA компоненте позициониране у *on-premise* делу, док су све остале представљене као кандидати за облак заједнице. Процењени ризик код SCADA-е је високог нивоа, што је прилично алармантно и без обзира на потребу за рачунарским ресурсима она остаје у приватном облаку. Прве три су своје место нашле овде због не велике потребе за рачунарским ресурсим, а и чињенице да им је ризик процењен као умерен. Компоненте SIEM, Historian, DMS, EMS захтевају високу потребу за рачунарским ресурсима, па уз умерен ризик моћи ће да искористе приступ значајним ресурсима у облаку заједнице.

У *Табела 34* видимо да за SCADA компоненту поред високог, постоји велики број процењених ризика умереног нивоа, па смо због тога њену резервну варијанту такође оставили у приватном облаку. Креирали смо и DR у облаку заједнице због тога што је DSO-ма велики издатак да улажу занчајне новце у резервне варијанте које се не користе толико често. У њега смо сместили OMS, DMS, EMS и SSM који поред SCADA представљају критичне компоненте са аспекта функционисања паметног ЕЕС-а.

7.2 Студија случаја #2: Мали DSO

Један могући критеријум за идентификовање малог оператора дистрибутивних система је да се провери број потрошача (тј. мерних тачака) и окарактерише се као „мали“ ако има до 500 000 (песто хиљада) потрошача у малом или слабо насељеном географском региону [99]. Данас такве компаније (обично) имају ограничене ИТ буџете, што заузврат значи да је њихов буџет намењен за рачунарски хардвер и могућност одржавања информација безбедним такође ограничен. Без обзира на ограничени ИТ буџет, ове компаније требају омогућити управљање имовином (GIS) и прекидом рада (OMS), што им омогућава увид у ажурни инвентар опреме у власништву и правовремено управљање ремонтом неопходно за прихватљив ниво задовољства потрошача. У зависности од својих потреба, могу инвестирати у комплетна решења SCADA, MDM, DMS или SSM решења. Њихове свакодневне операције најчешће ће се обављати без SIEM и/или Historical сервиса.

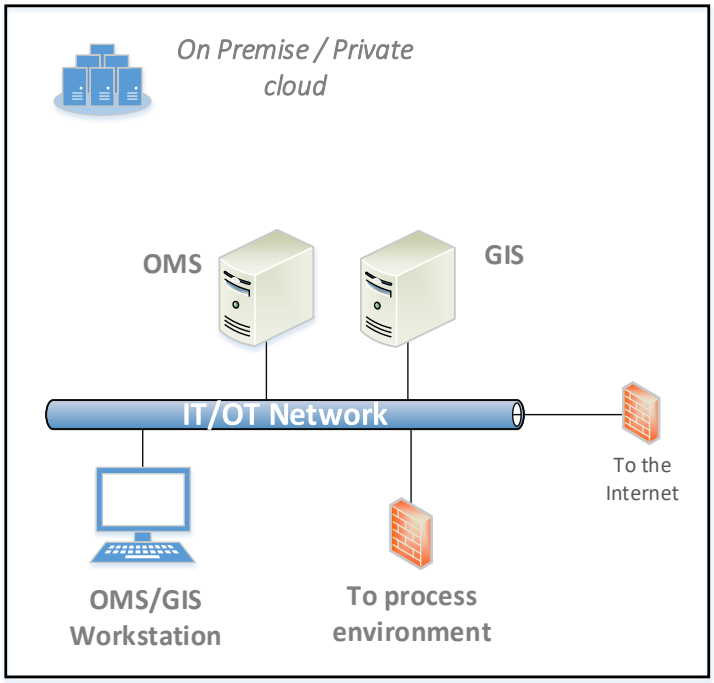
Укратко, закључујемо да овакве конфигурације система имају следеће домене у којима поседују ограничене могућности:

1. Без надгледања и информисања о безбедности због недостатка SIEM-а.
2. Нема аналитичких могућности без DMS/EMS.
3. Нема могућности ревизије без Historical и/или SIEM сервиса.
4. Нема могућности аутоматизације и даљинског управљања без SCADA-е.
5. Не постоји центар за опоравак од катастрофе (енг. *Disaster Recovery*) DR.

У нашој студији случаја разматраћемо мали DSO са следећим специфичним карактеристикама:

1. Постоји један, примарни центар података. Нема центра за опоравак од катастрофе (DR).
2. Ограничене ОТ могућности са само комбинацијом чврсто интегрисаних OMS и GIS услуга. Не постоје SCADA, MDM и други сервиси.

Дијаграм архитектуре претходно описаног малог DSO система приказан је на слици испод.



Слика 29 - Архитектура малог DSO подсистема

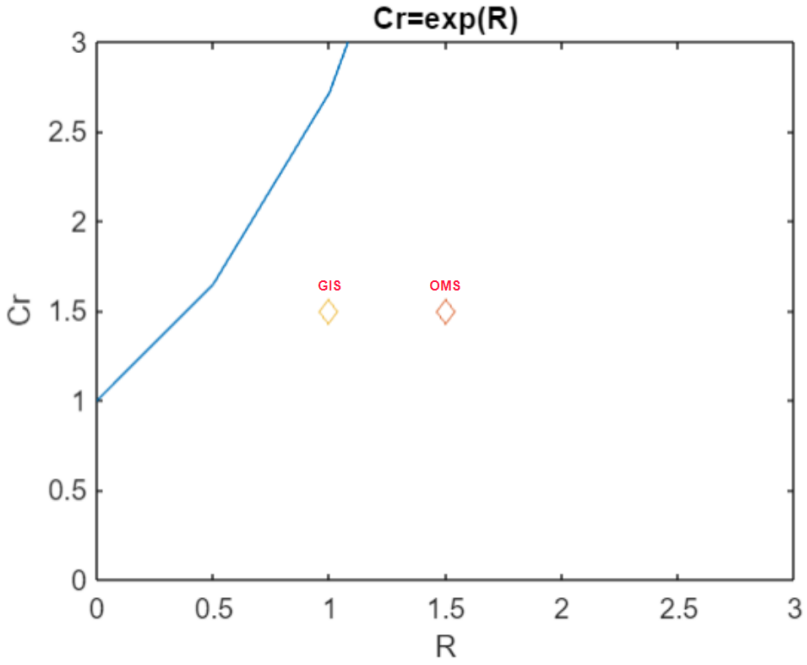
7.2.1 Стратегија миграције

Према [99] потреба за рачунарским ресурсима није иста у случају великог и малог DSO-а што се може видети у поглављу *6.3* где је то поткрепљено и практичним испитивањима. Следећа табела садржи све потребне информације – име компоненте, ниво процењеног ризика, као и потребу за рачунарским ресурсима и креирана је на основу *Табела 12*, *Табела 38*, *Табела 40*, *Табела 42* и *Табела 44*.

Табела 46 - Акумулирана процена ризика и потребе за рачунарским ресурсима малог DSO

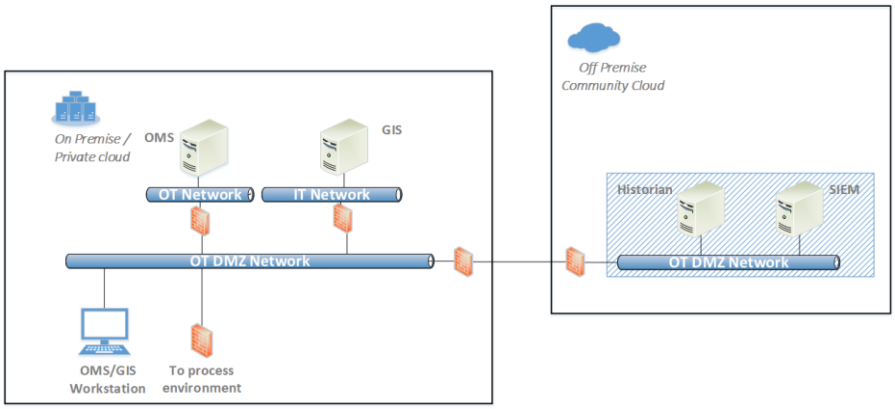
	Ризик	CPU	RAM	Network	I/O HDD
OMS	U	VN	N	U	N
GIS	N	VN	VN	VN	U

И у случају малог DSO користићемо исту математичку формулу у оквиру миграционе стратегије.



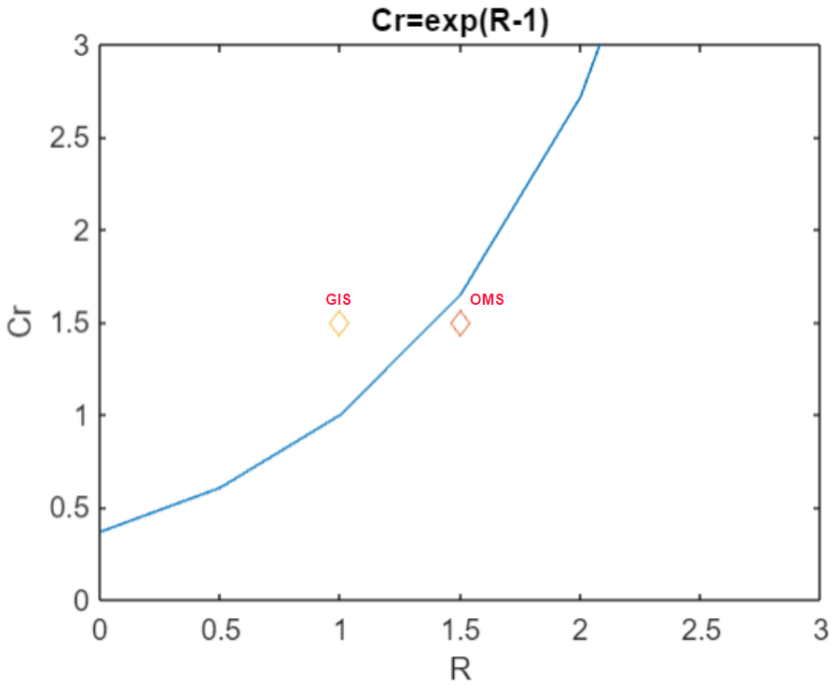
Слика 30 - Резултат основне функције миграционе стратегије (*Cr=exp(R)*) – мали DSO

Оно што и овде прво приметимо је да је већи акценат стављен на сајбер безбедност јер су обе компоненте кандидати за приватни облак.

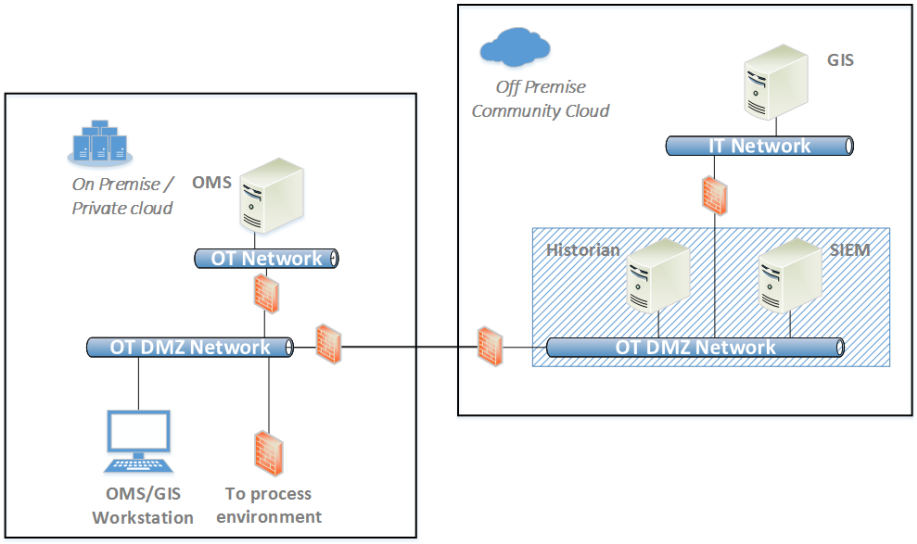


Слика 31 - Архитектура малог DSO као резултат основне функције (*Cr=exp(R)*) мирационе стратегије

Следећа слика представља резултат оптимистичније миграционе стратегије. Изменили смо основну функцију исто као у случају великог DSO, тако што смо се померели по ординати за један (*Cr=exp(R - 1)*), односно у формулу додали асимптоту *aR = 1*. На овај начин смо заначајно смањили ниво процењеног ризика и то је одмах резултовало са првим кандидатима у облаку заједнице. На следећој слици можемо видети да су у облаку заједнице своје место нашла GIS компонента која има умерен ниво потребе за рачунарсим ресурсима и низак процењени ризик. Нешто виши ниво процењеног ризика код OMS компоненте је разлог због чега је она предложена да се смести у приватни облак.



Слика 32 - Резултат функције миграционе стратегије (*Cr=exp(R -1)*) – мали DSO



Слика 33 - Архитектура великог DSO као резултат основне функције (*Cr=exp(R-1)*) мирационе стратегије

Као што се може видети, овде немамо центар за опоравак од катастрофе, али смо у облаку заједнице предложили да се убаце SIEM и Historian (које могу бити решења отвореног кода (енг. *open source*)) компоненте у зависности да ли мали DSO има довољно буџета јер представљају подршку за све остале компоненте како са безбедносног, тако и функционалног аспекта и требале би бити саставни дио сваког DSO-а.

8. ДИСКУСИЈА РЕЗУЛТАТА И ПРОВЕРА ХИПОТЕЗА

Хипотезе од којих смо кренули у овом истраживању су:

1. **Хипотеза 1**: Могуће је развити методологију за процену безбедносних ризика примене најновијих достигнућа у домену рачунарства у облаку у контексту надзора и управљања паметним електроенергетским системима
2. **Хипотеза 2**: Развијена методологија за процену безбедносних ризика може бити применљива у контексту ЕЕС различите сложености.

Као што је у претходним поглављима већ споменуто, критични инфраструктурни системи се у последње време углавном моделују као интеграција ИТ-ОТ подсистема. Са обзиром на ову интеграцију и методологија која би била усмерена на целокупни индустријски контролни систем би самим тим била доста сложена. Ми смо фокус методологије задржали на ОТ подсистему због тога што њему припадају компоненте које морају да раде у реалном времену.

Наша методологија се састојала од следећих корака:

1. Идентификације нежељених догађаја или претњи (енг. *threats*),
2. Одређивање вероватноће реализације датих претњи (енг. *likelihood*),
3. Одређивање утицаја потенцијалних губитака повезаних са датом претњом (енг. *impact*)
4. Дефинисања матрице ризика на основу вероватноће реализације и утицаја потенцијалних претњи
5. Креирања прототипа обрасца акумулиране процене ризика
6. Дефинисања нивоа потребе за рачунарским ресурсима
7. Дефинисања стратегија миграције

У поглављима 6 и *7* ове докторске дисертације, смо коришћењем наше методологије потврдили постављене хипотезе. Не само да смо доказали њену применљивост у контексту ЕЕС различите сложености, оставили потенцијалном кориснику могућност да на веома једноставан начин изабере оптималан сценарио миграције у рачунарски облак.

Ова методологија није уско везана за паметне ЕЕС-е, већ је њена употреба могућа и у ОТ подсистемима других инфраструктура (нпр. гас, вода и отпадне воде. Ако погледамо листу дефинисаних претњи (*Табела 4*), вероватноћу њихове реализације (*Табела 5*), утицај који се проузрокује потенцијалним реализовањем одговарајуће претње

(*Табела 6*), као и сам прототип обрасца акумулиране процене ризика (*Табела 12*) видећемо да су оне креиране за потребе индустријских контролних система различитих намена, и да се нисмо уско везали за EEC.

Њену примену на EEC различите сложености смо демонстрирали у претходном поглављу применивши је једанко успешно прво на велики DSO, а затим и на мали, са ограниченим ИТ буџетом.

Најистакнутије предности решења, заснованог на рачунарском облаку у поређењу са оригиналним, од кога смо кренули су следеће:

1. Снижени трошкови опоравка од катастрофе.
2. Надоградње на нове верзије OT услуга, тј. мали DSO не мора да надограђује своје подсистеме сваких 7-10 година јер ће провајдер облака заједнице то учинити у оквиру споразума о нивоу услуге.
3. Сајбер безбедност побољшана је сегментацијом мрежа у OT, OT DMZ и ИТ зоне, усклађене са IEC-62443.
4. Надгледање сајбер безбедности, свести и ревизије путем SIEM-а и Historical-а у Cloud-у.
5. Рачунарски ресурси се користе по потреби и плаћамо само онолико колико смо потрошили
6. Смањен капацитет ИТ-OT особља за редовно одржавање и подршку
7. Боље перформансе паметног EEC-а

У случају малог DSO-а, већина наведених уобичајних недостатака и ризика могу се ублажити ако мали DSO пређе на хибридну системску архитектуру засновану на рачуанрском облаку. Високи и средњи ризици идентификовани током процене ризика ублажавају се увођењем SIEM и Historical сервиса које свим корисницима рачунарског облака пружа CSP.

9. ЗАКЉУЧАК

Од почетка 21. века енергетска индустрија се суочила са различитим проблемима узрокованим информационо-безбедносним пропустима. Последице таквих инцидената могу бити финансијски значајне, доводе до губитка поверења корисника у компанију, и у екстремним ситуацијама могу да угрозе животну средину или доведу до људских жртава. Хакерски напади на различите критичне инфраструктуре у задњих 20 година су показали да није довољна примена адекватних мера физичке безбедности, већ је неопходно обезбедити заштиту и од напада у сајбер простору.

Можда најпознатији примери таквих напада, који уједно добро илуструју домете штете која може да настане као последица напада чији је извор у сајбер простору, а ефекти се осећају у физичком окружењу су следећи:

1. Stuxnet напад 2010. године који је представљао саботажу над нуклеарним постројењем у Ирану где је уз помоћ посебно дизајнираног злонамерног софтвера (енг. malware) преузета контрола над индустријским контролним системом и нанета штета у физичком простору.
2. *Malware* Duqu, откривен 2011. године, дизајниран да компромитује индустријске системе са циљем прикупљања информација из контролних система за будућу експлоатацију.
3. Хакерски напад у децембру 2015. године на Украјинске компаније у електроенергетском сектору услед којих је преко 200.000 потрошача остало без електричне енергије у трајању од више сати.

Осим малициозних напада који могу да угрозе правилно функционисање система, велики изазов представља и очување приватности корисника, са обзиром да су различите информације о потрошачима сада доступне у пословним информационим системима.

Употребом рачунарства у облаку одржавање и надоградња рачунарског хардвера, решавање потенцијалних проблема на оперативном систему и других се делегира трећем лицу. Предузећа за управљање електроенергетским системима су за сада већином скептична у погледу спајања паметних мрежа са рачунарством у облаку, углавном због велике количине осетљивих података и великог броја критичних процеса који су од јавног значаја. Предмет истраживања ове докторске дисертације је био да се развије методологија за безбедну примену рачунарства у облаку у надзору и управљању паметним електроенергетским системима. У раду је идентификовано и анализирано више од 30 претњи усмерених на паметне ЕЕС. Ова тема је значајна, јер њена темељна анализа може охрабрити власнике паметних ЕЕС да се одлуче на корак прихватања решења из домена рачунарства у облаку уз очување високог нивоа сајбер безбедности.

На основу прегледа актуелног стања у области закључили смо да не постоје студије засноване на процени ризика које би се посебно бавиле проблемом миграције ОТ подсистема на архитектуру засновану на рачунарском облаку, на систематски начин. То је јаз који смо испунили истраживањима која су представљена у овом раду. Наша методологија представља значајан алат за све власнике/операторе система паметног ЕЕС у одабиру оптималне стратегије миграције на рачунарски облак, прилагођавајући се њиховим специфичним захтевима и одржавајући адекватан ниво сајбер безбедности.

Методологију смо тестирали у двије студије случаја. Прва је укључивала велики DSO са сложенијим ОТ могућностима, док смо у другом случају је применили на мали DSO са ограниченим буџетом и ИТ особљем и на тај начин потврдили постављене хипотезе.

У овој докторксој дисертацији смо се фокусирали на безбедност информација, потребу за перформансама и предложену стратегију миграције облака. Анализиране студије случаја нису укључивале додатне кључне метрике, нпр. трошкови особља и облачних услуга, ниво подршке менаџмента или временски аспект извора и претњи, тј. чињеница да се извори претњи и претње временом мењају итд. Ове мере ће бити саставни део будућих истраживања.

ЛИТЕРАТУРА

[1] Maria Lorena Tuballa, Michael Lochinvar Abundo, “A review of the development of Smart Grid techologies” Renewable and Sustainable Energy Reviews Volume 59, June 2016, Pages 710-725.

[2] United States Department of Energy, "Smart Grid System Report", Washington, 2018.

[3] Dileep. G., "A survey on smart grid technologies and applications", Renewable Energy, Volume 146, Pages 2589-2625, February 2020.

[4] B. Jelacic, D. Rosic, I. Lendak, M. Stanojevic, and S. Stoja, “STRIDE to a secure Smart Grid in a hybrid cloud”, in Proc. European Symposium on Research in Computer Security, SECPRE 2017, CyberICPS 2017, Lecture Notes in Computer Science, vol 10683, pp. 77-90, Oslo, Norway, 2017.

[5] Bojan Jelacic, Imre Lendak, Sebastijan Stoja, Marina Stanojevic, Daniela Rosic,"Security Risk Assessment-based Cloud Migration Methodology for Smart Grid OT Services", Acta Polytechnica Hungarica, Journal of Applied Sciences, Volume 17, Issue Number 5, DOI: 10.12700/APH.17.5.2020.5.6, 2020.

[6] Gartner IT Glossary. (2015, August 15). Operational technology. Retrieved from http://www.gartner.com/it-glossary/operational-technology-ot.

[7] Gartner IT Glossary. (2015, August 15). Information technology. Retrieved from https://www.gartner.com/en/information-technology/glossary/it-information-technology.

[8] Adam Hahn, "Operational Technology and Information Technology in Industrial Control Systems", Cyber-security of SCADA and Other Industrial Control Systems pp 51-68, 24. August 2016.

[9] Russell Byfield, "A practical guide to IT OT convergence – getting value from your business analytics", The APPEA Journal 59(2) 526-530 https://doi.org/10.1071/AJ18190, 17 June 2019.

[10] [10] D. Rosic, I. Lendak, and S. Vukmirovic, "A Role-Based Access Control Supporting Regional Division in Smart Grid System", Acta Polytechnica Hungarica, vol 12, no 7, pp. 237-250, 2015.

[11] Azwirman Gusrialdi, Zhihua Qu, "Smart Grid Security: Attacks and Defenses", Smart Grid Control pp 199-223, 2018.

[12] Eric D. Knapp, Raj Samani, "Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure", Elsevier, 2013.

[13] Eric D. Knapp, "Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems", Elsevier, 2011.

[14] Mounesh Marali, Sithu D Sudarsan, Ashok Gogioneni, "Cyber security threats in industrial control systems and protection", DOI: 10.1109/ICACCE46606.2019.9079981, 2019 International Conference on Advances in Computing and Communication Engineering (ICACCE), 4-6 April 2019.

[15] Zakaria El Mrabet, Naima Kaabouch, Hassan El Ghazi, Hamid El Ghazi, "Cyber-security in smart grid: Survey and challenges", Computers & Electrical Engineering, Volume 67, Pages 469-482 April 2018.

[16] D. Healey, S. Meckler, U. Antia, E. Cottle, "Cyber Security Strategy for the Energy Sector", ITRE Committee, Oct. 2016.

[17] D. Kushner, "The real story of Stuxnet", IEEE Spectrum, vol 3(50), 2014.

[18] Daniela Rosić, Model kontrole pristupa u Smart Grid sistemima, Doktorska disertacija, Novi Sad, 2017.

[19] R. M. Lee, M. J. Assante, and T. Conway, “Analysis of the Cyber Attack on the Ukrainian Power Grid”, Defense Use Case, SANS ICS, Mar. 2016.

[20] Zeller. M, “Myth or reality—Does Aurora vulnerability pose a risk to my generator? “Schweitzer Engineering Laboratories. Texas A&M Conference for Protection Relay Engineers, 2011.

[21] Abrahams Abrams, M., & Weiss, J. Bellingham, “Washington, control system cyber security case study“, National Institute of Standards and Technology (NIST). Retrieved from http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Bellingham_Case_Study_report%2020Sep071.pdf, September 2007.

[22] Madihah Mohd Saudi, Azuan Ahmad, Muhammad Afif Husainiamer, “Malware Classification for Cyber Physical System (CPS) based on Phylogenetics”, International Journal of Engineering and Advanced Technology, DOI:10.35940/ijeat.A2711.109119, October 2019.

[23] Michael J. Assante and Robert M. Lee, “The Industrial Control System Cyber Kill Chain“, October 2015.

[24] Zakaria El Mrabet, Naima Kaaboucha, Hassan El Ghazi, Hamid El Ghazi, “Cyber-security in smart grid: Survey and challenges”, Computers and Electrical Engineering, 469–482, 2018.

[25] M. Zekeriya Gunduz, Resul Das, "Analysis of cyber-attacks on smart grid applications", 2018 International Conference on Artificial Intelligence and Data Processing (IDAP), IEEE, Malatya, Turkey, Turkey, 28-30 Sept. 2018.

[26] Taha Selim Ustun, S. M. Suhail Hussain, "A Review of Cybersecurity Issues in Smartgrid Communication Networks", 2019 International Conference on Power Electronics, Control and Automation (ICPECA), New Delhi, India, 16-17 Nov. 2019.

[27] National Institute of Standards and Technology Interagency Report 7628, Rev. 1," Guidelines for Smart Grid Cybersecurity" http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

[28] National Institute of Standards and Technology Special Publication 800-82, Rev. 2, "Guide to Industrial Control Systems (ICS) Security" http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[29] European Network and Information Security Agency, Annex II, Security aspects of the Smart Grid, https://www.enisa.europa.eu/

[30] Seref Sagiroglu, Yavuz Canbay, Ilhami Colak, "Solutions and Suggestions for Smart Grid Threats and Vulnerabilities", International Journal of Renewable Energy Research-IJRER, Vol 9, No 4 (2019).

[31] R. Leszczyna, "Cybersecurity and privacy in standards for smart grids – A comprehensive survey", Computer Standards & Interfaces, vol 56, Feb. 2018.

[32] J. Jarmakiewicz, K. Parobczak, and K. Maślanka, "Cybersecurity protection for power grid control infrastructures", International Journal of Critical Infrastructure Protection, Volume 18, September 2017.

[33] North American Electric Reliability Corporation (NERC), "Critical Infrastructure protection (CIP)", http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[34] R. Paes, D. C. Mazur, B. K. Venné, and Jack Ostrzenski, "A guide to securing industrial control networks — (IT/OT) convergence", in Proc. 2017 Petroleum and Chemical Industry Technical Conference (PCIC), Calgary, Canada, Dec. 2017.

[35] "Final Report - Study on cyber security in the energy sector of the Energy Community", Blueprint Energy Solutions GmbH, December 2019.

[36] "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector", Mission Support Center, Idaho National Laboratory, August 2016.

[37] NIST Special Publication 800-37, "Risk Management Framework for Information Systems and Organizations", October 2018.

[38] NIST Special Publication 800-30, "NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments", 2012.

[39] Vikas Lamba, Nikola Šimkova, Bruno Rossi, "Recommendations for smart grid security risk management", Journal Cyber-Physical Systems, Volume 5, 2019 - Issue 2.

[40] Technical Risk Assessment and Risk Treatment, UK Communications Electronics Security Group (CESG), Apr. 2012.

[41] Judith E.Y. Rossebø, ABB Norway; Reinder Wolthuis and Frank Fransen, TNO; Gunnar Björkman, KTH Royal Institute of Technology; Nuno Medeiros, EDP Distribuição; "An Enhanced Risk-Assessment Methodology for Smart Grids", IEEE Computer Society, 2017.

[42] Alan J. McBride and Andrew R. McGee, "Assessing Smart Grid Security", DOI: 10.1002/bltj, Bell Labs Technical Journal, 2012.

[43] NIST Federal Information Processing Standard (FIPS) 199, "New Standards for Security Categorization of Federal Information and Information Systems", Feb. 2015.

[44] NISTIR 7628 Revision 1, "Guidelines for Smart Grid Cybersecurity", 2014.

[45] Merz, Terry R., Fallon, Corey K., Scalco, Aleksandra, "A Context-Centered Research Approach to Phishing and Operational Technology in Industrial Control Systems", Journal of Information Warfare, 2019.

[46] Jean-Marc Thiriet, Stéphane Mocanu, "A course in cyber-security, with orientations towards cyber-physical systems", 29th Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEEIE), 2019.

[47] Carolina Adaros Boye, Paul Kearney, Mark Josephs, "Cyber-Risks in the Industrial Internet of Things (IIoT): Towards a Method for Continuous Assessment", International Conference on Information Security, 2018.

[48] Manish Shrestha, Christian Johansen, Josef Noll, DavideRoverso, " A Methodology for Security Classification applied to Smart Grid Infrastructures", International Journal of Critical Infrastructure Protection, Volume 28, March 2020.

[49] Hellen Maziku, Sachin Shetty, David M.Nicol, "Security risk assessment for SDN-enabled smart grids", Computer Communications, Volume 133, January 2019.

[50] Rafal Leszczyna, “A Review of Standards with Cybersecurity Requirements for Smart Grid“, DOI: 10.1016/j.cose.2018.03.011, Computers & Security, 2018.

[51] Rafal Leszczyna, “Standards on Cyber Security Assessment of Smart Grid“, DOI: 10.1016/j.ijcip.2018.05.006, International Journal of Critical Infrastructure Protection, June 2018.

[52] K. C. Ruland, J. Sassmannshausen, K. Waedt, N. Zivic, “Smart grid security – an overview of standards and guidelines”, Elektrotechnik & Informationstechnik, 134/1: 19–25. DOI 10.1007/s00502-017-0472-8, 2017.

[53] Evaluation of Cloud Computing Services Based on NIST SP 800-145, NIST Special Publication 500-322, February 2018.

[54] Isaac Odun-Ayo, Ananya M., Frank Agono and Rowland Goddy-Worlu, “Cloud Computing Architecture: A Critical Analysis”, 18th International Conference on Computational Science and Applications (ICCSA), DOI: 10.1109/ICCSA.2018.8439638, 2018.

[55] Priyanshu Srivastava, Rizwan Khan, “A Review Paper on Cloud Computing“, DOI: 10.23956/ijarcsse.v8i6.711, June 2018.

[56] M. Ali, S. U. Khan, and A. V Vasilakos, “Security in cloud computing: Opportunities and challenges,” Inf. Sci. (Ny)., vol. 305, pp. 357–383, 2015.

[57] Nikola Dalčeković, Platforma za transformaciju softverskih rešenja pametnih elektroenergetskih mreža na cloud bazirani višeorganizacijski SaaS, Doktorska disertacija, Novi Sad, 2018.

[58] Randy Garcia, C. Edward Chow, “Identity Considerations for Public Sector Hybrid Cloud Computing Solutions”, International Conference on Computer Communication and Informatics (ICCCI -2015), Jan. 08 – 10, 2015, Coimbatore, India.

[59] NIST SP 500-293: “US Government Cloud Computing Technology Roadmap Volume I, High-Priority Requirements to Further USG Agency Cloud Computing Adoption” National Institute of Standards and Technol-ogy (NIST), Gaithersburg, MD 20899, October 2014.

[60] B. Fortna, “Securing the federal hybrid cloud”, Industry Insight, GCN, 2018.

[61] M. Cancila, D. Toombs, A. D. Waite, and K. Elias, “Gartner: 2017 Planning Guide for Cloud Computing,” 2016.

[62] “Predictions 2018: Cloud Computing Accelerates Enterprise Transformation Everywhere.” [Online]. Available: https://www.forrester.com/report/Predictions+2018+Cloud+Computing+Accelerates+Enterprise+Transformation+Everywhere/-/E-RES139611. [Accessed: 12-Nov-2017].

[63] Jönköping University, Jönköping International Business School, JIBS, Informatics.(IT, Management & Innovation), "Security in Cloud Computing Environments", 2019.

[64] PanJun Sun, "Security and privacy protection in cloud computing: Discussions and challenges", Journal of Network and Computer Applications, Volume 160, 15 June 2020.

[65] Mrs.Soniya Bastwade, Ms. Neha D.Patil, "Homomorphic encryption scheme in cloud computing for security and privacy data", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056, June 2019.

[66] Josep Domingo-Ferrer, Oriol Farràs, Jordi Ribes-González, David Sánchez, "Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges", Computer Communications, Volumes 140–141, May 2019, Pages 38-60.

[67] Mouna Jouini (Institut Supérieur De Gestion De Tunis, Tunisia) and Latifa Ben Arfa Rabai (Institut Supérieur de Gestion de Tunis, Tunisia), "A Security Framework for Secure Cloud Computing Environments", 2019.

[68] P. Gayatri, M. Venunath, V. Subhashini, "Syed Umar Securities and threats of cloud computing and solutions", Coimbatore, India, 2018.

[69] P. Deshpande, S. C. Sharma, and P. Sateesh Kumar, “Security threats in cloud computing”, in Proc. 2015 International Conference Computing, Communication & Automation (ICCCA), Noida, India, 2015, pp. 632-636.

[70] Fabian Suß, Marco Freimuth, Andreas Aßmuth, George R S Weir and Bob Duncan, "Cloud Security and Security Challenges Revisited", CLOUD COMPUTING 2019: The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization.

[71] R. Wynn, “The 2016 Dirty Dozen: 12 cloud security threats”, Cloud Security Alliance Southwest Chapter meeting, Cloud Security Alliance, Apr. 2016.

[72] J.Y. Kimm, and Y. Kim, “Benefits of cloud computing adoption for smart grid security from security perspective”, The Journal of Supercomputing, vol 72, no 9, pp. 3522–3534, Sep. 2016.

[73] T. Radwan, M. A. Azer, and N. Abdelbaki, “Cloud computing security: challenges and future trends”, International Journal of Computer Applications in Technology, January 2017.

[74] Khalid EI Makkaoui, Abdellah Ezzati, Abderrahim Beni-Hssane, Cina Motamed, “Cloud Security and Privacy Model for Providing Secure Cloud Services”, 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech), DOI: 10.1109/CloudTech.2016.7847682, 2016.

[75] Issa M. Khalil, A. Khreishah, M. Azeem, "Cloud Computing Security: A Survey," Computers, Vol, 3, pp. 1-35,2014.

[76] The Cloud Services Measurement Initiative Consortium (CSMIC): Service Measurement Index Framework Version 2.1. Carnegie Mellon University Silicon Valley Moflett Field, CA USA, July 2014.

[77] K. EL MAKKAOUI, A. EZZATI, A. BENI-HSSANE, C. MOTAMED, "Data confidentiality in the word of c1oud," Journal of Theoretical and Applied Information Technology, Vo1.84. No.3, 2016.

[78] Yogeshwaran Sivasubramanian, Syed Zubair Ahmed, Ved Prakash Mishra, “Risk Assessment for Cloud Computing”, DOI: 10.24178/irjece.2017.3.2.07, IRJECE Vol 3(2) Jun 2017.

[79] EBIOS, Central Directorate for Information Systems Security, Version 2010 website. [Online]. Available: http://www.ssi.gouv.fr.

[80] Method Harmonized Risk Analysis (MEHARI) Principles and mechanisms CLUSIF, Issue 3, October 2004.

[81] Fariba Ghaffari, Hossein Gharaee, Mohammad Reza Forouzandehdoust, "Security Considerations and Requirements for Cloud Computing", 8th International Symposium on Telecommunications, 2016.

[82] P.S. Suryateja, "Threats and Vulnerabilities of Cloud Computing: A Review", International Journal of Computer Sciences and Engineering, 2018.

[83] ENISA, Cloud computing: benefits, risk and recommendations for information security.

[84] Erdal Cayirci, Alexandr Garaga, Anderson Santana de Oliveira2 and Yves Roudier, „A risk assessment model for selecting cloud service providers", Journal of Cloud Computing: Advances, Systems and Applications, DOI 10.1186/s13677-016-0064-x, 2016.

[85] The Open Web Application Security Project (OWASP). [Online], Available at: www.owasp.org.

[86] Fatimah M. Alturkistani and Ahmed Z. Emam, "A Review of Security Risk Assessment Methods in Cloud Computing", New Perspectives in Information Systems and Technologies, Volume 1 pp 443-453, DOI: 10.1007/978-3-319-05951-8_42, 2014.

[87] Kalaiprasath .R, Udaya Kumar, "Cloud security and compliance - A semantic approach in end to end security", DOI: 10.21307/ijssis-2017-265, International Journal on Smart Sensing and Intelligent Systems · September 2017.

[88] NIST Special Publication 800-30, "NIST Special Publication 500-291, Version 2, NIST Cloud Computing Standards Roadmap", 2012.

[89] Carlo Di Giulio, Charles Kamhoua, Roy H. Campbell, Read Sprabery, Kevin Kwiat, Masooda N. Bashir, „Cloud Standards in Comparison", IEEE 10th International Conference on Cloud Computing, 2017.

[90] Tomas Kulik, Peter W. V. Tran-Jørgensen, Jalil Boudjadar, „Compliance verification of a cyber security standard for Cloud-connected SCADA", IEEE, 2019.

[91] Pil Sung Woo, Balho H. Kim, "Risk analysis of power information control system based on smart grid security standardization", International Journal of Smart Grid and Clean Energy, 2018.

[92] Mirjana D. Stojanović, Slavica V. Boštjančič Rakas, Jasna D. Marković-Petrović, "Scada systems in the Cloud And Fog environments: Migration Scenario and Security Issues", Electronics and Energetics Vol. 32, No3, pp. 345-358, https://doi.org/10.2298/FUEE1903345S, September 2019.

[93] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, et. al, "A Review of Cyber Security Risk Assessment Methods for SCADA Systems", Comput. Secur., vol. 56, pp. 1–27, February 2016.

[94] N. Hossain, A. Hossain, T. Das and T. Islam, "Measuring the Cyber Security Risk Assessment Methods for SCADA System", Glob. J. Eng. Sci. Res. Manag., vol. 4, no. 7, pp. 1–12, July 2017.

[95] Philip Church, Harald Mueller, Caspar Ryan, Spyridon V. Gogouvitis, Andrzej Goscinski & Zahir Tari, "Migration of a SCADA system to IaaS clouds – a case study", Journal of Cloud Computing, volume 6, Article number: 11 (2017).

[96] Pooyan Jamshidi, Claus Pahl, Nabor C. Mendonça, Pattern-based multi-cloud architecture migration, 03. October 2016.

[97] Mahdi Fahmideh, Farhad Daneshgar, Fethi Rabhi, Ghassan Beydoun, A generic cloud migration process model, European Journal of Information Systems, Volume 28, 2019 - Issue 3.

[98] Z. Cao, J. Lin, C. Wan, Y. Song, Y. Zhang, and X. Wang, "Optimal Cloud Computing Resource Allocation for Demand Side Management", IEEE Transactions on Smart Grid, vol 8, no 99, pp. 1943 - 1955, Jul. 2017.

[99] N. Popovic, D. Popovic, and I. Seskar, "A novel cloud-based Advanced Distribution Management System solution", IEEE Transactions on Industrial Informatics, vol 14, no 8, pp. 3469-3476, Aug. 2018.

[100] David G. Rosado, Rafael Gómez, Daniel Mellado and Eduardo Fernández-Medina, "Security Analysis in the Migration to Cloud Environments", doi:10.3390/fi4020469, Future Internet 2012.

[101] Holland, R. Ten Steps to Successful Cloud Migration; Eagle Genomics Ltd.: Cambridge, MA, USA, 2011.

[102] C. Alcaraz et al., "Managing Incidents in Smart Grids a la Cloud," in Proceedings - 2011 3rd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2011, 2011, pp. 527–531.

[103] F. Ma et al., "Cloud Computing for Power System Simulations at ISO New England - Experiences and Challenges," IEEE Trans. Smart Grid, vol. 7, no. 6, pp. 2596–2603, Nov. 2016.

[104] Y. Simmhan et al., "Cloud-Based Software Platform for Big Data Analytics in Smart Grids," Computing in science & Engineering, vol.15. no 4. Pp 38-47, 2013.

[105] Y. Xin et al., "Virtual Smart Grid Architecture and Control Framework," 2011 IEEE Int. Conf. Smart Grid Commun. SmartGridComm 2011, pp. 1–6, 2011.

[106] M. Kralj, P. Kazmi, and A. Ruth, An Overview of Cloud Adoption Framework. Amazon Web Services, 2015.

[107] B. Briggs and E. Kassner, *Enterprise Cloud Strategy*. Redmond: Microsoft Press, 2016.

[108] J. Alonso, L. Orue-Echevarria, M. Escalante, J. Gorroñogoitia, and D. Presenza, "Cloud modernization assessment framework: Analyzing the impact of a potential migration to Cloud," in c2013 IEEE 7th International Symposium on the Maintenance and Evolution of *Service-Oriented and Cloud-Based Systems, MESOCA 2013,* 2013, pp. 64–73.

[109] L. O.-E. Arrieta, "From Software as a good to software as a service: Preparing the evolution of software products into the cloud," Int. Work. Maint. Evol. Serv. Cloud-Based Syst. (MESOCA - ICSM), pp. 58–59, 2012.

[110] A. Menychtas et al., "ARTIST methodology and framework: A novel approach for the migration of legacy software on the cloud," in Proceedings - 15th International

Symposium on Symbolic and Numeric Algorithms for Scientific Computing, SYNASC 2013, 2014, pp. 424–431.

[111] H. Bruneliere, J. Cabot, J. L. C. Izquierdo, L. O. E. Arrieta, O. Strauss, and M. Wimmer, “Software Modernization Revisited: Challenges and Prospects,” Computer (Long. Beach. Calif)., vol. 48, no. 8, pp. 76–80, 2015.

[112] J. Alonso, L. Orue-Echevarria, and M. Escalante, “Cloud compliant applications: A reference framework to assess the maturity of software applications with respect to cloud,” in 2015 IEEE 9th International Symposium on the Maintenance and Evolution of Service-Oriented Systems and Cloud-Based Environments, MESOCA 2015 - Proceedings, 2015, pp. 41–45.

[113] H. Trivedi, “Cloud Adoption Model for Governments and Large Enterprises,” Mit, no. May, p. 82, 2013.H. Trivedi, “Cloud Adoption Model for Governments and Large Enterprises,” Mit, no. May, p. 82, 2013.

[114] C. Pahl and H. Xiong, “Migration to PaaS clouds - Migration process and architectural concerns,” in c2013 IEEE 7th International Symposium on the Maintenance and Evolution of Service-Oriented and Cloud-Based Systems, MESOCA 2013, 2013, pp. 86–91.

[115] J. Zheng and W. Du, “Toward easy migration of client-server applications to the cloud,” ICSOFT-EA 2014 - Proc. 9th Int. Conf. Softw. Eng. Appl., pp. 101–108, 2014.

[116] Andy Wood, Ying He, Leandros A Maglaras, Helge Janicke, "A Security Architectural Pattern for Risk Management of Industry Control Systems within Critical National Infrastructure", Int. J. Electric and Hybrid Vehicles, Vol. x, No. x, 1–26, 2017.

[117] [100]David C. Mazur, Rob A. Entzminger, Pete A. Morell, John A. Kay, Erik Syme, "Defining the Industrial Demilitarized Zone and its Benefits for Mining Applications", DOI 10.1109/TIA.2016.2530045, IEEE Transactions on Industry Applications, 2016.

[118] International Electrotechnical Commission. Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. IEC 62443-3-3, Geneva, Switzerland, 2013.

[119] Chih-Che Suna, Adam Hahna, Chen-Ching Liua, "Cyber security of a power grid: State-of-the-art", Electrical Power and Energy Systems 99 45–56, 2018.

[120] Stefan Gheorghe, Nicolae Golovanov, George-Cristian Lazaroiu, Radu Porumb, "Smart Grid, Integration of Renewable Sources and Improvement of Power Quality", 21st International Conference on Control Systems and Computer Science, 2017.

[121] Erik Burger, Victoria Mittelbach, Anne Koziolek, " View-based and Model-driven Outage Management for the Smart Grid", Institute for Program Structures and Data Organization, Chair for Software Design and Quality Karlsruhe Institute of Technology, Karlsruhe, Germany, 2016.

[122] K. Kent, M. Souppaya "NIST Special Publication 800–92 Guide to Computer Security Log Management", September 2006.

[123] Stefan Marksteiner, Heribert Vallant, Kai Nahrganga, "Cyber security requirements engineering for low-voltage distribution smart grid architectures using threat modeling", Journal of Information Security and Applications, 2019.

[124] Zakaria El Mrabet, Naima Kaaboucha, Hassan El Ghazi, Hamid El Ghazi, "Cyber-security in smart grid: Survey and challenges", Computers and Electrical Engineering, 469–482, 2018.

[125] Michael J. Assante and Robert M. Lee, "The Industrial Control System Cyber Kill Chain", October 2015.

[126] Muhammed Zekeriya Gunduz, Resul Das, „Cyber-security on smart grid: Threats and potential solutions", Computer Networks 169, 2020.

[127] Anibal Sanjab, Walid Saad, Ismail Guvenc, Arif Sarwat and Saroj Biswas, „Smart Grid Security: Threats, Challenges, and Solutions", arXiv:1606.06992v1 [cs.IT] 22 Jun 2016.

[128] Abdulrahaman Okino Otuoze, Mohd Wazir Mustafa, Raja Masood Larik, „Smart grids security challenges: Classification by sources of threats", Journal of Electrical Systems and Information Technology 5, 468–483, 2018.

[129] J. Rittinghouse and J. Ransome, “Cloud Computing Implementation, Management, and Security,” CRC Press, 2010.

[130] R. C. Green et al., “Applications and Trends of High Performance Computing for Electric Power Systems: Focusing on Smart Grid,” IEEE Trans. Smart Grid, vol. 4, no. 2, pp. 922–931, Jun. 2013.

[131] E. Roloff et al., “High Performance Computing in the Cloud: Deployment, Performance and Cost Efficiency,” IEEE Int. Conf. Cloud Comput. Technol. Sci., pp. 371–378, 2012.

[132] S. Bera et al., “Cloud Computing Applications for Smart Grid: A Survey,” IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 5, pp. 1477–1494, May 2015.

[133] Dharmesh Faquir, Nestoras Chouliaras, Vlachou Sofia, Kalopoulou Olga, Leandros Maglaras, “Cybersecurity in smart grids, challenges and solutions”, AIMS Electronics and Electrical Engineering, Volume 5, Issue 1: 24-37. doi: 10.3934/electreng.2021002, 2021.

[134] Imran Ghafoor, Imran Jattala, Shakeel Durrani, Ch Muhammad Tahir, “Analysis of OpenSSL Heartbleed vulnerability for embedded systems”, 17th IEEE International Multi Topic Conference 2014.

[135] Arash Anzalchi, Arif Sarwat, “A survey on security assessment of metering infrastructure in Smart Grid systems”, SoutheastCon 2015, IEEE Xplore, 25. June 2015.

[136] R. C. Diovu, J. T. Agee, “Quantitative analysis of firewall security under DDoS attacks in smart grid AMI networks”, 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON), 7-10 Nov. 2017.

[137] Gogić D., Jelačić B., Lendak I. (2019), “Simulation-based evaluation of DDOS against smart grid SCADAs”, 5th Workshop on the Security of Industrial Control Systems & Cyber-Physical Systems (CyberICPS 2019), Luxembourg, Luxembourg.

[138] Yassine Mekdad, Giuseppe Bernieri, Mauro Conti, Abdeslam El Fergougui, “The Rise of ICS Malware: A Comparative Analysis”, ESORICS 2021: Computer Security. ESORICS 2021 International Workshops pp 496-511, 2021.

БИОГРАФИЈА

Бојан Јелачић је рођен 10.08.1988. у Мостару. Основну школу "Ристо Пророковић" је завршио 2003. године у Кифином Селу, а гимназију "Алекса Шантић" 2007. године у Невесињу. Исте године уписује Факултет техничких наука у Новом Саду, на коме завршава основне студије 2011., мастер студије 2012. и специјалистичке 2015. године када и уписује докторске студије.

Од 2012. године је запослен у компанији „*Schneider Electric DMS NS*", док је у истој компанији имао ангажман као стипендиста дуже од две године. Почео је као развојни инжењер, потом као груповођа, а од марта 2022. године као сениор груповођа где се и данас налази.

Ангажован је и на Факултету техничких наука. У звање асистента-мастера је изабран 2016. године. Тренутно држи вежбе из предмета Архитектура дистрибуираних система и Индустријски комуникациони протоколи у Електроенергетским системима са непуним радним временом. Године 2015. уписао је докторске студије на студијском програму Енергетика, електроника и телекомуникације, на Факултету техничких наука у Новом Саду. Положио је све испите предвиђене планом и програмом. Коаутор је на два научна рада обајвљена у међународним часописима, раду у националном часопису, као и шест радова објављених у саопштењима са међународних скупова.

Ожењен и отац једног детета.

ДОДАТАК А – ПРОТОТИП ОБРАСЦА АКУМУЛИРАНЕ ПРОЦЕНЕ РИЗИКА НА ЕНГЛЕСКОМ ЈЕЗИКУ

Табела 47 - Prototype of the accumulated risk assessment

Threat / Component	**OT component #1**		**…**		**OT component #N**	
	Impact	Likelihood			Impact	Likelihood
Threat #1						
Threat #2						
…						
Threat # N						

Овај Образац чини саставни део докторске дисертације, односно докторског уметничког пројекта који се брани на Универзитету у Новом Саду. Попуњен Образац укоричити иза текста докторске дисертације, односно докторског уметничког пројекта.

План третмана података

Назив пројекта/истраживања
Методологија за безбедну примену рачунарства у облаку у надзору и управљању паметним електроенергетским системима
Назив институције/институција у оквиру којих се спроводи истраживање
а) **Универзитет у Новом Саду, Факултет Техничких Наука** б) в)
Назив програма у оквиру ког се реализује истраживање
Истраживање се реализује у оквиру израде докторске дисертације на студијском програму Енергетика, Електроника и телекомуникације.
1. Опис података
1.1 Врста студије *Укратко описати тип студије у оквиру које се подаци прикупљају* **Докторска дисертација** _____ 1.2 Врсте података а) **квантитативни** б) **квалитативни** 1.3. Начин прикупљања података а) анкете, упитници, тестови

б) клиничке процене, медицински записи, електронски здравствени записи

в) генотипови: навести врсту _____

г) административни подаци: навести врсту _____

д) узорци ткива: навести врсту_____

ђ) снимци, фотографије: навести врсту_____

е) текст, навести врсту _____

ж) мапа, навести врсту _____

з) остало: описати **рачунарски експерименти**

1.3 Формат података, употребљене скале, количина података

1.3.1 Употребљени софтвер и формат датотеке:

a) Excel фајл, датотека _____

b) SPSS фајл, датотека _____

c) PDF фајл, датотека _____

d) Текст фајл, датотека _____

e) JPG фајл, датотека _____

f) Остало, датотека **.xml**

1.3.2. Број записа (код квантитативних података)

а) број варијабли **велики број**

б) број мерења (испитаника, процена, снимака и сл.) **велики број**

1.3.3. Поновљена мерења

а) **да**

б) не

Уколико је одговор да, одговорити на следећа питања:

а) временски размак између поновљених мера је **променљив**

б) варијабле које се више пута мере односе се на **време извршавања**

в) нове верзије фајлова који садрже поновљена мерења су именоване као _____

Напомене: _____

Да ли формати и софтвер омогућавају дељење и дугорочну валидност података?

а) ***Да***

б) Не

Ако је одговор не, образложити _____

_____

2. Прикупљање података

2.1 Методологија за прикупљање/генерисање података

2.1.1. У оквиру ког истраживачког нацрта су подаци прикупљени?

а) експеримент, навести тип **рачунарски експеримент**

б) корелационо истраживање, навести тип _____

ц) анализа текста, навести тип **Анализа доступне литературе**

д) остало, навести шта _____

2.1.2 Навести врсте мерних инструмената или стандарде података специфичних за одређену научну дисциплину (ако постоје).

_____

_____

2.2 Квалитет података и стандарди

2.2.1. Третман недостајућих података

а) Да ли матрица садржи недостајуће податке? Да **Не**

Ако је одговор да, одговорити на следећа питања:

а) Колики је број недостајућих података? _____

б) Да ли се кориснику матрице препоручује замена недостајућих података? Да Не

в) Ако је одговор да, навести сугестије за третман замене недостајућих података

_____

2.2.2. На који начин је контролисан квалитет података? Описати

Квалитет података је контролисан поређењем експерименталних и теоријских података

Квалитет података је контролисан поређењем експерименталних и теоријских података

2.2.3. На који начин је извршена контрола уноса података у матрицу?

Контрола уноса података је изведена на бази експертног знања

_____

3. Третман података и пратећа документација

1.1. Третман и чување података

3.1.1. Подаци ће бити депоновани у **Универзитет у Новом Саду** *репозиторијум.*

3.1.2. URL адреса https://www.cris.uns.ac.rs/searchDissertations.jsf

3.1.3. DOI _____

3.1.4. Да ли ће подаци бити у отвореном приступу?

а) ***Да***

б) *Да, али после ембарга који ће трајати до _____*

в) *Не*

Ако је одговор не, навести разлог _____

3.1.5. Подаци неће бити депоновани у репозиторијум, али ће бити чувани.

Образложење

_____

_____

3.2 Метаподаци и документација података

3.2.1. Који стандард за метаподатке ће бити примењен? **Стандард који примењује Репозиторијум докторских дисертација Универзитета у Новом Саду**

3.2.1. Навести метаподатке на основу којих су подаци депоновани у репозиторијум.

_____

_____

Ако је потребно, навести методе које се користе за преузимање података, аналитичке и процедуралне информације, њихово кодирање, детаљне описе варијабли, записа итд.

_____

_____

_____

_____

3.3 Стратегија и стандарди за чување података

3.3.1. До ког периода ће подаци бити чувани у репозиторијуму? _____

3.3.2. Да ли ће подаци бити депоновани под шифром? **Да** Не

3.3.3. Да ли ће шифра бити доступна одређеном кругу истраживача? **Да** Не

3.3.4. Да ли се подаци морају уклонити из отвореног приступа после извесног времена?

Да **Не**

Образложити

_____

_____

4. Безбедност података и заштита поверљивих информација

Овај одељак МОРА бити попуњен ако ваши подаци укључују личне податке који се односе на учеснике у истраживању. За друга истраживања треба такође размотрити заштиту и сигурност података.

4.1 Формални стандарди за сигурност информација/података

Истраживачи који спроводе испитивања с људима морају да се придржавају Закона о заштити података о личности (*https://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html*) и одговарајућег институционалног кодекса о академском интегритету.

4.1.2. Да ли је истраживање одобрено од стране етичке комисије? Да **Не**

Ако је одговор Да, навести датум и назив етичке комисије која је одобрила истраживање

_____

4.1.2. Да ли подаци укључују личне податке учесника у истраживању? Да **Не**

Ако је одговор да, наведите на који начин сте осигурали поверљивост и сигурност информација везаних за испитанике:

а) Подаци нису у отвореном приступу

б) Подаци су анонимизирани

ц) Остало, навести шта

_____

_____

5. Доступност података

5.1. Подаци ће бити

а) ***јавно доступни***

б) доступни само уском кругу истраживача у одређеној научној области

ц) затворени

Ако су подаци доступни само уском кругу истраживача, навести под којим условима могу да их користе:

_____

_____

Ако су подаци доступни само уском кругу истраживача, навести на који начин могу приступити подацима: _____

_____

5.4. Навести лиценцу под којом ће прикупљени подаци бити архивирани.

ауторство - некомерцијално

6. Улоге и одговорност

6.1. Навести име и презиме и мејл адресу власника (аутора) података

Бојан Јелачић, bojan.jelacic@uns.ac.rs

6.2. Навести име и презиме и мејл адресу особе која одржава матрицу с подацима

Бојан Јелачић, bojan.jelacic@uns.ac.rs

6.3. Навести име и презиме и мејл адресу особе која омогућује приступ подацима другим истраживачима

Бојан Јелачић, bojan.jelacic@uns.ac.rs