



УНИВЕРЗИТЕТ У НОВОМ САДУ  
**ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА У  
НОВОМ САДУ**

---



Драган Ерић

# **Напредна контрола приступа у паметним мрежама**

МАСТЕР РАД

Нови Сад, 2019



УНИВЕРЗИТЕТ У НОВОМ САДУ • ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА  
21000 НОВИ САД, Трг Доситеја Обрадовића 6

## КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА


Редни број, <b>РБР</b> :	
Идентификациони број, <b>ИБР</b> :	
Тип документације, <b>ТД</b> :	Монографска публикација
Тип записа, <b>ТЗ</b> :	Текстуални штампани документ/ ЦД
Врста рада, <b>ВР</b> :	Мастер рад
Аутор, <b>АУ</b> :	Драган Ерић
Ментор, <b>МН</b> :	др Дарко Чапко, ванр. професор
Наслов рада, <b>НР</b> :	Напредна контрола приступа у паметним мрежама
Језик публикације, <b>ЈП</b> :	Српски (писмо – латиница)
Језик извода, <b>ЈИ</b> :	Српски/енглески
Земља публиковања, <b>ЗП</b> :	Србија
Уже географско подручје, <b>УГП</b> :	Војводина
Година, <b>ГО</b> :	2019
Издавач, <b>ИЗ</b> :	Ауторски репринт
Место и адреса, <b>МА</b> :	Факултет техничких наука (ФТН), Д. Обрадовића 6, 21000 Нови Сад
Физички опис рада, <b>ФО</b> : (поглавља/страна/ цитата/табела/слика/графика/прилога)	8/32/28/6/19/0/0
Научна област, <b>НО</b> :	Електротехничко и рачунарско инжењерство
Научна дисциплина, <b>НД</b> :	Примењено софтверско инжењерство
Предметна одредница/Кључне речи, <b>ПО</b> :	Контрола приступа, РБАЦ, АОР, Смарт Грид
<b>УДК</b>	
Чува се, <b>ЧУ</b> :	Библиотека ФТН, Д. Обрадовића 6, 21000 Нови Сад
Важна напомена, <b>ВН</b> :	
Извод, <b>ИЗ</b> :	Проширење основне контроле приступа засноване на корисничким улогама (енгл. Role Based Access Control - RBAC) ентитетом АОР-а (енгл. Area of Responsibility), уз имплементацију сервиса за прикупљање и управљање догађајима и алармима у паметним мрежама.
Датум прихватања теме, <b>ДП</b> :	
Датум одбране, <b>ДО</b> :	
Чланови комисије, <b>КО</b> :	Председник: др Срђан Вукмировић, ванр. професор
	Члан: др Немања Недић, доцент
	Члан, ментор: др Дарко Чапко, ванр. професор
	Потпис ментора



UNIVERSITY OF NOVI SAD • FACULTY OF TECHNICAL SCIENCES  
21000 NOVI SAD, Trg Dositeja Obradovića 6

## KEY WORDS DOCUMENTATION

Accession number, <b>ANO</b> :			
Identification number, <b>INO</b> :			
Document type, <b>DT</b> :	Monographic publication		
Type of record, <b>TR</b> :	Textual material, printed/CD		
Contents code, <b>CC</b> :	Master's thesis		
Author, <b>AU</b> :	Dragan Erić		
Mentor, <b>MN</b> :	dr Darko Čapko, vanr. profesor		
Title, <b>TI</b> :	Advanced Access Control In Smart Grid		
Language of text, <b>LT</b> :	Serbian		
Language of abstract, <b>LA</b> :	Serbian/English		
Country of publication, <b>CP</b> :	Serbia		
Locality of publication, <b>LP</b> :	Vojvodina		
Publication year, <b>PY</b> :	2019		
Publisher, <b>PB</b> :	Author's reprint		
Publication place, <b>PP</b> :	Faculty of Technical Sciences, D. Obradovića 6, 21000 Novi Sad		
Physical description, <b>PD</b> : (chapters/pages/ref./tables/pictures/graphs/appendixes)	8/32/28/6/19/0/0		
Scientific field, <b>SF</b> :	Electrical and computer engineering		
Scientific discipline, <b>SD</b> :	Applied software engineering		
Subject/Key words, <b>S/KW</b> :	Access Control, RBAC, AOR, Smart Grid		
<b>UC</b>			
Holding data, <b>HD</b> :	Library of Faculty of Technical Sciences, D. Obradovića 6, 21000 Novi Sad		
Note, <b>N</b> :			
Abstract, <b>AB</b> :	Extension of Role Based Access Control (RBAC) by AOR (Area of Responsibility) with the implementation of event and alarm collection service in Smart Grid.		
Accepted by the Scientific Board on, <b>ASB</b> :			
Defended on, <b>DE</b> :			
Defended Board, <b>DB</b> :	President:	Dr. Srđan Vukmirović, Associate professor	
	Member:	Dr Nemanja Nedić, Assistant Professor	Menthor's sign
	Member, Mentor:	Dr Darko Čapko, Associate Professor	

	УНИВЕРЗИТЕТ У НОВОМ САДУ • ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА 21000 НОВИ САД, Трг Доситеја Обрадовића 6	Број:
	<b>ЗАДАТАК ЗА МАСТЕР РАД</b>	Датум:

(Податке уноси предметни наставник - ментор)

СТУДИЈСКИ ПРОГРАМ:	Примењено софтверско инжењерство
РУКОВОДИЛАЦ СТУДИЈСКОГ ПРОГРАМА:	др. Драган Поповић, ред. проф.

Студент:	Драган Ерић	Број индекса:	Е5 28/2018
Област:	Електротехничко и рачунарско инжењерство		
Ментор:	др Дарко Чапко, ванр. професор		
НА ОСНОВУ ПОДНЕТЕ ПРИЈАВЕ, ПРИЛОЖЕНЕ ДОКУМЕНТАЦИЈЕ И ОДРЕДБИ СТАТУТА ФАКУЛТЕТА ИЗДАЈЕ СЕ ЗАДАТАК ЗА МАСТЕР РАД, СА СЛЕДЕЋИМ ЕЛЕМЕНТИМА: <ul style="list-style-type: none"> <li>- проблем – тема рада;</li> <li>- начин решавања проблема и начин практичне провере резултата рада, ако је таква провера неопходна;</li> </ul>			

### НАСЛОВ МАСТЕР РАДА:

Напредна контрола приступа у паметним мрежама
---

### ТЕКСТ ЗАДАТКА:

Приликом дефинисања теме рада, постављени су следећи задаци: <ul style="list-style-type: none"> <li>- Анализирати развијене методологије у области контроле приступа у оквиру софтверских апликација</li> <li>- Истражити достигнућа у области контроле приступа у Smart Grid системима</li> <li>- Развити напредну контролу приступа</li> <li>- Тестирати развијену апликацију</li> </ul>
--

Руководилац студијског програма:	Ментор рада:

Примерак за: <input type="radio"/> - Студента; <input type="radio"/> - Ментора
--

## SPISAK KORIŠĆENIH SKRAĆENICA

AOR	Area Of Responsibility
CE	Calculation Engine
CIA	Confidentiality, Integrity, Availability
CNSS	Committee on National Security Systems
DER	Distributed Energy Resource
DERMS	Distributed Energy Resource Management System
DOE	Department of Energy
EPRI	Electric Power Research Institute
HMI	Human Machine Interface
LINQ	Language Integrated Query
NMS	Network Model Service
PIN	Personal Identification Number
RBAC	Role-Based Access Control
SCADA	Supervisory Control And Data Acquisition
SQL	Structured Query Language
TSDB	Time Series Database
UI	User Interface
WCF	Windows Communication Foundation
WFS	Weather Forecast Service
WPF	Windows Presentation Foundation
XMPP	eXtensible Message and Presence Protocol

## SADRŽAJ

1.	Uvod.....	6
2.	Teorijske osnove.....	7
	2.1 Tradicionalni elektroenergetski sistemi.....	7
	2.2 Smart Grid.....	8
	2.3 Informaciona bezbjednost .....	10
	2.4.1 Mandatorni model kontrole pristupa .....	11
	2.4.2 Diskrecioni model kontrole pristupa .....	12
	2.4.3 Model kontrole pristupa zasnovan na korisničkim ulogama – RBAC model.....	12
	2.5 Postojeće primjene RBAC modela u pametnim mrežama .....	15
3.	Arhitektura Smart Grid sistema .....	16
	3.3 Calculation Engine - CE .....	17
	3.4 Weather Forecast Service .....	17
	3.5 Remote Telemetry Unit – RTU.....	17
	3.6 Modbus Slave .....	17
	3.7 Modbus Simulator.....	18
	3.8 DERMS korisnički interfejs .....	18
4.	Implementacija napredne kontrole pristupa .....	20
	4.1 AOR Cache.....	21
	4.2 AOR Servis.....	22
	4.2.1 Manipulacija dodijeljenim AOR-ima – AOR Board.....	22
	4.2.2 Sinhronizacija AOR entiteta preko AOR Supervisor aplikacije.....	23
	4.3 Servis za obradu događaja i alarma .....	25
	4.3.1 Obrada događaja - Event-a.....	25
	4.3.2 Obrada alarmantih događaja - Alarma.....	25
5.	Testiranje napredne kontrole pristupa u okviru Smart Grid aplikacije.....	27
	5.1 Skup permisija u sistemu .....	28
	5.2 Skup uloga u sistemu .....	28
6.	Zaključak.....	32
7.	Literatura .....	33
8.	Podaci o kandidatu .....	35

## 1. Uvod

Pametne mreže (eng. *Smart Grid*) karakteriše veliki broj korisnika, kritičnih resursa i funkcionalnosti kojima je potrebno upravljati na adekvatan način kako bi bili dostupni svim korisnicima. Tradicionalni elektroenergetski sistemi prolaze kroz duboke promjene koje su rezultovale novim izazovima u procesu upravljanja i nadzora. Ranije fizički izolovan sistem, sa minimalnim mjerama zaštite ljudskog elementa i uređaja na mreži, danas mora biti prilagođen novim bezbjednosnim prijetnjama. Takve bezbjednosne prijetnje nisu postojale dok se u elektroenergetski sistem nije počeo uvoditi sve veći broj pristupnih tačaka za razmjenu podataka.

Potrebno je naglasiti važnost izuzetne moći obnovljivih izvora energije kao i njihovog priključivanja na distributivne mreže stvaranjem distribuiranih energetske resursa (eng. *Distributed Energy Resource* – skr. DER). Na taj način je započeo tranzitivni proces prelaska tradicionalnih pasivnih distributivnih mreža do aktivnih distributivnih sistema, tako da rast entuzijazma za priključivanjem DER-ova poslednjih godina enormno raste. Stručnjaci prognoziraju da će rast biti sve veći. Sve ovo dovodi do toga da je danas distributivna mreža veoma kompleksna i gotova nemoguća za kontrolu tradicionalnim načinima.

Kao što je opisano u [1], obnovljivi izvori energije poput sunca ili energije vjetra postaju sve važniji za stvaranje ekološki održive energije i tako smanjuju efekat staklene bašte koji vodi do globalnog zagrijavanja. Integriranje ovih distribuiranih energetske resursa u postojeću mrežu za distribuciju električne energije predstavlja velike izazove za automatizaciju energije: DER treba nadgledati i kontrolisati na sličan nivo kao centralizovanu proizvodnju energije u elektranama kako bi se održala stabilnost frekvencije elektroenergetske mreže. Pošto su DER-ovi obično geografski raštrkani, široko rasprostranjene komunikacione mreže potrebne su za razmjenu upravljačkih poruka ne samo između DER-a i kontrolnog centra već i između DER-ova [2].

Termin kontrola pristupa odnosi se na kontrolu pristupa sistemskim resursima nakon što su autentifikovani kredencijali korisničkog naloga i identitet, i pristup sistemu odobren. Cilj kontrole pristupa jeste ograničenje akcija ili radnji koje legitimni korisnik računarskog sistema može da obavlja. Korisniku pod kontrolom pristupa zasnovanoj na korisničkim ulogama (eng. *Role Based Access Control*, skr. RBAC) može biti dodijeljena samo jedna uloga u organizaciji. Npr. uloga programera može biti dodijeljena softverskom inženjeru. Pored toga, ne postoji način da se pojedinačnim korisnicima pruže dodatne dozvole koje nadmašuju one dostupne za njihovu ulogu. Gore opisani programer ima iste dozvole kao i svi drugi programeri, ništa više i ništa manje [3]. AOR (eng. *Area Of Responsibility*) kontrola pristupa, odnosno kontrola pristupa prema oblasti odgovornosti, predstavlja određeni vid nadogradnje RBAC modela. Oblast odgovornosti podrazumijeva skup dopuštenih operacija nad objektima koji imaju zajedničke karakteristike u okviru elektroenergetskog sistema [4]. Kako bi se ispitalo u kojoj mjeri je predloženo rješenje uspješno, prezentovana je softverska platforma za nadgledanje i upravljanje dijelom pametne mreže, koji obuhvata obnovljive izvore energije.

U drugom poglavlju rada su date neophodne teorijske osnove za sprovođenje istraživanja. Opisani su tradicionalni elektroenergetski sistemi, kao i pametne elektroenergetske mreže. Navedeni su osnovni koncepti o bezbjednosti, jer iskorišćavanje bezbjednosnih propusta kritičnih resursa koje Smart Grid sadrži može dovesti do ozbiljnih posljedica u funkcionisanju elektroenergetskih sistema. Uvedeni su osnovni termini vezani za RBAC model i prikazana je njegova organizacija po komponentama.

U trećem poglavlju rada prikazana je arhitektura i način rada jedne proste Smart Grid aplikacije, koja se koristi kao platforma za nadgledanje i kontrolisanje rada distribuiranih izvora električne energije.

Četvrto poglavlje rada sadrži proširenu arhitekturu sistema (u odnosu na arhitekturu opisanu u poglavlju 2) naprednom kontrolom pristupa. Opisano je funkcionisanje servisa za prikupljanje i upravljanje događajima.

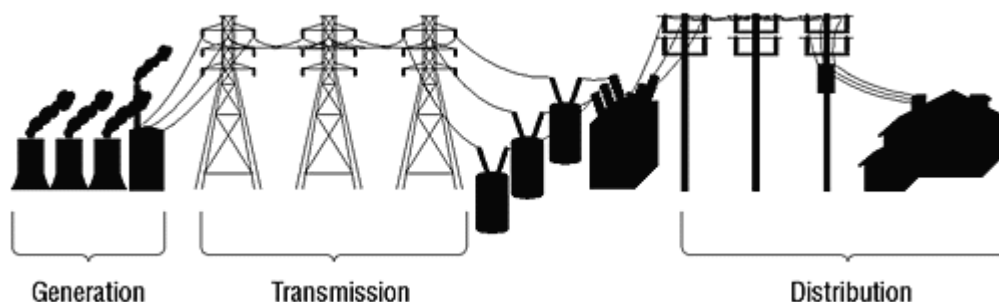
Peto poglavlje prikazuje uporedne karakteristike RBAC i proširenog modela.

## 2. Teorijske osnove

### 2.1 Tradicionalni elektroenergetski sistemi

Većina postojećih elektroenergetskih sistema danas ima zajedničke karakteristike. Na slici 1 su prikazane tri glavne cjeline elektroenergetskih sistema:

- proizvodnja u velikim elektranama,
- prenosna mreža, za prenos energije na visokom naponu i na velika rastojanja do krajnje potrošnje,
- srednjenaponska i niskonaponska distributivna mreža, koja dovodi energiju do krajnjih korisnika (domaćinstva, komercijalni ili industrijski potrošači).



Slika 1 Struktura elektroenergetskih sistema [5]

U klasičnim sistemima tok energije je jednosmjernan, od transmisije do distribucije i od velikih (eng. *bulk*) generatora ka potrošačima. U proizvodnom podsystemu se vrši transformacija različitih oblika energije (ugalj, voda, nuklearna energija) u električnu energiju. Proizvodni sistem čine generatori, koji su koncentrisani u veće tehničko-tehnološke cjeline – elektrane i dislocirani su od potrošača. Distribucija električne energije zasniva se na koncepciji izvoda (eng. *feeder*) koji predstavljaju dovoljno jake elektroenergetske veze kojima se mogu pridružiti veći dijelovi jednog potrošačkog područja. Izvodi sa svojim grananjem, sve do mjesta priključka individualnih potrošača čine distributivni podsystem, odnosno distributivnu mrežu [6]. Bilo bi netačno tvrđenje da elektroenergetski sistemi u prošlosti nisu bili kompleksni, ali uvođenjem sve većeg broja distribuiranih izvora električne energije postaju još složeniji.

Distributivna mreža je postala aktivna, dinamična i danas distributivni sloj može preuzeti na sebe dio proizvodnih i kontrolnih obaveza i na taj način može rasteretiti opterećen prenosni sistem. Direktna posljedica novih scenarija je kreirala jaču vezu između elektroenergetskih sistema sa drugim infrastrukturama, kao što su komunikacije ili druge energetske infrastrukture (npr. gasovodi). Koherentne infrastrukturne operacije i jedinstvene interakcije između proizvodnje, transmisije i distribucije, čine komunikacije kritičnijim nego ikada [7]. Za međuzavisne mreže, neophodna je distribucija funkcija kontrole i nadgledanja, zasnovana na principima automatizacije.

Konstantan porast zavisnosti od električne energije za obavljanje svakodnevnih aktivnosti prouzrokovao je da tradicionalni sistemi postanu neodrživi. Jedan od glavnih razloga kompleksnosti elektroenergetskih sistema jeste povećanje infrastrukturnih međuzavisnosti. Kako se ne bi narušila tri osnovna načela elektroenergetskih sistema (pouzdanost, sigurnost i ekonomičnost) elektroenergetski sistemi su morali da se razvijaju. Uvođenjem novih komunikacionih i informacionih tehnologija, pozivajući na decentralizovaniji pristup sistemskim funkcijama nadgledanja i kontrole, elektroenergetski sistem prerasta u inteligentnu mrežu (eng. *Smart Grid*) [6].

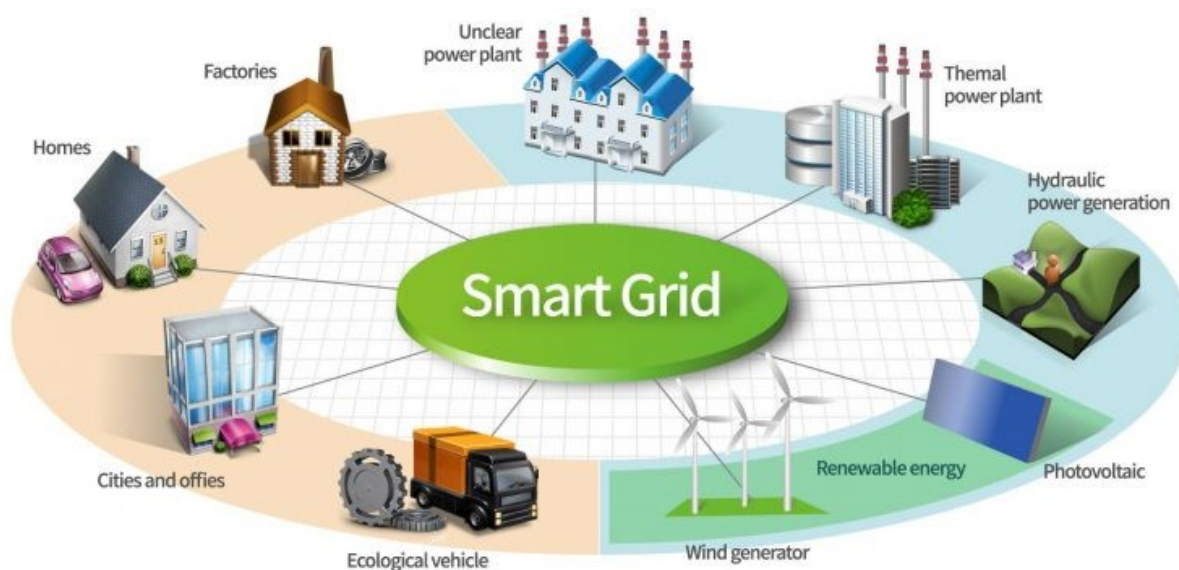


## 2.2 Smart Grid

Proces modernizacije elektroenergetskih sistema podrazumijeva integraciju tradicionalnih elektroenergetskih sistema sa brojnim naprednim sistemima, kao što su nadzorno-upravljački računarski sistemi za automatizaciju procesa upravljanja električnom energijom i optimizaciju potrošnje u zavisnosti od uslova snabdijevanja, zatim napredni mjerni sistemi za upravljanje potrošnjom i brojlama električne energije, automatizovani sistemi za naplatu i drugi sistemi za upravljanje poslovnim procesima elektroenergetske kompanije [7].

Evropska Tehnološka Platforma definiše pametnu mrežu kao energetska mrežu koja može na inteligentan način integrisati sve akcije korisnika povezanih na nju: generatore, potrošače ili oboje, sve u cilju efikasnije, ekonomičnije i sigurnije distribucije [8].

Na slici 2 je prikazana tipična *Smart Grid* infrastruktura.



Slika 2 Smart Grid infrastruktura [9]

Primarno pitanje nije šta je to Smart Grid, već koje benefite on donosi preduzećima, potrošačima, ekonomiji i životnoj sredini [10]. Definicije koje dovoljno dobro opisuju Smart Grid su:

- Inteligentna mreža [11] je elektroenergetska mreža koja može inteligentno integrisati akcije svih korisnika koji su na nju povezani, uključujući generatore, potrošače, ali i one koji obavljaju obe djelatnosti, u cilju efikasne isporuke električne energije, vodeći računa o održivosti, ekonomičnosti i sigurnosti elektroenergetskog sistema.
- U.S. DOE: Potpuno automatizovana elektroenergetska mreža koja nadgleda i kontroliše sve korisnike i čvorove, omogućavajući dvosmjerni tok informacija i električne energije između elektrane i krajnjih uređaja, kao i svih tačaka između njih [11].
- EPRI: Pojam Smart Grid se odnosi na modernizaciju sistema distribucije električne energije, tako što nadgleda, štiti i automatski optimizuje rad međusobno povezanih elemenata - počevši od centralnog i distributivnog generatora preko visokonaponskih vodova i distributivnog sistema, do industrijskih potrošača kao i izgradnje automatizovanih sistema, kao i do mjesta za skladištenje električne energije pa i do krajnjih korisnika i njihovih termostata, električnih vozila i raznih kućnih uređaja [12].

Smart Grid ne postoji kao zaseban proizvod. Umjesto toga, predstavlja integrisani skup tehnologija koji smanjuje troškove, pruža socijalne koristi „agentima“ i smanjuje zagađenje životne sredine. Postojećom elektroenergetskom mrežom se upravlja kompleksnim softverskim programima i automatizovanim rutinama i zaštićene su relejima zasnovanim na mikroprocesorima. Pred pametnim mrežama je i dalje dug razvojni put, i nastaviće se razvijati, vođene globalnim ekonomijama i

regulativama. Pametne mreže trebaju imati fokus na potrošačima, ne samo kroz pokušaj redukcije troškova električne energije nego i da pružaju i druge usluge [13].

Ključna komponenta, kako bi se efektivno u potpunosti ostvarila vrijednost realizacije pametnih mreža, jeste tehnologija sa funkcionalnostima i sposobnostima za postizanjem kohezivnih „end-to-end“ integrabilnih, skalabilnih i interoperabilnih rješenja.

Najveće dobiti od implementacije pametnih mreža jesu sledeći rezultati koji se mogu kvantifikovati [13]:

- Povećanje pouzdanosti, radnih performansi i cjelokupne produktivnosti.
- Efikasniji način dostavljanja električne energije do potrošača smanjuje potreban broj proizvodnih sistema i broj vodova koje treba izgraditi.
- Pouzdanija isporuka električne energije povećava energetska efikasnost, a dovodi do smanjenja emisije ugljen-dioksida.
- Pružanje mogućnosti korisnicima da na pametniji način koriste električnu energiju, davanjem uvida u cijenu električne energije u realnom vremenu.
- Optimizacija integracije obnovljivih izvora energije.

## 2.3 Informaciona bezbjednost

U poređenju sa tradicionalnim elektroenergetskim sistemima, Smart Grid mora u potpunosti integrisati dvosmjernu komunikaciju velike brzine, sa ogromnim brojem uređaja u polju, u cilju ostvarivanja dinamične i interaktivne infrastrukture. Međutim, takva zavisnost od prenosa podataka preko mreže neizbježno izlaže Smart Grid potencijalnim opasnostima, vezanim za komunikacione i mrežne sisteme. Zlonamjerni upadi u mrežu mogu dovesti do ozbiljnih posljedica u Smart Grid-u, od krađe korisničkih informacija do kaskadnih ispada i uništavanja infrastrukture.

Istorijski posmatrano, informaciona bezbjednost je definisana kao zaštita informacionih sistema protiv neautorizovanog pristupa ili modifikacija informacija bilo u skladištenju, obradi ili prenosu i protiv lišavanja usluga autorizovanih korisnika, uključujući neophodne mjere detekcije, dokumentovanja i otklanjanja takvih prijetnji [14].

Komitet Nacionalnih bezbjednosnih sistema (Committee on National Security Systems skr. CNSS) definiše informacionu sigurnost kao zaštitu informacija i njenih kritičnih elemenata, uključujući sisteme i hardver koji koristi, perzistira i prenosi datu informaciju. CNSS-ov model informacione bezbjednosti je nastao iz koncepta nastalog u industriji računarske bezbjednosti zvani CIA trijada [15]. CIA trijada (Slika 3) se zasniva na tri karakteristike informacija čije očuvanje je od značaja za organizaciju:

- povjerljivost (eng. *confidentiality*)
- integritet (eng. *integrity*)
- raspoloživost (eng. *availability*)



Slika 3 CIA trijada [16]

Raspoloživost omogućava autorizovanim korisnicima ili računarskim sistemima neometan pristup informacijama, u zahtijevanom obliku. Raspoloživost se najbolje osigurava rigoroznim održavanjem hardvera i korektnim funkcionisanjem ažuriranog operativnog sistema. Pružanje adekvatnog komunikacionog opsega i sprečavanje uskih grla su podjednako važni. Redundantnost, otpornost na otkaze, mogu da umanje ozbiljne posljedice kada dođe do hardverskih ispada [16].

Povjerljivost se može, grubo govoreći, poistovjetiti sa privatnošću [16]. Povjerljivost informacija podrazumijeva zaštićenost informacija od otkrivanja neautorizovanim licima ili sistemima. Povjerljivost obezbjeđuje da samo oni sa adekvatnim pravima i privilegijama mogu pristupiti informacijama. Kada neautorizovana osoba može pristupiti informacijama, povjerljivost je narušena [15]. Šifrovanje podataka (eng. *encryption*) predstavlja uobičajenu metodu za očuvanje povjerljivosti [16].

Integritet informacije postoji kada je ona neizmijenjena, konzistentna tokom čitavog svog životnog vijeka. Podaci ne smiju biti modifikovani u toku prenosa ili skladištenja informacije, i određeni koraci moraju biti preduzeti kako podaci ne bi bili promijenjeni od strane ljudi koji nisu autorizovani. [4][16]. Mnogi računarski virusi su eksplicitno namijenjeni za narušavanje integriteta podataka (eng. *data corruption*). Integritet informacija predstavlja kamen temeljac za informacione sisteme, zbog toga što informacija nema vrijednost ili upotrebljivost ukoliko korisnici ne mogu da verifikuju njen integritet [15].

Uvijek postoji mogućnost da se određene slabosti u sistemu iskoriste i eventualno mogu da dovedu do gubitka povjerljivosti, integriteta ili raspoloživosti informacionog sistema. Cilj informacione bezbjednosti jeste da se eliminišu ili smanje bezbjednosni rizici, kao i smanjenje posljedica eventualnih incidenata primjenom raznih bezbjednosnih mjera za prevenciju i detekciju napada, kao i reakciju na incidente [4]. Neke od bezbjednosnih mjera uključuju fajl permisije i korisničke kontrole pristupa (eng. *Access Controls*).

## 2.4 Kontrola pristupa

Cilj kontrole pristupa jeste ograničenje akcija ili radnji koje legitimni korisnik računarskog sistema može da obavlja [17]. Ključna uloga svakog sistema za kontrolu pristupa jeste identifikacija i autentifikacija korisnika. „AAA“ u sigurnosti predstavlja akronim za autentifikaciju (eng. *authentication*), autorizaciju (eng. *authorization*) i vođenje evidencije i analize događaja (eng. *auditing*).

Autentifikacija je proces u kome se potvrđuje da je korisnik onaj za koga se izdaje da jeste. Najčešća metoda je da korisnik prikaže korisničko ime da dokaže identitet, a zatim pomoću šifre da izvrši autentifikaciju. Najčešći tipovi autentifikacije su nešto [13]:

- što korisnik zna (korisnička šifra, PIN, neko lično pitanje kao što je ime prvog ljubimca),
- što korisnik posjeduje (pametne kartice, hardverski i softverski tokeni),
- što korisnik jeste (biometrijski podaci kao otisak prsta ili skeniranje retine).

Autorizacija predstavlja mapiranje autentifikovanih entiteta sa informacijama i pripadajućim nivoima pristupa. Kada se radi o autorizaciji korisnika, sistem radi provjeru da verifikuje svaki od entiteta i zatim daje pravo pristupa resursima samo tog entiteta. U autorizaciji članova grupe, sistem mapira autentifikovane entitete sa listom grupa, a nakon toga garantuje prava pristupa resursima bazirana na pravima pristupa grupe. Ovo je najčešći metod autorizacije. Treći metod je višesistemska autorizacija, u kojoj centralni autentifikacioni i autorizacioni sistem verifikuje identitet entiteta i dodjeljuje mu skup kredencijala [15].

Vođenje evidencije (eng. *accounting* ili *auditing*) odnosi se na praćenje aktivnosti korisnika i izvještavanje o relevantnim bezbjednosnim događajima u sistemu. Bezbjednosni sistemski događaji mogu biti neuspješni pokušaji da se pristupi nekom resursu, ali i legitimne, uspješno izvršene akcije. Akcije su ispraćene vremenskim zapisom, čime se omogućuje neporecivost [4]. Osnovni mehanizmi su logovi, kao što je npr. Security log u Windows sistemima.

Termin kontrola pristupa zapravo se odnosi na kontrolu pristupa sistemskim resursima nakon što su autentifikovani kredencijali korisničkog naloga i identitet i pristup sistemu odobren. Na primjer, određenom korisniku, ili grupi korisnika, može biti dozvoljen pristup samo određenim datotekama nakon prijavljivanja u sistem, dok se istovremeno uskraćuje pristup svim drugim resursima [3].

Postoje tri osnovne kategorije na koje se mogu podijeliti modeli kontrole pristupa: mandatorni (nediskrecioni) model, diskrecioni model kao i model zasnovan na korisničkim ulogama.

### 2.4.1 Mandatorni model kontrole pristupa

Mandatorni model kontrole pristupa (eng. *Mandatory Access Control*, skr. MAC) predstavlja model u kome se pristup bazira na klasifikaciji korisnika i objekata u sistemu od strane administratora sistema, zbog čega se ovaj model naziva i nediskrecioni model kontrole pristupa [4]. MAC je najstroži od svih nivoa kontrole, a kreiran je i korišten uglavnom od strane vlade.

Kontrola pristupa počinje sa sigurnosnim naljepnicama (eng. *security labels*) koje su dodijeljene svim resursnim objektima na sistemu. Ove sigurnosne naljepnice sadrže dvije informacije - klasifikaciju (strogo tajno, povjerljivo itd.) i kategoriju (koja je u suštini indikacija nivoa upravljanja ili projekta kojem je objekat dostupan). Slično tome, svaki korisnički nalog na sistemu takođe ima svojstva klasifikacije i kategorije iz istog skupa svojstava primjenjenih na objekte. Kada korisnik pokuša da pristupi resursu pod mandatornom kontrolom pristupa, operativni sistem provjerava korisničku klasifikaciju i kategorije i upoređuje ih sa svojstvima bezbjednosne naljepnice objekta. Da

bi korisnik mogao pristupiti određenom objektu, on mora imati dodijeljen nivo povjerenja jednak ili viši od nivoa definisanog za objekat kome pristupa [3].

Iako MAC pruža daleko najbezbjednije okruženje kontrole pristupa, prethodi mu značajno vrijeme potrebno za planiranje, a nameće visoke sistemske troškove upravljanja (stalno ažuriranje naljepnica objekata i korisnika u skladu sa promjenama kategorizacija i klasifikacija novih ili postojećih) [3].

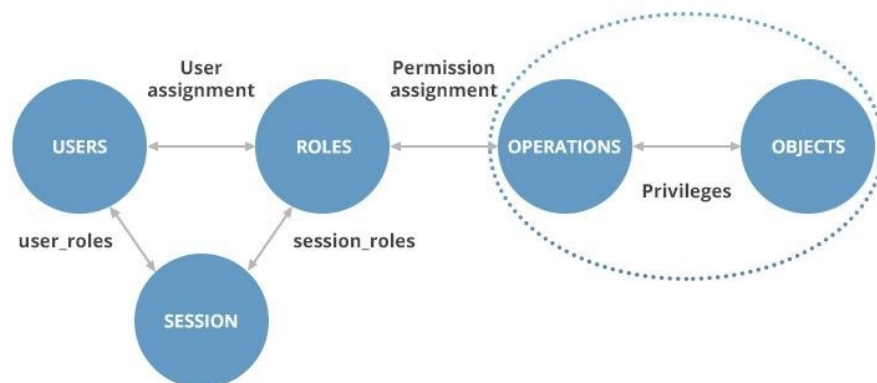
#### 2.4.2 Diskrecioni model kontrole pristupa

Diskretna kontrola pristupa (DAC) omogućava svakom korisniku da kontroliše pristup svojim podacima. DAC je obično podrazumijevani mehanizam kontrole pristupa za većinu desktop operativnih sistema. Umjesto bezbjednosne naljepnice u slučaju MAC-a, svaki objekat resursa na sistemu baziranom na DAC-u, ima pridruženu kontrolnu listu pristupa (eng. *Access Control List* skr. ACL). ACL sadrži listu korisnika i grupa kojima je korisnik dozvolio pristup zajedno sa nivoom pristupa za svakog korisnika ili grupu. Važno je napomenuti da pod DAC-om korisnik može postaviti samo dozvole pristupa za resurse koje već posjeduje.

Iako diskretna kontrola pristupa pruža dosta fleksibilnije okruženje u odnosu na MAC, sa sobom nosi rizik izlaganja podataka korisnicima koji ne trebaju nužno imati pristup [3].

#### 2.4.3 Model kontrole pristupa zasnovan na korisničkim ulogama – RBAC model

Model kontrole pristupa zasnovan na korisničkim ulogama (eng. *Role Based Access Control* skr. RBAC), u kome se pristup zasniva na korisnikovoj funkciji unutar organizacije [3]. U „role based“ sistemima glavna briga je zaštititi integritet informacija – “ko može izvršiti koju akciju, na kojoj informaciji”. Uloga (eng. *role*) predstavlja skup operacija koje korisnik ili više korisnika može izvršavati u kontekstu organizacije. Uloge su orijentisane ka grupama. Instanca korisnikove interakcije sa sistemom se zove sesija (eng. *session*)[19]. Permisije (eng. *permissions* ili *privileges*) su autorizacije za izvođenje odgovarajuće akcije u sistemu[19].



Slika 4 Osnovne RBAC komponente [20]

RBAC model je organizovan u četiri komponente, kao što je prikazano na slici 4 [21]:

- osnovni model (eng. *Core*)
- hijerarhijski (eng. *Hierarchical*)
- razdvajanje obaveza
  - statičko (eng. *Static Separation of Duty* – SSD)
  - dinamičko (eng. *Dynamic Separation of Duty* - DSD).

Osnovni RBAC model definiše skup entiteta i relacija koje čine RBAC model. Hijerarhijski RBAC uvodi pojam hijerarhije uloga kao način da se pojednostavi administracija modela u slučaju preklapanja korisničkih uloga po pitanju ovlašćenja unutar organizacije. Statičkim i dinamičkim razdvajanjem obaveza uvodi se pojam ograničenja u RBAC modelu, sa ciljem da se omogući ograničavanje dodjele konfliktnih uloga korisnicima [4].

RBAC modeli su sazreli do trenutka da su danas propisani kao generalizovani pristup kontroli pristupa. Ovi modeli su pokazali da su „neutralni u politici“ u smislu da se pomoću hijerarhija uloga i ograničenja može izraziti širok spektar sigurnosnih politika [Osborn et al. 2000]. Administracija bezbjednosti je takođe znatno pojednostavljena upotrebom uloga za organizovanje privilegija pristupa. Na primjer, ako korisnik pređe na novu funkciju unutar organizacije, korisnik može jednostavno biti dodijeljen novoj ulozi i uklonjen iz stare, dok u odsustvu RBAC modela stare dozvole korisnika moraju biti pojedinačno ukinute i nove dozvole bi morale biti odobrene [22].

Pored toga, možda će se morati primijeniti administrativna ograničenja kako bi se spriječila zloupotreba informacija i spriječile nedozvoljene aktivnosti. Tipično ograničenje ovlašćenja, široko rasprostranjeno i dobro poznato, je razdvajanje dužnosti (eng. *Separation of Duties* skr. SoD). Namjena SoD-a jeste smanjenje rizika od prevare tako što se ne dozvoljava nijednom pojedincu da ima dovoljno ovlašćenja unutar sistema da samostalno izvrši bilo kakvu prevaru. Takva ograničenja mogu se lako izraziti koristeći RBAC model preko SoD ograničenja na uloge, dodjeljivanjem uloga korisnicima i dodjeljivanjem permisija za ulogu. Osim toga, korišćenjem ograničenja za aktiviranje korisničkih uloga, korisnici se mogu prijaviti sa najmanjim skupom privilegija potrebnih za bilo koji pristup. U slučaju nenamjernih grešaka, takva dodjela minimalnog skupa može spriječiti eventualnu štetu [22].

Svrha bilo kog mehanizma kontrole pristupa jeste zaštita informacija i drugih resursa. Međutim, kada se govori o primjeni RBAC-a na računarske sisteme, govori se o zaštićenim objektima. Za sistem koji implementira RBAC, objekti mogu predstavljati informacione kontejnere (npr. datoteke, direktorijume u operativnom sistemu, ili kolone, redove, tabele i prikaze u okviru upravljanja bazom podataka) ili objekti mogu predstavljati iscrpljujuće systemske resurse kao što su štampač, prostor na disku i procesorski ciklusi. Pored toga, RBAC obezbeđuje kontekst za specifikacije i sprovođenje složenih bezbjednosnih politika koje su često nepraktične ili ih je čak nemoguće sprovesti putem direktne upotrebe konvencionalnim mehanizmima kontrole pristupa [23].

RBAC podržava nekoliko poznatih sigurnosnih principa i politika važnih za komercijalna i državna preduzeća koja obrađuju neklasifikovane, ali osjetljive informacije [Ferraiolo et al. 1993; van Solms i van der Merve 1994] [23].

Nisu sve RBAC karakteristike pogodne za sva okruženja niti dobavljači nužno implementiraju sva RBAC svojstva. Kao takav, ovaj standard obezbeđuje metod objedinjavanja svojstava kroz izbor funkcionalnih komponenti i opcija u okviru komponente, počevši od osnovnog skupa RBAC funkcija koje moraju biti uključene u sve pakete. Druge komponente koje mogu biti odabrane u dolasku relevantnog paketa karakteristika se odnose na hijerarhije uloga, statička ograničenja (statičko razdvajanje dužnosti) i dinamička ograničenja (dinamičko razdvajanje dužnosti) [22].

RBAC model i funkcionalna specifikacija su organizovani u četiri komponente, kao što je opisano u sledećim odeljcima [22].

#### **2.4.4 Osnovni RBAC model**

Osnovni (eng. *core*) RBAC utjelovljuje bitne aspekte RBAC-a. Osnovni koncept RBAC-a je da su korisnici dodijeljeni ulogama, permisije su dodijeljene ulogama i korisnici stiču permisije tako što su članovi uloga. Core RBAC uključuje zahtjeve da dodjeljivanje korisnik-uloga i dodjeljivanje permisija-uloga mogu biti kardinaliteta više ka više. Prema tome, isti korisnik može biti dodijeljen mnogim ulogama i jedna uloga može imati više korisnika. Slično tome, može se dodijeliti jedna permisija na više uloga i jedna uloga može biti dodijeljena na više permisija.

Core RBAC obuhvata karakteristike tradicionalne kontrole pristupa, zasnovanoj na grupama i kao takva je implementirana u operativnim sistemima trenutne generacije. Kao takva, ona je široko rasprostranjena i poznata tehnologija. Karakteristike neophodne za Core RBAC su neophodne za bilo koji oblik RBAC-a. Glavno pitanje u definisanju Core RBAC-a je da se odredi koje karakteristike treba isključiti iz njega.

Uslov da korisnicima mogu biti dodijeljene i istovremeno aktivirane višestruke uloge, može se smatrati previše jakim za osnovni RBAC model, prema tvrdnjama autora u [22]. Ovaj zahtjev čini se prikladnim kada postoji veliki broj različitih uloga (stotine ili hiljade).

## 2.4.5 Hijerarhijski RBAC

Ovaj model uvodi hijerarhiju uloga (eng. *role hierarchies* - RH). Hijerarhija uloga je često uključena kao glavni aspekt RBAC modela. Hijerarhije predstavljaju prirodno sredstvo strukturiranja rola kako bi se izrazila organizaciona linija autoriteta i odgovornosti. Hijerarhija rola definiše vezu nasleđivanja između rola. Nasleđivanje je definisano na sledeći način. Kaže se da r1 “nasleđuje” rolu r2 ukoliko su sve privilegije od r2, takođe i privilegije od r1. Standard prepoznaje opšte i ograničene hijerarhije uloga.

Opšta hijerarhija rola pruža podršku za parcijalno uređen skup koji će služiti kao hijerarhija uloga, kako bi se uključio koncept višestrukog nasleđivanja permisija i korisnika među rolama.

Ograničena hijerarhija uloga nameće ograničenja koja rezultuju jednostavnijom strukturom stabla (npr. rola može imati jednog ili više neposrednih roditelja, ali je ograničena na postojanje samo jednog neposrednog potomka). Korisnička pripadnost se nasleđuje od vrha ka dnu, dok se permisije uloga nasleđuju od dna ka vrhu [24].

## 2.4.6 Ograničeni RBAC

Ograničeni RBAC unosi razdvajanje obaveza u RBAC model. Razdvajanje obaveza se koristi kako bi se spriječilo da korisnici ne prevaziđu razuman nivo autoriteta na svojim pozicijama.

Kao sigurnosni princip, SOD je dugo prisutan i široko primijenjen u poslovanju, industriji, vladi. Pojedincima, različitih vještina ili različitih interesa, su angažovani na odvojenim zadacima za izvršenje biznis funkcije. Motivacija je da se prevare i velike greške ne mogu dogoditi bez dosluha nekoliko korisnika. Ovaj RBAC standard definiše statičko i dinamičko razdvajanje obaveza.

### 2.4.6.1 Statičko razdvajanje obaveza

Sukob interesa u sistemima zasnovanim na ulogama može proizaći kao rezultat kada korisnik dobije autorizaciju za permisije povezane sa konfliktnim ulogama. Jedan vid zaštite se radi kroz statičko razdvajanje obaveza, uvodeći ograničenja za dodjelu korisnika rolama. Statička ograničenja mogu imati dosta oblika. Jedan od primjera statičkog razdvajanja može biti definisanje međusobno nepovezanih dodjela korisnicima u odnosu na skup uloga. Iako su formalni RBAC modeli i specifikacije poslovanja odavno prerasli obične relacije, danas ne postoje komercijalna rješenja koja implementiraju ova napredna statička ograničenja relacija.

Statička ograničenja definisana u ovom modelu se odnose na one relacije koje postavljaju ograničenja na skup rola, tačnije na njihove mogućnosti da kreiraju UA - *user assignment* relacije. Ovo podrazumijeva da ukoliko je korisniku dodijeljena jedna rola, onda je korisniku zabranjeno da postane član druge role. Ovaj model se definiše preko dva argumenta: skup rola koji uključuje dvije ili više rola, i kardinalitet veći od jedan ukazuje na kombinaciju rola koje mogu konstituisati kršenje SSD politike.

Kada se primjenjuju SSD relacije na hijerarhije rola, sa posebnim oprezom se mora obezbijediti da nasleđivanje korisnika ne zanemari SSD pravila [24].

### 2.4.6.2 Dinamičko razdvajanje obaveza

Statičko razdvajanje obaveza redukuje broj potencijalnih permisija koje mogu biti dostupne korisniku postavljajući ograničenja na korisnike, koji mogu biti dodijeljeni na skup rola. Relacije dinamičkog razdvajanja obaveza, kao i SSD relacije, služe da ograniče permisije dostupne korisnicima i imaju veću operativnu fleksibilnost. Razlikuju se od SSD relacija u kontekstu u kome se izlažu ova ograničenja. SSD relacije definišu i postavljaju ograničenja na cjelokupan skup permisija.

Ova komponenta modela definiše DSD osobine, koje ograničavaju dostupnost permisija kroz korisnički prostor permisija, tako što postavljaju ograničenja na role koja mogu biti aktivirana u ili tokom korisničke sesije. DSD osobine pružaju proširenu podršku za princip sa najmanjim privilegijama, po kome za svakog korisnika postoji različit nivo permisija u različitim vremenima, u zavisnosti od uloge koju izvršava. Ove osobine garantuju da permisije ne postoje izvan vremena kada su potrebne za izvršavanje obaveza. DSD dozvoljava autorizaciju korisniku za 2 ili više rola, koje ne



stvaraju sukob interesa kada se izvršavaju nezavisno, ali prouzrokuju narušavanje politike organizacije kada se aktiviraju istovremeno [24].

Odluke o kontroli pristupa često se zasnivaju na ulogama koje pojedini korisnici preuzimaju kao dio organizacija. Uloga određuje skup transakcija koje korisnik ili skup korisnika može obavljati u kontekstu organizacije. RBAC je sredstvo za imenovanje i opisivanje odnosa između pojedinaca i prava, pružajući bezbjedne metode poslovanja mnogih komercijalnih i civilnih vladinih organizacija [21].

## 2.5 Postojeće primjene RBAC modela u pametnim mrežama

RBAC je nastao kao alternativa za DAC i MAC modele kako bi se odgovorilo zahtjevima različitih organizacija u državnom i u privatnom sektoru [26]. RBAC je jedan od najzastupljenijih modela za kontrolu pristupa u modernim informacionim sistemima, s obzirom na jednostavnost upravljanja bezbjednosnim politikama, kao i smanjenja troškova i kompleksnosti administracije.

Stoga, autori rada [21] predlažu RBAC model koji se zasniva na dodjeli prava pristupa korisnicima na osnovu njihovih uloga i odgovornosti u sistemu, kao i centralizovanoj administraciji bezbjednosnih politika unutar organizacije [4].

Autori u radu [25] navode da postojeće instalacije u digitalnim mrežama često koriste koncept da obavljaju lokalni oblik RBAC-a u zavisnosti od okruženja. Komunikacija između entiteta u kontrolnom centru se, na primjer, vrši na osnovu lokalno ili centralno povezanih korisnika na grupe dozvola. Ovo osigurava da lokalno izvršavanje naredbi može biti izvršeno samo ako su odobrene odgovarajuće dozvole, ali ne mora nužno osigurati udaljenom entitetu da provjeri ko će obaviti namijenjenu operaciju.

Pristup opisan u IEC 62351-8 podržava i lokalni trag revizije kroz mogućnost povezivanja informacija o identitetu i pristupu u pristupnom tokenu (eng. *access token*). U transformatorskim stanicama, lokalni fizički pristup već može biti dovoljan za pristup entitetima koji komuniciraju. Iako pristup koji koristi tokene za pristup zasnovane na X.509 ima svoje prednosti, on nije odmah primjenljiv u svim slučajevima. Takođe, treba imati na umu da je infrastruktura elektroenergetske mreže tokom godina rasla i da je životni vijek instaliranih uređaja dugačak, 20-25 godina.

Neki od potencijalnih nedostataka mogu se primjetiti jer npr. uređaji na terenu često imaju lokalni HMI kojim upravlja servisni tehničar. Takvi uređaji na terenu obično nemaju lokalni interfejs za pametnu karticu, već samo mali ekran i bročanu tastaturu koja omogućava unos PIN-a ili lozinke. Prema tome, RBAC informacije se ne mogu dati direktno, ali mogu biti preuzete od strane terenskog uređaja [25].

Nedavno proučavani različiti sigurnosni modeli u vezi sa kontrolom pristupa koristeći svijest o kontekstu, ali različite usluge koje se nude u pametnim mrežama i kontroli pristupa u takvom okruženju i dalje imaju ozbiljne ranjivosti [25]. Kao što je navedeno u [25] veb-bazirane usluge zasnovane na XMPP [27] su specificirane za integraciju distribuiranih (decentralizovanih) energetske resursa (DER) u digitalnu energetske mrežu. Ove usluge mogu iskoristiti već postojeće tehnologije koje podržavaju RBAC, kao što je OpenID Connect ili OAuth 2.0, umjesto da grade paralelnu infrastrukturu za rukovanje RBAC baziranim na X.509.

Autori rada [28] navode da podjela odgovornosti između korisnika kojima je dodijeljena ista uloga smanjuje vjerovatnoću (konfiguracionih) grešaka u sistemu. RBAC96 je prilično generički model kontrole pristupa i ne zadovoljava u potpunosti sve sigurnosne zahtjeve kritičnih infrastrukturnih sistema, poput separacije dužnosti i odgovornosti korisnika u skladu sa regionalnim podjelama kritičnih sredstava. U tu svrhu je uveden pojam područja odgovornosti (AOR) još jedan nivo kontrole pristupa u Smart Grid okruženju. Resursi pripadaju AOR-ima kao geografskim oblastima, koji se sastoje od jednog ili više logičkih područja. Korisnicima su AOR-i dodijeljeni kao logička područja, čime se dobija određeni nivo odgovornosti za geografska područja povezana sa tim logičkim oblastima. Samim tim se dobija granularnija podjela prava pristupa za korisnike koji pripadaju istoj ulozi [28].



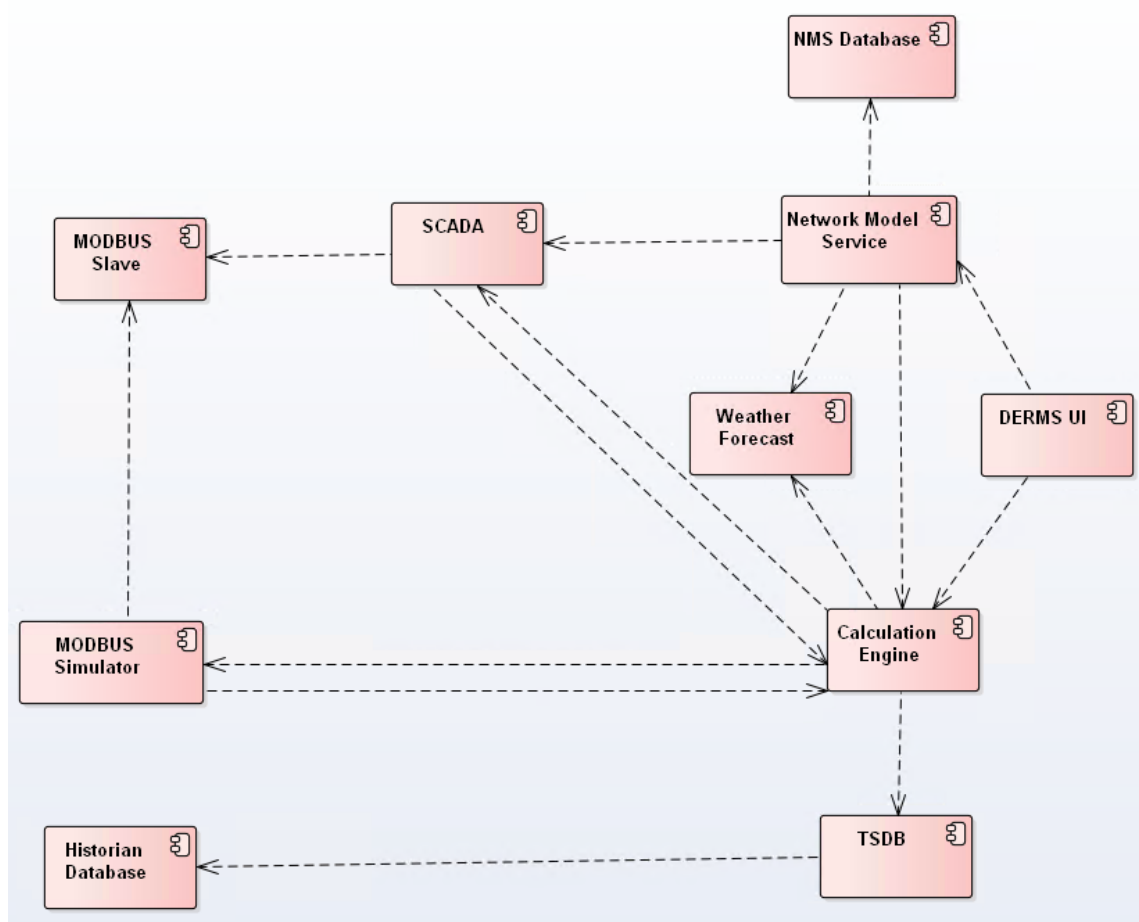
### 3. Arhitektura Smart Grid sistema

Arhitekturu *Smart Grid* sistema karakteriše kompleksnija arhitektura, za razliku od tradicionalnih elektroenergetskih sistema, koja je nastala uvođenjem distribuiranih energetske resursa kao što su razni tipovi baterija za skladištenje električne energije, distribuirani generatori. Aplikacija predstavlja softversku platformu koja služi za nadzor, upravljanje i regulaciju distribuiranih izvora energije odnosno *Distributed Energy Resource Management System*, skraćeno DERMS. Termin DERMS se najčešće odnosi na softver koji integriše potrebe dispečera sa mogućnostima energetske resursa sa fleksibilnom potražnjom na kraju mreže [10].

Aplikacija pruža mogućnost agregacije DER-ova po lokaciji ili tehnologiji (vjetrogeneratori i solarni paneli), kao i mogućnost nadgledanja i upravljanja radom svake DER grupe. Korisnik aplikacije je u mogućnosti da unese zathjevani iznos aktivne ili reaktivne snage koji želi da uzme ili da preda u mrežu. Komandovanje tj. postavljanje *setpointa* se oslanja na podatke iz dobavljene vremenske prognoze. Zahtijevana vrijednost, odnosno *setpoint*, se raspoređuje na odgovarajuće grupe DER uređaja na optimalan način, i to pomoću 2 algoritma:

- prema nominalnoj snazi DER-ova,
- prema raspoloživoj rezervi.

Arhitektura sistema je prikazana na slici 5.



Slika 5 Arhitektura sistema

Sistem prikazan u ovom poglavlju je proširen u poglavlju 4, sa implementiranom kontrolom pristupa. U nastavku će ukratko biti opisani postojeći servisi i njihova namjena.

### 3.1 Network Model Service - NMS

Predstavlja bitnu komponentu koja drugim servisima pruža statičke podatke o mreži. Statički podaci se unose preko CIM/XML fajla, preko DERMS korisničkog interfejsa i čuvaju se, nakon konverzije, u lokalnoj SQL bazi podataka. Podaci se čuvaju u formi Resource Description-a. Kada se vrši dobavljanje podataka sa ovog servisa, pristupa mu se preko adaptera koji pravi GDA upite i konvertuje podatke u objektni model i prosleđuje ih komponenti koja ih je zahtijevala. Podržane su operacije dodavanja novih delta objekata, za razliku od operacija ažuriranja i brisanja čija podrška nije implementirana.

Pored navedenog, NMS ima ulogu koordinatora distribuirane transakcije, kojom se osigurava konzistentnost podataka o mrežnom modelu, na nivou čitave aplikacije. Odnosno, dovoljno je da se samo na jednoj komponenti ne ažurira model kako bi došlo do odbacivanja cjelokupne transakcije.

### 3.2 Supervisory Control And Data Acquisition - SCADA

Predstavlja sistem za nadzor i upravljanje fizičkim procesima u elektroenergetskim sistemima. Za prikupljanje analognih i digitalnih podataka sa uređaja u polju se koriste RTU (eng. *Remote Terminal Unit*), kao i za komandovanje nad tim uređajima. Rad RTU kontrolera je simuliran pomoću Modbus Simulatora.

Statuse tačaka u polju prosleđuje ka Calculation Engine servisu i omogućava izdavanje komandi za izlazne tačke, simulirajući uspješno izvršavanje komandi (kao što je automatska promjena vrijednosti odgovarajućih ulaza).

### 3.3 Calculation Engine - CE

Centralna uloga mu je da obrađuje zahtjeve za komandovanjem, tj. zahtjeve za povećanje ili smanjenje proizvodnje aktivne i/ili reaktivne snage distribuiranih izvora električne energije. Nakon prikupljanja trenutnih vrijednosti u realnom vremenu, vrši se optimalna raspodjela po traženom *setpoint*-u. CE zatim odradi predviđanje proizvodnje za traženi vremenski period, za koji se planira komandovanje. Svakog sata se vrši ponovno preračunavanje *setpoint*-a. Ukoliko su ispunjeni uslovi da ne postoji već zadata komanda za određeni DER ili DER grupu, omogućava se komandovanje i tražena vrijednost *setpoint*-a se optimalno raspodjeljuje, pomoću dva ranije pomenuta algoritma. Komande su skladištene u memoriji.

### 3.4 Weather Forecast Service

Ova komponenta daje uvid u vremensku prognozu Calculation Engine-u, gdje je maksimalni period za koji se analiziraju podaci do 7 dana unaprijed, na nivou jednog časa. Weather Forecast se oslanja na NMS-ove statičke podatke kako bi na osnovu geografske širine i dužine transformatorske stanice (eng. *substation*) na koju su povezani DER-ovi, preko API-ja dobio potrebne podatke. Krična uloga komponente je dobavljanje podataka o trenutnim kao i o budućim vremenskim uslovima, čime se ostvaruje predikcija moguće proizvodnje solarnih i vjetro generatora. Podaci o vremenskoj prognozi se skladište lokalno, kako bi se drugim servisima omogućio brz pristup na osnovu geografske širine i dužine ili globalnog identifikatora.

### 3.5 Remote Telemetry Unit – RTU

Koriste se za prikupljanje izmjerenih analognih i digitalnih ulaza, kao i komandno komunikacioni kontroler za uređaje u polju. Omogućavaju (barem) Modbus komunikaciju.

### 3.6 Modbus Slave

Modbus protokol je telemetrijski protokol na aplikativnom nivou koji omogućava klijent-server komunikaciju između uređaja povezanih na različite vrste magistrala. Komunikacija koja se odvija

između povezanih uređaja uključuje slanje zahtjeva jednog uređaja (eng. *master*) drugom uređaju (eng. *slave*), obradu primljenog zahtjeva od strane drugog uređaja i slanje odgovora u zavisnosti od uspješnosti obrade.

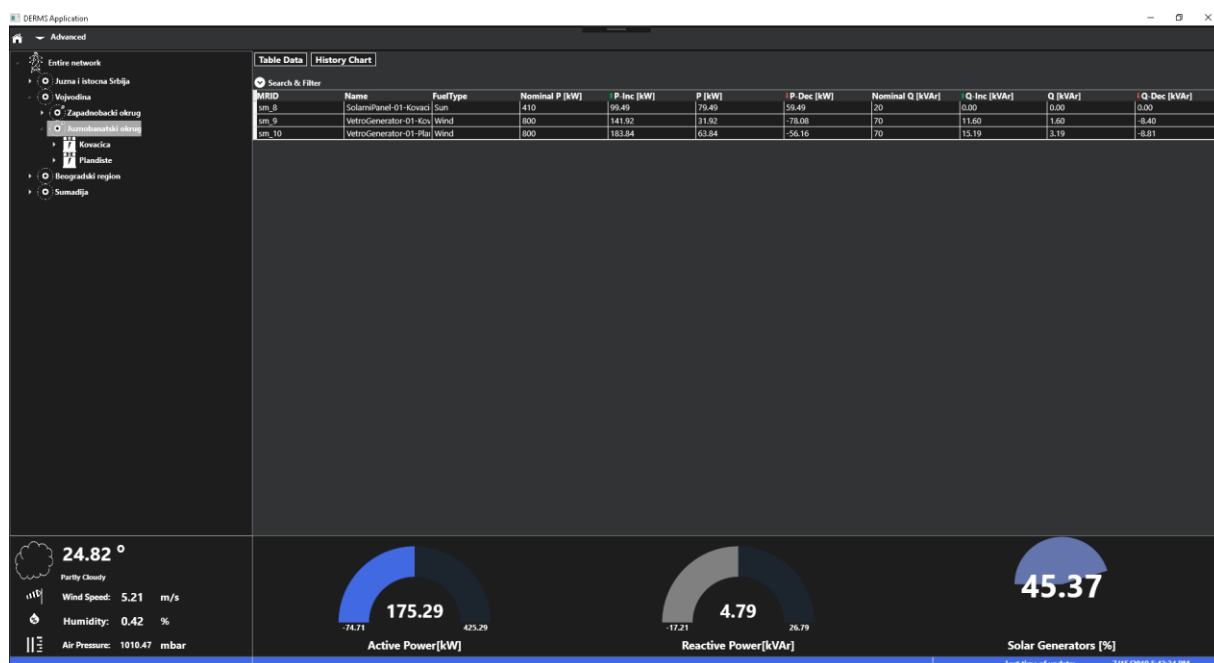
Modbus simulator koristi Modbus protokol da bi izvršavao simulaciju distribuiranih generatora u polju. Master uređaj je SCADA komponenta dok slave uređaje predstavlja upravo ovaj simulator.

### 3.7 Modbus Simulator

Iz praktičnih razloga i pogodnijeg načina testiranja radi se simuliranje realnih podataka, na osnovu vremenske prognoze. Simulira se proizvodnja solarnih i vjetro generatora. Zatim se radi upis tih podataka na Modbus Slave komponentu, odakle će dalje biti obrađivani od strane SCADA komponente.

### 3.8 DERMS korisnički interfejs

DERMS korisnički interfejs pruža uvid u cjelokupno stanje sistema. Glavni prozor aplikacije je ilustrovan na slici 6. Sa lijeve strane prozora je prikazana hijerarhijska struktura za grupisanje DER-ova, odnosno *treeview* u čijem se vrhu nalazi čitava mreža tj. *Entire Network* Ekspanzijom *Entire Network*-a otvara se prikaz *Region*, odnosno regiona (Južna i Istočna Srbija, Vojvodina...). Sledeći nivo hijerarhije jeste podregion (eng. *subregion*), koji u sebi sadrži transformatorske stanice (eng. *substation*). DER-ovi se vezuju na transformatorske stanice i predstavljaju dno pomenute hijerarhije. Po izboru elementa iz hijerarhije, u centralnom dijelu aplikacije se prikazuju svi DER-ovi koji se nalaze u tom sloju, sa informacijama o nazivu, nominalnoj i trenutnoj aktivnoj i reaktivnoj snazi.



Slika 6 Početni prozor aplikacije

Uvid u trenutno stanje vremenskih uslova se može dobiti klikom na odgovarajući element iz hijerarhije, a ažurirani prikaz je lociran na dnu prozora aplikacije, sa lijeve strane. Na većem dijelu dna prozora aplikacije je prikazana trenutna i maksimalna proizvodnja aktivne i reaktivne snage, za selektovani nivo hijerarhije (eng. *Active/Reactive Power*). Na tom dijelu se takođe daje uvid u procentualni udio solarnih panela u mreži, u odnosu na vjetro generatore.

Pored navedenog, postoji opcija za prikaz istorijata perzistiranih mjerenja aktivne i reaktivne snage, koje je SCADA sistem prikupio i obradio. Korisnik može izabrati datum i odgovarajući DER (ili grupu DER-ova), kao i rezoluciju sa kojom želi napraviti grafički prikaz proizvedene aktivne i reaktivne snage. Postoji opcija za prikaz istorije mjerenja na nivou sata, dana ili mjeseca.

Ukoliko korisnik želi da izda komandu, odabirom željenog elementa iz hijerarhije stabla može se izabrati između komandovanja aktivnom ili reaktivnom snagom tog distribuiranog izvora električne energije. Prikaz prozora koji se pojavljuje kada se izabere opcija komandovanja prikazuje slika 7. Pored zelene i crvene strelice se nalaze podaci o mogućem smanjenju/povećanju proizvodnje električne energije.

Nakon popunjavanja „Delta“ polja (zahtijevana snaga - *setpoint*) korisnik bira na koliko sati se odnosi komanda, kao i algoritam kojim će se vršiti raspodjela zahtijevane snage na pripadajuće DER-ove. Najduži rok na koji se vrši komandovanje je do kraja tekućeg dana. Na grafiku se vizuelno prikazuje moguće povećanje i smanjenje proizvodnje, zelenom i crvenom bojom, respektivno.

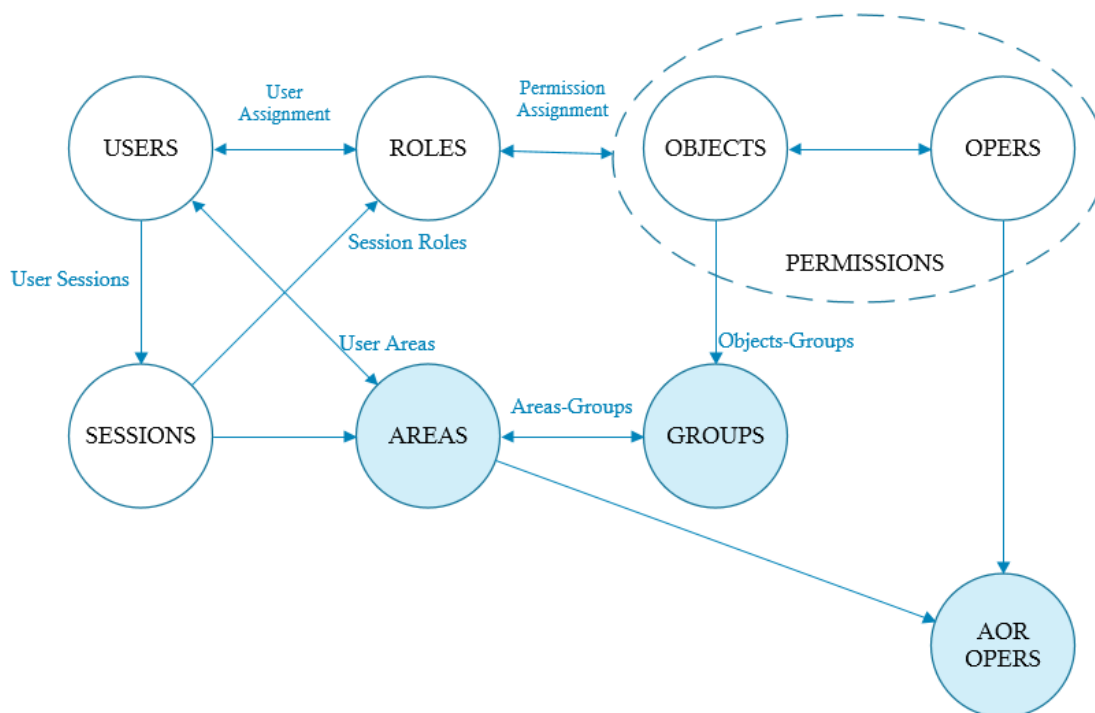


Slika 7 Uspješno izdavanje komande (povećanje snage)

#### 4. Implementacija napredne kontrole pristupa

Bezbednosni mehanizam pristupa prema oblasti kontrole (eng. *Area Of Responsibility*, skr. AOR) predstavlja koncept podjele odgovornosti prema oblastima, najčešće geografskim, u elektroprenosnoj mreži. Pored AOR-a implementiran je i prototip sistema za obradu alarma i događaja.

Za modelovanje elemenata elektroenergetskog sistema (geografski region, podregion i transformatorska stanica, respektivno) su iskorištene sledeće CIM klase, iz paketa *Core* : *GeographicalRegion*, *SubGeographicalRegion*, *Substation*. Distribuirani (decentralizovani) energetske resurs - DER modelovan je klasom *SynchronousMachine*, iz paketa *Wires*.



Slika 8 Model proširenog RBAC-a

Model kontrole pristupa demonstriran u ovom radu definiše proširenje RBAC modela, koje predstavlja segmente označene plavom bojom na slici 8. Model karakterišu tri tipična tipa aktivnosti u Smart Gridu (AOR OPERS na slici 8):

- Nadgledanje, koje podrazumijeva akcije praćenja stanja elektroenergetske mreže, statusa analognih ulaza, informacija o alarmima, čijim praćenjem se mogu preduprediti nepoželjne posljedice.
- Kontrola, koja obuhvata korektivne akcije manipulisanjem rada pojedinačnih distribuiranih energetske resursa (aktivna/reaktivna snaga), upravljanje alarmnim događajima.
- Ažuriranje, pod kojim se podrazumijeva unos novih ili modifikacija postojećih statičkih podataka o elementima mreže.

Korisniku (eng. *user*) je moguće pridružiti različite uloge (eng. *role*), od kojih svaka uloga posjeduje određene permisije (eng. *permission*). AOR oblast (eng. *area*) je sačinjena od više AOR grupa (eng. *group*) i poput korisnika posjeduje određene permisije. Operacije koje su sadržane u pripadajućem skupu AOR OPERS se mogu dozvoliti ili ne, u zavisnosti od permisija određene AOR oblasti, koje se porede sa permisijama koje posjeduje ulogovani korisnik aplikacije. Pripadnost objekta (jednog DER-a) određenoj AOR grupi se opisuje atributom objekta, odnosno relacijom „Objects-Groups“. Podaci o mapiranju AOR grupa na distribuirane energetske resurse su sadržani u Network Model servisu.

## 4.1 AOR Cache

Cache predstavlja SQL bazu trajno perzistiranih podataka, koja je locirana unutar AOR servisa. Cache sadrži podatke o AOR grupama, oblastima, permisijama, ulogama, korisnicima i DER generatorima. Redefinisanjem (eng. *Override*) metode *OnModelCreating*, klase *DbContext*, modelovani su odnosi između prethodno navedenih entiteta uslijed velikog broja veza „više ka više“. Objektno-relaciono mapiranje je realizovano u .NET okruženju preko *Entity Framework*-a. Osjetljivi korisnički podaci, poput lozinke, su sačuvani jednosmjernom funkcijom kao heš (eng. *hash*) vrijednost, pomoću funkcionalnosti .NET klase *RNGCryptoServiceProvider*. Uslijed determinističnosti i nepostojanja inverzne funkcije heš algoritam obezbjeđuje bezbjedan način za čuvanje osjetljivih podataka.

Tipovi entiteta koji su modelovani u AOR Cache-u su:

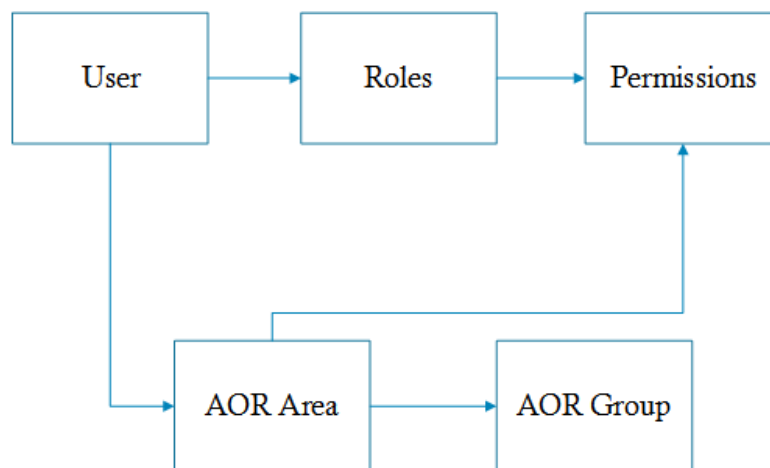
- Korisnik (eng. *user*)
- Uloga (eng. *role*)
- Permisija (eng. *permission*)
- AOR oblast (eng. *area*)
- AOR grupa (eng. *group*)

Grupa predstavlja logički skup resursa koji su blisko povezani. Skup grupa se organizuje u AOR oblasti. Jedna grupa može biti dio više oblasti i svaka oblast može biti član više grupa. Kako se navodi u [2], grupisanje (koje se ponekad naziva klasterisanje) je funkcija upravljanja DER-ovima koja se sastoji u definisanju i korištenju listi DER sistema prema posebnim karakteristikama (npr. jačini snage, lokaciji u topologiji mreže, vrsti priključenih DER jedinica). Grupe kreiraju svaki organi upravljanja DER-om sa posebnom svrhom.

Svakoj oblasti se dodjeljuje skup permisija, koje definišu prava pristupa korisnika. Jednom korisniku može biti povjereno više AOR oblasti, dok svaka AOR oblast može biti dodijeljena na više korisnika. Jednoj AOR oblasti može biti dodijeljen i proizvoljan skup drugih AOR oblasti pa na taj način nastaje hijerarhija AOR oblasti.

Uloga služi da grupiše određeni broj permisija i dodjeljuje se korisnicima. Veza je takođe više ka više.

Logičke veze unutar AOR Cache-a su prikazane na slici 9.



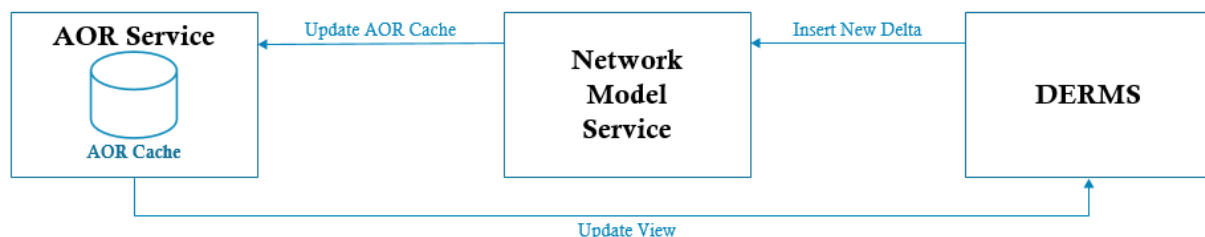
Slika 9 Logičke veze u AOR Cache-u

Network model servis (skr. NMS), kao što je ranije pomenuto, sadrži statičke podatke o mreži. Od interesa za AOR servis su podaci o AOR grupama. Svaka AOR grupa može biti povezana sa više solarnih ili vjetro generatora, a generatori mogu biti u više AOR grupa.

Po inicijalizaciji AOR servis uspostavlja komunikaciju sa NMS komponentom kako bi dobio podatke o grupama. Takođe se pretplaćuje na promjene o svim AOR grupama koje se dogode na

Network model servisu. Nakon toga AOR servis je spreman da opslužuje zahtjeve koji dolaze sa DERMS korisničke aplikacije.

U slučaju da korisnik želi da ažurira model statičkih podataka, npr. da promijeni povezanost nekog DER-a sa AOR grupom, napraviće novi CIM/XML fajl i odradiće učitavanje nove delte preko DERMS aplikacije. Tok aktivnosti je prikazan na slici 10. Operacija izmjene (promocije) modela će biti omogućena samo ukoliko korisnik posjeduje odgovarajuću permisiju, odnosno, ukoliko korisnik ima dodijeljenu ulogu koja posjeduje adekvatnu permisiju. Nakon uspješno obavljene model promocije šalje se obavještenje svim zainteresovanim servisima, između ostalih i AOR servisu. To dalje inicira povratnu reakciju od strane AOR servisa, koji propagira promjene na DERMS aplikaciju, kako bi se ažurirao aktuelni prikaz mreže.



Slika 10 Model promocija

Ulazna tačka svakog sistema za kontrolu pristupa jeste podsistem za autentifikaciju [4]. Prilikom logovanja korisnika na DERMS aplikaciju, obavlja se komunikacija sa AOR servisom kome se šalju korisničko ime i lozinka. Ukoliko je korisnik uspješno autentifikovan AOR servis vraća kao povratnu informaciju spisak naziva AOR oblasti koje su dodijeljene ulogovanom korisniku. Potom se korisnik preko *publish-subscribe* mehanizma pretplaćuje na spisak AOR oblasti koje su mu dodijeljene. Pretplaćivanje se vrši kako bi korisnik dobijao obavještenja kada se dese neke stvari od značaja i to u nekoj od oblasti koje su njemu dodijeljene. Stvari od značaja jesu događaji i alarmi, koje obrađuje sistem za obradu događaja i alarma (Event i Alarm System).

## 4.2 AOR Servis

AOR servis je zadužen je za autentifikaciju korisnika sistema. Služi i kao posrednik drugim servisima da dobave podatke iz AOR Cache-a. Podaci se pribavljaju uz pomoć LINQ upita. Na servisnoj strani je implementiran interfejs (eng. *interface*) *IAuthorizationPolicy*, sa značajnom metodom *Evaluate* koja preuzima identitet korisnika preko *IIdentity*, da bi se potom na osnovu korisničkog imena dobavile dodijeljene AOR oblasti, iz AOR Cache-a. Iz AOR Cache-a se takođe dobavljaju uloge sa kojima je ulogovani korisnik povezan. Preko korisniku dodijeljenih uloga se dobavljaju permisije korisnika. Na ovaj način su ispoštovane glavne karakteristike osnovnog (eng. *core*) RBAC model-a.

Nakon toga se kreira *custom* principal tj. *DERMSPrincipal* sa identitetom korisnika, dodijeljenim oblastima, skupom permisija i stavlja se u svojstva konteksta. Principal je entitet koji enkapsulira informacije o ovlašćenjima autentifikovanog korisnika u korisničkoj sesiji [4]. Za sve naredne pozive AOR servisa metoda *Evaluate* će dobiti oblasti za aktivnog korisnika, tako da će stanje biti ažurno.

### 4.2.1 Manipulacija dodijeljenim AOR-ima – AOR Board

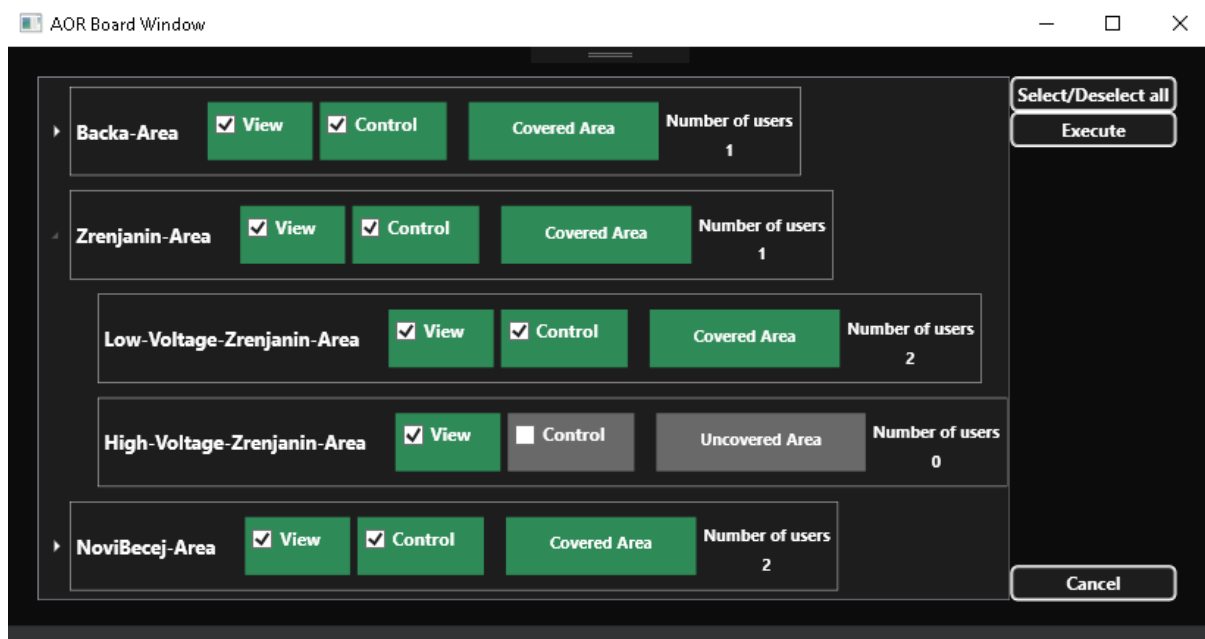
Prilikom uspostavljanja sesije korisnik nije u obavezi da aktivira sve AOR-e koji su mu dodijeljeni. Korisniku je ostavljena mogućnost da po želji aktivira i deaktivira dodijeljene AOR-e.

AOR Board prozor po otvaranju šalje upit na AOR cache kako bi dobio sve oblasti koje su dodijeljene korisniku na upravljanje. Od dodijeljenih oblasti korisnik može da izabere koje želi da nadgleda (eng. *view*) i/ili kontroliše (eng. *control*). Nadgledanje podrazumijeva mogućnost nadgledanja određenog dijela mreže, ali bez mogućnosti izdavanja nikakvih korektivnih akcija tj.



komandovanje nije omogućeno datom korisniku. Trenutno izabrane oblasti za nadgledanje i kontrolu, iz skupa dodijeljenih, su čekirane i uokvirene zelenom bojom kao što se vidi na slici 10. Oblasti koje trenutno nisu dodijeljene su uokvirene svijetlo sivom bojom i nisu čekirane. Takođe, postoji indikacija u analognim bojama o tome da li iko pokriva, tj. kontroliše određenu oblast („Covered Area“ ili „Uncovered Area“) i ukupan broj korisnika koji kontroliše svaku oblast.

Po selekciji i/ili deselekciji AOR oblasti potrebno je potvrditi akcije klikom na dugme *Execute*. Na AOR servisnu stranu pristignu nazivi oblasti, sa odgovarajućim stanjima AOR oblasti koje je potrebno ažurirati u zavisnosti od selekcija koje je korisnik napravio, odnosno da li korisnik želi da nagleda ili i kontroliše željenu AOR oblast. Njihovim ažuriranjem se ažurira i prikaz stanja mreže korisniku, kao i prikaz alarma i događaja. Biće prikazani samo alarmi i događaji koji se tiču dodijeljenih AOR oblasti (selektovanih za nadgledanje ili upravljanje), dok će ostale AOR oblasti biti zanemarene. Konkretno na slici 11 uvođenje hijerarhije AOR-a kao glavnu prednost omogućuje to što je svim korisnicima kojima je dodijeljena oblast „Zrenjanin-Area“, dodijeljena i „Low-Voltage-Zrenjanin-Area“ i „High-Voltage-Zrenjanin-Area“.



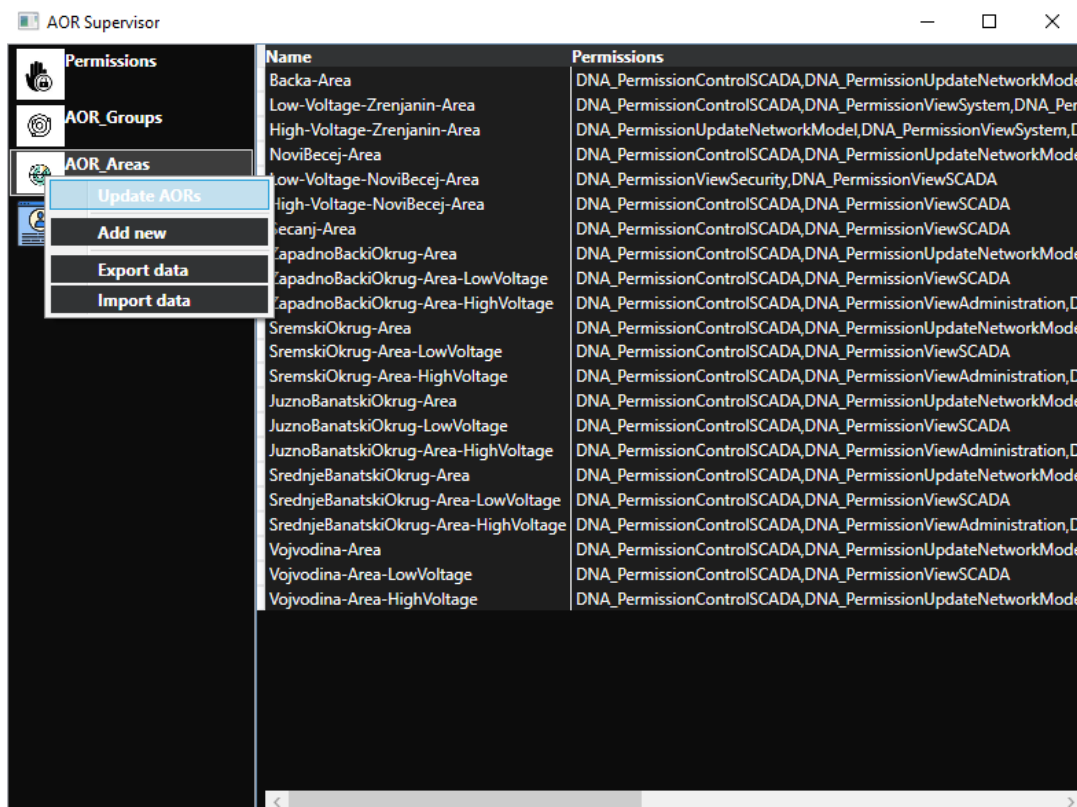
Slika 11 Hijerarhijski prikaz AOR oblasti

#### 4.2.2 Sinhronizacija AOR entiteta preko AOR Supervisor aplikacije

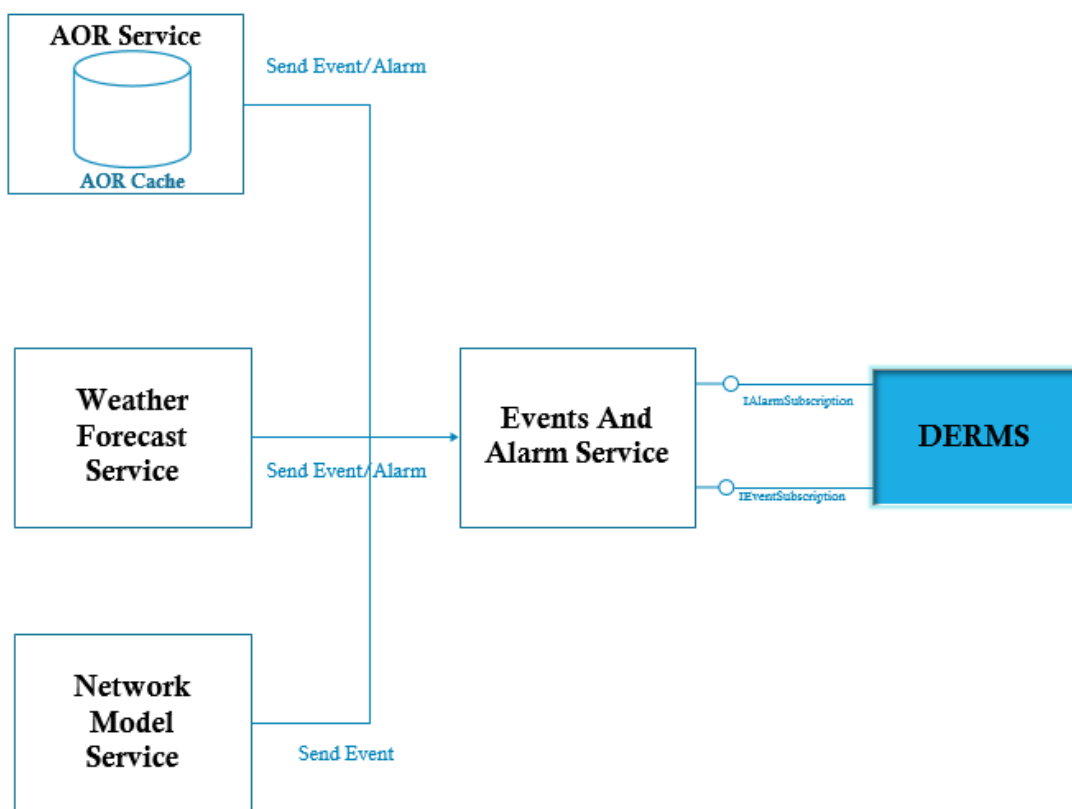
Izmjene postojećih ili dodavanje novih AOR oblasti i grupa se vrši preko AOR Supervisor aplikacije. AOR Supervisor predstavlja WPF aplikaciju. Preko nje je omogućena izmjena postojećih i dodjela novih permisija, uloga i korisnika. Nakon takvih akcija korisnik mora da ručno sinhronizuje (opcija „Update AORs“ na kontekstnom meniju na slici 12) izmjene koje se prosleđuju na AOR servis, a AOR servis potom ažurira stanje podataka u AOR Cache-u. Moguće je eksportovati i importovati podatke o AOR grupama i oblastima, u xml formatu.

Izgled prozora aplikacije je ilustrovan na slici 12. U lijevom dijelu prozora su sadržane permisije, AOR grupe, AOR oblasti i uloge. Izborom nekog od ova 4 tipa, u desnom dijelu aplikacije se vrši popunjavanje liste entiteta, sa detaljima.





Slika 12 Prozor AOR Supervisor aplikacije



Slika 13 Arhitektura sistema sa dodatim alarmima i događajima

### 4.3 Servis za obradu događaja i alarma

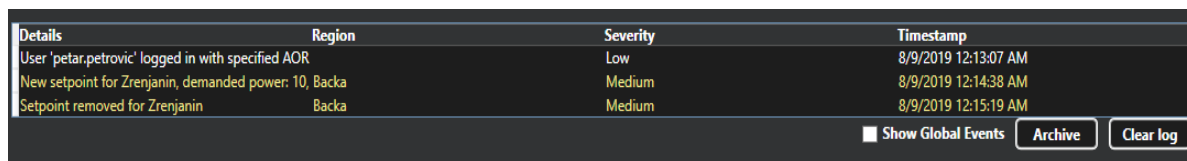
Predstavlja centralizovanu komponentu koja u sistemu agregira događaje od značaja. Servis za obradu događaja i alarma izlaže po dvije pristupne tačke (eng. *endpoint*) za događaje (eng. *event*) i alarme. U ovu namjenu izložena su dva para interfejsa, *IEventSubscription*, *IEventCollector*, i *IAlarmSubscription*, *IAlarmCollector*. Servis se zasniva na mehanizmu pretplate i objave (eng. *publisher-subscriber*). Arhitektura sistema sa dodatim alarmima i događajima je prikazana na slici 13.

Jedna pristupna tačka služi korisnicima kako bi se pretplatili na servis, recimo preko *IEventSubscription* interfejsa. Pretplata se vrši nakon uspješno završenog procesa autentifikacije, koji se obavlja preko DERMS aplikacije. Proces autentifikacije po uspješnom logovanju korisnika vraća listu njemu dodijeljenih oblasti odgovornosti. Na osnovu povratne informacije logovanja tj. dobijenih AOR oblasti, na servis za obradu događaja i alarma se šalju nazivi AOR oblasti i na njih se korisnik pretplaćuje. Nazivi AOR oblasti su jedinstveni u sistemu. Nakon što se korisnik pretplati na njemu dodijeljene AOR oblasti, servis čuva njegov kanal za kasnija obavještenja. Druga pristupna tačka se koristi kako bi ostali servisi mogli poslati povratnu informaciju kada se desi događaj od značaja, koji će dalje biti propagiran zainteresovanim stranama preko prethodno sačuvanog kanala pretplatnika i biće prikazan korisniku DERMS aplikacije.

#### 4.3.1 Obrada događaja - Event-a

Kako bi sistem kontrole pristupa posjedovao kompletan bezbjednosni mehanizam, potrebno ga je uvezati sa *auditing*-om. Auditing koji pomaže u smislu da loguje aktivnosti i zahtjeve korisnika za kasniju analizu, kao i davanje uvida u trenutno stanje u mreži. Notifikacije mogu biti različitog tipa, od obavještenja kada se uloguje novi korisnik koji ima istu dodijeljenu oblast odgovornosti, do izdavanja komande za manipulaciju povećanjem ili smanjenjem proizvodnje aktivne ili reaktivne snage određenog regiona, podregiona, transformatorske stanice ili pojedinačnog DER uređaja, iz neke od AOR oblasti koje su dodijeljene datom korisniku. Korisnik se takođe obavještava ukoliko dođe do model promocije (npr. ukoliko se primjeni novi CIM/XML fajl sa statičkim podacima mreže). Svaka promjena iz AOR Board prozora, o selekciji i deselekciji dodijeljenih oblasti odgovornosti se takođe upisuje u listu događaja.

Prikaz događaja u sistemu je ilustrovan na slici 14. Implementirana je klasifikacija prikaza različitim bojama, u zavisnosti od kritičnosti događaja koji se želi prikazati korisniku. Listu događaja je moguće arhivirati i obrisati. Omogućeno je filtriranje, kako bi bile prikazane samo akcije koje je prouzrokovao ulogovani korisnik, a ne i ostali korisnici koji istovremeno nadgledaju iste AOR oblasti.



Details	Region	Severity	Timestamp
User 'petar.petrovic' logged in with specified AOR		Low	8/9/2019 12:13:07 AM
New setpoint for Zrenjanin, demanded power: 10, Backa	Backa	Medium	8/9/2019 12:14:38 AM
Setpoint removed for Zrenjanin	Backa	Medium	8/9/2019 12:15:19 AM

Slika 14 Prozor sa evidentiranim događajima

#### 4.3.2 Obrada alarmanjih događaja - Alarma

Analogno događajima i u ovom slučaju će korisnik biti obaviješten ukoliko dođe do nekih bitnih promjena, u okviru skupa oblasti odgovornosti koje su mu dodijeljene. Alarmanjna notifikacija će biti poslata korisniku ukoliko nijedan korisnik (operater) u tom trenutku ne kontroliše navedenu oblast, a trenutno mu je dodijeljena. Osim toga svim korisnicima od interesa biće poslata poruka ukoliko dođe do problema pri dobavljanju vremenske prognoze, jer je to primarni alat na osnovu koga se vrše predikcije i zadavanje komandi za manipulacijama aktivnom i reaktivnom snagom distribuiranih energetske resursa. Za komunikaciju sa DERMS aplikacijom izlaže interfejs *IAORManagement* preko koga se korisnik loguje na sistem, sinhronizuje dodijeljene AOR-e.

Izgled prozora u koji korisnik ima uvid je prikazan na slici 15. Alarmi u tabeli su klasifikovani različitim bojama, u zavisnosti od kritičnosti.

Details	Region	Severity	Timestamp
Area 'Low-Voltage-Zrenjanin-Area' has become uncovered.	Backa	High	8/9/2019 12:06:58 AM
Weather Forecast is not available.	Backa	Medium	8/9/2019 12:13:03 AM

☐ Show Global Alarms

Slika 15 Prozor sa evidentiranim alarmima

Po pristizanju novog obavještenja o alarmu na statusnoj liniji glavnog prozora aplikacije simbol alarma će treperiti sve dok se alarm ne potvrdi ili dok se ne riješi stanje koja je i dovelo do alarmantnog obavještenja. Uz simbol alarma, na statusnoj liniji, stoji broj nepotvrđenih alarma, kao što je prikazano na slici 16.

2	Last update: 8/13/2019 1:09:22 PM
---	-----------------------------------

Slika 16 Notifikacija o novim alarmima, na statusnoj liniji

U slučaju alarma da je jedna od oblasti ostala nepokrivena, odnosno bez nadzora, korisnik sa posebnim permisijama (uloga „administrator“) može ručno izabrati iz liste aktivnih operatera jednog od njih i dodijeliti mu nepokrivenu oblast. Izgled prozora kojim se vrše manipulacije privremenog delegiranja AOR oblasti na druge korisnike, kojima nepokrivena oblast inače ne pripada, se nalazi na slici 17. Delegiranje se vrši biranjem komande „Assign user“, iz kontekstnog menija. Nakon što se razriješe alarmantne situacije, ostali korisnici (operateri) iz te oblasti će dobiti obavještenje npr. da je nepokrivena AOR oblast pokrivena, odnosno, da postoji dispečer koji je kontroliše. Događaji iz alarm servisa će takođe biti upisani i u tabelu koja prikazuje događaje.

Name	Number of users covering	Timestamp
Backa-Area	0	8/16/2019 4:03:26 PM

Assign user

Slika 17 Delegiranje nepokrivenih AOR-a

## 5. Testiranje napredne kontrole pristupa u okviru Smart Grid aplikacije

Model prezentovan u ovom radu je verifikovan simuliranjem na testnom sistemu, tj. simulirano je uprošćeno Smart Grid okruženje koje sadrži obnovljive izvore električne energije. Zbog praktičnih razloga, functionisanje dinamičnog i kompleksnog kritičnog infrastrukturnog sistema, kao što Smart Grid svakako jeste, korišćena je simulacija segmenta njegovog rada. U svrhu istraživanja u ovom radu iskorišćen je Modbus simulator, kako bi se vršilo simuliranje rada distribuiranih generatora u polju. Modbus simulator je baziran na Modbus protokolu, a obavlja operacije čitanja i pisanja analognih signala. Modbus simulator na osnovu realnih podataka, dobijenih vremenskom prognozom, omogućuje simulaciju proizvodnje solarnih i vjetro generatora i njihov rad u realnom vremenu. Te podatke simulator upisuje na Modbus *slave*, odakle ih dalje procesira SCADA sistem. Podaci se preračunavaju i upisuju u Modbus slave svakih pet sekundi, dok se vremenska prognoza dobavlja na svakih sat vremena. SCADA sistem koristi analogne ulazne i izlazne tačke i kako bi se dobavile informacije o trenutnom stanju tačaka (aktivna-reaktivna snaga distribuiranih generatora) odnosno sistema u cjelini.

Korisnik, u zavisnosti od privilegija koje posjeduje, može komandovati povećanjem ili smanjenjem aktivne ili reaktivne snage određenog segmenta mreže. U simuliranom okruženju je integrisan servis koji vrši kontrolu pristupa, koja se bazira na predstavljenom modelu.

Na osnovu dostupne stručne literature moglo bi se zaključiti da postojeći modeli ne mogu na adekvatan način odgovoriti na aktuelne zahtjeve koji se postavljaju u elektroenergetskoj industriji. Prilikom donošenja odluke o pristupu nekim resursima ABAC model daje mogućnost uvažavanja velikog broja atributa koje treba uzeti u razmatranje. Ipak, ABAC model nije prihvatljiv uslijed definisanja velikog broj autorizacionih pravila, jer Smart Grid obuhvata na hiljade korisnika i opreme. Osim toga, u toku izvršavanja, kada se vrši izračunavanje vrijednosti autorizacionih pravila može doći do ozbiljne degradacije performansi sistema. Takva degradacija performansi u kritičnom sistemu Smart Grid-a nije prihvatljiva.

Sve komponente prototipa sistema za naprednu kontrolu pristupa implementirane su korišćenjem programskog jezika C#, u Microsoft Visual Studio 2017 razvojnom okruženju.

## 5.1 Skup permisija u sistemu

Skup permisija tj. aktivnosti koje su dozvoljene nad objektima je prikazan u tabeli 1. Svaku aktivnost karakteriše njen tip, koji može biti: kontrola, nadgledanje ili ažuriranje.

**Tabela 1 Spisak permisija**

Permisija		Aktivnost	Tip aktivnosti
Skr.	Naziv		
P1	Komandovanje	Izdavanje komandi o povećanju ili smanjenju aktivne ili reaktivne snage DER-ova	Kontrola
P2	Nadgledanje stanja mreže	Uvid u generisane događaje i alarme u elektroenergetskoj mreži	Nadgledanje
P3	Uvid u mjerenja sistema	Čitanje izmjerenih vrijednosti snage grupe ili pojedinačnih DER-ova	Nadgledanje
P4	Ažuriranje modela mreže	Ažuriranje statičkih podataka o mreži	Ažuriranje
P5	Upravljanje alarmima	Manipulacija alarmima i njihovo rješavanje	Kontrola
P6	Delegiranje AOR-a	Privremeno delegiranje AOR-a drugim operaterima	Kontrola

## 5.2 Skup uloga u sistemu

Tabela 2 prikazuje koje su sve uloge dostupne u sistemu, sa pripadajućim permisijama i dozvoljenim tipom aktivnosti.

**Tabela 2 Spisak dostupnih uloga**

Uloga		Permisija						Tip aktivnosti		
Skr.	Naziv	P1	P2	P3	P4	P5	P5	Nadgledanje	Kontrola	Ažuriranje
U1	Operater	✓	✓	✓				✓	✓	
U2	Model operater			✓	✓			✓		✓
U3	Administrator			✓		✓	✓	✓	✓	

Za potrebe izvršavanja grupe eksperimenata kreirano je ukupno četiri korisnika:

- dva korisnika koji su članovi korisničke uloge operatera, pri čemu je osnovna razlika među njima u pogledu omogućenih AOR-a,
- jedan korisnik koji je član korisničke uloge model operatera,
- jedan korisnik, član uloge administratora.

**Tabela 3 Skup korisnika sa ulogama i dodijeljenim AOR-ima (O-oblast)**

Korisnik	Sesija	Korisnička uloga	O1- Nadgledanje	O1- Kontrola	O1- Ažuriranje
Operater1	S1	Operater	✓	✓	x
Operater2	S2	Operater	✓	x	x
ModelOperater1	S3	Model operater	✓	x	✓
Administrator1	S4	Administrator	✓	✓	x

Tabela 3 prikazuje skup korisnika sistema sa pripadajućim ulogama i AOR-ima. U nastavku će biti prikazani neki od eksperimenata koji naglašavaju prednosti proširenog modela, u odnosu na RBAC model. Model demonstriran u ovom radu će biti označen kao RBAC-U.

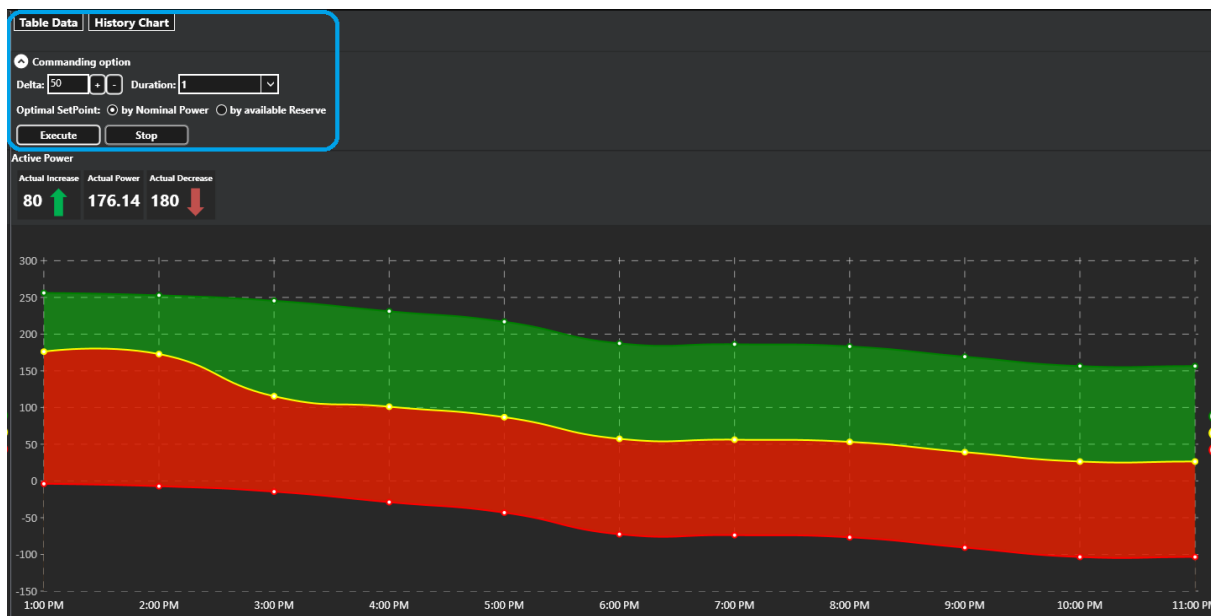
U prvom slučaju, kada se uspostavlja korisnička sesija svi korisnici sistema aktiviraju dodijeljene AOR-e. Stanja sesija za dva operatera, model operatera i administratora su demonstrirana tabelom 4. U tabeli 4 su prikazani rezultati koji uporedno prikazuju RBAC model, kao i model RBAC-U. Interpretacijom rezultata zaključuje se da nepostojanje permisije uzrokuje i nemogućnost izvršenja akcije. Kada se analiziraju korisnici koji imaju dodijeljen isti tip uloge, može se primjetiti da klasični RBAC ne podržava mogućnost podjele odgovornosti.

**Tabela 4 Uporedne karakteristike modela kontrole pristupa**

Korisnik	Sesija	Model kontrole pristupa	Nadgledanje	Kontrolisanje	Ažuriranje
Operater1	S1	RBAC	✓	✓	x
		RBAC-U	✓	✓	x
Operater2	S2	RBAC	✓	✓	x
		RBAC-U	✓	x	x
ModelOperater1	S3	RBAC	✓	x	✓
		RBAC-U	✓	x	✓
Administrator1	S4	RBAC	✓	✓	x
		RBAC-U	✓	✓	x

RBAC-U omogućuje dodatni nivo kontrole pristupa, u odnosu na RBAC. Operateri iz gornjeg primjera posjeduju pravo nadgledanja i kontrole samo nad onim dijelom mreže za koji imaju aktivirane AOR-e. (označeno simbolom ✓ u tabeli 3).

Prikaz prozora kada se preko DERMS aplikacije vrši komandovanje za određenu oblast u slučaju gdje jedan operater posjeduje, a drugi operater ne posjeduje permisiju za komandovanje, ilustruju slike 18 i 19.



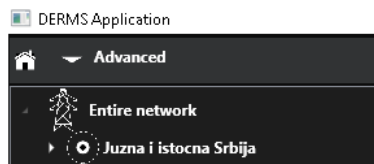
Slika 18 Prikaz za Operatera1, koji posjeduje permisiju za komandovanje



Slika 19 Prikaz za Operatera2, koji ne posjeduje permisiju za komandovanje

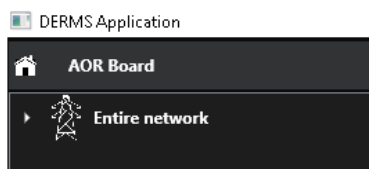
Razlika u prikazima za operatore je u tome što Operater2 ne posjeduje permisiju za kontrolisanje SCADA sistema nego posjeduje samo permisiju za nadgledanje. Kada Operater1 selektuje neku od oblasti iz *treeview*-a, koji sadrži hijerarhiju oblasti, i izabere opciju komandovanja za promjenu proizvodnje otvara mu se prikaz kao na slici 18. Segment *expander* WPF kontrole sadrži polja za unos *setpoint*-a, vremenski period na koji se komanda izdaje, kao i biranje algoritma raspodjele i na slici 18 je uokviren plavim okvirom. Za razliku od Operatera1, sekcija *Expander*-a je za Operatera2 sakrivena i ne može joj pristupiti kao što se može primjetiti na slici 19. Samim tim omogućen mu je samo prikaz grafikona sa mogućim smanjenjem i povećanjem snage, kao i vremenske linije izdatih komandi, ali bez mogućnosti da izdaje komande za datu oblast.

Posjedovanje permisije za ažuriranje statičkih podataka modela rezultuje različitim prikazima za operatore i model operatore. Model operaterima je omogućen pristup za primjenu novog CIM/XML fajla, kojim se ažuriraju postojeći podaci o mreži ili se unose novi. Pristup se omogućava preko dugmeta „Advanced“, iz menija. Prikaz za ModelOperater1 korisnika se nalazi na slici 20.



Slika 20 Prikaz za model operatera

Prikaz za Operatera1 se nalazi na slici 21, gdje se može primjetiti dugme „AOR Board“, koje otvara „AOR Board“ prozor, čija funkcionalnost je opisana u poglavlju 4.2.1. Dugme „Advanced“ operateru nije omogućeno tj. operater ne može vršiti operaciju ažuriranja statičkih podataka mreže.



Slika 21 Prikaz za operatera

U drugom eksperimentu se demonstrira slučaj kada jedna AOR oblast ostane nepokrivena, odnosno bez nadzora. U tabeli 5 se nalaze prikazani podaci za tri operatera i jednog administratora. Od operatera jedan ima selektovanu oblast 2 za nadgledanje i kontrolu, dok druga dva operatera nemaju.

Tabela 5 Skup korisnika sa dodijeljenim AOR-ima (O-oblast) prije deaktivacije Operatera1

Korisnik	Sesija	Korisnička uloga	O2- Nadgledanje	O2- Kontrola	O2- Ažuriranje
Operater1	S1	Operater	✓	✓	x
Operater2	S2	Operater	x	x	x
Operater3	S5	Operater	x	x	x
Administrator1	S4	Administrator	✓	✓	x

Nakon što se Operater1 izloguje sa sistema ili deaktivira dodijeljenu AOR oblast, poslaće se alarm zainteresovanim stranama. U tom slučaju Administator1 može da privremeno delegira nadležnosti upravljanja Oblasti 2, na Operatera 2 i/ili Operatera 3, tako da će Oblast2 biti pokrivena i stanje sistema biti ažurirano kao što se ilustruje plavom bojom u tabeli 6.

Tabela 6 Skup korisnika sa dodijeljenim AOR-ima (O-oblast) nakon delegiranja

Korisnik	Sesija	Korisnička uloga	O2- Nadgledanje	O2- Kontrola	O2- Ažuriranje
Operater1	S1	Operater	x	x	x
Operater2	S2	Operater	✓	✓	x
Operater3	S5	Operater	✓	✓	x
Administrator1	S4	Administrator	✓	✓	x



## 6. Zaključak

Povećanje broja distribuiranih energetske resursa (skr. DER) stvara decentralizovaniji elektroenergetski sistem i mijenja tradicionalnu dinamiku između lokalnih sistema distribucije i prenosnog sistema na nivou cijele regije. DER-ovi mogu donijeti mnogo koristi, čineći čistiji, efikasniji, pristupačniji i pouzdaniji sistem napajanja. Ali ove tehnologije se susreću se regulatornim sistemom namijenjenom starom svijetu centralizovanih elektrana, monopolskih komunalnih preduzeća i pasivnih potrošača. Danas je distributivna mreža postala jako kompleksna i integracija DER-ova sa tradicionalnom mrežom predstavlja veliki izazov. Informaciona bezbjednost postaje sve veća briga kako u fizičkom, tako i u elektronskom domenu. Sajber napadači se trude da pronađu i zloupotrijebe nedostatke sistema poput Smart Grida, pošto su servisi elektroenergetskog sistema od kritičnog značaja za moderno društvo.

Predmet istraživanja ovog rada spada u oblast kontrole pristupa u Smart Grid sistemima. S obzirom da RBAC model nije najpogodniji model u kritičnim infrastrukturnim sistemima kao što je Smart Grid, jer npr. ne uvažava parametre koji nisu dio identiteta korisnika, iako oni mogu uticati na dozvolu pristupa određenim resursima. Prilikom praktične primjene razvijenog modela napredne kontrole pristupa utvrđeno je da se proširenjem RBAC modela upravljanje pametnom mrežom može učiniti efikasnijim i pouzdanijim. Segmentiranjem nadzora, kontrole kao i izmjenama statičkog modela distributivnog sistema dobija se efikasniji način upravljanja kritičnom Smart Grid infrastrukturom. Hijerarhijska organizacija oblasti odgovornosti može da smanji broj oblasti odgovornosti koje je potrebno dodijeliti korisnicima čime se olakšava administracija modela kontrole pristupa.

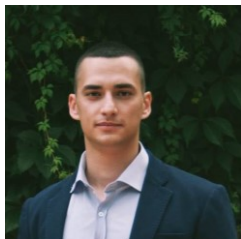
S obzirom da se trenutno rješenje bazira na manuelnom delegiranju nadležnosti kontrolisanja nepokrivene oblasti odgovornosti na drugog operatera, to je mjesto na kome bi bilo moguće implementirati naprednije rješenje. Dalji pravci istraživanja mogli bi da se baziraju na pronalaženju i optimizaciji algoritama koji bi vršili automatsku dodjelu nepokrivenih oblasti odgovornosti nekom od trenutno aktivnih operatera.

## 7. Literatura

- [1]. S. Fries, R. Falk, H. Dawidczak, and T. Dufaure, "Secure Integration of DER into Smart Energy Grid and Smart Market," Proceedings IARIA SMART 2015, June 2015, ISBN: 978-1-61208-414-5, page 56-61
- [2]. Fries, S., Falk, R., Dufaure, T., & Dawidczak, H. (2016). Decentralized Energy in the Smart Energy Grid and Smart Market—How to master reliable and secure control. Adv. Intell. Syst, 9, 65-75.
- [3]. Smyth, N. (2010). Security+ Essentials. eBookFrenzy.
- [4]. Rosić D. (2017). Model kontrole pristupa u Smart Grid sistemima. Novi Sad. RS:Faculty of technical sciences, University of Novi Sad
- [5]. Dahhaghchi, I., Christie, R. D., Rosenwald, G. W., & Liu, C. C. (1997). AI application areas in power systems. IEEE expert, 12(1), 58-66.
- [6]. Strezoski, V. C. (2014). Osnovi elektroenergetike. Fakultet tehničkih nauka, Novi Sad.
- [7]. Ponci F., Monti A., Electric Power Systems 2015. Monti, A., & Ponci, F. (2015). Electric power systems. In Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems (pp. 31-65). Springer, Berlin, Heidelberg.
- [8]. <http://www.smartgrids.eu> (pristup: jul 2019.)
- [9]. <http://www.low-carbonbritain.co.uk/smart-grid-energy-storage/> (pristup jul 2019.)
- [10]. The Distributed Energy Resource Management System Comes of Age <https://www.greentechmedia.com/articles/read/the-distributed-energy-resource-management-system-comes-of-age> (pristup: jul 2019.)
- [11]. Office of Electric Transmission and Distribution (2003). GRID 2030; A National Vision for Electricity's Second 100 Years, United States Department of Energy,
- [12]. Report to NIST on the Smart Grids Interoperability Standards Roadmap (2009), EPRI,
- [13]. Borlase, S. (2017). Smart grids: infrastructure, technology, and solutions. CRC press.
- [14]. Sinkovski, S., & Lučić, B. (2006). Informaciona bezbednost i kriptografija. Jugoimport SDPR Beograd, ZITEH, 06-R27.
- [15]. Whitman, M. E., & Herbert, J. (2011). Mattord Principles of information security. Course Technology., 290-301.
- [16]. Townsend Security Data Privacy Blog, <https://info.townsendsecurity.com> (pristup jul 2019.)
- [17]. [https://www.researchgate.net/publication/282219117\\_SECURITY\\_FUNDAMENTALS\\_ACCESS\\_CONTROL\\_MODELS/link/5608442d08ae8e08c09460d6/download](https://www.researchgate.net/publication/282219117_SECURITY_FUNDAMENTALS_ACCESS_CONTROL_MODELS/link/5608442d08ae8e08c09460d6/download) (pristup jun 2019.)
- [18]. Gibson, D., & Rogers, B. E. (2016). SSCP Systems Security Certified Practitioner: All-in-one Exam Guide. McGraw-Hill Education.
- [19]. Ferraiolo, D., Kuhn, D. R., & Chandramouli, R. (2003). Role-based access control. Artech House.
- [20]. <https://www.ekransystem.com/en/blog/rbac-vs-abac> (pristup avgust 2019.)
- [21]. David F. Ferraiolo and D. Richard Kuhn. (1992) Role-Based Access Controls Reprinted, National Institute of Standards and Technology. 15th National Computer Security Conference Baltimore, pp. 554-563
- [22]. Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security (TISSEC), 4(3), 224-274.

- [23]. Ferraiolo, D. F., Barkley, J. F., & Kuhn, D. R. (1999). A role-based access control model and reference implementation within a corporate intranet. *ACM Transactions on Information and System Security (TISSEC)*, 2(1), 34-64.
- [24]. Ferraiolo, D., Kuhn, D. R., & Chandramouli, R. (2007). *Role-based access control*. Second Edition Artech House.
- [25]. Fries, S., Falk, R., & Bisale, C. (2017, May). Handling Rolebased Access Control in the Digital Grid. In *ENERGY 2017: The Seventh International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies*.
- [26]. Ferraiolo, D. F., Gilbert, D. M., Lynch, N. An examination of Federal and Commercial Access Control Policy Needs. 16th National Computer Security Conference. Baltimore, Maryland. September 1993.
- [27]. <https://xmpp.org/> (pristup jul 2019.)
- [28]. D. Rosic, I. Lendak, S. Vukmirovic. (2015). A Role-based Access Control Model Supporting Regional Division in Smart Grid System, *Acta Polytechnica Hungarica* Vol. 12, No. 7

## 8. Podaci o kandidatu



Kandidat Dragan Erić je rođen 1994. godine u Zvorniku. Završio je srednju ekonomsku školu JU SŠC u Zvorniku 2013. godine. Osnovne akademske studije završio je 2018. godine na Fakultet tehničkih nauka u Novom Sadu. godine. Ispunio je sve obaveze i položio je sve ispite predviđene studijskim programom.