UNIVERZITET U NOVOM SADU
FAKULTET TEHNIČKIH NAUKA
U NOVOM SADU

Daniela Rosić

Model kontrole pristupa u Smart Grid sistemima

DOKTORSKA DISERTACIJA

Novi Sad, 2017. godine

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

КЉУЧНА ДОКУМЕНТАЦИЈСКА ИНФОРМАЦИЈА

Редни број, **РБР**:		
Идентификациони број, **ИБР**:		
Тип документације, **ТД**:		Монографска документација
Тип записа, **ТЗ**:		Текстуални штампани материјал
Врста рада, **ВР**:		Докторска дисертација
Аутор, **АУ**:		MSc Даниела Росић
Ментор, **МН**:		др Имре Лендак
Наслов рада, **НР**:		Модел контроле приступа у Смарт Грид системима
Језик публикације, **ЈП**:		српски
Језик извода, **ЈИ**:		српски
Земља публиковања, **ЗП**:		Република Србија
Уже географско подручје, **УГП**:		Аутономна покрајина Војводина
Година, **ГО**:		2017
Издавач, **ИЗ**:		Ауторски репринт
Место и адреса, **МА**:		Трг Доситеја Обрадовића 6, Нови Сад
Физички опис рада, **ФО**: (поглавља/страна/цитата/табела/слика/графика/прилога)		
Научна област, **НО**:		Електротехничко и рачунарско инжењерство
Научна дисциплина, **НД**:		Примењено софтверско инжењерство
Предметна одредница/Кључне речи, **ПО**:		Паметне мреже, контрола приступа, контрола приступа заснована на корисничким улогама
УДК		
Чува се, **ЧУ**:		Библиотека Факултета техничких наука, Нови Сад, Србија
Важна напомена, **ВН**:		
Извод, **ИЗ**:		У тези је анализиран проблем контроле приступа у Смарт Грид системима. Формално је специфициран модел контроле приступа за Смарт Грид који је заснован на унапређењу и проширењу *RBAC* модела и који је усклађен са актуелним захтевима у електроенергетској индустрији. Постављена је софтверска архитектура предложеног модела контроле приступа, чија је прототипска имплементација затим интегрисана у симулираном Смарт Грид окружењу.
Датум прихватања теме, **ДП**:		
Датум одбране, **ДО**:		
Чланови комисије, **КО**:	Председник:	др Владимир Стрезоски, редовни професор
	Члан:	др Игор Тартаља, ванредни професор
	Члан:	др Дарко Чапко, ванредни професор
	Члан:	др Милан Гаврић, доцент
	Члан:	др Горан Сладић, ванредни професор
	Члан, ментор:	др Имре Лендак, доцент

Потпис ментора

Образац **Q2.HA.06-05**- Издање 1

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

KEY WORDS DOCUMENTATION

Accession number, **ANO**:		
Identification number, **INO**:		
Document type, **DT**:		Monographic publication
Type of record, **TR**:		Textual printed material
Contents code, **CC**:		PhD thesis
Author, **AU**:		Daniela Rosić
Mentor, **MN**:		Professor Imre Lendak
Title, **TI**:		
Language of text, **LT**:		Serbian
Language of abstract, **LA**:		Serbian
Country of publication, **CP**:		Republic of Serbia
Locality of publication, **LP**:		Vojvodina
Publication year, **PY**:		
Publisher, **PB**:		Author's reprint
Publication place, **PP**:		Trg Dositeja Obradovića 6, Novi Sad
Physical description, **PD**: (chapters/pages/ref./tables/pictures/graphs/ appendixes)		
Scientific field, **SF**:		Electrical and Computer Engineering
Scientific discipline, **SD**:		Applied software engineering
Subject/Key words, **S/KW**:		Smart grid, access control, role-based access control
UC		
Holding data, **HD**:		Library of Faculty of Technical Sciences, Trg D. Obradovića 6, Novi Sad, Serbia
Note, **N**:		
Abstract, **AB**:		This thesis discusses the challenges related to access control in Smart Grid systems. A formal model for access control in the Smart Grid is specified, extending the role-based access control (*RBAC*) model to be in accordance with the existing security requirement in the power industry. Based on the proposed access control model, software architecture was developed and its prototype implementation is integrated in a Smart Grid simulated environment.
Accepted by the Scientific Board on, **ASB**:		
Defended on, **DE**:		
Defended Board, **DB**:	President:	Vladimir Strezoski, Ph.D., Full Professor
	Member:	Igor Tartalja, Ph.D., Associate Professor
	Member:	Darko Čapko, Ph.D., Assistant Professor
	Member:	Milan Gavrić, Ph.D., Assistant Professor
		Goran Sladić, Ph.D., Associate Professor
	Member, Mentor:	Imre lendak, Ph.D., Assistant Professor

Menthor's sign

Obrazac **Q2.HA.06-05**- Izdanje 1

Sadržaj

Spisak slika

Spisak tabela

Spisak skraćenica

ABAC	(eng. *attribute-based access control*) - model kontrole pristupa zasnovan na atributima
ACL	(eng. *access control list*) - lista kontrole pristupa
AOR	(eng. *area of responsibility*) - oblasti odgovornosti
APT	(eng. *advanced persistent threat*) - napredne trajne pretnje
CIM	(eng. *Common Information Model*) - standard za modelovanje elektroenergetskih sistema
CIS	(eng. *Customer Information System*) - sistem za skladištenje podataka o potrošačima
DAC	(eng. *Discretionary Access Control*) - diskrecioni model kontrole pristupa
DMS	(eng. *Distribution Management System*) - sistem za upravljanje distributivnom elektroenergetskom mrežom
DMZ	(eng. *demilitarized zone*) - demilitarizovana zona
DoS	(eng. *denial of service*) - napad uskraćivanjem usluge
DSoD	(eng. *Dynamic Separation of Duties*) - dinamička separacija/razdvajanje obaveza
DSS	(eng. *Decision Support System*) – sistem za podršku u odlučivanju
EMS	(eng. *Energy Management System*) - sistem za upravljanje prenosnom elektroenergetskom mrežom
ENISA	(eng. *European Network and Information Security Agency*) - Evropska agencija za bezbednost računarskih mreža i informacija
GIS	(eng. *Geographic Information System*) - geografski informacioni sistem
IEC	(eng. *International Electrotechnical Commission*) - Međunarodna elektrotehnička komisija
IED	(eng. *Intelligent Electronic Device*) - inteligentni elektronski uređaj
InfoSec	(eng. *information security*) - informaciona bezbednost
IS	(eng. *information system*) – informacioni sistem
ISA	(eng. *The International Society of Automation*) - Međunarodno udruženje za automatizaciju
ISO	(eng. *International Organization for Standards*) - Međunarodne organizacije za standarde
MAC	(eng. *Mandatory Access Control*) - mandatorni model kontrole pristupa
NERC	(eng. *North American Electric Reliability Corporation*)
NIST	(eng. *National Institute of Standards and Technology*) - nacionalni institut za standarde i tehnologije
NMS	(eng. *Network Model Service*) - sistem za upravljanje modelom podataka
OMS	(eng. *Outage Management System*) - sistem za upravljanje ispadima
PDC	(eng. *Phasor Data Concentrator*) - koncentrator fazora
PII	(eng. *personally identifiable information*) – lični podaci o korisniku
PIN	(eng. *Personal Identity Number*) - lični identifikacioni broj
PLC	(eng. *Programmable Logic Controllers*) - programabilni logički kontroleri
RBAC	(eng. *role-based access control*) – model kontrole pristupa zasnovan na korisničkim ulogama

RTU	(eng. *Remote Terminal Unit*) - udaljena terminalna jedinica
SCADA	(eng. *Supervisory Control and Data Acquisition*) - sistem za nadzor i upravljanje industrijskim procesima
SoD	(eng. *Separation of Duties*) - separacija/razdvajanje obaveza
SSoD	(eng. *Static Separation of Duties*) - statička separacija/razdvajanje obaveza
UML	(eng. *Unified Modeling Language*) - objedinjeni jezik modelovanja
UMS	(eng. *Utility Management System*) - sistem za nadzor i kontrolu, analizu i optimizaciju elektroenergetskog sistema
VLAN	(eng. *virtual local area network*) - virtuelna lokalna mreža
WFS	(eng. *WorkForce Management System*) - sistem za upravljane posadom na terenu
WMS	(eng. *Work Management Service*) - sistem za upravljanje radovima
XACML	(eng. *Extensible Access Control Markup Language*) – jezik za specifikaciju autorizacionih politika

1 Uvod

Pametne mreže (eng. *Smart Grid*) su savremene kritične infrastrukture koje podrazumevaju integraciju tradicionalnih energetskih sistema za proizvodnju, prenos i distribuciju energenata (električna energija, gas, voda) sa informacionim i komunikacionim tehnologijama u cilju povećanja pouzdanosti, sigurnosti i efikasnosti sistema kritičnih za svakodnevno funkcionisanje modernog društva. Informacione i komunikacione tehnologije su ključni faktor u razvoju pametnih mreža, ali njihovom primenom se savremene elektroenergetske infrastrukture istovremeno izlažu novim bezbednosnim pretnjama i rizicima. Oslanjanjem na komunikacione mreže i integrisanjem velikog broja podsistema koje odlikuje raznolikost u pogledu funkcionalnosti i korišćenih tehnologija znatno se usložnjava informaciona infrastruktura elektroenergetskog sistema, a time se povećava i ranjivost sistema. Tradicionalni pristup bezbednosti industrijskih kontrolnih sistema [60], koji se oslanjao na fizičku izolovanost i princip tajnosti nije više dovoljan za pouzdan i siguran rad savremenih elektroenergetskih sistema. Osim zaštite od fizičkih napada, neophodno je obezbediti zaštitu od napada u sajber prostoru, odnosno obezbediti zaštitu informacionih sistema i komunikacione mreže (eng. *cyber security*).

Informaciona bezbednost (eng. *information security*, skr. *InfoSec*) se odnosi na očuvanje poverljivosti, integriteta i raspoloživosti informacionih sistema primenom bezbednosnih mehanizama koji treba da budu unapred određeni, primenjeni, nadgledani i poboljšavani. Poverljivost (eng. *confidentiality*) se odnosi na zaštitu podataka od neovlašćenog čitanja i otkrivanja. Integritet (eng. *integrity*) se odnosi na zaštitu podataka od neovlašćenih izmena ili brisanja kako bi se obezbedila konzistentnost informacija. Raspoloživost (eng. *availability*) je mogućnost ovlašćenih korisnika da pravovremeno pristupaju sistemu i podacima, i odnosi se na zaštitu od neovlašćenog zadržavanja ili prekida koji mogu uzrokovati korumpiranost podataka ili nedostupnost sistema. Ova tri kriterijuma informacione bezbednosti, odnosno bezbednosni ciljevi, su poznati pod nazivom *CIA* (*Confidentiality-Integrity-Availability*) trijada [33].

Kontrola pristupa (eng. *access control*) je jedan od osnovnih bezbednosnih mehanizama kojim se obezbeđuje da samo ovlašćeni korisnici mogu pristupiti resursima računarskog sistema. Kontrola pristupa je ključna mera bezbednosti u očuvanju poverljivosti i integriteta podataka. Poverljivost se postiže tako što samo ovlašćeni korisnici mogu da čitaju podatke, dok se očuvanje integriteta odnosi na zahtev da samo ovlašćeni korisnici mogu da modifikuju ili brišu podatke. Kontrolu pristupa čine tri fundamentalna procesa [33][126]:

- Identifikacija (eng. *identification*) je predstavljanje korisnika sistemu.
- Autentifikacija (eng. *authentication*) je proces verifikacije identiteta korisnika, odnosno proces kojim se potvrđuje da se zaista radi o predstavljenom korisniku.

- Autorizacija (eng. *authorization*) je proces odlučivanja kojim resursima korisnik može da pristupi i koje operacije može da izvršava u sistemu.

Od početka XXI veka elektroenergetska industrija se suočava sa različitim problemima uzrokovanim informaciono-bezbednosnim propustima koji mogu imati izuzetno značajne posledice, npr. prekid redovnih operativnih aktivnosti uz značajne ekonomske gubitke, gubitak poverenja korisnika prema kompaniji i šteta za reputaciju kompanije, sve do prouzrokovanja katastrofa koje ugrožavaju životnu sredinu ili dovode do ljudskih žrtava. Jedan od najpoznatijih napada na industrijske kontrolne sisteme je *Stuxnet* [129] koji je otkriven 2010. godine. Meta napada su bila iranska nuklearna postrojenja, a metod napada je bio posebno razvijen zlonameran softver (eng. *malware*) dizajniran tako da iskoristi ranjivost operativnog sistema i industrijskog kontrolnog sistema sa ciljem preuzimanja kontrole nad sistemom za upravljanje industrijskim procesom, što je rezultovalo finansijskim gubicima i unazadilo razvoj nuklearnih mogućnosti države. Zlonamerni softver je dospeo u sistem putem USB memorijskih uređaja, odakle se širio na ostale računare koristeći ranjivosti *Microsoft Windows* operativnog sistema koje do tada nisu bile javno poznate, tzv. ranjivosti nultog dana. Na zaraženim računarima *Stuxnet* je tražio *Siemens WinCC* softver za upravljanje programabilnim logičkim kontrolerima (eng. *Programmable Logic Controllers*, skr. *PLC*), kao i *Step7* softver za programiranje PLC uređaja na *Windows* platformi. Instaliranjem rutkit softvera (eng. *rootkit*) na Windows računarima i PLC uređajima *Stuxnet* je uspeo da ostane potpuno neprimećen, kao i da maskira svoje prisustvo. Krajnji cilj je bilo preuzimanje kontrole nad *Siemens* PLC uređajima modela S7-300 čija je svrha kontrolisanje frekvencije obrtaja motora. Za pristup podacima PLC uređaja i modifikaciju koda iskorišćen je bezbednosni propust u WinCC upravljačkom softveru koji je u programskom kodu imao zapisanu administratorsku šifru. Nakon uspešnog inficiranja PLC uređaja, zlonameran softver je mogao da izdaje komande kojima modifikuje frekvenciju obrtaja motora van predviđenih opsega u vidu velikog broja ubrzanja i usporenja što je dovelo do kvara centrifuga za prečišćavanje uranijuma [32][65][129].

U decembru 2015. godine tri ukrajinske elektrodistributivne kompanije su bile meta hakerskog napada koji je uzrokovao prekid napajanja kod 225000 potrošača u trajanju do 6 sati. Napadači su preko udaljenog pristupa industrijskim kontrolnim sistemima izdali komande prekidačima i na taj način isključili delove elektrodistributivne mreže. Kasnijom analizom je utvrđeno da je na računarima zahvaćenih kompanija otkriven *BlackEnergy* (skr. *BE*) zlonamerni softver za koji se pretpostavlja da je korišćen za prikupljanje podataka za pristup sistemu. BE je dospeo u korporativnu mrežu kompanija preko *spear-phishing* napada [126] u kojem je zaraženi *Microsoft Office* dokument poslat kao e-mail prilog. Takođe, korišćen je i socijalni inženjering, jer su prikazane poruke navele radnike napadnutih kompanija da aktiviraju makroe u zaraženim dokumentima. U toku faze izviđanja za koju se pretpostavlja da je trajala nekoliko meseci, napadači su došli do korisničkih naloga za udaljeni pristup industrijskim kontrolnim sistemima.

Takođe, napadači su napisali maliciozni firmver (eng. *firmware*) sa ciljem da korumpiraju uređaje za konverziju podataka iz serijskog u *Ethernet* format, kako bi onemogućili dispečere da šalju komande iz kontrolnog centra. Prilikom realizacije napada, na dispečerskim radnim stanicama na kojima su stekli udaljeni pristup napadači su počeli sa izdavanjem komandi prekidačima za isključenje delova mreže. Istovremeno, izvršen je napad na sistem za prijavu kvarova u vidu velikog broja fiktivnih telefonskih poziva, koji su preopteretili telefonske centrale napadnutih kompanija, a sve sa ciljem da bi potrošači bili onemogućeni da prijave ispad ili dobiju informacije o isključenju. Na kraju, *KillDisk* zlonamerni softver je obrisao datoteke sa korumpiranih operatorskih radnih stanica [39][77][109][130]. Ovaj napad je tipičan primer napredne trajne pretnje (eng. *advanced persistent threat*, skr. *APT*) [18], odnosno predstavlja sinhronizovan i koordinisan proces iskorišćavanja ranjivosti sistema primenom sofisticiranih tehnika kako bi se dobio pristup ciljanom sistemu i omogućilo kontinuirano prikupljanje osetljivih informacija u dužem vremenskom periodu, odnosno do sprovođenja napada i postizanja krajnjeg cilja.

Zlonameran softver *Duqu* je otkriven 2011. godine i takođe je dizajniran da kompromituje industrijske sisteme, ali za razliku od *Stuxnet*-a, „samo“ sa ciljem da prikuplja podatke iz kontrolnih sistema za buduću eksploataciju [14].

Osim malicioznih napada koji mogu da izazovu modifikaciju, kašnjenje ili gubitak podataka i time ugroze pravilno funkcionisanje sistema, veliki izazov predstavlja i očuvanje privatnosti korisnika, s obzirom da su informacije o potrošačima sada dostupne u poslovnim informacionim sistemima. Takođe, propusti u softveru ili nenamerne greške validnih korisnika mogu da imaju ozbiljne posledice po rad elektroenergetskog sistema. Npr. u avgustu 2003. je usled izostanka alarma prouzrokovanog greškom u izvornom kodu (tzv. bug-a) u korišćenom sistema za kontrolu i nadzor dispečeri nisu dobili sve potrebne informacije pravovremeno, i nisu primenili neophodne mere, pa je došlo do kaskadnog ispada u elektroenergetskom sistemu koji je zahvatio veliku oblast Severne Amerike (tzv. *Northeast blackout of 2003*). Tada je nekoliko desetina miliona ljudi ostalo bez električne energije u trajanju od nekoliko dana [73][124]. U septembru 2003. su problemi uzrokovani ljudskom greškom i neefikasnom komunikacijom između operatora u kontrolnom centru doveli do prekida u napajanju u Italiji i delu Švajcarske rezultujući velikim finansijskim gubicima [10][53][119].

1.1 Predmet istraživanja

U prošlosti, industrijski kontrolni sistemi su bili razvijani kao specijalizovani sistemi za nadzor i upravljanje fizičkim procesima i uređajima u realnom vremenu. Ovi sistemi su se zasnivali na industrijskim protokolima i namenskim operativnim sistemima koji su dizajnirani za rad u realnom vremenu, odnosno za koje je od ključnog značaja vreme odziva i kontinualna dostupnost sistema. Sa stanovišta bezbednosti su se ti sistemi oslanjali na fizičku izolovanost (odnosno sistem i njegovi podaci su zaštićeni, jer su fizički

nedostupni) i princip tajnosti (eng. *security by obscurity*), uz minimalnu primenu bezbednosnih mehanizama za zaštitu ljudskog elementa, uređaja i industrijskih protokola [60][61].

Proces modernizacije elektroenergetskih sistema podrazumeva 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 snabdevanja, zatim napredni merni sistemi za upravljanje potrošnjom i brojilima električne energije, automatizovani sistemi za naplatu, i drugi sistemi za upravljanje poslovnim procesima elektroenergetske kompanije. Ključni faktor u procesu modernizacije je primena informacionih i komunikacionih tehnologija čija upotreba dovodi do povećanja pouzdanosti, efikasnosti i kvaliteta snabdevanja električnom energijom, smanjenja gubitaka električne energije i unapređenja zaštite životne sredine. Pored brojnih prednosti u pogledu poboljšanja procesa isporuke električne energije od proizvodnje do potrošnje i naplate, informacione i komunikacione tehnologije unose i nove slabosti koje u tradicionalnim sistemima nisu postojale, poput slabosti *Internet Protocol (IP)*-baziranih komunikacionih tehnologija ili slabosti u softveru, a čije iskorišćenje može da ima ozbiljne posledice po rad elektroenergetskog sistema. Osim toga, međusobno povezivanje sistema i sve veći broj pristupnih tačaka za razmenu podataka između sistema omogućuje lateralnu propagaciju zlonamernog softvera i/ili napadača kroz zahvaćeni sistem i uspešan napad na sistem. Poseban izazov predstavlja činjenica da se savremeni elektroenergetski sistemi sastoje od velikog broja podsistema koje odlikuje raznolikost u pogledu funkcionalnosti i korišćenih tehnologija, a time i bezbednosnih zahteva koje je potrebno razmotriti.

Primena efikasnih bezbednosnih mehanizama za zaštitu informacionih sistema je od suštinske važnosti za pouzdan, efikasan i siguran rad savremenih elektroenergetskih sistema, koji su zbog svoje kritičnosti za funkcionisanje modernog društva veoma česta meta sajber napada. Implementacija jakih i robusnih kontrola pristupa prilagođenih složenim zahtevima savremenih elektroenergetskih sistema je od suštinske važnosti za dostizanje adekvatnog nivoa informacione bezbednosti. Iako je u dostupnoj naučnoj i stručnoj literaturi kontrolama pristupa posvećena odgovarajuća pažnja, modeli koji bi zadovoljili specifične zahteve Smart Grid sistema su razmatrani samo delimično. Postojeća istraživanja se uglavnom baziraju na standardnom *role-based access control* (skr. *RBAC*) modelu kao jednom od najčešće korišćenih modela za kontrolu pristupa u sistemima koje karakteriše veliki broj korisnika i resursa koje je potrebno zaštititi. RBAC model čine sledeći entiteti: korisnici, korisničke sesije, uloge i privilegije, pri čemu se privilegije sastoje od operacija koje se izvršavaju nad objektima. Centralni deo RBAC modela predstavlja koncept uloge oko koje su formulisana prava pristupa. Ulogama se dodeljuju privilegije, a korisnicima se dodeljuju uloge. Osim osnovnog RBAC-a koji definiše skup entiteta i njihovih međusobnih relacija, standardom su definisana i njegova tri proširenja: model hijerarhije uloga kojim se pojednostavljuje administracija modela u

slučaju preklapanja korisničkih uloga po pitanju dodeljenih privilegija, model statičkog razdvajanja dužnosti kojim je moguće sprečiti dodelu konfliktnih korisničkih uloga korisniku u toku administracije modela, i model dinamičkog razdvajanja dužnosti kojim je moguće ograničiti skup korisničkih uloga dodeljenih korisniku prilikom uspostavljanja korisničke sesije. S obzirom na jednostavnost upravljanja bezbednosnim politikama, kao i smanjenja kompleksnosti i troškova administracije, RBAC je jedan od najzastupljenijih modela za kontrolu pristupa u modernim informacionim sistemima [29].

Sa razvojem heterogenih, distribuiranih (eng. *pervasive*) računarskih sistema sve češće se javlja potreba da neki drugi faktori koji nisu deo korisničkog identiteta (npr. vreme pristupa sistemu, lokacija sa koje se pristupa sistemu, itd.) utiču na odluke o pristupu resursima. Za upravljanje bezbednošću u Smart Gridu poseban izazov predstavlja dinamična i nepredvidiva priroda ovih sistema. Dinamičnost se ogleda u velikoj frekvenciji promena u elektroenergetskom sistemu (npr. izmene vrednosti napona, jačine struje, pozicije prekidača, itd.) na koje je potrebno adekvatno odgovoriti. Nepredvidivost se odnosi na uticaj nepredviđenih situacija na stabilan rad sistema, kao što su prirodne katastrofe, otkazi ili nedostupnost računarskih i komunikacionih resursa. S obzirom da RBAC model ne može da zadovolji takve zahteve bez dodatnih unapređenja, u literaturi postoje tri pristupa za prevazilaženje ovog problema. Prvi pristup se odnosi na proširivanje RBAC modela prema zahtevima i karakteristikama sistema. Drugi pristup predlaže primenu modela kontrole pristupa koji je zasnovan na atributima, *attribute-based access control* (skr. *ABAC*) model [52]. U ABAC modelu se autorizacione odluke donose u zavisnosti od vrednosti atributa korisnika, atributa objekata i kontekstnih atributa, pri čemu su kontekstni atributi obeležja okruženja čije se vrednosti mogu dinamički menjati. Treći pristup je kombinovanje prednosti RBAC i ABAC modela u tzv. RBAC-A hibridne modele [63].

Analizom zahteva kompanija za prenos i distribuciju električne energije, u ovom radu je identifikovan sledeći skup zahteva koje je potrebno ispuniti da bi se postigao odgovarajući nivo bezbednosti i omogućila ne samo zaštita od neovlašćenog pristupa, već i smanjili rizici od nenamernih grešaka validnih korisnika i omogućilo pouzdanije i efikasnije upravljanje sistemom:

- **Kontrola pristupa prema oblastima odgovornosti** (eng. *area of responsibility*, skr. *AOR*), odnosno podela odgovornosti između korisnika koji pripadaju istim korisničkim ulogama prema oblastima odgovornosti kako bi se obezbedilo pouzdanije i efikasnije izvršavanje kritičnih operacija unutar elektroenergetskog sistema. Oblast odgovornosti predstavlja skup dozvoljenih operacija nad objektima koji dele iste karakteristike unutar elektroenergetskog sistema.
- **Mogućnost delegiranja korisničkih zaduženja i odgovornosti** kako bi se obezbedilo efikasnije upravljanje elektroenergetskom mrežom u vanrednim situacijama uzrokovanim vremenskm nepogodama kao što su velike oluje, zemljotresi, i slično. Npr. zemljotresi mogu izazvati nedostupnost regionalnog

kontrolnog centra i tada bi operateri iz drugih kontrolnih centara trebali da imaju mogućnost upravljanja delovima mreže za koje u regularnim uslovima nemaju ovlašćenja. Oluje mogu izazvati veliki broj ispada u elektroenergetskom sistemu i tada bi operateri trebali da imaju mogućnost preuzimanja odgovornosti nad delovima mreže koji nisu u njihovoj nadležnosti kako bi se što efikasnije otklonili kvarovi u mreži i smanjilo vreme prekida napajanja krajnjih potrošača.

- **Kontrola pristupa prema lokaciji ili nameni radne stanice.** S obzirom na sve veći broj pristupnih tačaka u sistemu, uključujući i mogućnost pristupa preko javne mreže, bezbednosne politike treba da razmatraju lokaciju i namenu radne stanice sa koje korisnik pristupa sistemu. Npr. ukoliko korisnik pristupa sistemu iz poslovnog sistema ili sa udaljenih lokacija ne bi trebao da ima ovlašćenja za izvršavanje nadzorno-upravljačkih akcija u kontrolnom centru, bez obzira na korisničke uloge koje su mu dodeljene. O važnosti ovog zahteva svedoči primer napada u Ukrajini u kojem su napadači, kompromitovanjem korisničkih naloga operatora, uspeli da pristupe radnim stanicama u kontrolnom centru sa udaljenih lokacija i da izdaju komande za isključenje delova elektrodistributivne mreže u ime operatora.
- **Kontrola pristupa prema tipu Smart Grid aplikacije.** Pored klasičnih operacija upravljanja elektroenergetskim sistemom u realnom vremenu, Smart Grid nudi širok spektar funkcionalnosti koje su potrebne za efikasniji rad korisnika u kontrolnom centru, ali i unapređenje poslovnih procesa elektroenergetske kompanije. To obuhvata brojne analitičke elektroenergetske funkcije, simulaciju rada elektroenergetske mreže u željenim uslovima, istoriju podataka za potrebe analiza i kreiranje izveštaja regulatornim telima, integraciju sa drugim sistemima čiji podaci mogu biti od značaja za efikasno funkcionisanje. Stoga, prava pristupa treba da budu definisana u skladu sa specifičnim funkcionalnostima koje određena Smart Grid aplikacija nudi, npr. za aplikacije za rad u realnom vremenu treba da važe stroža pravila pristupa, u poređenju sa aplikacijama za simulacije rada sistema van realnog vremena ili poslovne aplikacije, itd. Npr. za pristup aplikacijama za upravljanje elektroenergetskim sistemom u realnom vremenu se najčešće zahteva više od jednog faktora autentifikacije, što nije slučaj za simulacione aplikacije.
- **Kontrola pristupa prema vremenskoj odrednici, pre svega period važenja licence.** Kako je izvršavanje određenih operacija unutar elektroenergetskog sistema regulisano licencom izdatom od strane regulatornih tela (npr. licenca za operatera prenosnog sistema, licenca za članove posade za radove na terenu), kontrola pristupa treba da omogući ograničavanje skupa korisničkih uloga u zavisnosti od toga da li korisnik poseduje važeću licencu.
- **Kontrola pristupa u više-domenskom okruženju.** Razvoj informacionih tehnologija i pojava Interneta doneli su suštinske promene u načinu poslovanja, uključujući i interorganizacione poslovne procese kada kompanije deo svog poslovnog procesa poveravaju drugim organizacijama ili omogućuju pristup podacima koji su od interesa za sve učesnike u interorganizaciji. Npr. čest je slučaj da elektroenergetske kompanije angažuju druge kompanije za izvršavanje radova na terenu i upravljanje članovima posade, što za posledicu

ima problem duple administracije korisničkih naloga i sinhronizacije podataka između kompanija. Odavde proizilazi da kontrola pristupa treba da bude primenljiva i u više-domenskom okruženju bez uvođenja dodatne kompleksnosti administracije i sinhronizacije podataka.

Bezbednost i zaštita Smart Grid sistema predstavlja prioritet ne samo za elektroenergetske kompanije i krajnje potrošače, već i za svaku državu čija nacionalna bezbednost, nacionalna ekomonija, javno zdravlje i bezbednost stanovništva može biti posredno ugrožena preko napada na pametne elektroenergetske sisteme. Definisanjem regulatornih mera u vidu standarda, propisa i preporuka država definiše i primenjuje mere za zaštitu Smart Grid sistema. Stoga, neophodno je da bezbednosni mehanizmi budu definisani prema zahtevima vladajućih standarda. Relevantni tela koja kreiraju i publikuju tehničke standarde za informacionu bezbednost u oblasti Smart Grida su: ISO (*International Organization for Standards*), NIST (*National Institute of Standards and Technology*), IEC (*International Electrotechnical Commission*), NERC CIP (*North America Electric Reliability Corporation Critical Infrastructure Protection*), ENISA (*European Network and Information Security Agency*). U okviru ove disertacije identifikovani su sledeći zahtevi propisani standardima koje je potrebno ispuniti prilikom definisanja modela za kontrolu pristupa u Smart Gridu:

- Očuvanje poverljivosti, integriteta i raspoloživosti podataka u skladu sa prioritetima za Smart Grid informacioni sistem. Npr. raspoloživost resursa predstavlja kritični zahtev za kontrolne sisteme, dok gubitak poverljivosti podataka nosi manje bezbednosne rizike u odnosu na raspoloživost i integritet. Nasuprot tome, u sistemima koji su orijentisani ka poslovnim procesima kompanije i uslugama za potrošače poverljivost podataka je kritičan zahtev, dok je kašnjenje podataka ili privremena nedostupnost sistema dozvoljena.
- Kontrolisan pristup informacionim sistemima i podacima u skladu sa bezbednosnom politikom organizacije.
- Kontrola toka podataka unutar sistema, između sistema sa različitim bezbednosnim zahtevima, a posebno prilikom pristupa iz eksternih sistema i preko javne mreže (npr. Internet) .
- Princip najmanjih privilegija (eng. *Least Privilege*), odnosno dodela najmanjeg skupa privilegija potrebnih za izvršavanje funkcija za koje je korisnik ovlašćen i sprečavanje mogućnosti da korisnik izvrši nepotrebne operacije.
- Princip razdvajanja obaveza (eng. *Separation of Duties*), odnosno raspodela odgovornosti prilikom izvršavanja kritičnih operacija tako da pojedinačno nijedan korisnik nije ovlašćen za izvršavanje celokupnog procesa.

Predmet istraživanja ove disertacije pripada oblasti kontrole pristupa u Smart Grid sistemima. Motivacija za istraživanjem leži u nedovoljno istraženoj oblasti kontrole pristupa u Smart Gridu, kao i nemogućnosti standardnog RBAC modela da odgovori specifičnim Smart Grid zahtevima. Analizom različitih modela kontrole pristupa koja su

istražena kroz dostupnu literaturu, ustanovljeno je da bez dodatnih modifikacija i unapređenja oni ne mogu da odgovore aktuelnim zahtevima u elektroenergetskoj industriji.

1.2 Cilj istraživanja i očekivani rezultati

Osnovni cilj ovog istraživanja je unapređenje standardnog RBAC modela tako da odgovori aktuelnim zahtevima u elektroenergetskoj industriji. Zarad prevazilaženja nedostataka navedenih u predmetu istraživanja i dostizanja gore navedenog cilja je potrebno uraditi sledeće, tj. proširiti RBAC model sledećim elementima:

- **Proširenje osnovnog RBAC modela sa oblastima odgovornosti.** Kontrola pristupa u zavisnosti od oblasti odgovornosti treba da omogući efikasniju raspodelu odgovornosti i obezbedi pouzdanije i efikasnije upravljanje elektroenergetskim sistemom.
- **Uvođenje hijerarhije oblasti odgovornosti.** Hijerarhijski organizovane oblasti odgovornosti treba da smanje broj oblasti odgovornosti dodeljenih korisniku i time olakšaju administraciju modela.
- **Uvođenje dinamičkih ograničenja i proširenja** u zavisnosti od korisničkih atributa (važeća licenca, organizacija kojoj korisnik pripada) i parametara okruženja (radna stanica sa koje se pristupa sistemu, tip Smart Grid aplikacije kojoj se pristupa, zahtevi za delegiranje zaduženja). Dinamička ograničenja/proširenja treba da omoguće uvažavanje različitih faktora koji mogu uticati na odluke o pristupu u Smart Gridu bez uvođenja dodatne kompleksnosti administracije i sinhronizacije podataka. Osim nepormenljivih dinamičkih ograničenja/proširenja čija se vrednost ne menja u toku korisničke sesije, uvode se i promenljiva tj. dinamička ograničenja i proširenja čija se vrednost može menjati u toku korisničke sesije (zahtevi za delegiranje odgovornosti).

U cilju ispitivanja primenljivosti predloženog proširenja RBAC modela u Smart Grid okruženju i usklađenosti sa zahtevima relevantnih bezbednosnih standarda, postavljena je softverska arhitektura odgovarajućeg sistema za kontrolu pristupa, čija je prototipska implementacija zatim integrisana u simuliranom Smart Grid okruženju koje je razvijeno u skladu sa standardnim IEC-62443 bezbednosnim modelom za Smart Grid. U ovoj disertaciji se kao referentni model bezbednosne arhitekture za Smart Grid predlaže proširenje IEC-62443 modela bezbednosnih zona kontrolnog sistema. Zatim je formiran niz test scenarija na osnovu zahteva sa realnih Smart Grid projekata u kojima je autorka učestvovala, a koji treba da pokažu da predloženi model kontrole pristupa može da odgovori postavljenim zahtevima, kao i to da je u poređenju sa postojećim modelima više usklađen sa specifičnostima zahteva i sistema.

1.3 Hipoteze

Iz predmeta istraživanja, u skladu sa postavljenim ciljevima istraživanja i do sada postignutim rezultatima u polju istraživanja predmetne oblasti i aktuelnog stanja istraživanja u oblasti, moguće je definisati sledeće hipoteze:

Hipoteza H1: RBAC model nije adekvatan model kontrole pristupa u Smart Grid sistemima.

Hipoteza H2: RBAC model je moguće uskladiti sa aktuelnim bezbednosnim zahtevima elektroenergetske industrije u oblasti kontrole pristupa, kako zahtevima postavljenim od strane elektroenergetskih kompanija, tako i zahtevima koji su definisani vladajućim standardima u oblasti informacione bezbednosti za Smart Grid.

Hipoteza H3: Prošireni RBAC model je moguće primeniti u Smart Grid sistemu u skladu sa postavljenim bezbednosnim zahtevima.

1.4 Prikaz disertacije po poglavljima

Doktorska disertacija je organizovana u osam poglavlja.

U prvom poglavlju je dat pregled problematike informacione bezbednosti u savremenim elektroenergetskim sistemima, uključujući i relevantne primere sajber napada na Smart Grid. Opisan je predmet istraživanja, cilj istraživanja i očekivani rezultati i postavljene su hipoteze istraživanja.

U drugom poglavlju su data osnovna teorijska razmatranja sa aktuelnim stanjem u oblasti istraživanja. Date su teorijske osnove iz oblasti informacione bezbednosti za razumevanje načina funkcionisanja postojećih modela za kontrolu pristupa. Takođe, opisani su modeli kontrole pristupa koji se pretežno koriste u upravljanju heterogenim distribuiranim računarskim sistemima. Zatim, dat je pregled vladajućih tehničkih standarda koji se odnose na informacionu bezbednost u Smart Gridu. Prikazani su referentni modeli za Smart Grid potrebni za razumevanje informacione infrastrukture ovih sistema i razvoj modela bezbednosne arhitekture za Smart Grid.

U trećem poglavlju dat je pregled aktuelnih bezbednosnih zahteva u oblasti kontrole pristupa u Smart Grid sistemima. Prvo su navedeni zahtevi propisani standardima u oblasti informacione bezbednosti za Smart Grid, a zatim zahtevi kompanija za prenos i distribuciju električne energije. Potom su diskutovani nedostaci postojećih modela kontrole pristupa sa aspekta postavljenih ciljeva istraživanja i hipoteza. Na kraju ovog poglavlja je prikazan predloženi model bezbednosne arhitekture za Smart Grid.

U četvrtom poglavlju predstavljena je metodologija istraživanja. Opisane su sve faze istraživanja i korišćene istraživačke metode, kao i tipovi eksperimentalnih istraživanja na osnovu kojih će biti izvršena provera primenljivosti predloženog rešenja.

U petom poglavlju je data formalna specifikacija modela kontrole pristupa za Smart Grid koji je zasnovan na unapređenju i proširenju RBAC modela. Formalnom specifikacijom su obuhvaćeni entiteti modela i njihove međusobne relacije, model dinamičkih ograničenja i proširenja, kao i model sprovođenja kontrole pristupa.

U šestom poglavlju je opisana softverska arhitektura sistema za kontrolu pristupa. Opisana je arhitektura sledećih podsistema prezentovanog modela:

- Modul za upravljanje bezbednosnim podacima,
- Modul za upravljanje statičkim kontekstom sesije, namenjen za dobavljanje vrednosti parametara koji mogu uticati na autorizacione odluke i upravljanje redosledom njihove primene prilikom uspostavljanja korisničke sesije,
- Modul za upravljanje korisničkim sesijama, namenjen za upravljanje aktivnim korisničkim sesijama i zahtevima izdatim u toku izvršavanja korisničkih sesija,
- Modul za donošenje autorizacionih odluka.

U sedmom poglavlju je izvršeno ispitivanje mogućnosti primene predloženog rešenja u Smart Grid okruženju. Prvo je definisan osnovni skup bezbednosnih podataka na kojima je bazirano eksperimentalno istraživanje. Zatim su opisani eksperimenti i prikazani dobijeni rezultati. Na kraju poglavlja, prikazana je analiza dobijenih rezultata i diskusija u smislu postavljenih hipoteza.

U osmom poglavlju predstavljeni su izvedeni zaključci doktorske disertacije, sa posebnim naglaskom na doprinose disertacije i prednosti predloženog rešenja u poređenju sa RBAC modelom. Takođe, prikazani su nedostaci i ograničenja razvijenog modela u Smart Grid okruženju, i naznačeni pravci daljeg istraživanja.

Na kraju disertacije je navedena korišćena literatura i prilozi.

2 Teorijske osnove i pregled literature

2.1 Osnovni pojmovi i principi informacione bezbednosti

Informaciona bezbednost (eng. *information security*, skr. *InfoSec*) se odnosi na očuvanje poverljivosti (eng. *confidentiality*), integriteta (eng. *integrity*) i raspoloživosti (eng. *availability*) informacionih sistema primenom bezbednosnih mehanizama koji treba da budu unapred određeni, primenjeni, nadgledani i poboljšavani. Ova tri kriterijuma informacione bezbednosti su poznati pod nazivom CIA (*Confidentiality-Integrity-Availability*) trijada [33][86][126]. Poverljivost se odnosi na zaštitu podataka od neovlašćenog pristupa, čitanja i otkrivanja. Integritet se odnosi na zaštitu podataka od neovlašćenih izmena ili brisanja kako bi se obezbedila konzistentnost informacija. Raspoloživost je mogućnost ovlašćenih korisnika da pravovremeno pristupaju sistemu i podacima, i odnosi se na zaštitu od neovlašćenog zadržavanja ili prekida koji mogu uzrokovati korumpiranost podataka ili nedostupnost sistema.

Pored gore navedene CIA trijade, neporecivost (eng. *non-repudiation*) i autentičnost (eng. *authenticity*) se takođe sve češće spominju kao važni aspekti informacione bezbednosti [33][114]. Neporecivost predstavlja nemogućnost pošiljaoca ili primaoca da negira transmisiju poruke. Autentičnost predstavlja mogućnost da svi učesnici u komunikaciji budu sigurni da sadržaj njihove komunikacije nije izmenjen (dokaz da poruka nije promenjena na putu od pošiljaoca do primaoca), kao i da poruka zaista potiče od onoga ko je poslao.

U cilju razumevanja krajnjeg cilja informacione bezbednosti, potrebno je definisati osnovne pojmove iz oblasti bezbednosti informacionih sistema i upravljanja bezbednosnim rizicima [33][92][112][126]:

- **Sistem** je uređeni poredak međusobno zavisnih komponenti povezanih zajedno prema nekom planu za postizanje određenog cilja.
- **Informacioni sistem** (eng. *information system*, skr. *IS*) je skup komponenti za prikupljanje, obradu, prenos i skladištenje informacija. Komponente, odnosno resursi (eng. *assets*) informacionog sistema su: hardver, softver, podaci, komunikaciona mreža, ljudski resursi i procedure.
- **Kritični resursi** (eng. *critical assets*) su fizički ili logički resursi IS odgovorni za izvršavanje kritičnih funkcija unutar sistema ili imaju direktan uticaj na njih. Iako su uglavnom kritični resursi krajnja meta napada na IS, neophodno je obezbediti zaštitu i nekritičnih resursa čijim kompromitovanjem je moguće ugroziti kritične resurse. Na primer, iskorišćavanje grešaka u softveru nije krajnji cilj napadača, ali predstavlja način da se kompromituju vredni podaci. Ljudski resursi su takođe česta meta napada. Socijalni inženjering je postupak manipulacije ljudskim resursima u cilju otkrivanja poverljivih informacija, pri čemu je krajnji cilj dobijanje pristupa IS ili realizacija kompleksnijih napada.

- **Pretnja** (eng. *threat*) je bilo koji događaj ili aktivnost koja može da kompromituje resurse informacionog sistem.
- **Ranjivost** (eng. *vulnerability*) ili slabost (eng. *weakness*) je propust ili greška u sistemu koja omogućuje uspešnu realizaciju pretnje. Slabosti mogu postojati u bilo kom delu sistema, npr. na mreži, u operativnom sistemu ili u funkcionalnosti aplikacije.
- **Napad** (eng. *attack*) predstavlja namernu ili slučajnu akciju kojom se realizuje pretnja, korišćenjem jedne ili više slabosti u sistemu.
- **Bezbednosni rizik** (eng. *security risk*) je mogućnost uspešne realizacije napada. Da bi organizacija mogla uspešno da upravlja bezbednosnim rizicima, neophodno je da razume faktore koji utiču na procenu bezbednosnog rizika u sistemu: 1) uticaj koji uspešno realizovana pretnja ima na sistem (eng. *risk impact*), 2) verovatnoća uspešne realizacije pretnje (eng. *risk likelihood*).
- **Bezbednosne protivmere** (eng. *countermeasure*) su mere zaštite u oblasti bezbednosnih tehnologija, politika i procedura koje imaju za cilj da eliminišu ili redukuju ranjivosti, pretnje i napade u sistemu. Bezbednosne mere mogu biti klasifikovane prema različitim kriterijumima. Prema cilju, bezbednosne mere mogu biti preventivne, detektivne i korektivne. Preventivne mere imaju za cilj da spreče napad, odnosno da smanje bezbednosne rizike u sistemu. Cilj detektivnih mera je prepoznavanje potencijalno malicioznih događaja pre nego što se napad dogodi ili nakon izvršenog napada. Korektivne mere su akcije koje se sprovode kako bi se umanjile posledice štetnih događaja (incidenata). Prema drugoj podeli, bezbednosne mere su dele u tri klase: tehničke, operativne i upravljačke. Tehničke (ili logičke) mere su hardversko-softverski mehanizmi zaštite. Operativne (ili fizičke) mere su mere zaštite kojima upravljaju ljudi i obuhvataju fizičku zaštitu sistema i okruženja, zaštitu osoblja, obuke i treninge, upravljanje incidentima, itd. Upravljačke (ili administrativne) du dokumentovane mere zaštite (procesi, procedure i prakse) koji se sprovode radi upravljanja rizicima i sistemom zaštite.

Osnovno načelo informacione bezbednosti je da IS nikada nije u potpunosti zaštićen, odnosno uvek postoji mogućnost iskorišćenja određenih slabosti u sistemu koje mogu da dovedu do gubitka poverljivosti, integriteta ili raspoloživosti informacionog sistema i/ili podataka. Cilj informacione bezbednosti je eliminacija ili smanjenje bezbednosnih rizika, kao i smanjenje posledica eventualnih incidenata primenom različitih bezbednosnih mera za prevenciju i detekciju napada, kao i reakciju na incidente [112][114]. U nastavku ove sekcije biće objašnjeni osnovni principi i koncepti u oblasti informacione bezbednosti, pre svega slojevita bezbednosna strategija, princip najmanjih privilegija i separacija obaveza.

2.1.1 Slojevita bezbednosna strategija

Slojevita bezbednosna strategija (engl. *defense in depth*) je neophodna, jer bez obzira na skup primenjenih bezbednosnih mera nikada nije moguće u potpunosti se zaštititi od

svih pretnji u sistemu. Zaštita kritičnih resursa ne bi trebala da se zasniva na jednom mehanizmu odbrane. Umesto toga, zaštita treba da se zasniva na više slojeva tako da u slučaju proboja jednog sloja, drugi slojevi mogu sprečiti napad [123].

Realizacija slojevite zaštite informacionih sistema i podataka pruža redundantnost bezbednosnih mehanizama tako da u slučaju da napadač uspe da iskoristi slabosti u jednom sloju ili zaobiđe bezbednosne kontrole u tom sloju, preostaju drugi komplementarni slojevi koji mogu sprečiti ili otežati napad [33][110][126]. Na primer, određeni mehanizam za kontrolu pristupa može biti implementiran kako bi se ograničio pristup poverljivim podacima neke organizacije. Kao dodatni nivo zaštite, poverljive podatke moguće je i šifrovati, tako da u slučaju da napadač uspe da zaobiđe mehanizam za kontrolu pristupa, on mora da dođe i do ključa za dešifrovanje podataka da bi kompromitovao poverljive podatke.

2.1.2 Princip najmanjih privilegija

Princip najmanjih privilegija (eng. *Principle of Least Privilege*) se odnosi na dodeljivanje minimalnog skupa privilegija neophodnih za izvršavanje samo onih zadataka za koje je svaki korisnik ovlašćen. Ovaj princip sprečava korisnika da izvršava nepotrebne operacije, čime se smanjuje mogućnost štete izazvane zloupotrebnom privilegija ili nenamernim greškama [28][33][111]. Dodatno, u nekim definicijama ovog principa se uvodi i vreme kao bitan faktor koji određuje kada će određene privilegije biti raspoložive korisniku. Naime, osim dodele privilegija u zavisnosti od zaduženja svakog korisnika, privilegije treba da budu raspoložive samo u vremenskom intervalu u kom se očekuje da određena operacija bude izvršavana [111]. Na primer, ukoliko se očekuje da korisnik može da pristupi sistemu samo u toku svog radnog vremena, tada skup dodeljenih privilegija treba da bude onemogućen van radnog vremena.

Osim za definisanje minimalnog skupa privilegija dodeljenih korisnicima, princip najmanjih privilegija je neophodno uvažavati i prilikom definisanja skupa privilegija za procese i aplikacije koji se izvršavaju u sistemu kako bi se smanjila mogućnost eskalacije privilegija. Na primer, ukoliko napadač uspe da iskoristi slabost u određenom delu aplikacije i umetne maliciozni kod sa ciljem da se pokreće kao deo aplikacije, to će za posledicu imati izvršavanje malicioznog koda sa ograničenim nivoom privilegija koji je definisan za kompromitovanu aplikaciju [91].

2.1.3 Separacija obaveza

Separacija obaveza (eng. *Separation of Duties*, skr. *SoD*) je princip kojim se zahteva da se izvršavanje kritičnih zadataka u okviru jednog poslovnog procesa raspodeli između dva ili više različitih korisnika, tako da pojedinačno nijedan korisnik ne može izvršiti kompletan poslovni proces. Sprečavanjem da isti korisnik kontroliše sve zadatke u okviru jednog poslovnog procesa smanjuje se mogućnost prevare, zloupotrebe ili slučajnih grešaka korisnika [28][33][106][111]. Na primeru procesa upravljanja planiranim

radovima unutar elektrodistributivne kompanije koje se sastoji od akcija pravljenja sekvence manipulacija prekidačkom opremom, odobravanja kreirane sekvence i izvršavanja, isti korisnik ne bi smeo da ima ovlašćenje da izvrši sve tri navedene akcije. Proces izgradnje elektroenergetske mreže se takođe sastoji iz nekoliko odvojenih akcija: kreiranje plana razvoja mreže, verifikacija predloženih izmena u testnom okruženju i odobravanje za primenu u produkcionom sistemu. Korisnik koji sastavlja planove ne bi smeo da ima ovlašćenje za njihovu primenu u produkciji.

Separacija obaveza može biti statička i dinamička. Statička separacija obaveza (eng. *Static Separation of Duties*, skr. *SSoD*) se odnosi na sprečavanje dodele konfliktnih privilegija prilikom administracije sistema. Dinamička separacija obaveza (eng. *Dynamic Separation of Duties*, skr. *DSoD*) podrazumeva primenu ograničenja u pogledu konfliktnih privilegija prilikom izvršavanja određenog poslovnog procesa u sistemu. Na primeru prethodno pomenutog procesa upravljanja planiranim radovima, moguće je definisati tri konfliktne privilegije, privilegija za pravljenje sekvence manipulacija prekidačkom opremom, privilegija za njeno odobravanje i privilegija za izvršavanje. Primena SSoD bi podrazumevala da nijedan korisnik koji ima pravo da izvrši sekvencu manipulacija ne sme imati pravo da ih pravi ili odobrava. S druge strane, primenom DSoD bi se dozvolilo da istom korisniku budu dodeljene konfliktne privilegije, uz izuzetak da ukoliko je korisnik kreirao određenu sekvencu, istu ne može da odobri ili izvrši. Prednost SSoD je jednostavnija implementacija, dok DSoD pruža veću fleksibilnost po cenu znatno težeg sprovođenja [28][80].

2.2 Kontrola pristupa

U najširem smislu, kontrola pristupa (eng. *access control*) definiše da li i na koji način korisnici mogu pristupiti resursima u sistemu, odnosno "*ko šta može da radi u sistemu*", npr. pristup određenoj fizičkoj lokaciji, fizičkim uređajima ili podacima. Sa aspekta informacione bezbednosti, kontrola pristupa predstavlja fundamentalni bezbednosni mehanizam za ograničavanje prava pristupa informacionim sistemima i podacima u cilju zaštite od neovlašćenog (neautorizovanog) pristupa, čitanja, modifikacije, brisanja, zadržavanja i snimanja. Kontrola pristupa se zasniva na sledećim bezbednosnim mehanizmima 1,2:

- identifikacija (eng. *identification*),
- autentifikacija, odnosno provera identiteta (eng. *authentication*),
- autorizacija (eng. *authorization*).

"*AAA*" (eng. *AAAs of security*) predstavlja akronim za tri osnovna bezbednosna mehanizma koji zajedno funkcionišu kako bi se obezbedio kontrolisan pristup informacionom sistemu i podacima (eng. *AAA = Authentication, Authorization,*

Accounting). U nastavku ove sekcije detaljno su objašnjeni pomenuti bezbednosni mehanizmi.

2.2.1 Identifikacija

U dostupnoj naučnoj i stručnoj literaturi se proces identifikacije vrlo često poistovećuje sa procesom autentifikacije ili se definiše kao sastavni deo procesa autentifikacije. Kako bi se objasnila razlika između procesa identifikacije i autentifikacije, prvo će biti definisani ključni aspekti digitalnog identiteta. Svaki entitet informacionog sistema (osoba, aplikacija ili hardverski uređaj kao što je računar, mobilni telefon ili mrežna oprema) može biti predstavljen digitalnim identitetom koji je jedinstven za taj sistem [56]. Digitalni identitet čine sledeće informacije [56]:

- Identifikator je informacija kojom je svaki entitet jedinstveno predstavljen u informacionom sistemu, npr. korisničko ime, jedinstevni matični broj građana (JMBG).
- Kredencijali (eng. *credentials*) su informacije kojima entitet potvrđuje da je vlasnik identiteta. Najčešće korišćeni tip kredencijala su šifre kojima se dokazuje validnost prethodno unetog korisničkog imena. U Smart Grid sistemima neretko se koriste digitalni sertifikati, ali i biometrijski podaci.
- Atributi su informacije koje definišu dodatni skup karakteristika o entitetu. To mogu biti personalni podaci o entitetu koji se mogu koristiti u slučaju potrebe za dodatnom validacijom (npr. prilikom pristupanja sa nepoznatog uređaja ili sa nepoznate lokacije), zatim podaci o ovlašćenjima entiteta u informacionom sistemu, itd.

Identifikacija je proces kojim se entitet koji zahteva pristup određenom resursu predstavlja informacionom sistemu korišćenjem jedinstvenog identifikatora. Procesom identifikacije se utvrđuje da li je identifikator prezentovan od strane entiteta poznat sistemu, ali se ne utvrđuje verodostojnost ove tvrdnje [33][126].

2.2.2 Autentifikacija

Autentifikacija, odnosno provera identiteta je proces validacije identiteta određenog entiteta u sistemu. Entiteti dokazuju svoj identitet na osnovu kredencijala [33][126]. Tipovi kredencijala, odnosno faktori autentifikacije, se mogu podeliti u tri kategorije u zavisnosti od načina na koji se identitet dokazuje:

- Faktor znanja koji se zasniva na nečemu što korisnik zna (eng. *something you know*) i podrazumeva posedovanje određene informacije koju samo vlasnik kredencijala treba da zna, poput lozinke (šifre) ili lični identifikacioni broj (eng. *Personal Identity Number*, skr. *PIN*). Ovaj metod je najčešće korišćeni tip autentifikacije zbog niske cene implementacije i jednostavnosti korišćenja, ali je najpodložniji napadima. Naime, da bi uspešno izvršio napad, napadač treba da otkrije informaciju koja se čuva u tajnosti. Iako savremeni sistemi za

upravljanje šiframa zahtevaju definisanje kompleksnih šifri koje je teško otkriti napadima uzastopnim pokušavanjem (eng. *brute force*), tehnike socijalnog inženjeringa predstavljaju ozbiljnu pretnju, jer koriste slabosti ljudskih resursa sa ciljem dobijanja pristupa tajnim informacijama. Jedna od najpoznatijih tehnika socijalnog inženjeringa je *phishing* napad u kojem se napadač predstavlja kao entitet od poverenja (npr. administrator IS, nadređeni) kako bi došao do lozinke ili PIN broja korisnika.

- Faktor posedovanja koji se zasniva na nečemu što korisnik ima (eng. *something you have*) i podrazumeva korišćenje autentifikacionog tokena koji korisnik treba da poseduje. To može biti pametna kartica, hardverski token (npr. RSA token), kreditna kartica, itd. Da bi uspešno izvršio napad, napadač treba fizički da dođe do tokena ili da ga falsifikuje.
- Faktor pripadnosti koji se zasniva na proveri biometrijskih podataka (eng. *something you are*), poput fizičkih karakteristika (npr. otisci prstiju, govor, analiza rukopisa) ili ponašanja karakterističnog za korisnika (npr. dinamika kucanja na tastaturi računara). Prednost ovog mehanizma autentifikacije je što je takve podatke teško ukrasti ili falsifikovati. Međutim, biometrijski uređaji za proveru validnosti ovakvih podataka su podložni greškama što utiče na tačnost i kvalitet autentifikacije.

Kako bi se otežali napadi vezani za autentifikaciju, a time smanjio i rizik od neovlašćenog pristupa sistemu često se primenjuje više od jednog faktora autentifikacije. To može biti kombinacija bilo koja dva faktora autentifikacije. Jedan primer takve dvofaktorske autentifikacije je korišćenje kreditne kartice na bankomatima. Da bi korisnik pristupio bankomatu neophodno je da poseduje kreditnu karticu (faktor posedovanja), a zatim da unese PIN kod (faktor znanja). *Google* takođe pruža mogućnost dvostruke autentifikacije prilikom pristupanja *Gmail* servisu kada se od korisnika zahteva šifra (faktor znanja) i pametni telefon (faktor posedovanja) na koji se šalje jednokratni verifikacioni kod kojim korisnik potvrđuje da poseduje pametni telefon. Umesto verifikacionog koda može se zahtevati otisak prsta (faktor pripadnosti), a moguće je kombinovati i sva tri faktora autentifikacije. Ovakav metod autentifikacije se naziva više-faktorska autentifikacija [33].

2.2.3 Autorizacija

Autorizacija, odnosno kontrola pristupa je proces dodele prava pristupa entitetima nad resursima informacionog sistema. U širem smislu, autorizacija se odnosi i na proces odlučivanja kojim resursima entitet može da pristupi i koje operacije može da izvršava nad resursima u sistemu [33][126]. Osnovni termini u oblasti kontrole pristupa su (informacioni) sistem, korisnik, subjekat, objekat, operacija i privilegija [106]. Korisnik je entitet (osoba, softver, računar, mrežna oprema) koji je u direktnoj interakciji sa sistemom. Sve korisnikove interakcije sa sistemom se odvijaju kroz određene procese (aplikacije). Subjekat predstavlja jednu instancu korisnikove interakcije sa sistemom. Korisnik istovremeno može imati više aktivnih subjekata sa različitim privilegijama.

Objekat je resurs u sistemu koji je potrebno zaštititi. Odnosi se kako na fizičke resurse (npr. uređaji) tako i logičke resurse (dokumenta, fajl sistem, baze podataka, aplikacije, konekcije, itd.). Operacija se odnosi na aktivni proces ili akciju koja se izvršava od strane subjekta, a privilegija se odnosi na dozvolu izvršavanja određene operacije nad objektom u sistemu [33][106].

Modeli kontrole pristupa se mogu podeliti u tri osnovne kategorije: diskrecioni model, mandatorni (nediskrecioni) model i model zasnovan na korisničkim ulogama [33][126]. Sa razvojem distribuiranih, heterogenih računarskih sistema uvodi se i četvrta kategorija modela kontrole pristupa zasnovanih na atributima [22][51].

Diskrecioni model kontrole pristupa

Diskrecioni model kontrole pristupa (eng. *Discretionary Access Control*, skr. *DAC*) je model u kojem je pristup objektima definisan na osnovu korisničkog identiteta i autorizacionih pravila kojima je za svakog korisnika ili korisničku grupu određen skup dozvoljenih operacija nad datim objektom (npr. čitanje, pisanje, brisanje, izvršavanje, itd.) [80][108]. Vlasnik objekta po sopstvenoj diskreciji definiše prava pristupa za objekat koji je u njegovom vlasništvu, a u većini DAC modela je vlasnik objekta upravo onaj ko je kreirao objekat. Zbog svoje fleksibilnosti, DAC model ima široku primenu u komercijalnim i industrijskim sistemima [33][108]. Tipičan mehanizam baziran na DAC modelu je lista kontrole pristupa (eng. *Access Control List*, skr. *ACL*) uz pomoć koje je realizovana kontrola pristupa na operativnim sistemima kao što su *Unix/Linux* i *Windows* [33][80][126]. Na primer, pristup objektima *Linux* fajl sistema se određuje na osnovu vlasničke kategorije (vlasnik, vlasnička grupa, ostali korisnici) i dodeljenog nivoa pristupa za svaku vlasničku kategoriju (čitanje, pisanje, izvršenje).

DAC model podrazumeva decentralizovanu administraciju, odnosno da vlasnici objekata definišu prava pristupa objektima. U komercijalnim sistemima se podrazumeva da svi resursi pripadaju kompaniji, a ne pojedinim korisnicima te ovakav pristup nije prihvatljiv [29][80]. Osnovni nedostatak DAC modela sa aspekta bezbednosti je to što je moguće jednostavno zaobići autorizaciona pravila. Naime, korisniku koji ima pravo da pristupi nekom objektu nije moguće nametnuti ograničenja u pogledu korišćenja tog objekta. Npr. DAC ne ograničava kopiranje podataka između objekata, te ukoliko korisnik ima pravo čitanja, on može da kopira podatke u drugi objekat čiji je on vlasnik i dodeli prava pristupa nad tim objektom proizvoljnim korisnicima. Na opisani način je moguće zaobići bezbednosnu politiku definisanu od strane vlasnika objekta i dodeliti prava pristupa korisnicima kojima je pristup izvornim podacima zabranjen [105][108].

Mandatorni model kontrole pristupa

Mandatorni model kontrole pristupa (eng. *Mandatory Access Control*, skr. *MAC*) je model gde je pristup baziran na klasifikaciji korisnika i objekata u sistemu od strane

sistemskog administratora, zbog čega se MAC model naziva i nediskrecioni model kontrole pristupa [80][126]. Za klasifikaciju korisnika i objekata se koriste unapred definisane bezbednosne labele. Bezbednosne labele dodeljene objektima definišu nivo osetljivosti informacija koje svaki objekat sadrži (npr. *top secret*, *secret*, *confidential*, *unclassified*), a bezbednosne labele dodeljene korisnicima predstavljaju nivo poverenja za pristup objektima. Da bi korisnik mogao da pristupi određenom objektu, on mora da ima dodeljen nivo poverenja koji je jednak ili viši od nivoa definisanog za objekat kome pristupa.

U poređenju sa DAC modelom, MAC obezbeđuje potpunu kontrolu pristupa osetljivim podacima, odnosno definisanje prava pristupa je centralizovano i samo vlasnik (administrator) sistema ima ovlašćenje da ih menja. Ostali korisnici ne mogu zaobići ili izmeniti uspostavljenu bezbednosnu politiku [105][108]. Stoga, MAC ima široku primenu u sistemima u kojima se obrađuju vrlo osetljivi podaci, kao što su sistemi vladinih organizacija i upravljački sistemi u vojnoj industriji (kao što su raketni sistemi, radarski sistemi, sistemi za obaveštavanje i navođenje) [105][108]. Tipičan primer upotrebe MAC modela je *Security Enanced Linux* (skr. *SELinux*) koji je usklađen sa specifikacijama agencije NSA (eng. *National Security Agency*).

Međutim, MAC model je zasnovan na klasifikaciji objekata i korisnika u sistemu, i kao takav nije primenljiv u industrijskim sistemima koji najčešće sadrže osetljive, ali neklasifikovane podatke. Dodatno, kompleksnost implementacije i administracije MAC modela nije prihvatljiva sa aspekta komercijalnih aplikacija [29][80].

Model kontrole pristupa zasnovan na korisničkim ulogama

Model kontrole pristupa zasnovan na korisničkim ulogama (eng. *Role-Based Access Control*, skr. *RBAC*) je model u kojem je pristup baziran na ulozi korisnika, odnosno obavezama i odgovornostima grupa ili tipova korisnika unutar organizacije. Korisnička uloga predstavlja skup funkcija koje mogu biti izvršene od strane jednog korisnika u sistemu. Svaka uloga je definisana kao skup privilegija koje označavaju dozvoljene operacije nad (određenim) objektima u sistemu, a privilegije se korisnicima dodeljuju posredstvom korisničkih uloga [29][33][80]. RBAC je nastao kao alternativa DAC i MAC modelima sa ciljem da se odgovori zahtevima različitih organizacija kako u državnom tako i u privatnom sektoru [27]. S obzirom na jednostavnost upravljanja bezbednosnim politikama, kao i smanjenja kompleksnosti i troškova administracije, RBAC je jedan od najzastupljenijih modela za kontrolu pristupa u modernim informacionim sistemima [80]. U *Sekciji 2.3* je dat detaljan pregled modela kontrole pristupa zasnovanog na korisničkim ulogama.

Model kontrole pristupa zasnovan na atributima

Model kontrole pristupa zasnovan na atributima (eng. *Attribute-based access control*, skr. *ABAC*) je model u kome je odluka o pristupu resursima bazirana na vrednostima atributa korisnika, objekata i okruženja koji se mogu dinamički menjati. Atribut je funkcija koja za određeni entitet vraća specifičnu vrednost iz unapred definisanog opsega vrednosti. Entiteti mogu biti korisnici, objekti ili uslovi okruženja, a odluka o pristupu resursima se donosi poređenjem vrednosti atributa sa vrednostima atributa definisanim u autorizacionim politikama [51][83].

U poređenju sa RBAC modelom, najvažnija prednost ABAC modela je mogućnost uvažavanja širokog spektra parametara okruženja, fleksibilnost u pogledu dodavanja novih autorizacionih pravila u skladu sa dinamičnih zahtevima u sistemu, kao i to što skup korisnika i njihovih atributa ne mora biti unapred poznat. Kompleksnost ABAC modela u slučaju velikog broja atributa koje treba uvažiti prilikom donošenja odluke o pristupu, kao i otežano praćenje privilegija korisnika su cena za fleksibilnost koju ABAC pruža [63].

2.2.4 Snimanje i analiza bezbednosnih događaja

Termin *accounting* se odnosi na proces kojim se obezbeđuje praćenje, snimanje, analiza i izveštavanje o relevantnim bezbednosnim događajima u sistemu. Osnovni mehanizam za praćenje i snimanje bezbednosnih događaja je audit log [33]. Bezbednosni događaji mogu biti kako uspešno izvršene akcije u sistemu, tako i neuspešni pokušaji pristupa resursima. Definisani bezbednosni događaji se zapisuju u različitim formatima u datotekama namenjenim za zapis događaja operativnog sistema, različitih aplikacija, mrežne opreme, i slično. Npr. *Microsoft Windows* operativni sistem podržava različite tipove log datoteka (bezbednosni, sistemski i aplikativni log), kao i *Windows Event Viewer* alat za njihov prikaz. Zapisi bezbednosno relevantnih događaja u audit logovima treba da pruže sve informacije o događajima, npr. akcije koje su izvršene, korisnik koji je izvršio akciju, rezultat i vreme izvršavanja akcije, dodatne informacije bitne za pojedinačne događaje. S obzirom da audit log predstavlja vremenski obeležene zapise o aktivnostima u sistemu, učesnici ne mogu naknadno poricati izvršene akcije čime se obezbeđuje neporecivost. Integritet, odnosno tačnost podataka koje sadrže audit logovi se obezbeđuje primenom mehanizama kontrole pristupa logovima, digitalnim potpisima, itd. Analizom prikupljenih informacija moguće je detektovati kako uspešne tako i neuspešne pokušaje kako redovnih tako i malicioznih aktivnosti u sistemu, odnosno naknadno utvrditi uzroke grešaka ili otkaza u sistemu [33][126].

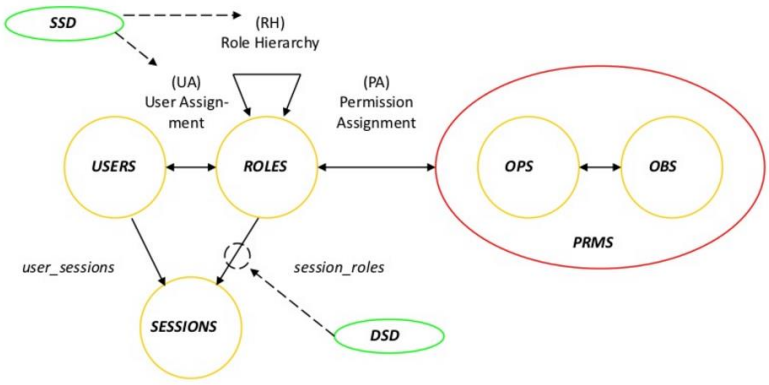
2.3 Model kontrole pristupa zasnovan na korisničkim ulogama - RBAC model

Studijom koju je NIST sproveo 1992. godine [27] ustanovljeno je da mehanizmi za kontrolu pristupa zasnovani na mandatornim i diskrecionim modelima ne mogu da odgovore zahtevima različitih organizacija kako u državnom tako i u privatnom sektoru. Decentralizovana administracija DAC modela nije prihvatljiva u komercijalnim sistemima gde se podrazumeva da svi resursi pripadaju kompaniji, a ne pojedinim korisnicima. S druge strane, kompleksnost implementacije i administracije MAC modela nije prihvatljiva u distribuiranim sistemima sa velikim brojem korisnika i objekata. Stoga, autori rada [28] predlažu RBAC model koji se zasniva na dodeli prava pristupa korisnicima na osnovu njihovih uloga i odgovornosti u sistemu, kao i centralizovanoj administraciji bezbednosnih politika unutar organizacije. Dalji pravci istraživanja RBAC modela su vodili ka njegovoj formalizaciji i standardizaciji sa ciljem da se na sistematičan način definiše skup RBAC funkcionalnosti [106][107]. Referentni RBAC model, definisan NIST standardom, se sastoji iz četiri komponente [29][30]:

- osnovni RBAC model (eng. *Core RBAC*),
- hijerarhija uloga (eng. *Hierarchical RBAC*),
- statičko razdvajanje obaveza (eng. *Static Separation of Duty*, skr. *SSD*),
- dinamičko razdvajanje obaveza (eng. *Dynamic Separation of Duty*, skr. *DSD*).

Na *Slici 1.* je dat šematski prikaz četiri standardne komponente NIST RBAC modela. 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 oranizacije. Statičkim i dinamičkim razdvajanjem obaveza uvodi se pojam ograničenja u RBAC modelu sa ciljem da se omogući ograničavanje dodele konfliktnih uloga korisnicima. Podela na statičko i dinamičko razdvajanje obaveza vrši se na osnovu toga kada se ograničenja primenjuju na uloge. SSD ograničenja se primenjuju u toku administracije modela, dok se DSD ograničenja primenjuju prilikom uspostavljanja korisničke sesije.

U nastavku je dat detaljan opis četiri standardne komponente RBAC modela, tj. objašnjenje koncepata prikazanih na *Slici 1.*



Slika 1. Komponente NIST RBAC modela

2.3.1 Osnovni RBAC model

Osnovni RBAC model čine sledećih pet osnovnih entiteta: korisnici, objekti, operacije, privilegije i uloge. Korisnici (eng. *USERS*) su entiteti (osobe, aplikacije, računari, mrežna oprema) koji su u direktnoj interakciji sa sistemom. Objekti (eng. *OBJECTS*, skr. *OBS*) su resursi u sistemu koje je potrebno zaštititi. Mogu biti fizički (npr. hardverski uređaji) ili informacioni (dokument, fajl sistem, baze podataka, aplikacije, konekcije, itd). Operacije (eng. *OPERATIONS*, skr. *OPS*) su aktivni procesi ili akcije koje se izvršavaju od strane korisnika u sistemu. Privilegije (eng. *PERMISSIONS*, skr. *PRMS*) predstavljaju dozvolu za izvršavanje određene operacije nad objektom u sistemu. Korisničke uloge (eng. *ROLES*) predstavljaju funkcije ili odgovornosti korisnika unutar organizacije. Korisničke uloge se dodeljuju korisnicima na osnovu njihovih obaveza i zaduženja unutar organizacije.

Svakom korisniku može biti dodeljena jedna ili više korisničkih uloga, dok svaka uloga može biti dodeljena jednom ili više korisnika. Ova relacija je označena kao UA (eng. *User Assignment*). Svaka korisnička uloga je definisana kao skup privilegija koje označavaju operacije nad objektima. Korisnicima se privilegije nikada ne dodeljuju direktno, već isključivo posredstvom dodeljenih uloga čime se postiže efikasnije definisanje prava pristupa i administracija sistema. Naime, na ovaj način moguće je jednostavno izmeniti privilegije pridružene određenoj ulozi, umesto izmene privilegija za svakog korisnika posebno. Relacije između korisničkih uloga i privilegija su označene kao PA (eng. *Permission Assigment*) [30][106].

Prethodno navedeni entiteti i relacije čine statičku komponentu osnovnog RBAC modela. Dodatno, osnovni RBAC može da sadrži i dinamičku komponentu u okviru koje se uvodi koncept subjekta i aktivacije uloga [29]. Dinamičku komponentu osnovnog RBAC modela čini entitet korisničke sesije (eng. *SESSIONS*) koja predstavlja jednu instancu korisnikove interakcije sa sistemom. Svaka sesija pripada tačno jednom korisniku, dok isti korisnik može imati više aktivnih sesija sa različitim privilegijama u zavisnosti od aktiviranog podskupa uloga koje su dodeljene korisniku. Skup sesija jednog

korisnika je označen kao US (eng. *User Sessions*), dok je skup aktiviranih uloga u okviru jedne sesije označen kao SR (eng. *Session Roles*). Skup raspoloživih privilegija (eng. *available session permissions*) se odnosi na skup privilegija dodeljenih aktiviranim ulogama u okviru date korisničke sesije [30][106].

2.3.2 Hijerarhija uloga

Hijerarhija uloga (eng. *Role Hierarchy*, skr. *RH*) je koncept kojim se pojednostavljuje administracija modela u slučaju preklapanja korisničkih uloga u pogledu zaduženja, odnosno u pogledu dodeljenih privilegija [29][30]. Na primer, unutar organizacije postoji skup funkcija koje su zajedničke za sve korisnike bez obzira na njihovu ulogu u sistemu, kao što je pregled stanja elektroenergetske mreže, pristup sistemu preko Web servera, i slično. Umesto da se skup privilegija za ove zajedničke funkcije definiše za svaku korisničku ulogu pojedinačno, može se definisati uopštena uloga koja sadrži privilegije za ove zajedničke funkcije koju nasleđuju ostale uloge u sistemu [29].

Hijerarhija uloga se opisuje relacijama nasleđivanja između dve korisničke uloge na sledeći način [29][30]:

- Korisnička uloga r_1 nasleđuje korisničku ulogu r_2 ukoliko r_1 sadrži sve privilegije koje sadrži r_2. Odnosno, privilegije korisničke uloge r_2 su podskup skupa privilegija od r_1.
- Korisnička uloga r_1 nasleđuje korisničku ulogu r_2 ukoliko su svi korisnici ovlašćeni za r_1 ovlašćeni i za r_2.

2.3.3 Statičko razdvajanje obaveza

Statičko razdvajanje obaveza, odnosno model statičkih ograničenja pruža mogućnost ograničavanja dodele konfliktnih uloga korisnicima u toku administracije modela. Relacije statičkih ograničenja (SSD relacije) se primenjuju nad UA relacijama. Ukoliko je korisnik član određene uloge, SSD relacijama je moguće zabraniti da taj korisnik bude član jedne ili više konfliktnih uloga u zavisnosti od definisanih SSD pravila. Primer primene statičkih ograničenja je zahtev da isti korisnik ne može biti član dve uloge koje su međusobno isključive [29][30].

Statička ograničenja se mogu primeniti i u slučaju hijerarhije uloga. SSD relacije se primenjuju na isti način kao i za osnovni RBAC model, s tim što se u ovom slučaju moraju uzeti u obzir ne samo direktno dodeljene uloge već i nasleđene uloge [29][30].

2.3.4 Dinamičko razdvajanje obaveza

Dinamičko razdvajanje obaveza, odnosno dinamički model ograničenja pruža mogućnost ograničavanja konfliktnih uloga prilikom uspostavljanja korisničke sesije. Relacije dinamičkih ograničenja (DSD relacije) se primenjuju nad SR relacijama. Za razliku

od SSD relacija koje sprečavaju dodelu konfliktnih uloga korisnicima prilikom admnistracije modela, DSD relacije ograničavaju samo njihovu istovremenu aktivaciju u korisničkim sesijama. Kod DSD relacija korisnik može biti član konfliktnih uloga, a ograničenja se razmatraju prilikom uspostavljanja korisničke sesije. Odnosno, slično kao i SSD, DSD relacije ograničavaju skup raspoloživih privilegija u korisničkoj sesiji, ali se razlikuje kontekst u kome se ograničenja primenjuju [29][30].

2.4 Modeli kontrole pristupa bazirani na RBAC modelu

Iako RBAC model sistematično širi spektar mogućnosti kroz četiri standardne komponente, sve one se zasnivaju na istoj strukturi gde pristup zavisi od identiteta korisnika [106]. U heterogenim, distribuiranim računarskim sistemima sve češće se javlja potreba da drugi faktori osim korisničkog identiteta utiču na odluke o pristupu resursima (npr. vreme pristupa sistemu, lokacija sa koje se pristupa sistemu, itd.). Međutim, bez dodatnih unapređenja RBAC model ne može da zadovolji takve zahteve.

U nastavku ove sekcije su prikazani RBAC bazirani modeli kontrole pristupa koji predstavljaju proširenje RBAC modela kako bi se uvažili različiti parametri okruženja i obezbedila efikasnija kontrola pristupa.

2.4.1 Temporalni RBAC modeli

U organizacijama gde poslovni procesi ili funkcije treba ili mogu da budu izvršeni u određenom vremenskom intervalu, vremenska dimenzija predstavlja značajan parametar za kontrolu pristupa. Na primer, kompanije često zahtevaju da zaposlenima bude dozvoljen pristup sistemu samo u toku radnog vremena, bez obzira na ulogu i ovlašćenja koja su dodeljena svakom korisniku. Proces deregulacije u elektroprivredi uslovio je razdvajanje energetskih delatnosti, uključujući i zakonski regulisana pravila za obavljanje energetskih delatnosti. Regulatorno telo izdaje licencu kojom se utvrđuje ispunjenost uslova za obavljanje određenih poslova, kao i period važenja licence, npr. licenca za upravljanje prenosnom mrežom, licenca za upravljanje distributivnom mrežom, licenca za obavljanje radova na terenu, itd. [57]. Stoga, važeća licenca može da bude uslov da bi korisnik mogao da obavlja određene zadatke unutar organizacije. Nakon što istekne period važenja licence, dodeljena ovlašćenja treba da budu onemogućena.

Kako bi se uvažila vremenska dimenzija prilikom donošenja odluke o dozvoli ili zabrani pristupa, u radu [11] autori predlažu *Temporal RBAC* (skr. *TRBAC*) model koji je primenljiv u organizacijama gde korisničke uloge treba da budu omogućene samo u određenom vremenskom intervalu. Tipičan zahtev ovog tipa je da organizacije gde zaposleni mogu raditi skraćeno radno vreme (npr. od 9-13h) zahtevaju da takvim korisnicima pristup sistemu bude omogućen samo u navedenom vremenskom intervalu. Stoga, TRBAC uvodi mogućnost periodičnog omogućavanja i onemogućavanja uloga, kao

i uspostavljanje zavisnosti između tih akcija izraženo preko trigera uloga (eng. *role triggers*). Uloge koje korisnik može da aktivira u toku sesije su omogućene, a koje ne može da aktivira su onemogućene. Trigeri uloga su aktivna pravila kojima se definišu vremenska ograničenja i u zavisnosti od kojih će korisničke uloge automatski biti omogućene ili onemogućene u aktivnim korisničkim sesijama. Dodatno, akcije omogućavanja i onemogućavanja uloga mogu imati definisane prioritete kako bi se izbegle konfliktne akcije. Da bi administrator mogao da reaguje u vanrednim situacijama, omogućena je dinamička promena statusa uloge, kao i skup korisnika kojima je dozvoljeno da aktiviraju određene uloge. Ovakve dinamičke promene su omogućene izdavanjem *run-time* zahteva.

U daljem istraživanju je uočeno da TRBAC ima nekoliko ograničenja. Pre svega, TRBAC podrazumeva da samo uloge mogu biti omogućene i onemogućene u različitim vremenskim intervalima, dok ograničenja nad relacijama između korisnika i uloga, kao i uloga i privilegija nisu razmatrana. Takođe, nije jasno definisana razlika između omogućavanja i aktivacije uloga što za posledicu ima da ograničenja koja se odnose na maksimalno vreme aktivacije uloga ili maksimalan broj aktivacija uloge od strane jednog korisnika u okviru određenog vremenskog intervala ne mogu biti definisana. Da bi prevazišli navedena ograničenja, u radovima [54][55] autori uvode *Generalized Temporal RBAC* (skr. *GTRBAC*) model koji proširuje TRBAC funkcionalnostima potrebnim za prevazilaženje navedenih problema.

2.4.2 Prostorni RBAC modeli

U okruženjima gde je pristup sistemu omogućen sa udaljenih lokacija putem mobilnih uređaja, prostorna dimenzija predstavlja bitan faktor za kontrolu pristupa. Na primeru zdravstvenog informacionog sistemima u kome se čuvaju i obrađuju zdravstveni podaci pacijenata, doktor ima ovlašćenja da pristupi elektronskim zdravstvenim kartonima svojih pacijenata (eng. *electronic patient record*, skr. *EPR*). S obzirom na osetljivost podataka koje EPR sadrži, doktorima treba da bude omogućen pristup samo kada se nalaze u određenoj oblasti. Ukoliko doktor pokuša da pristupi EPR podacima sa manje pouzdane lokacije (van teritorije bolnice, iz restorana, itd.), zahtev treba da bude odbijen bez obzira na ovlašćenja [37].

U članku [36] autori predlažu *Spatial RBAC* (skr. *SRBAC*) model koji prilikom definisanja skupa privilegija razmatra lokaciju korisnika. Odnosno, SRBAC omogućuje ograničavanje skupa privilegija aktivnih korisničkih uloga u zavisnosti od prostornih informacija o svakom korisniku. U člancima [12][21] autori opisuju GEO-RBAC model koji omogućuje rad sa prostornim i lokacijski-baziranim informacijama, oslanjajući se na *Open GeoSpatial Consortium* (skr. *OGC*) model [90] za predstavljanje prostornih objekata, pozicija korisnika i geografski ograničenih uloga. Druga bitna karakteristika ovog modela je da podržava rad kako sa fizičkim tako i sa logičkim lokacijama, čime je omogućeno predstavljanje pozicije nezavisno od realnih pozicija u prostoru. Prostorno rastojanje uloge (eng. *role extent*) definiše prostornu granicu uloge u sistemu, odnosno lokaciju u

okviru koje korisnik mora da se nalazi da bi mu dodeljena uloga bila omogućena prilikom uspostavljanja korisničke sesije. Uloge je moguće dodeliti korisnicima samo kada su logički pozicionirani unutar prostornog rastojanja uloge.

S obzirom na dinamičku prirodu korisnika koji sistemu pristupaju putem mobilnih uređaja, dalji razvoj GEO-RBAC modela je usmeren na problem kontrole pristupa dok korisnik menja lokaciju u sistemu. U radu [59] autori predlažu proširenje GEO-RBAC modela opisanog u članku [21] elementima modela korišćenja (eng. *usage control*, skr. *UCON*) kako bi se obezbedila kontinualna provera prava pristupa što znači da se provera prava ne sprovodi samo prilikom pristupa sistemu već da se prava kontinualno proveravaju. Konkretno, razmatran je $UCON_{ABC}$ model korišćenja [94] koji se zasniva na ovlašćenjima (eng. *Authorizations*), obligacijama (eng. *oBligations*) i uslovima (eng. *Conditions*) koje je potrebno izračunati prilikom donošenja odluke o pristupu. U istom radu autori kao poseban izazov prostorno-orijentisanih modela kontrole pristupa ističu autentičnost i integritet informacija o lokaciji korisnika i predlažu primenu *Near-Field Communication* (skr. *NFC*) tehnologije [70].

2.4.3 Prostorno-temporalni RBAC modeli

U radovima [64][99] autori predlažu *Spatio-Temporal RBAC* (skr. *STRBAC*) model kojim proširuju RBAC model i prostornim i vremenskim ograničenjima, pružajući mogućnost aktivacije uloga i privilegija u zavisnosti od različitih parametara okruženja istovremeno. Dodatno, u [64] autori razlikuju četiri tipa logičkih lokacija:

- Lokacija prema adresi (eng. *location-by-address*) - lokacija definisana prema fizičkoj poziciji.
- Lokacija prema nameni (eng. *location-by-use*) - lokacija definisana prema određenoj funkciji, npr. skup prostorija koje predstavljaju lokaciju laboratorija, a neki drug skup prostorija predstavlja lokaciju sala za sastanke.
- Lokacija prema organizaciji (eng. *location-by-organization*) – lokacija definisana prema organizacijama u čijem su vlasništvu,
- Lokacija definisana od strane korisnika (eng. *user-defined location*) – čime se obezbeđuje podela prema specifičnim kategorijama koje nisu obuhvaćene ovom podelom. Ova kategorija pruža mogućnost finije granulacije u pogledu grupisanja lokacija, npr. granularnija podela laboratorija prema vrsti istraživanja.

Uzimajući u obzir da podatak o lokaciji može biti poverljiva informacija, lokacijski model je proširen dodatnim atributom koji definiše vidljivost lokacije (eng. *location visibility*).

U [100] autori se bave primenom STRBAC modela u rasplinutim (eng. *pervasive*) računarskim sistemima koje karakteriše visok stepen dinamičnosti i nepredvidivosti. Uvođenjem koncepta delegacije u vanrednim situacijama kada je korisnik nedostupan i

ne može da izvrši zadatke omogućena je privremena dodela privilegija drugim korisnicima ili ulogama. U [122] autori se bave metodologijom za verifikaciju modela kontrole pristupa u kompleksnim sistemima. U ovom članku je prikazana automatizacija procesa verifikacije STRBAC modela formalizovanog preko UML (eng. *Unified Modeling Language*) i OCL (eng. *Object Constraint Language*) jezika. UML/OCL model se automatski prevodi u logičke iskaze koji se zatim verifikuju pomoću alata za proveru zadovoljivosti iskaznih formula, tzv. SAT rešavači (eng. *Satisfiability (SAT) solvers*). Konkretno, autori predlažu prevođenje u *Alloy* jezik baziran na logici prvog reda, a zatim automatsku validaciju primenom *Alloy Analyzer* alata sa namenskim SAT rešavačem.

2.4.4 Kontekstno-zavisni RBAC modeli

Kontekstno-zavisni RBAC modeli kontrole pristupa proširuju RBAC model sa kontekstnim informacijama, čime se omogućuje da stanje okruženja utiče na mehanizam sprovođenja kontrole pristupa. Pod kontekstno-zavisnim RBAC modelima mogu se podrazumevati i modeli opisani u prethodnim sekcijama (temporalni i prostorni modeli), jer koriste određene parametre okruženja prilikom sprovođenja kontrole pristupa. Međutim, u oblasti kontekstno-zavisne bezbednosti pojam konteksta obuhvata bilo koju informaciju koja se može koristiti za karakterizovanje situacije (stanja) entiteta. Entitet je osoba, mesto ili objekat koji se smatraju relevantnim za interakciju korisnika i aplikacije, uključujući samog korisnika i aplikaciju [2]. U radu [76] je bezbednosni kontekst definisan kao skup informacija sakupljenih iz okruženja korisnika i aplikacije, koji su relevantni sa stanovišta bezbednosne arhitekture za korisnika i/ili aplikaciju.

U [35][115] autori predlažu model kontekstno-zavisne kontrole pristupa (eng. *COntext-sensitive Business processes Access Control model*, skr. *COBAC*) u sistemima za upravljanje poslovnim procesima, gde odluke o kontroli pristupa mogu da zavise od značajnog broja različitih faktora koji se razlikuju od procesa do procesa. COBAC je zasnovan na RBAC modelu koji je proširen entitetima poslovnog procesa, aktivnostima, kontekstom i kategorijom resursa. Uvođenjem entiteta poslovnog procesa i aktivnosti omogućeno je efikasnije definisanje i sprovođenje kontrole pristupa za poslovne procese, jer odgovarajući aspekti kontrole pristupa moraju biti definisani za konkretan poslovni proces. S obzirom da je moguće da na kontrolu pristupa utiču faktori okruženja, pa i faktori koji čine sam sistem, ali ne eksplicitno i model kontrole pristupa, COBAC je proširen entitetom konteksta. Kategorizacija resursa omogućuje definisanje prava pristupa za čitavu kategoriju resursa i time potencijalno smanjuje broj prava pristupa koje je potrebo definisati.

2.4.5 Distribuirani RBAC modeli

Razvoj informacionih tehnologija i pojava Interneta doneli su suštinske promene u načinu poslovanja i složenosti informacione infrastrukture, a time i sprovođenju procesa kontrole pristupa. Različite organizacije sve češće formiraju interorganizacione sisteme radi postizanja različitih ciljeva što podrazumeva i pristup resursima i razmenu

informacija sa partnerskim organizacijama. RBAC model je namenjen pre svega za kontrolu pristupa unutar jedne organizacije koja je odgovorna za administraciju svih korisnika i resursa. Ova karakteristika ga čini teško primenljivim u distribuiranim okruženjima [22].

U članku [127] autori predlažu proširenje RBAC modela za Web bazirana okruženja. Za razliku od tradicionalnog RBAC modela gde su objekti pasivni entiteti, u predloženom modelu objekti su i aktivni i pasivni entiteti. Aktivni entiteti su servisi, a pasivni entiteti su parametri i povratne vrednosti servisa (tj. atributi servisa). Autori razlikuju kontrolu pristupa namenjenu za lokalni Web servis (eng. *Single Web Service (SWS) – RBAC*) i kompozitne Web servise (eng. *Composite Web Service - RBAC*). Kompozitni (globalni) servisi su Web servisi koji u toku izvršavanja pristupaju i servisima drugih provajdera. SWS-RBAC model omogućuje kontrolu pristupa na dva nivoa: na nivou servisa i na nivou atributa, dok CWS-RBAC model proširuje SWS-RBAC konceptom globalnih uloga. Za pristup lokalnom servisu koriste se lokalne uloge, a za pristup globalnim servisima globalne uloge, pri čemu CWS-RBAC omogućuje mapiranje globalnih uloga na lokalne uloge drugih servis provajdera.

U radu [101] je dat jedan predlog implementacije RBAC modela u Web okruženju koristeći kolačiće (eng. *cookies*). S obzirom da korišćenje kolačića u formatu tekstualne datoteke predstavlja značajan bezbednosni rizik, u [101] se uvodi koncept bezbednosnih kolačića (eng. *secure cookies*) koji obezbeđuju autentifikaciju, poverljivost i integritet. Bezbednosni kolačić sa ulogama (eng. *Role Cookie*) je bezbednosni kolačić koji sadrži informacije o relacijama između korisnika i korisničkih uloga na osnovu kojih Web server proverava koje akcije korisnik može da izvršava.

U interorganizacionim sistemima se često posredstvom Web servisa korisnicima iz jedne organizacije omogućuje pristup partnerskim organizacijama. U radu [7] se predlaže *GenericWA-RBAC* model za kontrolu pristupa u sistemima gde se Web servisi koriste za razmenu informacija između različitih organizacija. Predloženi model predstavlja proširenje NIST RBAC modela komponentom organizacije (*ORGN*) čime se omogućuje mapiranje uloga dodeljenih korisniku unutar sopstvene organizacije na uloge u drugim organizacijama.

U članku [67] je prikazano proširenje RBAC modela za potrebe sistema za integraciju podataka iz različitih izvora (eng. *data integration service*). Konkretno, za potrebe sistema za integraciju i analizu zdravstvenih podataka (eng. *Health Data Integration*) gde postoji potreba za kontrolom pristupa podacima u zavisnosti od tipa istraživanja (tzv. projekta), osnovni RBAC model je proširen tako da je korisniku moguće dodeliti različite uloge u zavisnosti od specificiranog projekta. U radu [23] se autori bave problemom integracije podataka iz sistema koji mogu pripadati potpuno različitim sektorima (npr. sistemi vojnih, finansijskih, zdravstvenih i privatnih institucija), uz mogućnost pristupa podacima i od strane eksternih korisnika i aplikacija. Autori navode da su osnovni zahtevi u heterogenim sistemima sa aspekta kontrole pristupa transparetnost, autonomnost i

bezbednost. Predloženo rešenje čine dve komponente: komponenta koja pruža jedinstven interfejs za podatke iz različitih izvora, kao i mapiranje bezbednosnih pravila između različitih sistema (eng. *wrapper*), i komponenta koja obrađuje globalne zahteve za pristup podacima (eng. *mediator*).

U članku [69] se razmatra problem kontrole pristupa u distribuiranim sistemima koji funkcionišu po principu pretplate (eng. *subscription-based remote network services*). Razmatrani su sistemi koje karakteriše to da jedna organizacija pruža usluge (tzv. servis provajder), a druge organizacije se pretplaćuju na jedan ili više servisa. Distribuirani RBAC model (skr. DRBAC) predložen u ovom radu proširuje RBAC konceptom distribuirane uloge. Organizacija koja ima ulogu pružaoca usluga definiše skup distribuiranih uloga, koje se zatim mapiraju na lokalne uloge svake pretplaćene organizacije. Svaka organizacija kontroliše relacije između korisnika i korisničkih uloga, dok je za relacije između privilegija i uloga odgovorna organizacija koja pruža usluge. Prednost predloženog DRBAC modela je i delegirana autentifikacija kojom se smanjuje kompleksnost u pogledu administracije korisnika iz drugih organizacija od strane servis provajdera, jer proces verifikacije korisničkih identiteta ostaje u nadležnosti svake organizacije.

Model za kontrolu pristupa u koalicionim okruženjima (eng. *coalition-based access control*, skr. *CBAC*) je opisan u članku [19], pri čemu koalicija podrazumeva udruživanje organizacija u cilju postizanja određenog cilja. Takođe je uveden model domena u koalicionom okruženju, opisan sa tri aspekta: nivo koalicije, nivo organizacije i operativni nivo.

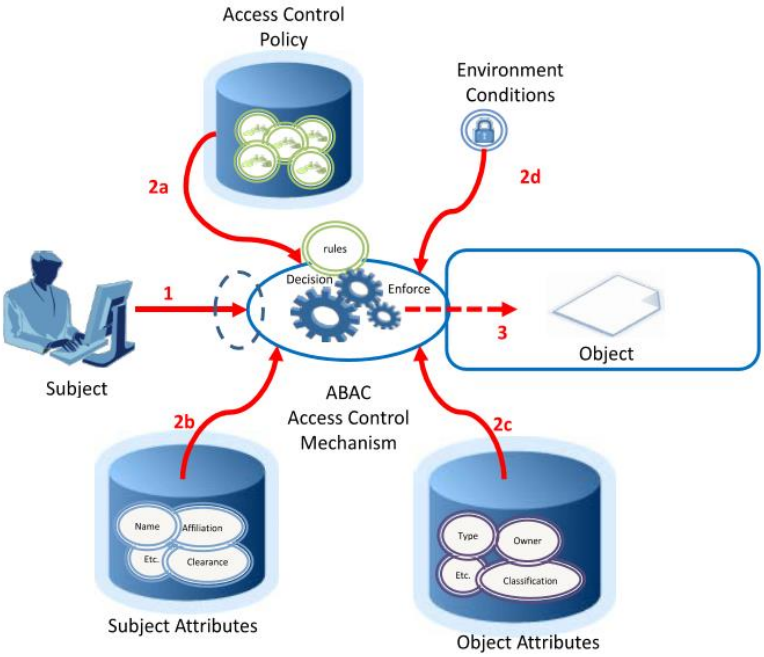
U radu [95] je prikazana primena *Generalized Temporal RBAC* (skr. *GTRBAC*) modela u labavo spregnutim multidomenskim okruženjima koje karakteriše potpuna nezavisnost domena koji učestvuju u višedomenskim uslugama, a nezavisni domeni se dinamički dogovaraju po pitanju deljenja informacija i resursa na određeni period. Predloženi model omogućuje primenu originalnih autorizacionih politika za lokalne korisnike, dok je za pristup resursima od strane korisnika iz drugih domena potrebno proširiti lokalne politike uvođenjem eksternih uloga. Primer praktične primene ovog modela kontrole pristupa je *Microsoft* servis federacije aktivnog direktorijuma (eng. *Active Directory Federation Services, skr. AD FS*) koji omogućuje deljenje informacija o identitetu korisnika između partnerskih organizacija od poverenja. AD FS omogućuje da partnerske organizacije dele servise za upravljanje identitetima tako što svaka organizacija upravlja sopstvenim identitetima i korisničkim nalozima, uz mogućnost prihvatanja identiteta iz drugih organizacija bez potrebe da se kreira više odvojenih identiteta za istog korisnika [3].

2.5 Model kontrole pristupa zasnovan na atributima – ABAC model

Umesto stalnog proširivanja RBAC modela kako bi se uvažili različiti faktori okruženja koji utiču na autorizacione odluke, u člancima [22][51] se predlaže potpuno novi pristup kontrole pristupa zasnovan na atributima (eng. *Attribute-based access control*, skr. *ABAC*). Suštinska karakteristika ABAC modela je mogućnost donošenja autorizacionih odluka u zavisnosti od vrednosti atributa dodeljenih korisnicima i objektima, kao i uslova okruženja [51][83]. Za razliku od RBAC modela čija formalizacija i standardizacija datira još iz 1990-tih godina, ABAC model je aktuelan tek od druge decenije XXI veka. Motivisani sve većim značajem i primenom ovog modela unutar različitih sistema, autori se u člancima [52][83] bave uvođenjem osnovnih koncepata i funkcionalnih komponenti ABAC modela.

Osnovni elementi ABAC modela su prikazani na *Slici 2.* Atributi predstavljaju karakteristike korisnika, objekata i okruženja, definisane uređenim parovima (ime atributa, vrednost) [52][83][117]. Atribut je funkcija koja za određeni entitet vraća specifičnu vrednost iz unapred definisanog opsega vrednosti. Entiteti mogu biti korisnici, objekti ili uslovi okruženja. Vrednost atributa može biti tačno jedna vrednost (eng. *atomic attributes*) ili podskup skupa vrednosti iz njegovog opsega (eng. *set-valued attributes*). Subjekat, odnosno aktivni entitet korisnika u sistemu, je određen skupom atributa relevantnih za korisnika, npr. ime korisnika, naziv organizacije kojoj pripada, uloga unutar organizacije, e-mail adresa, itd. Objektima, odnosno resursima koje je potrebno zaštititi se dodeljuje skup atributa karakterističnih za svaki objekat. Na primeru poverljivog dokumenta, to mogu biti autor i naziv dokumenta, organizacija u čijem je vlasništvu dokument, datum kreiranja, datum poslednje izmene, stepen poverljivosti sadržaja dokumenta, itd. Atributi se objektima dodeljuju prilikom njihovog kreiranja, a u zavisnosti od tipa atributa vrednosti se mogu i modifikovati. Uslovi okruženja opisuju kontekst u kom se iniciraju zahtevi za pristup i donose autorizacione odluke, kao što su vreme pristupa, lokacija korisnika, trenutni nivo bezbednosnog rizika u sistemu, temperatura, i slično. Još se nazivaju i kontekstni atributi, jer predstavljaju karakteristike okruženja koje su potpuno nezavisne od atributa dodeljenih korisnicima i objektima, i čije se vrednosti mogu dinamički menjati.

ABAC autorizacione politike (eng. *access control policies*) su dokumentovana pravila i procedure kojima su opisane dozvoljene operacije nad objektima unutar organizacije. Pravila predstavljaju formalnu specifikaciju autorizacionih politika, izraženo uz pomoć atributa korisnika, atributa objekata i uslova okruženja. Svakom objektu se dodeljuje jedno ili više pravila koja definišu skup dozvoljenih operacija koje mogu biti izvršene nad tim objektom u dozvoljenim uslovima okruženja [83]. Proces upravljanja autorizacionim politikama podrazumeva definisanje dokumentovanih pravila i procedura korišćenjem različitih jezika za specifikaciju politika. Jedan od jezika koji se može iskoristiti za specifikaciju prava pristupa u distribuiranom heterogenom okruženju je



Slika 2. Osnovni elementi ABAC modela [83]

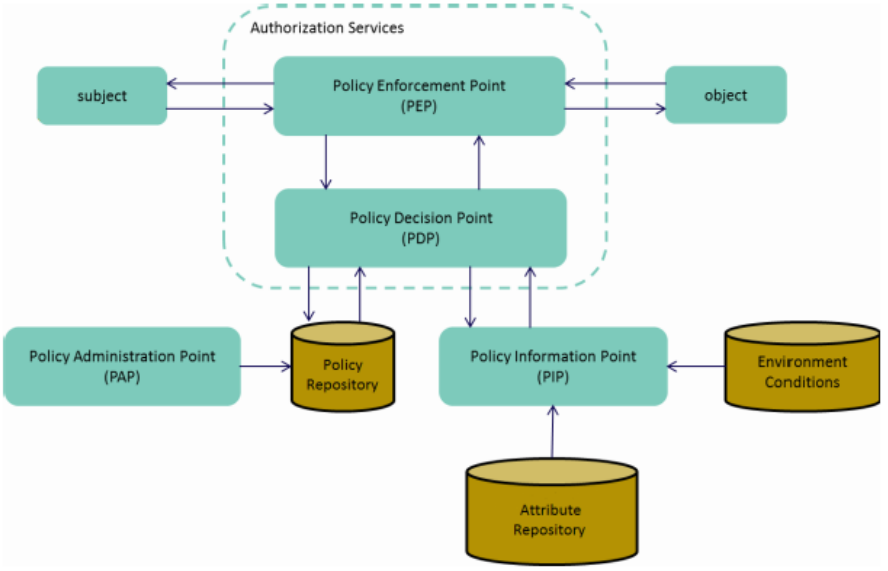
Extensible Access Control Markup Language (skr. *XACML*) jezika.XACML opisuje jezik za specifikaciju autorizacionih politika u skladu sa ABAC modelom, i opisuje model sprovođenja kontrole pristupa koji definiše tok podataka od prijema zahteva za pristup do formiranja odgovora [116].

U nastavku ove sekcije dat je prikaz funkcionalnih komponenti ABAC modela u skladu sa XACML modelom sprovođenja kontrole pristupa [83], a zatim je predstavljen XACML jezik za specifikaciju autorizacionih politika.

2.5.1 Funkcionalne komponente ABAC modela

Na *Slici 3.* su prikazane funkcionalne komponente ABAC modela prema standardu NIST SP 800-62 [83]. ABAC model čine dve logičke komponente koje zajedno funkcionišu kako bi se omogućilo donošenje autorizacionih odluka:

- komponenta za prikupljanje, procenu i administraciju atributa i politika (servis za administraciju podataka),
- komponenta za upravljanje procesom sprovođenja autorizacionih politika (autorizacioni servis),



Slika 3. Funkcionalne komponente ABAC modela **Error! Reference source not found.**

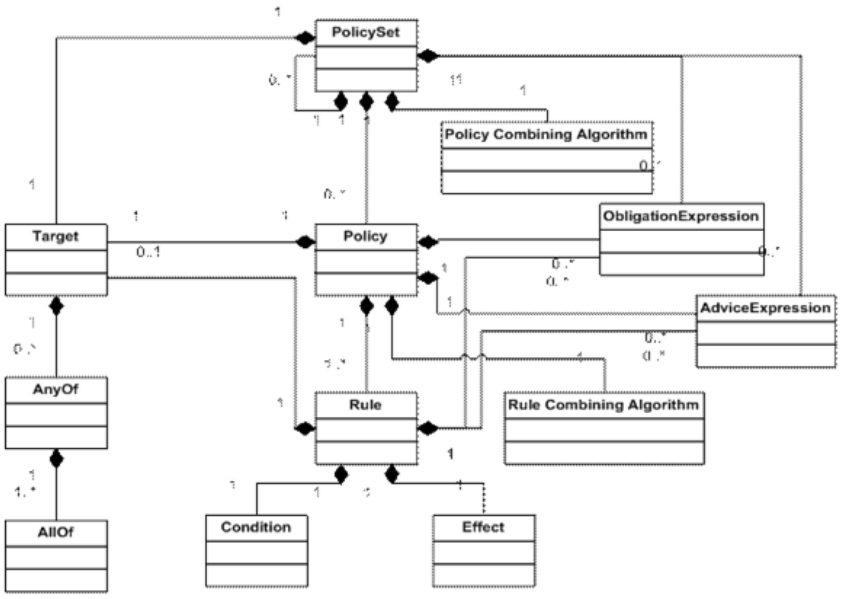
Servis za administraciju podataka se sastoji od komponente za skladištenje i administraciju atributa (eng. *Policy Information Point*, skr. *PIP*), komponente za skladištenje i administraciju pravila (eng. *Policy Administration Point*, skr. *PAP*), i opciono komponente za skladištenje autorizacionih politika (eng. *Policy Retrieval Point*, skr. *PRP*). PIP ima ulogu izvora svih atributa, odnosno predstavlja interfejs ka svim komponentama koje skladište atribute o subjektima, resursima i uslovima okruženja sistema. PAP je komponenta za skladištenje i upravljanje autorizacionim pravilima u sistemu, uključujući i njihovo generisanje na osnovu autorizacionih politika. PRP je komponenta za skladištenje autorizacionih politika u standardnom format, najčešće XACML fajlovi skladišteni u okviru baze podataka ili sistema datoteka.

Autorizacioni servis čine komponenta za donošenje autorizacionih odluka (eng. *Policy Decision Point*, skr. *PDP*) i komponenta za sprovođenje autorizacionih odluka (eng. *Policy Enforcement Point*, skr. *PEP*). PEP je komponenta koja prihvata zahteve za pristup resursima u sistemu, verifikuje identitet korisnika koji šalje zahtev, usmerava zahtev ka PDP komponenti, a zatim na osnovu odgovora može da dozvoli ili zabrani pristup i ukoliko je to zahtevano ispuni odgovarajuće obaveze (obligacije). PDP je komponenta u okviru koje se donosi odluka o tome da li pristup objektu treba da bude dozvoljen ili odbijen, u zavisnost od autorizacionih pravila definisanih za objekat kome se pristupa. Stoga, PDP treba da ima pristup vrednostima svih atributa, kao i autorizacionim pravilima u sistemu.

2.5.2 XACML jezik za specifikaciju autorizacionih pravila

XACML je deklarativni jezik za specifikaciju autorizacionih politika baziranih na atributima, ali i modela obrade koji opisuje kako doneti odluku o pristupu na osnovu pravila definisanih u politikama [93][116].

Na *Slici 4.* je prikazan UML dijagram klasa modela XACML jezika za specifikaciju autorizacionih politika.



Slika 4. UML dijagram klasa XACML modela jezika za specifikaciju autorizacionih politika [93]

Korenski element svih XACML autorizacionih politika je `PolicySet` koji predstavlja agregaciju drugih `PolicySet` ili `Policy` elemenata, gde `Policy` predstavlja pojedinačne autorizacione politike. Pošto `PolicySet` može da sadrži više `PolicySet` i `Policy` elemenata na osnovu kojih se određuje da li je pristup dozvoljen ili ne, algoritam kombinovanja njihovih rezultata se definiše pomoću `PolicyCombiningAlgorithm` elementa. Sa elementom Target se definiše ono na šta se `PolicySet` ili `Policy` element odnosi. To mogu biti subjekti (`Subjects` element), resursi (`Resources` element), akcije (`Actions` element) i stanje okruženja pri kome politika važi (`Environments` element). Obligations elementom moguće je definisati obaveze koje PEP komponenta treba da izvrši ukoliko je PolicySet primenjen i ukoliko se odluka o pristupu poklapa sa odlukom za koju je obaveza definisana. Svaka autorizaciona politika je predstavljena skupom pravila opisanih `Rule` elementom, a svako pravilo čine `Target`, `Effect` i `Condition` elementi. Kao i u prethodnim slučajevima, `Target` elementom se definiše na šta se pravilo odnosi. `Effect` specificira da li je pristup dozvoljen ili ne, a `Condition` elementom se može definisati uslov koji mora da se zadovolji da bi pravilo moglo da se

primeni. U suprotnom, pravilo se neće razmatrati. `RuleCombiningAlgorithm` je algoritam za kombinovanje rezultata pravila [116].

2.6 Hibridni modeli kontrole pristupa – RBAC-A modeli

U članku [63] autori razmatraju prednosti i nedostatke RBAC i ABAC modela sa aspekta definisanja, primene i administracije autorizacionih politika u heterogenim, distribuiranim i dinamičnim okruženjima. Zaključak je da inicijalno uspostavljanje strukture uloga u RBAC modelu (eng. *role engineering*) može biti kompleksno, ali jednom uspostavljena struktura pruža determinističnost u pogledu privilegija dodeljenih korisnicima. Međutim, u okruženjima gde je potrebno uvažiti dinamičke parametre prilikom donošenja odluke o pristupu, može doći do problema naglog porasta broja uloga (eng. *role explosion*) kako bi se podržali različiti skupovi privilegija u zavisnosti od dinamičkih parametara. S druge strane, kompleksnost ABAC modela u slučaju velikog broja atributa koje treba uvažiti i otežano praćenje privilegija dodeljenih korisnicima su cena za veliku fleksibilnost i mogućnost uvažavanja širokog spektra kontekstnih informacija prilikom definisanja autorizacionih pravila, kao i automatizovan proces administracije. Stoga, predlažu se tri pristupa za integraciju RBAC i ABAC modela (tzv. RBAC-A modeli) sa ciljem da se uspostavi veza između uloga i atributa, koristeći pritom prednosti oba modela kako bi se omogućila efikasna kontrola pristupa u dinamičnim okruženjima.

RBAC-A orijentisan ka ulogama (eng. *role-centric RBAC-A*) je pristup koji podrazumeva uvođenje atributa kako bi se ograničio skup raspoloživih privilegija unutar korisničke sesije. Naime, ovim pristupom se zadržava struktura RBAC modela zasnovana na ulogama i privilegijama koje su im dodeljene, dok se na osnovu ograničenja definisanih uz pomoć atributa može redukovati maksimalan broj raspoloživih privilegija. Osnovni nedostatak ovakvog pristupa je činjenica da se ograničenjima može samo redukovati skup raspoloživih privilegija, odnosno nije ga moguće proširiti u zavisnosti od određenih atributa.

RBAC-A orijentisan ka atributima (eng. *attribute-centric RBAC-A*) je pristup u okviru koga korisničke uloge predstavljaju skup vrednosti atributa korisnika čiji opseg vrednosti odgovara skupu privilegija. Za razliku od RBAC modela gde je korisnička uloga entitet kojim se definiše skup prava u sistemu posredstvom relacija između uloga i dodeljenih privilegija, u ovakvom pristupu korisnička uloga je samo dodatni atribut korisnika. Osnovni nedostatak ovakvog pristupa je to što se gubi jednostavnost administracije i praćenja dodeljenog skupa privilegija koju nudi RBAC model.

RBAC-A sa dinamičkim ulogama (eng. *dynamic roles RBAC-A*) je pristup koji podrazumeva dinamičku dodelu uloga korisnicima u zavisnosti od atributa. Dodela skupa korisničkih uloga može biti u potpunosti određena atributima, a moguće je i atributima samo ograničiti unapred definisani skup korisničkih uloga. Prednost ovakvog pristupa je

to što je struktura RBAC modela u potpunosti zadržana, uz mogućnost dinamičke izmene skupa uloga dodeljenih korisnicima u zavisnosti od ABAC pravila. Osnovni nedostatak ovakvog pristupa je nemogućnost dinamičke izmene skupa privilegija dodeljenih korisničkim ulogama.

2.7 Bezbednost u Smart Gridu

U prošlosti, industrijski kontrolni sistemi su bili razvijani kao specijalizovani sistemi za nadzor i upravljanje fizičkim procesima i uređajima u realnom vremenu. Sa stanovišta bezbednosti su se ti sistemi oslanjali na fizičku izolovanost (odnosno sistem i njegovi podaci su zaštićeni, jer su fizički nedostupni) i princip tajnosti (eng. *security by obscurity*), uz minimalnu primenu bezbednosnih mehanizama za zaštitu ljudskog elementa, uređaja i industrijskih protokola [60][61]. Primena informacionih i komunikacionih tehnologija u procesu modernizacije elektroenergetskih mreža donosi brojne prednosti, kao što su [6][9][31]:

- efikasnije upravljanje uređajima i operacijama u kontrolnom sistemu,
- efikasniji oporavak sistema u slučaju nepredviđenih događaja i otkaza,
- povećanje pouzdanosti i kvaliteta isporučene električne energije,
- smanjenje gubitaka električne energije,
- smanjenje troškova poslovanja i povećanje profita kompanije,
- aktivna uloga krajnjih potrošača i mogućnost donošenja odluka koje će uticati na smanjenje troškova snabdevanja,
- unapređenje procesa zaštite životne sredine i korišćenje obnovljivih izvora energije.

Pored brojnih prednosti u pogledu poboljšanja procesa isporuke električne energije od proizvodnje do potrošnje i naplate, informacione i komunikacione tehnologije unose i nove slabosti koje u tradicionalnim sistemima nisu postojale [5][9][75]. Na primer, *Internet Protocol (IP)*-bazirane komunikacione tehnologije na kojima se zasniva Smart Grid [82] unose širok spektar bezbednosnih pretnji, kao što su prisluškivanje i nadgledanje informacija, lažiranje IP adresa, razne vrste preusmeravanja paketa. Takođe, informacioni sistem je izložen raznim malicioznim programima (virusi, crvi, trojanski konji) koji mogu da uzrokuju izmene u načinu funkcionisanja sistema, ali i da izazovu prestanak rada servisa. Osim toga, međusobno povezivanje sistema i sve veći broj pristupnih tačaka za razmenu podataka između sistema omogućuje lateralnu propagaciju zlonamernog softvera i/ili napadača kroz zahvaćeni sistem. Poseban izazov predstavlja činjenica da se savremeni elektroenergetski sistemi sastoje od velikog broja podsistema koje odlikuje raznolikost u pogledu funkcionalnosti i korišćenih tehnologija. U tom kontekstu su tipični napadi u Smart Gridu:

- Napad uskraćivanjem usluge (eng. *denial of service*, skr. *DoS*) – napadi koji imaju za cilj da preopterete komunikacionu mrežu ili računarske resurse uzrokujući kašnjenje ili gubitak podataka, kao i nedostupnost sistema [5][68][126]. Primer DoS napada je napad na telefonsku centralu ukrajinskih elektrodistributivnih kompanija.
- Manipulacija servisima (eng. *manipulation of service*) - kategorija napada koji imaju za cilj da izmene podatke ili servise, ugrožavajući time pravilno funkcionisanje sistema, npr. donošenje pogrešnih upravljačkih odluka na osnovu netačnih ili nedostupnih podataka [5][61][68]. Tipičan primer ove klase napada je *Stuxnet* [65].
- Krađa informacija (eng. *theft of information*) - napadi koji imaju za cilj otkrivanje poverljivih informacija [5][68]. To može biti otkrivanje ličnih podataka o potrošačima (eng. *personally identifiable information*, skr. *PII*) čime se narušava privatnost korisnika, ali i otkrivanje poverljivih informacija o poslovanju kompanije [61]. Primer ove klase napada je *Duqu* [14].

Primena efikasnih bezbednosnih mehanizama za zaštitu informacionih sistema je od suštinske važnosti za pouzdan, efikasan i siguran rad savremenih elektroenergetskih sistema, koji su zbog svoje kritičnosti za funkcionisanje modernog društva veoma česta meta raznih napada. Stoga, bezbednost i zaštita Smart Grid sistema predstavlja prioritet svake države čija nacionalna bezbednost, nacionalna ekomonija, javno zdravlje i bezbednost stanovništva može biti posredno ugrožena preko uspešnih napada na elektroenergetski sistem. Definisanjem regulatornih mera u vidu standarda, propisa i preporuka država definiše i primenjuje mere i inicijative za zaštitu Smart Grida kako od namernih napada, tako i od nenamernih grešaka validnih korisnika (npr. nesavesni ili slabo obučeni zaposleni) i nepredviđenih situacija (npr. otkazi uređaja i opreme, prirodne katastrofe, itd.) [60][61][120].

U nastavku ove sekcije dat je pregled informacione infrastrukture Smart Grid sistema, kao i vladajućih tehničkih standarda u oblasti informacione bezbednosti za Smart Grid koji su publikovani i široko prihvaćeni kako u Evropi tako i u Severnoj Americi. Potom su prikazani su referentni modeli za Smart Grid neophodni za razumevanje bezbednosnih zahteva ovih sistema.

2.7.1 Pregled Smart Grid informacionih sistema

Smart Grid sistemi su sačinjeni od velikog broja informacionih sistema koji se sa aspekta uticaja za stabilan rad elektroenergetskih sistema, ali i bezbednosnih pretnji mogu grupisati u tri podsistema [61]:

- Procesni podsistem (eng. *process control network*, *industrial control network*),
- Komandno-kontrolni podsistem (eng. *control room environment*), odnosno kontrolna soba,

- Poslovni podsistem (eng. *enterprise environment*).

Procesni sistem, odnosno sistem za upravljanje industrijskim procesima, čine inteligentni elektronski uređaji (eng. Intelligent Electronic Device, skr. IED) u okviru podsistema za prenos, distribuciju i potrošnju električne energije, kao i uređaji za razmenu podataka sa komandno-kontrolnim sistemom, kao što su udaljene terminalne jedinice (eng. Remote Terminal Unit, skr. RTU) i koncentratori fazora (eng. Phasor Data Concentrator, skr. PDC). Ovi sistemi se zasnivaju na industrijskim protokolima i namenskim operativnim sistemima koji su dizajnirani za rad u realnom vremenu, odnosno za koje je od ključnog značaja vreme odziva i kontinualna dostupnost. Bezbednost ovog sistema se do početka XXI veka zasnivala na zatvorenosti i primeni specijalizovanih protokola. Praktična primena bezbednosnih mehanizama koji bi mogli da izazovu kašnjenje u prenosu podataka nije bila prihvatljiva. Specijalizovana i heterogena priroda resursa procesnog sistema zahteva primenu namenskih alata za čiju je implementaciju najčešće potrebna podrška od strane proizvođača uređaja. Ovo predstavlja veliki izazov za bezbednost Smart Grida, jer se procesni sistem mogu iskoristiti kao vektor napada na druge delove Smart Grid sistema [60][61]. Na primer, zaštitni releji su IED uređaji kod kojih se primena bezbednosnih mehanizama najčešće zasniva na korišćenju šifri. Loše prakse kada je u pitanju definisanje šifri, upotreba fabričkih (podrazumevanih) šifri, kao i mogućnost neograničenog broj pokušaja autentifikacije samo su neki od propusta koji dodatno olakšavaju kompromitovanje ovih uređaja, što dalje može izazvati DoS napad na DNP3 protokol (eng. *Distributed Network Protocol v3.0*) koji je namenjen za razmenu podataka između IED uređaja i udaljenog kontrolnog centra. DoS napad u vidu preplavljivanja DNP3 bafera za kolektovanje podataka (eng. *buffer flooding attack*) može izazvati kašnjenje ili gubitak podataka iz polja što direktno utiče na operacije nadzora i upravljanja u komandno-kontrolnom sistemu.

Komandno-kontrolni sistem čine sistem za nadzor i upravljanje industrijskim procesima (eng. *Supervisory Control and Data Acquisition*, skr. *SCADA*) i sistemi za podršku u odlučivanju (eng. *Decision Support System*, skr. *DSS*).

SCADA je kontrolni sistem koji podrazumeva interakciju sa fizičkim uređajima i procesima, npr. očitavanje mernih veličina sa uređaja, kao i slanje upravljačkih akcija. Osnovni zahtevi koji se stavljaju pred ove sisteme su stabilnost i dugoročnost, što za posledicu ima sporo prihvatanje novih tehnologija, poteškoće prilikom nadogradnje sistema i primene bezbednosnih mehanizama koji bi ugrozili rad u realnom vremenu (npr. antivirus softver, čvorni i mrežni sistemi za detekciju i prevenciju napada, itd.) [61][121].

Sistemi za podršku u odlučivanju su sistemi namenjeni je unapređenje procesa upravljanja i planiranja pogona elektroenergetske mreže u realnom vremenu. Iako SCADA sistemi mogu da funkcionišu potpuno nezavisno od sistema za podršku u

odlučivanju, integracijom sa SCADA-om ove komponente mogu imati značajan uticaj na stabilan rad elektroenergetskih sistema [74][96][102][121]. Sledi nekoliko primera ovih rešenja u savremenim elektroenergetskim kompanijama su:

- Sistem za upravljanje ispadima (eng. *Outage Management System*, skr. *OMS*) omogućava rukovanje greškama, evidenciju prekida i identifikaciju, analizu i otklanjanje ispada u sistemu sa ciljem da se spreče ili što efikasnije uklone kvarovi u mreži i na taj način minimizuje vreme ispada kao i ekonomske posledice nestanka napajanja.
- Sistem za upravljanje prenosnom elektroenergetskom mrežom (eng. *Energy Management System*, skr. *EMS*) se koristi kao ekspertski sistem sa ciljem optimizacije korišćenja električne energije, povećanja pouzdanosti i performansi sistema.
- Sistem za upravljanje distributivnom elektroenergetskom mrežom (eng. *Distribution Management System*, skr. *DMS*) ima za cilj da obezbedi pouzdaniji i efikasniji rad distributivne mreže, unapredi donošenje ispravnih upravljačkih odluka i poboljša kvalitet isporučene električne energije.
- Sistem za upravljanje modelom podataka (eng. *Network Model Service*, skr. *NMS*). NMS je sistem za upravljanje modelom podataka elektroenergetske mreže, kao što su podaci o generatorima, transformatorima, vodovima, prekidačima, potrošačima, o njihovoj međusobnoj povezanosti i konektivnosti. NMS je osnova funkcionisanja EMS/DMS/OMS sistema, jer tačnost modela podataka utiče na kvalitet estimacije stanja mreže, a time i na proračune niza upravljačkih akcija koje sistem treba da dovedu u željeni režim.

U poređenju sa SCADA sistemom, sistemi za podršku u odlučivanju se znatno brže razvijaju i zasnivaju se na modernim tehnologijama, npr. najnovije verzije operativnog sistema i softvera, uključujući i bezbednosne tehnologije. Kako ovi sistemi mogu imati uticaj na stabilnost rada sistema, tokom uvođenja ovih rešenja je neophodno voditi računa da ove aplikacije budu implementirane u skladu sa zahtevima za rad u realnom vremenu.

Poslovni sistemi. S obzirom na proces deregulacije u elektroprivredi i stvaranja otvorenog i slobodnog tržišta električne energije, različiti sistemi za upravljanje poslovnim procesima kompanije su sada uključeni kao integralni deo Smart Grid rešenja u cilju poboljšanja usluge i kvaliteta električne energije uz smanjenje troškova proizvodnje [8][62]. Primeri poslovnih sistema su:

- Sistem za skladištenje podataka o potrošačima (eng. *Customer Information System*, skr. *CIS*). Namena ovog sistema je skladištenje podataka o individualnim potrošačima, tj. kupcima električne energije [61][102].
- Sistem za naplatu (eng. *Billing*). Billing sistem je namenjen za obračun potrošnje i naplatu električne energije, pri čemu podaci o potrošnji stižu posredstvom sistema za daljinsko očitavanje potrošnje električne energije [102][113].

- Geografski informacioni sistemi (eng. *Geographic Information System*, skr. *GIS*). GIS predstavlja osnovni izvor podataka o modelu elektroenergetske mreže, pre svega podataka o geografskoj lokaciji uređaja i elemenata, kao i o konektivnosti mreže [57][102].
- Sistem za upravljanje radovima (eng. *Work Management Service,* skr. *WMS*). WMS je sistem kroz koji se vodi evidencija o planiranim radovima na distributivnoj mreži (npr. radovi na izgradnje mreže, priključivanje potrošača i instalacija brojila, itd.).
- Sistem za upravljane posadom na terenu (eng. *WorkForce Management System*, skr. *WFS*). WFS je sistem za upravljanje podacima o ekipama koje rade na terenu. To uključuje trenutnu lokaciju posade, radove na kojima su trenutno angažovani i status zadataka.

Slično DSS sistemima, poslovni sistemi su zasnovani na modernim tehnologijama, ali za razliku od DSS sistema oni nemaju uticaj na stabilan rad sistema. Međutim, u poslovnim sistemima se skladište podaci o poslovanju kompanije, podaci o zaposlenima, kao i privatni podaci o potrošačima, čije kompromitovanje može ugroziti privatnost korisnika ili naneti materijalnu štetu kompaniji.

Kako bi se omogućio pristup kontrolnom centru sa udaljenih lokacija ili pristup poslovnim sistemima kako od strane potrošača, tako i od strane partnerskih kompanija, odabrani elementi Smart Grid sistema su dostupni i preko javne mreže (npr. Internet). I dok pristup informacionom sistemu sa udaljene lokacije ima brojne prednosti, komunikacija koja se odvija preko nepoverljivih komunikacionih mreža je posebno izložena pretnjama [38].

2.7.2 Pregled bezbednosnih standarda za Smart Grid

U ovoj sekciji je dat pregled vladajućih tehničkih standarda u oblasti informacione bezbednosti za Smart Grid koji su kreirani i publikovani od strane relevantnih međunarodnih, regionalnih i nacionalnih organizacija za standardizaciju. Dat je pregled opštih standarda u oblasti informacione bezbednosti, a zatim bezbednosnih standarda za industrijske kontrolne sisteme i Smart Grid sisteme.

Opšti standardi u oblasti informacione bezbednosti

ISO/IEC 27000 je serija međunarodnih standarda informacione bezbednosti objavljenih od strane Međunarodne organizacije za standarde (eng. *International Organization for Standards*, skr. *ISO*) i Međunarodne elektrotehničke komisije (eng. *International Electrotechnical Commission*, skr. *IEC*) sa ciljem razvoja i primene sistema upravljanja bezbednošću informacija (eng. *Information Security Management System*, skr. *ISMS*) [48]. Standard je definisan tako da svaka organizacija, bez obzira na delatnost ili veličinu, može da proceni bezbednosne rizike i primeni odgovarajuće bezbednosne

mere u skladu sa svojim zahtevima koristeći unapred definisane preporuke i smernice. Standardom ISO/IEC 27001 se formalno specificira model za uspostavljanje, primenu, održavanje i poboljšanje ISMS unutar neke organizacije [49]. Standard ISO/IEC 27002 definiše skup preporuka za očuvanje poverljivosti, intergiteta i raspoloživosti informacija namenjenih organizacijama koje implementiraji ISMS [50].

Američki nacionalni institut za standarde i tehnologije (eng. *National Institute of Standards and Technology*, skr. *NIST*) definiše niz standarda za informacionu bezbednost organizacija u različitim sektorima. Specijalne publikacije serije 800 (NIST Special Publications – 800-series) obuhvataju skup preporuka i dobrih praksi za primenu i razvoj mera bezbednosti informacionih sistema. Specijalna publikacija NIST SP 800-53 daje smernice za primenu bezbednosnih mehanizama u informacionim sistemima državnih institucija [84].

Bezbednosni standardi za industrijske kontrolne sisteme

Problemom razvoja standarda za razmenu informacija elektroenergetskih i drugih srodnih sistema bave se radne grupe u okviru tehničkog komiteta IEC TC57 u okviru Međunarodne elektrotehničke komisije (eng. *International Electrotechnical Commission*, skr. *IEC*) [42]. IEC TC57 obuhvata komunikacione protokole za razmenu informacija u elektroenergetskim sistemima koji su danas globalno prihvaćeni. IEC 62351 je standard koji definiše bezbednosne mere za zaštitu IEC TC57 komunikacionih protokola [42].

ISA-99 predstavlja skup standarda i preporuka za bezbednost industrijskih procesnih i kontrolnih sistema objavljenih od strane Međunarodnog udruženja za automatizaciju (eng. *The International Society of Automation*, skr. *ISA*). Pre konačnog objavljivanja od strane Međunarodne elektrotehničke komisije, ovaj skup standarda i preporuka je promenio naziv u IEC 62443 [47].

North American Electric Reliability Corporation (skr. NERC) je definisao niz regulativa u cilju zaštite kritičnih infrastruktura, pre svega elektroenergetskih sistema pod nazivom *Critical Infrastructure Protection* (skr. CIP) [87].NERC CIP standardi se prvenstveno odnose na očuvanje pouzdanosti postrojenja u proizvodnji, prenosu i distribuciji električne energije. Usaglašenost sa propisima NERC CIP standarda je mandatorna u Severnoj Americi, a za kompanije koje nisu u skladu sa NERC CIP zahtevima propisane su velike novčane kazne.

U okviru specijalne publikacije NIST SP 800-82 NIST je objavio skup preporuka i smernica za zaštitu industrijskih kontrolnih sistema baziranih na bezbednosnim pretnjama i slabostima tipičnim za ove sisteme [85].

Bezbednosni standardi za Smart Grid

Prema Zakonu o energetskoj nezavisnosti i bezbednosti Sjedinjenih Američkih Država iz 2007. (eng. *Energy Independence and Security Act of 2007*), NIST ima ključnu ulogu u razvoju tehničkih standarda čiji krajnji cilj je postizanje interoperabilnosti između različitih komponenti i protokola u Smart Gridu. U tom smislu, NIST je objavio specijalnu publikaciju NIST SP 1108 pod nazivom NIST okvir i plan za izradu standarda za Smart Grid interoperabilnost (eng. *NIST Framework and Roadmap for Smart Grid Interoperability Standards*) u okviru koga je dat pregled standarda relevantnih za različite domene Smart Grid, uključujući i standarde koji se odnose na informacionu bezbednost u Smart Gridu. U istoj publikaciji je definisan i konceptualni model naprednih elektroenergetskih mreža čiji krajnji cilj je razumevanje kompleksnost i interoperabilnosti informacione infrastrukture Smart Grida [82]. Dokument koji čini sveobuhvatan skup zahteva za postizanje visokog stepena pouzdanosti i bezbednosti, uzimajući u obzir sve aspekte Smart Grida je izveštaj pod nazivom "NIST IR 7628 smernice za informacionu bezbednost Smart Grida" (eng. *NIST IR 7628 Smart Grid Cyber Security Strategy and Requirements*) [81].

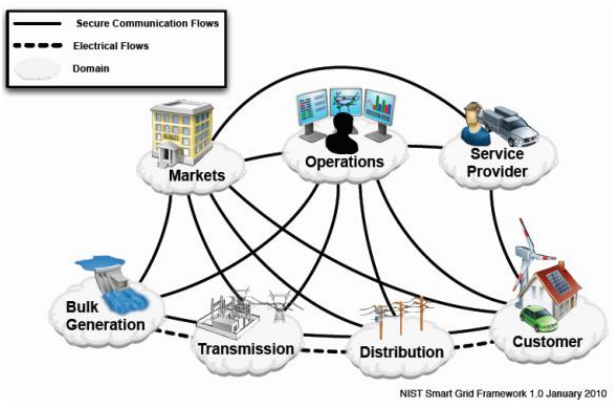
Evropska agencija za bezbednost računarskih mreža i informacija (eng. *European Network and Information Security Agency*, skr. *ENISA*) je objavila skup dokumenata u cilju podrške razvoju evropskih naprednih elektroenergetskih mreža. Dokument "Bezbednosni aspekti Smart Grida" (eng. *Security aspects of Smart Grids*) je namenjen obezbeđivanju održive informacione bezbednosti, zaštite podataka i privatnosti u Smart Gridu [24], dok se dokumentu "Odgovarajuće mere bezbednosti za Smart Grid" (eng. *Appropriate security measures for smart grids*) daju preporuke za primenu tehničkih bezbednosnih mera u Smart Gridu [25].

2.7.3 NIST referentni model za Smart Grid

Smart Grid je kompleksna infrastruktura sačinjena od velikog broja sistema (tzv. system of systems [17]) koje odlikuje visok stepen interkonektivnosti i interoperabilnosti, kao i raznolikost u pogledu funkcionalnosti i korišćenih tehnologija. Interkonektivnost se definiše kao međupovezanost različitih komponenti unutar jednog sistema, ali i međupovezanost različitih sistema, pri čemu se različiti sistemi mogu oslanjati na potpuno različite komunikacione mreže, od IP-baziranih mrežnih protokola specifičnih za poslovne sisteme, do specijalizovanih industrijskih protokola specifičnih za industrijske kontrolne sisteme. Interoperabilnost se definiše kao sposobnost dva ili više sistema, uređaja, mreža, aplikacija ili komponenti da funkcionišu zajedno, odnosno da razmenjuju i koriste informacije [82].

Referentni model za Smart Grid ima za cilj da opiše različite komponente u Smart Gridu, kao i interakcije između njih kako bi se što bolje razumela kompleksnost informacione infrastrukture Smart Grid sistema [82]. Na *Slici 5.* je konceptualno prikazan referentni model definisan u NIST SP 1108 [82], a u okviru koga je identifikovano sedam

Smart Grid domena koji su međusobno povezani energetskim tokovima i komunikacionim vezama.



Slika 5. NIST referentni model za Smart Grid [82]

Svaki domen se sastoji od učesnika i aplikacija. Učesnik može biti uređaj, računarski sistem, softverski program, organizacija ili pojedinac koji učestvuje u donošenju odluka i razmeni informacija neophodnih za izvršavanje zadataka unutar domena. Zadaci izvršavani od strane učesnika unutar domena se nazivaju aplikacije. Unutar jednog domena može biti više učesnika, a jedan učesnik može imati zaduženja u različitim domenima. Na primer, distributivna kompanija se ne sastoji isključivo iz domena za distribuciju električne energije. Distributivna kompanija može da sadrži učesnike iz domena operacija (npr. sistem za upravljanje distributivnom mrežom) i iz domena potrošača (npr. brojila električne energije) . Pregled sedam domena Smart Grid sistema dat je u *Tabeli 1.* [82].

Tabela 1. Smart Grid domeni prema NIST standardu [82]

Smart Grid domen	Opis
Domen potrošača (*Customers*)	Obuhvata krajnje potrošače električne energije, odnosno tri tipa krajnjih potrošača: domaćinstva, zgrade i industrijska postrojenja. Osim uloge potrošača, oni mogu biti i generatori električne energije. Tipične aplikacije iz ovog domena su upravljanje potrošnjom električne energije i distributivna proizvodnja (odnosno proizvodnja električne energije iz obnovljivih izvora).
Domen tržišta (*Markets*)	Predstavlja domen kupovine i prodaje električne energije. U okviru ovog domena, uloga učesnika je određivanje cene električne energije, balansiranje između proizvodnje i potrošnje unutar elektroenergetskog sistema, i upravljanje debalansima koji mogu nastati u realnom vremenu između ugovorenih i realizovanih količina. Tipične aplikacije iz ovog domena uključuju upravljanje veleprodajnim tržistem (kupovina električne energije od velikih generatorskih kompanija), upravljanje maloprodajnim tržištem (prodaja električne energije krajnjim potrošačima), itd.

Domen usluga (*Service Providers*)	Obuhvata različite servise za upravljanje poslovnim procesima proizvođača, distributera i kupaca električne energije. Tu spadaju aplikacije za upravljanje poslovanjem i odnosima sa klijentima, upravljanje poslovnim nalozima proizvođača i kupaca električne energije, sistemi za naplatu, itd.
Domen operacija (*Operations*)	Domen u kom su učesnici odgovorni za ispravno funkcionisanje elektroenergetskog sistema. Tipične aplikacije iz ovog domena su sistemi za nadzor i upravljanje u realnom vremenu, npr. sistem za upravljanje prenosnim delom elektroenergetskog sistema, sistem za upravljanje distributivnim delom elektroenergetskog sistema, itd.
Domen proizvodnje (*Bulk Generation*)	Obuhvata proces proizvodnje električne energije iz drugih oblika energije, npr. sagorevanjem fosilnih goriva (prirodni gas, ugalj), iz nuklearnih reaktora, ali i iz obnovljivih izvora. Tipične aplikacije podrazumevaju kontrolu procesa proizvodnje, zaštitu sistema u slučaju grešaka ili otkaza, i slično.
Domen prenosa (*Transmission*)	Obuhvata proces prenosa električne energije od mesta proizvodnje do distributivne mreže. Prenosni sistem električne energije je visoko-naponska mreža koja se snabdeva električnom energijom direktno iz elektrana, a na koju je povezana distributivna mreža, kao i veliki potrošači tipa rafinerije.
Domen distribucije (*Distribution*)	Obuhvata proces distribucije električne energije do krajnjih potrošača. Distributivni sistem električne energije je srednje-naponska i nisko-naponska mreža sa koje se snabdevaju krajnji potrošači, direktno ili putem snabdevača. Osim sa prenosne mreže, distributivna mreža se može snabdevati električnom energijom i preko distributivnih generatora.

2.7.4 IEC-62443 model bezbednosnih zona

Savremeni elektroenergetski sistemi su kompleksne infrastrukture sačinjene od različitih komponenti industrijskih kontrolnih sistema i poslovnih sistema koje učestvuju u procesu isporuke električne energije od proizvodnje do potrošnje i naplate električne energije. Čest uzrok bezbednosnih incidenata je ravna (eng. *flat*) mrežna arhitektura [1][15][98]. Naime, ravna mrežna arhitektura podrazumeva da je sistem odvojen od spoljašnjih sistema i spoljašnjih pretnji odgovarajućim bezbednosnim mehanizmima, dok se komunikacija unutar sistema odvija potpuno ravnopravno između svih uređaja [46]. U takvom okruženju, ukoliko bilo koja komponenta sistema postane kompromitovana, bezbednost čitavog sistema postaje ugrožena zbog mogućnosti jednostavne propagacije zlonamernog softvera unutar celog sistema putem korisničkih interakcija ili replikacijom unutar sistema [15][46].

IEC-62433 model bezbednosnih zona (eng. *Zone and Conduit Security Model*) se bazira na fizičkom i logičkom razdvajanju sistema koje je potrebno zaštititi, i formiranju grupe uređaja i aplikacija sa istim bezbednosnim zahtevima u pogledu kritičnosti resursa, ali i posledica koje bezbednosni incidenti mogu imati [1][15][98]. Ovaj model se zasniva na konceptu zone (eng. *zone*) i kontrolisanog komunikacionog kanala (eng. *conduit*) definisanih prema IEC-62443-3-2 standardu kako bi se obezbedila segmentacija i izolacija različitih komponenti unutar sistema [44]. Bezbednosna zona predstavlja

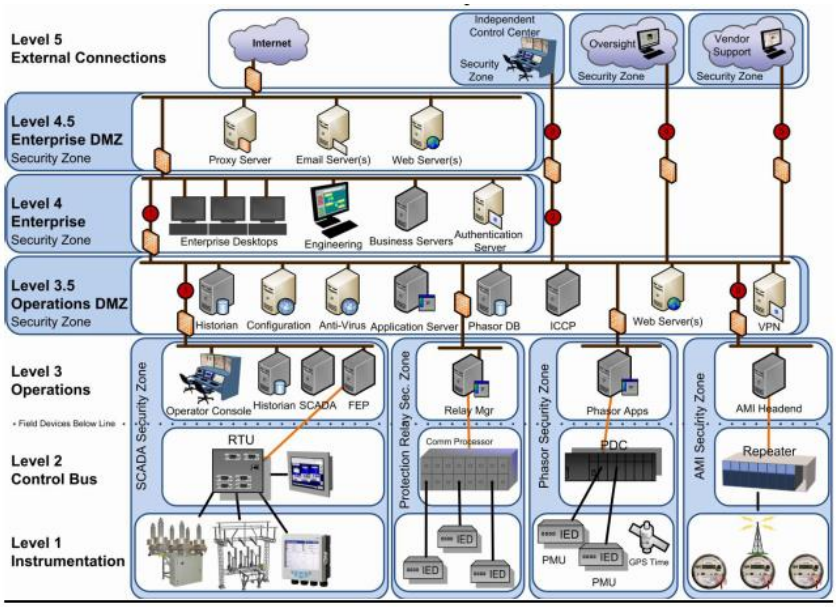
logičku grupu resursa koji predstavljaju jednu administrativnu celinu u kojoj važi ista bezbednosna politika, npr. pravila o pristupu resursima, dozvoljeni protokoli, i slično. Svaka zona može biti dodatno podeljena u podzone što omogućuje dalju segmentaciju resursa na osnovu određenog kriterijuma. Prema standardu međunarodnog udruženja za automatizaciju (eng. *The International Society of Automation*, skr. *ISA*), prvi nivo segmentacije se definiše na osnovu fizičke lokacije resursa, a dalja podela na podzone se definiše na osnovu logičkog grupisanja resursa prema specifičnim bezbednosnim zahtevima, kao što je npr. kritičnost resursa za pouzdan rad sistema [15][61][98]. Komunikacija između dve zone se vrši putem kontrolisanih komunikacionih kanala. Bezbedan komunikacioni kanal predstavlja tok podataka između dve zone, kao i odgovarajuće mehanizme koji omogućuju bezbednu razmenu podataka. Kontrola toka podataka između dve zone vrši se putem pristupnih tačaka koje se nalaze između dve zone i kontrolišu dolazni i odlazni saobraćaj u svakoj zoni. U nastavku je prikazan primer bezbednosne arhitekture industrijskog kontrolnog sistema koji je zasnovan na IEC-62433 modelu bezbednosnih zona.

Bezbednosna arhitektura industrijskog kontrolnog sistema

U članku [58] autori daju predlog bezbednosne arhitekture industrijskog kontrolnog sistema koji je zasnovan na IEC-62443 modelu bezbednosnih zona. Predložena arhitektura je sačinjena od šest bezbednosnih zona, kao što je prikazano na *Slici 6.* Koncept demilitarizovane zone (eng. *demilitarized zone*, skr. *DMZ*) predstavlja bezbednosnu zonu koja je logički postavljena između dve bezbednosne zone, u opštem slučaju između interne i spoljašnje zone, sa ciljem da se obezbedi kontrolisan pristup i interna zona zaštiti od spoljašnjih napada [58].

Spoljašnja zona (*Level 5. External connections*) predstavlja eksternu oblast koja nije u nadležnosti organizacije, i samim tim unutar koje nije moguće propisati bezbednosnu politiku koja će se primenjivati. Unutar ove zone mogu postojati podzone zavisno od namene, npr. za potrebe praćenja sistema od strane regulatornih tela, održavanje sistema od strane verifikovanih prodavaca softvera, za komunikaciju sa udaljenim kontrolnim centrima, itd.

Zona javnog pristupa (*Level 4.5. Enterprise DMZ*) predstavlja eksternu DMZ zonu koja štiti internu mrežu od spoljašnjih pretnji i ograničava izloženost internih resursa spoljašnjoj zoni. U ovoj zoni smešteni su uređaji i servisi namenjeni za direktan pristup od strane spoljašnjih korisnika, kao što su *Web server*, *e-mail server*, *proxy server*, itd. Po pravilu, osetljive informacije se ne skladište u ovoj zoni. One mogu prolaziti ili biti prikupljane u njoj, ali ih treba skladištiti u zonama višeg nivoa bezbednosti.



Slika 6. IEC-62433 model bezbednosnih zona kontrolnog sistema [58]

Poslovna zona (*Level 4. Enterprise*) je namenjena za svakodnevne operacije zaposlenih i sastoji se od različitih servisa za unapređenje poslovnih procesa (npr. sistem za upravljanje poslovanjem i odnosima sa klijentima, sistem za naplatu, itd.). U ovoj zoni, sva komunikacija sa spoljašnjom zonom se odvija preko servera zone javnog pristupa.

Operativna DMZ zona (*Level 3.5. Operations DMZ*) predstavlja internu DMZ zonu koja omogućuje bezbedan pristup operativnim podacima iz poslovne zone, npr. pristup istorijskim podacima. U ovu zonu se najčešće smeštaju servisi za administraciju sistema, servisi za administraciju bezbednosti i servisi za logove o sistemskim aktivnostima. Ovoj zoni se po pravilu može pristupiti samo iz drugih zona koje su pod kontrolom kompanije, ili iz eksternih sistema sa kojima su uspostavljena određena bezbednosna pravila, npr. primena ICCP protokol za komunikaciju sa udaljenim kontrolnim centrima, razmena izveštaja koji se razmenjuju sa regulatornim telima, itd.

Operativna zona (*Level 3. Operations*) predstavlja okruženje namenjeno za aplikacije sa strogim zahtevima za pouzdanost i raspoloživost, a čije narušavanje može imati posledice po stabilnost sistema, npr. SCADA (eng. *Supervisory Control and Data Acquisition*) sistemi.

Zona ograničenog pristupa je industrijski kontrolni sistem koji uključuje kritične servise namenjene za nadzor i upravljanje fizičkim procesima, a čiji bi gubitak značio prekid usluge. Čine je fizički uređaji (*Level 1. Instrumentation*) i uređaji za razmenu podataka sa kontrolnim sistemom (*Level 2. Control Bus*). Direktna komunikacija treba da bude omogućena samo sa operativnom zonom.

3 Opis problema

U ovom poglavlju je dat pregled aktuelnih zahteva u oblasti kontrole pristupa u Smart Gridu. U prvom delu su razmotreni zahtevi koji su propisani vladajućim *cyber security* standardima kako u Evropi tako i u Severnoj Americi. Pregledom dva standarda u oblasti bezbednosti informacionih sistema, četiri standarda za bezbednost industrijskih kontrolnih sistema i dva standarda za bezbednost u Smart Gridu ustanovljeno je da kontrola pristupa zasnovana na ulogama korisnika u sistemu preovlađuje kao najbolja industrijska praksa. Razlog tome su jednostavnost i cena implementacije, kao i centralizovana administracija RBAC modela. Dodatno, bezbednosni standardi za Smart Grid razmatraju i vanredne situacije u kojima je stabilan i kontinualan rad elektroenergetskog sistema prioritet, kada bezbednosni mehanizmi mogu privremeno biti izmenjeni ili potpuno isključeni na zahtev korisnika. Kako je RBAC je statički model koji nema mogućnost izmene bezbednosne politike nakon uspostavljanja korisničkih sesija, može se zaključiti da nije adekvatan u uslovima vanrednih situacija.

Iako industrijski standardi definišu osnovni skup uloga u kontekstu dozvoljenih operacija nad uređajima elektroenergetskog sistema, poslovni procesi savremenih elektroenergetskih kompanija obuhvataju znatno širi skup korisničkih uloga koji trenutno nije obuhvaćeno standardima u oblasti Smart Grida.

U drugom delu ovog poglavlja su prikazani zahtevi sa više od dvadeset projekata za Smart Grid u čijoj poslovnoj analizi je autorka rada učestvovala. Osim zahteva da se kontrolom pristupa ograniči pristup resursima u skladu sa korisničkim ulogama u sistemu, kompanije za prenos i distriuciju električne energije uglavnom zahtevaju i raspodelu odgovornosti između korisnika sa istim zaduženjima u cilju efikasnijeg izvršavanja kritičnih operacija. Primenom striktnih mehanizama za kontrolu pristupa kompanije nastoje da smanje mogućnost grešaka validnih korisnika, kao i mogućnost zloupotrebe udaljenog pristupa ili pristupa iz eksternih sistema koji su sastavni deo poslovnih procesa u Smart Gridu. Međutim, svi navedeni zahtevi prevazilaze mogućnosti RBAC modela.

U trećem delu su razmatrane prednosti i nedostaci postojećih modela kontrole pristupa sa aspekta postavljenih zahteva. Analizirani su modeli kontrole pristupa zasnovani na ulogama, zatim model kontrole pristupa zasnovan na atributima, kao i hibridni modeli kontrole pristupa.

Na kraju poglavlja je prikazan model bezbednosne arhitekture za Smart Grid koji je usaglašen sa razmatranim bezbednosnim standardima.

3.1 Bezbednosni zahtevi prema vladajućim standardima

3.1.1 Ciljevi bezbednosti i bezbednosni rizici

Informaciona bezbednost podrazumeva zaštitu poverljivosti, integriteta i raspoloživosti informacija sa ciljem minimizacije pretnji i rizika po informacioni sistem. Kako se Smart Grid sistemi mogu razlikovati sa aspekta kritičnosti procesa i podataka, kao i uticaja bezbednosnih rizika, očuvanje poverljivosti, integriteti i raspoloživosti nije podjednako važno za sve sisteme. U ovoj sekciji su opisani ciljevi bezbednosti Smart Grid informacionih sistema u kontekstu prioriteta CIA trijade. Prioriteti CIA zahteva su diskutovani sa aspekta bezbednosnih rizika i posledica po Smart Grid u slučaju njihovog narušavanja. U nadzorno-upravljačkim sistemima su na prvom mestu rizici od gubitka ljudskih života, oštećenja opreme i ugrožavanje životne sredine, dok se za poslovne sisteme rizici odnose na narušavanje integriteta poslovnih procesa i podataka koje ti procesi obrađuju, kao i otkrivanje poverljivih informacija [24][82].

Raspoloživost

Raspoloživost, odnosno mogućnost ovlašćenih korisnika da pravovremeno pristupaju sistemu i podacima, je kritičan zahtev za procesne i nadzorno-upravljačke sisteme gde je kontinualan rad u realnom vremenu i pravovremeni odgovor na različite događaje u sistemu od ključnog značaja, dok je za poslovne sisteme kašnjenje podataka ili privremena nedostupnost sistema dozvoljena [9][24][81][125]. Zagušenjem komunikacione mreže ili računarskih resursa, napadi poput DoS napada mogu uzrokovati kašnjenje ili gubitak podataka, kao i nedostupnost sistema. Osnovni mehanizmi za zaštitu raspoloživosti su redundancija i primena tehnika za toleranciju otkaza.

Integritet

Integritet se odnosi na tačnost i kompletnost podataka, odnosno nemogućnost neovlašćenih izmena ili brisanja podataka. Napadi na integritet podataka imaju za cilj da izmene podatke ili servise, uzrokujući pritom nepravilno funkcionisanje sistema, donošenje pogrešnih upravljačkih odluka na osnovu netačnih ili nedostupnih podataka, itd. Integritet podataka je podjednako važan za procesne, nadzorno-upravljačke i poslovne sisteme. Neovlašćeno rukovanje operativnim podacima (npr. upravljačke komande, očitane veličine sa mernih uređaja, itd.) može imati negativan uticaj na ispravan i stabilan rad sistema (npr. greške prilikom analize stanja mreže, proračuna, i slično). S druge strane, neovlašćeno rukovanje podacima iz poslovnih sistema može imati negativne posledice za kompaniju, npr. nevalidne izmene podataka o potrošnji prilikom očitavanja brojila ili izmene podataka u sistemima za naplatu potrošnje mogu imati negativan uticaj na prihod kompanije [9][24][81][125]. Osnovni mehanizmi za zaštitu integriteta podataka su heš funkcije, kontrolne sume, kontrole pristupa. Logovanje je

mehanizam kojim se može detektovati narušavanje integriteta i preduzeti adekvatne, zakonom propisane mere.

Poverljivost

Sa aspekta zaštite od neovlašćenog pristupa, čitanja i otkrivanja, podaci se dele na poverljive i tajne. Poverljivi su podaci čije otkrivanje može uzrokovati finansijske gubitke kompanije, smanjenje poverenja korisnika usluga, npr. plate zaposlenih, poverljivi ugovori, podaci o finansijama kompanije, itd. Tajni (privatni) podaci su podaci pojedinca (npr. lični podaci, podaci o finansijskim transakcijama) ili podaci od državnog značaja (npr. vojni podaci) za koje važe strožija pravila o pristupu, ali i kazne u slučaju njihovog otkrivanja. Očivanje poverljivosti je od ključnog značaja za poslovne sisteme gde se skladište podaci o poslovanju kompanije, ali i podaci o potrošačima čije otkrivanje može ugroziti privatnost korisnika. S obzirom da se PII podaci uglavnom ne skladište u nadzorno-upravljačkim sistemima, napadi usmereni na narušavanje njihove poverljivosti nose manje bezbednosne rizike [9][24][81][125]. Osnovni mehanizmi za zaštitu poverljivosti su šifrovanje podataka u toku korišćenja, prenosa i/ili prilikom skladištenja i kontrole pristupa.

3.1.2 Zahtevi za kontrolu pristupa

Danas postoji veliki broj standarda u oblasti bezbednosti informacionih sistema koji definišu zahteve, smernice i preporuke za primenu postojećih i razvoj novih mera bezbednosti. Neki standardi su primenljivi na različite tipove organizacija (ISO/IEC 27000, NIST SP 800-53), neki su namenjeni industrijskim kontrolnim sistemima (NIST SP 800-82, IEC 62351, ISA-99) ili su specifični za određenu industriju (NERC CIP), dok su neki rezultat standardizacije u oblasti informacione bezbednosti u Smart Gridu (NIST SP 1108, NIST IR 7628, ENISA). U ovoj sekciji je dat pregled zahteva, preporuka i smernica koje se odnose na kontrolu pristupa. Dodatno, u cilju razvoja prototipa bezbednosne arhitekture za Smart Grid, razmotreni su zahtevi i dobre prakse za izolaciju Smart Grid komponenti, uključujući i bezbednosne servise.

ISO/IEC 27002

ISO/IEC 27002 standard [50] definiše skup preporuka i dobrih praksi za upravljanje bezbednošću informacija. Sastoji se iz 14 oblasti koje se bave različitim aspektima bezbednosti informacija unutar organizacije: 1) politika bezbednosti, 2) organizacija informacione bezbednosti, 3) informaciona bezbednost sa aspekta ljudskih resursa, 4) upravljanje resursima, 5) kontrola i ograničavanje pristupa, 6) kriptografija, 7) fizička bezbednost, 8) operativna bezbednost, 9) komunikaciona bezbednost, 10) obnavljanje, razvoj i održavanje informacionih sistema, 11) odnosi sa dobavljačima, 12) upravljanje

bezbednosnim incidentima, 13) upravljanje poslovnim kontinuitetom, i 14) usaglašenost politike informacione bezbednosti sa standardima i zakonima.

Kontrola pristupa, odnosno ograničavanje pristupa informacijama zahteva uspostavljanje politike kontrole pristupa u skladu sa poslovnim i bezbednosnim potrebama organizacije, kao i primenu mehanizama za ograničavanje pristupa informacijama i aplikacijama u skladu sa definisanom politikom.

U oblasti bezbedne komunikacije, zahtev za razdvajanjem interne mreže se odnosi na definisanje relativno nezavisnih funkcionalnih celina sa aspekta uređaja, aplikacija i korisnika, i podelu mreže na izolovane segmente čime se postiže viši nivo kontrole saobraćaja između segmenata i smanjuje mogućnost propagacije malicioznih paketa.

NIST SP 800-53

NIST SP 800-53 [84] je specijalna publikacija koja definiše bezbednosne mere za zaštitu državnih informacionih sistema. Bezbednosne mere (kontrole) su organizovane u 18 familija koje se mogu podeliti u tri klase: 1) mere upravljanja: procena rizika, planiranje, sertifikacija, akreditacija i procena bezbednosti, 2) operativne mere: bezbednost zaposlenih, edukacija i obuke zaposlenih, fizička bezbednost, upravljanje konfiguracijom, održavanje, planiranje reakcije i odgovor na incidente, integritet sistema i informacija, 3) tehničke mere: identifikacija i autentifikacija, kontrola pristupa, nadzor sistema, zaštita sistema i komunikacije.

Kontrola pristupa zahteva uspostavljanje i primenu politike i procedura za kontrolu pristupa unutar organizacije u skladu sa zakonima, regulativama, propisima i preporukama. Sprovođenje kontrole pristupa podrazumeva primenu mehanizma za kontrolu pristupa koji treba da bude implementiran u skladu sa politikom kontrole pristupa (npr. kontrola pristupa zasnovana na identitetu, kontrola pristupa zasnovana na korisničkim ulogama, itd.). Politika kontrole pristupa mora biti definisana u skladu sa principom najmanjih privilegija i razdvajanja obaveza. Posebni aspekti kontrole pristupa su udaljeni pristup sistemu i pristup iz spoljašnjih sistema koji nisu u nadležnosti organizacije. Udaljeni pristup je pristup sistemu putem javne mreže (npr. Internet), a eksterni sistemi su sistemi koji nisu u nadležnosti organizacije. Udaljeni pristup mora biti striktno kontrolisan kako sa aspekta očuvanja poverljivosti, integriteta i autentičnosti podataka, tako i sa aspekta nadzora i kontrole udaljene sesije. U situacijama kada je potrebno omogućiti pristup iz eksternih sistema, neophodno je definisati uslove pristupa, pre svega aplikacije kojima je pristup dozvoljen, kategorije informacija koje se mogu slati, obrađivati i skladištiti u eksternim sistemima.

U cilju zaštite integriteta bezbednosnih servisa, ovim standardom se propisuje izolacija bezbednosnih servisa od ostalih funkcija u sistemu. Izolacija podrazumeva formiranje posebnog bezbednosnog domena u okviru koga se nalazi bezbednosni servis i kome može da pristupi mali broj visoko privilegovanih korisnika.

NIST SP 800-82

NIST SP 800-82 [85] sadrži skup preporuka i smernica za zaštitu industrijskih kontrolnih sistema. Preporuke su bazirane na bezbednosnim kontrolama definisanim u SP 800-53, ali su one formulisane u skladu sa specifičnostima industrijskih kontrolnih sistema.

Osnovni zahtev jeste izolovanost kritičnih operacija industrijskog kontrolnog sistema od poslovne mreže. Virtuelna lokalna mreža (eng. *virtual local area network*, skr. *VLAN*) je preporučeni način logičke segmentacije mreže kojim se grupa uređaja koji ne moraju pripadati istoj fizičkoj mreži povezuje u *broadcast* domen. Na ovaj način se poboljšavaju performanse, a pojednostavljuje upravljanje i administracija mrežom. Komunikacija između kontrolne i poslovne mreže ne bi smela da bude direktna, već posredstvom DMZ zone. Preporuka je da se *firewall* uređajima kontroliše saobraćaj između kontrolne i DMZ zone, odnosno između DMZ i poslovne zone po pravilu da se saobraćaj zabranjuje osim ukoliko nije eksplicitno dozvoljen (eng. *deny by default*).

Kontrola pristupa treba da se zasniva da dodeli najmanjeg skupa privilegija u skladu sa zaduženjima korisnika u sistemu. Preporučeni model kontrole pristupa za industrijske kontrolne sisteme koji su sačenjeni od velikog broja inteligentnih elektronskih uređaja je RBAC zbog jednostavnosti administracije i cene implementacije.

IEC 62351

IEC 62351 standard [42] je razvijen sa ciljem da se obezbedi informaciona bezbednost TC57 komunikacionih protokola, kao što su IEC 60870-5, IEC 60870-6 i IEC 61850 [42]. IEC 60870-5 je skup protokola namenjenih za komunikaciju između udaljenih terminalnih jedinica i nadzorno-upravljačkog sistema. Obuhvata protokole ostvarene serijskom vezom (IEC 60870-5-101, -102, -103), kao i TCP/IP bazirane protokole (IEC 60870-5-104, DNP3). IEC 60870-6 je protokol namenjen za razmenu podataka između kontrolnih centara. Poznat je i pod nazivom *Telecontrol Application Service Element.2* (skr. TASE.2) ili *Inter-Control Center Communication Protocol* (skr. ICCP). IEC 61850 je standard namenjen za automatizaciju transformatorskih stanica (skr. TS). Za razliku od IEC 60870-5, IEC 61850 definiše sve aspekte komunikacije u automatizovanim TS (komunikacija inteligentnih elektronskih uređaja koji učestvuju u procesu zaštite, nadgledanja, merenja i upravljanja elektroenergetskog sistema, komunikaciju između TS, kao i komunikacija između TS i kontrolnih centara). IEC 62351 je sastoji iz jedanaest delova koji su opisani u nastavku ove sekcije. Prva dva dela su izostavljena, jer obuhvataju uvod i rečnik termina.

IEC 62351-3 [42] definiše način ostvarivanja bezbednosti za protokole koji se zasnivaju na TCP/IP komunkacionom protokolu (IEC 60870-5-104, IEC 60870-6 i IEC 61850 za TCP/IP). Bezbednosni protokol treba da obezbedi poverljivost i integritet podataka, kao i autentifikaciju učesnika u komunikaciji. Najčešće korišćeni bezbednosni

protokol u savremenim elektroenergetskim sistemima je TLS (eng. *Transport Layer Security*) kojim se obezbeđuje poverljivost podataka primenom simetričnih kriptografskih algoritama. Digitalnim potpisivanjem se obezbeđuje zaštita od presretanja poruka, a autentičnost dvosmernom razmenom sertifikata.

IEC 62351-4 [42] se bavi bezbednošću komunikacionih protokola koji koriste MMS (eng. *Manufacturing Message Specification*) aplikativni protokol (IEC 61850 i IEC 60870-6). TLS se prvenstveno koristi za autentifikaciju učesnika u komunikaciji, dok se ACSE (eng. *Association Control Service Element*) koristi kao protokol za upravljanje komunikacijom između aplikacija koje koriste MMS poruke.

IEC 62351-5 [42] se bavi bezbednošću IEC 60870-5 komunikacionih protokola, uključujući i protokole izvedene iz IEC 60870-5 (npr. DNP3). Bezbednosne mere za IEC 60870-5 za TCP/IP bazirane protokole su definisani IEC 62351-3 standardom, dok se ovim standardom dodatno definišu bezbednosne mere za protokole bazirane na serijskoj vezi (IEC 60870-5-101, -102, -103). S obzirom da su protokoli zasnovani na serijskoj vezi uglavnom bazirani na medijima malog propusna opsega i uređajima slabije procesorske snage, korišćenje složenih kriptografskih algoritama nije prihvatljivo. Jedina bezbednosna mera koja se može primeniti je provera autentičnosti poruka. Poverljivost podataka se može obezbediti korištenjem VPN tehnologije, i slično.

IEC 62351-6 [42] se bavi bezbednošću *peer-to-peer* komunikacionih protokola IEC 61850 koji se koriste u lokalnim mrežama u transformatorskim stanicama. Zbog visokih zahteva sa aspekta performansi, jedina bezbednosna mera koja se može primeniti je provera autentičnosti poruka. IEC 62351-6 definiše mehanizme koji omogućuju digitalno potpisivanje poruka uz minimalne zahteve sa aspekta obrade.

IEC 62351-7 [42] je standard koji se odnosi na upravljanje bezbednošću mreže i sistema. Upravljanje komunikacionom mrežom u elektroenergetskim sistemima se zasniva na SNMP (eng. *Simple Network Management Protocol*) protokolu koji služi za nadzor stanja sistema i mreže.

IEC 62351-8 [42] se odnosi na standardizaciju mehanizma kontrole pristupa u elektroenergetskim sistemima sa ciljem da se obezbedi interoperabilnost između različitih proizvođača. Ovim standardom se propisuje primena RBAC modela za kontrolu pristupa korisnika ili aplikacija objektima elektroenergetskog sistema. Takođe, definisan je osnovni skup korisničkih uloga sa privilegijama definisanim u kontekstu IEC 61850 logičkih uređaja (za svaki fizički uređaj definiše se niz operacija grupisanih u celine tzv. logički uređaji).

IEC 62351-9 se odnosi na upravljanje ključevima i infrastrukturom za upravljanje digitalnim sertifikatima, IEC 62351-10 na bezbednosnu arhitekturu u kontekstu TC57 protokola, a IEC 62351-10 na poverljivost, autentičnost i integritet XML fajlova [42].

IEC 62443

IEC 62443 serija standarda i tehničkih izveštaja se može podeliti u četiri kategorije: 1) opšti pojmovi, koncepti, terminologija i metrike, 2) politike i procedure, 3) sistemski zahtevi i preporuke za bezbednost ICS, 4) tehnički zahtevi za razvoj ICS komponenti. Od interesa za ovu disertaciju su dva standarda iz kategorije sistemskih zahteva i preporuka: IEC 62443-3-2 "Procena bezbednosnih rizika i dizajn sistema" [44] i IEC 62443-3-3 "Bezbednosni zahtevi sistema i nivoi bezbednosti" [45].

IEC-62443-3-2 standard se bavi fizičkom i logičkom separacijom komponenti industrijskih procesnih i kontrolnih sistema u zavisnosti od bezbednosnih zahteva, zatim formiranjem bezbednosnih oblasti, kao i bezbednom razmenom podataka između različitih bezbednosnih oblasti [44]. U skladu sa ovim standardom je definisan model bezbednosnih zona za ICS koji je detaljno objašnjen u *sekciji 2.7.4*.

IEC-62443-3-3 definiše 7 osnovnih bezbednisnih zahteva (eng. *foundational requirements*, skr. *FR*) za industrijske kontrolne sisteme: 1) identifikacija i autentifikacija, 2) kontrola pristupa, 3) integritet sistema, 4) poverljivost podataka, 5) kontrola toka podataka, 6) pravovremeni odgovor na događaje u sistemu, 7) raspoloživost resursa. Za svaki FR se definišu sistemski zahtevi (eng. *system requirements*, skr. *SR*) kojima se propisuju bezbednosne mere za ispunjenje navedenih zahteva [45].

Sprovođenje kontrole pristupa u skladu sa uspostavljenom bezbednosnom politikom je osnovni zahtev za kontrolu pristupa, pri čemu je za izvršavanje kritičnih operacija i pristup osetljivim podacima potrebno omogućiti da samo privilegovani korisnici imaju pravo pristupa. Segmentacija mreže i formiranje bezbednosnih zona je osnovna mera bezbednosti kojom se postiže izolacija različitih podsistema unutar industrijskog kontrolnog sistema.

NERC CIP

NERC CIP [87] je vodeći standard po pitanju pouzdanosti i bezbednosti kritičnih infrastrukturnih sistema. Aktuelna verzija ovog standarda NERC CIP v5 sastoji se iz jedanaest sekcija koje obuhvataju različite aspekte zaštite kritičnih infrastrukturnih sistema, pre svega elektroenergetski sistema (eng. *bulk electric system*, skr. *BES*). Tu spadaju kategorizacija kritičnih resursa (CIP-002), upravljanje bezbednisnim kontrolama (CIP-003), edukacija i obuke zaposlenih (CIP-004), zaštita bezbednosnih perimetara (CIP-005), fizička zaštita BES sistema (CIP-006), mere zaštite kritičnih resursa, ali i drugih (nekritičnih) resursa u okviru bezbednosnog perimetra (CIP-007), planiranje i odgovor na incidente (CIP-008), plan oporavka BES sistema (CIP-009), upravljanje konfiguracijom i procena slabosti (CIP-010), zaštita informacija (CIP-011) [87].

Bezbednosni perimetar je logički skup kritičnih resursa unutar BES sistema. Zaštita bezbednosnih perimetara se odnosi na kontrolu pristupa primenom *firewall* uređaja i

sistema za detekciju i prevenciju upada u mrežu. Kontrola pristupa je deo CIP-003 standarda kojim se zahteva da dokumentovanje i implementacija programa za upravljanje pristupom informacijama sadržanih u okviru kritičnih resursa. To uključuje i spisak korisnika koji su odgovorni za dodelu ovlašćenja za fizički ili logički pristup kritičnim resursima [87].

NIST IR 7628

NIST IR 7628 smernice za informacionu bezbednost 36 su preporuke za primenu bezbednosnih kontrola za 22 kategorije logičkih interfejsa identifikovanih u Smart Gridu. Kategorije logičkih interfejsa su grupe Smart Grid učesnika grupisane prema CIA zahtevima, računskim zahtevima i ograničenjima u pogledu propusnog opsega. Bezbednosne kontrole su definisane u skladu sa NIST SP 800-53 standardom za bezbednost informacionih sistema, uz odgovarajuća prilagođenja za specifičnosti Smart Grida.

Sa aspekta kontrole pristupa, zahtevi i bezbednosne kontrole sa kojima Smart Grid sistem treba da bude usklađen se odnose na uspostavljanje politike i procedura za kontrolu pristupa unutar organizacije. Dodatno, potrebno je uspostaviti i politiku i procedure za udaljeni pristup. Ovim standadom se proposuje da mehanizam kontrole pristupa treba da bude u skladu sa uspostavljenom bezbednosnom politikom, pri čemu je u vanrednim situacijama dozvoljeno da ovi mehanizmi budu izmenjeni ili poništeni.

Zahtevi za razdvajanjem obaveza, dodelom najmanjeg skupa privilegija, udaljeni pristup, pristup iz eksternih sistema, kao i izolovanost bezbednosnih funkcija za Smart Grid su definisani prema SP 800-53. Dodatni zahtev za Smart Grid propisan NIST IR 7628 standardom je da pristup kontrolnom sistemu treba da bude ograničen iz poslovne mreže organizacije.

ENISA

U dokumentu “Odgovarajuće mere bezbednosti za Smart Grid“ [25], ENISA daje smernice u vidu minimalnog skupa bezbednosnih mera koje je potrebno implementirati u Smart Gridu. Bezbednosne mere su podeljene u 10 domena: 1) upravljanje bezbednošću i rizicima, 2) bezbednosne mere u interakciji sa trećim licima, 3) operativne procedure, konfiguracija i održavanje Smart Grid sistema, 4) bezbednost zaposlenih, edukacija i obuke, 5) odgovori na incidente, 6) nadzor sistema, 7) kontinuitet u radu sistema, 8) fizička zaštita, 9) bezbednost informacionih sistema, 10) bezbednost mreže.

Prema ovom standardu, u domenu bezbednosti informacionih sistema kontrola pristupa se odnosi na zaštitu Smart Grid informacionih sistema od neovlašćenog pristupa, kao i na bezbedan udaljeni pristup Smart Grid sistemu kako sa aspekta zaštićene

komunikacije tako i dobrih praksi u pogledu neaktivnih konekcija, mogućnosti automatskog prekida konekcija, i slično.

U domenu zaštite mreže, preporučene bezbednosne mere su razdvajanje interne mreže Smart Grida na izolovane segmente, kao i bezbedna komunikacija između različitih segmenata.

3.1.3 Mapiranje standarda na zahteve za kontrolu pristupa

U *Tabeli 2.* je dat pregled zahteva za kontrolu pristupa mapiranih na zahteve i preporuke bezbednosnih standarda. Standardima se uglavnom ne propisuje primena određenog modela kontrole pristupa. Umesto toga, standardi su orijentisani na zahteve koje modeli za kontrolu pristupa treba da ispune i pravila koja ne smeju biti narušena (npr. princip najmanjih privilegija i razdvajanje obaveza), dok je izbor konkretnog modela kompromis između bezbednosne politike organizacije i mogućnosti modela da odgovori postavljenim zahtevima. Izuzetak su standardi za industrijske kontrolne sisteme koji propisuju primenu RBAC modela zbog jednostavnosti administracije i troškova implementacije u sistemima koje karakteriše veliki broj uređaja koje je potrebno zaštititi.

U *Tabeli 3.* su date preporuke za implementaciju bezbednosne arhitekture za Smart Grid. Segmentacija mreže je osnovni mehanizam za logičko razdvajanje komponenti prema njihovoj kritičnosti za pouzdan rad elektroenergetskog sistema. Preporuka industrijskih standarda za implementaciju segmentacije fizičke mreže su VLAN-ovi. Komunikacija između VLAN-ova treba da bude strogo kontrolisana *firewall* uređajima koji su konfigurisani prema principu najmanjih privilegija, a za kontrolu toka podataka između različitih zona treba koristiti DMZ. Bezbednosni servisi treba da budu posebno izolovani od ostalih Smart Grid komponenti kako bi se obezbedio integritet servisa.

Tabela 2. S.AC.[1] Mapiranje standarda na zahteve za kontrolu pristupa

Zahtev za kontrolu pristupa	Zahtevi i preporuke standarda
S.AC.1. Uspostavljanje politike i procedura kontrole pristupa. Potrebno je uspostaviti politiku i procedure kontrole pristupa u skladu sa poslovnim i bezbednosnim potrebama organizacije. Politika kontrole pristupa treba da definiše koji korisnici mogu pristupiti kojim resursima u sistemu. To uključuje i spisak korisnika odgovornih za dodelu ovlašćenja za pristup kritičnim resursima.	**ISO/IEC 27002** 9.1.1 Develop a policy to control access to information **NIST SP 800-53** AC-1 Access control policy and procedures **NIST IR 7628** SG.AC-1 Access control policy and procudures **NIST IR 7628** SG.AC-2 Remote access policy and procedures
S.AC.2. Implementacija mehanizma za kontrolu pristupa. Implementacija mehanizma za kontrolu pristupa treba da bude u skladu sa autorizacionom politikom organizacije (npr. politika zasnovana na korisničkim ulogama, na identitetu korisnika, itd.). Industrijska preporuka je primena RBAC modela. Posebno je potrebno razmotriti vanredne situacije kada treba pružiti mogućnost izmene ili isključivanja bezbednosne politike kako ne bi bio ugrožen pouzdan i siguran rad sistema.	**ISO/IEC 27002** 9.4.1 Restrict access to information and applications **NIST SP 800-53** AC-3 Access enforcement **NIST SP 800-82** 6.2.1.1 Role-based access control (RBAC) **IEC 62351-8** Role-based access control for power system management **IEC-62443-3-2** FR.2 Use control, SR.2.1 Access enforcement **NERC CIP-003 R5** Access Control **NIST IR 7628** SG.AC-4 Access Enforcement **ENISA** SM.9.3. Logical access control
S.AC.3. Razdvajanje obaveza Kontrola pristupa mora biti definisana u skladu sa principom razdvajanja obaveza.	**NIST SP 800-53** AC-5 Separation of duties **NIST IR 7628** SG.AC-6 Separation of Duties
S.AC.4. Princip najmanjih privilegija Kontrola pristupa mora biti definisana u skladu sa principom najmanjih privilegija.	**NIST SP 800-53** AC-6 Least privilege **NIST IR 7628** SG.AC-7 Least Privilege

[1] S.AC = standard.access control

Tabela 3. S.SA.[2] Mapiranje standarda na zahteve za bezbednosnu arhitekturu Smart Grida

Zahtev za kontrolu pristupa	Zahtevi i preporuke standarda
S.SA.1. Segmentacija mreže Segmentacija mreže i formiranje bezbednosnih zona je osnovna mera bezbednosti kojom se postiže izolacija različitih komponenti Smart Grida. Kriterijum za grupisanje komponenti je kritičnost za pouzdan rad elektroenergetskog sistema, ali i posledice koje bezbednosni incidenti mogu imati (npr. kontrolni sistem i poslovni sistem). Preporuka industrijskih standarda za implementaciju segmentacije fizičke mreže su VLAN-ovi. Komunikacija između VLAN-ova treba da bude strogo kontrolisana firewall uređajima koji su konfigurisani prema principu najmanjih privilegija, a za kontrolu toka podataka između različitih zona treba koristiti DMZ. Bezbednosni servisi treba da budu posebno izolovani od ostalih Smart Grid komponenti.	**ISO/IEC 27002** 13.1.3 Use segregation to protect networks **NIST SP 800-82** 5.1. Network segmetation and segregation **NIST SP 800-82** 5.4 Logically Separated Control Network **IEC-62443-3-2** FR.5 Restricted data flow, SR.5.1 Network segmentation **IEC-62443-3-3** Security levels for zones and conduits **NERC CIP-005 R2** Electronic Access Control **ENISA** SM 10.1 Secure network segregation **NIST SP 800-82** 6.2.1.3 Virtual Local Area Network (VLAN) **NIST SP 800-53** SC-3 Security function isolation **NIST IR 7628** SG.SC-3 Security Function Isolation
S.SA.2. Kontrola toka podataka. Neophodno je obezbediti kontrolisan tok podataka između bezbednosnih zona, uključujući i komunikaciju sa eksternim sistemima i pristup sistemu sa udaljenih lokacija. Kontrolisan tok podataka podrazumeva integritet i poverljivost podataka, ali i kontrolu izvora i odredišta podataka. U situacijama kada je potrebno omogućiti pristup iz eksternih sistema, neophodno je definisati uslove pristupa, pre svega aplikacije kojima je pristup dozvoljen, kategorije informacija koje se mogu slati, obrađivati i skladištiti u eksternim sistemima, korisnike kojima pristup treba da bude dozvoljen.	**NIST SP 800-53** AC-4 Information flow enforcement **NIST IR 7628** SG.AC-5 Information Flow Enforcement **NIST IR 7628** SG.AC-19 Control System Access Restrictions **ENISA** SM.10.2. Secure network communications **NIST SP 800-53** AC-17 Remote access **NIST IR 7628** SG.AC-15 Remote Access **ENISA** SM.9.4. Secure remote access **NIST SP 800-53** AC-20 Use of external information systems **NIST IR 7628** SG.AC-18 Use of External Information Control Systems

[2]S.SA = standard.security architecture

3.2 Zahtevi sa stanovišta kontrole pristupa u elektroenergetskim sistemima

Uzimajući u obzir heterogeno, distribuirano Smart Grid okruženje koje karakteriše visok stepen dinamičnosti i nepredvidivosti, u radovima [4][20] se ističe da bilo kakav propust prilikom upravljanja uređajima i opremom može da destabilizuje i ugrozi rad celokupnog sistema. Stoga, elektroenergetske kompanije sve češće stavljaju pred proizvođače Smart Grid rešenja specifične zahteve za kontrolu pristupa kako bi se obezbedila ne samo zaštita od neovlašćenog pristupa, već i smanjili rizici od nenamernih grešaka validnih korisnika.

3.2.1 Tipovi korisničkih uloga i zaduženja u Smart Gridu

Smart Grid karakteriše veliki broj korisnika koji su uključeni u različite poslovne procese unutar organizacije. U ovoj sekciji su opisane tipične korisničke uloge i zaduženja u Smart Grid okruženju.

Korisničke uloge u kontrolnoj sobi

Operater (eng. operator) ili dispečer je zadužen za upravljanje elektroenergetskom mrežom. Osim za klasične SCADA funkcionalnosti (nadzor i komandovanje u sistemu, obrada alarma), operateri su odgovorni za upravljanje planiranim i neplaniranim aktivnostima u sistemu, što podrazumeva pravljenje sekvenci manipulacija prekidačkom opremom (eng. switching sequence), validaciju kreiranih sekvenci i njihovo izvršavanje. Može se praviti razlika između operatera prenosnog sistema i operatera distributivnog sistema kako sa aspekta delova elektroenergetske mreže kojom mogu upravljati, tako i sa aspekta licence koju operater mora da ima kako bi imao pravo da upravlja sistemom.

Supervizor (eng. *supervisor*) je zadužen da nadgleda i koordiniše aktivnosti operatera. Iako sa aspekta privilegija mogu da izvršavaju sve operaterske aktivnosti, supervizori najčešće preuzimaju odgovornost upravljanja elektroenergetskom mrežom samo u vanrednim situacijama. Dodatno, supervizor ima dodatna ovlašćenja, npr. da izmeni konfiguraciju sistema, npr. izvrši transfer kontrole sa primarnog na rezervni sistem u nepredviđenim situacijama.

Inženjer za podršku u kontrolnoj sobi (eng. *control room support engineer*) upravlja analitičkim funkcijama i proračunima u elektoenergetskoj mreži, npr. podešavanje parametara funkcija, pokretanje funkcija i tumačenje njihovih rezultata, pomoć operatorima, itd.

Korisničke uloge za upravljanje operacijama na terenu

Članovi posade (eng. *crew members*) su odgovorni za izvršavanje planiranih operacija, ali i izvršavanje akcija u slučaju neplaniranih događaja i ispada na terenu. Članovi posade pristupaju sistemu sa udaljenih lokacija za ažuriranje statusa izvršenih instrukcija sa terena, ali i kako bi imali uvid u trenutno stanje elektroenergetske mreže i telemetrijske podatke. Obavljanje poslova na terenu je najčešće regulisano važećom licencom koju korisnici koji su članovi posade moraju posedovati.

Dispečer posade (eng. *workforce dispatcher*) koordiniše i prati rad članova posade na terenu.

Korisničke uloge u poslovnom sistemu

Korisničke uloge u poslovnom sistemu se mogu podeliti u dve grupe. Prvu grupu čine inženjerske korisničke uloge, a drugu grupu korisničke uloge namenjene za upravljanje poslovnim procesima kompanije. Svi korisnici u poslovnom sistemu su ograničeni na izvršavanje zadataka koji nemaju uticaj na produkcioni sistem, osim određenih visoko privilegovanih korisnika.

Projektant mreže (eng. *grid planning engineer*) se bavi studijama planiranja izgradnje i proširenja elektroenergetske mreže. Sistem inženjer (eng. *switching planning engineer*) se bavi studijama i analizama u cilju optimizacije rada elektroenergetske mreže, i pravi planove za izmenu parametara funkcija ili za manipulaciju prekidačkom opremom. Ovi korisnici nemaju ovlašćenje za primenu napravljenih planova u produkcionom sistemu, već planovi moraju biti odobreni od strane ovlašćenih korisnika u kontrolnoj sobi.

SCADA inženjer (eng. *SCADA Engineer*) i Model inženjer (eng. *Model Engineer*) su zaduženi za testiranje i verifikaciju izmena konfiguracije uređaja i modela elektroenergetskog sistema pre primene u produkciji. SCADA inženjer je odgovoran za konfigurisanje novih ili rekonfigurisanje postojećih RTU tačaka u sistemu i njihovo testiranje, dok je Model inženjer odgovoran za testiranje izmena modela elektroenergetske mreže (npr. parametri uređaja i njihova međusobna povezanost, konektivnost u normalnom uklopnom stanju). Za primenu verifikovanih izmena modela u produkciji neophodna su dodatna ovlašćenja koja imaju visoko privilegovani SCADA inženjer i Model inženjer. Visoko privilegovani SCADA inženjer se još naziva i SCADA administrator (eng. *SCADA Admin*), dok se visoko privilegovani Model inženjer naziva Model koordinator (ili Koordinator ažuriranja izmena modela) (eng. *Model Coordinator*).

Upravljanje poslovnim procesima kompanije obuhvata širok spektar korisničkih uloga. Za potrebe ove disertacije su izdvojene dve tipične korisničke uloge, predstavnik korisničke službe i poslovni menadžer. Predstavnik korisničke službe (eng. *Customer Service Representative*) je zadužen za upravljanje odnosima sa potrošačima kako bi se efikasno odgovorilo zahtevima i potrebama klijenata. To obuhvata podršku za poslovne

procese (npr. zaključenje ugovora između potrošača i elektrodistributivne kompanije prilikom priključivanja na distributivnu mrežu), ali i različite analize podataka o potrošačima u cilju poboljšanja kvaliteta usluga za krajnje potrošače.

Poslovni menadžer (eng. *Business Manager*) ima ulogu u okviru finansijskog sektora kompanije, za razliku od predstavnika korisničke službe koji su deo sektora prodaje i marketinga.

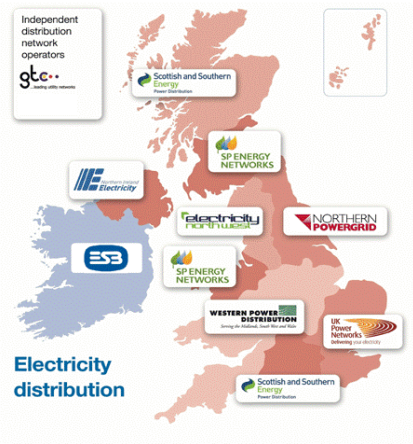
3.2.2 Kontrola pristupa prema oblastima odgovornosti

Proces deregulacije u industriji električne energije uticao je na uvođenje konkurencije u određene segmente poslovanja i razdvajanje aktivnosti kojima se bave elektroprivredne kompanije [57]. Na deregulisanim tržištima, podsistemi za proizvodnju, prenos i distribuciju električne energije su u vlasništvu različitih kompanija. Takođe, upravljanje, izgradnja i održavanje određenih delova elektroenergetskog sistema može biti u nadležnosti različitih entiteta [4][20][57].

Delatnost prenosa podrazumeva prenos električne energije od proizvođača do distributera ili krajnjih potrošača putem visoko-naponske mreže [118]. Unutar jedne države, vlasništvo prenosne mreže može biti podeljeno između više prenosnih kompanija koje su zadužene za održavanje i proširenje mreže, dok je za upravljanje prenosnom mrežom odgovoran operator prenosnog sistema (eng. *Transmission System Operator*, skr. *TSO*). Licencu TSO može imati prenosna kompanija, ali tu ulogu može obavljati i nezavisna organizacija [20][57]. S obzirom da se prenosni sistemi na nivou jedne države, ali i više susednih država povezuju u jedinstven prenosni sistem kako bi rezerve proizvodnje električne energije bile svedene na minimum, neophodno je obezbediti mogućnost nadzora svih prenosnih sistema koji učestvuju u interkonekciji od strane svih TSO [118]. Na *Slici 7.*6. je dat primer prenosnog sistema Velike Britanije koji je u vlasništvu tri prenosne kompanije, a svaka kompanija ima i licencu operatora prenosnog sistema [79][89].

Distribucija podrazumeva transport električne energije od prenosne mreže do krajnjih potrošača putem srednje-naponske i nisko-naponske mreže [118]. Distributivna mreža jedne države je podeljena na distributivne oblasti odakle se električna energija raspodeljuje do manjih potrošačkih područja, sve do krajnjih potrošača. Unutar jedne države, vlasništvo distributivne mreže može biti podeljeno između više distributivnih kompanija koje su zadužene za izgradnju, održavanje i upravljanje distributivnom mrežom na određenoj teritoriji, pri čemu jedna distributivna kompanija (eng. *Distribution System Operator*, skr. *DSO*) može biti zadužena za više distributivnih oblasti [20][57]. Na *Slici 8.* je dat primer distributivne mreže Velike Britanije koja je podeljena na četrnaest distributivnih oblasti koje su u nadležnosti šest DSO [78][88].

Slika 7. Prenosna mreža Velike Britanije [34]

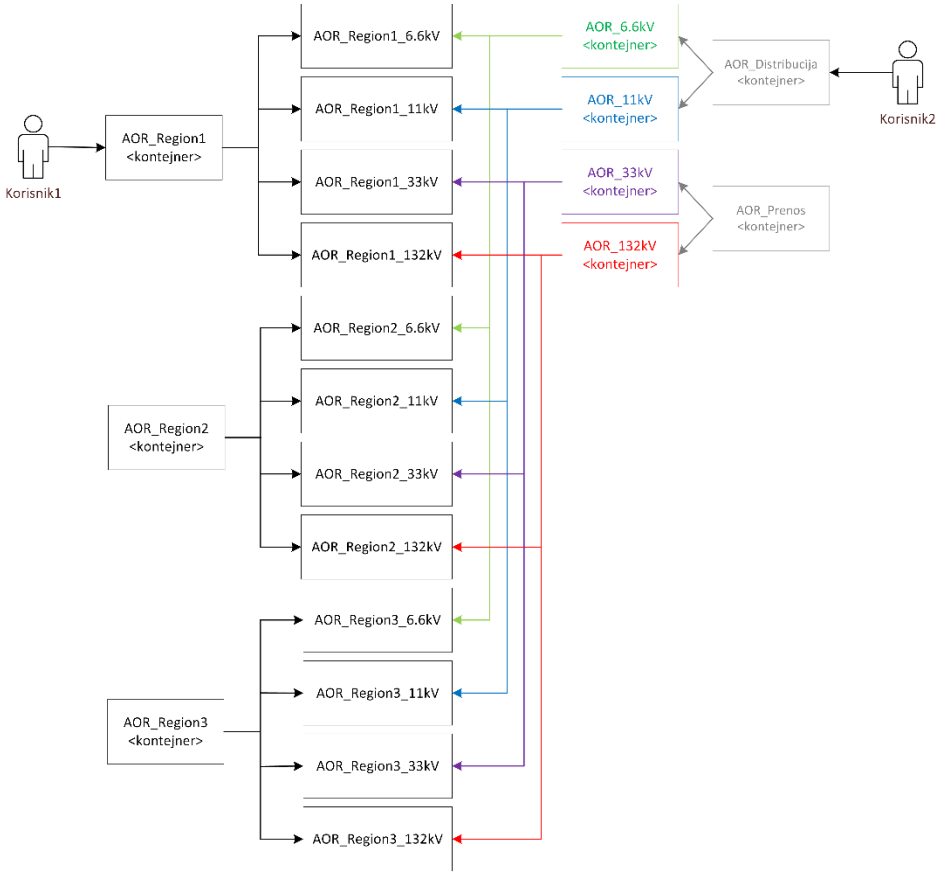


Slika 8. Distributivna mreža Velike Britanije [34]

Osim raspodele odgovornosti između različitih kompanija sa aspekta izgradnje/održavanje i upravljanja različitim oblastima u okviru elektroenergetske mreže, kompanije za prenos i distribuciju električne energije zahtevaju i raspodelu odgovornosti prema manjim oblastima unutar svojih informacionih sistema. Naime, savremeni elektroenergetski sistemi sadrže stotine hiljada uređaja i opreme i najmanji propust ili greška prilikom upravljanja može imati katastrofalne posledice [103][104]. Kako bi se obezbedilo pouzdano, efikasno i kvalitetno obavljanje poslova nadzora, upravljanja i razvoja elektroenergetske mreže, kompanije zahtevaju mogućnost razdvajanja zaduženja i odgovornosti korisnika koji pripadaju istim korisničkim ulogama prema manjim oblastima u njihovoj nadležnosti. Pritom, za svaku oblast odgovornosti se definiše nivo odgovornosti u zavisnosti od skupa dozvoljenih operacija nad objektima unutar date oblasti. U ovom radu su razmatrane operacije u okviru nadzorno-upravljačkih sistema i u tom kontekstu su identifikovani sledeći tipovi operacija: nadzorne operacije, upravljačke operacije i operacije ažuriranja modela elektroenergetskog sistema. Operacije u okviru poslovnih sistema su van okvira ovog rada.

Kriterijum za podelu odgovornosti može biti geografska raspodela ili podela mreže prema naponskim nivoima. Geografska raspodela podrazumeva podelu mreže na geografske regione i okruge (podregione), ali se često zahtevaju i granularnije podele kao što je podela na nivou transformatorskih stanica, zatim grupisanje elemenata unutar transformatorske stanice, sve do nivoa pojedinačnih elemenata elektroenergetskog sistema. Takođe, često se zahteva podela odgovornosti prema oba kriterijuma. Na *Slici 9.* je dat sledeći primer: prema geografskoj raspodeli mreže su definisana tri regiona: region1, region2 i region3, a svaki region se zatim može podeliti na prenosni deo

(naponski nivoi 132kV i 33kV) i distributivni deo (11kV i 6.6kV). Međutim, moguće je da određeni elementi elektroenergetskog sistema istovremenu budu deo različitih oblasti odgovornosti, npr. objekti delovi transformatorskih stanica koji se nalaze na granici između visoko-naponske prenosne mreže i srednje-naponske distributivne mreže.



Slika 9. Primer hijerarhije AOR-a

Operateri u kontrolnoj sobi su najčešće organizovani tako da svaki upravlja samo određenim delom elektroenergetske mreže, pri čemu svaki deo mreže mora konstantno biti pod nadzorom i kontrolom najmanje jednog operatera. To znači da operater ne bi smeo da prekine korisničku sesiju ukoliko to uzrokuje da neki AOR ostane bez nadzora i kontrole. Odavde proizilazi zahtev za mogućnošću preuzimanja odgovornosti nad delovima mreže koji su pod kontrolom drugih operatera u kontrolnom centru, npr. za vreme pauze u toku radnog vremena, prilikom smene operatera, i slično. Najčešće se operaterima prema određenom kriterijumu dodeljuje skup AOR-a kojima imaju pravo da upravljaju, a prilikom uspostavljanja korisničke sesije svaki operater aktivira samo podskup dodeljenih AOR-a, dok se deaktivirani AOR-i aktiviraju u skladu sa regularnim aktivnostima operatera u kontrolnoj sobi.

Uzimajući u obzir prethodno navedeni zahtev, kompanije za prenos i distribuciju električne energije zahtevaju hijerarhijsku strukturu AOR-a za potrebe efikasnije administracije i smanjenja broja oblasti odgovornosti koje je potrebno dodeliti korisnicima. Hijerarhijska struktura podrazumeva uvođenje dodatnih AOR-a, tzv. AOR kontejneri (eng. *AOR containers*), koji služe za grupisanje definisanih oblasti odgovornosti prema određenom kriterijumu. Radi ilustracije, dat je primer podele elektroenergetske mreže prema geografskoj podeli i prema naponskom nivou. Na *Slici 9.* su dati primeri tipičnih AOR kontejnera u takvoj situaciji. Korisniku *korisnik1*, koji treba da ima pravo upravljanja distributivnom mrežom jednog regiona, umesto dodele 4 AOR-a biće dodeljen samo jedan AOR, npr. *AOR_Region1*. Korisniku *korisnik2*, koji treba da ima mogućnost upravljanja celokupnom distributivnom mrežom, umesto dodele 6 pojedinačnih AOR-a biće dodeljen jedan *AOR_Distribucija*.

Uzimajući u obzir visok stepen dinamičnosti i nepredvidivosti koji karakteriše elektroenergetske sisteme, zahtev koji se stavlja pred Smart Grid je i mogućnost delegiranja odgovornosti u vanrednim situacijama od strane ovlašćenih korisnika kako bi se obezbedilo efikasnije upravljanje mrežom, npr. u slučaju oluje kada je potrebno da više korisnika istovremeno preuzme kontrolu nad sistemom, u slučaju otkaza radnih stanica ili nedostupnosti regionalnog centra kada su korisnici onemogućeni da nadziru i upravljaju određenim delom mreže.

3.2.3 Kontrola pristupa prema aplikativnom kontekstu

Proces modernizacije, razvoj tehnologija i otvoreno tržište električne energije nameću i nove zahteve u pogledu upravljanja i planiranja elektroenergetskim mrežama. SCADA sistemi se integrišu sa sistemima za podršku u odlučivanju (npr. NMS, EMS, DMS, OMS) u cilju poboljšanja procesa upravljanja elektroenergetskom mrežom u realnom vremenu [74][113][121]. Na primer, jedna od namena DMS sistema je izvršavanje analitičkih elektroenergetskih funkcija na osnovu podataka iz distributivne mreže. Na osnovu rezultata proračuna DMS funkcija i estimiranih vrednosti stanja elektroenergetske mreže operateri u kontolnom centru mogu znatno lakše da donose upravljačke odluke [118]. Takođe, korišćenjem sistema za podršku u odlučivanju van realnog vremena moguće je simulirati rad elektroenergetske mreže u željenim uslovima. Dva tipična slučaja korišćenja simulacije u Smart Gridu su: 1) "šta-ako" analize za predviđanje rezultata planiranih akcija u sistemu npr. manipulacija uređajima i opremom, optimizacija rada mreže, 2) studije i predviđanja ponašanja sistema na osnovu događaja iz prošlosti. Na primer, operateri u kontrolnoj sobi sa iste radne stanice upravljaju sistemom u realnom vremenu i izvršavaju "šta-ako" analize kako bi bili sigurni da su doneli ispravne upravljačke odluke [96][97]. Takođe, inženjeri za podršku u kontrolnoj sobi mogu koristiti simulacione sisteme za analizu rada elektroenergetskog sistema, npr. analiza nivoa opterećenja, kvaliteta napona, itd.

Funkcionisanje DMS sistema se oslanja na model elektroenergetske mreže kojom upravljaju, jer tačnost modela podataka utiče na kvalitet estimacije stanja mreže, a time

i na proračune niza upravljačkih akcija koje sistem treba da dovedu u željeni režim. Stoga, proces ažuriranja modela mreže zahteva testiranje i verifikaciju izmena pre primene nove verzije modela produkcionom sistemu kako bi se izbegle greške sistema za rad u realnom vremenu. Za to se koriste sistemi za proveru kvaliteta nove verzije modela koji rade van realnog vremena, ali se zasnivaju na trenutnom stanju sistema. Izmene modela se mogu dobiti integracijom sa drugim sistemima (npr. GIS) ili na zahtev korisnika prema određenom planu. Pre bilo kakvih izmena modela (npr. usled proširenja distributivne mreže) neophodne su analize uticaja planiranih izmena na rad sistema od strane projektanta mreže. Za te potrebe se koriste sistemi za planiranje koji služe za simulaciju proširenja elektroenergetske mreže i analizu uticaja planiranih izmena na rad sistema.

Članovi posade, odnosno ekipe koje izvode planirane, ali i neplanirane radove na terenu, moraju imati uvid u trenutno stanje elektroenergetske mreže, kao i mogućnost ažuriranja statusa izvršenih instrukcija sa terena u cilju povećanja efikasnosti izvršavanja operacija, ali i bezbednosti članova posade. S obzirom da oni ne smeju imati direktan pristup sistemu u kontrolnoj sobi, za ovu namenu se koriste sistemi za podršku operacijama na terenu.

Većina elektroenergetskih kompanija u svetu danas bazira svoje poslovne procese na prethodno opisanim tipovima Smart Grid sistema. Osim različite namene ovih sistema razlikuju se i zahtevi u pogledu raspoloživosti, integriteta i poverljivosti podataka koji se obrađuju i skladište u njima. Shodno tome, identifikovani su sledeći tipovi Smart Grid sistema (tzv. Smart Grid aplikativni konteksti) za koje treba da važe različite bezbednosne politike:

- **Aplikacije za rad u realnom vremenu** (eng. *real-time context*), odnosno integrisani SCADA/NMS/EMS/DMS/OMS sistemi namenjeni za nadzor i upravljanje elektroenergetskom mrežom u realnom vremenu. Ove aplikacije karakterišu visoki zahtevi za pouzdanost i raspoloživost čije narušavanje može imati posledice po stabilan rad elektroenergetskog sistema. Stoga, za ove aplikacije treba da važe najstroža pravila u pogledu prava pristupa, odnosno mogućnost pristupa samo unutar interne mreže i dodela minimalnog skupa privilegija potrebnih za izvršavanje zadataka.
- **Aplikacije za simulaciju rada sistema** (eng. *real-time simulation context*) su sistemi za podršku operaterima i inženjerima u kontrolnoj sobi. Mogu se nalaziti i u poslovnom sistemu, gde ih koriste inženjeri sistema za potrebe pravljenja planova manipulacije prekidačkom opremom. Predstavljau izolovane sisteme koji rade nad replikom podataka iz produkcionog sistema, bez uticaja na rad sistema u realnom vremenu. Odavde proizilazi da u poređenju sa aplikacijama za rad u realnom vremenu, korisnici mogu imati viši nivo privilegija u poređenju sa sistemima za rad u realnom vremenu.
- **Aplikacije za planiranje izgradnje i održavanja elektroenergetskog sistema** (eng. *planning context*) omogućuju simulaciju proširenja mreže i analizu uticaja planiranih izmena na rad sistema. Slično sistemima za simulaciju, sistemi za planiranje su izolovani i nemaju uticaj na rad sistema u realnom

vremenu. Međutim, za njih važi drugačija bezbednosna politika sa aspekta korisnika koji imaju pravo pristupa. Naime, ovi sistemi su namenjeni isključivo za pristup korisnika koji su projektanti mreže.

- **Aplikacije za testiranje i potvrdu kvaliteta** (eng. *quality assurance (QA) context*) su namenjene za testiranje izmena u sistemu pre njihove primene u produkciji. Potvrda kvaliteta se odnosi na testiranje i validaciju izmena modela elektroenergetskog sistema, kao i konfiguraciju novih ili rekonfiguraciju postojećih RTU uređaja u sistemu. Međutim, u opštem slučaju se to odnosi i na izmene i ažuriranje operativnog sistema i softvera. Ove aplikacije su namenjene za rad van realnog vremena, ali se baziraju na replici podataka iz produkcije. U poređenju sa simulacionim sistemima, operacije koje se izvršavaju u okviru QA konteksta mogu da ugroze rad produkcionog sistema, npr. promovisanjem nekorektnih izmena modela. Stoga, u okviru ovih aplikacija moraju da važe strože bezbednosne politike kada je u pitanju izvršavanje kritičnih operacija što je u ovom slučaju izmena modela mreže.
- **Aplikacije za podršku operacijama na terenu** (eng*. field operations context*) su aplikacije namenjene za pristup sistemu od strane korisnika koji upravljaju radovima na terenu. Naime, članovi posada moraju da imaju uvid u trenutno stanje elektroenergetske mreže, kao i mogućnost ažuriranja statusa izvršenih instrukcija sa terena. Kako pristup nadzorno-upravljačkom sistemu ne sme biti omogućen sa udaljenih lokacija, uvodi se poseban tip aplikacija koje su smeštene u poslovnom sistemu, a posredstvom kojih članovi posade mogu obavljati zadatke bez mogućnosti pristupa sistemu u kontrolnoj sobi.
- **Poslovne aplikacije** (eng. *business application context*). U domenu Smart Grida, poslovne aplikacije se odnosi na sisteme za upravljanje poslovnim procesima kompanije skladištene u poslovnom Smart Grid sistemu. U njima se mogu skladištiti poverljivi poslovni podaci i podaci o korisnicima. Bezbednosni zahtevi poslovnih sistema su van okvira ove disertacije te se neće posebno razmatrati. U ovoj disertaciji su istaknuti sa ciljem da se ukaže na značaj razdvajanja obaveza u poslovnom sistemu u zavisnosti od tipa podataka koji se tu mogu skladištiti.

3.2.4 Kontrola pristupa prema lokaciji radne stanice

S obzirom na sve veći broj pristupnih tačaka Smart Grid sistemu kako bi se omogućila razmena podataka između različitih Smart Grid komponenti, kao i pristup korisnika različitim Smart Grid aplikacijama, lokacija ili namena radne stanice sa koje korisnik pristupa sistemu predstavlja bitan aspekat prilikom donošenja odluke o pristupu resursima. Poseban izazov predstavlja mogućnost pristupa sistemu preko javne mreže ili sa nepoznate lokacije. Uzimajući u obzir lokaciju ili namenu radne stanice sa koje je moguće pristupiti sistemu, identifikovani su sledeći tipovi radnih stanica u Smart Gridu:

- Radne stanice u kontrolnoj sobi (eng. *Control Room workstations*) za koje se definišu strože bezbednosne politike u odnosu na radne stanice smeštene u drugim sistemima. Osim specifičnog skupa privilegija neophodnih za izvršavanje

nadzorno-upravljačkih funkcija, bezbednosne politike često podrazumevaju i kompleksnije lozinke prilikom autentifikacije, više-faktorsku autentifikaciju, zaključavanje radnih stanica kada nema aktivnosti određeni period vremena, itd.

- Radne stanice u poslovnom okruženju koje mogu biti inženjerske ili poslovne. Inženjerske radne stanice (eng. *Engineering workstations*) su namenjene za različite simulacije i planiranje razvoja elektroenergetskog sistema, dok su poslovne radne stanice (eng. *Enterprise workstations*) namenjene za pristup poslovnim i administrativnim podacima kompanije. Pristup aplikacijama i podacima nadzorno-upravljačkog sistema je omogućen samo na nivou čitanja, npr. čitanje vrednosti merenja ili statusa opreme, čitanje istorije podataka. Zbog potrebe za obradom podataka koji mogu doći integracijom sa drugim sistemima (npr.GIS, CIS), ove radne stanice ne bi smele da se nalaze u nadzorno-upravljačkom sistemu.
- Udaljene radne stanice (eng. *Remote consoles*). Udaljeni pristup se odnosi na pristup Smart Grid informacionom sistemu putem mobilnih uređaj, tableta preko javne mreže, laptopa sa VPN konekcijom [84]. Primeri udaljenog pristupa sistemu u Smart Gridu su: pristup operativnim podacima od strane članova posade, pristup poslovnim podacima od strane korisnika koji upravljaju poslovnim procesima kompanije ili krajnjih potrošača. Napad u Ukrajini, kada su napadači samo kompromitovanjem naloga operatera uspostavili udaljeni pristup radnim stanicama u kontrolnoj sobi i izdavali komande za isključenje delova elektrodistributivne mreže, jasno ukazuje na značaj kontrole pristupa sa udaljenih lokacija.

3.2.5 Kontrola pristupa u interorganizacionim sistemima

Razvoj informacionih tehnologija i pojava Interneta doneli su suštinske promene u načinu poslovanja, uključujući i interorganizacione poslovne procese kada kompanije deo svog poslovnog procesa poveravaju drugim organizacijama ili omogućuju pristup podacima koji su od interesa za sve učesnike u interorganizaciji. Za savremene elektroenergetske kompanije je tipičan B2B (eng. *business-to-business*) način poslovanja kada kompanije poveravaju deo svog poslovnog procesa partnerskim kompanijama. Npr. čest je slučaj da elektroenergetska kompanija angažuje druge kompanije za izvršavanje radova na terenu i upravljanje članovima posade. U takvim situacijama, jedno od ključnih pitanja je na koji način obezbediti kontrolu pristupa resursima jedne organizacije od strane korisnike iz partnerskih organizacija. Jedan pristup u rešavanju problema kontrole pristupa na ovom polju jeste da svaka kompanija vodi računa o pravima svih korisnika kojima pristup treba da bude dozvoljen, ali takav pristup uvodi probleme kao što su dupla administracija i sinhronizacija podataka o korisnicima i njihovim zaduženjima između kompanija. Stoga, u Smart Grid sistemima, gde je podela zaduženja između različitih organizacija očekivana, je potrebno omogućiti da kontrola pristupa bude primenljiva i u interorganizacionim sistemima bez uvođenja dodatne kompleksnosti administracije i sinhronizacije podataka. Najčešći zahtev je da svaka organizacija bude

nezavisan bezbednosni domen sa aspekta administracije svojih podataka, uz definisanje politika za deljenja informacija i resursa na određeni period.

3.2.6 Mapiranje zahteva kompanija na zahteve za kontrolu pristupa

U *Tabeli 4.* je dat pregled zahteva za kontrolu pristupa koji su identifikovani poslovnom analizom više od dvadeset projekata za Smart Grid na kojima je autorka učestvovala. Zahtevi kompanija za prenos i distribuciju električne energije proizilaze iz potrebe da se obezbedi pouzdan, siguran i efikasan rad elektroenergetskog sistema. Neki od zahteva su proširenje standardom definisanih zahteva i preporuka u skladu sa specifičnim slučajevima korišćenja u Smart Gridu.

Tabela 4. C.AC.[3] Mapiranje zahteva kompanija na zahteve za kontrolu pristupa

Zahtev za kontrolu pristupa	Zahtev kompanije za prenos i distribuciju električne energije
C.AC.1. **Kontrola pristupa prema AOR-ima**	Potrebno je omogućiti podelu odgovornosti između korisnika koji pripadaju istim korisničkim ulogama prema oblastima odgovornosti (odnosno prema AOR-ima) kako bi se obezbedilo pouzdano, efikasno i kvalitetno izvršavanje kritičnih operacija unutar elektroenergetskog sistema, pre svega: 1) nadzor i upravljanje elektroenergetskim sistemom u realnom vremenu, 2) (re)konfiguracija RTU uređaja i izmene modela elektroenergetske mreže, prilikom primene u produkcionom sistemu, ali i u toku potvrde kvaliteta napravljenih izmena pre primene u produkciji. Skup kritičnih operacija treba da bude proširiv za potrebe specifičnih zahteva svake kompanije. Podela odgovornosti unutar sistema može biti definisana prema različitim kriterijumima, kao što su geografska podela ili podela prema naponskom nivou mreže.
C.AC.2. **Hijerarhijska organizacija AOR-a**	Potrebno je omogućiti hijerarhijsku organizaciju AOR-a u cilju jednostavnije administracije i smanjenja broja AOR-a koje je potrebno dodeliti korisnicima.
C.AC.3. **Mogućnost konstantnog nadzora i kontrole svih AOR-a u sistemu**	Potrebno je obezbediti konstantan nadzor i kontrolu svih AOR-a. To znači da svaki AOR mora da bude pod konstantnim nadzorom i kontrolom najmanje jednog operatera u kontrolnoj sobi. Korisnik ne sme da prekine korisničku sesiju ukoliko bi u tom slučaju neki od AOR-a ostao bez nadzora i kontrole. Stoga, kao deo regularnih aktivnosti u kontrolnoj sobi potrebno je omogućiti preuzimanje odgovornosti nad AOR-ima između operatera u toku izvršavanja korisničkih sesija.
C.AC.4. **Kontrola pristupa u vanrednim situacijama**	Ovaj zahtev je dopuna standardom definisanog zahteva za kontrolu pristupa u Smart Gridu (S.AC.2.) koji se odnosi na mogućnost izmene bezbednosne politike ili isključivanja bezbednosnih mehanizama u vanrednim situacijama. Konkretan zahtev kompanija je mogućnost delegiranja odgovornosti nad AOR-ima kako bi se obezbedilo efikasnije upravljanje elektroenergetskom mrežom u vanrednim situacijama kada određeni AOR-i mogu ostati bez nadzora i kontrole. To mogu biti ispadi u sistemu uzrokovani vremenskm nepogodama kada je

	potrebno da više korisnika istovremeno preuzme kontrolu nad sistemom, ali i nedostupnost regionalnog centra kada su korisnici onemogućeni da nadziru i upravljaju određenim delom mreže.
C.AC.5. **Kontrola pristupa prema licenci**	Za obavljanje poslova čije izvršavanje je regulisano licencom, potrebno je omogućiti kontrolu pristupa, odnosno ograničavanje skupa korisničkih uloga u zavisnosti od toga da li korisnik poseduje važeću licencu.
C.AC.6. **Kontrola pristupa prema aplikativnom kontekstu**	Ovaj zahtev je dopuna standardom definisanog zahteva za kontrolu pristupa u Smart Gridu (S.AC.4.) koji se odnosi na dodelu najmanjeg skupa privilegija. Kontrola pristupa treba da pruži mogućnost definisanja različite bezbednosne politike u pogledu dozvoljenog nivoa privilegija zavisno od Smart Grid konteksta. Pritom, cena implementacije ne bi trebala da bude kompleksnost administracije uvođenjem različitih privilegija za iste operacije u različitim aplikacijama.
C.AC.7. **Kontrola pristupa prema lokaciji ili nameni radne stanice**	Ovaj zahtev je dopuna standardom definisanih zahteva za kontrolu pristupa u Smart Gridu (S.AC.1.) koji se odnosi na uspostavljanje bezbednosnih politika i procedura za udaljeni pristup sistemu, kao i zahteva koji se odnosi na dodelu najmanjeg skupa privilegija (S.AC.4.). Kontrola pristupa treba da omogući ograničavanje skupa ovlašćenja korisnika u skladu sa lokacijom ili namenom radne stanice sa koje se pristupa sistemu. Za pristup kontrolnom sistemu sa udaljenih lokacija treba definisati restriktivnije bezbednosne politike u poređenju sa pristupom iz interne mreže. Takođe, radne stanice u kontrolnoj sobi mogu biti podeljene prema delovima elektroenergetskog sistema kojima operateri mogu upravljati. S obzirom da se u poslovnim sistemima mogu skladištiti različiti tipovi podataka kojima imaju pristup korisnici kojima je dodeljeno više od jedne uloge, potrebno je omogućiti minimalan skup privilegija u zavisnosti od tipa radne stanice sa koje pristupaju sistemu, npr. sa poslovne radne stanice ne treba omogućiti privilegije namenjene za obavljanje inženjerskih zadataka, i obrnuto.
C.AC.8. **Kontrola pristupa u interorganizacionim sistemima**	Ovaj zahtev je proširenje standardom definisanog zahteva za kontrolu toka podataka iz eksternih sistema (S.SA.2.). Potrebno je obezbediti kontrolu pristupa resursima jedne organizacije od strane korisnike iz partnerskih organizacija bez uvođenja kompleksnosti administracije i sinhronizacije podataka. Takođe, sve organizacije treba da budu nezavisni bezbednosni domeni sa aspekta administracije svojih podataka, uz definisanje bezbednosnih politika za deljenja informacija i resursa na određeni period.

[3] C.AC = company.access control

3.3 Ograničenja RBAC i ABAC baziranih modela u Smart Gridu

Uvidom u aktuelno stanje u oblasti istraživanja, a u skladu sa postavljenim ciljevima istraživanja, u prethodnim sekcijama su postavljeni zahtevi kojima treba da odgovore modeli kontrole pristupa u Smart Grid sistemima. U *Tabeli 2.* je dat pregled zahteva i preporuka propisanih relevantnim industrijskim standardima u oblasti kontrole pristupa, dok su u *Tabeli 3.* istaknuti aktuelni zahtevi kompanija za prenos i distribuciju električne energije za kontrolu pristupa uz osvrt na zahteve propisane standardima. U nastavku ove sekcije slede razmatranja vezana za mogućnost postojećih modela kontrole pristupa da odgovore zahtevima navedenim u *Tabeli 3.*, kao i mogućnost njihove primene u Smart Grid okruženju.

3.3.1 Analiza mogućnosti podele odgovornosti između korisnika sa istim zaduženjima

Zahtevi C.AC.1-C.AC.4 se odnose na potrebu da se u cilju pouzdanijeg i efikasnijeg upravljanja elektroenergteskim sistemima obezbedi podela odgovornosti između korisnika kojima su dodeljene iste korisničke uloge i zaduženja. Odnosno, kontrola pristupa u Smart Gridu treba da omogući donošenje odluka o pristupu kako u zavisnosti od privilegija korisnika, tako i u zavisnosti od dozvoljenog nivoa odgovornosti nad objektima koji pripadaju određenoj oblasti odgovornosti unutar elektroenergetskog sistema.

Kako RBAC model nema mogućnost uvažavanja parametara koji nisu deo identiteta korisnika (u šta su uključeni i atributi objekta poput pripadnosti određenom AOR-u), on ne može da podrži postavljeni zahtev. Nasuprot RBAC-u, ABAC model omogućuje donošenje odluka u zavisnosti od različitih atributa objekata. Za svaki objekat se definiše jedno ili više autorizacionih pravila koja definišu skup dozvoljenih operacija koje mogu biti izvršene nad tim objektom u dozvoljenim uslovima izraženim preko atributa korisnika, objekata i/ili okruženja. Međutim, u elektroenergetskim sistemima koji sadrže milione uređaja i opreme ovaj pristup nije primenljiv zbog ogromnog broja autorizacionih pravila koja bi morala biti definisana. Poseban izazov predstavlja računanje vrednosti autorizacionih pravila tokom izvršavanja što u slučaju velikog broja autorizacionih pravila može značajno uticati na performanse sistema što u sistemima za rad u realnom vremenu naročito nije prihvatljivo. Na primer, da bi se definisala autorizaciona pravila za sve moguće kombinacije N atributa, potrebno je 2^N autorizacionih pravila.

RBAC-bazirani modeli razmatrani u dosadašnjim istraživanjima ne mogu da odgovore postavljenom zahtevu, jer imaju za cilj da ograniče skup korisničkih uloga prilikom uspostavljanja korisničke sesije u zavisnosti od razmatranih atributa. Kako se na taj način menja skup privilegija u korisničkoj sesiji, a time i skup zaduženja definisanih korisničkom

ulogom koja je korisniku dodeljena, ovaj pristup nije adekvatan. Naime, ovaj pristup ne može da podrži mogućnost raspodele odgovornosti između korisnika sa istim zaduženjima u sistemu kao što se navodi u postavljenom zahtevu. Takođe, prostorno-orijentisani RBAC modeli koji nastoje da uvaže atribute objekata prilikom donošenja odluke o pristupu uglavno razmatraju lokaciju objekta. Međutim, u oblasti kontrole pristupa u Smart Gridu je geografska lokacija objekta samo jedna od karakteristika objekata koja bi se mogla razmatrati. Uglavnom je potrebno uvažiti i neke druge karakteristike objekata elektroenergetskog sistema (npr. naponski nivo).

STRBAC model opisan u *Sekciji 2.4.3* osim fizičke pozicije razmatra i druge tipove lokacija u zavisnosti od kojih je moguće doneti odluku o pristupu, npr. lokacija definisana prema nameni (funkciji), prema organizaciji, kao i mogućnost definisanja specifičnim kategorijama koje nisu obuhvaćene ovom podelom. Iako bi ovako definisan lokacijski model bio primenljiv na objekte elektroenergetskog sistema, postupak donošenja odluke o pristupu STRBAC modela nije adekvatan. Naime, u zavisnosti od lokacije STRBAC donosi odluku o tome da li je pristup dozvoljen, ali nema mogućnost definisanja skupa dozvoljenih operacija nad datim objektom u zavisnosti od lokacije kao što je specificirano postavljenim zahtevom.

U zahtevima C.AC.3 i C.AC.4 akcenat je na mogućnosti kontrole pristupa da odgovori dinamičnim zahtevima Smart Grid okruženja koji se pre svega odnose na potrebu za izmenom skupa dodeljenih AOR-a nakon uspostavljanja korisničke sesije. Iako razmatrani modeli kontrole pristupa ne mogu adekvatno da odgovore zahtevima za AOR-e, interesantno je analizirati da li i na koji način ovi modeli mogu da odgovore zahtevima za dinamičku izmenu skupa ovlašćenja. RBAC je statički model koji nema mogućnost izmene skupa korisničkih uloga nakon uspostavljanja sesije. S druge strane, RBAC-bazirani modeli pružaju mogućnost izmene skupa ovlašćenja prilikom uspostavljanja sesije ili u toku izvršavanja sesije u momentu donošenja odluke o pristupu. Međutim, izmena ovlašenja na određeni period u toku sesije se retko razmatra. Primer modela gde je razmatran ovaj zahtev je STRBAC model za rasplinute računarske sisteme opisan u *Sekciji 2.4.3* kojim se predlaže koncept delegacije u vanrednim situacijama. Naime, u situacijama kada je korisnik nedostupan i ne može da izvrši zadatke omogućena je privremena dodela privilegija drugim korisnicima ili ulogama. Ovakav pristup može na sličan način da se primeni na koncept AOR-a. Međutim, u elektroenergetskim sistemima je osim u vanrednim situacijama delegiranje zaduženja potrebno omogućiti i u regularnom režimu rada. U skladu sa zahtevom C.AC.3 potreba za delegiranjem zaduženja se javlja i u regularnom režimu rada kada je potrebno dozvoliti izmenu ovlašćenja u skladu sa odgovornostima koje su korisnicima omogućene.

3.3.2 Analiza mogućnosti uvažavanja atributa korisnika i parametara okruženja

Zahtevi C.AC.5-C.AC.7 se odnose na mogućnost izmene skupa ovlašćenja prilikom uspostavljanja sesije u zavisnosti od određenih parametara. U Smart Grid su

identifikovani parametri koji predstavljaju atribute korisnika (licenca, zahtev C.AC.5) i parametara okruženja (radna stanica, zahtev C.AC.7, i Smart Grid kontekst, zahtev C.AC.6). Kao što je i ranije istaknuto, RBAC model nema mogućnost uvažavanja drugih parametara osim identiteta korisnika te ne može da zadovolji postavljene zahteve. Problem primene ABAC model je u ovom računanje vrednosti autorizacionih pravila u toku izvršavanja što može značajno uticati na performanse.

U dosadašnjim istraživanjima uočena su dva pristupa u prevazilaženju ovog problema. Prvi pristup je proširivanje i unapređenje RBAC modela. RBAC-bazirani modeli kontrole pristupa zadržavaju strukturu RBAC modela, proširujući ga u skladu sa zahtevima specifičnog sistema, npr. mogućnost aktivacije uloga u zavisnosti od vremenske i/ili prostorne dimenzije (konkretni primeri su navedeni u *Sekciji 2.4*). Osnovni problem ovakvog pristupa je to što ne postoji opšti model koji objedinjuje prednosti različitih proširenja i koji je moguće primeniti ili jednostavno proširiti za potrebe drugih sistema.

Drugi pristup se odnosi na primenu hibridnih modeli kontrole pristupa kojima se pokušavaju iskoristiti prednosti RBAC i ABAC modela kako bi se zadvoljili zahtevi heterogenih, distribuiranih sistema. U *Sekciji 2.6* su predstavljena tri tipa hibridnih RBAC-A modela. Prvi tip je RBAC-A orijentisan ka atributima koji nije pogodan za Smart Grid iz istog razloga kao i ABAC model obzirom da su korisničke uloge samo dodatni atribut korisnika. Drugi tip je RBAC-A model orijentisan ka ulogama koji zadržava strukturu RBAC modela. Kao što je istaknuto u *Sekciji 2.6*, osnovni nedostatak ovog pristupa činjenica da se ograničenjima može samo redukovati skup raspoloživih privilegija, ali ne i proširiti u skladu sa potrebama Smart Grida. Npr. operateri najčešće sa iste radne stanice upravljaju sistemom u realnom vremenu i izvršavaju različite "šta-ako" analize. U tom smislu, trebalo bi omogućiti da korisnik u simulaciji ima širi skup privilegija u poređenju sa privilegijama za rad u realnom vremenu. Treći tip je RBAC-A pristup sa dinamičkim ulogama, omogućuje dinamičku dodelu uloga korisnicima u zavisnosti od atributa. U tom smislu je ovaj pristup najbliži zahtevima u Smart Gridu, ali i dalje nema mogućnost da uvaži sve specifične zahteve za Smart Grid. Na primer, ovaj pristup ne razmatra mogućnost dinamičkog ograničavanja/proširivanja pojedinačnih privilegija bez izmene skupa korisničkih uloga. Ovakav pristup je posebno važan za AOR-e u situacijama kada nije potrebno izmeniti skup omogućenih AOR-a već samo definisane nivoe odgovornosti za dodeljene AOR-e u zavisnosti od Smart Grid konteksta kome se pristupa. Takođe, ovaj pristup ne razmatra mogućnost dinamičke izmene ovlašćenja u toku izvršavanja korisničke sesije.

3.3.3 Analiza mogućnosti primene u interorganizacionim sistemima

Zahtev C.AC.8 se odnosi na mogućnost primene modela kontrole pristupa kako u organizacijama zatvorenog tipa, tako i u višedomenskim okruženjima, pri čemu se kao osnovni zahtev postavlja mogućnost jednostavne primene modela bez uvođenja kompleksnosti administracije i sinhronizacije podataka. Takođe, sve organizacije treba

da budu nezavisni bezbednosni domeni sa aspekta administracije svojih podataka, uz definisanje bezbednosnih politika za deljenja informacija i resursa na određeni period. Problem kontrole pristupa u interorganizacionim sistemima je razmatran kroz različite primere primene distribuiranih RBAC modela u *Sekciji 2.4.5*. Sa zahtevima za Smart Grid su najviše usklađeni pristupi opisani u radovima [7] i [95], čijim objedinjavanjem će biti ispunjeni zahtevi za interorganizacijom u Smart Gridu.

3.4 Razvoj modela bezbednosne arhitekture za Smart Grid

Model bezbednosne arhitekture za Smart Grid razvijen za potrebe verifikacije rešenja koje se predlaže u okviru ove disertacije je zasnovan na IEC-62443 modelu bezbednosnih zona. Sa aspekta bezbednosnih zona, predloženi model prati bezbednosnu arhitekturu za industrijske kontrolne sisteme koja je detaljno opisana u *sekciji 2.7.4*, uz nekoliko ključnih izmena kako bi se uvažili zahtevi i preporuke propisane industrijskim standarima istaknutim u *Tabeli 3.*

Prva izmena se odnosi na proširenje Operativne DMZ zone Smart Grid sistemima za podršku u odlučivanju opisanim u *Sekciji 2.7.4*. U operativnoj DMZ zoni se nalaze komponente za podršku u odlučivanju koje su integrisane sa SCADA sistemom u cilju unapređenja procesa upravljanja.

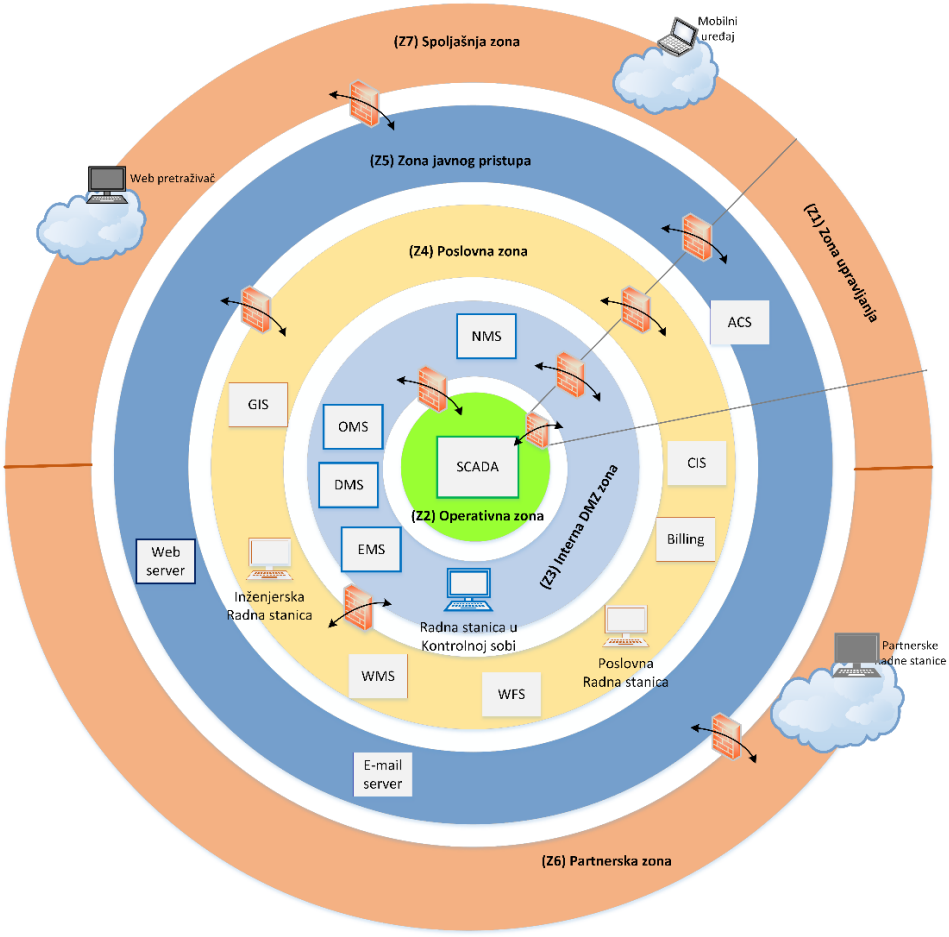
Druga izmena se odnosi na izmeštanje bezbednosnih servisa iz Operativne DMZ zone. Uvodi se zona upravljanja (eng. *Management zone*) namenjena za administraciju i nadzor celokupnog sistema. Tu se smeštaju servisi za upravljanje konfiguracijom servera, praćenje performansi, zapis i praćenje aktivnosti u sistemu, servisi za upravljanje bezbednošću, i slično. Cilj uvođenja zone upravljanja je izolacija bezbednosnih funkcija od ostalih komponenti sistema, kao što je propisano S.SA.1 zahtevom. Pošto je iz ove zone moguće pristupiti svim zonama, pristup zoni upravljanja treba da bude strogo kontrolisan i omogućen malom broju visoko privilegovanih korisnika za potrebe administracije i nadgledanja sistema. U ovoj zoni treba da bude smešten i servis za kontrolu pristupa u Smart Gridu (eng. *access control service*, skr. *ACS*).

Treća izmena se odnosi na uvođenje posebne zone namenjene za pristup sistemu od strane partnerskih kompanija. Prema S.SA.2 partnerska zona se razlikuje od spoljašnje iz razloga što spoljašnja zona predstavlja nekontrolisanu bezbednosnu zonu koja je u potpunosti van nadležnosti organizacije. S druge strane, partnerski sistem nije u nadležnosti organizacije, ali se uspostavljaju bezbednosne politike sa partnerskim organizacijama kojima se definišu pravila pristupa iz eksternih sistema.

Smart Grid aplikacije za rad van realnog vremena koje se baziraju na podacima iz eksternih sistema ili podrazumevaju pristup sa udaljenih lokacija smeštaju se u okviru postojeće poslovne zone koja se primenjuje bez izmena. Jedini izuzetak od ovog pravila mogu biti sistemi za simulaciju koji mogu biti smešteni i u Operativnoj DMZ zoni u skladu

sa S.SA.2, jer predstavljaju izolovane sisteme koji rade nad replikom podataka sistema za rad u realnom vremenu, a podaci se ne koriste od strane drugih komponenti.

Na *Slici 10.* je prikazan predloženi model bezbednosne arhitekture za Smart Grid koji se sastoji iz osam bezbednosnih zona. Bezbednosne zone su implementirane u skladu sa industrijskom praksom opisanom u S.SA.1. Radi jedostavnosti prikaza, zona ograničenog pristupa u koju se smešta industrijski kontrolni sistem nije prikazana. U operativnoj zoni se nalazi kontrolni SCADA sistem, dok se u operativnu DMZ zonu smeštaju servisi za podršku u odlučivanju integrisani sa SCADA-om, kao što su NMS, EMS, DMS, OMS. U poslovnu zonu se smeštaju servisi za unapređenje poslovnih procesa, kao što su CIS, Billing, WMS, WFS. U istoj zoni se smeštaju i različiti sistemi za podršku inženjerskim aktivnostima van realnog vremena koje rade nad replikom operativnih podataka, ali ne smeju da ugroze njihovu raspoloživost, integritet ili poverljivost. U zoni javnog pristupa se nalaze servisi namenjeni za komunikaciju sa spoljašnjom zonom.



Slika 10. Model bezbednosne arhitekture za Smart Grid

4 Metodologija istraživanja

4.1 Faze istraživanja

Istraživanje u okviru ove disertacije je sprovedeno u četiri faze.

Prva faza istraživanja je obuhvatila detaljnu analizu teorijskih osnova, upoznavanje sa predmetom istraživanja i aktuelnim stanjem u oblasti istraživanja putem dostupne naučne i stručne literature. Analizirani su modeli kontrole pristupa koji se pretežno koriste u upravljanju heterogenim, distribuiranim sistemima. Takođe, dat je pregled aktuelnog stanja u oblasti informacione bezbednosti u Smart Gridu, uz osvrt na referentne modele potrebne za razumevanje informacione infrastrukture Smart Grida i zahteve za kontrolu pristupa.

Druga faza istraživanja je usmerena na ispitivanje aktuelnih zahteva u elektroenergetskoj industriji i ograničenja postojećih modela kontrole pristupa da odgovore postavljenim zahtevima. Detaljnom analizom zahteva, u ovoj fazi je utvrđen skup zahteva koje model kontrole pristupa u Smart Grid sistemima treba da ispuni. Takođe, utvrđen je i model bezbednosne arhitekture za Smart Grid na kome će se bazirati simulirano Smart Grid okruženje za eksperimentalna istraživanja.

U trećoj fazi istraživanja je definisana formalna specifikacija modela kontrole pristupa koji je usklađen sa postavljenim zahtevima, i implementiran prototip servisa za kontrolu pristupa koji je zasnovan na predloženog modelu.

U četvrtoj fazi istraživanja je izvršena verifikacija primenljivosti predloženog modela u Smart Gridu integracijom prototipske implementacije servisa za kontrolu pristupa u simuliranom Smart Grid okruženju. Primenljivost predloženog rešenje će biti ispitana na osnovu slučajeva korišćenja koji su definisani prema zahtevima realnih projekata na kojima je autorka učestvovala.

Na kraju su analizirani rezultati eksperimentalnih istraživanja sa osvrtom na prednosti predloženog rešenja u poređenju sa RBAC modelom. Takođe, istaknuta su ograničenja predloženog rešenja i mogući pravci daljeg istraživanja i unapređenja.

4.2 Istraživačke metode

Tokom naučno-istraživačkog rada birane su metode naučnog istraživanja koje će obezbediti objektivnost, sistematičnost i pouzdanost.

4.2.1 Metoda kompilacije

Metoda kompilacije je primenjena u uvodnom razmatranju i prikazu aktuelnog stanja u oblasti informacione bezbednosti i kontrole pristupa u Smart Grid sistemima u smislu preuzimanja tuđih rezultata naučno-istraživačkog rada, odnosno tuđih opažanja, stavova i zaključaka.

4.2.2 Metoda uzorka

Metodom uzorka izabran je reprezentativan skup vladajućih tehničkih standarda u oblasti informacione bezbednosti za Smart Grid, od kojih su dva standarda u oblasti bezbednosti informacionih sistema, četiri standarda za bezbednost industrijskih kontrolnih sistema i dva standarda za bezbednost u Smart Gridu. Metodom uzorka izabrano je više od dvadeset projekata za implementaciju Smart Grid širom sveta u čijoj poslovnoj analizi je autorka rada učestvovala.

Metoda uzorka je korišćena i u četvrtoj fazi istraživanja prilikom definisanja inicijalnog skupa podataka na kojima se zasnivaju eksperimentalna istraživanja u ovoj disertaciji. Iako je za metodu uzorka karakterističan problem pouzdanosti, odnosno određivanja veličine uzorka i reprezentativnosti odabranih jedinica, sagledavanjem i analizom postavljenih zahteva se osnovano pretpostavlja da definisani uzorak ne utiče na opštost eksperimentalnog istraživanja.

4.2.3 Metoda analize

Metodom eksplikativne analize utvrđen je skup zahteva za kontrolu pristupa u Smart Gridu. Budući da je metoda eksplikativne analize postupak naučnog istraživanja gde se pokušava objasniti određena celina na osnovu njenih delova, ova metoda je omogućila zanemarivanje onih pojava, svojstava i odnosa koji na određenom nivou istraživanja otežavaju ispitivanje predmeta istraživanja.

4.2.4 Metoda sinteze

Metoda sinteze je korišćena za sintezu konačnog simulacionog Smart Grid okruženja. Sintezom zahteva, preporuka i najboljih industrijskih praksi za bezbednost u Smart Gridu formiran je model bezbednosne arhitekture za Smart Grid u okviru koga je integrisano predloženo rešenje.

4.2.5 Metoda komparacije

Metoda komparacije je postupak upoređivanja srodnih činjenica, pojava, procesa i odnosa, odnosno utvrđivanje njihove sličnosti i razlika u njihovom ponašanju i intenzitetu. Ova metoda je korišćena u drugoj fazi istraživanja za upoređivanje postojećih modela kontrole pristupa sa aspekta njihove primene u Smart Gridu.

Komparativna metoda je korišćena i tokom analize eksperimentalnih rezultata u cilju upoređivanja rezultata dobijenih primenom RBAC modela i predloženog RBAC proširenja pod istim uslovima u kojima se prati tok eksperimenta.

4.2.6 Metoda modelovanja

U trećoj fazi istraživanja primenjen je metod modelovanja korišćenjem objedinjenog jezika modelovanja (eng. *Unified Modeling Language*, skr. *UML*). Za specifikaciju autorizacionih politika korišćen je *eXtensible Access Control Markup Language* (skr. XACML) jezik. Za modelovanje objekata koji pripadaju domenu realnih elektroenergetskih sistema korišćen je *Common Information Model* (skr. CIM) standard za modelovanje elektroenergetskih sistema.

4.2.7 Metoda izrade prototipa

Metoda izrade prototipa je primenjena u trećoj fazi istraživanja za potrebe verifikacije formalne specifikacije predloženog modela kontrole pristupa u Smart Grid okruženju. Sve komponente prototipa servisa za kontrolu pristupa su implementirane u Microsoft Visual Studio 2013 razvojnom okruženju korišćenjem programskog jezika C#, dok je za skladištenje bezbednosnih podataka korišćen LDAP (eng. *Lightweight Directory Access Protocol*) direktorijum.

4.2.8 Metoda eksperimenta

Osnovni metod koji je primenjen u četvrtoj fazi istraživanja je metod eksperimenta. Usklađenost predloženog modela kontrole pristupa sa postavljenim zahtevima je verifikovana u simuliranom Smart Grid okruženju. Izvršena je integracija razvijenog prototipa servisa za kontrolu pristupa i testirani su slučajevi korišćenja formirani prema zahtevima realnih projekata. U cilju dobijanja uporednih rezultata, eksperimenti su izvršeni primenom RBAC modela i predloženog RBAC proširenja. Rezultati su predstavljeni uporednim tabelama.

4.2.9 Metoda generalizacije

Metoda generalizacije je korišćena za formiranje opštih stavova na osnovu pojedinačnih zaključaka. Generalizacijom zaključaka iz konkretno testiranih slučajeva korišćenja na ostale slučajeve koji u ovom istraživanju nisu testirani, formirani su zaključci o mogućnosti primene predloženog rešenja u Smart Gridu, prednostima predloženog rešenja u odnosu na analizirana rešenja, i ograničenjima predloženog rešenja u Smart Gridu.

5 Formalna specifikacija modela kontrole pristupa

RBAC model je jedan od najzastupljenijih modela kontrole pristupa u modernim informacionim sistemima. RBAC je zasnovan na korisničkim ulogama oko kojih su formulisana prava pristupa. Korisničkim ulogama se definišu različita zaduženja i odgovornosti u sistemu na osnovu skupa dodeljenih privilegija, a korisnicima se dodeljuju korisničke uloge u skladu sa njihovim zaduženjima unutar organizacije. Hijerarhijom uloga može se pojednostaviti administracija modela u slučaju preklapanja korisničkih uloga po pitanju dodeljenih privilegija, dok je modelom statičkog i dinamičkog razdvajanja dužnosti moguće sprečiti dodelu konfliktnih uloga u toku administracije modela ili prilikom uspostavljanja korisničke sesije. S obzirom na jednostavnost upravljanja bezbednosnim politikama, kao i smanjenje kompleksnosti i troškova administracije, RBAC je najčešće korišćeni model kontrole pristupa u sistemima karakterisanim velikim brojem korisnika i resursa koje je potrebno zaštititi. Međutim, RBAC je statički model zasnovan na unapred definisanim korisničkim ulogama u sistemu i ne može da odgovori zahtevima organizacija u okviru kojih postoji potreba da se osim dodeljenih korisničkih uloga razmatraju i drugi faktori prilikom donošenja odluke o pristupu. Kako bi se iskoristile prednosti RBAC modela, a pritom uvažili različiti faktori okruženja poput vremenske i prostorne dimenzije, u dostupnoj literaturi se predlažu unapređenja RBAC modela. Najčešće se radi o proširenjima RBAC-a koja imaju za cilj da ograniče skup korisničkih uloga u zavisnosti od vremena kada se pristupa sistemu ili lokacije korisnika/objekata. Predložena rešenja su uglavnom prilagođena specifičnim zahtevima određenog sistema, te je njihova primena ili mogućnost unapređenja za potrebe drugih sistema prilično kompleksna, ponekad čak i nemoguća.

U oblasti Smart Grida identifikovani su zahtevi koje je potrebno ispuniti kako bi se obezbedila zaštita od neovlašćenog pristupa, ali i pouzdano i efikasno upravljanje sistemom kako u regularnom režimu rada tako i u vanrednim situacijama. Jedna grupa zahteva se odnosi na mogućnost raspodele odgovornosti između korisnika koji pripadaju istim korisničkim ulogama prema oblastima odgovornosti unutar elektroenergetske mreže. Kako RBAC ne može da odgovori ovom zahtevu, u [103][104] autori predlažu proširenje RBAC modela entitetom AOR-a. Međutim, u navedenim radovima se ne razmatraju specifični zahtevi za pouzdan i stabilan rad sistema koji treba da bude prioritet kako u regularnom režimu rada, tako i u vanrednim situacijama. U regularnom režimu rada, potrebno je obezbediti kontinualno i efikasno upravljanje svim delovima elektroenergetske mreže, dok je u vanrednim situacijama dozvoljena privremena izmena prava koja su propisana autorizacionom politikom kako ne bi bio ugrožen pouzdan i stabilan rad elektroenergetskog sistema. Druga grupa zahteva se odnosi na mogućnost kontrole pristupa u zavisnosti od različitih faktora (parametara) koji mogu imati uticaj na donošenje odluke o pristupu u Smart Grid okruženju. Tu spadaju korisnički atributi (licenca za obavljanje određenih poslova i organizacija kojoj korisnik pripada) i parametri okruženja (lokacija ili namena radne stanice sa koje se pristupa sistemu i tip

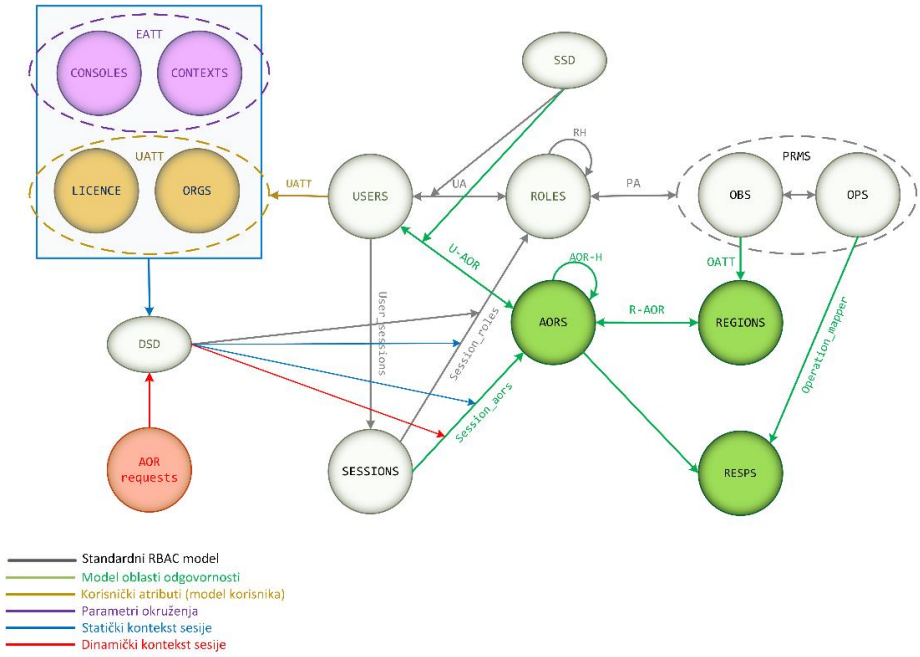
aplikacije kojoj se pristupa). Svi navedeni parametri su nepromenljivi u toku izvršavanja korisničke sesije. Izuzetak je licenca koja bi u opštem slučaju mogla da istekne u toku izvršavanja sesije. Međutim, poređenjem očekivanog trajanja korisničke sesije u Smart Grid sistemima (koje je maksimalno jedna radna nedelja, tj. na početku radne nedelje se sesija uspostavlja i na kraju radne nedelje se prekida prilikom gašenja radne stanice) i perioda važenja licence (licence za obavljanje poslova u elektroprivredi se izdaju za period od jedne do nekoliko godina), osnovano se može tvrditi da je i licenca nepromenljivi parametar u toku izvršavanja korisničke sesije.

Na osnovu postavljenih zahteva, u ovoj disertaciji se predlaže jedno rešenje modela kontrole pristupa u Smart Grid sistemima bazirano na RBAC modelu (skr. RBAC-AOR$_{SG}$). Predloženi model proširuje koncept AOR-a iz [103][104] kako bi se obezbedilo pouzdano, efikasno i kontinualno upravljanje elektroenergetskim sistemom. Dodatno, predloženi model proširuje RBAC model ograničenja kako bi se uvažili faktori koji mogu imati uticaj na donošenje odluke o pristupu u Smart Gridu. RBAC-AOR$_{SG}$ je kompatibilan sa RBAC-om, i isključivanjem predloženih proširenja iz razmatranja dolazi se do standardnog RBAC modela koga je moguće primeniti bez ikakvih izmena. Takođe, predloženi model je fleksibilan u smislu da je proširenja koja nije potrebno uvažiti moguće isključiti bez dodatnih izmena ili uticaja na ostale RBAC-AOR$_{SG}$ komponente.

Osnovni koncepti predloženog RBAC-AOR$_{SG}$ modela kontrole pristupa za Smart Grid, skup entiteta i njihovih međusobnih relacija prikazani su na dijagramu *na Slici 11.* RBAC-AOR$_{SG}$ obuhvata sledeća proširenja RBAC modela:

- Osnovni RBAC je proširen modelom AOR-a kako bi se omogućio dodatni nivo kontrole pristupa u zavisnosti od dozvoljenog nivoa odgovornosti nad objektom elektroenergetske mreže. Model AOR-a čine sledeći entiteti: regioni elektroenergetske mreže (eng. *REGIONS*), oblasti odgovornosti (*AORS*) i nivoi odgovornosti (eng. *RESPSONSIBILITIES*, skr. *RESPS*). REGIONS predstavlja atribut objekta kojim su modelovane karakteristike resursa elektroenergetskog sistema, a AORS definiše odgovornosti korisnika nad objektima koji pripadaju određenom regionu. RESPS su dozvoljeni nivoi odgovornosti nad objektima nekog regiona i određeni su tipovima operacija u Smart Gridu. Povezivanjem entiteta oblasti odgovornosti sa entitetom korisnika moguće je definisati skup dozvoljenih operacija nad objektima koji dele iste karakteristike unutar elektroenergetskog sistema.
- Model korisnika osnovnog RBAC-a je proširen entitetima organizacije (eng. *ORGANIZATIONS*, skr. *ORGS*) i licence (eng. *LICENCE*) koji predstavljaju atribute korisnika u RBAC-AOR$_{SG}$. ORGS omogućuje kontrolu pristupa za korisnike iz eksternih organizacija mapiranjem uloga i atributa iz eksternog sistema na korisničke uloge i atribute u izvornoj organizaciji, a LICENCE pruža mogućnost ograničavanja skupa korisničkih uloga koje su regulisane važećom licencom.
- RBAC model statičkih ograničenja (*SSD*) je proširen tako da je u toku administracije modela moguće ograničiti dodelu konfliktnih AOR-a istom korisniku.

- RBAC model dinamičkih ograničenja (*DSD*) je proširen tako da omogući izmenu skupa ovlašćenja korisnika prilikom uspostavljanja korisničke sesije, ali i u toku izvršavanja korisničke sesije. Statički kontekst sesije (eng. *static session context*) čine entiteti koji su nepromenljivi u toku izvršavanja korisničke sesije, te se njihova vrednost razmatra prilikom uspostavljanja korisničke sesije. Tu spadaju korisnički atributi (eng. *User Attrbiutes*, skr. *UATT*) i atributi okruženja (eng. *Environment Attributes*, skr. *EATT*). UATT su opisani modelom korisnika. EATT su radna stanica sa koje korisnik pristupa sistemu (*CONSOLES*) i tip Smart Grid aplikacije kojoj korisnik pristupa (*CONTEXTS*). Entitet CONSOLES omogućuje ograničavanje skup korisničkih uloga i oblasti odgovornosti u zavisnosti od lokacije ili namene radne stanice sa koje se pristupa sistemu, a uvažavanjem entiteta CONTEXTS moguće je izmeniti (ograničiti ili proširiti) skup omogućenih korisničkih uloga, privilegija i oblasti odgovornosti korisnika u zavisnosti od izabrane aplikacije. Dinamički kontekst sesije (eng. *dynamic session context*) čine entiteti čija se vrednost može menjati u toku izvršavanja korisničke sesije, odnosno kojima je moguće izmeniti skup ovlašćenja korisnika u okviru aktivnih sesija. U Smart Gridu se to prevashodno odnosi na zahteve za izmenu dodeljenih AOR-a u okviru aktvnih korisničkih sesija kako u regularnom režumu rada, tako i u vanrednim situacijama (eng. *AOR requests*).



Slika 11. Formalna specifikacija RBAC-AOR$_{SG}$ modela

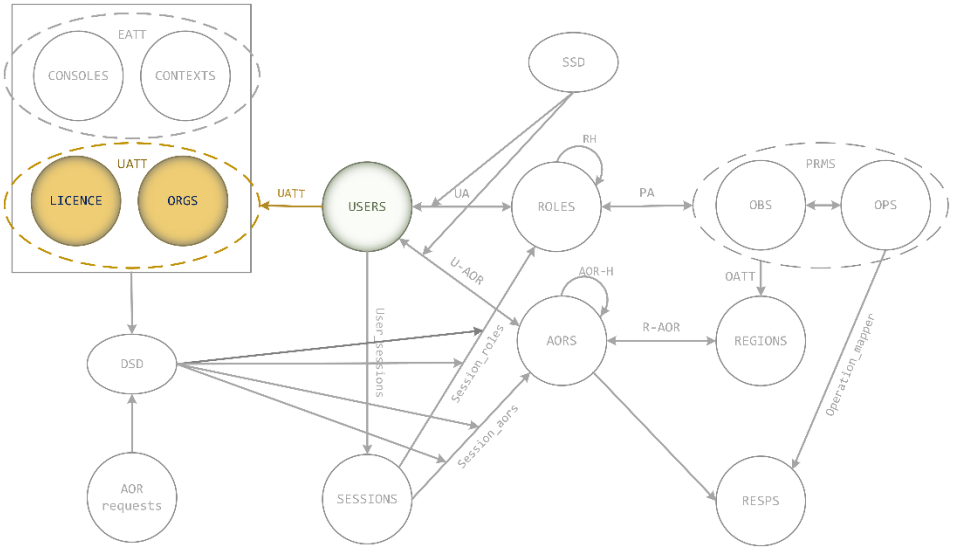
U nastavku ove sekcije detaljno su opisani entiteti RBAC-AOR$_{SG}$ modela. Prvo su opisani entiteti modela korisnika i oblasti odgovornosti, a zatim entiteti modela ograničenja i proširenja. Na kraju je prikazan postupak sprovođenja kontrole pristupa prema RBAC-AOR$_{SG}$ modelu.

5.1 Model korisnika

Prema zahtevu opisanom u C.AC.8, model kontrole pristupa za Smart Grid treba da bude primenljiv u interorganizacionim sistemima bez uvođenja kompleksnosti administracije i sinhronizacije podataka. Da bi RBAC zadovoljio navedeni zahtev, skup korisnika USERS bi trebao da sadrži kako korisnike internog sistema, tako i korisnike svih eksternih sistema. Osnovni problem kod ovog pristupa je dupla administracija korisnika koja nije adekvatna kako za organizacije koje treba da vode računa o sinhronizaciji podataka o korisničkim nalozima, tako i za korisnike koji bi na ovaj način morali da imaju poseban korisnički nalog za svaku organizaciju kojoj pristupaju. U zahtevu C.AC.5 se ističe da model kontrole pristupa za Smart Grid sisteme treba da pruži mogućnost ograničavanja korisničkih uloga ukoliko korisnik ne poseduje važeću licencu. RBAC model definiše skup korisničkih uloga za svakog korisnika poredstvom UA relacije, dok je SSD i DSD relacijama moguće statički i dinamički ograničiti dodelu konfliktnih uloga. Međutim, ograničenja korisničkih uloga bazirana na proveri dodatnih atributa korisnika nisu moguća.

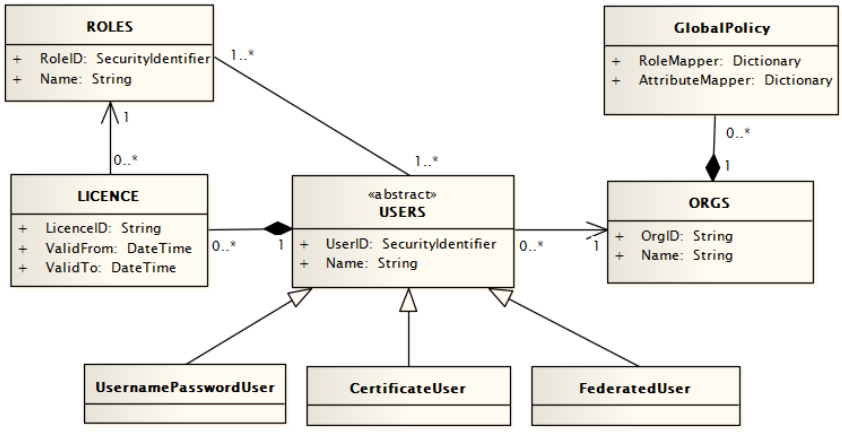
U cilju prevazilaženja predočenih problema, u ovom radu se predlaže proširenje modela korisnika osnovnog RBAC modela entitetima organizacije (*ORGS*) i licence (*LICENCE*), uključujući i njihove relacije sa entitetom korisnika. Entiteti korisnika, organizacije, licence i relacije između njih zajedno čine RBAC-AOR$_{SG}$ model korisnika koji je istaknut na *Slici 12.* ORGS predstavlja skup svih organizacija sa kojima je interna (izvorna) organizacija uspostavila labavo spregnuti federativni odnos. Labavo spregnuti federativni odnos znači da svaka organizacija zadržava potpunu kontrolu nad svojim resursima, kao i upravljanje uslugama eksternih organizacija. Za svakog korisnika se definiše korisnički atribut koji označava organizaciju kojoj korisnik pripada. LICENCE je skup svih licenci definisanih za korisnike iz skupa USERS. Za svakog korisnika se definiše korisnički atribut koji označava licence koje dati korisnik poseduje.

Na *Slici 13.* je prikazan UML dijagram klasa RBAC-AOR$_{SG}$ model korisnika. Svaki korisnik je član tačno jedne organizacije, koja može biti izvorna ili eksterna. Za svaku organizaciju se definiše globalna bezbednosna politika (eng. *GlobalPolicy*) koja propisuje pravila transformacije korisničkih uloga i/ili korisničkih atributa iz određene eksterne organizacije na odgovarajuće vrednosti iz izvorne organizacije. Detaljnije objašnjenje modela organizacije je dato u *Sekciji 5.3.2.* Odnos između eniteta korisnika i licence je modelovan relacijom kompozicije. Za svakog korisnika moguće je definisati proizvoljan broj licenci kojima se definiše period u kome datom korisniku može biti omogućena korisnička uloga za koji je licenca izdata.



Slika 12. Model korisnika RBAC-AOR$_{SG}$ modela

Klasama `UsernamePasswordUser` i `CertificateUser` predstavljeni su korisnici iz izvorne organizacije u zavisnosti od tipa autentifikacije. `UsernamePasswordUser` korisnici se autentifikuju upotrebom korisničkog imena i šifre, dok se u slučaju `CertificateUser` koristi digitalni sertifikat za autentifikaciju. `FederatedUser` klasom su modelovani eksterni korisnici čiju autentičnost i integritet garantuje partnerska kompanija svojim digitalnim potpisom.



Slika 13. UML dijagram klasa modela korisnika RBAC-AOR$_{SG}$ modela

5.2 Model oblasti odgovornosti

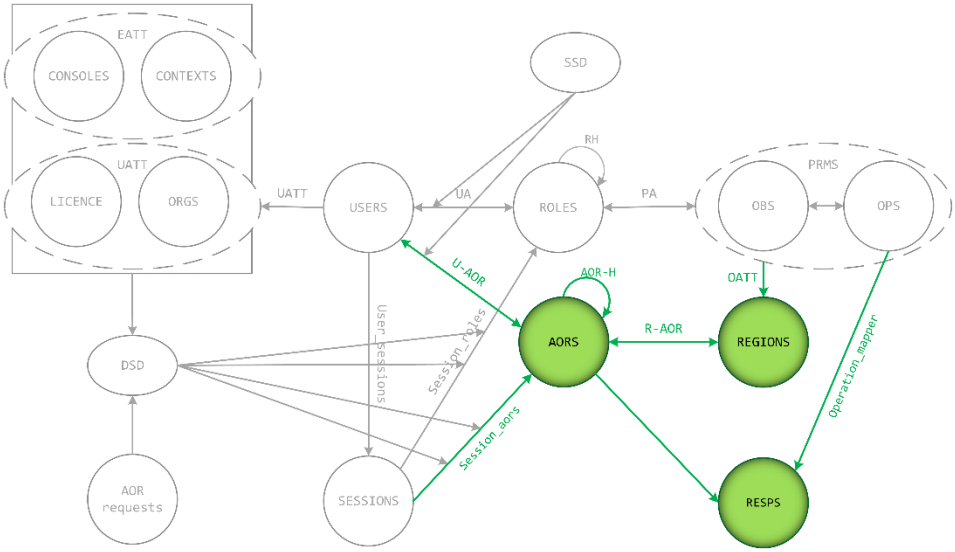
Prema C.AC.1, model kontrole pristupa u Smart Gridu treba da omogući podelu odgovornosti između korisnika koji mogu pripadati istim korisničkim ulogama u cilju pouzdanijeg i efikasnijeg izvršavanja kritičnih operacija. Razmatrana su tri tipa kritičnih operacija: 1) nadzor elektroenergetskog sistema, 2) upravljanje elektroenergetskim sistemom, 3) kao i izmene modela (izmene SCADA modela i modela elektroenergetske mreže), ali bi ovaj skup operacija trebalo da bude proširiv kako za potrebe granularnije podele kritičnih operacija, tako i za podršku novih tipova operacija. Kao što je istaknuto u radovima [103][104], navedeni zahtev prevazilazi mogućnosti RBAC modela gde su prava korisnika u potpunosti određena skupom privilegija dodeljenih posredstvom korisničkih uloga. U navedenim radovima se osnovni RBAC proširuje entitetom AOR-a (tzv. RBAC-AOR model) čime je omogućeno sprovođenje kontrole pristupa u zavisnosti od dodeljenog nivoa odgovornosti nad određenom oblašću unutar elektroenergetske mreže. Međutim, predloženi RBAC-AOR je orijentisan na proširenje relacija osnovnog RBAC-a i ne razmatra model hijerarhije AOR-a niti model statičkih i dinamičkih ograničenja koji su od ključnog značaja za Smart Grid okruženje. Takođe, RBAC-AOR nije dovoljno precizan kada je u pitanju skup objekata elektroenergetskog sistema za koje je moguće definisati AOR.

Stoga, u ovom radu se predlaže unapređenje modela AOR-a iz [103][104], tako da bude moguće podržati hijerarhijski model i model statičkih i dinamičkih ograničenja AOR-a. Takođe, formalizovan je skup Smart Grid objekata za koje je moguće definisati karakteristike elektroenergetskog sistema, pre svega pripadnost određenom geografskom regionu i/ili naponski nivo. Na *Slici 14.* su istaknuti entiteti i relacije RBAC-AOR_{SG} modela oblasti odgovornosti.

Entitet regiona (eng. *REGIONS*) omogućuje podelu elektroenergetske mreže na manje oblasti u zavisnosti od unapred definisanih kriterijuma, kao što su podela mreže po geografskim regionima, po manjim okruzima ili funkcionalnim celinama unutar regiona (npr. na nivou transformatorskih stanica unutar regiona), po naponskim nivoima, itd. REGIONS je skup svih regiona definisanih unutar elektroenergetske mreže definisanih prema jednom ili više izabranih kriterijuma.

Prema postavljenom zahtevu, model AOR-a treba da omogući kontrolu pristupa nad objektima elektroenergetske mreže za koje je moguće definisati region (tzv. fizički objekti). Za objekte kojima se ne može dodeliti takva karakteristika elektroenergetskog sistema, model AOR-a se ne razmatra, npr. podaci o poslovanju kompanije, podaci o potrošačima, podaci o konfiguraciji sistema i aplikacija (tzv. logički objekti). Skup fizičkih objekata RBAC-AOR_{SG} modela je određen skupom objekata koji pripadaju domenu realnih elektroenergetskih sistema opisanih standardnim klasama za modelovanje elektroenergetskih sistema (eng. *Common Information Model*, skr. *CIM*). Klase CIM

modela za prenosnu mrežu su definisane IEC 61970-301 standardom [41], odnosno za distributivnu mrežu definisanih IEC 61968-11 standardom [40].



Slika 14. Model AOR-a RBAC-AOR$_{SG}$ modela

Pripadnost objekta određenom regionu je opisana odgovarajućim atributom objekta (eng. *object attribute*, skr. *OATT*). Za potrebe modelovanja regiona je iskorišćena postojeća CIM klasa *Core* paketa, klasa `GeographicalRegion`. Ovim je omogućeno da region može biti definisan na nivou pojedinačnih elemenata, odnosno opreme (npr. prekidačka i zaštitna oprema, transformatori, generatori, itd.), ali i na nivou kontejnera koji služe za grupisanje opreme, npr. oprema unutar jedne transformatorske stanice, unutar određenog geografskog područja, ili oprema grupisana prema naponskom nivou.

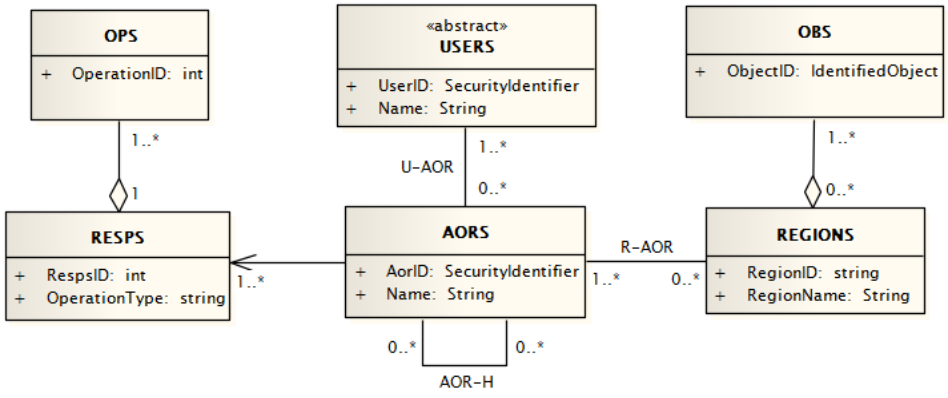
Entitet oblasti odgovornosti (skr. *AORS*) definiše skup dozvoljenih operacija nad objektima koji pripadaju određenom regionu. Ovo se postiže relacijom između regiona i oblasti odgovornosti (eng. *Region-AOR assignment*, skr. *R-AOR*), dok se relacijom između korisnika i oblasti odgovornosti (eng. *User-AOR assignment*, skr. *U-AOR*) definiše skup korisnika koji imaju pravo da izvršavaju određene tipove operacija nad objektima dodeljenih posredstvom R-AOR relacije. U predloženom RBAC-AOR$_{SG}$ modelu su definisana tri tipična tipa operacija u Smart Gridu koji predstavljaju nivoe odgovornosti (*RESPS*), ali je skup RESPS proširiv u skladu sa specifičnom zahtevima određene kompanije:

- Nadzor (eng. *supervise*) obuhvata operacije praćenja stanja elektroenergetskog sistema (statusi uređaja i opreme, tokovi snage i napona u sistemu, informacije o ispadima, itd.) na osnovu kojih se mogu identifikovati potencijalni problemi, i sprečiti kvarovi i otkazi u mreži.

- Kontrola (eng. *control*) obuhvata različite zaštitne, preventivne ili korektivne akcija u sistemu kao odgovor na različita stanja u sistemu (npr. upravljanje uređajima i opremom elektroenergetskog sistema, konfigurisanje različitih operativnih parametara koji utiču na proračune u sistemu, upravljanje incidentima, i slično).
- Ažuriranje (eng. *update*) obuhvata aktivnosti koje se odnose na inicijalni unos, kao i ažuriranje podataka kojima se opisuje model elektroenergetskog sistema (npr. podaci o generatorima, transformatorima, vodovima, prekidačima, potrošačima, o njihovoj međusobnoj povezanosti i konektivnosti).

Model hijerarhija AOR-a je prikazan relacijom AOR-H (eng. *AOR-Hierarchy*) i detaljnije će biti objašnjen u *Sekciji 5.2.1*.

Na *Slici 15.* je prikazan UML dijagram klasa RBAC-AOR$_{SG}$ modela AOR-a. R-AOR relacijom je definisano da svakom regionu može biti dodeljena jedna ili više oblasti odgovornosti, a oblast odgovornosti se može dodeliti proizvoljnom broju regiona. U-AOR relacijom je definisano da AOR može biti dodeljen proizvoljnom broju korisnika, ali najmanje jednom korisniku, a svakom korisniku može biti dodeljen proizvoljan broj oblasti odgovornosti. U zavisnosti od korisničke uloge u sistemu, moguće je da korisniku ne bude dodeljena nijedna oblast odgovornosti. Kao što je navedeno u *Sekciji 3.2.2*, za fizičke objekte se definiše pripadnost jednom regionu, ali je moguće da jedan objekat istovremeno pripada i većem broju regiona. Takođe, dozvoljeno je i da fizički objekti nemaju definisan region, npr. u fazi testiranja RTU uređaja i izmene modela elektroenergetskog sistema pre primene u produkciji. Kontrola pristupa za fizičke objekte koji nemaju definisan region odgovara kontroli pristupa logičkim objektima.



Slika 15. UML dijagram klase za oblasti odgovornosti (AORS)

5.2.1 Hijerarhija oblasti odgovornosti

Prema zahtevu C.AC.2 u cilju efikasnije organizacije i jednostavnije administracije modela kontrole pristupa potrebno je omogućiti hijerarhijsku organizaciju AOR-a. U opštem slučaju, hijerarhija AOR-a se može definisati na sledeći način:

- Oblast odgovornosti aor_1 nasleđuje aor_2 ako svi regioni koji pripadaju aor_2 pripadaju i aor_1.

Ovim je omogućeno grupisanje pojedinačnih AOR-a prema određenom kriterijumu. Na primeru sa *Slike 9.* svi AOR-i kojima je naponski nivo 11kV su grupisani u kontejner AOR_11kV. Glavna prednost uvođenja hijerarhije AOR-a je ta što je svim korisnicima kojima je dodeljen aor_1 dodeljen i aor_2. Odnosno, umesto da *korisniku3* koji treba da ima odgovornost nad svim delovima mreže sa naponskim nivoom 11kV bude dodeljen svaki AOR pojedinačno, hijerarhijom je omogućeno da uvezivanjem sa AOR_11kV za tog korisika bude definisana jedna relacija. Slično je i za *korisnika1* i *korisnika2* kojima je uz pomoć hijerarhije dodeljena odgovornost nad celim regionom, odnosno celokupnom distributivnom mrežom umesto dodele pojedinačnih AOR-a.

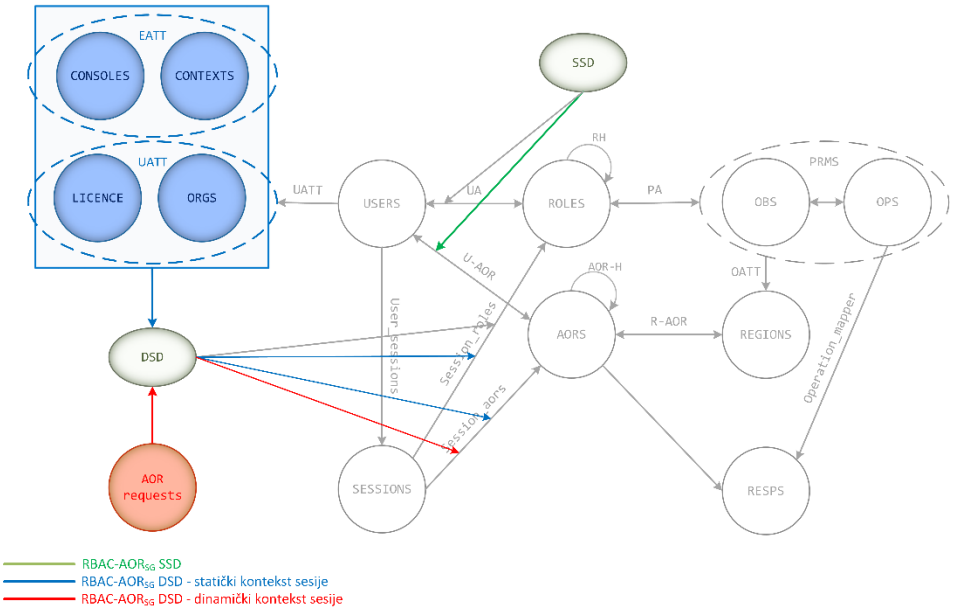
Hijerarhija AOR-a je na UML dijagramu klasa na *Slici 15.* prikazana rekurzivnom asocijacijom. Svaki AOR može imati nijedan ili više hijerarhijski nižih AOR-a, a svakom AOR-u može biti dodeljen nijedan, jedan ili više hijerarhijski viših AOR-a.

5.3 Model ograničenja i proširenja

Kao što je ranije objašnjeno, prilikom donošenja odluke o pristupu resursima često je potrebno uvažiti određene faktore koji mogu uticati na skup ovlašćenja korisnika kako prilikom uspostavljanja korisničke sesije, tako i u toku izvršavanja korisničke sesije. U Smart Gridu su identifikovani sledeći zahtevi:

- Ograničenje skupa korisničkih uloga u zavisnosti od toga da li korisnik poseduje važeću licencu (zahtev C.AC.5),
- Ograničenje skupa ovlašćenja u zavisnosti od lokacije radne stanice sa koje korisnik pristupa sistemu (zahtev C.AC.7),
- Izmena skupa ovlašćenja u zavisnosti od tipa aplikacije kojoj korisnik pristupa (zahtev C.AC.6),
- Mogućnost kontrole pristupa u interorganizacionim sistemima u zavisnosti od organizacije kojoj korisnik pripada (zahtev C.AC.8).
- Mogućnost preuzimanja odgovornosti nad AOR-ima u regularnm režimu rada sistema (C.AC.3), kao i u vanrednim situacijama (
- C.AC.4).

RBAC važi za statički model koji osim ograničenja konfliktnih uloga ne razmatra druge faktore koji bi mogli uticati na skup ovlašćenja korisnika u korisničkoj sesiji. U *Sekciji 2.4* su razmatrana različita unapređenja RBAC modela kako bi se odgovorilo specifičnih zahtevima različitih sistema. Međutim, nijedan od navedenih predloga ne može da odgovori postavljenim zahtevima u Smart Gridu. Stoga, u ovom radu se predlaže unapređenje RBAC modela ograničenja, kao što je istaknuto na *Slici 16.*



Slika 16. RBAC-AOR$_{SG}$ model ograničenja i proširenja

RBAC model statičkih ograničenja (*SSD*) je proširen tako da je u toku administracije modela moguće ograničiti kako dodelu konfliktnih uloga tako i dodelu konfliktnih AOR-a istom korisniku. Na taj način je moguće zabraniti da isti korisnik bude član jedne ili više oblasti odgovornosti u zavisnosti od definisanih SSD pravila. Na primer, korisnicima koji upravljaju prenosnim sistemom ne treba dozvoliti upravljanje nad distributivnim delom mreže (izuzetak od ovog primera može biti proces oporavka sistema od potpunog ili delimičnog prestanka napajanja sa prenosnog sistema (eng. *blackstart*), ali se ovakav scenario smatra vanrednom situacijom). Slično kao u RBAC modelu, SSD relacije se mogu primeniti i na hijerarhiju AOR-a.

RBAC model dinamičkih ograničenja (*DSD*) je proširen tako da omogući izmenu skupa ovlašćenja korisnika prilikom uspostavljanja korisničke sesije, ali i u toku izvršavanja korisničke sesije. Parametri čije se vrednosti ne menjaju u toku korisničke sesije predstavljaju statički kontekst sesije, i tu spadaju korisnički atributi (ORGS, LICENCE) i atributi okruženja (CONSOLES, CONTEXTS). Ograničenja i proširenja definisana statičkim

kontekstom sesije se mogu primeniti kako na skup korisničkih uloga i privilegija, tako i na skup oblasti odgovornosti. Nasuprot tome, parametri čije se vrednosti mogu menjati u toku izvršavanja korisničke sesije predstavljaju dinamički kontekst sesije. Ograničenja i proširenja definisana dinamičkim kontekstom sesije su primenljiva samo na oblasti odgovornosti. Tu spadaju zahtevi za ograničavanjem ili proširivanjem skupa AOR-a u korisničkoj sesiji kako u regularnom režimu rada, tako i u vanrednim situacijama (eng. *AOR requests*).

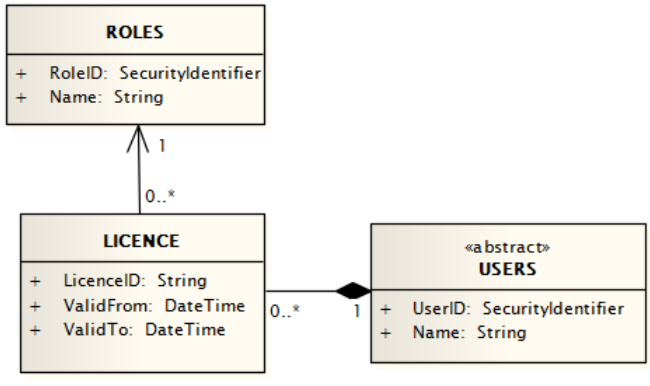
U nastavku ove sekcije dat je detaljan opis pojedinačnih elemenata RBAC-AOR$_{SG}$ modela ograničenja i proširenja.

5.3.1 Model licence

U zahtevu C.AC.5 se navodi da je za obavljanje poslova čije izvršavanje je regulisano licencom potrebno omogućiti ograničavanje skupa korisničkih uloga u zavisnosti od toga da li korisnik poseduje važeću licencu. Licenca je atribut korisnika ranije objašnjen u okviru opisa RBAC-AOR$_{SG}$ modela korisnika (videti *Sekciju 5.1*).

Na *Slici 17.* je prikazan deo UML dijagrama klasa modela korisnika relevantan za entitet licence. Za svakog korisnika je moguće definisati proizvoljan broj licenci, a licenca je relacijom kompozicije povezana sa tačno jednim korisnikom za koga se na taj način definiše period važenja date licence, odnosno period u kome će korisniku biti omogućena korisnička uloga na koju se licenca odnosi. Period važenja licence je definisan atributima `ValidFrom` i `ValidTo`, a korisnička uloga na koju se licenca odnosi je definisana relacijom asocijacije sa entitetom klase ROLES.

Prilikom uspostavljanja korisničke sesije se proverava da li su licence definisane za datog korisnika validne, odnosno da li vreme uspostavljanja sesije odgovara intervalu vremena u kom je licenca validna. Ukoliko to nije tačno, korisnička uloga na koju se licenca odnosi će biti onemogućena u datoj korisničkoj sesiji.



Slika 17. UML dijagram klase licence (LICENCE)

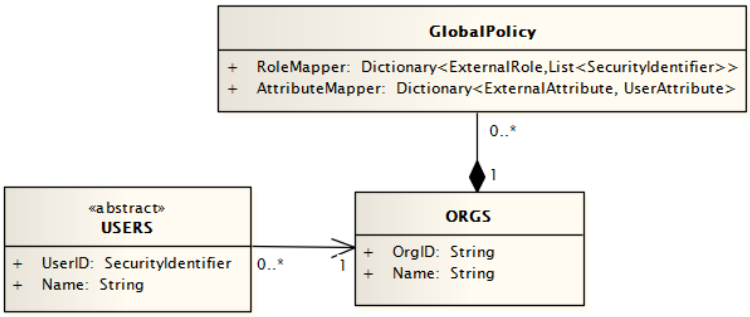
Nedostatak predloženog modela licence potiče od pretpostavke da je licenca deo statičkog konteksta sesije. Navedena pretpostavka potiče iz činjenice da je period važenja licence znatno duži od prosečnog trajanja korisničke sesije u savremenim elektroenergetskim sistemima. Ukoliko period važenja licence istekne u toku trajanja korisničke sesije, RBAC-AOR$_{SG}$ to neće detektovati i korisnička uloga će biti omogućena u toj sesija sve dok ona ne bude prekinuta. Takođe, ovaj model ne uključuje proveru da li su korisnicima zaista definisane licence za sve omogućene uloge koje treba da budu regulisane licencom, već je pretpostavka da se to definiše u okviru administracije modela.

5.3.2 Model organizacije

U zahtevu C.AC.8 se navodi da model kontrole pristupa treba da bude primenljiv kako unutar jedne organizacije (tzv. organizacije zatvorenog tipa), tako i u interorganizacionim sistemima bez uvođenja kompleksnosti administracije i sinhronizacije podataka. U okviru modela korisnika koji je opisan u *Sekciji 5.1* objašnjeno je na koji način je postavljeni problem prevaziđen u RBAC-AOR$_{SG}$ modelu. Naime, predlaže se uvođenje korisničkog atributa ORGS koji definiše pripadnost korisnika određenoj organizaciji. UML dijagrama klasa RBAC-AOR$_{SG}$ modela korisnika relevantan za entitet ORGS je prikazan na *Slici 18.*

Izvorna ogranizacija definiše skup organizacija ORGS sa kojima uspostavlja federaciju. U opštem slučaju, to može biti proizvoljan broj organizacija. U kontekstu RBAC-AOR$_{SG}$ modela, federacija se odnosi na uspostavljanje bezbednosne politike (*GlobalPolicy*) kojom se definišu pravila transformacije uloga i atributa korisnika iz eksternih organizacija na korisničke uloge i relevantne korisničke atribute iz interne organizacije. Pravilima transformacije korisničkih uloga (eng. *RoleMapper*) definiše se jedna ili više uloga izvornog sistema na koje se mapira određena uloga iz eksternog sistema. Pravilima transformacije korisničkih atributa (eng. *AttributeMapper*) definiše se korisnički atribut izvornog sistema na koji se mapira vrednost odgovarajućeg atributa iz eksternog sistema. U predloženom RBAc-AOR$_{SG}$ modelu, osim korisničkih uloga mapiraju se atributi koji se odnose na parametre licence.

Za svakog korisnika se definiše pripadnost tačno jednoj organizaciji. Ukoliko je korisnik član izvorne organizacije, model organizacije se ne razmatra prilikom uspostavljanja korisničke sesije. Za korisnike eksternih organizacija se model organizacije primenjuje prilikom uspostavljanja korisničke sesije kada se definiše skup korisničkih uloga i vrednosti atributa u izvornom sistemu. U kompanijama zatvorenog tipa RBAC-AOR$_{SG}$ je primenljiv bez naknadnih izmena. Skup ORGS je u tom slučaju prazan, odnosno ne definiše se nijedna eksterna organizacija i samim tim će sve korisničke uloge eksternih korisnika biti onemogućene.



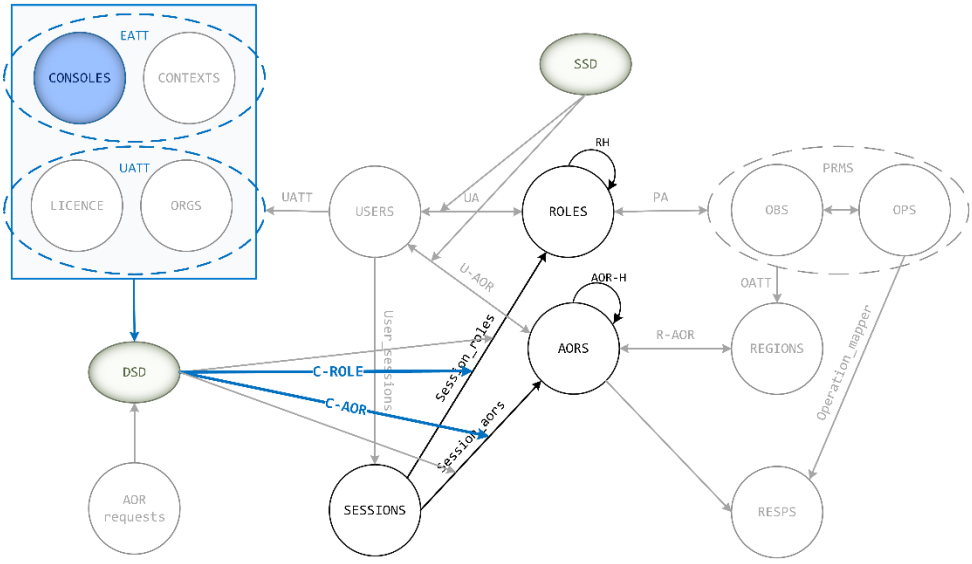
Slika 18. UML dijagram klase organizacije (ORGS)

5.3.3 Model radne stanice

U zahtevu C.AC.7 se navodi da je prilikom donošenja odluke o pristupu resursima u Smart Gridu neophodno razmotriti lokaciju ili namenu radne stanice sa koje se pristupa sistemu. Npr. pristup nadzorno-upravljačkom sistemu sa udaljenih lokacija treba da bude omogućen samo sa radnih stanica koje su poznate sistemu. U suprotnom, skup omogućenih korisničkih uloga treba da bude ograničen samo na korisničke uloge za koje je bezbednosnom politikom dozvoljen pristup sa nepoznate lokacije (npr. putem Web servisa u poslovni sistem). Takođe, korisnicima koji imaju više dodeljenih uloga unutar organizacije prilikom uspostavljanja sesije je potrebno ograničiti skup korisničkih uloga u skladu sa namenom radne stanice sa koje pristupaju sistemu (npr. ograničiti inženjerske uloge prilikom pristupa poslovnoj radnoj stanici, i obrnuto).

U ovom radu se za prevazilaženje navedenog problema predlaže uvođenje entiteta radne stanice (CONSOLES) kao što je prikazano na *Slici 19.* Radna stanica je parametar okruženja čija vrednost se razmatra prilikom uspostavljanja korisničke sesije kada korisnik pristupa sistemu i nepromenljiva je u toku izvršavanja korisničke sesije. U zavisnosti od izabrane radne stanice moguće je ograničiti skup omogućenih korisničkih uloga i/ili AOR-a prilikom uspostavljanja korisničke sesije na sledeći način:

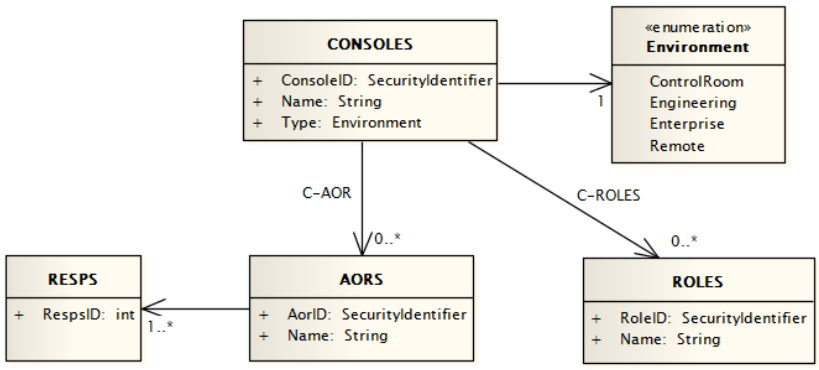
- Relacije između računara i korisničke uloge (eng. *Computer-Role Assignment*, skr. *C-ROLE*) definišu skup korisničkih uloga koje mogu biti omogućene prilikom pristupanja sistemu sa tog računara.
- Relacije između računara i oblasti odgovornosti (eng. *Computer-AOR Assignment*, skr. *C-AOR*) definišu skup oblasti odgovornosti koje mogu biti omogućene prilikom pristupanja sistemu sa određenog računara.



Slika 19. Model radne stanice RBAC-AOR$_{SG}$ modela (CONSOLES)

UML dijagramom klasa na *Slici 20.* je opisan model računara RBAC-AOR$_{SG}$ modela. `CONSOLES` je skup svih računara u sistemu. Za svaki računar se specificira tip radne stanice `ConsoleType` u zavisnosti od lokacije i/ili namene u sistemu. Tipovi radnih stanica su definisani u skladu sa zahtevima definisanim u *Sekciji 3.2.4* i opisani su enumeracijom `Environment`. Enumeracija `Environment` je proširiva za slučaj da postoje specifični zahtevi kompanija da se uvaže drugačiji tipovi radnih stanica.

Za svaku radni stanicu može biti definisan proizvoljan broj korisničkih uloga i AOR-a koji mogu biti omogućeni sa date radne stanice. Ukoliko nijedna korisnička uloga nije omogućena znači da radna stanica nije namenjenja za pristup sistemu od strane Smart Grid korisnika. Kada su u pitanju AOR-i, moguće je u potpunosti ograničiti AOR-e, a moguće je ograničiti i samo određene nivoe odgovornosti AOR-a. Na primeru inženjerske radne stanice u poslovnom sistemu, C-AOR relacije bi trebale da budu definisane tako da skup omogućenih AOR-a nikada ne uključuje mogućnost nadzora i kontrole sa tog računara, bez obzira na nivo odgovornosti koji je dodeljen korisniku.



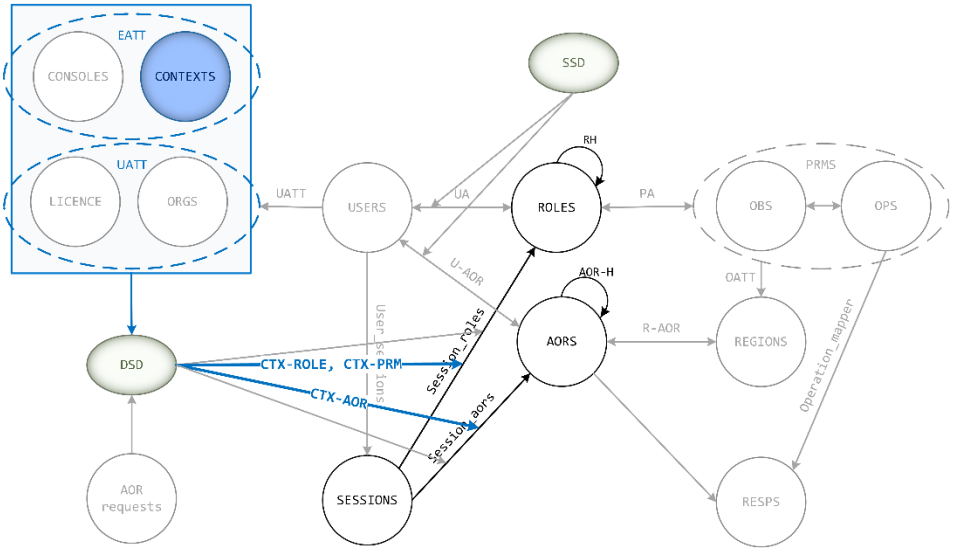
Slika 20. UML dijagram klase za radnu stanicu (CONSOLES)

5.3.4 Model aplikativnog konteksta

Prema zahtevu C.AC.6 model kontrole pristupa u Smart Gridu treba da omogući uvažavanje različitih bezbednosnih politika zavisno od tipa aplikacije kojoj se pristupa. Npr. korisnik u kontrolnoj sobi često sa iste radne stanice pristupa aplikaciji za rad u realnom vremenu i aplikaciji za simulaciju rada sistema, pri čemu u simulaciji može imati širi skup ovlašćenja nego u okviru aplikacije za rad u realnom vremenu.

U ovom radu se predlaže uvođenje entiteta aplikativnog konteksta (CONTEXTS) kao što je prikazano na *Slici 21.* U *Sekciji 3.2.3*. je identifikovano šest tipova Smart Grid aplikacija, odnosno aplikativnih konteksta: za rad u realnom vremenu, za simulaciju rada sistema, za planiranje izgradnje i održavanja elektroenergetskog sistema, za testiranje i potvrdu kvaliteta, za podršku operacijama na terenu i poslovne aplikacije. Slično kao radna stanica, tip Smart Grid aplikacije predstavlja parametar okruženja čija vrednost se ne menja u toku izvršavanja korisničke sesije. U zavisnosti od tipa konteksta moguće je ograničiti ili proširiti skup omogućenih korisničkih uloga, privilegija i/ili oblasti odgovornosti prilikom uspostavljanja korisničke sesije na sledeći način:

- Relacije između aplikativnog konteksta i korisničkih uloga (eng. CONTEXT-ROLE, skr. CTX-ROLE) definišu skup omogućenih korisničkih uloga nakon primene odgovarajuće bezbednosne politike za dati kontekst.
- Relacije između aplikativnog konteksta i privilegija (eng. CONTEXT-PERMISSION, skr. CTX-PRM) definišu skup omogućenih privilegija nakon primene odgovarajuće bezbednosne politike za dati kontekst.
- Relacije između aplikativnog konteksta i AOR-a (eng. CONTEXT-AOR, skr. CTX-AOR) definišu skup omogućenih AOR-a (uključujući i skup omogućenih odgovornosti za svaki AOR) nakon primene odgovarajuće bezbednosne politike za dati kontekst.



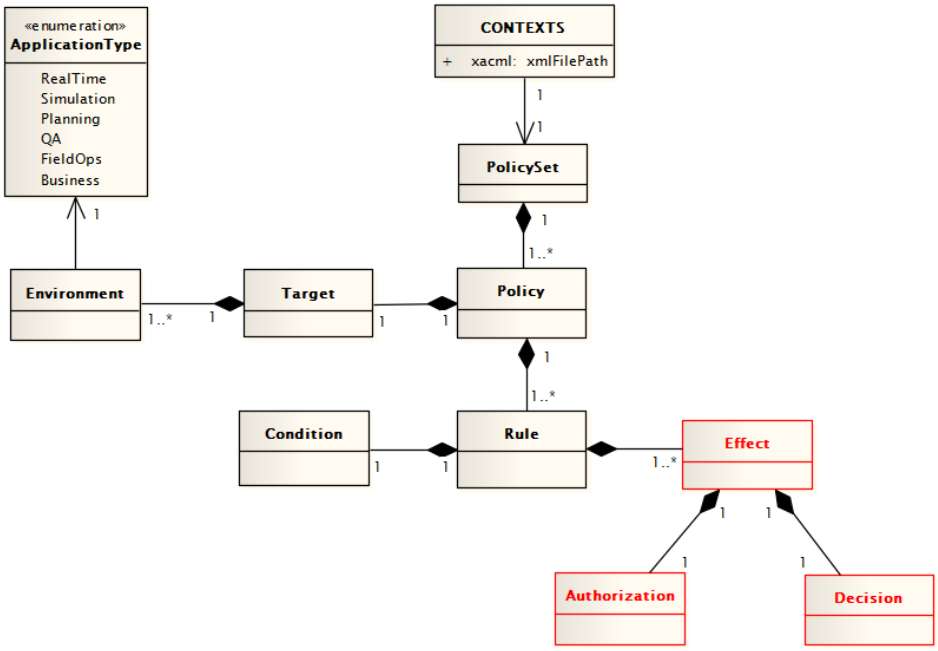
Slika 21. Model aplikativnog konteksta RBAC-AOR$_{SG}$ modela (CONTEXTS)

Za potrebe specifikacije bezbednosne politike aplikativnog konteksta proširen je XACML jezik za specifikaciju ABAC politika, predstavljen u *Sekciji 2.5.2.* Za razliku od XACML pravila koja rezultuju odlukom o dozvoli pristupa (pristup odobren, pristup zabranjen), rezultat obrade RBAC-AOR$_{SG}$ pravila aplikativnog konteksta treba da definiše da li će neka korisnička uloga, privilegija ili oblast odgovornosti biti omogućena prilikom uspostavljanja korisničke sesije. Stoga, `Effect` element koji definiše da li je pristup odobren ili zabranjen je izmenjen tako da sada definiše odluku o tome da li je određeno ovlašćenje omogućeno ili ne.

Na *Slici 22.* je prikazan UML dijagram klase RBAC-AOR$_{SG}$ aplikativnog konteksta. Aplikativni kontekst je modelovan entitetom `CONTEXTS` koji predstavlja skup XACML bezbednosnih politika (`PolicySet`) definisanih u XML datoteci. Svaka bezbednosna politika (`Policy`) definiše skup autorizacionih pravila (`Rule`), a elementom `Target` se definiše ono na šta se svaka bezbednosna politika odnosi. U slučaju RBAC-AOR$_{SG}$ modela, bezbednosna politika se odnosi na tip aplikativnog konteksta. Kako tip aplikativnog konteksta predstavlja stanje okruženja pri kome određena politika važi, `Target` element je u ovom slučaju element `Environment` čija vrednost je određena tipom aplikativnog konteksta, `ApplicationType`.

Bezbednosna pravila se sastoje iz `Condition` i `Effect` elemenata. `Condition` elementom se definiše uslov koji mora da se zadovolji da bi pravilo moglo da se primeni. U slučaju RBAC-AOR$_{SG}$ modela uslov se odnosi na to da li je korisnička uloga specificirana uslovom omogućena datom korisniku. Ukoliko `Condition` element nije definisan za neko pravilo, podrazumeva se da se pravilo primenjuje uvek. `Effect` elementom se zatim specificira odluka (`Decision` element) o tome da li je ovlašćenje (`Authorization`

element) omogućeno ili ne nakon primene bezbednosne politike. Svako pravilo može imati proizvoljan broj `Effect` elemenata.



Slika 22. UML dijagram klase za aplikativni kontekst (CONTEXTS)

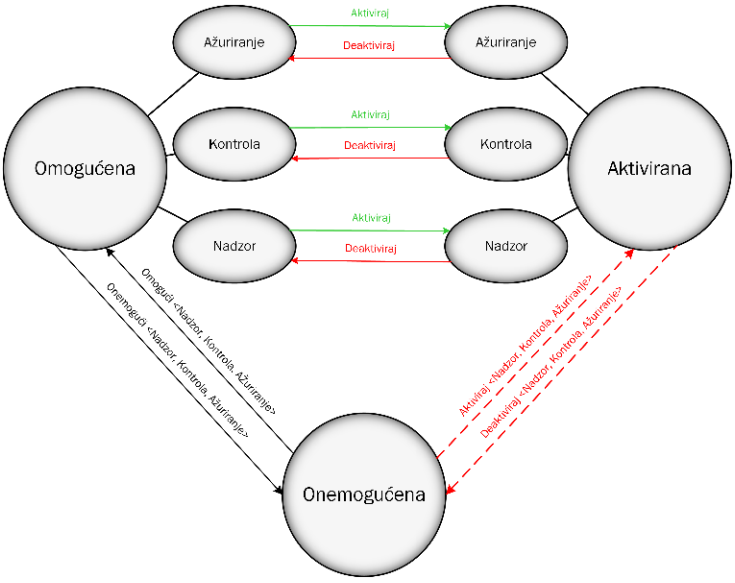
5.3.5 Model zahteva za izmenu stanja AOR-a

Prema zahtevima C.AC.3 i C.AC.4 neophodno je obezbediti kontinualan nadzor i upravljanje svim delovima elektroenergetske mreže kako u regularnom režimu rada, tako i u vanrednim situacijama. U regularnom režimu rada to znači da korisnik (operater u kontrolnoj sobi) ne bi smeo da prekine korisničku sesiju ukoliko bi u tom slučaju neki od AOR-a ostao bez nadzora i kontrole, dok se u vanrednim situacijama to odnosi na mogućnost preuzimanja privremene odgovornosti nad AOR-ima za koje korisnici nemaju ovlašćenje. Odavde proizilazi da korisnici ne moraju prilikom uspostavljanja korisničke sesije da aktiviraju sve AOR-e koji su im dodeljeni prilikom administracije modela ili uspostavljanja korisničke sesije. Umesto toga, korisnici treba da imaju mogućnost da na zahtev aktiviraju i deaktiviraju dodeljene AOR-e u toku izvršavanja korisničke sesije, pri čemu deaktivacija može biti dozvoljena samo ukoliko dati AOR neće u tom slučaju ostati bez nadzora i kontrole najmanje jednog korisnika. U vanrednim situacijama treba da bude dozvoljeno da korisnicima budu privremeno aktivirani AOR-i koji im nisu omogućeni prilikom uspostavljanja korisničke sesije. Ovi zahtevi mogu biti inicirani isključivo od strane visoko privilegovanih korisnika u vanrednim situacijama i njima se mogu aktivirati AOR-i u bilo kojoj aktivnoj sesiji.

Koncept aktiviranja/deaktiviranja korisničkih uloga nakon uspostavljanja korisničke sesije nije podržan u RBAC modelu. Jedno od unapređenja RBAC-a razmatranih u *Sekciji 2.4.1* je TRBAC model koji uvažava vremensku dimenziju na taj način što se prilikom uspostavljanja, ali i u toku izvršavanja korisničkih sesija proverava da li je dozvoljeno da u tom vremenskom periodu korisnička uloga bude omogućena. Ukoliko je dozvoljeno, prilikom uspostavljanja korisničke sesije uloga postaje aktivirana. Korisnička uloga se deaktivira prilikom zatvaranja korisničke sesije, pri čemu je moguće da u toku sesije prestane da važi uslov. To uključuje automatsku deaktivaciju u svim aktivnim sesijama gde je data uloga bila aktivirana. Međutim, zahtevi za aktiviranjem i deaktiviranjem AOR-a se razliku od koncepta aktivacije/deaktivacije korisničkih uloga TRBAC modela, jer korisnicima na zahtev treba da bude omogućena izmena stanja dodeljenih AOR-a na nivou pojedinačnih sesija. Takođe, ovaj model ne podržava mogućnost da se na zahtev privilegovanih korisnika omogući aktiviranje onemogućenih uloga na određeni skup aktivnih korisničkih sesija.

U ovom radu se predlaže uvođenje stanja AOR-a kao što je prikazano UML dijagramom stanja na *Slici 23.* AOR-i mogu biti u jednom od sledećih stanja:

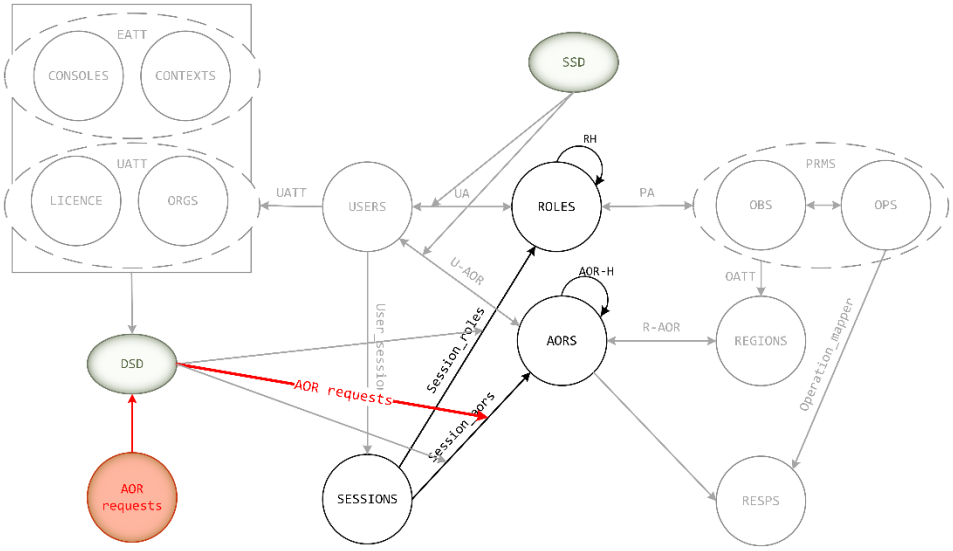
- Omogućeni (eng. *enabled AORs*) – AOR-i koje korisnik može da aktivira u toku korisničke sesije, uključujući i nivo odgovornosti za svaku od omogućenih oblasti.
- Onemogućeni (eng. *disabled AORs*) – AOR-i koje korisnik ne može da aktivira u toku sesije.
- Aktivirani (eng. *active AORs*) – AOR-i nad kojima korisnik ima određeni nivo odgovornosti u toku izvršavanja korisničke sesije. Kako korisnik ne mora da aktivira sve omogućene AOR-e prilikom uspostavljanja sesije, AOR-i su prošireni atributom *ActiveOnLogin* koji označava da li će omogućeni AOR biti automatski i aktiviran prilikom uspostavljanja sesije. Svi omogućeni AOR-i mogu biti aktivirati u toku izvršavanja sesije na zahtev korisnika.
- Deaktivirani (eng. *inactive AORs*) – omogućeni AOR-i koje nisu aktivirani u datoj korisničkoj sesiji, ali ih korisnik može aktivirati na zahtev u toku izvršavanja sesije.



Slika 23. UML dijagram stanja oblasti odgovornosti i nivoa odgovornosti

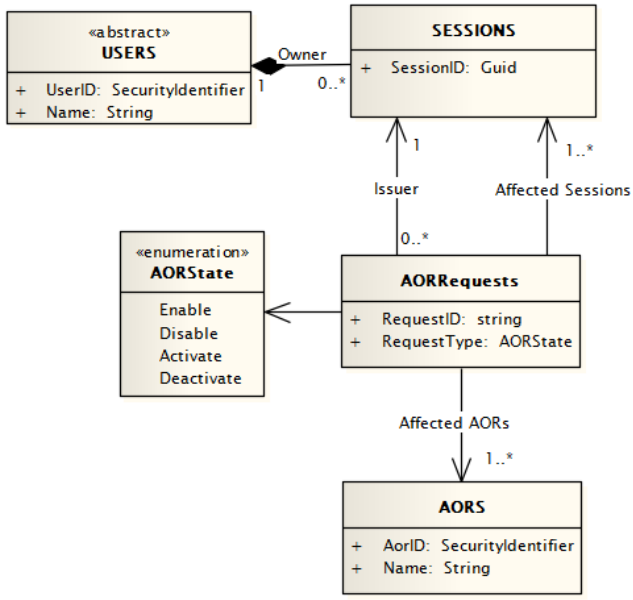
U kontekstu modela ograničenja i proširenja, uvodi se koncept dinamičkog konteksta sesije, kao što je istaknuto na *Slici 24.* Zahtevima o promeni stanja AOR-a (*AOR requests*) moguće je izmeniti skup aktiviranih AOR-a u toku izvršavanja korisničke sesije i to prema sledećim pravilima:

- U regularnom režimu rada korisnici mogu aktivirati/deaktivirati omogućene AOR-e u okviru svoje korisničke sesije, uz unapred definisana ograničenja. Na primer, korisnik ne može deaktivirati određeni AOR ukoliko to znači da će taj AOR ostati bez nadzora ili kontrole. Ovakvi zahtevi o promeni stanja AOR-a se nazivaju regularni AOR zahtevi (eng. *regular AOR requests*).
- U vanrednim situacijama, visoko privilegovani korisnici mogu izdati zahteve za aktiviranjem onemogućenih AOR-a (i obrnuto) za određeni skup korisnika, odnosno njihovih aktivnih korisničkih sesija. Ovakvi zahtevi o promeni stanja AOR-a se nazivaju vanredni/hitni AOR zahtevi (eng. *emergency AOR requests*).



Slika 24. RBAC-AOR$_{SG}$ model dinamičkog konteksta sesije

UML dijagram klase zahteva o promeni stanja AOR-a je prikazan na *Slici 25.* Svaki zahtev sadrži informaciju o tome iz koje sesije je zahtev izdat (odnosno ko je izdavalac zahteva) i na koje aktivne sesije se zahtev odnosi. U regularnoj situaciji, izdavalac zahteva je korisnik koji je aktivirao sesiju u okviru koje se zahtev izdaje, a zahtev se odnosi upravo na sesiju iz koje se izdaje. S druge strane, u vanrednim situacijama se zahtev može odnositi na jednu ili više aktivnih sesija različitih korisnika, a izdavalac zahteva mora biti korisnik koji ima odgovarajuća ovlašćenja, u suprotnom će zahtev biti odbijen. Odnos između zahteva za promenu stanja AOR-a i izdavaoca zahteva je opisan relacijom asocijacije `Issuer`, a između zahteva za promenu stanja AOR-a i sesije za koju se izdaje zahtev relacijom asocijacije `AffectedSessions`. Tip zahteva (`RequestType`) specificira stanje u koje AOR treba da pređe, dok je relacijom `AffectedAORs` definiše skup AOR-a na koje se dati zahtev odnosi. U okviru jednog zahteva dozvoljeno je izmeniti stanje za više AOR-a odjednom.



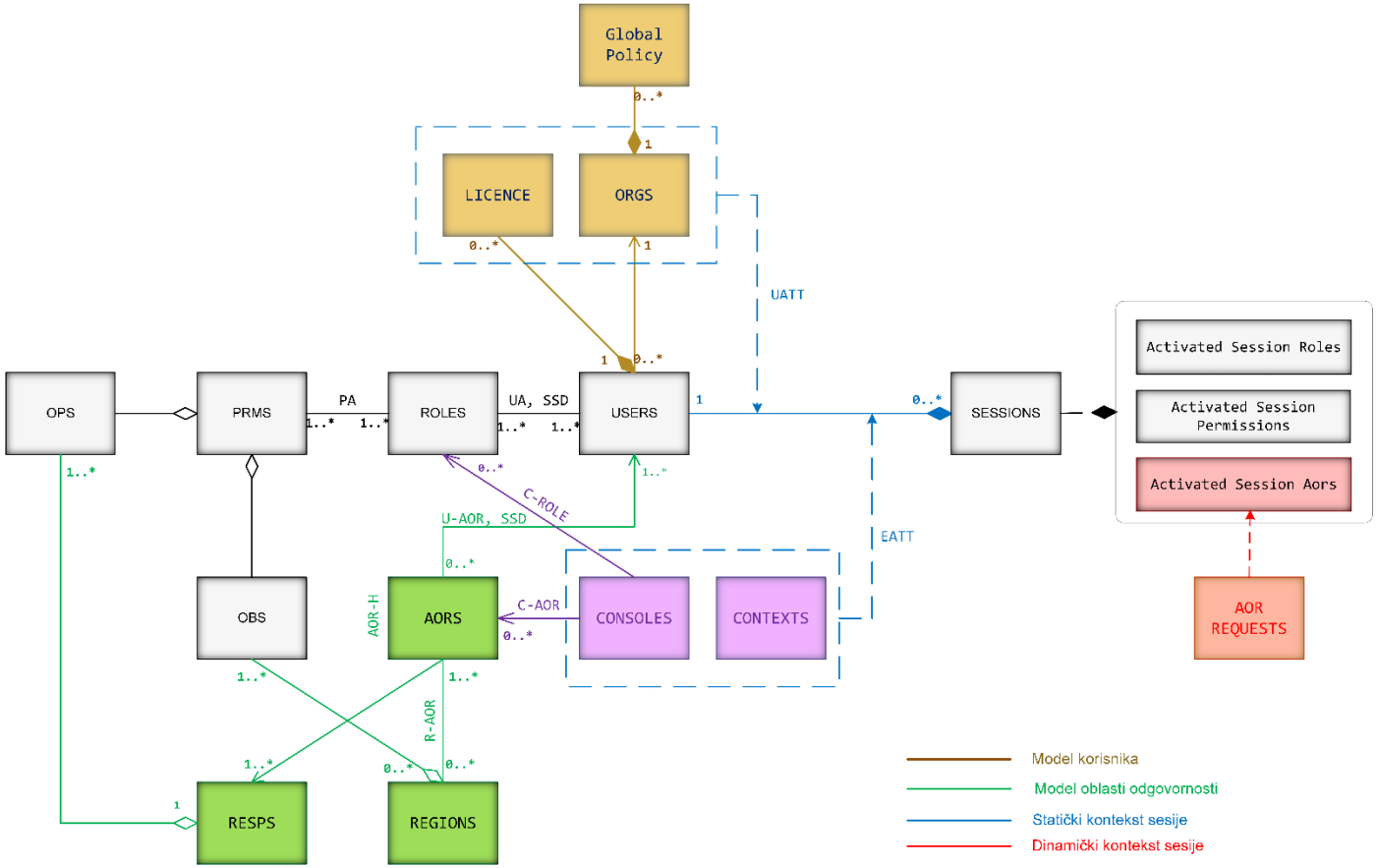
Slika 25. UML dijagram klase zahteva za izmenu stanja AOR-a (AORRequests)

5.4 Postupak sprovođenja kontrole pristupa

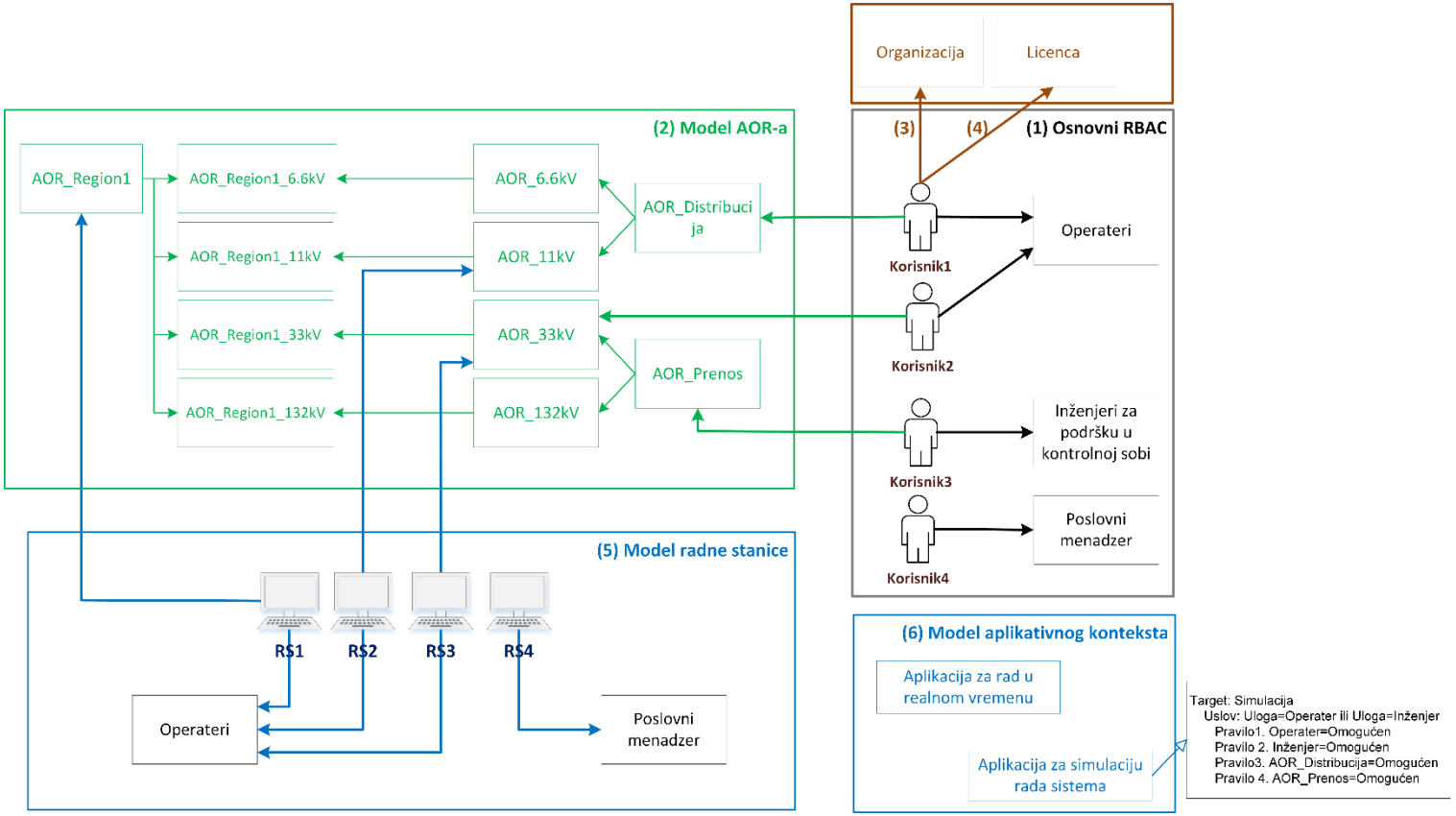
U ovoj sekciji je objašnjen postupak sprovođenja kontrole pristupa definisan RBAC-AOR$_{SG}$ modelom. Prvo je opisan postupak formiranja statičkog i dinamičkog konteksta sesije RBAC-AOR$_{SG}$ modela, a zatim je definisan postupak donošenja odluke o pristupu resursima primenom RBAC-AOR$_{SG}$ modela.

5.4.1 Formiranje statičkog i dinamičkog konteksta sesije

UML dijagramom klasa na *Slici 26.* je prikazana formalna specifikacija RBAC-AOR$_{SG}$ modela, pri čemu je za potrebe razumevanja dinamičkog konteksta sesije UML dijagram klasa proširen zahtevima za izmenu stanja AOR-a. Punim linijama su prikazane statičke relacije RBAC-AOR$_{SG}$ modela, odnosno relacije koje se definišu prilikom administracije modela: model korisnika, model oblasti odgovornosti, SSD model, model radne stanice i aplikativnog konteksta. Isprekidanim linijama su označene relacije modela RBAC-AOR$_{SG}$ ograničenja i proširenja. U nastavku je na primerima korisnika u kontrolnoj sobi objašnjen postupak formiranja statičkog i dinamičkog konteksta sesije. Korak po korak primena entiteta RBAC-AOR$_{SG}$ modela je ilustrovana na *Slici 27.*



Slika 26. UML dijagram klasa RBAC-AOR$_{SG}$ modela



Slika 27. Postupak formiranja statičkog konteksta sesije RBAC-AOR$_{SG}$ modela

Prvi korak (1) se odnosi na slučaj kada se kontrola pristupa zasniva na RBAC modelu. U zavisnosti od dodeljene korisničke uloge, korisnici mogu da upravljaju elektroenergetskom mrežom (operater), da upravljaju analitičkim funkcijama i proračunima u elektoenergetskoj mreži (inženjer za podršku u kontrolnoj sobi) ili da obavljaju poslove u finansijskom sektoru (poslovni menadžer). Primenom RBAC modela, sa aspekta dodeljenih ovlašćenja nema razlike između korisnika *korisnik1* i *korisnik2*.

Drugi korak (2) je primena modela AOR-a čime je omogućeno ograničavanje prava korisnika prilikom administracije modela u zavisnosti od dodeljenih oblasti odgovornosti unutar elektroenergetskog sistema. Za primer će biti uzeta podela elektroenergetske mreže sa *Slike 9.* gde je mreža podeljenja prema naponskim nivoima (npr. *AOR_Distribucija, AOR_11kV*), prema geografskim regionima (npr. *AOR_Region1*) i prema oba kriterijuma (npr. *AOR_Region1_11kV*). U ovom primeru je istaknut samo deo modela AOR-a potreban za razumevanje uticaja modela AOR-a na kontrolu pristupa. U poređenju sa RBAC-om, nakon primene modela AOR-a korisnici *korisnik1* i *korsnik2* imaju različita prava iako pripadaju istoj korisničkoj ulozi. *Korisnik1* kome je dodeljen *AOR_Distribucija* može da upravlja samo distributivnim delom mreže, a *korisnik2* kome je dodeljen *AOR_33kV* prenosnim delom mreže od 33kV. Slična raspodela bi se mogla primeniti i za inženjere za podršku u kontrolnoj sobi. U tom slučaju, *korisnik3* kome je dodeljen *AOR_Prenos* može da upravlja funkcijama i proračunima samo u okviru prenosnog dela mreže.

Sledeći korak je uvažavanje UATT i EATT parametara prilikom uspostavljanja korisničke sesije. Prvo se primenjuju UATT parametri, a zatim EATT parametri i to sledećim redosledom:

1. Primena RBAC-AOR$_{SG}$ modela organizacije (korak 3), kada se uloge i atributi iz eksternog sistema mapiraju na korisničke uloge i atribute u izvornom sistemu u skladu sa definisanom globalnom politikom. Ovim je omogućena dodela korisničkih uloga i atributa izvornog sistema eksternim korisnicima prilikom uspostavljanja sesije bez potrebe da za te korisnike postoje nalozi i u izvornom sistemu. U slučaju da korisnik pripada izvornoj organizaciji, ovaj korak se ne razmatra.
2. Primena RBAC-AOR$_{SG}$ modela licence (korak 4). Na primeru obavljanja uloge operatera koja može biti regulisana važećom licencom to znači da ukoliko korisnici *korisnik1* ili *korisnik2* nemaju licence koje su validne prilikom uspostavljanja korisničke sesije, oni neće moći da upravljaju elektroenergetskom mrežom bez obzira na dodeljenu ulogu operatera. Kako uloga inženjera za podršku u kontrolnoj sobi nije regulisana licencom, za korisnika *korisnik3* se ovo ograničenje neće uvažavati.
3. Primena RBAC-AOR$_{SG}$ modela radne stanice (korak 5). Na datom primeru modela radnih stanica to znači da sa RS1, RS2 i RS3 korisnicima koji nisu operateri neće biti omogućene dodeljene uloge, dok sa radne stanice RS4 će dodeljene uloge biti omogućene samo poslovnim menadžerima. Ukoliko korisnici kojima je dodeljena uloga operatera pokušaju da pristupe sistemu sa

RS4, uloga operatera će im biti onemogućena, jer je na RS4 omogućena samo uloga poslovnog menadžera. Dodatno, korisnicima *korisnik1* i *korisnik2* su omogućene uloge operatera na RS1, RS2 i RS3, ali u zavisnosti od izabrane radne stanice oni će imati različita prava u korisničkoj sesiji. Na primer, iako *korisnik2* ima pravo upravljanja svim delovima mreže sa naponskim nivoom 33kV, kada pristupa sistemu sa RS1 moći će da upravlja samo AOR_*Region1_33kV*, dok sa RS2 koja je namenjena za upravljanje distributivnim delom mreže naponskog nivoa 11kV neće imati pravo upravljanja. Prenosnim delom mreže naponskog nivoa 33kV moći će da upravlja samo sa RS3 kojoj je omogućen AOR_33kV.

4. Primena RBAC-AOR$_{SG}$ modela aplikativnog konteksta (korak 6). Tipične aplikacije u kontrolnoj sobi su aplikacija za rad u realnom vremenu i aplikacija za simulaciju rada sistema. Kako aplikacija za rad u realnom vremenu zahteva najstrožu bezbednosnu politiku, kada korisnik pristupa simulaciji moguće je proširiti skup ovlašćenja u toj korisničkoj sesiji. Na datom primeru bezbednosne politike za simulaciju, kada *korisnik2* pristupa sistemu sa RS1, u simulaciji će imati pravo da upravlja celokupnom mrežom iako u realnom vremenu ima pravo upravljanja samo AOR_*Region1_33kV*. Takođe, moći će da pokreće analitičke funkcije za šta u realnom vremenu nema ovlašćenja. Slično, *korisnik3* će u simulaciji moći da upravlja sistemom iako takva ovlašćenja u okviru aplikacija za rad u realnom vremenu nema.

Rezultat prethodno opisanih koraka je statički kontekst sesije kojim je definisan skup omogućenih korisničkih uloga, privilegija i AOR-a u datoj korisničkoj sesiji. Skup omogućenih uloga i privilegija je istovremeno i skup aktiviranih uloga i privilegija u datoj korisničkoj sesiji, jer se dinamički kontekst sesije ne odnosi na ove entitete. Skup aktiviranih AOR-a je određen skupom omogućenih AOR-a kojima je atribut *ActiveOnLogin* tačan, ali se ovaj skup može izmeniti zahtevima za izmenu stanja AOR-a u okviru dinamičkog konteksta sesije po sledećim pravilima:

- Regularni Smart Grid korisnici mogu da aktiviraju i deaktiviraju skup omogućenih AOR-a izdavanjem zahteva o promeni stanja AOR-a u okviru svoje korisničke sesije. Ograničenje koje se nameće prilikom deaktivacije je to da oblast odgovornosti ne sme ostati bez nadležnosti najmanje jednog korisnika nakon deaktivacije, pre svega kada su u pitanju kritične operacije, kao što je nadzor i upravljanje sistemom u realnom vremenu. Ograničenje se primenjuje kako prilikom deaktivacije u toku izvršavanja korisničke sesije, tako i u slučaju automatske deaktivacije prilikom prekida korisničke sesije.
- Visoko privilegovani Smart Grid korisnici mogu aktivirati onemogućeni skup ovlašćenja, ali i onemogućiti aktivirani skup ovlašćenja izdavanjem zahteva za promenu stanja AOR-a za određeni skup aktivnih korisničkih sesija.

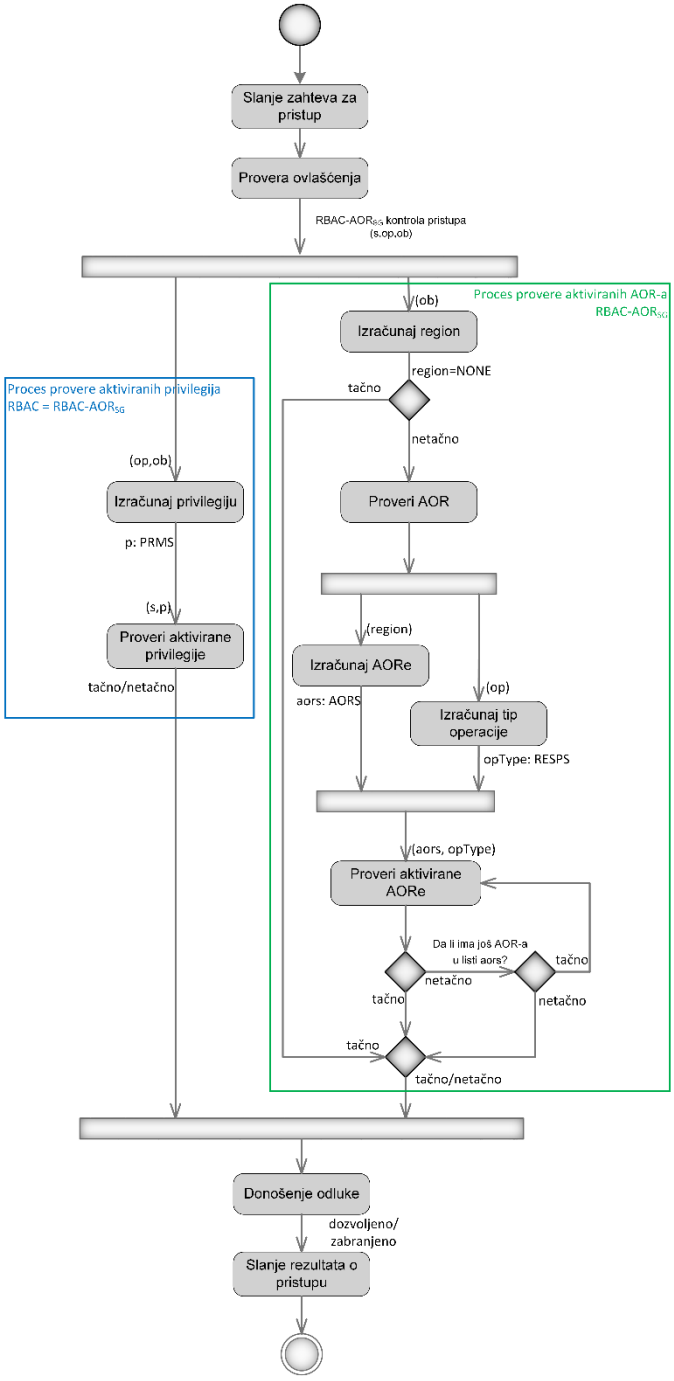
5.4.2 Postupak donošenja odluke o pristupu

UML dijagramom aktivnosti na *Slici 28.* prikazan je postupak sprovođenja kontrole pristupa koji se sastoji iz dva nezavisna procesa provere ovlašćenja da se izvrši zahtevana operacija *op* nad određenim objektom *ob* u korisničkoj sesiji *s*:

1. Proces provere aktiviranih privilegija (eng. *Permission Check*), odnosno proces kojim se proverava da li je u okviru korisničke sesije iz koje je zahtev iniciran aktivirana privilegija koja je definisana zahtevanom operacijom nad određenim objektom. Iako između RBAC i RBAC-AOR$_{SG}$ modela postoje značajne razlike u postupku računanja skupa aktiviranih privilegija, proces provere privilegija se sprovodi na isti način. Prvo se na osnovu zahtevane operacije i objekta računa privilegija koja se proverava, a zatim se proverava da li je ta privilegija aktivirana u korisničkoj sesiji *s*.
2. Proces provere aktiviranih oblasti odgovornosti (eng. *AOR Check*), odnosno proces kojim se proverava da li je u okviru korisničke sesije iz koje je zahtev iniciran aktivirana oblast odgovornosti koja je dodeljena regionu objekta, sa nivoom odgovornosti potrebnim za izvršavanje zahtevane operacije. Prvo se određuje region objekta kome se pristupa. Za objekte koji nemaju definisan region, proces provere aktiviranih oblasti odgovornosti se ne razmatra, odnosno postupak donošenja odluke o pristupu je zasnovan samo na rezutatu provere aktiviranih privilegija. U suprotnom, potrebno je odrediti oblasti odgovornosti dodeljene regionu (*aors*) i tip operacije koja se izvršava (*opType*). Na osnovu ovih vrednosti se proverava da li je u korisničkoj sesiji *s* aktivirana oblast odgovornosti *aors* sa nivoom odgovornosti koji odgovara tipu zahtevane operacije *opType*. S obzirom da jedan region može imati više AOR-a koji su mu dodeljeni, rezultat provere aktiviranih AOR-a je potvrdan ukoliko postoji bar jedan AOR iz liste *aors* aktiviran sa odgovarajućim nivoom odgovornosti.

Kako su navedeni procesi potpuno nezavisni, oni se izvršavaju paralelno kako bi se minimizovao uticaj kontrole pristupa na performanse celokupnog sistema.

Na osnovu dobijenih rezultata provere aktiviranih privilegija i oblasti odgovornosti se donosi autorizaciona odluka o pristupu. Da bi pristup bio dozvoljen, potrebno je da rezultat provere aktiviranih privilegija i aktiviranih AOR-a bude tačan. U suprotnom, pristup će biti zabranjen.



Slika 28. UML dijagram aktivnosti postupka donošenja odluke o pristupu u RBAC-AOR$_{SG}$ modelu

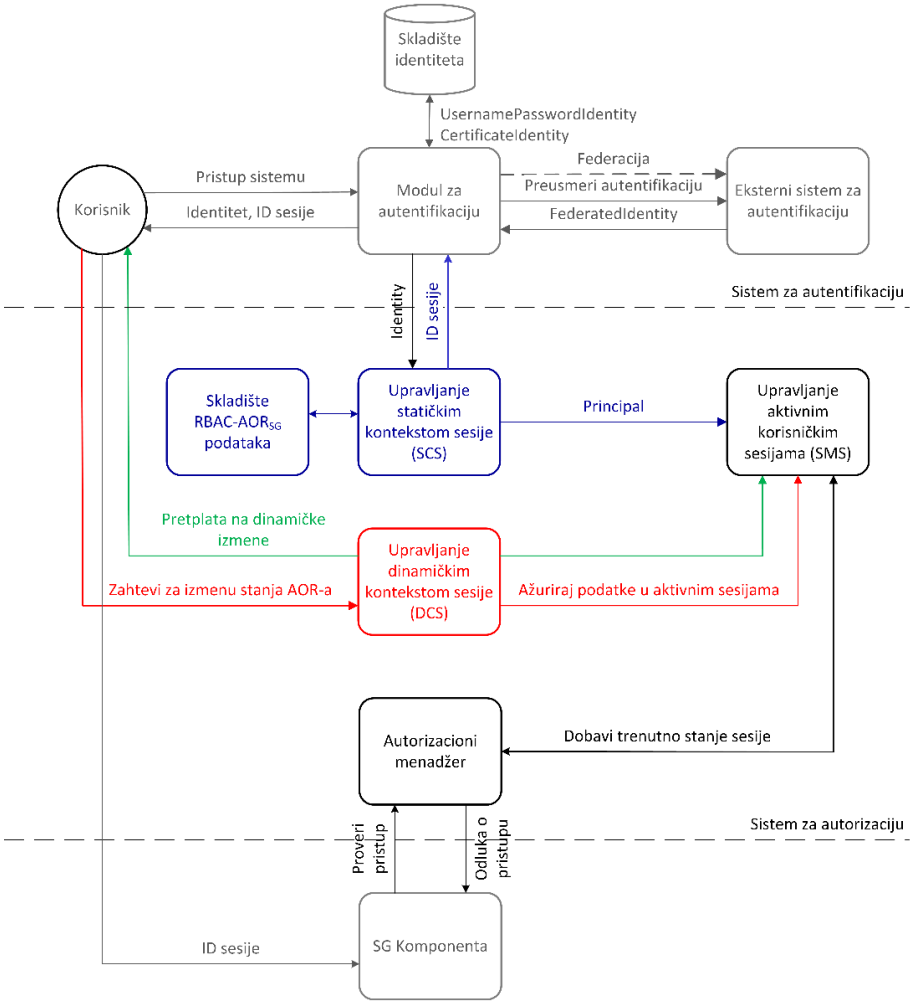
6 Softverska arhitektura sistema za kontrolu pristupa

Kako bi se ispitala primenljivost predloženog RBAC-AOR$_{SG}$ modela kontrole pristupa i proverila usaglašenost sa postavljenim zahtevima, razvijen je prototip sistema za kontrolu pristupa u Smart Gridu (eng. *Smart Grid Access Control Service*, skr. *SG-ACS*). SG-ACS obezbeđuje centralizovano upravljanje procesom sprovođenja autorizacionih politika u skladu sa RBAC-AOR$_{SG}$ modelom. Prototip predloženog rešenja je testiran u simuliranom Smart Grid okruženju koje je razvijeno prema modelu bezbednosne arhitekture za Smart Grid prikazanom u *Sekciji 3.4*. SG-ACS je bezbednosni servis koji je smešten u zoni upravljanja. Osim malog broja visoko privilegovanih korisnika za potrebe administracije i nadgledanja, SG-ACS servisu mogu da pristupe komponente Smart Grid sistema koje koriste usluge ovog servisa za donošenje odluke o pristupu resursima. To može biti bilo koja komponenta komandno-kontrolnog sistema (npr. SCADA, NMS, DMS, EMS, OMS), ili poslovnog sistema (npr. CIS, GIS, WMS, WFS), uključujući i servise zone javnog pristupa (npr. Web servis), kao što je prikazano na *Slici 10.*

Pritom, pristup je ograničen na slanje upita o proveri pristupa bez mogućnosti modifikacije podataka u SG-ACS. Jedini način da se izmene podaci SG-ACS servisa je slanjem zahteva za izmenu stanja AOR-a, ali je prihvatanje takvih zahteva strogo kontrolisano. Naime, Smart Grid korisnici ne mogu da pošalju zahtev direktno ka SG-ACS već se zahtevi šalju isključivo posredstvom modula čija namena je validacija zahteva, formiranje zahteva u očekivanom formatu i njegovo prosleđivanje na izvršavanje.

Softverska arhitektura SG-ACS servisa je prikazana UML dijagramom kolaboracije na *Slici 29.* S obzirom da je ulaz u SG-ACS digitalni identitet korisnika koji se formira u procesu autentifikacije, na dijagramu je istaknut i podsistem za autentifikaciju. Integracija sa podsistemom za autentifikaciju izvršena je posredstvom modula za upravljanje statičkim kontekstom sesije (eng. *Static Context Service*, skr. *SCS*). SCS omogućuje formiranje statičkog konteksta sesije nakon uspešne autentifikacije, što uključuje dobavljanje vrednosti svih parametara iz skladišta podataka RBAC-AOR$_{SG}$ modela koji mogu uticati na autorizacione odluke, i upravljanje redosledom njihove primene prilikom uspostavljanja korisničke sesije. Ukoliko je statički kontekst sesije uspešno kreiran, korisniku se šalje jedinstveni identifikator sesije koji se kasnije koristi u procesu donošenja odluke o pristupu. Podaci o omogućenim i aktiviranim ulogama, privilegijama i AOR-ima se šalju do komponente za upravljanje aktivnim korisničkim sesijama (eng. *Session Management Service*, skr. *SMS*) koja služi za skladištenje podataka o svim aktivnim korisničkim sesijama u sistemu. Za razliku od digitalnog identiteta koji sadrži informacije o autentifikovanom korisniku, principal je entitet koji enkapsulira informacije o ovlašćenjima autentifikovanog korisnika u korisničkoj sesiji. Komponenta za upravljanje dinamičkim kontekstom korisničkih sesija (eng. *Dynamic Context Service*, skr. *DCS*) omogućuje centralizovanu obradu zahteva za izmenu stanja AOR-a koji se

izdaju u toku izvršavanja korisničkih sesija od strane Smart Grid korisnika. Pre slanja zahteva na izvršenje SMS komponenti, DCS proverava da li je zahtev validan, odnosno da li korisnik koji je inicirao zahtev ima potrebna ovlašćenja. Takođe, posredstvom DCS modula Smart Grid korisnici dobijaju obaveštenje o svim izmenama aktivnih korisničkih sesija. Autorizacioni menadžer je komponenta zadužena za donošenje autorizacionih odluka u sistemu u skladu sa postupkom donošenja odluke o pristupu RBAC-AOR$_{SG}$ modela. Ova komponenta predstavlja interfejs ka ostalim komponentama Smart Grida koje koriste usluge SG-ACS servisa. Prilikom donošenja autorizacionih odluka, autorizacioni menadžer komunicira sa SMS komponentom kako bi dobio informacije o aktiviranim ovlašćenjima u korisničkoj sesiji iz koje je iniciran zahtev za pristup.



Slika 29. UML dijagram kolaboracije sistema za kontrolu pristupa zasnovanog na RBAC-AOR$_{SG}$ modelu

6.1 Modul za upravljanje bezbednosnim podacima

Modul za upravljanje bezbednosnim podacima obuhvata sledeće komponente od kojih svaka omogućuje skladištenje određenog tipa podataka RBAC-AOR$_{SG}$ modela, kao i interfejs za njihovo čitanje i administraciju:

- Komponenta za upravljanje korisničkim ulogama (eng. *RolesManager*), u okviru koje se skladište podaci u vezi sa korisničkim ulogama i privilegijama, uključujući i njihove međusobne relacije. Opis metoda ove komponente dat je u *Prilogu A.1*.
- Komponenta za upravljanje oblastima odgovornosti (eng. *AorsManager*) u okviru koje se skladište podaci o AOR-ima i regionima, kao i relacije AOR-a sa korisnicima i regionima u sistemu. Opis metoda ove komponente dat je u *Prilogu A.2.*
- Komponenta za upravljanje licencama (eng. *LicencesManager*) je zadužena za skladištenje, administraciju i čitanje korisničkih licenci u sistemu. Opis metoda ove komponente dat je u *Prilogu A.3.*
- Komponenta za upravljanje radnim stanicama (eng. *ConsolesManager*) u okviru koje se skladište podaci o radnim stanicama u sistemu, uključujući i skup omogućenih korisničkih uloga i oblasti odgovornosti sa svake radne stanice. Opis metoda ove komponente dat je u *Prilogu A.4.*
- Komponenta za upravljanje aplikativnim kontekstom (eng. *ContextManager*) je namenjena za upravljanje autorizacionim pravilima. Na osnovu definisanog tip aplikativnog konteksta i skup omogućenih korisničkih uloga, ova komponenta definiše skup autorizacionih pravila koje je potrebno primeniti u datoj korisničkoj sesiji. Opis metoda ove komponente dat je u *Prilogu A.5.*
- Komponenta za upravljanje globalnim politikama (eng. *ExternalPolicyManager*) je namenjena za mapiranje eksternih uloga i atributa na vrednosti iz izvornog sistema prema pravilima definisanim u okviru repozitorijuma globalnih politika. Opis metoda ove komponente dat je u *Prilogu A.6.*

6.2 Modul za upravljanje statičkim kontekstom sesije

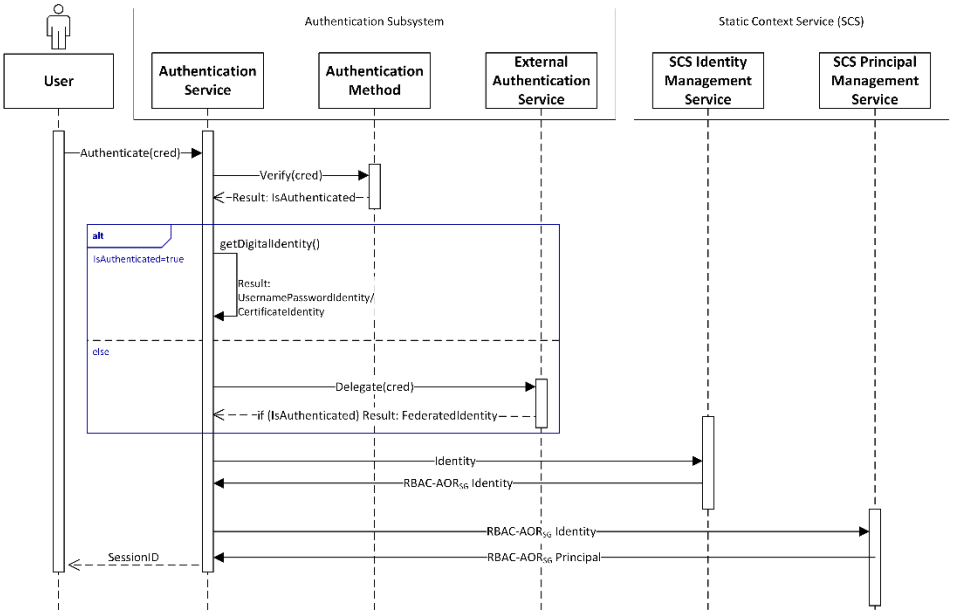
Namena podsistema za upravljanje statičkim kontekstom sesije (eng. *Static Context Service*, skr. *SCS*) je sprovođenje RBAC-AOR$_{SG}$ ograničenja i proširenja prilikom uspostavljanja korisničke sesije i formiranje statičkog konteksta sesije. Ulazni parametar za SCS je digitalni identitet korisnika čiji format se razlikuje u zavisnosti od tipa autentifikacije. SCS je zadužen za dobavljanje bezbednosnih podataka o pristiglom identitu i formiranje jedinstvenog principala koji enkapsulira podatke o ovlašćenjima korisnika bez obzira na tip autentifikacije.

UML dijagramom sekvenci na *Slici 30.* je prikazan postupak kreiranja statičkog konteksta sesije, uključujući i integraciju sa podsistemom za autentifikaciju. Podsistem

za autentifikaciju je ulazna tačka svakog sistema za kontrolu pristupa. Namena podsistema za autentifikaciju je validacija identiteta korisnika koji šalje zahtev za pristup sistemu. Predloženo rešenje podržava dva tipa autentifikacije korisnika iz izvorne organizacije: autentifikacija korišćenjem korisničkog imena i lozinke, kao i autentifikacija digitalnilnim sertifikatom koji identitet korisnika povezuje sa njegovim privatnim ključem. Prilikom formiranja digitalnog identiteta, iz skladišta identiteta se dobavljaju vrednosti atributa organizacije i licence, kao i skup korisničkih uloga koje su dodeljene datom korisniku. U interorganizacionim sistemima gde je uspostavljen labavo spregnuti federativni odnos, autentifikaciona logika se delegira partnerskoj organizaciji od poverenja tako da je eksterni sistem za autentifikaciju u potpunosti odgovoran za skladištenje, administraciju i autentifikaciju eksternih korisnika.

SCS čine dve komponente, koje su detaljno objašnjene u nastavku ove sekcije, dok je detaljan opis njihovih interfejsa dat u *Prilogu A.7*.

1. komponenta za upravljanje RBAC-AOR$_{SG}$ identitetom (eng. *SCS Identity Management Service*, skr. *SCS IMS*) zadužena za formiranje RBAC-AOR$_{SG}$ identiteta koji enkapsulira podatke o autentifikovanim korisnicima bez obzira na tip autentifikacije. Formirani RBAC-AOR$_{SG}$ identitet sadrži podatke o atributima datog korisnika, kao i skup dodeljenih uloga.
2. komponenta za upravljanje RBAC-AOR$_{SG}$ principalom (eng. *SCS Principal Management Service*, skr. *SCS PMS*) zadužena za formiranje RBAC-AOR$_{SG}$ principala koji enkapsulira podatke o omogućenim i aktiviranim ovlašćenjima korisnika u datoj korisničkoj sesiji, odnosno predstavlja statički kontekst sesije.

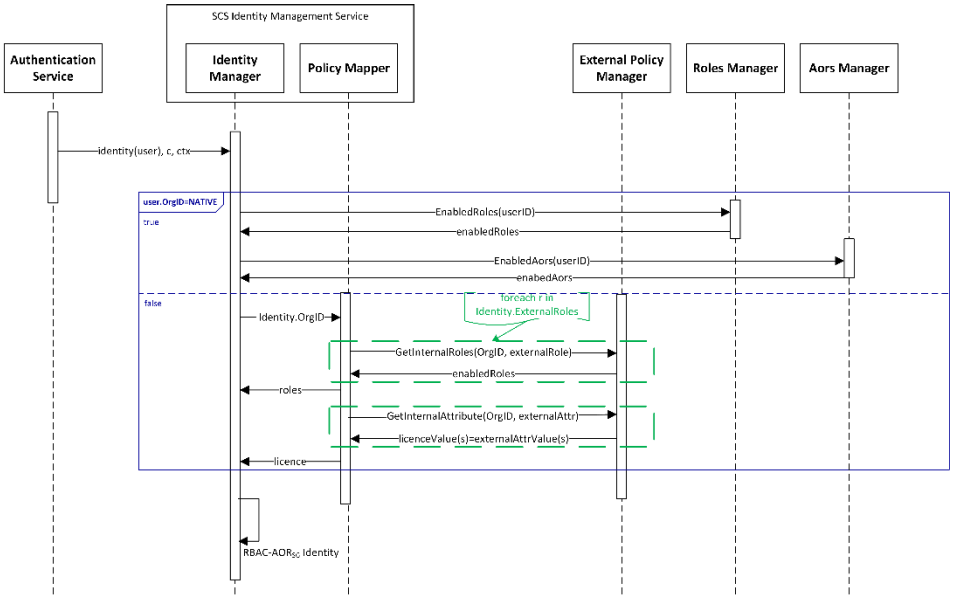


Slika 30. UML dijagram sekvence procesa formiranja statičkog konteksta sesije

6.2.1 Komponenta za upravljanje RBAC-AOR$_{SG}$ identitetom

Kao što je ranije pomenuto, SCS komponenta je tačka integracije SG-ACS servisa sa podsistemom za autentifikaciju. Podsistem za autentifikaciju šalje digitalni identitet uspešno autentifikovanog korisnika, pri čemu se format identiteta razlikuje u zavisnosti od tipa autentifikacije. Namena SCS komponente za upravljanje identitetom, odnosno SCS IMS je formiranje uniformnog RBAC-AOR$_{SG}$ identiteta koji sadrži informacije o autentifikovanim korisnicima bez obzira na tip autentifikacije. To uključuje pre svega informacije propisane RBAC-AOR$_{SG}$ modelom korisnika: jedinstveni identifikator i ime korisnika, organizacija, licenca i podaci o dodeljenim korisničkim ulogama i oblastima odgovornosti.

UML dijagram sekvenci procesa formiranja RBAC-AOR$_{SG}$ digitalnog identiteta je prikazan na *Slici 31.* Podsistem za autentifikaciju prosleđuje SCS modulu sve potrebne informacije o korisniku koji pristupa sistemu (identitet korisnika, radna stanica sa koje je korisnik pristupio sistemu i izabrana aplikacija). U zavisnosti od organizacije kojoj korisnik pripada, *IdentityManager* komponenta sama vrši dobavljanje podataka o korisničkim ulogama i AOR-ima, ili prosleđuje zahtev za transformaciju korisničkih uloga i atributa *PolicyMapper* komponenti. Za korisnike iz izvorne organizacije *IdentityManager* dobavlja informacije o korisničkim ulogama i AOR-ima posredstvom komponente za upravljanje ulogama (*RolesManager*), odnosno oblastima odgovornosti (*AorsManager*). Ukoliko korisnik nije član izvorne organizacije, *PolicyMapper* određuje skup internih uloga, kao i vrednosti atributa za datog korisnika na osnovu globalne politike koja je uspostavljena sa organizacijom kojoj korisnik pripada. Informacije o pravilima transformacije *PolicyMapper* dobija posredstvom komponente za upravljanje globalnim politikama (*ExternalPolicyManager*). Rezultat je RBAC-AOR$_{SG}$ digitalni identitet koji enkapsulira podatke o svim validnim korisnicima u sistemu.



Slika 31. UML dijagram sekvenci procesa formiranja RBAC-AOR$_{SG}$ digitalnog identiteta

6.2.2 Komponenta za upravljanje RBAC-AOR$_{SG}$ principalom

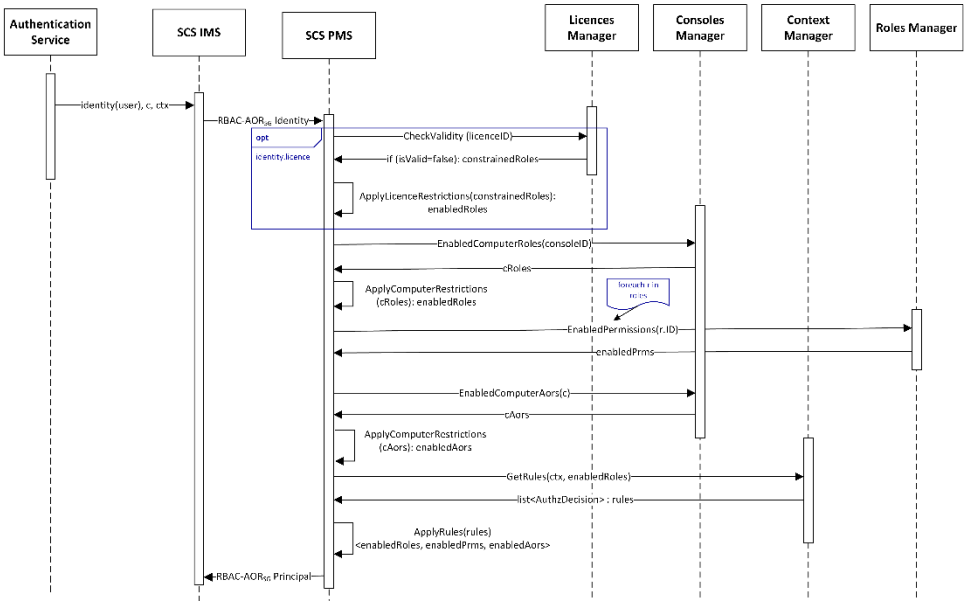
Nakon formiranja RBAC-AOR$_{SG}$ identiteta sledi primena RBAC-AOR$_{SG}$ modela ograničenja i proširenja. SCS komponenta za upravljanje principalima, odnosno SCS PMS konsultuje različite komponente modula za upravljanje bezbednosnim podacima radi dobavljanja informacija potrebnih za kreiranje statičkog konteksta sesije. UML dijagram sekvence procesa formiranja RBAC-AOR$_{SG}$ principala je prikazan na *Slici 32.*

Po prijemu RBAC-AOR$_{SG}$ identiteta, prvo se proverava validnost licence pozivom metode *LicencesManager* komponente, odnosno proverava se da li je istekao period važenja licence koja je dodeljena korisniku. U slučaju da je licenca nevažeća, uloga regulisana datom licencom će biti isključena iz skupa omogućenih korisničkih uloga. Kao što je označeno na dijagramu, provera validnosti licence je opciona, odnosno ukoliko za korisnika nije definisana nijedna licenca, provera se izostavlja.

Sledeći korak je dobavljanje omogućenih korisničkih uloga i oblasti odgovornosti za radnu stanicu sa koje korisnik pristupa sistemu posredstvom modula za upravljanje radnim stanicama (*ConsolesManager*), kao i računanje skupa omogućenih korisničkih uloga, omogućenih privilegija i oblasti odgovornosti nakon primene ovih ograničenja.

Poslednji korak prilikom kreiranja statičkog konteksta sesije je primena autorizacionih pravila u zavisnosti od tipa aplikativnog konteksta. Modul za upravljanje aplikativnom kontekstom (*ContextManager*) vraća skup ovlašćenja koje je potrebno omogućiti ili onemogućiti u redosledu u kom ih je potrebno primeniti. Rezultat primene autorizacionih pravila je bezbednosni principal koji enkapsulira podatke o omogućenim

korisničkim ulogama, privilegijama i oblastima odgovornosti u uspostavljenoj sesiji nakon primene RBAC-AOR$_{SG}$ ograničenja i proširenja.



Slika 32. UML dijagram sekvence procesa formiranja RBAC-AOR$_{SG}$ principala

6.3 Modul za upravljanje korisničkim sesijama

Modul za upravljanje korisničkim sesijama čine dve komponente, koje su detaljno opisane u nastavku ove sekcije, dok je detaljan opis njihovih interfejsa dat u *Prilogu A.8.*

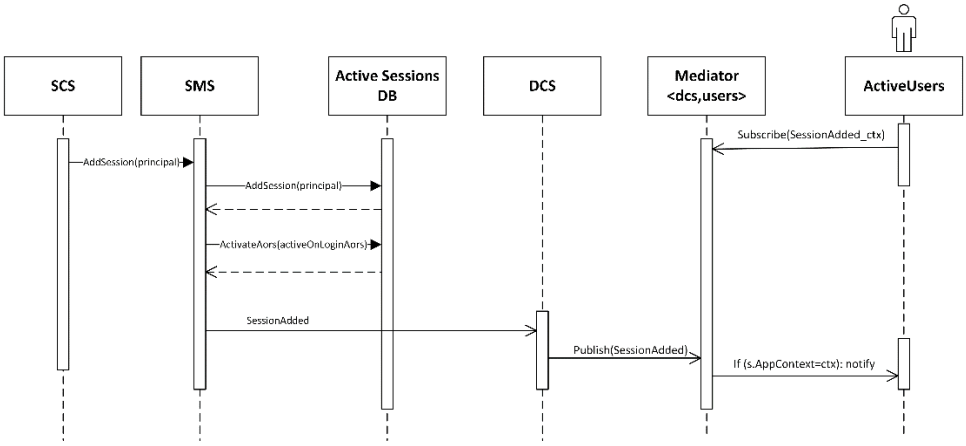
1. servis za upravljanje aktivnim korisničkim sesijama (eng. *Session Management Service*, skr. *SMS*) koji upravlja podacima o svim aktivnim korisničkim sesijama u sistemu,
2. servis za upravljanje dinamičkim kontekstom sesija (eng. *Dynamic Context Service*, skr. *DCS*), odnosno komponenta odgovorna za upravljanje zahtevima izdatim u toku izvršavanja korisničkih sesija i obaveštavanje korisnika o izmenama aktivnih korisničkih sesija.

6.3.1 Servis za upravljanje aktivnim korisničkim sesijama

Osnovna uloga SMS komponente je upravljanje podacima o aktivnim korisničkim sesijama, odnosno skladištenje podataka o aktiviranim korisničkim ulogama, privilegijama i oblastima odgovornosti za svaku aktivnu korisničku sesiju. Na taj način omogućeno je centralizovano dobavljanje podataka o stanju svake sesije.

Prilikom uspostavljanja korisničke sesije, modul za upravljanje statičkim kontekstom sesije (SCS) kreira bezbednosni principal koji zatim prosleđuje SMS komponenti. Dobijene podatke o principalu SMS skladišti u memorijskoj bazi podataka, a zatim aktivira skup omogućenih AOR-a u korisničkoj sesiji kojima je vrednost atributa *ActiveOnLogin* tačna. Za aktivirane oblasti odgovornosti se aktiviraju svi omogućeni nivoi odgovornosti u toj sesiji. Zaduženja SMS komponente prilikom uspostavljanja korisničke sesije su prikazana UML dijagramom sekvenci na *Slici 33.*

Mehanizmom pretplate je omogućeno da svi aktivni korisnici budu obavešteni da je uspostavljena nova sesija: izvor događaja je DCS modul kome SMS komponenta šalje informaciju o novododatoj korisničkoj sesiji, a zatim DCS generiše događaj o novododatnoj korisničkoj sesiji. Korisnici se pretplaćuju na klasu događaja koja odgovara njihovom aplikativnom kontekstu, a mediator `dcs-users` filtrira novonastale događaja u zavisnosti od aplikativnog konteksta i šalje notifikacije zainteresovanim korisnicima. Sličan mehanizam pretplate postoji i u slučaju prekida korisničke sesije, kao i prilikom obaveštavanja aktivnih korisnika o tome da je određena sesija prekinuta.

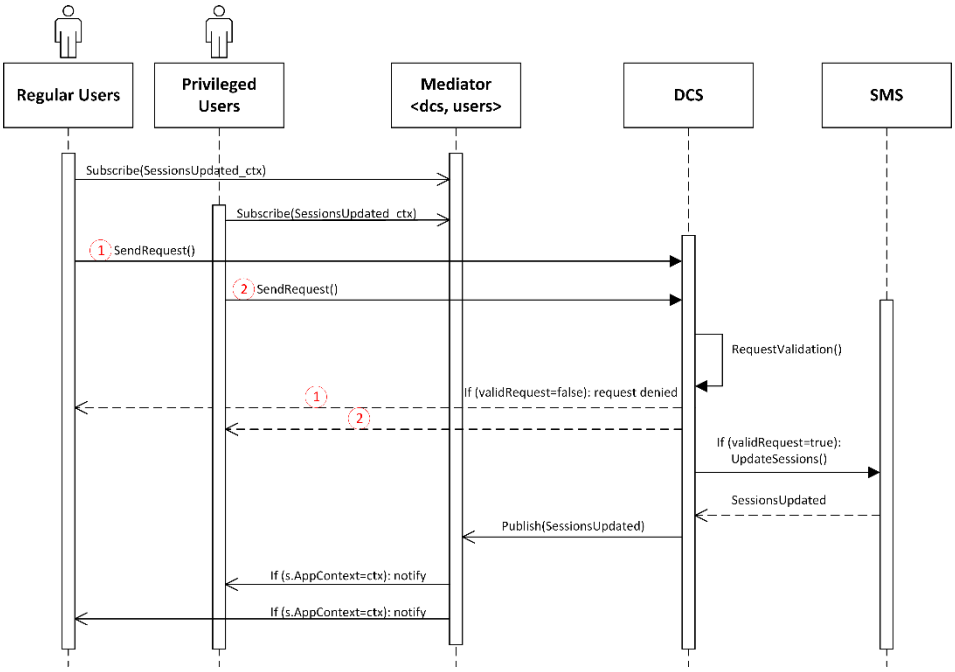


Slika 33. UML dijagram sekvence dodavanja nove korisničke sesije

6.3.2 Servis za upravljanje dinamičkim kontekstom sesije

DCS je komponenta namenjena za upravljanje zahtevima za izmenu stanja AOR-a u sistemu, kao i generisanje događaja o bilo kakvim izmenama o aktivnim korisničkim sesijama u sistemu.

Nakon prijema novog zahteva, prvo se proverava da li je izdati zahtev validan. Validni zahtevi se šalju SMS komponenti koja ažurira bazu aktivnih korisničkih sesija. UML dijagram sekvence za upravljanje dinamičkim kontekstom sesije je prikazan na *Slici* 34.



Slika 34. UML dijagram sekvence upravljanja dinamičkim kontekstom sesija

Kao što je prikazano UML dijagramom na *Slici 34.*, zahtevi za izmenu stanja AOR-a mogu biti izdati od strane regularnih Smart Grid korisnika koji imaju pravo da aktiviraju i deaktiviraju skup omogućenih oblasti odgovornosti u toku izvršavanja korisničke sesije. Takođe, privilegovani Smart Grid korisnici, tzv. supervizori, mogu izdavati zahteve za izmenu stanja AOR-a i na taj način aktivirati onemogućeni skup ovlašćenja, ali i onemogućiti aktivirani skup ovlašćenja u toku aktivnih sesija različitih korisnika. S obzirom da Smart Grid korisnici ne smeju da imaju direktan pristup komponentama bezbednosnog servisa, zahtevi se šalju posredstvom DCS modula koji validne zahteve prosleđuje na dalje izvršavanje SMS komponenti. Po prijemu zahteva, DCS proverava da li korisnik koji je inicirao zahtev ima odgovarajuća ovlašćenja u datoj korisničkoj sesiji, a zatim i da li će u slučaju zahteva za deaktivaciju AOR ostati bez nadležnosti bar jednog aktivnog korisnika (pre svega kada su u pitanju kritične operacije tipa nadzora i kontrole). U slučaju uspešne validacije, zahtev za izmenu stanja AOR-a se šalje SMS komponenti gde se ažurira baza aktivnih korisničkih sesija.

Slično kao i prilikom uspostavljanja nove korisničke sesije, svi aktivni korisnici treba da budu obavešteni o izmenama u aktivnim sesijama nakon izvršenja zahteva za izmenu stanja AOR-a. S obzirom da je RBAC-AOR$_{SG}$ model namenjen za kontrolu pristupa u sistemima za rad u realnom vremenu, brzina obaveštavanja korisnika o kritičnim akcijama u sistemu je od ključnog značaja za pouzdan i efikasan rad sistema. Stoga, model zahteva za izmenu stanja AOR-a je baziran na mehanizmu pretplate koji omogućuje slanje poruka svim zainteresovanim klijentima u trenutku kada se određena

promena (događaj) desi, bez potrebe da svaki klijent sam zahteva podatke od servisa. Izvor događaja je DCS komponenta kojoj SMS šalje informaciju o izmenama u aktivnim korisničkim sesijama. DCS zatim generiše događaj o izmenama aktivnih korisničkih sesija. Korisnici se pretplaćuju na klasu događaja koja odgovara njihovom aplikativnom kontekstu. Mediator `dcs-users` filtrira novonastale događaja u zavisnosti od aplikativnog konteksta i šalje notifikacije zainteresovanim korisnicima.

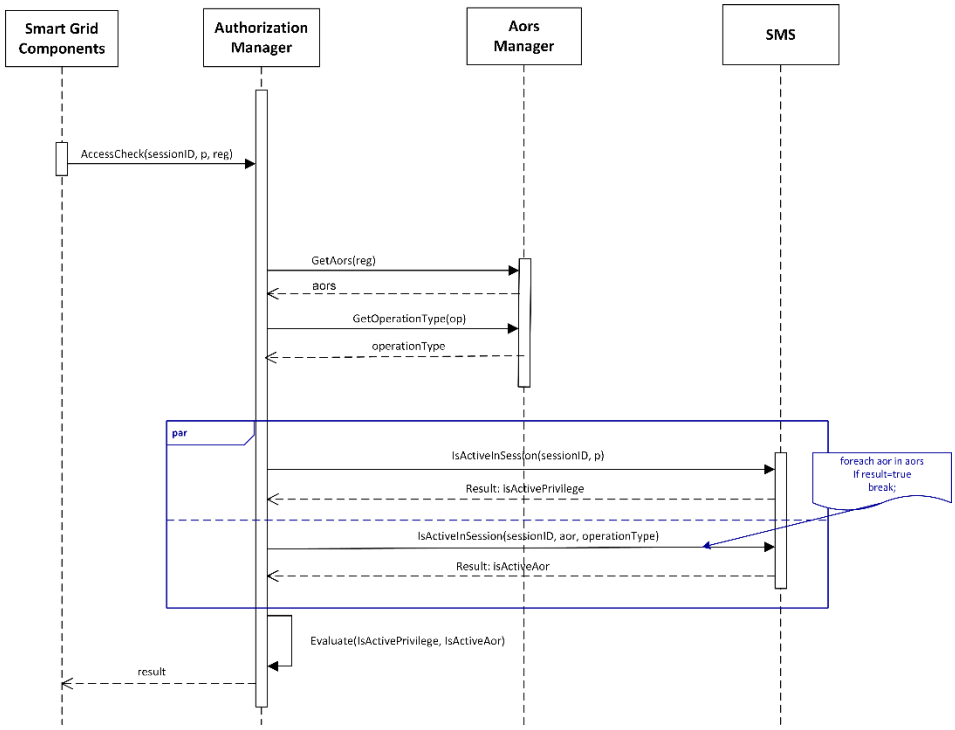
6.4 Modul za donošenje autorizacionih odluka

Namena podsistema za donošenje autorizacionih odluka (eng. *Authorization Manager*) je donošenje odluke o izvršavanju zahtevane operacije nad određenim resursom u sistemu. Odluka se donosi u skladu sa postupkom sprovođenja kontrole pristupa RBAC-AOR$_{SG}$ modela, koji je opisan u *Sekciji 5.4.2*. Autorizacioni menadžer pruža interfejs ka ostalim Smart Grid komponentama koje koriste usluge sistema za kontrolu pristupa.

UML dijagramom sekvenci na *Slici 35.* je prikazan postupak donošenja autorizacionih odluka. Po prijemu zahteva, autorizacioni menadžer u paraleli može da izvršava dva nezavisna procesa provere ovlašćenja:

1. Proces provere aktiviranih privilegija, koji podrazumeva proveru da li je u korisničkoj sesiji aktivirana privilegija definisana kao operacija nad objektom.
2. Proces provere aktiviranih oblasti odgovornosti, koji podrazumeva proveru da li je u korisničkoj sesiji aktiviran bar jedan AOR koji je dodeljen regionu objekta, takav da aktivirani nivo odgovornosti odgovara tipu zahtevane operacije. Ukoliko objekat nema dodeljeni region, proces provere aktiviranih oblasti odgovornosti se ne razmatra, odnosno smatra se da je rezultat provere aktivnih oblasti odgovornosti tačan.

Zahtev za proveru pristupa, odnosno pravo izvršavanja određene operacije nad objektom u sistemu može stizati od različitih komponenti Smart Grid sistema. Pre slanja upita o aktivnim privilegijama i odgovornostima u korisničkoj sesiji ka SMS komponenti, autorizacioni menadžer posredstvom komponente za upravljanje AOR-ima dobavlja informacije o AOR-ima za region kome objekta pripada, kao i o tipu operacije. Na osnovu rezultata SMS servisa, autorizacioni menadžer računa da li je izvršavanje zahtevane operacije nad određenim objektom iz korisničke sesije dozvoljeno. Opis metoda modula za donošenje autorizacionih odluka je dat u *Prilogu A.9*.



Slika 35. UML dijagram sekvence postupka donošenja autorizacionih odluka

.

7 Prikaz i diskusija rezultata

Verifikacija primenljivosti RBAC-AOR$_{SG}$ modela kontrole pristupa u Smart Gridu i ispitivanje usklađenosti predloženog rešenja sa postavljenim zahtevima je izvršena simulacijama na test sistemu. Test sistem je pojednostavljeno Smart Grid okruženje koje obuhvata sisteme za upravljanje i planiranje elektroenergetske mreže u okviru koga je integrisan prototip servisa za kontrolu pristupa u skladu sa modelom bezbednosne arhitekture prikazanim u *Sekciji 3.4*. Testovi koji su izvršavani u okviru eksperimentalnog istraživanja su formirani na osnovu realnih poslovnih procesa elektroenergetskih kompanija.

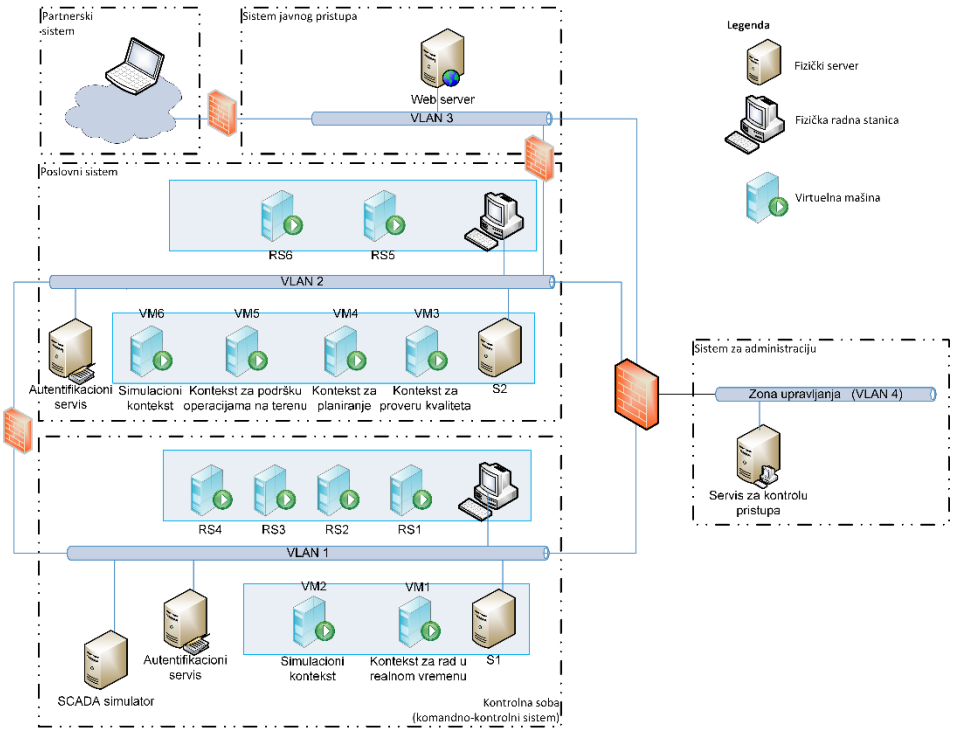
U nastavku ove sekcije dat je opis test sistema, kao i konfiguracija sistema za kontrolu pristupa baziranog na RBAC-AOR$_{SG}$ modelu, na kome će biti bazirana sva eksperimentalna istraživanja. Nakon izvršenih eksperimenata i prikaza rezultata, analizirani su dobijeni rezultati i diskutovano je njihovo značenje, sa naglaskom na prednosti predloženog rešenja u poređenju sa RBAC modelom.

7.1 Opis test sistema

Test sistem u kome je izvršeno eksperimentalno istraživanje je prikazan na *Slici 36.* Bezbednosne zone su implementirane u skladu sa preporukama industrijskih standarda, odnosno svaka bezbednosna zona predstavlja poseban VLAN, a komunikacija između VLAN-ova je kontrolisana *firewall* uređajima.

Za potrebe eksperimentalnog istraživanja korišćen je SCADA simulator koji simulira komunikaciju sa procesnim sistemom, čime je omogućen razvoj testnog okruženja bez prisustva potrebne opreme i konekcija ka procesnom postrojenju (npr. transformatorske stanice, lokalno upravljanje, itd.). U kontrolnoj sobi se na jednom fizičkom serveru S1 nalaze dve virtuelne mašine, VM1 i VM2. Na VM1 se nalaze moduli sistema za nadzor i kontrolu, analizu i optimizaciju elektroenergetskog sistema (eng. *Utility Management System*, skr. *UMS*) za rad u realnom vremenu i koji komuniciraju sa SCADA simulatorom. Na VM2 je simulacioni kontekst koji radi nad replikom podataka sistema za rad u realnom vremenu bez mogućnosti njihove izmene. Na fizičkoj radnoj stanici u kontrolnoj sobi nalaze se četiri VM, na *Slici 36.* označene sa RS1, RS2, RS3 i RS4, sa kojih je moguće pristupiti kontekstima u ovom sistemu. U poslovnom sistemu se na fizičkom serveru S2 nalaze četiri virtuelne mašine na kojima se nalaze kontekst za proveru kvaliteta (VM3), kontekst za planiranje (VM4), kontekst za podršku operacijama na terenu (VM5) i simulacioni kontekst (VM6). Svi navedeni konteksti rade nad replikom podataka sistema za rad u realnom vremenu. Na fizičkoj radnoj stanici u poslovnom sistemu se nalaze dve VM, jedna inženjerska (RS5) i druga poslovna (RS6). U okviru sistema javnog pristupa se nalazi Web server posredstvom koga će biti simuliran pristup korisnika iz partnerskih sistema. Servis za kontrolu pristupa u Smart Gridu, tzv. SG-ACS, je izolovan od ostalih

komponenti u okviru posebnog VLAN-a koji predstavlja zonu upravljanja, a gde je instaliran na posebnom fizičkom serveru. Za potrebe integracije razvijenog prototipa servisa za kontrolu pristupa bilo je potrebno izvršiti njegovu integraciju sa postojećim sistemom za autentifikaciju tako da se nakon uspešne autentifikacije identitet korisnika prosleđuje SG-ACS servisu.



Slika 36. Prikaz Smart Grid testnog okruženja

Za potrebe izvođenja eksperimenata razvijena je aplikacija koja simulira rad klijenata u testnom okruženju, tzv. test klijent. Test klijent je instaliran na svakoj RS, a nakon njegovog pokretanja i uspešne autentifikacije, korisnik može da izabere proizvoljan aplikativni kontekst. Za ime radne stanice sa koje korisnik pristupa sistemu podrazumeva se ime VM na kojoj je test klijent pokrenut. Komunikacija će biti uspešno uspostavljena ukoliko se izabrani kontekst nalazi na VM koja je u istom VLAN-u kao i radna stanica. Nakon uspešno uspostavljene korisničke sesije, test klijent nudi mogućnost poziva metoda različitih UMS modula, koje su navedene u *Sekciji 7.2*.

UMS moduli su prošireni tako da se prilikom poziva testiranih metoda proveravaju prava korisnika pozivom odgovarajuće metode autorizacionog menadžera. Takođe, modul za upravljanje dinamičkim kontekstom sesije SG-ACS servisa je dodat na svaku VM na kojoj se nalaze UMS moduli, a posredstvom koga klijenti mogu da šalju zahteve o izmeni stanja AOR-a ka SG-ACS i posredstvo koga mogu da prate stanja korisničkih sesija.

Sve komponente prototipa sistema za kontrolu pristupa su implementirane u *Microsoft Visual Studio 2013* razvojnom okruženju korišćenjem programskog jezika C#, dok je za skladištenje konfiguracije korišćen LDAP (eng. *Lightweight Directory Access Protocol*) direktorijum, odnosno hijerarhijska baza podataka dizajnirana da podrži relativno veliki broj operacija čitanja i pretrage, i znatno manji broj operacija promena i unosa podataka. Izuzetak je model aplikativnog konteksta koji se skladišti u XML fajlu. Primena LDAP direktorijuma za skladištenje konfiguracije ima prednost u odnosu na tradicinalne relacione baze, jer se konfiguracija menja retko nakon inicijalnog unosa. Međutim, kako se radi o kontroli pristupa u sistemima sa kritičnom odzivom, SG-ACS komponente koje su namenjene za rad u realnom vremenu se baziraju na memorijskim bazama podataka u cilju poboljšanja performansi. To je se pre svega odnosi na komponentu za upravljanje aktivnim korisničkim sesijama koja u realnom vremenu treba da obezbedi informacije o trenutnom stanju aktivnih sesija u sistemu. Prototipskom implementacijom servisa za kontrolu pristupa i njegovom integracijom u simuliranom Smart Grid okruženju u skladu sa standardnim IEC-62443 modelom bezbednosne arhitekture potvrđena je Hipoteza H3, koja kaže da je prošireni RBAC model moguće primeniti u Smart Grid sistemu u skladu sa postavljenim bezbednosnim zahtevima.

7.2 Konfiguracija sistema za kontrolu pristupa

Za potrebe eksperimentalnog istraživanja definisana je konfiguracija sistema za kontrolu pristupa na kojoj su bazirana ispitivanja usklađenosti predloženog modela sa zahtevima u Smart Gridu. Kako su Smart Grid komponente korišćene prilikom testiranja kompleksni UMS moduli koji obuhvataju širok spektar operacija, bez umanjenja opštosti eksperimentalnog istraživanja odabran je podskup skupa operacija kojima je definisan okvir za eksperimente u okviru ove disertacije. Skup mogućih operacija prilikom izvođenja eksperimenata je sledeći:

- Praćenje, odnosno pregled stanja elektroenergetske mreže. Tu spada čitanje podataka o izmerenim veličinama i statusima uređaja u mreži (vrednosti napona, jačina struje, stanje prekidača), pregled generisanih događaja i alarma u toku rada sistema, itd.
- Upravljanje uređajima i opremom u elektroenergetskoj mreži, obrada alarma i upravljanje alarmnim stanjima.
- Upravljanje sekvencama/planovima manipulacija prekidačkom opremom (kreiranje, odobravanje i izvršavanje).
- Pokretanje funkcija za analizu i optimizaciju rada elektroenergetske mreže, kao i podešavanje konfiguracionih parametara ovih funkcija.
- Koordinacija aktivnosti operatera u kontrolnoj sobi, pre svega mogućnost izdavanja zahteva za izmenu stanja AOR-a u toku rada sistema.
- Ažuriranje modela elektroenergetske mreže, npr. dodavanje novih elemenata u sistem, izmene parametara uređaja, i slično.
- Dodeljivanje planova članovima posade na terenu,

- Ažuriranje podataka o lokaciji i statusu posade na terenu.

U nastavku ove sekcije prikazana je konfiguracija RBAC-AOR$_{SG}$ modela koja je definisana prilikom administracije modela.

7.2.1 Skup privilegija

Skup privilegija, tj. dozvoljenih operacija nad objektima je prikazan u *Tabeli 5.* Skup privilegija je formiran u skladu sa skupom operacija definisanim za eksperimentalno istraživanje. Za svaku operaciju na koju se privilegija odnosi je određen tip operacije u skladu sa definicijom nivoa odgovornosti iz *Sekcije 5.2*. Za svaki objekat je definisan tip objekta u skladu sa definicijom fizičkog i logičkog objekta iz *Sekcije 5.2*. Shodno tome, ukoliko se operacija odnosi na akcije nad logičkim objektima, tip operacije nije definisan.

Tabela 5. Skup privilegija

Privilegija		Operacija	Tip operacije	Tip objekta
P1	Pregled (čitanje) podataka o uređajima i opremi	čitanje podataka o izmerenim veličinama i statusima uređaja u mreži	nadzor	fizički
P2	Praćenje stanja elektroenergetske mreže	pregled generisanih događaja i alarma u sistemu	nadzor	fizički
P3	Komandovanje	upravljanje uređajima i opremom u elektroenergetskoj mreži; izvršavanje sekvence manipulacija prekidačkom opremom	kontrola	fizički
P4	Obrada alarma	obrada alarma i upravljanje alarmnim stanjima	kontrola	fizički
P5	Kreiranje sekvence/plana manipulacija	kreiranje sekvence/plana manipulacija prekidačkom opremom	nije definisan	logički
P6	Odobravanje sekvence ili plana manipulacija	odobravanje sekvence/plana manipulacija prekidačkom opremom	nije definisan	logički
P7	Koordinacija aktivnostima u kontrolnoj sobi	koordinacija rada u kontrolnoj sobi, pre svega mogućnost izdavanja zahteva za izmenu stanja AOR-a u vanrednim situacijama	nije definisan	logički
P8	Izvršavanje analitičkih funkcija	izvršavanje funkcija za analizu i optimizaciju rada distributivne mreže	kontrola	fizički
P9	Konfigurisanje analitičkih funkcija	podešavanje konfiguracionih parametara analitičkih funkcija	nije definisan	logički
P10	Dodela planova posadi na terenu	dodeljivanje odobrenih planova članovima posade na terenu	nije definisan	logički
P11	Upravljanje posadom na terenu	ažuriranje podataka o lokaciji i statusu posade na terenu	nije definisan	logički
P12	Ažuriranje modela	ažuriranje modela elektroenergetske mreže	ažuriranje	fizički
P13	Aktuelizacija modela	aktuelizacija, odnosno promovisanje modela elektroenergetske mreže u produkcioni sistem	ažuriranje	fizički

7.2.2 Skup korisničkih uloga

U *Tabeli 6.* je dat skup korisničkih uloga formiran u skladu sa zaduženjima korisnika u savremenim elektroenergetskim kompanijama opisanim u *Sekciji 3.2.1*. Zatim je na osnovu opisanih zaduženja za svaku ulogu definisano mapiranje na odgovarajući skup privilegija iz *Tabele 5.* Potrebno je napomenuti da skup korisničkih uloga kao i njihova zaduženja mogu varirati zavisno od elektroenergetske kompanije. Kao što je ranije navedeno u *Sekciji 3.2.3* u ovom radu akcenat je na sistemima za upravljanje i planiranje elektroenergetskim sistemom, te su iz razmatranja izuzete korisničke uloge za pristup poslovnim sistemima.

Dodatno, za svaku korisničku ulogu su u *Tabeli 7.* navedeni dozvoljeni nivoi odgovornosti nad omogućenim AOR-ima, kao i konteksti kojima korisnici navedenih uloga mogu pristupati u skladu sa zaduženjima unutar organizacije. Takođe, označene su uloge čije obavljanje je najčešće regulisano licencom, kao i one čije obavljanje može biti delegirano partnerskim organizacijama.

Tabela 6. Skup korisničkih uloga (✓-dodeljena privilegija)

Karakteristike korisničkih uloga		**Privilegije**												
		P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
R1	operater	✓	✓	✓	✓	✓	✓							
R2	supervizor	✓	✓	✓	✓	✓	✓	✓						
R3	inženjer za podršku kontrolne sobe	✓							✓	✓				
R4	model koordinator	✓											✓	✓
R5	model inženjer	✓											✓	
R6	sistem inženjer	✓				✓			✓	✓				
R7	projektant mreže	✓												
R8	član posade	✓	✓	✓								✓		
R9	dispečer posade	✓	✓								✓	✓		

Tabela 7. Karakteristike korisničkih uloga (RT-kontekst za rad u realnom vremenu, SIM-simulacioni kontekst, QA-kontekst za proveru kvaliteta, PLAN-kontekst za planiranje, FIELD-konteks za podršku operacijama na terenu, ✓-dozvoljeno/omogućeno)

Karakteristike korisničkih uloga		**Oblasti odgovornosti**			**Tip konteksta**					**Važeća licenca**	**Organizacija**	
		Nadzor	Kontrola	Ažuriranje	RT	SIM	QA	PLAN	FIELD		Izvorna	Eksterna
R1	operater	✓	✓		✓	✓				✓	✓	
R2	supervizor	✓	✓		✓	✓				✓	✓	
R3	inženjer za podršku kontrolne sobe	✓	✓		✓	✓					✓	
R4	model koordinator	✓		✓	✓		✓				✓	
R5	model inženjer			✓		✓	✓				✓	
R6	sistem inženjer					✓					✓	
R7	projektant mreže							✓			✓	
R8	član posade								✓	✓	✓	✓
R9	dispečer posade								✓		✓	✓

7.2.3 Skup oblasti odgovornosti

Konfiguracija oblasti odgovornosti je prikazana u *Tabeli 8.* prema primeru sa *Slike 9.* Navedeni primer obuhvata podelu mreže prema dva kriterijuma (podela prema geografskom regionu i prema naponskom nivou), uključujući i hijerarhiju AOR-a. Kvačicom su označene relacije hijerarhije i tako prikazan odnos između AOR-a koji definišu podelu mreže po oba kriterijuma sa AOR-ima više hijerarhije koji objedinjuju ove AOR-e prema jednom kriterijumu. Npr. svi AOR-i koji se odnose na Region1, bez obzira na naponski nivo su grupisani u okviru AOR_R1. Takođe, svi AOR-i koji se odnose na isti naponski nivo, npr. 11kV, su objedinjeni u okviru AOR_11. Na vrhu hijerarhije je AOR_D koji objedinjuje sve AOR-e koji se odnose na distributivni deo mreže, bez obzira na naponski nivo ili region. Radi pojednostavljenja prikaza, u ovoj tabeli nisu istaknuti nivoi odgovornosti za svaki AOR. Konfiguracija nivoa odgovornosti će biti posebno naglašena u odgovarajućim eksperimentima.

Tabela 8. Skup oblasti odgovornosti (R1-region1, R2-region2, R3-region3, D-distribucija, ✓-hijerarhijska veza)

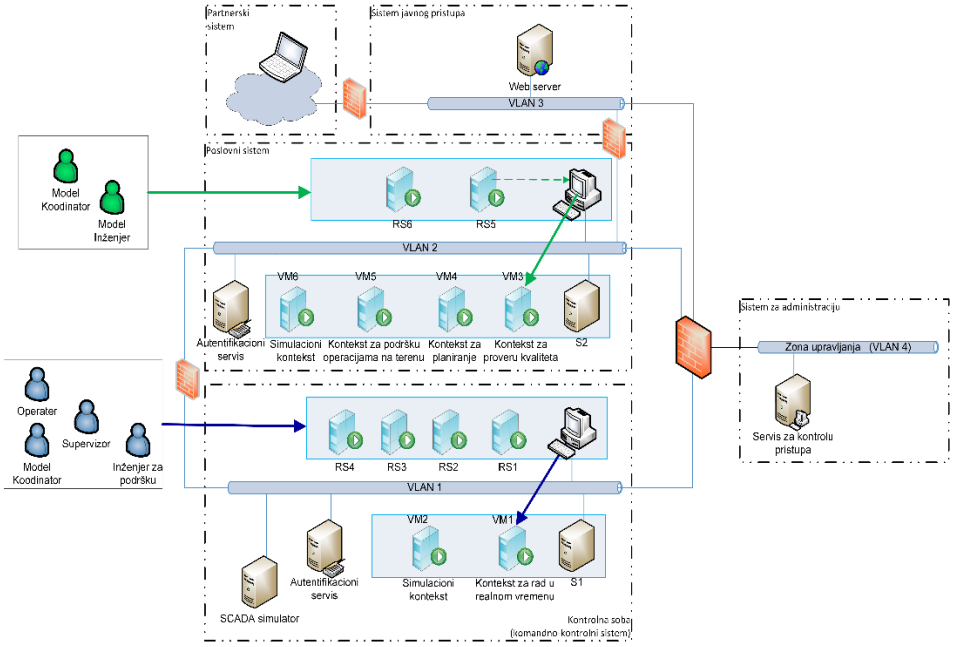
AOR	**Geografska podela**			**Podela pema naponskom nivou**		
Podela po dva kriterijuma	AOR_R1	AOR_R2	AOR_R3	AOR_6.6	AOR_11	AOR_D
AOR_Region1_6.6kV	✓			✓		
AOR_Region1_11kV	✓				✓	
AOR_Region2_6.6kV		✓		✓		
AOR_Region2_11kV		✓			✓	
AOR_Region3_6.6kV			✓	✓		
AOR_Region3_11kV			✓		✓	
AOR_R1						✓
AOR_R2						✓
AOR_R3						✓
AOR_6.6						✓
AOR_11						✓

7.3 Kontrola pristupa prema oblasti odgovornosti

U cilju provere usaglašenosti predloženog RBAC-AOR$_{SG}$ modela sa postavljenim zahtevima za kontrolu pristupa prema oblasti odgovornosti izvršeni su eksperimenti koji imaju za cilj da ispitaju mogućnost raspodele odgovornosti između korisnika koji pripadaju istim korisničkim ulogama, pre svega u slučaju izvršavanja kritičnih operacija, kao što su upravljanje elektroenergetskim sistemom i izmena modela elektroenergetske

mreže u sistemu za rad u realnom vremenu. Takođe, potvrda kvaliteta modelskih izmena elektroenergetske mreže u poslovnom okruženju se smatra kritičnom operacijom, jer se potvrđene izmene promovišu u sistem za rad u realnom vremenu. U kontekstima koje nemaju direktan uticaj na rad sistema u realnom vremenu, razmatranje oblasti odgovornosti nije od značaja.

Relevantne komponente okruženja za izvođenje ove grupe eksperimenata su istaknute na *Slici 37.* Plavim su označeni korisnici u kontrolnoj sobi koji pristupaju kontekstu za rad u realnom vremenu sa proizvoljne RS, dok su zelenim označeni korisnici koji sa inženjerske radne stanice (RS5) pristupaju kontekstu za proveru kvaliteta izmena modela.



Slika 37. Test okruženje za analizu kontrole pristupa prema AOR-ima

Za potrebe izvršavanja ove grupe eksperimenata kreirano je ukupno sedam korisnika:

- tri 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 supervizora.
- jedan korisnik koji je član uloge inženjera za podršku u kontrolnoj sobi.
- jedan korisnik kome je dodeljena uloga inženjera modela. Kako je ova uloga zadužena za obavljanje poslova u okviru konteksta za proveru kvaliteta, podrazumevani nivo odgovornosti je ažuriranje modela.
- jedan korisnik kome je dodeljena uloga model koordinatora, a koja je specifična po tome što ima zaduženja ne samo u okviru konteksta za proveru kvaliteta,

već i u okviru konteksta za rad u realnom vremenu za potrebe aktuelizacije modela u produkcionom sistemu.

Skup omogućenih AOR-a za pojedinačne korisnike je prikazan u *Tabeli 9.* Svim korisnicima su omogućeni AOR-i sa nivoima odgovornosti koji odgovaraju dodeljenim korisničkim ulogama (videti *Tabelu 7.*). Radne stanice korišćenje prilikom izvršavanja ove grupe eksperimenata su konfigurisane bez ograničenja u pogledu omogućenih uloga i AOR-a.

Tabela 9. Skup korisnika za analizu kontrole pristupa prema AOR-ima (N-nadzor, K-kontrola, U-ažuriranje, ✓-omogućeni AOR, ×-onemogućeni AOR)

Korisnik	Korisnička uloga	AOR_R1_N	AOR_R1_K	AOR_R1_U	AOR_R2_N	AOR_R2_K	AOR_R2_U	AOR_R3_N	AOR_R3_K	AOR_R3_U
operater1	operater	✓	✓	×	✓	✓	×	×	×	×
operater2	operater	×	×	×	✓	✓	×	✓	✓	×
operater3	operater	✓	✓	×	×	×	×	✓	✓	×
inženjer	inženjer za podršku u kontrolnoj sobi	✓	✓	×	✓	✓	×	×	×	×
modelInženjer	model inženjer	×	×	✓	×	×	×	×	×	×
modelAdmin	model koordinator	✓	×	✓	×	×	×	✓	×	✓
supervizor	supervizor	✓	✓	×	✓	✓	×	✓	✓	×

U nastavku ove sekcije prikazana su tri eksperimenta koja će potvrditi pretpostavljenu prednost predloženog RBAC-AOR$_{SG}$ modela u odnosu na RBAC u pogledu restriktivnije kontrole pristupa za izvršavanje kritičnih operacija, ali i pouzdanijeg i efikasnijeg upravljanje sistemom kako u regularnom režimu rada tako i u vanrednim situacijama. Time će biti potvrđena Hipoteza H1 koja kaže da RBAC nije adekvatan za Smart Grid u pogledu kontrole pristupa prema oblastima odgovornosti, kao i Hipoteza H2 koja kaže da je RBAC moguće uskladiti sa ovim bezbednosnim zahtevom.

7.3.1 Podela odgovornosti između korisnika iste korisničke uloge

Cilj ovog eksperimenta je ispitivanje mogućnosti predloženog rešenja da zadovolji postavljeni C.AC.1 zahtev, odnosno da omogući podelu odgovornosti između korisnika koji pripadaju istim korisničkim ulogama prema oblastima odgovornosti. To je potrebno ispitati prilikom izvršavanja operacija nadzora i upravljanja elektroenergetskim sistemom u realnom vremenu, zatim prilikom izmene modela elektroenergetske mreže

u produkcionom sistemu, kao i prilikom verifikacije i odobravanja napravljenih izmena pre primene u produkcionom sistemu. Istim eksperimentom biće ispitana i mogućnost modela da podrži hijerarhijsku organizaciju AOR-a prema zahtevu C.AC.2. Naime, svim korisnicima su dodeljeni AOR-i definisani geografskom podelom mreže koji predstavljaju drugi nivo hijerarhije, jer grupišu AOR-e definisane po oba kriterijuma.

U prvom delu eksperimenta razmatrana su prava korisnika u kontrolnoj sobi koji pristupaju kontekstu za rad u realnom vremenu: operater, inženjer za podršku u kontrolnoj sobi i model koordinator. Prilikom uspostavljanja korisničke sesije svi korisnici aktiviraju omogućene AOR-e sa omogućenim nivoom odgovornosti. Stanja aktivnih korisničkih sesija na početku izvođenja eksperimenta za dva operatera, jednog inženjera i jednog koordinatora modela su prikazana u *Tabeli 10.a)*. Prilikom izvršavanja eksperimenta korisnici izvršavaju različite tipove operacija nad objektima koji pripadaju različitim regionima elektroenergetskog sistema:

1. Operacije tipa nadzora: čitanje statusa uređaja,
2. Operacije tipa kontrole: otvaranja/zatvaranja prekidača, izvršenje UMS analitičke funkcije,
3. Operacije tipa ažuriranja: aktuelizacija modela u produkciji,
4. Operacije nad logičkim objektima: kreiranje sekvence manipulacija.

U *Tabeli 10.b)* su prikazani uporedni rezultati dobijeni primenom standardnog RBAC modela i predloženog RBAC-AOR$_{SG}$ proširenja u zavisnosti od regiona objekta elektroenergetskog sistema kome se pristupalo iz različitih korisničkih sesija. Analizom dobijenih rezultata može se zaključiti da ukoliko korisnik nema odgovarajuću privilegiju, on nema pravo da izvrši operaciju bez obzira da li je primenjen RBAC ili RBAC-AOR$_{SG}$ model. Na primeru operatera to znači da on ni u jednom slučaju ne može da izvršava analitičke funkcije ili ažurira model mreže (istaknuto crvenim u tabeli). Međutim, ako se analiziraju prava korisnika koji pripadaju istim korisničkm ulogama, može se zaključiti da RBAC nema mogućnost podele odgovornosti između korisnika koji pripadaju istoj korisničkoj ulozi. U slučaju RBAC-a svi operateri mogu da izvršavaju operacije čitanja i komandovanja, inženjer za podršku u kontrolnoj sobi može da izvršava analitičke funkcije, a model koordinator da primenjuje izmene modela u produkcionom sistemu nad svakim delom elektroenergetskog sistema. Za razliku od RBAC-a, RBAC-AOR$_{SG}$ omogućuje dodatni nivo kontrole pristupa. U zavisnosti od aktiviranih AOR-a korisnici koji pripadaju istoj ulozi mogu imati različita prava nad određenim delom elektroenergetskog sistema. Dva operatera iz navedenog primera imaju pravo čitanja i komandovanja samo onim delom mreže za koji su aktivirali AOR (označeno zelenim u tabeli). Takođe, inženjer za podršku u kontrolnoj sobi može da izvršava analitičke funkcije, a model koordinator da promoviše model samo nad delom mreže za koji ima aktivirane AOR-e. Dodatno, ukoliko korisnik ima omogućen, ali ne i aktiviran AOR on ne može da izvrši operaciju nad tim delom mreže. Na primer, ukoliko neki od operatera

Tabela 10. Rezultati analize mogućnosti podele odgovornosti između korisnika u kontrolnoj sobi

Stanja aktivnih korisničkih sesija (N-nadzor, K-kontrola, U-ažuriranje, ✓-omogućeni AOR, ×-onemogućeni AOR, ☑-aktivirani AOR)

a)

Korisnička sesija	Korisnik	Korisnička uloga	AOR_R1_N	AOR_R1_K	AOR_R1_U	AOR_R2_N	AOR_R2_K	AOR_R2_U	AOR_R3_N	AOR_R3_K	AOR_R3_U
s1	operater1	R1	☑	☑	×	☑	☑	×	×	×	×
s2	operater2	R1	×	×	×	☑	☑	×	☑	☑	×
s3	inženjer	R3	☑	☑	×	☑	☑	×	×	×	×
s4	modelAdmin	R4	☑	×	☑	×	×	×	☑	×	☑

Uporedni rezultati dobijeni primenom RBAC i RBAC-AOR$_{SG}$ (✓-zabranjeno, ×-dozvoljeno, R1-region1, R2-region2, R3-region3)

b)

Korisnička sesija	Korisnik	Primenjeni model	Čitanje			Komandovanje			Izvršavanje Fje			Aktuelizacija modela			Kreiranje sekvence
			R1	R2	R3	R1	R2	R3	R1	R2	R3	R1	R2	R3	
s1	operater1	RBAC	✓	✓	✓	✓	✓	✓	×	×	×	×	×	×	✓
		RBAC-AOR-SG	✓	✓	×	✓	✓	×	×	×	×	×	×	×	✓
s2	operater2	RBAC	✓	✓	✓	✓	✓	✓	×	×	×	×	×	×	✓
		RBAC-AOR-SG	×	✓	✓	×	✓	✓	×	×	×	×	×	×	✓
s3	inženjer	RBAC	✓	✓	✓	×	×	×	✓	✓	✓	×	×	×	×
		RBAC-AOR-SG	✓	✓	×	×	×	×	✓	✓	×	×	×	×	×
s4	modelAdmin	RBAC	✓	✓	✓	×	×	×	×	×	×	✓	✓	✓	×
		RBAC-AOR-SG	✓	×	✓	×	×	×	×	×	×	✓	×	✓	×

deaktivira određeni AOR za kontrolu on neće moći da komanduje uređajima iz regiona za koji ima omogućen, ali ne i aktiviran AOR.

S druge strane, sa aspekta pristupa logičkim objektima između RBAC i RBAC-AOR$_{SG}$ modela nema razlike, jer se AOR-i ne razmatraju za ovaj tip objekata. Na pomenutom primeru se može uočiti da oba operatera uvek imaju mogućnost kreiranja sekvence manipulacija prekidačkom opremom (označeno plavim).

U drugom delu eksperimenta razmatrana su prava korisnika u poslovnom sistemu koji rade u okviru konteksta za proveru kvaliteta modela: inženjer modela i koordinator ažuriranja modela. Prilikom uspostavljanja korisničke sesije svi korisnici su aktivirali omogućene AOR-e sa omogućenim nivoom odgovornosti. Stanja aktivnih korisničkih sesija na početku izvođenja eksperimenta za navedene korisnike su prikazana u *Tabeli 11.a)*. Prilikom izvršavanja eksperimenta, ispitane su mogućnosti korisnika da izvrše sledeće operacije nad objektima koji pripadaju različitim regionima elektroenergetskog sistema:

1. Izmene (ažuriranje) i testiranje modela,
2. Aktuelizacija (odobravanje izmena) modela u produkcioni sistem.

U *Tabeli 11.b)* su prikazani uporedni rezultati dobijeni primenom standardnog RBAC modela i predloženog RBAC-AOR$_{SG}$ proširenja u zavisnosti od regiona objekta elektroenergetskog sistema kome se pristupalo iz svake od navedenih korisničkih sesija. Za razliku od RBAC-a, primenom predloženog rešenja korisnik može ažurirati model ili odobriti izmene za one delove elektorenergetske mreže za koje ima aktiviran AOR sa nivoom odgovornosti za ažuriranje.

Tabela 11. Rezultati analize mogućnosti podele odgovornosti između korisnika u poslovnom sistemu

Stanja aktivnih korisničkih sesija (U-ažuriranje, ✓-omogućeni AOR, ×-onemogućeni AOR, ☑-aktivirani AOR)

a)

Korisnička sesija	Korisnik	Korisnička uloga	AOR_R1_U	AOR_R2_U	AOR_R3_U
s1	modelInženjer	R5	☑	×	×
s2	modelAdmin	R4	☑	×	☑

Uporedni rezultati dobijeni primenom RBAC i RBAC-AOR$_{SG}$ (✓-zabranjeno, ×-dozvoljeno, R1-region1, R2-region2, R3-region3)

b)

Korisnička sesija	Korisnik	Primenjeni model	Izmena modela			Aktuelizacija modela		
			R1	R2	R3	R1	R2	R3
s1	modelInženjer	RBAC	✓	✓	✓	×	×	×
		RBAC-AOR-SG	✓	×	×	×	×	×
s2	modelAdmin	RBAC	✓	✓	✓	✓	✓	✓
		RBAC-AOR-SG	✓	×	✓	✓	×	✓

Analizom dobijenih rezultata u okviru predstavljenog eksperimenta može se zaključiti da u poređenju sa RBAC modelom RBAC-AOR$_{SG}$ pruža restriktivniju kontrolu pristupa. Ovim se postiže efikasnije upravljanje sistemom i ažuriranje modela elektroenergetskog sistema, jer korisnici ne moraju da upravljaju celokupnom mrežom već samo određenim regionima. Dodatno, u slučaju da je upravljanje ili razvoj određenih delova elektroenergetske mreže u nadležnosti različitih organizacija, model AOR-a pruža mogućnost razdvajanja zaduženja unutar sistema. Da bi RBAC model zadovoljio postavljeni zahtev, bilo bi potrebno definisati onoliko puta više privilegija koliko ima oblasti odgovornosti unutar elektroenergetskog sistema. Npr. u primeru prikazanom u *Tabeli 10.* su razmatrane četiri privilegije grupisane u tri korisničke uloge, i tri oblasti odgovornosti, dok bi u slučaju RBAC-a bilo potrebno definisani 4x3 privilegije (4 privilegije X 3 oblasti odgovornosti) koje bi se zatim grupisale u N korisničkih uloga. Ako se uzme u obzir da u realnim sistemima broj oblasti odgovornosti unutar nekog sistema može biti par stotina ili hiljada entiteta to bi značilo da RBAC model treba da podrži stotine ili hiljade puta više privilegija da bi zadovoljio navedeni zahtev.

Dodatno, analizom dobijenih rezultata može se zaključiti da model ispunjava zahtev za mogućnošću hijerarhijske organizacije AOR-a, jer dodelom AOR-a višeg nivoa hijerarhije korisnicima su dodeljeni odgovarajući AOR-i nižeg nivoa hijerarhije.

7.3.2 Kontinualan nadzor i kontrola svih AOR-a

Cilj ovog eksperimenta je ispitivanje mogućnosti predloženog rešenja da zadovolji postavljeni C.AC.3 zahtev, odnosno mogućnost RBAC-AOR$_{SG}$ modela da obezbedi da svaki AOR bude pod konstantnim nadzorom i kontrolom najmanje jednog operatera u kontrolnoj sobi.

U prvom delu eksperimenta aktivna su tri operatera sa disjunktnim skupom aktiviranih AOR-a za nadzor i kontrolu. Prilikom izvršavanja eksperimenta prvo je ispitana mogućnost operatera da deaktivira AOR koji je u njegovoj nadležnosti, a zatim i da zatvori sesiju. Kako bi u oba slučaja AOR ostao bez nadležnosti, pokušaj deaktivacije AOR-a, odnosno pokušaj zatvaranja sesije je neuspešan. Ovo je pokazano primerom u *Tabeli 12.a)*. U drugom koraku jedan od operatera aktivira AOR tako da u slučaju

deaktivacije ili prekida sesije od strane drugog operatera, AOR ostaje u nadležnosti tog operatera. U ovom slučaju, pokušaj deaktivacije, kao i pokušaj zatvaranja sesije je uspešan, kao što je pokazano primerom u *Tabeli 12.b)*. Ukoliko operater pokuša da zatvori sesiju, a nijedan aktivni operater ne može da preuzme sve njegove aktivirane AOR-e pošto im nisu omogućeni, korisniku ova akcija neće biti dozvoljena sve dok svi AOR-i koje je aktivirao ne budu preuzeti od strane bar jednog operatera. Primer neuspešng pokušaja zatvaranja sesije je prikazano primerom u *Tabeli 12.c)*.

U drugom delu eksperimenta, na početku su aktivna tri korisnika: dva operatera koji pokrivaju disjunktni skup AOR-a, i jedan inženjer za podršku u kontrolnoj sobi koji je takođe aktivirao AOR za potrebe izvršavanja funkcija. U ovom slučaju operater će uspešno deaktivirati AOR koji je aktivirao i inženjer, jer on ostaje u nadležnosti jednog korisnika (inženjera) kao što je pokazano primerom u *Tabeli 12.d)*.

Na osnovu prvog eksperimenta može se zaključiti da RBAC-AOR$_{SG}$ obezbeđuje striktnu kontrolu pristupa u smislu da u regularnom režimu rada nije moguće da neka oblast odgovornosti ostane bez nadzora i kontrole, što RBAC model ne može da obezbedi. Analizom drugog dela ovog eksperimenta može se zaključiti da je primenom RBAC-AOR$_{SG}$ modela obezbeđena konstantna kontrola svakog AOR-a od strane bar jednog korisnika. Na konkretnom primeru prikazanom u *Tabeli 12.d)*, AOR je ostao pod kontrolom inženjera za podršku u kontrolnoj sobi koji nema pravo komandovanja ili obrade alarma. Ovo ograničenje je moguće jednostavno prezavići definisanjem dodatnog nivoa odgovornosti tako da operacije koje izvršava inženjer u kontrolnoj sobi budu različitog tipa u poređenju sa operacijama tipa kontrole koje izvršava inženjer u kontrolnoj sobi..

Tabela 12. Rezultati analize mogućnosti konstantnog nadzora i kontrole AOR-a (N-nadzor, K-kontrola, ✓-omogućeni AOR, ×-onemogućeni AOR, ☑-aktivirani AOR)

Deaktivacija AOR R1 K neuspešna: operator1

a)

Korisnička sesija	Korisnik	Korisnička uloga	AOR_R1_N	AOR_R1_K	AOR_R2_N	AOR_R2_K	AOR_R3_N	AOR_R3_K
s1	operater1	R1	☑	☑	✓	✓	×	×
s2	operater2	R1	×	×	☑	☑	✓	✓
s3	operater3	R1	✓	✓	×	×	☑	☑

Deaktivacija AOR R1 K uspešna: operator1

b)

Korisnička sesija	Korisnik	Korisnička uloga	AOR_R1_N	AOR_R1_K	AOR_R2_N	AOR_R2_K	AOR_R3_N	AOR_R3_K
s1	operater1	R1	☑	☑	✓	✓	×	×
s2	operater2	R1	×	×	☑	☑	✓	✓
s3	operater3	R1	☑	☑	×	×	☑	☑

Zatvaranje sesije neuspešno: operator3

c)

Korisnička sesija	Korisnik	Korisnička uloga	AOR_R1_N	AOR_R1_K	AOR_R2_N	AOR_R2_K	AOR_R3_N	AOR_R3_K
s2	operater2	R1	×	×	☑	☑	☑	☑
s3	operater3	R1	☑	☑	×	×	☑	☑

Deaktivacija AOR_R1_K uspešna: operator1

d)

Korisnička sesija	Korisnik	Korisnička uloga	AOR_R1_N	AOR_R1_K	AOR_R2_N	AOR_R2_K	AOR_R3_N	AOR_R3_K
s1	operater1	R1	☑	☑	☑	☑	×	×
s2	operater3	R1	✓	✓	×	×	☑	☑
s3	inženjer	R3	☑	☑	☑	☑	×	×

7.3.3 Kontrola pristupa u vanrednim situacijama

Zadatak ovog eksperimenta je ispitivanje mogućnosti predloženog rešenja da zadovolji postavljeni C.AC.4 zahtev, odnosno da obezbedi pouzdano i efikasno upravljanje sistemom u vanrednim situacijama. Za razliku od regularnih situacija, u vanrednim situacijama oblasti odgovornosti mogu ostati bez nadzora i kontrole usled nedostupnosti kontrolnog centra, otkaza radnih stanica, i slično.

Na početku ovog eksperimenta aktivna su tri operatera koji imaju aktiviran disjunktni skup AOR-a, odnosno svaki operater ima eksluzivan nadzor i upravljanje za jedan određeni AOR koji ne može biti preuzet od strane drugih operatera. Takođe, u posebnoj

sesiji supervizor nadgleda sistem, ali ne može da upravlja. Prilikom izvršavanja testa, simuliran je kvar radne stanice jednog od operatera tako da AOR koji je bio u nadležnosti tog operatera ostane van nadzora i kontrole. S obzirom da nijednom od aktivnih operatera nije omogućen problematični AOR, oni ne mogu da ga aktiviraju. U ovoj situaciji RBAC-AOR$_{SG}$ omogućuje da supervizor u okviru svoje sesije izda zahtev za delegiranjem odgovornosti drugim operaterima, te da se za njih privremeno aktiviraju onemogućeni AOR-i. Nemogućnost da takav zahtev izda neko od operatera je obezbeđena privilegijom supervizora za koordinaciju u kontrolnoj sobi. Opisani eksperiment je prikazan u *Tabeli 13.*

Tabela 13. Rezultati analize kontrole pristupa u vanrednim situacijama (N-nadzor, K-kontrola, ✓-omogućeni AOR, ×-onemogućeni AOR, ☑-aktivirani AOR)

a)

Korisnička sesija	Korisnik	Korisnička uloga	AOR_R1_N	AOR_R1_K	AOR_R2_N	AOR_R2_K	AOR_R3_N	AOR_R3_K
s1	operater1	R1	☑	☑	×	×	×	×
s2	operater2	R1	×	×	☑	☑	×	×
s3	operater3	R1	×	×	×	×	☑	☑
s3	supervisor	R2	☑	✓	☑	✓	☑	✓

b)

Korisnička sesija	Korisnik	Korisnička uloga	AOR_R1_N	AOR_R1_K	AOR_R2_N	AOR_R2_K	AOR_R3_N	AOR_R3_K
s1	operater1	R1	☑	☑	×	×	×	×
s2	operater2	R1	×	×	×	×	×	×
s3	operater3	R1	×	×	×	×	☑	☑
s3	supervisor	R2	☑	✓	☑	✓	☑	✓

c)

Korisnička sesija	Korisnik	Korisnička uloga	AOR_R1_N	AOR_R1_K	AOR_R2_N	AOR_R2_K	AOR_R3_N	AOR_R3_K
s1	operater1	R1	☑	☑	☑	☑	×	×
s3	operater3	R1	×	×	☑	☑	☑	☑
s3	supervisor	R2	☑	✓	☑	✓	☑	✓

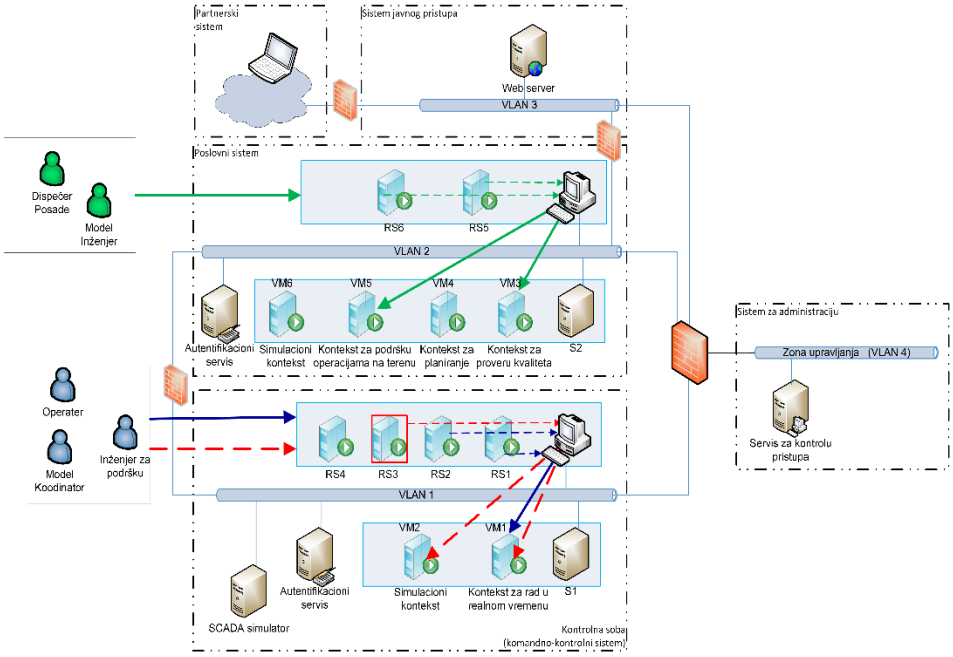
Iako sa jedne strane RBAC-AOR$_{SG}$ pruža restriktivniju kontrolu pristupa u poređenju sa RBAC modelom, ovaj model omogućuje određeni nivo fleksibilnosti u vanrednim situacijama kada se zahtev za pouzdanim i stabilnim radom kritičnih sistema stavlja ispred bezbednosti. Iako postoji nekoliko načina da se prevaziđe problem sa otkazom radnih stanica, poput prelaska operatera čija se radna stanica pokvarila na rezervnu radnu stanicu ili dodela AOR-a drugim operaterima izmenom konfiguracije, ovde se predlaže privremeno delegiranje odgvornosti u toku izvršavanja korisničkih sesija. Prvi predlog jeste primenljiv u slučaju kvara radne stanice, ali ne i u uslovima vremenskih nepogoda kada kompletan regionalni centar može da ostane bez kontrole, a operateri iz drugih kontrolnih centara nemaju omogućene AOR-e. Drugi predlog, izmena modela podataka AOR-a kada se problem desi podrazumeva da supervizori imaju pristup podacima bezbednosnog servisa što nije u skladu sa modelom bezbednosne arhitekture i zahtevom za izolovanje bezbednosnih servisa od ostalih funkcionalnosti.

7.4 Kontrola pristupa prema radnoj stanici

U ovom delu rada su prikazani eksperimenti za proveru usaglašenosti predloženog proširenja RBAC modela sa zahtevima za kontrolu pristupa u zavisnosti od lokacije ili namene radne stanice sa koje korisnik pristupa sistemu. Relevantne komponente okruženja za izvođenje ove grupe eksperimenata su istaknute na *Slici 38.* Plavim su označeni korisnici u kontrolnoj sobi koji pristupaju kontekstu za rad u realnom vremenu sa proizvoljne RS u kontrolnoj sobi. Crvenim je istaknut pristup kontekstu za rad u realnom vremenu sa lokacije koja nije unapred definisana, čime će biti simuliran pristup kontrolnoj sobi sa sa “nepoznate lokacije”. Zelenim su označeni korisnici koji sa inženjerske radne stanice (RS5) pristupaju kontekstu za proveru kvaliteta izmena modela.

Za potrebe izvršavanja ove grupe testova kreirano je ukupno pet korisnika:

- jedan korisnik koji je član korisničke uloge operatera i kome su omogućeni svi AOR-i sa nivoom odgovornosti za nadzor i kontrolu.
- jedan korisnik koji je član uloge inženjera za podršku u kontrolnoj sobi i kome su omogućeni svi AOR-i sa nivoom odgovornosti za nadzor i kontrolu.
- jedan korisnik kome je dodeljena uloga model koordinatora i kome su omogućeni svi AOR-i sa nivoom odgovornosti za nadzor i ažuriranje modela.
- jedan korisnik kome je dodeljena uloga model inženjera, i u skladu sa tim nivo odgovornosti za sve dodeljene AOR-e je ažuriranje modela.
- jedan korisnik koji je član uloge dispečera posade. Za obavljanje poslova dispečeru ne trebaju AOR-i te on nema omogućen nijedan AOR.



Slika 38. Test okruženje za analizu kontrole pristupa prema radnoj stanici

Konfiguracija radnih stanica koje su korišćene prilikom izvođenja eksperimenata je prikazana u *Tabeli 14.* Za svaku radnu stanicu je definisan tip radne stanice prema test okruženju, kao i skup omogućenih uloga i oblasti odgovornosti sa svake radne stanice u skladu sa zahtevima definisanim u *Sekciji 3.2.4*.

Tabela 14. Konfiguracija radnih stanica

Radne stanice	Omogućene korisničke uloge										Omogućeni AOR								
											AOR_R1			AOR_R2			AOR_R3		
	Operater	Inženjer za podršku u kontrolnoj sobi	Supervizor	Model koordinator	Model inženjer	Dispečer posade	Član posade	Projektant mreže	Sistem inženjer	Poslovni menadžer	Nadzor	Kontrola	Ažuriranje	Nadzor	Kontrola	Ažuriranje	Nadzor	Kontrola	Ažuriranje
#RS1	✓	✓	✓	✓							✓	✓	✓	✓	✓	✓			
#RS2	✓	✓	✓	✓													✓	✓	✓
#RS3						✓	✓			✓									
#RS5				✓	✓	✓	✓	✓	✓				✓			✓			
#RS6										✓									

Ovim eksperimentima će biti potvrđena prednost predloženog RBAC-AOR$_{SG}$ modela u poređenju sa RBAC-om kada je u pitanju kontrola pristupa u zavisnosti od lokacije ili namene radne stanice sa koje se pristupa sistemu. Time će biti potvrđena Hipoteza H1

koja kaže da RBAC nije adekvatan za Smart Grid u tom polju, kao i Hipoteza H2 koja kaže da je RBAC moguće uskladiti sa ovim bezbednosnim zahtevom.

7.4.1 Kontrola pristupa sa udaljene lokacije

Cilj ovog eksperimenta je ispitivanje mogućnosti predloženog rešenja da zadovolji zahtev C.AC.7 da se omogući ograničavanje pristupa sistemima u kontrolnom centru sa radnih stanica koje nisu unapred definisane, odnosno za koje se ne očekuje da se koriste za pristup kontrolnoj sobi. S obzirom da se na istoj radnoj stanici zajedno sa kontekstom za rad u realnom vremenu najčešće nalazi i simulacioni kontekst za koji važe manje restriktivna pravila u poređenju sa kontekstom za rad u realnom vremenu, ispitana su prava korisnika u okviru oba konteksta, jer bi zloupotrebom simulacionog konteksta napadač potencijalno mogao da kompromituje i sistem za rad u realnom vremenu.

Prvo su razmatrana prava korisnika u kontrolnoj sobi koji pristupaju kontekstu za rad u realnom vremenu: operater, inženjer za podršku u kontrolnoj sobi i koordinator ažuriranja modela (na *Slici 38.* označeno plavim). Eksperiment je zatim ponovljen za pristup simulacionom kontekstu (na *Slici 38.* označeno crvenim). Prilikom izvršavanja eksperimenta korisnici izvršavaju različite tipove operacija nad objektima elektroenergetskog sistema:

1. Operacije tipa nadzora: čitanje statusa uređaja,
2. Operacije tipa kontrole: otvaranja/zatvaranja prekidača, izvršenje UMS analitičkih funkcije,
3. Operacije tipa ažuriranja: aktuelizacija modela mreže u produkciji.

Bez obzira na tip konteksta u kontrolnoj sobi, kada se sesija uspostavlja sa lokacije koja nije unapred definisana u sistemu korisnicima su onemoguće sve korisničke uloge u kontrolnoj sobi. U *Tabeli 15.* su prikazani uporedni rezultati dobijeni primenom RBAC modela i predloženog RBAC-AOR$_{SG}$ proširenja kada korisnik uspostavlja sesiju sa radne stanice koja nije unapred definisana bezbednosnom politikom. Na primer, u slučaju primene RBAC modela operater može regularno da izvršava razmatrane operacije, dok u slučaju primene RBAC-AOR$_{SG}$ modela operater nema pravo izvršavanja istih operacija bez obzira na dodeljenu korisničku ulogu. Na ovaj način RBAC-AOR$_{SG}$ omogućuje ograničavanje pristupa sa radnih stanica koje nisu unapred poznate sistemu, čime se smanjuje rizik od potencijalno malicioznog pristupa sistemu sa udaljenih lokacija.

Tabela 15. Rezultati analize kontrole pristupa sa udaljene lokacije

a) Kontekst za rad u realnom vremenu

	Korisnik	Primenjeni model	Čitanje			Komandovanje			Izvršavanje Fje			Aktuelizacija		
			R1	R2	R3	R1	R2	R3	R1	R2	R3	R1	R2	R3
s1	operater	RBAC	✓	✓	✓	✓	✓	✓	×	×	×	×	×	×
		RBAC-AOR-SG	×	×	×	×	×	×	×	×	×	×	×	×
s2	inženjer	RBAC	✓	✓	✓	×	×	×	✓	✓	✓	×	×	×
		RBAC-AOR-SG	×	×	×	×	×	×	×	×	×	×	×	×
s3	model Admin	RBAC	✓	✓	✓	×	×	×	×	×	×	✓	✓	✓
		RBAC-AOR-SG	×	×	×	×	×	×	×	×	×	×	×	×

b) Kontekst za simulaciju

	Korisnik	Primenjeni model	Čitanje			Komandovanje			Izvršavanje Fje			Aktuelizacija		
			R1	R2	R3	R1	R2	R3	R1	R2	R3	R1	R2	R3
s1	operater	RBAC	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		RBAC-AOR-SG	×	×	×	×	×	×	×	×	×	×	×	×
s2	inženjer	RBAC	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		RBAC-AOR-SG	×	×	×	×	×	×	×	×	×	×	×	×
s3	model Admin	RBAC	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		RBAC-AOR-SG	×	×	×	×	×	×	×	×	×	×	×	×

7.4.2 Kontrola pristupa prema nameni radne stanice u kontrolnoj sobi

Zadatak ovog eksperimenta je ispitivanje mogućnosti predloženog rešenja da odgovori zahtevu C.AC.7 da se omogući raspodela odgovornosti između operatera u kontrolnoj sobi u zavisnosti od radne stanice sa koje uspostavljaju korisničku sesiju. Prikazani eksperiment je relevantan za kontekst za rad u realnom vremenu (na *Slici 38.* označeno plavim). Razmatrana su dva operatera sa istim skupom omogućenih AOR-a, dok su radne stanice konfigurisane sa ekskluzivnim pravom upravljanja određenim geografskim područjem (videti *Tabelu 14.*).

Prilikom izvršavanja eksperimenta operateri izvršavaju različite operacija nad objektima koji pripadaju različitim regionima elektroenergetskog sistema. Od interesa su samo operacije koje su operaterima omogućene privilegijama, jer u suprotnom operacija nije dozvoljena bez obzira na dodeljene i odabrane AOR-e:

1. Operacije tipa nadzora: čitanje statusa uređaja,
2. Operacije tipa kontrole: otvaranja/zatvaranja prekidača.

U *Tabeli 16.* su prikazani uporedni rezultati dobijeni primenom RBAC modela i predloženog RBAC-AOR$_{SG}$ proširenja u zavisnosti od regiona objekta elektroenergetskog sistema kome se pristupalo iz različitih korisničkih sesija. Primenom RBAC modela svim operaterima je omogućeno izvršavanje operacija čitanja i komandovanja bez obzira na radnu stanicu sa koje pristupaju sistemu. Za razliku od RBAC-a, primenom RBAC-AOR$_{SG}$ modela moguće je ograničiti izvršavanje operacija u zavisnosti od unapred određene namene radne stanice i time omogućiti podelu odgovornosti između korisnika sa istim zaduženjima u zavisnosti od radne stanice sa kojim pristupaju sistemu.

Tabela 16. Rezultati analize kontrole pristupa prema nameni radne stanice u kontrolnoj sobi

Korisnička sesija	Korisnik	Radna stanica	Primenjeni model	Čitanje			Komandovanje		
				R1	R2	R3	R1	R2	R3
s1	operater1	#RS1	RBAC	✓	✓	✓	✓	✓	✓
			RBAC-AOR-SG	✓	✓	×	✓	✓	×
s2	opeater2	#RS2	RBAC	✓	✓	✓	✓	✓	✓
			RBAC-AOR-SG	×	×	✓	×	×	✓

7.4.3 Kontrola pristupa prema nameni radne stanice u poslovnom okruženju

Cilj ovog eksperimenta je ispitivanje mogućnosti modela kontrole pristupa da ispuni zahtev C.AC.7 koji se odnosi na raspodelu odgovornosti između korisnika u poslovnom sistemu u zavisnosti od namene radne stanice. Za korisnike kojima su dodeljene dve (ili više) korisničkih uloga potrebno je ispitati da li će im biti omogućen minimalan skup privilegija u zavisnosti od toga da li pristupaju inženjerskoj ili poslovnoj radnoj stanici.

Razmatrana su dva korisnika iz poslovnog sistema kojima su dodeljene dve uloge: jedna inženjerska i jedna poslovna. Prvom korisniku je omogućena uloga inženjera modela i predstavnika korisničke službe tako da on može da izvršava operacije testiranja izmena modela u kontekstu za proveru kvaliteta, ali i da upravlja podacima o potrošačima u okviru poslovnog sistema. Drugom korisniku je dodeljena uloga dispečera posade i predstavnika korisničke službe, tako da on može da upravlja poslovima na terenu u okviru konteksta za upravljanje operacijama na terenu, ali i da upravlja podacima o potrošačima u okviru poslovnog sistema. S obzirom da u razmatranom testnom okruženju nema poslovnih sistema (poput sistema za upravljanje potrošačima, sistema za naplatu potrošnje, i slično), prilikom izvršavanja ovog eksperimenta razmatran je samo pristup inženjerskim kontekstima u poslovnom sistemu (na *Slici 38.* scenario označen zelenim).

Prvi deo eksperimenta se odnosi na ispitivanje prava model inženjera da izvršava operacije izmene i testiranja modela u okviru konteksta za proveru kvaliteta. U prvom slučaju kontekstu pristupa sa inženjerske radne stanice (RS5), a u drugom slučaju sa poslovne radne stanice (RS6). Drugi deo eksperimenta se odnosi na ispitivanje prava dispečera posade da izvrši operacije dodele plana članovima posade u okviru konteksta za podršku operacijama na terenu. Takođe, dispečer posade prvo pristupa sistemu sa inženjerske radne stanice (RS5), a zatim sa poslovne radne stanice (RS6). Kako su inženjerske radne stanice konfigurisane tako da pristup bude omogućen samo inženjerskim korisničkim ulogama (uključujući model inženjera i dispečera posade), oba korisnika su uspešno izvršili operacije prilikom pristupa sistemu sa inženjerske radne stanice. Nasuprot tome, poslovne radne stanice su konfigurisane tako da inženjerskim ulogama pristup bude onemogućen te sa ovih radnih stanica nijedan od razmatranih korisnika nije imao pravo da izvrši navedene operacije. U *Tabeli 17.a)* i *Tabeli 17.b)* je prikazana uporedna analiza RBAC i predloženog RBAC-AORSG modela u zavisnosti od radne stanice sa koje model inženjer, odnosno dispečer posade uspostavlja korisnička sesija. Za razliku od RBAC modela koji ne razmatra radnu stanicu kao faktor koji može da utiče na odluke o pristupu resursima, RBAC-AOR$_{SG}$ pruža mogućnost ograničavanja skupa korisničkih uloga i oblasti odgovornosti u zavisnosti od namene radne stanice čime je prilikom uspostavljanja sesija korisnicima moguće dodeliti najmanji skup privilegija potreban za obavljanje zadataka u okviru korisničke sesije i tako smanjiti rizik od eskalacije privilegija usled dodele većeg nivoa privilegija od minimalno potrebnog.

Tabela 17. Rezultati analize kontrole pristupa prema nameni radne stanice u poslovnom sistemu

Kontekst za proveru kvaliteta

a)

Korisnik	Korisnička sesija	Radna stanica	Primenjeni model	Izmena modela
modelInženjer	**s1**	#RS5	RBAC	✓
			RBAC-AOR-SG	✓
	s2	#RS6	RBAC	✓
			RBAC-AOR-SG	×

Kontekst za podršku operacijama na terenu

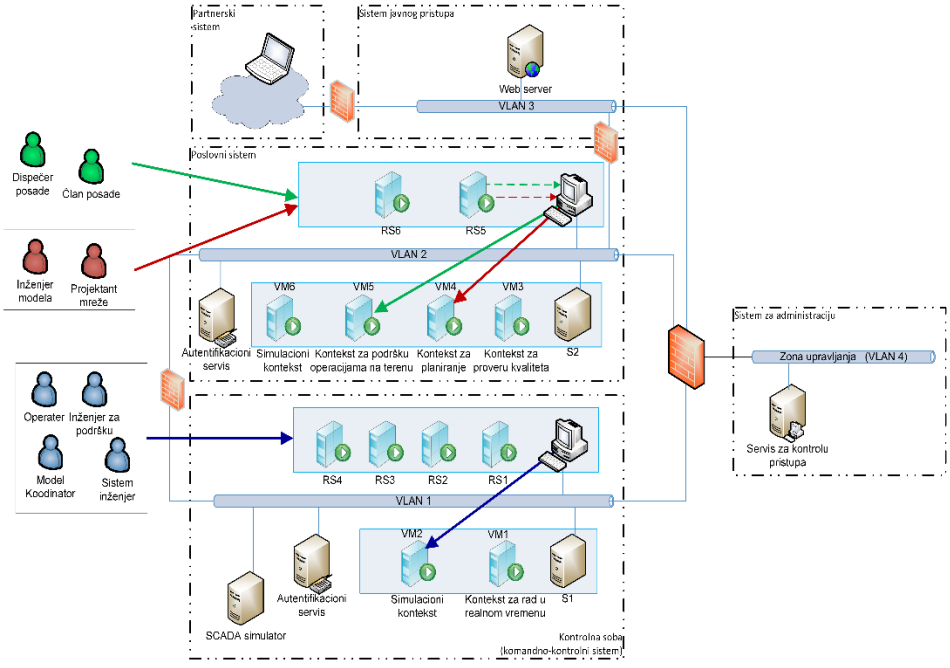
b)

Korisnik	Korisnička sesija	Radna stanica	Primenjeni model	Dodela plana posadi
dispečer Posade	**s1**	#RS5	RBAC	✓
			RBAC-AOR-SG	✓
	s2	#RS6	RBAC	✓
			RBAC-AOR-SG	×

7.5 Kontrola pristupa aplikativnim kontekstima

U ovom delu rada su prikazani eksperimenti za proveru usaglašenosti predloženog modela sa zahtevima za kontrolu pristupa prema tipu konteksta kojem korisnik pristupa kao što je navedeno u zahtevu C.AC.6. U zavisnosti od tipa konteksta, određene operacije nad objektima u sistemu nemaju isti stepen kritičnosti i bezbednosnih rizika, npr. operacija komandovanja nije podjednako kritična za aplikaciju za rad u realnom vremena i za simulacionu aplikaciju. Za istu operaciju u kontekstu za podršku operacijama na terenu treba da važi drugačija bezbednosna politika jer članovi posade treba da ažuriraju status izvršenih instrukcija u skladu sa dodeljenim planom koji ne mora da bude u vezi sa AOR-ima. Takođe, u zavisnosti od tipa konteksta različiti korisnici mogu imati pravo izvršavanja iste operacije. Npr. izvršavanje operacija u okviru konteksta za planiranje treba da bude omogućeno isključivo projektantima mreže, dok drugi korisnici ne bi smeli da imaju pristup ovom kontekstu.

Relevantne komponente okruženja za izvođenje ove grupe eksperimenata su istaknute na *Slici 39.* Plavim su označeni korisnici u kontrolnoj sobi koji pristupaju simulacionom kontekstu sa proizvoljne RS u kontrolnoj sobi. Crvenim je istaknut pristup korisnika iz poslovnog sistema kontekstu za planiranje, a zelenim kontekstu za podršku na terenu.



Slika 39. Test okruženje za analizu kontrole pristupa prema aplikativnom kontekstu

Za potrebe izvršavanja ove grupe testova kreirano je ukupno šest korisnika:

- Operater, inženjeri za podršku u kontrolnoj sobi i model koordinator u kontrolnoj sobi, pri čemu model koordinator ima prava pristupa i kontekstu za proveru kvaliteta u poslovnom sistemu.
- Sistem inženjer koji može imati pristup kontrolnoj sobi ali isključivo kontekstu za rad van realnog vremena.
- Dispečer posade i član posade koji pristupaju kontekstu za podršku operacijama na terenu.

Skup omogućenih AOR-a za pojedinačne korisnike je prikazan u *Tabeli 18.* Svim korisnicima su omogućeni AOR-i sa nivoima odgovornosti koji odgovaraju dodeljenim korisničkim ulogama (videti *Tabelu 7.*). Prilikom izvršavanja eksperimenata korišćene radne stanice su konfigurisane bez ograničenja u pogledu omogućenih uloga i AOR-a. Konfiguracija aplikativnih konteksta je definisana u skladu sa zahtevima opisanim u *Sekciji 3.2.3*. (videti *Prilog B.*). Potrebno je napomenuti da se konfiguracija svakog konteksta može menjati u skladu sa specifičnim zahtevima kompanija.

Tabela 18. Skup korisnika za analizu kontrole pristupa prema tipu konteksta (N-nadzor, K-kontrola, U-ažuriranje, ✓-omogućen AOR, ×-onemogućen AOR)

Korisnik	Korisnička uloga	AOR_R1_N	AOR_R1_K	AOR_R1_U	AOR_R2_N	AOR_R2_K	AOR_R2_U	AOR_R3_N	AOR_R3_K	AOR_R3_U
operater	R1	✓	✓	×	✓	✓	×	×	×	×
inženjer	R3	✓	✓	×	✓	✓	×	×	×	×
modelAdmin	R4	✓	×	✓	×	×	×	✓	×	✓
sisInženjer	R6	×	×	×	×	×	×	×	×	×
dispečer Posade	R9	×	×	×	×	×	×	×	×	×
clan Posada	R8	×	×	×	×	×	×	×	×	×

Ovi eksperimenti će potvrditi prednost RBAC-AOR$_{SG}$ modela u odnosu na RBAC u pogledu dinamičke izmene skupa ovlašćenja korisnika u zavisnosti od tipa konteksta kome se pristupa. Dodatno, ovi eksperimenti će pokazati prednost predloženog modela u rešavanju problema naglog porasta broja uloga koji bi mogao biti uzrokovan definisanjem različitih privilegija za iste operacije nad objektima u zavisnosti od tipa konteksta. Time će biti potvrđena Hipoteza H1 koja kaže da RBAC nije adekvatan za Smart Grid kada su u pitanju navedeni zahtevi, kao i Hipoteza H2 koja kaže da je RBAC moguće uskladiti sa ovim bezbednosnim zahtevom.

7.5.1 Dinamičke izmene ovlašćenja u kontrolnoj sobi

Zadatak ovog eksperimenta je ispitivanje mogućnosti dinamičkog proširenja skupa ovlašćenja korisnika u kontrolnoj sobi prilikom pristupanja simulacionom kontekstu, bez narušavanja principa najmanjih privilegija u kontekstu za rad u realnom vremenu (na *Slici 39.* označeno plavim).

U ovom eksperimentu su razmatrana prava korisnika u kontrolnoj sobi: operater, inženjer za podršku u kontrolnoj sobi i model koordinator za koje u simulacionom kontekstu ne treba da važe ograničenja kakva su u sistemu za rad u realnom vremenu, kako sa aspekta privilegija tako i sa aspekta AOR-a. Dodatno, razmatran je i sistem inženjer koji može imati pristup kontrolnoj sobi za potrebe studija i analiza optimizacije rada elektroenergetske mreže van realnog vremena, ali ne sme da ima pristup kontekstu za rad u realnom vremenu. Prilikom izvršavanja ovog eksperimenta navedeni korisnici pristupaju simulacionom kontekstu i izvršavaju različite tipove operacija nad objektima koji pripadaju različitim regionima elektroenergetskog sistema:

1. Operacije tipa nadzora: čitanje statusa uređaja,
2. Operacije tipa kontrole: komandovanje (npr otvaranja/zatvaranja prekidača), izvršenje UMS analitičkih funkcija
3. Operacije tipa ažuriranja: aktuelizacija modela mreže u produkciji,
4. Operacije nad logičkim objektima: kreiranje sekvence manipulacija.

U *Tabeli 19.* su prikazani uporedni rezultati dobijeni primenom predloženog RBAC-AOR_{SG} modela u zavisnosti od tipa aplikativnog konteksta, uključujući i rezultate dobijene primenom RBAC-a. Može se uočiti da iako korisnicima nisu omogućeni svi AOR-i, kada se pristupa simulacionom kontekstu dozvoljeno je izvršavanje operacija nad objektima bez obzira na dodeljene AOR-e. Takođe, skup omogućenih privilegija je proširen te korisnici mogu izvršavati operacije za koje nemaju dodeljene privilegije. Na primeru operatera se može da videti da on ima pravo da izvršava UMS analitičke funkcije ili menja model elektroenergetske mreže, kao i da upravlja svim delovima mreže bez obzira na skup omogućenih AOR-a u okviru simulacionog konteksta. A druge strane, inženjer sistema koji uopšte nema ovlašćenja u okviru konteksta za rad u realnom vremenu (nema omogućene AOR-e te ne može ni da čita podatke o stanju mreže), može da se bavi analizama sistema i kreiranjem planova manipulacija u okviru simulacionog konteksta, jer su mu prilikom uspostavljanja sesije dinamički omogućeni AOR-i.

Tabela 19. Rezultati analize mogućnosti dinamičke izmene ovlašćenja u kontrolnoj sobi (R1-region1, R2-region2, R3-region3, RT-RBAC-AOR$_{SG}$ kontekst za rad u realnom vremenu, SIM-RBAC-AOR$_{SG}$ simulacioni kontekst)

Korisnička sesija	Korisnik	Korisnička uloga	Primenjeni model	Čitanje			Komandovanje			Izvršavanje Fje			Aktuelizacija			Kreiranje sekvence
				R1	R2	R3	R1	R2	R3	R1	R2	R3	R1	R2	R3	
s1	operater	R1	RBAC	✓	✓	✓	✓	✓	✓	×	×	×	×	×	×	✓
			RT	✓	✓	×	✓	✓	×	×	×	×	×	×	×	✓
			SIM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
s2	inženjer	R3	RBAC	✓	✓	✓	×	×	×	✓	✓	✓	×	×	×	×
			RT	✓	✓	×	×	×	×	✓	✓	×	×	×	×	×
			SIM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
s3	modelAdmin	R4	RBAC	✓	✓	✓	×	×	×	×	×	×	✓	✓	✓	×
			RT	✓	×	✓	×	×	×	×	×	×	✓	×	✓	×
			SIM	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
s4	sisInženjer	R6	RBAC	✓	✓	✓	×	×	×	×	×	×	×	×	×	✓
			RT	×	×	×	×	×	×	×	×	×	×	×	×	
			SIM	✓	✓	✓	×	×	×	✓	✓	✓	×	×	×	✓

7.5.2 Dinamičke izmene ovlašćenja u poslovnom sistemu

Zadatak ovog eksperimenta je ispitivanje mogućnosti izmene skupa ovlašćenja prilikom pristupa kontekstima u poslovnom sistemu, pre svega kontekstu za podršku operacijama na terenu i kontekstu za planiranje. Kontekst za podršku operacijama na terenu je namenjen članovima posade koji unose podatke o izvršenim radovima na terenu. Kako članovima posade konfiguracijom nije omogućen nijedan AOR, oni nemaju pravo manipulacije u okviru konteksta za rad u realnom vremenu. Kontekst za planiranje je namenjen isključivo projektantima mreže koji prave planove izgradnje i održavanja elektroenergetskog sistema. Projektantima mreže nisu dodeljeni AOR-i niti privilegije za izmenu modela, jer bi u tom slučaju mogli da rade u okviru konteksta za proveru kvaliteta. S druge strane, koordinator ima odgovarajuće privilegije i AOR-e za ažuriranje modela, ali to ne sme da mu bude omogućeno u okviru planerskog konteksta.

U prvom delu eksperimenta, članovi i dispečeri posade pristupaju kontekstu za podršku operacijama na terenu (na *Slici 39.* označeno zelenim) i izvršavaju operacije dodele planova posadi i ažuriranje statusa o izvršenim operacijama na terenu. Kako članovima posade nisu omogućeni AOR-i oni nemaju pravo da unesu podatke o izvršenim operacijama. Primenom bezbednosne politike za kontekst za podršku operacijama na terenu članovima posade su dinamički omogućeni svi AOR-i prilikom uspostavljanja sesije i time proširen skup prava u datoj korisničkoj sesiji. U *Tabeli 20.* su prikazani uporedni rezultati dobijeni primenom predloženog RBAC-AOR$_{SG}$ proširenja u zavisnosti tipa aplikativnog konteksta, kao i rezultati dobijeni primenom RBAC-a. Na primeru korisnika kome je dodeljena uloga člana posade može se videti da on može da izvršava operacije u okviru konteksta za podršku operacijama na terenu, dok istu operaciju ne može da izvrši u okviru konteksta za rad u realnom vremenu. Kako politikom za ovaj kontekst nije definisana izmena skupa omogućenih privilegija, članovi posade ne mogu da izvrše operaciju dodele planova, već samo dispečeri kojima je dodeljena odgovarajuća privilegija.

Tabela 20. Rezultati analize mogućnosti dinamičke izmene ovlašćenja u u okviru konteksta za podršku operacijama na terenu (R1-region1, R2-region2, R3-region3, RT-RBAC-AOR$_{SG}$ kontekst za rad u realnom vremenu, FIELD-RBAC-AOR$_{SG}$ kontekst za podršku operacijama na terenu)

	Korisnik	Korisnička uloga	Primenjeni model	Čitanje			Izvršavanje sekvence			Dodela plana posadi	Ažuriranje stanja o posadi
				R1	R2	R3	R1	R2	R3		
s1	član Posade	R8	RBAC	✓	✓	✓	✓	✓	✓	×	✓
			RT	×	×	×	×	×	×	×	✓
			FIELD	✓	✓	✓	✓	✓	✓	×	✓
s2	dispečer Posade	R9	RBAC	✓	✓	✓	×	×	×	✓	✓
			RT	×	×	×	×	×	×	✓	✓
			FIELD	✓	✓	✓	×	×	×	✓	✓

U drugom delu eksperimenta model koordinator i projektant mreže pristupaju kontekstu za planiranje (na *Slici 39.* označeno crvenim). Prilikom izvršavanja eksperimenta oni izvršavaju operaciju izmene modela mreže. U *Tabeli 21.* su prikazani uporedni rezultati dobijeni primenom predloženog RBAC-AOR$_{SG}$ modela u zavisnosti od izabranog aplikativnog konteksta, uključujući i rezultat dobijen primenom RBAC-a. Može se zaključiti da je bezbednosnom politikom konteksta za planiranje izvršeno dinamičko proširenje skupa ovlašćenja za korisnike koji su članovi uloge projektanta mreže, dok su istom bezednosnom politikom ostale korisničke uloge onemogućene uključujući i model koordinatora.

Tabela 21. Rezultati analize mogućnosti dinamičke izmene ovlašćenja u u okviru konteksta za planiranje (R1-region1, R2-region2, R3-region3, RT-RBAC-AOR$_{SG}$ kontekst za rad u realnom vremenu, PLAN-RBAC-AOR$_{SG}$ kontekst za planiranje)

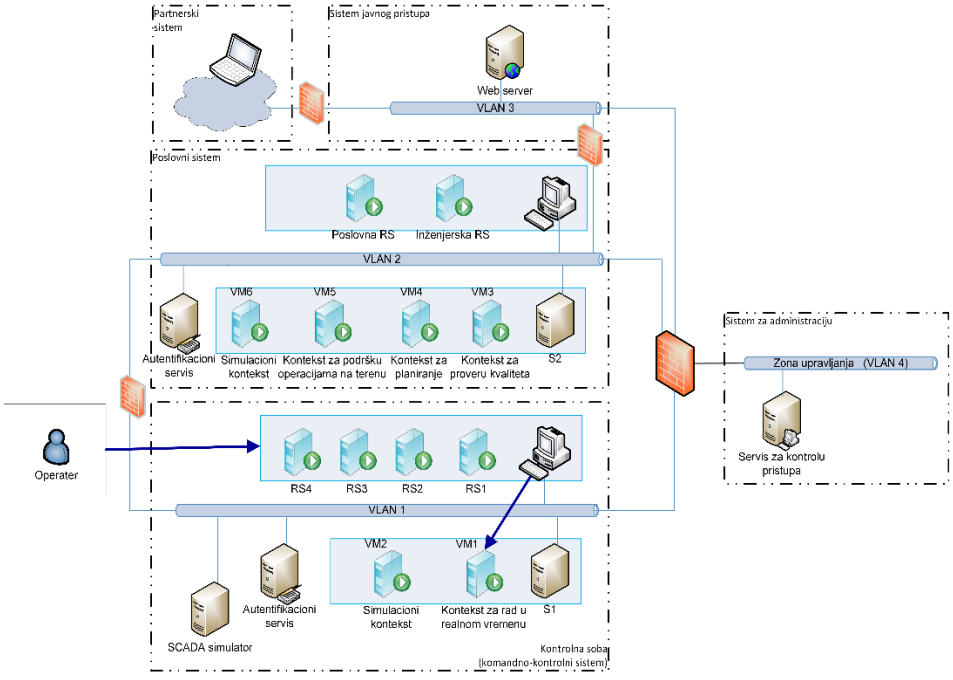
	Korisnik	Korisnička uloga	Primenjeni model	Čitanje			Izmena modela		
				R1	R2	R3	R1	R2	R3
s1	projektant	R7	RBAC	✓	✓	✓	×	×	×
			RT	×	×	×	×	×	×
			PLAN	✓	✓	✓	✓	✓	✓
s2	model Admin	R4	RBAC	✓	✓	✓	✓	✓	✓
			RT	✓	✓	✓	✓	✓	✓
			PLAN	×	×	×	×	×	×

Prednost RBAC-AOR$_{SG}$ modela u poređenju sa RBAC-om se ogleda u mogućnosti dinamičke izmene (proširenja ili ograničenja) skupa ovlašćenja kada korisnici pristupaju aplikacijama koje nemaju direktan uticaj na rad sistema u realnom vremenu. Da bi RBAC model zadovoljio ovaj zahtev bilo bi potrebno definisati odgovarajući skup ovlašćenja za svaki kontekst posebno, što u realnom sistemu gde može biti definisano nekoliko desetina privilegija ovakav pristup vodi ka naglom porastu broja privilegija. Umesto definisanja različitih privilegija za operacije nad objektima u zavisnosti od tipa konteksta, RBAC-AOR$_{SG}$ omogućuje dinamičke izmene prilikom uspostavljanja korisničke sesije u skladu sa bezbednosnim pravilima određenog Smart Grid konteksta, pritom ne narušavajući princip najmanjih privilegija u okviru aplikacija za rad u realnom vremenu. Odnosno, RBAC-AOR$_{SG}$ pruža mogućnost definisanja različitog skupa ovlašćenja za korisničke uloge bez uvođenja dodatnih privilegija i bez narušavanja principa najmanjih privilegija.

7.6 Kontrola pristupa prema licenci

U ovom delu rada će biti prikazani rezultati eksperimenata za proveru usaglašenosti RBAC-AOR$_{SG}$ modela sa zahtevima za kontrolu pristupa prema važećoj licenci korisnika, kao što je navedeno u zahtevu C.AC.5. Ovim eksperimentom će biti potvrđena prednost predloženog RBAC-AOR$_{SG}$ modela u pogledu ograničavanja pristupa sistemu u zavisnosti od toga da li korisnik poseduje važeći licencu za izvršavanje zadataka koji su regulisani licencom. Time će biti potvrđena Hipoteza H1 koja kaže da RBAC nije adekvatan za Smart Grid kada su u pitanju kontrola pristupa prema određenim vremenskim odrednicama poput važeće licence korisnika, kao i Hipoteza H2 koja kaže da je RBAC moguće uskladiti sa ovim bezbednosnim zahtevom.

Prilikom izvršavanja ovog eksperimenta razmatrana su tri korisnika iz grupe operatera i definisane odgovarajuće licence. Pritom, za jednog korisnika je licenca istekla, drugom korisniku je period važenja podešen tako da licenca ističe za pet minuta nakon uspostavljanja sesije tako da licenca postane nevažeća u toku sesije, a trećem korisniku licenca važi narednih godinu dana. Prilikom izvršavanja eksperimenta, operateri pristupaju kontekstu za rad u realnom vremenu sa proizvoljne RS u kontrolnoj sobi, kao što je istaknuto na *Slici 40.* i izvršavaju operaciju komandovanja. Podrazumeva se da su svim operaterima aktivirani svi AOR-i te oni nemaju uticaj na rezultat izvršavanja operacije komandovanja.



Slika 40. Test okruženje za analizu kontrole pristupa prema licenci

U *Tabeli 22.* su prikazani uporedni rezultati dobijeni primenom RBAC-AOR$_{SG}$ i RBAC modela. RBAC ne razmatra licencu korisnika te nema razlike u ovlašćenjima zavisno od toga da li je licenca važeća. Za razliku od RBAC-a, RBAC-AOR$_{SG}$ pruža mogućnost ograničavanja korisničkih uloga ukoliko korisnik nema važeću licencu. Na primeru operatera1 može se zaključiti da on nema pravo komandovanja, jer je licenca nevažeća u momentu uspostavljanja sesije, te su mu su onemogućene privilegije dodeljene posredstvom uloge regulisane datom licencom. Na primeru drugog operatera može se uočiti manjkavost predloženog rešenja kada je u pitanju kontrola pristupa prema licenci. Naime, u toku izvršavanja sesije operateru2 je istekla licenca, ali mu je omogućeno izvršavanje operacija komandovanja i nakon isteka. Tek prilikom uspostavljana naredne sesije odgovarajuća uloga će biti onemogućena. Ovaj nedostatak je uzrokovan početnom pretpostavkom da je licenca nepromenljivi parametar sesije.

Tabela 22. Rezultati analize kontrole pristupa prema licenci (1-trenutak odmah nakon uspostavljanja korisničke sesije, 2-period nakon uspostavljanja korisničke sesije)

	Korisnik	Primenjeni model	Period važenja licence	Komandovanje nakon uspostavljanja ssije	Komandovanje 5 min nakon uspostavljanja sesije
s1	operater1	RBAC	istekla	✓	✓
		RBAC-AOR-SG		×	×
s2	operater2	RBAC	istekla 5min nakon uspostavljanja sesije	✓	✓
		RBAC-AOR-SG		✓	✓
s3	operater3	RBAC	ističe za 1god	✓	✓
		RBAC-AOR-SG		✓	✓

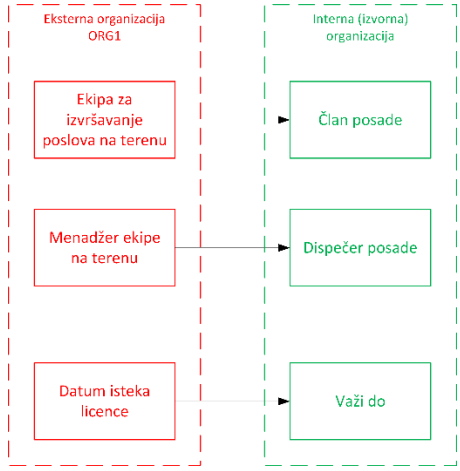
7.7 Kontrola pristupa u interorganizacionim sistemima

Cilj ovog eksperimenta je ispitivanje mogućnosti primene predloženog rešenja u interorganizacionim sistemima u skladu sa postavljenim C.AC.8 zahtevima. U okviru ovog esksperimenta se ispituje mogućnosti uvažavanja globalne politike kojom su definisana pravila transformacije korisničkih uloga i atributa između organizacija, sa ciljem da se potvrdi prednost RBAC-AOR$_{SG}$ modela u pogledu rešavanja problema duple administracije podataka o eksternim korisnicima u interorganizacionim sistemima. Za razliku od RBAC modela koji nije primenjiv u distribuiranom, više-domenskom okruženju, primenom modela globalne politike RBAC-AOR$_{SG}$ to omogućuje bez uvećanja kompleksnosti administracije ili problema sinhronizacije podataka o korisnicima. Time će biti potvrđena Hipoteza H1 koja kaže da RBAC nije adekvatan za više-domenske sisteme kakav Smart Grid često jeste, kao i Hipoteza H2 koja kaže da je RBAC moguće uskladiti sa ovim bezbednosnim zahtevom.

Kako federacija u labavo spregnutom okruženju i delegiranje autentifikacije nije tema ovog istraživanja, kreiranje identiteta eksternih korisnika je simulirano u test okruženju tako što su kreirani interni korisnici kojima su dodeljene uloge koje ne postoje u izvornom sistemu već predstavljaju eksterne uloge. Takođe, umesto unapred definisanog korisničkog atributa koji predstavlja jedinstveni identifikator licence u izvornom sistemu korišćen je neki drugi atribut korisnika koji označava datum isteka licence iz eksterne organizacije. U *Tabeli 23.* je dat primer konfiguracije eksternih korisnika (označeno plavim), dok je na *Slici 41.* dat primer globalne politike koja je korišćena u ovom eksperimentu. Prva dva korisnika za naziv organizacije imaju vrednost ORG1 koja je definisana globalnom politikom, dok treći korisnik za naziv organizacije ima vrednost ORG2 za koju ne postoji definisana globalna politika.

Tabela 23. Model globalne politike i model korisnika iz eksternih organizacija

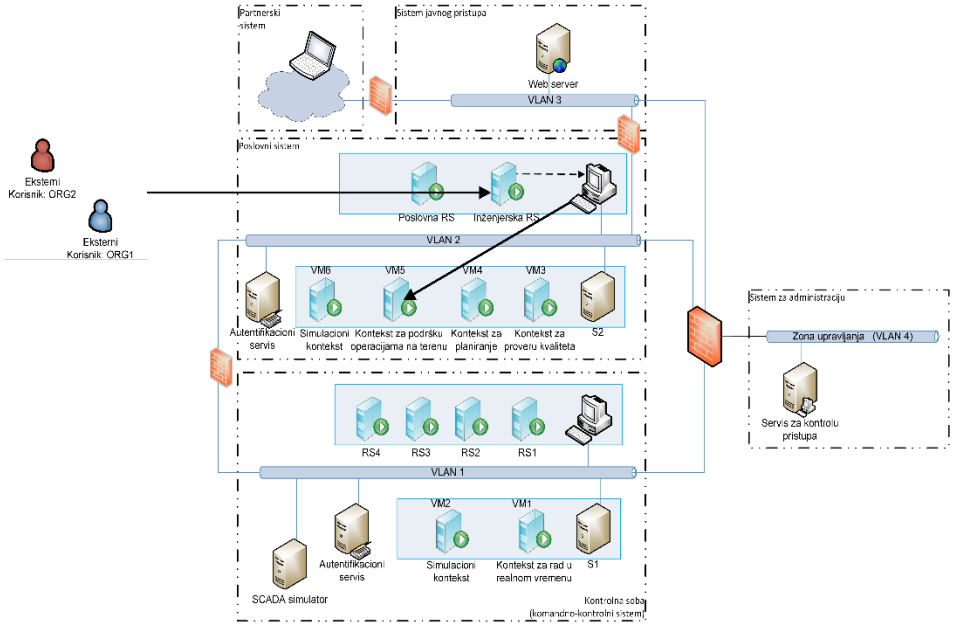
	Korisnik	Org	Eksterna uloga	Eksterni atribut	Upravljanje posadom
				Datum isteka licence	
s1	posada1	ORG1	Ekipa za obavljanje poslova na terenu	31.12.2017.	✓
s2	posada2	ORG1	Ekipa za obavljanje poslova na terenu	01.01.2017.	×
s3	posada3	ORG2	Ekipa za obavljanje poslova na terenu	31.12.2017.	×



Slika 41. Primer globalne politike

Na primeru tipične korisničke uloge koja može biti dodeljena korisnicima iz eksternih organizacija (član posade) ispitana je mogućnost izvršavanja operacija u internom sistemu, kao što je prikazano na *Slici 42.* Eksterni korisnici pristupaju kontekstu za podršku operacijama na terenu i izvršavaju tipične operacije članova posade, npr. ažuriranje statusa o lokaciji posade. Prilikom pristupa sistemu korišćena je inženjerska

radna stanica konfigurisana bez ograničenja u pogledu omogućenih uloga kako podešena konfiguracija ne bi imala uticaj na ishod rezultata.



Slika 42. Test okruženje za analizu kontrole pristupa u interorganizaciji

Prvo su ispitane mogućnosti korisnika koji pristupaju sistemu iz eksternih organizacija za koje je definisana globalna politika. Na primeru prvog korisnika može se zaključiti da je vrednost eksterne korisničke uloge i atributa licence uspešno mapirana na odgovarajuće interne vrednosti i da je korisniku omogućeno izvršavanje operacije ažuriranja statusa o lokaciji. Na primeru drugog korisnika može se zaključiti da su vrednost eksterne korisničke uloge i atributa licence uspešno mapirana na odgovarajuće interne vrednosti, a kako je istekao period važenja licence (tj. podešen datum isteka u prošlosti) korisniku je onemogućena uloga člana posade te nema pravo da izvrši datu operaciju. Zatim su ispitane mogućnosti korisnika koji pristupaju sistemu iz eksternih organizacija za koje nije definisana globalna politika. Na primeru trećeg korisnika može se uočiti da korisniku nije dozvoljeno da izvrši navedenu operaciju, odnosno da je korisnička uloga onemogućena. Potrebnoje napomenuti da u realnim sistemima podsistem za autentifikaciju uopšte neće dozvoliti pristup korisnicima iz organizacija sa kojima nije uspostavljena federacija.

8 Zaključak

Poslednjih godina elektroenergetska industrija se suočava sa različitim problemima uzrokovanim informaciono-bezbednosnim propustima koji mogu imati izuzetno značajne posledice. Zbog svoje kritičnosti za funkcionisanje modernog društva savremeni elektroenergetski sistemi (odnosno Smart Grid sistemi) su veoma česta meta sajber napada. Jedan od najpoznatijih napada na industrijske kontrolne sisteme je *Stuxnet* napad na iranska nuklearna postrojenja koji je rezultovalo finansijskim gubicima i unazadio razvoj nuklearnih mogućnosti države. Ukrajinski napad 2015. godine je hakerski napad koji je uzrokovao prekid napajanja kod 225000 potrošača u trajanju do 6 sati kada su napadači preko udaljenog pristupa industrijskim kontrolnim sistemima isključili delove elektrodistributivne mreže.

Informacione i komunikacione tehnologije su ključni faktor u razvoju pametnih mreža, ali njihovom primenom se savremene elektroenergetske infrastrukture istovremeno izlažu novim bezbednosnim pretnjama i rizicima koji u tradicionalnim sistemima nisu postojali. Oslanjanjem na komunikacione mreže i međusobnim povezivanjem sistema koje karakteriše raznolikost u pogledu funkcionalnosti i korišćenih tehnologija povećava se i ranjivost sistema na različite napade koji imaju za cilj da ugroze raspoloživost, integritet i poverljivost informacionih sistema. Osim toga, međusobno povezivanje sistema i sve veći broj pristupnih tačaka za razmenu podataka između sistema omogućuje lateralnu propagaciju zlonamernog softvera i/ili napadača kroz zahvaćeni sistem i uspešan napad na sistem. Implementacija jakih i robusnih kontrola pristupa prilagođenih složenim zahtevima savremenih elektroenergetskih sistema je od suštinske važnosti za dostizanje adekvatnog nivoa informacione bezbednosti.

Predmet istraživanja ove distertacije pripada oblasti kontrole pristupa u Smart Grid sistemima. Sistematizacijom zahteva savremenih elektroenergetskih kompanija, kao i zahteva propisanih tehničkim standardima u oblasti informacione bezbednosti za Smart Grid, formiran je skup zahteva za kontrolu pristupa u Smart Gridu. Analizom zahteva je ustanovljeno da model kontrole pristupa u Smart Grid sistemima pored zaštite od neovlašćenog pristupa i zloupotrebe privilegija treba da obezbedi zaštitu od nenamernih grešaka validnih korisnika i omogući pouzdanije i efikasnije upravljanje sistemom.

Hipoteza H1 kaže da RBAC nije adekvatan model kontrole pristupa za Smart Grid. RBAC je najčešće korišćeni model kontrole pristupa u sistemima koje karakteriše veliki broj korisnika i resursa koje je potrebno zaštititi. Međutim, RBAC nije primenljiv u Smart Grid okruženju, jer nema mogućnost uvažavanja parametara koji nisu deo identiteta korisnika, ali mogu uticati na odluke o pristupu resursima. Takođe, RBAC ne može da obezbedi podelu odgovornosti između korisnika koji pripadaju istim korisničkim ulogama što je ključni zahtev za pouzdano i efikasno izvršavanje kritičnih operacija u Smart Gridu, niti može da odgovori dinamičnim zahtevima okruženja kao što su

vanredne situacije uzrokovane velikim vremenskim nepogodama, otkazi radnih stanica, i slično.

Na osnovu detaljne analize dostupne naučne i stručne literature zaključeno je da postojeći modeli kontrole pristupa ne mogu da odgovore aktuelnim zahtevima u elektroenergetskoj industriji. ABAC model pruža mogućnost uvažavanja širokog spektra atributa koje je potrebno razmotriti prilikom donošenja odluke o pristupu resursima. Međutim, u Smart Grid sistemima koji uključuju hiljade korisnika i milione uređaja i opreme ABAC model nije prihvatljiv zbog velikog broja autorizacionih pravila koje je potrebno definisati. Takođe, računanje vrednosti autorizacionih pravila u toku izvršavanja može značajno uticati na performanse što u sistemima za rad u realnom vremenu nije prihvatljivo. U cilju prevazilaženja ograničenja RBAC i ABAC modela u heterogenim distribuiranim sistemima u dostupnoj literaturi se razmatraju dva pristupa. Prvi pristup je proširivanje i unapređenje RBAC modela. Osnovni problem ovakvog pristupa je to što ne postoji opšti model koji objedinjuje prednosti različitih proširenja i koji je moguće primeniti ili jednostavno proširiti za potrebe drugih sistema. Drugi pristup je razvoj hibridnih RBAC-A modela kojima se pokušavaju iskoristiti prednosti RBAC i ABAC modela. Međutim, nijedan od navedenih pristupa integracije RBAC i ABAC modela ne može da odgovori postavljenim zahtevima u Smart Gridu. RBAC-A orijentisan ka atributima nije pogodan za Smart Grid iz istog razloga kao i ABAC model obzirom da su korisničke uloge samo dodatni atribut korisnika. RBAC-A orijentisan ka ulogama i RBAC-A pristup sa dinamičkim ulogama imaju ograničenja sa aspekta primene dinamičkih ograničenja prilikom uspostavljanja korisničke sesije te ne mogu adekvatno da odgovore specifičnim zahteva u Smart Gridu. Dodatno, nijedan od razmatranih modela nema mogućnost izmene ovlašćenja u toku izvršavanja korisničke sesije kako bi se obezbedilo kontinualno upravljanje elektroenergetskim sistemom kako u regularnom režimu rada tako i u vanrednim situacijama.

Hipoteza H2 kaže da je RBAC moguće uskladiti sa aktuelnim bezbednosnim zahtevima elektroenergetske industrije u oblasti kontrole pristupa, kako zahtevima postavljenim od strane elektroenergetskih kompanija, tako i zahtevima koji su definisani vladajućim standardima u oblasti informacione bezbednosti za Smart Grid. Osnovni doprinos ove disertacije se ogleda u razvoju RBAC-AOR$_{SG}$ modela kontrole pristupa koji predstavlja prošireni RBAC model koji je usklađen sa postavljenim zahtevima za kontrolu pristupa u Smart Gridu. RBAC-AOR$_{SG}$ ima mogućnost podele odgovornosti između korisnika koji pripadaju istim korisničkim ulogama prema oblasti odgovornosti čime se obezbeđuje pouzdano i efikasno upravljanje sistemom u skladu sa zahtevima za rad u realnom vremenu. To se odnosi na mogućnost konstantnog nadzora i kontrole svih delova elektroenergetskog sistema u regularnom režimu rada sistema, ali i u vanrednim situacijama. Hijerarhijskom organizacijom oblasti odgovornosti moguće je olakšati administraciju modela kontrole pristupa i smanjiti broj oblasti odgovornosti koje je potrebno dodeliti korisnicima. RBAC-AOR$_{SG}$ uvažava lokaciju ili namenu radne stanice sa koje korisnik pristupa sistemu prilikom donošenja odluke o pristupu resursima, čime se

smanjuje rizik od zloupotrebe u slučaju pristupa sistemu sa udaljenih lokacija, i sprečava omogućavanje višeg nivoa privilegija nego što je potrebno za obavljanje zadataka u uspostavljenoj sesiji. U zavisnosti od tipa Smart Grid konteksta, RBAC-AOR$_{SG}$ pruža mogućnost dinamičke izmene bezbednosne politike prilikom uspostavljanja korisničke sesije bez uvođenja kompleksnosti administracije ili narušavanja principa najmanjih privilegija u sistemima za rad u realnom vremenu. Primenom RBAC-AOR$_{SG}$ modela moguće je ograničiti korisničke uloge čije je obavljanje regulisano važećom licencom u situacijama kada licenca prestane da važi. Dodatno, bez uvođenja kompleksnosti administracije i sinhronizacije podataka o korisnicima, RBAC-AOR$_{SG}$ je jednostavno primenljiv i u multi-domenskom okruženju.

Na osnovu predloženog RBAC-AOR$_{SG}$ modela postavljena je softverska arhitektura servisa za kontrolu pristupa. Prototipskom implementacijom servisa za kontrolu pristupa i njegovom integracijom u simuliranom Smart Grid okruženju u skladu sa standardnim IEC-62443 modelom bezbednosne arhitekture potvrđena je Hipoteza H3 koja kaže da je prošireni RBAC model moguće primeniti u Smart Grid u skladu sa postavljenim bezbednosnim zahtevima. Takođe, ovim je potvrđena i praktična vrednost predloženog modela kontrole pristupa u Smart Gridu.

Mogućnost daljeg istraživanja i usavršavanja predloženog modela ogleda se pre svega u unapređenju modela kontrole pristupa u sistemima za podršku operacijama na terenu. Predloženi model razmatra podelu odgovornosti između korisnika kada je u pitanju izvršavanje kritičnih operacija koje imaju direktan uticaj na stabilan i ispravan rad elektorenergetskog sistema. To uključuje operacije sistema za rad u realnom vremenu i sistema za proveru kvaliteta modela elektroenergetske mreže. Predloženo rešenje ne razmatra podelu odgovornosti između korisnika u sistemima za podršku operacijama na terenu čija osnovna namena je pružanje informacija ekipi na terenu o trenutnom stanju mreže kao i mogućnost ažuriranja statusa izvršenih instrukcija. U sistemima za podršku operacijama na terenu je potrebno omogućiti kontrolu pristupa prema oblasti odgovornosti, ali tako da se umesto statičke dodele AOR-a omogući automatska aktivacija/deaktivacija AOR-a u zavisnosti od trenutne lokacije članova posade na terenu. To se može postići integracijom modela kontrole pristupa sa sistemom za pozicioniranje objekata, i računanjem oblasti odgovornosti na osnovu geografske lokacije ekipe na terenu. Pritom, osim problema autentičnosti i integriteta informacija o lokaciji korisnika, posebnu pažnju treba posvetiti poverljivosti ovih podataka čijim kompromitovanjem može biti ugrožena privatnost korisnika.

Literatura

[1] Aberg, E. Review of an industrially implemented model of zoning principles for electricity distribution and energy production. Degree project in ICS Master thesis, KTH, School of Electrical Engineering (EES). Stockholm, Sweden 2011.

[2] Abowd, G. D., Dey, A. K., Brown, P. J., Davies, N., Smith, M., Steggles, P. Towards a better understanding of context and contextawareness. In Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing (HUC '99), pp. 304–307, London, UK, 1999. Springer-Verlag.

[3] Active Directory Federation Services, https://msdn.microsoft.com/en-us/library/bb897402.aspx

[4] A Harris Williams & Co. White Paper. Transmission & Distribution Infrastructure. 2014.

[5] Aloul, F., Al-Ali, A.R., Al-Daku, R., Al-Mardini, M., El-Hajj, W. Smart Grid Security: Threats, Vulnerabilities and Solutions. International Journal of Smart Grid and Clean Energy. September 2012. Vol. 1, No. 1, pp. 1-6.

[6] Anwar, A., Mahmood, A. Cyber Security of Smart Grid Infrastructure. The State of the Art in Intrusion Prevention and Detection. CRC Press, Taylor & Francis Group, USA. January 2014. pp. 449-472.

[7] Bammigatti, P. H., Rao, P. R. Generic WA-RBAC: role based access control model for web applications. Proceedings of the 9th International Conference on Information Technology (ICIT '06). pp. 237–240, Washington, DC, USA, 2006. IEEE Computer Society.

[8] Barroso, L. A., Cavalcanti, T. H., Geisbertz, P., Purchala, K. Classification of electricity market models worldwide. CIGRE/IEEE PES, 2005. International Symposium, New Orleans, LA. October 2005. pp. 9-16.

[9] Baumeister, T. Literature Review on Smart Grid Cyber Security. Technical Report. December 2010.

[10] Berizzi, A. The Italian 2003 blackout. IEEE PES General Meeting Denver. 7th – 11th June 2004.

[11] Bertino, E., Bonatti, P. A., Ferrari, E. TRBAC: A Temporal Role-based Access Control Model. ACM Transactions on Information and System Security (TISSEC). August 2001. Vol. 4, No. 3, pp. 191-233.

[12] Bertino, E., Catania, B., Damiani, M. L., Perlasca, P. GEO-RBAC: A Spatially Aware RBAC. 10th ACM symposium on Access control models and technologies. 2005. pp. 29-37.

[13] Bojanić, S., Đorđević, S. Tehnološka rešenja i zakonska regulativa za zaštitu privatnosti korisnika naprednih elektroenergetskih mreža. Naučno-stručni simpozijum Energetska efikasnost (ENEF 2013), Banja Luka, Novembar 2013.

[14] Boldizsar B., Gabor P., Levente B., Mark F. Duqu: A Stuxnet-like malware found in the wild. Laboratory of Cryptography and Systems Security (CrySyS), Budapest University of Technology and Economics, Department of Telecommunication. 2011.

[15] Byres, E. Using ISA/IEC 62443 Standards to Improve Control System Security. Tofino Security, WhitePaper. Version 1.2., May 2014.

[16] Caswell, J. A Survey of Industrial Control Systems Security. http://www.cse.wustl.edu/~jain/cse571-11/ftp/ics/index.html (pristup: maj 2016.).
[17] Chandy, K. M., Gooding, J., McDonald, J. Smart Grid System-of-Systems Architectures, Systems Evolution to Guide Strategic Investments in Modernizing the Electric Grid.
[18] Chen P., Desmet L., Huygens C. A Study on Advanced Persistent Threats. In: De Decker B., Zúquete A. (eds) Communications and Multimedia Security. CMS 2014. Lecture Notes in Computer Science, vol 8735. Springer, Berlin, Heidelberg.
[19] Cohen, E., Thomas, R. K., Winsborough, W., Shands, D. Models for coalition-based access control (CBAC). Proceedings of the 7th ACM symposium on Access control models and technologies (SACMAT '02), pp. 97–106, New York, NY, USA, 2002.
[20] Committee on America's Energy Future, Division on Engineering and Physical Sciences, National Research Council, National Academy of Engineering. America's Energy Future: Technology and Transformation. http://nap.edu/12091
[21] Damiani, M. L., Bertino, E., Catania, B., Perlasca, P. GEO-RBAC: A Spatially Aware RBAC. ACM Transactions on Information Systems and Security (TISSEC). February 2007. Vol. 10, No. 1.
[22] Damiani, E., Vimercati, S. D. C., Samarati, P. New paradigms for access control in open environments. 5th IEEE International Symposium on Signal Processing and Information technology, Athens. December 2005. pp. 540-545.
[23] Dawson, S., Qian, S., Samarati, P. Providing security and interoperation of heterogeneous systems. Distributed and Parallel Databases, 8(1):119–145, 2000.
[24] European Network and Information Security Agency, Annex II. Security aspects of the Smart Grid. https://www.enisa.europa.eu/
[25] European Network and Information Security Agency. Appropriate security measures for smart grids - Guidelines to assess the sophistication of security measures implementation. 2012.
[26] Fan, X., Fan, K., Wang, Y. Overview of cyber-security of industrial control system. 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC). Shanghai, China. August 2015.
[27] 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.
[28] Ferraiolo, D. F., Kuhn, D. R. Role-Cased Access Controls. 15th National Computer Security Conference. Baltimore, MD. October 1992. pp. 554-563.
[29] Ferraiolo, D. F., Kuhn, D. R., Chandramouli, R. Role-Based Access Control. Artech House, Second Edition, 2007..
[30] Ferraiolo, D. F., Sandhu, R. S., Gavrila, S., Kuhn, D. R., Chandramouli, R. Proposed NIST Standard for Role-Based Access Control. ACM Transactions on Information and System Security. August 2001. Vol. 4, No. 3, pp. 224–274.
[31] Ghansah, I. Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks. California Energy Commission, PIER Energy-Related Environmental Research Program, CEC-500-2012-047, 2009.
[32] Gibney, A. Zero Days. Documentary, 2016.
[33] Gibson, D. SSCP Systems Security Certified Practitioner All-in-One Exam Guide, Second Edition. McGraw-Hill Education. April 2015..

[34] Global Smart Grid Federation (GSGF). UK Policy Drivers. April 2014.
[35] Gostojić, S., Sladić, G., Milosavljević, B., Konjović, Z. Context-Sensitive Access Control Model for Government Services. Journal of Organizational Computing and Electronic Commerce. 2012. 22:2, 184-213.
[36] Hansen, F., Oleshchuk, V. SRBAC: A Spatial Role-Based Access Control Model for Mobile Systems. 7th Nordic Workshop on Secure IT Systems (NORDSEC'03). 2003.
[37] Hansen, F., Oleshchuk, V. Application of Role-Based Access Control in Wireless Healthcare Information Systems. Scandinavian Conference in Health Informatics. 2003. pp. 30-33.
[38] Homeland Security. Recommended practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. October 2009.
[39] ICS-CERT. Cyber-Attack Against Ukrainian Critical Infrastructure.
[40] IEC 61968-11:2013. Application integration at electric utilities - System interfaces for distribution management - Part 11: Common information model (CIM) extensions for distribution. IEC, Edition 2.0. Mart 2013.
[41] IEC 61970-301:2013. Energy management system application program interface (EMS-API) - Part 301: Common Information Model (CIM) Base. IEC, Edition 5.0. December 2013.
[42] IEC 62351 Security Standards for the Power System Information Infrastructure. IEC TC57 WG15. International Electrotechnical Commission (IEC). June 2012.
[43] IEC/TR 62443-3-1: Security for industrial automation and control systems - security technologies for IACS. International Society of Automation (ISA). 2007.
[44] IEC-62443-3-2: Security for industrial automation and control systems - Security risk assessment and system design. International Society of Automation (ISA). 2016.
[45] IEC 62443-3-3: Security for industrial automation and control systems - System security requirements and security levels. International Society of Automation (ISA). 2016.
[46] InfoSec Institute. VLAN Network Segmentation and Security – Chaper 5. InfoSec Institute. April 2012. http://resources.infosecinstitute.com/vlan-network-chapter-5/ (pristup: avgust 2016.).
[47] International Society of Automation (ISA). Overview - The 62443 series of standards - Industrial Automation and Control Systems Security. 2015.
[48] International Standard ISO/IEC 27000:2016, Information technology – Security techniques – Information security managemet systems – Overview and vocabilary, Fourth edition, February 2016.
[49] ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems. International Standards Organization (ISO). 2013.
[50] ISO/IEC 27002:2013. Information technology - Security Techniques - Code of practice for information security management. International Standards Organization (ISO). 2013.
[51] Jin, X. Attribute-based Access Control Models and Implementation in Cloud Infrastructure as a Service. The University of Texas at San Antonio. May 2014.
[52] Jin, X., Krishnan, R., Sandhu, R. A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC. Proceedings of the 26th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec '12), pp. 41-55, Springer-Verlag Berlin, Heidelberg, 2012.

[53] Johnson, C. W. Analysing the Causes of the Italian and Swiss Blackout, 28th September 2003. Proceedings of the twelfth Australian workshop on Safety critical systems and software and safety-related programmable systems (SCS '07), Adelaide, Australia. August 30-31, 2007. Volume 86, Pages 21-30. Australian Computer Society.

[54] Joshi, J. B. D. TRBAC: A Generalized Temporal Role Based Access Control Model for Developing Secure Systems. Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette. August 2003.

[55] Joshi, J. B. D., Bertino, E., Latif, U., Ghafoor, A. TRBAC: A Generalized Temporal Role-Based Access Control Model. IEEE Transactions on Knowledge and Data Engineering. January 2005. Vol. 17, No. 1.

[56] Jøsang, A., Pope, S. User Centric Identity Management. AusCERT Asia Pacific Information Technology Security Conference. 2005. pp. 1-13.

[57] Katić, N. Elektroprivreda u uslovima slobodnog tržišta. Fakultet tehničkih nauka, Novi Sad. 2012.

[58] Kirkham, H., Clements, S. L., Tews, C., Mahan, R.E., Fluckiger, J. D., Burnette, J. R., Goranson, C. A. Secure Data Transfer Guidance for Industrial Control and SCADA Systems. 2011.

[59] Kirkpatrick, M. S., Bertino, E. Enforcing Spatial Constraints for Mobile RBAC Systems. 15th ACM Symposium on Access control models and technologies (SACMAT'10). 2010. pp. 99-108.

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

[61] Knapp, E. D., Samani, R. Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure. Elsevier. 2013.

[62] Kopsakangas-Savolainen, M., Svento, R. Modern Energy Markets. Springer. 2012.

[63] Kuhn, D. R., Coyne, E. J., Weil, T. R. Adding Attributes to Role-Based Access Control. IEEE Computer. June 2010. Vol. 43, No. 6, pp. 79-81.

[64] Kumar, M., Newman, R. E. STRBAC – An approach towards spatio-temporal role-based access control. Communication, Network, and Information Security. 2006. pp. 150-155.

[65] Kushner, D. The Real Story of Stuxnet. IEEE Spectrum. March 2013. pp. 48-53.

[66] Kuzlu, M., Pipattanasomporn, M., Rahman, S. Communication network requirements for major smart grid applications in HAN, NAN and WAN. Computer Networks. July 2014. Vol. 67, pp. 74-88.

[67] Lamb, P., Power, R., Walker, G., Compton, M. Role-based access control for data service integration. Proceedings of the 3rd ACM workshop on Secure web services (SWS '06), pp. 3–12. New York, NY, USA, 2006.

[68] Li, X., Liang, X., Lu, R., Shen, X., Lin, X., Zhu, H. Securing smart grid: cyber attacks, countermeasures, and challenges. IEEE Communications Magazine. August 2012. Vol. 50, Issue 8, pp. 38-45.

[69] Ma, M., Woodhead, S. Constraint-enabled distributed rbac for subscription-based remote network services. Proceedings of the 6th IEEE International Conference on Computer and Information Technology (CIT '06), p. 160, Washington, DC, USA, 2006. IEEE Computer Society.

[70] Michahelles, F., Thiesse, F., Schmidt, A., Williams, J. R. Pervasive RFID and Near Field Communication Technlogy. IEEE Pervasive Computing. 2007. Vol. 6, No. 3, pp. 94-96.
[71] Microsoft .NET Framework, IIdentity Interface, https://msdn.microsoft.com/en-us/library/system.security.principal.iidentity(v=vs.110).aspx
[72] Microsoft .NET Framework, IPrincipal Interface, https://msdn.microsoft.com/en-us/library/system.security.principal.iprincipal(v=vs.110).aspx
[73] Minkel, J.R. The 2003 Northeast Blackout - Five Years Later. Scientific American. August 2008. https://www.scientificamerican.com/article/2003-blackout-five-years-later/ (pristup: oktobar 2016.).
[74] Mithani, A., Popovic, D., Huang, M. Advanced Distribution Management Systemin BC Hydro's Distribution Network. 21st International Conference on Electricity Distribution, Frankfurt. June 2011.
[75] Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., Sinopoli, B. Cyber-Physical Security of a Smart Grid Infrastructure. Proceedings in the IEEE. January 2012. Vol. 100, Issue 1, pp. 195-209.
[76] Mostefaoui, G. K., Brezillon, P. A generic framework for context-based distributed authorizations. 4th International and Interdisciplinary Conference on Modeling and Using Context (Context'03), pp. 204–217, Berlin, DE, 2003. SpringerLink.
[77] National Cybersecurity and Communications Integration Center (NCCIC). Seven Strategies to Defend ICSs. December 2015.
[78] National Grid (Great Britain). Distribution Network Operator (DNO) Companies. http://www2.nationalgrid.com/UK/Our-company/Electricity/Distribution-Network-Operator-Companies/ (pristup: septembar 2016.).
[79] National Grid (Great Britain). What we do in the Electricity Industry. http://www2.nationalgrid.com/uk/our-company/electricity/ (pristup: septembar 2016.).
[80] National Institute of Standards and Technology Interagency Report 7316. Assessment of Access Control Systems. http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf
[81] National Institute of Standards and Technology Interagency Report 7628, Rev. 1. http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf
[82] National Institute of Standards and Technology Special Publication 1108: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf
[83] National Institute of Standards and Technology Special Publication 800-162. http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf
[84] National Institute of Standards and Technology Special Publication 800-53, Rev. 4. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[85] National Institute of Standards and Technology Special Publication 800-82, Rev. 2. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
[86] National Security Agency. National Information Systems Security (INFOSEC) Glossary (NSTISSI No. 4009). September 2000.
[87] North American Electric Reliability Corporation (NERC) Critical Infrastructure protection (CIP). http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[88] Office of Gas and Electricity Markets (Ofgem). The GB electricity distribution network. https://www.ofgem.gov.uk/electricity/distribution-networks/gb-electricity-distribution-network (pristup: septembar 2016.).
[89] Office of Gas and Electricity Markets (Ofgem). The GB electricity transmission network. https://www.ofgem.gov.uk/electricity/transmission-networks/gb-electricity-transmission-network (pristup: septembar 2016.).
[90] Open Geospatial Consortium (OGC). http://www.opengeospatial.org/standards
[91] Open Web Application Security Project(OWASP). Architectural Principles That Prevent Code Modification or Reverse Engineering. https://www.owasp.org/index.php/Architectural_Principles_That_Prevent_Code_Modification_or_Reverse_Engineering (pristup avgust 2016.).
[92] Open Web Application Security Project (OWASP). Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology (pristup: avgust 2016.).
[93] Organization for the Advancement of Structured Information Standards (OASIS). Extensible Access Control Markup Language (XACML), V3.0. January 2013.
[94] Park, J., Sandhu, R. The UCONABC Usage Control Model. ACM Transactions on Information and System Security. February 2004. Vol. 7, No. 1, pp. 128–174.
[95] Piromruen, S., Joshi, J. B. D. An RBAC framework for time constrained secure interoperation in multi-domain environments. Proceedings of the 10th IEEE International Workshop on Object-Oriented Real-Time Dependable Systems (WORDS '05), pp. 36–48, Washington, DC, USA, 2005. IEEE Computer Society.
[96] Popovic, D. Power Application-A Cherry on the Top of the DMS Cake. DA/DSM DistribuTECH Europe 2000. Vienna. Track 3, Session 3, Paper 2.
[97] Popovic, D. S., Strezoski, V. C., Katic, N. A. Power Applications – a Powerful Tool for Distribution Networks Management. 16th International Conference on Electricity Distribution CIRED, Amsterdam. 2001. 240-246.
[98] Ranathunga, D., Roughan, M., Kernick, P., Falkner, N., Nguyen, H. Identifying the Missing Aspects of the ANSI/ISA Best Practices for Security Policy. Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, New York, NY, USA. 2015. pp. 37-48.
[99] Ray, I., Toahchoodee, M. A Spatio-Temporal Role-Based Access Control Model. Data and Application Security XXI. 2007. Vol. 4602, pp. 211-226.
[100] Ray, I., Toahchoodee, M. A Spatio-Temporal Role-Based Access Control Model Supporting Delegation for Pervasive Computing Applications. 5th International Conference on Trust, Privacy and Security in Digital Business. 2008. pp. 48-58.
[101] Robles, R. J., Choi, M. K., Yeo, S. S., Kim, T. H. Application of role-based access control for web environment. Proceedings of the 2008 International Symposium on Ubiquitous Multimedia Computing (UMC ’08). pp. 171–174. Washington, DC, USA, 2008. IEEE Computer Society.
[102] Roncero, J. R. Integration is key to Smart Grid management. CIRED Seminar 2008: SmartGrids for Distribution, Frankfurt. June 2008. pp. 1-4.
[103] Rosic, D., Lendak, I., Vukmirovic, S. Role-based Access Control Model Supporting Regional Division in Smart Grid System. Acta Polytechnica Hungarica. Vol 12, No 7. 2015.

[104] Rosic, D., Novak, U., Vukmirovic, S. Role-based Access Control Model Supporting Regional Division in Smart Grid System. 5th International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN). Madrid. June 2013.
[105] Sandhu, R. S. Lattice-Based Access Control Models. IEEE Computer Society. November 1993. Vol. 26, No. 11, pp. 9-19.
[106] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., Youman, C. E. Role-Based Access Control Models. IEEE Computers. February 1996. Vol. 29, No. 2, pp. 38-47.
[107] Sandhu, R., Ferraiolo, D., Kuhn, R. The NIST Model for Role-Based Access Control: Towards a Unified Standard.
[108] Sandhu, R. S., Samarati, P. Access Control: Principles and Practice. IEEE Communications Magazine. September 1994. pp. 40-48.
[109] SANS Institute. Analysis of the Cyber Attack on the Ukrainian Power Grid. Report. March 2016.
[110] SANS Institute. Defense In Depth. 2001.
[111] SANS Institute. Implementing Least Privilege at your Enterprise. 2003.
[112] SANS Institute. Information Security - Managing Risk with Defense in Depth. August 2003.
[113] Shahraeini, M., Alishahi, S. A survey on information and communication technology (ICT) applications in distribution systems. 21st International Conference on Electricity Distribution, Frankfurt. June 2011.
[114] Sinkovski, S., Lučić, B. Informaciona bezbednost. Ziteh '06.
[115] Sladić, G., Milosavljević, B., Konjović, Z. Context-sensitive Access Control Model for Business Processes. Computer Science and Information Systems. 2013. Vol. 10, No. 3.
[116] Sladić, G., Milosavljević, B., Milosavljević, G. Kontrola pristupa dokumentima bazirana na XACML standardu. YU INFO 2010. Kopaonik. Januar 2010.
[117] Strembeck, M., Neumann, G. An Integrated Approach to Engineer and Enforce Context Constraints in RBAC Environments. ACM Transactions on Information and System Security. August 2004. Vol. 7, No. 3, pp 392–427.
[118] Strezoski, V. Osnovi elektroenergetike. Fakultet tehnickih nauka, Novi Sad. 2014.
[119] Swiss Federal Office of Energy (SFOE). Report on the blackout in Italy on 28 September 2003. November 2003.
[120] Škero, M., Ateljević, V. Zaštita kritične infrastrukture i osnovni elementi usklađivanja sa Direktivnom Saveta Evrope 2008/114/ES. Vojno delo. 2015. Vol. 67, Br. 3, str. 192-207.
[121] Taylor, T., Kazemzadeh, H. Integrated SCADA/DMS/OMS: Increasing Distribution Operations Efficiency. Electric Energy T&D Magazine. Mart-April 2009.
[122] Toahchoodee, M., Ray, I., Anastasakis, K., Georg, G., Bordbar, B. Ensuring spatio-temporal access control for real-world applications. 14th ACM symposium on Access control models and technologies (SACMAT '09), New York, NY, USA. 2009. pp. 13–22.
[123] Understanding layered security and defense in depth. http://www.techrepublic.com/blog/it-security/understanding-layered-security-and-defense-in-depth/ (pristup: avgust 2016.).

[124] U.S.-Canada Power System Outage Task Force. Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. April 2004.

[125] Wang, W., Lu, Z. Survey Cyber security in the Smart Grid: Survey and challenges. The International Journal of Computer and Telecommunications Networking. April 2013. Vol. 57, Issue 5, pp. 1344-1371.

[126] Whitman, M. E., Mattord, H. J. Principles of Information Security. Course Technology. 2011.

[127] Wonohoesodo, R., Tari, Z. A role based access control for web services. Proceedings of the 2004 IEEE International Conference on Services Computing (SCC '04). pp. 49-56. Washington, DC, USA. 2004. IEEE Computer Society.

[128] Yan, Y., Qian, Y., Sharif, H., Tipper, D. A Survey on Cyber Security for Smart Grid Communications. IEEE Communications Surveys & Tutorials. 2012. Vol. 14, Issue 4, pp. 998-1010.

[129] Zetter, K. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Broadway Books. September 2015.

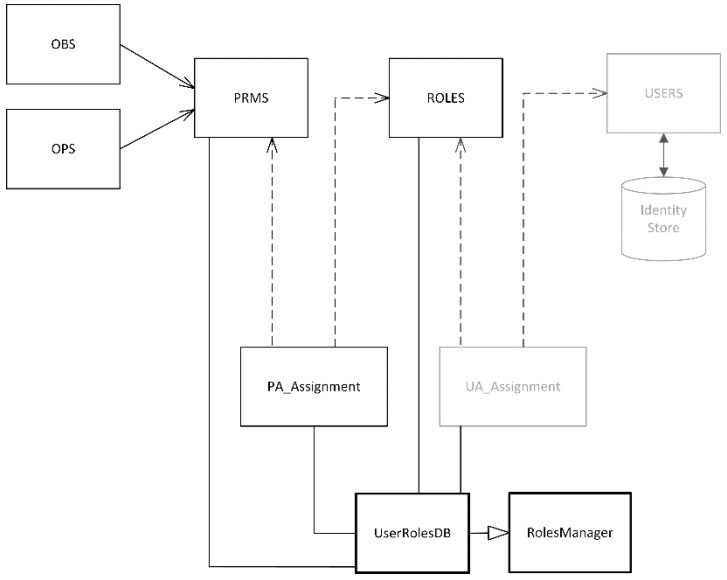
[130] Zetter, K. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Wired. March 3rd, 2016.

Prilozi

Prilog A. Opis modula softverske arhitekture

A.1 Modul za upravljanje korisničkim ulogama

UML dijagram klasa modula za upravljanje korisničkim ulogama je prikazan na *Slici 43.* `UserRolesDB` sadrži podatke o korisničkim ulogama (`ROLES`), privilegijama (`PRMS`), kao i odgovarajuće relacije (`PA_Assignment`). Podaci o korisnicima (`USERS`) i njihovim relacijama sa korisničkim ulogama (`UA_Assignment`) se ne skladište u okviru ove baze podataka, već je ona integrisana sa `IdentityStore` komponentom podsistema za autentifikaciju gde se skladište podaci o identitetu korisnika. `RolesManager` je komponenta kojom je realizovan pristup skladištu podataka `UserRoleDB` za potrebe administracije i čitanja.



Slika 43. UML dijagram klasa modula za upravljanje korisničkim ulogama

`RolesManager` implementira interfejs `IRolesManager` čije metode su date u *Listingu 1.*, a kratak opis metoda koje implementira `RolesManager` komponenta je dat u nastavku. Istaknute su metode koje su potrebne za razumevanje ostalih modula softverske arhitekture sistema za kontrolu pristupa u *Sekciji 6*.

Metoda `EnabledRoles` vraća skup omogućenih uloga za korisnika čiji je jedinstveni identifikator `userID`, odnosno vraća skup uloga dodeljenih korisniku posredstvom UA relacije.

Metoda `DisabledRoles` vraća skup onemogućenih uloga za korisnika čiji je jedinstveni identifikator `userID`, odnosno skup uloga koje datom korisniku nisu dodeljene posredstvom UA relacije.

Metodom `IsEnabled` se proverava da li je određena uloga omogućena korisniku, odnosno da li se data uloga nalazi u skupu omogućenih uloga datog korisnika.

Metoda `EnabledPrms` vraća skup privilegija dodeljenih korisničkoj ulozi posredstvom PA relacije.

```
[ServiceContract]
public interface IRolesManager
{
    [OperationContract]
    public List<Roles> EnabledRoles(SecurityIdentifier userID);

    [OperationContract]
    public List<Roles> DisabledRoles(SecurityIdentifier userID);

    [OperationContract]
    public bool IsEnabled(SecurityIdentifier userID, SecurityIdentifier
roleID);

    [OperationContract]
    public List<Prms> EnabledPrms(SecurityIdentifier roleID);
}
```

Listing 1. Interfejs modula za upravljanje korisničkim ulogama

A.2 Modul za upravljanje oblastima odgovornosti

UML dijagram klasa modula za upravljanje oblastima odgovornosti je prikazan na *Slici 44.* `UserAorsDB` sadrži podatke o oblastima odgovornosti (`AORS`), nivoima odgovornosti (`RESPS`), regionima (`REGIONS`), kao i relacije AOR-a i regiona (`RAOR_Assignment`), odnosno korisnika (`UAOR_Assignment`). Podaci o korisnicima se ne skladište u okviru `UserAorsDB`, već je ona integrisana sa `IdentityStore` komponentom podsistema za autentifikaciju gde se skladište podaci o identitetu korisnika.

`AorsManager` implementira interfejs `IAorsManager` čije metode su date u *Listingu 2.*, a kratak opis metoda koje implementira `AorsManager` komponenta je dat u nastavku. Istaknute su metode koje su potrebne za razumevanje ostalih modula softverske arhitekture sistema za kontrolu pristupa u *Sekciji 6.*

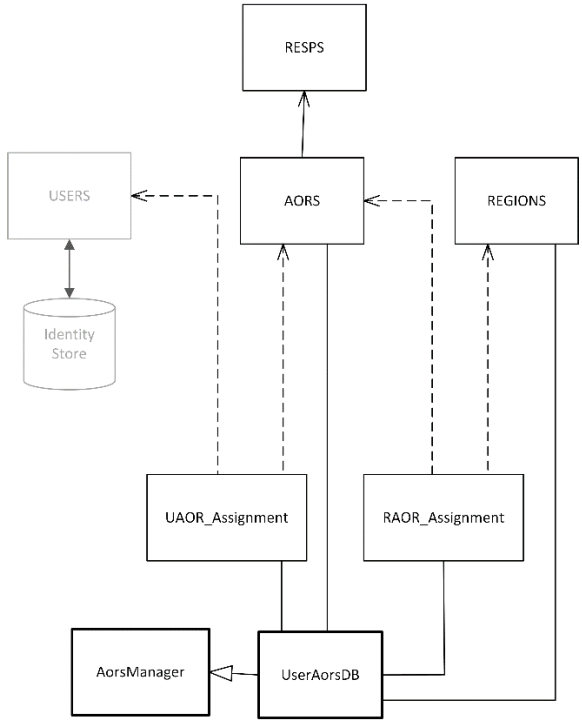
Metoda `EnabledAORs` vraća skup omogućenih oblasti odgovornosti za korisnika čiji je jedinstveni identifikator `userID`, odnosno vraća skup AOR-a dodeljenih korisniku posredstvom U-AOR relacije. Za svaki omogućeni AOR je pomoću metode `EnabledResps` moguće dobiti nivoe odgovornosti definisane za dati AOR.

Metoda `DisabledAORs` vraća skup onemogućenih oblasti odgovornosti za korisnika čiji je jedinstveni identifikator `userID`, odnosno skup AOR-a koji nisu dodeljeni korisniku posredstvom U-AOR relacije.

Metoda `IsEnabled` proverava da li je određena oblast odgovornosti omogućena korisniku sa zadatim nivoom odgovornosti.

Metoda `GetAors` vraća skup oblasti odgovornosti za određeni region, odnosno vraća skup AOR-a dodeljenih regionu posredstvom R-AOR relacije.

Metoda `GetOperationType` vraća jedinstveni identifikator koji označava nivo odgovornosti kojim je opisan tip date operacije. Ukoliko za neku operaciju nije definisan tip, odnosno nivo odgovornosti, ova metoda vraća vrednost `-1`.



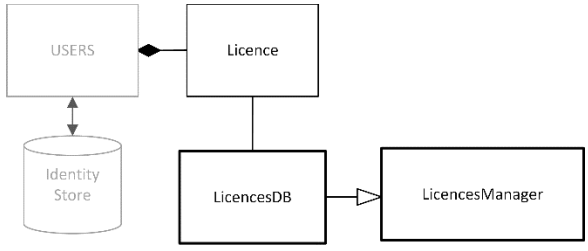
Slika 44. UML dijagram klasa modula za upravljanje oblastima odgovornosti

```
[ServiceContract]
public interface IAorsManager
{
    [OperationContract]
    public List<Aors> EnabledAors(SecurityIdentifier userID);

    [OperationContract]
    public List<Resps> EnabledResps(SecurityIdentifier aorID);

    [OperationContract]
    public List<Aors> DisabledAors(SecurityIdentifier userID);

    [OperationContract]
    public bool IsEnabled(SecurityIdentifier userID, SecurityIdentifier
aorID, int respsID);

    [OperationContract]
    public List<Aors> GetAors(string regionID);

    [OperationContract]
    public int GetOperationType(int operationID);
}
```

Listing 2. Interfejs modula za upravljanje oblastima odgovornosti

A.3 Modul za upravljanje licencama

UML dijagram klasa modula za upravljanje licencama je prikazan na *Slici 45.* `LicencesDB` sadrži podatke o svim licencama u sistemu, a `LicencesManager` implementira interfejs `ILicencesManager` čije metode su date u *Listingu 3.* Sledi kratak opis metoda koje implementira `LicencesManager`, a koje su potrebne za razumevanje ostalih modula softverske arhitekture sistema za kontrolu pristupa u *Sekciji 6*.



Slika 45. UML dijagram klasa modula za upravljanje licencama

Za svaku licencu je na osnovu jedinstvenog identifikatora moguće dobiti informacije o tome kada je licenca izdata (metoda `ValidFrom`) i do kada licenca važi (metoda `ValidTo`). Metoda `GetRestrictedRole` vraća identifikator korisničke uloge na koju se licenca odnosi.

Metodom CheckValidity se proverava da li je licenca važeća u trenutku provere, odnosno računa se vrednost isValid=DateTime.Now<ValidTo. Ukoliko je vrednost isValid tačna, odnosno vrednost ValidTo veća od trenutnog vremena znači da je licenca u trenutku provere validna.

```
public interface ILicencesManager
{
    [OperationContract]
    public SecurityIdentifier GetRestrictedRole(string licenceID);

    [OperationContract]
    public DateTime ValidFrom(string licenceID);

    [OperationContract]
    public DateTime ValidTo(string licenceID);

    [OperationContract]
    public bool CheckValidity(string licenceID);
}
```

Listing 3. Interfejs modula za upravljanje licencama

A.4 Modul za upravljanje radnim stanicama

UML dijagram klasa modula za upravljanje radnim stanicama je prikazan na *Slici 46.* ConsolesDB sadrži podatke o svim radnim stanicama (CONSOLES) u sistemu, uključujući i poseban entitet kojim su modelovane udaljene radne stanice. Za svaku radnu stanicu se definiše tip radne stanicem, kao i skup omogućenih uloga (CROLE_Assignment) i oblasti odgovornosti (CAOR_Assignment) sa date radne stanice.

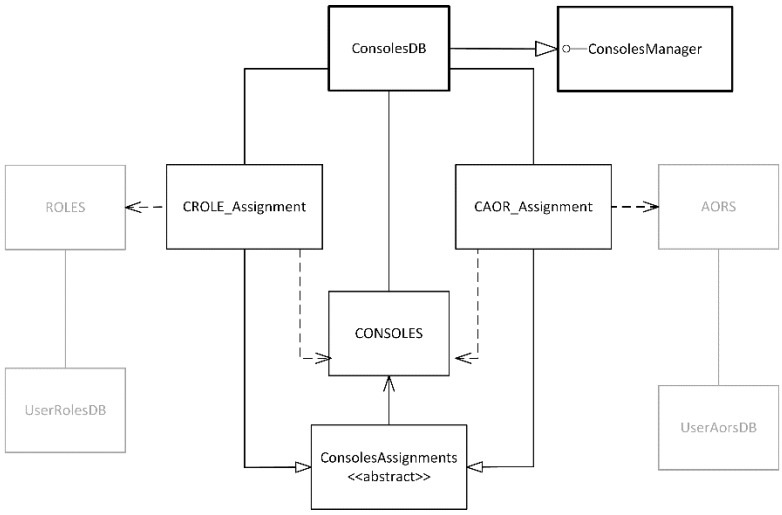
ConsolesManager implementira interfejs IConsolesManager čije metode su date u *Listingu 4.* Kratak opis metoda koje implementira ConsolesManager komponenta potrebnih za razumevanje ostalih modula softverske arhitekture sistema za kontrolu pristupa u *Sekciji 6.* je dat u nastavku.

Metoda GetConsoleType vraća tip radne stanice opisan enumeracijom Environment.

Metoda EnabledComputerRoles vraća skup omogućenih korisničkih uloga sa radne stanice čiji jedinstveni identifikator je consoleID, odnosno skup uloga dodeljenih radnoj stanici posredstvom C-ROLE relacije. Metoda DisabledComputerRoles vraća skup onemogućenih uloga sa radne stanice čiji jedinstveni identifikator je consoleID, odnosno skup uloga koje nisu dodeljene radnoj stanici posredstvom C-ROLE relacije.

Metoda EnabledComputerAors vraća skup omogućenih oblasti odgovornosti sa radne stanice čiji jedinstveni identifikator je consoleID, odnosno skup AOR-a dodeljenih radnoj stanici posredstvom C-AOR relacije. Funkcija DisabledComputerAors vraća skup onemogućenih oblasti odgovornosti sa radne stanice stanice čiji jedinstveni identifikator

je consoleID, odnosno skup AOR-a koji nisu dodeljeni radnoj stanici posredstvom C-AOR relacije.



Slika 46. UML dijagram klasa modula za upravljanje radnim stanicama

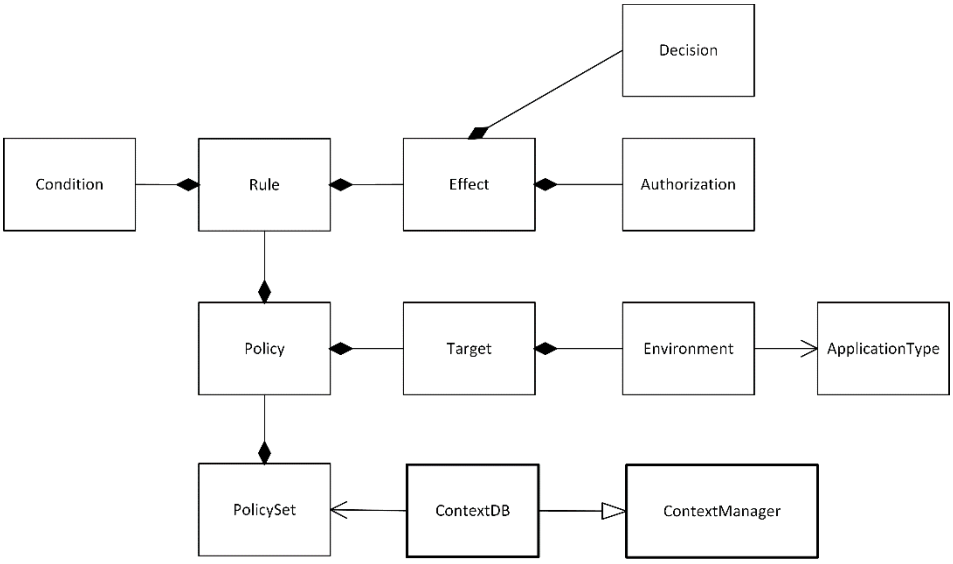
```
public enum Environment { ControlRoom = 0, Engineering = 1, Enterprise
= 2, Remote = 3 }

public interface IConsolesManager
{
    [OperationContract]
    public Environment GetConsoleType(SecurityIdentifier consoleID);

    [OperationContract]
    public List<Roles> EnabledComputerRoles(SecurityIdentifier
consoleID);

    [OperationContract]
    public List<Roles> DisabledComputerRoles(SecurityIdentifier
consoleID);

    [OperationContract]
    public List<Aors> EnabledComputerAors(SecurityIdentifier
consoleID);

    [OperationContract]
    public List<Aors> DisabledComputerAors(SecurityIdentifier
consoleID);
}
```

Listing 4. Interfejs modula za upravljanje radnim stanicama

A.5 Modul za upravljanje aplikativnim kontekstom

UML dijagram klasa modula za upravljanje aplikativnim kontekstom je prikazan na *Slici 47.* Skup XACML bezbednosnih politika kojima je modelovan aplikativni kontekst se

skladišti u `ContextDB` XML datoteci. `ContextManager` implementira interfejs `IContextManager` čije metode su date u *Listingu 5.* Kratak opis metoda koje implementira `ContextManager` komponenta potrebnih za razumevanje ostalih modula softverske arhitekture sistema za kontrolu pristupa u *Sekciji 6.* je dat u nastavku.



Slika 47. UML dijagram klasa modula za upravljanje aplikativnim kontekstom

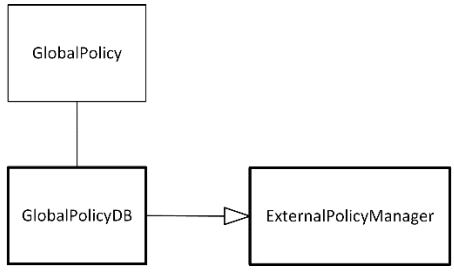
Ulazni parametri metode `GetRules` su tip aplikativnog konteksta `ApplicationType` koji definiše ciljanu bezbednosnu politiku (`target`) i skup omogućenih uloga datog korisnika kojim su definisani uslovi (`conditions`) koji moraju biti zadovoljeni da bi određeno pravilo bilo primenjeno. Rezultat metode je lista `AuthzDecision` elemenata kojim se specificira odluka o tome da li je neko ovlašćenje dozvoljeno ili zabranjeno (`effect`). `AuthzDecision` je struktura koju čine jedinstveni identifikator ovlaščenja (uloge, privilegije ili AOR-a) i odluka o tome da li ovlašćenje treba da bude omogućeno. Odluka je opisana enumeracijom `Decision`. Dodatno, po potrebi je u okviru `GetRules` metode moguće implementirati logiku o redosledu primene elemenata rezultujuće liste. U ovom radu se elementi smeštaju u listu u redosledu kojim su definisani XACML pravilima.

```
public enum ApplicationType { RealTime = 0, Simulation = 1, Planning =
2, QA = 3, FieldOps = 4, Business = 5 }

public enum Decision { Deny = 0, Allow = 1 }

public struct AuthzDecision
{
    public string name;
    public Decision decision;
}

public interface IContextManager
{
    [OperationContract]
    public List<AuthzDecision> GetRules(ApplicationType target, List<
string> conditions);
}
```

Listing 5. Interfejs modula za upravljanje aplikativnim kontekstom

A.6 Modul za upravljanje globalnim politikama

UML dijagram klasa modula za upravljanje globalnim politikama je prikazan na *Slici 48.* `GlobalPolicyDB` sadrži pravila transformacije uloga i atributa iz eksternih sistema na korisničke uloge i atribute u izvornom sistemu. Pravila transformacije za svaki eksterni sistem su opisana klasom `GlobalPolicy`, a `ExternalPolicyManager` implementira interfejs `IExternalPolicyManager` za dobavljanje rezultata transformacije. Metode `IExternalPolicyManager` interfejsa su date u *Listingu 6.* a kratak opis metoda potrebnih za razumevanje ostalih modula softverske arhitekture sistema za kontrolu pristupa u *Sekciji 6.* je dat u nastavku.



Slika 48. UML dijagram klasa modula za upravljanje globalnim politikama

Metoda `GetInternalRoles` vraća skup korisničkih uloga iz izvornog sistema na koje se mapira odgovarajuća uloga `ExternalRole` iz eksterne organizacije čiji je jedinstveni identifikator `orgID`.

Metoda `GetInternalAttribute` vraća korisnički atribut iz izvornog sistema na koji se mapira određeni atribut `ExternalAttribute` iz eksterne organizacije čiji je jedinstveni identifikator `orgID`.

```
public class GlobalPolicy
{
    string orgID;
    Dictionary<ExternalRole, List<SecurityIdentifier>> RoleMapper;
    Dictionary<ExternalAttribute, UserAttribute> AttributeMapper;

    public List<roleID> GetRoles(ExternalRole er)
    { return globalPolicy.RoleMapper(er); }

    public UserAttribute GetAttribute(ExternalAttribute ea)
    { return globalPolicy.AttributeMapper(ea); }
}

public interface IExternalPolicyManager
{
    public List<SecurityIdentifier> GetInternalRoles(string orgID,
ExternalRole eRole);
    public UserAttribute GetInternalAttribute(string orgID,
ExternalAttribute eAttribute);
}
```

Listing 6. Interfejs modula za upravljanje globalnim politikama

A.7 Modul za upravljanje statičkim kontekstom sesije

RBAC-AOR$_{SG}$ Identitet

`IRBACAORIdentity` je interfejs koji enkapsulira podatke o različitim tipovima identiteta u zavisnosti od tipa autentifikacije. `IIdentity` [71] interfejs je bazni interfejs koji objedinjuje različite tipove identiteta, a `IRBACAORIdentity` dat na *Listingu 7.* proširuje `IIdentity` podacima o organizaciji korisnika, njegovim licencama i ulogama.

```
public interface IRBACAORIdentity : IIdentity, IDisposable
{
        public string Name; // IIdentity
        public string AuthenticationType; // IIdentity
        public bool IsAuthenticated; // IIdentity

        public SecurityIdentifier UserID;
        public string OrgID;
        public List<string> LicenceIDs;
        public List<SecurityIdentifier> UserRoles;
}
```

Listing 7. Interfejs RBAC-AOR$_{SG}$ identiteta

RBAC-AOR$_{SG}$ Principal

`IRBACAORPrincipal` je interfejs koji enkapsulira podatke o statičkom kontekstu sesije, odnosno o omogućenim i aktiviranim ovlašćenjima korisnika u datoj korisničkoj sesiji. `IPrincipal` [72] je bazni interfejs, a `IRBACAORPrincipal` prikazan na *Listingu 8.* proširuje bazni principal specifičnim RBAC-AOR$_{SG}$ podacima o korisničkoj sesiji, pre svega radna stanica (`SelectedConsole`) i tip aplikacije (`SelectedApplication`) sa koje je sesija uspostavljena, kao i skup omogućenih i aktiviranih ovlašćenja prilikom uspostavljanja sesije. `EnabledRoles` vraća skup omogućenih korisničkih uloga, `EnabledPrms` skup omogućenih privilegija, a `EnabledAors` skup omogućenih AOR-a nakon primene RBAC-AOR$_{SG}$ modela ograničenja i proširenja prilikom uspostavljanja korisničke sesije. Metoda `IsInRole` proverava da li je ovlašćenje omogućeno u datoj korisničkoj sesiji. Potrebno je napomenuti da se na ovaj način ne uvažavaju bilo kakve izmene skupa ovlašćenja nakon uspostavljanja korisničke sesije, odnosno `IRBACAORPrincipal` pruža informacije samo o statičkom kontekstu uspostavljene sesije.

```
public interface IRBACAORPrincipal : IPrincipal, IDisposable
{
        public IIdentity Identity;     // IPrincipal
        public bool IsInRole(string role); // IPrincipal

        public Guid SessionID;
        public SecurityIdentifier SelectedConsole;
        public ApplicationType SelectedApplication;

        public List<Roles> EnabledRoles;
        public List<Aors> EnabledAors;
        public List<Prms> EnabledPrms;
}
```

Listing 8. Interfejs RBAC-AOR$_{SG}$ principala

SCS komponenta za upravljanje identitetima

SCS identity Management Service implementira `IIdentityManagement` interfejs za formiranje RBAC-AOR$_{SG}$ identiteta (`IRBACAORIdentity`) dat na *Listingu 9.* Metoda `CreateIdentity` kreira identitet korisnika tako da na unificiran način objedinjuje atribute korisnika bez obzira na tip autentifikacije. U zavisnosti od organizacije kojoj korisnik pripada (`orgID`), `IdentityManager` formira identitet ili zahtev prosleđuje `PolicyMapper` komponenti koja je zadužena za transformaciju korisničkih uloga i

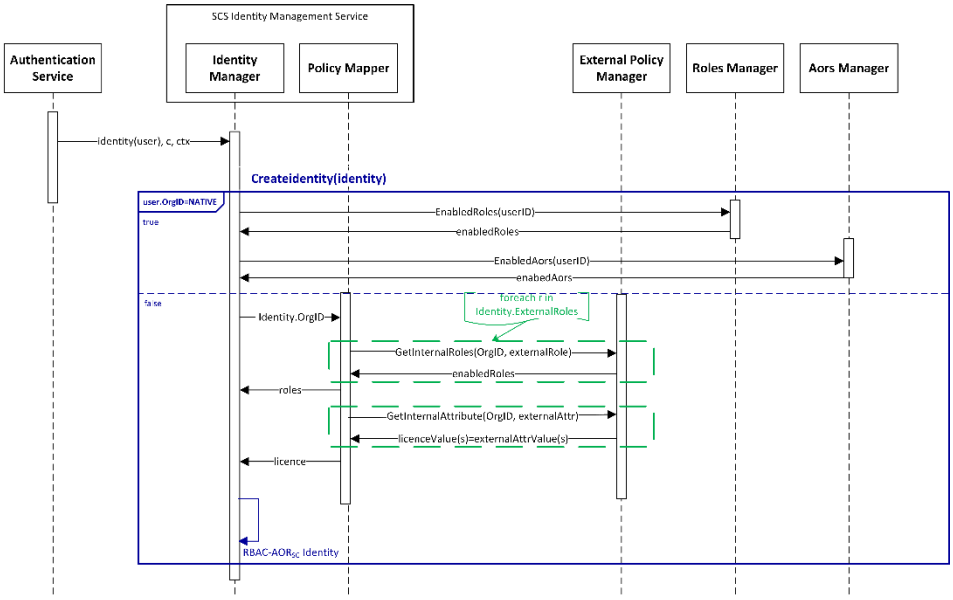
atributa u slučaju eksternih korisnika. Postupak kreiranja `IRBACAORIdentity` je istaknut na *Slici 49.*

```
public interface IIdentityManagement
{
        public IRBACAORIdentity CreateIdentity(IIdentity identity);
}
```

Listing 9. Interfejs SCS komponente za upravljanje identitetima

Ukoliko korisnik pripada izvornoj organizaciji (`OrgID=NATIVE`) `IdentityManager` poziva metode `RolesManager` i `AorsManager` modula radi dobavljanja skupa omogućenih uloga i AOR-a za korisnika koji uspostavlja sesiju (`userID` je jedinstveni identifikator korisnika).

U suprotnom, jedinstveni identifikator organizacije kojoj korisnik pripada (`orgID`) se prosleđuje `ExternalPolicyManager` komponenti koja vrši transformaciju korisničkih uloga i atributa eksternog korisnika, nakon čega `IdentityManager` može da formira RBAc-AOR$_{SG}$ identitet za eksternog korisnika.



Slika 49. UML dijagram sekvence Postupka kreiranja RBAC-AOR$_{SG}$ Identiteta

SCS komponenta za upravljanje principalima

SCS Principal Management Service implementira `IPrincipalManagement` interfejs za formiranje RBAC-AOR$_{SG}$ principala (`IRBACAORPrincipal`) dat na *Listingu 10.* Metoda `CreatePrincipal` se sastoji od poziva četiri metode za primenu RBAC-AOR$_{SG}$ modela ograničenja i proširenja, označene zelenim na dijagramu na *Slici 50.* Iako pozivi ovih metoda moraju biti sekvencijalni, dobavljanje podataka iz odgovarajućih modula za upravljanje bezbednosim podacima se može paralelizovati i time ubrzati postupak kreiranja principala. Dodatno, razdvajanjem metoda za primenu ograničenja moguće je jednostavno izuzeti iz razmatranja određena ograničenja i proširenja RBAC-AOR$_{SG}$ modela ukoliko takav zahtev postoji.

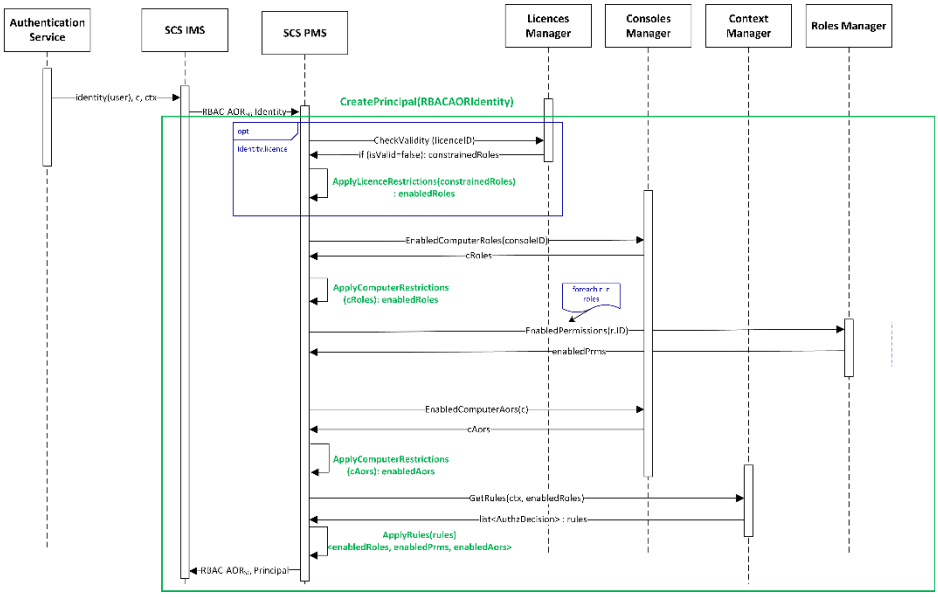
```
public interface IPrincipalManagement
{
    public IRBACAORPrincipal CreatePrincipal(IRBACAORIdentity identity,
SecurityIdentifier consoleID, ApplicatonType appType);

    void ApplyLicenceRestrictions(IRBACAORPrincipal principal,
SecurityIdentifier constrainedRole);

    void ApplyComputerRestrictions(IRBACAORPrincipal principal,
List<SecurityIdentifier> enabled);

    void ApplyRules(IRBACAORPrincipal principal, AuthzDecision rules);
}
```

Listing 10. Interfejs SCS komponente za upravljanje principalima

Metoda `ApplyLicenceRestrictions` ograničava skup omogućenih uloga principala (`EnabledRoles`) isključivanjem uloge `constrainedRole` koja je definisana licencom. Takođe, istovremeno se ažurira i skup omogućenih privilegija datog principala (`EnabledPrms`) u skladu sa izmenjenim skupom uloga.

Metoda `ApplyComputerRestrictions` ograničava skup omogućenih uloga (`EnabledRoles`), odnosno oblasti odgovornosti (`EnabledAors`) principala u skladu sa modelom radne stanice `consoleID`. Skup omogućenih uloga je presek skupa omogućenih uloga principala (`EnabledRoles`) i radne stanice (`enabled`). Isti algoritam važi i za skup omogućenih AOR-a. Skup omogućenih AOR-a je presek skupa omogućenih AOR-a principala (`EnabledAors`) i radne stanice (`enabled`). Takođe, istovremeno se ažurira i skup omogućenih privilegija datog principala (`EnabledPrms`) u skladu sa izmenjenim skupom uloga.

Metoda `ApplyRules` primenjuje skup autorizacionih odluka (`rules`) definisanih autorizacionom politikom odgovarajućeg aplikativnog konteksta. `AuthzDecision` je struktura koja sadrži jedinstveni identifikator ovlašćenja kao i odluku o tome da li ovlašćenje treba da bude dozvoljeno (`Allow`) ili zabranjeno (`Deny`). Dodatno, ukoliko se ovlašćenjem menja skup omogućenih uloga principala (`EnabledRoles`) istovremeno se ažurira i skup omogućenih privilegija (`EnabledPrms`) datog principala.



Slika 50. UMLdijagram sekvence postupka kreiranja RBAC-AOR$_{SG}$ principala

A.8 Modul za upravljanje korisničkim sesijama

Servis za upravljanje aktivnim korisničkim sesijama

Implementacija SessionManagementService (SMS) komponente je realizovana posredstvom dva interfejsa, `ISessionManagement` koji izlaže metode ka SCS i DCS komponentama za upravljanje korisničkim sesijama i `IAccessManagement` koji izlaže metode ka autorizacionom menadžeru koji proverava trenutno stanje aktivnih sesija prilikom donošenja odluke o pristupu.

Metode `ISessionManagement` interfejsa su navedene na *Listingu 11.* Metoda `AddSession` se dodaje podatke o novoj sesiji u `ActiveSessionsDB` memorijsku bazu podataka. Za svaku sesiju se osim jedinstvenog identifikatora sesije (`SessionID`) i korisnika (`UserID`) zapisuju informacije o aktiviranim ovlašćenjima. Metoda `ActivateAors` je interna metoda kojom je realizovano aktiviranje svi omogućenih AOR-a kojima je atribut `ActiveOnLogin` tačan.

Metoda `RemoveSession` briše podatke o sesiji iz `ActiveSessionsDB` baze prilikom prekida sesije.

Metoda `UpdateSessions` menja podatke o aktivnim korisničkim sesijama u toku njihovog izvršavanja. Metoda je namenjena DCS servisu koji pozivom ove metode šalje

zahteve o izmeni stanja AOR-a, kako regularnih tako i vanrednih. U okviru iste metode moguće je poslati istovremeno više zahteva u cilju efikasnije obrade zahteva u vanrednim situacijama.

Metoda `UserSessions` vraća skup aktivnih sesija određenog korisnika. Metoda `ActiveRoles` vraća skup aktiviranih uloga u određenoj korisničkoj sesiji, a `ActivePermissions` skup raspoloživih (tj. aktiviranih) privilegija u određenoj korisničkoj sesiji. Metoda `ActiveAORs(guid)` vraća skup aktiviranih oblasti odgovornosti u određenoj korisničkoj sesiji, a metoda `ActiveAORs(guid, int)` vraća skup aktiviranih oblasti odgovornosti `aor` sa odgovarajućim nivoom odgovornosti u datoj korisničkoj sesiji `s`.

```
public interface ISessionManagement
{
    public void AddSession(IRBACAORPrincipal principal);
    public void RemoveSession(Guid SessionID);
    public void UpdateSessions(List<AORRequest> requests);
    void ActivateAors(Guid SessionID);

    public List<Guid> UserSessions(SecurityIdentifier UserID);
    public List<Roles> ActiveRoles(Guid SessionID);
    public List<Prms> ActivePermissions(Guid SessionID);
    public List<Aors> ActiveAORs(Guid SessionID);
    public List<Aors> ActiveAORs(Guid SessionID, int RespsID);
}
```

Listing 11. Interfejs servisa za upravljanje aktivnim sesijama (1)

Metode `IAccessManagement` interfejsa su navedene na *Listingu 12.* Metodom `IsActiveInSession(SecurityIdentifier, guid)` je moguće proveriti da li je neko ovlašćenje aktivirano u određenoj sesiji.

Metodom `IsActiveInSession(SecurityIdentifier, guid, int)` moguće je proveriti da li je određeni AOR aktiviran u određenoj sesiji sa nivoom odgovornosti `RespsID`.

```
public interface IAccessManagement
{
    public bool IsActiveInSession(SecurityIdentifier SID, Guid
SessionID);
    public bool IsActiveInSession(SecurityIdentifier aorID, int
respsID, Guid SessionID);
}
```

Listing 12. Interfejs servisa za upravljanje aktivnim sesijama (2)

Servis za upravljanje dinamičkim kontekstom sesije

Dynamic Context Service (DCS) implementira dva interfejsa, `IUserContext` koji izlaže metode ka Smart Grid korisnicima i `IDynamicContext` koji izlaže metode ka SMS modulu. `IUserContext`, prikazan na *Listingu 13.*, izlaže jednu metodu `SendRequest` za prihvatanje zahteva za izmenu stanja AOR-a. `RequestValidation` je interna metoda koja je zadužena za validaciju pristiglih zahteva. Svi validni zahtevi se pozivom metode `UpdateSessions` SMS komponente šalju na izvršenje.

`IDynamicContext`, prikazan na *Listingu 13.*, izlaže metode pozivom kojih SMS šalje informacije o izmenjenim korisničkih sesija, kako bi DCS mogao da obavesti sve zainteresovane aktivne korisnike o napravljenim izmenama.

```
public interface IUserContext
{
    SendRequest(List<AORRequest> requests);
    bool RequestValidation(AORRequest request);
}


public interface IDynamicContext
{
    public void SessionAdded(SessionInfo);
    public void SessionRemoved(SessionInfo);
    public void SessionsUpdated(List<SessionInfo>);


    public delegate void SessionAdded(SessionInfo);
    public delegate void SessionRemoved(SessionInfo);
    public delegate void SessionsUpdated(List<SessionInfo>);

}
```

Listing 13. Interfejsi servisa za upravljanje dinamičkim kontekstom sesije

Za potrebe generisanja događaja da je dodata nova sesija, definisan je delegat `SessionAdded` kojim DCS šalje svim zainteresovanim stranama informacije o novododatoj sesiji (`SessionInfo`). Pomoću delegata `SessionRemoved` se sve zainteresovane strane obaveštavaju o tome da je određena sesija prekinuta. `SessionsUpdated` je delagat pomoću koga se sve zainteresovane strane obaveštavaju o izmenama u korisničkim sesijama nakon izvršavanja zahteva o izmeni stanja AOR-a.

A.9 Modul za donošenje autorizacionih odluka

Authorization Manager implementira `IAuthorizationCheck` interfejs koji izlaže metodu za proveru pristupa kao što je prikazano na *Listingu 14.*

`AuthorizationManager` poziva metode SMS komponente za proveru da li su odgovarajuća privilegija i AOR aktivirani u korisničkoj sesiji `SessionID`. Pozivom metode `IsActiveInSession` SMS modula se proverava da li je privilegija `prmsID` aktivirana u

sesiji SessionID. Pozivom druge metode IsActiveInSession SMS modula se proverava da li je u u sesiji SessionID AOR aorID aktiviran sa nivoom odgovornosti koji odgovara tipu operacije operationType.

Na osnovu rezultata IsActivePrivilege i IsActiveAor, Authorization Manager pozivom metode interne Evaluate računa da li je izvršavanje zahtevane operacije nad određenim objektom iz korisničke sesije dozvoljeno. Krajnji rezultat predstavlja logičku operaciju AND nad rezultatima izvršenih metoda, IsActivePrivilege i IsActiveAor.

```
public interface IAuthorizationCheck
{
    public bool AccessCheck (Guid SessionID, SecurityIdentifier
prmsID, string RegionID);
    bool Evaluate(bool IsActivePrivilege, bool IsActiveAor);
}
```

Listing 14. Interfejs modula za donošenje autorizacionih odluka

Prilog B. Primer konfiguracije aplikativnog konteksta

Konfiguracija aplikativnog konteksta koja je korišćena u toku ovog istraživanja je definisana u skladu sa zahtevima opisanim u *Sekciji 3.2.3*. Potrebno je napomenuti da se bezbednosne politike svakog konteksta mogu menjati u skladu sa specifičnim zahtevima kompanija.

Bezbednosna politika aplikativnog konteksta za rad u realnom vremenu (`RealTime`) je definisana tako da nije moguće izmeniti skup omogućenih ovlašćenja prilikom

```
<Policy Name="RealTimeContext" PolicyId="0">
    <Target Environment="RealTime">
        <Rule ID="1">
            <Condition> </Condition>
            <Effect> </Effect>
        </Rule>
    </Target>
</Policy>
```

Listing 15. Primer bezbednosne politike RealTime aplikativnog konteksta

uspostavljanja korisničke sesije. Na isti način je definisana i bezbednosna politika poslovnog aplikativnog konteksta (`Business`). Ovako definisana (prazna) bezbednosna politika predstavlja podrazumevanu (*default*) konfiguraciju aplikativnog konteksta ukoliko se drugačije ne specificira. Podrazumevana bezbednosna politika je prikazana na *Listingu 15.*

Na *Listingu 16.* je prikazan aplikativni kontekst za testiranje i proveru kvaliteta (`QA`). QA kontekst je definisan tako da korisnicima koji su predviđeni za rad u okviru ovog konteksta bude omogućen nadzor nad svim AOR-ima. Kako je izmena modela kritična operacija za QA kontekst, ovlašćenja sa aspekta ažuriranja modela ne treba da budu izmenjena. Za korisnike čija zaduženja ne podrazumevaju rad u okviru QA konteksta nisu definisane dodatne izmene ovlašćenja prilikom uspostavljanja korisničke sesije.

```
<Policy Name="QAContext" PolicyId="3">
    <Target Environment="QA">
        <Rule ID="1">
            <Condition Name="KoordinatorAzuriranjaModela,
                        InzenjerZaAzuriranjeModela" />
            <Effect Name="AORS.Nadzor" Decision="Allow" />
            <!-- AORS == applies to AORs assigned to a user -->
        </Rule>
    </Target>
</Policy>
```

Listing 16. Primer bezbednosne politike QA aplikativnog konteksta

Na *Listingu 17.* je prikazana bezbednosna politika aplikativnog konteksta za planiranje izgradnje i održavanja elektroenergetskog sistema (`Planning`) koja treba da omogući pristup samo projektantima mreže i to na taj način da korisnicima koji su članovi

ove korisničke uloge bude omogućen nadzor i ažuriranje modela celokupne elektroenergetske mreže. Za sve ostale korisničke uloge privilegije treba da budu onemogućene.

```
<Policy Name="PlanningContext" PolicyId="2">
    <Target Environment="Planning">
        <Rule ID="1">
            <Condition Name="ProjektantMreze" />
            <Effect Name="AzuriranjeModela" Decision ="Allow" />
            <Effect Name="All_AORS.Nadzor" Decision ="Allow" />
           <Effect Name="All_AORS.Azuriranje" Decision="Allow" />
            <!-- All_AORS == applies to all AORs in the system -->
        </Rule>
        <Rule ID="2">
            <Condition Name="KoordinatorAzuriranjaModela" />
            <Effect Name="KoordinatorAzuriranjaModela" Decision="Deny"/>
        </Rule>
       <Rule ID="3">
            <Condition Name="InzenjerZaAzuriranjeModela" />
            <Effect Name="InzenjerZaAzuriranjeModela" Decision="Deny" />
       </Rule>
        <Rule ID="4">
            <Condition Name="InzenjerSistema" />
            <Effect Name="InzenjerSistema" Decision="Deny" />
       </Rule>
       <Rule ID="5">
            <Condition Name="ClanPosade" />
            <Effect Name="ClanPosade" Decision="Deny" />
        </Rule>
        <Rule ID="6">
            <Condition Name="DispecerPosade" />
            <Effect Name="DispecerPosade" Decision="Deny" />
        < /Rule>
    < /Target>
< /Policy>
```

Listing 17. Primer bezbednosne politike Planning aplikativnog konteksta

Na *Listingu 18.* je prikazana bezbednosna politika aplikativnog konteksta za podršku operacijama na terenu (`FieldOps`) koja treba da izmeni ovlašćenja članova posade tako da im omogući odgovornost nadzora i kontrole nad svim AOR-ima u sistemu. Za ostale korisničke uloge nema izmena.

```
<Policy Name="FieldOpsContext" PolicyId="4">
    <Target Environment="FieldOps">
        <Rule ID="1">
            <Condition Name="ClanPosade" />
            <Effect Name="All_AORS.Nadzor" Decision="Allow" />
            <Effect Name="All_AORS.Kontrola" Decision="Allow" />
            <!-- All_AORS == applies to all AORs in the system -->
        </Rule>
    < /Target>
< /Policy>
```

Listing 18. Primer bezbednosne politike FieldOps aplikativnog konteksta

Bezbednosna politika simulacionog aplikativnog konteksta (`Simulation`), prikazana na *Listingu 19.* treba da izmeni skup svim korisničkim ulogama koje su predviđene da rade u simulaciji, bilo iz kontrolne sobe ili iz poslovnog sistema.

```
<Policy Name="SimulationContext" PolicyId="1">
    <Target Environment="Simulation">
        <Rule ID="1">
            <Condition Name="Operater, Supervizor,
                       InzenjerZaPodrskuKontrolnojSobi,
                       KoordinatorAzuriranjaModela" />
            <Effect Name="All_PPRMS" Decision="Allow" />
            <!-- All PRMS == applies to all PRMSs in the system -->
            <Effect Name="All_AORS.Nadzor" Decision="Allow" />
            <Effect Name="All_AORS.Kontrola" Decision="Allow" />
            <Effect Name="All_AORS.Azuriranje" Decision="Allow" />
            <!-- All_AORS == applies to all AORs in the system -->
        < /Rule>
        <Rule ID="2">
            <Condition Name="InzenjerSistema,
                        InzenjerZaAzuriranjeModela" />
            <Effect Name="All_AORS.Nadzor" Decision ="Allow" />
            <Effect Name="All_AORS.Kontrola" Decision ="Allow" />
            <Effect Name="All_AORS.Azuriranje" Decision ="Allow" />
            <!-- All_AORS == applies to all AORs in the system -->
        < /Rule>
    < /Target>
</Policy>
```

Listing 19. Primer bezbednosne politike Simulation aplikativnog konteksta