|  |  |  |
| --- | --- | --- |
|  | UNIVERZITET U NOVOM SADU  FAKULTET TEHNIČKIH NAUKA  NOVI SAD |  |

Grupa 26

Marko Mijatovic PR21/2015, Andrej Simunovic PR28/2015, Aleksandar Jovic PR144/2015, Igor Resman PR142/2015

Zadatak 31

Sigurnost i bezbednost u elektroenergetskim sistemima

* Primenjeno softversko inženjerstvo -

Novi Sad, 15.11.2018.

Sadrzaj

[1. OPIS REŠAVANOG PROBLEMA](#__RefHeading___Toc209_3190288126) 3

[2. TEORIJSKE OSNOVE](#__RefHeading___Toc211_3190288126) 4

[3. DIZAJN IMPLEMENTIRANOG SISTEMA](#__RefHeading___Toc321_3190288126) 5

[4. TESTIRANJE SISTEMA](#__RefHeading___Toc215_3190288126) 6

# OPIS REŠAVANOG PROBLEMA

Očekivano je da ovo poglavlje bude dužine do **jedne stranice**. Navesti detaljan opis problema rešavanih u radu, odnosno opisati sta je bio zadatak.

Tema projektnog zadatka je distribuirano skladistenje podataka potrosnje elektricne energije za odredjeni grad. U sistemu postoji 3 vrste korisnika (Roles):

* Reader – ima pravo da prikaze odgovarajuce informacije iz baze i racuna srednju vrednost godisnje potrosnje za odredjeni grad.
* Editor – azurira potrosnju za aktuelni mesec i prikazuje odgovarajuce informacije iz baze.
* Administrator – nalazi se na vrhu hijerarhije ima pravo da dodaje ili brise postojece entitete iz baze.

Serveri medjusobno pozivaju IntegrityUpdate metodu koja preuzima bazu ostalih servera i osvezava izmene. Metoda IntegrityUpdate se poziva na svakih 30 sekundi. Broj servera kao i njihove konfiguracije se nalaze u zasebnom fajlu i pri pokretanju servera se ucitavaju. Prilikom gasenja jednog od servera ostali nastavljaju sa svojim radom ali dobijaju obavestenje da je neki od servera ugasen. Kada se ugaseni server ponovo podigne svi uspostavljaju prethodne veze.

Klijenti sa servisima komuniciraju preko sertifikata (Chain Trust). U zavisnosti od sertifikata koji klijent poseduje (admin, editor, reader), ima mogucnost izvrsavanja odredjenih metoda. U sertifikatu klijenta osim grupe kojoj pripada ima i organizaciju.

Sve akcije nad bazom podataka koje podrazumevaju izmene podataka su logovane u Windows Event Log-u.

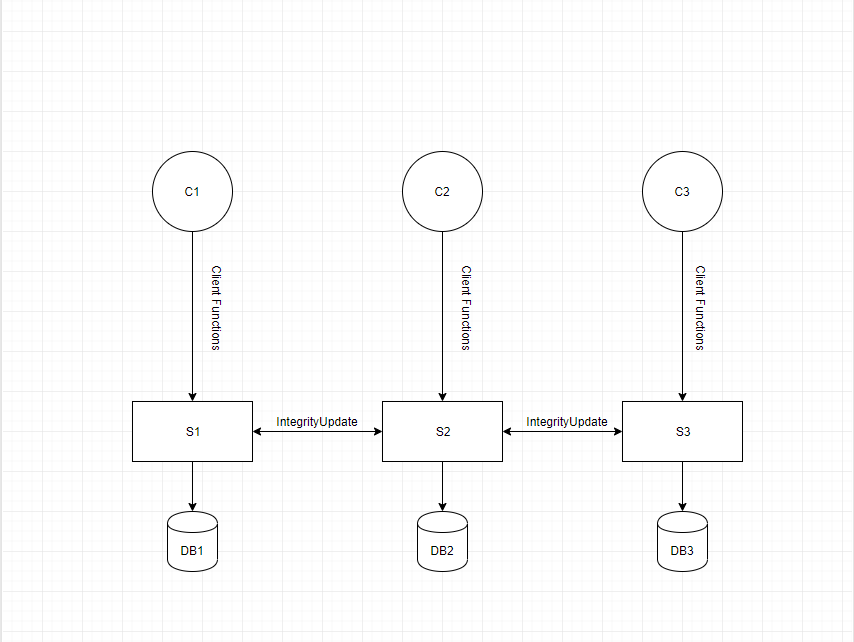
# TEORIJSKE OSNOVE

Neophodno je objasniti funkcionisanje bezbednosnih mehanizama koji su korišćeni pri izradi zadatka.

Autentifikacija je proces u kome se dokazuju identiteti krajnjih učesnika u komunikaciji. Bezbednosni mehanizmi koristeni u izradi projekta su Windows autentifikacija (komunikacija izmedju servera) i koriscenje Sertifikata (komuniikacija izmedju klijenta i servera). Servisi se medjusobno javljaju jedan drugom bez slanja poverljivih podataka, ali kod NTLM autentifikacionog protokola izostaje verifikacija strane koja je primila zahtev. Komunikacija klijent-server zasnovana je na sertifikatima, nase sertifikaciono telo je nazvano TestCA1. Ono izdaje sertifikate za servera i klijente. U sertifikat se ugradjuje javni kljuc korisnika, dok se tajni ne razmenjuje. Autorizacija prava klijenata se vrsi primenom RBAC autorizacione seme. U klasi CustomAuthorizationManager na osnovu rola koje se citaju iz baze podataka se vrsi autorizacija klijenta.

# DIZAJN IMPLEMENTIRANOG SISTEMA

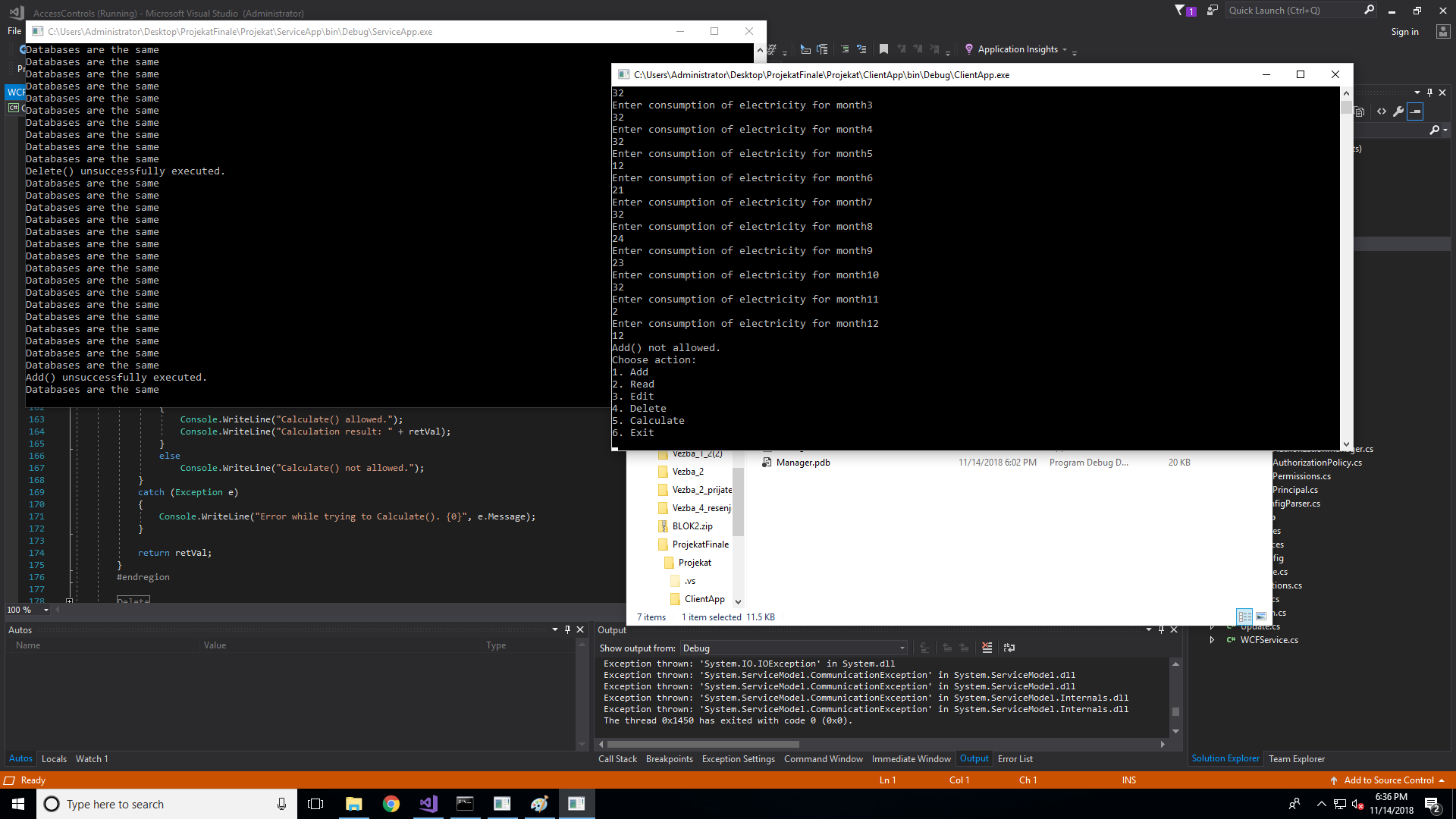
Arhitektura i dizajn implementiranog sistema, kao i detaljan opis korišćenih komunikacionh protokola, interfejsa i bezbednosnih mehanizama. Prilikom kreiranja arhitekturalnog dijagrama neophodno je naglasiti koja komponenta izlaže koji interfejs, kao i koji je tip autentifikacije korišćen između komponenti.



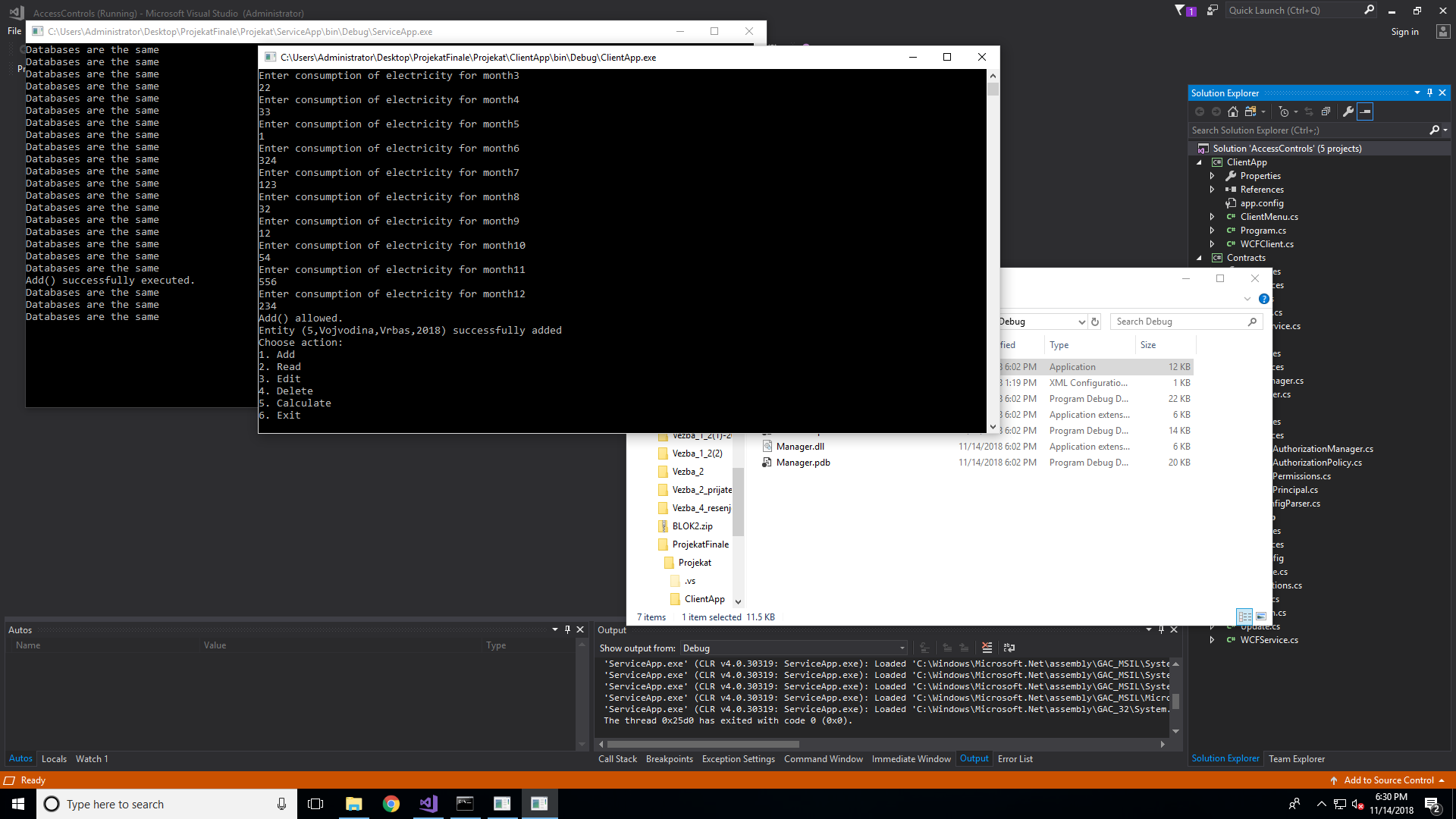
Za komunikacija izmedju servera se koristi interfejs IUpdate sa metodom IntegrityUpdate za razmenu baze podataka i sinhronizaciju. IWCFService se koristi za komunikaciju izmedju klijenta i servera. U njemu su metode: Read, Edit, Delete, Add, Calculate.

# TESTIRANJE SISTEMA

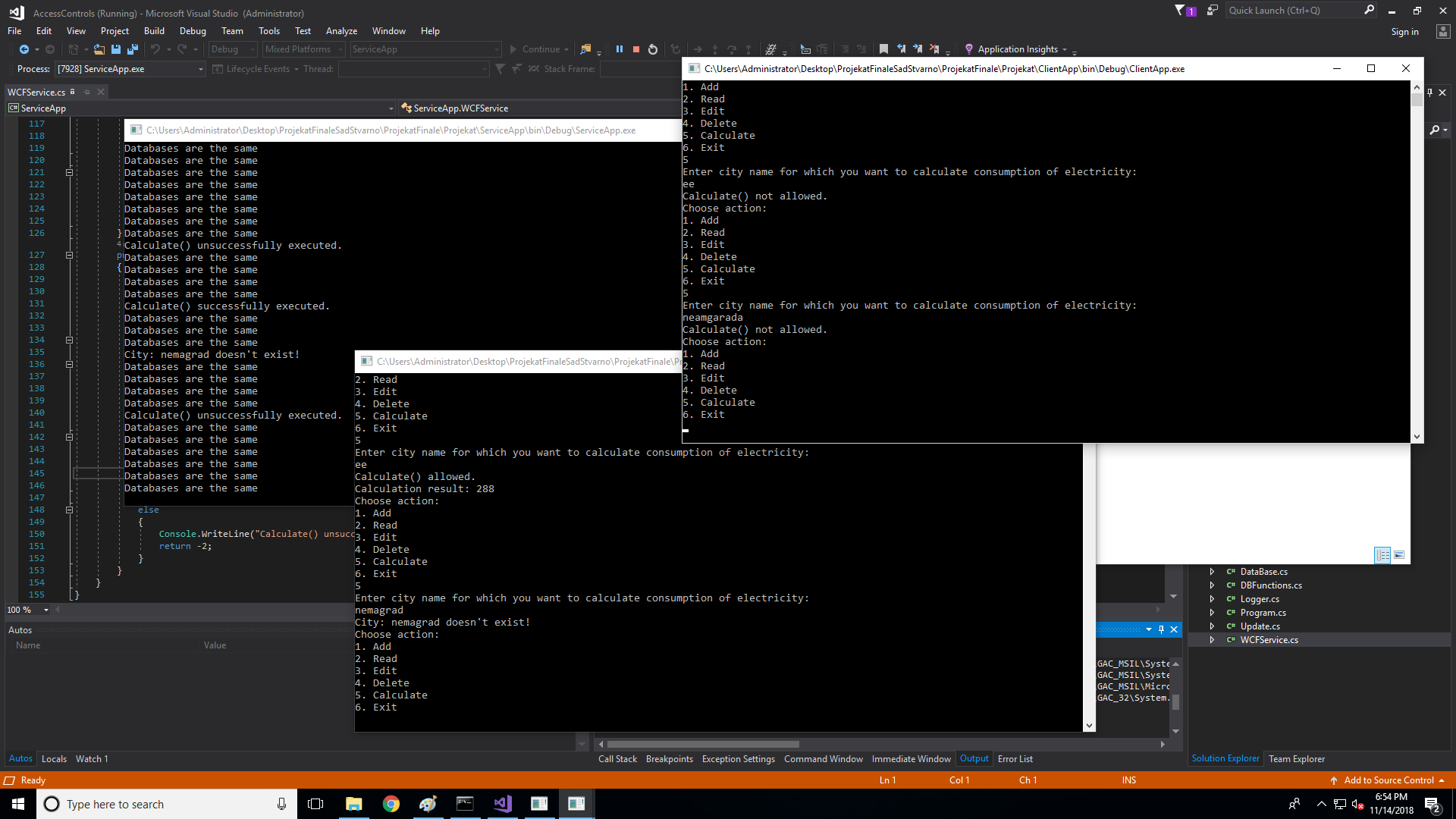
Prikaz rezultata testiranja. Očekuju se prikazi pozitivnih i negativnih (npr. neuspešna autentifikacija, neuspešna autorizacija, itd.) test scenarija.



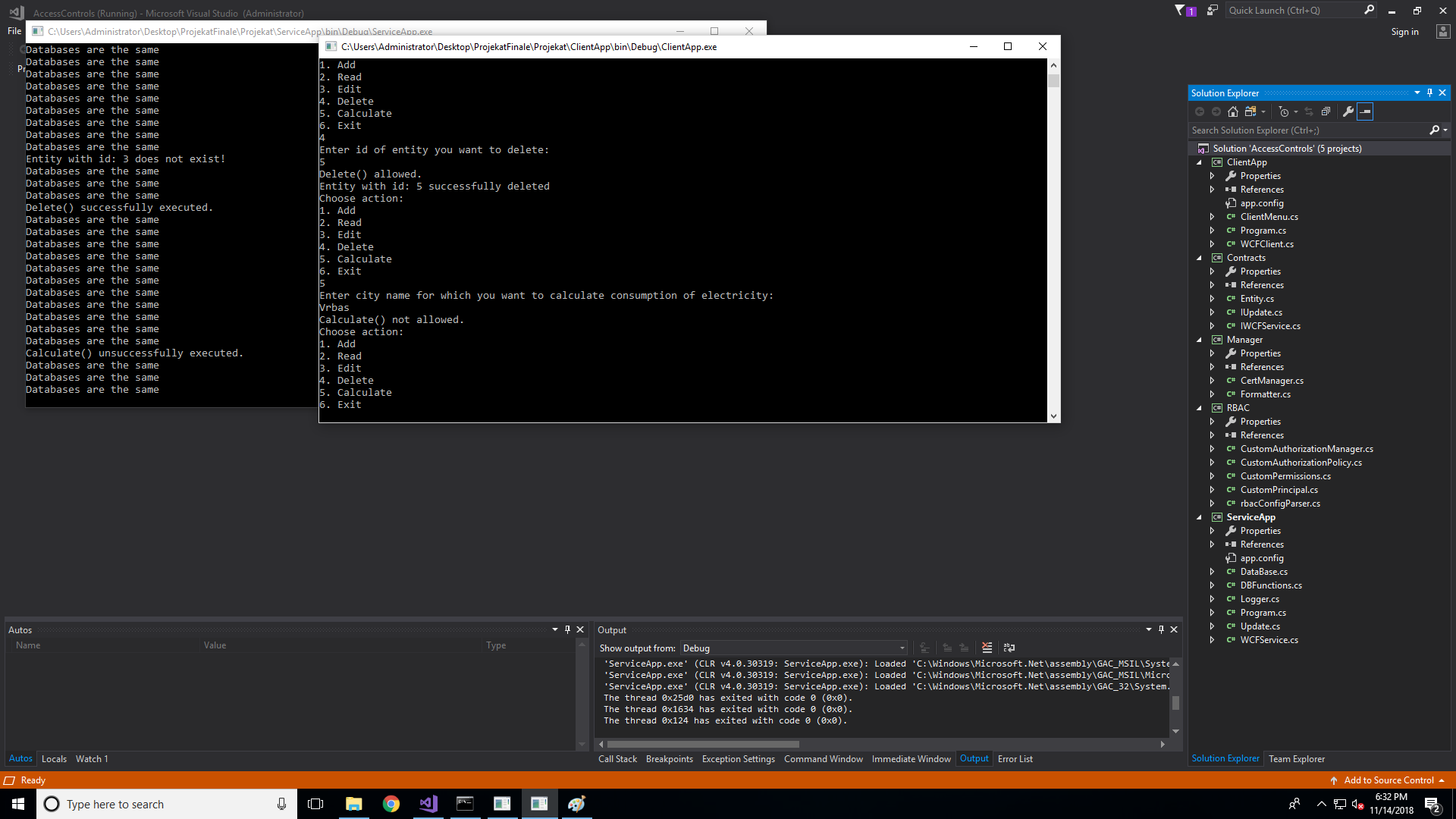
*Slika 2.1. Delete neuspesan i Add neuspesan.*



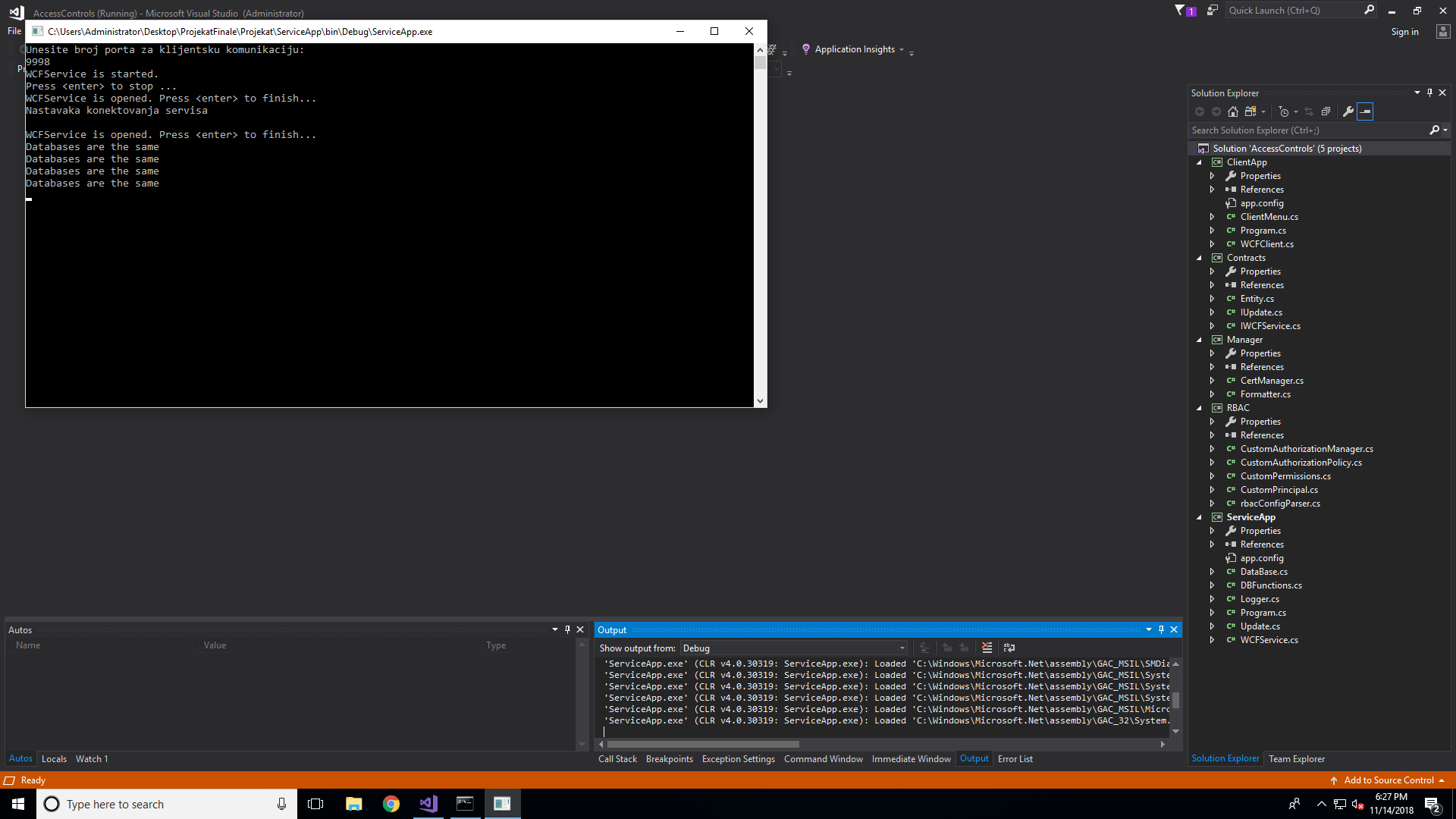
*Slika 2.2. Add uspesan.*



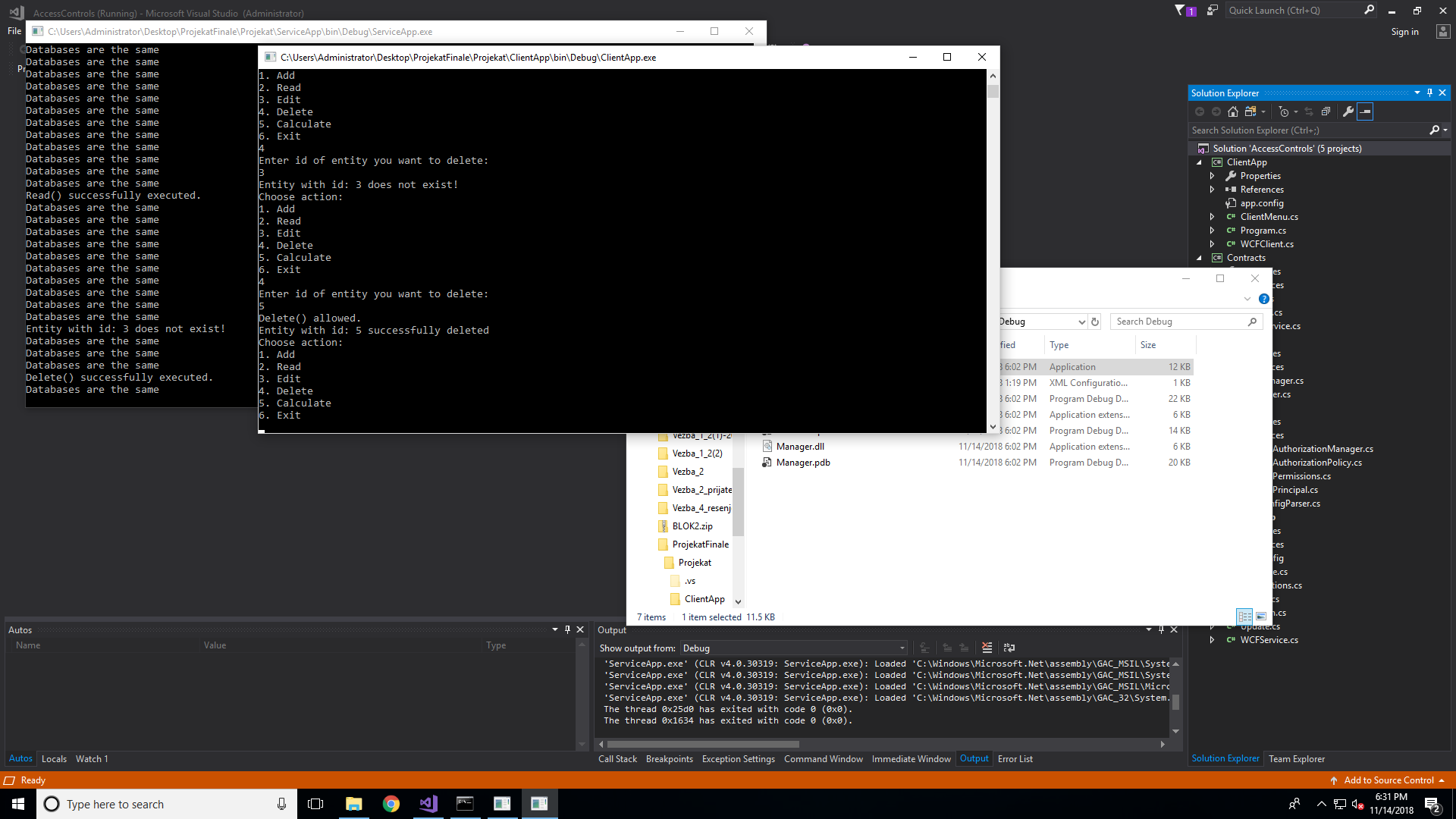
*Slika 2.2. Calculate metoda.*



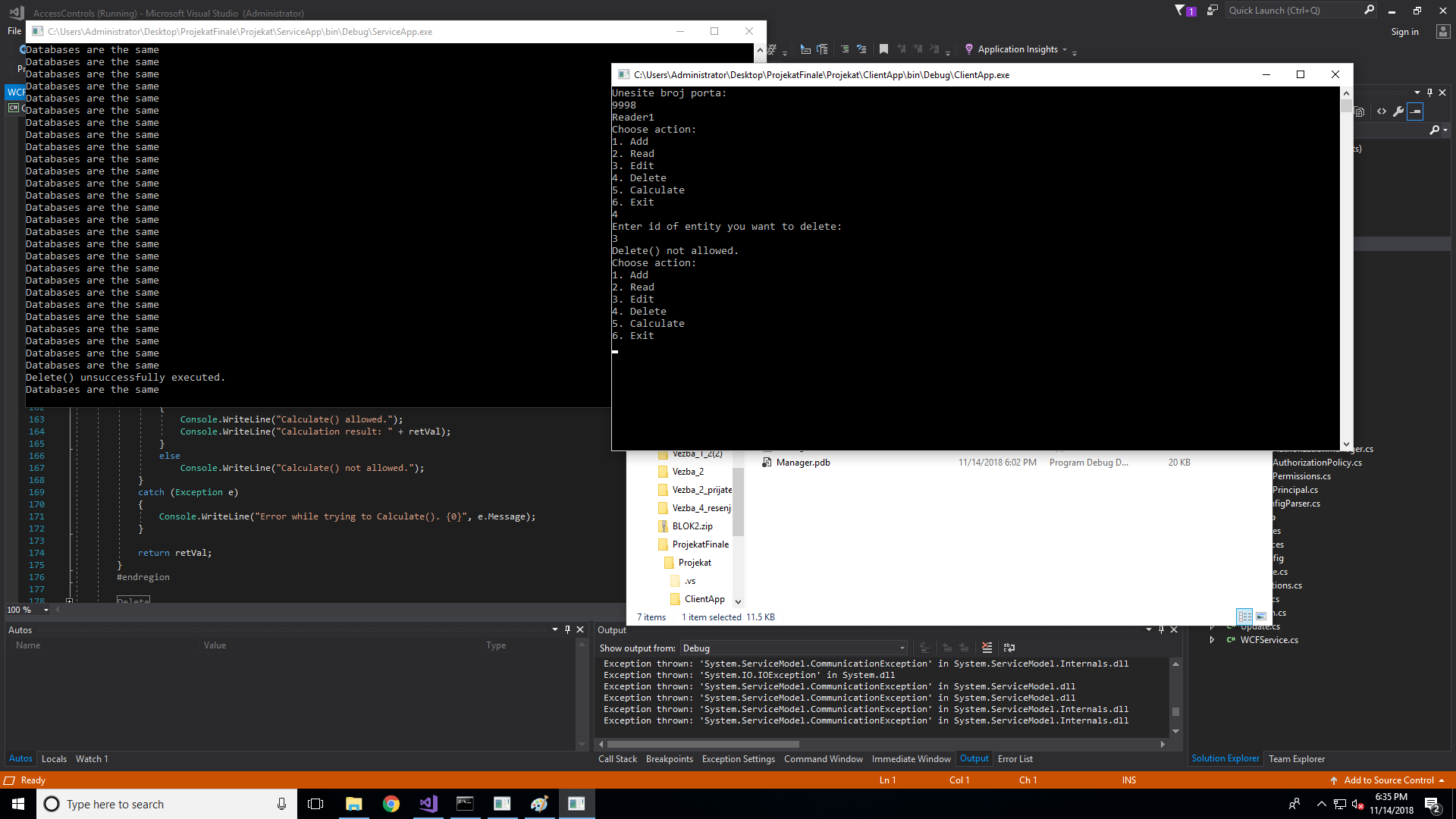
*Slika 2.3. Delete izvrsen, Calculate nesupesan.*



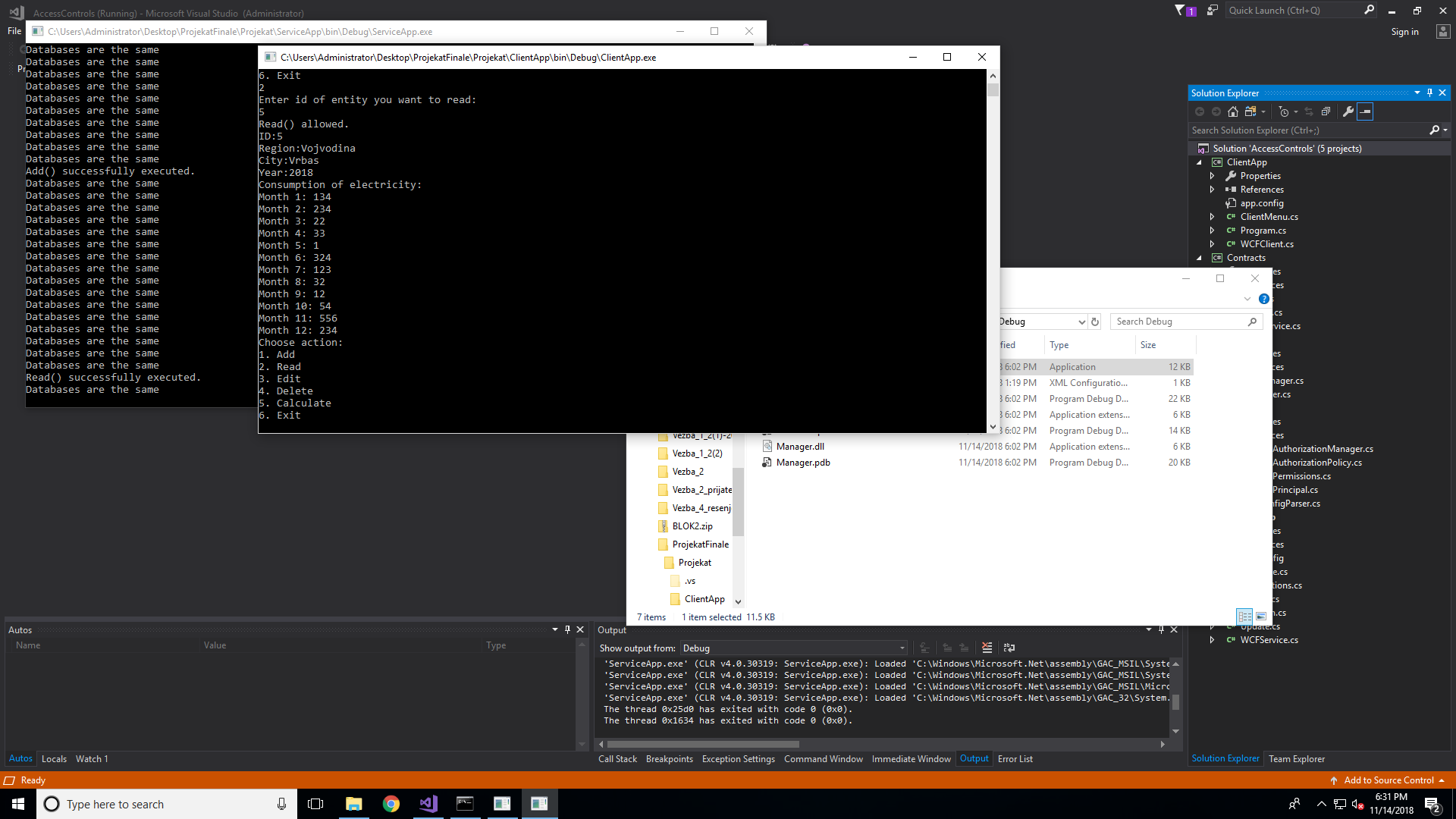
*Slika 2.4. Prikaz IntegrityUpdate metode.*



*Slika 2.5. Prikaz Delete i Read metoda.*



*Slika 2.6. Delete neuspesan.*



*Slika 2.7. Add uspesan, Read uspesan.*