



**ТЕХНИЧЕСКИ УНИВЕРСИТЕТ - СОФИЯ**

**ФАКУЛТЕТ КОМПЮТЪРНИ СИСТЕМИ И ТЕХНОЛОГИИ**

**СПЕЦИАЛНОСТ: КОМПЮТЪРНО И СОФТУЕРНО ИНЖЕНЕРСТВО**

# **КУРСОВА РАБОТА**

**Дисциплина:** UML ООП

**Тема:** Охранителна система от тип COT

**Образователно-квалификационна степен:** Магистър

**Студент:** Исмаил Салех; Фак. №: 121323039 /...../

**хн. ас.:** инж. Зеки Малунски /...../

**София 2024**

## Съдържание

Увод.....	3
Резюме.....	3
Use case диаграми .....	5
Class диаграма .....	7
Sequence диаграми .....	8
Communication диаграми.....	11
State Machine диаграми .....	12
Activity диаграми .....	15
Deployment диаграма .....	18

## Увод

Обектът на настоящата курсова работа представлява съвременна охранителната система от тип СОТ. За проектирането ѝ използваме UML, придържайки се към ООР принципите с цел да създадем стабилно и мащабируемо решение, което задоволява сигнално-охранителните нужди на всякакви по големина предприятия. Системата предоставя уеб платформа, чийто графичен интерфейс позволява на потребителите да взаимодействат с нея.

## Резюме

Една охранителна система се състои от множество охраняеми периметри, които от своя страна обединяват множество локации. В локациите са разположени и въведени в експлоатация сигнално-охранителните устройства.

Както се вижда на клас диаграмата (фигура 3):

- Шаблонът за:
  - Потребителите е класът User. По-особеният атрибут тук е ролята, която представлява стойност от enumeration Role.
  - Охраняемите периметри е класът PerimeterSystemControl.
  - Алармените сигнали е класът Alert.
  - Бизнес договорите е класът ContractEvent.
  - Охраняемите локации е класът Location.
  - Устройствата е класът Device.
  - Събития по поддръжка (СП) е MaintenanceEvent.
- Потребителите са персонала на една охранителна система. Всеки потребител има една роля- мениджър или охранител.
- С един периметър са асоциирани множество потребители; алармени сигнали; бизнес договори и локации.
- Един потребител може да взема роля в множество охраняеми периметри. Един проект включва множество участници. Затова е сформирана Many-To-Many релация отразена в асоциативния клас UserPSC, където има допълнителен атрибут createdAt. Този атрибут представя датата и часа на наемане на определено лице върху определен проект (създадена се асоциация потребител-периметър).
- Към една локация са асоциирани множество устройства, които пък от своя страна са асоциирани с ремонтна документация и гаранционни документи.

- Класът Device е родителски клас на 5 класа, които представляват специализирана сигнално-охранителна технология.

Причината да е използвана стрелка за композиция от ContractEvent към PSC, от Alert към PSC, от MaintenanceEvent към Device: Обект от детския клас не може да съществува без наличието на обект от родителския клас. Например ако изтрием определено сигнално-охранително устройство, то прилежащите му обекти от клас MaintenanceEvent също ще бъдат изтрети.

Причината да е използвана стрелка за агрегация от Device към Location, от Location към PSC: Инстанция на обект от детски клас може да съществува независимо от съществуването на обект от прилежащия му родителски клас. Например можем да имаме съхранено устройство без да е въведено в експлоатация (без да е инсталирано на определена локация).

Относно способностите на различните роли:

- Охранителите могат да се логват в охранителна система; разглеждат, активират или деактивират охраняван периметър; разглеждат, създават и обработват локации; разглеждат, добавят и редактират устройства; разглеждат, добавят и редактират СП; разглеждат, редактират и ръчно да подават алармени сигнали.
- Мениджърите притежават привилегиите на охранителите, но също могат да създават, редактират и трийт периметри; достъпват и обработват данни относно различните итерации на сключения договор или няколко отделни договора между охранителната фирма и клиентите; достъпват и обработват данни относно личната/потребителска информация на охранителите.

## Use case диаграми

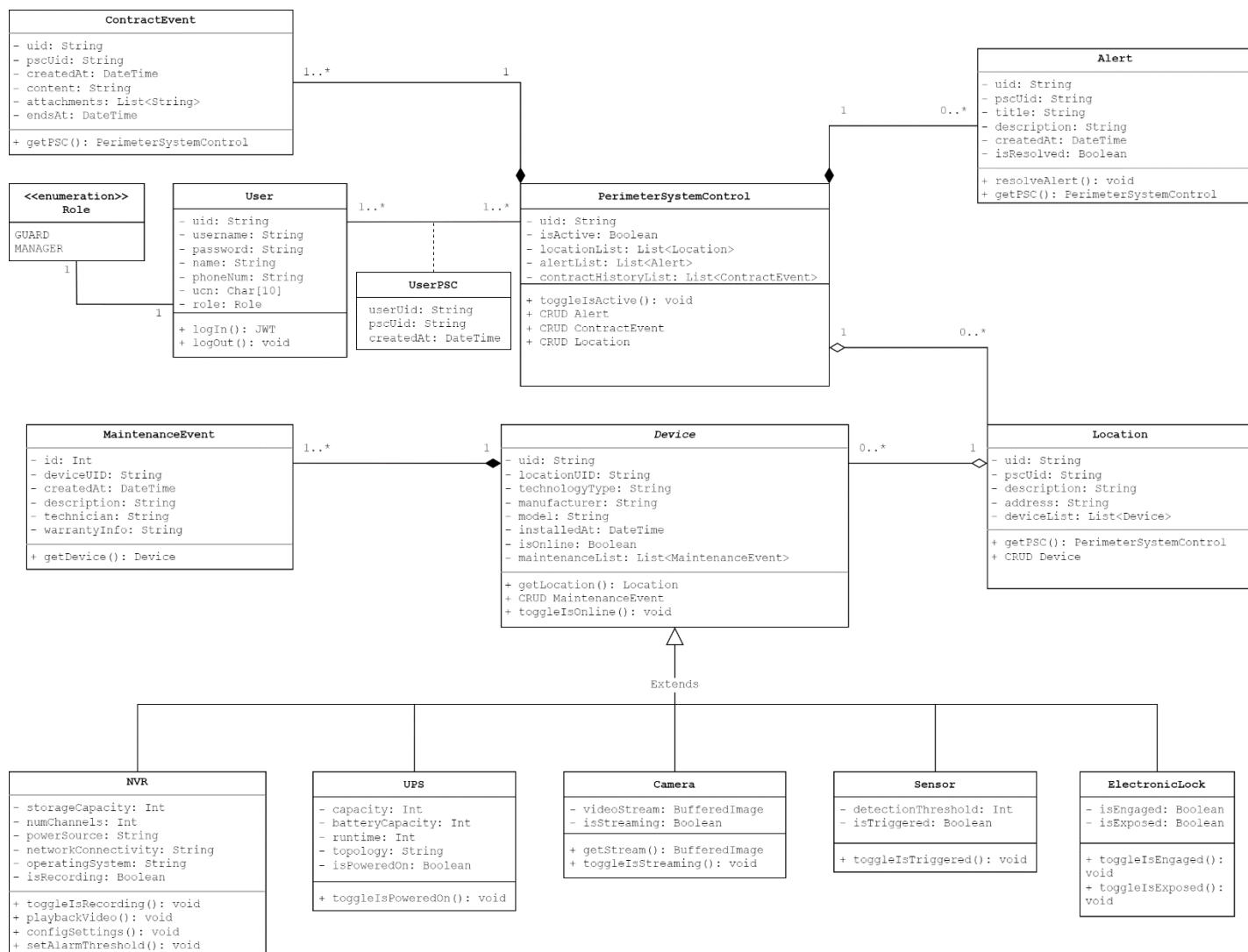


Фиг. 1. Use case диаграма относно процеса на оторизация.

Представено е поведението на системата при опит за логване в нея. Посредством IP адреса на клиента и акаунта, който клиентът се опитва да достъпи, се идентифицира броят на опитите за влизане. При твърде много неуспешни опити, системата връща актуално съобщение. Ако не са извършени твърде много неуспешни опити, системата верифицира подадените кредитенции. При успешна верификация системата препраща потребителя към таблото му за работа. В противен случай системата връща съобщение за подадени грешни кредитенции и неуспешните опити се инкрементират.

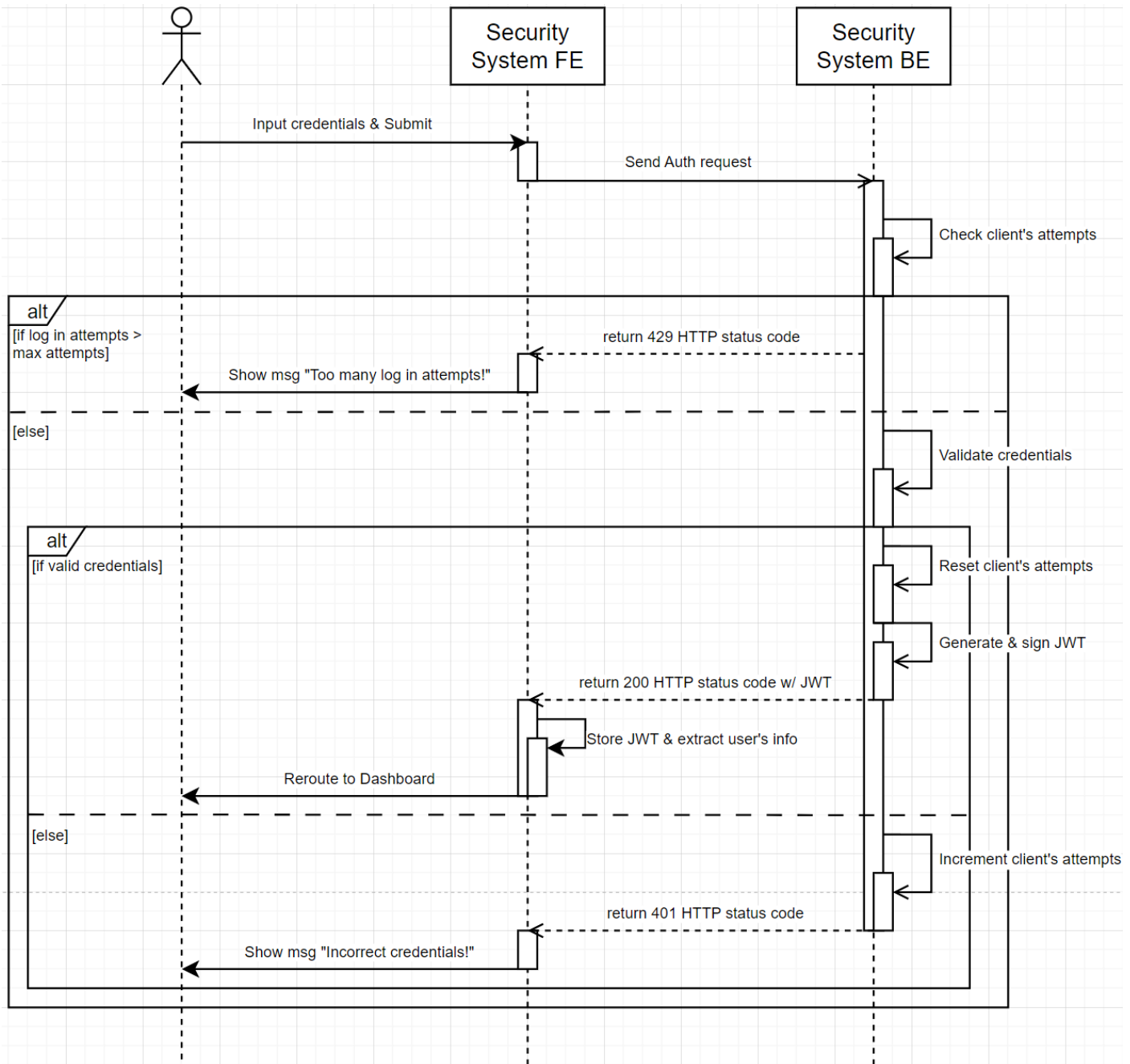


# Class диаграмма



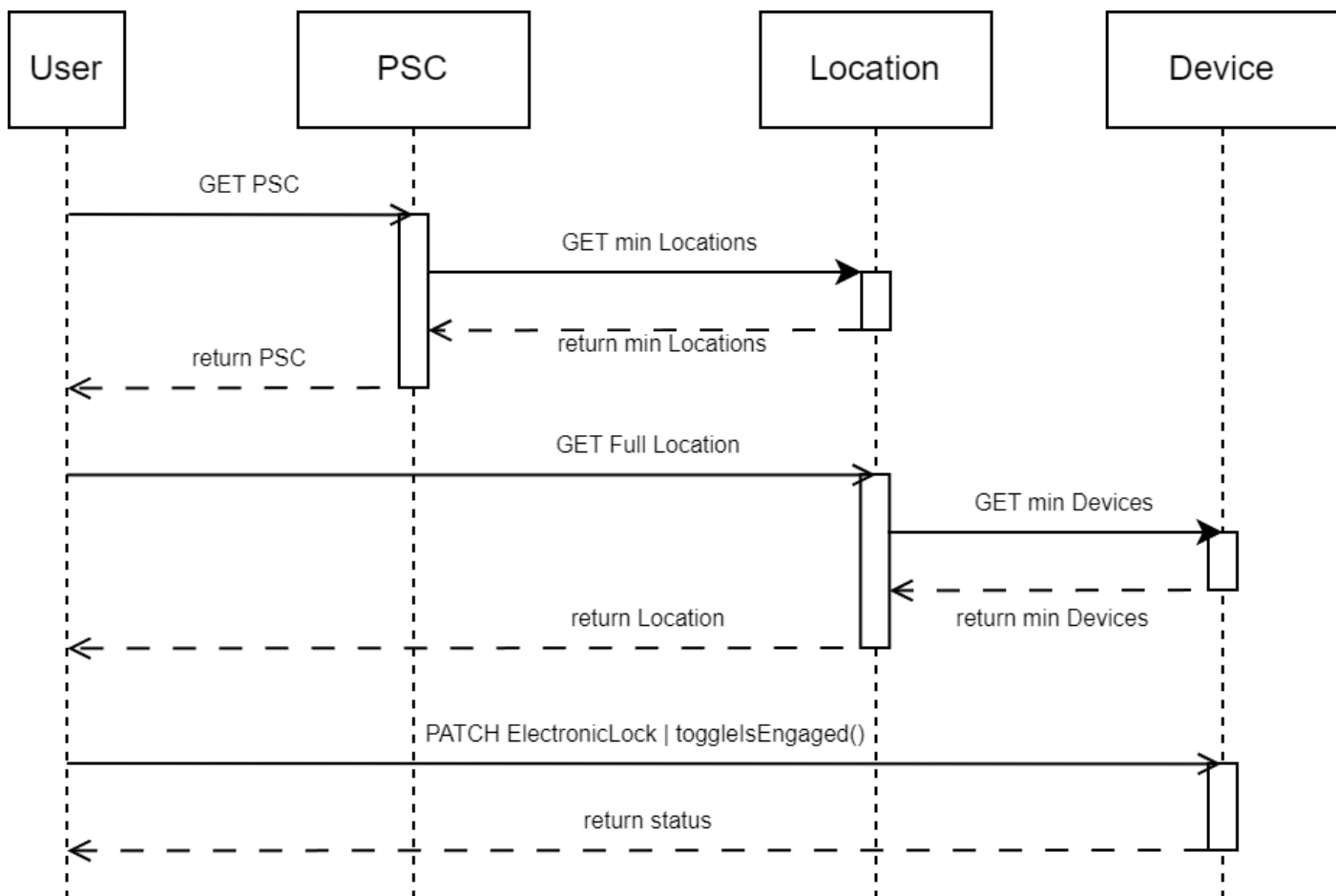
Фиг. 3. Class диаграмма.

## Sequence диаграми

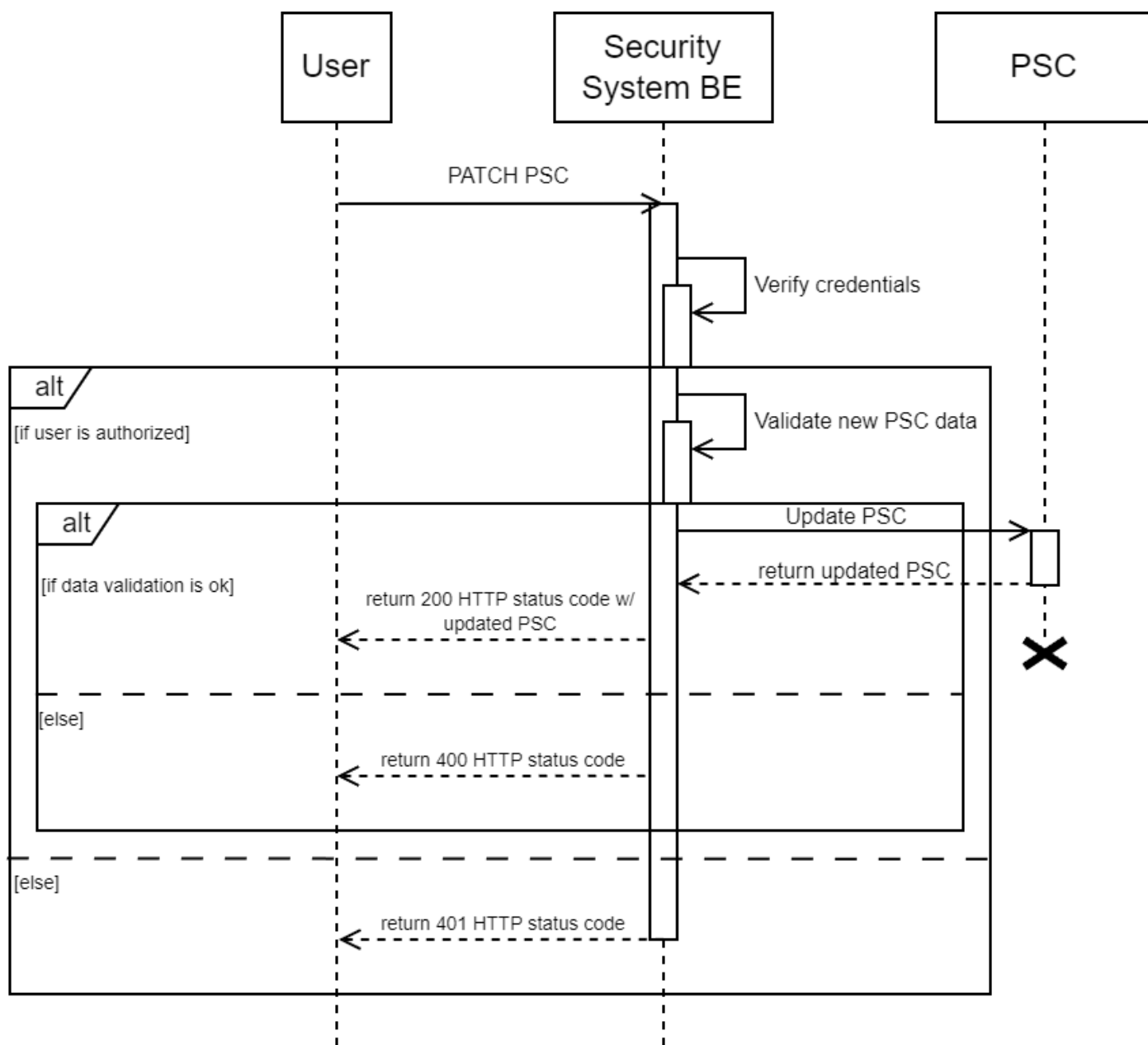


Фиг. 4. Диаграма на последователност относно процеса на оторизация.



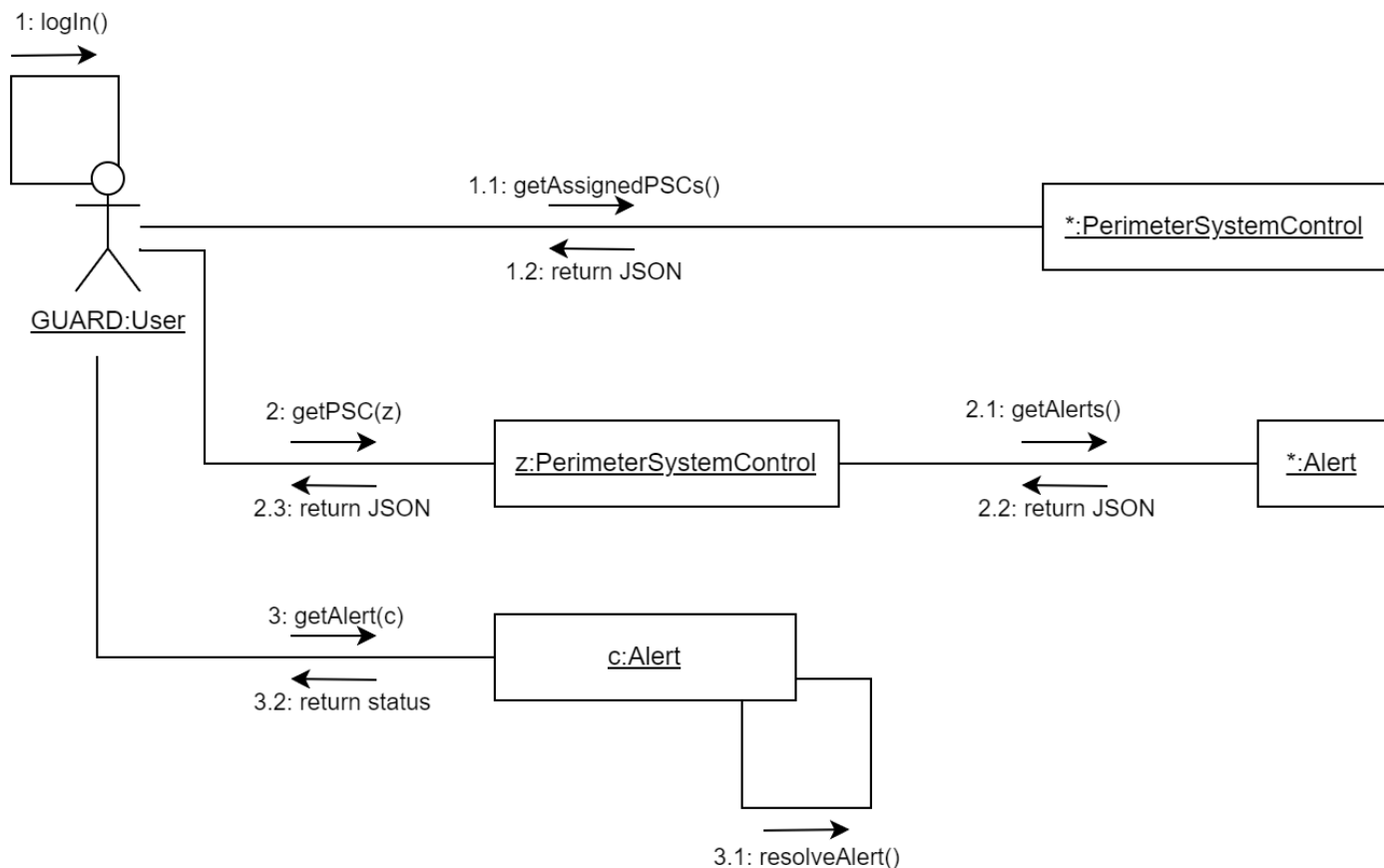


**Фиг. 5.** Диаграма на последователност относно процеса на дистанционно заключване/отключване на ел. ключалка.

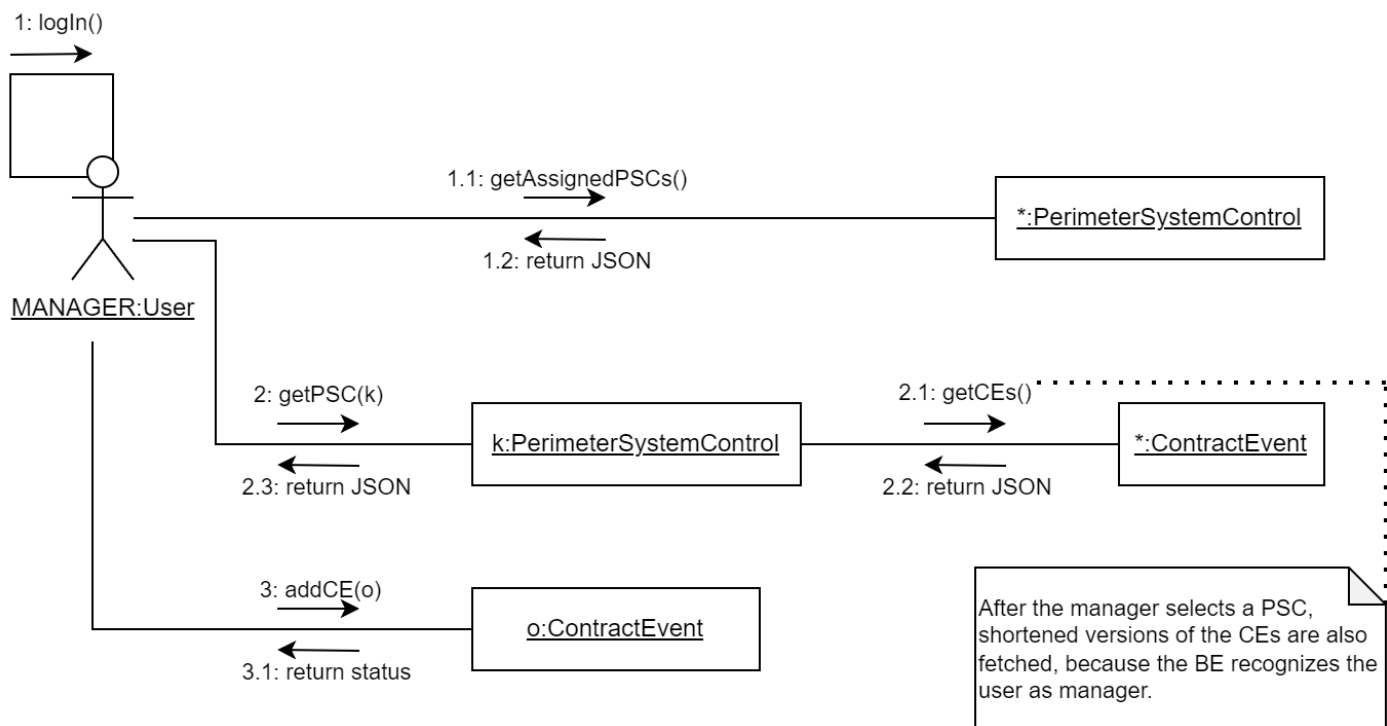


**Фиг. 6.** Диаграма на последователност относно процеса на обновление на PSC.

## Communication диаграми



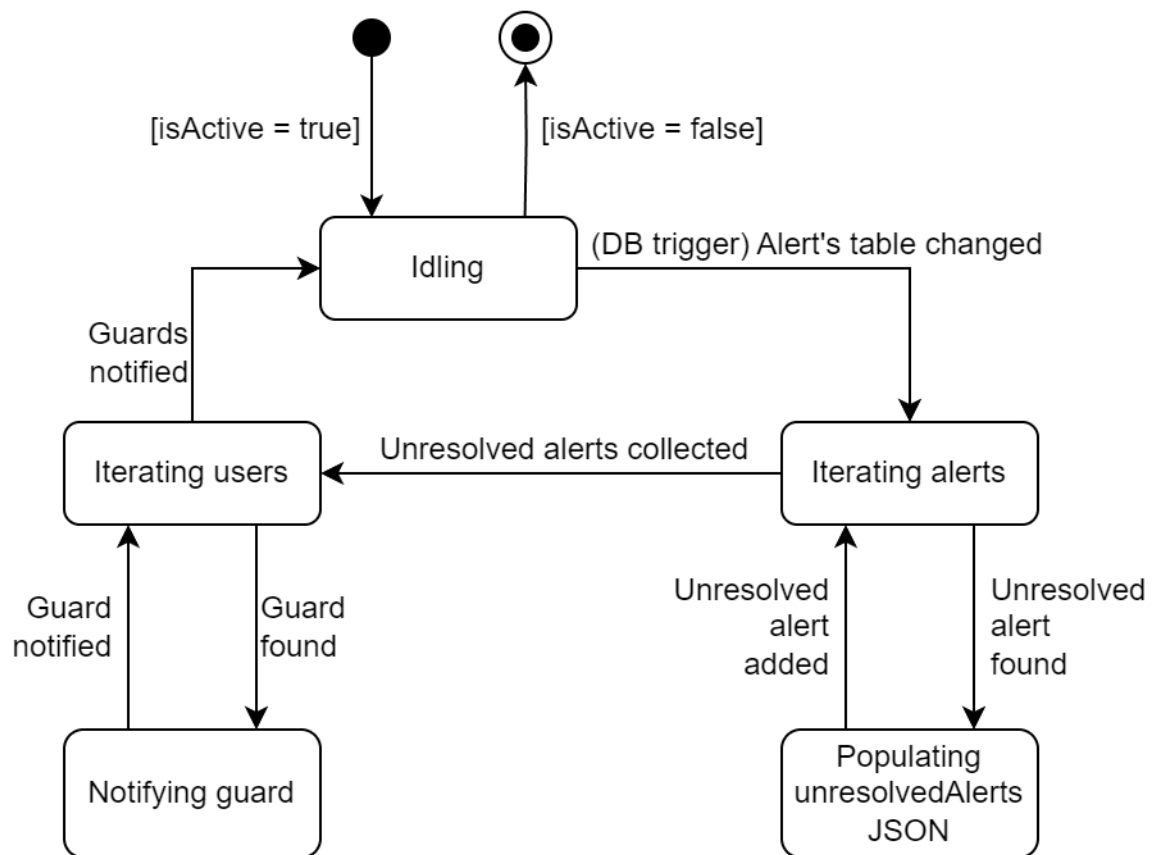
Фиг. 7. Communication диаграма – охранител разрешава/деактивира алармен сигнал.



Фиг. 8. Communication диаграма - мениджър добавя нов бизнес договор.

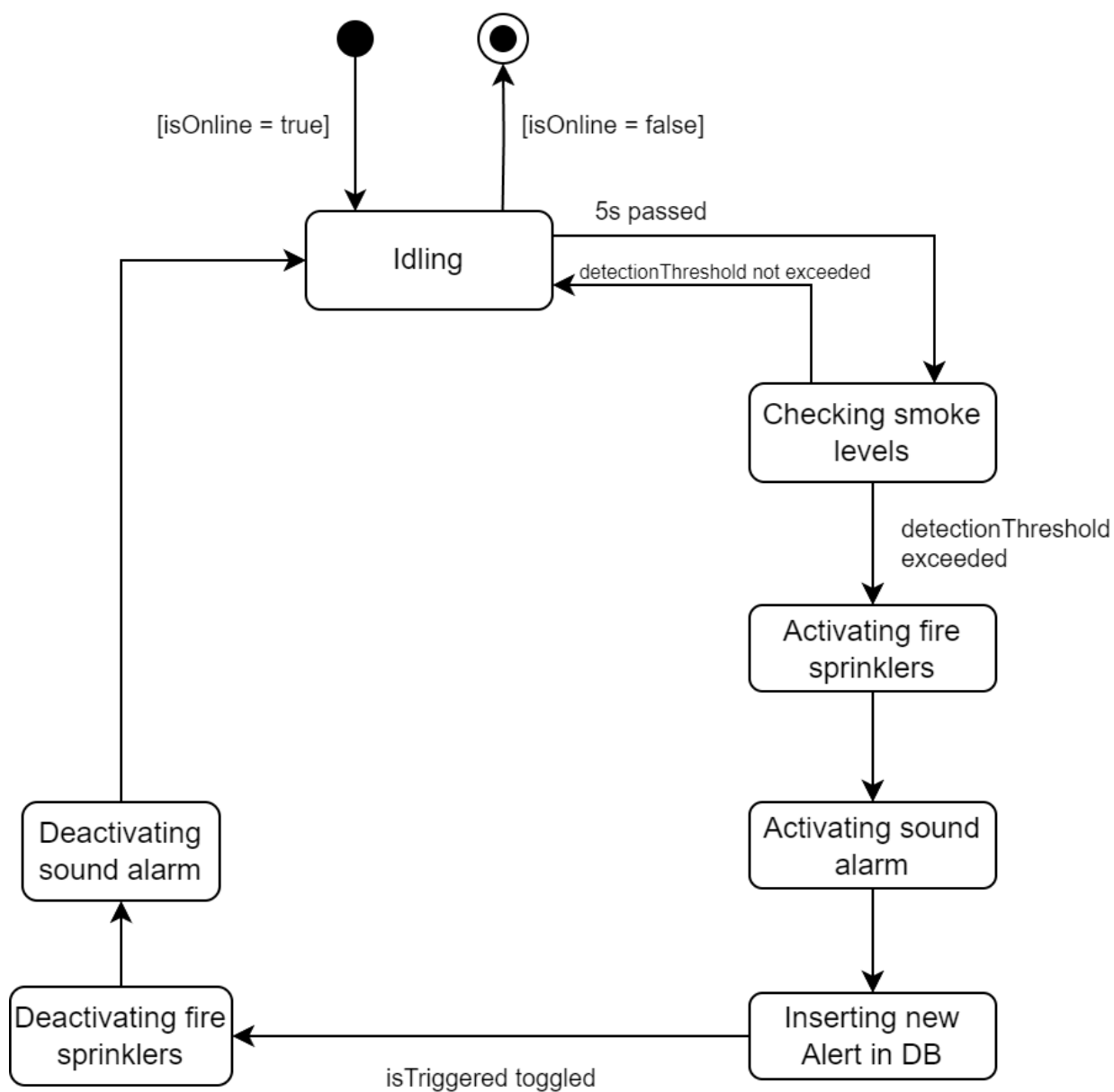
## State Machine диаграми

### PSC's Alert Relay



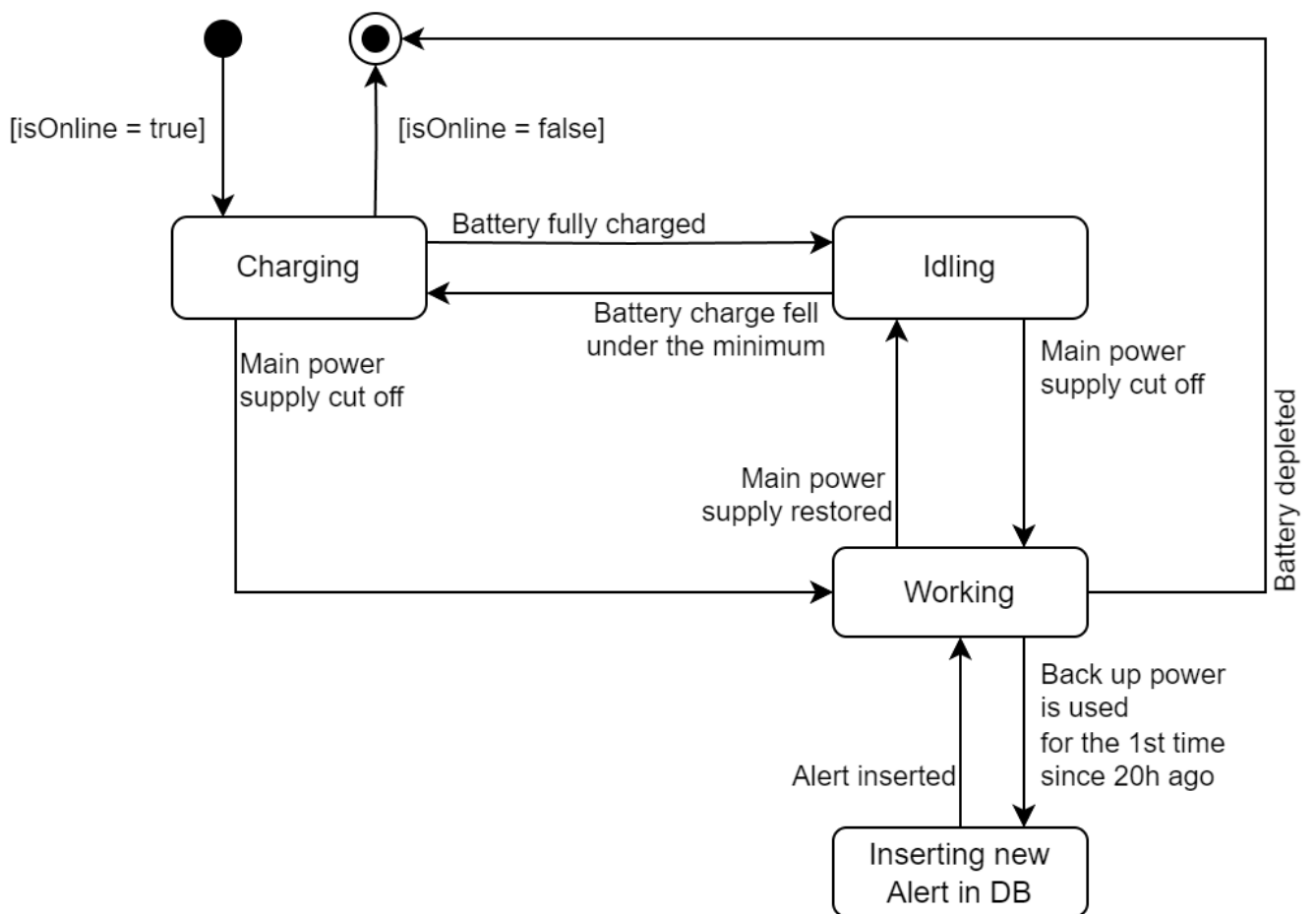
Фиг. 9. Диаграма на състоянията на уведомителното реле.

## Smoke sensor



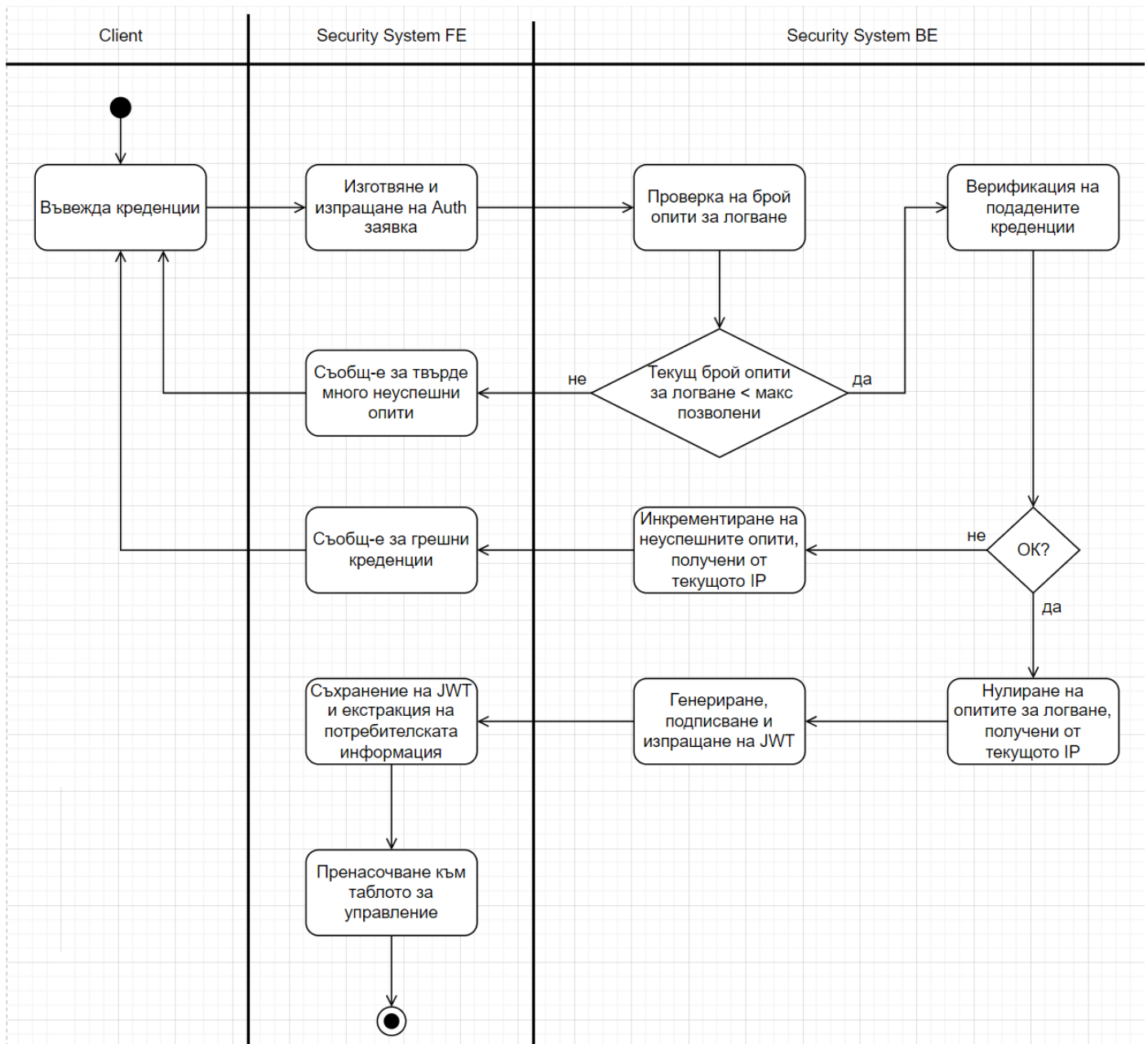
Фиг. 10. Диаграма на състоянията на димен сензор.

## Uninterruptible power supply (UPS)

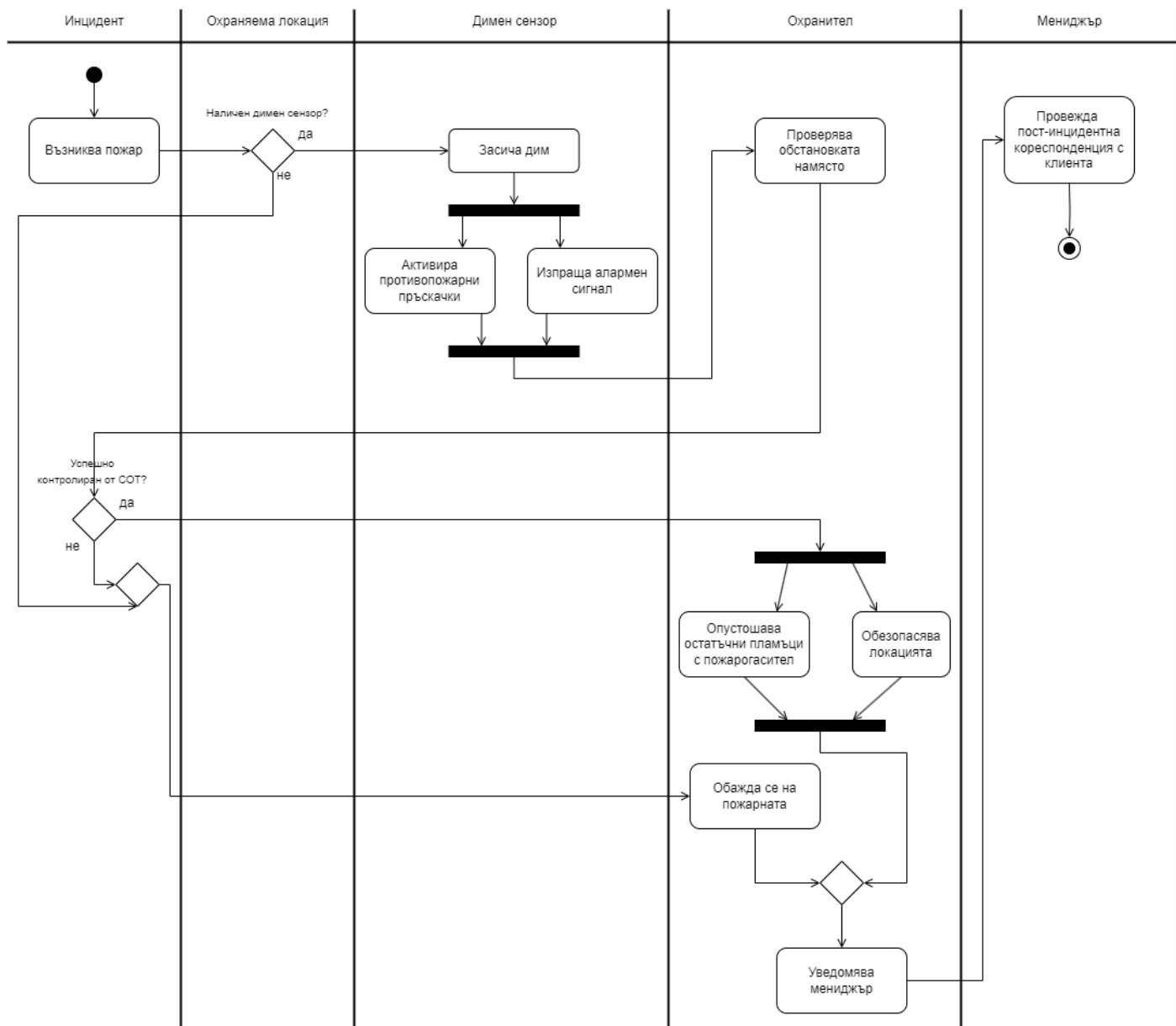


Фиг. 11. Диаграма на състоянията на непрекъсваемо захранване.

## Activity диаграми

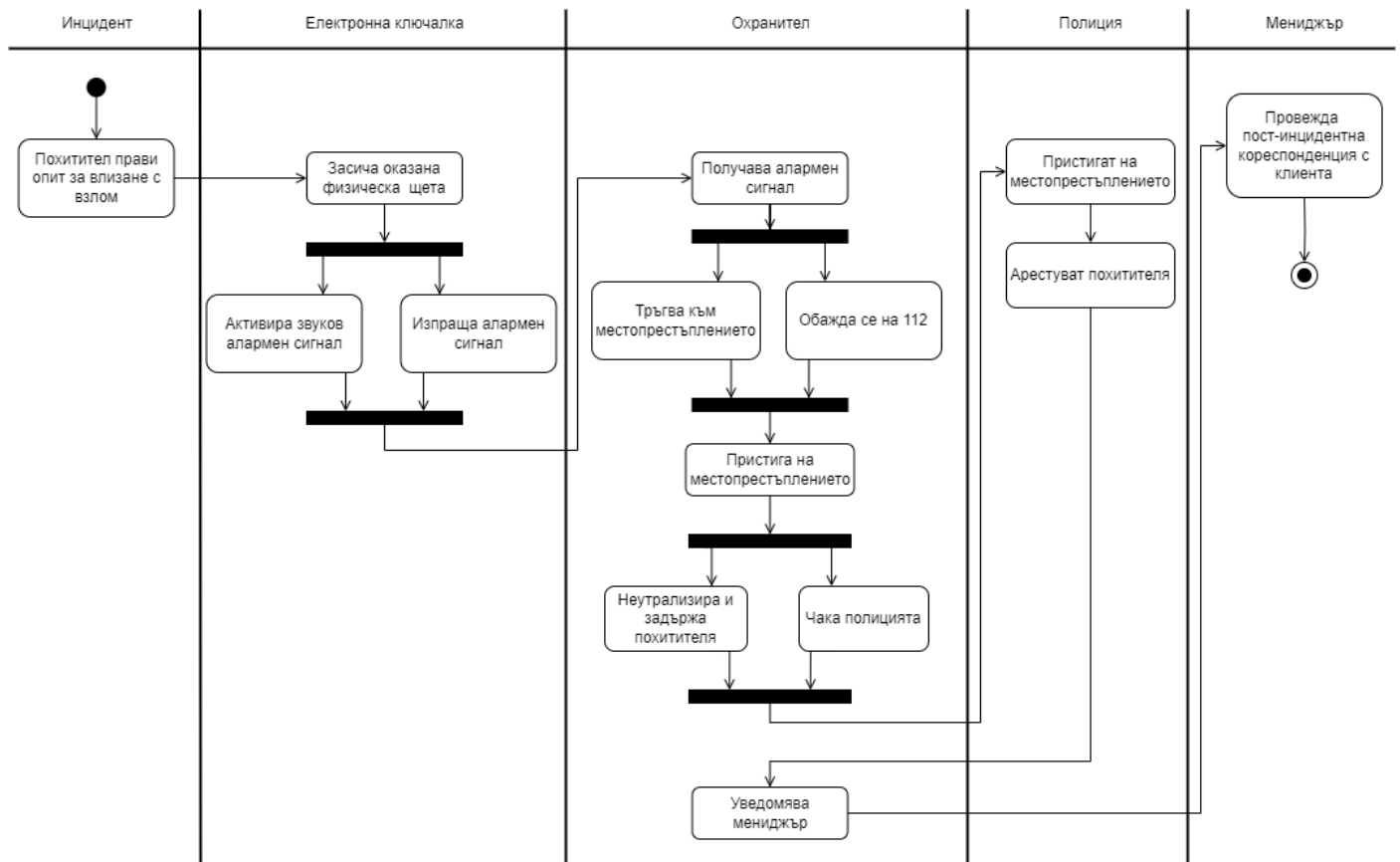


Фиг. 12. Диаграма на дейности при оторизация.



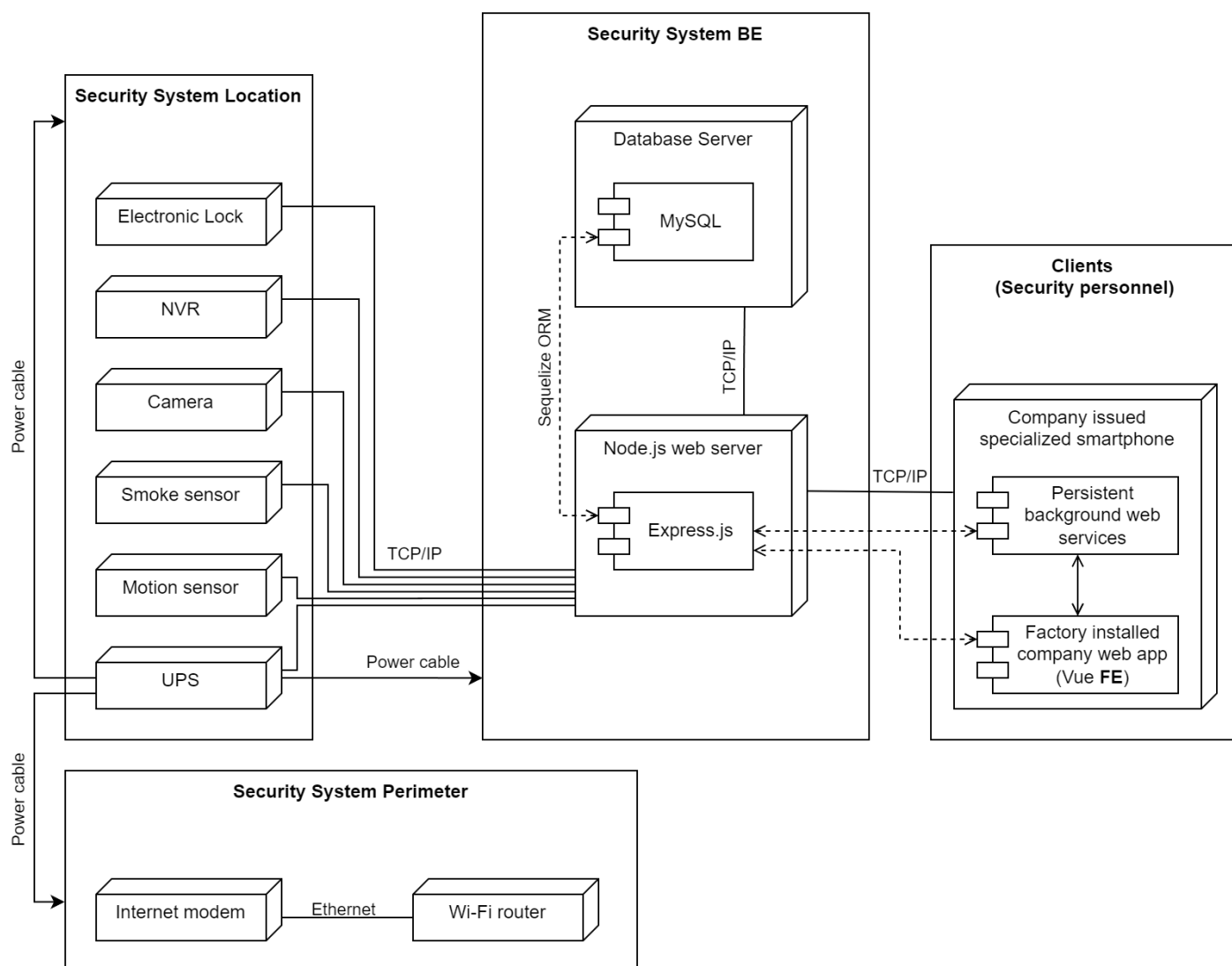
Фиг. 13. Диаграма на дейности при възникването на пожар в охраняема локация.





**Фиг. 14.** Диаграма на дейности при инцидент, където похитител разбива ел. ключалка, въведена в експлоатация.

## Deployment диаграма



Фиг. 15. Deployment диаграма.

Персоналът на охранителната система притежава специализирани работни смартфони, върху които е изтеглено мобилно приложение. То постоянно комуникира със системния бекенд посредством уеб услуги, вървящи във фона. Бекендът от своя страна е в постоянна комуникация със сигнално-охранителни устройства.

Непрекъсваемо токово захранване е в готовност да предоставя електрическа енергия на критичните за охранителната система ел. устройства в случай на авария.

Посредством TCP/IP се осъществява комуникацията между: Node уеб сървър и сигнално-охранителните устройства; Node уеб сървър и ДБ сървър; Node уеб сървър и клиентското уеб приложение.