Smart City  
Aplicație pentru gestiunea  
orașelor inteligente

Croitoru Traian

Lupșan Tudor Adrian  
C-112-B

# Pagina principala - Academia Tehnica Militara „Ferdinand I”

Plan de Testare - Smart-City

Proiect: Smart-City

Versiune: 1.0

Autori: Croitoru Traian, Lupșan Tudor Adrian

Organizație: Academia Tehnică Militară „Ferdinand I”, C-112-B

# 1. Strategia de testare

## 1.1 Scopul proiectului

Acest document are scopul de a defini testele necesare pentru validarea aplicației Smart-City, care permite gestiunea inteligentă a unui oraș printr-un sistem de senzori, hărți digitale și conturi instituționale.

## 1.2 Lista definițiilor

* PT: Plan de Testare
* DCS: Document de Cerințe Software
* HW: Hardware
* SW: Software
* 2FA: Autentificare cu doi factori
* UI: Interfață Utilizator

## 1.3 Resurse necesare testării

- Hardware: procesor minim 2 GHz, 4 GB RAM

- Software: Windows 11, Qt, Microsoft Visual Studio

- Resurse umane: 1 dezvoltator, 1 responsabil testare

# 2. Descrierea testelor

## Test 1 – Autentificare utilizator (cu rol Admin sau Instituție)

Cerință verificată: 3.1 – Autentificare și autorizare

Referință DCS: DCS v1.0, Capitolul 3.1

Modalitate de testare:

1. Se deschide aplicația.  
2. Se introduc username și parolă.  
3. Se apasă Log In.

Rezultat așteptat: Afișarea mesajului „Autentificare cu succes” și redirecționarea către interfața principală.

Rezultat obținut:

Observații:

Calificativ test: [ ] PASS [ ] FAILED

## Test 2 – Adăugare instituție pe hartă

Cerință verificată: 3.3 – Adăugarea instituțiilor

Referință DCS: DCS v1.0, Capitolul 3.1

Modalitate de testare:

1. Utilizatorul Admin accesează harta.  
2. Trage o instituție pe o zonă liberă.  
3. Confirmă plasarea.

Rezultat așteptat: Instituția apare pe hartă și se generează un cont cu rol limitat.

Rezultat obținut:

Observații:

Calificativ test: [ ] PASS [ ] FAILED

## Test 3 – Adăugare și declanșare senzor

Cerință verificată: 3.5 – Adăugarea și configurarea senzorilor

Referință DCS: DCS v1.0, Capitolul 3.1

Modalitate de testare:

1. Utilizator Instituție se autentifică.  
2. Adaugă un senzor.  
3. Simulează declanșarea.

Rezultat așteptat: Notificarea este trimisă către instituția responsabilă și conturile cu permisiune.

Rezultat obținut:

Observații:

Calificativ test: [ ] PASS [ ] FAILED

## Test 4 – Generare raport

Cerință verificată: 3.8 – Raportare și analiză

Referință DCS: DCS v1.0, Capitolul 3.1

Modalitate de testare:

1. Accesează secțiunea „Rapoarte”.  
2. Selectează perioada și tipul de senzor.  
3. Generează raportul.

Rezultat așteptat: Se afișează un raport grafic/statistic cu datele corespunzătoare.

Rezultat obținut:

Observații:

Calificativ test: [ ] PASS [ ] FAILED

## Test 5 – Autentificare eșuată (eroare)

Cerință verificată: 3.1 – Autentificare și autorizare

Referință DCS: DCS v1.0, Capitolul 3.1

Modalitate de testare:

1. Se deschide aplicația.  
2. Se introduce username valid și parolă greșită.  
3. Se apasă Log In.

Rezultat așteptat: Mesaj de eroare: „Autentificare eșuată. Verificați datele introduse.”

Rezultat obținut:

Observații:

Calificativ test: [ ] PASS [ ] FAILED

## Test 6 – Gestionarea permisiunilor (vizualizare date senzor)

Cerință verificată: 3.9 – Gestionarea permisiunilor

Referință DCS: DCS v1.0, Capitolul 3.1

Modalitate de testare:

1. Instituția adaugă senzor.  
2. Atribuie permisiuni altui utilizator.  
3. Acesta se conectează și accesează datele.

Rezultat așteptat: Utilizatorul poate accesa doar senzorul pentru care are permisiune.

Rezultat obținut:

Observații:

Calificativ test: [ ] PASS [ ] FAILED