# Kamerový systém FRS pro provoz turniketů

Tento dokument definuje požadované fungování kamerového systému FRS (Face Recognition System), který bude samostatným technologickým celkem, ale musí spolupracovat s turniketovým a vstupenkovým systémem stadionu.

# 1. **Účel kamerového systému FRS**

Kamerový systém FRS má umožnit biometrickou detekci a identifikaci návštěvníků v prostoru turniketů.

# 2. **Provozní logika FRS v návaznosti na turnikety**

1. Kamera zachytí přicházející osobu k turniketu.
2. Systém vytvoří biometrickou šablonu a vyhodnotí ji vůči bezpečnostním seznamům.
3. FRS odešle turniketu stavové informace: „bezpečný průchod“, „riziková osoba“, „nelze ověřit“.
4. Turniket na základě stavu musí umět následující úkony:

* zablokovat průchod;
* aktivovat alarm;
* informovat obsluhu.

FRS nikdy samostatně nepovoluje průchod – pouze informuje turniketový systém.

# 3. **Architektura kamerového systému**

### *3.1 Kamerové snímací body*

* Každá průchozí linie musí mít vlastní snímací bod optimalizovaný pro výšku procházející osoby.

### *3.2 Kamerové senzory – funkční parametry*

* venkovní a antivandal provedení;
* minimálně Full HD;
* IR/noční režim;
* nízká latence přenosu - do 50 ms.

### *3.3 Hlavní výpočetní jednotka FRS*

* AI akcelerace (GPU/TPU/VPU);
* kapacita pro min. 20 video streamů;
* archivace min. 30 dní;
* šifrované úložiště a zabezpečený přístup.

# 4. **Integrace FRS s turnikety**

Systém FRS předá informaci o stavu vyhodnocení turniketům v reálném čase, a to fyzickým kontaktem, datovou větou nebo pomocí API.

Turnikety na základě této informace vyhodnotí vpuštění osoby přes turniket.

# 5. **Funkce FRS během vstupního procesu**

Normální provoz:

* kamera identifikuje osobu → turniket ověří vstupenku → systémy vyhodnotí kombinovaně.

Shoda s nežádoucí osobou:

* turniket může zablokovat vstup, aktivovat alarm nebo předat informaci obsluze;
* vstup se neotevře bez zásahu obsluhy.

## 6. Logování a auditní stopa

Systém musí ukládat:

* čas detekce;
* biometrickou šablonu;
* výsledek porovnání;
* ID turniketu a kamery;
* návaznost na vstupenkové rozhodnutí.

Veškerá data musí být šifrovaná a přístupná pouze oprávněným osobám.

## 7. Bezpečnost

* Žádná data nesmí být přenášena ani ukládána na externí úložiště;
* povinná šifrování přenosů a uložených dat;
* auditní logování všech přístupů.

## 8. Provozní požadavky

* Automatické restartování komponent dle požadavků;
* vzdálená správa, včetně monitoring veškerých klíčových funkcí;
* propojení FRS API s turnikety;
* harmonizace reakčních časů obou systémů, zajištění s přiřazeným turniketem.