ČESKÉ VYSOKÉ
UČENÍ TECHNICKÉ
V PRAZE

FAKULTA
BIOMEDICÍNSKÉHO
INŽENÝRSTVÍ

DIPLOMOVÁ PRÁCE

2020

TOMÁŠ
ŠVAGR

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta biomedicínského inženýrství

Katedra zdravotnických oborů a ochrany obyvatelstva

Detekční systémy pro rozpoznání obličejů a vzorců chování s možností nasazení na fotbalových stadionech s využitím pro zamezení vstupu nežádoucích osob, prevenci vzniku a forenzního šetření mimořádných událostí

Detection Systems for Facial Recognition and Behavior Patterns at Soccer Stadiums for Entrance Prevention of Unwanted People to the Stadium and Mitigation and Forensic Investigation of Emergencies

Diplomová práce

Studijní program: Ochrana obyvatelstva
Studijní obor: Civilní nouzové plánování

Vedoucí práce: Ing. Václav Navrátil

Tomáš Švagr

Kladno, květen 2020

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Švagr**	Jméno:	**Tomáš**	Osobní číslo:	**461619**
Fakulta:	**Fakulta biomedicínského inženýrství**				
Garantující katedra:	**Katedra zdravotnických oborů a ochrany obyvatelstva**				
Studijní program:	**Ochrana obyvatelstva**				
Studijní obor:	**Civilní nouzové plánování**				

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Detekční systémy pro rozpoznání obličejů a vzorců chování s možností nasazení na fotbalových stadionech s využitím pro zamezení vstupu nežádoucích osob, prevenci vzniku a forenzního šetření mimořádných událostí

Název diplomové práce anglicky:

Detection Systems for Facial Recognition and Behavior Patterns at Soccer Stadiums for Entrance Prevention of Unwanted People to the Stadium and Mitigation and Forensic Investigation of Emergencies

Pokyny pro vypracování:

Cílem diplomové práce bude v teoretické části provést rešerši kamerových systémů s možností rozpoznání obličeje a vzorců lidského chování, které jsou dostupné na českém i zahraničním trhu. Na základě sociálních a ekonomických faktorů bude provedena analýza metodou Cost Benefit Analysis (nebo jiná vhodná analýza) implementace systému. Bude popsáno typické nezákonné chování, vedoucí k újmám na zdraví a ke škodám na majetku při fotbalových utkáních v České republice. V praktické části bude na základě metody Bazické varianty (případně obdobné metody) vybrán nejvhodnější systém, jehož nasazení na fotbalový stadion (splňující parametry kategorie II. a výše dle UEFA kategorizace stadionů) bude následně modelováno.

Seznam doporučené literatury:

[1] JONÁK, Jiří, Využití záznamů z bezpečnostních kamer ve forenzní praxi, Brno: Tribun EU, 2008, ISBN 978-80-7399-643-7
[2] PATÁK, Jaroslav, KLVAŇA, Karel, PROTIVINSKÝ, Miroslav, Zabezpečovací systémy: situační prevence kriminality, Praha: Armex, 2000, 118 s., ISBN 80-86244-13-X
[3] LUKÁŠ, Luděk, Bezpečnostní technologie, systémy a management, Zlín: VeRBuM, 2015, ISBN 978-80-87500-05-7

Jméno a příjmení vedoucí(ho) diplomové práce:

Ing. Václav Navrátil

Jméno a příjmení konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **23.09.2019**
Platnost zadání diplomové práce: **18.09.2021**

prof. MUDr. Leoš Navrátil, CSc., MBA, dr.h.c.	prof. MUDr. Ivan Dylevský, DrSc.
podpis vedoucí(ho) katedry	podpis děkana(ky)

Prohlášení

Prohlašuji, že jsem diplomovou práci s názvem „Detekční systémy pro rozpoznání obličejů a vzorců chování s možností nasazení na fotbalových stadionech s využitím pro zamezení vstupu nežádoucích osob, prevenci vzniku a forenzního šetření mimořádných událostí“ vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Kladně dne 08.05.2020

……

Bc. Tomáš Švagr

Poděkování

Rád bych poděkoval vedoucímu mé práce panu Ing. Václavu Navrátilovi za odborné vedení při sepisování této práce. Děkuji především za jeho pečlivost při čtení každé věty a perfekcionismus který pomohl vybrousit tuto práci do finální podoby. Poděkování patří také týmu programátorů spol. Colsys s.r.o., za jejich odlišný pohled na svět a jejich podměty, které tuto práci posunuly o další úroveň.

Děkuji také autorům knih, výzkumů a odborných článků ze kterých jsem mohl čerpat a staly se zdrojem této práce. Děkuji také panu Petru Ludwigovi, jehož články, knihy a semináře byly motivací pro dopsání této práce.

Abstrakt

Práce je věnována kamerovým systémům s možností detekce tváře a její rozpoznání s využitím pro zvýšení bezpečnosti na fotbalových stadionech. Je zde srovnáno několik výrobců systémů se stručným popisem a pomocí bazické varianty vybrán nejvhodnější z nich. Dále se práce zabývá samotnou implementací tohoto systému na konkrétní stadion. Smysluplnost řešení je ověřena analýzou užitku varianty.

Pro uvedení do problematiky se práce ve své první polovině zabývá popisem metod pro rozpoznání obličeje, vysvětluje pojem biometrie a uvádí legislativu, která se tímto zabývá.

Klíčová slova

Biometrie, antropometrie, rozpoznání obličeje, kamerový systém, fotbalový stadion, bezpečnost, bazická varianta, analýza užitku.

Abstract

This work is dedicated to camera systems with face recognition used for security on soccer stadiums. Few picked manufacturers were compared and using basic variance method, the most relevant one was selected. Furthermore, this work is dealing with implementation of selected system on an actual stadium. Relevance of this solution is verified using variance analysis.

In spite of introduction into the subject, the first half of the work is dedicated to description of face recognition methods, optical biometry and the legislation relating the subject.

Keywords

Biometrics, anthropometry, face recognition, camera system, football stadium, security, basic variant, utility analysis.

Obsah

Použité zkratky

IP – Internet protokol

SW – Software (počítačový program)

PTV – Průmyslová televize

DB – Databáze

FBI – Federal Bureau of Investigartion

AFIS – Automated fingerprint Identification Systém

PCA – Principal Component Analysis

ASM – Active Shape Model

AAM – Active Appearance Model

ICP – Interactive Closest Point

PZTS – Poplachový zabezpečovací tísňový systém

EPS – Elektronická požární signalizace

EKV – Elektronická kontrola vstupu

CCTV – Closed Circuit Television (uzavřené televizní okruhy)

DVR – Digital Video Recorder

FAČR – Fotbalová asociace České republiky

MD – Man Day (jednotka pracnosti)

1 Úvod

Na tribunách stadionů není bezpečno. Rodiny s dětmi se bojí jít na fotbal. Toto jsou věty, které často slyšíme ve spojení s fotbalovými utkáními. Přispívají tomu události poslední doby, kdy došlo k několika zraněním, a to bohužel i vážným, ke kterým došlo při násilném chování fotbalových fanoušků na utkáních. Jelikož na fotbalová utkání nejvyšších soutěží chodí divácké návštěvy v řádech tisíců až desetitisíců diváků, je to problém, který je třeba efektivně řešit.

Zlepšení situace v oblasti bezpečnosti lze docílit obecně dvěma přístupy. První možností je represivní přístup tedy až reakce na již vzniklou událost. Například policejní zákrok. Nebo druhá možnost, předcházet těmto situacím čili zajistit dostatečnou prevenci. Všeobecně platí, že prevence je nad všechna řešení. Otázkou je, jaká prevence by měla být zvolena, aby bylo dosaženo cíle co nejefektivněji.

Tato práce může být právě jednou z odpovědí na tuto otázku. Práce je koncipována jako případová studie nasazení kamerového systému s možností rozpoznání tváře na stadion s napojením na vstupní turnikety a automatickým vyhodnocením, zda osoba bude vpuštěna či nikoli. Než jsem ale mohl přistoupit k samotnému návrhu řešení bylo třeba analyzovat jaké možnosti kamerových systémů trh nabízí, jaké existují přístupy k rozeznávání tváře, nebo jak je dané téma zpracováno v české legislativě. Po výběru vhodného systému, prostudování legislativy, objektivní analýze nakolik jsou utkání české ligy pro diváky riziková, jsem přistoupil k popisu navrhovaného řešení. To spočívá v modelovém příkladu nasazení kamerového systému doplněného o software určený k rozpoznání tváře na konkrétní stadion. Tento systém má být propojen s centrální databází nežádoucích osob a automaticky ovládat vstupní turnikety. Implementace takového systému sebou nese ale řadu dalších výhod, o kterých se zmiňuji v této práci.

Mimo výše uvedené také čtenář této práce získá v teoretické části základní povědomí v oblasti biometrie, pochopí jednotlivé pojmy a k čemu lze tuto vědní oblast obecně využít při řešení bezpečnosti.

2 Cíle a hypotézy

Cílem práce je provedení rešerše výrobců kamerových systémů, ze kterých bude následně pomocí metody bazické varianty vybrán nejvhodnější pro modelaci nasazení takového systému ve spojení s detekcí tváře na fotbalový stadion. Dále bude v práci vyhodnocena efektivita přínosu navrhované varianty.

Hypotéza 1

Navrhované řešení pro zvýšení bezpečnosti na fotbalových stadionech nepřinese zvýšení bezpečnosti.

Hypotéza 2

Navrhované řešení s automatickým rozpoznáním tváře zvýší počet záchytu nežádoucích osob u vstupu na stadiony.

Hypotéza 3

V desetiletém horizontu přinese navrhované řešení finanční úsporu.

3 Úvod do biometrie

Biometrika a biometrie se těší velké pozornosti zejména v několika posledních letech až několika málo desetiletích, ale její počátky sahají až do doby před naším letopočtem. V této kapitole se dozvíte, jak vznikaly první biometrická měření, k čemu se využívala, jaké jsou výhody a nevýhody biometrie a co znamená pojem Biometrický systém.

3.1 Historie

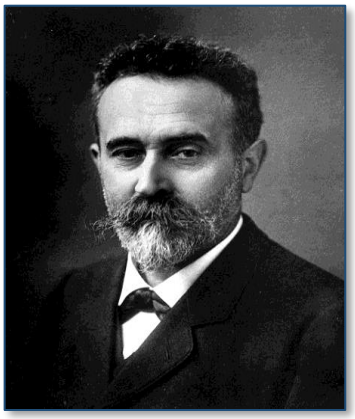
Již od pradávna je známo užívání biometrických vlastností. Běžně se denně setkáváme s biometrickým rozpoznáváním, aniž bychom si toho byly vědomi. Osoby v našem okolí rozeznáváme podle hlasu, obličeje, ale například i podle způsobu chůze. Tyto vlastnosti se souhrnně označují jako lidské biometrické vlastnosti. Tyto vlastnosti můžeme ale zaznamenat a dále strojově zpracovat, jsou to signály nesoucí informaci o biometrických vlastnostech. [1]

První dochované známky o použití biometrických údajů pochází z Číny ze 14. století. Jedná se však o nepřímé důkazy použití biometrických údajů. Nalezeny byly kresby na skalních stěnách, které znázorňovaly strukturu podobající se otisku prstu, nebo otisk prstu na keramice. To mohlo v minulosti sloužit jako důkaz autorství. [1]

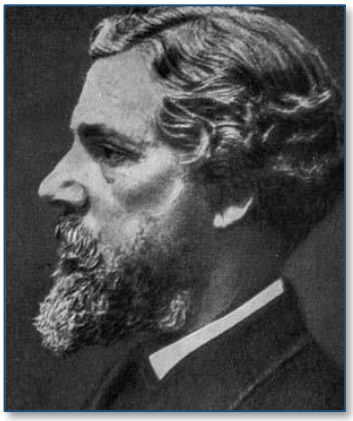
První průkazné použití biometrie pochází z 19. století. Jedná se o počátek využívání otisků prstů převážně v kriminalistice. Z dochovaných materiálů se jedná konkrétně o následující příklady: [1]

- 1858 – William James Herschel – Anglický guvernér působící v Indii. Zde začal používat otisky prstů u zaměstnanců dráhy, kteří byli většinou negramotní, a tak bylo nemožné, aby se podepsali například na výplatní pásky. Herschel nechal každého zaměstnance otisknout svůj palec na originál výplatní pásky, čímž bylo stvrzena identita pracovníka. Při této příležitosti začal otisky prstů shromažďovat a dále je zkoumal, to vedlo k jednomu z historicky prvních děl o původu otisku prstů. [2] [1]

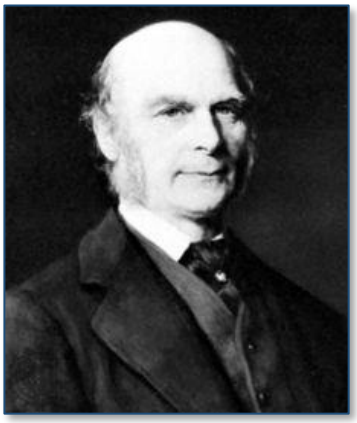
- 1880 – Alphonse Bertillon jako první na světě vypracoval použitelnou metodu individuální identifikace zločinců postavenou na vědeckém základě. Jeho metoda se zabývala poměřováním jednotlivých částí lidského těla. Svou novou metodu nazval antropometrií. Můžeme se také setkat s pojmenováním "bertillionage" – bertillonáž, takto označili metodu ve svých článcích novináři. [3]
- 1888 - Francis Galton byl anglický přírodovědec, který ve své publikaci použil teoreticko – vědecké základy daktyloskopie, vědy zabývající se otisky prstů. Matematickými metodami vypočítal, že existuje celkem 64 miliard různých variant uspořádání papilárních linií. Tím Galton prakticky vyloučil možnost výskytu dvou jedinců se stejným otiskem prstu. [4]
- 1924 – FBI zakládá oddělení identifikace otisků prstů [1]
- 1965 – Poprvé použit daktyloskopický systém AFIS (810 tisíc otisků prstů) [5]
- 2000 – Systém AFIS obsahuje 4 miliony „Desetic“ otisků prstů (otisky všech prstů obou rukou). Denně dochází průměrně k 50 tisícům prohledávání. Reakce na vyhledávání je přibližně 2 hodiny. [1] [5]
- 2010 – Systém AFIS obsahuje okolo 66 milionů „Desetic“ otisků prstů. Denně dochází průměrně k 168 tisícům prohledávání. Reakce na vyhledání je okolo 1 hodiny a v urgentních případech je možné toto provést i během 10 minut. [1] [5]



Obrázek 3: Alphonse Bertillon (3)



Obrázek 2: William James Herschel [37]



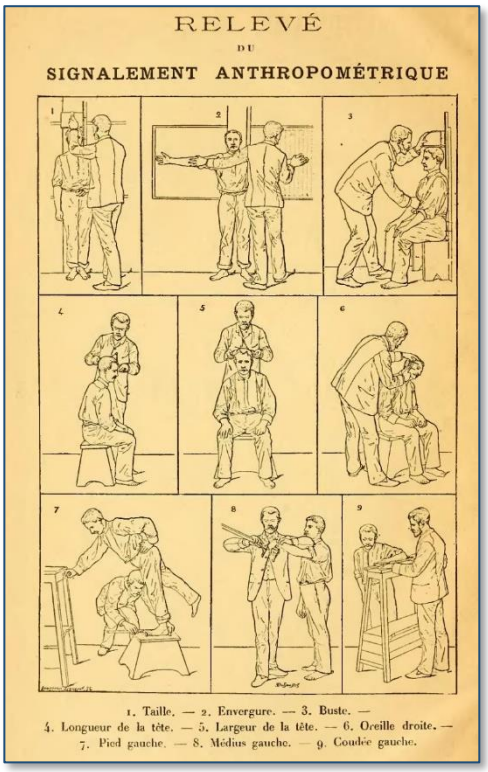
Obrázek 1: Francis Galton [36]

3.2 Antropometrie

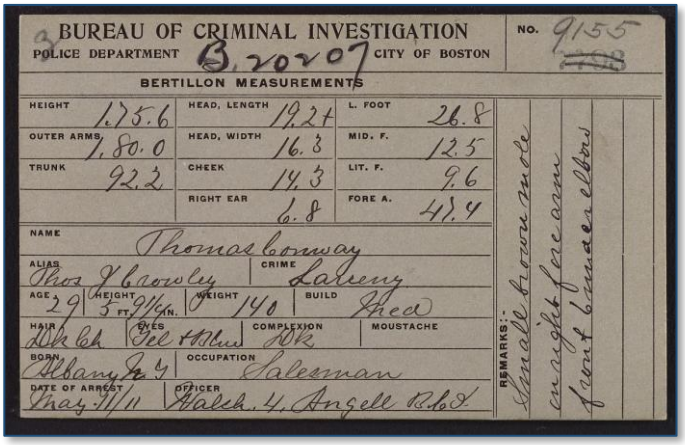
Pojem Antropometrie pojmenovává metodu měření různých lidských rozměrů, jejich záznamu a následnému použití při identifikaci, nebo verifikaci osoby. V rámci zkoumání bylo prokázáno, že po 20. roce života se tělesné rozměry nemění. S rostoucím počtem korektně změřených tělesných rozměrů klesá riziko záměny osob. Tímto způsobem je možné osobu zcela jistě identifikovat, či verifikovat. [1] [6]

Měření se provádělo na jedenácti různých tělesných rozměrech (obrázek 4,5):

- Tělesná výška
- Délka natažené paže
- Výška v sedu
- Délka hlavy
- Šířka hlavy
- Délka pravého ucha
- Šířka pravého ucha
- Délka levé nohy
- Délka levého prostředníčku
- Délka levého malíčku
- Délka levého předloktí



Obrázek 4: Měření tělesných rozměrů [38]



Obrázek 5: Karta se zápisem o provedených měření [39]

3.3 Biometrie

Pojmenování Biometrie má svůj původ v řečtině, kde se skládá ze slov *„bios“ a „metron“.* První ze slov znamená život a druhé měřit. V trochu přeneseném významu můžeme toto spojení přeložit jako *„měření života“.* Biometrie tedy měří určité charakteristiky člověka. [1]

Biometrii můžeme charakterizovat jako obor, který se zaměřuje na měření a vyhodnocování biologických charakteristik a charakteristik chování lidí. [1]

Pro efektivní identifikaci osoby je nutná jedinečnost fyzických a psychických vlastností, které jsou pro každého člověka přirozené už od narození a je téměř nemožné je absolutně napodobit nebo pozměnit. [7]

3.3.1 Biometrické vlastnosti

Biometrické systémy snímají vlastnosti, které lze obecně rozdělit na anatomické (statické) a behaviorální (dynamické). [7]

Pro anatomické vlastnosti platí, že jeden pevný rys je jednou konkrétní biometrickou vlastností. Tato vlastnost je vždy přítomna, bez snadného ovlivnění stavu člověka. Metoda analýzy anatomických vlastností je také označována jako *statická metoda*. [1] [8]

Behaviorální, nebo také dynamické vlastnosti jsou typické tím, že jsou spojeny s nějakou akcí uživatele. Každé snímání jednotlivé vlastnosti může vést ke zcela rozdílným biometrickým vzorkům. To se v praxi nezřídka také stává. Metoda analýzy dynamických vlastností se nazývá *dynamická metoda*. [9] [10]

Anatomické vlastnosti:

- Otisk prstu
- Geometrie ruky
- Rozpoznání obličeje
- Oční duhovka
- Oční sítnice
- Lůžko nehtu
- DNA

Behaviorální vlastnosti:

- Hlas, Řeč
- Dynamika podpisu
- Chůze
- Mimika obličeje
- Dynamika stisku klávesy

Tabulka 1: Přehled základních biometrik (8)

Biometrické vlastnoti ve vztahu k přesnosti a ceně			
Typ	**Biometrika**	**Přesnost**	**Cena**
Anatomické (statické)	Otisk prstu	★ ★ ★	★
	Geometrie ruky	★ ★	★ ★
	Rozpoznání obličeje	★ ★	★ ★
	Oční duhovka	★ ★ ★	★ ★ ★
	Oční sítnice	★ ★ ★	★ ★ ★
	Lůžko nehtu	★ ★ ★	★ ★
	DNA	★ ★ ★	★ ★ ★
Behaviorální (dinamické)	Hlas, Řeč	★	★
	Dynamika podpisu	★ ★	★
	Chůze	★	★
	Mimika obličeje	★	★
	Dynamika stisku klávesy	★ ★	★
Nízká ★	Střední ★ ★	Vysoká ★ ★ ★	

3.3.2 Výhody biometrie

K hlavním výhodám biometrie patří jednoznačně jednoduchost uživatelského užití. V podstatě stačí přijít ke čtečce biometrických údajů, přiložit svou dlaň, prst, podívat se do kamery apod. Odpadá nutnost pamatovat si heslo, které je následně potřeba vyťukat na klávesnici. Není nutné zdlouhavé seznamování s návody. Velkým plusem pro biometrii je fakt, že se biometrické údaje těžko falšují. Samozřejmě, že je to možné, ale dobře nastavený a implementovaný systém by tomuto případu měl zcela zabránit. [11]

Výčet výhod biometrie tedy může být následující:

- napomáhá ke zvýšení bezpečnosti,
- pro svou složitost odrazuje útočníky od podvodů,
- biometrie nemůže být lehce přenesena, zapomenuta, či ztracena,
- eliminuje pokusy o popření identity,
- zvyšuje pohodlí. [1]

3.3.3 Nevýhody biometrie

Navzdory tomu, že ve světě biometrie došlo za posledních několik let ke značnému posunu, nemůžeme říct, že je biometrie stoprocentně spolehlivá. Důvodem je, že nikdy nedokážeme dodat naprosto stejný vzorek, jako je uložený v šabloně. Například prst přiložíme ke čtečce vždy pod nepatrně jiným úhlem, pokožka je vždy jinak vlhká, a podobně.

Při snaze využít biometrii narážíme také na netechnické překážky. Ty mohou být např., že ne každý je schopen, nebo ochoten poskytnou své biometrické údaje, a to ať z etických nebo náboženských důvodů. Těchto případů není mnoho a jedná se spíše o hraniční případy, ale i na takové je třeba myslet. Masové rozšíření jednoho způsobu biometriky by také mohlo znamenat, že bude možné propojit jinak nepropojitelné databáze informací. Každá mince má dvě strany – a tato nevýhoda se může proměnit ve značnou výhodu, neboť biometrika je schopna nabídnout způsoby ochrany, které vám ostatní metody ani zdaleka nezajistí. Je ale žádoucí, aby se s touto technologií nakládalo odpovídajícím způsobem a s opatrností.

Další nevýhodou může být i pomalost systému využívající biometriku. A úplně na závěr se zmiňme ještě o jednom obecném riziku, které se stává větším problémem, jak kvalita celé biometriky roste. Jedná se o možnost identifikace na dálku. Třeba oční duhovka se dá snímat bez vědomí majitele, stejně tak otisky prstů za sebou zanecháváme na každém kroku. Dále není problém získat informace o DNA z vlasů nebo zbytků slin, které necháme třeba na příboru nebo sklenici v restauraci… I toto jsou otázky, které by měli mít tvůrci biometrických systémů na paměti – ať již z hlediska etického nebo bezpečnostního. [11] [1]

Výčet nevýhod může být následující:

- možné zneužití biometrických údajů (například ze zanechaných otisků prstů na předmětu),
- neochota poskytnout biometrické údaje,
- vysoké nároky na výpočetní výkon systému, který biometrické údaje zpracovává.

3.4 Biometrický systém

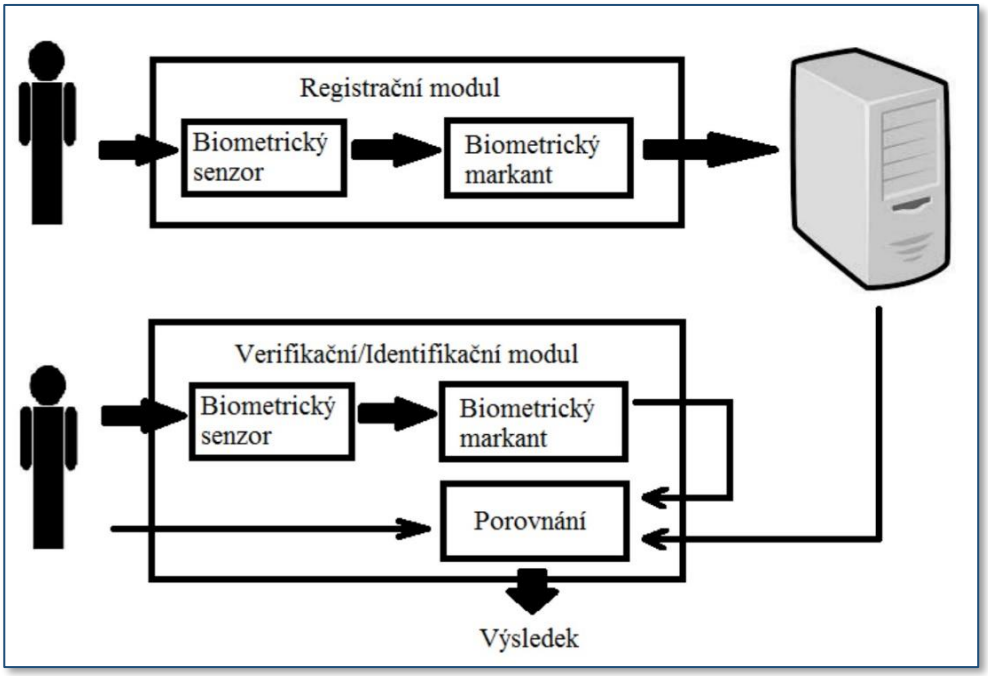
Biometrické systémy následně slouží k automatické identifikaci, nebo ověření identity člověka na základě jeho naměřených unikátních fyziologických, nebo behaviorálních hodnot. [1] [9]

Biometrie ale není zcela jednoduchá disciplína. Při zpracování biometrických signálů a informací pracujeme s řadou problémů, jakými například jsou mezitřídní a vnitrotřídní variabilita, segmentace, zašuměný vstup, výkonnost systému (chyby, rychlost, náklady), jednoznačnost biometrické vlastnosti, fúze několika biometrických vlastností, útoky na biometrický systém, otázka privátních dat a další. [9]

Biometrický systém se skládá ze dvou modulů – registrační modul a verifikační/identifikační modul. Zpravidla jsou tyto dva moduly dodávány jako ucelené řešení. Oba moduly obsahují biometrický senzor, který slouží k získání biometrického vzorku a převedení do digitálního světa. V obou modulech se také

shodně nachází tzv. biometrický markant, což jsou již extrahované rysy i biometrického vzorku na vstupu. Tyto biometrické rysy jsou následně s pomocí registračního modulu uloženy do databáze. Jedná se o jednorázovou registraci informace při jejím následném používání. Verifikační/identifikační modul provede totéž co registrační modul, pouze neukládá biometrické rysy do databáze. Tento modul data z databáze načítá a následně porovná s aktuálně získanými biometrickými rysy. Po provedeném porovnání je stanoven výsledek. [1]

Jako každý systém, má i biometrický systém slabá místa. Může dojít např. k zmanipulování senzoru podvrhem biometrické vlastnosti, replikaci starých dat, ke změně dat v databázi a další. [1]



Obrázek 6: Znázornění biometrického systému [1]

3.4.1 Identita, identifikace a verifikace

Každý den každý z nás automaticky rozeznává u jiných osob obličej, postavu, rty, hlas, chůzi či písmo. K tomuto rozpoznávání dochází automaticky v lidském mozku. Strojové rozpoznávání se snaží pracovat na podobných principech. Rozpoznávání jiných osob je založeno na jednoznačné a jedinečné identitě jedince. Můžeme tedy říct, že identita je jednoznačná charakteristika každého z nás. Pod pojmem identita míníme fyzickou identitu, u které neexistuje na světě člověk, který by ji měl shodnou s jiným člověkem. Pro pojem elektronická identita toto tvrzení neplatí.

V elektronickém světě si můžeme vytvořit libovolný počet identit. K pojmu identita se váží další dva pojmy – identifikace a verifikace. Mnoho lidí považuje tyto dva pojmy milně za shodné. [1] [10]

Při verifikaci předkládá svoji totožnost a tu následně potvrzuje znalostí nějakého sdíleného tajemství. Pro verifikaci platí, že uživatel sděluje svou elektronickou identitu, např. při přihlášení do počítače. Na základě sdělení elektronické identity dojde k ověření fyzické identity. Verifikaci se také říká porovnání 1:1, neboť dochází k porovnání jedněch vstupních dat s jedněmi daty uloženými do databáze. [9] [12]

Identifikace slouží ke zjištění identity osoby. Osoba zadá systému pouze svou biometrickou vlastnost bez sdělení své identity. Systém má následně za úkol rozpoznat identitu uživatele. Dochází k porovnání vzorku ze vstupu s celou databází uložených vzorků, výsledek je bud *identita nalezena*, nebo *identita nenalezena*. Tento proces je poměrně časově ale i výkonově náročný, přičemž je tato náročnost úměrná velikosti databáze. U velkých databází se pro úsporu času a výkonu používá rozdělení do podkategorií. Např. databáze otisků prstů je rozdělena do jednotlivých tříd otisků prstů. Identifikaci se říká porovnáni 1:N. Jedním z příkladů systému pro identifikaci je například daktyloskopický systém AFIS.

3.4.2 Unimodální a multimodální systémy

Dále ve spojitosti s biometrickými vlastnosti rozlišujeme unimodální a multimodální systémy. Unimodální systémy využívají právě jednu biometrickou vlastnost. Nevýhodou těchto systémů může být nižší spolehlivost, vyšší náchylnost k vnějšímu útoku. Výhodou těchto systémů je ale jejich nižší pořizovací cena.
V praxi se většinou setkáváme právě s těmito systémy. Multimodální systémy naopak využívají kombinaci biometrických vlastností (pozorování obličeje, oční duhovka) nebo kombinaci více příznaků jedné biometrické vlastnosti (statické a dynamické rozpoznání podpisu). Výhodou těchto systémů je jejich vyšší spolehlivost a poměrně velká robustnost vůči falšování pokusů k útoku. Jejich nevýhodou je vyšší cena oproti prvnímu druhu systému. [1] [10]

Biometrické vlastnosti sebou nesou také své charakteristiky, které jsou většinou velmi důležité při rozhodování pro konkrétní biometrický systém. Mezi základní charakteristiky patří: [10]

- *„univerzalita – každá osoba by tuto vlastnost měla mít*
- *jedinečnost – žádné dvě osoby nesmí vlastnit stejnou vlastnost*
- *konstantnost – vlastnost zůstává neměnná v čase*
- *získatelnost – vlastnost je kvantitativně měřitelná*
- *akceptace – ochota lidí si nasnímat biometrickou vlastnost*
- *finanční náklady na pořízení – cenové náklady na pořízení systému.“* [10]

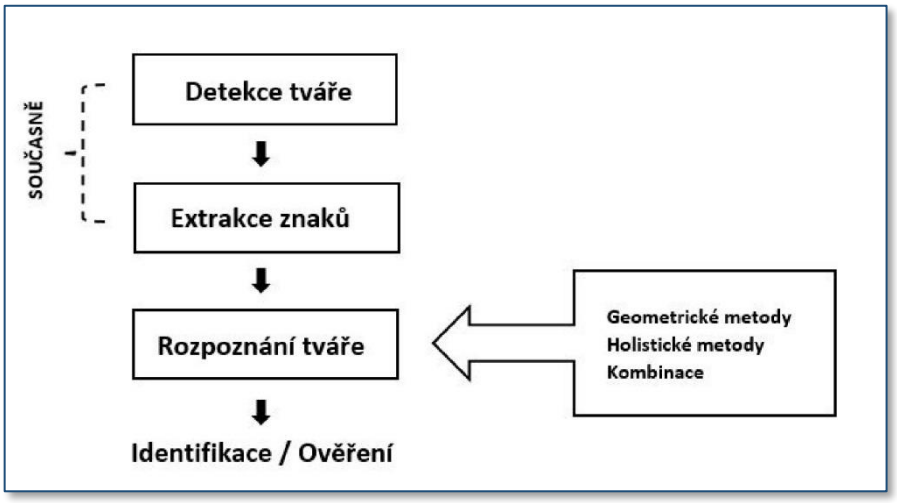
Mezi další faktory lze také zařadit dostupnost, údržbu, provedení, ale také anonymitu. Jedním z velmi důležitých faktorů je také spolehlivost. Měly bychom vědět, co se stane při změně například osvětlení, teploty, po použití brýlí a podobně. [10]

4 Biometrika rozpoznání obličeje

Každý obličej je jedinečný, ale každý také vykazuje velkou vnitrotřídní variabilitu, např. při změně gestikulace. Vedle vnitrotřídní variability má v mnoha případech i vyšší procento výskytu mezitřídní variability, např. dvojčata, nebo dvojníci. Aby nedocházelo k podvodům s fotografiemi, či bustou hlavy, lze systém doplnit o možnost pořízení termo snímku obličeje. Samotné termosnímky lze použít jako samostatnou rozpoznávací metodu. [1] V posledních letech byla vyvinuta řada metod, které rozpoznávání obličeje zvládají velmi dobře. Detekce obličeje byla přitom ještě před několika lety považována za jednu z nejsložitějších a nejnáročnějších úloh v oblasti umělé inteligence. [13]

4.1 Obecný postup rozpoznávání

Proces rozpoznání obličeje lze obecně rozdělit do několika kroků. Prvním krokem je přítomnost videozáznamu, či statické fotografie, ze které je záměr obličej rozpoznat. Následně je systémem vyhodnocena přítomnost tváře. Pokud systém detekuje obličej, provede následně extrakci důležitých znaků pro porovnání.
V praxi se detekce obličeje a extrakce bodů dějí současně. [14] [15]



Obrázek 7: Schéma postupu rozpoznávání tváře [14]

Znaky jsou ve většině případů extrahovány pomocí integrální projekce. V této metodě se obraz určený pro extrahování označí jako $O(x, y)$. Integrální projekce se dále rozděluje na dvě podskupiny: Vertikální integrální projekce a Horizontální vertikální projekce. [14] [15] [12]

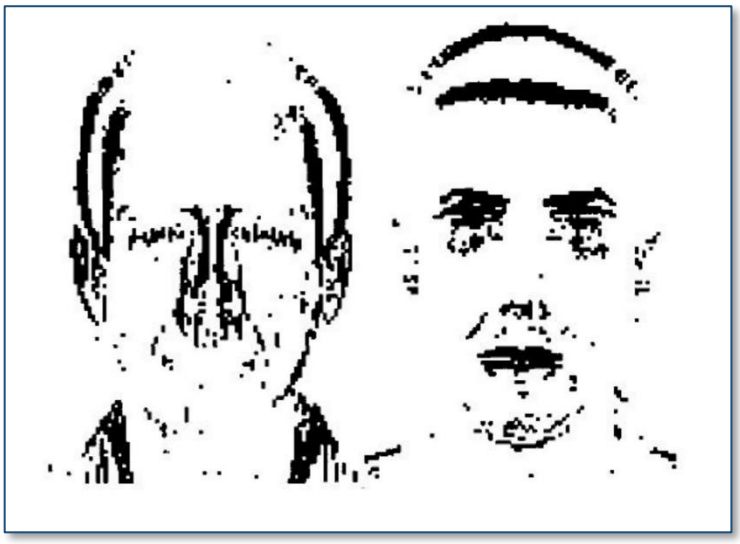
Definice vertikální integrální projekce:

$$V(x) = \sum_{y=y1}^{y2} O(x, y)$$

Definice horizontální integrální projekce:

$$H(y) = \sum_{x=x1}^{x2} O(x, y)$$

Takto předpřipravená tvář se stává vstupem pro následné porovnání a vyhledání shody pomocí jedné z metod. Jednotlivé metody jsou popsány níže v samostatných kapitolách. [14] [15]



Obrázek 8: Vertikální projekce (vlevo) a horizontální projekce (vpravo) [14]

4.2 Metody pro rozpoznávání obličeje

Metody pro rozpoznání obličeje můžeme rozdělit do dvou skupin. Pro první skupinu platí, že obsahují metody založené na porovnání s maximální možnou sadou šablon, obrazů, nebo různých modelů. Velmi důležitá pro tuto metodu je sada šablon tvořena různými nástroji. Souhrnně označujeme tyto metody jako holistické. Druhou skupinou jsou metody, které jsou založeny na pozorování výrazných tělesných znaků. Tyto znaky mají v každé tváři unikátní geometrii (vzájemné postavení). Tyto metody se označují jako geometrické. V praxi jsou tyto dvě skupiny metod většinou kombinovány pro dosažení co nejlepší přesnosti vyhledání. [14] [15]

4.2.1 Holistické metody

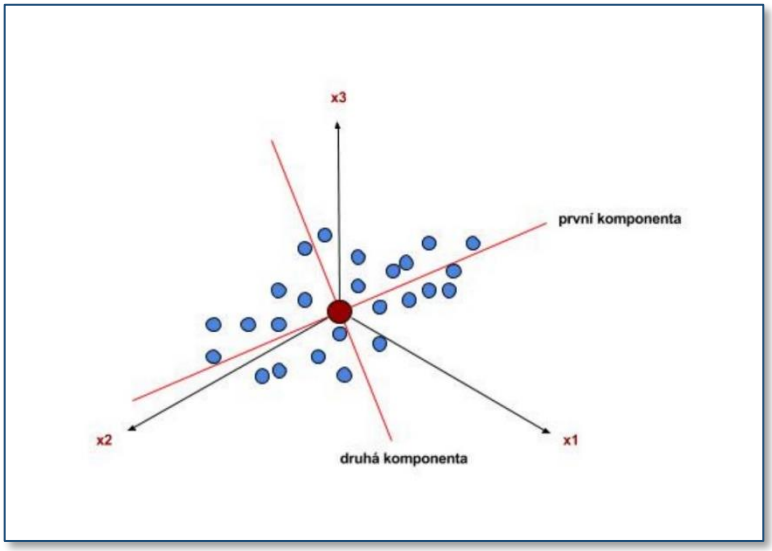
Slovo Holismus pochází z řeckého slova „holos“, což znamená v překladu znamená celek. Už z názvu je tedy patrné, že holistické metody porovnávají obličej jako celek, bod po bodu. Největší výhodou těchto metod je, že není vynechána žádná část obličeje a nedochází tak k možnému opomenutí některé části, která by mohla v porovnání pomoci. To se ale zároveň stává nevýhodou, jelikož je kladen velký nárok na výpočetní výkon, oproti metodám, které porovnávají pouze jednotlivé části obličeje. Dnešní výkon výpočetních systémů ale dokáže tuto nevýhodu ve velké míře ošetřit. Některé z metod jsou již nyní zdokonaleny tak, že poskytují vysoce spolehlivé výsledky. [14] [15]

4.2.1.1 Metody statistické

V této metodě je obraz znázorněn d příznakem a pohlíží se tedy na něj jako na datový bod v d rozměrném prostoru. Statistické metody se používají k extrakci a analýze požadovaných bodů, a to z toho důvodu, jelikož množství informací potřebné k určení soudnic a vlastností bodů je obrovské a je potřeba je zredukovat. Nástroj správně a vhodně urči obličejový prostor v obraze a z něj extrahuje důležité základní informace. [14] [15]

Často používaná statistická metoda je Analýza hlavních komponent (PCA). Tato metoda je určena pro redukci rozměrů mnohorozměrných dat. Tato analýza pracuje tak, že extrahuje požadované množství hlavních komponent, což jsou lineární kombinace původních proměnných. *„První hlavní komponenta je obvykle lineární kombinace z originálních rozměrů s nejvyšší odchylkou. Druhá komponenta je kolmá na první a popisuje rozptyl, který nezahrnuje komponenta první. Třetí je kolmá na první a druhou a popisuje rozptyl, který není zahrnutý ani v první ani v druhé komponentě. N-tá hlavní komponenta je s maximální odchylkou kolmá na n-1 komponentu. Hlavní komponenty jsou seřazeny podle důležitosti, největší rozptyl, a tedy variabilita v obraze vždy zatěžuje první hlavní komponentu.“* [14]

Další ze zástupců statistických metod jsou např. Diskrétní kosinová transformace nebo Goborova vlnková transformace.



Obrázek 9: Grafické znázornění grafických komponent při použití PCA [1]

4.2.1.2 Metody založené na porovnávání s šablonami

Předchozí metoda funguje pro libovolné rozpoznávání vzorků, v podstatě je jedno, jestli je na vstupu obraz obličeje, nebo čehokoli jiného. Metody založené na porovnání šablony se liší v tom, že se prvotně snaží obrázek identifikovat jako obličej. V obraze se snaží nalézt např. oči, ústa, obočí nos atd. a až následně hledá podobnost.

Šablona pro porovnání se skládá ze dvou až tří desítek bodů, které si v obličejích vzájemně významově odpovídají. Jedná se např. o uši, nos, ústa atd. Pro tyto

metody se vytváří tzv. testovací sady snímků. U těchto snímků se ve fázi předzpracování ručně určí pozice všech bodů šablony. Z této testovací sady šablon si model zapamatuje vzájemnou polohu bodů. Zástupci těchto metod jsou ASM (Active Shape Model) a AAM (Active Appearance Model). [1]

- Metoda ASM – „šablona se skládá pouze z bodů a hran mezi nimi. Tyto hrany se snaží interaktivně namapovat na hranový obraz zkoumaného snímku. Informace o textuře se extrahují až po konvergenci šablony. Textura je pak deformována v závislosti na výsledném tvaru šablony. „ [1]

Obrázek 10: Grafická ukázka bodů v modelu ASM [41]

- Metoda AAM – *„šablona se skládá nejen z bodů a hran, ale i z informací o textuře uvnitř šablony. Tvar šablony a texturní informace jsou v procesu iterování šablony používány společně, proto obvykle dosahuje lepších výsledků.“* [1]

Obrázek 11: Grafická ukázka bodů v modelu AAM [42]

4.2.2 Geometrické metody

Na geometrických metodách byly založeny nejstarší metody sloužící k rozpoznání tváře. Geometrické metody jsou založeny na jedinečnosti geometrie a na vzájemném postavení podstatných struktur tváře. Podstatné znaky lze popsat číselným vektorem, ve kterém jsou obsaženy informace o jejich pozici a velikosti. Aby byla metoda co nejpřesnější je vhodné dodržovat několik základních podmínek, jako jsou např. co nejjednodušší odhad, malá závislost na drobných změnách ve výrazu obličeje a malá závislost na světelných podmínkách. [16]

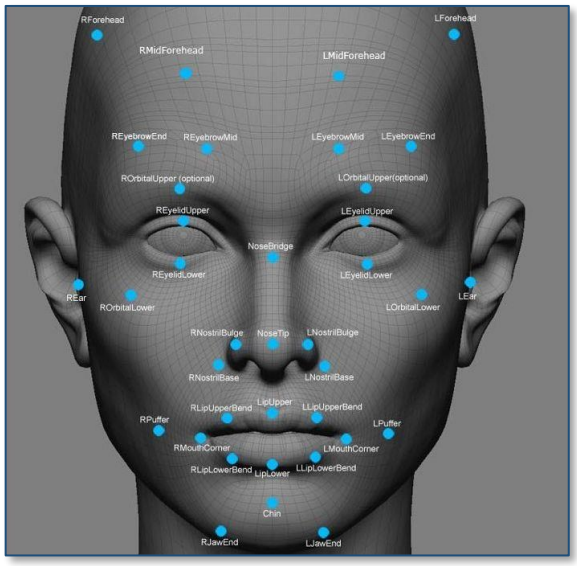
Složitým úkolem v rámci těchto metod je normalizace obličeje. Normalizace je v podstatě proces, při kterém je zajištěno, že extrahované znaky jsou nezávislé na apozici, měřítku, nebo rotaci snímaného obličeje. Základem pro to je stanovit počáteční souřadnice detekovaného obličeje, následně je stanoven rozměr mezi očima, spolu se směrem osy, která oči spojuje. Toto zajistí eliminaci závislosti na rotaci obličeje. [16]

Výhodou geometrických metod je velmi rychlé rozpoznání a zařazení vstupního obličeje, další z výhod je tolerance na změnách ve vstupním obraze. U těchto metod je na druhé straně ale nevýhodou to, že je složité určit, které znaky jsou významné a jejich následná automatická detekce. [17]

4.2.2.1 Metoda porovnávající obličejové vektory

Jedna z prvních metod využívající vektory byla vyvinuta Takeo Kanade v roce 1973. Metoda zpracovávala obraz tak, že z tváře získala vektor šestnácti obličejových parametrů, následně mezi nimi zahrnula poměry vzdáleností obličejových znaků, jejich umístění v obličeji a úhly, které vzájemně svírají. Tato metoda dosahovala na svém začátku úspěšnosti okolo 75 %, kdy byla použita DB s dvaceti obličeji. Tato metoda byla nadále vyvíjena a zlepšována přidáváním měřených parametrů a zvětšováním DB, což vedlo k zvýšení její úspěšnosti. [17] [14]

Při použití DB s 685 obličeji, kdy každý patřil jedné osobě a znakového vektoru odvozeného z třiceti pěti obličejových znaků bylo dosaženo úspěšnosti 95 %. Značnou nevýhodou této metody je, že je nutné ručně extrahovat jednotlivé obličejové znaky. [14]

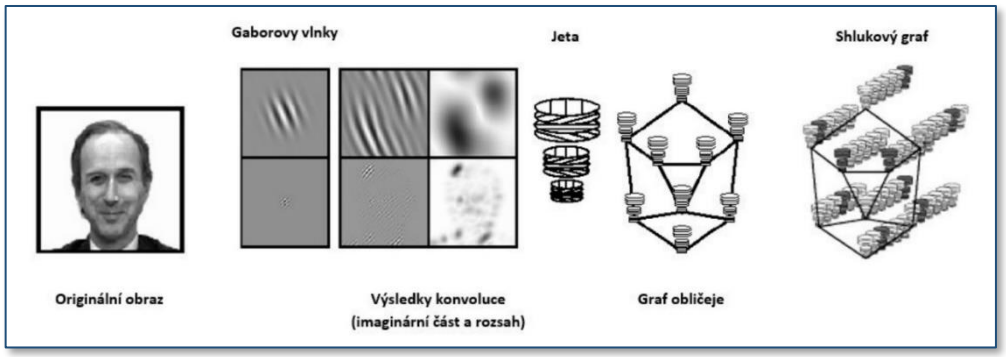


Obrázek 12: Extrakce obličejových bodů [44]

4.2.2.2 Metoda shlukových grafů

Metoda shlukování grafů bývá poměrně často také využívána. Tato metoda je založena na Gaborové vlnové transformaci. Výhodou metody je primárně možnost rozlišení tváře i při změně podmínek v okolí, nebo samotného obrazu. To zajišťují právě použité vlnky. Metoda obličej reprezentuje jako graf, kde jeho uzly odpovídají pozici jednotlivých významných struktur v obličeji a hrany následně tyto uzly propojují. [14]

Obrázek níže zachycuje proces získávání shlukového grafu od konvoluce s Gaborovými vlnkami po tvorbu samotného grafu. [14]

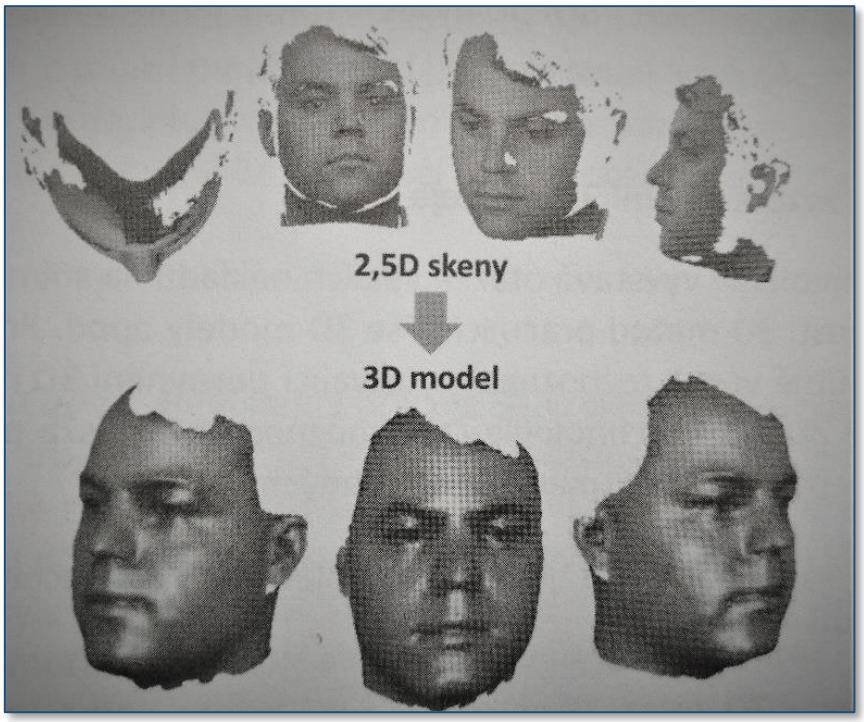


Obrázek 13: Postup získávání shlukového grafu z obličeje [14]

4.2.3 Metody na základě 3D snímku

Výše zmiňované metody se týkají metod na základě 2D. Při porovnání projekce do 2D roviny ale dochází ke ztrátě podstatné části dat. 2D metody se pokouší tento nedostatek eliminovat simulací využitím předpokládaného tvaru obličeje. Skutečné 3D snímání obličeje nabízí mnohem širší možnosti. [1]

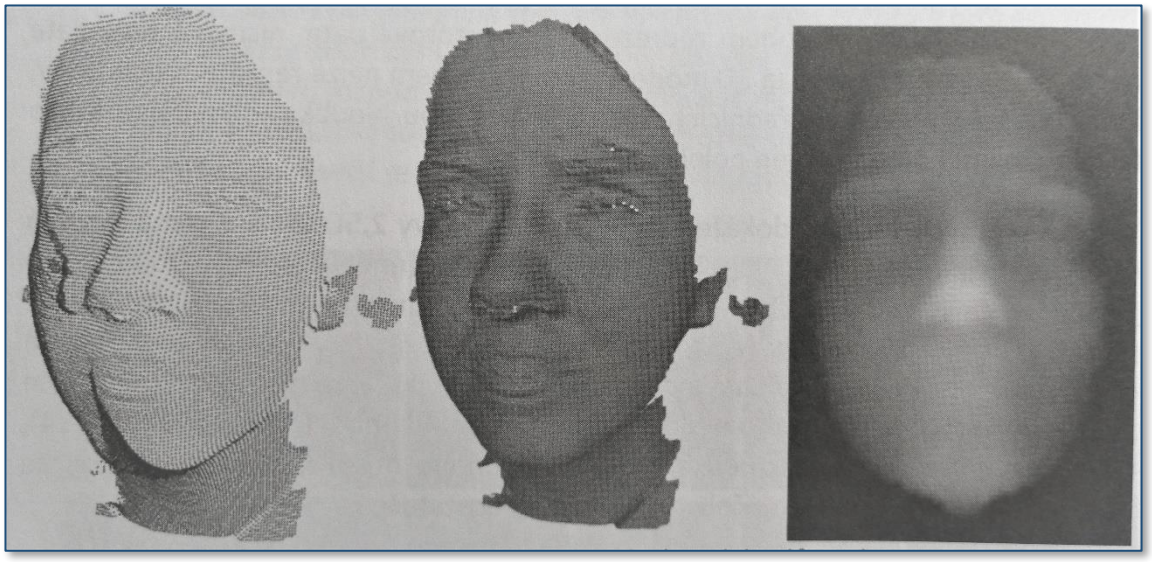
Zásadní technologický rozdíl mezi 2D a 3D je v konstrukci snímacího zařízení. Zatímco pro 2D je dostatečný jakýkoli fotoaparát, nebo kamera, 3D vyžaduje specifické zařízení. Tato zařízení obvykle fungují na principech 2,5D skeneru. Tento skener je v podstatě 2D obraz nesoucí sebou informaci o hloubce každého bodu. Tímto však nelze vytvořit plnohodnotný 3D model, jelikož nelze reprezentovat body ležící na stejných souřadnicích, ale s jinou hloubkou. Například u tvaru koule by takto vznikl jen obrazec polokoule. Pro sestavení plnohodnotného 3D modelu se používá několik 2,5D skenerů rozmístěných v prostoru. Informace z nich se následně složí do 3D modelu. V praxi se však obvykle používá varianta snímání z jednoho místa a předpokládá se, že získaná informace bude pro účely rozpoznání dostatečná. [1]



Obrázek 14: Rekonstrukce 3D modelu z 2,5D skeneru [43]

Takto nasnímaná data lze následně v počítači reprezentovat několika způsoby:

- Mrak bodů – Jedná se o nejjednodušší reprezentaci, která využívá pouze 3D souřadnice bez vzájemných vazeb.
- Polygrafní síť – Tento model se využívá v počítačové grafice. Povrch je reprezentován navazující sítí polygonů.
- Hloubková mapa – Zde se jedná v podstatě o 2,5 skener. 2D obraz, kde intenzita jednotlivých bodů odpovídá vzdálenosti v prostoru. [1]



Obrázek 15: 3D modely (mrak bodů, polygrafní síť, hloubková mapa) [1]

Podobně jako při práci s 2D, ani v 3D neexistuje jedna ideální metoda pro vyhledání podobnosti. Jednotlivé metody se liší v náročnosti na kapacitu systému, spolehlivost nebo její složitost. Základní metody hledání podobnosti ve 3D jsou: Podobnost 3D modelů, Podobnost založená na tvaru a vzhledu, Podobnost hloubkových map.

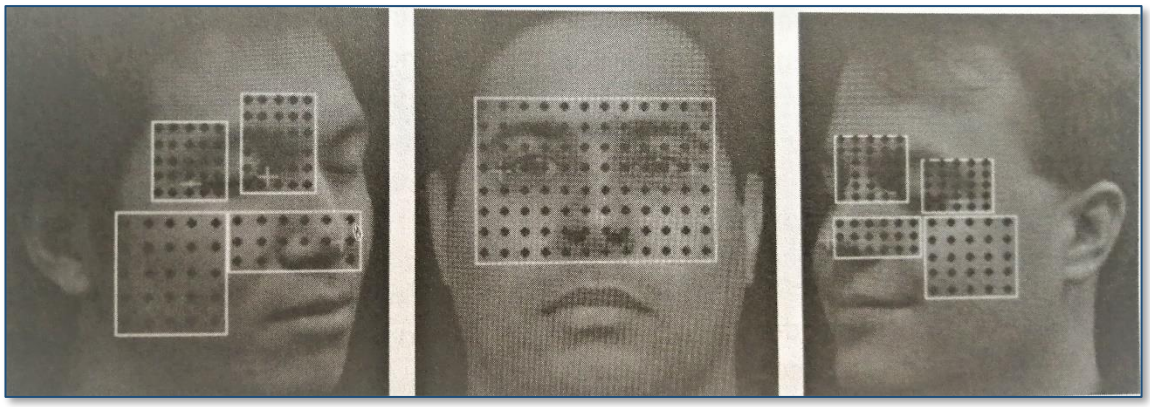
4.2.3.1 Podobnost 3D modelů

V tomto modelu se užívá algoritmus ICP (Interactive Closest Point), který pracuje tak, že najde jemné zarovnání testovacího snímku a šablony a výsledná podobnost je určena jako rozdíl tvarů zarovnaných 3D reprezentací. [1]

Postup algoritmu ICP:

1. Výběr kontrolního bodu v jedné množině.
2. Nalezení nejbližšího bodu v druhé množině.
3. Vypočtení optimální transformace mezi oběma množinami na základě aktuální korespondence.
4. Transformace bodů.
5. Opakování algoritmu od bodu2 až do konvergence. [1]

Kontrolní body jsou vybírány v málo tvárných oblastech (oblasti s malou změnou při různých výrazech obličeje), ale tak, aby pokrývaly co možná největší plochu obličeje. [1]



Obrázek 16: Výběr bodů pro algoritmus ICP [1]

4.2.3.2 Podobnost založená na tvaru vzhledu

Ideální případ pro práci s touto metodou je kompletní 3D model, který je uložen v šabloně a 2,5D skenem aktuálního testovacího snímku. Podstata je založena v hledání transformace původního modelu tak, aby maximálně odpovídal testovanému snímku a zároveň hledá projekci, která se bude nejlépe vizuálně shodovat s aktuálním snímkem. [1]

4.2.3.3 Podobnost hloubkových map

Toto je jedna z nejjednodušších metod porovnání 3D. Tato metoda spočívá v práci s hloubkovou mapou získanou z určitého výřezu normalizovaného 3D obličeje. Tuto hloubkovou mapu již lze chápat jako 2D obraz, pro který lze využít některou z technik využívaných ve 2D. [1]

4.3 Systémy pro rozpoznávání obličeje

Jedná se o systém, který je určen k samotnému rozpoznání obličeje a který pracuje na základě jedné z výše uvedených metod. Oproti jiným způsobům identifikace pomocí biometrických údajů, jako je například otisk prstu, snímaní oční duhovky, má rozpoznání tváře neoddiskutovatelnou výhodu. Tou je fakt, že snímání identifikačních údajů z tváře může probíhat na větší vzdálenost od snímacího zařízení, než je tomu u výše zmíněných alternativ. [9]

Pokud budeme hovořit o možnosti rozpoznání obličeje systémem, je potřeba rozlišovat dva základní, ale technologicky velmi odlišné způsoby a to, zda je pro provedení identifikace potřeba interakce identifikované osoby, či nikoli. V prvním případě se identifikovaná osoba aktivně podílí na procesu rozpoznání tváře. Toto probíhá například ve vymezeném prostoru před snímacím zařízením a dále vyčká na rozhodnutí o identifikaci. Tato zařízení se začínají hojně využívat jako alternativa proti otiskům prstů nebo čtecích karet v systémech EKV. [9]

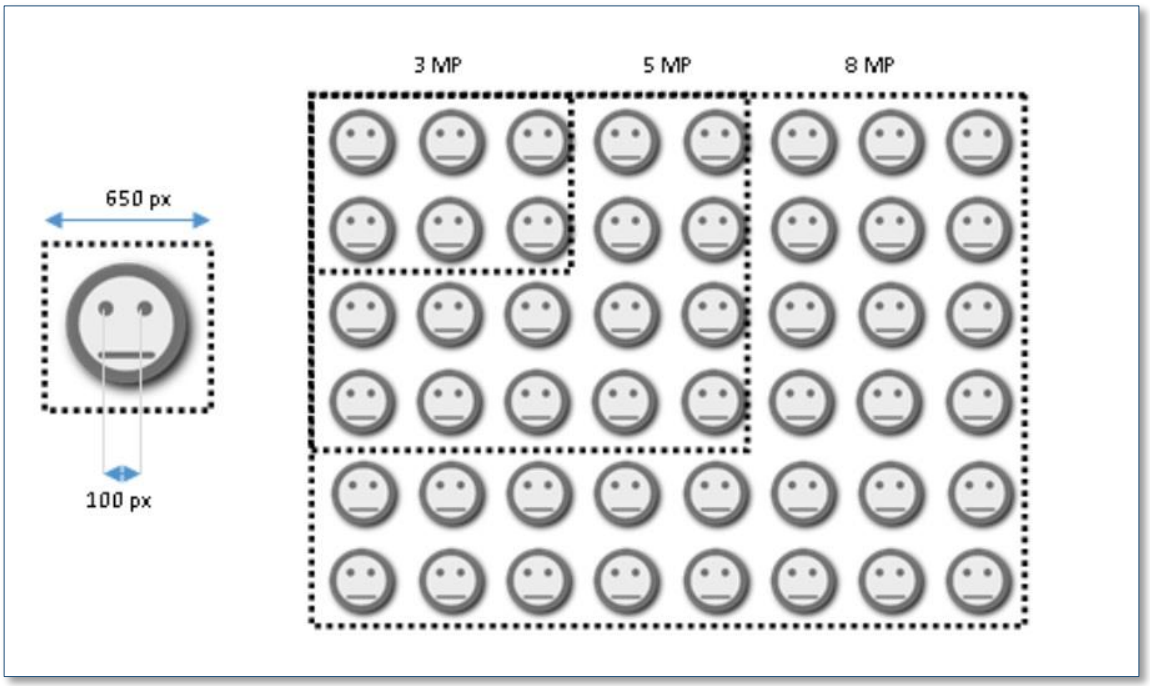
V druhém případě, tedy pokud je potřeba provést identifikaci obličeje bez interakce identifikované osoby v živém videu, nebo v záznamu, kde se pohybuje větší množství osob, je úloha mnohem složitější a náročnější. Právě této variantě se budeme v této práci dále věnovat. Pro tyto případy lze využít standardní IP kamery, které jsou připojeny do speciálních SW propojených s databází zájmových osob. Zvolenou metodou se v reálném čase vyhledají v obraze jednotlivé obličeje a provede se biometrická analýza. Dále získané výsledky porovná systém s databází. Výsledkem porovnání je míra shody porovnávaného vzorku s obsahem databáze. Do systému je zadána hodnota prahu pravděpodobnosti, při jejíž překročení je operátor upozorněn. Tyto systémy bývají doplněny o další funkce, jako je například uchovávání snímků pro pozdější použití. [9]

Teoreticky platí, že pro rozpoznání tváře v živém videu lze použít standartní kamerové systémy. V praxi je však problém s využitím standardních kamer díky jejím nevhodném umístění, neboť byly primárně použity jako přehledové kamery, nebo mají jinou konkrétní funkci. Proto se ve většině případů instalují kamery

určené pouze k detekci tváře. Aby byla zajištěna maximální možná míra rozpoznání tváře, je třeba dodržet několik zásadních podmínek.

4.3.1 Podmínky pro rozpoznání obličeje

- Viditelnost obličeje – jednotlivé části obličeje, jako jsou oči, nos a ústa by neměly být zakryty. Je nutné, aby byl obličej dostatečně osvětlen, ale nesmí být přesvětlen např. přímým slunečním světlem nebo reflektorem. [18]
- Rozlišení obličeje – pro systémy rozpoznávání obličeje je vyžadován digitální obraz tváře, který má minimálně 40 pixelů mezi zorničkami očí. Optimální vzdálenost je však 80-100 pixelů. Pokud bude hodnota nižší než 40 pixelů, prudce klesá úspěšnost identifikace (nikoliv rozpoznání) osoby. [18]
- Počet obličejů v jednom snímku – snímek video streamu může obsahovat více tváří. S ohledem na rozlišení kamery a požadavek na minimální počet obrazových bodů mezi zorničkami očí lze snadno odvodit, kolik obličejů „se vejde“ do snímku kamery s různým rozlišením, až do mezní hodnoty stanovené podle dostupného výpočetního výkonu. [18]



Obrázek 17: Znázornění možného počtu obličejů ve snímku [18]

Rámec 650 pixelů na obrázku zhruba představuje normální rozlišení analogové CCTV kamery a přibližnou velikost tváře v obraze, pokud je 100 pixelů mezi očima. Je však nutné uvažovat, jaká úloha rozpoznávání obličejů je v konkrétním projektu řešena. Zda je požadováno rozpoznávání nebo identifikace. Tomu odpovídá i návrh serverového hardware, který dokáže úlohu zvládnout v požadovaném čase a kvalitě. [18]

- Úhel natočení obličeje – mezi úlohy rozpoznávání obličeje patří zjednodušeně řečeno rozpoznání kontur obličeje, jako jsou oči, koutky úst, kořen nosu a jejich vzájemný poměr vzdáleností. Čím více takových bodů odpovídá uloženému vzoru v databázi, tím přesnější je identifikace osoby. Svou roli hraje natočení obličeje, které je optimálně menší než +/- 15 stupňů horizontálně a +/- 15 stupňů vertikálně. Při překročení těchto hodnot dochází k deformaci poměru vzdáleností obličejových kontur a tím se znepřesňuje výsledek identifikace. [18]

Obrázek 18: Míra natočení obličeje vůči kameře [18]

4.3.2 Měření výkonnosti rozpoznávacích algoritmů

Jal bylo zmíněno, technologie na rozpoznání obličeje jsou dnes v rozkvětu a jejich vývoji se věnuje čím dál větší řada společností. Již dnes na trhu existuje množství produktů s různými algoritmy. Není výjimkou, že dva různí výrobci softwaru použijí stejný algoritmus, který má různě nastavené parametry. [18]

Americký institut National Institute for Standards and Technology (NIST) zavedl pro potřeby měření výkonu a kvality algoritmů různých výrobců speciální metodiky. Pro testovaní jsou využívány databáze s více jak 1,8 miliony osob včetně jejich fotografií. [18]

Algoritmy rozpoznávání lze nastavit mnoha způsoby a pro různé podmínky. NIST měří desítky technických parametrů v různých světelných konfiguracích, ale pro vyhodnocení celkové úspěšnosti rozpoznávání jsou tyto klíčové hodnoty:

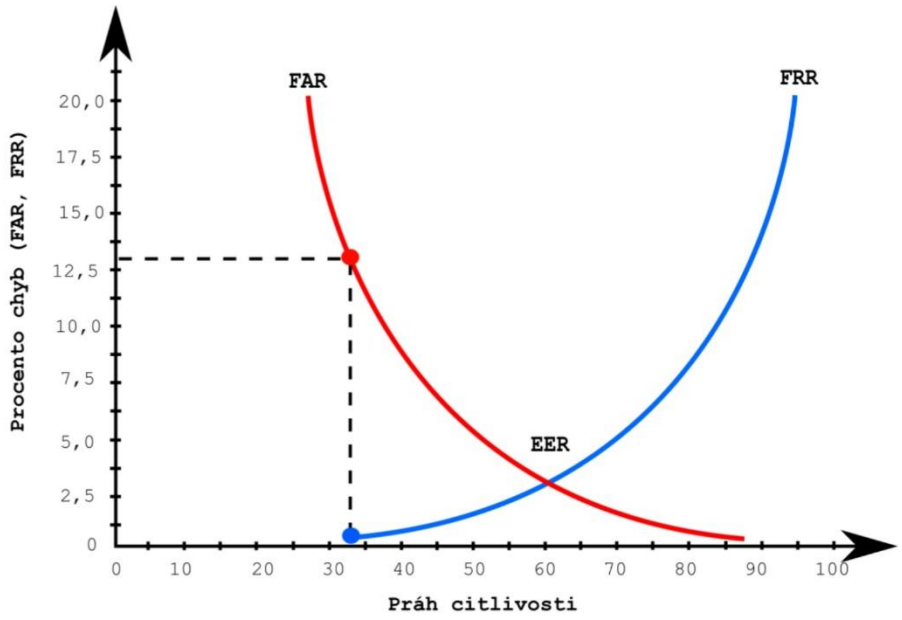
- False Acceptance Rate (FAR) – jedná so o ukazatel míry toho, že uživatel, který není autorizovaný je systémem špatně rozpoznán. Tedy uživatel, který nemá oprávnění pro přístup je vyhodnocen tak, jako oprávněný. Tento koeficient je používán pro udání míry bezpečnosti. Vztah koeficientu nesprávného přijetí: [19] [9] [18]

$$FAR = \frac{Nesprávná\ přijetí\ (počet)}{Celkový\ počet\ pokusů} * 100[\%]$$

- False Rejaction Rate (FRR) – jedná se o koeficient nesprávného odmítnutí. Pravděpodobnost toho, že rozpoznávací systém odmítne oprávněného uživatele jako uživatele neoprávněného. Uživateli se samozřejmě nelíbí, když dojde k jeho neoprávněnému odmítnutí. Proto tento koeficient udává míru komfortu jednotlivých systémů. Označováno také jako chyba typu I. Vztah koeficientu nesprávného odmítnutí: [19] [9]

$$FRR = \frac{Nesprávná\ odmítnutí\ (počet)}{Celkový\ počet\ pokusů} * 100[\%]$$

- Equal Error Rate (ERR) - Koeficient vyrovnané chyby známý jako křížový koeficient. Tento koeficient se nachází na pomezí koeficientů FAR a FRR. Čím se EER nachází níž, tím přesnější je rozpoznávací systém. Samotná hodnota EER však nevypoví nic o tom, jak je celý systém bezpečný. K tomu je potřeba znát hodnoty koeficientů FAR a FRR.



Obrázek 19: Závislost FAR a FRR na prahové hodnotě [40]

- False Non-Match Rate (FNMR) – jedná so o procento snímků, kdy osoba v databázi nalezena nebyla, přestože databáze tuto osobu obsahovala. [18] Na rozdíl od FRR se zde nepočítá s odmítnutím z důvodu špatně sejmutého vzorku (kvalita sejmutí). [20]

4.3.3 Využití detekce a rozpoznání obličeje

4.3.3.1 Bezpečnost

Velký rozvoj zaznamenaly systémy pro rozpoznání obličeje v oblasti bezpečnosti. Rozvoj je poměrně hodně tažen událostmi spojenými s teroristickými útoky, jako reakce na zvýšení bezpečnosti. Dnes jsou například na řadě mezinárodních letišť instalovány systémy pro rozpoznání obličeje, které jsou napojeny na DB s tvářemi osob podezřelých z teroristického útoku. [14]

4.3.3.2 Databáze osob pro vyšetřování

Detekce a rozpoznání obličeje se využívá i jako pomoc policii při vyšetřování nejrůznějších případů. Využívané systémy jsou vždy nastaveny přesně pro dané odvětví, využívají v podstatě stejné metody, ale jsou napojeny na jiné DB. Např. se může jednat o pátrání po hledaných a pohřešovaných osobách, identifikace profesionálních řidičů a další. [14]

4.3.3.3 Obecné ověření totožnosti

Systémy pro ověření totožnosti jsou čím dál častěji využívány v běžném životě. Jejich rozmach můžeme zaznamenat například v bankovnictví, jako alternativu pro klasické zadávání hesel, nebo pro identifikaci zaměstnanců ve společnostech.

4.3.3.4 Dohled

Pro dohled se tyto systémy využívají podobně jako u hlídání bezpečnosti. Jednotlivé kamery jsou instalovány ve veřejném prostoru, kde snímají trestnou činnost. Jako příklad z praxe lze uvést Newham (Londýnská čtvrť), kde klesl po instalaci kamer s rozpoznáním obličeje počet spáchaných trestných činů o 35 %.

4.3.3.5 Zábava

Zábava je dalším odvětvím, díky kterému se detekce a rozpoznání obličeje vyvíjí extrémní rychlostí. V zábavním průmyslu se s těmito systémy setkáváme u herních konzolí, ale dnes již i jako běžnou součást mobilních telefonů.

5 Právní předpisy pro sledování osob kamerovým systémem

Právní úpravy se v oblasti sledování osob kamerovým systémem v jednotlivých zemích velmi liší. Shodným prvkem je, že jednotlivé právní úpravy většinou rozlišují, zda se jedná o využití systému správním úřadem např. policií, nebo soukromou osobou, které nemají pravomoci správního úřadu. Některé země využívají institutu povolávacího řízení či dozorové úřady.

5.1 Právní úprava v ČR

„Kamerový systém je Úřadem pro ochranu osobních údajů uznáván za legitimní a legální možnost k ochraně majetku a zdraví osob a k zabezpečení ostatních právem chráněných zájmů. Na druhou stranu musí být ovšem splněny veškeré podmínky Zákona o ochraně osobních údajů, dodrženy všechny stanovené principy a zároveň splněna přiměřenost a úměrnost zásahu do osobnostních práv subjektů údajů.“ [21]

Přiměřenost a účelnost zásahu do osobních práv určuje § 5 odst. 1 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů, jako deklarovanou účelem a dále zvolenými prostředky. Bohužel nevýhoda kamerových systémů je, že dochází k tzv. neselektivnímu výběru osob. To znamená, že ve sledované skupině osob kamerovým systémem je jen velmi malé procento těch, kteří skutečně trestnou činnost páchají. Záznam z kamerového sledování pak může být použit i proti "poctivým" lidem, kteří neporušují právo, ale jsou díky kamerám snadno identifikovatelní. Případné zneužití by na tyto osoby mělo výrazný osobnostní dopad, ačkoliv – a to je nutné opět zdůraznit – nejde o osoby, které by se provinily. [21] [22]

Zpracování osobních údajů kamerovým systémem je možné:

- Při dodržení rámce zákonů ČR (např. Policie České republiky).
- S výslovným souhlasem subjektu údajů. To je ale možné jen v případě, kdy lze přesně určit okruh osob v dosahu kamery.
- Bez souhlasu subjektu údajů při využití výjimky v § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. při současném respektování podmínek v § 4. zákona č. 101/2000 Sb.

Znění § 5 odst. 2 písm. e) zákona č. 101/2000 Sb: *„pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života“* [22]

Zákon o ochraně osobních údajů se na provozovatele vztahuje tehdy, kdy se systematicky zpracovávají osobní údaje. Systematické zpracování v duchu zákona znamená, že je kamerovým systémem prováděn záznam. Pokud je kamerový systém pouze v režimu on-line, nemá provozovatel oznamovací povinnost vůči Úřadu. [21]

Povinnosti provozovatele kamerového systému:

- Kamerový systém nesmí být použit tak, že nadmíru zasahuje do soukromí.
- Provozovatel musí dokázat, že stanoveného účelu nelze dosáhnout alternativní metodou.
- Kamerový systém nesmí být použit v rámci prostor sloužících k soukromým účelům (např. toaleta). Pokud provozovatel takový prostor sleduje, musí vždy vyčlenit místo v prostoru, který není snímán.
- Vždy musí být specifikován účel pro který je systém zřízen. Záznamy pak mohou být využity pouze v rámci tohoto účelu.
- Musí být stanovena lhůta pro uchování záznamů, která by neměla být delší, než je maximálně přípustná doba pro splnění účelu kamerového systému. Po uplynutí této doby by se data měla přemazat novými daty. Je možná výjimka,

a to v případě zjištění bezpečnostního incidentu, kdy jsou záznamy předávány orgánům činným v trestním řízení.

- Musí být zajištěna ochrana snímacích zařízení, přenosových cest a datových nosičů se záznamy.
- Subjekt údajů musí o kamerovém systému vědět, tzn. být o něm vhodně informován.
- Zpracování osobních údajů musí být předem registrováno u Úřadu, není-li splněna některá z výjimek, která umožňuje zpracování neoznamovat. [21]

5.1.1 Veřejný prostor

Je místo, které může být navštíveno v podstatě kýmkoli a za jakýchkoli okolností. Tyto prostory jsou pod správou veřejných autorit. Jedná se např. o městské parky, obytné ulice apod. [21]

5.1.2 Soukromý prostor

Je specifikován jako prostor, který není přístupný všem a jeho přístup je omezen zákonem. Moc veřejné autority je oproti veřejným prostorům omezena. Zároveň je to prostor, ve kterém je každý chráněn proti médiím, veřejným institucím a jiným lidem. [21]

6 Prostředí fotbalového výtržnictví

Pojem fotbalové výtržnictví je bohužel neméně známý jako fotbal takový. Každou chvíli se dozvídáme z médií, že při fotbalovém utkání došlo k výtržnictví. Vytrhané sedačky, dýmovnice, zranění fanoušci, přerušené utkání pro nepokoje na tribunách, vhozené předměty na hrací plochu, nebo vulgární skandování. To vše, a nejen to jsou jedny z nejčastějších projevů výtržnictví u nás. S fotbalem je bohužel tento fenomén spojen asi víc než s jakýmkoli jiným sportem.

Samotný zápas ale není jediným místem, kde se fanoušci svým násilným chováním projevují. Případy, kdy jsou davem fanoušků při cestě na zápas ničeny automobily, lampy, vlastně cokoli se nachází na ulici, nejsou až tak velkou výjimkou. Řada z těchto rádoby fanoušků má toto chování jako svůj druh zábavy a samotný zápas je v podstatě až tolik nezajímá. Fotbalový zápas se tak stává pouze jakousi záminkou, aby se skupiny těchto lidí mohli setkávat. [23]

Divácké násilí ale nelze spojovat primárně se sportovním odvětvím. V podstatě stejné projevy násilí můžeme pozorovat na masových akcích, kde dochází k větší kumulaci lidí, festivaly, koncerty, technopárty apod., zde jsou tyto projevy umocněny konzumací alkoholu a v řadě případů i drog. Tomuto se například Fotbalová asociace snaží předcházet zákazem prodeje jakýchkoli alkoholických nápojů během utkání, dokonce i pivo, které je s fotbalovým divákem neodmyslitelně spojováno se nyní čepuje pouze nealkoholické. [23]

„Projev sportovního výtržnictví není moderním úkazem, své kořeny má již v antickém Řecku. Například v roce 532 došlo ke střetu dvou táborů fanoušků při závodech cirku (závody jednomužných vozů zapřažených za koňmi). Jelikož byl toto v té době velmi oblíbený sport, navštěvovalo tyto závody až 30.000 fanoušků. Při tomto střetu se nepokoje rozšířily do celého města a daly tak vzniknout jednomu z největších povstání v historii říše. Toto povstání je dodnes známe jako povstání Nika“. [23]

6.1 Typologie účastníků fotbalových utkání

Motivace pro návštěvu fotbalového utkání, nebo jakéhokoli jiného sportu může být pro každého jiná. Někdo jde podpořit svůj oblíbený klub, někdo se jde pobavit sportem bez konkrétní klubové přízně a někteří mohou mít zájmy daleko vzdálené od sledování sportovního výkonu. Této problematice se podrobněji věnují pánové Mareš, Smolík a Suchánek ve své knize *Fotbalový chuligáni*, kteří účastníky na fotbalových utkání rozdělili do tří základních skupin popsaných v následujících kapitolách.

6.1.1 Fotbalový divák

Fotbalového diváka můžeme s trochou nadsázky přirovnat k divadelnímu divákovy. Na fotbalovém utkání zastává roli pasivního přihlížejícího, bez prioritizování některého z klubů. Jeho záměrem je shlédnout atraktivní utkání s kvalitním sportovním výkonem. Tito diváci na sobě zpravidla nemají žádné klubové předměty a na stadionu se nijak výrazně neprojevují. Fotbalový diváci patří do nejméně rizikové skupiny z pohledu páchání jakéhokoli výtržnictví na stadionu. [23]

6.1.2 Fotbalový fanoušek

Oproti fotbalovému divákovi, je fotbalový fanoušek k fotbalu poutám prostřednictvím svého oblíbeného klubu. V utkání tedy fandí a podporuje svůj tým k vítězství. Úspěch, či neúspěch týmu často vnímá jako svůj vlastní. Fotbalový divák obvykle nevnímá děj utkání příliš objektivně, a proto lze očekávat bouřlivé reakce na rozhodnutí rozhodčího vůči jeho týmu, nebo dosažení branky jeho týmu. Fotbalový fanoušek utkání většinou sleduje oblečen v klubových barvách, nebo má alespoň nějaké klubové předměty jako například šála, čepice apod. Princip fandovství je založen na faktu, že při zapase vzniká určitý druh rivality dvou proti sobě stojících skupin s vlastní identitou. Tyto fanoušky charakterizuje bipolární dělení na my a oni. Tato supina je podstatně rizikovější a je třeba činit určitá opatření k zajištění bezpečnosti. Pokud nejsou fandové, ale ovlivněni například alkoholem, zůstávají v drtivé většině u verbálních projevů. [24]

6.1.3 Fotbalový výtržník

Tyto skupiny se také označují jako fotbalový chuligáni, hooligans, rowdeas, hools a jiné. Charakteristické je pro ně, že se sdružují do menších ale dobře organizovaných skupin se stejnou hodnotovou orientací. Pro tuto skupinu lidí je sport pouze záminkou k jejich hlavnímu prožitku. Tím jsou často potyčky se stejně orientovanou skupinou soupeře. Stává se, že pokud je potyčkám zamezeno v prostorách stadionu, organizovaně se tyto dva tábory sejdou mimo stadion na volném prostranství, kde proti sobě svedou souboj. Cítění k ostatním skupinám soupeře se dá označit až za nenávistné. Známými skupinami v oblasti českého fotbalu jsou výtržníci hlásící se k Baníku Ostrava, Spartě Praha a Slavii Praha. [24]

Tyto skupiny jsou extrémně rizikové z pohledu bezpečnosti na stadionech. K jejich projevům patří házení předmětů na hrací plochu, vniknutí na hrací plochu, výtržnictví, vandalismus, vulgarita. Každoročně si jejich řádění vyžádá vysoké finanční náklady na opravu poškozeného vybavení stadionů, ale bohužel i ublížení na zdraví, a to i z řad běžných diváků.

Jelikož se dlouhodobě nedaří na stadionech tyto skupiny efektivně „hlídat“ je aktuálním trendem zajištění prevence jejich jednání. Jedním z preventivních opatření může být i zamezení vstupu na stadion osobám, které se již v minulosti nějakého činu na stadionu dopustili.

7 Zabezpečovací prvky fotbalových stadionů

Zabezpečení fotbalového stadionu vychází z celé řady norem. Bezpečností se zabývají i samotná pravidla fotbalu, kde jsou mimo jiné vyjmenovány úkoly pořadatelské služby, zabezpečení hráčských laviček, nebo prostoru hřiště a udávají například i postup rozhodčích při výtržnostech obecenstva, aby bylo maximálně možně ochráněno zdraví všech účastníků. Pravidla ale už neřeší, jaký způsobem by měly být chráněni samotní fanoušci, jak mají být koncipovány technické a mechanické prvky ochrany celého stadionu. Na tyto otázky reagují další normy, vyhlášky a zákony. Zabezpečení stadionů bychom mohli rozdělit do několika kategorií: aktivní prvky ochrany, pasivní prvky ochrany, prostředky technického zabezpečení a prostředky mechanického zabezpečení.

V podstatě se jedná o řešení otázek objektové ochrany se specifickými požadavky. Před každou samotnou instalací je nutné provést bezpečnostní analýzu, stanovit hrozby a na ty následně sestavit ideální řešení, které povede ke snížení hrozeb na akceptovatelnou míru. Důležité je si uvědomit, že žádná hrozba nemůže být nikdy eliminována na nulovou pravděpodobnost, vždy bychom měli hledat vyvážení mezi náklady na zabezpečení a mírou rizika, že hrozba nastane.

Při řešení ochrany stadionu je dobré mít na mysli, že většina řešení, která přispívají k ochraně majetku a zdraví způsobují určitý divácký diskomfort. Například ochranné sítě mohou zhoršovat viditelnost na hrací plochu, ploty omezují pohyb po stadionu a podle některých studií mohou dokonce působit jako určitý stimul agresivního chování. I z tohoto důvodu je kladen důraz na zajištění bezpečnosti moderními technologiemi, které nebudou snižovat divácký komfort a v ideálním případě předejdou újmám na zdraví a škodám na majetku.

7.1 Aktivní prvky ochrany

Jedná se o prvky, které se snaží nějakým způsobem předejít protiprávnímu jednání. Aktivní prvky ochrany se mohou velkou částí překrývat s prostředky mechanického nebo technického zabezpečení. Příklad aktivního prvku může být například vstupní turniket, který zajistí, že na stadion nemá přístup osoba bez zakoupeného lístku. Toto zabezpečení se také řadí do prvků technického

zabezpečení, neboť je většinou propojeno s přístupovým systémem. Pokud je turniket čistě mechanický a lístek je kontrolován pořadatelskou službou, zařadili bychom ho do mechanického zabezpečení. Dalším z prvků aktivní ochrany můžeme označit například kamerové systémy, které jsou neustále sledovány pořadatelskou službou z dohledového místa a pokud je vyhodnoceno chování některého, nebo některých fanoušků za rizikové, může pořadatelská služba zasáhnout včas. Tento prvek bychom zařadili do technických prostředků zabezpečení.

7.2 Pasivní prvky ochrany

Tyto prvky naopak oproti aktivním prvkům nepředchází protiprávnímu jednání, ale snaží se snížit jeho následky. Za typický prvek pasivní ochrany můžeme považovat nejrůznější plotové systémy v hledišti, ochranné sítě, ale mohou to být i žáruvzdorné plastové sedačky pro diváky, nebo únikové cesty.

7.3 Prostředky technického zabezpečení

Fotbalový stadion je potřeba chránit i mimo dny, kdy se hrají fotbalová utkání. Na stadionu se nachází hráčské zázemí, kanceláře vedení klubu, technické místnosti a například i reprezentativní místnosti. V celém stadionu je tedy řada hodnotných aktiv, která je potřeba chránit.

Technické prvky ochrany jsou obvykle kombinovány s fyzickou ochranou objektu a tím napomáhají k efektivnějšímu střežení celého objektu. Jedná se o řadu systémů, jako jsou PZTS, EPS, EKV, CCTV, nebo rozhlas. Tyto systémy představují náklad v prvotní investici a dále v provozních nákladech, ale snižují nároky na lidské zdroje. Z řady studií vyplývá, že velká část nehod, nebo chyb je způsobena lidským faktorem. Tyto systémy tedy velmi výrazně přispívají k celkovému zvýšení bezpečnosti a jsou využívány v podstatě nepřetržitě, a to tedy jak při konání utkání, tak i mimo něj, pro ochranu majetku.

7.4 Prostředky mechanického zabezpečení

Prvky mechanické ochrany jsou nejčastěji využívané prvky ochrany stadionů. Jejich použití ovšem snižuje divácký komfort, a tak jsou stále více doplňovány, nebo zcela nahrazovány modernějšími technologiemi. Bohužel i dnes je stále tyto prvky potřeba využívat, jelikož jsou v některých případech nejúčinnějším prvkem.

Obecně bychom mohli do prvků mechanického zabezpečení zařadit všechny prvky ochrany, které fyzicky zpomalí, nebo znemožni vstup nežádoucí osoby do určitého prostoru. Jedná se například o mříže, zámky, zdi apod. U fotbalových stadionů se v souvislosti se zřízením ochrany vůči agresivním fanouškům využívají nejčastěji ploty, sítě a mříže. [25]

Ploty a mříže jsou využívány mezi jednotlivými fanouškovskými sektory, aby nedošlo ke konfliktu, mezi dvěma tábory fanoušků. Jedná se o účinný, ale zastaralý způsob ochrany. Ochranné sítě slouží většinou k tomu, aby zabránilyfanouškům vhazování předmětů na hrací plochu stadionu a tím narušovali průběh hry.

Obrázek 20: Bezpečnostní oplocení sektoru fanoušků v Generali aréně [54]

7.5 Služby zajišťující bezpečnost

Při konání fotbalových utkání se pro zvýšení bezpečnosti využívá i lidská síla. FAČR řeší tuto otázku ve dvou úrovních. Zaprvé je stanovena nutnost zajištění pořadatelské služby na každém utkání konané pod záštitou FAČR. Konkrétní složení, práva a povinnost pořadatelské služby určují pravidla fotbalu. Zadruhé byla uzavřena Dohoda o spolupráci k zajišťování bezpečnosti a pořádku, při fotbalových utkáních mezi FAČR a PČR.

7.5.1 Pořadatelská služba

Krom povinností stanovených pravidly týkajících se zajištění konání utkání má Hlavní pořadatel za úkol podílet se na zajištění bezpečnosti na stadionu. Práva a povinnosti pořadatelů uvádí mimo jiné normy i Publikace Manuál pro fotbalové kluby vydaná ministerstvem vnitra.

Pořadatelská služba je zřizována pořádajícím klubem a výběr členů je volbou tohoto klubu. Členové pořadatelské služby by měli být jak fyzicky, tak psychicky schopní, řádně vyškolení jedinci, kteří mají s klubem uzavřen smluvní vztah. Povinnosti pořadatelské služby v oblasti bezpečnosti jsou:

- řízené vpuštění diváků a dohled nad nimi,
- prohlídka stadionu před a po utkání,
- poskytování informací ohledně infrastruktury stadionu a záchranných službách uvnitř stadionu,
- rozpoznání nežádoucích diváků a jejich následné vykázání,
- poskytnutí informací PČR o divácích narušujících pořádek,
- předcházet možným situacím, které by mohlyvyústit v narušení pořádku nebo ke škodám na majetku a zdraví. [26]

Obrázek 21: Zásah pořadatelské služby [54]

7.5.2 Policie ČR a další složky IZS

Obecně platí, že složky IZS zasahují při mimořádných situacích, a to jak kdekoli v běžném životě, tak i při fotbalových utkáních. Samy o sobě jsou fotbalová utkání, co se týče bezpečnosti rizikovou záležitostí mimo jiné i proto, že se na relativně malém prostoru nachází větší množství lidí. Na některých utkáních i desetitisíce.

Jednotlivé složky IZS se na tyto mimořádné situace v ne zcela standartním prostředí také připravují a cvičí. PČR a FAČR dokonce vzájemně uzavřeli tzv. *„Dohodu o spolupráci k zajišťování bezpečnosti a pořádku při fotbalových utkáních.“* Tato dohoda je zřízena za účelem zajištění bezpečnosti v rámci utkání pořádaných asociací a při mezinárodních utkání. Tato dohoda upravuje vztah mezi pořadatelskou službou a PČR, kdy PČR v určitých případech nahrazuje pořadatelskou službu. Dále také stanovuje potřebu přítomnosti příslušníků PČR i mimo stadion jako bezpečnostní prevenci, při rizikových utkáních kamerový dohled v přilehlých ulicích a v neposlední řadě také doprovod rizikových skupin fanoušků na vlakové spoje. V ojedinělých případech může PČR využít i letecké služby pro monitorování situace. Na utkáních jsou také přítomné jednotky HZS jako kontrolní orgán požárních předpisů a požární prevence. Samozřejmě jsou na utkáních přítomny i posádky ZZS. [25]

Obrázek 22: Pořádková jednotka PČR přítomná na fotbalovém utkání [55]

Praktická část

8 Aktuální situace v oblasti bezpečnosti na fotbalových stadionech v ČŘ

O problémy týkající se diváckého násilí se aktivně zajímá i současný ministr vnitra Jan Hamáček, který za účelem urychlení řešení situace svolal 19. 03. 2019 expertní skupinu. Akcelerátorem bylo ligové utkání AC Sparta Praha – FC Viktoria Plzeň, při kterém díky použití pyrotechniky bylo zraněno několik diváků, z niž jeden byl zraněn vážně.

Základní body, které míní ministerstvo dále prosazovat jsou posílení pořadatelské služby, změna zákona o přestupcích, kde by měl být uveden zákaz vnášení pyrotechniky na stadion se sankcí 10 tisíc až 100 tisíc korun. Dalším bodem je zavedení centrální databáze problémových fanoušků.

„Rodiny s dětmi se nesmí bát chodit na fotbal, protože je tam někdo zraní. Fotbalovým asociacím jsme proto jasně řekli, v čem musejí přidat a k jakým krokům mají rychle přistoupit,“ [56] uvedl ministr Hamáček na jednání.

Obrázek 23 - Novinový titulek [57]

8.1 Míra rizika diváckého násilí na fotbalových utkáních v ČR

8.1.1 Určení míry rizika diváckého násilí pro fanoušky klubů

Pro určení, do jaké míry jsou zápasy české nejvyšší soutěže rizikové v oblasti diváckého násilí jsem použil metodu multikriteriální analýzy. Touto metodou budu nejprve určovat, do jaké míry mohou být rizikoví fanoušci jednotlivých klubů. Z tohoto zjištění budu následně vycházet pro určení míry rizika diváckého násilí v jednotlivých utkáních. Posuzovány budou kluby, které hrají nejvyšší českou fotbalovou soutěž v sezoně 2019–2020.

Jednotlivá kritéria posuzovaná v analýze pro zjištění rizikovosti chování fanoušků jsou následující:

- Četnost konfliktů
- Počet fanoušků zapojených do konfliktu
- Míra agrese při konfliktu
- Četnost použití pyrotechniky
- Vliv na utkání

Jelikož se domnívám, že všechny z výše uvedených kritérií jsou ve výsledku stejně závažná, nebo mají stejně závažný dopad, rozhodl jsem se jim přiřadit shodnou váhu 1. Jednotlivá kritéria mohou nabývat hodnot v číselné řadě od 1 do 5, přičemž jedna je nejmenší riziko, nebo četnost, pět naopak největší.

Určení koeficientu rizikovosti fanoušků jednotlivých klubů:

Tabulka 2 - Určení koeficientu rizikovosti fanoušků jednotlivých klubů

Určení koeficientu rizikovosti fanoušků příslušného klubu						
Seznam klubů	Posuzovaná kritéria (rozmezí 1-5; pro všechny kritéria platí váha 1.0)					
	Četnost konfliktů	Počet fanoušků zapojených do konfliktu	Míra agrese při konfliktu	Četnost použití pyrotechniky	Vliv na utkání	Celkem
1. FC Slovácko	1	2	2	2	1	8
1. FK Příbram	1	1	2	1	1	6
AC Sparta Praha	4	5	5	4	4	22
Bohemians Praha 1905	3	3	4	4	4	18
FC Baník Ostrava	5	5	5	4	4	23
FC Slovan Liberec	3	3	3	3	2	14
FC Viktoria Plzeň	4	5	5	4	4	22
FC Zastav Zlín	2	2	3	3	2	12
FK Jablonec	3	2	3	3	2	13
FK Mladá Boleslav	2	2	2	3	1	10
FK Teplice	3	3	3	2	2	13
MFK Karviná	2	2	2	2	1	9
SK České Budějovice	2	2	2	3	2	11
SK Sigma Olomouc	3	3	3	2	2	13
SK Slavia Praha	4	5	4	4	4	21
Slezský FC Opava	3	2	3	3	2	13

Popis koeficientu rizikovosti fanoušků klubu:

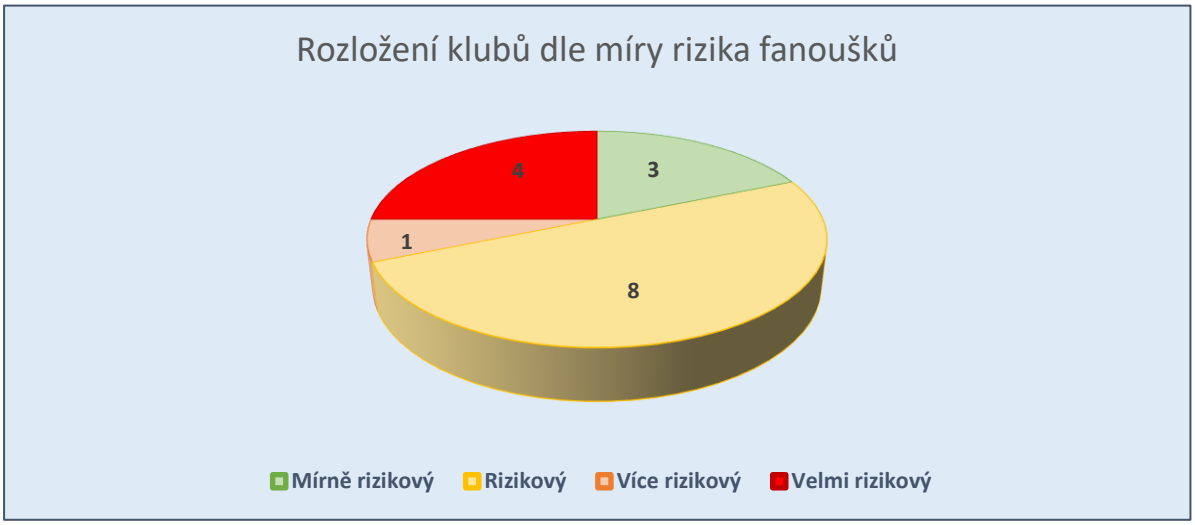
- 0-9 Mírně rizikoví fanoušci
- 10-14 Rizikoví fanoušci
- 15-20 Více rizikoví fanoušci;
- 20 a více Velmi rizikoví fanoušci;

Tabulka 3 - Seznam klubů seřazený dle rizikovosti fanoušků

Seznam klubů	Rizikový koeficient
FC Baník Ostrava	23
AC Sparta Praha	22
FC Viktoria Plzeň	22
SK Slavia Praha	21
Bohemians Praha 1905	18
FC Slovan Liberec	14
FK Jablonec	13
FK Teplice	13
SK Sigma Olomouc	13
Slezský FC Opava	13
FC Zastav Zlín	12
SK Dynamo České Budějovice	11
FK Mladá Boleslav	10
MFK Karviná	9
1. FC Slovácko	8
1. FK Příbram	6

Tabulka 4 - Počet klubů v jednotlivých kategoriích

Kategorie rizikovosti fanoušků	Počet klubů
Mírně rizikoví fanoušci	3
Rizikoví fanoušci	8
Více rizikoví fanoušci	1
Velmi rizikoví fanoušci	4



Obrázek 24 - Graf rozložení klubů do jednotlivých kategorií rizikovosti

Z výše uvedených dat tedy vyplývá, že jsou v české lize minimálně čtyři velmi rizikové tábory fanoušků. Co je však znepokojující je fakt, že do mírně rizikové skupiny spadají pouze tři fanouškovské základny a celou polovinu, tedy osm klubů spadá do rizikové skupiny.

Z tohoto lze předpokládat, že v sezoně dochází k řadě utkání, která mohou být co do diváckého násilí skutečně riziková. Určením, do jaké míry utkání skutečně riziková jsou a kolik se takových utkání za jednu ligovou sezonu odehraje se zabývá následující kapitola.

8.1.2 Určení rizikovosti jednotlivých utkání

České nejvyšší fotbalové soutěže se účastní cekem 16 klubů. Tato soutěž se hraje dvoukolovým systémem, tedy tzv. doma x venku. Celkem se v sezoně odehraje 242 utkání. Cílem této kapitoly je určit míru rizika diváckého násilí jednotlivých utkání.

Průměrná návštěvnost na utkání české nejvyšší soutěže je 5 550 diváků za sezonu 2018-2019. Za jednu fotbalovou sezonu navštíví utkání celkem okolo 1 330 000 diváků.

Nejvíce navštěvovaná jsou utkání klubu SK Slavia Praha s průměrem 13 511 diváků na domácí utkání. Nejméně navštěvované jsou utkání klubu FK Mladá Boleslav s průměrem 2 850 diváků na domácí utkání.

Pro určení míry rizika jednotlivých utkání jsem použil křížovou tabulku, ve které je u každého klubu zapsán koeficient rizikovosti fanoušků. Ten se v tabulce křížem jednotlivě násobí s dalšími kluby.

**Poznámka: Data o počtu fanoušků na utkání jsou čerpána z oficiálních webových stránek FORTUNA:LIGA pro sezonu 2018-2019.*

Tabulka 5 - Míra rizika fotbalových utkání

Míra rizika fotbalových utkání

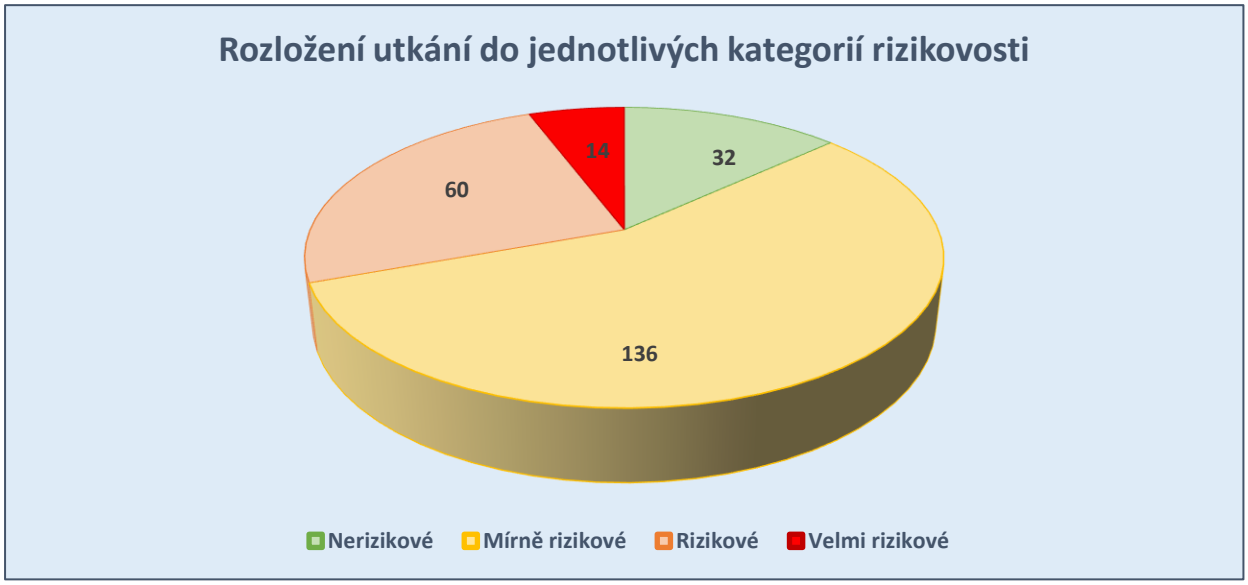
Seznam klubů s koeficientem rizika			1. FC Slovácko	1. FK Příbram	AC Sparta Praha	Bohemians Praha 1905	FC Baník Ostrava	FC Slovan Liberec	FC Viktoria Plzeň	FC Zastav Zlín	FK Jablonec	FK Mladá Boleslav	FK Teplice	MFK Karviná	SK České Budějovice	SK Sigma Olomouc	SK Slavia Praha	Slezský FC Opava
			8	6	22	18	23	14	22	12	13	10	13	9	11	13	21	13
			Podzimní část															
1. FC Slovácko	8	Jarní část		48	176	144	184	112	176	96	104	80	104	72	88	104	168	104
1. FK Příbram	6		48		132	108	138	84	132	72	78	60	78	54	66	78	126	78
AC Sparta Praha	22		176	132		396	506	308	484	264	286	220	286	198	242	286	462	286
Bohemians Praha 1905	18		144	108	396		414	252	396	216	234	180	234	162	198	234	378	234
FC Baník Ostrava	23		184	138	506	414		322	506	276	299	230	299	207	253	299	483	299
FC Slovan Liberec	14		112	84	308	252	322		308	168	182	140	182	126	154	182	294	182
FC Viktoria Plzeň	22		176	132	484	396	506	308		264	286	220	286	198	242	286	462	286
FC Zastav Zlín	12		96	72	264	216	276	168	264		156	120	156	108	132	156	252	156
FK Jablonec	13		104	78	286	234	299	182	286	156		130	169	117	143	169	273	169
FK Mladá Boleslav	10		80	60	220	180	230	140	220	120	130		130	90	110	130	210	130
FK Teplice	13		104	78	286	234	299	182	286	156	169	130		117	143	169	273	169
MFK Karviná	9		72	54	198	162	207	126	198	108	117	90	117		99	117	189	117
SK České Budějovice	11		88	66	242	198	253	154	242	132	143	110	143	99		143	231	143
SK Sigma Olomouc	13		104	78	286	234	299	182	286	156	169	130	169	117	143		273	169
SK Slavia Praha	21		168	126	462	378	483	294	462	252	273	210	273	189	231	273		273
Slezský FC Opava	13		104	78	286	234	299	182	286	156	169	130	169	117	143	169	273	

Popis rizikovosti utkání:

- 0-100 Nerizikové utkání;
- 100-250 Mírně rizikové utkání;
- 250-400 Rizikové utkání;
- 400 a více Velmi rizikové utkání;

Tabulka 6 - Počet utkání v jednotlivých kategoriích rizika

Kategorie rizikovosti	Počet utkání
Nerizikové utkání	32
Mírně rizikové utkání	136
Rizikové utkání	60
Velmi rizikové utkání	14



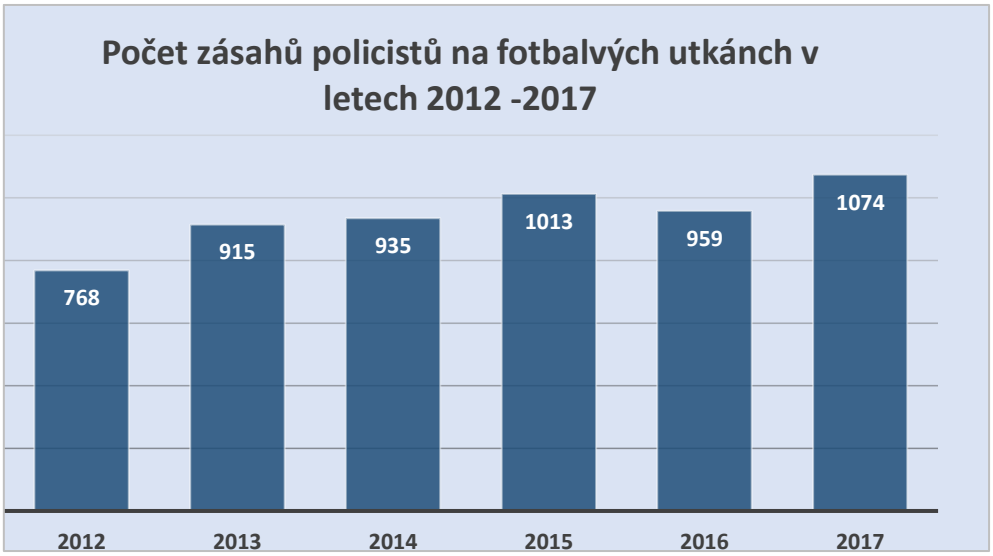
Obrázek 25 - Graf rozložení utkání do jednotlivých kategorií rizikovosti

Dle výše uvedených dat lze předpokládat, že se v sezóně odehraje 14 velmi rizikových utkání. Lze také předpokládat, že počet diváků na těchto utkáních bude vyšší než je návštěvnostní průměr, a to i téměř více jak 3x, tedy okolo 15 000 diváků, jelikož tato utkání jsou spojovaná s kluby, které mají vyšší návštěvnost. Celkem se tedy může jednat o 90 000 diváků na velmi rizikových utkáních za sezonu.

Rizikových utkání se v sezoně odehraje celkem 60. Zde bude předpokládaná návštěvnost o něco nižší, přesto však můžeme počítat, že bude zhruba 1,5x vyšší než průměr, tedy 8 325 diváků na jednom utkání. Cekem se může jednat o návštěvnost okolo 466 200 diváků na rizikových utkáních.

8.2 Počty zásahů PČR na utkání

Z veřejně dostupných informací Ministerstva vnitra, vyplývá, že počet zásahů PČR v letech 2012 až 2017 stále mírně stoupá. To i navzdory tomu, že od roku 2010 vyšel v platnost paragraf umožňující uložení alternativního trestu zákazu vstupu osoby na sportovní, kulturní a jiné společenské akce.



Obrázek 26 – Počet zásahů policie na fotbalových utkání sezón 2012-2017 [58]

Každý takový zákrok sebou nese značná rizika jak pro zasahující policisty, skupinu, proti níž je veden zákrok, ale i pro nezúčastněné osoby. S těmito zákroky jsou obvykle spojena zranění osob, škody na majetku a další náklady, které PČR ročně stojí miliony korun. Z veřejně dostupných informací se nepodařilo vyhledat počty zranění při zásazích nebo konkrétní částku vynaloženou na tyto zásahy.

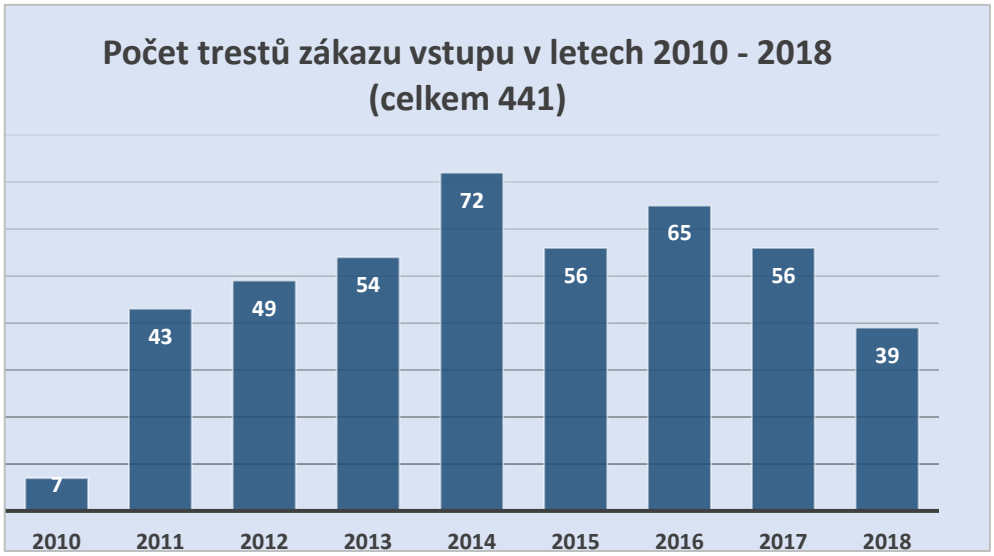
8.3 Soudně udělené zákazy vstupu

Od roku 2010 je možné díky úpravě legislativy uložit trest zákaz vstupu na sportovní, kulturní a jiné společenské akce, což v sobě zahrnuje samozřejmě i fotbalová utkání. Tato úprava je zakotvena v zákoně č. 40/2009 Sb., konkrétně ji řeší § 76 Zákaz vstupu na sportovní, kulturní a jiné společenské akce a § 77 Výkon trestu zákazu vstupu na sportovní, kulturní a jiné společenské akce [27]

Soud dle těchto paragrafů může uložit trest zákazu vstupu až na deset let při úmyslném spáchání trestného činu. Trest zákazu vstupu může být uložen zcela samostatně, bez dalších trestů. Na výkon trestu následně dohlíží probační a

mediační služba, jejíž úředník stanoví podmínky výkonu trestu. Jednou z podmínek může být například povinnost odsouzeného dostavit se v čase utkání ke kontrole na příslušný útvar PČR. [27]

Do roku 2018 bylo uděleno celkem 441 zákazů vstupu, z toho většina byla pro vstup na fotbalové stadiony. [28]



Obrázek 274 – Počet trestů zákazu vstupu v letech 2010–2018 [28]

Z těchto informací tedy vyplývá, že je v České republice dostatečná právní opora pro to, aby se dalo zamezit vstupu problémových fanoušků na stadiony. Značné zlepšení je ale třeba zajistit v prevenci, to znamená zajistit, že se tyto osoby skutečně na stadion nedostanou. Je potřeba si uvědomit že to, že má někdo stanoven zákaz vstupu, neznamená, že toto bude také dodržovat. Dále je potřeba myslet na to, že se jedná o soudně řešené osoby – zákaz vstupu určí až soud, což může v praxi trvat i několik měsíců.

Jiný případ nastává ve chvíli, kdy fanouškovi zakáže vstup na stadion samotný klub, na což má klub právo. Toto právo klubu vzniká na základě zakoupení vstupenky, čímž je uzavřen smluvní vztah mezi klubem a kupujícím, který je povinen se řídit návštěvním řádem. Klub už ale nemá žádný dobře fungující mechanizmus na vymáhání tohoto zákazu. Kvůli GDPR není možné například vyvěsit fotku člověka se zákazem vstupu u pokladny, ale fotku u sebe nesmí mít ani pořadatel u vstupní brány. Ostraha si může v nejlepším případě prohlédnout fotografie v zázemí.

Pořádající kluby už některé své problémové fanoušky znají, ale jistě ne zdaleka všechny. Problém také nastává při výjezdu těchto fanoušků na venkovní zápas. Kluby to částečně řeší tím, že vyšlou své pořadatele společně s fanoušky a ti mohou upozornit své pořádající kolegy na fanoušky, které by neměli pouštět na stadion. Toto je ale velmi neefektivní a reálný záchyt problémových fanoušků se pohybuje v nízkých procentech.

8.4 Vyhodnocení aktuálního stavu

Na základě zjištěných informací v této kapitole, se domnívám, že jsou v České republice nastavena opatření spíše represivního charakteru. Tato opatření jsou ale poměrně náročná na lidské zdroje, jsou drahá a nejsou ani příliš efektivní. Na tribunách se stále objevuje velké množství agresivních fanoušků, což dokazuje 74 utkání v kategorii velmi rizikové a rizikové.

Můj názor je, že chybí opatření spíše preventivní, která by vedla k snížení počtu agresivních fanoušků na tribunách a tím by se docílilo bezpečnějších fotbalových utkání. Což by sebou přineslo i další pozitiva, jako například zvýšení návštěvnosti rodin s dětmi.

Další část mé práce se bude tedy věnovat návrhu konkrétního opatření, které by zamezovalo přístupu agresivních fanoušků na stadiony, a svým řešením by bylo efektivnější než stávající represivní řešení.

9 Návrh řešení

9.1 Charakteristika řešení

Navrhované řešení má primárně pomoci k optimalizaci vymahatelnosti trestu zákazu vstupu na stadion. To znamená proces kontroly u vstupu přenést z pořadatelské služby do automatizovaného režimu. Tím se výrazně zvýší procento záchytu osob se zákazem vstupu, sníží se nároky na lidské zdroje, které mohou vykonávat jinou činnost v rámci pořadatelské služby a tím ji posílit v dalších oblastech vedoucích k celkovému zvýšení bezpečnosti na stadionu.

Podstata řešení je kontrola vstupu osob u vstupní brány kamerovým systémem, který má za úkol snímat obličej osoby. Takto nasnímaná data se v reálném čase porovnají s daty získanými před utkáním z centrální databáze (sdílená databáze všemi ligovými kluby) a pokud bude nalezena shoda s obličejem v databázi, bude osobě zamezen vstup, ideálně elektronickým turniketem napojeným na systém.

Databáze by obsahovala osoby, které již byly pravomocně odsouzené a byl jim uložen trest zákazu vstupu na stadiony. Takové řešení je dále možné rozšiřovat o další funkce, jako například vkládání osob přímo samotnými kluby, nebo tzv. bodování osob anebo označení osoby jako rizikové Takové osoby by například podléhaly důkladnější kontrole u vstupu, nebo byly průběžně při utkání sledovány ostrahou, nebo dokonce automaticky samotným kamerovým systémem.

Pro pilotní provoz bych doporučil nejprve implementovat systém, který bude splňovat základní funkce, tedy detekci a rozeznání obličeje a bude možné jej propojit s přístupovým systémem obsluhujícím turnikety. Pokud se toto řešení osvědčí a reálný provoz prokáže jeho skutečný přínos, navrhoval bych jej doplnit o další rozšiřující funkce pro podporu bezpečnosti.

9.2 Požadavky

9.2.1 Základní požadavky pro implementované řešení

- Centrální databáze a server
    - Serverová a databázová architektura systému bude koncipována formou centrálního serveru a databáze. Lze běhu na jednom hardware serveru s dvěma virtuálními servery (server – databáze). K tomuto centrálnímu serveru budou vzdáleně připojeny servery z jednotlivých stadionů.
- Možnost vkládání soudně trestaných osob
    - Do centrální databáze bude mít možnost uživatel s příslušným systémovým oprávněním vkládat osoby, které mají uložen trest zákazu vstupu na stadion. Tyto informace budou následně serverem poskytnuty pro servery jednotlivých stadionů. Pravděpodobně by v praxi takovým uživatelem byl některý ze státních subjektů.
- Automatické zamítnutí vstupu na stadion
    - Systém musí v reálném čase zpracovat data (obličej na vstupu) a vyhodnotit, zda lze povolit přístup, či nikoli. Je tedy podmínkou, aby bylo možné server na stadionu propojit se serverem přístupového systému stadionu, který ovládá turnikety.
- Rozšiřitelnost systému
    - Systém musí být možné dle potřeby uživatele zakázkově rozšířit o další funkce
- Kybernetická bezpečnost
    - Částečně uzavřený okruh
    - Provedení penetračních testů
    - Zabezpečení ochrany před neoprávněným manipulováním se zařízeními počítačového systému
    - Ochrana před neoprávněnou manipulací s daty
    - Ochrana informací před krádeží (nelegální tvorba kopií dat) nebo poškozením
- Vytváření provozních a auditních logů

- Třívrstvá architektura
    - Modularizace funkčnosti na malé služby, které půjdou samostatně testovat, vyvíjet, nasazovat, restartovat, a bude možné sledovat komunikace mezi službami
        - Prezentační vrstva
        - Aplikační vrstva
        - Datová vrstva
- Profylaxe systému
    - Pravidelná kontrola stavu serverů
    - Pravidelná kontrola logů systému
    - Pravidelná kontrola prostupnosti sítě a datového toku v síti

9.2.2 Další možné funkce k budoucímu rozšíření

Jedním ze základních požadavků je možná budoucí rozšiřitelnost systému, tak aby ho bylo možné uživatelsky a funkčně maximálně přizpůsobit potřebám uživatele. Sada možných doplňkových funkcí může být následující:

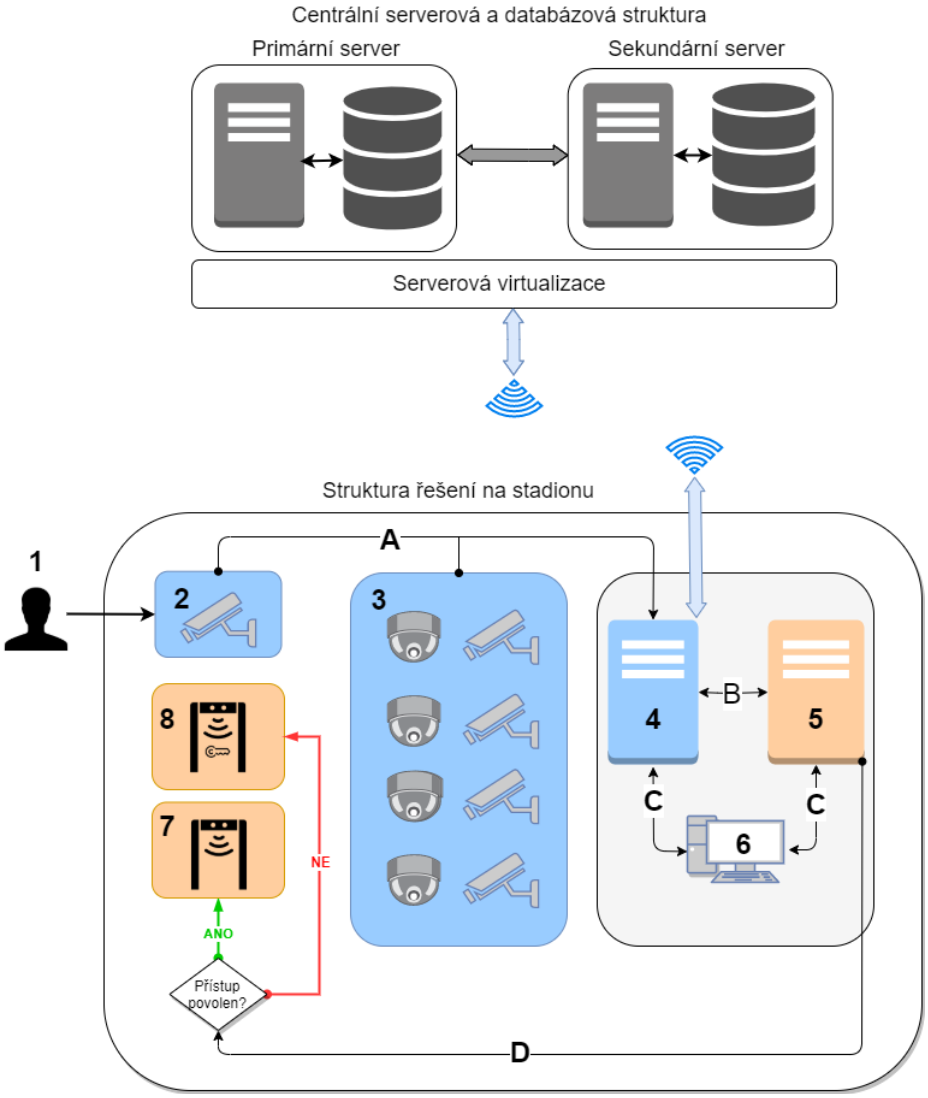
- Možnost vkládání osob kluby
    - Do systému by bylo možné vkládat nejen osoby se soudním trestem zákazu vstupu, ale samotné kluby by mohly zadat osobu, kterou na svůj stadion dále nechtějí pouštět. K takto označené osobě by bylo nutné vybrat důvod, pro jaký byla osoba do systému vložena a následně by toto bylo podřízeno schválení etické komise.
- Označení osoby jako rizikové
    - Klub by měl možnost označit osobu jako rizikovou. Takto označené osoby by následně měly podléhat důslednější kontrole u vstupu na stadion, nebo také průběžnému sledování pořadatelské služby na utkání. V optimálním případě by takto označené osoby mohly být automaticky sledovány kamerovým systémem na stadionu a průběžně vyhodnocováno jejich chování.
- Možnost bodování osob

    - Klub by měl mít možnost každé osobě udělovat tzv. trestné body. Obdobně jako tomu je u řidičského oprávnění. Podmínkou by bylo vznik „přestupků“ s bodovým hodnocením a stanovení maximální hranice bodového zisku, při jehož překročení by byl zamezen přístup na stadion. Takto „vybodovaná“ osoba by měla zákaz vstupu na stadion na předem definovanou dobu.
- Počítání osob v zónách
    - Jedná se o možnost nastavit libovolné zóny v objektu, kdy systém automaticky počítá počet osob v dané zóně. Pokud počet osob překročí maximální limit, systém na to uživatele upozorní. Dohled u monitorů tak může dát informaci ostraze, aby zamezila dalšímu vstupu osob do dané zóny.
- Virtuální střežené zóny
    - Kamerový systém dokáže v mnoha případech nahradit zabezpečovací systém právě funkcí střežení virtuálních zón. Uživatel si v obrazu vytvoří libovolné zóny, které může virtuálně zastřežit. Pokud do takto zastřežené zóny vstoupí osoba, systém vyhlásí alarm.
- Vyhledávání podezřelého chování
    - Možnost analýzy obrazu a automatické upozornění například na manipulaci s pyrotechnikou, či další nežádoucí chování.

9.2.3 Další podněty

Takto implementovaný systém lze nadále propojit například s adresným ticketingem, který je také jedním z diskutovaných řešení pro zamezení nechtěného chování fanoušků na stadionech. Pokud by byla tyto dvě opatření zavedeny a v budoucnu propojeny, je možné díky rozpoznání obličeje kamerou u pokladny zamezit už samotnému nákupu vstupenky. Toto je ale samostatné téma, které by bylo třeba samostatně analyzovat a sepsat návrh řešení.

9.3 Schéma řešení



Obrázek 28 - Schéma řešení systému

Legenda schématu:

1. Snímaná osoba
2. Kamera u turniketu pro snímání obličeje
3. Přehledové kamery uvnitř stadionu
4. Server kamerového systému
5. Server přístupového systému
6. Klientské PC s uživatelským rozhraním
7. Přístupový turniket – povoleno
8. Přístupový turniket – zamítnuto

A. Komunikace v rámci kamerového systému (jednotlivé kamery se serverem)
B. Komunikace mezi kamerovým serverem a serverem přístupového systému
C. Komunikace mezi servery a uživatelským PC
D. Komunikace v rámci přístupového systému (server – přístupové turnikety)

10 Výběr vhodného kamerového systému

Na českém i zahraničním trhu se nabízí řada dodavatelů systémů CCTV. Výrobci technologií většinou spolupracují se svými integračními partnery, kteří systémy implementují a následně pro zákazníka drží servisní podporu. Není příliš obvyklé, aby si koncový zákazník mohl objednat jednotlivé produkty či celá řešení přímo u výrobce.

Pro pilotní projekt rozpoznání obličeje na stadionu doporučuji minimálně tyto komponenty:

- Detekční kamery u vstupu na stadion
    - Pro potřeby detekce obličeje u vstupu na stadion je možné použít běžnou průmyslovou kameru. Rozpoznání obličeje bude zajišťovat následně software.
- Přehledové kamery v prostoru stadionu
    - Slouží pro monitoring dění mimo tribuny, např. přístupové uličky za tribunou, prostor před stánky s občerstvením atd. Pro tento účel jsou dostatečné běžné přehledové průmyslové kamery.
- Kamery pro sledování dění na tribunách
    - Pro sledování dění na tribunách bych doporučil panoramatické kamery. Ty zajistí nepřetržitý přehled v širokém poli záběru. Výhodou je, že pokud obsluha obraz přiblíží na konkrétní místo, zbytek scény je stále snímán a ukládán. Tyto kamery lze nahradit například kombinací přehledových statických a otočných kamer, ideálně s technologií fish eye.
- Záznamové zařízení
    - Záznamové zařízení musí splňovat možnost napojení SW třetích stran. Kapacita pro zápis je 72 h. Při dodržení této lhůty nemusí provozovatel žádat o povolení Státní úřad pro ochranu osobních údajů. Zároveň je to ale dostatečně dlouhá doba k tomu, aby mohl být obraz analyzován a případně předán k řešení Policii ČR.

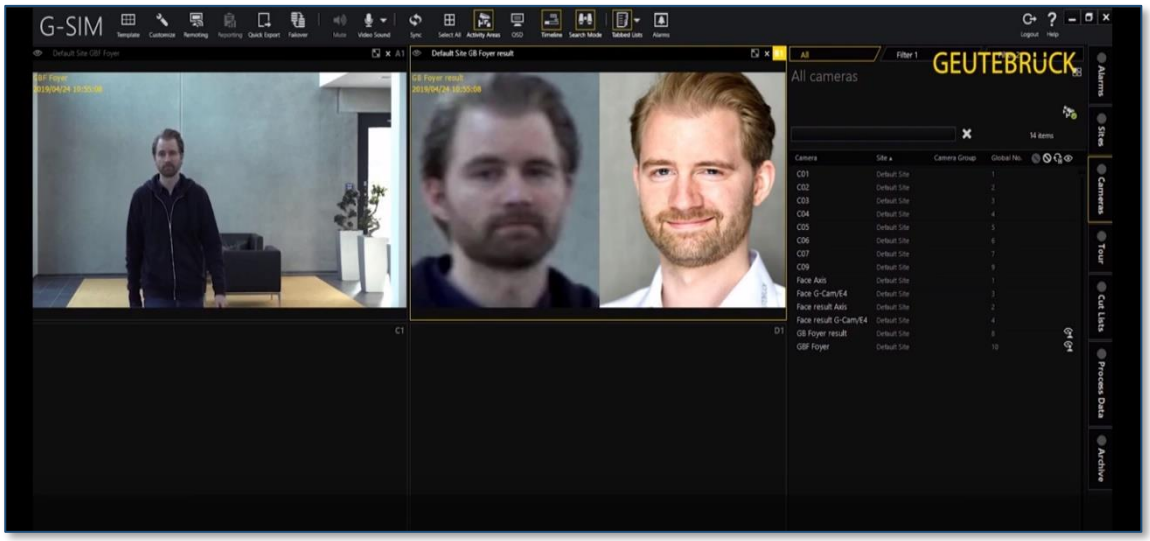
10.1 Vybraní výrobci na trhu

10.1.1 Geutebruck

Geutebruck je německá společnost založena roku 1970. Dnes má společnost zastoupení ve víc jak 70 zemích světa. Geutebruck se zabývá dodávkou řešení zabezpečení videa včetně kompletního hardware a software. Geutebruck také vyvíjí vlastní nadstavbový software k obsluze videa, jeho vyhodnocení a práci s ním. Výhodou je poskytnutí obrázků v proprietárním formátu gbf, který je soudně uznávaný jako oficiální důkaz ve většině zemí.

Nadstavbový systém je vybaven funkcemi pro detekci nejrůznějších objektů v obrazu. Detekce ochranných prostředků, počítání osob v objektu, automatické ovládání vstupu ale také rozpoznání a porovnání obličeje.

Systémy této společnosti jsou nasazovány především na rozsáhlé instalace obsahující vysoké stovky až tisíce kamer. Významné reference sbírá tato společnost instalacemi v muzeích, projekty pro státní správu, zabezpečením promyslových objektů a také zabezpečením prvků kritické infrastruktury. Jednou z největších referencí je instalace kompletního kamerového dohledu v Pražském metru. V české republice má tato společnost řadu partnerů, jedním z nejznámějších je spol. SCANLOG. [29]



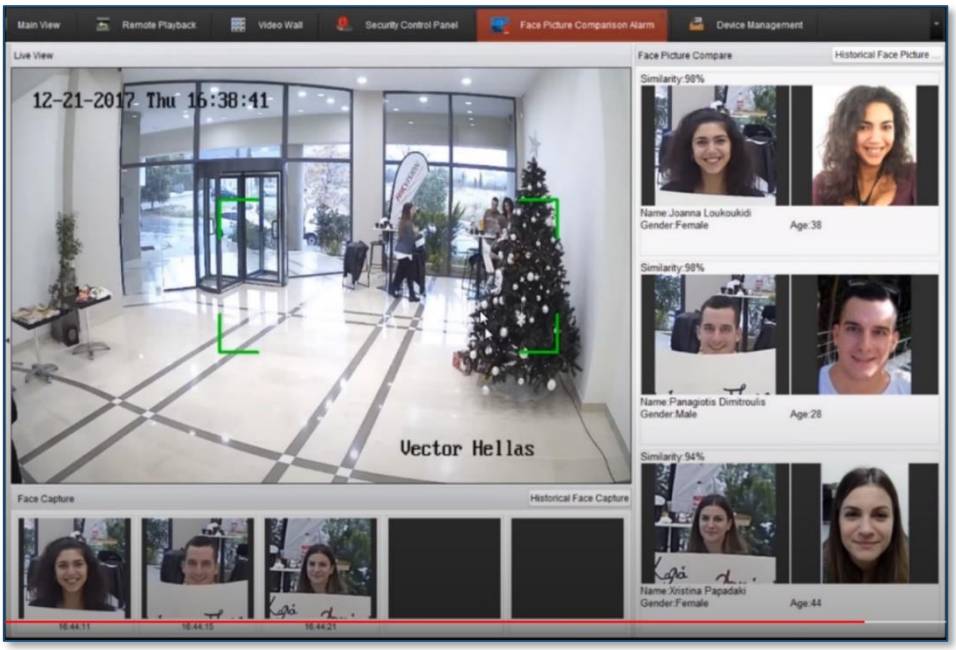
Obrázek 29 - Rozpoznání obličeje systémem Geutebruck [29]

10.1.2 HIK Vision

HIK Vision je společnost založena v roce 2010. Za dobu svého působení se stal jedním z předních světových poskytovatelů bezpečnostních produktů a ucelených řešení. HIK Vision klade velký důraz na vývoj a inovace svých produktů, to dokazuje každoroční investice okolo 8 % svého ročního obratu do výzkumu a vývoje. Centra výzkumu a vývoje jsou rozmístěna po celém světě.

HIK Vision vytvořil jednu z nejrozsáhlejších sítí podpory v oboru. Ta zahrnuje desítky regionálních dceřiných společností po celém světě, což zajišťuje rychlé reakce na potřeby zákazníků, uživatelů a partnerů.

Společnost má za sebou také řadu významných referencí. Své systémy provozují rozsáhlé průmyslové objekty, státní správa, ale v kontextu problematiky této práce je zásadní reference spolupráce s fotbalovými kluby po celém světě. HIK Vision spolupracuje s argentinským klubem Atlético Boca Juniors, pro něž řeší celkové zajištění bezpečnosti na stadionu. Součástí řešení není rozpoznání obličeje. Systémy HIK Vision jsou ale dobře koncipovány pro možnost integrace do systémů třetích stran. [30]



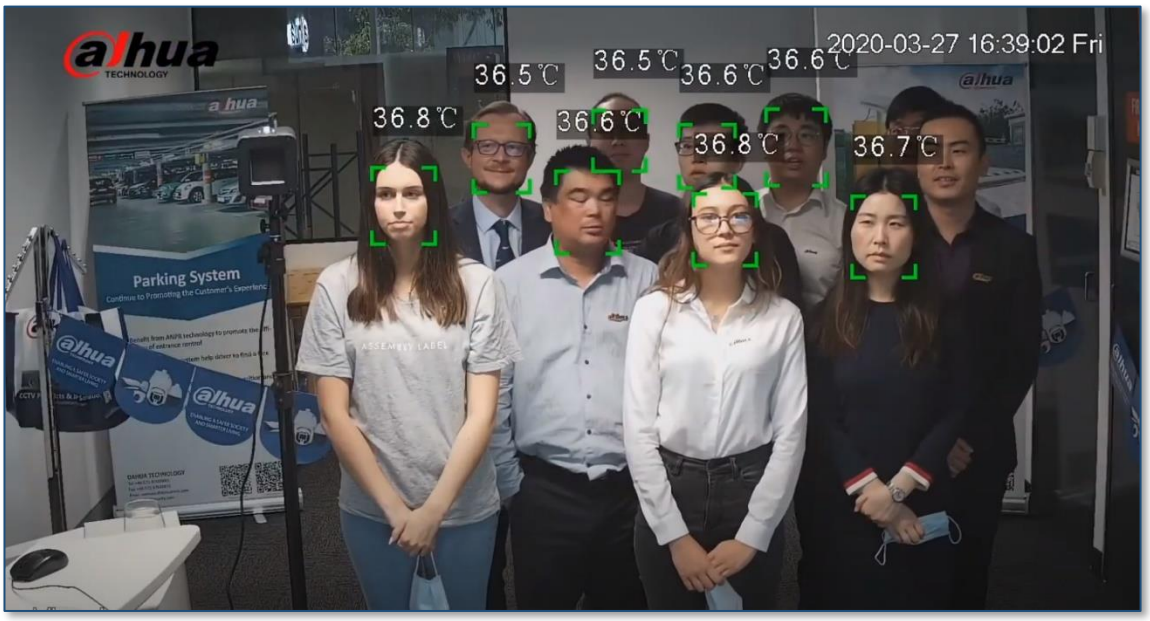
Obrázek 30 - Rozpoznání obličeje systémem HIK Vision [30]

10.1.3 Dahua

Dahua je čínská společnost, která se stala v roce 2008 veřejně obchodovatelnou na burze cenných papírů. Společnost nabízí svým zákazníkům komplexní řešení bezpečnosti především pro firemní správu a spotřebitele. I když se Dahua snaží prosadit ve velkých průmyslových instalacích, veřejné správě a dalších, není zatím plnohodnotným konkurentem světově silných značek jako například HIK Vision nebo Geutebruck.

V posledních několika letech se společnosti ale daří své jméno stále více prosazovat. Zásluhu na tom má vlastní vývoj a inovace, do které Dahua investuje značnou část svých příjmů. Pro své zákazníky budují po celém světě partnerskou síť dodavatelů.

Produkty Dahua jsou založeny na otevřené platformě, která nabízí snadnou integraci s partnery třetích stran prostřednictvím standardní sady SDK. Pokud se Dahue podaří nastolený trend udržet, lze předpokládat, že se z ní za několik let stane skutečně silný hráč na trhu. [31]



Obrázek 31 – Ukázka zpracování obrazu Dahua s měřením tělesné teploty [31]

10.1.4 Siemens

Siemens je jednou z největších technologických společností. V české republice má již více jak 125 let trvající tradici. Společnost Siemens se nezabývá výhradně kamerovými systémy, ale ve svém portfoliu pokrývá technologické řešení v oblasti průmyslu, energetiky, dopravy, veřejné infrastruktury a v posledních letech i tzv. Smart City.

Předností dodávek Siemens je kompletní technologické pokrytí spočívající v optimalizaci fungování budov, technických procesů apod. Odvětví kamerových systémů je pro Siemens jednou z řady oblastí, na které se společnost zaměřuje. Pokud se podíváme na opravdu rozsáhlé instalace v řádu tisíců kamer, nebo dodávku pouze kamerového systému, obvykle nebude Siemens hlavním dodavatelem celého řešení, ale jeho komponenty se pravděpodobně v řešení objeví.

Obrázek 32 - Ukázka dohledového systému Siemens ([59]

10.2 Vyhodnocení vhodnosti pro nasazení v projektu

Pro objektivní kvalifikaci vhodného systému, který by mohl být použit při implementaci navrhovaného řešení jsem se rozhodl využít metodu bazické varianty. Touto metodou sestavím pořadí systému od nejvhodnějšího po nejméně vhodný. Alternativy, mezi kterými se budu dále rozhodovat, jsou výše popsané systémy.

10.2.1 Hodnotící kritéria a výpočet jejich vah

Hodnotící kritéria jsem zvolil po konzultaci s bezpečnostními manažery v Dopravním podniku hlavního města Prahy, kde aktuálně probíhá také projekt modernizace kamerových systémů, takže otázku výběru dodavatele řešili v nedávné minulosti. Dále jsem toto konzultoval s manažerem stadionu Generali aréna v Praze, který mi sdělil jaké priority by bylo potřeba zohlednit při výběru.
Seznam kritérií použitých pro rozhodování:

- Spolehlivost systému
- Reference
- Cena řešení
- Zajištění dlouhodobého servisu
- Náročnost provozu
- Nativní funkce rozpoznání obličeje
- Možnost integrace do nadstavbového systému třetí strany

Pro určení váhy každého z kritérií jsem použil Saatyho metodu. Základní preference plynoucí z řízených rozhovorů s bezpečnostními manažery zmíněnými v předešlém odstavci vyplynulo, že:

- spolehlivost je absolutně preferovaná reference;
- cena řešení je silně preferovaná před náročností provozu;
- nativní rozpoznání obličeje je velmi silně preferovaná funkce před možností integrace do systému třetích stran.

Dále pro Saatyho metodu platí jedinečná škála preferencí:

- 1 = Rovnocennost
- 3 = Slabá preference
- 5 = Silná preference
- 7 = Velmi silná preference
- 9 = Absolutní preference

Tabulka 8 – Určení hodnoty kritéria Saatyho metodou

Určení hodnoty kritéria									
Hodnotící kritéria	Spolehlivost systému	Reference	Cena řešení	Zajištění dlouhodobého servisu	Náročnost na provoz	Nativní funkce rozpoznání obličeje	Možnost integrace do nadstavbového systému třetích stran	Geometrický průměr	Váha kritéria
Spolehlivost systému	1	9	3	1/5	7	5	1/3	3,98	0,21
Reference	1/9	1	1/7	3	1/3	5	1/5	0,25	0,01
Cena řešení	1/3	7	1	3	5	7	5	10,70	0,57
Zajištění dlouhodobého servisu	5	1/3	1/3	1	3	1/5	7	2,33	0,12
Náročnost na provoz	1/7	3	1/5	1/3	1	3	5	0,75	0,04
Nativní funkce rozpoznání obličeje	1/5	1/5	1/7	5	1/3	1	7	0,41	0,02
Možnost integrace do nadstavbového systému třetích stran	3	5	1/5	1/7	1/5	1/7	1	0,23	0,01
							CELKEM	18,65	1,00

Tabulka 7 – Pořadí kritérií dle hodnoty váhy

Pořadí kritérií dle hodnoty		
Pořadí	Kritérium	Váha
1	Cena řešení	0,57
2	Spolehlivost systému	0,21
3	Zajištění dlouhodobého servisu	0,12
4	Náročnost na provoz	0,04
5	Nativní funkce rozpoznání obličeje	0,02
6	Reference	0,01
8	Možnost integrace do nadstavbového systému třetích stran	0,01

Výběr systému pomocí bazické varianty

Metoda Bazické varianty vyjadřuje vztah hodnocení kritérií vůči tzv. bazické variantě. Pro bazickou variantu hodnotitel vybere buď nejlepší nebo předem požadované hodnoty. Výhodou vyjádření hodnoty vůči bazické variantě je zobjektivnění hodnocení. Pro výpočet kompromisní, tedy bazické varianty jsou použity váhy hodnot zjištěných v předešlé kapitole Saatyho metodou.

Tabulka 9 – Tabulka přiřazení hodnot

Tabulka přiřazení hodnot							
	Spolehlivost systému	Reference	Cena řešení	Zajištění dlouhodobého servisu	Náročnost na provoz	Nativní funkce rozpoznání obličeje	Možnost integrace do nadstavbového systému třetích stran
Geutebruck	7	8	10	9	8	7	2
HIKVision	6	10	8	8	8	6	5
Dahua	5	6	7	7	6	2	10
Siemens	6	6	8	9	6	2	8
Váhy	0,21	0,01	0,57	0,12	0,04	0,02	0,01
Povaha	MAX	MAX	MIN	MAX	MIN	MAX	MAX

V tabulce pro přiřazení hodnot jsou dále určeny povahy – maximální a minimální. Tyto povahy určují, zda je kritérium posuzováno jako nejlepší pro nejvyšší hodnotu, nebo naopak pro nejnižší.

Postup při výpočtu bazické varianty:

1. Nejprve byla určena tzv. báze (ideální varianta). Báze se rovná nejlepší hodnotě ze sloupce. Ve sloupcích s povahou MAX to jsou nejvyšší hodnoty, naopak s povahou MIN ty nejnižší.
2. Následně byly do tabulky doplněny jedničky na místa, kde se hodnota ve sloupečku rovná bázi pro daný sloupeček.
3. Dále byly dopočítány zbylé hodnoty pomocí dvou vzorců:
    a. Pro sloupečky s MAX povahou:

$$MAX = \frac{Původní\ hodnota}{Báze}$$

b. Pro sloupečky s MIN povahou:

$$MIN = \frac{Báze}{Původní\ hodnota ze}$$

4. Předposledním krokem byl dopočet hodnoty W. V metodě bazické varianty se W rovná skalárnímu součinu mezi hodnotami v tabulce a váhami pro jednotlivá kritéria.

Příklad: pro řádek Geutebruck je vzoreček následující:

$$W = 1 \times 0{,}21 + 0{,}8 \times 0{,}01 + 0{,}7 \times 0{,}57 + 1 \times 0{,}12 + 075 \times 0{,}04 + 7 \times 0{,}02 + 0{,}2$$

5. Nakonec tedy W s nejvyšší hodnotu je naším kompromisním řešením. V terminologii této metody jsem určil bazickou variantu.

Tabulka 10 – Tabulka pro výpočet kompromisní – bazické varianty

Tabulka pro výběr systému dle bazické varianty								
	Spolehlivost systému	Reference	Cena řešení	Zajištění dlouhodobého servisu	Náročnost na provoz	Nativní funkce rozpoznání obličeje	Možnost integrace do nadstavbového systému třetích stran	W
Geutebruck	1	0,80	0,70	1	0,75	7	0,20	0,91
HIKVision	0,86	1	0,88	0,89	0,75	0,86	0,5	0,85
Dahua	0,71	0,60	1	0,78	1	0,29	1	0,88
Siemens	0,86	0,60	0,875	1	1	0,29	0,80	0,86
Váhy	0,21	0,01	0,57	0,12	0,04	0,02	0,01	
Povaha	MAX	MAX	MIN	MAX	MIN	MAX	MAX	
Báze	7	10	7	9	6	7	10	

Tabulka 11 – Pořadí systémů dle bazické varianty

Pořadí systémů		
Pořadí	Kritérium	W
1	Geutebruck	0,91
2	Dahua	0, 88
3	Siemens	0,86
4	HIKVision	0,85

10.2.2 Vyhodnocení

V rámci této kapitoly byla řešena otázka výběru nejvhodnějšího systému pro následující modelaci nasazení na reálný stadion. Pro zúžení systémů, které se na českém i zahraničním trhu nabízí, byl proveden řízený rozhovor se zkušenými servisními techniky, kteří z řady systémů vybrali čtyři k následnému posouzení. Jedná se o systémy Geutebruck, HIK Vision, Dahua a Siemens.

Dalším řízeným rozhovorem, tentokrát s bezpečnostními manažery, byly určeny kritéria, dle kterých bylo na tyto systémy nahlíženo. Cílem rozhovorů bylo také k těmto kritériím přiřadit priority a hodnoty, což bylo dále použito pro potřebné výpočty.

K udržení objektivity jsem se rozhodl určit ještě před samotným zjištěním bazické varianty i objektivní hodnoty. K tomu byla použita Saatyho metoda. S touto ucelenou škálou informací jsem přistoupil k určení bazické varianty v samostatné tabulce.

Výsledkem tohoto komplexního procesu je zjištění, že nejvhodnější z posuzovaných systémů je systém Geutebruck. Proto jsem další modelace vytvořil na základě tohoto systému.

11 Realizace projektu s vybraným systémem

11.1 Draft projektu

Modelace projektu bude provedena na jednom stadionu splňujícím standardy UEFA kategorie 4 a vyšší. V rámci modelace bude stanoven cenový předpoklad dodávky řešení a harmonogram dodání řešení.

V modelaci projektu bude počítáno s variantou bez doplňkových funkcí software, tedy půjde čistě o implementaci kamerového systému s detekcí obličeje navázaného na přístupový systém a centrální databázi nežádoucích osob.

Cílem je ověřit, jak významný dopad bude mít instalace tohoto systému na zlepšení bezpečnostní situace na stadionu. Toto budu dále ověřovat metodou posouzení nákladů a výnosů, případně jinou obdobnou metodou.

11.2 Standardy UEFA

Standardy stadionů v rámci UEFA kategorizace jsou obsaženy ve směrnicích o infrastruktuře stadionů UEFA. Dle této směrnice jsou stadiony rozděleny do čtyř kategorií ve vzestupném pořadí. UEFA nezveřejňuje seznamy stadionů, které splňují kritéria pro některou z kategorií definovaných v nařízení o infrastruktuře stadionů UEFA.

Kritérií, dle kterých jsou stadiony hodnoceny je nemalé množství. Krom kritérií jako je počet míst k sezení, velikost hrací plochy, nebo parametry osvětlení jsou posuzovány také např. kritéria, zda je stadion vybaven elektronickými turnikety, počet míst k parkování, počet pracovních ploch pro pres atd.

Stadion spadající do kategorie 4 musí mimo dalších kritérií splňovat tyto požadavky:

- Hrací plocha minimálně 105 m dlouhá, 68 m široká
- Minimální osvětlení
    - 1400 E h (lx) horizontální osvětlení jednotnost poměry U1h> 0,5

- U2h> 0,7 1000 E v (lx) vertikální osvětlení jednotnost poměry U1h> 0,4 a U2h> 0,5
- Elektronické turnikety s kontrolou vstupenek
- Bez míst pro stání diváků
- Minimální kapacita 8 000 míst k sezení
- VIP parkování pro 150 vozů

11.3 Stadion pro modelaci projektu

Na základě výše uvedených kritérií a po prostudování směrnice o infrastruktuře stadionů UEFA, jsem se rozhodl modelovat studii pro stadion Generali Aréna, kde hraje domácí zápasy klub AC Sparta Praha. Zároveň utkání tohoto klubu vyšla v analýze rizikovosti jako jedny z nejrizikovějších. S přihlédnutím k těmto důvodům se domnívám, že je tato volba adekvátní.

11.3.1 Popis stadionu

11.3.1.1 Historie

První stadion byl zhotoven z dřevěné konstrukce a otevřen roku 1921. V roce 1934 byla jeho kapacita rozšířena na 45 000 diváků, v tomto roce také vyhořela hlavní tribuna. O tři roky později byla otevřena nová hlavní tribuna z železobetonové konstrukce, která je dnes cennou historickou památkou. Zásadní rekonstrukce proběhla v letech 1967 a 1969. Byly postaveny nové ocelové tribuny, které integrovaly západní hlavní tribunu.

11.3.1.2 Zajímavost

Hrací plocha stadionu je zahloubena o 2,9 m pod úroveň okolního terénu. To z hlediska výšky stadionu umožnilo udržení horizontu sousedních domů. Nový sparťanský stadion byl první v naší fotbalové historii, který neměl hlediště a hřiště oddělené plotem.

11.3.1.3 Poloha

Stadion se nachází v centrální části Prahy 7. Stadion je ohraničen významnou komunikační tepnou Milady Horákové a městským parkem Stromovka. V blízkosti stadionu se nachází dvě stanice metra (Hradčanská a Vltavská), tramvajová stanice Sparta a také rozlehlé parkoviště.

Obrázek 33 - Poloha stadionu Generali Aréna

11.3.1.4 Technické informace

- Kapacita: 18 185 diváků
- Počet vstupů: 5
- Počet turniketů: 17

Obrázek 34 - Plánek stadionu Generali aréna

11.4 Řešení implementace na stadionu

Dle výše popsaného rámce řešení bude na stadionu nasazena verze řešení se základními požadavky s komponentami spol. Geutebruck. Pro řešení předpokládám využití stávající infrastruktury, čímž se značně sníží náklady. S využitím stávajícího kamerového systému se pro tuto dodávku primárně nepočítá. Důvodem je sjednocení celého řešení pod jednoho výrobce, které povede k zjednodušení servisních prací a celkovému užívání.

Řešení tedy spočívá v instalaci dvou přehledových kamer ke každému vstupu. Tyto kamery nebudou samy o sobě vyhodnocovat tvář, ale odešlou obraz do záznamového zařízení, kde tvář rozpozná a vyhodnotí k tomu určený SW. Takto získaná data se porovnají s daty z centrální databáze nežádoucích osob, která se zpřístupní vždy před započetím vstupu fanoušků na stadion před utkáním. Dodávka centrální serverové a databázové struktury není předmětem dodávky této modelace. Dále budou instalovány přehledové kamery k monitoringu dění vně stadionu a vybrané kamery pro monitoring tribun.

Kamerový server a server elektronické kontroly vstupů který ovládá turnikety budou vzájemně propojeny včetně nastavení automatického otevření či uzamčení turniketu v závislosti na poskytnutých datech z kamerového systému. Na stadionu jsou v současné době elektronické turnikety, které možnost propojení umožňují, nejsou tedy předmětem dodávky řešení.

Získané záznamy budou uchovávány na lokálním serveru po dobu 72 h. Po uplynutí této doby budou automaticky smazány. Seznam nežádoucích osob bude v centrální databázi zpřístupněn dvě hodiny před zahájením utkání.

11.4.1 Specifikace položek dodávky a cenový rozpis

Tabulka 12 – Specifikace položek dodávky a cenový rozpis

Specifikace položek dodávky a cenový rozpis					
Seznam položek	**Parametry**	**Poznámka**	**Počet ks**	**Cena za kus**	**Cena celekm**
Server					
G-ST 800+	16x HDD, 2x SSD, CPU NEXON, 320 TB, DVI-D, 2x zobrazovací port, 2 x rozhraní Ethernet 10/100/1000 base-TX	Počítáno se záznamem všech kamer v jejich nevyšším rozlišení s délkou uchování záznamu 72h. V ceně zahrnuta licence operačního systému Windows server 2016 esentials.	2	90 000 Kč	180 000 Kč
Pevný disk SATA RAID HT helium	10 TB, S-ATA 6 Gbit / s, 5400 ot / min	V konfuguraci Raid1 (10x10TB disků - 5 disků pro záznam, 5 disků pro redundanci)	10	9 900 Kč	99 000 Kč
Kamerypro pokrytí turniketů					
G-Cam/ESD-4230 Bundle	Efektivní pixely 2720 x 1536, Mega pixel 4MP, Obrazový snzor 1/3, Formát obrázku 16:9, Snímková frekvence (plné rozlišení)H.264 / H.265 w / HDR: 4M @ 30fps + 2M @ 30fps, Živé vysílání videaSingle, Dual, Triple, Quad	Na stadionu je aktuálně 5 vstupů. Na každý vstup jsou počítány dvě kamery, což zajistí plné pokrytí prostoru okolo přístupových turniketů a to s dostatečnou rezervou v případě zvýšení počtu turniketů u jednoho vstupu. Detekci a rozpoznání obličeje neprovádí kamera, ale SW.	10	19 000 Kč	190 000 Kč
Kamery pro pokrití tribun					
G-Cam/ESD-4230 Bundle	Efektivní pixely 2720 x 1536, Mega pixel 4MP, Obrazový snzor 1/3, Formát obrázku 16:9, Snímková frekvence (plné rozlišení)H.264 / H.265 w / HDR: 4M @ 30fps + 2M @ 30fps, Živé vysílání videaSingle, Dual, Triple, Quad	Počítáno se třemi kamerami na delší straně tribuny a se dvěmi na kratších stranách. Tyto kamery budou doplněny o otočné modely s funkcí tzv. střežení.	10	19 000 Kč	190 000 Kč
G-Cam/EHC-4888	Mega pixely 12MP, Obrazový senzor1 / 1,7 "progresivní CMOS, Formát obrázku16: 9, Čočkaf = 1,65 mm (fish eye)	Počítáno po jednom kusu na dlouhou stranu tribuny. Díky technologii fish eye dokáže snímat ve velmi vysokém detailu okolí v 360°rozsahu.	2	95 000 Kč	190 000 Kč
Kamery pro pokrytí vnitřích prostor					
G-Cam/EWPC-4250	Efektivní pixely2720 x 1536, Mega pixel4 MP, Formát obrázku16: 9, Rychlost obrázkuMJPEG: 1080p @ 30 fps, Detekce pohybu4 zóny	Počet kamer je odhadnut na základě půdorysného plánu stadionu. Konečný počet kamer se může lišit v závyslosti na konkrétní potřebě monitoringu ve vztahu k členění prostor.	40	8 500 Kč	340 000 Kč
Licence					
SW modul pro rozpoznání tváře G-tect VCABridge	Licence zahrnuje možnost připojení jednoho serveru (G-ST 800+), přístup pro 5 klientských účtů a neomezený počet připojených kamer.	Využito bude prvotně deset licencí. Šestnáct licencí je dostatečné pro možné budoucí rozšíření počtu vstupů.	1	59 000 Kč	59 000 Kč
G-Core	serveru (G-ST	Licence pro nahrávání záznamu a spouštění živého obrazu z kamer včetně jeho správy. Výhodou je přívětivé uživatelské rozhraní, které zařučije jednoduché a intuitivní ovládání.	1	250 000 Kč	250 000 Kč
Infrastruktura					
SWITCH Cisco WS-C2960 48GC-L		Centrální switch připojen do stávající infrastruktury	1	38 600 Kč	38 600 Kč
SWITCH Cisco SG100-16		Dílčí switch	3	6 000 Kč	18 000 Kč
Klientská pracoviště					
Sestava PC	CPU I7, 24GBRAM, 1xHDD, GPU invidia Gforce RTX 2070	Sestava PC včetně dvou monitorů a dvou přehledových monitorů	1	65 000 Kč	65 000 Kč
Seznam služeb	**Popis služby**	**Poznámka**	**Počet MD**	**Cena za MD**	**Cena celkem**
Implementační úkony					
Instalace HW	Montáž kamer a serverové infrastruktury		45	4 800 Kč	216 000 Kč
Oživení systému	Instalace SW, připojení kamer do SW, nastavení systému		15	5 900 Kč	88 500 Kč
Zkušební provoz	Parametrizace systému, přizpůsobení porvpzním podmínkám (různé denní doby a světelné podmínky)		10	5 900 Kč	59 000 Kč
				Celkové předpokládané náklady na realizaci	**1 983 100 Kč**

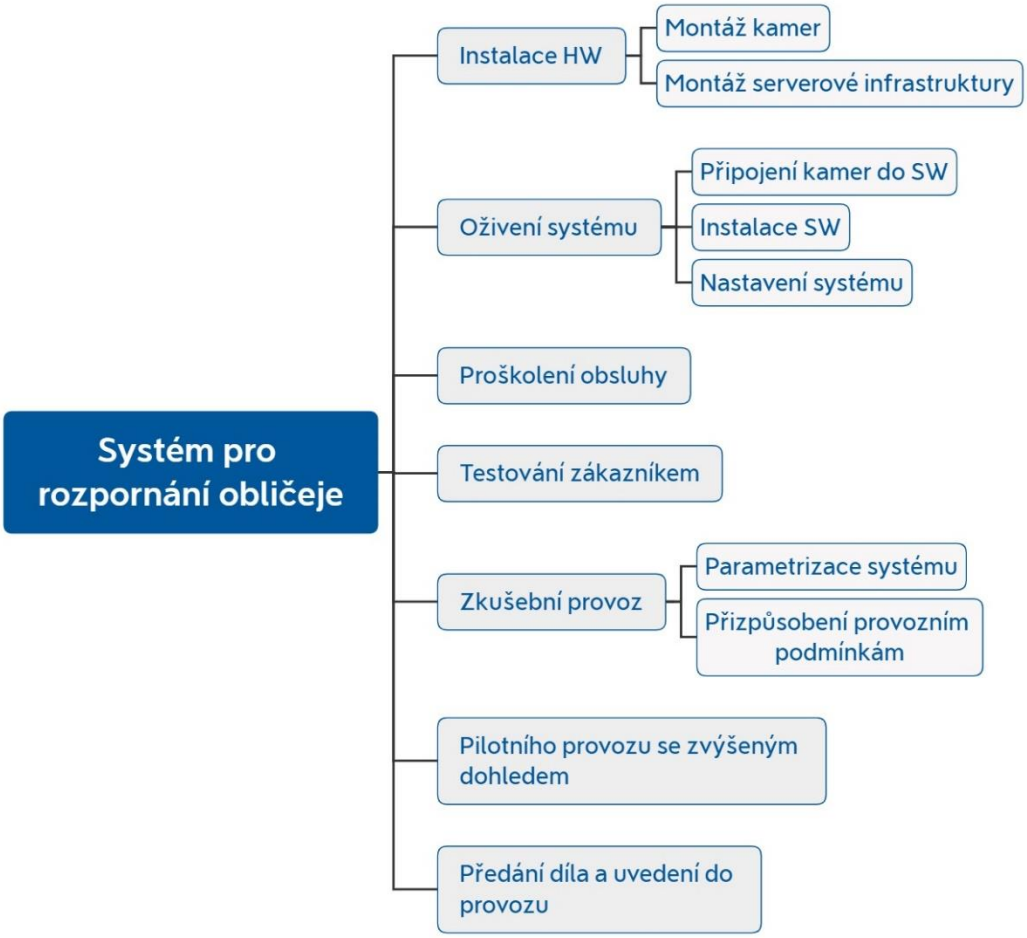
Specifikaci položek a služeb jsem konzultoval s technickým specialistou, který je jedním z implementátorů systému Geutebruck. Seznam položek je sestaven tak, aby splnil základní verzi požadavků. Počet kusů jednotlivých položek může být v rámci implementace korigován v závislosti na členitosti prostředí tak, aby bylo dosaženo požadovaného cíle. Při korekci položek musí být dodrženo navýšení rozpočtu maximálně o 5 % z předpokládané ceny. [32]

Celková předpokládaná cena řešení je 1 983 100,- Kč. V ceně jsou započítány jak náklady na HW a SW, tak ale i na služby zajišťující dodání a implementaci. Při dodržení navýšení o maximálně 5 % by celková cena činila 2 082 255,- Kč.

Cena řešení zahrnuje testovací provoz u zákazníka, proškolení obsluhy a zvýšený servisní dohled při pilotním provozu.

11.4.2 Harmonogram

11.4.2.1 Produktový rozpad dodávky (PBS)



Obrázek 35 - Produktový rozpad dodávky

11.4.2.2 Časové ohodnocení položek PBS

Produktový rozpad dodávky (PBS) byl vytvořen na základě mých zkušeností s projektovým řízením obdobného typu dodávek a znalostí metodiky PRINCE II. Odhady časových rozmezí byly následně konzultovány s techniky, kteří kamerové systémy implementují.

Celou dodávku bych navrhoval realizovat v čase od konce června, kdy končí jarní část soutěže a tím celá soutěž. Během červencové a srpnové pauzy je reálné systém připravit na testování a pilotní provoz včetně proškolení obsluhy. Při následném startu soutěže od cca poloviny srpna budou následovat kroky testování, zkušebního provozu a předání. Předpoklad dodání celého řešení je do konce října. Celá implementace by tedy měla trvat okolo 4 měsíců. Při implementaci v navrhovaném období bude možné systém pilotně spustit pro reálná utkání. V tuto dobu ale musí být ze strany dodavatele zvýšený dohled a pořadatel musí být připraven na variantu selhání systému a okamžitého přepnutí na „starý „režim vstupu.

Časový odhad náročnosti implementace:

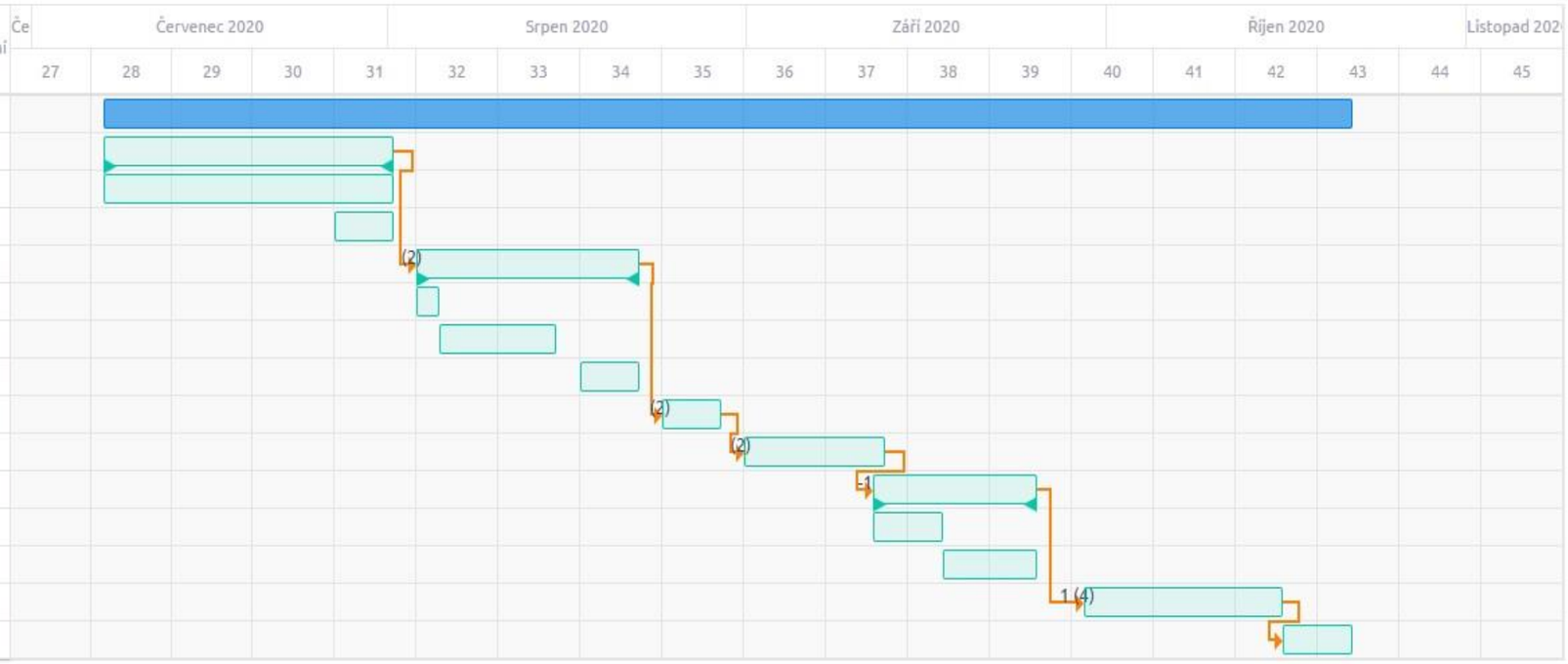
Tabulka 13 - Časové odhady implementace dodávky

Časový odhad náročnosti implementace				
Předmět úkolu	**Náročnost v MD (pro dodavatele)**	**Počet pracovníků**	**Začátek**	**Datum dokončení**
Instalace HW	**45**		07.07.2020	31.07.2020
Montáž kamer	40	4	07.07.2020	31.07.2020
Montáž serverové infrastruktury	5	1	27.07.2020	31.07.2020
Oživení systému	**15**		03.08.2020	21.08.2020
Instalace SW	2	1	03.08.2020	04.08.2020
Instalace kamer do SW	8	1	05.08.2020	14.08.2020
Nastavení systému	5	1	17.08.2020	21.08.2020
Proškolení obsluhy	**5**	1	24.08.2020	28.08.2020
Testování zákazníkem	**3**	1	31.08.2020	11.09.2020
Zkušební provoz	**10**		11.09.2020	24.09.2020
Parametrizace systému	5	1	11.09.2020	16.09.2020
Přizpůsobení provozním podmínkám	5	1	17.09.2020	24.09.2020
Pilotní provoz se zvýšeným dohledem	**20**	2	29.09.2020	15.10.2020
Předání díla a uvedení do provozu	**5**	1	16.10.2020	21.10.2020

Poznámka: MD je jednotka pracnosti odvozená z anglických slov Man Day. Do češtiny překládáno jako člověko-den. V projektovém řízení se také používá jednotka MH odvozená od Men Hours, čili člověko-hodina.

11.4.2.3 Vizualizace harmonogramu včetně návazností

Předmět úkolu	Začátek	Datum dokončení
Implementace systému pro rozpoznání obličeje		
Instalace HW	07.07.2020	31.07.2020
Montáž kamer	07.07.2020	31.07.2020
Montáž serverové infrastruktury	27.07.2020	31.07.2020
Oživení systému	03.08.2020	21.08.2020
Instalace SW	03.08.2020	04.08.2020
Instalace kamer do SW	05.08.2020	14.08.2020
Nastavení systému	17.08.2020	21.08.2020
Proškolení obsluhy	24.08.2020	28.08.2020
Testování zákazníkem	31.08.2020	11.09.2020
Zkušební provoz	11.09.2020	24.09.2020
Parametrizace systému	11.09.2020	16.09.2020
Přizpůsobení provozním podmínkám	17.09.2020	24.09.2020
Pilotní provoz se zvýšeným dohledem	29.09.2020	15.10.2020
Předání díla a uvedení do provozu	16.10.2020	21.10.2020



Obrázek 36 - Harmonogram dodání řešení

Poznámka: Při uvažování o časové rámci projektu je nutné počítat s tím, že pokud úkol vyžaduje např. 10MD a tento úkol budou realizovat 2 pracovníci, neznamená to vždy, že úkol splní za 5 dní. Musíme počítat s prostoji při práci, návazné činnosti atd.

11.5 Vyhodnocení

Pro vyhodnocení, zda lze předpokládat, že má navrhované řešení žádoucí užitečnost, jsem použil Analýzu užitečnosti nákladů. Tato analýza je jednou z variant k analýze nákladů a přínosů.

11.5.1 Analýza užitečnosti nákladů – definice

Tato analýza je vhodná u posouzení projektů, kde se výstupy dají těžko nebo vůbec vyjádřit v peněžní hodnotě, a tedy výstupem je užitečnost. Analýza užitečnosti nákladů poměřuje efekty jednotlivých možností řešení prostřednictvím vážené užitečnosti, která bývá pro každého jedince jiná. Analýza posuzuje varianty s nejistými, subjektivně porovnatelnými výsledky a její funkcí je zjistit nakolik jednotlivé hodnocení nabídky, s ohledem na vynaložené náklady, odpovídají očekávanému uspokojení potřeb a cílů. Jinými slovy analýzou zjistíme, jak vynaložené náklady vedou ke změnám užitku u sledovaných variant. Ta varianta, u níž je změna užitku nejvyšší, je k realizaci dodatečných nákladů nejvhodnější. [33]

11.5.1.1 Popis postupu zpracování analýzy

Při zpracování analýzy bylo prvním nezbytným krokem vytvořit soupis faktorů jako vstupů do analýzy (posuzované varianty, cíle projektu včetně jejich vah, bodovací stupnice cílů, náklady pro obě varianty). V následujících kapitolách jsou tedy tyto vstupy jednotlivě definovány včetně popisu, jakým způsobem byly stanoveny.

Po splnění předchozích náležitostí bylo možno přistoupit k samotné analýze. Ta je rozdělena na dvě samostatné tabulky. První z tabulek je „Vážená užitečnost daných variant. Tato tabulka určuje užitečnost varianty na základě posouzení každého z cílů projektu, který je označen svou váhou a ohodnocen pomocí bodovací stupnice. Touto multikriteriální metodou vypočteme hodnocení pro každou variantu. Varianta s vyšším hodnocením je posuzována jako užitečnější. Do této tabulky ale nevstupuje faktor nákladů. Proto je tato tabulka doplněna o druhou - „Hodnocení nabídek“

V tabulce hodnocení nabídek je již zohledněna i výše nákladů. V našem případě nákladů na deset let provozu. I zde se pracuje s hodnocením cílů z bodovací stupnice. Hodnoty jednotlivých cílů se ale mezi sebou nenásobí. Hodnoty se sčítají a následně jsou děleny celkovou výší nákladů varianty. Varianta s vyšší hodnotou výsledku je vyhodnocena, jako užitečnější a vhodnější varianta.

Náhled na výsledky těchto dvou tabulek nám dává dobrý pohled na to, jaká z variant je užitečnější a tedy pro kterou bychom se měli dále rozhodnout.

11.5.2 Posuzované varianty

V analýze jsou vzájemně porovnávány dvě varianty. První varianta – stávající řešení. Tedy aktuální kamerový systém, který je provozován samostatně a nezávisle na elektronických turniketech. Druhá varianta – navrhované řešení. Tato varianta zahrnuje sjednocení dodavatele kamerového systému doplněným o modul rozpoznání tváře, napojený na elektronické turnikety.

11.5.3 Cíle pro hodnocení variant

Pro posouzení užitečnosti variant jsem na začátku modelace projektu stanovil po předchozí diskuzi s bezpečnostními manažery následující cíle:

- Míra snížení počtu lidských zdrojů pro dohled
- Snížení počtu potřebných zásahů PČR
- Efektivita záchytu nežádoucích osob
- Zvýšení bezpečnosti na fotbalových utkáních
- Možnost rozšířeného využití v rámci systému pro zefektivnění dohledu

Každý z cílů je samostatně ohodnocen váhou. Váha je určena pomocí Saatyho metody, kdy platí že:

1. Efektivita záchytu nežádoucích osob má absolutní preferenci před mírou snížení počtu lidských zdrojů pro dohled;
2. Zvýšení bezpečnosti na fotbalových utkáních má velmi silnou preferenci před možností rozšířeného využití v rámci systému pro zefektivnění dohledu;

3. Snížení počtu potřebných zásahů PČR má silnou preferenci před možností rozšířeného využití v rámci systému pro zefektivnění dohledu.

Tabulka 14 – Tabulka pro výpočet hodnoty cíle projektu

Určení hodnoty cílů projektu							
Hodnotící kritéria	Míra snížení počtu lidských zdrojů pro dohled	Snížení počtu potřebných zásahů PČR	Efektivita záchytu nežádoucích osob	Zvýšení bezpečnosti na fotbalových utkáních	Možnost rozšířeného využití v rámci systému pro zefektivnění dohledu	Geometrický průměr	Váha kritéria
Míra snížení počtu lidských zdrojů pro dohled	1	3	1/9	1/7	3	0,68	0,09
Snížení počtu potřebných zásahů PČR	1/3	1	3	1/9	5	0,89	0,11
Efektivita záchytu nežádoucích osob	9	1/3	1	1/5	7	1,33	0,17
Zvýšení bezpečnosti na fotbalových utkáních	7	9	5	1	7	4,66	0,60
Možnost rozšířeného využití v rámci systému pro zefektivnění dohledu	1/3	1/5	1/7	1/7	1	0,27	0,03
					CELKEM	7,83	1,00

Tabulka 15 - Tabulka pořadí cílů dle váhy

Pořadí cílů dle hodnoty		
Pořadí	Kritérium	Váha
1	Zvýšení bezpečnosti na fotbalových utkáních	0,60
2	Efektivita záchytu nežádoucích osob	0,17
3	Snížení počtu potřebných zásahů PČR	0,11
4	Míra snížení počtu lidských zdrojů pro dohled	0,09
5	Možnost rozšířeného využití v rámci systému pro zefektivnění dohledu	0,03

11.5.3.1 Bodovací stupnice cílů

Tabulka 16 - Stupnice hodnocení cílů projektu

Počet bodů	Splnění cíle (pocit očekávání)
0	Není splněn (vůbec není zajišťován)
1	Je mimořádně špatně plněn (jsem absolutně nespokojen)
2	Je velmi špatně plněn (jsem velmi nespokojen)
3	Je špatně plněn (jsem nespokojen)
4	Je velmi slabě plněn (nejsem spokojen, mám neutrální dojem)
5	Je sotva přijatelně plněn (jsem spokojen jen v základních rysech)
6	Je přijatelně plněn (jsem spokojen jen s výhradami)
7	Je dobře plněn (jsem spokojen s výhradami)
8	Je velmi dobře plněn (jsem spokojen s drobnými výhradami)
9	Je velmi kvalitně plněn (jsem spokojen bez výhrad)
10	Splnění je vynikající, výborné (je to optimální způsob)

11.5.4 Náklady variant

Náklady jsou počítány v desetiletém horizontu, a to z důvodu rozložení počáteční investice navrhované varianty v čase. Dále jsou pro každý rok kalkulovány náklady na servis a pravidelnou údržbu systému. Položky nákladů byly diskutovány s implementátorem kamerových systémů ze společnosti Colsys.

Výpočty nákladů (v desetiletém horizontu):

- Navrhovaná varianta
  - 1. rok – náklady na implementaci systému a s tím spojených služeb
  - 2.-5. rok – Náklady na servisní služby a profylaxe
  - 6.-10. rok – náklady na servisní služby, profylaxe a obměnu v malém množství
- Původní varianta
  - 1.-10. rok – náklady na servisní službu, profylaxe a obměnu komponent.

Tabulka 17 – Náklady daných variant v desetiletém výhledu

Varianta	Náklady na provoz, obměnu a servis										Celkem
	1.rok	2.rok	3.rok	4.rok	5.rok	6.rok	7.rok	8.rok	9.rok	10.rok	
Navrhovaná varianta	1 983 100 Kč	45 000 Kč	45 000 Kč	45 000 Kč	45 000 Kč	75 000 Kč	75 000 Kč	75 000 Kč	75 000 Kč	75 000 Kč	**2 538 100 Kč**
Původní varianta	120 000 Kč	120 000 Kč	120 000 Kč	120 000 Kč	120 000 Kč	120 000 Kč	120 000 Kč	120 000 Kč	120 000 Kč	120 000 Kč	**1 200 000 Kč**

11.5.5 Vážená užitečnost daných variant

Vážená užitečnost variant je v následující tabulce vypočítána pomocí váhou ohodnocených kritérií, která jsou pro každou z variant ohodnocena. Hodnocení probíhalo kvalifikovaným odhadem s bezpečnostním analytikem, zástupcem pořádkové policie ČR a manažerem stadionu Generali aréna.

Tabulka 18 - Vážená užitečnost variant

Kritérium	Váha	Původní varianta	Navrhovaná varianta
Zvýšení bezpečnoti na fotbalových utkáních	0,6	4	8
Efektivita záchytu nežádoucích osob	0,17	3	9
Snížení počtu zásahů PČR	0,11	3	7
Míra snížení počtu lidských zdrojů pro dohled	0,09	4	8
Možnost rozšířeného využití v rámci systému pro zefektivnění dohledu	0,03	4	7
Celkový užitek		**3,72**	**8,03**

Postup výpočtu:

1. Doplnění vah ke kritériu (cíli);
2. Stanovení hodnot pro kritéria napříč variantami;
3. Pro každou z variant provést součet kritérií součinů variant a váhy;
4. Porovnání výsledků.

Z výsledků tohoto posouzení vyplývá, že užitečnější varianta by byla nově navrhovaná. Pro ucelený pohled a relevantní výsledek je ale ještě potřeba započítat náklady obou variant. Tomuto se věnuje následující kapitola.

11.5.6 Hodnocení nabídek

Hodnocení variant se zohledněním nákladů pro jednotlivé varianty má potvrdit nebo vyvrátit výsledek z předchozí tabulky užitečnosti variant.

Tabulka 19 - Hodnocení kritérií se zohledněním nákladů

Kritérium	Původní varianta	Navrhovaná varianta
Zvýšení bezpečnoti na fotbalových utkáních	4	8
Efektivita záchytu nežádoucích osob	3	9
Snížení počtu zásahů PČR	3	7
Míra snížení počtu lidských zdrojů pro dohled	4	8
Možnost rozšířeného využití v rámci systému pro zefektivnění dohledu	4	7
Celkové uspokojení	**18**	**39**
Hodnocení	**0,0000150**	**0,0000154**

Postup výpočtu:

1. Doplnění vah ke kritériu (cíli);
2. Součet hodnot variant pro každou variantu;
3. Výpočet podílu celkového uspokojení a nákladů varianty;
5. Porovnání výsledků.

Z hodnocení vychází lépe nově navrhovaná varianta. Tento výpočet potvrzuje předchozí kapitolu, a tedy lze předpokládat, že tato varianta by v čase přinesla větší užitek i s přihlédnutím nákladů na pořízení a provoz.

11.5.7 Vyhodnocení hypotéz

Hypotéza 1

Na základě výsledků z tabulky 19 - Hodnocení kritérií se zohledněním nákladů, kde je bodový rozdíl srovnání obou variant vyšší o jednonásobek ve prospěch navrhované varianty, jsem dospěl k závěru, že je tato hypotéza vyvrácena.

Hypotéza 2

Toto kritérium bylo porovnáno v tabulce 19 - Hodnocení kritérií se zohledněním nákladů. Z tabulky vyplývá, že zvýšení záchytu nežádoucích osob u navrhované varianty má třikrát vyšší bodové hodnocení než varianta stávající. Dle tohoto výsledku konstatuji, že je tato hypotéza potvrzena.

Hypotéza 3

Dle výsledků tabulky 17 – Náklady daných variant v desetiletém výhledu, jsem dospěl k závěru, že je tato hypotéza vyvrácena.

11.5.8 Shrnutí

Z poslední kapitoly je patrné, že dává užitkově i ekonomicky smysl investovat do nové varianty. Na základě výpočtů v této práci bych navrhoval postupnou implementaci tohoto řešení na stadiony klubů v nejvyšší soutěži.

12 Diskuze

V předložené práci jsem se zabýval, jakým způsobem lze zajistit vyšší bezpečnost na fotbalových stadionech. Inspirace pro myšlenku kontroly a rozpoznání tváře vzešla z jednoho z mnou vedených projektů, kde jsem měl jako projektový manažer na starost dodávku video detekčního systému do metra. Tento systém má na starosti vyhodnocovat chování osob na nástupišti a na jejich chování reagovat dle daných algoritmů. Napadlo mě, že by vlastně něco podobného mohlo být užito i v prostředí fotbalového stadionu. Nejprve jsem zamýšlel navrhnout systém stejný jako v Pražském metru, s tím, že by byl algoritmus nastaven na jiné tipy chování, které by vyhodnocoval. Jenže, to bychom se pohybovali stále v oblasti řešení následků. A tak jsem přemýšlel dál, jak by mohlo vypadat řešení, díky kterému by se nežádoucí chování nejen odhalilo, ale hlavně by se mu předešlo, tedy jak zajistit prevenci. A odtud následně vznikla myšlenka detekce tváře s napojením na elektronické turnikety a centrální databázi.

Při rešerši různých zdrojů jsem zjistil, že tato myšlenka nenapadla nejen mě. V českých novinových článcích se můžeme dočíst o diskuzích v rámci této myšlenky v různých obměnách. A v některých zahraničních ligách dokonce již tyto systémy implementovány jsou a jejich výsledky nasazení jsou v souladu s očekáváním. I to mě utvrdilo, že by toto mohla být správná cesta i pro českou republiku.

Doplnit stávající systémy, nebo implementovat celý systém?

V mé studii jsem šel cestou úplné výměny kamerového systému, který by byl doplněn o software pro rozpoznání obličeje. Toto řešení by bylo propojeno s centrální databází nežádoucích osob a elektronickým vstupem na stadionech. Přemýšlel jsem, zda využít a počítat se stávajícím kamerovým systémem, který musí být dle nařízení FAČR instalován na každém stadionu, jehož tým hraje nevyšší fotbalovou soutěž. Zde by ale nastal problém s kompatibilitou jednotlivých kamerových systémů a softwarem pro detekci obličeje. Kdyby byl na každém stadionu nasazen jiný systém, téměř jistě by byly i jeho výstupy rozdílné kvality a spolehlivosti. Další úskalí by mohlo nastat při propojení s centrálním serverem.

Z mých osobních zkušeností a na doporučení servisních techniků, kteří řeší implementace kamerových systémů a následně je servisují jsem se rozhodl pro sjednocení dodavatele pro celé řešení. Tím bude zajištěno sjednocení výstupních dat ze systému. Lze nad těmito daty bez následného konvertování vytvářet nejrůznější analytické sestavy.

V případě reálného nasazení je nutné toto rozhodnutí pečlivě konzultovat s majiteli jednotlivých klubů, jelikož se jedná o nemalou finanční částku investovanou do nového systému. Proto bych doporučoval pro každý stadion vytvořit studii finanční návratnosti a přidané hodnoty, podobně tak, jako jsem vyčíslil implementaci systému v této práci.

Pouze technické řešení nestačí

Pokud bychom spoléhali pouze na jedno řešení, nepřineslo by to jistě očekávaný výsledek. V praxi bych navrhoval jistě bezpečnostní řešení spolu kombinovat a v ideálním případě v budoucnu i spojovat do inteligentních systémů. Jedna věc je ale použití systémů a různých opatření, které potlačí nežádoucí chování, nebo ho v samém zárodku rozpoznají. Druhá, podle mého názoru důležitější, ale také složitější a náročnější je cesta postupné edukace a odbourávání tohoto chování jako takového. Pokud chceme mít v budoucnu opravdu bezpečné stadiony, ale i další veřejné akce je třeba plnit také „osvětu“ již od mládí návštěvníků. Já sám jako rozhodčí České fotbalové ligy mám možnost vidět na vlastní oči, jak vypadá fotbalové prostředí téměř v celé republice napříč věkovými kategoriemi. Nemůžeme čekat, že na fotbalová utkání budou v budoucnu chodit diváci, kteří byli jako děti vychováváni v zápasech nadávkami svých trenérů, ale dokonce i rodičů. Bohužel tento pohled se mi naskýtá v mládežnických kategoriích velmi často. Silná frustrace trenérů, dosti často bez odborných znalostí, ústí v agresivní chování vůči svým svěřencům, rozhodčím, nebo divákům, kteří pro vulgární výrazy, jak se říká také nechodí daleko. Ojedinělé není ani to, že tatínek vezme svého syna na fotbal a sám na tribuně následně místo povzbuzování oblíbeného týmu nadává směrem k rozhodčím, hráčům, a napadá slovně fanoušky soupeře. Jak můžeme následně čekat, že se tyto děti budou v dospělosti chovat na fotbalových utkáních? Odpovědí nám může být dnešní situace.

Samozřejmě řešení této situace není jednorázové a vyžaduje velké úsilí i finančních prostředků. Naštěstí již dnes probíhají projekty pro edukaci mládežnických trenérů, jsou aktivovány různé programy, které podporují zdravý přístup ke sportování a snaží se eliminovat orientaci pouze na výsledek, což také způsobovalo častou frustraci. Toto se jistě neprojevuje jen ve fotbale, ten je jen jedním z mnoha odvětví, kde toto můžeme pozorovat. O to je ale důležitější individuální přístup každého a snaha o lepší společenské chování.

Odhad budoucího vývoje

Další technický vývoj v oblasti zabezpečení stadionů, ale nejspíš i jiných masových akcí, vidím v inteligentním propojení bezpečnostních technologií, které dokáží navzájem sdílet informace a okamžitě je vyhodnocovat. V oblasti kamerových systémů se pravděpodobně bude budoucnost ubírat směrem rozpoznání nebezpečného a nežádoucího chování skupin, nebo jednotlivce již v jeho zárodku. Budoucí inteligentní kamerové systémy ve spojení s inteligentním softwarem budou pravděpodobně reagovat již na neverbální projevy těla, tělesnou teplotu a jiné fyzické projevy. Tím by se mělo podařit předejít nebezpečnému chování, ale také v nejzazším případě i teroristickým útokům. Jednotlivé střípky těchto řešení už můžeme nyní vídat například na letištích, kde je u cestujících snímána tělesná teplota, a další tělesné funkce, které mohou napovídat například vyšší nervozitě.

V budoucnu bude nutné, aby pořadatelé fotbalových utkání a dalších velkých akcích dostali větší pravomoci v oblasti řešení bezpečnosti, aby bylo možné tyto systémy užívat ve svém plném potenciálu. Každý z přítomných diváků a účastníků si musí být vědom, že pro svoje nevhodné či nebezpečné chování vůči ostatním se dopouští činu, který může být okamžitě potrestán v rámci platné legislativy ČR.

Další funkce pro komfortní dohled

Jak jsem se již v práci zmínil, další potenciál bezpečnostních systémů leží v jejich propojení a možném dovývoji dalších funkcí. Ne všechny funkce musí být zaměřeny na řešení bezpečnosti. Kamerové systémy lze využít například pro počítání osob na stadionu, nebo dokonce v jednotlivých virtuálních zónách. Na stadionu si tak může pořadatel určit virtuální zóny, ve kterých chce mít pouze omezený počet osob

v jednu chvíli. Kamerové systémy mohou suplovat i bezpečnostní technologie. Dnes je již standardní funkcí takzvané virtuální zastřežení prostoru. V obraze si uživatel vyznačí určitou oblast, do které když vstoupí osoba, systém vyhlásí poplach. Toto si dokážu představit jako ideální řešení pro kontrolu vniknutí diváků na hrací plochu v situaci, kdy pořadatelská služba nezaregistruje diváka, který se snaží vniknout na hrací plochu.

Zkvalitnění dohledu by bylo možné podpořit také například integrací jednotlivých systémů do bezpečnostní nadstavby. Jedná se o systém, který do sebe integruje nejrůznější typy technologií, zabezpečovací a požární systém, kamerový systém, přístupový systém atd. Uživateli následně interpretuje informace jednotně v jednom uživatelském rozhraní. Odpadá tak potřeba separátního software pro každou technologii. Výhodou bezpečnostních nadstaveb je také možnost o doplnění mapového podkladu, nebo automatické akce systému. Například pokud vyhlásí bezpečností čidlo poplach, automaticky se uživateli zobrazí kamerový stream z místa vzniku poplachu. Nadstavbové systémy jsou dnes již zcela běžně užívány pro dohled v průmyslových objektech, kancelářských budovách, letištích a dalších rozsáhlých prostorách, kde se nachází větší množství technologií.

Je třeba dbát na legitimní použití

S použitím takto sofistikovaných systémů, které nakládají s daty o každé detekované osobě roste i míra nejistoty o možném zneužití získaných údajů. Je třeba důsledně dbát na to, aby tyto systémy byly užity výlučně pro řešení bezpečnosti a nedošlo k úniku dat, či jiného zneužití. Jakým způsobem toho lze docílit je jednoduchá otázka, na kterou už ale není tak snadné odpovědět. Cest k řešení je několik. Domnívám se ale, že dané způsoby řešení bude třeba vzájemně kombinovat, aby bylo riziko sníženo na akceptovatelnou míru. Postupy řešení bych rozdělil do dvou hlavních kategorií. Tzv. tvrdá opatření a měkká opatření. Tvrdými opatřeními mám namysli všechny technické a systémové možnosti určené proti úniku dat a napadení systému. Měkká opatření vnímám jako jasně a přesně specifikovanou legislativu, kdy krom jiného bude jasně vymahatelná v případě porušení. Další v řadě jsou nejrůznější řády, směrnice, postupy nakládání se systémem atd., které bude muset obsluha a uživatelé systému striktně dodržovat.

Dnes se pohybujeme ve světě, kde jednou z nejcennějších komodit jsou informace. Na trhu je celá řada společností, které jsou ochotny za osobní údaje, které mohou pomoci například k cíleným reklamám a podobným sofistikovaným kampaním, zaplatit nemalé obnosy. Krom takovýchto společností je také velká řada tzv. hackerů, kteří data nelegálně získávají buď právě pro takové společnosti, nebo na nich pomocí nejrůznějších forem výkupného bohatnou. Mimo oblast zpeněžení dat se nabízí diskuze nad dalšími důvody pro zneužití. Mohou to být osobní důvody, snaha o znedůvěryhodnění systému a další. Nad tématem zneužití dat určitě doporučuji se velmi dobře a dlouze zamyslet a nastavit co nejlepší řešení.

Aspekty ovlivňující nasazení

Jak bude systém fungovat a jak vysoký efekt přinese závisí na různých faktorech, které mohou významně ovlivnit využitelnost. Těchto faktorů je celá řada, jako nejpodstatnější, a to platí pro drtivou většinu softwarových projektů, vidím následující: detailní sepsání analýzy požadavků, komunikace se zadavatelem, odladění systému ve fázi nasazení, proškolení obsluhy.

Důraz na sepsání detailní analýzy, která by postihla všechny požadavky, ale také vymezila funkce, které systém podporovat nebude je pro úspěšné dokončení projektu klíčové. Pokud není na počátku analýza kvalitně zpracována a pochopena zadavatelem i dodavatelem stejně, vzniká velké riziko, že na konci nebude dodán systém, který bude plně vyhovovat požadavkům zadavatele. Díky tomu následně vznikají spory, vytváří se vícenáklady, nebo dokonce ruší projekty, jelikož nemusí přinášet požadovaný efekt. V průběhu celého dodání projektu je nutné pravidelně komunikovat se zadavatelem a ověřovat si dílčí výstupy. Důvod je naprosto stejný jako u nutnosti sepsání analýzy.

Po dodání systému navrhuji, a toto počítám i ve své modelaci, zvýšenou podporu a odladění systému. Některé projekty jsou odsouzeny k zániku jen díky tomu, že po jejich implementaci nebylo vyvinuto dostatečné úsilí ke skutečně podrobnému nastavení pro uživatele a odladění všech počátečních provozních problémů. Uživatel takový systém nechce používat, vidí ho jako problémový a namísto toho, aby mu přinášel užitek, vnímá ho jako něco, co mu práci ztěžuje. S tímto jde ruku

v ruce proškolení obsluhy systému. Právě tito lidé budou systému nejblíže a je bezpodmínečně nutné, aby systém pochopili a správně užívali.

Při dodávce projektových řešení existuje celý zástup dalších rizik a oblastí na které je třeba myslet. Dnes je naprosto běžné, že se pro řízení najímá projektový manažer, a to jak na straně dodavatele, tak na straně zadavatele. Tato pozice má zajistit plnění zájmů obou stran.

Pro dodávky softwarových projektů existují různé metodiky, které napomáhají řízení projektů. Praxí ověřenou metodikou, kterou bych navrhoval pro podporu řízení, je mezinárodně uznávaná a často používaná metodika PRONCE II, která má svůj původ ve Velké Británii. Tato metodika postihuje dodávku od jejího obchodního vzniku před implementaci až po sledování přínosů projektu v době jeho užívání.

13 Závěr

V samotném závěru bych rád zhodnotil naplnění cílů této práce. Hlavní myšlenkou bylo objasnit jakým způsobem funguje systémové rozpoznání tváře a jak lze tento biometrický údaj využít pro zvýšení bezpečnosti na fotbalových stadionech. S přihlédnutém na obsah práce si troufám tvrdit, že se cíl povedlo splnit. V práci jsem také provedl rešerši výrobců kamerových systémů vhodných pro navrhované řešení a pomocí analytických metod vybral tu nejvhodnější, se kterou jsem dále rozpracoval a vyhodnotil modelovou situaci na jednom vybraném stadionu.

V průběhu zpracování jsem získal pro mě cenné informace a znalosti z oblasti kamerových systémů, bezpečnostního řešení a metod objektivního výběru varianty. Pevně věřím, že tyto nabyté zkušenosti mi pomohou v dalším profesním životě. Další neocenitelný benefit této práce je rozšíření vztahů ve spol. Colsys, která nabízí studentům ČVUT možnost stáží v různých technických oborech.

Bylo by pro mě velkým potěšením, kdyby se v budoucnu některé mé myšlenky a poznatky z této práce dostaly do skutečné realizace.

14 Reference

1. Martin Drahanský, Filip Orság. *BIOMETRIE.* Brno : Computer Praha a.s., 2011. 978-80-254-8979-6.

2. Hereschel, James William. *The Orion of Finger-Printing.* místo neznámé : Oxford university press, 1916.

3. Wikipedia. [Online] [Citace: 21. 3 2020.] https://cs.wikipedia.org/wiki/Alphonse_Bertillon.

4. Jain A. K., Bolle R., Pankarti S. *Biometrics – Personal identification in Network Society.* místo neznámé : Kluwer Academic Publisher, 1999.

5. P., Komirinski. *Automatized Fingerprint Identification System .* místo neznámé : Academic Press, 2004. 978-01-241-8351-3.

6. Hauptvogel K. H., Ritzsche M. *Biometrie um die Jahrunderwende.* 2004.

7. Rak Roman, Orság Filip. *Biometrie a identita člověka ve forenzních a komerčních.* Praha : Grada, 2008. 978-80-247-2365-5.

8. Michal, Ruttkay. BIOMETRICKÁ IDENTIFIKACE OTISKU PRSTU. Brno : FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ, 2015.

9. Bitto, Ondřej. *Šifrování a biometrika aneb tajemné bity a dotiky.* místo neznámé : Computer Media s.r.o., 2005. 80-86686-48-5.

10. Ruud Bille, Jonathan Connell, Nalini Ratha, Andrew Senior. *Guide to Biometric.* místo neznámé : SpringerVerlag, 2003. 0387400893.

11. Tomáš, Přibyl. scienceworld.cz. [Online] [Citace: 29. 12 2019.] https://www.scienceworld.cz/biologie/vyhody-a-nevyhody-biometrickych-systemu-1-515/?switch_theme=mobile.

12. Stávková, prof. Ing. Jana a prof. Ing. Jaroslav Dufek, DrSc. *Biometrika.* Brno : Mendelova Univerzita v Brně, 2012. 978-80-7375-634-5.

13. *Face Recognition for Smart Enviroments.* Pentland Alex, Chouhury Tanzeem. místo neznámé : IEEE Computer, 2000.

14. Andrea, Rozhoňová. Detekce a rozpoznávaní tváře s využitím platformy Raspberry Pi. Brno : FAKULTA ELEKTROTECHNIKY, 2017.

15. Ion, MARQUÉS. Face Recognition Algorithms. Leioa : Universidad del, 2010.

16. T., Brunelli R. Poggio. http://cbcl.mit.edu/. [Online] 1993. [Citace: 30. 12 2019.] http://cbcl.mit.edu/people/poggio/journals/brunelli-poggio-IEEE-PAMI-1993.pdf. 0162-8828.

17. jips-k.org. [Online] 2009. [Citace: 30. 12 2019.] http://jips-k.org/?lang=en. DOI : 10.3745/JIPS.2009.5.2.041.

18. tzb-info. *https://www.tzb-info.cz/.* [Online] 2017. [Citace: 26. 12 2019.] https://www.tzb-info.cz/kamerove-systemy/16681-rozpoznavani-obliceju.

19. Miroslav, Koutník. Teorie pro detekci tváře. *Bakalářská práce.* Milevsko : autor neznámý, 2010.

20. Lukáš, Adamec. is.muni.cz. [Online] [Citace: 28. 12 2019.] https://is.muni.cz/th/208425/fi_b/Srovnavaci_testy_vybranych_biometrickych_zarizeni.pdf.

21. Veronika, Braunová. *mvcr,cz.* [Online] [Citace: 28. 12 2019.] https://www.mvcr.cz/clanek/kamerove-sledovani-verejnych-prostranstvi-a-instituci.aspx.

22. Zákon č. 101/2000 Sb. Zákon o ochraně osobních údajů a o změně některých zákonů. 2000.

23. Pail, Čestmír. Bezpečnost na fotbalových stadionech. Praha : Univerzita Karlova v Praze, 2014.

24. Slepička, Pavel. *Sportovní diváctví.* místo neznámé : Olympia, 1990. ISBN 8070330120.

25. Maryník, Tomáš. *Technické zabezpečení fotbalových stadionů.* 2018.

26. republiky, Ministerstvo vnitra České. Manuál pro fotbalové kluby. místo neznámé : Ilustrace: Petr Morke, 2008.

27. *Zákon č. 40/2009 Sb.Trestní zákoník.* místo neznámé : arlament české Republiky, 2009.

28. Probační a mediační služba. [Online] 31. 12 2018. [Citace: 2020. 03 22.] https://www.pmscr.cz/statistiky-2/.

29. GUETEBRUCK. [Online] Guetebruck, 2019. [Citace: 20. 04 2020.] https://www.geutebrueck.com/technology/software.html.

30. HIK Vision. [Online] [Citace: 20. 04 2020.] https://www.hikvision.com/cz/Press/Success-Stories/Venue/Stadium/305529089059414.

31. Dahua. [Online] Copyright 2019 (ASM) 100MEGA DISTRIBUTION spol. s r.o., 2019. [Citace: 20. 04 2020.] https://www.dahua.cz/.

32. Hrazdil, Jakub. *Osobní sdělení.* Kladno, duben 2020.

33. *Nákladové užitkové metody.* místo neznámé : Město Valašské Meziříčí.

34. Jan Lepš, Petr Šmilauer. *Biostatistika.* České Budějovice : Nakladatelství Jihočeské univerzity v Českých Budějovicích, 2016. 978-80-7394-587-9.

35. Kewal Krishan, M.Sc., Ph.D. ispub.com. [Online] [Citace: 30. 12 2019.] https://print.ispub.com/api/0/ispub-article/10656.

36. wikipedia.org. [Online] [Citace: 27. 12 2019.] https://cs.wikipedia.org/wiki/Francis_Galton.

37. wikipedia.org. [Online] [Citace: 27. 12 2019.] https://cs.wikipedia.org/wiki/William_James_Herschel.

38. fr.wikisource.org. [Online] [Citace: 28. 12 2019.] https://fr.wikisource.org/wiki/Page:Bertillon_-_Identification_anthropom%C3%A9trique_(1893).djvu/8.

39. .nlm.nih.gov. [Online] [Citace: 28. 12 2019.] https://www.nlm.nih.gov/exhibition/visibleproofs/media/detailed/iii_c_118b.jpg.

40. dspace.vsb.cz. [Online] [Citace: 28. 12 2019.] http://dspace.vsb.cz/bitstream/handle/10084/87808/HYZ026_FMMI_B3922_3902R040_2011.pdf?sequence=1&isAllowed=y.

41. https://www.researchgate.net/. [Online] ResearchGate, 2019. [Citace: 29. 12 2019.] https://www.researchgate.net/figure/Two-images-used-for-building-the-Active-Shape-Model-faces-labelled-with-83-landmarks_fig1_283052638.

42. *http://codecapsule.com/.* [Online] Emmanuel Goossaert, 12. 8 2010. [Citace: 29. 12 2019.] http://codecapsule.com/2010/08/12/active-appearance-models-in-c-plus-plus/.

43. Dirk Colbry, Anil K. Jain. *researchgate.net.* [Online] ICPR, 2004. https://www.researchgate.net/publication/2889015_Three-Dimensional_Model_Based_Face_Recognition/link/0912f50b044f88bf49000000/download.

44. *i.kym-cdn.com.* [Online] [Citace: 30. 12 2019.] https://i.kym-cdn.com/entries/icons/original/000/018/394/facial-recognition-technology.jpg.

45. Luděk, Lukáš. *Bezpečnostní technologie, systémy a management I.* Zlín : autor neznámý, 2011. ISBN 978-80-87500-05-7.

46. *Podniková norma: Poplachové systémy - Pravidla zřizování poplachových zabezpečovacích systémů objektu.* místo neznámé : Jablotron, 2007.

47. rtzholding.cz. [Online] Holding a.s., 2010. [Citace: 2. 1 2020.] http://www.rtzholding.cz/nabidka-sluzeb/bezpecnostni-systemy/zabezpecovaci-systemy-ezs/.

48. http://www.alcamprofi.cz/. [Online] D3Soft s.r.o., 2011. [Citace: 2. 1 2020.] http://www.alcamprofi.cz/elektricka-pozarni-signalizace-eps-evakuacni-rozhlas-er.html.

49. .assidu.cz. [Online] Assidu, spol. s r.o. [Citace: 2. 1 2020.] http://www.assidu.cz/EPS.php.

50. briliancesecuritymagazine.com. [Online] Brilliance Security Magazine . [Citace: 2. 1 2020.] http://briliancesecuritymagazine.com/guest-contributor/by-scott-lindley/a-primer-on-contactless-cards-and-readers-for-electronic-access-control-systems/.

51. Vladimír, Laucký. *Technologie komerční bezpečnosti I. .* Zlín : Univerzita Tomáše Bati ve Zlíně, 2010. ISBN 978-80-7318-889-4.

52. ladinn.cz. [Online] [Citace: 3. 1 2020.] http://www.ladinn.cz/ostatni/technika/kamerovy_system.html.

53. vija.cz. [Online] VIJA.cz. [Citace: 3. 1 2020.] http://www.vija.cz/bezpecnostni-kamerove-systemy/cctv-dvr-kamerovy-system/.

54. isport.blesk.cz. [Online] [Citace: 4. 1 2020.] https://isport.blesk.cz/galerie/muj-isport-blogy-redaktori-jan-vacek/352726/sparta-poznala-ze-fotbal-neodpousti-otresny-prvni-duel-ji-dohnal?foto=7.

55. olomoucka.drbna.cz. [Online] 17. 10 2017. [Citace: 6. 1 2020.] https://olomoucka.drbna.cz/sport/fotbal/6223-policie-se-chysta-na-fotbalove-fanousky-v-olomouci-bude-hrat-zlin-proti-kodani.html.

56. Pěknicová, Klára. Ministerstvo vnitra ČR. [Online] 2019. [Citace: 2020. 03 22.] https://www.mvcr.cz/clanek/jan-hamacek-kluby-museji-pridat-v-zabezpeceni-stadionu-rodiny-s-detmi-se-nesmi-bat-chodit-na-fotbal.aspx.

57. ČTK. ČT 24. *https://ct24.ceskatelevize.cz/domaci/2764412-databaze-problemovych-fanousku-se-mohla-zacit-testovat-uz-pristi-sezonu.* [Online] 19. 03 2019. [Citace: 2020. 03 22.]

58. Ministerstvo vnitra ČR. [Online] [Citace: 15. 02 2020.] https://www.mvcr.cz/.

59. new.siemens. *new.siemens.com.* [Online] Siemens, s.r.o, 2020. [Citace: 21. 04 2020.] https://new.siemens.com/cz/cs/products/technologie-budov/bezpecnostni-systemy/video-management.**html.**

15 Seznam použitých obrázků

16 Seznamu použitých tabulek