

Popis technického zadání předmětu díla

1. Předmět díla

Předmětem díla je dodávka IP kamerového systému, který bude vybaven megapixelovými IP kamerami, biometrickým systémem pro porovnání tváří osob s databází provozovatele (policie ČR), systémem pro zpracování dat z čteček u přístupových turniketových bran a integračním bezpečnostním systémem (vše společně dále jen bezpečnostní systém). Celkový počet kamer je dán požadavky provozovatele systému a odvíjí se mimo jiné od velikosti konkrétního stadionu a velikosti jednotlivých tribun. Kamerový systém bude vybaven nejen pevnými, ale i otočnými PTZ kamerami, turnikety budou osazeny dvojicí kamer, jedna pro biometrickou identifikaci osoby, druhá kamera pro celkový přehled.

Jednotlivé podsystémy budou vytvářet jednotný bezpečnostní systém, který poskytne dohled nad děním v celém prostoru stadionu a umožní analýzu dat na základě vzniklých událostí. Počet a umístění kamer, switchů apod. je dán stávající infrastrukturou a požadavky na optimální instalaci kamerových bodů.

2. Účel výstavby

Hlavním úkolem kamerového systému na Městském stadionu Ostrava je zajistit bezpečnost nejen návštěvníků, hráčů a obsluhujícího personálu, ale i ochránit svěřený majetek před možným poškozením. Kamerový systém se tímto stane mocným nástrojem v boji proti nechtěným osobám, vandalům, teroristům apod., který bude mít nejen preventivní, ale především bezpečnostní účel při samotných utkáních a jiných akcích. Kamerový systém dále přispěje k poklidnější atmosféře a lepšímu sportovnímu vyžití všech zúčastněných. Provozovatelem bezpečnostního systému bude policie České republiky.

3. Kamerový systém (CCTV)

Kamerový systém stadionu bude složen z níže uvedených částí či podsystémů, které budou zaměřeny na sledování jednotlivých sektorů stadionu a svými funkcemi budou vytvářet ucelený systém pro zajištění bezpečného dění na stadionu. Kamerový systém bude založen na architektuře Server – Klient.

1) Kamerový systém

a) Pevné kamery pro sledování tribun

Kamery budou umístěny, dle možností buď na protější tribuně, nebo na sloupech nacházejících se u hřiště. Cílem je, aby instalované kamery pokryly prostor protilehlých tribun jak po celé délce, tak i po celé šířce stadionu.

b) PTZ kamery pro podrobnější sledování stadionu

PTZ kamery budou umístěny v rozích stadionu na tribuně, nebo sloupech tak, aby pokryly celý prostor stadionu a v případě incidentu mohly poskytnout mnohem detailnější záběr, než mohou poskytnout pevné kamery.

c) Pevné kamery pro sledování dění u vstupních bran, turniketů

Kamery budou umístěny u vstupních, turniketových bran tak, aby svým záběrem poskytly detailní obraz scény před vstupem na stadion a v součinnosti s biometrickým systémem pomohly identifikovat nechtěnou osobu. Každý turniket bude osazen 2 statickými kamerami, jedna pro

„Městský stadion Ostrava - kamerový systém“

Příloha č. 1 Podmínek pro zpracování nabídky

potřebu biometrické identifikace osoby vstupující do areálu sportoviště, druhá pro celkový přehled vstupující osoby.

d) Pevné kamery pro sledování vnějšího perimetru stadionu

Kamery budou umístěny na plášti stadionu tak, aby svým zorným uhlém pokryly scénu kolem celého stadionu. Vzhledem k tomu, že tyto kamery budou s největší pravděpodobností snímat i veřejná prostranství, musí umožnit nastavení skrytých zón.

2) Dohledové pracoviště

- a) Dohledové pracoviště stadionu bude vybaveno klientskou desktop stanicí s monitorem, vč. programového vybavení a CCTV klávesnicí pro monitoring a ovládání kamer, konfiguraci systému, analýzu dat, přehrávání a export záznamu. Pro potřebu obsluhy CCTV budou vytvořena 2 pracoviště, dále jedno pracoviště pro práci s biometrickou identifikací a jedno pracoviště pro správu integračního bezpečnostního systému.

Programové vybavení bude vybaveno analýzou pro zpracování dat pořízených z čteček u vstupních turniketových bran, aby při incidentu mohlo být získáno co nejvíce informací napomáhajících k odhalení trestného činu. Data získaná z čteček (číslo sedadla, číslo lístku apod.) u turniketových bran budou synchronně zaznamenávána s video záznamem turniketových kamer na serveru. Pokud např. dojde k incidentu na sedadle č. 80 tribuny, obsluha kamerového systému pomocí analýzy programového vybavení vyhledá dané číslo sedadla v záznamu a zobrazí tak odpovídající video z turniketové kamery, které bylo zachyceno v době, kdy osoba přiložila vstupní lístek s označením sedadla k turniketové čtečce. Tímto bude moci obsluha kamerového systému rozpoznat hledanou osobu v davu.

Napájení technologie dohledového pracoviště bude jištěno záložními zdroji UPS. Dohledové pracoviště se bude nacházet v prostoru stadionu a bude umístěno ve vybrané místnosti s omezeným přístupem, aby byla zajištěna bezpečnost dat.

- b) Vzdálená dohledová pracoviště, dle potřeb provozovatele (policie ČR), mohou být vybavena klientskou desktop stanicí pro monitoring a ovládání kamer, konfiguraci systému, analýzu dat, přehrávání a export záznamu.

3) Záznamové centrum

Záznamové centrum bude vybaveno uzamykatelnou rackovou skříní, v níž budou umístěny servery s datovými úložišti pro záznam kamer a dat (číslo sedadla, číslo lístku apod.) pořízených z čteček u turniketových bran. V rackové skříní budou dále umístěny servery pro porovnání tváří, switche pro konektivitu TCP/IP prvků kamerového systému, optické převodníky pro optickou páteřní síť, záložní zdroje napájení UPS, apod. Záznamové centrum se bude nacházet v prostoru stadionu a bude umístěno ve vybrané místnosti s omezeným přístupem, aby byla zajištěna bezpečnost ukládaných dat.

Kamerový systém bude vybaven IP megapixelovými kamerami s rozlišením minimálně 24Mpx/kameru, které umožní sledovat scénu tribun stadionu tak, aby v případě incidentu mohl uživatel kamerového systému rozpoznat osobu v davu, a to i ze záběru kamery z protilehlé strany stadionu.

Pro tyto účely jsou níže stanoveny min. parametry rozlišení, které musí kamera splňovat.

- a) Pro bezproblémové monitorování je nutné, aby každé místo (sedačka) na stadionu byla nasnímána minimálně v kvalitě 300 pixelů/m.

„Městský stadion Ostrava - kamerový systém“

Příloha č. 1 Podmínek pro zpracování nabídky

- b) Pro sektor ULTRAS - Domáci a ULTRAS - Hosté je nutné, aby kvalita rozlišení byla minimálně 500 pixelů/m.

4. Biometrická identifikace osob (BIO)

Tento podsystém bude vybaven servery se SW aplikací, která umožní identifikovat a porovnat tváře osob zachycených turniketovými kamerami s tvářemi v databázi policie ČR. Tento podsystém dále ovlivní průchod osob na stadion, tzn., že pokud tento systém vyhodnotí návštěvníka jako nechtěnou osobu, zamezí mu vstup na stadion.

Každý vstup, turniket, bude vybaven dvěma kamerami, jedna kamera pro biometrickou identifikaci osoby, druhá kamera jako přehledová – celá postava. Každá turniketová kamera bude zapojena jak do kamerového záznamového serveru, tak i do biometrického serveru pro rozpoznávání tváří.

Biometrický systém musí být schopen pracovat s centrální databází, která bude umístěna v souladu s potřebami policie ČR. Databáze bude obsahovat seznam osob, které mají soudní zákaz vstupu na fotbalová utkání nejvyšší soutěže. V případě, že server pro porovnávání tváří nalezne shodu osoby stojící u turniketu s tvářemi uloženými v databázi, obsluha turniketu bude upozorněna a turniket bude zablokován pro případný neoprávněný vstup.

Systém automatické detekce tváře s rozpoznáním osob a porovnáním s databází nežádoucích osob musí podporovat připojování dalších serverů pro případné rozšíření systému, systém nemůže mít limit pro maximální počet serverů v síti. Databáze tváří se musí nacházet na jednom centrálním serveru, přičemž všechny ostatní servery umí tuto databázi sdílet a vyhodnocovat. Systém musí mít vysokou spolehlivost a úspěšnost rozpoznání. Je nutné, aby systém měl možnost nastavit úroveň pro citlivost detekce a citlivost rozpoznávání. Vyhodnocení musí probíhat v reálném čase (realtime) a s minimálním zpožděním, s rychlostí prohledávání minimálně 500 000 tváří za sekundu. Systém musí podporovat integraci do SW třetích stran přes volné SDK. Rozpoznání tváře musí probíhat bez nutnosti nějakého impulzu na rozpoznání. Systém musí být odolný vůči dioptrickým i většině slunečních brýlí. Podpora nastavení různých práv pro různé brány pro stejnou osobu.

V případě detekce nežádoucí osoby musí systém zablokovat otevření turniketu a tím nevpustit nežádoucí osobu do objektu. Ostraha objektu dostane informaci o pokusu nežádoucí osoby o vstup.

5. Integrovaný bezpečnostní systém (IBS)

Cílem je komplexní monitorování a řízení technologií v oblasti objektové bezpečnosti v rámci celého areálu, případně organizace (správce). Otevřenost celkového řešení přispěje k plnění požadavků kladených na oddělení bezpečnosti i v budoucnosti. V rámci otevřenosti systémů umožní rozšíření o nové funkcionality, případně plnohodnotné propojení s ostatními systémy podniku.

Pro potřeby integrace bezpečnostních systémů bude instalován integrovaný bezpečnostní systém, integrující technologie: nově budovanou část CCTV a stávající technologie PZTS (EVS) a EPS. Běh systému bude provozován na vyhrazeném serveru vybaveném vlastní aplikací klient – server, využívající databáze MS SQL.

IBS musí splňovat nejvyšší nároky na bezpečnost. Bezpečnost celkového řešení by měla využívat nejmodernější techniky v oblasti informační bezpečnosti, např. využití digitálních certifikátů, šifrované spojení, atd. V rámci integrace více technologií do jednotného systému se očekávají zvýšené nároky na odbornost pracovníků dodavatele.

Vzhledem k rozsahu celkového řešení jsou následující požadavky na IBS:

„Městský stadion Ostrava - kamerový systém“

Příloha č. 1 Podmínek pro zpracování nabídky

- podpora IBS pro práci v síťovém prostředí – víceuživatelský přístup, aktivita uživatele (zrušení poplachu) na jednom dispečinku se projeví i na ostatních pracovištích. IBS musí umožnit nastavovat oprávnění přístupu k aplikacím jednotlivým uživatelům, případně skupinám uživatelů a to v širokém rozsahu. Zároveň by měl zabezpečovat ovládání zařízení z více míst současně podle priority uživatelů.
- transparentní přístup k datům z centrální databáze prostřednictvím třívrstvé architektury. Tato funkcionalita zabezpečí kontrolu oprávnění jednotlivých uživatelů až na straně serveru, což výrazně zvýší bezpečnost řešení. Zároveň se sníží riziko neoprávněných pokusů o přístup k datům z centrální databáze.
- jednotná databáze pro všechny pracoviště – umožnit sdílet více uživatelům společné zdroje informací potřebných k jejich práci. Pro celkové nainstalování a spuštění systému je potřeba mít možnost konfigurace všech parametrů jen v jedné databázi.
- jednotná správa osob pro všechny technologie – všechny nastavení týkající se nastavení přístupu osob k jednotlivým zařízením se budou zobrazovat uživateli v jednotném rozhraní. Uživatel by měl být zbaven potřeby nastudovat si specifika jednotlivých zařízení. Systém automaticky zabezpečí, aby se nastavené údaje naprogramovali do každého zařízení správně.
- nezávislost informačního systému od jednoho výrobce zařízení - umožnit integraci zařízení od různých výrobců (jak lokálních tak celosvětových značek) v rámci jednotného řešení. Tato vlastnost umožní organizaci možnost optimalizace výběru zařízení podle konkrétních potřeb pro jednotlivé objekty. Zároveň by měla snížit náklady na celkové řešení.
- vzhledem k nárokům na personální obsazení obsluhy bude požadované řešení, které minimalizuje nároky na zaškolení a umožňuje jednoduchou a intuitivní obsluhu. Klientská část aplikace musí umožnit jednoduchou obsluhu jako například práci s klávesovými zkratkami. Řešení na straně klienta bude využívat standardní klientskou aplikaci.
- systém nesmí využívat technologie vyžadující zvýšené oprávnění na straně klientských počítačů. Proto systém nesmí využívat prvky na bázi technologie ActiveX. Toto omezení má význam i z hlediska celkové bezpečnosti počítačové sítě organizace/zadavatele veřejné zakázky, kde případné povolení automatického instalování takovýchto komponent vzniká riziko neoprávněného přístupu k citlivým údajům.
- jednotné a provázané integrované řešení. Tento požadavek by měl zabezpečit jednoduchou konfiguraci celé aplikace v jednotném prostředí. Odpadá složité paralelní konfigurování více aplikací.
- jednotná a hierarchická správa osob umožňující správu osob v organizační struktuře zadavatele, případně doplňkově i zařazování osob do skupin. Práce s takovou hierarchií umožní efektivní nastavování oprávnění – nastavování oprávnění na oddělení zabezpečí zdědění oprávnění všem zařazeným osobám. Od této vlastnosti systému se očekává výrazné snížení nároků na administraci.
- správa poplachových a evidence kroků obsluhy v průběhu řešení pro potřeby vyhodnocování situace v budoucnosti.

6. Topologie sítě

Jednotlivé TCP/IP prvky budou mezi sebou propojeny ethernetovou sítí, jejíž konektivita bude zajištěna pomocí switchů. Kamery, servery a klientské stanice budou ke switchům připojeny metalickým kabelem, popř. kabelem optickým. Jednotlivé switche pak budou mezi sebou propojeny optickou páteřní linkou kruhové topologie (ring topology). Bude využito stávající páteřní infrastruktury s doplněním potřebných aktivních prvků včetně jejich managementu.

7. Elektroinstalace

Technologie kamerového systému bude napájena ze stávajících el. rozvaděčů, případně zásuvkových okruhů. Pro napájení kamer bude použito primárně PoE switche, pro doplňkové napájení budou použity zdroje 12VDC/24VAC nebo PoE injektory (standard IEEE 802.3 af, IEEE802.3 at).

Elektroinstalace, vč. uzemnění musí být provedena v souladu se všemi platnými předpisy a ČSN platnými v době realizace. Zařízení bude uvedeno do provozu až po provedení výchozí revize el. instalace dle ČSN 33 2000-6.

8. Zabezpečení kamerového systému

Jelikož z provozování kamerového systému plynou povinnosti ukládané zákonem o ochraně osobních údajů, je nezbytné zajistit bezpečnost kamerového systému a to jak po fyzické stránce, tak i po stránce softwarové.

Tzn., že:

- a) přenos dat mezi klientem a serverem bude šifrovaný (min. protokol SSLv3.0, 128 bit SHA, RSA RC4)
- b) záznam dat bude probíhat na centrálních záznamových serverech umístěných na jednom místě, tj. nepřipouští se více distribuovaných úložišť,
- c) kamery budou zabezpečeny polohou, tj. budou instalovány v takové výšce, aby nebyly volně dostupné, vyjma turniketových kamer,
- d) kabelová vedení budou v místech volného přístupu opatřena ochrannými elektroinstalačními trubkami, v bezpečných prostorech pak ochrannými lišty,
- e) kabelová vedení budou v nehořlavém provedení,
- f) pokud bude nutné technologii instalovat do volně přístupných míst, bude nutné tuto technologii vybavit zábranami znemožňující volný přístup bez použití nástrojů,
- g) servery pro záznam, datová úložiště a klientské stanice budou instalovány v místnostech s omezeným přístupem (vstup bude povolen pouze oprávněným osobám, bezpečnostní službě apod.),
- h) servery a datová úložiště budou instalovány v uzamykatelných rackových rozvaděčích,
- i) veškerý přístup do kamerového systému bude zabezpečen uživatelským oprávněním, které bude podmíněno zadáním uživatelského jména a hesla, přičemž přístup do záznamu může být podmíněn povinnou změnou hesla, aby se předešlo možným únikům dat při dlouhodobém používání jednoho hesla,
- j) záznamové servery budou vybaveny min. dvěma LAN porty, aby se oddělila kamerová část od klientské části,
- k) záznam musí probíhat na serverovém zařízení tak, aby nebyl přehratelný na jiném počítači bez obslužného software po zadání jména a hesla, tzn., že po vyjmutí pevného disku ze záznamového zařízení a po vložení tohoto disku do jiného počítače nebude možné sledovat video záznam,
- l) databáze zakázaných osob musí být uložena pouze na vyhrazeném serveru policie ČR,
- m) kvůli zákonu o ochraně osobních údajů je dále nutné, aby kamery, které budou snímat a zasahovat i do prostoru mimo samotný stadion, podporovaly nastavení privátních zón,
- n) každý operátor kamerového systému musí být vyškolen k obsluze systému a stejně tak musí být seznámen s právními normami.

9. Záruka a kvalita systému

Vzhledem k tomu, že Zadavatel na výstavu systému specifikovaného v „Zadávací dokumentaci“ vynaloží nemalé investice, předpokládá, že kamerový systém bude dodán ve vysoké kvalitě s dlouhou dobou životnosti. Z tohoto důvodu Zadavatel požaduje, aby technologie kamerového systému byla dodána od jednoho výrobce. Tímto si chce Zadavatel zajistit kvalitu dodávané technologie, osvědčenou funkčnost systému, dostupnost náhradních dílů, včasnou výměnu poškozené technologie a pružné jednání jak s dodavatelem, tak i s výrobcem dodávané technologie. Zadavatel dále od dodavatele, výrobce technologie kamerového systému očekává on-line spolupráci při řešení technických problémů. Vzhledem k těmto požadavkům Zadavatel nepředpokládá, že by centrální monitorovací aplikace, serverová aplikace pro záznam kamer a kamery dodavatel ve své nabídce uvedl od různých výrobců. Zadavatel si dále nevyhrazuje žádné speciální podmínky, kromě splnění „Minimálních požadavků na technologii“, na dodání ostatní technologie. Zadavatel dále připouští dodání „Biometrického systému“ od jiného výrobce, než je výrobce kamerového systému, jelikož si je vědom, že ne všichni výrobci kamerových systémů disponují biometrickým systémem. V takovém případě však dodavatel při zpracování nabídky musí brát v úvahu, že „Biometrický systém“ musí být integrován do kamerového systému tak, aby splnil podmínky „Zadávací dokumentace“.

„Městský stadion Ostrava - kamerový systém“

Příloha č. 1 Podmínek pro zpracování nabídky

Na všechny produkty kamerového systému (kamery, servery, klientské stanice) musí být poskytnuta záruka minimálně po dobu 36 měsíců.

10. Legislativa a normy

- zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů
- Nařízení vlády č. 17/2003 Sb., kterým se stanoví technické požadavky na elektrická zařízení nízkého napětí
- ČSN EN 50 132 – Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích
- zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

11. Závěr

Pokud minimální požadavky na technologii nejsou v tomto dokumentu blíže specifikovány, jsou podrobnější informace obsaženy v níže uvedených dokumentech

- a) Minimální požadavky na technologii, které tvoří Přílohu č. 2 Podmínek pro zpracování nabídky

Uchazeč je povinen minimální požadavky na technologii uvedené v „Podmínkách pro zpracování nabídky“ dodržet.

V souladu s ust. § 36 odst. 4 zákona č. 134/2016 Sb., o zadávání veřejných zakázek zadavatel uvádí, že zpracovatelem této části Podmínek pro zpracování nabídky je

Ing. Roman Stuchlík
PERFECTED s.r.o.
Hybešova 42
602 00 Brno

Datum: 21.11.2016