

Technické zabezpečení sportovních stadionů firmami PKB

Maintenance of sports stadiums from firms in commercial security

Bc. Petr Hložek

Diplomová práce
2010

 Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Petr HLOŽEK**
Studijní program: **N 3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Technické zabezpečení sportovních stadiónů firmami PKB**

Zásady pro vypracování:

1. Zhodnoťte současný stav technického zabezpečení a organizace stadiónů pro různé sporty.
2. V teoretické části zpracujte jejich vývoj, zákonné a normativní úpravy platné v ČR.
3. V praktické části navrhnete technické řešení integrace jednotlivých bezpečnostních systémů a aplikujte na konkrétní sportovní areál.
4. Odhadněte další vývoj těchto systémů.

Rozsah práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **LOVEČEK, Tomáš, Komerční bezpečnostní systémy, Žilina : Žilinská univerzita, 2008, ISBN 80-8070-893-1**
2. **NĚMEČEK, Milan, CCTV kamery a jejich využití v zabezpečení objektů, Zlín : Univerzita Tomáše Bati, 2008. 105 s. Diplomová práce.**
3. **ČANDÍK, Marek, Objektová bezpečnost II, Zlín : Univerzita Tomáše Bati, 2004, ISBN 80-731-8217-3 (brož.)**
4. **Laucký, V., Technologie komerční bezpečnosti II, Učební texty vysokých škol,, Univerzita Tomáše Bati ve Zlíne, Zlín, 2004, ISBN 80-7318-231-9**
5. **Kindl, J., Projektování bezpečnostních systémů I. díl, Učební texty vysokých škol 2004, Univerzita Tomáše Bati ve Zlíne, Zlín, 2004, ISBN 80-7318-165-7**
6. **JASEK, Roman. Informační a datová bezpečnost. Zlín: Univerzita Tomáše Bati ve Zlíne. Fakulta managementu a ekonomiky, 2006. 140 s. ISBN 80-7318-456-7**
7. **CERNÝ, Josef, IVANKA, Ján a kolektiv.: Technické prostředky a prvky zabezpečovací techniky, UTB-Academia Centrum Zlín**
8. **LAUCKÝ, Vladimír.: Objektová bezpečnost -- Mechanické prvky, UTBAcademia Centrum Zlín, 2003. ISBN 80-7318-119-3**
9. **CERNÝ, Josef.: Evropský výcvikový modul pro základní ostrahu, UTBAcademia Centrum Zlín, 2003. ISBN 80-7318-107-X**

Vedoucí diplomové práce:

Ing. Rudolf Drga

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

19. února 2010

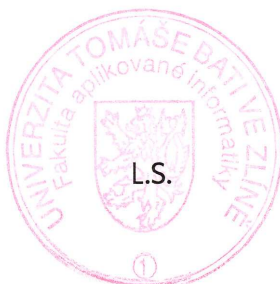
Termín odevzdání diplomové práce:

7. června 2010

Ve Zlíně dne 19. února 2010

prof. Ing. Vladimír Vašek, CSc.

děkan



doc. RNDr. Vojtěch Křesálek, CSc.

ředitel ústavu

ABSTRAKT

Předmětem této diplomové práce je zhodnocení současného stavu technického zabezpečení sportovních stadionů, specifikace konkrétních technických prostředků se zaměřením na zvýšení bezpečnosti a specifické požadavky objektu.

V praktické části je zpracován návrh jednotlivých bezpečnostních systémů, jejich aplikace na konkrétní hokejový stadion a vypracován návrh řešení.

Klíčová slova: sportovní stadion, technické zabezpečení, spolupráce, elektrická zabezpečovací signalizace, uzavřený televizní okruh, systém kontroly vstupu.

ABSTRACT

The subject of this thesis is to assess the current state of technical support sports stadiums, the specification of specific technical resources to focus on improving safety and the specific requirements of the building.

The practical part contains a proposal of security systems and their application to specific hockey stadium, and developed a proposed solution.

Keywords: sport stadium, providing technical assistance, cooperation, electrical security alarm, closed circuit television, access control systems.

Poděkování:

Chtěl bych na tomto místě poděkovat všem, kteří mi umožnili při mé pracovní vytíženosti studium, a měly na něj kladný vliv.

Zvláštní díky patří Ing. Rudolfu Drgovi, který je vedoucím této diplomové práce, za jeho přístup a ochotu při konzultacích mých výsledků a jejich řešení.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 14.6.2010

.....
podpis diplomanta

OBSAH

ÚVOD	11
1.1 CO JE TŘEBA ZMĚNIT	12
1.2 VÝTRŽNICTVÍ V ČÍSLECH	12
1.3 REGISTR	12
I TEORETICKÁ ČÁST	14
2 TRESTNÝ ČIN	15
2.1 DEFINICE TRESTNÉHO ČINU	15
2.2 ZNAKY TRESTNÉHO ČINU	15
2.3 VZTAH TRESTNOSTI A ZAKÁZANOSTI ČINU.....	17
3 ORGANIZACE STADIONU PRO RUZNE SPORTY	18
3.1 ZÁKLADNÍ DRUHY OCHRANY	18
3.2 ROZDĚLENÍ OCHRANY DLE CHARAKTERU STŘEŽENÉ OBLASTI.....	18
3.2.1 Plášťová ochrana	18
3.2.2 Prostorová ochrana.....	18
3.2.3 Předmětová ochrana	18
3.2.4 Obvodová ochrana.....	19
3.3 ROZDĚLENÍ STADIÓNŮ A SPORTOVNÍCH AKCÍ	19
3.3.1 Stadióny s uzavřeným perimetrem	20
3.3.2 Stadióny s částečně uzavřeným perimetrem.....	20
3.3.3 Sportovní akce konané na volném prostranství.....	20
4 TECHNICKÉ PROSTŘEDKY PRO ZABEZPEČENÍ STADIÓNŮ	21
4.1 ELEKTRONICKÁ ZABEZPEČOVACÍ SIGNALIZACE (EZS)	21
4.1.1 Detektor	21
4.2 KAMEROVÝ SYSTÉM (CCTV).....	22
4.2.1 IP kamery	23
4.3 ELEKTRONICKÁ KONTROLA VSTUPU (EKV)	24
4.4 ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE (EPS)	24
4.4.1 OPPO.....	24
4.4.2 KTPO	25
4.5 NOUZOVÝ ZVUKOVÝ SYSTÉM (NZS)	25
5 TECHNICKÉ PROSTŘEDKY PRO PŘENOS DAT	26
5.1 STRUKTUROVANÝ KABELÁŽNÍ SYSTÉM (SKS).....	26
5.1.1 Kategorie datové sítě.....	27
5.2 ZAŘÍZENÍ DÁLKOVÉHO PŘENOSU (ZDP)	28
5.2.1 Přes pevnou telefonní linku - GENOVA.....	28
5.2.2 Bezdrátový přenos - NAM	28
5.2.3 Bezdrátový přenos - LATIS	29

6	MECHANICKÉ ZÁBRANNÉ SYSTÉMY (MZS).....	30
6.1	PRŮLOMOVÁ ODOLNOST.....	30
6.2	VYBRANÉ MECHANICKÉ ZÁBRANNÉ PROSTŘEDKY.....	31
6.2.1	Turniket.....	31
6.2.2	Mříže.....	31
6.2.3	Bezpečnostní skla.....	31
6.2.4	Rolety.....	31
6.2.5	Ploty a zdi.....	32
7	SLUŽBY FIREM V PKB.....	33
7.1	ZÁKLADNÍ ROZDĚLENÍ.....	33
7.1.1	Operativa PKB.....	33
7.1.2	Výkonné technické služby PKB.....	33
7.1.3	Služby obecného bezpečnostního výkonu PKB.....	33
7.1.4	Pomocné služby PKB.....	34
7.1.5	Speciální služby PKB.....	34
7.1.6	Analytické služby.....	34
7.2	SLUŽBY ZAMĚŘENÉ NA ZABEZPEČENÍ STADIÓNŮ.....	34
7.2.1	Provozování Pultu Centralizované Ochrany (PCO).....	34
7.2.2	Pořadatelská služba.....	35
7.2.3	Bezpečnostní služba.....	35
7.2.4	Zásahová služba.....	35
7.2.5	Kontrolní propustková služba.....	36
7.2.6	Kontrolní činnost.....	36
7.2.7	Střežení objektu.....	36
7.2.8	Vyrozumění míst poskytující pomoc.....	36
7.3	HLAVNÍ ÚKOLY.....	36
8	ZÁKONNÉ A NORMATIVNÍ ÚPRAVY PLATNÉ V ČR.....	37
8.1	PLATNÉ NORMY.....	37
8.2	TABULKOVÝ PŘEHLED EVROPSKÝCH NOREM PRO ZABEZPEČOVACÍ A SIGNALIZAČNÍ SYSTÉMY.....	42
8.2.1	Poplachové systémy - Elektrické zabezpečovací systémy (EN 50 131- X).....	43
8.2.2	Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích (EN 50 132-X).....	43
8.2.3	Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích (EN 50 133-X).....	44
8.2.4	Poplachové systémy - Systémy přivolání pomoci (EN 50 134-X).....	44
8.2.5	Elektrická požární signalizace (EN 54 – X).....	45
8.3	ZÁKONNÉ ÚPRAVY TÝKAJÍCÍ SE POŽÁRNÍ OCHRANY.....	46
8.3.1	Zákona č. 133/1985 Sb., o požární ochraně.....	46
8.3.2	VYHLÁŠKA 23-2008 o technických podmínkách požární ochrany staveb.....	46
8.3.3	VYHLÁŠKA 246-2001 o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci).....	46
8.3.4	Únikové východy.....	47

8.3.4.1	Základní druhy únikových cest	47
8.3.4.2	Jak má vypadat úniková cesta	48
8.4	PROVOZOVÁNÍ KAMEROVÉHO SYSTÉMU Z HLEDISKA ZÁKONA O OCHRANĚ OSOBNÍCH ÚDAJŮ	49
II	PRAKTICKÁ ČÁST	52
9	VÝBĚR PŘEDMĚTU NÁVRHU	53
10	NÁVRH SYSTÉMŮ TECHNICKÉ ZABEZPEČENÍ	56
10.1	ELEKTRICKÁ ZABEZPEČOVACÍ SIGNALIZACE (EZS)	56
10.1.1	Představení navrhované technologie	56
10.1.2	Koncepční řešení	58
10.1.2.1	Použité detektory	58
	TRIPLE PB-150	58
10.1.3	Blokové schéma návrhu EZS	59
10.1.4	Návrh rozmístění prvků systému EZS	60
10.2	KAMEROVÝ SYSTÉM (CCTV)	60
10.2.1	Představení navrhované technologie	60
10.2.1.1	Použité kamery	61
10.2.2	Koncepční řešení	63
10.2.3	Blokové schéma návrhu systému CCTV	64
10.2.4	Ověření správného výběru rozlišení a pokrytí kamer na tribunách výpočtem	65
10.2.5	Návrh rozmístění prvků systému CCTV	66
10.3	ELEKTRONICKÁ KONTROLA VSTUPU (EKV)	66
10.3.1	Představení navrhované technologie	66
10.3.2	Koncepční řešení	69
10.3.3	Blokové schéma návrhu systému EKV	70
10.3.4	Online prodejní a rezervační systém Ticketportal	71
10.3.5	Návrh rozmístění prvků systému EKV	72
10.4	ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE (EPS)	72
10.4.1	Představení navrhované technologie	72
10.4.2	Koncepční řešení	74
10.4.2.1	Použité detektory	75
10.4.3	Blokové schéma návrhu systému EPS	77
10.4.4	Návrh rozmístění prvků systému EPS	78
10.5	NOUZOVÝ ZVUKOVÝ SYSTÉM (NZS)	78
10.5.1	Představení navrhované technologie	78
10.5.2	Koncepční řešení	80
10.5.3	Blokové schéma návrhu systému NZS	80
10.5.4	Návrh rozmístění prvků systému NZS	81
10.6	OSTATNÍ TECHNICKÉ SYSTÉMY DETEKCE	81
10.6.1	Detekce úniku čpavku	81
10.6.1.1	Detektor	81
10.6.2	Detekce kovových předmětů	82
10.6.2.1	Detektor	82

11	VÝSLEDNÁ INTEGRACE JEDNOTLIVÝCH SYSTÉMŮ	84
12	ODHAD DALŠÍHO VÝVOJE	85
	ZÁVĚR	86
	CLOSE.....	87
	FOTOGALERIE OBJEKTU.....	88
	SEZNAM POUŽITÉ LITERATURY.....	92
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	93
	SEZNAM OBRÁZKŮ	96
	SEZNAM FOTOGRAFIÍ.....	97
	SEZNAM PŘÍLOH.....	98

ÚVOD

Zabezpečení stadiónů je v dnešní době spíše podceňovaná skutečnost a prvky technického zabezpečení jsou na velmi nízké až nulové úrovni. Většina stadiónů se spoléhá pouze na prvky mechanického zabezpečení (ploty, zábrany), vstupní turnikety bez další návaznosti a na pořadatelskou službu, což bývá ve většině smluvní bezpečnostní agentura. Samozřejmě se najde i pár výjimek, příkladem je Sazka Aréna.

Rozbroje mezi fanoušky jsou stále častější. Ministr Vnitra přitom nepožaduje tvrdší tresty a v novém zákonu o policii navrhuje, aby policisté nebyli při utkání přímo na stadionu. Odborníci na násilí na stadionech to odmítají.

Násilnosti při fotbalovém derby nemají v Česku v posledních letech obdoby. Není zvláštností, kdy fanoušci propašují na stadion rachejtle, dýmavnice a jiné prostředky agrese.

Chuligáni nemají strach z trestů. Nízké sazby za výtržnictví nebo jen pokuty za vběhnutí na hřiště je neodradí, je nutné zpřísnit postihy za výtržnosti na stadionech. A především dosáhnout toho, aby se problémoví fanoušci do ochozů vůbec nedostali.

Legislativa by potřebovala doplnit. Jedná se o komplexní opatření, která se osvědčila např. proti fotbalovým rowdies v Německu nebo Anglii. Soud by měl více využívat zákazů vstupů na stadiony nebo přímo do měst, kde se zápas hraje. Důležité také je, aby se osoby, které se v minulosti dopustily výtržností na stadionu, musely v době utkání hlásit na policejních služebnách.

Policejní rada však nepovažuje v tuto chvíli za vhodné, aby se o pořádek na stadionech starali výhradně pořadatelé. Navrhuje to nový zákon o policii - je v něm napsáno, že policisté už nebudou při utkání přímo na stadionu. Zasáhnou jen v případě, kdy se ochrance vymkne situace z rukou.

Nemyslím si, že bude rozdíl, zda jsou policisté na stadionu, či za stadionem. Tím se žádné peníze neušetří, jen doba od násilí k zásahu se prodlouží. Je nutné pořadatelům na stadionech vytvořit právní podmínky, aby byli oprávněni zjednat pořádek. Dnes jsou před zákonem ve stejném postavení jako návštěvníci, nejradikálnější fanoušci to dobře vědí a zneužívají toho.

1.1 Co je třeba změnit

a) Zvýšení pravomoci pořadatelské služby

Je třeba zvýšit počet pořadatelů a změnit zákon.

b) Vyšší tresty výtržníkům

Zpřísnit legislativu, aby fanoušci za řádění nevyvázli jen s pokutou. Donutit "recidivisty", aby se v době zápasu hlásili na policii.

c) Instalace kamer z vysokých rozlišením pro identifikaci výtržníků

Zvýšit počet a kvalitu kamer, aby bylo možné výtržníky identifikovat.

d) Důkladnější kontroly u vstupu

Ideální jsou bezpečnostní rámy, které zatím fungují jen v hokejové O2 Aréně.

1.2 Výtržnictví v číslech

Škoda na stadionu Evžena Rošického 500 tisíc Kč, duben 2008. Chuligáni na stadionu zničili zhruba 600 sedaček. Na derby bylo nasazeno 600 policistů a vrtulník. Policisté zadrželi 31 výtržníků - 12 před utkáním, 19 po skončení. Z výtržnictví bylo v průběhu večera obviněno 21 lidí. Dva lidé čelí obvinění z útoku na veřejného činitele. Zraněno bylo 16 fanoušků a 4 policisté. Škoda na tramvaji, kterou napadli spartanští chuligáni, je 5 000 Kč. V areálu Rošického stadionu byl poničen také plot a toalety. [5]

1.3 Registr

Registr fotbalových výtržníků, jehož vznik doporučila policie fotbalovým klubům, už existuje. Jsou to lidé, kteří byli za násilí na stadionech odsouzeni.

Má ho k dispozici pouze samotná policie, ale informace z něj nemůže poskytovat třetím osobám, v tomto případě klubům. Proto vznikl nápad s dalším registrem, který by si vedly kluby samotné.

Zapsaní by v něm měli být ti fanoušci, kteří se na stadionu dopustili nějaké výtržnosti, záleží přímo na návštěvním řádu jednotlivého stadionu, o jaké konkrétní výtržnosti půjde. O zařazení jmen do registru by rozhodovali sami majitelé fotbalového stadionu. Informace by kluby mohly sdílet.

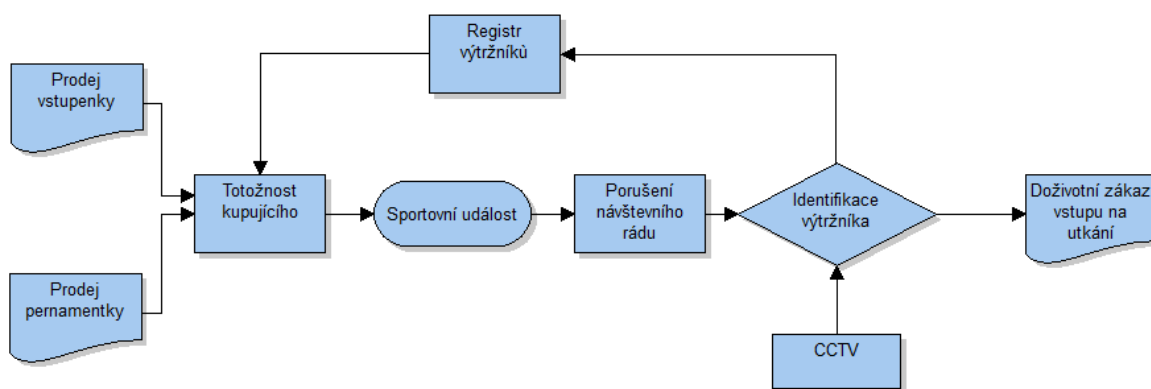
Ministerstvo zatím klubům připravilo instrukce, jak proti chuligánům postupovat, ale žádné zákonné posílení jejich pravomocí nechystá. Například zakázat někomu vstup na stadion by po právní stránce neměl být podle úřadů problém.

Prodejem lístku vznikne obchodně právní vztah, a pokud budou porušeny podmínky "smlouvy", třeba návštěvní řád, může klub takovou smlouvu vypovědět.

Ovšem v tom případě by musely kluby zajistit identifikaci diváků. Muselo by to fungovat podobně jako u zápasů Ligy mistrů nebo reprezentace, kdy se lístek prodává oproti občanskému průkazu, na který je možno zakoupit maximálně čtyři kusy.

Ministerstvo se při tvorbě manuálu proti rowdies nechalo inspirovat i ve Velké Británii nebo Itálii. Tam podobným opatřením nahrává i fakt, že zápasy jsou vyprodané a velké procento diváků tvoří majitelé permanentek.

Pak je zákaz skutečně definitivní a znamená vyloučení z fanouškovského prostředí, ze subkultury, kterou představuje. U nás to může dopadnout tak, že si prostě ten dotyčný nechá koupit lístek do jiné části hlediště.



Obr. 1 Blokové schéma funkce registru výtržníků

I. TEORETICKÁ ČÁST

2 TRESTNÝ ČIN

Je označení pro jednání, kterým pachatel zásadním způsobem poškozuje nebo ohrožuje státní mocí chráněné zájmy a které proto stát trestá zpravidla vězením nebo jiným způsobem. Termín je morálně indiferentnější náhradou za původně eticko-právní výrazy zločin a přečin. Méně závažný delikt se nazývá přestupek. [15]

2.1 Definice trestného činu

Trestný čin (u mladistvých pachatelů je nazýván též provinění) je v českém trestním právu jediným základem trestní odpovědnosti. Je chápán jako ucelená množina přesně vymezených znaků, jež musí být všechny naplněny v zákonem předpokládané míře, a to v době spáchání skutku, v němž je trestný čin spatřován. Absence byť i jednoho znaku má za následek, že čin, který se trestnému činu podobá, trestným činem právě pro nenaplnění či nedostatečné naplnění byť i jednoho znaku být nemůže. K trestní odpovědnosti za trestný čin je třeba úmyslného zavinění, nestanoví-li trestní zákon výslovně, že postačí zavinění z nedbalosti.

Podle § 3 trestního zákona (č. 140/1961 Sb. ve znění novel) byl trestný čin pro společnost nebezpečný čin, jehož znaky byly uvedeny v tomtéž zákoně. Tato formulace vyjadřovala jednak překonání praxe, kdy skutkové podstaty trestných činů byly obsaženy i v mnoha speciálních zákonech, jednak vymezení vůči pojetí, v němž by bylo možno trestat činy, které nejsou v zákoně explicitně popsány. [15]

2.2 Znaky trestného činu

V první, obecné části trestního zákona byly popsány obecné znaky trestných činů, mezi něž patřily:

1. Společenská nebezpečnost větší než nepatrná

Stupeň nebezpečnosti činu pro společnost je určován zejména významem chráněného zájmu, který byl činem dotčen, způsobem provedení činu a jeho následky, okolnostmi, za kterých byl čin spáchán, osobou pachatele, mírou jeho zavinění a jeho pohnutkou. Zákon

však nespecifikuje, jakým způsobem se z těchto faktorů stupeň nebezpečnosti odvozuje, například které osoby pachatelů nebo pohnutky společenskou nebezpečnost zvyšují nebo snižují. Blíže nespecifikované přihlížení k „osobě pachatele“ může znamenat narušení ústavou zaručené rovnosti před zákonem.

2. Zavinění

K trestnosti činu je třeba úmyslného zavinění, nestanoví-li trestní zákon výslovně, že postačí zavinění z nedbalosti.

3. Trestní odpovědnost z hlediska věku a přičetnosti pachatele

Vyloučení trestnosti za podmínek krajní nouze, nutné obrany a oprávněného použití zbraně.

4. Územní a personální omezení působnosti zákona

5. Trestnost pokusu, přípravy i podílnictví na činu

6. Podmínky zániku trestnosti a promlčení trestního stíhání

Ve druhé, tzv. zvláštní části trestního zákona byly definovány znaky takzvané formální skutkové podstaty jednotlivých trestných činů.

Trestní zákoník č. 40/2009 Sb., účinný od 1. ledna 2010, přinesl drobné korekce v pojetí trestného činu. Podle § 13 odst. 1 je trestným činem protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně. Tato definice trestného činu opustila uvádění nebezpečnosti činu pro společnost jako samostatné a nezávislé podmínky trestnosti a sjednotila její posuzování s posuzováním formálního naplnění skutkové podstaty. [15]

2.3 Vztah trestnosti a zakázanosti činu

Trestní zákon popisované skutky nezakazuje výslovně, ale pouze je označuje za trestné a stanoví za ně trest (podobně je koncipován i přestupkový zákon). Pojetí a jazyk trestního zákona (převzaté z původního trestního zákona z roku 1852) jsou tímto nekompatibilní s jazykem Listiny základních práv a svobod a ústavy platné od roku 1993, podle nichž občan může činit vše, co není zákonem zakázáno (čl. 3 odst. 4 Ústavy ČR, čl. 2 odst. 3 Listiny ZPS).

V praxi se při výkladu předpokládá, že z trestnosti činu vyplývá jeho zakázanost implicitně, tj. spáchání trestného činu bývá běžně označováno jako porušení (přestoupení) zákona. Pro osoby bez trestní odpovědnosti se termín „trestný čin“ nepoužívá, v některých zákonech (o sociálně-právní ochraně dětí a o soudnictví ve věcech mládeže) se používá termín „čin jinak trestný“, aniž by bylo výslovně stanoveno, že takové činy jsou dětem zakázány. [15]

3 ORGANIZACE STADIONU PRO RÚZNE SPORTY

3.1 Základní druhy ochrany

1. Režimová opatření
2. Činností příslušníka fyzické ostrahy
3. Ochranou technickými prostředky: EZS, EPS, ACS, CCTV,....

3.2 Rozdělení ochrany dle charakteru střežené oblasti

3.2.1 Plášťová ochrana

Zajišťuje plášť objektu na styku s prostorami jiných uživatelů nebo veřejnými prostorami. Jedná se obvykle o kombinaci detektorů tříštění skla, magnetických kontaktů detekujících otevření otvíratelných ploch.

3.2.2 Prostorová ochrana

Detekuje pohyb narušitele uvnitř objektu. Obvykle se jedná o kombinaci pasivních infračervených (PIR) detektorů pohybu a detektorů duálních (detektor má vestavěny dva senzory a poplach vyhlašuje jako logický součin poplachů od jednotlivých senzorů; obvyklá je kombinace PIR a mikrovlnného senzoru). Výběr detektoru závisí na jeho stanovišti a místních podmínkách. Duální detektory jsou obecně odolnější proti falešným poplachům způsobeným vnějším prostředím. V prostorách s pohybem veřejnosti, například v historických budovách a národních památkách, bývá zvykem instalovat detektory s antimaskingem, který detekuje případné pokusy o vyřazení detektoru z funkce např. zakrytím.

3.2.3 Předmětová ochrana

Doplňuje zabezpečení plášťové a prostorové. Je to samostatné zabezpečení vybraných předmětů v objektu. Obvykle jsou detektory předmětové ochrany přiřazeny do samostatně ovládané skupiny (skupin), což umožňuje střežení těchto předmětů i v době, kdy je budova v provozu. Jako příklad poslouží magnetické kontakty a otřesová čidla na dveřích nebo stěnách trezorových skříní, komorových trezorů, dveřích skříní s IT technologiemi apod.

Otřesové detektory na stěnách (příp. stropěch a podlahách) místností, které jsou současně obvodovou stěnou objektu, jsou také součástí plášťové ochrany.

3.2.4 Obvodová ochrana

Jedná se o zvláštní druh pro střežení obvodu rozsáhlých areálů a komplexů budov, jako jsou rozvodny, energetické podniky, vojenské objekty, skladové areály, letiště a velké průmyslové objekty. Perimetrické systémy jsou schopny na základě venkovních duálních infrabariér, mikrofonních či zemních kabelů zachytit narušitele ještě před vlastním vniknutím do střeženého prostoru. Tímto poskytují bezpečnostním složkám větší časový interval k provedení zásahu. Principů a možností nasazení perimetrické ochrany je více a vhodnost jejich aplikace vždy posuzujeme v závislosti na konkrétních podmínkách a terénu areálu. Nejvyšší efektivitu pro střežení ploch je dosahováno kombinací perimetrického systému se systémem kamerovým.

3.3 Rozdělení stadiónů a sportovních akcí

Slovo stadion pochází z antiky, kde se jednalo o podélné sportovní závodiště v délce 600 stop. Což v Olympii činilo asi 192 metrů, v římské době to bylo asi 180 metrů. Dnes je tímto slovem označováno prakticky každé větší sportoviště vybavené technickým a organizačním zázemím jak pro samotné sportovce, sportovní organizátory, sportovní novináře a diváky. Hlediště stadionu bývá stupňovité tak, aby všichni diváci dobře viděli. Stadion určený pro kolektivní hry, atletiku, plavecké sporty, dráhovou cyklistiku atd. může, ale nemusí být krytý, velké moderní stadiony mívají střechu vždy, ty nejmodernější z nich pak mívají konstrukce se střechou částečně či úplně zatahovací. Moderní stadiony bývají také velmi často řešeny jako víceúčelová zařízení, která mohou sloužit pro mnoho různých kulturních a společenských akcí mimo-sportovní povahy. [15]

Každý stadión svojí strukturou klade odlišný důraz na použité technologie, či prvky ochrany. Např. u sportovních stadionů, které mají rozlehlé otevřené plochy chráněné ploty, (např. motokrosový, běžecký) může být hlavní důraz kladen na perimetrickou ochranu, obráceně u uzavřeného objektu (např. hokejový, krytý fotbalový) spíše na plášťovou a prostorovou detekci.

3.3.1 Stadióny s uzavřeným perimetrem

Např. zimní, plavecký, cyklistický, tenisový,....

Hlavní nároky kladeny na : - plášťovou ochranu
- prostorovou ochranu

3.3.2 Stadióny s částečně uzavřeným perimetrem

Např. motokrosový, golfový, atletický, olympijský,...

Hlavní nároky kladeny na : - obvodovou ochranu
- prostorovou ochranu

3.3.3 Sportovní akce konané na volném prostranství

Např. závody na divoké řece, orientační běh, biatlon,...

Hlavní nároky kladeny na: - pořadatelskou službu
- zábrany

4 TECHNICKÉ PROSTŘEDKY PRO ZABEZPEČENÍ STADIÓNŮ

4.1 Elektronická Zabezpečovací Signalizace (EZS)

Jádrem EZS je zabezpečovací ústředna, která vyhodnocuje stav detektorů a je uživatelem ovládána nejčastěji pomocí klávesnice. Uživatel pomocí kódu přes klávesnici ústřednu zapíná do střežení nebo ji ze střežení vypne a může se po objektu pohybovat. Pomocí detektorů jsou hlídány všechny prostory, u kterých je nežádoucí, aby do nich pachatel vniknul nebo se v nich pohyboval. Detektorem je myšleno zařízení, které předá zabezpečovací ústředně signál v případě, že vyhodnotí stav, který je považován za narušení. Je potřeba si uvědomit, že EZS nezabrání narušení objektu, ale pouze upozorní na skutečnost, že k narušení došlo. Na tento stav může systém upozornit (lokálně) akustickou a optickou signalizací nebo (dálkově) předat zprávu ostraze. Akustická a optická signalizace je aktivována ihned po narušení, na pachatele působí psychicky, ale nezaručuje ochranu objektu.

Zprávu o narušení fyzické ostraze lze předat pomocí telefonních linek nebo bezdrátovým přenosem. Fyzickou ostrahu může představovat sám zákazník nebo je možné předat zprávu bezpečnostní agentuře, která zásah provede. Pro bezpečnostní agenturu se vžil název „Pult Centrální Ochrany – PCO“. Nespornou výhodou zásahu je přímé zadržení pachatele, ale zásah je proveden až po příjezdu ostrahy. Při návrhu je tedy nutné uvažovat o určitém zpoždění od okamžiku narušení do okamžiku, kdy dojde k zásahu. Například v případě narušení okna je zpoždění zásahu rozhodující a pachateli stačí poměrně krátká doba k loupeži a k opuštění místa. V takovém případě je vhodné instalovat i mechanické zábrany, které pachateli komplikují přístup a prodlužují dobu narušení – loupeže. [6]

4.1.1 Detektor

Zařízení bezprostředně reagující na fyzikální změny (jevy) související s narušením střeženého prostoru, jevu indikace stavu narušení vyvolává v čidle vyslání poplachového signálu, zprávy.

4.2 Kamerový systém (CCTV)

Zkratka CCTV je odvozena od anglického pojmu „Closed Circuit Television“, čemuž odpovídá český ekvivalent „uzavřené televizní okruhy“. Zatímco veřejné televizní vysílání je přístupné každému, kdo vlastní televizor, CCTV obraz je přístupný pouze tomu, kdo je připojen přímo do jeho okruhu. Často se pro kamerové systémy používá rovněž starší pojem průmyslová televize (nebo průmyslové kamery), což vyjadřuje původní použití CCTV kamer převážně pro průmyslové aplikace. Postupně se však začala průmyslová televize používat rovněž ve školství a zdravotnictví, ke sledování dopravy, ke kontrole výrobních procesů atd. Největší uplatnění však našly CCTV kamerové systémy při zabezpečení nejrůznějších objektů. Proto se můžeme často setkat rovněž s pojmem bezpečnostní kamery. [6]

Každý kamerový systém se skládá z kamer, přenosových tras a z jednoho nebo více pracovišť pro sledování, vyhodnocení a zpracování informací. Jednotlivé kamery mohou být pevné (nepohyblivé) nebo otočné. Například dálkově ovládané kamery SpeedDome umožňují výběr úhlu pohledu, přiblížení a zvětšení detailu, detekci aktivity atd.

V některých aplikacích může být výhodné i použití IP kamer umožňujících přenos signálu po síti Ethernet. Pro záznam a zpracování informací z kamer jsou v poslední době používány především digitální videosystémy. Samozřejmostí je i připojení do počítačové sítě LAN/WAN a kompletní dálková správa.

Při použití kamer ze standardní rozlišovací schopností (cca 400 TV řádků) můžeme požadavky na rozpoznání detailu v rámci snímané scény kategorizovat do čtyř skupin:

- snímání podrobného obrazu - identifikace kde by cílový objekt neměl představovat při zobrazení méně než 120 % výšky obrazovky
- snímání detailu - rekognoskace kde by cílový objekt neměl představovat při zobrazení méně než 50 % výšky obrazovky
- snímání polodetailu – detekce kde by cílový objekt neměl představovat při zobrazení méně než 10 % výšky obrazovky

- přehledové snímání – monitorování skupiny osob kde by cílový objekt neměl představovat při zobrazení méně než 5 % výšky obrazovky

4.2.1 IP kamery

Tato technologie kamer je u nás celkem mladá a stále se vylepšuje díky neustálému vývoji nových technologií a různých funkcí, ale to ji nebrání na obrovském vzestupu díky jednoduchosti instalace, kvalitnímu obrazu a dostupnosti.

Můžeme se také setkat s názvem síťové kamery, jelikož kamery se zapojují přímo do počítačové sítě dvěma způsoby a to pomocí kabelu (UTP) nebo bezdrátově pomocí WIFI. V případě zapojení kamery pomocí kabelu je obrovskou výhodou napájení pomocí stejného kabelu (UTP), po kterém jsou přenášena data. Toto napájení se nazývá PoE (Power over Ethernet), ke kterému je zapotřebí speciální switch, který PoE podporuje (stejně tak musí PoE podporovat i kamera, což je dnes již standardní funkce). Tohle je obrovskou výhodou, ke kameře nám stačí pouze jeden kabel, který se postará o vše. Další výhodou je videosever, právě díky němu se můžeme na obraz z kamery vzdáleně pomocí internetového prohlížeče podívat.

Dále je možné použít přímo nahrávací zařízení k záznamu IP kamer tzv. Network Video Recorder (NVR). Každý typ NVR má různé modely, které se nejčastěji liší počtem zařízení (IP kamer, webserverů), které dovolují spravovat a to 4, 8, 16, 48 a 64. Od počtu podporovaných se pak odvíjí výkonnost procesoru, operační paměti a kapacita harddisku (např. 1TB). Při výběru NVR zařízení je důležité zkontrolovat podporu IP kamer, jelikož ne vždy mají veškeré ovladače a to z důvodu, že výrobci nepoužívají vždy stejný protokol komunikace. Zapojení NVR do systému zvládne naprosto každý, jelikož zařízení stačí zapojit do internetové sítě, vyhledat kamery na určených IP adresách a nastavit parametry nahrávání.

4.3 Elektronická kontrola vstupu (EKV)

Systémy kontroly vstupu se používají k řízení přístupu osob, resp. vozidel do chráněných prostorů nebo ke chráněným zařízením nebo informacím, na základě přidělených přístupových práv. Tato zařízení také umožňují sledovat pohyb osob v prostorových zónách. Systémy EKV využívají koncové aktivní prvky, např. elektrické zámky, turnikety, propouštěcí brány a další. Jako nositel přístupového oprávnění jsou využívána různá média, např. magnetické a čipové karty, čipové přívěšky různých tvarů a nejnověji se využívá biometrických informací, např. otisky prstů, zobrazení oční duhovky nebo sítnice nebo čtení obrazu obličeje.

4.4 Elektrická Požární Signalizace (EPS)

Vhledem ke zvýšeným požadavkům pojišťovacích ústavů a s přechodem na normy EU nachází stále více uplatnění systémy požární signalizace (EPS). EPS je zařízení, které včasnou signalizací umožňuje snížit výši škod zapříčiněných požárem, jehož častou příčinou bývá nedodržení technologických postupů a nedůsledná kontrola bezpečnostních předpisů. Proti požárům se bráníme jednak odpovědným přístupem k požární prevenci, jednak použitím nejmodernější techniky. Velmi důležité je i včasné zjištění vznikajícího požáru, které do značné míry ovlivní jeho likvidaci a tím i výši vzniklých škod.

4.4.1 OPPO

Obslužné pole požární ochrany je prvek EPS pro systémy napojené prostřednictvím zařízení dálkového přenosu (ZDP) na útvary požární ochrany.

OPPO indikuje provozní stavy zařízení EPS v jednotné formě a umožňuje zásahovým složkám požární ochrany ergonomickou a jednotnou obsluhu zařízení v případě poplachu a při zkouškách. Indikační a obslužné prvky jsou rozmístěny na předním panelu, který je přehledně rozdělen na osm polí.

4.4.2 KTPO

Klíčový trezor KTPO slouží k úschově a ochraně objektového klíče na přístupném místě. Klíč je uložen a elektricky kontrolován pod dvěma dvířky. Při vyhlášení požárního poplachu v uzavřeném objektu ústředna EPS uvolní vnější dvířka KTPO pro přístup zásahové jednotky HZS. Otevření vnějších dvířek je monitorováno v systému elektrické zabezpečovací signalizace (EZS). Vnitřní dvířka otevírají členové příslušné jednotky HZS, na základě dokumentace zdolávání požáru regionálním klíčem, a tím je umožněn přístup k objektovému klíči.

4.5 Nouzový zvukový systém (NZS)

Nouzový zvukový systém je systém pro zesílení nebo distribuci zvuku, který se používá pro rychlou a uspořádanou mobilizaci obyvatel při nouzových situacích. Vhodnější neoficiální název je Evakuační rozhlas. Pokud jde o systém používaný k řízení evakuace při požáru, používá se často název Požární rozhlas.

NZS tvoří nedílnou součást bezpečnostních systému a opatření pro ochranu osob ve veřejných a průmyslových objektech. Nezbytným předpokladem funkce systému evakuačního ozvučení je v každém okamžiku zaručení srozumitelnosti a reprodukce řeči. Konkrétní zpráva musí být zřetelná, jasná, přenesená v odpovídající hlasitosti na odpovídající místo, zároveň musí být potlačeny případné odrazy způsobené velkými plochami a různé dozvuky, které by mohly výslednou kvalitu reprodukce zcela znehodnotit. Základním prvkem systému je řídicí jednotka. V případě větších systémů se zde používá programovatelná dálkově ovládaná modulární matice, která podle potřeby digitálně zpracovává a přepíná jednotlivé audio signály a směřuje je do příslušných okruhů. Tyto procesy probíhají automaticky (na základě aktuálních vstupních informací a časového harmonogramu) nebo je řídí operátor. Součástí řídicí jednotky mohou být i moduly pro digitální záznam a reprodukci zpráv. Systém lze také využít jako efektivní komunikační nástroj pro reprodukci náladové hudby, různých reklamních spotů, směřování automaticky generovaných nebo živých hlášení do příslušných oblastí.

5 TECHNICKÉ PROSTŘEDKY PRO PŘENOS DAT

5.1 Strukturovaný Kabelážní Systém (SKS)

Každá výkonná datová síť je tvořena dvěma nedílnými součástmi. Infrastrukturou - komunikačním prostředím a aktivními prvky, které jej využívají. Infrastrukturou může být strukturovaný kabelážní systém založený na melickém nebo optickém vedení, bezdrátový přenosový systém apod. Kvalita a výkonnost infrastruktury přímo ovlivňuje výsledné vlastnosti a výkon datové sítě.

S prudkým rozvojem internetových aplikací a technologií je kladen stále větší důraz na zabezpečení přístupu do datových sítí a ochranu vlastních dat systému před zneužitím nebo napadením. Je patrný trend integrace různých bezpečnostních funkcí již do základních prvků sítě, jako jsou přepínače, směšovače, switche (aktivní prvky) apod.

Trend konvergence datových a telefonních linek do jediné komunikační infrastruktury si vynutil potřebu zajistit kvalitu služby (QoS) pro provoz citlivý na kvalitu datové sítě (IP telefonie, videokonference). Moderní datová síť je schopna pracovat s několika třídami provozu a každé z těchto tříd je schopna zajistit potřebnou kvalitu služby.

Datová síť je stále více integrována do bezpečnostních aplikací jako komunikační kanál s uživateli, a to jak po místní síti či po internetu. Také je hlavním přenosovým médiem v rámci IP kamer.

V dnešní době je využívána hvězdicová topologie. Síť je propojena pomocí kabelů k centrálnímu prvku (switch). Tento koncentrátor tvoří pomyslný střed sítě. Výhodou je menší chybovost, protože porucha jednoho kabelu vyřadí z provozu pouze jednu stanicí. K propojení prvků sítě se používá kroucené dvojlinky. Hvězdicová topologie je nejpoužívanější metodou propojení v sítích LAN. [6]

Důvodem kroucení vodičů je zlepšení elektrických vlastností kabelu. Minimalizují se takzvané přeslechy mezi páry a snižuje se interakce mezi dvojlinkou a jejím okolím, tj. je omezeno vyzařování elektromagnetického záření do okolí i jeho příjem z okolí.

5.1.1 Kategorie datové sítě

Kategorie 1: Tento typ rozvodů není určen k datovým přenosům, lze jej použít např. k telefonním rozvodům. Přenosové rychlosti do 1 Mbit/s, vhodné např. pro analogové telefonní rozvody, ISDN a podobně.

Kategorie 2: Určen pro přenos dat, s maximální šířkou pásma 1,5 MHz. Používá se pro digitální přenos zvuku a především pro rozvody IBM Token Ring. Přenosové rychlosti kolem 4 Mbit/s.

Kategorie 3: Rozvody určené pro rozvody dat a hlasu s šířkou pásma 16 MHz a přenosovou rychlostí do 10 Mbit/s. Využívá se u datových přenosů označovaných jako 10Base-T Ethernet.

Kategorie 4: Určen pro přenos dat v síti Token ring, s šířkou pásma 20 MHz a přenosovou rychlostí do 16 Mbit/s.

Kategorie 5: Pracuje v šířce pásma do 100 MHz. Rozvody pro počítačové sítě s přenosovou rychlostí 100 Mbit/s, resp. 1 Gbit/s v případě využití všech 8 vláken. Využíván u 100 Mbit/s TPDDI a 155 Mbit/s ATM. V současné době je nahrazen standardem kategorie 5E.

Kategorie 5e: Pracuje rovněž v šířce pásma do 100 MHz, avšak vyžaduje nové způsoby měření parametrů a v některých parametrech je přísnější. Cílem je provozovat 1 Gbit/s. Využíván u 100 Mbit/s TPDDI, 155 Mbit/s ATM a GigabitEthernet.

Kategorie 6: Pracuje s šířkou pásma 250 MHz. Využívá se pro ultra-rychlé páteřní aplikace v oblasti lokálních sítí. V současné době nejpobulárnější kabeláž pro nově budované rozvody.

Kategorie 6a: Pracuje s šířkou pásma 500 MHz. Používá se pro zvláště rychlé páteřní aplikace v oblasti lokálních sítí. Využívá se i pro 10GBASE-T Ethernet (10 Gbit/s).

Kategorie 7: Pracuje v šířce pásma do 600 - 700 MHz. Kabel je plně stíněný - každý pár je stíněn zvlášť Al fólií a kabel sám má ještě celkový štít. Tato „plně stíněná“ konstrukce má ale za následek větší váhu, větší vnější průměr a menší ohebnost kabelu než UTP nebo ScTP. Používá se pro přenosy plné šířky videa.

5.2 Zařízení Dálkového Přenosu (ZDP)

5.2.1 Přes pevnou telefonní linku - GENOVA

Slouží k automatickému přenosu informací o stavu z objektů zabezpečených protipožárními poplachovými systémy EPS do místa, odkud je organizován zásah. K přenosu informace jsou využívány metalické okruhy jednotné telekomunikační sítě nebo pobočkové ústředny, od kterých je zařízení galvanicky a kapacitně odděleno. Běžný hovorový provoz na těchto linkách není narušen, komunikace probíhá nezávisle na jejich obsazení v nadhovorovém pásmu.

Přenosový systém tvoří:

- přenosové zařízení PZ1-VK, objektová karta, vysílač
- přenosové zařízení PZ1-PK, ústřednová karta, přijímač

5.2.2 Bezdrátový přenos - NAM

Rádiová síť Global 2 je několika frekvenční síť, která využívá výhod jednosměrného a obousměrného rádiového přenosu. Data z rádiových objektových zařízení jsou na jedné frekvenci (f_1) přenášena do páteřní sítě sběrných stanic RSN 451. Přenos v páteřní síti pak probíhá na frekvenci druhé (f_2). Rozdělením přenosu dat na více frekvencí tak několikrát vzrostla kapacita rádiové sítě. Komunikace mezi sběrnými stanicemi je obousměrná a mezi objektovými zařízeními a sběrnými stanicemi jednosměrná. Obousměrný provoz umožňuje po páteřní síti přenášet efektivně velké datové toky, konfigurovat a ovládat činnost sběrných stanic na dálku. Výhodou jednosměrného provozu je nízká cena objektového zařízení, velká kapacita sítě a odolnost vůči místnímu rušení.

5.2.3 Bezdrátový přenos - LATIS

Síť LATIS je tvořena objektovými stanicemi LATIS 2400 a LATIS 2400N na straně objektů a radiovým modemem LR 324 pro hlavní - radiovou komunikaci a telefonním modemem LT 300 pro záložní komunikaci na straně centrální stanice systému.

Síť LATIS je sítí řízenou, tzn., že provoz probíhá na principu „výzva-odpověď“; je řízen centrální stanicí (PCO).

Komunikace se všemi objekty je obousměrná, tzn., že bezchybný přenos informace je příjemcem potvrzen a teprve potom je tato informace vymazána v paměti zdroje zprávy. Žádná zpráva se tedy neztratí ani v případě externího rušení, výpadku napájení nebo jiného technického problému a je předána po obnovení normální funkce sítě. V případě, že nelze v určitém okamžiku předat události radiovou cestou (rušení, sabotáž na anténě...), objektové zařízení předá události telefonní cestou.

Obousměrnost sítě je kromě potvrzování příjmu zprávy využívána pro přenosy povelů na objekty. Povelem může být obecně spuštění určitého zařízení, jako zapnutí kamery, světel, sirény ap. Nebo zastřežení/odstřežení objektu, zaklíčování stanice pro servisní účely, případně provedení změny v parametrech objektové stanice z PCO.

Síť LATIS komunikuje rychlostí 2400 Bd s kódovaným přenosem dat a může zpracovávat data nejen z ústředen EZS a EPS, ale i data technologického charakteru. Všechny tyto systémy je možné v síti LATIS monitorovat a ovládat z centrálního pracoviště (PCO).

Každé z objektových zařízení LATIS 2400 nebo LATIS 2400N může pracovat jako retranslační stanice. Může zde pracovat až 15 objektových zařízení v řadě za sebou - 15 vrstev (pro vykrytí území velikosti okresu obvykle dostačuje 5 retranslačních vrstev). Počet retranslátorů v jednotlivých vrstvách není omezen. Je zde propracovaný režim automatického nalezení nové cesty spojení objektu s PCO v případě výpadku některého z používaných retranslátorů. Všechna objektová zařízení v síti LATIS pracují na jedné frekvenci. Každé objektové zařízení může být v síti LATIS dálkově ovládáno a programováno přímo z centrální stanice.

6 MECHANICKÉ ZÁBRANNÉ SYSTÉMY (MZS)

Jedná se zejména o prostředky pro ohraničení prostoru (např. zdi, ploty, vstupní bezpečnostní systémy vrat, branek), prostupů (mříže, bezpečnostní skla, fólie) a vlastní uzamknutelné systémy. K MZS řadíme i prostředky individuální ochrany, které mohou sloužit i samostatně, převážně jako úschovné objekty. Patří sem především mobilní a stacionární trezory, trezorové skříně, ohnivzdorné skříně, příruční pokladny, přenosné kontejnery a kufry. Základní úlohou mechanických zábranných systémů je vytvořit pevnou překážku proti násilnému vniknutí osob a zabránit znehodnocení a krádeži předmětů, techniky a zařízení umístěných v chráněném objektu.

Poskytují ochranu svou mechanickou pevností => vytvoření překážky, která je definovaná určitým odporem proti destruktivnímu narušení.

6.1 Průlomová odolnost

Je to doba, kterou musí pachatel vynaložit na překonání mechanické pevnosti MZS.

Každý MZS je překonatelný, avšak rozlišnost jednotlivých druhů je dána množstvím vydané energie, času a druhu náradí, kterých je třeba k překonání. Tím je dána úroveň bezpečnosti jednotlivých objektů.

Postavení MZS u systému komplexního zabezpečení je dáno jejich schopností vytvořit kvalifikovanou zábranu proti průniku pachatelů do objektů chráněného zájmu, to je vyjádřeno maximálním prodloužením časového intervalu Δt , který pachatel potřebuje k překonání překážky a tím dosažení chráněného zájmu.

$$\Delta t = t_2 - t_1 \text{ [min]}$$

kde: Δt časový interval potřebný k překonání překážky

t_1 čas zahájení útoku na překážku

t_2 čas konečného překonání překážky

6.2 Vybrané mechanické zábranné prostředky

6.2.1 Turniket

Je to zařízení, které funguje jako brána, kterou může v jednu chvíli projít pouze jeden člověk. Turnikety byly původně používány jako jiný druh ohrady, který měl dovolit průchod lidem, ale zabránit ovčím a jiným zvířatům ohradu opustit. Dnes se používají zejména k usměrnění pohybu lidí.

Může být vytvořený tak, že průchod je umožněn pouze po vložení mince nebo po ověření dokladu o zaplacení. Turnikety bývají použity v místech placeného vstupu jako v veřejné dopravě, na placených toaletách, pro přístup k atrakcím, parkům nebo zařízením atd. V neveřejných objektech (např. administrativních nebo průmyslových) může turniket sloužit ke kontrole oprávněnosti vstupu a k evidenci příchodů a odchodů.

Některé druhy turniketů nepodmiňují průchod žádným poplatkem ani oprávněním, ale jejich účelem je umožňovat průchod jen jedním směrem. Takové typy turniketů se používají například v místě vstupu do samoobslužné prodejny, v místě východu z placeného prostoru (metra, zoologické či botanické zahrady) apod.

6.2.2 Mříže

Mechanický zábranný prostředek plášťové ochrany a jde o jeden z nejstarších prostředků určených k zabezpečení prosklených výplní proti násil. vniknutí. Dle provedení rozdělujeme: Nůžkové, rolovací a pevné.

6.2.3 Bezpečnostní skla

Chrání takto zajištěné prosklené výplně proti násilnému vniknutí, jedná se o mechanický zábranný prostředek plášťové ochrany. Vyrábějí se v provedení bezpečnostní skla tvrzená a vrstvená.

6.2.4 Rolety

Neposkytují takovou ochranu jako mříže, ale působí preventivně. Jsou konstrukčně tvořeny lamelami, které jsou pružné, ale bezpečně navzájem spojeny. Vyrábí se jako dutý profil z plastu (nemá ochranou hodnotu), nebo z hliníku, extrudovaného hliníku a oceli. Bývá to

vypěněno tzv. ultra tvrdým polyuretanem - vlastnosti tvrdého dřeva a taženými vlnitohliníkovými profily. Lamely zapadají do vodicích lišt, ve spodní části do sedacích lišt. Existuje také kombinace centrálně plánovaných rolet, kdy uživatel může naprogramovat zatahování a vytahování rolet (mříží).

6.2.5 Ploty a zdi

Plot či oplocení je volně stojící stavba, která má za úkol zabránit nebo omezit pohyb přes nějakou hranici. Na rozdíl od zdi má mnohem jednodušší konstrukci. Zeď je postavena z kamene nebo betonu a zabraňuje nejenom pohybu ale i průhledu.

7 SLUŽBY FIREM V PKB

7.1 Základní rozdělení

7.1.1 Operativa PKB

- detektivní služba
- osobní ochrana
- služby přeprav peněz a cenností a zpracování peněžních hotovostí
- obranné konkurenční zpravodajství
- ofenzivní konkurenční zpravodajství
- vlivové zpravodajství

7.1.2 Výkonné technické služby PKB

- monitorování statických objektů
- monitorování pohyblivých objektů
- obsluha telefonních PCO, GSM a GIS PCO
- dispečerská pracoviště PCO
- dodávka a montáž EZS, CCTV, EPS, ACS
- datová bezpečnost
- mechanické a elektronické zabezpečení vozidel
- přenos bezdrátových signálů a dat
- mříže, tapety, bezpečnostní skla a fólie, perimetre
- ochrana zboží

7.1.3 Služby obecného bezpečnostního výkonu PKB

- objektová bezpečnost a režimová opatření
- fyzická ochrana a ostraha (pochůzkáři, patrol systém, vrátník, klíčová služba, recepční, psovodi)
- zásahové jednotky PCO

- bezpečnostní projekty ostrahy
- statická a pohyblivá ochrana objektů
- bezpečnostní doprovody osob, bezpečnostní dozor

7.1.4 Pomocné služby PKB

- speciální úklidové služby
- výdej klíčů
- technická zpráva objektu

7.1.5 Speciální služby PKB

- krizové plánování a řízení
- akreditační a certifikační orgány
- znalecké a posudkové orgány
- provoz hasičských zákonných sborů podniku

7.1.6 Analytické služby

- bezpečnostní experti
- poradci a konzultanti
- oceňování bezpečnostních rizik
- bezpečnostní projektová činnost
- bezpečnostní analýza a audit
- bezpečnostní poradenství

7.2 Služby zaměřené na zabezpečení stadiónů

7.2.1 Provozování Pultu Centralizované Ochrany (PCO)

Pult centralizované ochrany je dispečerské pracoviště, které zajišťuje střežení objektů zabezpečených pomocí elektrické zabezpečovací signalizace (EZS). Na PCO jsou v zakódované podobě přenášeny veškeré relevantní informace, které je systém EZS schopen poskytnout. Při vyhlášení poplachu na objektu vysílá operátor PCO na objekt zásahovou jednotku nebo, podle typu zvolené služby, informuje kontaktní osobu určenou majitelem

objektu. V případě, že zásahová skupina zjistí narušení objektu, usiluje o zadržení pachatele a minimalizuje škody, které pachatel v objektu může napáchat. Operátor PCO přivolá Policii ČR a kontaktní osoby. Zásahová skupina objekt střeží až do příjezdu policie a majitele nebo pověřené osoby. Rychlý zákrok zásahové jednotky chrání život, zdraví a majetek uživatelů střeženého objektu.

Přenos informací z ústředny elektrického zabezpečovacího systému na pult centralizované ochrany lze zajistit mnoha způsoby – přes rádiový vysílač, GSM a GPRS komunikaci, přenos v síti internet až po připojení pomocí jednotné telekomunikační sítě. V čem spočívají hlavní rizika při přenosu dat po pevné lince? Není nic jednoduššího, než přestříhnout jeden telefonní drát v ústředním rozvaděči (ten je obvykle snadno přístupný nejen pro techniky telefonní společnosti), a o vloupání se nikdo nedoví.

7.2.2 Pořadatelská služba

Slouží pro organizaci příchodů, pohybu a odchodů účastníků akce, dále pro kontrolu oprávněnosti účastníka na akci a pro podání základních informací. Její úloha je i preventivně bezpečnostní. Podle požadavků zákazníka může být v civilním oděvu s nebo bez označení, či uniformě.

7.2.3 Bezpečnostní služba

Slouží pro udržení pořádku a práva, dohlíží na respektování pokynů organizátora účastníky akce. Její úloha je nejen preventivně bezpečnostní, aktivně zasahuje proti narušitelům průběhu akce. Může plnit i úkoly pořadatelské služby. Podle požadavků zákazníka může být v civilním oděvu s nebo bez označení, či uniformě.

7.2.4 Zásahová služba

Používá se pouze v případě vyššího rizika narušení akce větším počtem osob (sportovní akce - fanoušci, společenské a kulturní akce - demonstranti). Je tvořena vycvičenou, adekvátně vyzbrojenou taktickou jednotkou v uniformách. Zabráňuje vzniku větších škod na zdraví a majetku před tím, než mohou účinně zasáhnout určené státní složky.

7.2.5 Kontrolní propustková služba

Zabraňuje neoprávněnému vstupu osob, vjezdu vozidel do objektu, provádí kontrolu osob a dopravních prostředků, které opouštějí objekt s cílem zabránit vyvážení či vynášení majetku.

7.2.6 Kontrolní činnost

Zabraňuje rozkrádání, ztrátě, poškození, zneužití či zničení majetku, plní úkoly spojené s objektovou a protipožární bezpečností v rozsahu vymezeném ve smlouvě o ochraně objektu.

7.2.7 Střežení objektu

Na pevných stanovištích, podnikovým službám, patrol systémem, úkolem na pevných stanovištích ⇒ zabránit vstupu a vjezdu osob do objektu na místech mimo kontrolní propustkovou službu, zabránit nekontrolovanému vývozu, vnesení materiálu a dalších věcí ze střeženého objektu a zabránit vzniku mimořádných událostí v objektu, zabránit vstupu, vjezdu mimo stanovené místo vstupu, vjezdu, zabránění vloupání.

7.2.8 Vyrozumění míst poskytující pomoc

Vyrozumění havarijních služeb, hasičských útvarů, lékařské záchranné služby, policie. Zajištění dalších opatření v zájmu zákazníka – další doplňkové služby, které byly sjednány.

7.3 Hlavní úkoly

Dle zákona zabránit trestné a protiprávné činnosti:

- zasáhnout při zjištění protiprávní a trestné činnosti a to v souladu s přiměřeností zásahu na daný zájem
- zalarmovat síly k pomoci (HZS, PČR, ...)
- udržet či obnovit klid bezpečnosti a veřejného pořádku
- včas rozpoznat a odhadnout nebezpečí při havárií, požárech a jiných mimořádných událostech ⇒ realizovat opatření

8 ZÁKONNÉ A NORMATIVNÍ ÚPRAVY PLATNÉ V ČR

8.1 Platné normy

ČSN EN 50130-4:1997 Poplachové systémy. Část 4: Elektromagnetická kompatibilita.

Norma skupiny výrobků: Požadavky na odolnost komponentů požárních systémů, zabezpečovacích systémů a systémů přivolání pomoci. Tato norma stanovuje požadavky na odolnost komponentů poplachových systémů, určených pro použití uvnitř a v okolí budov, v prostředích obytných, obchodních, lehkého průmyslu a průmyslových:

- Elektrické zabezpečovací systémy (EZS)
- Elektrická požární signalizace (EPS)
- Uzavřené televizní okruhy pro zabezpečovací účely (CCTV)
- Systémy kontroly vstupů (EKV)
- Systémy přivolání pomoci
- Systémy tísňové
- Systémy přenosové

Norma uvádí zkušební postupy provádění zkoušek a stanovuje stupně přísnosti na zařízení používaná pro vnitřní a venkovní aplikace, pro pevná, pohyblivá a přenosná zařízení. Norma se nezabývá elektromagnetickým vyzařováním. Tato norma je prvním představitelem přebíraných evropských norem na poplachové systémy.

ČSN EN 50131-1 Poplachové systémy - elektrické zabezpečovací systémy uvnitř a vně budov.

Část 1: Všeobecné požadavky.

Tato norma zavádí termín Poplachové systémy místo dříve používaného termínu Elektrická zabezpečovací signalizace (EVS) a uvádí termín Elektrické zabezpečovací systémy se zkratkou EZS. Tato evropská norma je specifikací pro elektrické zabezpečovací systémy. Konkrétně popisuje čtyři stupně zabezpečení a čtyři třídy vlivu prostředí. Popisuje dále sestavování zabezpečovacích systémů. Norma je určena jako vodítko pro pojišťovací společnosti, dodavatele EZS, uživatele a policii při stanovování kompletní a přesné specifikace ochrany pro konkrétní objekty. Norma však neurčuje druh zabezpečovacího systému, rozsah nebo míru detekce a ani nutně nepokrývá všechny požadavky na

konkrétní systém. Všechny odkazy a požadavky této normy na elektrické zabezpečovací systémy se týkají základních minimálních požadavků a projektanti daného objektu musí vzít v úvahu povahu objektů, hodnotu majetku uvnitř objektů, míru rizika vniknutí případného narušitele a kterékoli další faktory, které mohou ovlivnit výběr stupně a složení zabezpečovacího systému. Aby byla zajištěna úroveň požadovaného zabezpečení, elektrické zabezpečovací systémy a jeho komponenty jsou rozděleny do stupňů zabezpečení, které berou v úvahu míru rizika, která závisí na typu objektu, hodnotě majetku a na předpokládaném typu narušitele. Stupeň zabezpečení 4 je nejpřísnější (opačný než u ČSN 334590). Tato norma specifikuje požadavky na provedení nainstalovaných zabezpečovacích systémů, neobsahuje požadavky pro návrh, projekci, instalaci, provoz údržbu. Toto řeší změna Z1 ČSN EN 50131-1 do doby, než bude vydána ČSN EN 50131-7. V normě jsou specifikovány požadavky pro komponenty elektrických zabezpečovacích systémů příslušné klasifikace prostředí. Tato klasifikace popisuje prostředí, ve kterém se předpokládá, že bude komponent EZS pracovat v souladu se svým provedením.

Norma byla zaváděna do soustavy ČSN dle rozhodnutí ČSNI následujícím způsobem:

Bylo rozhodnuto o souběžné platnosti ČSN EN 50131-1 s ČSN 334590 ČSN EN 50131-1 je schválena a vydána K ČSN 334590 je vydána změna, která obsahuje upozornění na souběžnou platnost a odůvodnění souběžné platnosti s ČSN EN 50131-1. Jsou opraveny odvolávky na platné ČSN.

K ČSN EN 50131-1 je vypracována změna Z1, která ve formě národních informativních příloh specifikuje požadavky na jednotlivé komponenty elektrických zabezpečovacích systémů včetně jejich zkoušení a jejich vlastních aplikací.

Současně s vydáním této Změny Z1 bylo ČSN 334590 zrušena v celém rozsahu.

ČSN EN 50131-6 Poplachové systémy - Elektrické zabezpečovací systémy

Část 6: Napájecí zdroje.

Tato evropská norma je specifikací pro napájecí zdroje elektrických zabezpečovacích systémů instalovaných v budovách. Norma také obsahuje požadavky pro napájecí zdroje instalované vně budov ve vztahu ke komponentům instalovaným v budově, které se normálně instalují na vnější plášť budovy. PŘÍKLAD - Doplnková ovládací zařízení nebo signalizační zařízení. Tato norma stanoví požadavky, zkušební postupy a stupně

zabezpečení (označené arabskými číslicemi 1 až 4) na napájecí zdroje používané v elektrických zabezpečovacích systémech a systémech přivolání pomoci používaných v budovách. Norma uvádí povinné funkce, které musí zajišťovat napájecí zdroje a funkce volitelné, včetně požadavků, které se mají splňovat.

ČSN EN 50132-7 Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích.

Část 7: Pokyny pro aplikaci.

Norma obsahuje doporučení zřizovatelům CCTV sledovacích systémů, řídicí a organizační postupy pro instalaci, testování, obsluhu a údržbě systému technického vybavení.

ČSN EN 50134-7 Poplachové systémy - Systémy přivolání pomoci.

Norma obsahuje doporučení poskytovatelům pro efektivní a účinné řídicí a organizační postupy pro instalaci, testování, obsluhu a údržbě systému přivolání pomoci včetně technického vybavení a organizování pomoci.

ČSN EN 50136-1-1 Poplachové systémy - Poplachové přenosové systémy a zařízení.

Část 1-1: Všeobecné požadavky na poplachové přenosové systémy. Norma stanovuje základní požadavky na provedení, spolehlivost a charakteristické bezpečnostní znaky poplachových přenosových systémů. Zahrnuje všeobecné požadavky spojení s podmínkou signalizace mezi poplachovým systémem a poplachovým přijímacím centrem. Uvádí terminologii.

ČSN EN 50136-1-2 Poplachové systémy - Poplachové přenosové systémy a zařízení.

Část 1-2: Požadavky na systémy využívající vyhrazené poplachové přenosové cesty. Norma stanovuje požadavky na poplachové přenosové systémy využívající drátová vedení (např. stejnosměrná vedení nebo přenos modulovaného signálu po symetrickém vedení), spojení v hovorovém pásmu nebo datové linky a může obsahovat multiplexery nebo zařízení na zpracování hlášení, linky společné s jinými službami, které zahrnují účastnickou telefonní přípojku ve střežených prostorech, televizní kabelové rozvody nebo energetickou rozvodnou síť.

ČSN EN 50136-1-3 Poplachové systémy - Poplachové přenosové systémy a zařízení.

Část 1-3: Požadavky na systémy s digitálními komunikátory využívající veřejnou komutovanou telefonní síť. Norma stanovuje požadavky na komutovaná spojení, která zajišťují řízený přenos událostí mezi poplachovým systémem a vzdáleným centrem (PCO) pomocí digitalizovaných signálů.

ČSN EN 50136-1-4 Poplachové systémy - Poplachové přenosové systémy a zařízení.

Část 1-4: Požadavky na systémy s hlasovými komunikátory využívající veřejnou komutovanou telefonní síť. Norma stanovuje požadavky na spojení přenášející namluvených hlasových zpráv uložených v paměťovém mediu.

ČSN EN 50136-2-1 Poplachové systémy - Poplachové přenosové systémy a zařízení.

Část 2-1: Všeobecné požadavky na poplachová přenosová zařízení. Norma specifikuje všeobecné požadavky na poplachová přenosová zařízení, která se používají v poplachových přenosových systémech.

ČSN EN 50136-2-2 Poplachové systémy - Poplachové přenosové systémy a zařízení.

Část 2-2: Požadavky na zařízení v systémech využívajících vyhrazené přenosové cesty. Tato norma uvádí dodatečné požadavky na zařízení v systémech využívajících vyhrazené přenosové cesty k požadavkům, které jsou stanoveny v normě ČSN EN 50136-2-1. Přenosový poplachový systém může používat drátové vedení (např. stejnosměrné vedení nebo přenos modulovaného signálu po symetrickém vedení), spojení v hovorovém pásmu nebo datové linky a může obsahovat multiplexery nebo zařízení na zpracování hlášení. Normu lze také použít pro přenosové poplachové systémy, které využívají jako přenosové médium linky společné s jinými službami. Tyto služby zahrnují účastnickou telefonní přípojku ve střežených prostorech k místní ústředně, televizní kabelové rozvody nebo energetickou rozvodnou síť, jsou-li použitelné i pro jiné systémy.

ČSN EN 50136-2-3 Poplachové systémy - Poplachové přenosové systémy a zařízení.

Část 2-3: Požadavky na zařízení v systémech s digitálními komunikátory využívající veřejnou komutovanou telefonní síť. Tato norma uvádí dodatečné požadavky na zařízení v systémech s digitálními komunikátory využívajícími veřejnou komutovanou telefonní síť k požadavkům, které jsou stanoveny v normě ČSN EN 50136-2-1. Vzdálená centra jsou

většinou poplachovými přijímacími centry. Mohou to být však i přenosová zařízení v satelitních stanicích splňující požadavky normy ČSN EN 50136-1-2. Účelem této normy je stanovit znaky provedení na zařízení v systémech s digitálními komunikátory využívajícími veřejnou komutovanou telefonní síť, k zabezpečení jejich způsobilosti pro použití a kompatibility s různými druhy poplachových systémů.

ČSN EN 50136-2-4 Poplachové systémy - Poplachové přenosové systémy a zařízení.

Část 2-4: Požadavky na zařízení v systémech s hlasovými komunikátory využívajícími veřejnou komutovanou telefonní síť. Tato norma uvádí dodatečné požadavky na zařízení v systémech s digitálními komunikátory využívajícími veřejnou komutovanou telefonní síť k požadavkům, které jsou stanoveny v normě ČSN EN 50136-2-1. Vzdálená centra jsou většinou poplachovými přijímacími centry. Mohou to být však i přenosová zařízení v satelitních stanicích splňující požadavky normy ČSN EN 50136-1-2. Účelem této normy je stanovit znaky provedení na zařízení v systémech s digitálními komunikátory využívajícími veřejnou komutovanou telefonní síť, k zabezpečení jejich způsobilosti pro použití a kompatibility s různými druhy poplachových systémů.

ČSN EN 50130-5 Poplachové systémy - Zkoušky vnějších vlivů

Tato norma určuje metody zkoušek vlivu prostředí použité pro zkoušení komponentů systému následujících poplachových systémů určených pro použití uvnitř a v okolí budov:

- Elektrické zabezpečovací systémy
- Systémy tísňové
- Systémy přivolání pomoci
- Systémy CCTV pro bezpečnostní aplikace
- Systémy kontroly vstupů
- Poplachové přenosové systémy

ČSN EN 50133-1 Poplachové systémy-Systémy kontroly vstupů v bezpečnostních aplikacích.

Část 1: Systémové požadavky. Tato norma popisuje všeobecné požadavky na funkčnosti systému kontroly vstupů pro použití v zabezpečovacích aplikacích. Norma také popisuje všeobecné požadavky na komponenty z hlediska prostředí. Pokud některá část systému kontroly vstupů (například rozhraní přístupného místa) tvoří část zabezpečovacího

poplachového systému, musí tato část splňovat současně i příslušné požadavky norem na zabezpečovací systémy.

ČSN EN 50133-7 Poplachové systémy-Systémy kontroly vstupů v bezpečnostních aplikacích.

Část 7: Aplikační směrnice. Tato evropská norma byla vydána jako zdroj informací pro správce a zřizovatele systémů kontroly vstupů a jako vodítko pro vyhledávání nabídek a pro montáže a údržbu. Tato norma uvádí pokyny k použití automatizovaných systémů kontroly vstupů a komponentů uvnitř a vně budov na základě norem řady ČSN EN 50133. Zahrnuje návrh systému, instalaci, předávání, provoz a údržbu systémů kontroly vstupů.

ČSN EN 60849 Nouzové zvukové systémy

Nejdůležitější dokument pro NZS, definuje požadavky na návrh systému, způsob zapojení, na technologická zařízení, montáž, zkoušení a provoz NZS.

ČSN EN 60268-16 Elektroakustická zařízení

Norma předepisující metodiku měření srozumitelnosti.

8.2 Tabulkový přehled evropských norem pro zabezpečovací a signalizační systémy

Jednotlivé části ve skupinách norem EN 50 13y-x jsou děleny následovně:

- 1 - Systémové požadavky
- 2-4 - Požadavky na jednotlivé části systému
- 5 - Propojení, komunikace, přenos signálu
- 6 - Napájení, rezerva v číslování
- 7 - Pokyny pro aplikace

8.2.1 Poplachové systémy - Elektrické zabezpečovací systémy (EN 50 131-X)

Číslo normy	Název části
EN 50 131-1	Všeobecné požadavky
EN 50 131-2-2	Pasivní detektory
EN 50 131-2-3	MW detektory
EN 50 131-2-4	Kombinované detektory- pasivní/MW
EN 50 131-2-5	Kombinovaná detektory - pasivní/UZ
EN 50 131-2-6	Detektory otevření
EN 50 131-3	Ústředny
EN 50 131-4	Výstražná zařízení
EN 50 131-5-3	Požadavky na zař. využívající bezdrátové připojení
EN 50 131-6	Napájecí zdroje
EN 50 131-7	Pokyny pro aplikace
EN 50 131-8	Zamlžovací bezpečnostní zařízení

8.2.2 Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích (EN 50 132-X)

Číslo normy	Název části
EN 50 132-5	Přenos videosignálu
EN 50 132-7	Pokyny pro aplikaci

8.2.3 Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích (EN 50 133-X)

Číslo normy	Název části
EN 50 133-1	Systémové požadavky
EN 50 133-2-1	Všeobecné požadavky na komponenty
EN 50 133-7	Pokyny pro aplikace

8.2.4 Poplachové systémy - Systémy přivolání pomoci (EN 50 134-X)

Číslo normy	Název části
EN 50 134-1	Systémové požadavky
EN 50 134-2	Aktivační zařízení
EN 50 134-3	Místní jednotka a kontrolér
EN 50 134-5	Propojení a komunikace
EN 50 134-7	Pokyny pro aplikace

8.2.5 Elektrická požární signalizace (EN 54 – X)

Číslo normy	Název části
EN 54-1	Úvod
EN 54-2	Ústředna
EN 54-3	Požární poplachová zařízení - Sirény
EN 54-4	Napájecí zdroj
EN 54-5	Hlásiče teplot
EN 54-7	Hlásiče kouře - Hlásiče bodové využívající rozptýleného světla, vysílaného světla a ionizace
EN 54-10	Hlásiče plamene
EN 54-11	Tlačítkové hlásiče
EN 54-12	Lineární optické hlásiče
EN 54-13	Posouzení kompatibility komponentů systému
EN 54-14	Aplikační návody
EN 54-16	Ústředny pro hlasová výstražná zařízení
EN 54-17	Izolátory
EN 54-18	Vstup/výstupní zařízení
EN 54-20	Nasávací hlásiče
EN 54-21	Přenosová zařízení
EN 54-24	Komponenty pro hlasové výstražné systémy
EN 54-25	Komponenty využívající rádiové spoje

8.3 Zákonné úpravy týkající se požární ochrany

8.3.1 Zákona č. 133/1985 Sb., o požární ochraně

Účelem zákona je vytvořit podmínky pro účinnou ochranu života a zdraví občanů a majetku před požáry a pro poskytování pomoci při živelních pohromách a jiných mimořádných událostech stanovením povinností ministerstev a jiných správních úřadů, právnických a fyzických osob, postavení a působnosti orgánů státní správy a samosprávy na úseku požární ochrany, jakož i postavení a povinností jednotek požární ochrany.

Každý je povinen počínat si tak, aby nezavdal příčinu ke vzniku požáru, neohrozil majetek, život a zdraví osob. Při zdolávání požárů, živelních pohrom a jiných mimořádných událostí je povinen poskytovat přiměřenou osobní pomoc, nevystaví-li tím vážnému nebezpečí, ohrožení sebe, osoby blízké a nebrání-li mu v tom důležitá okolnost.

8.3.2 VYHLÁŠKA 23-2008 o technických podmínkách požární ochrany staveb

Sbírka zákonů č.23/2009

Tato vyhláška stanovuje technické podmínky požární ochrany pro navrhování, provádění a užívání stavby. Byla oznámena v souladu se směrnicí Evropského parlamentu a Rady 98//34/ES ze dne 22. června 1998 o postupu poskytování informací v oblasti technických norem a předpisů a pravidel pro služby informační společnosti, ve znění směrnice 98/48/ES1).

8.3.3 VYHLAŠKA 246-2001 o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci)

Sbírka zákonů č. 246/2001

Z této vyhlášky vyplývá povinnost projektovat veškeré systémy sloužící pro technickou ochranu osob podle platných norem. Tím se tedy pro normy, které mají jinak pouze charakter doporučení, stávají závazné.

8.3.4 Únikové východy

Úniková cesta je komunikace, která umožňuje bezpečnou evakuaci osob z budovy nebo z její části ohrožené požárem na volné prostranství, kde nemohou být ohroženy. Únikové cesty a východy musí svým počtem, polohou, kapacitou, technickým vybavením a konstrukčním provedením odpovídat normovým hodnotám a tím vytvářet předpoklady k bezpečnému úniku osob.

Za únikovou cestu lze také považovat:

- rampy
- eskalátory
- evakuační výtahy, které slouží především k evakuaci osob s omezenou nebo žádnou schopností pohybu a osob z výškových objektů

8.3.4.1 Základní druhy únikových cest

Podle stupně ochrany, kterou únikové cesty poskytují unikajícím osobám, rozlišují se únikové cesty nechráněné a chráněné.

a) Nechráněná úniková cesta

NÚC je každý trvale volný komunikační prostor směřující k východu na volné prostranství nebo do chráněné únikové cesty. Nechráněné únikové cesty nemusí být od ostatních prostor v objektu odděleny stavebními konstrukcemi.

b) Chráněná úniková cesta

ChÚC je trvale volný komunikační prostor vedoucí k východu na volné prostranství a tvořící samostatný požární úsek, chráněný proti požáru požárně dělicími konstrukcemi. Za chráněnou únikovou cestu považujeme také komunikace (pavlače, schodiště), pokud jsou od vnitřních prostorů protipožárně odděleny obvodovými stěnami z nehořlavých hmot.

8.3.4.2 Jak má vypadat úniková cesta

Na únikové cestě musí být zřetelně označeny únikové východy, evakuační výtahy a směry úniku osob, (toto označení nemusí být provedeno v objektech s východy do volného prostoru, které jsou zřetelně viditelné a dostupné z každého místa). Bezpečnostní značení se umísťuje především tam, kde se mění směr úniku, kde dochází ke křížení komunikací a při jakékoli změně výškové úrovně. Dveře na únikových cestách musí být opatřeny odblokovatelným zámekem. Únikové cesty musí mít zajištěno dostatečné osvětlení. Chráněné únikové cesty, částečně chráněné únikové cesty (pokud nahrazují chráněnou únikovou cestu), cesty sloužící k evakuaci osob se sníženou schopností pohybu a orientace a osob neschopných samostatného pohybu musí být vybaveny nouzovým osvětlením. Musí být trvale volně průchodné komunikační prostory (chodby, schodiště apod.), které jsou součástí únikových cest, tak, aby nebyla omezena nebo ohrožena evakuace nebo záchranné práce. Nejmenší šířka nechráněné únikové cesty je 550 mm a nejmenší šířka chráněné a částečně chráněné únikové cesty je 825 mm se šířkou dveří alespoň 800 mm. Chráněné únikové cesty a všechny jejich součásti nesmí být využívány způsobem zvyšujícím požární riziko.

Ve stavbách s více než třemi nadzemními podlažími, ve kterých se trvale nebo pravidelně vyskytuje více než 10 osob s omezenou schopností pohybu a orientace nebo osob neschopných samostatného pohybu, musí být zřízeny evakuační výtahy. V ostatních budovách se evakuační výtahy zřizují v závislosti na normových hodnotách. Funkce evakuačního výtahu musí být zajištěna dodávkou elektrické energie ze dvou na sobě nezávislých zdrojů.



Obr. 2 Bezpečnostní značení únikových cest

8.4 Provozování kamerového systému z hlediska zákona o ochraně osobních údajů

Provozování kamerového systému je považováno za zpracování osobních údajů, pokud je vedle kamerového sledování prováděn záznam pořizovaných záběrů, nebo jsou v záznamovém zařízení uchovávány informace a zároveň účelem pořizovaných záznamů, případně vybraných informací, je jejich využití k identifikaci fyzických osob v souvislosti s určitým jednáním. Samotné kamerové sledování fyzických osob není zpracováním osobních údajů podle zákona č. 101/2000 Sb., protože postrádá úroveň podmínek pro zpracování údajů ve smyslu § 4 písm. e) zákona č. 101/2000 Sb. To však nevylučuje aplikaci jiných právních předpisů, zejména ustanovení občanského zákoníku upravujícího podmínky ochrany osobnosti.

Údaje uchovávané v záznamovém zařízení, ať obrazové či zvukové, jsou osobními údaji za předpokladu, že na základě těchto záznamů lze přímo či nepřímo identifikovat konkrétní fyzickou osobu (tedy: informace z obrazových či zvukových nahrávek umožňují, byť nepřímo, identifikaci osoby). Fyzická osoba je identifikovatelná, pokud ze snímku, na němž je zachycena, jsou patrné její charakteristické rozpoznávací znaky (zejména obličeje) a na základě propojení rozpoznávacích znaků s dalšími disponibilními údaji je možná plná identifikace osoby. Osobní údaj pak ve svém souhrnu tvoří ty identifikátory, které umožňují příslušnou osobu spojit s určitým, na snímku zachyceným, jednáním.

Zpracování osobních údajů provozováním kamerového systému je přípustné:

- a) v rámci plnění úkolů uložených zákonem (např. Policii České republiky); v těchto případech je třeba dbát ustanovení příslušného zákona,
- b) dále je toto možné na základě řádného souhlasu subjektu údajů; to však je prakticky realizovatelné ve velmi omezených případech, kdy je možné jednoznačně vymezit okruh osob nacházejících se v dosahu kamery,
- c) užití kamerového systému však je možné i bez souhlasu subjektu údajů s využitím ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb.

Povinnosti správce při provozování kamerového systému vybaveného záznamovým zařízením:

a) Kamerové sledování nesmí nadměrně zasahovat do soukromí. Kamerový systém je možno použít zásadně v případě, kdy sledovaného účelu nelze účinně dosáhnout jinou cestou (např. majetek je možno chránit před odcizením uzamčením místnosti). Dále je vyloučeno užití kamerového systému v prostorách určených k ryze soukromým úkonům (např. toalety, sprchy). Je ovšem možné řešení, kdy subjekt údajů má na výběr z alternativ (např. lze monitorovat prostory šatny stadionu za předpokladu, že je vymezen prostor pro převlékání, který není kamerami sledován).

b) Specifikace sledovaného účelu. Je třeba předem jednoznačně stanovit účel pořizování záznamů, který musí korespondovat s důležitými, právem chráněnými zájmy správce (např. ochranou majetku před krádeží). Záznamy tak mohou být využity pouze v souvislosti se zjištěním události, která poškozuje tyto důležité, právem chráněné zájmy správce. Přípustnost využití záznamů pro jiný účel musí být omezena na významný veřejný zájem, např. boj proti pouliční kriminalitě.

c) Je třeba stanovit lhůtu pro uchovávání záznamů. Doba uchovávání dat by neměla přesáhnout časový limit maximálně přípustný pro naplnění účelu provozování kamerového systému. Uchovávaná data by měla být uchovávána v rámci časové smyčky např. 24 hodin, pokud jde o trvale střežený objekt, nebo případně i dobu delší, v zásadě však nepřesahující několik dnů, nejde-li o pořizování záznamů policejním orgánem podle zvláštního zákona, a po uplynutí této doby vymazána. Pouze v případě existujícího bezpečnostního incidentu by měla být data zpřístupněna orgánům činným v trestním řízení, soudu nebo jinému oprávněnému subjektu.

d) Je třeba řádně zajistit ochranu snímacích zařízení, přenosových cest a datových nosičů, na nichž jsou uloženy záznamy, před neoprávněným nebo nahodilým přístupem, změnou, zničením či ztrátou nebo jiným neoprávněným zpracováním - viz § 13 zákona č. 101/2000 Sb.

e) Subjekt údajů musí být o užití kamerového systému vhodným způsobem informován (např. nápisem umístěným v monitorované místnosti), viz § 11 odst. 5 zákona č. 101/2000 Sb., nejde-li o uplatnění zvláštních práv a povinností vyplývajících ze zvláštního zákona.

f) Je třeba garantovat další práva subjektu údajů, zejména právo na přístup ke zpracovávaným datům a právo na námitku proti jejich zpracování, viz § 1 zákona č. 101/2000 Sb.

g) Zpracování osobních údajů je třeba registrovat u Úřadu pro ochranu osobních údajů, nejde-li o uplatnění zvláštního práva či povinností vyplývajících ze zvláštního zákona, viz § 18 odst. 1 písm. b) zákona č. 101/2000 Sb. [17]

II. PRAKTICKÁ ČÁST

9 VÝBĚR PŘEDMĚTU NÁVRHU

Celková koncepce návrhu zabezpečení je dána vlastnostmi objektu, jeho typologickým využitím, nároky kladenými na správu a požadavky provozovatele. Také je nutné zohledňovat zákonné úpravy, či nároky pojišťoven.

Výběr technického zabezpečení je dán podrobnou obhlídkou objektu, zpracováním bezpečnostních rizik a požárně bezpečnostního řešení.

Pro zpracování konkrétního řešení zabezpečení jsem zvolil hokejový stadion v Kroměříži. Jedná se o uzavřenou budovu tvořenou zděnou a z části kovovou konstrukcí. Budova se dělí na dvě části. A to ledovou plochu s tribunami a dvoupodlažní zázemí, které je využíváno i komerčně.

Zimní stadión je využíván pro pravidelné tréninky žákovských tříd, dorostu, juniorů i mužů (pravidelné utkání mistrovských zápasů 2. ligy ledního hokeje); samozřejmě je bruslení veřejnosti; dále je nabízen pronájem ledové plochy pro jednotlivce z řad veřejnosti, tak zde mají zajištěný pronájem i "soukromé" hokejové hobby oddíly hrající zde své soutěže. Kapacita 3000 diváků.



Obr. 3 Fotomapa objektu zimního stadionu [16]

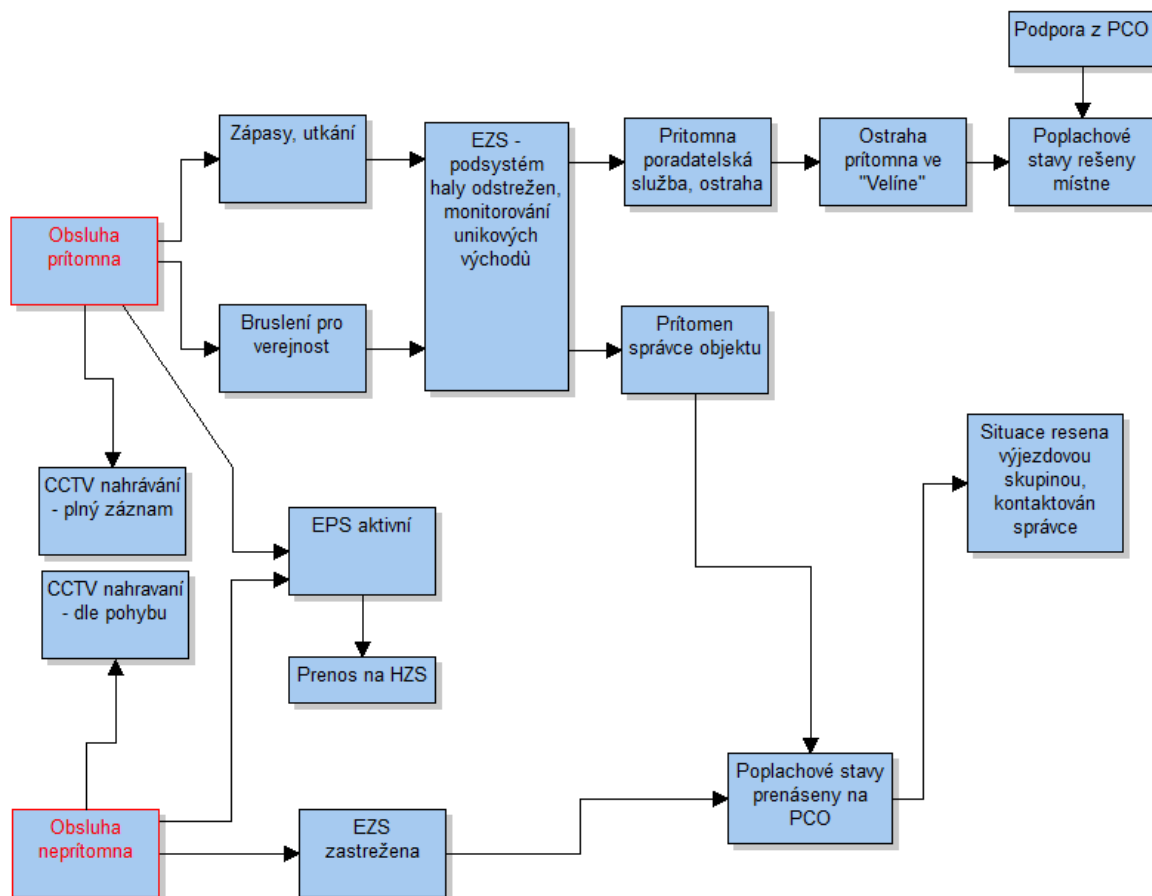
Objekt je v rámci dohledu a výstupu informací řešen z 2 pohledů:

1. Obsluha přítomna (konání akcí, atd.)

- přítomna poradatelská služba (bezpečnostní agentura)
- zřízeno monitorovací pracoviště v objektu
- vzniklé situace řešeny místně, s možnou podporou s dispečinkem PCO

2. Obsluha nepřítomna (objekt zabezpečen)

- veškeré informace přenášeny na PCO
- možnost dálkové správy a monitorování objektu



Obr. 4 Blokové schéma využití tech. prostředků dle režimu objektu

10 NÁVRH SYSTÉMŮ TECHNICKÉ ZABEZPEČENÍ

10.1 Elektrická zabezpečovací signalizace (EZS)

10.1.1 Představení navrhované technologie

S ohledem na úroveň zabezpečení a možné využití komerčních prostor a kanceláří v zázemí objektu jsem zvolil sběrníkový systém Galaxy Dimension GD520.

Ústředny Galaxy jsou již velmi dlouhou dobu oblíbeným zabezpečovacím systémem využívaným ve velmi široké řadě objektů. Příkladem jsou mnohé obchodní domy, obchodní řetězce, budovy státní správy, výrobní závody, restaurace, administrativní budovy, atd.

Nové nástroje jako např. zdokonalení správy uživatelů, možnost definice velkého počtu časových zón, přináší další nové možnosti využití ústředny.

Ústředna využívá ke komunikaci s uživatelem i instalačním technikem velmi srozumitelné textové menu s propracovanou nápovědou. K pohodlí přispívá i široké spektrum dostupných komunikačních kanálů počínaje RS232 a konče TCP/IP.

Barevná grafická klávesnice s dotykovým displejem výrazně usnadňuje orientaci v menu a přibližuje tak celý systém samotnému uživateli. Příkladem je přehledné zobrazení stavu detektorů před zapnutím nebo nové možnosti v zobrazení historie událostí.

Samozřejmostí je možnost integrace do grafických softwarových nadstaveb.

Nově jsou dostupné velmi užitečné uživatelské vzory oprávnění a časové přístupové zóny. To vše doplňuje kalendář definující svátky nebo libovolná mimořádná období v kalendáři.

Hlavním rysem je jednotná hardwarová platforma. To umožňuje snadné rozšiřování kapacity systému dle potřeb.

Základní parametry Galaxy Dimension:

- až 32 samostatných oblastí
- až 520 smyček
- až 64 bezkontaktních čteček
- až 1000 uživatelů s kódem a kartou
- až 67 týdenních časových rozvrhů
- až 32 LCD klávesnic
- až 4 grafické dotykové klávesnice
- možnosti komunikace (tel. linka, Ethernet, RS-232)
- až 32 audio modulů pro příposlech
- integrace do grafických nadstaveb
- vyhovuje evropským normám EN 50131-1 a CLC TS 50131-3



Obr. 5 Ústředna EZS Galaxy Dimension

10.1.2 Konceptní řešení

System bude rozdělen na několik podsystémů. Hokejová hala, společné prostory, bufet, restaurace, Tipsport, administrativní prostory v 2.NP, kde se počítá dále s několikanásobným rozdělením dle využívání kanceláří.

Prostorová ochrana haly bude řešena duálními detektory RISCO RK325DT, které kombinují pasivní infračervenou a mikrovlnnou technologii. Tím dosáhneme zvýšenou ochranu proti falešným poplachům. Dále pak zázemí digitálními detektory Digigard 55. Plášťová ochrana bude tvořena magnetickými kontakty a v případě prosklené plochy nad tribunami použita infrazávora Triple PB-150.

Ovládání systému bude prováděno LCD klávesnicemi umístěnými u vstupu, v administrativní části a grafickou dotykovou klávesnicí ve „Velíně“.

10.1.2.1 Použité detektory

RK325DT

Navrhnuo pro náročnější prostředí haly.

Duální detektor digitální PIR+MW, dlouhý dosah (27 m), 2 nezávislé PIR snímače a 2 MW kanály, Antimasking, Krytí IP65, Technologie Greenline - V odstřeženém stavu je vypnuta MW část detektoru.

TRIPLE PB-150

Navrhnuo pro zabezpečení prosklené části nad tribunami.

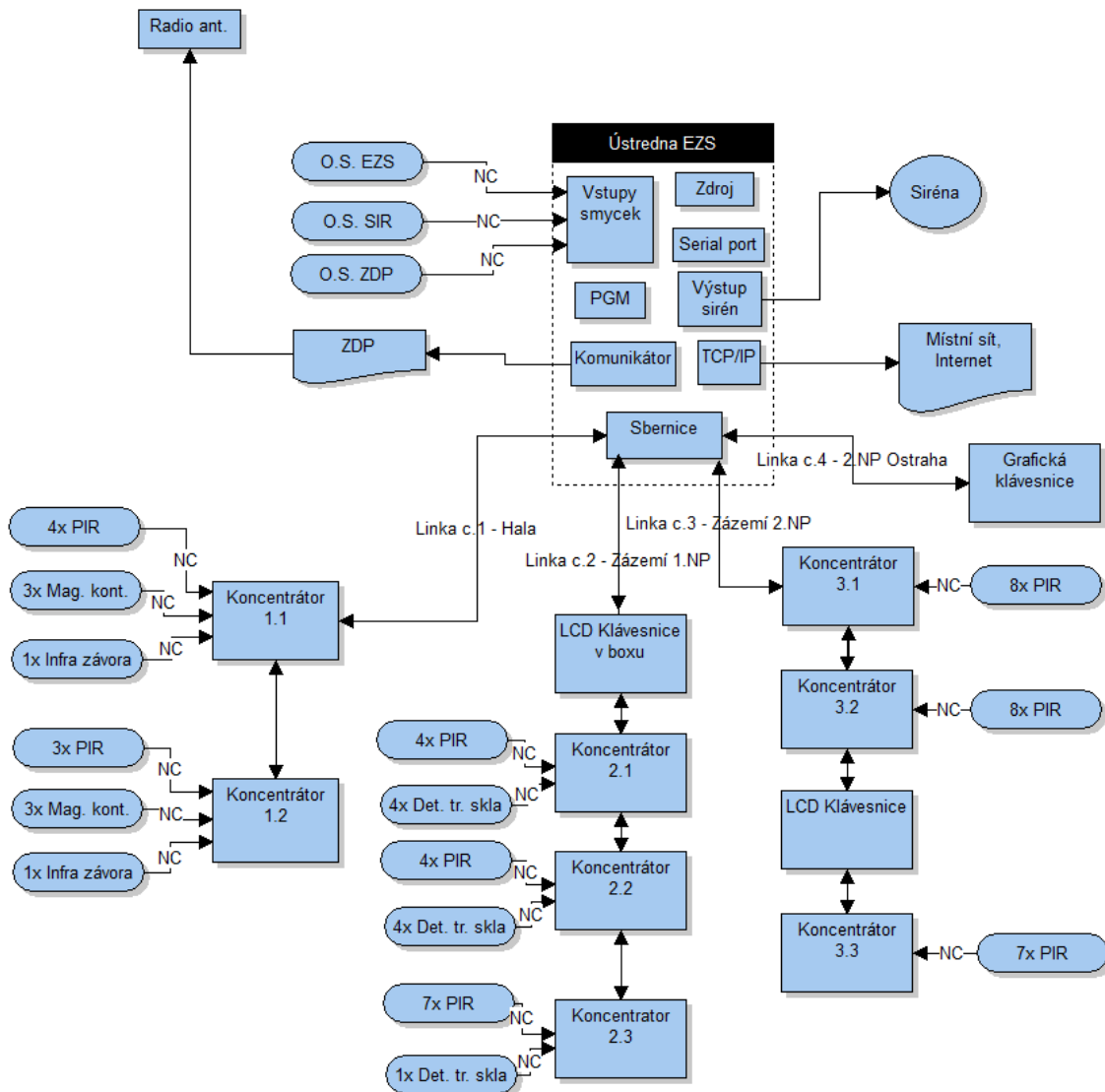
Tří paprsková infračervená závora určená pro venkovní nebo vnitřní instalaci. Dosah 150m. Použití 3 paprsků zvyšuje odolnost proti falešným poplachům a zvyšuje spolehlivost v nepříznivých klimatických podmínkách.

DIGIGARD 55

Navrhnuo pro zabezpečení kancelářských prostor v zázemí.

Dvojitý snímací prvek, digitální zpracování signálu, dosah 12 x 12m, úhel 110°, patentovaná technologie digitálního zpracování a počítání pulzů, kovový kryt pro odrušení VF polí.

10.1.3 Blokové schéma návrhu EZS



Obr. 6 Blokové schéma navrhovaného systému EZS

10.1.4 Návrh rozmístění prvků systému EZS

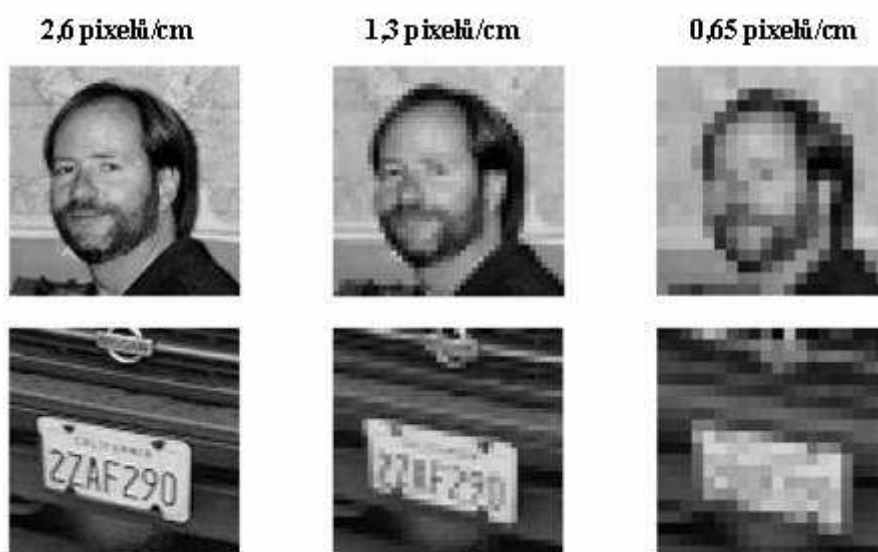
Viz. příloha č. 1.

10.2 Kamerový systém (CCTV)

10.2.1 Představení navrhované technologie

Klasické CCTV kamery pracují s rozlišením 640x480 pixelů. Obraz snímáný navrhovanými kamerami má rozlišení 3264x2448 pixelů tj. snímají několikanásobně větší počet bodů. Chceme-li dosáhnout jednoznačnou identifikaci osob, potřebujeme rozlišení alespoň 1,3 pixelů na cm. Proto klasické kamery potřebují přiblížit sledovaný objekt.

Toho se dá dosáhnout především trvalou obsluhou kamerového systému. Jedině tak se dá konkrétní záznam získat. S přiblížením se však ztrácí záznam zbývající části zorného pole, které v dané chvíli kamera snímala.



Obr. 7 Zobrazení detailu na základě počtu pixelů

Naproti tomu navrhované řešení s vysokým rozlišením pro získání stejně kvalitního záznamu žádné přibližování detailů nepotřebuje. Proto se při něm neztrácí záznam celého pole a není potřebná obsluha. Další výhodou je navíc i to, že pokud při sledování daného objektu potřebujeme přiblížit některý detail, můžeme si ho digitálně zvětšit, ale záznam celého předchozího objektu běží nerušeně dál a pokud by v této době došlo k incidentu, událost bude zaznamenána a může být potom zpětně dohledána.

Horizontální velikost zorného pole kamery je 180° . Klasické kamery dovedou zaznamenat přibližně 30° . Pokud bychom tedy chtěli mít stejný zorný úhel, potřebujeme šest klasických kamer. Pokud chceme dosáhnout již výše vzpomenutého stupně rozlišení, klesne nám úhel záběru na přibližně 3 - 5 stupňů. Jinak se nepodaří dosáhnout takového stupně rozlišení.

Pokud bychom tedy potřebovali dosáhnout stejně vysokého stupně rozlišení v celém zorném poli, potřebovali bychom k tomu přibližně deset klasických kamer CCTV. To za podmínky stejného zorného pole, stejné kvality záznamu a nepřetržitého sledování objektu.

10.2.1.1 Použité kamery

Arecont Vision AV8185

IP kamera dome barevná 180° , 4x1/2", 8MPix, f=4x8mm, H.264/MJPEG, PoE

Megapixel panoramatická IP kamera 180° , 4x CMOS 1/2", 4x 2MPixel, 4x (1600x1200 pixelů) při 24 sn./s, 4x objektiv f=8.0mm, 0.2 Lux/F2.0, H264, MJPEG, napájení PoE (IEEE 802.3af).



Obr. 8 Kamera Arecont Vision AV8185

Arecont Vision AV8365

IP kamera dome barevná 360°, 4x1/2", 8MPix, f=4x4mm, H.264/MJPEG, PoE

Megapixel panoramatická IP kamera 360°, 4x CMOS 1/2", 8.0, 4x 2MPixel, 4x (1600x1200) při 24 sn./s, 4x objektiv f=4.0mm, 0.2 Lux/F2.0, H264, MJPEG, napájení PoE (IEEE 802.3af).



Obr. 9 Kamera Arecont Vision AV8365

Arecont Vision AV1355DN

IP kamera dome Den/Noc, ICR, 1/2", 1.3MPix, f=4.5-10mm, H.264/MJPEG, 12V, PoE
Megapixel den/noc IP kamera, venkovní dome provedení, antivandal, mechanický ICR filtr, CMOS 1/2", 1.3 MPixel, 1280x1024 při 32 sn./s, VF objektiv s IR korekcí f=4.5-10mm, 0.1 Lux/F1.4, H264, MJPEG, montáž na strop nebo na zeď (3axis), napájení 12-48V DC nebo PoE (IEEE 802.3af), IP66.



Obr. 10 Kamera Arecont Vision AV1355DN

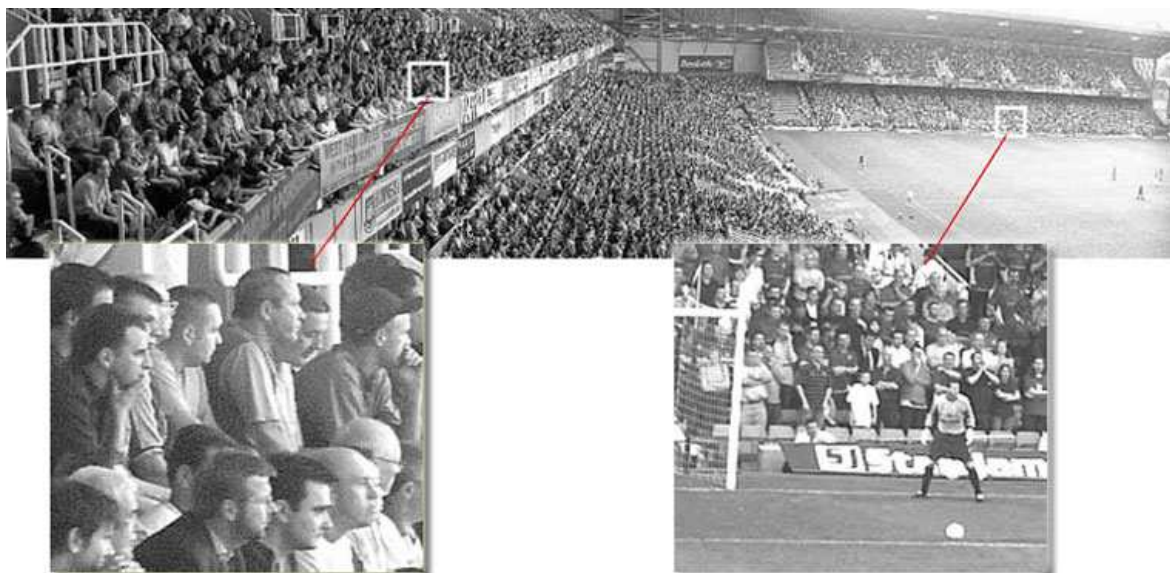
10.2.2 Konceptní řešení

Tradiční kamerové systémy mohou kontrolovat velké oblasti s vysokým rozlišením, ale jen za podmínky, že operátor ustavičně otočnou kamerou monitoruje ve správném směru a s přiměřeným zoomem danou oblast.

Pokud operátor vynechá místa s rozhodující událostí, tak tato nejsou zaznamenána. IP kamery řeší tento problém nahráváním celé oblasti ve vysokých rozlišeních.

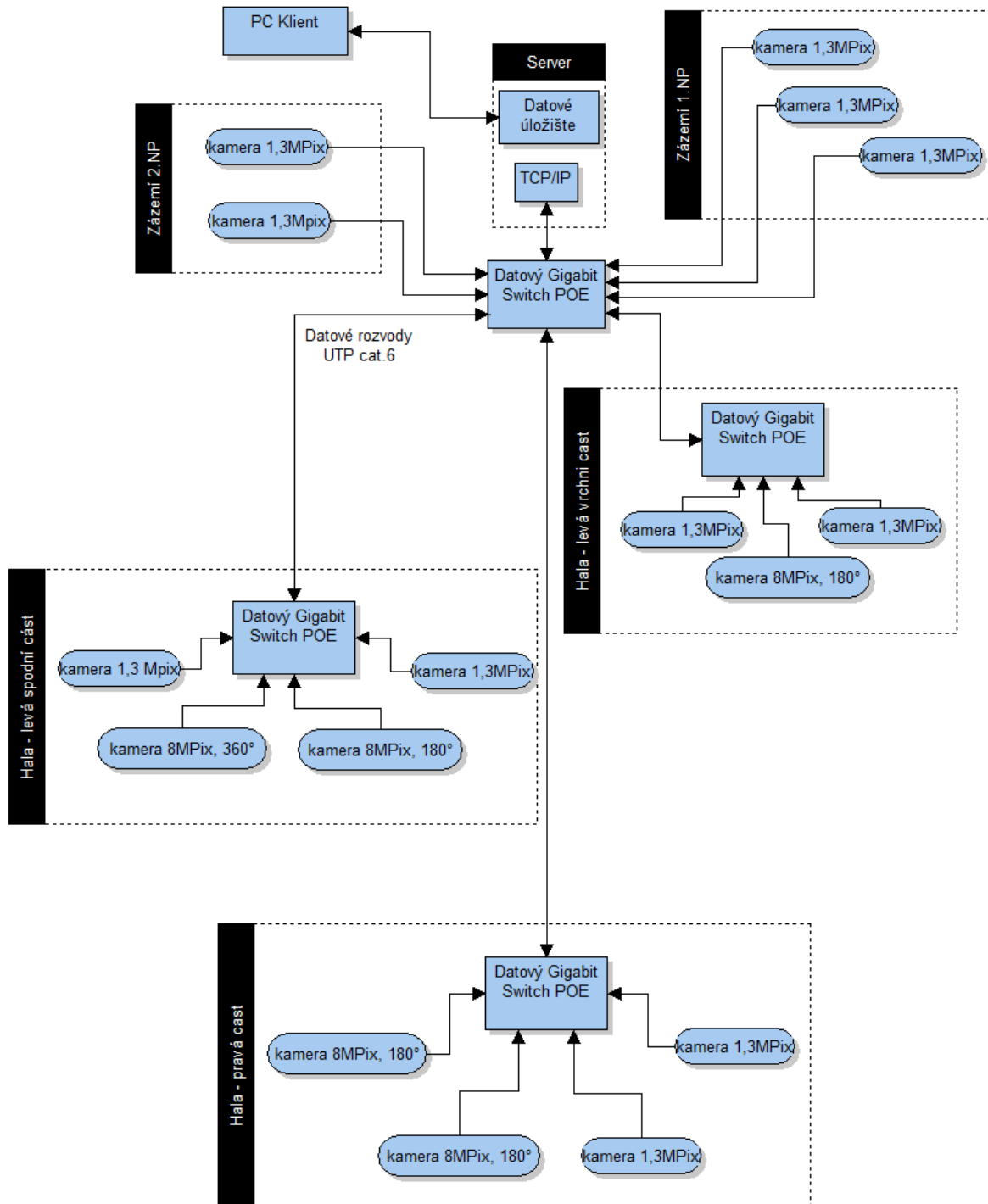
Navrhuji tzv. **Systém bez dozoru**, což je videosystém bez lidské obsluhy, které pouze zaznamenává dění ve střeženém prostoru pro pozdější prohlížení. Použití telemetrických kamer zde postrádá smysl, neboť chybí operátoři, kteří by natáčení a zoom kamer obsluhovali. Střežená plocha pak musí být kompletně vykryta fixními kamerami.

Na tribuny jsem použil kamery Arecont Vision AV8365 s 180° úhlem záběru (celkem 4ks), typ Arecont Vision AV8365 s 360° nad hrací plochu s instalací pod budoucí informační LCD-LED panel (kostku). Pro zbývající pokrytí únikových východů a prostor v zázemí kamery Arecont Vision AV1355DN.



Obr. 11 Příklad širokoúhlého záběru ve vysokém rozlišení s následným digitálním zvětšením

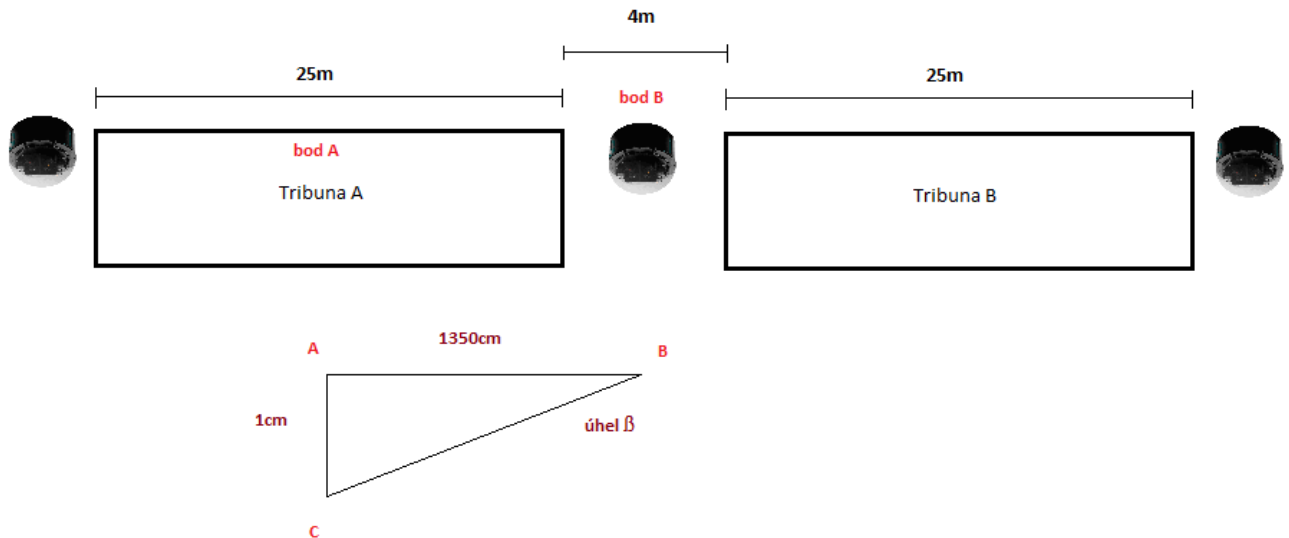
10.2.3 Blokové schéma návrhu systému CCTV



Obr. 12 Blokové schéma navrhovaného systému CCTV

10.2.4 Ověření správného výběru rozlišení a pokrytí kamer na tribunách výpočtem

Zvolená kamera obsahuje čtyři CMOS snímače o rozlišení 1600x1200 pixelů. Každý z nich pokrývá úhel 45°. Celkový záběr kamery je 180°. Cílem výpočtu je počet pixelů na 1 cm uprostřed zvolené tribuny, aby byla zabezpečena identifikace potencionálního výtržníka. Výsledný počet pixelů by měl být minimálně 1,3 pixelů/1cm.



Obr. 13 Náskres pro výpočet rozlišení kamer na tribunách

$$\text{tg} \beta = \frac{1}{1350}$$

$$\beta = 0,042^\circ$$

$$45^\circ \dots\dots\dots 1600 \text{ pixelů}$$

$$0,042^\circ \dots\dots\dots \underline{x \text{ pixelů}}$$

$$x = \frac{1600 \times 0,042}{45}$$

$$x = 1,5 \text{ pixelů} / \text{cm} \dots\dots\dots \text{návrh je vyhovující}$$

10.2.5 Návrh rozmístění prvků systému CCTV

Viz příloha č. 2.

10.3 Elektronická Kontrola Vstupu (EKV)

10.3.1 Představení navrhované technologie

Mým hlavním cílem je integrace vstupního, vstupenkového a pokladního systému. Variabilita a koncepce vstupenkového a pokladního systému jej předurčuje jak pro uzavřené lokální aplikace, tak i pro velké projekty v různých oblastech: Aquaparky, koupaliště, bazény, stadiony, haly, lyžařská střediska.

Implementací tohoto systému získáme účinný nástroj, který přinese komplexní a bezpečné řešení na vysoké technické úrovni na straně jedné a komfort a snadnou obsluhu na straně druhé.

ZÁKLADNÍ VLASTNOSTI:

- současná podpora více typů identifikátorů (vstupenka s čárovým kódem a bezkontaktní čip)
- modulární koncepce systému garantující trvalý rozvoj produktu
- snadné rozšíření a další aplikace včetně vzájemné vazby mezi aplikacemi
- možnost využití mobilních technologií
- evidence všech uživatelů a realizovaných událostí

VÝHODY SYSTÉMU CARDPAY:

- eliminuje na minimum lidský faktor kontroly
- šetří čas při prodeji a vyúčtování

- komfort a vysoká kultura poskytovaných služeb
- 100% kontrola všech pokladních operací
- vysoká ochrana proti neoprávněnému vstupu návštěvníků
- záznamy pokusů při neoprávněném pokusu o vstup

POKLADNA:

Pokladní místo zprostředkovává první kontakt se zákazníkem. Návštěvníkům je zde prodána vstupenka umožňující vstup do areálu, případně do dalších placených prostor. Tato vstupenka může být reprezentována standardní papírovou vstupenkou Cardpay nebo modernějším bezkontaktním médiem (napr. pro permanentku).

Pokladna zajišťuje následující operace:

- výdej různých typů identifikačních médií
- prodej vstupenek s čárovým kódem
- zabezpečení obslužné funkce dobíjení částek na účty karet
- výpisy poskytnutých služeb pro zpětnou kontrolu

SOFTWARE:

System je koncipován pro široké použití od systémů s jednou pokladnou až po řešení s více prodejními místy včetně možnosti prodeje přes Internet. Přehlednou formou poskytuje uživateli veškerá data zpracovaná během provozu s možností následného tisku či exportu údajů v datové formě včetně napojení na jiné informační systémy.

Variabilita nastavení umožňuje uživateli nadefinovat si různé typy vstupného: jednoúčelové, permanentky, slevy, skupinové, rodinné vstupné, bodové či časové.

TISKOVÉ SESTAVY:

Představují jeden z základních modulů lokálního pokladního, vstupenkového platebního systému CARDPAY a jejich primární funkcí je zpřístupnění dat v tiskové podobě v

odpovídající statistické struktury pro provozovatele. Program umožňuje uživateli vytvářet tiskové sestavy (statistiky), které popisují prodej nebo zachycují jeho historii. Sestavy jsou určeny pro tisk, respektive je může uživatel archivovat.

VSTUPENKY:

Vstupenky mají různá provedení, většinou jsou řešeny s perforací, s možností celobarevného potisku na líc i rub. Vstupenky jsou navrhovány individuálně v takové podobě, aby u zákazníka mohl bezproblémově proběhnout dotisk a zpracování. Balení je volitelně v kotoučích, či skládané. Materiál je nesamolepicí, většinou silnější papír, eventuálně s termocitlivou vrstvou (54x85mm - 190g/m²) pro dotisk vstupenek nebo je možné nabídnout i PET folie (250g/m²) pro aplikace, kde by hrozilo rozmočení vstupenky.

Varianty:

ČÁROVÝ KÓD:

Pro svoji jednoduchou výrobu je stále cenově nejvýhodnější, obsažená funkcionalita pokrývá většinu všech požadavků pokladních systému. Možnost využití kvalitních barevných potisků vstupenek, s definovanou oblastí pro dotisk čárového kódu, v komplexním grafickém návrhu provozovatele, je jejich dominantní předností. V případě požadavku na vyšší bezpečnost zabraňující možnosti kopírování vstupenek lze využít řešení s neviditelným infračerveným čárovým kódem.

BEZKONTAKTNÍ ČIPOVÉ KARTY:

Tento moderní, elegantní identifikační prvek, využívaný v pokladních systémech, disponuje širokou škálou využití. Použitá technologie je jedinečná zejména při nabídce věrnostních programů a bezhotovostních plateb. Nabízí dokonalejší barevný potisk v grafickém provedení. V případě permanentek může být součástí potisku fotografie zákazníka, pro jeho snadnou identifikaci při průchodu do areálu.

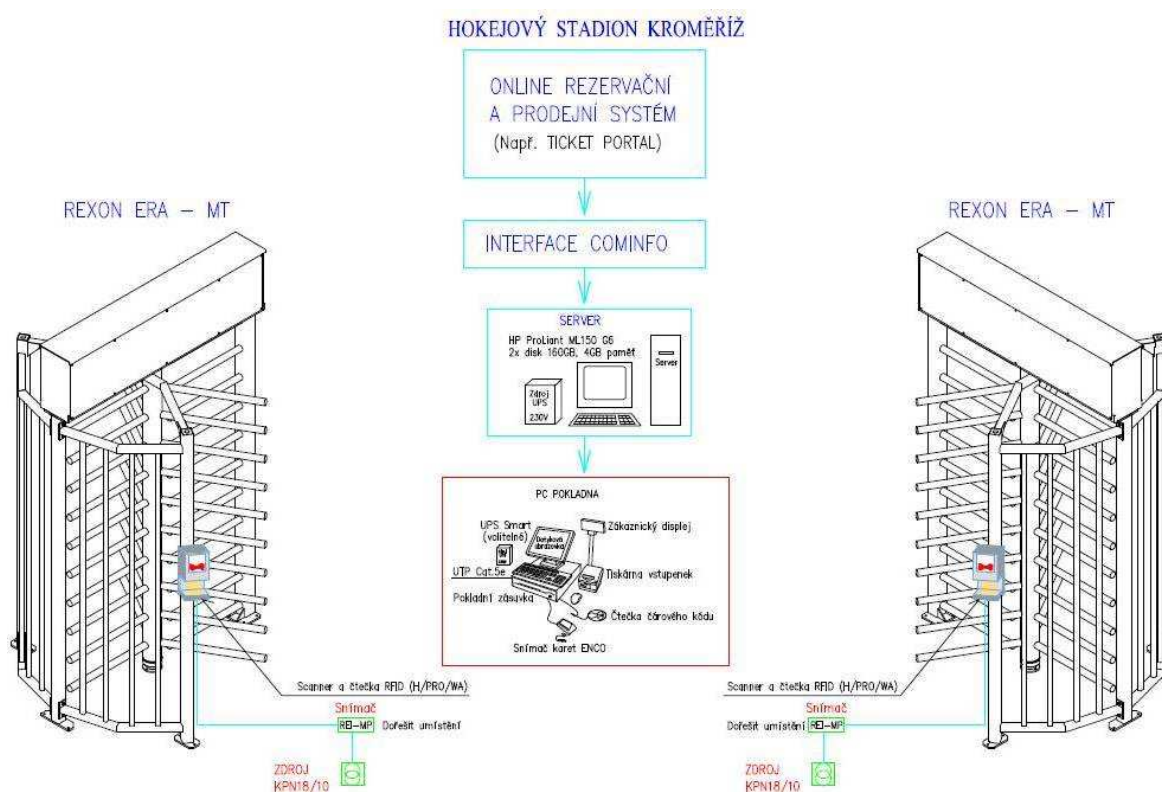
Pro zaměstnavatele je toto ideální médium, které je možno využívat pro přístupový systém a zároveň slouží jako zaměstnanecká průkazka.

SNÍMAČ VSTUPENEK:

Je určen pro čtení vstupenek s viditelným i neviditelným čárovým kódem, tak i bezkontaktních čipů. Opticky signalizuje povolení nebo zamítnutí průchodu s možností doplňující textové zprávy na LCD displeji a řídí činnost turniketů, elektromagnetických otvíračů, elektromechanických zámků.

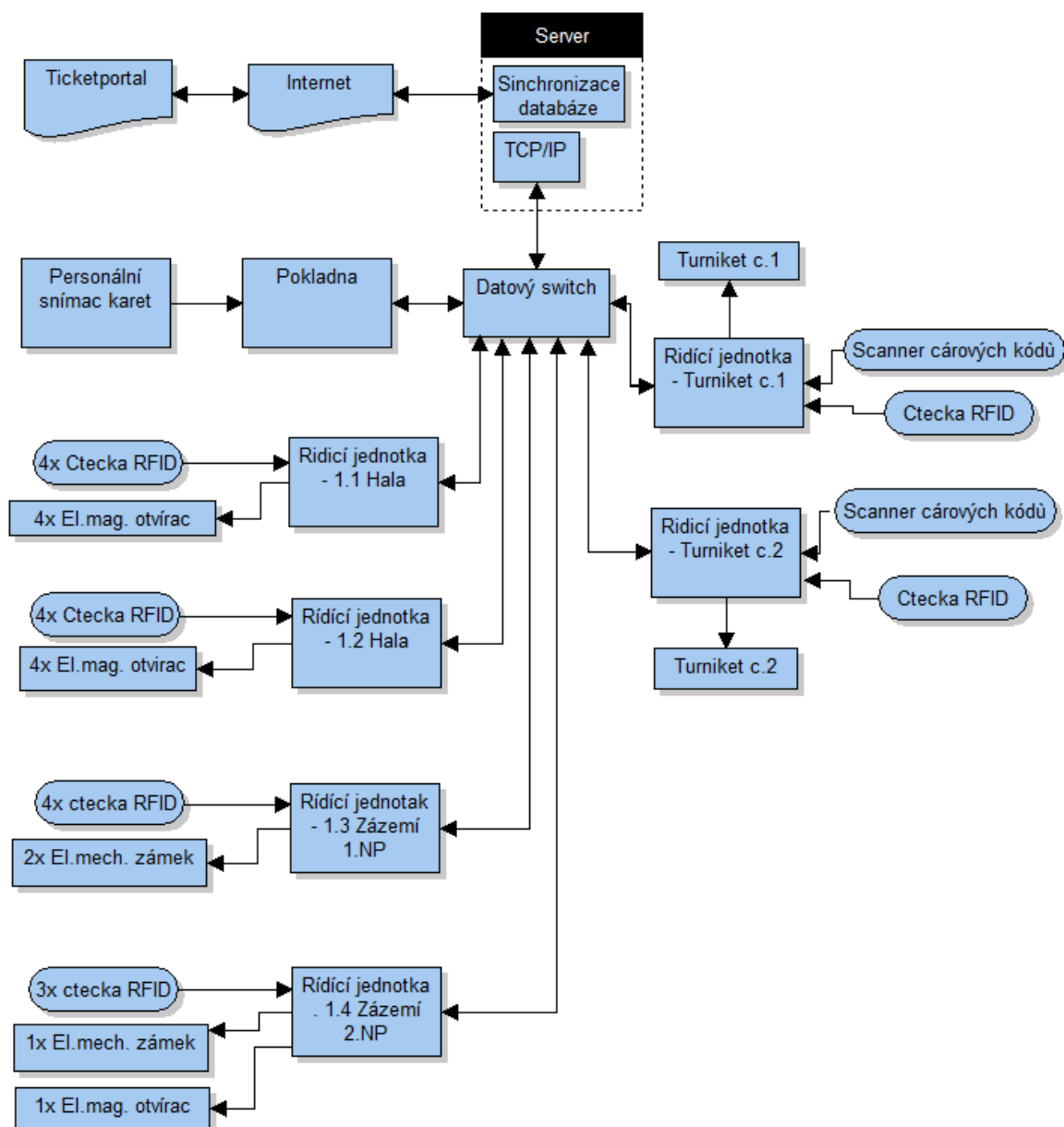
10.3.2 Koncepční řešení

Celý systém je koncipován jako integrace přístupového, pokladního a vstupenkového systému. U vchodu do stadiónů jsou navrženy dvě turniketové brány, které slouží pro průchod návštěvníků. Obsahují jak čtečku čárových kódů (vstupenky), tak čtečku bezkontaktních karet (zaměstnanci, permanentky). Technologie čárových kódů pro vstupenky byla zvolena v rámci ekonomické výhodnosti řešení. Pokladna u vstupu řeší zprávu vstupenkového systému, s možností místního prodeje či správu karet. Celý systém je přes strukturovanou kabeláž zaintegrovan jako celek, včetně kontroly přístupu do chráněných oblastí (bezkontaktní technologie RFID) a propojen s portálem Ticket portal (internetový prodej). Hlavní datový server je umístěn v dohledovém centru.



Obr. 14 Nákras řešení vstupenkového a pokladního systému s turnikety

10.3.3 Blokové schéma návrhu systému EKV



Obr. 15 Blokové schéma navrhovaného systému EKV

10.3.4 Online prodejní a rezervační systém Ticketportal

Hlavním cílem informačního a rezervačního systému Ticketportal je ulehčit všem zájemcům získávání informací o různých kulturních, ale i sportovních akcích a dále pak především realizace přímého prodeje vstupenek na tyto akce a nebo pouze realizace rezervace vybraných vstupenek.

Systém umožňuje:

- výběr konkrétního místa v hledišti daného představení či utkání
- pohodlný a pružný management všech pravidelných i jednorázových akcí, založený na moderních technologiích
- rychlé a jednoduché objednání či přímý prodej vstupenek
- přehledné vyhledávání informací o konaných akcích
- spolupráci v oblasti marketingu

Způsoby distribuce vstupenek:

Pro distribuci vstupenek využívá několik distribučních kanálů, které pokrývají široké spektrum zájemců o vstupenky na kulturní a sportovní akce. Vedle vlastního call centra, zajišťujeme distribuci prostřednictvím internetového portálu www.ticketportal.cz a sítí více jak 150 prodejních míst po celé České republice mimo jiné v téměř všech významných městech, kde se konají extraligová hokejová utkání. Veškeré rezervace jsou zdarma a cena je shodná s cenou vstupenek u pořadatele.

Zákazník má vedle klasické koupě za hotové další širokou škálu možností, jak získat požadované vstupenky:

- online rezervace po Internetu s následným vyzvednutím a zaplacením hotově v libovolném prodejním místě Ticketportal
- platby prostřednictvím VISA, MC s možností:
 - a) vyzvednutí vstupenek na jakémkoli prodejním místě sítě Ticketportal
 - b) doručení vstupenek poštou na dobírku

- c) doručení vstupenek kurýrem na území Prahy
- d) využití čipové karty jako vstupenky (goTICKET). V tomto případě může zákazník z čipovou kartu navštívit přímo akci bez nutnosti vyzvedávání klasických vstupenek.

10.3.5 Návrh rozmístění prvků systému EKV

Viz. příloha č. 3

10.4 Elektrická Požární Signalizace (EPS)

10.4.1 Představení navrhované technologie

ZETTLER® Expert je moderní adresovatelný analogový systém EPS pracující na základě tyco MX TECHNOLOGY využívající nejnovější detekční principy:

- MX FASTLOGIC – detekční algoritmus pracující na bázi fuzzy logic, který vyhodnocuje změnu koncentrace kouře se současnou změnou teploty.
- MX HPO – teplotně kompenzovaný opticko-kouřový princip.
- MX CCO – teplotně kompenzovaná detekce oxidu uhelnatého.
- TRIOTEC - multisenzor (optický-CO-tepelný) sdružující výhody principů MX HPO a MX CCO a výrazně zlepšuje detekční možnosti bodových hlásičů.

Ústředna ZETTLER® Expert ZX4

Kompaktní ústředna pro montáž na stěnu, 2 kruhová vedení po 250 adresovatelných prvcích, možnost rozšíření (XLM800) až na 8 kruhových vedení, tj. max. 1000 adresovatelných prvků. Obsahuje desku procesoru CPU800, základní desku FIM802, zdroj PSB800 (24VDC/4A), zobrazovací panel ODM800 CZ (s grafickým 16 řádkovým displejem) a ovládací panel OCM800 CZ. Prostor pro 2 akumulátory 12V max. 38Ah.



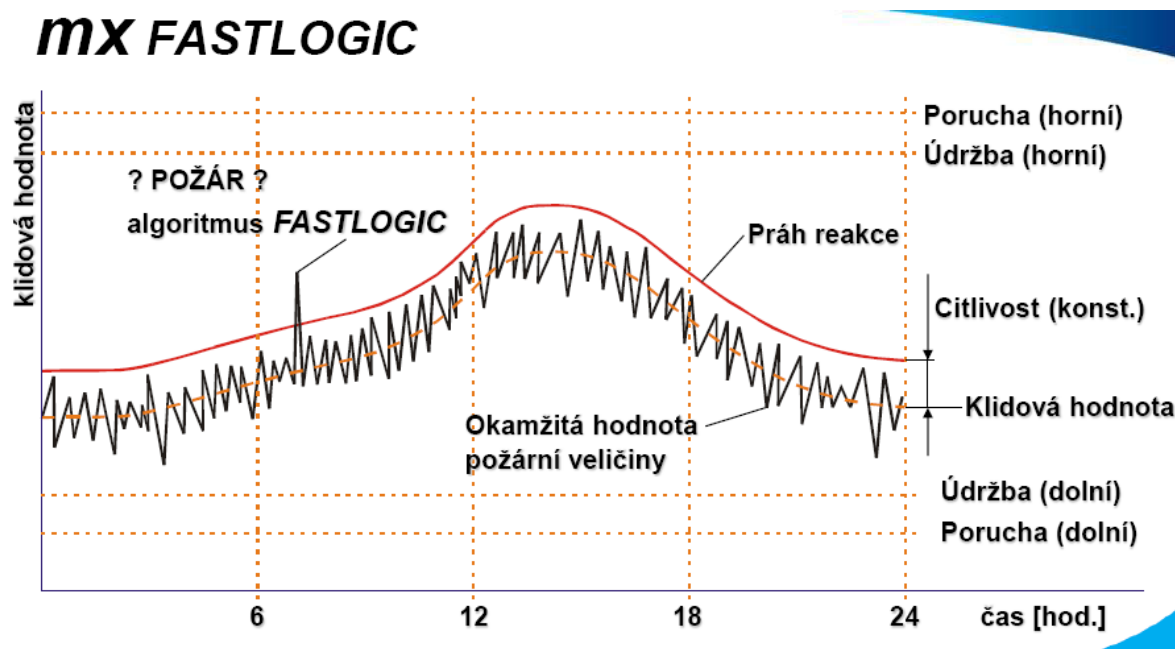
Obr. 16 Ústředna EPS Tyco Zettlet Expert ZX4

Vstupy a výstupy základní desky FIM802:

- výstup POŽÁR, PORUCHA
- 2 výstupy pro připojení sirén
- vstup pro nouzový poplach
- 2 obecné vstupy
- sériová sběrnice RBUS (RS485) pro další rozšiřování systému
- 3 sériové linky

Linkový protokol MX DIGITAL použitý v systému ZETTLER® Expert je velmi odolný proti rušení a k jeho základním vlastnostem patří:

- zcela volná topologie požární linky – kruhová a nekruhová vedení, libovolné větvení a odbočování
- možnost použití i stávajících kabelů (nestíněných, nekroucených párů apod.) při rekonstrukcích.



Obr. 17 Technologie MX Fastlogic

10.4.2 Koncepční řešení

System EPS je rozdělen z důvodu oddělení (bezpečnost) a vzdálenosti prvků (optimalizace rozvodů), rozdělen na 4 samostatné kruhové sběrnice linky. Linka č.1 – 1.NP zázemí, linka č.2 – 2.NP zázemí, linka č.3 – hala tribuny domácích, linka č.4 – hala tribuny hostů. V rámci ledové plochy (haly) jsem navrhl využití nasávacího systému instalovaného 2m pod stopem na nosné konstrukci. Z důvodu spolehlivosti a odolnosti vůči falešným polachům při zábavné produkci (např. koncerty) – odolnost vůči bílému kouři a vysoké relativní vlhkosti, jsem tomuto systému dal přednost před řešením Linárními paprskovými hlásiči. Zbytek zázemí je řešen multisenzorovými hlásiči, u nichž je možné v případě potřeby prostor (např. kuchyň restaurace) potlačit optickokouřovou složku, a vytvořit tímto hlásič tepelný. Poplachový signál bude vyveden přes bezdrátové přenosové zařízení na pult HZS (popřípadě v integraci se systémem EZS na PCO bezpečnostní agentury). Navržena instalace obslužného pole požární ochrany (OPPO) a klíčového trezoru (KT) pro případ zásahu v době opuštění objektu. V případě vyhlášení požárního poplachu dojde k aktivaci sirén, aktivaci nouzového zvukového systému, otevření KTPO, otevření zámků Abloy systému EKV a přenosu poplachové zprávy přes ZDP.

10.4.2.1 Použité detektory

Multisenzor interaktivní 801PH

Kombinace optický a tepelný hlásič. Kombinace detekčních módů v MX multisenzorech umožňuje změnu detekčního módu z ústředny bez fyzické výměny hlásičů. MX senzory tak mohou pracovat buď v jednom módu nebo ve dvou, což umožňuje optimalizovat detekci s ohledem na rychlost a spolehlivost. Multisenzory lze rozdělit na samostatné senzory, je možné vytvářet dvouhlásičové závislosti.

Tlačítkový hlásič DIN820

Vnitřní – červený, rozměr 135x135x32mm.

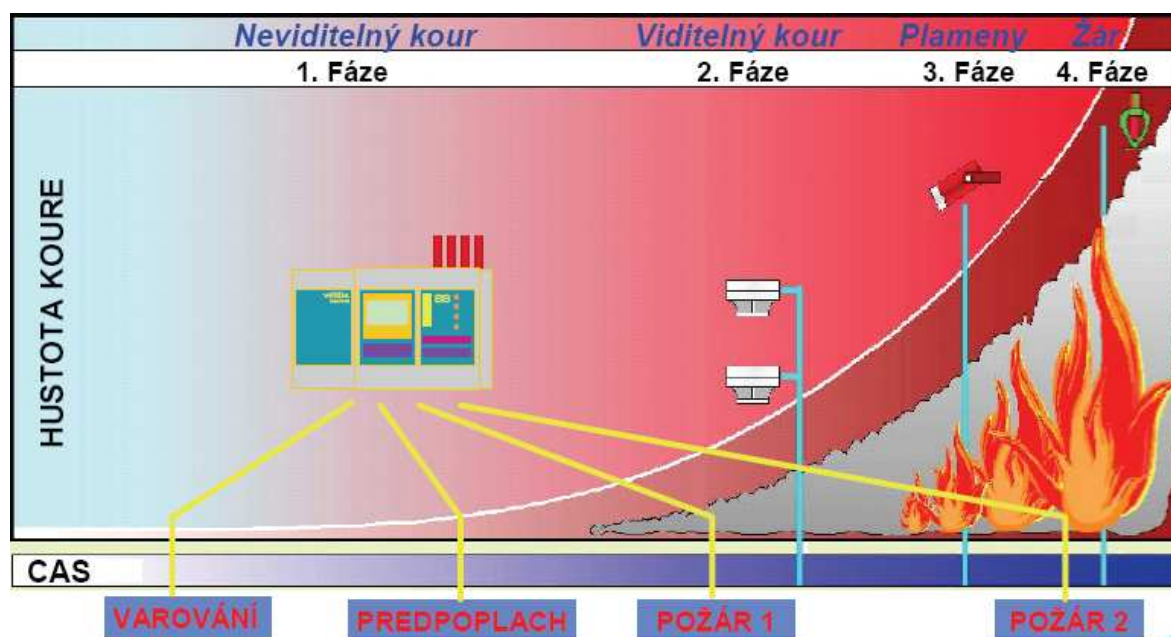
Systém VESDA

Systém VESDA® jsou aktivní systém detekce kouře. Vestavěné nasávací zařízení nasává pomocí sítě trubek vzorky vzduchu ze střežených prostor a přivádí je k laserovému detektoru v hlásiči. Síť nasávacího potrubí sestává z 1 nebo více trubek s množstvím kalibrovaných nasávacích otvorů, které jsou svou funkcí srovnatelné s bodovými kouřovými hlásiči podle EN 54-7. Tímto způsobem je docíleno rovnoměrného pokrytí velkých prostor při extrémní vysoké citlivosti a rychlosti detekce kouře.

Lze ho s výhodou použít v případech, kdy použití bodového kouřového hlásiče není možné s ohledem na prostředí (teplota, prašnost, vlhkost, proudění vzduchu, elektromagnetické záření atd.). Hlásiče pracují na principu rozptylu světelného paprsku generovaného vysokoenergetickým pulsním laserem a detekovaného vysoce výkonnými fotosensory. Vestavěný filtr zachycuje prach a propouští pouze částice kouře, což i při vysoké citlivosti laserové komory minimalizuje nebezpečí vyhlášení falešného poplachu.

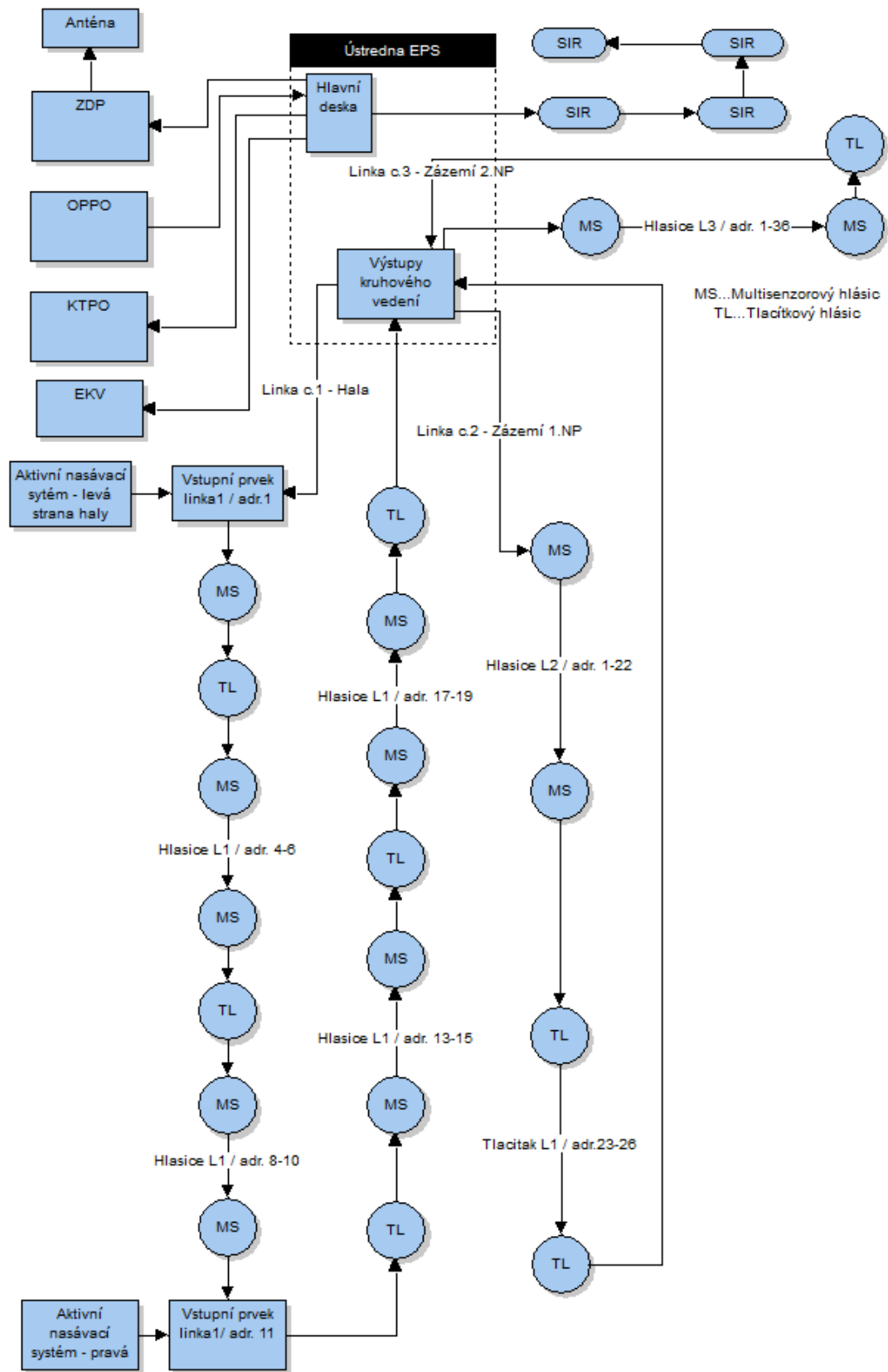


Obr. 18 Systém VESDA



Obr. 19 Rychlost detekce aktivního systému detekce kouře

10.4.3 Blokové schéma návrhu systému EPS



Obr. 20 Blokové schéma navrhovaného systému EPS

10.4.4 Návrh rozmístění prvků systému EPS

Viz. příloha č. 4.

10.5 Nouzový zvukový systém (NZS)

10.5.1 Představení navrhované technologie

Systém plošného evakuačního ozvučení Audix® je modulární systém určený pro řízení evakuace osob v ohrožených prostorech. Systém plně splňuje požadavky normy ČSN EN 60849 pro "Nouzové zvukové systémy". Srdcem systému je řídicí jednotka Alpha. Řídicí jednotka je přepínatelná plně programovatelná analogová matice audio signálů, která má 12 audio vstupů a 16 audio výstupů. Matici lze libovolně naprogramovat pro nasměrování každého audio vstupu do libovolného - jednoho či několika - audio výstupů.

Parametry:

- kapacita matice 12 x 16 analogová matice
- kmitočtový rozsah 20Hz÷20kHz v pásmu ± 1 dB
- harmonické zkreslení 0,01%
- odstup signál/šum 80dB
- kmitočtový rozsah zpráv 8kHz
- odstup signál šum zpráv 72dB
- příkon se 3 kartami zpráv 11W
- rozměry 19" rozvaděč, výška 2U
- (šířka x výška x hloubka),(480 x 89 x 325mm)

Součástí řídicí jednotky Alpha mohou být až 3 karty pro digitální záznam zpráv. Na každou kartu je možno nahrát až 10 zpráv. Karty zpráv zároveň generují pilotní signál 20kHz pro kompletní hlídání audio linky od karty zpráv až po reproduktorovou linku. Pokud je požadována možnost současného hlášení dvou různých zpráv, musí být Alpha osazena alespoň dvěma kartami zpráv.

V systému je používán jeden typ konfigurovatelného zesilovače 240W sestávající ze 4 výkonových bloků po 60W. Zesilovač je možno nakonfigurovat např. pro 4 reproduktorové zóny po 60W, pro 2 zóny o 180W a 60W, jednu zónu 240W atd. Zároveň lze spojovat paralelně celé zesilovače až do výkonu 1000W. Pokud jsou spojeny alespoň dva 60W bloky, je automaticky splněn požadavek normy ČSN EN 60849, že při poruše zesilovače nesmí dojít k výpadku celé zóny. Zesilovače mají regulaci zisku a hlasitosti, ochranu proti zkratu a teplotní pojistku zabráňující poškození zesilovače přehřátím. Součástí zesilovačů je i tzv. "sleeping" mód, který výrazně snižuje odběr proudu v klidovém stavu, kdy neprobíhá žádné hlášení.

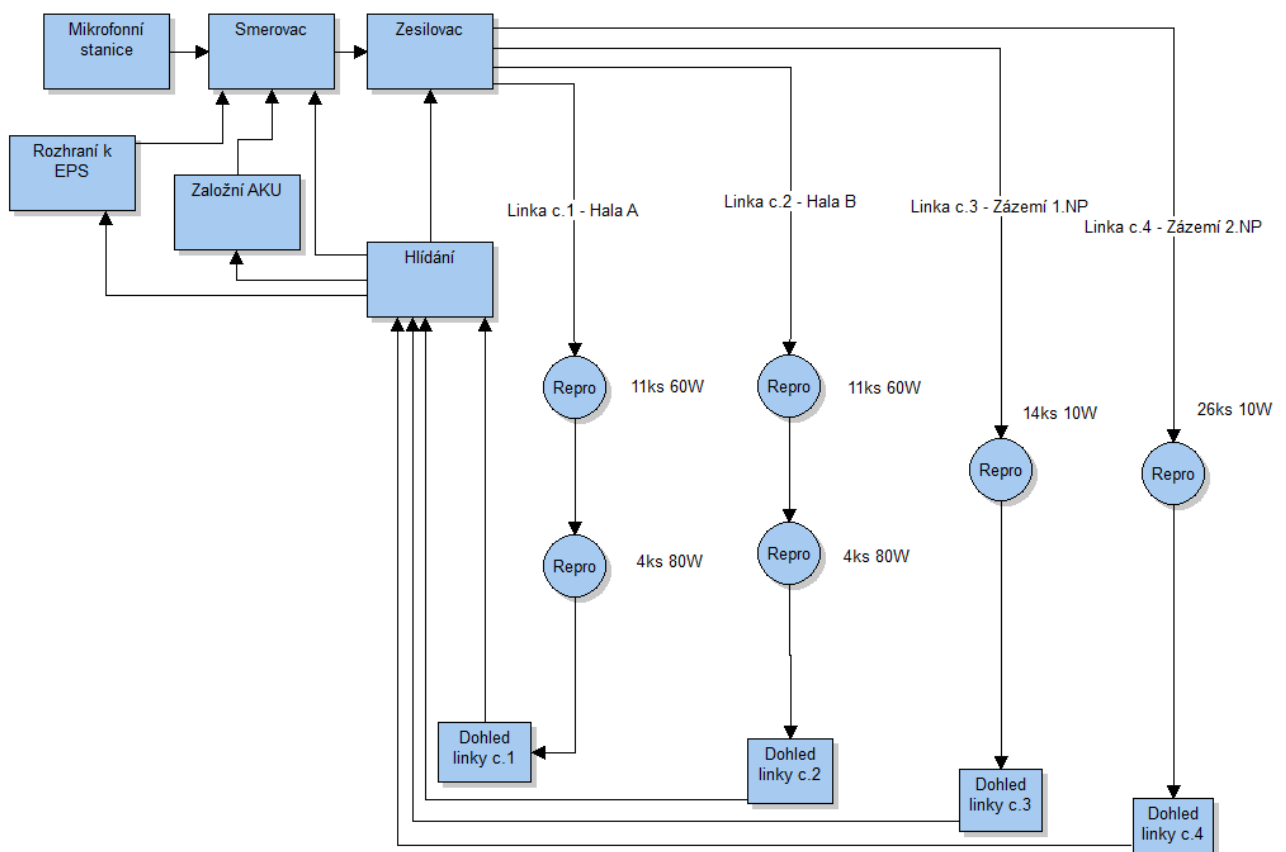
Řídicí jednotka Alpha má 8 datových linek RS485, které se používají pro připojení mikrofonních jednotek a jednotek pro výběr hudby na pozadí. Rovněž rozhraní pro připojení k systému EPS se připojuje pomocí sériové datové linky RS485. Použití sériových datových linek výrazně snižuje množství připojovaných kabelů. Např. pro připojení mikrofonní jednotky s 8 tlačítky tak stačí připojit k řídicí jednotce 3 páry vodičů - napájení, audio a data. Zároveň RS485 umožňuje připojení jednotek až ze vzdálenosti 500m.

Součástí systému Audix® je kromě standardní jednotky pro připojení k libovolnému systému EPS pomocí bezpotenciálových kontaktů také rozhraní MX / Audix pro ovládání systému Audix® systémem EPS ZETTLER® Expert. Pro kompletní ovládání 16 zón i s možností současného hlášení dvou různých zpráv (např. varování a evakuace) v různých zónách stačí 3 páry vodičů - 1 pár pro RBUS (RS485) a 2 páry pro kruhové adresovatelné vedení systému ZETTLER® Expert.

10.5.2 Koncepční řešení

Jsou použity 4 linky (2 x zázemí, 2 x stadion). V prostoru zázemí jsou navrženy skříňkové reproduktory v kombinaci se stropními reproduktory. V systému je modul pro komunikaci s EPS. V hale jsou uvažovány reproduktory o výkonu 80W nad plochu kluziště, vždy 4ks a 4ks na jednu stranu do tzv. "hroznu". Další reproduktory o výkonu 60W jsou uvažovány po obvodu hlediště. V případě potřeby lze systém doplnit o technologii bezdrátových mikrofonů a využívat ozvučení i pro komentátorské aktivity při pořádání akcí, samozřejmě s nejvyšší prioritou evakuačního hlášení.

10.5.3 Blokové schéma návrhu systému NZS



Obr. 21 Blokové schéma navrhovaného systému NZS

10.5.4 Návrh rozmístění prvků systému NZS

Viz. příloha č. 5.

10.6 Ostatní technické systémy detekce

10.6.1 Detekce úniku čpavku

Chlazení ledových plochy zimního stadiónů je zajišťováno pomocí strojního kompresorového chlazení. Použitou pracovní látkou (chladivem) je čpavek NH₃, který se řadí k ekologicky nejšetrnějším chladivům. Pro lidský organismus je však jedovatý, při kontaktu s lidskou tkání hrozí riziko omrznutí a při koncentracích ve vzduchu větších než 15% je dokonce výbušný. Chladivo (čpavek) je použito pouze v primárním okruhu vlastního kompresorového chlazení, jež je umístěno ve strojovně. Chlazení vlastní ledové plochy je pak zajištěno průtokem nemrznoucí kapaliny (roztokem ethylen-glykolu) v sekundárním okruhu. Strojovna chlazení musí být vybavena systémem havarijní ventilace a v mém návrhu doplněna o detektory úniku čpavku.

10.6.1.1 Detektor

DEGA04-2-DC-A

Slouží k jednostupňové nebo dvoustupňové signalizaci velikosti koncentrace detekovaného plynu v prostředí. Detektor používá polovodičový senzor, který transformuje změnu koncentrace příslušného plynu na změnu měrného elektrického odporu. Překročení nastavených mezí je signalizováno opticky, akusticky a přepnutím bezpotenciálových kontaktů relé. Přístroj je možné napájet síťovým napětím 230 V AC, popř. 12, nebo 24 V DC.



Obr. 22 Detektor DEGA04-2-DC-A

10.6.2 Detekce kovových předmětů

Pro detekci pronášených kovových předmětů je nejčastěji užíván rámový detektor, který je primárně určen pro detekci zbraní u osob procházejících rámem. Cílem je zabezpečit, aby do určeného prostoru nevnikly ozbrojené osoby. Při průchodu rámu návštěvníky je nutná přítomnost pracovníka fyzické ostrahy pro možný zásah, či dohledání předmětu přenosnými ručními detektory kovu.

10.6.2.1 Detektor

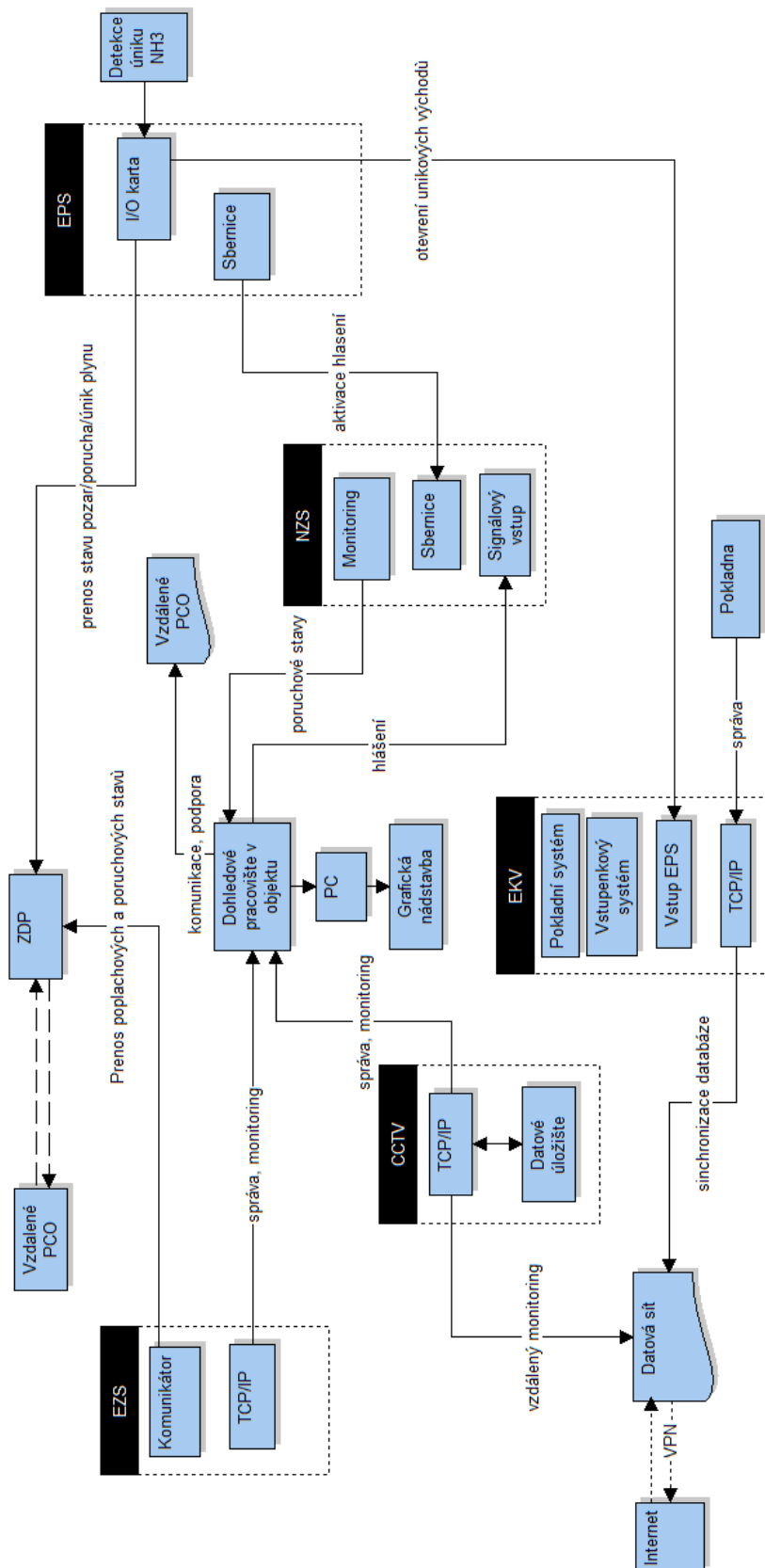
GATE211LCD

Multizónový průchozí detekční rám s šesti vzájemně překrývajícími detekčními oblastmi a LCD zobrazovacím displejem. Detekční rám má velmi vysokou citlivost, která je nastavitelná. Výhodou je možnost automatické kalibrace na detekovaný předmět. Brána má světelnou a akustickou signalizaci, potlačuje interferenci a má ochranu proti neoprávněné manipulaci. Doplnkové funkce jsou statistiky průchodů a vyhodnocených poplachů.



Obr. 23 Detekční rám GATE211LCD

11 VÝSLEDNÁ INTEGRACE JEDNOTLIVÝCH SYSTÉMŮ



Obr. 24 Blokové schéma integrace systémů

12 ODHAD DALŠÍHO VÝVOJE

Vývoj v rámci zabezpečení stadiónů předpokládám v celkové integraci všech systémů technického zabezpečení s jednotnou správou. A také s návazností na internetová média a internetový prodej, což také v této práci navrhuji.

K dalšímu pokroku dle mého názoru dojde v oblasti prevence nežádoucích jevů (teroristické útoky, agrese fanoušků) prostřednictvím inteligentní SW aplikace provázanou se systémem CCTV.

Jedná se o bezkontaktní zařízení umožňující senzory zjistit zlý úmysl osoby vůči svému okolí. Technologie registruje neverbální projevy těla okem nepostižitelných, jakými jsou tělesná teplota, srdeční tep či rytmus dýchání a další. Pokud zjistí, že jsou mimo normál, bezpečnostní služba může povolat dotyčného k pohovoru.

Dalším krokem je skenování kontrakce obličejových svalů, které umí zařízení rozdělit do sedmi základních emocí a jejich projevů a téměř v reálném čase o výsledku informovat.

Technologie dokáže také rozlišit mezi teroristou a spěchajícím člověkem, i tím, který se přirozeně víc potí.

Americký úřad pro národní bezpečnost (Homeland Security), založený v roce 2001 po útocích na WTC, vyvíjí tuto technologii v programu Project Hostile Intent (PHI). Mezi použité technologie mají patřit lasery, kamery, snímače očí, mikrofony a senzory tlukotu srdce a dýchání.

ZÁVĚR

Zabezpečení stadiónů nelze brát na lehkou váhu. Stále se zvyšující kriminalita a zuřivost fanoušků klade na prvky technického zabezpečení stále vyšší nároky.

Náročné řešení systému CCTV vyžaduje důkladné pokrytí prostoru pro jasnou identifikaci pachatele, kterou řeším v návrhu kamerami z vysokým rozlišením a kvalitním záznamovým zařízením.

V rámci integrace EKV se zaměřuji na pokladní systém a systém prodeje vstupenek za účelem vysoké efektivity jejich prodeje a následné propojení s internetovým portálem pak zajišťuje bezobslužný prodej a úplnou evidenci vstupenek prodaných a již použitých pro vstup na sportovní událost, takže možnost jejich vícenásobného použití je prakticky nulová.

Vzhledem k možnému výskytu škodlivých plynů v takto náročném prostředí, řeším jejich detekci aktivním nasávacím systémem umístěným nad ledovou plochou, který je součástí EPS a zajišťuje jejich zjistitelnost již při velmi nízkých koncentracích.

Systémem EZS řeším kompletní zabezpečení objektu v době nepřítomnosti obsluhy a monitorování únikových východů při konání akcí.

Do celkové koncepce integrace začleňuji místní dohledové pracoviště, které svou hlavní funkci plní v době sportovních utkání.

V závěru práce se pokouším o prognózu budoucího trendu týkající se zajištění sportovních akcí.

CLOSE

Security stadiums can not be taken lightly. Ever-increasing crime and fury of fans paid to technical security features ever more demanding.

Demanding CCTV solution requires thorough coverage area to clearly identify the offenders we deal with in the draft from high-resolution cameras and high-quality recording equipment.

In the integration of EKV is focused on the POS system and ticketing system for high efficiency in their sales and subsequent connections with the Internet portal provides unattended sales and complete record of tickets sold and no longer used for input to a sporting event, so the possibility of multiple use is virtually zero.

Due to the possible presence of harmful gases in such a challenging environment, solves the detection of an active intake system located above the ice surface, which is part of the EPS and ensures their detectability at very low concentrations.

Alarm system solve the complete security building at the time and no personnel monitoring at emergency exits of events.

The total integration concept incorporates local surveillance department, which performs its main function during sports events.

In conclusion an attempt to forecast future trends with regard to ensuring the sporting events.

FOTOGALERIE OBJEKTU



Foto 1 Prosklená část nad tribunami



Foto 2 Konstrukce stropu haly



Foto 3 Hlavní vstup pro diváky



Foto 4 Pokladna u hlavního vstupu



Foto 5 Vchod pod tribuny



Foto 6 Zázemí 1.NP



Foto 7 Zázemí 2.NP



Foto 8 Únikový východ z haly

SEZNAM POUŽITÉ LITERATURY

- [1] Kindl J., Projektování bezpečnostních systému I. díl, Zlín: vyd. Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-165-7.
- [2] Laucký V., Technologie komerční bezpečnosti I., Zlín: vyd. Univerzita Tomáše Bati ve Zlíně, 2003. ISBN 80-7318-119-3.
- [3] Laucký V., Technologie komerční bezpečnosti II., Zlín: vyd. Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-231-9.
- [4] IP kamerové systémy, Magazín SECURITY, roc.XVI, c.5/2009, ISSN 1210-8723
- [5] Článek portálu IDNES Dostupné z WWW:
< http://zpravy.idnes.cz/krimi.asp?r=krimi&c=A080401_160840_krimi_pei>
- [6] Hložek Petr, Bakalářská práce - Inteligentní dům řešený pomocí spolupráce bezp. a inteligentních řídicích technologií, Univerzita Tomáše Bati ve Zlíně, 2003
- [7] Katalogové listy a informační materiál firmy ADI Global Distribution
- [8] Katalogové listy a informační materiál firmy Tyco Fire & Integrated Solutions s.r.o.
- [9] Katalogové listy a informační materiál firmy Cominfo, a.s.
- [10] Katalogové listy a informační materiál firmy Trade FIDES, a.s.
- [11] Katalogové listy a informační materiál firmy NAM system a.s.
- [12] Katalogové listy a informační materiál firmy Vectra, spol. s r.o.
- [13] Katalogové listy a informační materiál firmy Alfa Secure s.r.o.
- [14] Katalogové listy a informační materiál firmy Eurosat CS, spol. s r.o.
- [15] WIKIPEDIE - Otevřená encyklopedie, dostupná z WWW:
< http://cs.wikipedia.org/wiki/Hlavn%C3%AD_strana>.
- [16] Fotomapa objektu, dostupná z WWW: < <http://www.mapy.cz>>.
- [17] Publikace Úřadu na ochranu osobních údajů, dostupná z WWW:
< <http://www.uoou.cz/uoou.aspx> >.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Access Control System (Systém kontroly vstupu)
AL	Aluminium (Hliník)
CCTV	Circuit Closed Television (Uzavřený televizní okruh)
CMOS	Complementary Metal–Oxide–Semiconductor (Technologie obrazových senzorů)
ČSN	Česká Státní Norma
EKV	Elektronická Kontrola Vstupu
EN	Evropská Norma
EPS	Elektrická požární signalizace
EZS	Elektrická zabezpečovací signalizace
GIS	Geographic Information System (Geografický informační systém)
GPRS	General Packet Radio Service (Mobilní datová služba)
GSM	Global System for Mobile communications (Mobilní síť)
HW	Hardware
HZS	Hasičský Záchranný Sbor
ChÚC	Chráněná Úniková Cesta
ICR	Infrared Cutfilter Removat (Odnímatelný IR filtr)
IEEE	Institute of Electrical and Electronics Engineers (Institut pro elektrotechnické a elektronické inženýrství)
IP	Internet Protocol (Komunikační protokol)
IR	Infra Red (Infračervené)
ISDN	Integrated Services Digital Network (Digitální síť integrovaných služeb)
KTPO	Klíčový Trezor Požární Ochrany
LAN	Local Area Network (Místní síť)

LCD	Liquid Crystal Display (Displej z tekutých krystalů)
LED	Light-Emitting Diode (Světlo emitující dioda)
MC	MasterCard (Asociace platebních karet)
MJPEG	Metoda komprese
MS	Multisenzorový hlásič
MW	Micro Wave (Elektromagnetické vlny)
NH ₃	Amoniak (triviální název <i>čpavek</i>), bezbarvý velmi štiplavý plyn
NÚC	Nechráněná Úniková Cesta
NVR	Network Video Recorder (Sít'ový videorekordér)
OPPO	Obslužné Pole Požární Ochrany
PCO	Pult Centralizované Ochrany
PET	Poly Ethylen Tereftalat (Termoplast ze skupiny polyesterů)
PGM	ProGraMmable input / output (Programovatelný vstup / výstup)
PHI	Project Hostile Intent (název projektu)
PIR	Passive Infra Red detektor (Pasivní infračervený detektor)
PKB	Průmysl Komerční Bezpečnosti
POE	Power Over Ethernet (Napájení po datovém síťovém kabelu)
QoS	Quality of Service (Kvalita služeb)
RF	Radio frequency (Bezdrátový přenos)
RFID	Radio Frequency Identification (Identifikace na rádiové frekvenci)
ScTP	Stream Control Transmission Protocol (Transportní vrstva)
SIR	Siréna
SKS	Strukturovaná Kabelážní Systém
SW	Software
TCP	Transmission Control Protocol (Komunikační protokol)

TL	Tlačítkový hlásič
UTP	Unshielded Twisted Pair (Nestíněná kroucená dvojlinka)
VF	Vysokofrekvenční
VISA	Visa International Service Association (Asociace platebních karet)
VPN	Virtual Privacy Network (Virtuální soukromá síť)
WAN	Wide Area Network (Rozlehlá počítačová síť)
WiFi	Wireless network (Bezdrátová síť)
WTC	World Trade Center (Světové obchodní centrum)
ZDP	Zařízení Dálkového Přenosu

SEZNAM OBRÁZKŮ

Obr. 1 Blokové schéma funkce registru výtržníků.....	13
Obr. 2 Bezpečnostní značení únikových cest.....	48
Obr. 3 Fotomapa objektu zimního stadionu [16].....	54
Obr. 4 Blokové schéma využití tech. prostředků dle režimu objektu.....	55
Obr. 5 Ústředna EZS Galaxy Dimension.....	57
Obr. 6 Blokové schéma navrhovaného systému EZS.....	59
Obr. 7 Zobrazení detailu na základě počtu pixelů.....	60
Obr. 8 Kamera Arecont Vision AV8185.....	61
Obr. 9 Kamera Arecont Vision AV8365.....	62
Obr. 10 Kamera Arecont Vision AV1355DN.....	62
Obr. 11 Příklad širokoúhlého záběru ve vysokém rozlišení s následným digitálním zvětšením.....	63
Obr. 12 Blokové schéma navrhovaného systému CCTV.....	64
Obr. 13 Náskres pro výpočet rozlišení kamer na tribunách.....	65
Obr. 14 Náskres řešení vstupenkového a pokladního systému s turnikety.....	69
Obr. 15 Blokové schéma navrhovaného systému EKV.....	70
Obr. 16 Ústředna EPS Tyco Zettlet Expert ZX4.....	73
Obr. 17 Technologie MX Fastlogic.....	74
Obr. 18 Systém VESDA.....	76
Obr. 19 Rychlost detekce aktivního systému detekce kouře.....	76
Obr. 20 Blokové schéma navrhovaného systému EPS.....	77
Obr. 21 Blokové schéma navrhovaného systému NZS.....	80
Obr. 22 Detektor DEGA04-2-DC-A.....	82
Obr. 23 Detekční rám GATE211LCD.....	83
Obr. 24 Blokové schéma integrace systémů.....	84

SEZNAM FOTOGRAFIÍ

Foto 1 Prosklená část nad tribunami	88
Foto 2 Konstrukce stropu haly	88
Foto 3 Hlavní vstup pro diváky	89
Foto 4 Pokladna u hlavního vstupu.....	89
Foto 5 Vchod pod tribuny	90
Foto 6 Zázemí 1.NP	90
Foto 7 Zázemí 2.NP	91
Foto 8 Únikový východ z haly	91

SEZNAM PŘÍLOH

Příloha č.1	Návrh rozmístění prvků systému EZS
Příloha č.2	Návrh rozmístění prvků systému CCTV
Příloha č.3	Návrh rozmístění prvků systému EKV
Příloha č.4	Návrh rozmístění prvků systému EPS
Příloha č.5	Návrh rozmístění prvků systému NZS
Příloha č.6	Cenová kalkulace navrhovaného řešení