Význam uzavřených, dozorových kontrolních a střežících systémů v průmyslu komerční bezpečnosti (CCTV)

Michaela Dočkalová

Bakalářská práce
2006

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2005/2006

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Michaela DOČKALOVÁ**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Význam uzavřených, dozorových kontrolních a střežících systémů v průmyslu komerční bezpečnosti (CCTV)**

Zásady pro vypracování:

1. Seznámit se s problematikou uzavřených, docházkových a kontrolních systémů v průmyslu komerční bezpečnosti
2. Přehledně uveďte fyzikální principy a základy videotechniky.
3. E-learningovou metodou zpracujte přehlednou formou základní členění zařízení a prvků systému CCTV, aplikace při využití kamerových systémů.
4. Význam CCTV při zabezpečení budov, objektů a veřejných prostranství.
5. Proveďte analýzu problematiky kamerových systémů a nové trendy ve vývoji systémů CCTV.

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] Tauš, G.: Video. Praha, SNTL 1989.
[2] Klugl, J.: Montáž EZS. Praha 1993.
[3] Skřivan, Z.: Nebojte se zlodějů. Praha, Grada 1994.
[4] Graham, J., Bennett, T.: Strategie 'prevence kriminality v Evropě a Severní Americe.Praha, Institut pro kriminologii a sociální prevenci 1996.
[5] Ivanka, J. : Technické prostředky bezpečnosti a elektromagnetická kompatibilita. In. Řešení krizových situací v specifickém prostředí. EDIS – Žilinská univerzita, Žilina, 2004, str. 77–82, ISBN 80–8070–272–1
[6] Ivanka, J.: Měření rušivých signálů pomocí antén., Sborník z 10. vědecké konference s mezinárodní , Řešení krizových situací ve specifickém prostředí, FŠI Žilinská univerzita, Žilina 2005, str. 211 – 214, ISBN 80–8070–425–2[8]
[7] Kocábek, P., Koníček, T.: Situační prevence a kamerové monitorovací systémy. Praha, Odbor prevence kriminality MV ČR 1997.
[8] Křeček, S.: Ochrana majetku systémy průmyslové televize. Praha, Grada 1997.

Vedoucí bakalářské práce: **Ing. Ján Ivanka**
Ústav elektrotechniky a měření

Datum zadání bakalářské práce: **14. února 2006**

Termín odevzdání bakalářské práce: **13. června 2006**

dne

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ Fakulta aplikované informatiky DĚKAN

L.S.

prof. Ing. Vladimír Vašek, CSc.
pověřený děkan

doc. RNDr. Vojtěch Křes
ředitel ústavu

ABSTRAKT

Kamerové systémy jsou v dnešní době spolu se zabezpečovacími systémy nejpoužívanější bezpečnostním zařízením v České republice. Přispívají k udržování veřejného pořádku na ulicích, k dopadení pachatelů při páchání trestné činnosti a k přehledu pohybu osob ve střeženém prostředí. Studenti fakulty aplikované informatiky oboru Bezpečnostní systémy, řízení a management se dozvídají velké množství informací o dané problematice, ale jen okrajově. Proto podnětem bakalářské práce je poskytnou hlubší pohled na danou problematiku s názornými příklady a statistikami z praxe. Pomůže tak studentům lépe pochopit význam kamerových systémů v běžném životě.

ABSTRACT

Nowdays the most widely used safety devices in the Czech Republic are camera and security systems. They contribute to maintain law and order in the streets, to capture offenders while commiting crime and to record movements of people in the watched areas. Students of the branch learn about this problems but not in a detailed way. Therefore the intent of this topic is to give a deeper eyeview about this issue. That way it will be easier for students to understand the importance of the camera systems in a common life.

Poděkování

Ráda bych poděkovala vedoucímu mé bakalářské práce Ing. Jánu Ivánkovi za jeho podnětné připomínky, návrhy, profesionální vedení, pomoc při tvorbě bakalářské práce a za odborné konzultace.

Dále děkuji Bc. Milanu Kladníčkovi z Městské policie Zlín za obrázkovou dokumentaci, která byla použita v mé práci jako příklad využití z praxe.

Souhlasím s tím, že s výsledky mé práce může být naloženo podle uvážení vedoucího bakalářské práce, ředitele ústavu a institutu. V případě publikace budu uvedena jako spoluautorka.

Prohlašuji, že jsem na bakalářské práci pracovala samostatně s použitou literaturou a radami Ing. Ivánky. Použitou literaturu jsem citovala.

V Sazovicích,

…….

Podpis

OBSAH

ÚVOD

Předložená bakalářská práce vznikla ve spolupráci s Městskou policií ve Zlíně a je zaměřena na téma uzavřené kamerové dozorové a kontrolní systémy, které slouží jako ochrana proti majetkové a násilné trestné činnosti. Zrychlující se technický vývoj všech komponentů CCTV zejména záznamových a přenosových prvků, velká nabídka, cenová dostupnost a velké potřeby trhu dělají v současné době ze CCTV jeden z nejvíce se rozvíjejících systémů v rámci technických zabezpečovacích systémů.

Důvodů proč je CCTV tak důležitý je skutečně mnoho. Obzvlášť významné místo má v situační prevenci kriminality ve městech po celé České republice. Tento systém rovněž zvyšuje počet případů, kdy záznam obrazu kamerového systému, rozhodujícím způsobem pomohl k dopadení a usvědčení pachatele (jako podpůrného materiálu pro trestní řízení Orgánu činného trestního řízení (dále jen OČTŘ) a vlastního soudního líčení) nebo samotná instalace odradí pachatele od páchání trestné činnosti. Na mnoha veřejných místech a prostranstvích, jako jsou náměstí, parky, nádraží, pěší a obchodní zóny zabezpečují bezpečí a bezpečnost občanů. CCTV slouží k dohledu v místních záležitostech veřejného pořádku a k předcházení pouliční trestné činnosti a přestupkům. Proto je potřebné věnovat pozornost a získávat nové informace z této oblasti.

Žít v příjemném a bezpečném prostředí si přeje většina občanů. Pro svůj pocit bezpečí podnikají občané kroky k zabezpečení majetku a zdraví, s využitím nejrůznějších technických prostředků a při respektování pravidel bezpečného chování. Ukazuje se, že to ale nestačí, že pro ochranu majetku a osob je nutné podniknout konkrétní bezpečnostní opatření. A to přímo v konkrétním domě, na sídlišti, v obci, ve městě a v regionu za aktivní účasti volených orgánů.

Městské kamerové systémy mají v systému prevence kriminality České republiky důležité a nepřehlédnutelné místo. Obsluhují ho lidé, kteří jsou schopni přijímat rozhodnutí, ví kam se zaměřit a jaké kroky podniknout na základě toho, co vidí v době záznamu nebo při jeho přehrávání.

Prevence kriminality vyžaduje provázaný preventivní systém. Jedním z důležitých předpokladů kvalitní funkce kamerového komplexu je dobrá úroveň zkušebnictví a certifikace. Právě pochopení a posléze využití výsledků zkoušek a certifikace je totiž

rozhodující pro kvalifikované a odpovědné zajištění majetku a zdraví, kam funkce CCTV jednoznačně patří.

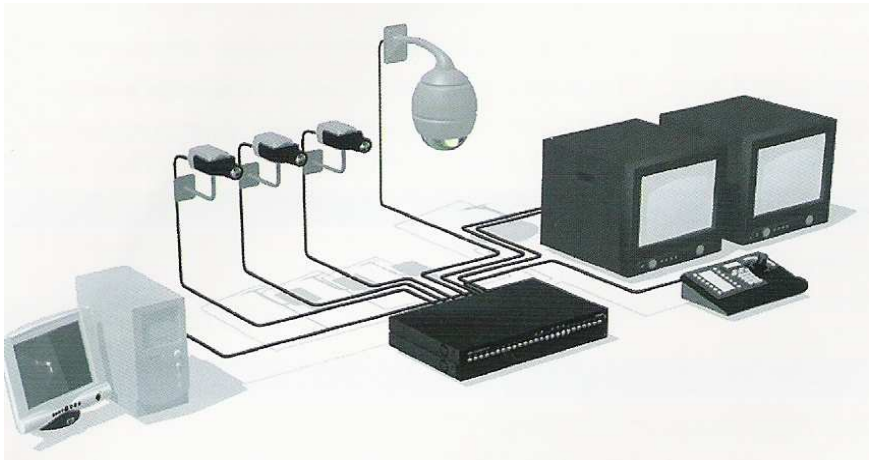
Následující bakalářská práce má lidem, kteří se v dané problematice neorientují, poskytnout lepší představu o složení a významu CCTV, a lidem, kteří jsou v oboru zainteresováni rozšířit obzory o aktuální trendy a vývoj v této oblasti.

I. TEORETICKÁ ČÁST

1 VÝZNAM CCTV

Uzavřený kamerový dozorový kontrolní a střežící systém obvodové, prostorové, plášťové a předmětové ochrany v průmyslu komerční bezpečnosti (dále jen PKB).

CCTV je zkratka z anglického názvu **C**losed **C**ircuit **T**elevision **S**ystem. Je to televizní systém, který se skládá z jedné nebo více kamer, zařízení pro přenos a zobrazení nebo záznam obrazu. Celý systém je obvykle určen pro omezený počet uživatelů. Využívá se pro zabezpečení různých objektů. Systém CCTV umožní efektivním způsobem monitorovat střežený prostor a kontrolovat tak velmi rozsáhlé prostory v reálném čase. Systém umožňuje obraz ze střeženého prostoru zaznamenat na pásku nebo na digitální datové médium. Tento záznam slouží k následnému vyhodnocení poplachových situací, ke zpětnému dohledávání dříve zaznamenaných informací, apod. Systém CCTV lze vhodně provázat se systémem EZS nebo jej provozovat jako samostatnou bezpečností aplikaci. Překážku většího rozšíření je jejich vysoká pořizovací cena. Jsou ideálním řešením v jednodušších aplikacích, kde pro pokrytí sledovaného prostoru postačuje několik kamer. Kamerové systémy slouží k monitorování veřejných a služebních prostor objektů a jejich okolí. Jsou vhodné hlavně pro členité či několika poschoďové prostory, kde je nutné mít alespoň částečnou kontrolu nad pohybem návštěvníků a to z bezpečnostních nebo jiných důvodů. Primárním zdrojem informace v systému je CCTV kamera.



Obr. 1. Typické zapojení CCTV s pevnými i otočnými kamerami, dvěma monitory a PC

1.1 Systémy průmyslové televize (CCTV) - uzavřené kamerové dozorové a kontrolní systémy.

1.1.1 Systémy kontroly vstupu

Používají se samostatně nebo s kombinací docházkového systému. Elektronická kontrola vstupu ACESS kontrol umožňuje chráněný vstup do objektu po identifikaci. Osoby mají přístup do prostorů, které jim správce systému povolí.

1.1.2 Docházkový systém + kontrola vstupu

V kombinaci docházkového systému a kontroly vstupu nám systém zaznamená vstup do objektu a zároveň čas příchodu (docházku). Kombinace přístupového systému, výdaje stravy a pomůcek nám dává přehled o umožněném přístupu, odběru stravy i pomůcek. Vše je zaevidováno a ztráty mohou být odčítány ve mzdě.

1.1.3 Kontrola vstupu + ACCESS kontrol

Kombinace kontrola vstupu a ACCESS kontrol zaznamenává vstup do objektu, odkódování zabezpečovací signalizace, odblokování všech potřebných čidel a detektorů tak, aby nevyvolaly poplach. Časový sled se sleduje a eviduje.

1.1.4 Kontrola vstupu + CCTV

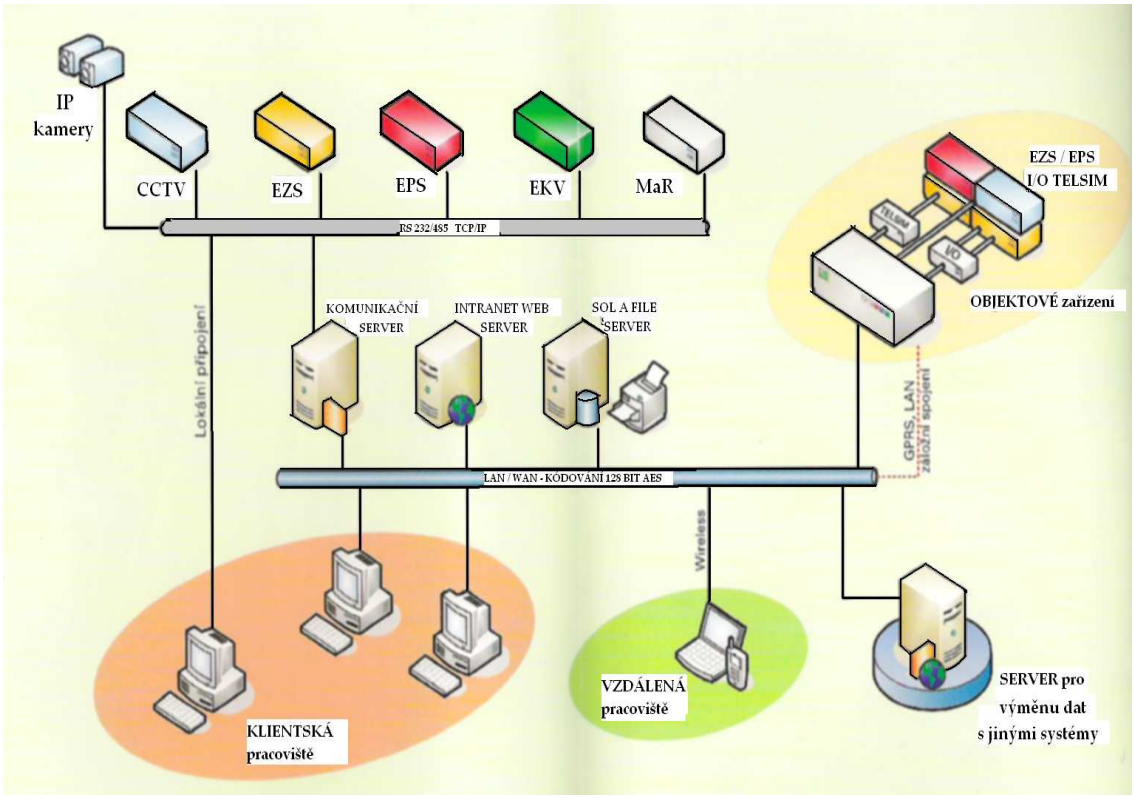
Kombinace kontroly vstupu a CCTV zaznamená pohyb osob po objektu a jejich činnost. Je tak zajištěna včasná reakce na nežádoucí situaci např. ve věznici.

1.1.5 Elektronická kontrola vstupu

Elektronická kontrola vstupu nám snižuje náklady na hesla a vyšší komfort při vstupu. Řídí pohyb osob v denním režimu, kdy je systém EZS odblokován a nestřeží objekt. Poskytuje informace o pohybu osob v objektu. Informace jsou zaznamenány a průběžně se sledují. Ze záznamu pak vyčteme osobu, místo pohybu a čas. Výhodou je omezený přístup nepovolaných osob do systému a přístup osob mimo časové úseky. Registruje se datum, čas, místo, účel a sčítají se místa kde se daná osoba pohybuje. Elektronická kontrola vstupu sleduje počet návštěv, vytížení pracovníků, využívání materiálů, spojů, vytížení kapacit, dohled a využití pracovní doby. Je upravena normou ČSN EN 50 – 133 – 1 , která má 7 částí (1.systémové požadavky, 2.identifikační zařízení,

3.vyhodnocovací, zobrazovací, programovací zařízení, 4. výstupní ovládací prvek, 5. komunikace, 6. ochrana a 7. pokyny pro aplikaci).

Elektronická kontrola vstupu je ovládána spínacími zařízeními. Jsou to nosiče informací uváděné systémem do stavu klidu nebo střežení. Jsou upraveny Českou asociací pojišťoven (dále jen ČAP) P-131-8 o spínacím zařízení.



Obr. 2 Systém pro integraci bezpečnostních a řídících technologií

1.1.6 ACCESS kontrol + informační technologie

Kombinace ACCESS kontrol s informační technologií je přístup umožněn po přihlášení se do sítě, softwaru,… Používají se identifikační prvky nebo biometrické prvky. Identifikační prvky – ISO 7816 – normalizované kontaktní rozhraní. Biometrické prvky – otisk prstů, duhovka, geometrie ruky. Informace je chráněna prostředky operačního systému (API).

1.1.6.1 Teoretické základy videotechniky a fyziologie lidského oka

Z důvodu velké analogie konstrukce lidského oka a konstrukce kamery s objektivem, jsou níže uvedeny základní fyziologické vlastnosti lidského oka. Optický systém umožňuje vytvořit na sítnici převrácený, zmenšený a neskutečný obraz vnějšího světa. Nervový systém slouží k příjmu, výběru a zachování zrakové informace. Pro zrakový vjem jsou podstatné dva typy fotoreceptorů, a to tyčinky a čípky. Denní, tzv. fotopické barevné vidění zprostředkovávají čípky, kterých je v oku cca 6,5 mil. Noční, tzv. skotopické vidění nám zprostředkovávají tyčinky, kterých je v oku cca 125 mil.

Obr. 3. Fyziologie lidského oka

Fyziologické vlastnosti oka jsou akomodace oka (schopnost zobrazit na sítnici blízké předměty menší než 6m), adaptace oka (schopnost přizpůsobit se různým intenzitám osvětlení), rychlost vnímaní (setrvačnost oka) – závislé na jasu a kontrastu detailů, zorné pole (část prostoru ohraničená vertikálně a horizontálně), obhledové pole (část prostoru, kterou může pozorovatel obsáhnout pohybem očí), rozlišovací schopnost (schopnost oka rozeznat dva blízké detaily, jejich barevnost), zraková ostrost (schopnost oka rozeznat 2 blízké detaily vzdálené úhlově 1´), prostorové vidění (stereoskopické binokulární vidění) a stálost vnímaní barevných odstínů.

1.2 Přehled vývoje snímací techniky

Chronologie:

V roce 1878 se uskutečnil první pokus přenést obraz elektronickou cestou. V roce 1881 byl zaznamenán první dokumentovaný přenos obrazu elektrickou cestou. Vynález principu řádkového rozkladu obrazu se objevil v roce 1884 a po něm v roce 1934

následoval vynález snímací elektronky. Pravidelné televizní vysílání (300 přijímačů TV) bylo zahájeno v roce 1936 stanicí BBC. Ke zdokonalení elektronky došla až v roce 1940. A rok na to (1941) byla vyrobena první průmyslově vyrobená kamera.

V polovině 50. let. byly vyrobeny kamery s malými rozměry. Ke zdokonalení snímací elektronky, dostupné a využitelné i pro CCTV došlo v polovině 60. let. V polovině let 70. byly vytvořeny citlivé vrstvy z mozaiky Si diod. První elektronku s akumulační elektrodou tvořenou přechodem PN, a přechodem selenem vyvinuli v polovině let 80. A v polovině 90. let začal počátek vývoje CCD obrazového snímacího prvku (CCD – nábojově vázaná struktura, zavedení nových technologií firmami SONY, FUJI, HITACHI, NEC, TOSHIBA, SHARP, PHILIPS, VALVO, CDS, EEV.

Rozsah systému je dán počtem kamer, kde se může jednat o systém s černobílým, barevným rozlišením, nebo dokonce kombinovaný systém. Zdokonalování technologie zlepšuje možnosti snímaní kamer. Schopnost barevných kamer uspokojivě pracovat za nízkých úrovní osvětlení a při osvětlení smíšenými zdroji světla se neustále zlepšuje. I tak musíme počítat s omezenou schopností věrně zobrazit konkrétní barvu za umělého osvětlení.

Možnost přepínaní režimu černobílý / barevný / kombinovaný je požadavek velmi rozumný, ne však nezbytný. Rozlišovací schopnost kamer by při běžné aplikaci měla být určitě vyšší než 400 řádků. Přenos: je třeba uvažovat odděleně o přenosu videosignálu a o přenosu řídících

signálů. Přenos videosignálu v digitální formě (slow – scan) je takový, kdy signál je přenášen obvykle po komutovaných či vyhrazených linkách jednotné telefonní sítě (dále jen JTS), nebo po ISDN linkách. Přenos v digitální formě je dnes již realitou .

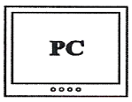
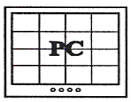
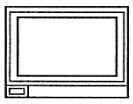
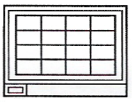
1.3 Základní druhy a typy přenosu

- **přenos po nesymetrickém vedení** (koax. kabel) - jedná se o nejčastější způsob přenosu , který je omezen řádově na stovky metrů. Nevýhodou je galvanické propojení i poměrně vzdálených prvků, možnost projevu brumových pásů přes obraz. Charakteristická impedance přenosového kabelu by měla být 75 ohmů. Na dlouhých kabelových trasách nutno počítat s využitím videozesilovačů nebo korekčních videozesilovačů s vyrovnáním kabelového útlumu.

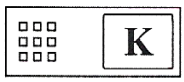
- **přenos po symetrickém vedení** (kroucený pár) – umožněn přenos do vzdálenosti cca 10 km. Jedná se v podstatě o dvojici vodičů telekomunikačního kabelu. Nevýhodou je jako obdoba u nesymetrického kabelu, pár však vykazuje vyšší odolnost proti impulsnímu rušení do přenosové trasy. Tento systém používá standardní symetrické vedení s charakteristickou impedancí 120 – 150 ohmů.
- **bezdrátový přenos**: tento přenos je schválen podle kmitočtových pásem dle normy GL 14/R/2000 ČTÚ a to pro pásma : a) 10 GHz – směrová účinnost větší b) 2,4 GHz – antény YAGI
- **infračervený a laserový přenos** – má krátký dosah, nevýhodou je vliv povětrnostních podmínek. Je použitelný pouze na trasách bez terénních a jiných překážek. Výstup těchto přenosových zařízení může být nebezpečný pro zrak, musí proto být označen výstražným znamenímpodle příslušných bezpečnostních pravidel. Při volbě nuté vzít v úvahu, že dosah a kvalita spoje může být snížena klimatickými podmínkami. Proto jsou zde vyšší nároky na nastavení a stálost parametrů.
- **přenos po optickém vlákně** – ztráty při přenosu jsou velmi nízké a nedochází k prakticky žádným elektrickým interferencím. Přenos je možný až do vzdálenosti cca 50 km. Instalace optických vláken je levnější něž jiné přenosové systémy. Možné je využít optických tras v podobě závěsných kabelů.
- **Mikrovlnný a rádiový přenos** – vyžaduje správné nastavení vysílacího a přijímacího zařízení a jeho použití musí být schváleno příslušným zákonným orgánem.
- **Úzkopásmový přenos** – je vhodný pro veřejné i soukromé telefonní a datové sítě.

1.4 Systémové projekční symboly

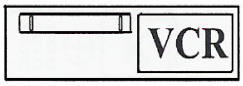
Systémové projekční symboly byly připraveny a vydány zejména jako pomůcka pro projekční a montážní firmy. Jejich účelem je kultivace oboru ve smyslu sjednocení používaných značek systémových komponentů CCTV a k nim odpovídajícímu názvosloví. Systémové projekční symboly vycházejí z názvosloví normy ČSN EN 50132-7, které se v některých případech doplňují o nové dle zvyklostí a četnosti používání. Systémové symboly jsou rozděleny do kategorií na značky pro zobrazovací zařízení, značky pro ovládací zařízení, značky pro řídící a záznamové jednotky a značky pro kamerovou sestavu.

Značky pro zobrazovací zařízení	
	PC monitor pro jednotlivé zobrazení
	PC monitor pro vícenásobné zobrazení
	Monitor pro jednotlivé zobrazení
	Monitor pro vícenásobné zobrazení

Obr. 4. Značky pro zobrazovací zařízení

Značky pro ovládání zařízení	
	Ovládací klávesnice s telemetrií
	Ovládací klávesnice

Obr. 5. Značky pro ovládání zařízení

ZNAČKY PRO ZÁZNAMOVÉ JEDNOTKY	
	ANALOGOVÝ REKORDER
	DIGITÁLNÍ REKORDER

Obr. 6. Značky pro záznamové jednotky

ZNAČKY PRO ŘÍDÍCÍ JEDNOTKY	
C.U.	ŘÍDÍCÍ JEDNOTKA
MTX	VIDEOMATICE
SEQ	SEKVENČNÍ PŘEPÍNAČ
MUX	MULTIPLEXER
Q	KVADRÁTOR

Obr. 7. Značky pro řídící jednotky

ZNAČKY PRO KAMEROVOU SESTAVU	
	KAMEROVÁ SESTAVA STÁVAJÍCÍ
	KAMEROVÁ SESTAVA NOVÁ
	DESKOVÁ KAMEROVÁ SESTAVA
	KAMEROVÁ SESTAVA VE VNITŘNÍM KRYTU
	KAMEROVÁ SESTAVA VE VENKOVNÍM KRYTU
	POLOHOVACÍ KAMEROVÁ SESTAVA
	POLOHOVACÍ KAMEROVÁ SESTAVA VE VNITŘNÍM KRYTU
	POLOHOVACÍ KAMEROVÁ SESTAVA VE VENKOVNÍM KRYTU
	POLOHOVACÍ DOME KAMEROVÁ SESTAVA VE VNITŘNÍM KRYTU
	POLOHOVACÍ DOME KAMEROVÁ SESTAVA VE VENKOVNÍM KRYTU

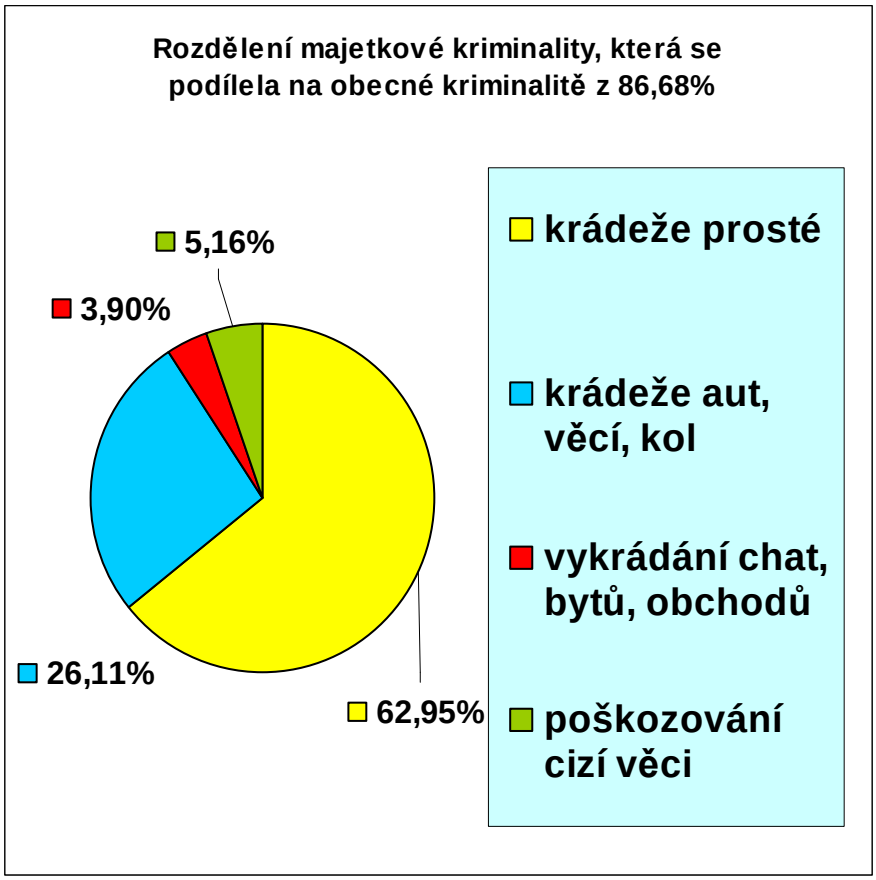
Obr. 8. Značky pro kamerovou sestavu

2 VÝZNAM CCTV V SYSTÉMU PREVENCE KRIMINALITY ČESKÉ REPUBLIKY

2.1 Kriminalita ve městech ČR

Policejní statistická čísla za rok 2000 uvádějí, že největší podíl na celkové kriminalitě má kriminalita obecná 83,78 % a kriminalita hospodářská 9,61 %. Z obecné kriminality vede jednoznačně kriminalita majetková s 86,68 % (krádeže prosté 62,95 % - krádeže aut, věcí z aut, jízdních kol, kapesní krádeže, krádeže vloupáním 26,11 % - do chat, bytů, do obchodů, podvody 3,90 % a poškozování cizí věci 5,16 % ...).

Graf 1. Rozdělení majetkové kriminality



2.2 Místo CCTV v systému prevence kriminality České republiky

CCTV nebo – li průmyslová televize nebo také uzavřený kamerový dozorový a kontrolní systém, zvyšuje bezpečnost střežených objektů. Nalezne uplatnění tam, kde je nutné kontrolovat přítomnost osob, pohyb zboží, nebo průběh technologického procesu. Slouží k přenosu pohyblivých, nepohyblivých, černobílých, barevných i kombinovaných obrazů na dálku. Má uzavřený okruh uživatelů. Používá se v průmyslu, dopravě, školství a všude tam, kde chceme sledovat děje v těžce dostupných místech, nebo ve zdraví škodlivém prostředí. Tento systém je určen pro sledování a kontrolu libovolných prostor. Kamerové systémy lze libovolně sestavovat a rozšiřovat pomocí různých přídavných zařízení dle požadavku na počet kamer a velikost snímaného prostoru.

Pro záznam obrazu se používají především průmyslové digitální záznamové jednotky (dále jen DVR), které využívají jako záznamové médium pevný disk, podobně jako PC.

2.2.1 Systém prevence kriminality v České republice

CCTV má v systému prevence kriminality České republiky své důležité a nepřehlédnutelné místo. Vyvážený systém prevence kriminality vyžaduje provázaný preventivní systém, kde kromě projektů situační prevence jsou zastoupeny i projekty sociální prevence, projekty určené k informování veřejnosti o možnostech ochrany před trestnou činností a projekty na pomoc obětem trestných činů.

K podpoře měst zatížených vysokou mírou kriminality byl vytvořen v roce 1996 státní dotační systém, který spravuje Odbor prevence kriminality Ministerstva vnitra (dále jen OPK).

Preventivní systém ČR tvoří především resortní programy prevence kriminality, z které vychází komplexní program prevence kriminality na místní úrovni je realizovaný ve městech samosprávnými orgány, programy nevládních a charitativních organizací, analytické a praven-tivní aktivity Policie České republiky a její podíl na přípravě preventivních programů měst, projekty nestátních komerčních subjektů - členů Poradního sboru pro situační prevenci kriminality Ministerstva vnitra (zástupci České asociace pojišťoven, Asociace technických bezpečnostních služeb Grémium Alarm, Asociace soukromých bezpečnostních služeb,...)

2.2.2 Projekty v rámci Komplexního součinnostního programu prevence kriminality na místní úrovni

Komplexní součinnostní program prevence kriminality na místní úrovni (dále jen KSP) je základem systému prevence kriminality v ČR. Prevence kriminality má na komunální úrovni velkou odezvu a stala se nosným tématem a součástí politiky. Ve městech se podařilo vytvořit celou řadu navzájem provázaných projektů, které vedou ke snižování míry a závažnosti trestné činnosti, zvyšování pocitu bezpečí u občanů a ke stabilizaci a poklesu trestné činnosti. Velkým pozitivem KSP je zapojení Policie České republiky. U Policie ČR vznikly v průběhu posledních let tzv. preventivně informační skupiny (dále jen PIS), kterých je v současné době již přes 70. Některé PIS otevřely policejní poradenské místnosti, kde policisté poskytují občanům poradenství ohledně ochrany majetku a osob. Hlavním cílem KSP je podnítit ve městech, která jsou nejvíce zatížené kriminalitou, spolupráci konkrétních subjektů (městská zastupitelstva, policie, občanská sdružení, církve apod.) a dělat patřičné kroky ke snížení kriminality. Města v rámci KSP realizují konkrétní projekty sociální a situační prevence. Oba typy projektů se vzájemně ovlivňují, doplňují a prolínají. Tím získává KSP města na vyváženosti a kvalitě a tím se jeho účinek násobí. Samotné sociální projekty přinášejí efekt později, ale zato trvaleji. Naopak dobře realizované projekty situační prevence mohou některé pachatele odvrátit od úmyslu spáchat trestný čin, odstranit cíle útoku, ztížit dostupnost těchto cílů, snížit výnosnost činu, popřípadě pachatele dopadnout. Umožňují dosáhnout výsledku ihned a efektivně.

Stát přispívá na projekty nemalými prostředky. V níže uvedené kapitoly jsou uvedeny základní projekty prevence, mezi které můžeme zařadit :

- Projekty situační prevence (CCTV, zabezpečení objektů města a zřízení pultů centralizované ochrany, osvětlení atd.) - celkem 383 projektů, částku 24 144 480,- Kč**.**

- Projekty z oblasti sociální prevence (zaměřené na rizikové skupiny mládeže, oběti trestné činnosti, sociálně handicapované romské obyvatelstvo a další rizikové skupiny – bez-domovce,drogově závislé, prostitutky) - celkem 1476 projektů,částku 185 383 000,- Kč.

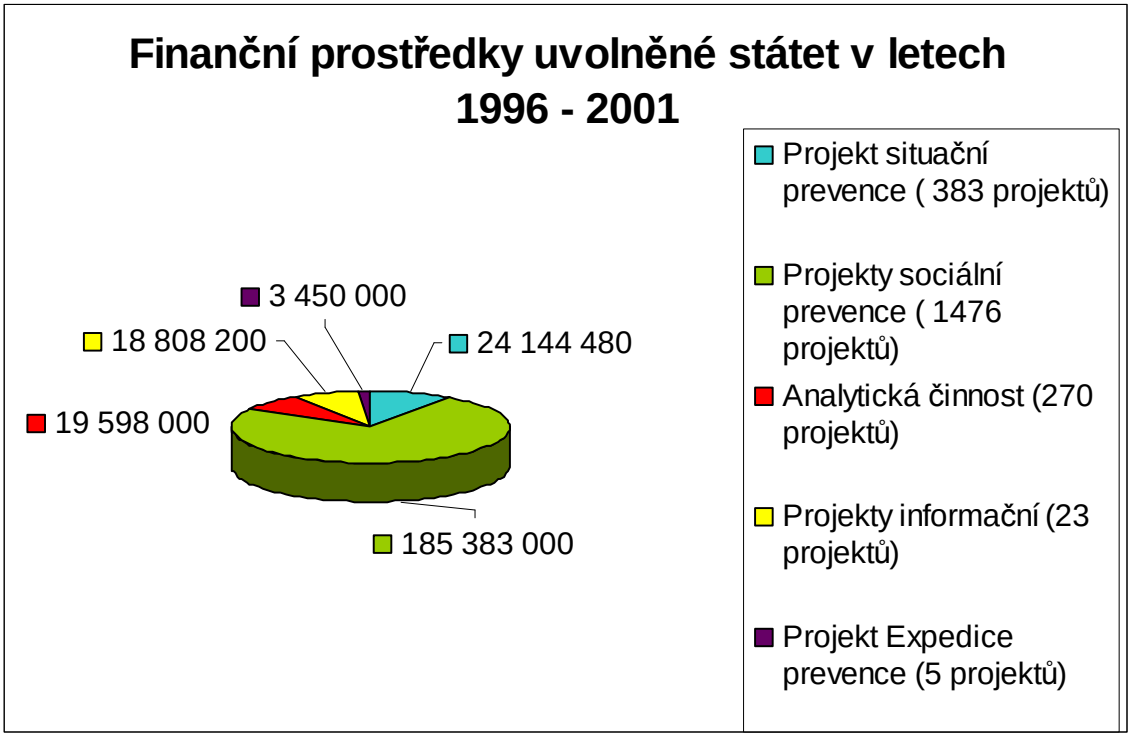
- Analytickou činnost, vybavení analytických pracovišť okresních ředitelství PČR výpočetní technikou (vytvoření základních podmínek pro průběžnou analytickou činnost pro potřeby realizujících KSP), vybavení manažerů KSP výpočetní technikou včetně internetu, vzdělávání manažerů KSP atd. - celkem 270 projektů, částku 19 598 000,- Kč

- Projekty informující občany o bezpečnostních rizikách ve městě, o možné ochraně před trestnou činností, o existenci krizových a poradenských zařízeních apod. - celkem 242 projektů, částku 18 808 200,- Kč.

- Projekt Expedice prevence - celkem 23 projektů (30minutový televizní pořad věnovaný prezentaci úspěšných preventivních projektů ve městě) - částku 3 450 000,- Kč.

- Podporu činnosti Středisek výchovné péče (na doplnění jejich materiálně technického vybavení, zpracování metodických materiálů a vzdělávání) - celkem 5 projektů, částku 1 966 000,- Kč

Graf. 2. Finanční prostředky uvolněné státem v letech 1996 – 2001



Na základě dosavadního hodnocení jsou v oblasti situační prevence nejvíce ceněny projekty CCTV, zabezpečení objektů a jejich připojení na pulty centralizované ochrany, osvětlení nepřehledných míst, preventivní informace pro občany, schránky důvěry a technika pro policii. V oblasti sociální prevence jsou dobré zkušenosti zaznamenány zejména u následujících projektů: sportovní plácky, kluby mládeže, centra volného času, skateparky se sociální asistencí, níz-

koprahová zařízení pro "děti ulice", otevřená školní hřiště, azylová zařízení, streetwork pro drogovou problematiku.

2.3 CCTV, metropolitní a geografické informační systémy měst

Základní charakteristikou provozování a využívání CCTV je jejich preventivní funkce, tj. vytváření bezpečných zón v exponovaných lokalitách. Kamery se instalují v místech, kde se nejčastěji pohybují občané a návštěvníci měst, kde jsou koncentrovány kulturní, komerční a společenské instituce i dopravní uzly, zahrnuty v klíčové ochraně osob. Jde zejména o městská centra - ulice, křižovatky, pěší zóny, různá podloubí, tržiště, náměstí, obchodní a nákupní centra, parkoviště, sídliště - obytné zóny, víceúčelová a dětská hřiště, parky, kolonády, peněžní ústavy. Zde všude bývá velký problém s trestnou a přestupkovou činností.

CCTV slouží k dohledu v místních záležitostech veřejného pořádku a k předcházení pouliční trestné činnosti a přestupků. CCTV přinášejí okamžitý výsledek (snížení kriminality v určeném místě). Musí se stát součástí celkové strategie prevence kriminality v určité lokalitě.

Kamerovým monitoringem se snižuje kriminalita a zvyšuje se pocit bezpečí u občanů. Tím vzrůstá důvěra občanů k policii. Kriminalita se sice zčásti přesouvá do jiných - vedlejších ulic nebo lokalit, ale na to reaguje policie a komunita operativně jinými opatřeními. Policie zefektivněla instalací CCTV svou práci a postupně získává na svou stranu veřejnost.

CCTV umožňují podchycení závadového jednání v samotném počátku a jeho dokumentaci. Mají význam i pro vedoucího pracovníka policie, který má možnost takto kontrolovat úkoly zadané policistům a strážníkům při instruktáži. Systém totiž dokumentuje i zákroky hlídky, chování a vystupování jejich členů.

Lokální CCTV se neustále rozvíjejí. Budou přicházet metropolitní kamerové dohlížecí systémy, jichž budou využívat všechny složky integrovaného záchranného systému (dále jen IZS) - úřad města, policie, hasiči a záchranná služba. Z páteřních městských rozvodů (např.optická vlákna) si budou jednotlivé složky IZS na základě schválených přístupových oprávnění monitorovat zájmové oblasti města.

Další směr vývoje představuje městský geografický informační systém (dále jen GIS). Systém propojuje grafické a negrafické informace, ale zároveň tyto informace přesně lokalizuje v

mapě. Jako podklad pro systém slouží dvě mapová díla - katastrální mapa a digitální technická mapa. Prioritní je katastrální mapa, která je dokonale skladebná a pokrývá i popisuje beze zbytku celé zájmové území. GIS je výborným pomocníkem pro práci obou policií. Slouží k okamžitému lokalizování a úkolování hlídek, vyhodnocení nápadu trestné a přestupkové činnosti, vyhledávání závadových lokalit i pro sledování průjezdnosti vozovek a míst se zvýšenou nehodovostí. GIS umožňuje i využití kamerových systémů, pultů centralizované ochrany (alarmová signalizace z elektrického zabezpečovacího systému či z elektrické požární signalizace chráněného objektu) a připojení dalších technických novinek.

3 TECHNICKÉ POŽADAVKY NA SYSTÉMY UZAVŘENÝCH TELEVIZNÍCH DOZOROVÝCH KONTROLNÍCH A STŘEŽÍCÍCH SYSTÉMŮ VE SMYSLU ZÁKONA Č. 22/97 SB. VE ZNĚNÍ POZDĚJŠÍCH PŘEDPISŮ

S ohledem na vstoupení ČR do Evropské unie se mění legislativní požadavky spojené s uváděním výrobků na trh včetně zařízení CCTV dovážených do ČR i vyráběných českými výrobci. Nejdůležitější změnou je zjednodušení postupů posuzování shody pro dovozce zboží ze zemí Evropské unie (EU), které umožňuje novela zákona 22/1997 Sb., o technických požadavcích na výrobky, ve znění pozdějších předpisů, v návaznosti na nabytí platnosti dohody o posuzování shody a akceptaci průmyslových výrobků se zeměmi EU. Tento “Protokol k Evropské dohodě zakládající přidružení mezi Českou republikou na jedné straně a Evropskými společenstvími a jejich členskými státy na straně druhé o posuzování shody a akceptaci průmyslových výrobků” (tzv. dohoda PECA). Byl parafován velvyslancem ČR v EU a zástupcem komise Evropského Společenství (dále jen ES). V říjnu 2000 byl schválen vládou ČR a předložen parlamentu a k ratifikaci prezidentem republiky a vešel v platnost v ČR od 1. 7. 2001.

PECA umožňuje, aby se ČR podílela na některých výhodách vnitřního trhu EU. Vzájemné uznání systému posuzování shody odstraní duplicitní, časově a finančně náročné prověřování výrobků v dohodnutých sektorech. Dohodnutých sektorů je zatím deset a zahrnují poplachové systémy relevantní oblasti bezpečnosti elektrických zařízení, elektromagnetickou kompatibilitu zařízení a ochranné systémy určené pro prostředí s nebezpečím výbuchu (v případě, že je to pro konkrétní zařízení relevantní).

Pro dovozce je pozitivní to, že smluvní strany vzájemně uznávají výsledky posuzování shody, nebudou vyžadovat opakování jejího posuzování a ani nebudou klást dodatečné požadavky (nad rámec směrnic ES, resp. nařízení vlády). Asi nejpodstatnějším zjednodušením postupů při uvádění výrobků dovezených ze zemí ES a nesoucích označení CE na trh ČR ve smyslu novely zákona 22/1997 Sb., ve znění pozdějších předpisů je to, že dovozce nemá povinnost na území ČR uchovávat doklady o použitém způsobu posouzení shody, je však povinen zajistit jejich předložení orgánu dozoru na jeho žádost, odůvodněnou podezřením na nebezpečí vážného

ohrožení oprávněného zájmu, v jím stanovené přiměřené lhůtě, a to v jazyce stanoveném nařízením vlády.

Výrobci jsou vázáni i nadále postupy posuzování shody, které jsou s ohledem na charakter výrobku relevantní. PECA jim však umožní uvést na výrobek evropskou značku shody (CE) a bez dalších procedur uvádět výrobek v zemích Evropského společenství.

Novela zákona 22/1997 Sb. a navazující zákon 102/2001 Sb. o obecné bezpečnosti výrobků připravily ve vymezených oblastech půdu k plné kompatibilitě českých právních předpisů s předpisy ES, což bylo podmínkou přijetí PECA.

Realizace PECA tedy umožňuje umisťovat na české výrobky po posouzení shody značku evropské shody CE a volně je uvádět na trh EU a naopak výrobky, mající původ v zemích EU a nesoucí označení CE, uvádět na trh v ČR bez dalších procedur. Další informace o přijetí PECA na internetové stránce Úřadu pro technickou normalizaci a státní zkušebnictví (www.unmz.cz).

3.1 Relevantní nařízení vlády

Se zákonem souvisí nařízení vlády, která stanovují konkrétní požadavky na jednotlivé skupiny vybraných výrobků. V souvislosti s přijetím PECA byla řada nařízení vlády novelizovaná s platností od 1. října 2000 s cílem plné kompatibility se směrnicemi ES ve vymezených sektorech (přehled o zákonech, nařízeních vlády a dalších právních předpisech viz www.sbcr.cz). Právní účinnosti nabývají okamžikem nabytí účinnosti PECA - tedy od 1. 7. 2001.

Nařízení vlády vymezuje především okruh výrobků, na něž se nařízení vztahuje - rámcově, (popř. nevztahuje - konkrétně), základní požadavky na výrobky, postupy posuzování shody, požadavky na obsah dokumentace a náležitosti prohlášení o shodě. Nařízení vlády obsahují také klauzuli presumpce splnění požadavku při splnění požadavků harmonizovaných Českých technických norem.

Pro systémy uzavřených televizních okruhů (CCTV) jsou z pohledu zákona 22/97 Sb., ve znění pozdějších předpisů, nejdůležitější nařízení vlády, kterým se stanoví:

3.1.1 Technické požadavky na zařízení nízkého napětí (L VL)

Za elektrická zařízení pro účely tohoto nařízení se považují výrobky určené pro provoz v rozsahu jmenovitých napětí střídavých od 50V do 1000V a stejnosměrných v rozsahu od 75V do 1500V. Stanovené výrobky jsou všechna elektrická zařízení podle zákona 22/97 Sb. s výjimkou zařízení uvedených v příloze 1. V příloze uvedená elektrická zařízení podléhají působnosti jiného nařízení vlády (např. zařízení do výbušného prostředí, elektrické části výtahů, elektroměry apod.). V příloze 2 nařízení vlády jsou uvedeny hlavní zásady bezpečnosti pro elektrická zařízení. Posouzení shody před uvedením výrobku na trh zajišťuje výrobce (nebo dovozce). O použitém způsobu posouzení shody je povinen zajistit náležité doklady včetně technické dokumentace (viz. § 5 nařízení vlády). Nebudou-li použity, je nutno dokumentaci doplnit o popis technického řešení s ohledem na splnění základních požadavků nařízení vlády.

3.1.2 Technické požadavky z hlediska elektromagnetické kompatibility (EMC)

Nařízení pro problematiku kompatibility systémů se vztahuje na elektrická nebo elektronická zařízení včetně vybavení a instalací obsahujících elektrické anebo elektronické součásti. Elektromagnetickou kompatibilitu můžeme charakterizovat jako schopnost zařízení, jednotky zařízení nebo systému fungovat uspokojivě v elektromagnetickém prostředí, aniž by samo způsobovalo nepřípustné elektromagnetické rušení jakéhokoliv zařízení v daném prostředí. Stanovené výrobky jsou přístroje, které mohou způsobovat elektromagnetické rušení, nebo jejichž funkce může být takovým rušením ovlivněna, s výjimkou amatérských vysílacích rádiových stanic běžně dostupných v obchodní síti. V příloze 1 nařízení vlády jsou uvedeny základní technické požadavky na přístroje, zařízení a systémy z hlediska elektromagnetické kompatibility. Posouzení shody před uvedením výrobku na trh zajišťuje výrobce (nebo dovozce). O použitém způsobu posouzení shody je povinen zajistit náležité doklady včetně technické dokumentace. Pro posouzení shody je možno použít harmonizovaných ČSN. Nebudou-li použity, je nutno dokumentaci doplnit o popis postupů použitých k posouzení shody zařízení se základními požadavky nařízení vlády a zkušebním protokolem nebo certifikátem akreditované zkušebny.

3.2 Harmonizované normy pro systémy uzavřených televizních okruhů (CCTV)

Vodítkem pro užívání norem na poplachové systémy v rámci směrnic ES je Technická zpráva RO79 CLC/TC79. Jejím účelem je kromě všech dalších směrnic EC registrovat směrnice o zařízení použitém v poplachových systémech, identifikovat základní požadavky vyplývající z výše uvedených směrnic EC, které je třeba zohlednit v procesu standardizace a které by měly být známy orgánům zabývajících se zařízením použitým v poplachových systémech a registrovat normy doporučené Technickým výborem TC79 pro prokazování shody se směrnicemi EC a se základními požadavky identifikovanými výše.

Tato technická zpráva zahrnuje především zařízení využívaná v následujících oblastech:

- Řízení přístupu (ACS).
- Přenos poplachu (ATS).
- Systémy uzavřených televizních okruhů (CCTV).
- Poplachový systém pro detekci požáru a při požáru (PAS).
- Poplachový systém proti vloupání a při přepadení (AIS).
- Poplachový systém sociální (SAS).

Tab. 1. Odpovídající Nařízení vlády ČR

Směrnice EU	Název	Nařízení vlády ČR
L YD 73/23	Technické požadavky na elektrická zařízení nízkého napětí	NV 168
EMC 89/336	Technické požadavky na výrobky z hlediska elektro-magnetické kompatibility	NV 169
ATEX 94/09*)	Technické požadavky na zařízení a ochranné systémy určené pro použití v prostředí s nebezpečím výbuchu	NV 176
CPD 89/106**)	Bezpečnost při požáru	-
1TE 91/263***)	Telekomunikační koncová zařízení	-
EEC 92/58****)	Ochrana zdraví při práci	-

POZNÁMKA:

*) Pouze pro systémy instalované do prostředí s nebezpečím výbuchu.

**) Pouze pro instalace systémů kontroly a řízení vstupů - evakuace (pro zařízení se v současné době neuplatňuje).

***) Pouze pro zařízení napojená na JTS.

****) Pouze Poloha IV. pro systémy s akustickou signalizací (siréna, bzučák...).

Harmonizované evropské normy pro splnění směrnice LYD 73/23 jsou EN 60950 a EN *60065*. Dále jsou v tabulce uvedeny harmonizované České technické normy ve vztahu k Nařízení vlády č. 168/1997Sb., kterým se stanoví technické požadavky na elektrická zařízení nízkého napětí.

Tab. 2. Normalizované České technické normy ve vztahu k Nařízení vlády č. 168/ 1997 Sb.

Harmonizovaná ČSN	**Název**	**Třídící znak**
ČSN EN 60065 vydána: duben 2000	Zvukové, obrazové a podobné elektronické přístroje Požadavky na bezpečnost	36 7000
Harmonizace:	NV 168 - Věstník ÚNMZ 2000/06	
ČSN EN 90950+Al *+A2+A3* vydána: červenec 2000	Informační technika - Bezpečnost zařízení informační techniky včetně elektrických kancelářských zařízení (obsahuje změny AI, A2, A3)	36 9060
Harmonizace:	NV 168 - Věstník ÚNMZ 2000/06	

Pro zařízení CCTV instalované ve složitých klimatických prostředích se jeví jako smysluplný požadavek aplikace normy ČSN EN 60529 Stupně ochrany krytem (krytí - IP kód) harmonizované v systému českých technických harmonizovaných norem Věstníkem 1997/09 včetně opravy (Cor.) harmonizované Věstníkem 1998/12.

Harmonizované Evropské normy pro splnění směrnice EMC 89/336 jsou pro emise (vyzařování) normy EN 50 *081-1,* EN 50 *081-2,* EN 55022 a pro odolnost EN *50130-4* a pro bezdrátová zřízení ETS 300 339.

Dále jsou v tabulce uvedeny harmonizované České technické normy ve vztahu k Nařízení vlády č. 169/1997 Sb., kterým se stanoví technické požadavky na výrobky z hlediska jejich elektromagnetické kompatibility:

Tab. 3. Normalizované České technické. normy ve vztahu k Nařízení vlády č. 169/1997 Sb.

Harmonizovaná ČSN	**Název**	**Třídící znak**
ČSN EN *50 081-1* vydána: únor 1994	Elektromagnetická kompatibilita. Všeobecná norma týkající se vyzařování. Část 1: Prostory obytné, obchodní a lehkého průmyslu	33 3433
Harmonizace:	**NV 169 - Věstník ÚNMZ 1997/09**	
ČSN EN 50 *081-2* vydána: únor 1994	Elektromagnetická kompatibilita. Všeobecná norma týkající se vyzařování. Část 2: Průmyslové prostředí	33 3433
Harmonizace:	**NV 169 - Věstník ÚNMZ 1997/09**	
ČSN EN 55 022 vydána: srpen 1996	Meze a metody měření charakteristik rádiového rušení zařízením informační techniky	33 4290
Harmonizace:	**NV 169 - Věstník ÚNMZ 1997/09, 1998/06, 1998/12**	
ČSN EN 50 082-1 vydána: únor 1999	Elektromagnetická kompatibilita - Kmenová norma pro odolnost - Část 1: Prostory obytné, obchodní a lehkého průmyslu	33 3434
Harmonizace:	**NV 169 - Věstník ÚNMZ 1999/03**	
EN 50 082-2*)	Elektromagnetická kompatibilita. Všeobecná norma týkající se odolnosti. Část 2: Průmyslové prostředí	
Harmonizace:	**není uvedena v seznamu Českých technických harmonizovaných norem**	
ČSN EN 50 130-4**) vydána: prosinec 1997	Poplachové systémy - Část 4: Elektromagnetická kompatibilita - Norma skupiny výrobků: Požadavky na odolnost komponentů požárních systémů, zabezpečova-cích systémů a systémů přivolání pomoci	33 4590
Harmonizace:	**NV 169 - Věstník ÚNMZ 1998/06,1999/12**	

ČSN EN 50 132-2-1 vydána: červenec 1999	Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích - Část 2-1: Černobílé kamery	33 4582
Harmonizace:	**NV 169 - Věstník ÚNMZ 1999/12**	

POZNÁMKA:

*) Tato norma není uvedena ani v seznamu vydaných ČSN, ani v seznamu Harmoniz. norem.

**) Tato norma je zde uvedena pro úplnost, její uplatnění pro komponenty CCTV není v názvu uvedeno, přesto ve výjimečných případech, zvláště u komplexních integrovaných a funkčně propojených systémů, je aplikace této normy na nakupované či vyráběné komponenty CCTV účelná.

Pro bezdrátový přenos videosignálu je nutno dodržovat zákon č. 151/2000 Sb., O telekomunikacích a je možno využívat pouze zařízení, které bylo schváleno pro provoz v ČR a na které bylo vydáno prohlášení o shodě ve smyslu Nařízení vlády 426/2000 Sb., kterým se stanoví požadavky na rádiová a na telekomunikační koncová zařízení. Tato zařízení jsou označena v souladu s Vyhláškou Ministerstva dopravy a spojů č. 182/2000 Sb., o schvalovací značce pro rádiová a telekomunikační koncová zařízení.

K termínu zpracování příspěvku však nebyly ve Věstníku ÚNMZ uvedeny žádné harmonizované normy k Nařízení vlády 426/2000 Sb., kterým se stanoví požadavky na rádiová a na telekomunikační koncová zařízení. Soupis zařízení, podléhajících procesu schvalování norem uplatňovaných při schvalování těchto zařízení je však k dispozici na internetové adrese www.ctu.cz. Režim regulace vychází ze směrnice ES 99/05 a není doposud plně harmonizován. Oblast není pokryta dohodou PECA.

Zařízení využívají pásma stanovená generálními licencemi (dále jen GL) ČTÚ (nezpoplatněná pásma). Ani využitím těchto pásem a splněním technických požadavků stanovených těmito GL se výrobce či dovozce nezbavuje povinnosti nechat zařízení schválit pro provoz v ČR a provést posouzení shody se všemi nařízeními vlády, jež se na ně vztahují.

Vzhledem k tomu, že se režim uvádění koncových telekomunikačních a rádiových zařízení na trh s ohledem na sjednocení postupů s ES v poslední době změnil, je nutno se v této oblasti věnovat technickým požadavkům na přenosová zařízení pro aplikace v CCTV, a to jak pro širokopásmový přenos videosignálu, tak pro případný digitální přenos ovládacích signálů. Přístroje a zařízení schválená do 30. června 2000 podle vyhlášky Ministerstva hospodářství č. 26/1996 Sb., o způsobu, podmínkách a postupu při ověřování a schvalování telekomunikačních koncových zařízení, mohou být uváděna na trh nejpozději do 30. června 2002.

Je nutno upozornit, že se s ohledem na přistoupení ČR do struktur NATO mění kmitočtový plán, a některá pásma využívaná dnes pro přenosová zařízení a systémy v rámci CCTV bude nutno perspektivně uvolnit. Např. pásmo 10 GHz (ošetřené původně Generálním povolením), ošetřené dnes Generální licencí GL14 a hojně využívané pro přenosy videosignálu v CCTV, musí být uvolněno do roku 2005. Obdobná situace je i v pásmech využívaných pro přenos řídících signálů v rámci CCTV Na základě probíhajících jednání je pravděpodobné, že uvedené termíny budou prodlouženy.

Tab. 4. Skupina norem pro sledovací systémy pro použití v bezpečnostních aplikacích

Číslo normy	Zjednodušený název
EN 50132-1	Systémové požadavky
EN 50132-2-1	Černobílé kamery
EN 50132-2-2	Barevné kamery
EN 50132-2-3	Objektivy
EN 50132-2-4	Příslušenství
EN 50132-3	Místní a hlavní řídící jednotka
EN 50132-4-1	Černobílé monitory
EN 50132-4-2	Barevné monitory
EN 50132-4-3	Záznamová zařízení
EN 50132-4-4	Zařízení pro okamžitý výtisk obrazu
EN 50132-4-5	Videodetektor pohybu
EN 50132-5	Přenos videosignálu
EN 50132-6	(volná)
EN 50132-7	Pokyny pro aplikace

4 PROVOZNÍ POŽADAVKY

Systém může například fungovat tak, že bude provádět záznamy pro pozdější zpracování. CCTV se v určitých případech používá na parkovištích za účelem analýzy událostí a podniknutí příslušných kroků v pozdějším časovém období. Můžeme provádět záznamy pro pozdější zpracování a současně i monitorovat. To nám umožní pozdější prohlížení, ale v případě potřeby i okamžitý zásah. Můžeme také provádět záznamy za účelem soudního stíhání, provádět živé sledování za účelem zásahu a nebo zadržení a současně záznam za účelem soudního stíhání. Specifikace vybavení se budou rovněž lišit podle místa, na němž má systém pracovat. Jedná se převážně o venkovním prostředí, za denního světla / v noci a nebo v různých ročních obdobích.

4.1 Světlo

Množství světla se měří v měrných jednotkách známých jako lux. Denní světlo je tvořeno spektrálním složením záření o různých vlnových délkách a CCTV je vůči některým barevným kombinacím citlivější než vůči jiným. Množství světla odrážené od předmětů určuje, jak výrazné se tyto předměty jeví. Při úvahách o umístění kamer je nutno s touto skutečností počítat. Vždy vybíráme místa tak, aby kamera neměla v zorném poli silné zdroje světla, ale současně byla zachována dostatečná úroveň osvětlení snímané scény s ohledem na danou citlivost použité kamery. Vhodné je tedy zjistit úroveň osvětlení k dohledu vytipovaných prostor.

Tab. 5. Typické úrovně osvětlení

Intenzita osvětlení (lux)	Popis
50 000	Letní slunce
5 000	Zatažené nebe
500	Dobře osvětlený obchod nebo kancelář
300	Minimální světlo pro snadné čtení
60	Schody / průchody za denního světla
15	Noc – dobře osvětlená hlavní ulice
10	Noc – normální osvětlení na hlavní ulici
10	Noc – západ slunce
5	Normální osvětlení ve vedlejší ulici
2	Minimální bezpečnostní osvětlení
1	Soumrak
0,3	Jasný úplněk
0,1	Měsíční světlo při zataženém nebi
0,001	Průměrné světlo hvězd
0,0001	Slabé světlo hvězd

Dále je třeba počítat se vzdáleností, v které je kamera umístěna (osvětlení klesá se čtvercem vzdálenosti), a s průměrnou odrazivostí sledované scény, která je uváděna v procentech dopadajícího světla.

4.2 Kamerové jednotky

Zdokonalování technologie zlepšuje možnosti snímání kamer. Ze všech prvků systému jsou právě kamery spolu se správně zvolenými objektivy a dalším příslušenstvím (kamerová jednotka) tím nejdůležitějším prvkem, který limituje kvalitu zobrazení celého systému.

Je nutno přiznat, že schopnost barevných kamer pracovat za nízkých úrovní osvětlení a při osvětlení smíšenými zdroji světla se neustále zlepšuje a ceny takových kamer se stávají přijatelnými. Musíme počítat s omezenou schopností věrně zobrazit konkrétní barvu zvláště za umělého osvětlení, jehož spektrální složení je vzdálené dennímu světlu (např. sodíková či rtuťová výbojka).

Pokud budeme trvat na požadavku přečíst poznávací značku auta v noci za slabého světla, které se nedá zlepšit, bude v dnešní době jediným řešením černobílá kamera.

I dnes už například řada výrobců vyrábí barevné kamery, které zajišťují výborný barevný záznam za denního světla a za soumraku automaticky přepnou na černobílý. V současné době je toto provedení dražší než u běžných barevných kamer, ale v tomto odvětví ceny spíše klesají, než stoupají!

Obr. 9. Kamerové jednotky

Přisvětlení scény v infračerveném spektru by mělo být až posledním řešením - výhodnější je zlepšit běžné veřejné osvětlení v místě. Rozlišovací schopnost kamer by pro danou aplikaci měla být určitě vyšší než 400 řádků, a to jak v černobílém, tak barevném režimu.

4.2.1 Mezní citlivost kamer

Jsou-li zóny sledování v noci osvětleny veřejným osvětlením, měla by být citlivost s ohledem na současně dosažitelné parametry v ekonomických mezích lepší než 1,5 lx v barevném režimu (popř. lepší než 0,2 lx v černobílém režimu) stanovena s rezervou. Parametr citlivost je vždy vázán na světelnost použitého objektivu a v nabídce by měla být citlivost uváděna vždy ve spojení se světelností objektivu, ke které je vztažena.

Existuje pří1iš mnoho vlivů, které mohou splnění požadavku omezit, některé působí pro, jiné proti a lze je systémem eliminovat pouze v omezené míře. Počet stupňů volnosti je zde prostě pří1iš velký (umístění na voze, vlastní kombinace znaků, značky - italská má menší znaky, arabská...), barva značky, barva vozu, směr odkud přijíždí, odjíždí, kde stojí, špinavé, naleštěné,

poloha slunce vůči sledovanému objektu, poloha sledovaného objektu vůči umělému osvětlení, denní doba, noční doba, roční doby - zima, léto, počasí - déšť, mlha, světla na autě - rozsvícena, zhasnuta, rychlost jakou se auto pohybuje, apod.

Požadavek na maximální ohniskovou vzdálenost objektivu by měl být uživatelsky specifikován jednoznačněji - např. dle ČSN EN 50132-7 - v kategoriích zobrazení na hranici sledované zóny (tj. identifikace, rekognoskace, detekce, monitorování). Např.: "Objektivy volit tak, aby bylo možno na hranici sledované zóny (viz plán města) objekt odpovídající standardní výšce postavy zobrazit min. na 50 % výšky obrazovky kontrolního monitoru (stupeň 2. rekognoskace dle ČSN EN 50132-7).

U polohovací hlavice a kamerového krytu je důležitým požadavkem stupeň krytí pro venkovní nasazení v nepřetržitém provozu. Podstatným požadavkem je rychlost otáčení polohovací hlavice zvláště v horizontálním směru. Je-li kamera umístěna na nároží a chceme-li sledovat prostor v celém rozsahu 270°, potřebuje standardní hlavice s rychlostí otáčení 6° *Is* k přetočení z jedné mezní polohy do druhé 45 s!

Nezbytným požadavkem je ochrana proti přepětí na signálových i napájecích trasách.

4.3 Přenos

Je třeba uvažovat odděleně o přenosu videosignálu a o přenosu řídících signálů. Možností, jak přenos videosignálu a řídících signálů zajistit, existuje dnes více.

4.3.1 Přenos videosignálu

4.3.1.1 Přenos v digitální formě (tzv. slow-scan)

Signál je přenášen obvykle, po komutovaných či vyhrazených linkách jednotné telefonní sítě (JTS), v lepším případě po ISDN linkách. Problém je především s cenou pronájmu přenosových cest. Pomalé prohlížení se může používat i pro barevné záznamy, ale jeho obraz je nespojitý a za současného stavu techniky se rozhodně nehodí ke sledování dynamických dějů. Dále je za tohoto stavu obtížné ovládání kamer (zoomování, ostření, polohování), s výjimkou systému, který umožňuje přednastavení pozic. Tento systém se obvykle používá u systémů řízení provozu, kde jsou přijatelné statické kamery a pomalá informace.

4.3.1.2 Přenos po nesymetrickém vedení (koaxiální kabel)

Uvedený přenos se často používá ke spojení kamer s ovládací místností. Koaxiální kabel může vést současně videosignál i ovládací signál. Přenos je omezen vzdáleností (řádově na stovky metrů), přičemž se v závislosti na útlumu použitého kabelu zhoršuje rozlišovací schopnost systému jako celku (ztrácí se schopnost zobrazit jemný detail, obrázky vypadají jakoby rozostřené). Samozřejmě lze zařadit do přenosové trasy korekční zesilovače videosignálu, pak ale ztrácíme možnost přenosu řídících signálů ke kamerové jednotce po jednom kabelu. Jedná se o nejběžnější druh přenosu, relativně levný, ale předpokládá buď možnost instalace závěsných vedení, což není často v zájmu města, nebo existenci kabelových kolektorů ve městě, což je řídký případ. Budování vlastních tras jako podzemní vedení je pak velice nákladné a v řadě případů prakticky nemožné. Ideální je spojit budování tras např. s telefonizací či budováním jiných sítí města (např. kabelové televize). Možnost koordinace jak časové, tak technické je bohužel velice obtížná, a proto lze o tomto ideálu hovořit jen v teoretické rovině. Nejčastěji je tedy přenos po koaxiálním kabelu používán v CCTV pro část přenosové trasy od kamerové jednotky k vysílacímu zařízení pro bezdrátový přenos.

Nevýhodou tohoto druhu přenosu je galvanické propojení i poměrně vzdálených prvků systému, což může přinést problémy s vyrovnávacími zemními proudy, které se na obrazovce v monitorovacím pracovišti projeví jako brumové pásy přes obraz. Další nevýhodou galvanického propojení je riziko přenosu přepěťových pulsů (např. vlivem atmosférických výbojů) k dalším prvkům systému.

4.3.1.3 Symetrické vedení (kroucený pár)

Další druh umožňuje přenos signálu na větší vzdálenosti než koaxiální kabel, v zásadě je používán až do vzdálenosti 10 kilometrů. Symetrické vedení, nazývané obvykle "kroucený pár", je v podstatě dvojice vodičů telekomunikačního kabelu. Obvykle jsou použity dvě sady párových kabelů - jedna pro přenos videosignálu a druhá pro přenos řídících signálů. Za vhodných podmínek to může představovat účinné a relativně levné řešení, ale určitou nevýhodou je, že každý zdroj i přijímač videosignálu vyžaduje zvláštní přenosovou jednotku.

Nevýhody jsou obdobné jako u přenosu po koaxiálním vedení, symetrický pár však vykazuje vyšší odolnost proti impulsnímu rušení, naindukovanému do přenosové trasy.

4.3.1.4 Bezdrátový přenos

Právně přípustný je přenos pomocí přenosových zařízení schválených pro provoz v provozních kmitočtových pásmech stanovených GL 14/R/2000 ČTÚ v pásmu 10 GHz a revidovaných GL 30/R/ 2000 v pásmu 2,4 GHz. Je třeba říci, že se nejedná o vyhrazená pásma, kde by byl garantován nerušený provoz a která by byla zpoplatňována. Jedná se o pásma sdílená více uživateli na základě zásad v GL uvedených. V současné době jsou kmitočtové pásma rozděleny do 3. úrovní (podle modulace) a to na 1. úroveň (800 MHz – 2,45 GHz), 2. úroveň (2,45 – 10 GHz), 3. úroveň (10 – 24 GHz), respektive nově předcertifikační úrovně do 42 GHz.

Z fyzikálního principu má vyšší pásmo vyšší úrovně směrové účinky, a i když na blízkém kmitočtu pracuje jiné zařízení, riziko rušení je minimální. Mikrovlnný přenos je možno realizovat s přijatelnými náklady na několik kilometrů s možností pasivní retranslace a až na desítky kilometrů s aktivní retranslací. Přenosové vzdálenosti jsou závislé rovněž na použité anténě, která má vzhled běžné satelitní antény pro družicový televizní příjem. Praktické omezení vyplývá z potřeby přímé viditelnosti, popř. zařazení retranslačních bodů. Antény se obvykle musí umísťovat na nejvyšší budovy nebo věže. Při nepříznivých povětrnostních podmínkách (hustý déšť, sněžení) se může snížit kvalita obrazu.

Nižší používané pásmo s nižší úrovní (např. 2,4 GHz) je prioritně určeno pro přenos dat s rozprostřeným spektrem, což přináší vyšší riziko rušení přenosu a rovněž směrové účinky těchto kmitočtů jsou menší, takže i z fyzikálního principu přenosu vyplývá vyšší náchylnost k rušení. Antény jsou většinou buď směrové - klasické Y AGI či anténní řady s reflektorem podobné televizním anténám či zvláštní dielektrické antény, popř. se využívají i všesměrové antény. Cena takového přenosového zařízení je nižší, ovšem při výše jmenovaných rizikách, že v kritickém okamžiku operátor neuvidí, co vidět má, popř. že záznam bude nepoužitelný. Jednoznačnou výhodou bezdrátových přenosů je galvanické oddělení jednotlivých částí systému a eliminace přenosu přepěťových pulsů.

4.3.1.5 Infračervený přenos

Infračervené spojení je další možností z oblasti bezdrátových technologií, o níž lze uvažovat při přenosu na krátkou vzdálenost. Je to další pomůcka, která se na krátký dosah velice osvědčila,

ale povětrnostní podmínky ji ovlivňují daleko výrazněji než mikrovlnné zařízení. Výhody jsou stejné jako u předcházejícího bezdrátového přenosu.

4.3.1.6 Přenos po optickém vlákně

Jedná se o teoreticky poměrně reálnou možnost, protože telefonní optická vedení bývají obvykle budována s dostatečnou rezervou. V praxi ovšem narážíme na umístění bodů připojení, ke kterým musíme náš signál dostat, a rovněž podmínky pronájmu volných optických tras jsou z hlediska dlouhodobé kalkulace provozních nákladů na CCTV zatěžující.

Optický kabel se skládá z jemných skleněných vláken, která mají vysokou optickou propustnost a působí jako vlnové vodiče pro světelné paprsky. Ztráty při přenosu jsou velice nízké a nedochází prakticky k žádným elektrickým interferencím. Přenos je možný na vzdálenosti větší než *50* kilometrů. Kabely jsou schopny přenášet velké množství signálů najednou, což umožňuje vyhovět i požadavkům na přenos řídících a jiných pomocných signálů (např. hlídání technologie). Instalace optických vláken může být levnější než jiné přenosové systémy, a to především u větších projektů. Možné je i využití optických tras v podobě závěsných kabelů.

Je třeba poznamenat, že pokud se systém rozšíří a bude pokrývat oblasti vzdálenější od monitorovacích míst, mohou prudce vzrůst náklady na přenos. Tím pádem technologie s krátkým dosahem už nemusí být schopna kvalitně přenášet obraz a pak může ke slovu přijít přenos po optickém vlákně.

Výhodou je galvanické oddělení jednotlivých částí systému a eliminace přenosu jak přepětí, tak rušení. I vlastní přenosové médium je zcela imunní proti indukovanému rušení.

4.3.2 Přenos řídících signálů

Pro přenos řídících signálů můžeme v podstatě použít kterýkoli z popsaných způsobů. U bezdrátových přenosů to předpokládá použití duplexních (obousměrně komunikujících) zařízení s možností modulace dat na přenosovou frekvenci či využití samostatného kanálu. Častější je však využití kmitočtových pásem vyhrazených pro dálkové ovládání pomocí dat (pásma telemetrie) pomocí tzv. radiomodémů. I tato zařízení podléhají působnosti Telekomunikačního zákona a musí mít od ČTÚ schválení do provozu v ČR.

4.4 Monitorovací pracoviště

Počet řídících míst a konfigurace řídícího pracoviště jsou určeny provozními požadavky a personálními možnostmi. Tyto parametry mohou být naprosto různé. Činnosti související se sledováním by měly být soustředěny do řídícího pracoviště, které je umístěno v chráněném prostoru. Kritéria pro konfiguraci řídícího pracoviště mohou být dána systémovými parametry, způsobem záznamu obrazu, ztrátovými výkony zařízení, případnou nutností klimatizace, omezeními danými polohou a prostorem, počtem monitorů, videozařízením pro ovládání kamer.

Je vhodné uvažovat, kam pracoviště umístit (např. na služebně městské policie, vyznačit ji na plánu města a uvažovat o reálné možnosti přenosu od zvolených lokalit umístění kamer).

Obr. 10. Monitorovací pracoviště Městské policie ve Zlíně

Je-li k dispozici výkres místnosti s předpokládaným umístěním zřizovacích předmětů, je vhodné ho připravit jako podklad pro zpracování nabídky řešení monitorovacího pracoviště. Vhodné je stanovit i počet pracovníků, kteří budou systém obsluhovat, popř. požadavek paralelního pracoviště např. pouze pro monitorování či pro práci s archivem snímků (u velitele). Zálohování napájení pro případ výpadku napájení zařízení celého monitorovacího pracoviště je rozumné. Z praktických důvodů ho omezíme pouze na dobu nezbytnou k "úklidu" dat či ošetření případně použitého software.

4.4.1 Monitory

Práce operátorů závisí na kvalitě obrazu monitoru. V první řadě platíte za dobrý obraz. Lidé musí u monitoru strávit řadu hodin. Monitory mohou zobrazovat jeden obraz nebo prostřednictvím multiplexních zařízení až šestnáct obrazů z různých kamer při zobrazení tzv. multiscreen. Proto je kvalita obrazu samozřejmě velmi důležitá - ale nezapomínejte na osvětlení v ovládací místnosti.

Kvalitu obrazu na televizní obrazovce může značně zhoršit světlo z prostředí, které na ni dopadá, a v některých případech se může stát, že přehlédneme důležitý záznam, který by byl ve správně osvětlené místnosti dobře viditelný. Světlo v místnosti může změnit i reprodukci barev. Špatné barvy, které bývaly přičítány barevným monitorům, se zlepšováním jejich kvality postupně mizí. Přesto je třeba vždy správně barvy nastavit a nezapomínat na uspokojivou úroveň kontrastu a jasu. Důležité je i pravidelné porovnávání nastavení monitoru při pravidelných technických prohlídkách.

Obr. 11. Monitory umístěné v monitorovacím pracovišti ve Zlíně

Je účelné zvážit požadavky na vybavení monitorovacího pracoviště s ohledem na režim provozu nepřetržitý/omezený, organizaci času, střídání směn, počet pracovníků obsluhy. S ohledem na zkušenosti z praxe a reálnou schopnost obsluhy, omezenou fyziologickými i psychologickými faktory, sledovat dlouhodobě více obrazovek je relevantní požadavek umístění alespoň dvou barevných monitorů s dostatečným rozlišením (s ohledem na rozlišovací schopnost kamer, přenosových tras i zařízení na zpracování videosignálu, minimálně však *400* řádků). Jinou možností je vícenásobné zobrazení pohledu všech kamer na jednom monitoru (multiscreen),

popř. sekvenční přepínání a druhý větší monitor pro sledování aktuálně vybrané zóny. Výběr monitorů je důležité přizpůsobit požadavkům na ergonomii, fyziologii, bezpečnost a ochranu zdraví při práci i prostorovým dispozicím pracoviště.

4.4.2 Ovládací zařízení

Podobně jako u volby monitorů je s ohledem na režim provozu - nepřetržitý/omezený, organizaci času - střídání směn a počtu pracovníků obsluhy, účelné zvážit požadavky na vybavení monitorovacího pracoviště. Relevantní je požadavek na předvolbu nastavení sledování oblastí zájmu v rámci sledovaných zón volitelně pro každé stanoviště min. počtem pozic denního sledování a min. počtem jiných pozic pro noční sledování.

Rovněž požadavek na kapacitu ovládacího zařízení by měl korespondovat s cílovým stavem pokrytí rizikových oblastí ve městě pomocí CCTV. Výhodou je nabídka modulové konstrukce ovládacího zařízení.

4.4.3 Záznamové zařízení

Zde se mohou vyskytnout odlišná technická řešení. Tato zařízení prožívají dynamický vývoj zvláště v oblasti digitálního záznamu. Připustíme provoz CCTV po omezenou dobu se zařízením, které poněkud degraduje parametry všech předcházejících prvků v systému, a zvolíme možnost multiplexního analogového záznamu na time-Lapse videomagnetofon s omezenou rozlišovací schopností (VHS černobílý 300 řádků, v barvě dokonce jen 240 řádků!). V následující etapě doplníme systém o dokonalejší, digitální záznam.

Využití time-lapse videorekordérů je běžné pro více kamerový záznam. S pomocí multiplexeru zaznamenávají až 16 obrazů v černobílém nebo barevném provedení na běžné videokazetě. Prohlížet se dá buď jediný obrázek, nebo můžeme rozčlenit monitor na několik polí, z nichž každé bude zobrazovat pohled jiné kamery. Frekvence, s níž budou obrazy zaznamenávány, se liší podle počtu kamer a podle rychlosti posuvu pásky. Pro představu je čas prodlevy mezi jednotlivými snímky (mrtvý čas) uveden v následující tabulce.

Tab. 6. Mrtvé časy v závislosti na počtu kamer a nastaveném režimu záznamu

Počet kamer	**Režim záznamu**			
	Standardní - 3 hodiny	8 hodin	12 hodin	24 hodin
8	0,24 s	0,64 s	0,96 s	1,92 s
16	0,48 s	1,28 s	1,92 s	3,84 s

K přehrávání musíme mít druhý nezávislý videomagnetofon stejného typu a monitor, abychom nemuseli při prohlížení archivu přerušit aktuální záznam. Při aplikaci time-Lapse videorekordérů je podstatná volba vhodných pásků, neboť při time-Iapse záznamu je pásek extrémně mechanicky namáhán. Použití nevhodných pásků způsobí horší kvalitu záznamu a nebo může poškozovat hlavy videorekordéru. Pro operativní nasazení je někdy vhodné zařazení videotiskárny. Tyto tiskárny mohou vytvářet barevné nebo černobílé snímky, které lze využívat jako trvalý záznam nebo lépe jako operativní prostředek k předávání informací důležitým zdrojům (např. policii). U digitálních záznamových zařízení může tuto úlohu převzít PC tiskárna.

Při stanovení požadavků na vybavení záznamového zařízení je nutno opět uvažovat o cílovém stavu rozsahu CCTV. Požadavek na dobu archivace by měl vycházet z reálného režimu provozu monitorovacího pracoviště a z "hodnoty" záznamu rizikové události. Jeho hodnota logicky s časem klesá a záznam by měl sloužit prioritně pro okamžitou analýzu situace a přijetí optimálního opatření během několika dnů. Je to zvažování prakticky využitelné doby archivace v rozumném ekonomickém rámci. U digitálních záznamových zařízení lze obvykle kapacitu paměti postupně rozšiřovat pomocí např. diskových polí, připojení externích paměťových médií (např. VXA mechaniky, DAT kazetopáskové jednotky, magnetooptický disk apod.).

Obr. 12. Záznamové zařízení

Požadavek na minimální rozlišovací schopnosti záznamu (min. 400 televizních řádků) souvisí s požadovanou "frekvencí vzorkování" - to je počet snímků od každé kamery za sekundu. Tento požadavek má rovněž souvislost s požadovanou kapacitou záznamového zařízení. V každém případě by minimální rozlišovací schopnost záznamového zařízení měla být stejná nebo vyšší než u celého systému od kamery přes přenosové trasy až k zobrazovacímu zařízení. Zvláště v počátcích bychom měli klást důraz na systematičnost práce se záznamem vytvoření pravidel pro archivaci, přepisování dat, na práci s daty vůbec včetně selektivních přístupových práv i na vytvoření přiměřené ochrany poměrně citlivých informací a v každém případě vytvořit systémová opatření proti zneužití těchto informací ve vztahu k platné legislativě na ochranu osobních údajů.

5 ZKOUŠENÍ A CERTIFIKACE KOMPONENTU

Jedním z důležitých předpokladů kvalitní funkce kamerového komplexu je dobrá úroveň zkušebnictví a certifikace v obecné rovině. Právě pochopení a posléze využití výsledků zkoušek a certifikace je totiž rozhodující pro kvalifikované a odpovědné zajištění majetku a zdraví, kam funkce CCTV jednoznačně patří.

5.1 Standardy v Evropě a prozatímní problémy v ČR

Ve všech vyspělých státech je hodnocením technické úrovně výrobku pověřena státní či státem pověřená instituce, která není a nesmí být zainteresována na obratu prodeje výrobku. Ta samozřejmě musí zaručit tři základní atributy zkušebnictví, praktikované v zemích Evropského společenství - nestrannost, objektivnost a opakovatelnost. Metodika hodnocení přesně vymezuje, do které bezpečnostní (rizikové) kategorie je výrobek na základě zkoušek zařazen. Jen tak je možné spotřebiteli nabídnout kvalitu a odpovídající stupeň bezpečnosti.

Důležitým počinem v oblasti zkušebnictví a certifikace bylo ustanovení Technické normalizační komise č. 124 s názvem "Elektrická požární a zabezpečovací signalizace", jejím cílem je vytvoření optimální soustavy českých norem nového typu, založených na principech účelné harmonizace s obdobnými mezinárodními a evropskými normami. Komisi zřídil Český normalizační institut. Pro správnou informovanost širokých vrstev potenciálních zákazníků je řešením vydávání objektivních seznamů a doporučení certifikovaných výrobků.

5.2 Obsah, způsob a rozsah zkoušení

Hlavním cílem zkoušek je ověření kvality systému, která je dána parametry, funkčními a uživatelskými vlastnostmi systémů a jejich komponent, a porovnání zjištěných výsledků s požadavky u nás platných standardů a směrnic. Ověření kvality zařízení jsou u nás oprávněny provádět akreditované zkušební laboratoře, jejichž ověřené metodické postupy by měly poskytovat záruku seriozních výsledků zkoušek. V oblasti standardizace se problematikou zabezpečovacích technologií zabývá Technický výbor TC 79 při evropské komisi CENELEC, jehož členem je i Česká republika. Z tohoto členství pro nás vyplývá povinnost zavádět do našich systémů ČSN i ty standardy, které zpracovává tato organizace. To znamená postupný přechod na

evropské standardy. Požadavky na systémy CCTV jsou uvedeny ve standardech skupiny EN 50 132. Na popsané situaci ve standardizaci je přímo závislá oblast jejich zkoušení a hodnocení. Zkušební laboratoře musí vycházet z uvedených norem a dokumentů při tvorbě svých metodických postupů pro ověřování těchto systémů.

V rámci ověřování systémů CCTV se provádějí zkoušky všech jejich komponentů. Jedná se například o kamery včetně objektivů, monitory, řídící jednotky (kvadrátory, přepínače, multiplexery, videoústředny atd.), kryty kamer (venkovní s vytápěním), otočné hlavice, infrareflektory, vyhodnocovací jednotky a záznamová zařízení.

Velmi důležité je ověřování jejich spolehlivosti a odolnosti proti vnějším vlivům. Na jednotlivé typy systémů působí vlivy různě. Opomenutí ověření spolehlivých parametrů může vést při konkrétní instalaci ke znehodnocení celého systému, a to z důvodu výskytu velkého množství neidentifikovatelných poplachů, případně naopak ke znecitlivění části systému.

Zkoušky jsou prováděny podle akreditovaných (metodicky definovaných) postupů a jsou rozděleny do několika oblastí podle charakteru testované veličiny. Rozsah zkoušek tak obsahuje všeobecné zkoušky (zejména posouzení obecných požadavků na výrobek a jeho provedení, kontrola úplnosti údajů o zkoušeném výrobku a posouzení průvodní dokumentace z hlediska jejího obsahu a úplnosti), zkoušky elektrických veličin (vyjímáme např. ověření funkce při mezních napájecích napětích, ověření funkce při kolísání a krátkých přerušeních napájecího napětí, odolnost proti přepólování, zkratu či přetížení napájecího zdroje, ochranu výstupů proti přepětí, kontrolu velikosti zvlnění zdroje a ověření funkce dobíjení náhradního zdroje).

Dále jsou prováděny výchozí revize (mimo jiné jde o měření izolačního odporu a zkoušku přechodových odporů), ověřování funkčních a provozních vlastností (sem lze zařadit např. kontrolu plnění požadavků norem na funkční vlastnosti systémů, ověření parametrů výrobku udaných výrobcem v jeho technickém popisu, ověření odolnosti výrobku proti vnějším provozním vlivům a zkoušku spolehlivosti zařízení).

Jednou z velmi náročných zkoušek je zkouška spolehlivosti. Ověřuje se reakce systému na různé vlivy okolního prostředí a zjišťují se slabá místa systému. Zkoušky probíhají v laboratořích a jejich podstatná část v reálném nasazení, na zkušebním polygonu nebo přímo na instalaci na reálném objektu. Na výsledky takovýchto zkoušek se klade velký důraz

Na zkušebním polygonu se mimo jiné ověřuje možnost překonání systému. Důležité je také ověřování spolehlivosti systémů v rámci zkušebního provozu, kdy se provádí zejména ověření pracovních podmínek systému a nastavení jeho parametrů v závislosti na prostředí jeho nasazení a vhodnost provedené instalace s ohledem na princip systému.

Velmi důležitou zkouškou je prověření elektromagnetické kompatibility. V rámci těchto zkoušek se ověřuje například odolnost zařízení proti elektrostatickým výbojům, proti rušení elektromagnetickým polem, proti poruchám indukovaným do přívodních kabelů, činnost zařízení při poklesech a přerušení napájecího napětí, při změně napájecího napětí a ověření hodnot rušení elektromagnetickým polem vysílaným zkoušeným zařízením do sítě a do volného prostoru. K důležitým způsobům prověřování patří klimaticko-mechanické zkoušky. Při nich se ověřuje například činnost CCTV při nízké a vysoké okolní teplotě, při teplotních změnách, odolnost proti mechanickým rázům, proti vibracím, proti vnějším klimatickým vlivům jako je prach, déšť, slaná voda.

5.3 Akreditované zkušebny

Jejich hlavní náplní je zkoušení prvků a systémů EZS podle schválených metodik, které již předpokládají kompatibilitu s normami EU. Obsah a rozsah zkoušek je vždy uveden ve zkušebním protokolu každé akreditované zkušebny včetně použitých norem a metodik zkoušení. Obecně jde o zkoušky zařízení elektrické požární a zabezpečovací signalizace, elektromagnetické kompatibility, elektrické bezpečnosti, uzavřených televizních systémů, systémů kontroly vstupu, kontrolu parametrů výrobků při působení klimatických a mechanických vlivů.

Přezkoušení výrobku neboli zjištění shody s technickými předpisy provádějí akreditované zkušební laboratoře na základě osvědčení o akreditaci, vydávaného Českým institutem pro akreditaci. Tato osvědčení jsou vydávána na určenou dobu po splnění akreditačních kritérií podle *ČSN* EN 45 001 a po zjištění, že zkušební laboratoř je odborně způsobilá objektivně a nezávisle vykonávat zkoušky v rozsahu předmětu akreditace.

Výsledkem práce zkušební laboratoře je protokol o zkoušce (stanovuje, zda přezkoušený výrobek odpovídá předložené technické dokumentaci).

5.4 Certifikační orgány

Vyšším stupněm je v oboru EZS provádění certifikace výrobku, při němž je na základě předchozích zkoušek produkt zařazen do určité kategorie či bezpečnostní třídy. Provádí ji certifikační orgán, který je akreditován k této činnosti dle ČSN EN 45011. Pro obor EZS je velmi důležitá nová norma *ČSN* EN 50131-1 (Poplachové systémy - Elektrické zabezpečovací systémy uvnitř a vně budov; Část 1: všeobecné podmínky, které plně odpovídají evropským normám. Norma zavádí nový pojem "stupně zabezpečení" a předpokládá celkem čtyři stupně rizik, přičemž stupeň 1 je nejnižším, základním stupněm a stupeň 4 představuje nejvyšší rizika

1- *stupeň* - nízké riziko
2- stupeň - nízké až střední riziko
3- stupeň - střední až vysoké
4- stupeň - vysoké riziko

V nadstavbě zkušebnictví, tedy v certifikaci, existují pro oblast poplachových systémů zatím dva certifikační orgány. Jednak jde o Certifikační institut České asociace pojišťoven, jednak o Certifikační orgán poplachových systémů VTÚE.

Pro certifikaci výrobků z oboru CCTV nejsou v rámci evropských norem stanoveny žádné kategorie či stupně zabezpečení. Bohužel zde neexistuje opora v oblasti normalizace a nelze tedy ani při certifikaci komponentů CCTV stanovovat jakékoli stupně zabezpečení (popř. kategorie), tak jak je to obvyklé u prvků pro EZS.

Přesto však můžeme alespoň rámcově posoudit úroveň rizik vztahujících se k objektu a režimu provozu budoucího systému CCTV. Výběr techniky, výbavy doplňkovými funkcemi a způsob montáže zpravidla odpovídá konkrétní úrovni rizik. Běžné provozní monitorování lze zařadit do úrovně 1 (standardní aplikace). Úroveň 2 v sobě zahrnuje bezpečnostní aspekt využití CCTV (střední úroveň rizik). Objekty, kde je CCTV využit v rámci integrovaného bezpečnostního systému spolu s EZS, elektrickou požární signalizací (dále jen EPS), s kartovými systémy, popř. kde plní CCTV sama o sobě určitou střežící úlohu, spadají do vysokých rizik ohrožení - úroveň 3.

5.5 Národní bezpečnostní úřad

Důležitou roli v oblasti certifikace sehrává Národní bezpečnostní úřad (dále jen NBÚ). Ten vznikl na základě zákona č. 148/1998 Sb., O ochraně utajovaných skutečností a o změně některých předpisů, ve znění zákona č. 164/1999 Sb. NBÚ je ústředním celostátním správním úřadem. Zákonodárce mu přisoudil oblast ochrany utajovaných skutečností. V rámci zásad činnosti ústředních orgánů státní správy plní v oblasti utajovaných skutečností mimo jiné úkoly, které souvisejí s pravidly pro zabezpečení objektů.

K důležitým vyhláškám, kterými se provádějí jednotlivá ustanovení popisovaného zákona, patří zejména vyhláška NBÚ č. 12/1999 Sb., o zajištění technické bezpečnosti utajovaných skutečností a certifikaci technických prostředků, ve znění vyhlášky Českého národního bezpečnostního úřadu (dále jen ČNBÚ) č. 337/1.999 Sb. a vyhláška NBÚ č. 339/ 1999 Sb., o objektové bezpečnosti. Pro oblast CCTV jsou velmi praktická ustanovení, která se zařazují mezi technické prostředky i speciální televizní systémy pro snímání, přenos a zobrazování pohybu osob a dopravních prostředků v objektech. Je podstatné, že NBÚ provádí certifikaci technických prostředků na základě předložení výsledků měření a posudku podle zmíněné nové normy ČSN EN 50131-1 a její národní přílohy, vystaveného některou z akreditovaných zkušeben. NBÚ přitom postupuje podle uvedených vyhlášek.

Technické prostředky se podle stupně utajení utajovaných skutečností, k jejichž ochraně se používají, zařazují do těchto kategorií:

- "V" - technické prostředky k ochraně utajovaných skutečností stupně utajení "Vyhrazené"
- "D" - technické prostředky k ochraně utajovaných skutečností stupně utajení "Důvěrné"
- "T" - technické prostředky k ochraně utajovaných skutečností stupně utajení "Tajné"
- "PT" - technické prostředky k ochraně utajovaných skutečností stupně utajení "Přísně tajné"

Stupeň PT je stupněm nejvyšším. Jednotlivé prostředky se při certifikaci zařazují do příslušné kategorie. Vlastní certifikát obsahuje - identifikační číslo certifikátu technického prostředku, jednoznačné typové určení prostředku, údaje o výrobci technického prostředku, údaje o držiteli certifikátu technického prostředku, stupeň utajení, pro který byla schválena způsobilost technického prostředku, dobu platnosti a datum vydání certifikátu technického prostředku.

5.6 Seznamy zkoušených a certifikovaných komponent

V současné době je nejrozšířenější formou dosažení relevantních výsledků certifikačního procesu prostřednictvím seznamů, zveřejňovaných na internetových stránkách. Certifikát, který potvrzuje a schvaluje způsobilost technického prostředku pro použití k ochraně utajovaných skutečností a přisuzuje stupeň utajení. Mimo tento způsob vydává NBÚ pro veřejnost periodickou publikaci - věstník, který kromě řady důležitých informací z oblasti utajovaných skutečností obsahuje i seznamy certifikovaných výrobků.

Ale jsou i jiné informační kanály pro šíření takovýchto seznamů. Aktuálními seznamy disponují dále policejní preventisté na jednotlivých PIS nebo v policejních poradenských místech pro veřejnost v rámci okresních ředitelství Policie ČR. Tyto seznamy by měly být samozřejmě dostupné na přepážkách jednotlivých pojišťovacích subjektů.

6 APLIKACE PŘI VYUŽITÍ KAMEROVÝCH SYSTÉMŮ

Kamerové systémy dnes mohou uživatelé využívat se značným komfortem a použít se dají v rozmanitých oblastech – průmyslu, v měřící technice, dopravě, ve zdravotnictví, školství,… Zkrátka všude tam, kde je obtížně sledování průběhu člověkem (zdraví škodlivé prostředí, nepřetržitý dohled,…). Existuje mnoho příležitostí, kde s důvodů ekonomických nebo praktických, lze takovou technologii uplatnit (dohled v parcích, dálnicích, …) kde monitoring těchto oblastí nelze efektivně zajistit přítomností člověka. Videomonitorování nesmí být chápáno jako technologie snižující náklady související s pracovní silou, nýbrž díky němu lze i optimalizovat dostupně lidské zdroje. Tyto systémy mají po nainstalování tzv. presence effect – elektronické oči, které jsou kdykoliv k dispozici a umožňují rychlejší bezpečnější a mnohem efektivnější reakci. Soubor je složen z pohyblivých nebo pevných kamer, které posílají signál do řídícího centra. Všechny funkce kamer jako ZOOM, ostření a rotace lze odtud bez problémů řídit. Hlavní částí systémů je CODEC, který zprostředkuje propojení řídícího centra s kamerou pro přenosové rychlosti od 64 – 384 Kb dle typu. Možno použít rozhraní X.21, V.35, G 703 či RF 449. Codec může být přímo připojen až ke 4 kamerám. Počet kamer lze rozšířit až na 32 pro jeden CODEC použitím další přípravně videomatrice. Uvedená zařízení nalézají největší uplatnění v různých oblastech - monitoring zdrojů pitné vody (přehrady a okolí), monitoring nebezpečných provozů (elektrárny, chemické továrny, vojenské sklady, apod.) nebo monitoring parků, ulic, tunelů, hraničních přechodů, dálnic či železnic.

Zajímavé aplikace nabízí systém v bankovním sektoru. Hlavní rozdíl oproti stávajícím systémům, je v tom že videorekordér není umístěn na pobočce, kde se záznam může znehodnotit (zničit, ztratit), ale je ve vzdáleném řídícím centru. Systém je možné provázat se zabezpečovacím systémem a nabízí dvě velké výhody:

1. Osoba z jednoho řídícího centra může provádět rutinní kontrolu periodickým voláním různých poboček banky.
2. Pokud je aktivován jakýkoliv způsobem alarm, dojde k automatickému volání do řídícího centra a navázání spojení.

K dalším unikátním bezpečnostním prvkům charakterizujícím tento systém patří například odmítnutí příchozích hovorů od neautorizovaných čísel, videozáznam těsně před alarmem a po alarmu na tzv. memory card, automatické testování linky, kompletní dálkové ovládání

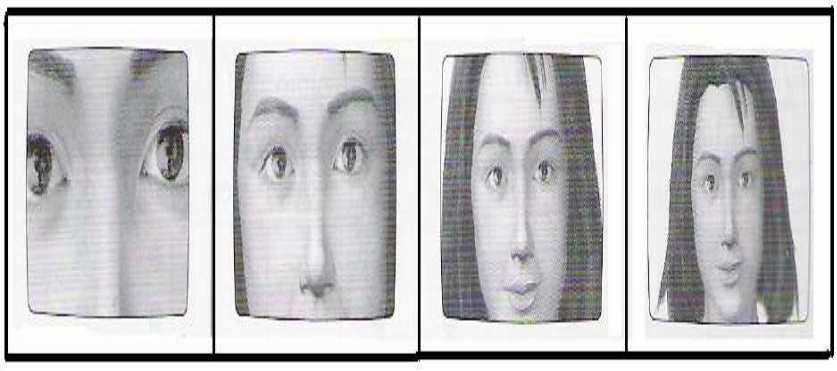
jednotlivých kamer a možnost konfigurace externích zařízení pro zapínání nebo vypínání světla, otvírání nebo zavírání brány apod.

6.1 Biometrie a videoanalýza

S rostoucím využíváním výpočetní techniky v oblasti identifikace osob a bezpečnostních technik získávají na významu inteligentní kontrolní přístupové systémy. Skutečná identita a autentičnost osob není při běžných způsobech identifikace zcela garantována. Takové systémy nezabrání použití zcizeného klíče, násilím vynucené informace o tajném kódu nebo zcizení karty a průkazu, které mohou přijít do nesprávných rukou a být použity pro falešnou identifikaci.

Stále širší pole působnosti proto v oblasti zabezpečovacích zařízení v současné době získává inteligentní videoanalýza. Biometrické systémy kontroly přístupu jsou již několik let úspěšně v provozu po celém světě. Biometrie jako klíčová technologie získává stále více na významu. Její základní myšlenkou je využívat nejenom průkazné fyzikální identifikační metody, ale současně i vlastní tělesná specifika (obličej, oční sítnice, geometrie ruky, otisk prstů, hlas aj.), která jsou ojedinělá a nezaměnitelná. Tato specifika musí být taková, aby každá osoba disponovala rozdílnými údaji a dovolovala tak jednoznačnou identifikaci.

Nová generace "obličejové biometrie" dokáže však obličeje nejen verifikovat, ale i automaticky vybrat ze sekvence videosnímků. Důležitou schopností je též spolehlivé rozpoznání živých tváří a jejich odlišení od neživých. Tím dochází k výraznému zvýšení bezpečnosti, komfortu, obsluhy zařízení.



Obr. 13. Biometrie lidského obličeje

6.1.1 Požadavky na biometrii

Mezi základní požadavky můžeme zařadit:

A) Vysoká kvalita rozlišení – stanovuje se pomocí faktoru FAR (False Acceptance Rate), chyba akceptování osoby a FRR (False Rejection Rate) – chyba odmítnutí osoby. Ideální systém by měl splňovat FAR = FRR = 0. Vzhledem k tomu, že biometrické systémy snímají vždy senzorická, a tudíž na okolí závislá data, je určitá zvyková chyba v praxi nevyhnutelná

B) Jistota před oklamáním systému – dnes je relativně snadné vytvořit falsifikát otisku prstů z latexových materiálů nebo masku obličeje. Některé systémy pro rozpoznání obličeje lze přelstít předloženou fotografií. Ale vůbec nebo jen se značnou námahou lze vytvořit napodobeniny některých biometrických znaků. Systém musí rozpoznat a identifikovat osobu i při změněné image, při jiném pohledu snímku nebo při jiné velikosti snímku.

C) Komfort obsluhy – zde vyniká metoda rozpoznání obličeje oproti ostatním, neboť snímá biometrický znak bez dotykově, aniž by musela kontrolovaná osoba např. uvolňovat či obnažit ruce, obličej je systémem rozpoznán automaticky v okamžiku kdy se nachází před kamerou ve vhodné pozici (face – spotting).

Spojení výhod biometrických verifikačních metod a video analýzy využívá zařízení používána k plně automatickému rozlišení obličeje pro účely identifikace osob při kontrole vstupu do objektu, při vydávání hotovostních finančních obnosů, při přístupu do přísně střežených a utajovaných míst nebo při „login“ do PC. Některá zařízení obličejové biometrie umožňují překládat vedle vlastní identifikace osob také obrazové protokoly všech přístupových míst, do nichž je možné pohodlně nahlédnout na serveru a které lze třeba vytisknout, poslat po síti,… Zejména při neoprávněných pokusech proniknout do neoprávněných prostor lze snadněji zjistit identitu osob pomocí uložených obličejových snímků. To je zcela nový aspekt, který biometrická metoda rozpoznání obličeje přináší oproti jiným metodám (otisk prstů, rozpoznání ruky, sítnice oka, pohyb rtů,…). Jde o metodu bezdotykovou a rychlou, která kontrolovanou osobu neobtěžuje. Pracuje na bázni neuronálních sítí. Neuronální sítě jsou robustní výkonné algoritmy, které se snaží napodobovat činnost mozku a mají k tomu odpovídající schopnost učit se. Tím lze dosáhnout vysoké spolehlivost rozpoznání (chyba FAR / FRR = 0,5%). Systém vyhodnocení pracuje na principu síťových grafů, takže dokáže rozpoznat identifikovanou osobu i při změněném image, při jiném pohledu, nebo při jiné velikosti snímku.

Běžným jevem je, že systém spolehlivě rozpozná osobu při nasazení či odstranění brýlí, při změně účesu,… Takový kompletní systém se stává z verifikační stojanové konzoly s integrovanou kamerou počítačové jednotky a verifikačního softwaru. Ergonomie stojanu zaručuje jistá pohodlné snímání osob různého vzrůstu. Na základě požadavků lze do stojanu integrovat počítačovou jednotku a tím ji ochránit před zásahy z venku. Software se stává z modulových částí. Systém může pracovat jak jako samostatné „standalone“ zařízení tak v počítačové síti jako server s více verifikačními stanicemi. Verifikace osoby je velmi rychlá, trvá maximálně 1 sec.

Další inovační novinkou je tzv. Live-Check – pro snímání obličeje z dynamické videosekvence. Nesnímá již jednotlivý obraz obličeje, ale analyzuje sekvenci snímků z videokamery s četností 12 až 16 snímků / sec. Doplňuje tedy verifikaci obličeje pomocí analýzy pohybu. Rychlým zpracováním obrazu je pak možno:

- Rozeznat a vybrat okamžik, kdy se obličej nachází ve vhodné pozici před kamerou (Face – Spotting).

- Zjistit, zda se jedná o živý obličej (Live – Check). K tomu jsou analyzovány pohyby obličeje. Jedná-li se pouze o pohyby celého obličeje, tak jak by bylo možné např. při předsunutí fotografie či 3 – D masky, není snímek akceptován. Teprve při zjištění jemných intrinsických pohybů uvnitř obličeje (mimika, pohyb rtů, pohyb očních partií) je obraz akceptován jako živý a je povoleno jeho další zpracování.

Aby bylo možné takovéto jemné intrinsické pohyby rozpoznat, je nutno nejprve identifikovat mnohem větší celkové pohyby obličeje a ty ze snímku vyloučit. Teprve potom lze spolehlivě nalézt intrinsické pohyby které fotografie anebo 3 – D maska nemůže předvádět ani předstírat.

Hlavním kladem této nové metody je schopnost vyřešit tento úkol spolehlivě a rychle. Tím bylo dosaženo zlepšení všech požadovaných kritérií na biometrii

- Dynamické sledování a vyhledání obličeje dovoluje pro účastníky akceptovatelnější bezdotykovou biometrii.
- Lépe normovaný snímek obličeje pomocí Face - Spotting činí systém spolehlivějším a snižuje omyly typu **FRR.**
- Inovační novinka Live-Check vytváří pomocí analýzy pohybu přesvědčivou odolnost systému proti oklamání.

Rozpoznání podle oční duhovky je rychlá, přesná a bezpečná metoda. Jedinečné vzorce v lidské duhovce jsou stabilizovány během jednoho roku od narození a zůstávají během lidského života neměnitelné. Vzorec duhovky je mnohem individuálnější než otisk prstu, takže je to perfektní kritérium pro identifikaci.

Neopakovatelný vzorec duhovky nelze napodobit žádnou známou technologií. Používání je pohodlné, rychlé a prováděné bezkontaktními metodami. Není vyžadován žádný fyzický kontakt mezi duhovkou a kamerou, uživatel se prostě dívá do kamerové čočky ze vzdálenosti 10 až 15 cm. Proces snímání dát je podobný, jako když je užívána standardní video kamera. Identifikace může být provedena během 1 až 2 sekund (s vyhledáváním v databázi *4000* souborů). Přihlášení může být dokončeno v cca 30 sekundách.

6.2 Možné aplikace

Využívají se v rámci systému kontroly přístupu - pro zabránění rizik ztráty karet, zapomenutí hesla a pro kontrolu omezených vstupních/výstupních oblastí (úřady vlády, objekty elektráren, letecké kontrolní věže atd.) nebo v počítačovém bezpečnostním systému pro zvýšení bezpečnosti a zabránění neoprávněnému přístupu. Je to náhrada nebo dodatečná ochrana před zneužitím metod založených na vlastnictví (např. karty, klíče) a znalostech (např. hesla, PIN). Jako další aplikace lze uvést bankomaty, prodej jízdenek či letenek, jiná prodejní místa, hraniční kontroly anebo transakce kreditních karet.

Biometrické technologie poskytují automatizovaný způsob zjištění nebo ověření identity žijící osoby na základě měřitelných a nezaměnitelných fyziologických charakteristik.

6.2.1 Venkovní videodetektory

V běžných aplikacích se používají kamery pouze pro sledování prostoru, který je zabezpečen jiným elektronickým zabezpečovacím zařízením. Funkce spočívá pouze v ověření příčiny poplachu, ať již jsou kamery umístěny v místnostech, nebo ve venkovním prostředí. S použitím videodetektoru pohybu lze pomocí běžných kamer a videosystémem nahradit klasický zabezpečovací systém. Plochu obrazu lze rozdělit na 64 detekčních polí, přičemž u každého můžeme nezávisle definovat velikost, polohu a citlivost. Nezanedbatelnou výhodou je možnost získání vizuální informace při narušení objektu. A to nejen živého obrazu, ale díky vestavěné videopaměti i snímků předpoplachovým a také snímkům zachycujícím průběh poplachu.

Uvedené podrobnosti jsou velmi důležitými informacemi pro zvolení taktiky, postupu a nasazení zákrskové jednotky. Systém musí spolehlivě odlišit příchod zloděje od náhodné změny kontrastu způsobené přechodem mraku po obloze, pohybem větví stromů ve větru, pohybem malých zvířat a ostatními nepodstatnými příčinami.

Aby videodetektor fungoval ve venkovním prostředí spolehlivě a bez falešných poplachů, je nutno zvážit řadu faktorů.

Mezi nejdůležitější faktory, které ovlivňují spolehlivost detekce a vyloučení falešných poplachů patří zejména:

- Počet citlivých zón na jednu kameru, jichž by mělo být minimálně 20.
- Možnost volby velikosti jednotlivých zón.
- Možnost volného rozmístění detekčních zón v ploše obrazu, s možností vytvářet virtuální perspektivu.
- Délka měřícího cyklu - nezbytně nutné je, aby byl detektor schopen porovnávat snímky s prodlevou řádu desetiny sekundy, ideálně až živý signál (40msec).
- Počet měřících cyklů - protože je potřeba detekovat pohyby o různé rychlosti, musí detektor používat více měřících cyklů.
- Logické vazby mezi zónami, které umožňují rozlišovat směr průchodu a způsobovat podmíněný poplach, vyvolat nejprve předpoplach atd.
- Schopnost eliminace venkovních vlivů - tento poslední parametr hraje klíčovou roli při výběru detektoru. Detektor bez této funkce bude způsobovat falešné poplachy několikrát denně při východu slunce, při příchodu mraku, při průjezdu auta v noci apod. Je pochopitelné že takovéto zařízení nelze použít pro zabezpečení.

6.2.2 Eliminace falešných poplachů vlivem počasí

Videodektor musí bezproblémově pracovat v jakémkoliv počasí. Proto je využíván speciální vyhodnocovací algoritmus, který odliší globální změny kontrastu způsobené chvěním kamery ve větru, deštěm, mraky a jinými povětrnostními vlivy od lokalizovaného pohybu způsobeného pohybem člověka. Falešné poplachy způsobené vlivem počasí jsou tímto způsobem velmi spolehlivě potlačeny.

6.2.3 Povolený a zakázaný pohyb

V zorném poli kamer se často nacházejí taková místa, kde je pohyb normálním jevem. Jde například o kamery, které sledují vjezd do objektu s automaticky se otevírající bránou nebo závorou či kamery, jejichž výhled je směrován na silnici, po které jezdí vozidla. Kvalitní videodetektory rozliší různě veliké objekty pohybující se rozdílnou rychlostí různými směry.

Obr. 14. Monitorovací bod křižovatky tř. T. Bati a ulice Školní

S použitím extrémně rychlého videodetektoru pohybu rozhodně nedojde k promeškání žádného kritického okamžiku. Některé z výrobků dokáží porovnat dva po sobě jdoucí snímky za pouhých 40 milisekund, bez ohledu na počet připojených kamer. Tato rychlost je dána tím; že detektor neprovádí digitalizaci celého obrazu, ale analyzuje pouze změny v zónách, které nás zajímají, a také tím, že deska pro každou kameru obsahuje svůj vlastní procesor a proto není ovlivňována děním na jiných kamerách.

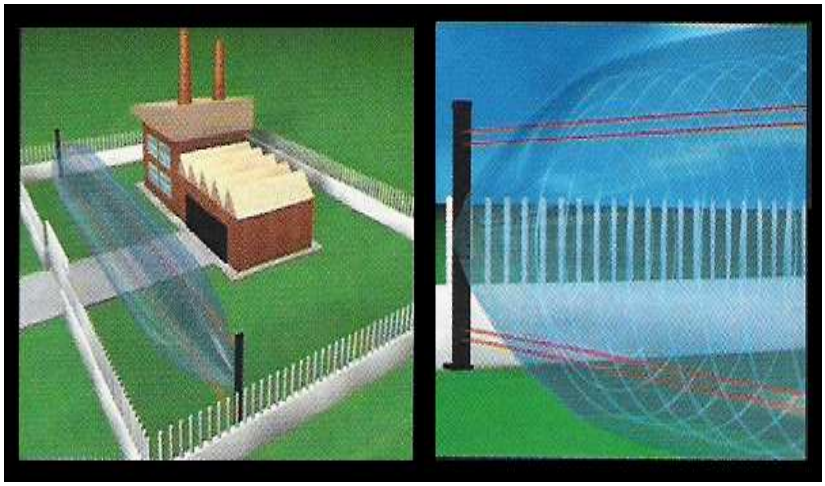
6.2.4 Systémové možnosti

Detektor lze velmi jednoduše zařadit do stávajícího CCTV systému - deska pro každou kameru má svůj vlastní videovstup i výstup. Kromě video výstupů na jednotlivých kamerových deskách bývá k dispozici několik systémových video výstupů, díky kterým jej lze použít také jako malou videomatici. Videodetektor disponuje datovými sběrnicemi, které umožňují jeho

bezproblémovou integraci do větších systémů. Z hlediska kladného hodnocení je jednoduchý přenosový protokol možno lehce integrovat do jiných systémů. Další nezbytnou součástí každého videosystému je záznamové zařízení. Často je potřeba provádět monitorování vzdálených objektů a použít zařízení pro přenos videosignálu po globální sítích.

6.2.5 Detekce pohybu

V některých aplikacích může být integrován detektor pohybu. Pomocí detekce aktivity lze střežit objekt, místnosti a nebo jednotlivé předměty v nich. Místo, které monitoruje kamera, je rozděleno do 192 čtverců. Z těchto čtverců lze pomocí šipek zadat jak jedno, tak všechna pole. Tam, kde jsou ponechány čtverce, je střežená zóna, a pokud je narušena, spustí se alarm. Forma oznámení se zadá v příslušném menu. Nabídka je široká, menu nabízí např. tón bzučáku, sepnutí alarmových kontaktů, případně sepnutí poplachové smyčky zabezpečovací ústředny. Další výhodou popisované možnosti je, že multiplexer, který zajišťuje nahrávání sledu událostí v případě alarmu, přepne způsob nahrávání do reálného času po dobu stanovenou uživatelem. Výsledkem je, že poplachové stavy jsou zaznamenávány ve vyšší kvalitě, s kratšími intervaly mezi jednotlivými snímky.



Obr. 15. Virtuální návrh střežení objektu pomocí CCTV

6.3 Sledování a řízení dopravy

Nejvíce je kamer využíváno v silniční dopravě, ke kontrole tunelů, dálnic, důležitých a z hlediska městského provozu nejkonfliktnějších křižovatek. Technika dovoluje měřit dopravní zátěž, rychlost a hustotu provozu.

Obrázky z kamer slouží i v případě vyšetřování dopravních nehod a hledání jejich viníka. Počítačové řízení může navrhovat objízdné trasy při haváriích, při opravách, rekonstrukcích a údržbových pracích na komunikacích.

Obr. 16. Monitorovací bod č. 4 – křižovatka ul. Štefánikova a ul. Gahurva, nám. T. G. M. – sloup trakčního vedení

Automatické kamery mohou pohlídat místo lidských sil i neukázněné řidiče, kteří porušují zvlášť závažným způsobem pravidla silničního provozu - projíždějí křižovatkou na červený signál. Celou sestavu tvoří dvě kamery k zachycení přestupce z obou stran - zepředu i zezadu. Jsou spouštěny speciálním spínačem, jenž je umístěn pod vozovkou. Při průjezdu vozidla na červenou se celá elektronika "rozběhne" a auto je zachyceno na třech fotografiích. K dalšímu řízení jsou snímky automaticky doplněny o důležité údaje:

- Místo, křižovatka.
- Druh přestupku.
- Datum a čas přestupku.
- SPZ.

6.4 Kamery ve školách reagují na zvyšující se násilí

V Anglii a v USA po nedávných krvavých scénách, kdy děti vraždily své kamarády střelnými zbraněmi v době školního vyučování, přistoupili tamní odpovědní pracovníci k instalacím kamerových monitorovacích systémů do škol. Kamery zde mají preventivní i represivní charakter. Monitorováno je okolí školy, vstupy do budov, chodby i některé učebny. Systém je propojen se selektivní kontrolou vstupu dětí a dalších osob přicházejících do škol (karetní nebo jiné systémy, identifikační rámy na kovové předměty) včetně nezbytných organizačních opatření.

6.5 Videotelefony a videovrátní

Díky technickému rozmachu a neustálému poklesu nákladů na pořízení základních komponent videotechniky lze jednotlivé prvky kamerových systémů montovat do dříve nevídaných aplikací. Princip je velmi jednoduchý. Než kdokoliv vstoupí do domu, můžeme si ho v klidu prohlédnout ze svého bytu pomocí miniaturní zabudované CCD kamery, aniž by o tom neznámý návštěvník vůbec věděl. Uvedená kamera je většinou vybavena širokoúhlým objektivem. Při montáži je důležité mít na zřeteli nutnost dostatku světla pro nepříznivé a večerní světelné podmínky. Proto jsou někdy používány i infrakamery.

Obr. 17. Konkrétní příklad videotelefonu Kanrich S- 913

6.6 Speciální použití

Kamery mají také skryté využití. K podobným účelům se vlastně používá jen část kamery, a to objektivy, tzv. PINHOLE. Jsou o velikosti špendlíkové hlavičky a ke snímaní určené scény potřebují např. pouze otvor o průměru několika milimetrů ve zdi.

7 UZAVŘENÍ SMLOUVY NA REALIZACE, VÝSTAVBU A PŘEDÁNÍ CCTV DO PROVOZU

Výstavba CCTV probíhá v několika etapách. V etapě předprojektové (zpracování výchozích bezpečnostních rozborů, zpracování zadání realizace systému, předvýběr vhodných řešitelů, vyhodnocení nabídek a výběrové řízení), v etapě projekční (zpracování projektové dokumentace - etapa probíhá i v době výstavby systému), v etapě realizace (výstavba systému, zpracování technické, průvodní a uživatelské dokumentace, zkušební provoz, kolaudace systému) a v etapě provozování (záruční a pozáruční provoz). Každá z těchto etap má velký podíl na konečném výsledku - funkčním a kvalitním CCTV. Žádnou z nich nelze podcenit.

V této části výstavby CCTV je třeba ověřit právní náležitosti návrhu smlouvy a hlavně si pohlídat soulad nabídky se specifikací ve smlouvě či příloze smlouvy. Vyplatí se uzavírat spolu se smlouvou na realizaci buď přímo servisní smlouvu, nebo mít v rámci smlouvy na realizaci zajištěny servisní podmínky v souladu s nabídkou. Podstatnou částí smlouvy musí být vyjasnění kritérií pro předání a převzetí systému uživatelem včetně metodiky objektivních testů prokazujících, že bylo dosaženo provozních požadavků zadavatele. Zde můžete opět s výhodou použít zkušební postupy s testovacím objektem ROTAKIN, specifikované v ČSN EN 50132-7.

7.1 Instalace CCTV

Před zahájením plánované instalace musí být posouzeny všechny závažné bezpečnostní požadavky. Ty se liší podle charakteru místa instalace (budovy, náměstí apod.). Elektrická instalace musí vyhovovat platným normám a musí být provedena techniky s patřičným oprávněním. Provedení instalace CCTV musí vycházet z příslušných norem. Garanci dobře provedené práce jistí například obdržený certifikát ISO 9000, získání značky - Czech Made, délka působení firmy v oboru a reference z minulých obdobných instalací. Instalace zařízení a jeho připojení musí být provedeny v souladu s doporučeními výrobce při respektování vlivu prostředí. Uzemnění musí být řešeno s ohledem na možnost zásahu bleskem a působení elektrického rušení. Dokumentace musí odrážet celý systém, počítat s jeho případným rozšířením a vyhovovat požadavkům údržby. Její rozsah je dán složitostí systému.

7.2 Předání a uvedení CCTV do provozu

Musí být provedena kontrola a test zahrnující vizuální kontrolu a kontrolu funkce všech částí instalace CCTV. Základem funkční prověrky je testovací postup odvozený z funkčních požadavků (vizuálním testem se kontroluje splnění funkčních požadavků a shoda se systémovou specifikací, funkční test zahrnuje kontrolu kompatibility komponentů instalace, kontrolní testy se provádějí na částech instalace obvykle během kompletování). Dále se musí předat potvrzení o kompletnosti uživatelské příručky, podepsat kontrolní zprávu obsahující výsledky provozního testování a předat plán údržby systému, pokud nebyla uzavřena smlouva o údržbě.

Zadavatel musí uplatnit a využít povinností, které má montážní firma v době zkušebního provozu, zejména povinnosti kvalitně zaškolit obsluhu a převzít v rámci kolaudace pouze plně odzkoušený systém, splňující všechny požadavky zadání.

7.3 Údržba systému

Údržba systému musí být prováděna periodicky v souladu s plánem. V plánu údržby musí být uvedeny speciální testovací přístroje a nástroje pro údržbu. K provádění nezbytných oprav musí být k dispozici seznam příslušných náhradních dílů. Výsledky periodických testů se musí zaznamenávat a porovnávat s testy předešlými. Údržbu a testování musí provádět pouze kvalifikovaný personál.

Pokud se provádějí úpravy instalace CCTV nebo jejich konfigurace, musí být dokumentace aktualizována a kontrolní test se musí provádět na těch částech systému, kterých se úprava týká.

8 HODNOCENÍ PROVOZU

Rozsáhlé a poctivé hodnocení a proces monitorování by měly být začleněné do nákladů a musí být přizpůsobeny specificky definovaným problémům. Hodnocení musí být založeno na výsledcích. Velmi nutné je mapovat výskyt incidentů a provádět srovnání v odpovídajících obdobích během roku. Když začne systém pracovat, měla by se získaná data rozlišovat mezi viděnými a zaznamenanými událostmi, mezi událostmi, které ležely v potenciálním dosahu kamer, ale nebyly zaznamenány, a událostmi, které byly mimo dosah kamer v obecně pokryté oblasti.

Důležité je všímat si změn ve využívání pokryté části města, protože pocit bezpečí, které nabízí CCTV může toto využívání rozšířit. Při zkoumání počtu přestupků a trestných činů se projeví změny i v počtu potenciálních obětí. Více aut na parkovištích například jednoznačně znamená více potenciálních cílů pro pachatele.

Při monitorování práce CCTV je třeba vést pečlivé záznamy. Ty by měly obsahovat datum každé významné události. Mezi významné události patří instalace hardwaru, změny hardwaru, jeho poruchy a opravy, podrobnosti v uspořádání sledování záznamu CCTV a jejich změny (počet operátoru, doba, kterou každý operátor stráví sledováním obrazovek, a manipulací s kamerami atd.), zavádění a rušení doplňkových opatření v příslušné oblasti, které mohou buď záměrně, nebo náhodně ovlivnit zločinnost.

9 ZKUŠENOSTI A DOPORUČENÍ Z VÝSTAVBY A PROVOZU CCTV

Zahraniční a tuzemské zkušenosti, které byly získány investory, dodavateli, provozovateli, policejními techniky, preventisty, manažery ze všech etap výstavby a provozu nejrůznějších aplikací kamerových systémů jsou velice cenné. Měly by být inspirací pro ty pracovníky, které výstavba CCTV teprve čeká.

9.1 Zahraniční zkušenosti se CCTV

Využívání CCTV jako technického prostředku, který umožňuje zobrazovat obrazy snímané kamerami na monitoru prostřednictvím vlastního přenosového systému k ochraně majetku a osob je velmi důležitý. Kamery se používají s velmi dobrými výsledky již několik desetiletí pro vojenské a policejní účely, k monitorování státních úřadů a institucí, letišť a přistávacích ploch, předmětů v muzeích a galeriích, k dohledu v peněžních ústavech, ve veřejné dopravě, v obchodních domech, obchodech, provozovnách,...V obytných blocích a prostorách (vchody, chodby, výtahy, sklepy apod.). Kamery a video senzory se často požívají i ve spojení s EZS. Tím získává zabezpečovací systém objektu vyšší kvalitu (poplachová signalizace, reálný obraz a dokumentace).

Velké zkušenosti z provozem kamerových systémů má Velká Británie. Kamerové systémy jsou zde budovány v centrech měst, která vykazují velké problémy se skupinami mládeže, žebráky, podnapilými osobami, kapsáři, krádežemi aut a věcmi z nich a vandalismem. Kamerové systémy plní podle britských poznatků svou funkci pouze za předpokladu, že jsou součástí celkové strategie prevence kriminality ve městě. Samotná kamerová technika strategií není. Proto je třeba nejprve jasně definovat problémy a teprve potom hledat nejvhodnější řešení, jak problémům čelit, jak je eliminovat. Kamerové systémy představují ve Velké Británii základ situační prevence kriminality. Majitelem a provozovatelem kamer je vždy příslušné město, provoz zabezpečují civilní zaměstnanci, nahrává se nepřetržitě 24 hodin a systém využívá i policie. Nahrávky jsou využívány jako důkazní materiál pro potřebu orgánů činných v trestním řízení.

Nesmí se stávat, aby osoba, která je zodpovědná za kamerový systém, byla laik, který má malou znalost o systému, o jeho provozu a vyhodnocování o spolupráci s policií a s veřejností. Systém může být efektivní pouze v případě, že zodpovědná osoba je odborníkem v oboru, nebo

je řádně vyškolena. Zodpovědný pracovník musí mít k dispozici aktuální informace, problémy promýšlet a musí být schopen pozorně a kriticky prostudovat jednotlivé systémy. Pracovník musí spolupracovat s nejrůznějšími konzultanty.

Dobré výslednosti kamerových systémů dosáhneme optimálně zřízeným a fungujícím operačním střediskem. Operační středisko bývá obvykle umístěno v budovách policie; místního úřadu nebo na jiném bezpečném místě nedaleko od centra města. Rozhodující pro činnost střediska je ergonomie jeho interiér, kvalitní operátoři a jejich motivace. Důležité je školení operátorů, které musí rozšířit a zdokonalit jak jejich technické znalosti o systému, tak i znalosti v oblasti právních a bezpečnostních dovedností. Operátoři musí být vyškoleni tak, aby dovedli zachovávat mlčenlivost. Všichni operátoři musí projít odborným školením, které provádí certifikovaná firma. Operátorovi je vystaven certifikát.

Pokud operátor zjistí podezřelé dění, má možnost si přepnout provoz příslušné kamery na speciální, monitor a s kamerou pracuje. Celý provoz je v tomto případě nahráván. Pokud operátor vyhodnotí dění na obrazovce jako závažné, spojí se přímo s policií a po projednání má možnost přepnout monitorování příslušné kamery na monitor v úřadě policie.

9.2 Nespokojenost s obrazovou produkcí

Příčin špatné kvality obrazové "produkce" je několik. Některé spadají do technické oblasti a některé souvisí s problematikou provozování CCTV. Obtížné jsou situace, kdy je systém objednán, dodán a "zapojen do akce", při níž se zjistí, že systém má nedostatky a nesplňuje očekávání.

9.3 Potřeby uživatelů obrazové produkce

Při zvažování provozních požadavků se musí vycházet z potřeb uživatelů. Jednu skupinu uživatelů obrazů představují pozorovatelé, kteří pracují s obrazovou produkcí každý den a představují integrální součást systému. Díky složitosti a množství úkolů, které se od systémů požadují se efektivita systémů mnohdy řídí podle operátora, na jehož výkon se značně spoléhá. Systémy se často rozšiřují a operátoři se mění. Způsob využívání systému je tak založen na neformálním praktickém Know how které si operátoři vzájemně předávají což může jednak vést ke značným nedostatkům systému, které nejsou zdokumentovány, ale zejména k tomu, že vlastní

funkčnost systému bude značně vzdálena očekávání vedoucích pracovníků. Tento přístup rovněž často vede k tomu, že dovednosti a zkušenosti operátora určují způsob jakým je systém využíván v kritické situaci.

Rychlý rozvoj v oblasti dohledu nad veřejnými prostorami vedl ke vzniku nové skupiny přímých nebo nepřímých uživatelů obrazové produkce. Tuto skupinu představují hlavně uživatelé z řad Policie. Dopad těchto systémů na služby poskytované policií může být značně široký. V některých systémech je pozorovatelem obrazové produkce přímo policie, v jiných systémech provádí monitorování třetí strana (nejčastěji městské policie) s tím, že výsledky jejího pozorování jsou předmětem Výstražných hlášení předávaných přímo policejní jednotce.

Druhou skupinou uživatelů mohou být vyšetřovatelé, kteří mají z obrazové produkce záznamu vyvodit určité informace a důkazy, které by jim pomohly objasnit trestný čin. Nejsou definovány výkonnostní ukazatelé založené na potřebách vyšetřovatelů, nelze očekávat, že jim systémy dají jasné odpovědi. Důležité je si uvědomit, že kritika technických nedostatků po incidentu, která je při zpětném pohledu zdánlivě na místě, není vždy oprávněná. Kritéria přijatelnosti obrazového záznamu závisí na účelu využití jednotlivých systémů. Systémy zaměřené na detekci neoprávněné osoby jsou považovány za plně efektivní a přijatelné, pokud je ze záznamu jasně zřetelná přítomnost nebo absence určité osoby. Pokud však osoba má být rozpoznána a identifikována, je nezbytné rozlišit mnohem více podrobností. Jednoduché testování výkonu může snadno ukázat, jak lze kvalitu zvýšit.

9.4 Běžné chyby zobrazení

Nejobvyklejší chyby zobrazení jsou:

- Objekty jsou příliš malé na to, aby mohly být identifikovány.
- Obrazy jsou rozostřené
- Obrazy pohybujících se objektů jsou rozmazané a nelze rozlišit detail.
- Kontrast cílového objektu je malý.
- Cílový objekt není zřetelný nebo je vidět příliš krátkou dobu nebo jej není vidět!

Často se stává, že se tyto chyby vyskytují současně.

9.4.1 Nevhodná velikost zobrazení

Velikost zobrazení je kritickým faktorem při navrhování systému, neboť určuje úsek, který budou pokrývat jednotlivé kamery, a rovněž určuje umístění kamer, jejich počet a parametry objektivů. Snaha omezit náklady často vede k příliš velkému zornému poli, protože příliš veliký, úsek je pokryt příliš malým počtem kamer. Kvalitu obrazů ovlivňuje řada faktorů, ale širokoúhlé záběry nejsou pro pozorovatele dostatečně podrobné, a tudíž jsou neefektivní. Velikost obrazu závisí především na tom, za jakým účelem je prováděno pozorování. Nelze však zavést přísná a efektivní pravidla, protože jednotlivé faktory, které mají dopad na výkon jsou propojeny, a řada z nich je velice subjektivních. Požaduje-li se detekce cílového objektu, bude prodloužen interval prohledávání díky velikosti cílových objektů, přičemž se zvýší pravděpodobnost, že cílový objekt bude "promeškán". Pro rozpoznání cíle a jeho identifikaci jsou nutné větší velikosti zobrazeného cíle.

Obr. 18. Nevhodná velikost monitorů způsobující rozostření

9.4.2 Rozostření

Rozostření je běžným rysem zobrazení. Pokud dojde na základě incidentu k analýze videonahrávky s cílem identifikovat podezřelé osoby a přitom je příslušné obrazové "zpravodajství" rozostřené, je důležité si uvědomit, že operátor si nebyl vědom toho, že určitá konkrétní osoba se měla v tu chvíli stát obětí nebo podezřelým. Problémem však je, že v případě řízení zobrazování a záznamu obsluhou nemohou operátoři často objektivně získat přiměřeně kvalitní obraz, ačkoli vynaloží maximální úsilí.

Obrazy produkované dálkově řízenými kamerami se velice obtížně zaostřují, především v noci, kdy je clona objektivu maximálně otevřená a hloubka ostrosti minimální. Čím je objektiv

důmyslnější z hlediska schopnosti zvětšit obraz (ohnisková vzdálenost) a "shromáždit" světlo (světelnost objektivu), tím více je systém závislý na dovednostech a zkušenostech obsluhy. Automatické zaostřování není vždy východiskem. Ergonomická řešení systémů na dálkové ovládání jsou často nevhodná. Někdy není jasné, jakým směrem by zaostřování mělo být nastaveno. Ovládací prvky jsou mnohdy špatně umístěny a špatně se s nimi manipuluje. Ovládací prvky pro zaostřování jsou často seřízeny nepřesně, což znemožňuje přesné nastavení. Polohovací hlavice jsou příliš rychlé a telemetrický systém reaguje pomalu, což vede k tomu, že operátor mine okamžik zaostření.

9.4.3 Rozostřování pohyblivých obrazů

Mnoho bezpečnostních incidentů zahrnuje pohyblivé cíle. Obraz vytvářený kamerami CCTV byl před pár lety snímán s expozicí přibližně 1/50 sekundy. Při běžné chůzi se během doby expozice daná osoba posune o několik centimetrů. Jednoduše řečeno, zvětšením cílového objektu se nevyrovná ztráta detailu způsobená rozostřením nebo vyvolaným pohybem. Negativní dopad lze snížit správným umístěním kamery, tak aby pohyb byl směrem ke kameře a nikoli napříč zorným polem. Alternativním řešením je použití dnes již běžných kamer s elektronicky řízenou clonou. Tyto elektronické clony/závěrky jsou nyní běžně dostupné a umožňují předem nastavit efektivní

dobu expozice v rozsahu hodnot od 1/50 do 1/2000 sekundy. Některé kamery nabízejí delší a kratší expozice pro zvláštní účely. Řada kamer nabízí výběr rychlosti automatické clony. Se změnou intenzity osvětlení dochází díky automatickému řízení expozice k vyrovnání a zachování úrovně obrazového signálu.

9.4.4 Kontrast a barva cílového objektu

Osvětlení je zásadním faktorem ovlivňujícím kvalitu obrazu. Předpokladem vysoce kvalitních a spolehlivých obrazů je efektivní a předem promyšlené osvětlení scény založené na specifických potřebách CCTV. Nejdůležitější je nasměrování a úroveň osvětlení. Rovněž kompatibilita mezi použitým zdrojem osvětlení a citlivostí kamery hraje podstatnou roli, pokud je důležitá barva obrazů nebo jejich tónování v případě barevných systémů.

Cílový objekt osvětlený zezadu, jenž se rýsuje v obrysech, je přijatelný z hlediska detekce, ale nerozlišuje žádné detaily umožňující jeho identifikaci. Rozptýlené světlo snižuje možnost

identifikace dobře zamaskovaného "vetřelce". Ti, kteří očekávají záběry obličeje stejné kvality, jakou mají záběry v televizních přijímačích v jejich domácnostech, by se měli lépe informovat o zdrojích, množství a analýze osvětlení potřebného k dosažení takovýchto výsledků.

9.4.5 Magnetický záznam obrazového signálu

Při testování CCTV je zásadní věnovat pozornost zejména kvalitě reprodukovaného obrazu. Analogové standardy mají omezené možnosti, zvláště co se týče rozlišovací schopnosti. Technickou specifikací garantovaná rozlišovací schopnost není úplně využita vinou podcenění nezbytnosti údržby páskové dráhy a hlavového bubnu v nepřetržitém provozu, nebo dokonce podceněním nutnosti včasné výměny vícekrát použitých pásek, či nevhodnou volbou typu pásku. V současnosti jsou pro archivaci záběrů kamer k dispozici 3 technické prostředky videorekordér, videotiskárna a uchování obrazu na pevném disku. Videorekordér byl vyvinut speciálně pro potřeby záznamu dějů v bezpečnostních aplikacích systému CCTV. Vedle běžného typu záznamu v reálném čase (50 půlsnímků/s) umožňuje nahrávat signál ve vzorkovacím režimu. Vzorkovací režim prodlužuje záznam na běžnou kazetu E 180. Podle nastavení 24,48,72,120,168,240,480 až 960 hodin. Volba vzorkovacího režimu pro konkrétní aplikace závisí na dynamičnosti snímaných dějů a velikost zorného pole snímané kamery. Na trhu jsou k dispozici tři kategorie : do 24 hod, do 480 hod a do 960 hod. Videorekordér umožňuje i poplachový vstup, změnu záznamového režimu, které lze využít pro kombinaci s EZS.

9.5 Synchronizace

Důležitým parametrem kamer je způsob, jakým lze u dané kamery zajistit synchronizaci signálu se signály ostatních kamer používaných v systému CCTV.

9.5.1 Interní synchronizace

Nejlevnější typy kamer mají pouze interní synchronizaci. To znamená, že kamera obsahuje ve své elektronické části stabilní oscilátor, od něhož se odvozují všechny časové signály v tolerancích daných příslušnou TV normou. Vzhledem k tolerancím jednotlivých oscilátorů nelze v systému žádným způsobem zajistit synchronizaci s ostatními kamerami. Jsou – li takovéto kamery připojeny k analogovému zařízení dochází při přepnutí z jedné kamery na druhou k vyrovnávání fáze nesynchronních signálů, a tím k „poskočení obrazu“ obvykle o jeden

půl snímek. Tento jev je zvýrazněn v případě záznamu na videorekordér a výsledkem je záznam s výpadky obrazu na malý časový okamžik po přepnutí kamer. Kamery s interní synchronizací je možné použít pouze u autonomních systémů kamera – monitor, kamera – videorekordér – monitor, nebo u multiplexních systémů založených na digitalizaci obrazu a zpětném převodu do analogové podoby.

9.5.2 Synchronizace od napájecí sítě (linelock)

Je to nejjednodušší způsob synchronizace v rámci CCTV. Synchronizační signál jeodvozen od střídavého napájecího napětí sítě 230 V, 50 Hz či nízko voltového střídavého napájení 24 V, 50 Hz. Pro dorovnání rozdílů při zapojení kamer na různé fáze slouží ovládací prvek na kameře jímž je možné nastavit minimální fázový rozdíl a tím minimální rušivý efekt na obraze při přepnutí z jedné kamery na druhou.

9.6 Přepínače, spínače a multiplexery .

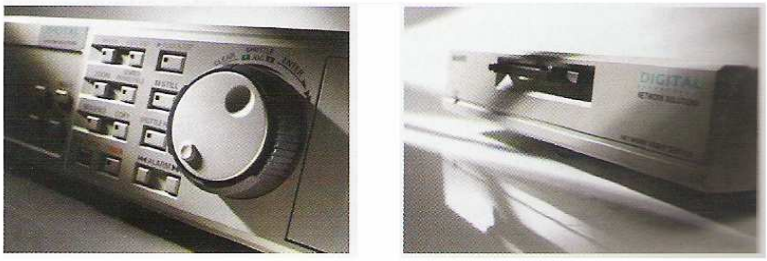
Dobře navržené přepínání by nemělo mít výrazný negativní dopad na kvalitu obrazu. Komprimování obrazů s cílem zobrazení více obrazů na obrazovce vede ke snížení kvality obrazu, přičemž původní kvalitu nelze obnovit. V extrémním případě může být zaznamenán pouze jeden nebo dokonce žádný obraz podezřelé osoby, ačkoli kamera vytvořila bezchybnou řadu obrazů, během incidentu. Důležitý je způsob jak se osoba pohybuje. Značně rozsáhlé úrovně rozpoznání jsou možné díky vyškoleným pozorovatelům ačkoliv záběry z obličejových partií jsou nejasné, a nejsou rozeznatelné. Sled nesouvislých obrazů vytvořených přepínáním, multiplexery a nebo time-lapse videorekordéry je často málo použitelný,vinou nevhodné volby nastavení parametru (režimu záznamu).

Integrování nekompatibilního zařízení může vést k neočekávaným problémům, které způsobí ztrátu obsahu a kvality obrazu. Například není-li možné kamery synchronizovat frekvence v jaké jsou obrazy z každé kamery zobrazovány či zaznamenávány, může selhat.

9.7 Digitální záznamová zařízení

Digitál v daných ekonomických mezích nemůže překonat fyzikální hranice principu sdíleného času záznamu u více kamerových systémů. Nerealistické požadavky na dobu záznamu mnohdy zbytečně prodražují záznamové zařízení, přitom využitelnost starých informací je v práci městské

policie či Policie ČR omezena. Hranice rozlišovací schopnosti, daná použitým systémem analogového záznamu (VHS, S-VHS, BETA) a uváděná v televizních řádcích, je u digitálního záznamu vyjadřována skutečnou maticí obrazových bodů (HxV) odpovídající vymezenému počtu paměťových míst vyjadřujících umístění v rámci celého snímku. Pro každé paměťové místo je navíc stanoven určitý počet úrovní šedé (při černobílém záznamu) nebo počet od sebe rozlišitelných barevných odstínů (8, 10, 16, 32 bit). Navíc digitální záznamová zařízení používají různé způsoby komprese signálu (kompresní algoritmy), aby co nejlépe využily kapacity paměťového média. U analogového systému a multiplexního režimu záznamu můžete jednoznačně stanovit pro danou dobu záznamu mrtvé časy mezi záběry jednotlivých kamer, nebo naopak s maximálně přijatelných mrtvých časů stanovit potřebný režim záznamu. Tím lze vymezit jednoznačně ve vazbě na technické možnosti použitého zařízení i režim výměny pásek a organizaci skutečné knihovny záznamu. U digitálního záznamu je však proměnných více a uživatel může volit rozlišovací schopnost záznamu (nejčastěji super rosolution, normál a extended rocord) někdy i počet stupňů šedé či počet barevných odstínů. Může sám volit (či je systémově dána četnost záznamu apod. Znalost práce na PC je zde nezbytnou kvalifikační podmínkou. Organizace knihovny (v tomto případě virtuální) v podobě PC souborů je základem efektivního využití systému.



Obr. 19. Videorekordér Sanyo slouží k digitálnímu záznamu

9.7.1 Digitální kamery

Zde dochází k ukládání snímků přímo do paměti kamery.

Největší rozlišovací schopnost obrazu ve standardu CCIR:

- počet řádků : 625
- formát obrazu: 4:3
- počet viditelných řádků 575

Pro teoreticky stejnou rozlišovací schopnost viditelného obrazu ve vertikálním i horizontálním směru potřebujeme podél řádků rozlišit (4:3) x 575 = 767 obrazových bodů. Viditelný obraz lze tedy vyjádřit jako matici 575x767 = 441 025 obrazových bodů.

Tab. 7. Objem dat pro jeden snímek

Typ videosignálu	**Počet obrazových**	**Počet stupňů šedé**	**Počet barevných**	**Objem dat (M bit)**
Černobílý	440 000	256	-	3,5
Černobílý	440 000	1024	-	4,4
Barevný	440 000	256	256	7
Barevný	444 000	1024	1024	8,8

V tabulce je uveden objem dat odpovídající jednomu snímku. Z toho lze spočítat potřebnou kapacitu paměti, v případě, že by byla umístěna přímo v kameře a i kdybychom chtěli omezený záznam, vždy se dostaneme do kapacity řádově jednotky M Byte.

Na CCTV není možné spoléhat jako na zařízení, které vše samo vyřeší. Jde především o to, aby ho určení pracovníci podle předpisů efektivně využívali. CCTV přináší výsledky, které se projevují celkovým snížením kriminality ve městech. Technika se dynamicky rozvíjí, a proto je třeba i CCTV neustále vylepšovat a inovovat.

10 OCHRANA A KONTROLA CCTV

Kamerové systémy musí být stejně jako každé jiné zařízení, které je zapojeno do bezpečnostního řetězce, důsledně a důkladně ochráněny a zároveň kontrolovány. Následující stať popisuje zejména oblast ochrany proti povětrnostním vlivům, problematiku přepěťové ochrany, ochranu proti odcizení, poškození či zneužití. V závěru je pozornost věnována kontrole činnosti systému.

10.1 Ochrana proti povětrnostním vlivům

Dislokace systému by měla respektovat povětrnostní vlivy. Montážní místa by měla být volena s ohledem na převládající směr větrů a možné zasněžení kamer. Povětrnostní podmínky působí dlouhodobě. Toto je třeba mít na paměti hlavně u zařízení, která se časem mohou uvolnit z uchycení a svým pádem způsobit škodu nebo zranění lidí. Proto je třeba věnovat pozornost nejen technologii montáže (plastové hmoždinky do zdí), ale i kontrole při servisní činnosti. Montáž je nutno provádět za dobrého počasí, jinak zcela objektivně klesá její kvalita, poškozují se kabely a ochranné plastové krabice, těsnící tmely ztrácejí účinnost a potom vlivem povětrnostních vlivů klesá odolnost systému rychleji.

Kamery a další komponenty musí být připraveny na podmínky obvyklé v mírném klimatickém pásmu. Do povětrnostních vlivů lze zařadit i vliv exhalací. Ty je nutno posoudit individuálně.

Obr. 20. Otočná kamera Panasonic odolná proti povětrnostním podmínkám

Důležitým prostředkem proti povětrnostní ochraně je instalace vytápěných krytů kamer s patřičným stupněm krytí (IP 65). Kývání při silném větru zamezí dostatečně pevná a tuhá kamerová ramena a kvalitní polohovací zařízení. Přenosové kabely, pokud je jich použito a jsou vedeny po stožárech či na budovách, musí odolávat nízkým teplotám a působení ultrafialového záření.

10.2 Přepěťová ochrana

Elektronická výbava výpočetní, telekomunikační, záznamové, zabezpečovací a další techniky je obsažena ve všech segmentech CCTV. Všechna tato zařízení jsou většinou napojena na elektrorozvodnou síť (na napětí 230 V) a některá mohou být zapojena i v různých jiných sítích (např. počítačové sítě).

Velkou část poruch elektronických zařízení připojovaných k síti způsobuje přepětí. V našich podmínkách je krátkodobé přepětí způsobováno buď bleskem - atmosférické přepětí - nebo spínáním v elektrických obvodech - spínací přepětí.

10.2.1 Atmosférické přepětí

Vzniká při velkých elektrických výbojích, tedy při bouřkách. Mohou být zasažena elektronická zařízení v místě úderu blesku či v jeho okolí až do vzdálenosti 2 km. Nejvíce jsou ohroženy objekty umístěné ve vysokých budovách nebo v osamělých stavbách na vyvýšených místech.

10.2.2 Spínací přepětí

Může vznikat nejen v rozvodech elektrického napájení (230 V, rozvody vyšších napětí), ale i v dalších (signalizačních, anténních, telekomunikačních a počítačových) rozvodech. Zdrojem jsou spínací špičky různých elektrických spotřebičů a strojů, zejména při spouštění motorů s velkou indukčností a transformátorů, při zapínání neonových výbojek (firemní reklamy a loga), přerušení obvodů napájení z nejrůznějších důvodů či kmitajícími kontakty.

Dalším druhem přepětí jsou elektrostatické výboje způsobené obsluhou vlastního CCTV. Lidské tělo lze totiž přirovnat ke kondenzátoru, jehož vlastností je hromadit elektrický náboj do hodnoty tisíců voltů. Připojení tohoto "kondenzátoru" velmi negativně působí zvláště na

mikroprocesorové části zařízení. Nebezpečí popisovaného efektu vzrůstá při užívání nevhodných oděvů, podlahových krytin a sedacího nábytku.

Důsledkem působení přepětí na nedostatečně ochráněné elektronické přístroje a zařízení je zničení polovodičových součástek průrazem polovodičových přechodů, zničení metalizace pasivních součástek, zničení vodivých drah plošných spojů a urychlené stárnutí součástek. Tím dochází ke zkrácení výrobcem garantované životnosti a spolehlivosti celého přístroje. Problémy se většinou projeví ztrátou dat, chybami v ovládání nebo nesprávným přenosem dat na jiná média.

Dalšími nepříjemnými následky mohou být případně poruchy na nainstalovaném elektrickém zabezpečovacím nebo požárním systému. Projevují se zejména falešnými poplachy, které bývají spojeny se zbytečnými výjezdy policie, hasičů případně některé ze soukromých bezpečnostních služeb anebo s úplnou disfunkcí zasaženého zařízení.

Příčiny poruch způsobené přepětím jsou zejména absence účinných ochran v rozvodu napájecí sítě, telekomunikačních a počítačových sítích a jiných rozvodech, nedokonalý systém uzemňování v budovách a nesladěnost hromosvodní a přepěťové ochrany, nedostatečná odolnost elektronických zařízení (zařízení nemá provedeny zkoušky příslušné zkušebny a není zařazeno certifikačním orgánem do patřičné bezpečnostní třídy) a užívání oděvů, podlahových krytin a potahů nábytku s nízkou elektrickou vodivostí. Přepěťové ochrany mají v konečném součtu velký vliv na bezporuchovou funkci jakéhokoliv elektronického zařízení, a tím i na dobrý chod CCTV.

V procesu harmonizace našich předpisů a zákonů s Evropskou unií se musí výrobci elektrických a elektronických přístrojů a zařízení, zajímat o směrnici Rady EU číslo 89/336/EEC z 3. května 1989 “O sbližování zákonů členských států týkajících se elektromagnetické kompatibility”. V současné době je tato směrnice přijata již jako zákon v zemích EU. Směrnice Rady EU definují požadavky ochrany týkající se EMC a nerozlišují elektrické a elektronické zařízení podle výkonu, provedení nebo druhu a místa provozu.

Elektromagnetická kompatibilita je posuzována ve dvou základních směrech. Jednak jde o úroveň vyzařované elektromagnetické energie - rušení (dále jen EMI) z elektrotechnických zařízení. Jednak jsou požadovány odpovídající parametry elektromagnetické citlivosti (susceptibilita) na rušení (dále jen EMS). K nebezpečným elektromagnetickým vlivům tak náleží např. přepětí, přechodné děje, vf a nf emise a imise, nestabilita napájení či elektrostatické výboje.

K odstranění uvedených vlivů může sloužit např. stínění, filtrace, přepěťové ochrany, zemnění, pospojování, změna designu nebo změna signálových úrovní.

10.3 Ochrana proti odcizení a poškození

Prostředí, kde je instalován kamerový terminál nebo mikrovlnné pojítko, neskýtá mnoho možností ochrany. Zamezit přístup k těmto zařízením nelze. Přístup je však možno omezit například mechanickými zábranami, organizačními opatřeními a v neposlední řadě jej registrovat elektronickým zařízením. Přístup k zařízení CCTV by měl být registrován jeho uživatelem.

Určitým řešením je instalace EZS, jehož detektory jsou umístěny tak, aby byl minimalizován počet klamných úmyslných i neúmyslných poplachů. Instalace EZS je dnes vzhledem k nízkým cenám komponentů PCO umístěným zpravidla velmi blízko řídícího centra kamerového systému, správným a efektivním krokem. Velmi účinné je označit chráněný prostor varovnými tabulkami.

Přesto zůstává problémem, jak omezit výjezdy vozidel k poplachům. Nejprve je třeba rozlišit je na falešné a platné. Druhý problém spočívá v tom, že EZS je pouze informační systém a člověka nezastaví. Situace je ještě složitější, jestliže je do místa instalace kamerového systému více přístupů. Ve všech uvedených případech je velmi efektivním řešením instalace bezpečnostní kamery, která snímá přístup k chráněné technologii. Tato kamera je připojena do sledování a nahrávání po zachycení signálu od detektoru EZS (PIR, mikrovlnný, kontaktní, otřesový detektor ap.) místo hlavní kamery. Je-li kamera doplněna zařízením, které dá osobě jenž vstoupila do střežených prostor na vědomí, že je zachycena, udělali jsme zřejmě pro ochranu maximum. Kamera musí být doplněna reflektorem. Tento reflektor v noci poskytne osvětlení pro kameru a zároveň indikuje pohotovost systému. Kromě světla může být pro nezvaného návštěvníka výstrahou i zvukový signál. Uvažovat lze o siréně nebo zařízení generující předem namluvený text.

10.3.1 Důležitou roli hraje vzdálenost

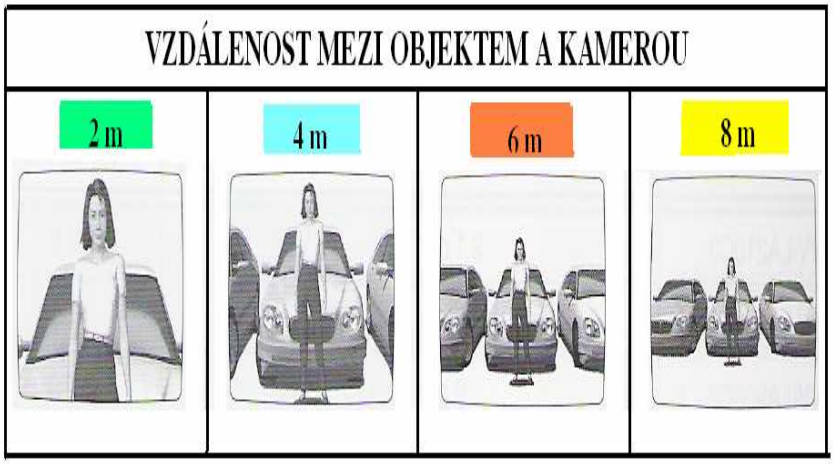
Videoochrana vzdáleného kamerového místa, rádiového pojítka nebo retranslačního bodu je zřejmě nejefektivnějším způsobem ochrany. Zprostředkovává operátorovi optický a sluchový vjem, což je dostačující pro správné vyhodnocení, zda vyslat nebo nevyslat zásahovou jednotku.

Systém rozlišujeme podle způsobu komunikace mezi řídícím centrem a místy instalace částí systému. Tato místa pak nazýváme vzdálená. Abychom ze vzdáleného místa dostali jakoukoli informaci, musíme tam mít rádiový vysílač. Způsob komunikace, ať je realizována po metalice, optice nebo rádiem, musí umožňovat obousměrnou - duplexní nebo poloduplexní komunikaci.

Ve stávajících městských systémech jsou hojně používány oba způsoby komunikování. Tedy kromě obousměrného komunikování i komunikování jednosměrné - simplexní. Ovládání vzdálených zařízení simplexním způsobem umožňuje pouze předávat povely. Povely předává řídící subjekt ovládanému subjektu na podkladě informací zjištěných pouze vlastníma očima.

Druhý způsob, moderní a perspektivní, je charakterizován obousměrným přenosem dat. Vyžaduje vysílač a přijímač na obou stranách, a je tedy nákladnější. Uvedená technika zabezpečí že vedle jednoho páru očí tvořících zpětnou systémovou vazbu v "simplexním systému" přibudou desítky mikroprocesorů formující zprávy o stavu "duplexního systému".

Vzdálenosti jednotlivých prvků v CCTV jsou značné. Pro ochranu těchto prvků je potřeba prosazovat zařízení, jejichž odstrašující efekt je vysoký. Efektivní je nasvícení zájmového prostoru a přepnutí hlavní kamery na kameru bezpečnostní, která je do zájmového prostoru směrována.



Obr. 21. Vzdálenost sledovaného objektu od kamery

10.4 Ochrana proti zneužití

Tak jako u všech společensko-technických systémů je významným zdrojem ohrožení funkčnosti a spolehlivosti CCTV člověk - operátor. Největším nebezpečím v případě CCTV hrozícím ze strany obsluhy, je únik a následné zneužití informací. Nejdůležitějším způsobem je správný návrh struktury CCTV, v němž hraje rozhodující úlohu počítačové řízení a obousměrný přenos dat a z toho vyplývající možnost efektivní kontroly.

Určitým nebezpečím, které je možno identifikovat jako "možnost zneužití CCTV", může být paralerní sledování scény, zachycené kamerou CCTV neoprávněnou osobou. Za určitých okolností je nutno věnovat tomuto problému pozornost.

Výrazný nástroj v oblasti ochrany před zneužitím CCTV je důsledná evidence záznamů, videokazet (pokud jsou v systému začleněny jako paměťové médium) a uložení videokazet. Evidence záznamů pořízených na záznamovém zařízení je přesně vedena např. v knize "Evidence záznamů monitorovacího zařízení", která je uložena na pracovišti operátora. Videokazety určené pro monitorovací zařízení jsou označeny evidenčním číslem, razítkem a podpisem příslušného velitele. Vše je evidováno např. v knize "Evidence videokazet monitorovacího zařízení". Velmi důležité je uložení videokazet. Veškeré kazety, určené pro potřebu monitorovacího pracoviště, jsou uschovány v trezoru u velitele. Pořízený záznam je uchován a po stanovené lhůtě zničen. Zničení záznamu provede na technickém zařízení velitel či jeho zástupce. O zničení záznamu se provede zápis.

10.4.1 Přístupová práva

Další z možností jak uchránit CCTV před zneužitím, je využití různých přístupových práv. Práva umožňující ovládat a nastavovat jednotlivé prvky lze např. rozdělit pomocí hesel na uživatelská a na práva pro správce systému. Heslo může obsahovat několik čísel či znaků a má určitý stupeň hierarchie. Po zadání hesla správcem systému jsou přidělena přístupová práva obsluze k ovládání jednotlivých položek menu. V praxi je zcela běžné, že uživatelé CCTV oddělí část položek, které zůstanou pro běžnou obsluhu nepřístupné. Po vstupu do ovládacího menu se zobrazí nabídka kritérií, které je možno nastavit. Přehledným menu postupuje uživatel krok za krokem.

10.4.2 Utajený záznam

Zapojení funkce utajeného záznamu umožňuje zaznamenávat kamery, které zůstanou pro obsluhu systému nedostupné. Může jít o určitý specifický záměr uživatele, kdy není vhodné, aby mohla obsluha s vyčleněnou kamerou manipulovat a mít přehled, co a kde se vlastně nahrává. V praxi půjde nejčastěji o využití této možnosti v případech, kdy je požadováno utajované nahrávání a kdy je potřeba pořídit záznam z bezpečnostních důvodů. Možnost utajeného záznamu není sice typické pro použití v CCTV, ale bylo vhodné se o ní zmínit jako o jedné z technických možností.

10.5 Kontrola činnosti systému

Kontrolní činnost je jedním ze základních předpokladů zachování potřebné odolnosti systému. Zásadním způsobem ovlivňuje úroveň odolnosti společensko-technických systémů člověk, který je obsluhuje.

Kontrola činnosti systému musí tedy probíhat v obou jeho částech, tj. v lidské části i v části technické, byť i na nejvzdálenějším prvku. Jakákoliv porucha nebo pokus o sabotáž musí být okamžitě identifikovány a dokumentovány v centru.

Nejefektivnějším prostředkem kontroly, zaměřeným na činnost operátorů, je zaznamenávání pozic středu objektivu kamery při ručním řízení pohybu kamery a jeho graficky přehledné ztvárnění v každodenním hlášení odpovědnému funkcionáři. V technických možnostech systému musí být vymezení zakázaných zón, dohlížení a vydání informace o jejich narušení. Systém musí umožňovat reprodukci směrování kamery v libovolném čase.

10.5.1 Kontrola obsluhy

Povinnosti a rozsah pracovní činnosti operátorů musí upravovat směrnice (výkon služby - den/noc, archivace, využití záznamu apod.). Důležitým dokumentem je i směrnice, která vymezuje součinnost monitorovacího pracoviště obecní policie s Policií ČR při organizování nezbytného zákroku proti pachatelům, zjištěných trestných činů. Výhodnější je umístění monitorovacího pracoviště také na Policii ČR (profesionalita, zákrok). Popularizace CCTV musí být přiměřená, aby nedošlo k dekonspiraci a odhalení slabých míst systému, což je do jisté míry otázka loajality, ale i bezpečnosti operátorů.

10.5.2 Technická kontrola

Hlavními formami kontroly technické části CCTV jsou pravidelné prohlídky jednotlivých částí systému. Kontrolovat je nutno stav a upevnění konstrukcí na stěnách, střechách a sloupech. Akumulátory záložních zdrojů postupně ztrácejí kapacitu a k jejich "odchodu" dojde zpravidla v nejnevhodnější dobu. Kvalitu zobrazení získanou drahými kamerami mohou významně snížit umazaná skla ochranných krytů.

Počítačové řízení a obousměrný přenoso-datový protokol však umožňují využívat nejefektivnější metody založené na korelaci dat uložených v databázi výsledků testů. V současné době lze data transportovat třeba elektronickou poštou do servisní firmy, odkud může přijít návod k zásahu nebo odkud se dostaví dobře připravený servisní technik. Ale především bude známa předpověď výskytu poruch.

11 ODOLNOST CCTV SYSTÉMŮ, JEJICH PERIFERNÍ A ELEKTRONICKÉ VÝBAVY PROTI PŘEPĚTÍ

Pojem odolnost systémů (elektromagnetická susceptibilita) jako působení rušivé elektromagnetické energie na jednotlivé systémy můžeme v rámci uzavřených kamerových dozorových a kontrolních systémů (CCTV) všeobecně charakterizovat jako odolnost daného zařízení pracovat nepřetržitě v jakémkoliv prostředí souběžně s nenadálými povětrnostními vlivy, elektrickými přepětími (Electromagnetic disturbing) a podobně. Tento pojem můžeme též pro jednoduchost vyjádřit slovem životnost, aby daný systém mohl v daném prostředí co nejdéle obstát. Odolnost je vedle výkonnosti nejdůležitějším parametrem pro hodnocení systémů. Kvantifikací úrovně odolnosti a kvalifikací jednotlivých opatření je možno stanovit, jak dlouho a za jakých vnějších podmínek bude systém pracovat spolehlivě, jak bylo předpokládáno v základním návrhu a koncepce daného systému, pro jeho využitelnost na určitém pracovišti nebo prostředí.

Provedení a změření systému v rámci elektromagnetické kompatibility (dále jen EMC) sice je pro navrhované systémy finančně náročnější, ale na druhé straně obnova nebo úprava nedostatečně odolného systému může být v průběhu časového intervalu životnosti navrhovaného systému nákladnější, nebo dokonce může dojít ke zničení systému a jeho absolutní nefunkčnosti. Správná definice odolnostních parametrů a z nich vyplývajících technických opatření je součástí podstaty správného návrhu efektivního systému.

Uzavřené kamerové dozorové a kontrolní systémy můžeme chápat i jako sociálně – technické systémy, které mají za cíl zvyšovat bezpečnost občanů, k prevenci a potírání kriminality sledováním obrazu prostor – scén, na určitých exponovaných místech. Jsou to technické systémy, které jsou obsluhovány pracovníky soukromých bezpečnostních služeb (dále jen SBS) nebo policií, kteří jsou schopni vyhodnotit z televizního obrazu situace, v jejichž důsledku budou nebo již jsou ohrožováni občané nebo jejich majetek a předat dál tyto informace orgánům schopným zasáhnout a pomoci.

Do popředí se dostává podstatný problém CCTV, který není u běžných privátních kamerových systémů zdůrazňován, neboť u těchto zařízení posuzujeme kvalitu systému podle kvality kamer, objektivů, monitorů a videorekordérů a kde všechny tyto řídící funkce zastane multiplexer, jehož inteligence je vesměs vyčerpána manipulací s videosignály a kde jedinou možnou strukturou je

přísně centralizovaná hvězdicová struktura, i když v poslední době existují struktury s jinou konfigurací

Schopnost kontroly je základní systémovou vlastností a měla by být podporována technickými parametry jednotlivých prvků systému. Schopnost kontroly je nejdůležitější vlastností vytvářející předpoklady pro znemožnění zneužití videozáznamů nebo úmyslné blokování činnosti systémů CCTV vlastní obsluhou. I komunikace musí mít určitou úroveň. Aby bylo možné využít inteligence technických prvků a zabezpečit rychlou odezvu v řídicím elektronickém počítači zpracované informace v určité formě, je třeba používat obousměrný komunikační protokol.

V současné době je řízení systémů zabezpečováno počítačově, kde zařízení jako kamery, polohovací hlavice, objektivy, kvadrátory, záznamová zařízení, detektory pohybu a multiplexery jsou připojeny prostřednictvím jednotek k počítači.

Počítačové řízení umožňuje efektivně sbírat data o průběhu chodu systému, výsledcích testování a použitých režimech práce. Tato technická možnost podmiňuje kontrolní činnost o využívání systému, jeho efektivnost a využití jako informačního zdroje.

Dislokace systému CCTV by měla respektovat povětrnostní vlivy. Pokud je to možné, je nutné vyhnout se montážím zařízení, která jsou za ztížených povětrnostních podmínek špatně přístupná, tím snížíme pravděpodobnost úrazů při opravách. Z hlediska vlastních montáží je nutné, aby byla provedena montáž kamerových prvků na ta místa, která jsou chráněna proti zasněžení a ze strany převládajících směrů větrů. Kamery a další komponenty musí být připraveny na podmínky obvyklé v mírném klimatickém pásmu.

Elektronická výbava výpočetní, telekomunikační, záznamové, zabezpečovací a další techniky má být obsažena ve všech segmentech CCTV. Uvedená zařízení jsou většinou napojena na síť (NN pro U = 230 V) a některá mohou být zapojena i v jiných dalších sítích.

Velkou část poruch elektronických zařízení připojovaných k síti způsobuje přepětí. V našich podmínkách je krátkodobé přepětí způsobeno bleskem – atmosférické přepětí, nebo spínáním v elektrických obvodech – spínací přepětí.

Mezi základní zdroje rušení můžeme zařadit průmyslové zdroje rušení, zdroje napěťového přepětí a zdroje kontinuálního rušení a speciální zdroje rušení tzv. nukleární elektromagnetický impuls (NEMP – Nuclear Electromagnetic Pulse)

Z periodických spojitých rušivých signálů jsou nejdůležitější harmonické složky kmitočtu napájecí sítě 50 Hz, které jsou často produkovány již samotnými generátory při vlastní výrobě elektrické energie. Největšími průmyslovými zdroji rušení jsou řízené polovodičové měniče velkých výkonů, které produkují v napájecí síti harmonické kmitočty cca až do 30 MHz.

V sítích vysokého a velmi vysokého napětí dochází k vysokofrekvenčním oscilacím při zapínání vlivem kapacity a indukčnosti spínaných vedení.

Další typ rušení vzniká v napájecích sítích pro nízké napětí (U nn) při činnosti stykačů a jističů nebo v poslední době méně používaných mechanických relé. V okamžiku rozpojení kontaktů dochází k rychlé změně proudů, a tím ke vzniku vysokého rušivého napětí. Mezi kontakty tak vznikne obloukový výboj a napětí na kontaktech klesne skokem k nule.

Mezi rušivé procesy také patří typy rušení, která souvisejí se spínacími pochody, ty např. vznikají v usměrňovačích diodového typu nebo v systémech tyristorového řízení, do kterého můžeme zařadit např. systémy pro provoz tramvají, regulace otáček velkých motorů a podobně.

Silné rušivé účinky vykazují energetická vedení vysokého (vn) a velmi vysokého napětí (vvn), která se velmi těžko vyhledávají a také odstraňují.Zdrojem rušivých signálů vedení vn a vvn jsou koronové výboje (jen u vvn) cca 110 kV a více a kapacitní výboje (jen u vn) cca 22 kV.

Rušivé procesy můžeme nalézt také např. u zářivek, osvětlovacích a jiných výbojek, kde startéry zářivek se přemosťují odrušovacími kondenzátory, které zkratují vf. složky vznikající při rozpojování startérového kontaktu. Nesmíme zapomenout vzpomenout i vznik častých poruch při činnosti zážehových spalovacích motorů jejich zapalovacích jednotek.

Zdroje napěťového přepětí možno podle jejich původu rozdělit na :

a/ přírodní zdroje (LEMP – Lightning Electromagnetic Pulse). Bleskový výboj, který může ohrožovat elektrická a elektronická zařízení do vzdálenosti cca 4 km .

b/ zdroje umělé vytvořené lidskou činností (patří sem v podstatě všechna spínací zařízení, u kterých dochází ke vzniku elektrického oblouku. K umělým zdrojům přepětí patří lokální elektrostatické výboje (ESD – Electrostatic Discharge) Jedná se o výboje, které vznikají u všech přístrojů a zařízení, která svojí činností mohou vyvolat tření mechanických částí, a tím vznik elektrostatického výboje.

Zdroje kontinuálního rušení jsou charakterizovány jako zdroje, které působí obvykle nepřetržitě nebo alespoň relativně delší dobu. Sem můžeme zařadit rušení rozhlasových a televizních vysílačů nebo rušení radarových vysílačů jak pro potřeby vojenské, tak i pro potřeby civilní. Dalším masově se rozšiřujícím potenciálním zdrojem elektromagnetického spojitého rušení jsou systémy pro společný rozvod rozhlasových a TV signálů, kde se zejména jedná o společné TV antény a celoplošné TV kabelové rozvody.

Všechny druhy přepětí mohou ovlivnit kamerový systém. Z tohoto důvodu je velmi důležité neopomenout dostatečnou ochranu proti přepětí u všech částí systému, především signálových a napájecích tras. Důsledkem působení všech druhů přepětí je zničení polovodičových součástek průrazem polovodičových přechodů, zničení metalizace pasivních součástek, zničení vodivých drah plošných spojů a stárnutí součástek a zařízení

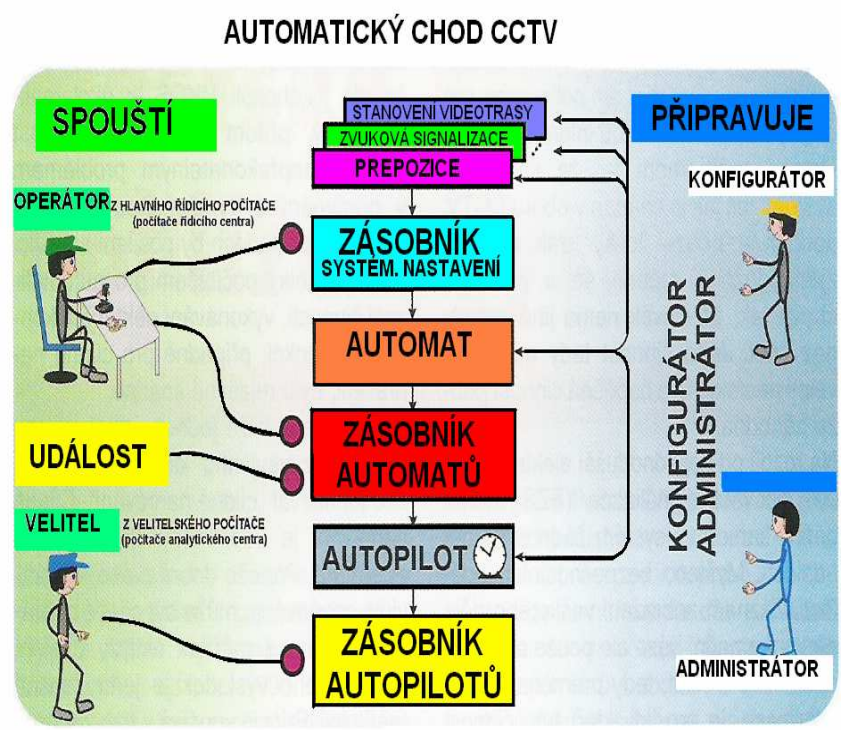
Východiskem analýzy provedené příčinami poruch způsobené přepětím bývají absence účinných ochran v rozvodu napájecí sítě, telekomunikačních a počítačových sítích a jiných rozvodech, nedokonalý systém uzemňování dále žádná kontinuita hromosvodní a přepěťové ochrany, nedostatečná odolnost elektronických zařízení a používání oděvů, podlahových krytin a potahů nábytku s nízkou elektrickou vodivostí.

Zákonitosti působení vlivu EMC by měly být více než dosud zohledňovány při schvalování zařízení do provozu, ale především se musí požadavek na ochranu tohoto typu objevit v zadávacích podmínkách vlastního výběrového řízení.

II. PRAKTICKÁ ČÁST

12 LIDSKÝ FAKTOR A CCTV

CCTV musí obsluhovat lidé, kteří jsou schopni přijímat rozhodnutí, ví kam se zaměřit a jaké kroky podniknout na základě toho co vidí v době záznamu nebo při jeho přehrávání. Může to znít podivně, ale my vlastně nevíme, jak dlouho se člověk dokáže soustředit na to, co vidí na panelu obrazovek, které ukazují scény snímané množstvím různých kamer. Operátoři jsou chybující lidé stejně jako všichni ostatní. Tato "video slepota" může způsobit, že člověk něco uvidí, ale nebude na to správně reagovat. Operátoři budou rovněž potřebovat prostředky k tomu, aby upozornili ty, kteří mohou provést příslušné kroky na základě toho, co se objeví na záznamu. K těmto lidem mohou patřit policisté, ale především strážníci.



Obr. 22. Automatický chod kamerového docházkového a kontrolního systému

12.1 Vlastní výběr pracovníků obsluhy

Je důležité určit kdo bude pracovat na monitorovacím pracovišti. To, co operátoři uvidí, musí považovat za přísně důvěrné a nesmí vzniknout ani náznak podezření, že by se nechovali v souladu se stanovenými pravidly. Vybrané operátory musíme zaškolit podle pečlivě připravených plánů. Rovněž je třeba rozvíjet dobré pracovní vztahy.

12.1.1 Důležitost lidského činitele

Monitoringy nejsou jen záležitostí techniky, ale i lidského činitele. Nároky na pozornost, soustředění, rozlišovací schopnost a správnost rozhodnutí obsluhy jsou značné. Osoba provádějící monitoring je neustále ve střehu a podle vnitřní směrnice režimového pracoviště operativně spolupracuje s dozorčí službou policie, v zájmu případného zákroku zásahové skupiny. Nejdůležitější součástí z hlediska celkové výslednosti CCTV je lidský faktor neboli operátoři a jejich nadřízení. Práce operátorů je náročná. Obsluha musí mít nejen dokonalou místní a osobní znalost, ale také znalost způsobů páchání trestné činnosti, zejména je-li páchána ve skupinách nacvičeným a dokonale propracovaným způsobem. Operátor musí mít tzv. policejní čich, musí umět dokonale přečíst pozorovanou scénu, a pokud sledovaný probíhající děj směřuje k nezákonnému jednání, bleskurychle se kvalifikovaně rozhodnout a patřičně konat. Výsledkem nemusí být vyslání policejní hlídky do dotčeného prostoru za každou cenu. Podle konfigurace CCTV bude někdy stačit např. dálkově sepnout světelnou či předem připravenou a namluvenou výstrahu. Pokud to koncept kamerového systému umožňuje, lze využít i hlasové komunikace s přestupcem či pachatelem trestné činnosti výběru osob.

Značnou pozornost je třeba věnovat osobám, které budou obsluhovat CCTV. Před jejich nástupem je vhodné provést s nimi osobní pohovor s cílem prověřit, zda se jedná o osobu schopnou, důvěryhodnou a spolehlivou. Je také vhodné, aby kandidáti na obsluhu mimo jiné absolvovali lékařské prohlídky a podrobili se psychotestům. Vybrané pracovníky je poté třeba odeslat do některého z akreditovaných školících středisek, kde se proškolí v dané problematice. Školení by nemělo být jednorázovou akcí, ale mělo by jít o nepřetržitou a plánovanou aktivitu všech operátorů, nikoli pouze s cílem zlepšení jejich znalostí a schopností využívat systém, ale s cílem rozšířit jejich znalosti v oblasti právních a bezpečnostních postupů.

CCTV musí řídit lidé, kteří jsou schopni rozhodnout o tom, kam se kamery nasměrují a jaká konkrétní opatření budou provedena na základě přímého přenosu kamer či záznamu. Operátoři musejí být dostatečně motivováni i pro dobu relativního klidu na obrazovkách. Je vhodné je též udržovat v co nejvyšší výkonnosti např. pomocí prezentací úspěšnosti systému v předcházejícím období.

12.1.2 Bezpečnost operátorů

Protože CCTV jsou také bezpečnostními systémy, je nutné věnovat se oblasti bezpečnosti operátorů. Existují totiž reálné obavy, že monitorovací centra s operátory mohou být vystavena potenciálnímu nebezpečí. V závislosti na typu monitorovaného a nahrávaného incidentu je operátor vystaven různým hrozbám, počínaje nátlakem, nabídnutým úplatkem nebo přímému vyhrožování. Cesta k eliminaci obdobných případů vede přes důsledné dodržování stanovených směrnic, mlčenlivosti a naprosté profesionality obsluhy pramenící z průběžného proškolování a kontrolní činnosti nadřízených.

12.2 Ergonomie a hygiena práce

Monitorovací pracoviště tvoří spolu s operátory jádro systému a úspěch či neúspěch proto zcela závisí na této premise. Mnoho systémů bezchybných po stránce technické selhalo právě vinou práce monitorovacího pracoviště. Při budování CCTV proto nelze opomenout ergonomické a hygienické zásady a dodržet všechna závazná ustanovení týkající se osvětlení, konstrukce nábytku, rozmístění ovládacích prvků, obrazovek, místa pro pořizování poznámek apod. Režimové pracoviště musí být vybaveno klimatizací nebo regulovaným zdrojem tepla a ventilátorem, chladničkou a snadno dostupným sociálním zařízením. Na pracovišti operátorů se nekouří. Cigaretový kouř škodí i technice i zdraví.

Počet monitorů pro obsluhu by měl být určen na základě počtu instalovaných kamer, funkčních hledisek a počtu operátorů ve službě. Není možné vybavit kontrolní místnost zbytečně velkým počtem monitorů (tvar, kvalita). Počet kamer k monitorům by neměl překročit poměr 10:1. Velikost obrazovky monitoru by měla být volena optimálně vzhledem k pozorovací vzdálenosti. Doporučená vzdálenost činí přibližně pětinásobek úhlopříčky zobrazení. Obrazovka monitoru či počítače, podle toho, čím je vyhodnocovací pracoviště vybaveno, je místem, kde je

nejužší kontakt mezi člověkem a technickým podsystémem. Způsobům, jakým se elektronicky zpracovávaná informace dostává k lidem, je třeba věnovat maximální pozornost. Lidské oko se velmi rychle unaví, pokud bude přetíženo pozorováním nekvalitního obrazu.

Velikost objektu na obrazovce monitoru musí být odvozena od požadovaného stupně jeho rozpoznání. Je-li cílem osoba a CCTV systém má omezenou rozlišovací schopnost cca 400 televizních řádků, doporučují se následující minimální velikosti pozorovaného objektu na obrazovce:

- Pro identifikaci by cíl neměl představovat méně než 120 % výšky obrazovky.
- Pro rekognoskaci by cíl neměl představovat méně než 50% výšky obrazovky.
- Pro detekci by cíl neměl představovat méně než 10% výšky obrazovky.
- Pro monitorování skupiny osob by cíl neměl představovat méně než 5% výšky obrazu.

12.3 Vnitřní směrnice, režimová opatření

Vnitřní směrnice takovéhoto pracoviště se musí řídit zákonnými podmínkami pro výkon práce a musí obsahovat určité odlišnosti, neboť činnost na vyhodnocovacím pracovišti se musí blížit standardům pro zvláštní režimová pracoviště. Koncept CCTV je v každém městě jedinečný. K obecným pracovně právním předpisům bude v podmínkách obecní policie patřit zejména zákoník práce a zákon o obecní policii. U příslušníků Policie ČR je potom tato oblast řešena jiným zvláštním předpisem - zákonem o služebním poměru a zákonem o Policii ČR. Pokud kamerový systém obsluhují jiní pracovníci (např. zaměstnanci soukromých bezpečnostních služeb nebo obyčejní civilisté), vztahují se na ně ustanovení zákoníku práce.

Vlastní rozvrh pracovních hodin obsluhy bude přímo úměrný velikosti města, počtu kamerových bodů, složitosti bezpečnostní situace a v neposlední řadě počtu možných a vhodných operátorů. Operátoři se během dne střídají jak na operačním pracovišti, tak v normálních pěších či motorizovaných hlídkách ve městech. Tím neztratí místní a osobní znalosti, nebudou odtrženi od bezpečnostní reality ve městě a budou dobře organizovat z centrály CCTV případný zákrok bezpečnostních sil. Podstatným problémem je počet hodin, kdy je pracovník obsluhy schopen pozorovat snímanou scénu a vyhledávat zde možné počátky nevhodného chování.

13 LEGISLATIVNÍ POŽADAVKY NA VÝBĚROVÉ ŘÍZENÍ

13.1 Veřejná zakázka malého rozsahu (§ 49b)

Zadavateli je dána možnost zadat zakázku konkrétnímu uchazeči za cenu v místě plnění obvyklou. Zadavatel se tedy řídí výhradně situací na trhu. Zákon nepředepisuje povinnou dokumentaci. Je však nutné ošetřit smluvně předmět zakázky, vést předepsaným způsobem faktury a daňové doklady. Dle místních podmínek si lze vztah zadavatel - uchazeč blíže specifikovat.

13.2 Zjednodušené zadání veřejné zakázky (§ 49a)

Obdobně jako předchozí způsob zadávání veřejné zakázky nevyžaduje písemnou formu styku zadavatele s uchazeči. Takovouto zakázku lze tedy zadat ústně či telefonicky (§ 68 zákona). Podle mého názoru takovéto řešení není velmi šťastné. A to z toho důvodu, že má-li mít nabídka požadovanou průkazní hodnotu, měla by mít písemnou podobu.

Výzva k podání nabídky musí být zaslána nejméně třem zájemcům. To neplatí, pokud zadavatel již má alespoň tři nabídky k dispozici. I zde je vhodná písemná forma, i když to zákon nevyžaduje. Pokud ale dojde k ústní či jiné nepísemné formě výzvy, zákon stanoví zadavateli povinnost doložit ji písemným záznamem. Zde by měl být záznam ověřený.

Kromě výše budoucího peněžního závazku stanoví zákon u tohoto druhu zadávání veřejné zakázky další tři podmínky zpracování nabídkové ceny podle místa plnění veřejné zakázky, dobu plnění a další podmínky plnění veřejné zakázky (obě tyto podmínky musí být stanoveny ve výzvě) a zveřejnění textu výzvy k podání nabídky na centrální adrese, a to i v případě, že zadavatel má již tři nabídky k dispozici. Další, zákonem vymezené podmínky u tohoto druhu veřejné zakázky nejsou. Přesto nebude na závadu stanovit v podmínkách případnou povinnost prokázat kvalifikační předpoklady, či alespoň oprávnění k podnikání apod.

Hodnocení nabídek je rovněž věcí zadavatele. Zákon mu nestanoví žádný závazný postup. Proto je možné nabídky hodnotit komplexně podle toho jak jsou výhodné. S uchazečem jehož nabídka byla vybrána, uzavře zadavatel smlouvu.

13.2.1 Přijímání nabídek a otevírání obálek

Zákon u tohoto druhu zadávání veřejné zakázky ponechává zadavateli prostor, jak si tuto část procesu veřejné zakázky upraví. Jde však o úkony, které by měl zadavatel v duchu respektování práva řádně a objektivně dokumentovat a doložit. Je proto na místě přiměřeně respektovat úpravu části druhé zákona, platnou pro obchodní veřejnou soutěž (konkrétně ust. §§ 27 až 30) a doručené nabídky řádně označit, jmenovat komisi pro otevírání obálek (alespoň tříčlennou) a zpracovat o otevírání obálek protokol.

13.2.2 Posuzování a hodnocení nabídek

I v této činnosti je vhodné, aby se zadavatel řídil alespoň přibližně podmínkami průběhu obchodní veřejné soutěže, i když zákon tento závazný způsob nestanoví. Doporučuje se jmenovat komisi pro posuzování a hodnocení nabídek (tři až pět členů, náhradníky není nutné jmenovat), zpracovat prohlášení členů komise o nepodjatosti. Komise posoudí nabídky z hlediska kvalifikačních předpokladů a provede zhodnocení nabídek podle určených kritérií, zpracuje zprávu (§ 37) a veškerou dokumentaci předá zadavateli.

13.2.3 Oznámení výsledku výběru nejvhodnější nabídky, uzavření smlouvy a evidence veřejné zakázky

Zákon stanoví zadavateli povinnost oznámit své rozhodnutí o výběru nejvhodnější nabídky všem zájemcům (§ 49 odst. 10). Součástí oznámení je poučení o možnosti podat k rozhodnutí zadavatele námitky. Povinnost uzavřít smlouvu se zájemcem, který předložil nejvhodnější nabídku, plyne přímo ze zákona, pokud si zadavatel v podání nevyhradil možnost neuzavření smlouvy se žádným ze zájemců. Po uzavření smlouvy je zadavatel povinen ve lhůtě 15 dnů zpracovat a odeslat evidenční list zakázky orgánu dohledu. Liší-li se cenové údaje veřejné zakázky uvedené v evidenčním listu o více než 10 %, je zadavatel povinen do 15 dnů od splnění veřejné zakázky zaslat orgánu dohledu evidenční list veřejné zakázky s uvedením údajů podle skutečnosti (skutečné ceny zakázky) .

13.3 Obchodní veřejná soutěž

Jedná se o nejsložitější druh zadávání veřejné zakázky, v němž zákon taxativně stanoví podmínky, které musí být splněny. Veřejnou obchodní soutěž lze podle specifických úkonů rozdělit zhruba do osmi činností. Jsou to: zveřejnění obchodní veřejné soutěže, předávání zadávací dokumentace, přijímání nabídek, otevírání obálek s nabídkami, posuzování a hodnocení nabídek, oznámení o výběru nejvhodnější nabídky, uzavření smlouvy a ukončení obchodní veřejné soutěže. Z jednotlivých činností pořizuje zadavatel přesnou dokumentaci, která má dokladovat zákonnost postupu a bude sloužit příslušným orgánům kontroly i orgánům dalším.

13.3.1 Posuzování a hodnocení nabídek

Komise pro posuzování a hodnocení nabídek - zákon specificky upravuje v ustanoveních paragrafů 31 až 37. Zadavatel jmenuje komisi, jejíž členové zpracují (podepíší) čestné prohlášení o nepodjatosti a zvolí si předsedu a místopředsedu. V úvodu komise posoudí nabídky z hlediska úplnosti a též obsahu. Při zjištění nedostatků navrhne zadavateli vyloučení nabídky. Komise provede kontrolu prokázání kvalifikačních předpokladů a kontrolu zda nabídka obsahuje všechny požadavky podmínek soutěže. Je-li vše v pořádku, postoupí nabídka do hodnocení nabídek.

Vlastní hodnocení nabídek je velmi důležité a vyžaduje naprostou objektivitu v uplatňování určených kritérií soutěže. Je vhodné mít zpracována kritéria tak, aby po vyhodnocení soutěže nebylo rozhodnutí zadavatele napadnutelné. V práci komise je důležité to, že hodnocení nabídek provádí každý člen komise pro každou z nabídek u každého kritéria. Komise v každém kritériu určí pořadí nabídek a přidělí podle pořadí body. Získaný počet bodů pak určuje pořadí nabídek. Z jednání komise pořídí zápis, v němž má být stručně popsáno, co bylo předmětem jednání, jaké postupy komise při hodnocení zvolila. Popíše též vlastní průběh jednání. Před ukončením činnosti zpracuje komise zprávu o posouzení a hodnocení nabídek a předá ji zadavateli - zprávu podepisují všichni členové komise.

13.3.2 Uzavření smlouvy

Po uplynutí lhůty k podání námitek, nebyla-li námitka podána, jsou jak zadavatel, tak i uchazeč povinni uzavřít smlouvu. Je vhodné, aby zadavatel určil uchazečům povinnost zahrnout do jejich návrhu smlouvy to, co sám považuje za důležité a na čem bezpodmínečně trvá.

13.3.3 Ukončení obchodní veřejné soutěže

Po uzavření smlouvy s uchazečem stanoví zákon zadavateli povinnosti, vztahující se k ukončení obchodní veřejné soutěže:

1. Do 15 dnů po podpisu smlouvy odeslat na Úřad pro ochranu hospodářské soutěže evidenční list zakázky.

2. Do 30 dnů po podpisu smlouvy uveřejnit výsledek soutěže v Obchodním rejstříku.

3. Liší-li se údaje o ceně po splnění veřejné zakázky o více než 10 % oproti ceně původní - zadavatel zašle do 15 dnů od splnění veřejné zakázky nový evidenční list zakázky a zveřejní v Obchodním rejstříku na centrální adrese skutečnou cenu zakázky.

13.4 Výzva jednomu zájemci k podání nabídky (§ 50)

Ve speciálních případech, zákonem vymezených, je zadavateli umožněno zadat veřejnou zakázku zadáním výzvy jednomu zájemci. Sleduje se tím řada potřeb, jako např. zbytečné náklady na jiné podání nebo nemožnost zveřejnění soutěže, časová tíseň apod. Zákon je vymezuje v ustanovení § 50.

14 VYHODNOCENÍ VÝBĚROVÉHO ŘÍZENÍ

Při vyhodnocení musí být vyřazeny všechny nabídky, které neodpovídají provozním požadavkům. Klíčové je hodnocení podle stanovených kritérií ve stanoveném pořadí priorit. Zde si dopředu připravíme pro členy výběrové komise hodnotící tabulky a předem dohodneme systém vyhodnocování. Pro jednání výběrové komise je vhodné připravit srovnávací tabulky cen podle stanovené struktury. Technickou část nabídek je možno nechat posoudit třetí, nezávislou stranou. Vlastní průběh testů v rámci užšího kola výběrového řízení je možno postavit na zkušebních postupech s využitím testovacího objektu ROTAKIN dle ČSN EN 50132-7. Metodika hodnocení může kopírovat dohodnuté postupy kvantifikace z prvního kola a převádět buď přes bodovou stupnici hodnocení na pořadí, či přímo stanovovat pořadí v jednotlivých testech, a poté přes součty bodů či četnost umístění na jednotlivých příčkách pořadí stanovit vítěze.

14.1 Funkčnost navrhovaného projektu

Funkční požadavky na CCTV musí zpracovávat osoba s odbornou kvalifikací, která jasně stanoví představu zadavatele, jak má systém pracovat. Představa o tom, k čemu, kde, kým a proč bude systém využíván, musí vycházet z důkladně provedené analýzy trestné činnosti daného místa, z doporučení evropských norem a Odbor prevence kriminality (dále jen OPK), ze stanovisek zástupců města, obce, manažera prevence kriminality, ze zkušeností operátorů, policejních techniků, kriminalistů atd.

14.2 Hodnocení projektů

Velmi často je velký rozdíl mezi znalostmi, požadavky a návrhy zadavatele, které předkládají firmy. Způsobuje to neznalost problematiky ze strany zadavatele, který sice rozhoduje o udělení veřejné zakázky, ale mnohdy nemá odborníky s patřičným vzděláním. Je optimální, když se výběrová komise při posuzování a hodnocení předložených projektů řídí kromě zákona č. 199/94 Sb., o zadávání veřejných zakázek, ve znění dalších předpisů, i stanoviskem nezávislého odborného subjektu (zkušebna, soudní znalec, technický expert). Tento subjekt může poskytnout členům výběrové komise celou řadu důležitých technických a organizačních argumentů a množství vlastních zkušeností. Stanovisko nezávislého subjektu slouží k usnadnění rozhodování výběrové komise. Vlastní hodnocení nabídek je však vždy v plné kompetenci zadavatele.

15 PROJEKT CCTV

Pod pojmem "projekt" zde nechápeme detailní technické řešení jako podklad pro realizaci. Je to soubor podkladů různých aktivit, které navrhuje město, zapojené do programu prevence kriminality, pro daný rok k realizaci. Častým požadavkem v rámci projektu bývá žádost o cílenou podporu prvků technické prevence kriminality ve městech.

15.1 Kroky tvorby projektu

15.1.1 Vytvoření týmu

Prvním krokem by mělo být vytvoření průřezového týmu, který by zahrnoval všechny zainteresované strany. CCTV pomáhá řešit problémy více zájmových skupin ve městě a kompetentní zástupci těchto skupin mohou přinést jiný zorný úhel.

15.1.2 Identifikace možných problémů

V tomto stádiu je třeba nechat techniku nutnou pro dobré zvládnutí CCTV stranou a identifikovat problémy. Nesmíme si myslet, že CCTV problémy vyřeší - a pak se snažit, aby je skutečně vyřešil. Cílem je získat vyčerpávající seznam relevantních problémů vztahujících se k prevenci kriminality. Velmi důležité jsou údaje od policie, od obchodníků, od místního úřadu a ostatních zainteresovaných stran.

Některé okruhy problémů, které mohou vyplynout:

- Vykrádání a krádeže motorových vozidel na ulicích a parkovištích.
- Vykrádání a krádeže v obchodech
- Vandalismus.
- Užívání nebo prodej drog.
- Opilství.
- Vloupání do nejrůznějších objektů.
- Strach ze zločinnosti mezi obchodníky i návštěvníky.
- Teroristické útoky.
- Rasové útoky.
- Sexuální obtěžování.

- Krádeže nebo loupežná přepadení.
- Krádeže pohonných hmot

CCTV může fungovat ve spojení s účinnějším rozmístěním bezpečnostních stráží nebo policistů, kteří tak mohou "chytit" pachatele přímo při činu, ztlumit problémy v zárodku nebo zakročit proti skupinám bezdomovců, zabránit potenciálním pachatelům v páchání zločinů, protože riziko přistižení je větší, získávat důkazy, které mohou napomoci k nalezení a usvědčení pachatelů, ujistit uživatele centra města, že jsou ve větším bezpečí, varovat ty, jejichž chování je podezřelé, upoutat pozornost na zločiny v centru města, umožnit nalezení a zadržení pachatelů buď na ulici, nebo při páchání dalších přestupků a jako nástroj ke zvýšení pořádku v centru města.

CCTV sami o sobě samozřejmě k prevenci zločinu nestačí. Podle všeho je k uchování účinnosti opatření na prevenci proti zločinu nesmírně důležitá publicita. Dobře míněná opatření na prevenci proti zločinnosti mohou někdy bohužel problémy nejen řešit, ale i působit. Musíme si uvědomit některá potenciální rizika např. že CCTV přesune zločinnost do jiné části. Pokud jsou zavedena opatření na prevenci proti zločinu ne všechny zločiny se přesunou. A příznivé účinky CCTV mohou alespoň po nějakou dobu dosáhnout i za hranice své oblasti. CCTV nesmí snížit bdělost jinak aktivních občanů. Zavedení CCTV nesmí vyvolat přehnaný pocit bezpečí mezi zranitelnými členy komunity. Bude třeba jim připomínat, aby byli vůči riziku zločinnosti stále ostražití.

15.2 Systémový návrh - koncept CCTV

Od CCTV se očekává, že se kamery budou dívat, otáčet se a monitory budou ukazovat obrázky s vysokou rozlišovací schopností. Záznamová zařízení budou zaznamenávat tak, abychom rychle našli informaci, kterou potřebujeme. Předpokládáme, že vše bude dobře a dlouho fungovat. Nemusí tomu tak být vždy. Příčin ohrožení funkčnosti systému je celá řada. Vliv všech těchto příčin je umocňován nebo zmenšován systémovým návrhem - konceptem CCTV. Všechna tato ohrožení je třeba eliminovat výběrem vhodných prvků a instalací příslušných ochran na všech místech CCTV. Všechny příznaky ohrožení nebo závady narušující chod musí být okamžitě "nahlášeny" operátorovi. Rozhodující skupiny systému musí mít zálohované napájení a systém se musí dát ochránit i proti samotnému operátorovi.

15.2.1 Celková odolnost systémů

Odolnost je vedle výkonnosti nejdůležitější vlastností systémů. Kvantifikací úrovně odolnosti a kvalifikací jednotlivých "odolnostních" opatření je možno stanovit, jak dlouho a za jakých vnějších podmínek bude systém pracovat. Výkonnostní a odolností parametry systému od sebe nelze úplně oddělit. Zvyšování odolnosti klade značné nároky na zvyšování finančních nároků. Správná definice odolnostních parametrů a z nich vyplývajících technických opatření je součástí podstaty správného návrhu efektivního systému.

15.3 Východiska konceptu CCTV

CCTV jsou prostředky policie ke zvýšení bezpečnosti občanů, k prevenci a potírání kriminality, sledování dopravní situace na exponovaných místech města. Jsou to technické systémy obsluhované pracovníky, kteří jsou schopni vyhodnotit z televizního obrazu stupeň nebezpečnosti chování závadových osob nebo stupeň ohrožení občanů a předat tyto informace orgánům schopným zasáhnout a pomoci. Kromě reálného zachycení právě probíhajícího dění je pořizován videozáznam potřebný k následné analýze událostí, případně k vyšetřování.

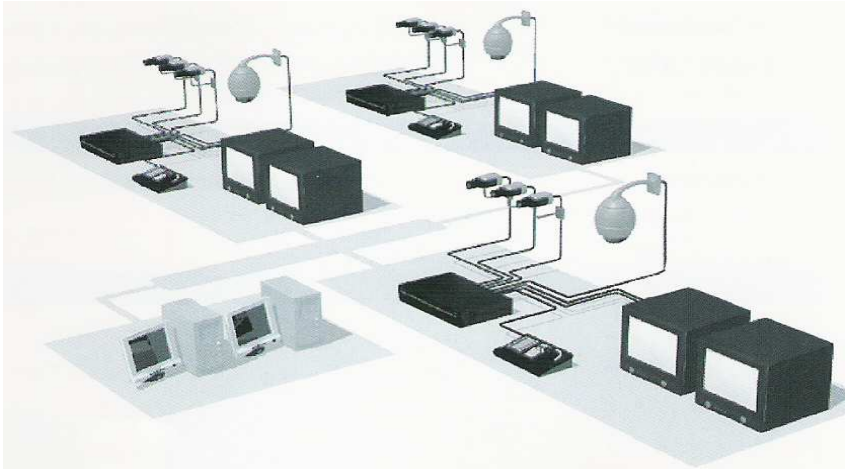
Systém musí být schopen vytvářet struktury šetřící nákladná spojovací zařízení vytvářením skupin (buněk) sdílejících technické prostředí, nezávisle zobrazovat a dokumentovat přehled o situaci i detail, kontrolovat své funkce, kontrolovat činnost obsluhy, řízení předem naprogramovaným automatem nebo ručně - operátorem, případně kombinovaně a sdružovat se s dalšími bezpečnostními subsystémy. Schopnost kontroly je základní systémovou vlastností a musí být všestranně podporována technickými parametry jednotlivých prvků systému a řídícího členu.

CCTV je zařízení se širokou působností. Je to systém pořízený z veřejných prostředků, jeho provoz je z veřejných prostředků hrazen, jeho prostřednictvím je veřejnost sledována a veřejnosti musí být umožněna jeho důsledná kontrola. Tento kvalitativní posun oproti privátním systémům, způsobený požadavkem veřejnosti a odpovědnosti CCTV, se musí projevit ve struktuře systému. Řídící člen a způsob, jakým komunikuje s ostatními prvky systému, zásadně ovlivňují veškeré systémové vlastnosti a charakteristiky. Na tomto místě dobře poslouží analogie s procesem rozvoje pultů centralizované ochrany (dále jen PCO). Na PCO se využívají vysoce výkonné

počítače, schopné provozovat rozsáhlé databáze a zajišťující svým programovým vybavením vysoký stupeň kontroly činnosti operátora a technického prostředí. Stejným způsobem lze směřovat i vývoj CCTV. Vhodnou strukturou CCTV jak z výkonnostního, tak z odolnostního hlediska, je stromová struktura s decentralizovanou inteligencí, s prvky obousměrně komunikujícími, jejímž ústředním řídícím prvkem je počítač. Počítač pracuje podle pokynů operátora zadávajícího mu příkazy operativně, ovládá systém podle předem připravených a naprogramovaných variant z podnětu automaticky vyhodnocovaných vnitrosystémových stavů nebo z podnětu vněsystémových příčin. Struktura může být ve vhodných případech, kdy se jedná o malý a vhodně dislokovaný systém, zjednodušena až do podoby triviální struktury hvězdicové.

15.3.1 Způsob řízení systému

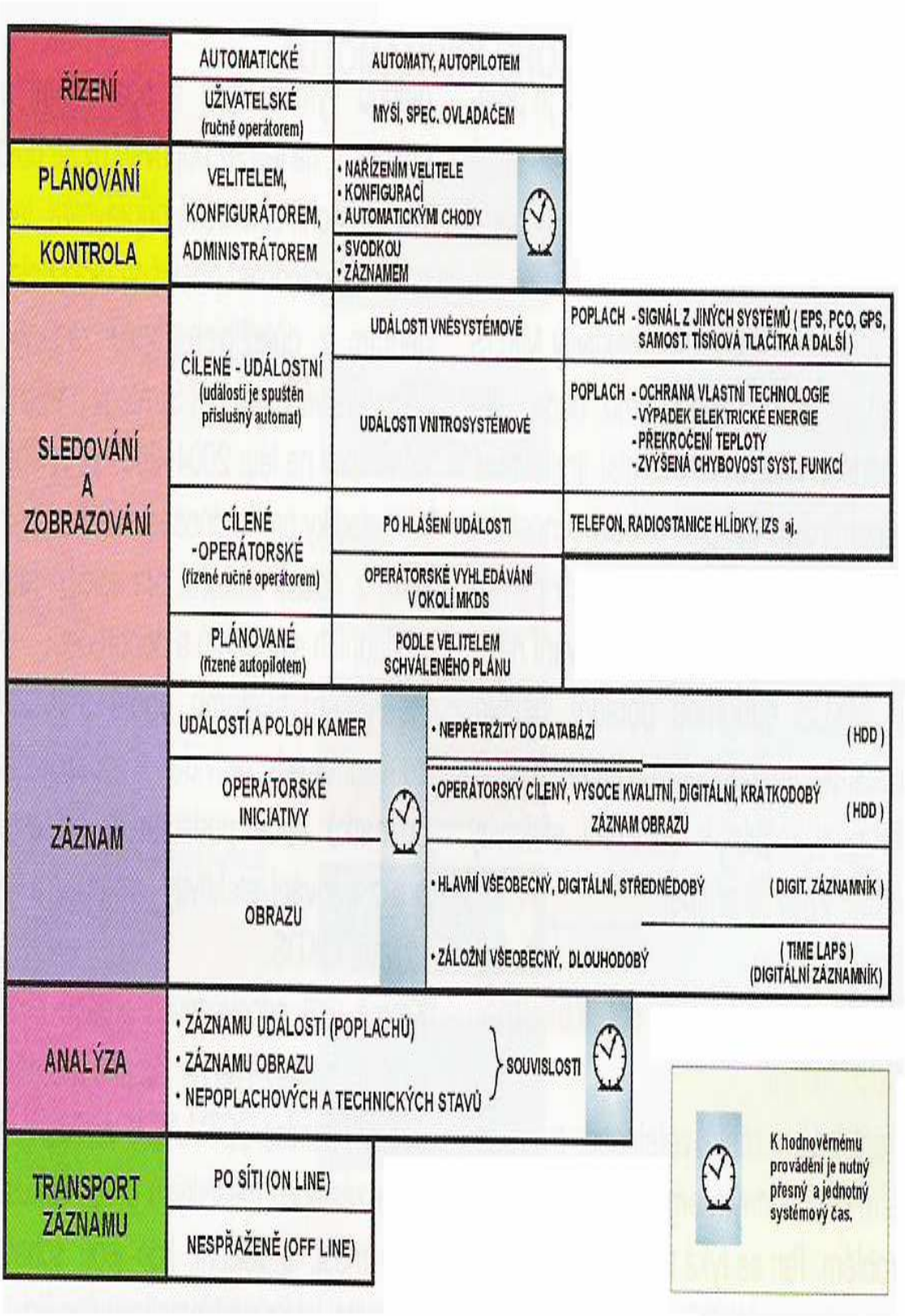
Řízení systému je výhodné orientovat "počítačově". Zařízení (kamery, polohovací hlavice, objektivy, přepínače, kvadrátory, multiplexery, pojítka, záznamová zařízení, detektory pohybu apod.) jsou připojena prostřednictvím mezilehlých programovatelných jednotek k počítači. Počítačově řízeny musí být zejména změny režimů činnosti snímacích zařízení, změny polohy snímacích, přepínání cest videosignálu mezi snímacími, záznamovými a zobrazovacími jednotkami, změna rychlosti nahrávání, analogový nebo digitální záznam, identifikace záznamu, změna pořadí a délky nahrávaných scén a komunikace mezilehlých počítačů s hlavním počítačem.



Obr. 23. Zapojení několika samostatných systémů

prostřednictvím počítačové sítě

Tab. 8. Tabulka funkcí CCTV



Počítačové řízení umožňuje efektivně sbírat data o průběhu chodu systému, výsledcích testování technologií a všech použitých režimech práce. Tato technická možnost podmiňuje kontrolní činnost o využívání systému, vytváří předpoklady pro efektivní preventivní údržbu a kromě uchovaných videozáznamů je dalším informačním zdrojem. Programové vybavení řídícího počítače a mezilehlých programovatelných jednotek musí kromě výše uvedených činností zabezpečit viditelné a slyšitelné upozornění o nestandardních (chybných) stavech zařízení a o jeho ohrožení okolím. Zejména pak o vzniku podmínek pro narušení činnosti zařízení lidmi nebo jinými okolními vlivy, jimiž mohou být přechod na náhradní zdroje, snížení průchodnosti komunikačního systému, napadení vzdálených součástí systému, indikované elektrickou zabezpečovací signalizací. I Pokles nebo vzrůst teploty zařízení nad stanovenou mez apod. Programové vybavení musí podporovat rychlý přechod jednotlivých systémů do samoochranného režimu (rozsvícení bezpečnostního osvětlení, spuštění odstrašujících promluv, připojení speciálních bezpečnostních kamer sledujících přístupy k technologii do sledovacích a záznamových režimů).

15.3.2 Komunikace

V dosud realizovaných aplikacích CCTV jsou používány v zásadě oba způsoby komunikování jednosměrné a obousměrné. Pro splnění veškerých náležitostí a pro plné využití technických možností celého konceptu CCTV se jeví jako výhodnější obousměrný způsob komunikace, založený např. na principu duplexního nebo poloduplexního přenosu dat realizovaného např. široce užívaným průmyslovým protokolem RS-485. Způsob komunikace předpokládá nadřízený řídící člen a podřízené prvky. Snímáním některých hodnot vhodnými hlásiči a jejich vyhodnocováním v jednotlivých mikropočítačích nebo v hlavním počítači lze stav systému předpovídat a dělat příslušná opatření (detektorem elektrického zabezpečovacího systému je možno předpovědět, že dojde k napadení systému zlodějem, vandalem apod.) Díky aplikaci tohoto způsobu komunikace mohou být zpětné vazby v systému realizovány již v datové úrovni.

15.3.3 CCTV jako prostředky důvěryhodného odstrašování

CCTV mimo základní funkce - dohlížení na bezpečnostní situaci v daném místě - plní i funkci

důvěryhodného odstrašování potenciálních pachatelů, tedy funkci nanejvýš preventivní. Zajímavá je proto zkušenost s instalacemi tzv. kamerových kamuflů, kdy jde pouze o vnější kryty bez vnitřní optiky a elektroniky. Takto "vybavené" kamery je možno velmi operativně přesunovat, aniž by to průměrný občan zpozoroval. Do mechanismu důvěryhodného odstrašování také patří uniformy policistů a strážníků, jejich označená vozidla, případně viditelně umístěné nálepky na zabezpečených objektech a viditelně umístěné poplachové sirény a další zařízení, běžně ztotožňovaná se zabezpečovacími systémy a videosystémy. Na rozdíl od elektrického zabezpečovacího systému (dále jen EZS) má populace mnohem rozvinutější představy o možnostech televizních kamer a přítomnost kamery stimuluje jednání lidí. Odstrašování související s CCTV je způsobeno atributy jako jsou viditelností kamerových neprůhledných krytů, na nichž není patrno, kam je kamera právě směřována, neznalostí všech technických možností CCTV, vytvářející prostor pro fantazii, popularizací správně vybraných technických možností a statistických údajů, nepřehlédnutelným označením, že je veřejné prostranství pod kontrolou CCTV. Důvěryhodnost je podporována zejména popularizací úspěšných příkladů využití CCTV v regionálním tisku, kabelové televizi, regionálním rozhlasovém vysílání, viditelnou péčí o systém, dobrou technickou úrovní systému, zamezením neřízené popularizace, jinak řečeno úmyslné nebo náhodné dekonspirace vedoucí k odhalení slabých míst systému a jejich zveřejnění.

15.3.4 CCTV jako součást bezpečnostních a záchranných systémů

Přehlednost, kvalita a obsažnost archivovaných záznamů je zajištěna vícenásobným nahráváním. Optimálním způsobem zobrazování umožňuje rychlý přechod libovolné scény z digitalizovaného zobrazování na věrné přímé zobrazení zájmové scény. V takto pojatém systému je velká pozornost věnována ochraně před elektrickým přepětím a výpadky napájecího napětí. Systém disponuje zařízením pro obnovu a normalizaci videosignálu. Všechny funkce znázorněného systému jsou řízeny počítačem nebo jeho prostřednictvím. Systém je vybaven obousměrným přenosem dat.

15.3.4.1 Definování používaných pojmů

Řízení = *p*roces, prováděný člověkem nebo automatem, vycházející z plánu a reagující na okolní a vnitrosystémové podmínky.

Operativnost = reakce na nepředvídané okolnosti jsou podmíněny přítomností a kvalitou lidského činitele.

Rychlost = neomylnost reakcí na předem definované stavy jsou dány použitím řídícího automatu hlavního počítače.

Kvalita řízení = je podmíněna kvalitou zpětné vazby, umožněné obousměrným dostatečně průchozím přenosem dat.

15.3.4.2 Struktura organizace transportu videosignálů

Technické prostředí, jehož funkce plní řídící počítač a spočívají ve vytvoření cesty videosignálu od kamery po obrazovku nebo videonahrávač.

Brána = soubor zařízení určených k normalizování vstupních signálů, tj. k jejich očištění od účinků vnějších elektromagnetických polí, ke galvanickému oddělení dlouhých metalických vedení od citlivé a drahé elektroniky centra a k přeměně transportního tvaru signálu do tvaru zpracovatelného technologií centra.

Kamerové místo = kamerový terminál, slouží jako ochrana proti zlodějům, vandalům a zvědavcům, ochrana proti přepětí. Záložní napájení s indikací výpadku sítě. Zařízení pro přenos dat a videosignálů.

Distribuční stanoviště = prostor, v němž je dislokováno zařízení pro přenos dat a videosignálů, zajišťující vhodné podmínky pro šíření rádiových vln a umožňující optimální propojení těchto zařízení s místem řízení CCTV.

Zobrazování = hlavní produkt CCTV využívaný lidskou částí řídícího místa CCTV a dalšího místa řízení k okamžitému jednání v důsledku právě pozorované scény.

Záznam = hlavní produkt CCTV využívaný lidskou částí řídícího místa CCTV, dalšího místa řízení a dalšími odpovědnými osobami k analýze předchozích událostí zachycených v zobrazené scéně.

Cílené sledování = dochází k důležité změně v pojetí funkcí CCTV, způsobené interakcí s jiným zcela nezávislým systémem. Hlavní myšlenkou cíleného sledování je zařídit, aby ohrožené objekty volaly kamerový systém v případě nouze samy. Následné rychlé natočení

kamer do předem určených směrů zvyšuje pravděpodobnost zachycení důležitých markantů na záznamové médium a průvodní poplachový signál v řídícím centru přivolá pozornost operátora. Nejdůležitější technologií pro realizaci cíleného sledování je obousměrný přenos dat a schopnost systému nastavovat polohovací hlavice do předem nastavených pozic nebo v lepším případě do pozic definovaných automaticky předávanými souřadnicemi.

Další místo řízení = pracoviště vybavené kompetencemi, prioritami, lidmi a technikou k převzetí řízení části CCTV a využívání jeho produktů. Další místo řízení (dále jen DMŘ) již nemusí být součástí CCTV. DMŘ ovlivňuje CCTV přímo manuálními operacemi svých příslušníků nebo daty produkovanými automaticky jinými procesy dalšího místa řízení.

Celkové rozhodnutí o budování CCTV musí být totiž jedním ze závěrů bezpečnostní koncepce, z níž vyplyne, že CCTV je systémem účelně propojený s ostatními bezpečnostními systémy do efektivně pracujícího komplexu.

16 PROJEKT BEZPEČNÁ LOKALITA

16.1 Pilotní projekt

Projekt „Bezpečná lokalita „ byl dne 27. září 2001 doporučen Poradním sborem pro situační prevenci kriminality MV (dále jen PS MV). Projekt „Bezpečná lokalita“ má dát konkrétní příklad a návod všem lidem v ČR, kteří se nehodlají smířit s kriminalitou v místě svého bydliště a hodlají jí aktivně čelit. Projekt nabízí rychlé a efektivní řešení, jak docílit pocitu bezpečí a pořádku v konkrétním domě. Jeho cílem je minimalizovat podmínky pro páchání trestné činnosti dostupnými organizačními a technickými prostředky.

Od tohoto projektu se očekává podstatné omezení pohybu cizích lidí v objektech, zvýšení ochrany majetku před vandaly, snížení rizika krádeží v bytech, sklepních kójích, zvýšení bezpečnosti především žen, dětí a seniorů v objektech a snížení náhrad vyplácených pojišťovnami, vyvolání zájmu dalších vlastníků domů o podobné projekty zejména na větších sídlištích.

16.2 Závěrečné shrnutí projektu Bezpečná lokalita

Projekt "Bezpečná lokalita" je dlouhodobá celostátní preventivní akce MV a Policie ČR, zaměřená na ochranu majetku a osob. Lokalita je bezpečná pouze tehdy, když budou bezpečné její základní prvky - občané, obydlí, okolní prostředí atd. Projekt "Bezpečná lokalita" vyváženě propojuje sociální a situační prevenci kriminality. Je projektem, který je otevřený všem subjektům v oblasti ochrany majetku a osob. Smyslem projektu "Bezpečná lokalita" není vytváření nedobytných pevností a izolovaných lokalit, ale bydlení, které vytváří přirozené podmínky pro vzájemný dohled a spolupráci občanů.

17 INFORMAČNÍ TECHNOLOGIE A SYSTÉMY VE SLUŽBÁCH PREVENCE KRIMINALITY

Je zřejmé, že značný rozsah přestupkové a trestné činnosti generuje na vstupech bezpečnostních systémů obrovské množství dílčích událostí, které musí policejní složky zachytit, detekovat a reagovat na ně. Bezpečnostním systémem přitom rozumíme soubor lidských sil, technických prostředků, norem apod, zaměřených na ochranu v nejširším slova smyslu před výskytem nebezpečných a ohrožujících událostí i jejich důsledky. Činnost bezpečnostních složek, především pak činnost Policie ČR i místních složek městských policií, je nepochybně jedním z hlavních faktorů prevence kriminality. Vybavení policejních složek výkonnými informačními a bezpečnostními technologiemi, která umožňují zrychlit první reakci systému, má rozhodující účinky i v oblasti prevence kriminality. Ukazuje se však, že účinnost bezpečnostního systému neroste lineárně s rostoucím nasazováním technologických prostředků a systémů a mnohdy neodpovídá očekáváním.

17.1 Koncepce systému

Navržený systém pro podporu práce městských policií a Policie ČR je řešen jako důsledně integrovaný bezpečnostní systém s jednotlivými pracovišti, propojenými do řídícího jádra systému. IBS je systémem událostního typu. To znamená, že činností obsluhy nebo činností automatických prvků systému jsou vyvolávány přesně lokalizované události, které jsou na jednotlivých pracovištích okamžitě zobrazeny. Na tyto události reaguje systém automaticky nebo z podnětu obsluhy hlavního pracoviště a pracovišť specializovaných. K základním cílům celého řešení patří vytvořit inteligentní událostní systémy pro prvotní detekci událostí, vytvořit nástroje automatické registrace událostí a odlehčit zdlouhavou práci operačních při detekci událostí, integrovat událostní podsystémy a zrychlit průchod událostí systémem, zvýšit a zlepšit okamžitou informovanost operačních pracovníků a umožnit jim rychlé a efektivnější nasazování zdrojů pro řešení jednotlivých událostí, snížit potřeby zdlouhavé hlasové komunikace operačních pracovníků a hlídek při detekci událostí a hlášení polohy a posunout práci operačních pracovníků do polohy subjektu, který rozhoduje o efektivním nasazení zdrojů.

Systém rozlišuje jednotlivé událostní podsystémy jako jsou pracoviště operačních GPS kamerový systém, EZS a PCO. Tyto událostní podsystémy mají vlastní činnost a jsou

řízeny vlastními událostními servery propojenými do celého systému pomocí tohoto propojení a pomocí automatizovaných filtrů je možno události z jednotlivých událostních podsystémů přenést do celého systému. Pracoviště IBS jsou neustále propojená a jejich činnost může být systémem synchronizována buď automaticky nebo z podnětu operátora. Každá událost, kterou systém registruje a zaznamenává, je lokalizována. Události jsou zobrazovány selektivně, podle typu pracovišť a naléhavosti jednotlivých událostí. Na události nejvyšší naléhavosti reaguje celý systém, na události menšího významu pouze jednotlivá pracoviště. Kromě pracovišť operátorů může v systému existovat libovolný počet klientských pracovišť, kam mohou být přenášeny a zobrazovány jednotlivé scény, nebo jejich vybrané části.

Každé specializované pracoviště - kamerový systém, GPS, EZS a PCO, popř. pult hlavního operátora, řídí samostatný server, spojený s příslušnými technickými komponentami událostního podsystému. Kromě specializovaného serveru, který běží v pozadí, je v činnosti i tzv. "lokální klient", který pracuje na tomtéž počítači jako specializovaný server. Lokální klient umožňuje řídit a modifikovat práci serveru a je vlastním komunikačním prostředkem příslušného operátora s daným událostním podsystémem. Kromě lokálního klienta může mít každý událostní podsystém připojen libovolný počet vzdálených klientů, na nichž lze pozorovat aktuální scénu, z nichž však není možno řídit a modifikovat práci serveru. Lokální klienty je možno umístit na libovolná místa, dostupná v místní LAN, nebo WAN síti.

Každý událostní podsystém je vybaven prostředky pro záznam činnosti. Výskyt všech událostí je trvale zaznamenáván. Tak je možno pro každý událostní podsystém "přehrávat" (dále jen replay) jeho scény a vývoj událostí v čase. Replay každého událostního systému je možno spustit z klientských stanic. Protože všechny události jsou geograficky lokalizovány, replay probíhá i se zobrazením v mapové scéně. Tak je možno sledovat výskyt událostí trestné a přestupkové činnosti, polohy a činnost kamer i pohyb vozidel ve vybraném časovém úseku. Pro řídící pracovníky policejních složek je tak k dispozici rozsáhlý materiál pro vyhodnocování činnosti, efektivity zásahů a efektivity přidělení zdrojů.

17.2 Pracoviště operátora kamerového systému

Zde je soustředěno řízení kamer a zobrazování kamerových scén, systém nahrávání a kamerový monitoring. Jednotlivé kamery a jejich záběrové podmínky jsou zobrazeny v mapové scéně na panelu operátora kamerového systému. Na něm jsou pro informaci současně zobrazovány aktivní události z panelu hlavního operátora, popř. pohyb vozidel hlídek. Operátor kamerového systému může manuálně zaměřit kamery do míst vzniku událostí, popř. do míst pohybu hlídek.

Obr. 24. Zásah jednotky Městské policie Zlín

Z panelu operátora je možno definovat místa, plochy nebo trajektorie, k nimž mají být dostupné kamery zaměřeny. Zaměření kamer probíhá automaticky nebo manuálně. Pohyby a zaměření kamer je možno programovat v prostoru a čase. To znamená, že je možno určit, do kterých prostorů (bodů, ploch a tras) mají být kamery zaměřeny v předem určené době, impulsů. Systém má v každém okamžiku k dispozici nahrávací systém apod. Podstatou integrace kamerového systému do celého IBS je trvalé sledování činnosti kamer (zaznamenává se jakákoliv změna vektoru kamery, elevace, ohniska, aktivní kamery), integrace řídících činností a řídí informace o tom, které kamery jsou v činnosti, jak jsou zaměřeny, se kterými kamerami pracuje obsluha a u kterých kamer je spuštěn obrazový záznam. Vznikne-li v IBS událost, která je nebo může být v dosahu některých kamer, systém tuto skutečnost vyhodnotí a dané kamery automaticky zaměří na místa události. Kamerový operátor je o této skutečnosti informován. Systém současně přenese obraz vybrané kamery na monitor operačního pracovníka a automaticky spustí záznamové zařízení. Další sledování události může provádět kamerový operátor, nebo sám hlavní

operátor. Kamerovému operátorovi systém současně zpřístupní scénu události. V daném okamžiku mají tedy jak hlavní, tak i kamerový operátor na svých počítačích stejnou informaci a jejich činnost může být efektivně koordinována. Jsou-li kamery vyčleněny z pultu operátora kamerového systému (při vzniku události s vyšší nebo vysokou naléhavostí), operátor kamerového systému je o tom informován změnou zobrazení kamer v mapové scéně. Vyčleněné kamery ovládá operátor kamerového systému, nebo na podnět hlavního operátora hlavní operátor.

17.3 Reakce systému IBS na události

17.3.1 Rekce kamerového systému

Při vzniku události s vyšším nebo vysokým stupeň naléhavosti systém automaticky detekuje nejbližší kamery v dosahu, vyčlení je z řízení specializovaného pracoviště a zaměří je automaticky bez činnosti obsluhy do místa v němž byla událost lokalizována. Automaticky je zpuštěn obrazový záznam.

Obr. 25. Monitorovací bod č. 9, II. Segment – Jižní Svahy

Obraz těchto kamer je automaticky preferován a přenesen na pracoviště hlavního operátora. Tyto aktivní kamery jsou na panelu hlavního operátora zobrazeny. Řízení kamer může být rovněž přeneseno na pracoviště hlavního operátora. O vzniku situace s vyčleněním kamer je operátor kamerového systému automaticky informován na svém panelu, bez jakékoliv hlasové komunikace. Po dohodě s hlavním operátorem, operátor kamerového systému buď dále sám řídí činnost vybraných kamer nebo může jejich řízení předat hlavnímu operátoru.

17.3.2 Reakce systému dálkového satelitního sledování polohy

Při vzniku události s vyššími nebo vysokým stupněm naléhavosti systém automaticky detekuje nejbližší (aktivní) vozidla hlídek a zobrazí je na panelu hlavního operátora. Současně je na panelu hlavního operátora zobrazena optimální trasa jednotlivých vybraných vozidel k místu události. Hlavní operátor tak může, bez prodlení a bez zjišťování polohy hlídek přes pojítka,

vyslat na místo události objektivně nejbližší hlídku: popř. navigovat hlídky tak, aby se přiblížily k místu události optimá1ním způsobem (např. z různých příjezdových směrů).

Obr. 26. Křižovatka ul. Dlouhá a tř. T. Bati - monitorovací bod č. 1

Navigaci vybraných vozidel může rovněž převzít operátor GPS sledování. Pokyn k převzetí dává hlavní operátor prostřednictvím systému, tento pokyn je okamžitě přenesen. Pro vybraná vozidla, která budou použita při řešení událostí, je automaticky nastaven fokusační režim. To znamená, že GPS systém přejde z nastaveného (klidového) režimu sledování polohy v dalších časových intervalech k intenzivnímu sledování, kdy je poloha vybraných vozidel sledována v sekundových intervalech. Hlavní operátor i operátor GPS tak mají k dispozici scénu pohybu vozidel prakticky v reálném čase, mohou polohu vozidel přesně sledovat a v případě potřeby vozidla podrobně navigovat změní-li se průběh událostí.

17.3.3 Reakce hlavního operátora

Hlavním úkolem hlavního operátora (operačního důstojníka) je rozhodovat o klasifikaci a závažnosti jednotlivých událostí a přidělovat pro řešení událostí dostupné zdroje (hlídky,

popř. další zdroje IBS). Automatická komunikace v IBS snižuje časové nároky na prvotní detekci událostí snižuje nároky na hlasovou komunikaci a podstatně zrychluje proces prvotní registrace a detekce událostí. Snahou celého IBS je zbavit hlavního operátora pracné, zdlouhavé detekce a komunikace podstatnou měrou zkrátit dobu prvotní odezvy systému. Na panelech ostatních účastníků (jsou li k systému připojeni) se objeví mapová scéna s aktivními vozidly a kamerami přenesené záběry vybraných aktivních kamer kamerového systému. To umožní příslušným operátorům Policie ČR a IZS optimalizovat a lépe koordinovat své akce. Při obousměrném propojení jsou pak jejich akce zobrazeny v systému městské policie.

Hlavní operátor zajišťuje obsluhu události, tedy způsob jejího řešení a předělení potřebných zdrojů. Podrobný popisem události se zabývá jeho pomocník. Hlavní operátor může převzít řízení ostatních prvků nebo koordinovat jejich činnost. Smyslem podpory, kterou systém poskytuje, je především odstranění prodlev a zkrácení reakční doby, uvolnění hlavního operátora pro činnosti zásadního významu.

17.4 Analýza trestné a přestupkové činnosti

17.4.1 Podstata analýzy kriminality v mapovém prostředí

V prostoru středně velkého města jsou ročně zaznamenány řádově desítky až stovky tisíc událostí trestné a přestupkové činnosti. Tyto události nejsou v prostoru města rozloženy – rovnoměrně a zpravidla se koncentrují v oblastech, které představují oblasti zvýšeného rizika. Na základě výsledků přesné analýzy lze efektivně organizovat činnost hlídek, umístění prvků kamerových a signalizačních systémů apod. Uvedená opatření vykonaná na základě analýzy kriminality, patří ke krátkodobým opatřením prevence kriminality.

Analýza kriminality v prostoru města však může být provedena jako korelační analýza, pomocí nástrojů geodemografické a gebsociální analýzy. Vychází se přitom z předpokladu, že koncentrace trestné a přestupkové činnosti není náhodná, ale je podmíněna demografickými a sociálními faktory, stejně jako faktory urbanistické a technické struktury města. Tyto faktory se zpravidla vyvíjejí dlouhodobě a mají v čase poměrně značnou setrvačnost. Závěry a opatření, učiněná na základě analýzy v této oblasti, patří k dlouhodobým opatřením v oblasti prevence kriminality.

Je zřejmé, že systematická činnost v oblasti prevence kriminality bude využívat jak krátkodobých (technicky zaměřených), tak i dlouhodobých opatření (kauzálních). Systematická analýza kriminality v prostoru města je tedy významnou složkou prevence kriminality.

17.4.2 Principy analýzy kriminality v mapovém prostředí

Protože IBS pracuje s přesnou geografickou lokalizací každé události (událost je lokalizována bodem se zeměpisnými a mapovými souřadnicemi), je tak vytvořena základní podmínka pro geografickou analýzu trestné a přestupkové činnosti. Je-li k dispozici geograficky zpracovaná urbanistická struktura města (členění města na blokovou strukturu - tj. přesně ohraničené prostory, s nimiž např. pracují urbanisté při řešení územních plánů), je možno provádět základní i korelační geoanalýzu kriminality v takovéto městské struktuře.

Výsledkem takové analýzy je pak zobrazení četností jednotlivých druhů trestné a přestupkové činnosti v prostorové struktuře města a vymezení problémových a rizikových míst (analýza pro

operativní opatření), popř. souvislosti s demografickou, sociální, urbanistickou a technickou strukturou města (analýza pro dlouhodobá opatření). Výsledky geografické analýzy trestné a přestupkové činnosti lze porovnávat v čase a zjišťovat vývoj změn kriminality v prostoru města a jejich závislost např. na územně plánovacích aktivitách.

Analýza kriminality v prostorové struktuře města je systémem prováděna automaticky. Může být provedena za libovolné časové období (výskyt trestné a přestupkové činnosti může být ovlivněn i sezónními faktory), současně mohou být porovnávány výsledky dvou či řady analýz, provedených za různá období. Projekce výsledků analýzy je systémem provedena a zobrazena ve formě digitálních map, zobrazovaných na pozadí mapové struktury města.

17.5 Závěrečné vyhodnocení

Zkušenosti ukazují, že navržené řešení je efektivní a přináší značné zvýšení okamžité informovanosti operačních pracovníků, aniž by přitom docházelo k jejich informačnímu přetížení či dokonce zahlcení. Např. informace o současném pohybu a lokalizaci vozidel je operačním k dispozici bezprostředně a je viditelná na celkové přehledové (situační) mapě - mapové scéně, aniž by tuto informaci musel operační pracovník vyvolávat, nebo zjišťovat pomocí komunikačních prostředků. Podobně je tomu i s integrací státních událostních podsystémů.

ZÁVĚR

Vstup CCTV mezi nás zabrání dalšímu rozvoji kriminality. Pocit lidí, že jsou neustále sledováni, jim nedovolí páchat zločiny v tak velkém množství a rozsahu. Neustálý vývoj a zdokonalování prostředků kamerových systémů, se stávají jednoznačným technickým prvkem v ochraně bezpečnosti a veřejného pořádku ve městech, objektech i na veřejných prostranstvích. Je důležité vyhledávat novější kvalitnější zařízení, neboť trestná činnost se neustále mění. Musí se dbát také na obměnu starého systému za novější, modernější zařízení, protože CCTV je preventivní prostředek v boji proti zločinnosti.

CCTV je důležitý faktor pro soukromé bezpečnostní složky, městskou policii i Policii ČR. Hraje významnou roli v prevenci i v boji proti kriminalitě. Pomocí kamer můžeme sledovat dění v daném úseku, předcházet působení trestné činnosti a zpětně dohledat zaznamenané údaje. Dostaneme tak celkový přehled o pohybu osob, automobilů, přepadení, krádežích, sabotážích, vandalismu i dění v lokalizované oblasti. Můžeme sledovat hustotu provozu, rychlou jízdu, autonehody a jiné stejně důležité faktory, které přispívají při dohledu na udržování veřejného pořádku. Pomocí tohoto systému se daří zabránit páchání trestné činnosti a při páchání trestné činnosti dopadnout pachatele. O tom že CCTV má velký význam pro bezpečnost slouží statistiky odhalení trestných činů, dopadení pachatelů, udržování veřejného pořádku i bezpečnosti v ulicích. Legální záznamy z kamerových systémů slouží jako důkazný materiál pro soudní řízení, k odhalení pachatelů, přestupků a dalších trestných činů. Jsou archivovány na požadovanou dobu v Policejních archívech.

CCTV se využívá i jako bezpečnostní opatření ve firmách, ke sledování pracovních výkonů, dění v prostorách firmy a pohybu osob. Dále se používá k nahrávání záznamů a v případě potřeby ke zpětnému dohledání dříve zaznamenaných skutečností. Jsou vhodné hlavně pro členité či několika poschoďové prostory, kde je nutné mít alespoň částečnou kontrolu nad pohybem návštěvníků a to z bezpečnostních nebo jiných důvodů. Mezi typickými příklady použití monitorování patří obvodové střežení, kontrola přístupu, zajištění bezpečnosti a ochrana majetku. Kamerový systém slouží k přenosu pohyblivých, nepohyblivých, černobílých, barevných i kombinovaných obrazů na dálku. Má uzavřený okruh uživatelů.

Televizní technika a prostředky CCTV se stávají běžnou součástí ochrany objektů od malých obchodů a provozoven až po rozsáhlé systémy v areálech a městských aglomeracích. Je dobře, že investoři již zařazují tuto techniku do nově plánovaných staveb. Ta nachází uplatnění v nemocnicích, hotelech, věznicích, v peněžních ústavech, v kulturních a muzejních zařízeních, při kontrole v dopravě a v důležitých technologických objektech (elektrárny,vodárny, plynárny).

Avšak nezapomínejme, že samotný systém nestačí. Velmi důležitou roli hraje operátor neboli pracovník na centrále nebo pultu centralizované ochrany. Jeho pozorovací schopnost, orientace ve sledovaném obrazu a předvídavost, může včas zabránit nebo odhalit trestný čin. Je tedy velmi důležité určit, kdo bude pracovat na monitorovacím pracovišti. To, co operátoři uvidí, musí považovat za přísně důvěrné a nesmí vzniknout ani náznak podezření, že by se nechovali v souladu se stanovenými pravidly. Proto při výběru pracovníka se klade největší důraz na kvality a schopnosti operátora. Pokud pracovníka už máme, dbáme na pravidelné školení. Neboť v prevenci je základ úspěchu.

Dalším velmi důležitým faktorem je monitorovací pracoviště. Počet řídících míst a konfigurace řídícího pracoviště jsou určeny provozními požadavky a personálními možnostmi. Tyto parametry mohou být naprosto různé. Činnosti související se sledováním by měly být soustředěny do řídícího pracoviště, které je umístěno v chráněném prostoru. Kritéria pro konfiguraci řídícího pracoviště mohou být dána systémovými parametry, způsobem záznamu obrazu, ztrátovými výkony zařízení, případnou nutností klimatizace, omezeními danými polohou a prostorem, počtem monitorů, video zařízením pro ovládání kamer. Nejdůležitější však je zabránit vstupu neoprávněných osob, do prostor pracoviště.

Při navrhování kamerového systému nesmíme zapomenout na důkladně provedené bezpečnostní analýzy v daném místě a prostoru, odstrašující psychologický efekt CCTV, možnost dalšího rozšíření stávajícího systému, možnost rychlého a účinného zákroku po signalizování zakázané činnosti na monitorovacím místě, nepřetržitou nutnost sledovat monitory, adekvátně zvolené podmínky pro obsluhu, certifikované komponenty kamerových systémů a případné zkušenosti z obdobných aplikací. Při návrhu instalace sledovacího CCTV systému je nutné brát do úvahy funkční požadavky jako např. určení zóny nebo objektů, jež jsou předmětem sledování, určení počtu a rozmístění kamer potřebných k monitorování vymezených zón nebo objektů, stanovení způsobu údržby, volba způsobu napájení, určení funkčních požadavků a provozních postupů, vyhodnocení

stávající úrovně osvětlení a provedení rozvahy o zavedení nového nebo přídavného osvětlení a volba kamer a jejich vybavení v závislosti na provozních podmínkách. Jakmile byly stanoveny zóny a objekty, které vyžadují sledování, může být stanoven počet kamer s ohledem na vybrané systémové řešení, jejich zorné pole a charakter sledovaných zón. Detaily obrazu by měly odpovídat realitě a požadované úrovni služeb. Provozní požadavky na systém, právě tak jako omezení vyplývající z umístění, případných oprav, mohou ovlivnit umístění kamer a určit případné požadavky na další kamery.

S vývojem a zkvalitňováním prostředků kamerových systémů , podle mých odhadů, budou do roku 2020 vybaveny všechny města České republiky. S růstem konkurenčního okolí a možností dosahu kamerových zařízeních, v přijatelné cenové hladině, vzroste i počet uživatelů kontrolních a docházkových kamerových systémů. V dnešní době je více než pravděpodobné, že se spojí kamerové jednotky s dalšími elektronickými, technickými i soukromými bezpečnostními zařízeními do uceleného celku a tím vznikne Integrovaný bezpečnostní systém a na jeho podněty bude reagovat Integrovaný záchranný systém tudíž Policie ČR, městská policie, Hasičský i lékařský záchranný sbor a to nejen v jednotlivých městech a později dojde k propojení jednotlivých segmentů v rámci celé České republiky.

SEZNAM POUŽITÉ LITERATURY

[1] TAUŠ, G. *Video*. Praha, SNTL 1989.

[2] Klugl, J. *Montáž EZS*. Praha 1993.

[3] SKŘIVAN, Z. *Nebojte se zlodějů*. Praha, Grada 1994.

[4] GRAHAM, J., BENNETT T. *Strategie 'prevence kriminality v Evropě a Severní Americe*. Praha, Institut pro kriminologii a sociální prevenci 1996.

[5] IVANKA, J. *Technické prostředky bezpečnosti a elektromagnetická kompatibilita*. In. Řešení krizových situací v specifickém prostředí. EDIS - Žilinská univerzita, Žilina, 2004, str. 77-82, ISBN 80-8070-272-1

[6] Ivanka, J. *Měření rušivých signálů pomocí antén.*, Sborník z 10. vědecké konference s mezinárodní , *Řešení krizových situací ve specifickém prostředí*, FŠI Žilinská univerzita, Žilina 2005, str. 211 – 214, ISBN 80-8070-425-2

[7] VEČERKA, K. a kolektiv autorů Prevence kriminality v teorii a praxi. Praha, Themis 1997.

[8] *Prevence kriminality ve městech. Praha*, Odbor prevence kriminality MV ČR 1997.

[9] KOCÁBEK, P., KONÍČEK, T. *Situační prevence a kamerové monitorovací systémy*. Praha, Odbor prevence kriminality MV ČR 1997.

[10] KŘEČEK, S. *Ochrana majetku systémy průmyslové televize*. Praha, Grada 1997.

[11] KONEČNÝ, L. *Etapy výstavby zabezpečovacího a kamerového systému*. Praha, VTÚE 1998.

[12] KOCÁBEK, P., ČERVENÁ, R., KONÍČEK, T. *Klíč k bezpečí*. Praha, Odbor prevence kriminality 2000.

[13] *Ročenka prevence kriminality 1999*. Praha, Odbor prevence kriminality MV ČR 2000.

[14] *Zpráva o plnění úkolů vyplývajících ze strategie prevence kriminality za léta 1997-2000 a strategie prevence kriminality na léta 2001-2003*. Praha, MV ČR 2000,

[15] *Časopis POLICISTA*: 3/1998, 6/2000, 12/2000.

Zákon č. 199/1994 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

Zákon č. 22/1997 Sb., o technických požadavcích na výrobky, ve znění pozdějších předpisů.

ČSN EN *50132* - Poplachové systémy - CCTV pozorovací systémy pro použití v bezpečnostních aplikacích.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

OČTŘ	Orgán činný trestného řízení
PKB	Průmysl komerční bezpečnosti
CCTV	Zkratka z anglického názvu Closed Circuit Television Systém
EZS	Elektronická zabezpečovací signalizace
EZS	elektrického zabezpečovacího systému
JTS	Jednotné telefonní sítě
OPK	Odbor prevence kriminality Ministerstva vnitra
DVR	Digitální záznamové jednotky
KSP	Komplexní součinnostní program
PIS	Preventivně informační skupiny
IZS	Složky integrovaného záchranného systému
GIS	Geografický informační systém
EU	Evropské unie
ES	Evropského Společenství
PECA	Posuzování shody a akceptaci průmyslových výrobků”
EMC	Elektromagnetická kompatibilita
ACS	Řízení přístupu
ATS	Přenos poplachu
CCTV	Systémy uzavřených televizních okruhů
PAS	Poplachový systém pro detekci požáru a při požáru
AIS	Poplachový systém proti vloupání a při přepadení
SAS	Poplachový systém sociální
GL	Generální licence
TC	Technický výbor

EPS	Elektrická požární signalizace
NBÚ	Národní bezpečnostní úřad
ČNBÚ	Český národního bezpečnostní úřad
EMI	Elektromagnetická energie – rušení
SBS	Soukromých bezpečnostních služeb
NEMP	Nuclear Electromagnetic Pulse
PCO	Pult centralizované ochra y
DMŘ	Další místo řízení
ACESS kontrol	Systém kontroly vstupu

SEZNAM OBRÁZKŮ

SEZNAM GRAFŮ A TABULEK