Kritéria návrhu kamerových systémů

Criteria of closed circuit television concept

Martin Maluš

Bakalářská práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martin MALUŠ**
Osobní číslo:	**A09187**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Kritéria návrhu kamerových systémů**

Zásady pro vypracování:

1. **Analyzujte legislativní požadavky na kamerové systémy.**
2. **Specifikujte technické požadavky na komponenty kamerových systémů pro jednotlivé modelové objekty.**
3. **Proveďte komparaci technických parametrů dostupných komponentů kamerových systémů.**
4. **Pojednejte o vývojových trendech v oblasti kamerových systémů.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **CAPUTO, Tony C. Digital video surveillance and security. 1. Boston: Butterworth-Heinemann/Elsevier, 2010, 333 s. ISBN 18-561-7747-5.**
2. **LOVEČEK, Tomáš; NAGY, Peter . Bezpečnostné kamerové systémy. Žilina: EDIS, 2008. ISBN 978-80-8070-8931.**
3. **RANDA, Michal. Guideline IP CCTV ? Průvodce návrhem systému síťového videa, část 1.-5. [online]. 2011, 12.09.2011. Dostupné z: http://www.orsec.cz**
4. **ČSN EN 50-132-1. Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky. 2010.**
5. **ČSN EN 50-132-7. Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích - Část 6: Pokyny pro aplikaci. 1999.**
6. **Česká republika. Zákon č. 101/2000 Sb. Parlamentu České republiky o ochraně osobních údajů a o změně některých zákonů. In: 101/2000 Sb. 2000. Dostupné z: http://ff.osu.cz/dokumenty/praxe/zakon1012000.pdf**
7. **Doporučení Výboru pro občanská a politická práva ohledně provozu kamerových systémů. Magazín Security. 5/2010, XVII., 97, s. 6-7**
8. **AXIS COMMUNICATIONS. Technical Guide to Network Video [online]. 2008. ISBN 292249. Dostupné z: http://www.axis.com/files/brochure/bc_techguide_33334_en_0811_lo.pdf**

Vedoucí bakalářské práce: **Ing. Jiří Ševčík**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **24. února 2012**

Termín odevzdání bakalářské práce: **25. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Tato bakalářská práce se zabývá problematikou návrhu kamerových systémů z hlediska faktorů, které přímo ovlivňují výběr jednotlivých zařízení a účel jejich nasazení v dané aplikaci. Z důvodu budoucí perspektivy jsou upřednostňovány systémy síťového videa – IP kamerové systémy. Teoretická část obsahuje analýzu stěžejních legislativních požadavků, včetně příslušných platných i připravovaných norem a doporučení vydaných odborným sdruženími z oblasti CCTV. V další části práce jsou popsány základní technické parametry jednotlivých zařízení a jejich souvislost s návrhem kamerových systémů. Závěrečná kapitola teoretické části se zabývá vývojovými trendy.

V praktické části práce jsou podle zvolených kritérií charakterizovány vybrané modelové objekty a analyzovány jejich specifické požadavky na kamerové systémy.

Přílohová část kromě doplňujících informací obsahuje zejména tabulkové srovnání technických parametrů základních prvků kamerových systém dostupných v současnosti na trhu.

Klíčová slova: CCTV, IP, kamerové systémy, kritéria návrhu, modelové objekty, normy, legislativa

ABSTRACT

This bachelor work is concerned with matters of closed television concept in light of factors, which directly influence the selection of individual devices and their purpose in the application deployment. By the reason of future perspective, there are preferred network video systems – IP CCTV. The theoretical part contains an analysis of key legislative requirements, including the existing and upcoming standards and recommendations issued by professional associations in the field of CCTV. The next section describes the basic technical parameters of individual devices and their connection with the proposal of CCTV. The final chapter deals with the development tendency.

In the practical part, there are characterized chosen model objects and analyzed their specific requirements for CCTV systems by the selected criteria.

The attachments section also contains additional information, especially tabular comparison of technical parameters of the basic elements of the camera system available on the market today.

Key words: CCTV, IP, Video surveillance system, criteria of concept, model objects, standards, legislation

Tímto bych chtěl poděkovat jednak vedoucímu bakalářské práce Ing. Jiřímu Ševčíkovi za odborné konzultace a cenné připomínky, které mi v průběhu zpracování zadaného tématu poskytoval, a také rodině a blízkým za morální podporu.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….……

podpis diplomanta

OBSAH

ÚVOD

Z důvodu neustále klesající koncové ceny jednotlivých komponentů se stávají kamerové systémy běžným řešením z nejen z hlediska ochrany zdraví a majetku osob, ale také v celé řadě komerčních aplikací. Všeobecným trendem je snaha o centralizaci a vzájemnou spolupráci kamerových systémů se systémy jinými (kontrola vstupu, zajištění bezpečnosti v dopravě a veřejných prostorech apod.) za účelem vyšší efektivnosti a s tím související úspory nákladů. Není se tedy čemu divit, že CCTV stále více zasahují do běžného života. Stejně jako jiné moderní technologie, mohou být i kamerové systémy v nepovolaných rukou zneužity. Mělo by být tedy v zájmu celé společnosti, aby byl jejich provoz ošetřen legislativou, která jasně stanoví práva a povinnosti provozovatele kamerového systému.

Jelikož je postup technologického vývoje v této oblasti velmi rychlý, je také žádoucí, aby byly na jeho základě dynamicky aktualizovány obsahy norem, řešící problematiku kamerových systémů. Kromě pověřených autorit se na této činnosti v současnosti aktivně podílí zejména sami výrobci v rámci profesních sdružení. Jejich záměrem je v prvé řadě vytvoření trhu s produkty jednotlivých výrobců, mezi kterými bude možno při realizaci kamerových systémů vzájemně kombinovat. Tato situace je z pohledu koncového zákazníka, resp. projektanta výhodná z toho důvodu, že již není nutné v takové míře zkoumat možnosti spolupráce zařízení od odlišných výrobců.

Co se týče technických požadavků na kamerové systémy, vychází vždy z analýzy konkrétní aplikace a požadavků zadavatele. Výběr optimálního zařízení ovlivňuje celá řada faktorů od povětrnostních a jiných nepříznivých vlivů, kterým jsou při provozu vystaveny, přes charakter monitorované scény, až po požadavek na integraci několika typů systémů dohromady a jejich součinnost. Cílem této práce je tedy vymezení zásadních kritérií pro návrh kamerových systémů a současně analýza specifických požadavků, které je možné názorně demonstrovat u jednotlivých modelových objektů. Čtenář si tak může vytvořit představu o tom, jak při návrhu kamerového systému v dané aplikaci postupovat a na jaké kritéria je nutné brát ohled.

I. TEORETICKÁ ČÁST

1 LEGISLATIVNÍ POŽADAVKY NA KAMEROVÉ SYSTÉMY

Úvodní kapitola práce se zabývá analýzou legislativy, jež se vztahuje k problematice návrhu kamerových systémů. Jedná se zejména o zákon č. 101/2000 Sb., o ochraně osobních údajů a s ním související výklady Úřadu pro ochranu osobních údajů a jednotlivé části technické normy ČSN EN 50132, včetně jejich připravovaných revizí. Dále jsou také uvedeny doporučení a aplikační směrnice profesních odborných sdružení, popř. pojišťoven. Je nutné upozornit na skutečnost, že instalace a provozování kamerových systémů a zpracování jimi pořízených záznamů není zatím ošetřeno specifickým zákonem. Jako celá řada moderních technologií, mohou být i kamerové systémy zneužity, proto je nutné, aby byly provozovány v souladu s platnými právními předpisy.

1.1 ZÁKON Č. 101/2000 SB., O OCHRANĚ OSOBNÍCH ÚDAJŮ

Tento zákon vydaný 4. dubna 2000 vychází ze zaručeného práva Listinou základních práv a svobod [1] na ochranu občana před zasahováním do jeho soukromí neoprávněným shromažďováním, zveřejňováním, popř. jiným zneužíváním osobních údajů. Dle § 2 zákona č. 101/2000 Sb. [2] byl zřízen Úřad pro ochranu osobních údajů se sídlem v Praze (dále jen ÚOOÚ), jehož hlavním úkolem je činnost dozorového orgánu pro oblast ochrany osobních údajů s působností vyplívající z § 3 a dalších mezinárodních smluv, které jsou součástí právního řádu.

Co se týče problematiky kamerových systémů, je zásadní zejména níže uvedené stanovisko ÚOOÚ č. 1/2006 [3], které jasně vymezuje povinnosti a práva provozovatele kamerového systému.

1.1.1 Stanovisko ÚOOÚ č. 1/2006

Z tohoto prohlášení ÚOOÚ lze jednoznačně vyvodit tyto závěry:

1. Za **zpracování osobních údajů** je provozování kamerového systému považováno v případě, je-li:
    a. kromě sledování kamerovým systémem prováděn i **záznam** pořizovaných záběrů

   b. uchovávaná informace v záznamovém zařízení pořizována za účelem jednoznačné **identifikace** fyzické osoby v souvislosti s určitým jednáním
2. **Osobní údaje** jsou uchovávané informace (obrazové, zvukové) v záznamovém zařízení za předpokladu, že lze na jejich základě identifikovat (přímo/nepřímo) konkrétní fyzickou osobu.
3. Použití kamerového systému je možné i **bez souhlasu** subjektu údajů (zaznamenané fyzické osoby) dle § 5 odst. 2 písm. e) zákona o ochraně osobních údajů.

Ad 1. a) Z tohoto závěru vyplývá, že samotné sledování fyzických osob za použití kamerového systému bez záznamu (sledování „online“) **není považováno za zpracování osobních údajů**. Tento fakt však nevylučuje aplikaci jiných právních předpisů, jako např. § 11 zákona č. 40/1964 Sb., občanského zákoníku, který určuje ochranu osobnosti [4].

Ad 3) Provoz kamerového systému a následné zpracování osobních údajů je také přípustné v rámci plnění úkolů uložených jinými zákony. To se týká výlučně kompetencí Policie České republiky dle § 2 zákona č. 283/1991 Sb., o Policii České republiky [5] a částečně obecní policie podle § 1 odst. 2 zákona č. 553/1991 Sb., o obecní policii [6].

Výklad zákona č. 101/2000 Sb. a stanovisek vydaných ÚOOÚ lze v rámci problematiky CCTV systémů se záznamem shrnout do následujících povinností správce:

1. **Provést registraci u ÚOOÚ dle zákona o ochraně osobních údajů,**
2. **informovat subjekty údajů o účelu a rozsahu sledování a o způsobu zpracování záznamu,**
3. **uchovávat pořízené záznamy jen po dobu nezbytně nutnou,**
4. **zabezpečit kamerový systém,**
5. **vyvarovat se nadměrnému zásahu do soukromí.**

Ad 2) Oznamovací povinnost správce lze splnit:

- u třetích osob **písemnou informací** umístěnou na viditelném místě (např. vstup do střeženého prostoru), která musí obsahovat upozornění na použití kamerového systému a informace o provozovateli,
- u osob, které vstupují do střeženého prostoru pravidelně (např. zaměstnanci), **vydáním vnitřního předpisu**. Ten by měl rovněž obsahovat informace o účelu a umístění kamerového systému, době provozu, okruhu

osob, které budou zaznamenané informace zpracovávat a době jejich uchovávání. Je nutné, aby byly dotyčné osoby fyzicky a prokazatelně o vnitřním předpisu informovány, v ideálním případě proti podpisu.

U obou uvedených možností je nutné, aby oznámení o monitorování daného prostoru kamerovým systémem obsahovalo zejména informace o jeho správci, resp. kontaktní údaje, na základě kterých je možné získat detailní o provozu kamerového systému, účelu záznamu a způsobu jeho zpracování a zabezpečení.

Obrázek 1 – Štítek pro splnění oznamovací povinnosti, zdroj: Security magazín č. 5/2008

Obrázek 2 – Umístění štítku v praxi, zdroj: Security magazín č. 5/2008

Ad 3) To znamená uchovávat záznamy např. po dobu potřebnou k tomu, aby byl zaznamenaný incident prošetřen a aby bylo možné získat další informace nezbytné při vyšetřování příslušných orgánů. U běžně zaznamenaných informací by neměla jejich délka uchování přesáhnout 3 dny.

Ad 4) Kamerový systém by měl být patřičně zabezpečen včetně uchovávaných záznamů proti neoprávněnému přístupu a případnému zničení, změně nebo zneužití zaznamenaných dat.

Ad 5) Provoz CCTV systému by měl být patřičně opodstatněn (tzn. nelze použít jinou alternativu střežení, která nezasahuje do soukromí fyzických osob). Jeho použití není dovoleno v prostorech určených pro vykonávání ryze osobních úkonů, jako např. toalety, šatny apod. V tomto případě je však možné tyto prostory střežit za předpokladu, že je vyhrazen prostor, který kamerovým systémem není sledován (např. kabinka pro převlečení atd.) [7].

1.2 PROBLEMATIKA NOREM KAMEROVÝCH SYSTÉMŮ

Současná situace v oblasti technických norem týkajících se kamerových systémů je výsledkem rychlého technologického pokroku. S postupným přechodem z analogových systémů na digitální, firmy investují značné prostředky do vývoje, a snaží si tak vypracovat co nejvýhodnější postavení na trhu. Je tak logické, že se tento trend postupně přeměnil na iniciativu o standardizaci jednotlivých komponentů, aby bylo dosaženo rovného postavení pro všechny výrobce. Postupně tak začaly vznikat sdružení, jejichž cílem bylo umožnění vzájemné spolupráce mezi systémy různých výrobců (tzv. interoperability). Těmi nejvýznamnějšími v oboru kamerových systémů jsou PSIA[1] a ONVIF[2] (obě založeny v roce 2008). Ačkoliv obě sdružení prosazují velice podobné zájmy, je u nich patrná jistá rivalita s cílem ovládnout trh. Rozdíl mezi nimi je především v používaných specifikacích a jejich aplikačních technologiích. ONVIF se zaměřuje zejména na přenosové vlastnosti IP[3] videa a k tomu využívá standard SOAP[4], navržený sdružením IT firem jako např. IBM a Microsoft. Výhodou využívání protokolu SOAP je zejména kvalitní podpora vývoje a striktní dodržování pravidel pro komunikaci mezi jednotlivými zařízeními. Je tak zaručena nejvyšší možná míra interoperability mezi výrobky se stejnou specifikací. Naproti tomu PSIA, které se specializuje nejen na přenos videa, ale také na jeho využití např. v přístupových a integrovaných systémech, analýzu obrazu apod., využívá specifikace REST[5]. Protokoly pracující na této platformě jsou v porovnání s konkurencí obecně snadněji zpracovatelné a jednodušší, což usnadňuje jejich integraci do zařízení. Otevřenost této specifikace však na druhou stranu neumožňuje poskytnout tak vysokou míru interoperability jako u standardu

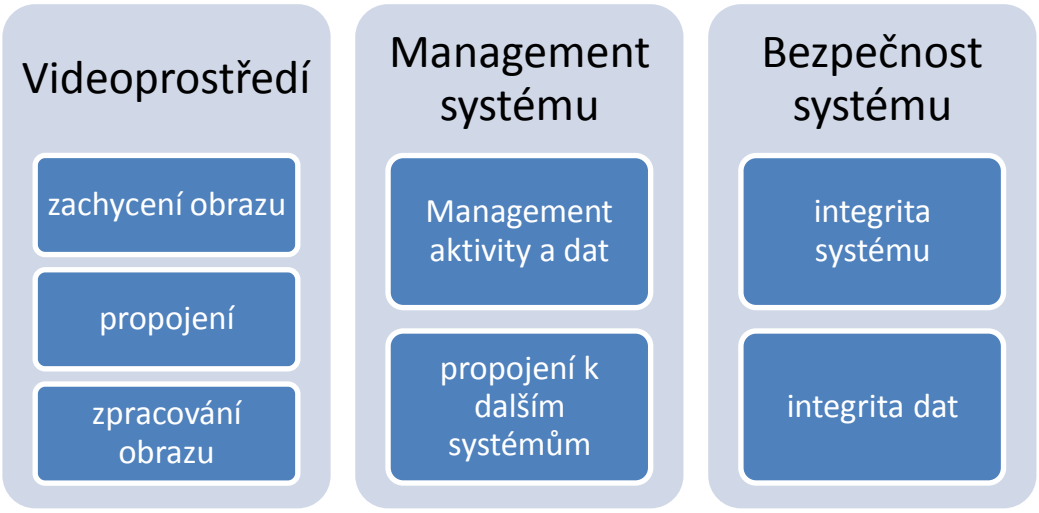
[1] Physical Security Interoperability Alliance.
[2] Open Network Video Interface Forum.
[3] Internet Protokol.
[4] Simple Object Acces Protokol.
[5] Representational State Transfer.

SOAP. V současné době je již na trhu objevuje celá řada zařízení (např. IP kamery), které podporují obě výše uvedené specifikace.

Na základě tlaku výše uvedených sdružení PSIA a ONVIF probíhají ve spolupráci s organizací CENELEC[6] intenzivní práce na revizi současných platných norem v oblasti kamerových systémů. Nejzásadnější změnou bude plné respektování IP technologií. To znamená, že se tato technologie stane plnohodnotnou alternativou při zabezpečení pomocí CCTV a nebude chápána jako doplňková, jak tomu bylo donedávna [8].

1.2.1 ČSN EN 50132-1:2010 Systémové požadavky

Norma ČSN EN 50132, skládající se původně pouze z části 5: Přenos videosignálu a části 7: Pokyny pro aplikace, byla v roce 2010 rozšířena o část 1: Systémové požadavky. V aktuální verzi již není na jednotlivé prvky kamerového systému nahlíženo jako dříve (kamera-přenos-zpracování-záznam-zobrazení), ale nově se skládá z 3 funkčních bloků. Jsou jimi video prostředí, management systému a bezpečnost systému. Toto členění je výhodné z hlediska návrhu IP CCTV, neboť u tohoto typu systémů je realizováno několik funkcí v rámci jednoho zařízení (IP kamera - záznam, komprese atd.).

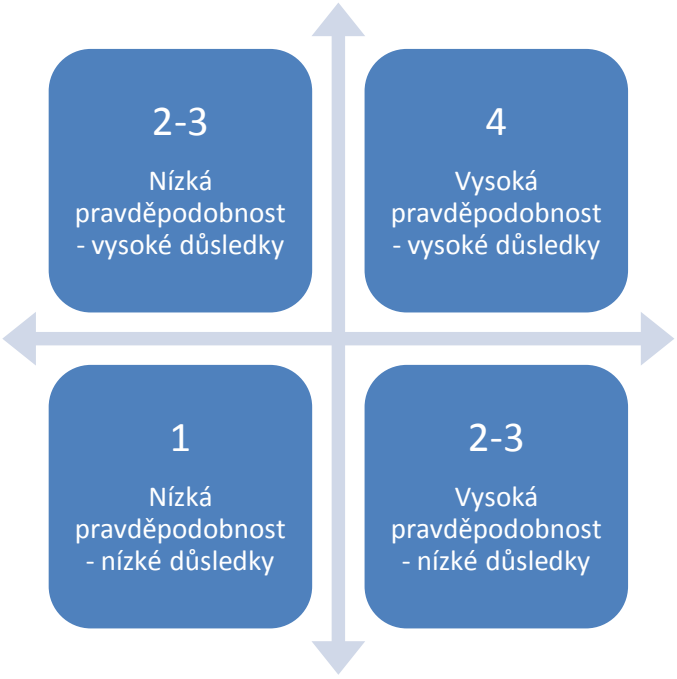


Obrázek 3 – Funkční bloky systému CCTV dle ČSN EN 501312-1

Další změnou je zařazení kamerových systémů do čtyř stupňů zabezpečení (jako u PZTS dle ČSN EN 50131-1) podle hlediska pravděpodobnosti incidentu a míry možných

[6] European Comittee for Electrotechnical Standardization.

důsledků. Na základě tohoto rozdělení jsou pak kladeny požadavky na kamerové systémy podle jednotlivých stupňů zabezpečení, např. v oblasti systémových protokolů, přístupových úrovní, zálohování, archivace atd. (viz Přílohy P I a P II).



Obrázek 4 – Rizika a stupně zabezpečení CCTV dle ČSN EN 50132-1

Nově je též možné zařazení prvků systému do 4 tříd prostředí podle očekávaných klimatických podmínek (opět jako u ČSN EN 50131-1). Poměrně významnou změnou je částečné implementování IP CCTV (pouze video). Je však nutné zdůraznit, že této technologii stále chybí opora ve zbylých částech normy [9].

1.2.2 ČSN EN 50132-5:2002 Přenos videosignálu

Tato část normy je určena především výrobcům zařízení pro přenos videosignálů a zkušebnám, ověřujícím splnění technický požadavků. Stanovuje základní specifikace technických parametrů přenosových systémů, využívaných v kamerových systémech CCTV. Kromě technických požadavků definuje také metody ověřování jejich splnění. Na základě pravidel stanovených touto částí normy lze přenosová zařízení zařadit do jedné ze 4 tříd klimatické odolnosti. Norma zároveň odkazuje na další normy z problematiky EMC a elektrické bezpečnosti [10]. V současné době tato verze nedostačuje, neboť řeší pouze analogové systémy, proto se intenzivně pracuje na její revizi prEN 50132-5. Z důvodů časové náročnosti je revize rozdělena na 3 části, a to:

- prEN 50132-5-1 General Video Transmission Performance Reguirements
- prEN 50132-5-2 IP Video Transission Protocols
- prEN 50132-5-3 Analog and Digital Video Interface Standard

Cílem této revize je sjednocení standardů kamerových systémů, aktualizace používaných technologií a také využití spolupráce mezi normotvornými organizacemi a sdruženími výrobců. Jak je z anglických názvů jednotlivých částí patrné, budou se kromě analogových CCTV systémů zabývat také systémy digitálními, tedy IP CCTV [11].

1.2.2.1 prEN 50132-5-1 General Video Transmission Performance Reguirements

V této části normy se řeší pouze IP přenos (analogový byl přesunut do prEN 50132-5-3). Klade základní požadavky na konektivitu zařízení a přenosové vlastnosti (časování, kvalita,…). Mimo jiné popisuje také postupy při návrhu architektury sítě, zejména z hlediska QoS[7]. Tento pojem zahrnuje mimo jiné definice parametrů, jako např. zpoždění (latence), kolísání zpoždění (jitter), šířka pásma (bandwith) atd. Co se týče bezpečnosti, norma definuje požadavky na přenos z hlediska šifrování dat, autentifikace, kontroly integrity apod. Na základě spolupráce ONVIF a PSIA norma obsahuje také popis několika metod, určených pro detekci zařízení v síti Device Dicovery (WS-Discovery, Zeroconf, UPnP) [11].

1.2.2.2 prEN 50132-5-2 IP Video Transission Protocols

Na vývoji této normy se značně podílely organizace ONVIF a PSIA. Je rozdělena do 4 částí, přičemž první obecně popisuje protokoly a jejich význam při přenosu, druhá protokoly, které využívá sdružení ONVIF a třetí protokoly, které podporuje sdružení PSIA. Jelikož se očekává, že vývoj v oblasti přenosových protokolů bude i nadále pokračovat, je poslední čtvrtá část normy vyhrazena do budoucna pro případné doplnění [11].

1.2.2.3 prEN 50132-5-3 Analog and Digital Video Interface Standard

Do této části byla přesunuta původní ČSN EN 50132-5, nově popisuje definice videorozhraní (analogové i digitální) a respektuje formáty videa o vysokém rozlišení [11].

---

[7] Quality of Service.

1.2.3 ČSN EN 50132-7:1999 Pokyny pro aplikaci

Norma ČSN EN 50132-7:1999 Pokyny pro aplikaci má v současné době při návrhu kamerového systému největší význam. Kromě výčtu definic z oblasti kamerových systémů obsahuje především základní funkční a systémové požadavky. Z nich pak budou vycházet kritéria u jednotlivých modelových objektů. Cílem normy je jednak poskytnout informace investorům, montérům apod., nutné ke stanovení požadavků, popř. k objektivnímu zhodnocení nainstalovaného kamerového systému, ale především pomoci projektantům při výběru vhodných zařízení [12].

1.2.3.1 prEN 50132-7 Aplication Guidelines

Příčinou přepracování této normy je harmonizování s připravovanými revizemi prEN 50132-5 a nedávno vydanou ČSN EN 50132-1. Její struktura je téměř totožná se současnou verzí, avšak obsah je soustředěn zejména na IP CCTV systémy. Zásadní změnou je přidání 2 nových stupňů identifikace:

- Přehled (Observe) – výška osoby na monitoru > 25% (1 pixel/16 mm)
- Inspekce/detailní identifikace (Inspect) – výška osoby na monitoru > 400% (1 pixel/1 mm)

Revize obsahuje také tabulku přepočtů pro jednotlivé stupně identifikace u nejběžněji používaných rozlišení, včetně vysokého (HD[8]). Dále doporučení pro výběr vhodného zobrazovacího zařízení a specifikaci řídícího pracoviště. Součástí normy je rovněž příklad výpočtu předpokládané velikosti záznamu a přílohy zabývající se testováním při identifikaci obličeje a funkcí rozpoznání registračních značek (LPR[9]). Jako v ostatních připravovaných revizích, je i v této části kladen důraz na znalost projektantů technologie síťového přenosu a využití QoS [13].

1.3 DOPORUČENÍ A APLIKAČNÍ SMĚRNICE PRO NÁVRH CCTV

Při návrhu kamerových systémů je vhodné se řídit i směrnicemi vydanými různými profesními sdruženími. Tyto dokumenty obsahují metodické pokyny a doporučení pro pro-

[8] High Definition.
[9] License Plate Recognition, také Automatic Number Plate Recognition.

jektanty, montážní firmy apod. a upozorňují např. na možné konflikty s legislativou. Bohužel staří některých z uvedených směrnic se blíží k deseti letům, tudíž nemusí být v mnoha ohledech aktuální.

1.3.1 Směrnice AGA 004 – Sbírka zásad CCTV

Směrnice z roku 2007 vydaná sdružením AGA[10] řeší problematiku nakládání s osobními údaji z hlediska správce kamerového systému, jeho povinnosti apod., přičemž obsahuje řadu příkladů a modelových situací. Vychází ze zákona č. 101/2000 Sb., o ochraně osobních údajů [14].

1.3.2 Směrnice AGA 005 – Kamery, kamerové systémy a ochrana osobních údajů

Další směrnicí vydanou výše uvedeným sdružením je AGA 005, taktéž z roku 2007. Záměrem této publikace je upozornit na možné rozpory se zákonem o ochraně osobních údajů při provozování kamerového systému a pokud možno nabídnout řešení daných problémů z pozice projektanta, montážní firmy nebo správce kamerového systému [15].

1.3.3 Aplikační směrnice ČAP – P132-7

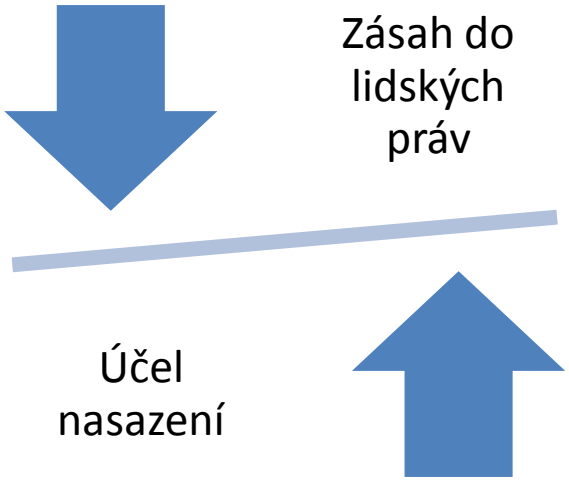
Tato aplikační směrnice byla v roce 2003 vydána Českou asociací pojišťoven. Ačkoliv od té doby uplynula již řada let, dá se částečně při návrhu kamerového systému z této směrnice i v dnešní době vycházet. Dokument vychází z normy ČSN EN 50132-7:1999 Pokyny pro aplikaci a požadavků CEA[11]. Obecně slouží montážním firmám a pojišťovnám jako doporučení při ochraně pojištěného majetku systémy CCTV. Stručně popisuje provozní požadavky na kamerový systém (definice objektů zájmů a zachycované činnosti, systémové a obrazové vlastnosti apod.) a technické požadavky na jednotlivé části systémy (kamery, objektivy, osvětlení, přenosová zařízení). Další samostatné kapitoly se věnují funkci video-detekce pohybu (VMD[12]), požadavkům na obsluhu lokálního a vzdáleného (RVRC[13]) monitorovacího centra a náležitostem, které musí obsahovat dokumentace, předávaná montážní firmou obsluze kamerového systému. Přílohou směrnice je dotazník ur-

[10] Asociace Gremium Alarm.
[11] Comité Européen des Assurances.
[12] Video Motion Detection.
[13] Remote Video Response Centre.

čený pro pojišťovny při ohodnocování stávajícího systému CCTV, popř. při specifikaci nového [16].

1.4 DÍLČÍ ZÁVĚR

Při nasazení kamerového systému nastává v řadě případů konflikt na hranici mezi opodstatněným účelem provozu a současným zachováním veškerých lidských práv a svobod. Jeho použití je sice zákonem respektováno jako jeden ze způsobů ochrany života, zdraví, majetku a zbylých právem chráněných zájmů osob, je však nutné, aby bylo v rovnováze s osobnostními právy jedince. Kamerový dohled může svým provozem narušit i několik lidských práv – jedná se zejména o právo na soukromý život, volný pohyb a ochranu osobních údajů. V případě monitorování na pracovišti se k výše uvedeným právům přidají i další vycházející ze zákoníku práce (právo na soukromí na pracovišti). Jak už bylo uvedeno v úvodu, tato problematika není v současné době řešena žádným specifickým zákonem. Na provoz kamerového systému se záznamem (vyjma provozu na základě úkolů daných jinými zákony – viz kapitola 1.1.1, ad 3)) je tedy za jistých okolností pouze pohlíženo jako na zpracování osobních údajů dle zákona 101/2000 Sb., o ochraně osobních údajů. Z této skutečnosti vychází i jednotlivé požadavky, které musí být splněny, aby byl provoz kamerového systému v souladu se zákonem a nedocházelo v budoucnu ke konfliktům. Dohledovým orgánem nad dodržováním výše uvedené legislativy je ÚOOÚ. Ten však zřejmě z personálních důvodů neprovádí kontrolu právních předpisů příliš důkladně, resp. případné postihování není v takové míře, jak by bylo třeba. Tuto situaci by mohla vyřešit novelizace platných zákonů nebo vydání nového, který by jasně definoval práva a povinnosti při použití kamerového systému.

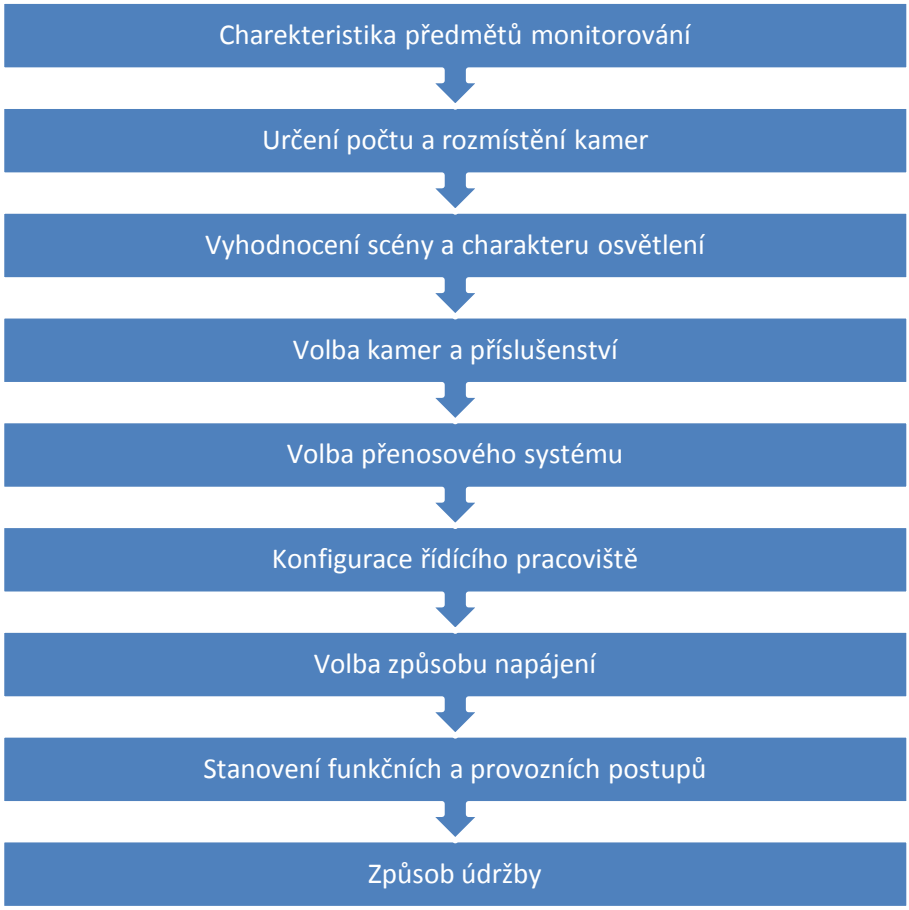


Obrázek 5 – Konflikt při nasazení kamerového systému, zdroj: archiv autora

Co se týče situace v oblasti norem řešících kamerové systémy, je nyní ve fázi očekávání na připravené revize prEN 50132-5-1,2 a 3 a prEN 50132-7. Současné platné verze poskytují pouze základní pokyny, resp. neodpovídají současným trendům a používaným technologiím v praxi. S příchodem výše uvedených revizí dojde k plnému respektovaní IP kamerových systémů, jak z hlediska jednotlivých parametrů přenosu dat, tak i z hlediska aplikačních pokynů. Tyto zásadní změny však s sebou přinesou i nárůst požadavků na projektanty, zejména v případě znalosti problematiky norem ICT, na které se jednotlivé revize odkazují.

2 KRITÉRIA NÁVRHU KAMEROVÉHO SYSTÉMU

V této části práce je na základě analýzy platné normy ČSN EN 50132-7 [12] a dalších doporučení popsán výčet jednotlivých kritérií, podle kterých se projektant při návrhu kamerových systémů obecně řídí. Z hlediska budoucí perspektivy jsou jednotlivá kritéria u modelových objektů specifikována s ohledem na **IP kamerové systémy**.



Obrázek 6 – Kritéria návrhu CCTV dle ČSN EN 50132-7

2.1 CHARAKTERISTIKA PŘEDMĚTŮ MONITOROVÁNÍ

Výchozím kritériem při návrhu CCTV je rozvaha, zdali je vůbec nutné tento systém instalovat, resp. nedá-li se dosáhnout stejných výsledků za použití jiného, méně invazivního systému. Aby provoz kamerového systému nebyl v rozporu s legislativou (zákon č. 101/2000 Sb.), musí mít **opodstatněný účel nasazení**. Tím mohou být v prvé řadě bezpečnostní aplikace, popř. jiné doplňkové funkce (počítání osob, měření rychlosti apod.). Co se týče nasazení kamerových systémů z bezpečnostních důvodů, jedná se ve většině případů o:

- zajištění bezpečnosti osob (veřejné prostory, letiště, průmyslové provozy),
- střežení,
  - perimetru,
  - pláště,
  - prostoru,
  - předmětů,
- kontrolu vstupu osob/vozidel,
- ochrana majetku,
- monitorování (technologické procesy, doprava).

Obrázek 7 – Faktory ovlivňující oblast zájmu, zdroj: archiv autora

Projektant by měl při návrhu v ideálním případě vycházet z **bezpečnostního posouzení** daného objektu, na jehož základě může zvolit optimální konfiguraci kamerového systému, zařadit ho do adekvátního stupně zabezpečení, zohlednit speciální požadavky na jednotlivá zařízení atd. Z bezpečnostního posouzení jsou pro návrh výchozí např. tyto výstupy:

- základní vlastnosti objektu (umístění, přístupnost atd.),
- popsání zabezpečovaných aktiv (život, zdraví, majetek),
- analýza možných hrozeb, stanovení míry rizika,
- charakteristika předpokládaného pachatele.

Na základě těchto kritérií a v souladu s požadavky legislativy a zákazníka je možné vytipovat **oblasti zájmu** (zóny, objekty), které mají být pod dohledem kamerového systému a určit charakter jejich snímání.

2.2 URČENÍ POČTU A ROZMÍSTĚNÍ KAMER

Po definování požadovaných zón je nutné stanovit počet kamer, potřebných k jejich monitorování. V této fázi návrhu je důležité zejména zvolit jejich **vhodné umístění**. To by mělo vycházet z(e):

- způsobu realizace systému,
- požadavků na charakter záznamu,
- zorného pole kamer,
- bezpečnostního hlediska,
- funkčního hlediska (přístupnost z důvodu údržby, oprav),
- estetického hlediska (památky),
- platné legislativy (viz Kapitola 1).

Dalším možným kriteriem, na které musí při rozmísťování kamer brán zřetel, je i předpokládané využití speciálních funkcí jako např. inteligentní analýzy obrazu (počítání procházejících osob). Při nevhodně zvoleném umístění kamery totiž může dojít ke snížení schopnosti rozlišit jednotlivé osoby a následného zkreslení výsledků videoanalýzy [17].

2.3 VÝBĚR VHODNÉ KAMERY NA ZÁKLADĚ TECHNICKÝCH PARAMETRŮ

Volba kamer a jejich příslušenství je závislá na **provozních podmínkách** těchto zařízení a **charakteru** snímané scény. Důležité je jednak zohlednit **klimatické** a **mechanické vlivy**, kterým budou jednotlivá zařízení při provozu systému vystavena, ale také vyhovět případným **požadavkům zákazníka** (např. skrytá montáž pod omítku). Na základě analýzy výše uvedených faktorů je možné vyvodit základní kritéria, podle kterých budou voleny jednotlivé prvky kamerového systému [12].

2.3.1 Technické kritéria výběru kamery

2.3.1.1 Rozlišovací schopnost

Každý optický snímač se skládá z určitého množství pravidelně uspořádaných snímacích buněk, tzv. pixelů (px). Rozlišovací schopnost kamery je závislá především na počtu aktivních buněk jejího snímače. Tato vlastnost je klíčová pro výslednou kvalitu pořízeného obrazu, neboť vysoké rozlišení snímků dovoluje bezproblémovou analýzu obrazových dat a získání požadovaných informací z monitorovaného prostoru (SPZ automobilů, obličej pachatele apod.).

Zkratka	Celý název (v AJ)	Šířka [px]	Výška [px]	Počet Mpx
CIF	Common Intermediate Format	352	288	**0,10**
2CIF	-	704	288	**0,20**
PAL (576i)	Phase Alternation Line	720	400	**0,29**
4CIF	-	704	576	**0,41**
D1	-	720	576	**0,41**
VGA	Video Graphics Array	640	480	**0,31**
SVGA	Super Video Graphics Array	800	600	**0,48**
720p	HD	1 280	720	**0,92**
SXGA	Super Extended Graphics Array	1 280	1 024	**1,31**
1080p	Full HD	1 920	1 080	**2,07**
QXGA	Quad Extended Graphics Array	2 048	1 536	**3,15**
QSXGA	Quad Super Extended Graphics Array	2 560	2 048	**5,24**
WQSXGA	Wide Quad Super Extended Graphics Array	3 200	2 048	**6,60**
WQUXGA	Wide Quad Ultra Extended Graphics Array	3 840	2 400	**9,20**
WHUXGA	Wide Hex Ultra Extended Graphics Array	7 680	4 800	**36,9**

Tabulka 1 – Používané rozlišení, zdroj: IP CCTV Guideline [18]

Současné IP kamery na trhu běžně disponují rozlišeními řádově v desetinách až jednotkách megapixelů (formáty: PAL, VGA, 720p, SXGA,… viz Tabulka 1 - Používané rozlišení) [18].

2.3.1.2 Počet snímků za sekundu

Tento parametr určuje množství snímků, které je schopna IP kamera za 1 sekundu pořídit (FPS[14]). Na rozdíl od analogových kamer, které vysílají konstantní tok videa, je u systémů síťového videa možné FPS měnit na základě požadavků na snímání scény, popř. z důvodů snížení vytížení přenosové sítě. Nastavení hodnoty FPS je variabilní pro jednotlivá snímací zařízení a jeho změna může být podmíněna vznikem určité události (např. zvýšení FPS na základě detekování pohybu v obraze). V praxi bývá FPS uváděn vždy ve vtahu k danému rozlišení snímku, např.:

- 60 snímků/s v rozlišení 720 x 576 px,
- 60 snímků/s v rozlišení 1 280 x 720 px,
- 30 snímků/s v rozlišení 640 x 480 px apod [19].

2.3.1.3 Komprese

Se vzrůstajícím rozlišením a FPS pořízených záznamů roste i celkový objem přenášených dat. Aby nedocházelo k vysokému zatěžování přenosové sítě, je důležité, aby byla při výběru IP kamery zvolena optimální metoda komprese. V současné době je dostupná celá řada standardů, jak pro kompresi statických obrazů, tak i pro kompresi videa.

Pro kompresi statických obrazů je nejpoužívanější standard **JPEG**[15]. Jedná se o kvalitní ztrátovou kompresi s několika úrovněmi v závislosti na poměru kvalita/velikost obrazových dat. To znamená, že se zvyšující se úrovní komprese, úměrně klesá kvalita komprimovaného obrazu. Obecně také platí, že čím více detailů snímaná scéna obsahuje, tím větší bude objem dat a požadavky na propustnost přenosové sítě (např. barevné listí stromu/monotónní barva stěny) [20].

[14] Frames Per Second.
[15] Joint Photographic Experts Group

Obrázek 8 – Scéna s nízkými detaily, zdroj: www.netcam.cz

Obrázek 9 – Scéna s vysokými detaily, zdroj: www.netcam.cz

Co se týče komprese videa, v současnosti používané standardy M-JPEG[16] a MPEG-4[17] postupně nahrazuje moderní sjednocený **standard H.264** (známý také jako MPEG-4 Part 10, nebo MPEG-4 AVC). Oproti svým předchůdcům přináší dvojnásobnou míru komprese, vysokou kvalitu obrazu při nízké přenosové rychlosti, vyšší přesnost pohybového vektoru apod. Z ekonomického hlediska tento standard přináší úsporu prostředků, jelikož není potřeba velké úložiště dat [21].

2.3.1.4 Způsob napájení

Jednou z hlavních výhod systémů síťového videa je specifický způsob napájení IP kamer. Tzv. **PoE**[18] (standard IEEE802.3af) je realizováno v rámci datového kabelu Cat 5e (několik vyhrazených vodičů) vedoucího ke kameře. Hlavními přínosy této technologie je především úspora kabeláže (není nutné navrhovat napájecí vedení), snadné zajištění zálohy napájení a umožnění vzdáleného restartování zařízení. U systémů menšího rozsahu ve většině případů postačí PoE vedené ze switche, v případě rozsáhlejšího systému lze napájení kabelové trasy posílit tzv. injektory.

Je-li vyžadován provoz dalších podpůrných zařízení (přísvit, vytápění, ventilace, motorové ovládání,…) pro zvýšení kvality pořizovaného záznamu, lze využít další z několika standardů PoE, které mohou poskytnout vyšší úroveň napájení, nebo vybavit kameru

[16] Motion Joint Photographic Experts Group.
[17] Motion Picture Experts Group.
[18] Power over Ethernet

vhodným napájecím adaptérem. Běžně se jedná o stejnosměrné napětí 12 – 48 V, popř. střídavé 24 V [19].

2.3.1.5 Citlivost

Citlivost kamery udává hodnotu osvětlení v luxech, při kterém je kamera schopna snímat obraz při minimálním možném nastavení clony. Nejedná se však přímo o osvětlení monitorované scény, ale o míru osvětlení, které se odráží od snímaných objektů (viz Tabulka 2).

Intenzita osvětlení [lux]	Obecný popis snímané scény
100 000	Přímé sluneční světlo
50 000	Slunečno
5 000	Zataženo, vysoká oblačnost
500	Kvalitně osvětlený prostor (prodejna, kancelář)
300	Minimální intenzita pro čtení
100	Nedostatečně osvětlený prostor
60	Chodby, schodiště při denním světle
15	Kvalitně osvětlená ulice v noci
10	Běžně osvětlená ulice v noci
10	Osvětlení při západu Slunce
5	Běžně osvětlená vedlejší ulice v noci
2	Minimální bezpečnostní osvětlení
1	Soumrak
0,3	Osvětlení při jasném úplňku
0,1	Světlo Měsíce při zatažené obloze
0,001	Běžné světlo hvězd
0,0001	Slabé světlo hvězd

Tabulka 2 – Orientační hodnoty intenzity osvětlení za daných podmínek, zdroj: Bezpečnostné kamerové systémy [17].

Výběru vhodného typu kamery by měla předcházet **analýza světelných podmínek** v místě monitorované scény. Na základě požadavků na snímání (např. 24 hodin denně) se provádí rozbor světelných podmínek v zájmové oblasti jak v denní, tak i v noční době, přítomnost protisvětla v zorném poli kamer apod. Kromě přirozeného osvětlení, je nutné brát v úvahu také umělé zdroje světla nacházející se v blízkosti snímaných prostorů (zářivky, lampy, výbojky,…). S tím souvisí volba mezi černobílou a barevnou kamerou. Černobílé kamery vykazují obecně lepší citlivost i při zhoršených podmínkách osvětlení, avšak za cenu ztráty doplňujících informací o snímaném objektu, které mohou být při analýze

záznamu zásadní (barva vozidla, oblečení, vlasů pachatele apod.). Naopak barevné kamery jsou poměrně náchylné na typ a intenzitu osvětlení snímané scény, zejména pokud se jedná o osvětlení umělé, které má odlišné spektrální složení než osvětlení přirozené. Současné IP kamery na trhu disponují citlivostí řádově v desetinách až tisícinách luxu [17].

2.3.1.6 Režim D/N

Výhod barevného i černobílého snímání je využíváno u kamer, které podporují tzv. režim „Den/Noc“ (Day/Night). Tyto kamery pracují při dostatečné úrovni osvětlení v barevném režimu. Při poklesu osvětlení pod danou mez (obvykle kolem 1 luxu) se kamera automaticky přepne do černobílého režimu s vysokou citlivostí (v noci). Při následném zvýšení úrovně osvětlení nad nastavenou hodnotu, se opět aktivuje barevný režim (ve dne). Této funkce je v praxi využíváno především u kamer, určených k nepřetržitému monitorování 24 hodin denně [17].

2.3.1.7 Přísvit

a) Přisvícení ve viditelném spektru – při snížených světelných podmínkách lze použít externí přisvícení v oblasti viditelného spektra s intenzitou osvětlení odpovídající citlivosti použité kamery. Jako zdroje světla jsou nejčastěji používány halogenové reflektory (vysoká spotřeba, nízká životnost) a LED[19] reflektory (nízká spotřeba, vysoká životnost). Z důvodů úspory energie bývá v praxi jeho aktivace podmíněna např. detekcí pohybu v monitorovaném prostoru (PIR detektor).
b) Přisvícení v IR spektru - je-li intenzita osvětlení extrémně nízká, požívá se při snímání za těchto podmínek přisvícení v IR[20] spektru (850 nm, 950 nm). To je realizováno IR LED diodami umístěnými buď přímo v pouzdře kamery (Obrázek 8) nebo v samostatném reflektoru (Obrázek 9). K aktivaci přisvícení dochází automaticky, např. v rámci režimu D/N. Při volbě tohoto typu přisvícení je nutné brát ohled na následující faktory:
    - citlivost kamery na IR záření v požadovaném spektru (IR Cut Filter),
    - stanovení potřebné vzdálenosti, do které má být prostor přisvícen,

[19] Light-Emitting Diode.
[20] Infra Red.

- zajištění rovnoměrného osvícení scény (velikost úhlu přisvícení většinou nekoresponduje s úhlem záběru kamery), např. několika reflektory,
- výběr objektivu schopného zaostřit při IR přisvícení [22] [23].

Obrázek 10 - IP kamera s integrovaným IR přísvitem, zdroj: www.viakom.cz

Obrázek 11 - Externí IR přísvit, zdroj: www.viakom.cz

2.3.1.8 Speciální kamery a funkce

V případě nutnosti detekovat přítomnost osob bez ohledu na světelné podmínky snímané scény je možné použití tzv. **termokamery**. Toto zařízení poskytuje tepelný obraz snímaných objektů v rozmezí teplot -30°C až +2 000°C s citlivostí až 0,05°C. Použití této speciální techniky je v těch nenáročnějších aplikacích, zejména z důvodu méně spolehlivé detekce u běžných typů kamer s IR přísvitem za nízké úrovně osvětlení [17] [24].

Funkce	IP kamera	IP termo kamera
Identifikace	●●●●●	●
Detekce ve dne	●●●●	●●●●●
Detekce v noci	●●	●●●●●
Detekce ve ztížených podmínkách	●●●	●●●●

Tabulka 3 – Přednosti běžné IP a termo IP kamery, zdroj: www.axis.com [24].

V současné době je na trhu celá řada kamer se speciálními funkcemi, které zvyšují kvalitu pořízených záznamů při různých nepříznivých podmínkách. Tyto funkce jistě najdou uplatnění v mnoha aplikacích, kde mohou částečně eliminovat nežádoucí vlivy způ-

sobené např. nevhodně zvoleným typem a umístěním kamery dynamicky proměnlivými podmínkami osvětlení, pohybu objektů apod. [25].

Zkratka	Celý název (v AJ)	Stručný popis
ESC	Electronic Shutter Control	Elektronická závěrka – automaticky reguluje množství dopadajícího světla na snímač na základě osvětlení snímané scény
LSS	Low Speed Shutter	Obrazová paměť – zajišťuje kvalitní obraz při nízkém osvětlení scény
BLC	Back Light Compensation	Eliminace protisvětla – zvýšením kontrastů zájmových objektů částečně kompenzuje vliv silných zdrojů protisvětla
HCL	High Light Compensation	Bodová kompenzace protisvětla – část obrazu s vysokým jasem nahrazuje obrazem tmavým
AWB	Automatic White Balance	Automatické vyvážení bílé – možnost nastavení režimu pro vnitřní/venkovní prostředí na základě teploty chromatičnosti osvětlení
AGC	Automatic Gain Control	Automatické řízení zisku – zvýšení zisku z důvodu zajištění konst. hodnoty výstupního napětí při změnách napětí vstupního
PZM	Privacy Zone Masking	Maskování privátních zón – možnost výběru části obrazu, která nebude zaznamenávána (ochrana soukromí)
DNR	Digital Noise Reduction	Digitální redukce šumu – automatické potlačení šumu vznikajícího při zvyšování citlivosti za nízké úrovně osvětlení
3D DNR	3D Digital Noise Reduction	Vylepšené DNR – kromě výše uvedeného snižuje objem ukládaných dat (až 70%)
DIS	Digital Image Stabilization	Digitální stabilizace obrazu – eliminuje nežádoucí rozostření obrazu při pohybech kamery
WDR	Wide Dynamic Range	Široký dynamický rozsah – umožňuje získat detailní informace z tmavých částí obrazu bez saturace (nasycení) světlých částí obrazu

Tabulka 4 – Příklady speciálních funkcí "inteligentních" kamer, zdroj: Bezpečnostní technologie, systémy a management I. [25].

2.3.2 **Technické kritéria výběru objektivu**

Volba vhodného objektivu do značné míry ovlivňuje výslednou kvalitu pořizovaného záznamu. Primárně rozhodujícími faktory jsou především rozměry snímané scény, resp. vzdálenost sledované zóny od kamery, a charakter pohybu narušitelů v monitorovaném prostoru. Na základě těchto údajů jsme schopni, za pomoci tabulek (viz

Příloha P III), speciálních SW[21] aplikací apod., určit požadované specifikace objektivu. V současnosti je na webu dostupná celá řada nástrojů, určená ke snadným výpočtům (na základě velikosti snímacího čipu) vhodné ohniskové vzdálenosti objektivu, úhlu záběru kamery a dalších parametrů kamerových systémů (např. CCTV kalkulátor) [26]. Tyto aplikace mohou v řadě případů zjednodušit práci při výběru vhodné kamerové soustavy.

Mezi základní parametry objektivů patří zejména:

- způsob uchyceni ke kameře,
- ohnisková vzdálenost,
- světelnost,
- clona,
- možnosti nastavení (clona a ohnisková vzdálenost),
- hloubka ostrosti [17].

2.3.2.1 Způsob uchycení objektivu

V současnosti jsou požívány 2 standardy – C a CS. Oba využívají pro upevnění totožný závit, liší se však ve vzdálenosti roviny poslední čočky od optického snímače kamery. Z hlediska návrhu kamerového systému není tento fakt příliš rozhodující, protože za použití redukce C/CS (5 mm kroužek), můžeme jednotlivé standardy mezi sebou kombinovat [17].

2.3.2.2 Ohnisková vzdálenost

Velikost ohniskové vzdálenosti (f) objektivu určuje rozměry zorného pole snímaného kamerou. Čím je hodnota ohniskové vzdálenosti menší, tím větší prostor bude kamerou snímán. Na základě této závislosti se objektivy dělí na:

- extrémně širokoúhlé (f = 8 mm, tzv. „rybí oko“),
- širokoúhlé (f = 18 – 35 mm),
- základní (f = 45 – 50 mm),
- krátké teleobjektivy (f = 80 – 300 mm),
- dlouhé teleobjektivy (f = 400 – 1 200 mm).

[21] Software.

Jak je z uvedeného výčtu jednotlivých typů patrné, jejich použití se v každé aplikaci liší. Je-li zájmovou oblastí rozsáhlý prostor, volíme objektivy s menším ohniskem, v případě požadavku na úzké zorné pole jsou výhodnější objektivy s vyšší ohniskovou vzdáleností. V tomto případě je však kladen důraz na stabilní upevnění kamery, aby nedocházelo k nežádoucímu rozostření obrazu.

Některé objektivy mají tzv. **zoom**[22], což je schopnost plynule měnit ohniskovou vzdálenost při zachování rozlišení snímku. Toto nastavení probíhá buď manuálně, nebo motoricky. Této funkce je využíváno zejména při monitorování rozsáhlejších oblastí s požadavkem na optické přiblížení obrazu, resp. v případech, kdy není vzdálenost sledovaného objektu stálá (např. městské dohledové systémy, průmyslové areály atd.) [17].

2.3.2.3 Clona

Clona (iris) je mechanické zařízení uvnitř objektivu, které ovlivňuje množství světla dopadajícího na optický snímač kamery. Její nastavení ve vysoké míře určuje kvalitu záznamu (rozlišovací schopnost). Při postupném uzavírání clony se kvalita obrazu zpočátku zlepšuje (světlo prochází přes střední část čoček). Je-li však otvor ve cloně příliš malý, kvalita opět klesá. Toto nastavení velikosti otvoru ve cloně může být pevné nebo manuálně či automaticky nastavitelné [27].

Ohnisková vzdálenost	Clona	Označení
pevná	-	fixfocus bez clony
pevná	manuálně nastavitelná	fixfocus
manuálně nastavitelná	manuálně nastavitelná	variofocus
pevná	motoricky nastavitelná	autoiris (AI)
manuálně nastavitelná	motoricky nastavitelná	variofocus – autoiris
pevná	galvanometricky nastavitelná	autoiris (DC)
manuálně nastavitelná	motoricky nastavitelná	variofocus – autoiris
motoricky nastavitelná	motoricky nastavitelná	motorzoom
motoricky nastavitelná	galvanometricky nastavitelná	DC motorzoom

Tabulka 5 – Technické vybavení objektivů a jejich označení,

zdroj: Bezpečnostné kamerové systémy [17]

[22] Jeho hodnota je udávána jako poměr minimální a maximální ohniskové vzdálenosti.

Při výběru optimální clony se řídíme především provozními podmínkami v místě instalace kamery. Na základě těchto podmínek volíme objektiv podle výše uvedeného clonového čísla F, které udává podíl ohniskové vzdálenosti a průměru otvoru ve cloně (čím nižší, tím je objektiv kvalitnější). Při venkovním použití jsou obecně doporučovány objektivy s automaticky nastavitelnou clonou, která reaguje na úroveň okolního osvětlení. Je tak zajištěn rozsah snímání od úrovně přímého slunečního světla, až po úroveň omezenou vlastní citlivostí kamery [17].

2.3.2.4 Světelnost

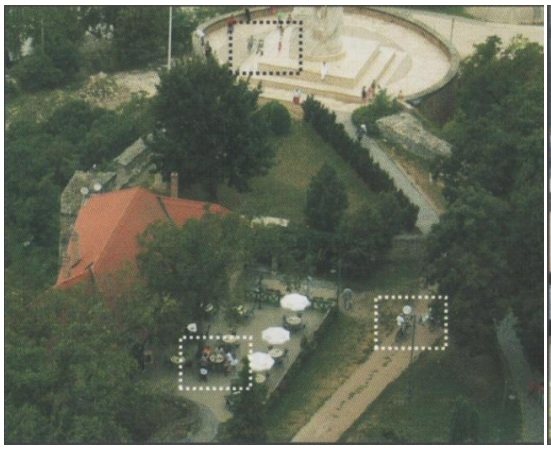
Další charakteristickou vlastností objektivů je **světelnost**. Jedná se o maximální schopnost objektivu přijímat odražené světlo. Bývá popisována tzv. clonovým číslem (F), přičemž čím je jeho hodnota nižší, tím je světelnost větší. Při výběru optimálního objektivu obecně platí, že při snímání méně osvětlené scény volíme nižší hodnoty clonového čísla a naopak [17].

2.3.3 Doporučené velikosti objektu

Dalším z významných faktorů ovlivňujících umístění a volbu kamery a objektivu je požadovaná velikost snímaného objektu na zobrazovacím zařízení, resp. požadovaný stupeň rozpoznání dle ČSN EN 50132-7. Při volbě jednotlivých stupňů identifikace se navrhovatel kamerového systému řídí podle požadavků investora, resp. podle toho, co má být předmětem snímání (pohyb osob, prováděná činnost, detail tváře apod.). Níže uvedená tabulka (Tabulka 3) popisuje kromě aktuálních stupňů identifikace také 2 nové, které specifikuje revize normy prEN 50132-7 (přehled a inspekce).

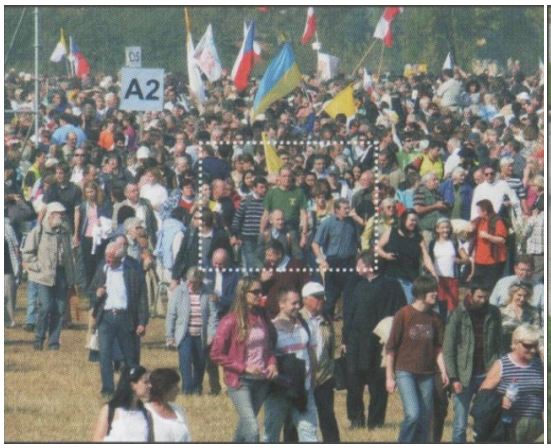
Název	Výška osoby na monitoru [%]	[mm/1 pixel]
Monitorování skupiny (davu)	> 5	80
Detekce	> 10	40
Přehled	> 25	16
Rekognoskace (rozpoznání obrysů)	> 50	8
Identifikace	> 100	4
Inspekce	> 400	1

Tabulka 6 – Doporučené výšky postavy na zobrazovacím zařízení dle prEN 50132-7 pro rozlišení PAL (576i), zdroj: IP CCTV Guideline [18]



Obrázek 12 – Monitoring,
zdroj: IP CCTV Guideline [18]

Obrázek 13 – Detekce,
zdroj: IP CCTV Guideline [18]



Obrázek 14 – Přehled,
zdroj: IP CCTV Guideline [18]

Obrázek 15 – Rekognoskace,
zdroj: IP CCTV Guideline [18]

Obrázek 16 – Identifikace,
zdroj: IP CCTV Guideline [18]

Obrázek 17 – Inspekce,
zdroj: IP CCTV Guideline [18]

Postupný přechod z analogových kamerových systémů na digitální s sebou přinesl mimo jiné i nové možnosti z hlediska rozlišení pořizovaných záznamů. Kamery s vysokým rozlišením umožňují zachytit kvalitní záznam z oblasti zájmu, ze kterého lze s využitím digitálního přiblížení snadněji identifikovat objekty, osoby, automobily apod. Dalším přínosem je také schopnost kamery pokrýt větší zorné pole při současném zachování kvality pořizovaného záznamu, což s sebou přináší především úsporu z hlediska potřeby nižšího počtu kamer, zjednodušení systému a menšího objemu instalačních prací. Při použití kamer s vysokým rozlišením však rostou požadavky na kvalitu osvětlení monitorovaného prostoru (pixely snímače pojmou za jednotku času menší množství světla) a na datovou propustnost přenosové sítě. Zároveň již také není možné vycházet z procentuelní velikosti objektu na zobrazovací jednotce u jednotlivých stupňů identifikace. U jiných rozlišení než PAL, je tedy nutné provést samostatný přepočet (viz Tabulka 4) na základě poměru rozlišení. V těchto případech se při výpočtu vychází z předpokladu, že rozlišení PAL (576i) odpovídá rozlišení cca 400 pixelů (tzv. Kellův faktor $K \approx 0{,}75$) [18] [27].

Typ záběru	**Rozlišení**						
	PAL	1080p	720p	SVGA/4CIF	VGA	2CIF/CIF	QCIF
Inspekce	400	150	250	300	350	600	1 200
Identifikace	100	40	60	70	85	150	300
Rozpoznání	50	20	30	35	45	70	150
Přehled	25	10	15	25	25	35	70
Detekce	10	10	10	10	10	15	30
Monitoring	5	5	5	5	5	10	15

Tabulka 7 – Přepočet pro nejběžnější rozlišení dle prEN 50132-7 (uvedeno v %), zdroj: IP CCTV Guideline [18]

2.3.4 **Příslušenství**

Pro zajištění bezproblémového provozu kamerového systému je nutné zvolit vhodné příslušenství na základě funkčních požadavků a klimato-mechanických podmínek jednotlivých kamer v místě monitorování. Důležité je zejména analyzovat veškeré nepříznivé vlivy, kterým může být kamera při svém provozu vystavena. Obecně se jedná o:

- povětrnostní vlivy (voda, vítr, změny teplot, UV záření, vlhkost atd.)
- mechanické vlivy (vibrace, vandalismus)
- chemické vlivy (koroze)
- elektromagnetické rušení

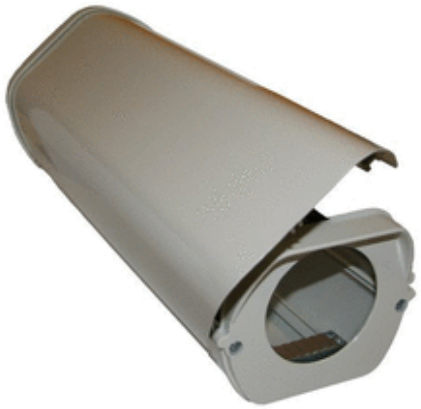
- nebezpečné prostředí (výbuch, vysoké teploty, apod.)

Informace získané při analýze výše uvedených faktorů je vhodné doplnit např. statistickými informacemi o počasí (Český hydrometeorologický ústav), kriminalitě (Policie ČR) atd. v daném lokalitě instalace kamerového systému [12] [17].

2.3.4.1 Kamerové kryty

Kamerový kryt slouží primárně k ochraně kamery, objektivu a dalších zařízení před vnějšími vlivy (prach, vlhkost,…), neoprávněnou manipulací, popř. odcizením. Podle provozních podmínek, ve kterých pracují, se dají rozdělit na kryty pro vnitřní a venkovní použití. Jejich součástí bývají také utěsněné průchody pro kabely.

Obrázek 18 - Kamerový kryt pro vnitřní použití, zdroj: www.viakom.cz



Obrázek 19 - Polohovací hlavice pro vnitřní použití, zdroj: www.escatrade.cz

Ve vnitřních prostorech chrání kamerové kryty především proti manipulaci, odcizení a ve speciálním provedení „antivandal“ také proti mechanickému poškození. Tyto odolné kryty bývají označovány tzv. IK kódem dle ČSN EN 62262, stupně ochrany poskytované kryty elektrických zařízení proti vnějším mechanickým nárazům. Nasazení „antivandal“ krytů má v praxi význam především ve veřejně přístupných prostorech, resp. v místech s vysokým rizikem poškození nebo odcizení kamery.

Co se týče krytů pro venkovní použití, musí kromě mechanické ochrany poskytnout také ochranu proti povětrnostním vlivům, prachu atd. Tento požadavek řeší norma ČSN EN 60529, stupně ochrany krytem. Kvalita krytí je dle normy popisována tzv. IP kódem ve tvaru IP XY, přičemž X označuje úroveň krytí před nebezpečným dotykem a vniknutí ci-

zích předmětů a Y ochranu před vniknutím vody. Jelikož jsou kamery ve venkovním prostředí často vystavené velkým změnám teplot (den/noc), je nutné zajistit jednak dostatečné odvětrávání, ale také přídavné vyhřívání krytu, aby nedocházelo např. k vysrážení vzdušné vlhkosti, přehřívání elektroniky apod.

V současné době jsou na trhu k dostání také kryty pro speciální aplikace. Jedná se zejména a o nebezpečná a agresivní prostředí (výbušné, s vysokou teplotou, chemicky agresivní apod.), popř. prostředí vyžadující sterilitu a zdravotní nezávadnost (kontrola léčiv, potravin atd.).

Výběr optimálního krytu souvisí také s umístěním kamery z hlediska budoucí údržby a servisních prací. Proto by měl být pro technika snadno přístupný (např. z plošiny, žebříku) [17].

2.3.4.2 Polohovací hlavice

Toto příslušenství umožňuje obsluze kamerového systému (popř. dle nastavených předvoleb) dálkově měnit horizontální i vertikální orientaci zorného pole kamer. Podle provozních podmínek je můžeme rozdělit na polohovací hlavice pro vnitřní a vnější použití, podle konstrukce na externí a integrované. Externí polohovací hlavice umožňují upevnění kamerového krytu a následné uchycení celého systému na zeď, strop, svěrkou na sloup, popř. na jeho vrchol. Hlavice integrované tvoří polohovací systém, který je umístěný společně s kamerou v krytu. Tento typ hlavic (krytů) bývá označován „DOME“. Co se týče parametrů rozhodujících při výběru vhodné polohovací hlavice, jedná se zejména o:

- nosnost (až 30 kg)
- horizontální a vertikální rychlost natočení (např. 6°/s)
- horizontální a vertikální úhel natočení (např. 0 – 330°)
- napájení (24 – 230V)
- speciální funkce („autopan“ – automatický režim otáčení)
- provedení (antivandal, speciální aplikace)

Pozornost je nutné také věnovat případné nežádoucí vůli v osách pohybu, která může způsobit při silném větru rozechvění kamery, přesnosti pohybu nastavených programových předvoleb a dostatečné vzdálenosti okolních předmětů od kamery [17].

Obrázek 20 - Polohovací hlavice pro venkovní použití, zdroj: www.escatrade.cz

Obrázek 21 - Polohovací hlavice pro vnitřní použití, zdroj: www.escatrade.cz

2.3.4.3 Upevnění

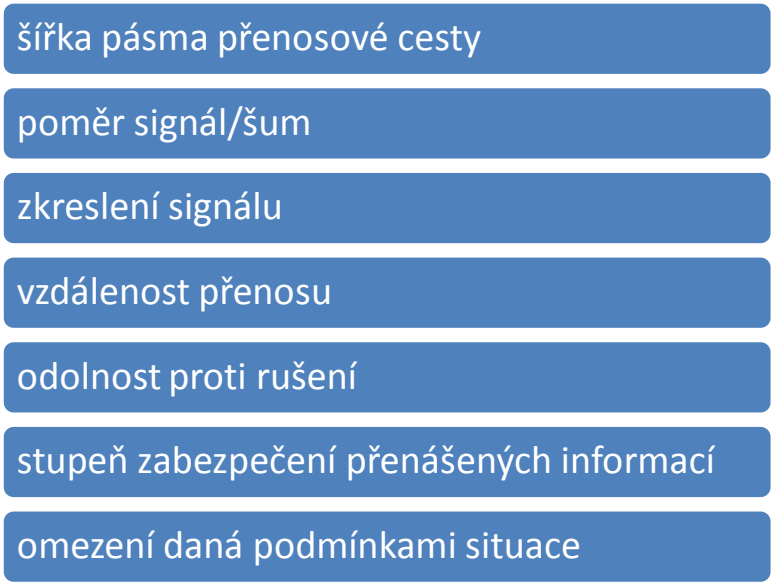
Upevnění kamery by mělo být dle ČSN EN 50132-7 mechanicky stabilní, přístupné a bezpečné z hlediska manipulace, s ohledem na stavební požadavky. Způsob a stabilitu upevnění kamery ovlivňuje zejména její hmotnost (včetně příslušenství) a zorný úhel snímaní. Obecně platí, že čím je zorný úhel kamery menší, tím jsou požadavky na stabilitu a kvalitu upevnění vyšší. V náročnějších aplikacích (banky, čerpací stanice,…) může být jedním z požadavků i ochrana proti sabotáži – ta je z hlediska upevnění řešena především skrytým vedením přívodních kabelů [17].

2.4 PŘENOSOVÝ SYSTÉM

Obrovskou výhodou systémů síťového videa je fakt, že využívají k přenosu dat (video, zvuk,…) digitální TCP/IP sítě. Tuto problematiku řeší normy pro ICT[23] ČSN EN 50174 a ČSN EN 50173. Z toho vyplývá, že jednotlivé způsoby přenosu, topologie systému, záznam dat, zálohování dat apod. budou u kamerových systémů síťového videa obdobné jako u počítačových sítí.

[23] Information and communication technologies

Volbu způsobu přenosu a přenosového média je nutné pečlivě vyhodnotit pro každou aplikaci zvlášť – zohledňují se zejména podmínky a prostředí, ve kterých má přenos signálu probíhat, vzdálenost přenosové trasy mezi jednotlivými prvky systému, datová propustnost přenosového systému, nepříznivé vlivy na přenos (EMI[24]) apod.



Obrázek 22 – Kritéria výběru zařízení pro přenos videosignálu dle ČSN EN 50132-7

U kamerových systémů síťového videa je k přenosu dat využíváno zpravidla metalického (UTP/STP), bezdrátového (Wi-Fi) nebo optického spojení (FO – fiber optic). Každé z nich má jiné specifické vlastnosti, přičemž volba optimální varianty závisí na výše uvedených kritériích [18].

2.5 KONFIGURACE ŘÍDÍCÍHO PRACOVIŠTĚ

Řídící pracoviště kamerového systému a jeho konfigurace vychází z provozních požadavků a personálních možností provozovatele systému. Obecně se skládá ze zobrazovacích a ovládacích zařízení kamerového systému, datového úložiště a další podpůrných zařízení. Při návrhu konfigurace řídícího pracoviště je nejprve nutné stanovit jeho účel a

[24] Elektromagnetická interference = elektromagnetické rušení

režim. Podstatný je především časový provoz pracoviště – ten může být nepřetržitý (24/7), časově omezený (v rámci pracovní směny), podmíněný vznikem události (poplach) atd. Dále se rozlišuje, zdali je potřebná fyzická obsluha k vyhodnocování pořízených záznamů nebo zdali jsou záznamy analyzovány automaticky (např. softwarově). Všeobecným trendem v současnosti je snaha o co největší míru automatizace a samostatné činnosti kamerových systémů – jednak z důvodu většího komfortu obsluhy, ale především z důvodu efektivnějšího a kvalitnějšího vyhodnocování pořízených záznamů. U rozsáhlejších aplikací s velkým množstvím kamer (letiště, průmyslové podniky, obchodní centra) to bývá často obtížné, resp. vyžaduje zvýšené personální požadavky. Jelikož je řídící pracoviště důležitou součástí kamerového systému, je vhodné ho vybavit záložním zdrojem energie (UPS[25]), který se automaticky aktivuje v případě výpadku standardního napájení systému. S prolínáním kamerových a ICT systémů též souvisí pojem tzv. **redundance**. Jedná se o použití více prvků systému, než je nutné, z důvodu zajištění jeho provozu v případě poruchy některého zařízení. Z hlediska systémů síťového videa se jedná zejména o redundanci na úrovni síťové, hardwarové a softwarové. Norma ČSN EN 50132-7 a další legislativa (viz kapitola 1) dále vyžaduje, aby bylo řídící pracoviště patřičně zabezpečeno proti neoprávněnému přístupu, manipulaci s pořízenými záznamy atd. Zabezpečení bývá zpravidla realizováno za pomoci poplachvých zabezpečovacích systémů (ČSN EN 50131) a systémů pro kontrolu vstupu (ČSN EN 50133). Celkovou koncepci a uspořádání řídícího centra, zobrazovací zařízení (displeje), ergonomii atd. popisuje norma ČSN EN ISO 11064-3, Ergonomické navrhování řídících center – Část 3: Uspořádání velínu [18] [12].

2.6 STANOVENÍ ZPŮSOBU ÚDRŽBY

Způsob a rozsah údržby musí být v souladu s požadavky projektanta nebo dodavatele kamerového systému. Jednotlivé zkoušky funkčnosti probíhají periodicky dle předem stanoveného plánu údržby. Tento plán by měl také obsahovat seznam speciálních zkušebních přístrojů a nástrojů, přičemž před samotnou údržbou je vyžadováno, aby byly použité zařízení kalibrovány. Jelikož se v případě údržby jedná o zodpovědnou činnost, měla by být prováděna pouze patřičně kvalifikovanými pracovníky. Ti musí být také pravidelně

[25] Uninterruptible Power Supply

proškolováni z hlediska údržby systému v souladu s legislativními požadavky (zákon 101/2000 Sb.) Výsledky jednotlivých zkoušek, oprav apod. je vhodné pečlivě zaznamenávat, aby bylo možné jejich vzájemné porovnání [12].

2.7 DÍLČÍ ZÁVĚR

Jak je patrné z obsahu předchozích kapitol, návrh kamerového systému může ovlivňovat celá řada faktorů. Kromě požadavků platné legislativy je nutné vyhovět také specifickým požadavkům zákazníka (zadavatele) – zejména jaké výsledky od nasazení kamerového systému očekává. Zadavatel proto musí definovat jednotlivé oblasti monitorování a konkrétní objekty, prováděné činnosti a dalších informace, které budou z pořízených záznamů analyzovány. Na základě těchto požadavků projektant zvolí optimální počet a rozmístění jednotlivých kamer. Tato fáze návrhu je poměrně důležitá, neboť ovlivňuje nejen kvalitu a charakter pořizovaných záznamů, ale také finanční náklady celého systému. Jednotlivé komponenty jsou sice stále cenově dostupnější, ale provoz systému se může zbytečně prodražit např. při nákupu licencí pro jednotlivé kamery u softwarových aplikací apod. Kromě toho se může provozovatel kamerového systému při špatném rozmístění kamer dostat do konfliktu se zákonem (viz kapitola 1).

Ze stanovených umístění lze na základě analýzy provozních podmínek a požadavku na charakter snímání vybrat konkrétní typy a provedení kamer včetně jejich příslušenství. V případě analýzy provozních podmínek jsou stěžejní zejména povětrnostní a světelné podmínky ve snímaného prostoru. Co se týče světelných podmínek, tak ty přímo ovlivňují výběr technologie snímání kamery, použitého objektivu a dalších parametrů kamerové sestavy (kamera, objektiv a nezbytné příslušenství). Proto je důležité zhodnotit podmínky pro celou dobu provozu dané kamery, v případě nepřetržitého monitorování tedy ve dne i v noci. Na základě znalosti předpokládaných povětrnostních a ostatních vlivů, kterým bude kamerová sestava při provozu vystavena, je pak k jednotlivým kamerám přiřazeno vhodné příslušenství (kryty, upevnění atd.).

Dalším kritériem při návrhu kamerového systému je požadovaný způsob přenášení videozáznamu a dat z kamer. Jak už bylo uvedeno dříve, u systémů síťového videa je pro přenos využíváno sítí pracujících s protokolem TCP/IP. V tomto případě je z hlediska návrhu situace poměrně jednodušší – lze totiž pro přenos dat využít stávající sítě (LAN, in-

ternetu), která je již u řady objektů běžným standardem. Musí ovšem splňovat požadavky na datovou propustnost apod., aby nedocházelo k jejímu přetížení.

Co se týče konfigurace řídícího pracoviště, definování jednotlivých kritérií pro návrh kamerového systému není tak jednoduché. Jednou z výhod systémů síťového videa je možnost kompletní vzdálené správy celého systému. Uživatel kamerového systému se tak nemusí vůbec nacházet v blízkosti střeženého objektu. Tento fakt však nic nemění na tom, že řídící pracoviště je jednou ze stěžejních částí kamerového systému, a proto je tedy nutné ho kvalitně zabezpečit, ať už proti neoprávněnému přístupu nebo jiným možným hrozbám (výpadky el. energie, přepětí v síti, zálohování dat apod.).

S návrhem kamerového systému úzce souvisí také stanovení způsobu a rozsahu údržby. Ta probíhá na základě smluvní dohody mezi provozovatelem a dodavatelem kamerového systému. Četnost a míra úkonů v rámci údržby závisí zejména na jeho provozních podmínkách – v průmyslových a jiných náročných aplikacích budou nároky na údržbu značně vyšší, než v menší prodejně s relativně stálými provozními podmínkami. Ať už jsou požadavky na údržbu jakékoliv, měly by jednotlivé prohlídky probíhat v předem stanovených intervalech, přičemž veškeré provedené činnosti, zkoušky a jejich výsledky musí být patřičně zdokumentovány.

3 VÝVOJOVÉ TRENDY V OBLASTI KAMEROVÝCH SYSTÉMŮ

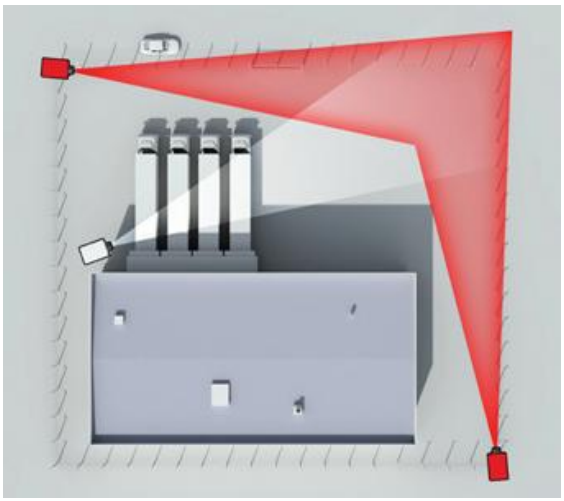
Co se týče blízké budoucnosti kamerových systémů, jsou vývojové trendy již víceméně jasné. Digitální kamerové systémy brzy plně nahradí stávající analogové. Donedávna tomuto vývoji bránila vysoká pořizovací cena jednotlivých IP zařízení. To už však v nynější době neplatí – za takřka srovnatelné náklady v porovnání s analogovým systémem lze realizovat IP kamerový systém (plně digitální), který současně nabízí nesrovnatelně větší flexibilitu, snadnější správu a řadu dalších užitečných funkcí. Současně se také zvyšuje míra konvergence mezi kamerovými systémy a ICT a spolupráce s dalšími bezpečnostními i komerčními aplikacemi. Na základě těchto okolností již současná zkratka CCTV (Closed = uzavřený) vzhledem k otevřenosti IP systémů neodpovídá skutečnosti. CENELEC proto plánuje v blízké době nahradit dosavadní označení CCTV novým - VSS (Video Surveillance System).

Jako tomu bylo po nástupu digitálních fotoaparátů a videokamer na trh, i v oblasti IP kamer se dá očekávat „hon“ výrobců za co největším rozlišením. Vývoj a postupné zdokonalování technologií snímání obrazu povede k tomu, že IP kamery s rozlišením v řádech jednotek až desítek megapixelů budou běžným standardem. Současně se zvyšujícím rozlišením přirozeně porostou i nároky na datové sítě v oblasti kvality služeb, metod komprese a rychlosti přenosu dat. S inovací technologií úměrně klesne koncová cena jednotlivých zařízení, což povede k větší dostupnosti běžným uživatelům. Mezi další novinky, které umožňují současné IP kamery na trhu, je možnost lokálního záznamu obrazových dat na paměťové SD karty přímo v kameře.

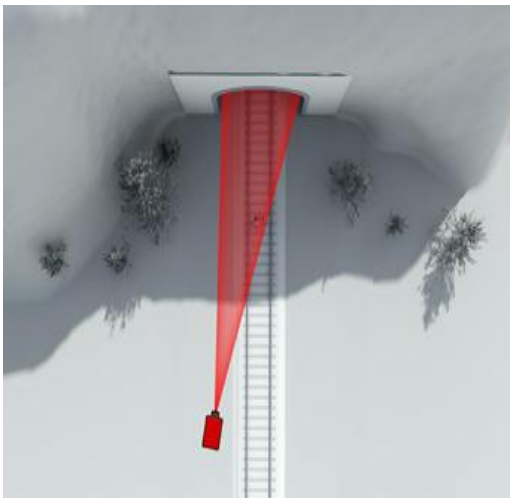
Řada komerčních subjektů začíná postupně nabízet službu tzv. VSaaS (Video Surveillance as a Service). Tato služba pracuje na principu vzdáleného úložiště dat (tzv. cloudu). Uživatel se tak nemusí v praxi starat o správu a zabezpečení pořízených záznamů, jejich uchovávání, zálohování apod. Firma nabídne v rámci VSaaS na základě smluvních závazků kompletní řešení pro danou aplikaci dle požadavků zákazníka. Ten zjednodušeně řečeno pouze připojí vhodné kamery do sítě internet a o víc se nestará. S „cloudovými“ službami úzce souvisí také služby mobilní – současné mobilní platformy již dovolují vývoj kvalitního softwaru pro bezpečnostní aplikace a vzdálený přístup ke kamerovému systému, včetně jeho ovládání. Uživatel má tak možnost monitorovat kamerový systém odkudkoliv a kdykoliv ze svého mobilního telefonu, tabletu apod.

Další z oblastí, ve které se dá očekávat vývoj, jsou možnosti inteligentní videoanalýzy obrazu. Obecný trendem je snaha o přenesení zodpovědnosti obsluhy na jednotlivá zařízení či software. To má pak za následek zvýšení efektivity a optimalizace kamerového systému. Inteligentní videoanalýza tak najde uplatnění zejména ve veřejně přístupných budovách, vlakových a jiných nádražích, letištích apod., kde zvyšuje úroveň bezpečnosti a ochrany veřejných zájmů. Kamera tak např. na základě překročení definované virtuální linie (detekce osob v kolejišti) nebo v případě zjištění odloženého předmětu (podezřelá zavazadla) upozorní obsluhu kamerového systému, která může včasně a efektivně reagovat na danou situaci. Kromě bezpečnostních aplikací inteligentní videoanalýza otvírá další možnosti komerčního využití kamerových systémů. Jedná se zejména o součinnost s jinými systémy [28].

Současná úroveň technologické vyspělosti dostupných IP kamer dovoluje jejich použití v řadě náročných aplikací (IP termokamery), mimo jiné i k zajištění perimetrické ochrany průmyslových či jiných rozsáhlejších objektů (fotovoltaické elektrárny), zvyšování bezpečnosti (detekce osob v tunelech a jiných nebezpečných prostředích) apod [24].



Obrázek 23 – Střežení perimetru pomocí IP termokamery, zdroj: www.axis.com [24]

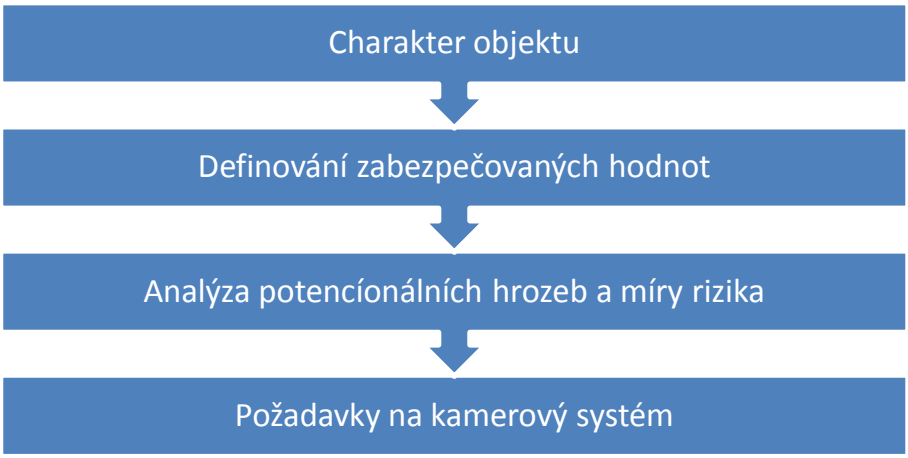


Obrázek 24 – Detekce přítomnosti osob v tunelu pomocí IP termokamery, zdroj: www.axis.com [24]

II. PRAKTICKÁ ČÁST

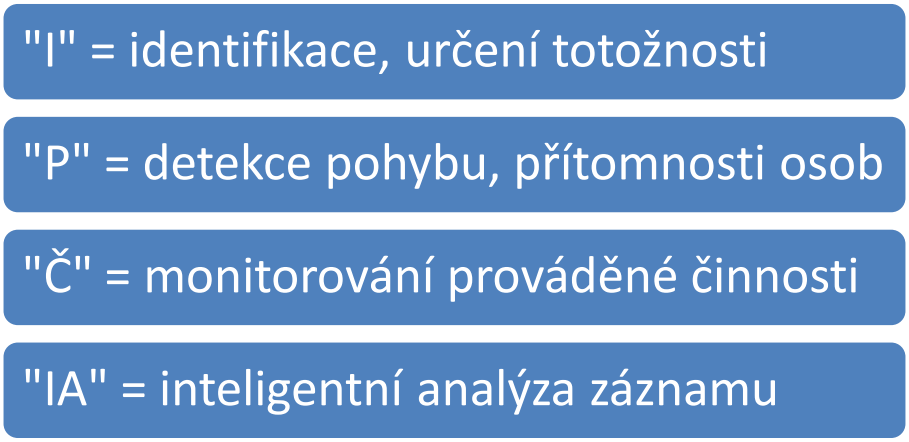
4 SPECIFIKACE MODELOVÝCH OBJEKTŮ

V této kapitole jsou popsány vybrané modelové objekty a analyzovány jejich **unikátní požadavky** na kamerové systémy. Jednotlivé modelové objekty jsou voleny tak, aby jejich specifikace zahrnovala nejčastější bezpečnostní aplikace CCTV v praxi a aby jejich požadavky na kamerový systém byly diametrálně odlišné. Současně jsou objekty záměrně navržen, aby znázorňovaly využití co možná nejširší škály aplikací CCTV, a tvořily tak sofistikovaný model pro tvorbu návrhu kamerových systémů. Jako stěžejní kritéria, na které je nutné při návrhu kamerového systému přihlížet, jsou zvoleny zejména základní **charakteristiky** daných **objektů** z hlediska dislokace, provozní (pracovní) doby, personálního zajištění apod. Zohledněny jsou také režimová opatření, která v rámci jednotlivých modelových objektů obecně platí. Dalším z kriterií návrhu je **definování** zabezpečovaných **aktiv**, tzn. podrobná analýza hodnot, které mají být u daného modelového objektu chráněny nasazením kamerového systému. Ze znalosti zabezpečovaných hodnot se dá dále vytipovat charakter potencionálního pachatele (předpokládané chování, vybavenost, způsoby průniku do objektu atd.) popř. jiné nežádoucí situace, které mohou při ochraně aktiv nastat.



Obrázek 25 – Kritéria návrhu kamerového systému u modelových objektů, zdroj: archiv autora

Co se týče konkrétních zón monitorování, jsou vytipovány na základě požadovaných stupňů identifikace dle prEN 50132-7, očekávaných provozních podmínek (třída prostředí dle ČSN EN 50132-1) a objektu snímání.



Obrázek 26 – Stanovené objekty snímání pro konkrétní prostory modelových objektů, zdroj: archiv autora

4.1 FINANČNÍ INSTITUCE - BANKA

4.1.1 Charakteristika objektu

Banky byly odedávna střetem zájmu trestné činnosti, ať už se jedná o loupežná přepadení jedinců nebo organizovaných skupin. Ačkoliv se to zdá být v současné době plné vyspělých zabezpečovacích technologií nemožné, stávají se bankovní instituce i dnes častým terčem loupežných přepadení. Vysoká atraktivita těchto objektů je dána především manipulací s velkým množstvím finančních prostředků, popř. jiných cenných propriet. Zabezpečení takového objektu je tedy na místě. V řadě případů bývá realizováno kombinací několika typů technického zabezpečení (MZS, PTS, PZS, CCTV, ACS,…) popř. doplněnou o fyzickou ostrahu a striktní režimová opatření. V každém větším městě můžeme najít i několik finančních institucí. Jedná se buď o samostatné budovy (sídlo banky) nebo o pronajímané prostory určené pro jednotlivé pobočky (částečné omezení poskytovaných služeb). Tyto objekty jsou v průběhu otvírací doby (zpravidla přes den) volně přístupné veřejnosti, některé z prostor (schránky, místnost s bankomatem) dokonce 24 hodin denně. Tato skutečnost sice zvyšuje komfort služeb poskytovaným zákazníkům, ale současně také požadavky na kvalitu zabezpečení a unikátní řešení režimových opatření.

Obrázek 27 – Budova KB, Třebíč,

zdroj: www.kb.cz

4.1.2 Zabezpečovaná aktiva

V případě zabezpečovaných hodnot se u bankovních institucí jedná zejména o:

- hmotný majetek (finanční hotovost, předměty v úschově, bankomaty atd.)
- nehmotný majetek (informace o klientech, účtech apod.)
- bezpečnost zaměstnanců, klientů

4.1.3 Potencionální rizika a hrozby

Jak již bylo výše zmíněno, bankovní instituce jsou pro páchání trestné činnosti vysoce atraktivní. Jedná se zejména o loupežná přepadení s cílem odcizit finanční hotovost. Pachatelé jsou obecně (až na výjimky) kvalitně technicky a takticky vybavené organizované skupiny, které disponují v řadě případů podrobnou znalostí daného objektu a pravidlem bývá také použití maskování a různých typů zbraní, popř. výbušnin [30].

4.1.4 Oblasti zájmu monitorování

Z charakteru zabezpečovaných hodnot a potencionálních pachatelů vyplývají jednotlivé oblasti zájmu, které je z hlediska bezpečnosti nutné kamerovým systémem monitorovat. Kamerový systém jako takový sice páchání trestné činnosti fyzicky nezabrání, ale v součinnosti s ostatními typy zabezpečení (technické, fyzické,…) vede ke zvýšení úrovně ochrany zájmů a aktiv banky. Cíle nasazení kamerového systému jsou tedy:

a) možnost identifikace případného pachatele ze záznamu

b) sledování činnosti pracovníků banky, klientů
c) detekce pohybu
d) inteligentní analýza záznamu
e) ochrana majetku instituce

Ad b) Na základě záznamu činnosti zaměstnanců banky, lze zpětně analyzovat např. podezřelé chování, nedodržování standardních postupů, zanedbání povinností atd., což může vést např. k zajištění personálních opatření, změny režimových opatření atd.

Ad c) Jedním ze zájmů je také ochrana majetku instituce. Jedná se zejména o technické (bankomaty, IT technika,…) a materiální vybavení, které je volně přístupné veřejnosti.

V následující tabulce (Tabulka 8) jsou uvedeny nejběžnější monitorované prostory v budově banky a k nim vztažené předpokládané objekty snímání [29].

Stupeň identifikace	Prostory	Třída prostředí	Objekt snímaní[26]
Inspekce	pokladna, hotovostní pracoviště	I.	I
Identifikace	hotovostní pracoviště	I.	I
	vstupy do trezorů	I.	I, P
	vstupy do technických prostorů	I., II.	I, P
	dotační trasy	I., II.	I, P
	příchodové a odchodové trasy	I., II.	I, P
	přístup k zákaznickým schránkám	I., II.	I, Č
	přístup k úschovnému místu	II., III.	I, Č
	provoz bankomatu	II., III.	I, Č
Rekognoskace	bankovní hala	II.	P, IA
	komunikační cesty	III., IV.	P, IA
	průběh pracovní směny	I.	Č
Přehled	vjezd do dotačního boxu	III., IV.	P, IA

Tabulka 8 – Oblasti zájmu u modelového objektu – Banka, zdroj: archiv autora

4.1.5 **Požadavky na kamerový systém**

V případě zabezpečení bankovní instituce jsou kladeny jedny z nejvyšších požadavků na zabezpečovací systémy a další opatření. Zanedbání některého z nich může vést ke značným ztrátám, ať už na zdraví osob, nebo majetku. Jednotlivé prvky systému proto

[26] Uvedené objekty snímání nejsou závazné a mohou se dle dané aplikace lišit.

bývají zařazeny do stupně zabezpečení 3 a 4. Z důvodu častého geografického rozptýlení jednotlivých poboček bank je též nutné zajistit dostatečné zálohování napájení bezpečnostních systémů a kvalitní zabezpečené připojení na datovou síť (např. optický přenos). Vyžadována může být také spolupráce kamerového systému s jinými bezpečnostními prvky (poplachové zabezpečovací a tísňové systémy,…).

Použití systémů síťového videa v těchto aplikacích, přináší s sebou řadu výhod, které vedou ke včasnému rozpoznání nebezpečí a efektivní reakci na něj. Jednou z nich např. analýza zvuků v monitorovaném prostoru. Nebezpečí v řadě případů předchází křik, výhružky atd. - detekce zvýšené hladiny zvuku pak může být signálem pro aktivaci záznamu a upozornění obsluhy (ostrahy). Další výhodou je vysoká kvalita pořízených záznamů, která umožňuje snadnější identifikaci pachatele. S režimovými opatřeními v rámci bankovní instituce úzce souvisí oprávněnost osob přistupovat do určitých prostorů. Inteligentní videoanalýza obrazu umožňuje nastavení virtuálních zón, linií a perimetrů, přičemž dojde-li k jejich narušení, systém je schopen na tyto okolnosti v reálném čase reagovat. Obdobně to platí např. při využití detekce odložených předmětů, podezřelého postávání v daném prostoru atd. Všechny tyto možnosti jednak snižují míru rizika újmy na zdraví a majetku, ale především usnadňují práci obsluze kamerového systému. Ta je schopna rychle a efektivně reagovat na hrozící nebezpečí a minimalizovat případné následky.

4.2 ČERPACÍ STANICE

4.2.1 Charakteristika objektu

Čerpací stanice jsou dalšími z rizikových objektů. Jejich umístění bývá často izolované, na okraji městských částí, popř. u dálnic a rychlostních silnic. Co se týče zabezpečení, je v mnoha případech (malé čerpací stanice) neodborně nainstalováno, popř. zvolená technologie neodpovídá požadavkům investora. Příčinou obvykle bývá požadavek provozovatele čerpací stanice na co nejnižší cenu kamerového systému. Stává se tak například, že kamera sice zachytí pachatele, SPZ[27] atd., ale pořízený obraz nelze přiblížit při zachování dostatečné kvality záznamu. Jednoznačná identifikace pachatele (vozidla) je pak z takového záznamu nemožná. Provoz těchto zařízení bývá dvojího typu:

[27] Státní poznávací značka

a) non-stop (24 hodin denně)
b) s omezeným provozem

Vetší čerpací stanice nadnárodních společností (Shell, OMV, Agip,…) v dnešní době obvykle kromě prodeje pohonných hmot (dále jen PH) plní i řadu dalších funkcí, jako například samoobsluhy, restaurace, odpočívadla, prodeje základního auto/moto příslušenství, servisu atd. Tomuto stavu však často z personálního hlediska neodpovídá počet zaměstnanců.

Obrázek 28 – Čerpací stanice OMV, Staré Město u Uherského Hradiště, zdroj: www.trevo.cz

4.2.2 **Zabezpečovaná aktiva**

Čerpací stanice sice primárně slouží k prodeji PH a poskytování dalších služeb, mezi zabezpečovaná aktiva však kromě nich může patřit celá řada dalších hodnot. U tak rizikového objektu je to především bezpečnost osob, ochrana životního prostředí apod. Střežené hodnoty tedy v případě čerpací stanice obecně tvoří:

- bezpečnost personálu, zákazníků
- finanční hotovost
- majetek čerpací stanice (PH, spotřební zboží, příslušenství atd.)
- ochrana životního prostředí

4.2.3 Potencionální rizika a hrozby

Odlehlé umístění, dlouhá provozní doba a nedostatečné zabezpečení (technické, personální) – to vše je příčinou tak časté kriminální činnosti, která se týká čerpacích stanic. Jedná se zejména o krádeže PH (menšího rozsahu), krádeže zboží (cigarety, alkohol, příslušenství auto/moto) a loupežné přepadení ozbrojenými jednotlivci nebo organizovanými skupinami. Co se týče dalších hrozeb, je důležité zohlednit také reálnou možnost výbuchu a požáru a s tím související dodržování bezpečnostních opatření [29].

4.2.4 Oblasti zájmu monitorování

Stupeň identifikace	Prostory	Třída prostředí	Objekt snímaní[28]
Identifikace	prostor pokladny	I.	I, Č
	zboží v prodejně	I.	I, Č
	stojany s PH	III.	I, Č
	průběh pracovní směny	I., II.	I, Č
Rekognoskace	příjezdové/odjezdové trasy	III., IV.	I, P, IA
Přehled	vstupní ventily zásobníků s PH	III., IV.	P
	perimetr čerpací stanice	III., IV.	P, IA
	skladovací a ostatní prostory (myčka)	III., IV.	P, IA

Tabulka 9 – Oblasti zájmu u modelového objektu - Čerpací stanice, , zdroj: archiv autora

4.2.5 Požadavky na kamerový systém

Z hlediska obecných provozních podmínek kamerového systému na čerpací stanici, je nutné zajistit, aby použité kamery zvládaly pracovat v režimu Den/Noc (v případě nízkého osvětlení rozšířený o IR přísvit) a měly dostatečné rozlišení nutné k pořízení kvalitních záběrů. Jsou-li podmínky osvětlení až příliš nepříznivé, je možné použití IP termokamer. Vhodná je také volba kamer (softwaru) ovládajících speciální obrazové funkce (viz kapitola 2.3.1.8), jedná se zejména o rozpoznávání SPZ projíždějících vozidel. Venkovní kamery je navíc potřeba vybavit krytem s dostatečnou úrovní IP krytí, vyhříváním, ventila-

[28] Uvedené objekty snímání nejsou závazné a mohou se dle dané aplikace lišit.

cí a pokud možno i v „antivandal“ provedení s detekcí sabotáže. Z důvodu častého průjezdu motorových vozidel je také na místě vhodně zvolené a stabilní upevnění z důvodu nežádoucí vibrací. Jak už bylo u charakteristiky objektu uvedeno, čerpací stanice se často nachází na osamocených místech. V takových případech je doporučováno vybavení kamerového systému o záložní zdroj napájení (UPS).

4.3 PRŮMYSLOVÝ OBJEKT – AREÁL PODNIKU

4.3.1 Charakteristika objektu

V případě areálu průmyslového podniku se jedná ve většině případů o rozsáhlejší objekt složený z několika dílčích částí – administrativních budov, vývojových oddělení, výrobních provozů, skladových prostor apod. propojených komunikačními trasami, jak pro fyzický (cesty, chodníky, koleje), tak pro vzdálený přístup (např. datová, telekomunikační síť). Celý tento prostor bývá zpravidla na hranicích pozemku zabezpečen prvky obvodové ochrany mechanických zábranných systémů – ploty, zdmi atd., přičemž vstup/vjezd (výstup/výjezd) do prostoru je umožněn pouze na striktně určených místech (brány, vstupy pro zaměstnance apod.) z důvodu kontroly.

Na rozdíl od bankovních institucí a čerpacích stanic, nejsou průmyslové objekty v takové míře volně přístupné veřejnost, resp. jsou kladeny vyšší nároky na přehled o tom, kdo do areálu nebo daných prostor firmy vstupuje/vjíždí a naopak. Kamerové systémy v průmyslu mohou plnit jednak funkci bezpečnostní, ale také mohou být využity přímo ve výrobě k monitorování jednotlivých fází, dodržování pracovních postupů, počítání výrobků, detekci zmetků, poskytnutí dálkové technické podpory apod. Návrhu kamerového systému by tedy v těchto případech měla předcházet důkladná analýza chodu podniku v pracovní době i mimo ni, včetně interních režimových opatření atd.

Obrázek 29 – Průmyslový areál Meopta, Přerov,

zdroj: www.meopta.cz

4.3.2 **Zabezpečovaná aktiva**

Výčet zabezpečovaných hodnot u větších průmyslových objektů zahrnuje zpravidla kromě materiálních hodnot i hodnoty nehmotné – tedy firemní „know-how“, interní informace a dokumenty atd. Ochraně obou uvedených typů aktiv je nutné věnovat zvýšenou pozornost, neboť při ztrátě většího rozsahu jakéhokoliv z nich je přímo ohrožena existence daného podniku. Chráněnými hodnotami v případě průmyslového objektu jsou tedy především:

- ochrana zaměstnanců,
- ochrana hmotného majetku podniku,
- ochrana nehmotného majetku podniku,
- ochrana životního prostředí (průmyslové havárie).

4.3.3 **Potencionální rizika a hrozby**

Potencionální hrozby v rámci průmyslového objektu se dají podle zdroje působení obecně rozlišit na vnější a vnitřní. Mezi vnější patří běžná trestná činnost a škodlivé působení člověka – zejména krádeže materiálu, výrobků, technického vybavení, citlivých informací (dokumentace, „know-how“), sabotování výroby, průmyslová špionáž atd. Kromě vnějších hrozeb není vhodné podceňovat také hrozby působící zevnitř průmyslového podniku, resp. vycházející přímo od zaměstnanců podniku. V krajních případech mohou být dopady vnitřního nepříznivého působení několikanásobně závažnější než působení vně

průmyslového objektu. Minimalizace tohoto typu rizika spořívá zejména v dodržování stanovených režimových opatření v rámci objektu, mimo jiné s využitím kamerového systému pro kontrolu dodržovaní daných zásad.

Jelikož řada průmyslových podniků využívá k výrobě poměrně nebezpečné (toxické, hořlavé, výbušné, radioaktivní atd.) látky a materiály, mohou se i tyto aktiva stát potencionálním zdrojem hrozby pro daný podnik. Jejich odcizení, zneužití, únik apod. mohou přímo ohrozit existenci výroby, vést ke vzniku závažných průmyslových havárií atd. Proto při návrhu kamerového systému je nutné tyto faktory vzít v úvahu, zejména z hlediska ochrany osob a životního prostředí. Z toho důvodu je vhodné přehledově monitorovat volná prostranství, komunikace atd., aby bylo v případě nutnosti možné využít kamerový systém ke koordinaci složek integrovaného záchranného systému (IZS) [30].

4.3.4 **Oblasti zájmu monitorování**

Stupeň identifikace	**Prostory**	**Třída prostředí**	**Objekt snímaní**[29]
Identifikace	kontrola vstupu/výstupu osob z areálu	I., II.	I
	monitorování výrobních pracovišť	II.	I, P, Č
	monitorování vývojových pracovišť	I., II.	I, P, Č
	monitorování administrativních prostorů	I., II.	I, P, IA
Rekognoskace	kontrola vjezdu/výjezdu vozidel z areálu	III., IV.	I, P, IA
Přehled	monitorování parkoviště pro návštěvy a zaměstnance	III., IV.	I, P, IA
	kontrola zaměstnanců	I., II.	I, Č
	monitorování skladovacích prostor a expedice	II., III.	P, IA
Detekce	perimetr, hranice pozemku	III., IV.	P, IA
	volná prostranství	IV.	P, IA

Tabulka 10 – Oblasti zájmu u modelového objektu – Průmyslový objekt – areál podniku, , zdroj: archiv autora

4.3.5 **Požadavky na kamerový systém**

Z charakteristického prostředí průmyslové výroby vyplývají specifické nároky na kamerový systém. Obecným požadavkem je vysoká odolnost a funkční spolehlivost jed-

[29] Uvedené objekty snímání nejsou závazné a mohou se dle dané aplikace lišit.

notlivých zařízení z důvodu značně nepříznivých podmínek, kterým jsou běžně vystaveny (prašné, vlhké, agresivní prostředí, prudké změny teplot). Proto je nutností dostatečné IP a IK krytí, vyhřívání, klimatizace a další speciální příslušenství. Díky přítomnosti energeticky náročných strojů, vysokonapěťového vedení a jiných rušivých elementů je také důležité, aby použitá zařízení, přenosové a další systémové prvky splňovali podmínky elektromagnetické kompatibility (EMC). V případě aplikací většího rozsahu je proto výhodné použití např. přenosu dat pomocí optických vláken (za použití převodníků LAN[30]/optika, optika/LAN). Kamerový systém musí zajistit nepřetržité monitorování oblastí zájmu bez ohledu na provozní (pracovní) dobu podniku, i v případě výpadku dodávky el. energie (záložní napájení). V závislosti na rozsahu střeženého objektu (tedy i kamerového systému) je nutné zvolit optimální způsob obsluhy. Současné systémy mohou být plně automatizované, přičemž lidský faktor je zachován pouze k řešení výjimečných a krizových situací (havárie, detekce pohybu ve střeženém prostoru apod.). U tohoto typu objektů je výhodné použití kamerového systému ke střežení perimetru. Může se jednat buď o součinnost se systémy PZTS (vizuální potvrzení poplachu → minimalizace planých poplachů) nebo o samostatné řešení perimetrické ochrany (využití IP termokamer) [24].

4.4 VEŘEJNÁ BUDOVA – STÁTNÍ INSTITUCE

4.4.1 Charakteristika objektu

Na první pohled by se mohlo zdát, že specifikace budovy státní instituce a její požadavky na kamerový systém budou takřka totožné s budovou banky. Zásadní rozdíl je však jednak v charakteru zabezpečovaných aktiv a s tím souvisejícími hrozbami. Budovy státních institucí (městské a krajské úřady, úřady katastrální, úřady práce, finanční úřady atd.) se obecně nacházejí ve větších městech z důvodu snadné přístupnosti co největšímu počtu lidí. Provozní doba (úřední hodiny) tohoto typu budov je jasně stanovená, přičemž zpravidla probíhá pouze v určité dny v týdnu a nepřesahuje dobu 10 hodin. Jelikož se jedná o majetek státu, jsou kladeny vysoké nároky na technické i fyzické zabezpečení dané budovy. V praxi bývá obdobně jako u bankovních budov použita kombinace několika typů poplachových zabezpečovacích systémů, mechanických zábranných systémů, režimových opatření, doplněných u vybraných institucí o fyzickou ostrahu objektu.

[30] Local Area Network

Obrázek 30 – Budova krajského úřadu, Zlín,

zdroj: archiv ©Mediafaxfoto.cz

4.4.2 Zabezpečovaná aktiva

Jak už bylo zmíněno, charakter zabezpečovaných aktiv u budovy státní instituce bude diametrálně odlišný od aktiv u předchozích modelových objektů. Kromě vybavení a budovy jako takové (vandalismus) je primárně nutné zajistit bezpečnost zejména citlivých dokumentů, informací, dokladů atd., jejichž případné zneužití by mohlo přinést instituci (tedy i státu) značnou újmu. Obecně lze tedy zabezpečované hodnoty popsat jako:

- ochranu utajovaných informací,
- ochranu majetku instituce,
- zajištění veřejného pořádku.

4.4.3 Potencionální rizika a hrozby

Bezprostřední nebezpečí újmy na zdraví osob (návštěvníků, zaměstnanců) a životním prostředí je u tohoto typu budovy zanedbatelné, veškeré potencionální hrozby tedy víceméně vychází pouze z charakteru zabezpečovaných aktiv. Největšími z nich jsou v případě státní instituce buď samotní zaměstnanci, nebo osoby z řad veřejnosti. Jelikož jsou budovy státní správy veřejně přístupné a zaměstnanci v řadě případů ani netuší, jestli pohybující se osoby v objektu pracují či nepracují, otvírá se tak potencionálnímu pachateli možnost předběžného vytipování slabých míst v zabezpečení a jejich následné využití ve svůj prospěch. Obdobně to platí i u samotných zaměstnanců, kteří tak mohou škodlivým

působením (korupce, snaha o vlastní obohacení) přispět k nežádoucímu úniku utajovaných informací, a v řadě případů tak ohrozit bezpečnost nejenom instituce, ale v krajních případech i celého státu.

4.4.4 Oblasti zájmu monitorování

V případě použití kamerového systému u tohoto typu budov jsou oblasti zájmu monitorování jednoznačně dané – jedná se zejména o prostory, kde dochází ke styku s utajovanými informacemi, kanceláře, jednací místnosti apod. Další oblastí zájmu je přehled o pohybu, popř. podezřelém chování jednotlivých osob v rámci celého objektu. Vhodné je také sledovat plášť a perimetr budovy (v rámci mezí legislativy) z důvodu ochrany proti poškozování majetku instituce (např. sprejování na fasádu budovy) [30].

Stupeň identifikace	Prostory	Třída prostředí	Objekt snímaní[31]
Identifikace	vyhrazené prostory pro zaměstnance	I.	I, P
	archivy, skladové prostory pro dokumenty	I.	I, P
	technické místnosti (serverovny, kotelny)	I., II.	I, P
Rekognoskace	chodby, schodiště, lobby	I., II.	I, P, IA
Přehled	perimetr a plášť budovy	III., IV.	I, P, IA
	příjezdové/odjezdové komunikace	III., IV.	I, P, IA

Obrázek 31 - Oblasti zájmu u modelového objektu – Státní (veřejná) instituce, , zdroj: archiv autora

4.4.5 Požadavky na kamerový systém

Co se týče požadavků na kamerový systém u státní instituce a podobných objektů, nejsou z technického hlediska nijak výjimečně nadstandardní. Nedochází zde ve většině případů k působení vnějších nepříznivých vlivů jako u průmyslových a podobných objektů (povětrnostní vlivy, EMI, vysoké teploty, prašné prostředí,…). Důraz je kladem především na systémové požadavky kamerového systému, jeho spolehlivý, bezpečný a stabilní pro-

[31] Uvedené objekty snímání nejsou závazné a mohou se dle dané aplikace lišit.

voz. Příkladem aplikace IP kamerového systému v objektu státní správy může být např. jeho propojení a spolupráce se systémem kontroly vstupu. V tomto případě jednotlivé kamery plní funkci ověřování totožnosti osoby, která se pokouší do zabezpečeného prostoru vstoupit. Spuštění záznamu a jeho přiřazení ke konkrétnímu pokusu o vstup, vyhlášení poplachu, upozornění obsluhy, uzamčení dveří apod. může probíhat na základě splnění předem nastavených podmínek. Jedná se mimo jiné o:

- pokus o průchod osoby bez oprávnění (časově nebo místně omezená identifikace),
- sabotáž čtecího zařízení,
- překročení počtu *n*-neúspěšných pokusů o vstup,
- násilné otevření dveří bez identifikace,
- detekce otevřených dveří,
- překročená doba otevření dveří.

Obsluha má tak možnost snadno a efektivně analyzovat pořízené záznamy ve vztahu k daným úspěšným, či neúspěšným pokusům o vstup do střeženého prostoru. Veškerá správa i několika kamerových systémů může probíhat současně z jediného centrálního řídícího pracoviště, což s sebou přináší značnou úsporu nákladů na technické vybavení a personální zajištění.

4.5 VEŘEJNÁ BUDOVA – NÁUPNÍ CENTRUM

4.5.1 Charakteristika objektu

Ačkoliv často nebývá příliš frekventovaný pohyb osob ve střeženém prostoru žádoucí, u některých aplikací se musí kamerový systém tomuto faktu přizpůsobit. Názorným příkladem mohou být nákupní a obchodní centra, kde je obecně požadováno, aby se v nich pohyboval co největší počet osob, tedy potencionálních zákazníků. Jejich umístění bývá záměrně situováno u hlavních silničních tahů a dálnic, popř. co nejblíže centru města. V současné době také vzniká řada multifunkčních komplexů, které kromě prodeje zboží poskytují celou řadu dalších služeb, jako např. multikina, restaurace, výstavní galerie, prostory pro kulturní akce, jarní výprodeje, likvidace zásob - to vše má záměrně nalákat davy lidí, což se následně positivně projevuje na zisku majitelů. S rostoucím počtem lidí však úměrně roste míra bezpečnostních rizik, proto je nasazení kamerových systémů u tohoto

typu objektů na místě. Pravidlem bývá také přítomnost fyzické ostrahy, zejména v rámci poskytování služeb soukromými bezpečnostními agenturami. Jelikož se jedná o stavby často nové nebo pár let staré, vybavené kvalitní infrastrukturou (datové a komunikační sítě, elektroinstalace,…), poskytují tyto budovy ideální podmínky pro nasazení systémů síťového videa.

Obrázek 32 – Nákupní galerie Vaňkovka, Brno,

zdroj: www.nakupni-centra.com

4.5.2 **Zabezpečovaná aktiva**

Jak je z charakteru objektu patrné, zabezpečovaná aktiva budou tvořit především zdraví a bezpečnost přítomných osob (zákazníci, prodejci, personál) a také zboží a další majetek obchodníků. V případě přítomnosti kanceláří a jiných administrativních prostor se okruh aktiv může dále rozšířit o citlivé informace. Mezi zabezpečovaná aktiva mohou patřit také zaparkovaná vozidla, za předpokladu, že je součástí nákupního centra velkokapacitní parkoviště.

4.5.3 **Potencionální rizika a hrozby**

Potencionální hrozby u nákupního centra mohou mít odlišnou míru dopadů. Mezi ty méně závažné patří zejména drobné krádeže zboží (elektronika, drogistické zboží, potraviny, oblečení atd.), ničení vybavení nákupního centra, okrádání zákazníků (kapsáři) a různé druhy podvodů (přelepování cenovek, otvírání obalů výrobků). Závažnějšími hrozbami mohou být např. činnosti organizovaných skupin pachatelů a krádeže většího rozsahu ve skladovacích prostorech. Jelikož se předpokládá přítomnost značného množství osob, mohou se mezi ty nejzávažnější hrozby zařadit různé druhy havárií (požár) a také možnost teroristického útoku (nastražení výbušniny, použití chemických a biologických zbraní).

4.5.4 Oblasti zájmu monitorování

Stupeň identifikace	Prostory	Třída prostředí	Objekt snímaní[32]
Identifikace	prodejny s atraktivním zbožím	I.	I, Č, IA
	vstupy do prostorů pro personál	II.	I, P
	kanceláře, administrativní prostory	I.	I, P
Rekognoskace	prodejny s méně atraktivním zbožím	I.	I, Č, IA
	vstupy do technických prostor	I., II.	I, P
Přehled	hlavní haly, chodby, lobby	I., II.	I, P, IA
	prostor pro zásobování, logistiku	III.	P, Č
	parkoviště	III., IV.	P, Č

Tabulka 11 - Oblasti zájmu u modelového objektu – veřejná budova – nákupní centrum, zdroj: archiv autora

4.5.5 Požadavky na kamerový systém

V obchodních centrech může kamerový systém plnit řadu funkcí, obecně se dají rozdělit na bezpečnostní a komerční aplikace. V případě bezpečnostních aplikací je účel jasný a odpovídá potencionálním hrozbám, tzn. možnost identifikace pachatele ze záznamu, včasné upozornění ostrahy na hrozící nebezpečí atd. Z důvodu poměrně dlouhé otvírací doby (př. 8:00 – 22:00) je nutné, aby byl provoz kamerového systému spolehlivý, a bylo tak zajištěno nepřetržité monitorování rizikových prostor. Toho lze docílit např. redundancí nejvíce vytěžovaných zařízení, zálohováním dat a napájení apod.

Co se týče komerčních aplikací, přední výrobci IP CCTV technologií nabízejí kompletní technické a softwarové řešení provozu prodejny. To umožňuje propojení a spolupráci kamerového systému s dalšími systémy (EAS[33], POS[34]), což vede ke zvýšení efektivity ochrany zboží a usnadňuje řešení případných incidentů. Lze tak např. asociovat video s řešením reklamace u pokladny nebo s detekcí odcizeného zboží u východu z prodejny a minimalizovat tak finanční ztráty. Příkladem další komerční aplikace je využití IP CCTV k analýze chování zákazníků z marketingového hlediska. Na základě pořízených záznamů je systém schopen určit atraktivnost jednotlivých výrobků pro zákazníky (jak se dlouho zdrželi rozhodováním, kolik bylo daných výrobků prodáno během časového intervalu atd.),

[32] Uvedené objekty snímání nejsou závazné a mohou se dle dané aplikace lišit.
[33] Electronic Article Surveillance
[34] Point of Sale

přiřazovat videozáznamy k datům POS a řadu dalších funkcí. Obchodníci jsou tak schopni efektivně a v reálném čase upravovat nabídku produktů na základě projeveného zájmu zákazníků.

ZÁVĚR

Z analýzy legislativních požadavků vyplývá, že problematika kamerových systémů není v současné ošetřena specifickým zákonem. Na jejich provoz je v určitých případech pohlíženo buď jako na zpracování osobních údajů (zákon 101/2000 Sb., o ochraně osobních údajů), nebo na plnění úkolů daných zákony (o policii ČR a obecní policii). Úřad pro ochranu osobních údajů, který je dle výše uvedeného zákona kontrolním orgánem, sice v minulosti vydal některá prohlášení a stanoviska z hlediska provozování kamerového systému a zpracování osobních údajů, to však současnou situaci příliš neřeší. Řada kamerových systémů tak postrádá opodstatněný smysl nasazení a jeho provoz je tedy v rozporu se zákonem. Této situaci přispívá také skutečnost, že zjištěné přečiny proti legislativě nejsou nijak přísně postihovány. Řešením by mohla být například novelizace stávajících zákonů, popř. vytvoření nového samostatného zákona o provozování kamerových systémů, které jasně stanoví práva a povinnosti zodpovědných osob. Co se týče současného stavu platných norem, které se zabývají CCTV, z větší části jejich obsah neodpovídá aktuálním trendům a používaným technologiím. Zatímco v praxi bývá hojně využíváno digitálních kamerových systémů, normy ČSN EN 50132-5 a ČSN EN 50132-7 řeší víceméně pouze analogové systémy. Této skutečnosti jsou si orgány pověřené normotvorbou a sdružení výrobců již delší dobu vědomy, a proto se v dohledné době očekává zavedení harmonizovaných revizí jednotlivých částí normy (-5 a -7). S jejich příchodem dojde k plnému respektování IP kamerových systémů, což pomůže zejména projektantům, montážním firmám i koncovým zákazníkům se lépe v dané problematice orientovat.

Z hlediska vývojových trendů v oblasti CCTV (změna na VSS) se dá v blízké budoucnosti očekávat zvyšování míry konvergence mezi kamerovými systémy a dalšími aplikacemi, které využívají datových TCP/IP a jiných digitálních sítí. Nasvědčuje tomu zejména zájem výrobců o co největší úroveň interoperability jednotlivých zařízení. V současné době již přední výrobci a větší společnosti v oblasti VSS nabízejí celou řadu nových služeb, které tyto uvedené vývojové trendy umožňují. Jedná se zejména o využití distribuované inteligence IP kamerových systémů, možností analýzy obrazových dat, jejich asociace s danými událostmi apod. Kamery tak již neslouží pouze k ochraně zdraví, majetku osob a jiných zájmů, ale bývají stále častěji využívány v komerčních aplikacích

(např. marketingové analýzy). S nárůstem počtu funkcí a míry prolínání jednotlivých systémů se úměrně zvyšují požadavky na odborné a komplexní znalosti projektanta nejenom v oblasti kamerových systémů, ale také počítačových sítí a dalších zainteresovaných systémů.

Co se týče technických parametrů a požadavků jednotlivých zařízení, je nutné, aby měl projektant povědomí o jejich významu z hlediska návrhu kamerového systému. Tzn. správně volit optimální zařízení pro dané aplikace na základě analýzy provozních podmínek, bezpečnostního posouzení objektu, zabezpečovaných hodnot, charakteru možného pachatele a jiných hrozeb. Z těchto uvedených faktorů mimo jiné vyplývají specifické požadavky u jednotlivých modelových objektů. Jejich charakter byl zvolen záměrně, aby byla popsána co nejširší oblast využití kamerových systémů, nejenom v bezpečnostních aplikacích.

Přínosem práce je tedy specifikace technických parametrů součástí kamerového systému jako jednoho z kritérií návrhu VSS a následné přiřazení k modelovým objektům a uvedením příkladů nasazení kamerového systému v praxi.

ZÁVĚR V ANGLIČTINĚ

An analysis of legislative requirements shows that the issue of camera systems is not currently regulated by a specific law. Their operation is seen in certain cases, either the processing of personal data (Act 101/2000 Coll. On personal data protection), or the fulfillment of the relevant laws (the Police and municipal police). The Office for Personal Data Protection, which is the control body according to the law above, made some statements and opinions in the past in terms of operation of the camera system and processing of personal data, but this does not solve the current situation. Many camera systems lack sense of commitment and its operation is in a conflict with the law. This situation is supported by the fact that the detected offenses against legislation are not dealt severely. The solution could be for example, amendments to existing laws, or a creation of a new separate law on the operation of camera systems, which would clearly define the rights and obligations of the responsible person. Regarding the current status of the applicable standards that deal with camera systems, the greater part of their contents does not match current trends and technologies that are used. While in the practice is widely used digital camera systems, standards ČSN EN 50132-5 and ČSN EN 50132-7 regulate only analog systems. This fact has been awared by the bodies responsible for standardization and producer associations for a long time therefore the introduction of harmonized standards revisions of individual parts (-5 and -7) is expected in the future. With their arrival the IP videocameras will be fully respected which would help especially designers, and installers even end users to better understand this issue.

From the point of view of new trends in CCTV (change in VSS) can be expected in the near future, increasing rate of convergence between the camera systems and other applications that use data TCP / IP and other digital networks. The indications can be seen particularly in the interest of manufacturers to maximize the level of interoperation of single devices. In the present the leading manufacturers and larger companies in the VSS field offer a range of new services provided by these new developments. In particular, the use of distributed intelligence systems, IP cameras, image data analysis options, their association with events, etc. The video cameras haven´t protect only the health, property and other interests, but they are increasingly used in commercial applications (eg. marketing analysis). With the increase in the number of functions and the degree of overlapping of individ-

ual systems, also the requirements for professional and comprehensive knowledge increase not only on the designer of CCTV systems, but the computer networks and other relevant systems as well.

As to the technical characteristics and requirements of individual devices, it is necessary to have a designer awareness of their importance to design a camera system. It means correctly select the optimal device for the application based on an analysis of operating conditions, safety assessment of the building, secured values, the nature of possible offenders and other threats. The specific requirements of individual model objects can be seen from these factors listed above. Their character was deliberately chosen to be described as the broadest range of applications of CCTV systems, not only in security applications. The benefit of such work is part of the specification of technical parameters of the camera system as one of the VSS design criteria and the subsequent assignment to model objects and examples of specifying deployment of CCTV in practice.

SEZNAM POUŽITÉ LITERATURY

[1] Česká republika. *Listina základních práv a svobod*. In: č. 2/1993 Sb. 1993. Dostupné z WWW: http://www.psp.cz/docs/laws/listina.html

[2] Česká republika. *Zákon o ochraně osobních údajů*. In: č. 101/2000 Sb. 2000. Dostupné z WWW: http://www.uoou.cz/uoou.aspx?menu=4&submenu=5&loc=20

[3] Česká republika. *Stanovisko ÚOOÚ č. 1/2006 - Provozování kamerového systému z hlediska zákona o ochraně osobních údajů*. In: č. 1/2006. 2006. Dostupné z WWW: http://www.uoou.cz/files/stanovisko_2006_1.pdf

[4] Česká republika. *Občanský zákoník*. In: č. 40/1964 Sb. 1964. Dostupné z WWW: http://www.sbirkazakonu.info/obcansky-zakonik/

[5] Česká republika. *Zákon o Policii České republiky*. In: 273/2008 Sb. 2008. Dostupné z WWW: http://www.policie.cz/soubor/galerie-soubory-273-2008-sb-o-policii-ceske-republiky-pdf.aspx

[6] Česká republika. *Zákon o obecní policii*. In: 553/1991 Sb. 1991. Dostupné z WWW: http://www.straznici.com/zakon-o-obecni-policii/

[7] RANDA, Michal. *Správa kamerových systémů a zákonem daná informační povinnost*. Security magazín. roč. 2008, č. 05.

[8] MIKULA, Tomáš. *Současný stav standardizace CCTV*. Security magazín. 2010, č. 05.

[9] ČSN EN 50132-1. *Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích*: *Část 1: Systémové požadavky*. 2010

[10] ČSN EN 50132-5. *Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích*: *Část 5: Přenos videosignálu. 2002.*

[11] MIKULA, Tomáš. *Nové normy z oblasti kamerových systémů a „IP CCTV“*. Konference Bezpečnostní systémy. 30. 08. 2010. [prezentace].

[12] ČSN EN 50132-7. *Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích*: *Část 7: Pokyny pro aplikaci*. 2007.

[13] MIKULA, Tomáš a Michal RANDA. *Legislativa a normy v IP CCTV*. Konference MODnet: CCTV a průmyslové sítě. 2011. [prezentace].

[14] URBAN, Aleš. AGA. *AGA 004 - Sbírka zásad CCTV*. edice 1. 2007. [online] Dostupné z WWW: http://www.komora.cz/Files/AGA/Code%20of%20Practise.pdf

[15] URBAN, Aleš et al. AGA. *AGA 005 - Kamery, kamerové systémy a ochrana osobních údajů*. 2007.

[16] CI. *Aplikační směrnice ČAP P132-7*: *Poplachové systémy, CCTV sledovací systémy* [online]. 16. 12. 2003. Dostupné z WWW: http://www.cap.cz/FileFromWSS.ashx?file=http://capsrv02/DOKUMENTY_01%2fTECHSMER_CAP_P132_7.pdf

[17] LOVEČEK, Tomáš a Peter NAGY, *Bezpečnostné kamerové systémy*, 2008, EDIS, ISBN 978-80-8070-893-1

[18] RANDA, Michal, Jaromír VOMÁČKA, Tomáš MIKULA a Zdeněk VIENER. ORSEC. *IP CCTV Guideline - Průvodce návrhem síťového videa*. Calamarus, s.r.o., 2011.

[19] CAPUTO, Tony C. *Digital video surveillance and security*. Boston: Butterworth-Heinemann/Elsevier, 2010, xvii, 333 p. ISBN 18-561-7747-5.

[20] Standardy komprese videa. *Netcam.cz* [online]. [cit. 2012-05-08]. Dostupné z WWW: http://www.netcam.cz/encyklopedie-ip-zabezpeceni/standardy-komprese-videa.php

[21] VEINER, Zdeněk. *Standard H.264 pro kompresi videa.* Security magazín. roč. 2010, č. 05.

[22] Noční přisvícení bezpečnostních kamer. *ELNIKA plus s.r.o.* [online]. [cit. 2012-05-06]. Dostupné z WWW: http://www.elnika.cz/elnika.php?p=cze/cctv-kucharka-5

[23] ŠPONDR, Marek. *Laboratorní úloha dohledového kamerového systému*: *Laboratory task of the surveillance camera system.* Brno: VUT, Fakulta elektrotechniky a komunikačních technologií, 2008. Dostupné z WWW: http://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=9200

[24] *Axis thermal network cameras*. AXIS COMMUNICATIONS. [online]. [cit. 2012-04-15]. Dostupné z WWW: http://www.axis.com/products/video/camera/thermal/index.htm

[25] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I.* 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7.

[26] CCTV kalkulátor. KAŠPAR, Martin a Pavla POZDÍLKOVÁ. [online]. 2012. vyd. [cit. 2012-05-03]. Dostupné z WWW: http://cctvkalkulator.infoalarm.cz

[27] ŘÍČNÝ, Václav. *Videotechnika*: *přednášky*. vyd. 4., uprav. Brno: VUT FEKT, ústav radioelektroniky, 2006. 135 s. ISBN 80-214-3225-X.

[28] ŠELEMBERK, Filip. *IP kamerové systémy – současné trendy.* Security magazín. roč. 2010, č. 05. str. 19-21.

[29] KŘEČEK, Stanislav. *Ochrana majetku systémy průmyslové televize*. Vyd. 1. Praha: Grada, 1997, 183 s. ISBN 80-716-9402-9.

[30] ŠEVČÍK, Jiří. *Bezpečnostní posouzení objektu*. 2011. Diplomová práce. UTB ve Zlíně. Vedoucí práce Ing. Jan Valouch, Ph.D.

[31] HAYNES, Matt. *Get more from access control solutions*. SIEMENS BUILDING TECHNOLOGIES. [online]. [cit. 2012-04-23]. Dostupné z WWW: http://www.sourcesecurity.com/news/articles/co-1546-ga-co-268-ga.2971.html

[32] technické materiály firem AXIS, PELCO, Bosch, Brickcom

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CCTV	Closed-circuit television, uzavřený televizní okruh
IP	Internet protocol, datový protokol pro přenos dat přes paketové sítě
ČSN	Česká technická norma
ÚOOÚ	Úřad pro ochranu osobních údajů
PSIA	Physical Security Interoperability Alliance, sdružení výrobců
ONVIF	Open Network Video Interface Forum, sdružení výrobců
SOAP	Simple Object Acces Protokol, protokol pro výměnu zpráv přes síť (XML)
REST	Representational State Transfer, softwarová architektura
CENELEC	European Comittee for Electrotechnical Standardization
PZTS	Poplachové zabezpečovací a tísňové systémy
EMC	Electromagnetic compatibility, elektromagnetická kompatibilita
UPnP	Universal Plug and Play, síťový protokol
HD	High Definition, vysoké rozlišení
LPR	Licence Plate Recognition, rozeznávání státních poznávacích značek
QoS	Quality of Service, „kvalita služeb“, speciální požadavky na přenos dat
AGA	Asociace Gremium Alarm
ČAP	Česká asociace pojišťoven
CEA	Comité Européen des Assurances, Evropská asociace pojišťoven
VMD	Video Motion Detection, detekce pohybu kamerou
RVRC	Remote Video Response Centre, Vzdálene dohledové centrum
ICT	Information and communication technologies, informační a komunikační technologie
px	Pixel, jednotka rozlišovací schopnosti optického snímače
FPS	Frames Per Second, počet snímků za sekundu
JPEG	Joint Photographic Experts Group, standard komprese obrazu

M-JEPG	Motion JPEG, standard komprese videa
MPEG-4	Motion Picture Experts Group, standard pro kompresi videa a zvuku
PoE	Power over Ethernet, standard napájení přes datovou síť
lux	Jednotka intenzity osvětlení
LED	Light-Emitting Diode, polovodičová součástka vyzařující světlo
PIR	Passive Infrared, pasivní infračervený detektor
IR	Infrared, označení infračerveného spektra
SW	Software, programové vybavení
C/CS	Standard uchycení objektivu ke kameře
IP	Ingress Protection, stupeň krytí proti vniknutí kapalin a cizího tělesa
TCP/IP	Transmission Control Protocol/Internet protokol, sada komunikačních protokolů
EMI	Elektromagnetická interference, rušení
UTP	Unshielded Twisted Pair, nestíněná kroucená dvojlinka
STP	Shielded Twisted Pair, stíněná kroucená dvojlinka
FO	Fiber Optic, přenos pomocí optických vláken
UPS	Uninterruptible power supply, záložní zdroj napájení
LAN	Local Area Network, lokální datová síť
VSS	Video Surveillance Systém, video monitorovací systém
SD	Secure Digital, standard paměťových karet
VSaaS	Video Surveillance as a Service, kamerový dohled jako služba
MZS	Mechanické zábranné systémy
PTS	Poplachový tísňový systém
PZS	Poplachový zabezpečovací systém
ACS	Systém kontroly vstupu
IT	Informační technlogie

IZS	Integrovaný záchranný systém
EAS	Electronic Article Surveillance, způsob ochrany zboží
POS	Point of Service, pokladní systémy

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: POŽADAVKY DLE ČSN EN 50132-1 (STUPEŇ ZABEZPEČENÍ)

POŽADAVKY	STUPEŇ ZABEZPEČENÍ			
	1	2	3	4
Ukládání				
Systém CCTV musí být schopen:				
zálohování dat			X	X
uchovat v případě selhání paměti nebo automaticky přepnout z jednoho paměťového média na jiné v případě jeho selhání				X
reagovat na aktivační impuls s maximální prodlevou		1 s	500 ms	250 ms
reprodukovat obraz z paměti s maximální prodlevou po incidentu nebo během aktuálního záznamu s časovým odstupem			2 s	1 s
Archivace a zálohování				
archivace musí nabídnout:				
autentifikaci každého jednotlivého obrazu a obrazové sekvence				X
automaticky plánované zálohování poplachových obrazových dat				X
zálohování poplachových obrazových dat na manuální vyžádání			X	X
ověření úspěšného zálohování obrazů			X	X
Systémové protokoly				
Systém musí zaznamenat spolu s časovým údajem, událost, zdroj:				
poplach		X	X	X
narušení ochrany před neoprávněnou manipulací			X	X
ztráta videosignálu a jeho obnovení			X	X
výpadek napájení		X	X	X
poruchy základních funkcí a obnovení po poruše			X	X
zprávy o poruchách zobrazené uživateli				X
systémový reset, zapnutí, vypnutí		X	X	X
diagnostické akce (prověření stavu systému)				X
export, tisk/kopírování včetně identifikace zdroje obrazu, časového rozsahu			X	X
přihlášení a odhlášení uživatele od/do systému na pracovní stanici, úspěšná a odmítnutá přihlášení do systému (místně/vzdáleně) včetně důvodů odmítnutí (špatné heslo, neznámý uživatel, překročený účet)			X	X
změny v autorizačních kódech			X	X
řízení funkcí kamer				X
vyhledávání a přehrávání obrazů			X	X
manuální změny záznamových parametrů			X	X
potvrzení poplachu/obnovení po poplachu			X	X
změny konfigurace systému			X	X
datum a čas nastavení a změny času			X	X

POŽADAVKY	STUPEŇ ZABEZPEČENÍ			
	1	2	3	4
Monitorování propojení				
Systém musí:				
kontinuálně ověřovat správnost propojení v pravidelných intervalech o maximální délce			30 s	10 s
zkusit obnovit spojení s následujícím počtem pokusů před oznámením			5	2
oznámit operátorovi poruchu spojení nejpozději po			180 s	30 s
Detekce sabotáže				
Systém musí detekovat:				
narušení zařízení (např. otevření nebo odpojení) definovaná v OR			X	X
ztrátu videosignálu		X	X	X
změnu pozice (nasměrování) snímacího zařízení (kamerové sestavy)			X	X
úmyslné zatemnění nebo zaclonění zájmového prostoru snímacího zařízení			X	X
substituci jakýkoliv obrazových dat od zdrojů, propojení nebo zpracování				X
významné zmenšení kontrastu obrazu				X
Autorizace				
Požadavky na autorizační kód:				
počet možností logického klíče [v tis.]		> 10	> 100	> 1 000
počet možností fyzického klíče [v tis.]		> 3	> 15	> 50
Identifikace dat				
Systém CCTV musí jedinečným způsobem označit data o:				
umístění (např. jméno stanoviště)		X	X	X
zdroji – snímacím zařízení (např. číslo kamery)		X	X	X
datu a času	X	X	X	X
datu a času v GMT včetně kompenzace pro místní čas				X

PŘÍLOHA P II: POŽADAVKY DLE ČSN EN 50132-1 (PŘÍSTUPOVÉ ÚROVNĚ)

POŽADAVKY	PŘÍSTUPOVÉ ÚROVNĚ			
	1	2	3	4
Přístupové úrovně				
Funkce:				
konfigurace systému	NP	NP	P	P
změna jednotlivých autorizačních kódů	NP	P	P	P
přiřazování a mazání uživatelů	NP	NP	P	P
obnovení továrního nastavení	NP	NP	P	P
aktualizace systému	NP	NP	P	P
spuštění/vypnutí systému CCTV nebo prvků	NP	NP	P	P
Přístup k datům				
Funkce:				
prohlížení živých obrazů dat	P	P	P	P
prohlížení uložených obrazů a dat, pokud je záznam k dispozici	NP	P	P	P
prohlížení informací v archivu, pokud je archiv součástí systému CCTV	NP	P	P	P
tisk a ukládání obrazových dat	NP	P	P	P
export obrazů a dat	NP	NP	P	P
mazání obrazů a dat (jen s potvrzením)	NP	NP	P	P
Přístup k systémovým protokolům				
Funkce:				
prohlížení systémových protokolů	NP	P	P	P
export z protokolů	NP	NP	P	P
mazání protokolů	NP	NP	P	P
Přístup k nastavení systému				
Funkce:				
konfigurace a nastavení	NP	NP	P	P
obnovení po poruše systému	NP	P	P	P
obnovení po narušení sabotážní ochrany	NP	P	P	P

PŘÍLOHA P III: TABULKA PRO URČENÍ VELIKOSTI OHNISKA OBJEKTIVU V ZÁVISLOSTI NA VZDÁLENOSTI A ROZMĚRECH POZOROVANÉHO OBJEKTU (PRO 1/3“ SNÍMAČ)

objektiv f [mm]	rozměry záběru [m]	Odstup snímaného předmětu od kamery [m]																			
		1	1,5	2	3	4	5	6	7	8	9	10	15	20	25	30	40	50	80	100	200
2,8 (130°)	V	1,30	1,90	2,50	3,80	5,10	6,40	7,50	8,80	10,40	11,20	12,90	19,30	25,70	21,10	38,60	51,40	64,30	103,00	128,60	254,00
	Š	1,70	2,50	3,30	5,10	6,80	8,60	10,40	12,00	13,60	15,20	17,10	25,70	34,40	42,90	51,40	68,60	85,70	137,00	171,40	339,00
3,5 (92°)	V	1,00	1,60	2,00	3,10	4,10	5,10	6,10	7,10	8,40	9,10	10,30	15,40	20,60	25,70	30,90	41,10	51,40	82,30	103,00	206,00
	Š	1,40	2,00	2,70	4,20	5,60	6,90	8,50	9,80	11,00	12,40	13,70	20,60	27,40	34,30	41,10	54,90	68,60	109,70	137,00	275,00
4 (78°)	V	0,80	1,20	1,60	2,40	3,20	3,80	4,70	5,50	6,50	7,00	8,00	12,00	16,00	20,00	24,00	32,00	38,50	63,50	78,50	159,00
	Š	1,00	1,60	2,10	3,20	4,30	5,50	6,50	7,50	8,50	9,50	10,50	16,00	21,00	26,50	32,00	42,50	53,00	85,00	106,00	212,00
6 (53°)	V	0,50	0,80	1,10	1,60	2,20	2,80	3,30	3,70	4,50	5,90	6,50	8,50	11,00	14,00	16,50	22,00	27,50	44,00	55,00	110,00
	Š	0,70	1,10	1,40	2,20	2,90	3,60	4,40	5,00	6,00	6,50	7,50	11,00	14,50	19,00	22,00	29,50	36,50	60,00	75,00	150,00
8 (40°)	V	0,40	0,60	0,80	1,20	1,60	2,00	2,40	2,80	3,20	3,50	3,90	6,00	8,00	10,00	12,00	16,00	20,00	32,00	39,50	79,50
	Š	0,50	0,80	1,50	1,60	2,10	2,60	3,20	3,70	4,20	4,70	5,50	8,00	10,50	13,00	16,00	21,00	26,00	47,00	53,00	106,00
12 (28°)	V	0,25	0,40	0,50	0,70	1,00	1,30	1,50	1,80	2,00	2,30	2,50	3,80	5,00	6,50	7,50	10,00	12,50	20,50	25,50	51,00
	Š	0,35	0,50	0,70	1,00	1,20	1,40	2,00	2,40	2,70	3,00	3,40	5,00	7,00	8,50	10,00	13,50	17,00	27,00	34,00	68,00
16 (20°)	V	0,15	0,30	0,40	0,60	0,80	1,00	1,20	1,40	1,60	1,80	2,00	3,00	4,00	5,00	6,00	8,00	10,00	16,00	20,00	40,00
	Š	0,20	0,40	0,50	0,80	1,00	1,30	1,60	1,80	2,10	2,40	2,60	4,00	5,50	6,50	8,00	10,50	13,00	21,00	27,00	53,00
25	V	0,10	0,20	0,25	0,40	0,50	0,70	0,80	0,90	1,00	1,20	1,30	1,90	2,50	3,50	3,80	5,00	6,50	10,00	12,50	25,50
	Š	0,15	0,25	0,35	0,50	0,70	0,90	1,00	1,20	1,40	1,50	1,70	2,50	3,40	4,30	5,00	7,00	8,50	13,50	17,00	34,00
50	V	x	x	0,15	0,20	0,25	0,30	0,40	0,45	0,50	0,60	0,65	1,00	1,30	1,60	1,90	2,50	3,20	5,00	6,60	12,50
	Š	x	x	0,20	0,25	0,35	0,40	0,50	0,60	0,70	0,75	0,85	1,30	1,70	2,10	2,50	3,40	4,30	7,00	8,50	17,00
100	V	x	x	x	x	x	0,15	0,20	0,20	0,25	0,30	0,30	0,50	0,65	0,80	0,95	1,25	1,60	2,50	3,20	6,50
	Š	x	x	x	x	x	0,20	0,25	0,30	0,35	0,40	0,40	0,65	0,85	1,00	1,25	1,70	2,10	3,40	4,30	8,50

PŘÍLOHA IV: POROVNÁNÍ TECHNICKÝCH PARAMETRŮ – „FIXED“ KAMERY

Technické parametry				
Výrobce	AXIS	AVTECH	AXIS	Brickcom
Model	P1346	AVN806	M1031-W	CB-502Ap
Provedení kamery	Fixed „bullet“	Fixed „bullet“	Fixed cube	Fixed cube
Obrazový snímač	CMOS 1/3“	CCD HR 1/4“	1/4“ CMOS	CMOS 1/2.5“
Optika	variofocus 3.5 – 10 mm/F1.6	fixfocus 3.8 mm/F1.5	fixed iris 4.4 mm/F2.0	4.05mm/F1.5
Zoom (optický/dig.)	-	-	-	-
Úhel záběru H~V	72° - 27° (H)	53.7° (H), 34.1° (V)	47° (H)	65.4° (H), 49.9° (V)
Uchycení objektivu	CS	-	-	CS
Režim Den/Noc	✓	✓	✓	-
Citlivost [lux]	0,5 (barevná) 0,08 (č/b)	0.1 (0 lux s IR)	1 (0 lux s LED)	0.8 lux
IRC/přísvit (dosah)	-	✓/✓ (10 m)	-	-
Komprese	H.264 MJPEG	H.264 MPEG-4 MJPEG	H.264 MPEG-4 MJPEG	H.264 MPEG-4 MJPEG
Maximální rozlišení	2 048 x 1 536	1 280 x 1 024 (1.3 Mpx)	640 x 480	2 592 x 1 944
Počet snímků za sekundu [fps]	20 (2 048 x 1 536) 30 (HDTV 1 080p) 30 (1 600 x 1 200)	30 (752 x 480) 25 (720 x 576)	30 (640 x 480)	30 (1 Mpx) 20 (3 Mpx) 11 (5 Mpx)
PTZ	-	-	-	-
Audio podpora	obousměrná, vestavěný mikrofon	obousměrná (vestavěný mikrofon + reproduktor)	obousměrná, vestavěný mikrofon a reproduktor	obousměrná
Poplachové I/O	1/1	✓	-	-
Inteligentní analýza	detekce pohybu detekce zvuku detekce sabotáže	detekce pohybu detekce zvuku	detekce pohybu detekce zvuku detekce sabotáže	detekce pohybu detekce zvuku
Napájení	PoE Class 2	PoE Class 2	PoE Class 2	PoE Class 2
IP krytí	IP 66	-	-	-
Antivandal provedení	-	-	-	-
Ostatní	WDR, podpora SD/SDHC, ONVIF	ONVIF, podpora iOS a Android	přisvětlovací dioda, vestavěný PIR detektor, wifi	ONVIF, PSIA, podpora SD/SDHC (až 32 GB)

PŘÍLOHA V: POROVNÁNÍ TECHNICKÝCH PARAMETRŮ – „FIXED DOME“ KAMERY

Technické Parametry				
Výrobce	AXIS	Brickcom	Panasonic	Bosch
Model	P3346	VD-130Ap	WV-NW502S	NDN-832
Provedení kamery	Fixed dome	Vandal dome	Mini dome	Dome
Obrazový snímač	CMOS 1/3“	CMOS 1/4“	CCD 1/3“	CMOS 1/2.7“
Optika	variofocus 3 – 9 mm/F1.2	auto iris, 3.3 – 12 mm/F1.6	variofocus 2.8 – 9 mm/F1.2 2.8 – 9 mm/F1.8	1.8 – 3 mm 3.8 – 13 mm 9 – 40 mm
Úhel záběru H~V	30° - 84° (H)	89.8°~23.9°	35.0°~26.2° (tele) 100.0°~73.4° (wide)	-
Uchycení objektivu	-	-	-	-
Režim Den/Noc	✓	✓	✓	✓
Citlivost [lux]	0.5 (barevná) 0.08 (č/b)	1.00 (0 s IR)	2.00 (barevná) 0.16 (č/b)	0.22 (barevná) 0.05 (č/b)
IRC/přísvit (dosah)	-/-	✓/✓ (15 m)	-/-	✓/-
Komprese	H.264 Motion JPEG	H.264 MPEG-4 Motion JPEG	H.264 MPEG-4 Motion JPEG	H.264 Motion JPEG
Maximální rozlišení				1 920 x 1 080
Počet snímků za sekundu [fps]	20 (2 048 x 1 536) 30 (1 080p) 30 (1 600 x 1 200)	20 (H.264) 20 (MPEG-4) 20 (MJPEG)	15 (H.264) 15 (MPEG-4) 30 (JPEG)	25/30 (1 080p) 25/30 (720p)
PTZ	-	-	-	-
Audio podpora	obousměrná, ve-stavěný mikrofon	obousměrná	vstup pro mikrofon	obousměrná/ jednosměrná
Poplachové I/O	1/1	-	3/2	2/1
Inteligentní analýza	detekce pohybu detekce zvuku detekce sabotáže	detekce pohybu detekce zvuku detekce sabotáže	detekce pohybu rozpoznání obličeje	detekce pohybu detekce zvuku detekce sabotáže
Napájení	PoE Class 2	High Power PoE	PoE Class 2	PoE
IP krytí	-	IP 67	IP 66	IP 66
Antivandal provedení	✓	✓ (IK 10)	✓	✓ (IK 10)
Ostatní	podpora mikro SD/SDHC, dig. PTZ,	podpora mikro SD/SDHC	-	podpora mikro SD/SDHC (až 2 TB)

PŘÍLOHA VI: POROVNÁNÍ TECHNICKÝCH PARAMETRŮ – „BOX“ KAMERY

Technické Parametry				
Výrobce	PELCO	Brickcom	AXIS	Panasonic
Model	Sarix® IXS0LW	GOB-100AP	M1114	WV-SP306
Provedení kamery	Box	Fixed „bullet“	Fixed box	Fixed box
Obrazový snímač	CMOS 1/3“	CMOS 1/4“	CMOS 1/4“	MOS 1/3“
Optika	variofocus auto iris, 3.3 – 12 mm/F1.4	variofocus auto iris, 3.3 – 12 mm/F1.4	variofocus, DC iris, 2.8 – 8 mm/F1.4	
Úhel záběru H~V	63.6°~17.9°	63.6°~17.9°	87° - 29° (H)	
Uchycení objektivu	CS	-	CS	
Režim Den/Noc	✓	✓	-	
Citlivost [lux]	0.005 (barevná) 0.0013 (č/b)	0.68 (0 s IR)	0.6	0.3 (barevné) 0.05 (č/b)
IRC/přísvit (dosah)	✓/-	✓/✓ (15 m)	-	
Komprese	H.264 MPEG-4 MJPEG	H.264 MPEG-4 MJPEG	H.264 MJPEG	H.264 MJPEG
Maximální rozlišení	800 x 600	1 280 x 800	1 280 x 800	1 280 x 960
Počet snímků za sekundu [fps]	30 (H.264) 30 (MPEG-4) 30 (MJPEG)	15 (H.264) 15 (MPEG-4) 30 (MJPEG)	30 (1 280 x 800) 30 (720p)	30 (1 280 x 960)
PTZ	-	-	-	-
Audio podpora	-	obousměrná	-	obousměrná
Poplachové I/O	✓	-	-	1/1
Inteligentní analýza	detekce pohybu detekce zvuku	detekce pohybu detekce zvuku detekce sabotáže	detekce pohybu detekce sabotáže	detekce pohybu detekce zvuku
Napájení	PoE Class 3	PoE Class 2	PoE Class 1	PoE Class 2
IP krytí	-	IP 67	IP 67	-
Antivandal provedení	-	-	✓	-
Ostatní	podpora mikro SD/SDHC	podpora mikro SD/SDHC, 3G přenos dat	digitální PTZ	podpora mikro SD/SDHC

PŘÍLOHA VII: POROVNÁNÍ TECHNICKÝCH PARAMETRŮ – „PTZ DOME“ KAMERY

Technické Parametry				
Výrobce	AXIS	PELCO	Brickom	Bosch
Model	Q6032	Spectra® IV	OSD-040/E	VG5-825
Provedení kamery	PTZ dome	PTZ dome	PTZ speed dome	PTZ dome
Obrazový snímač	CCD 1/4“	CCD 1/4“	CCD 1/4“	CMOS 1/1.28
Optika	AI, autofocus, 3.4 – 119 mm/F1.4	variofocus auto iris, 3.4 – 119 mm/F1.4	3.4 – 122.4 mm/F1.6 – 4.5	AI, 4.7 – 94 mm/F1.6 – F3.5
Zoom (optický/dig.)	35x/12x	35x/12x	35x/12x	20x/12
Úhel záběru H~V	1.7° - 55.8° (H)	63.6°~17.9°	2° - 61.2° (H)	2.9° – 55.4° (H)
Uchycení objektivu	-	-	-	-
Režim Den/Noc	✓	✓	✓	✓
Citlivost [lux]	0,5 (barevná) 0,008 (č/b)	0.55 (barevná) 0.00018 (č/b)	0.1 (barevná) 0.01 (č/b)	0.8 (berevná) 0.12 (č/b)
IRC/přísvit (dosah)	✓/-	✓/-	✓/-	-
Komprese	H.264 MJPEG	H.264 MPEG-4 MJPEG	H.264 MPEG-4 MJPEG	H.264 MPEG-4 MJPEG
Maximální rozlišení	752 x 480	1 024 x 768	752 x 480	1 920 x 1 080
Počet snímků za sekundu [fps]	30 (752 x 480) 25 (720 x 576)	25 (H.264) 30 (MPEG-4) 30 (MJPEG)	30 (752 x 480) 25 (720 x 576)	30 (1 920 x 1 080) 60 (1 280 x 720)
PTZ	P (360°) T (180°) 100 předvoleb	✓	P (360°) T (200°) 0.5 – 400°/s	P (360°) T (18°) 0.1 – 120°/s
Audio podpora	obousměrná	-	obousměrná	obousměrná
Poplachové I/O	4/4	✓	-	-
Inteligentní analýza	detekce pohybu detekce zvuku auto-tracking	detekce pohybu detekce zvuku autotracking	detekce pohybu detekce zvuku autotracking	detekce pohybu detekce zvuku autotracking
Napájení	PoE+	PoE Class 3	High Power PoE	High Power PoE
IP krytí	IP 66	-	IP 66	IP 66
Antivandal provedení	✓	✓	✓	✓
Ostatní	WDR, podpora SD/SDHC, stabilizátor obrazu, kontrola teploty	podpora mikro SD/SDHC, stabilizace obrazu	3D privátní maskování, WDR	-

PŘÍLOHA VIII: POROVNÁNÍ TECHNICKÝCH PARAMETRŮ – IP TERMO KAMERY

Technické Parametry				
Výrobce	AXIS	AXIS	Bosch	PELCO
Model	Q1910	Q1922-E	VOT-320	TI2500
Provedení kamery	Fixed box	Fixed box	Fixed box	Fixed „bullet“
Obrazový snímač	mikro bolometr	mikro bolometr	oxid vanadia	oxid vanadia
Optika	13 mm/F1.25	10 mm/F1.2 19 mm/F1.0 35 mm/F1.2 60 mm/F1.2	9 mm 13 mm 19 mm 60 mm	35 mm 50 mm
Úhel záběru H~V	17°	10 mm: 57° 19 mm: 32° 35 mm: 18° 60 mm: 10°	-	-
Citlivost [mK]	< 100	< 100	-	85
Detekční vzdálenost [m]	200 (osoby) 550 (vozidla)	320 – 1 800 (osoby) 990 – 5 500 (vezidla)	3 900	-
Komprese	H.264 MJPEG	H.264 MJPEG	H.264 JPEG MJPEG	H.264 MJPEG
Maximální rozlišení	160 x 128	640 x 480	320 x 240	320 x 240
Počet snímků za sekundu [fps]	8.3	8.3/30	8.3/30	8.3
Audio podpora	obousměrná, ve-stavěný mikrofon	obousměrná	-	-
Poplachové I/O	2/2	2/2	-	-
Inteligentní analýza	detekce pohybu detekce zvuku detekce sabotáže	detekce pohybu detekce zvuku detekce sabotáže	-	-
Napájení	PoE Class 3	PoE Class 3	-	
IP krytí	-	IP 66	IP 66	IP 66
Antivandal provedení	-	✓	-	-
Ostatní	podpora SD/SDHC	podpora SD/SDHC	podpora SD/SDHC	-