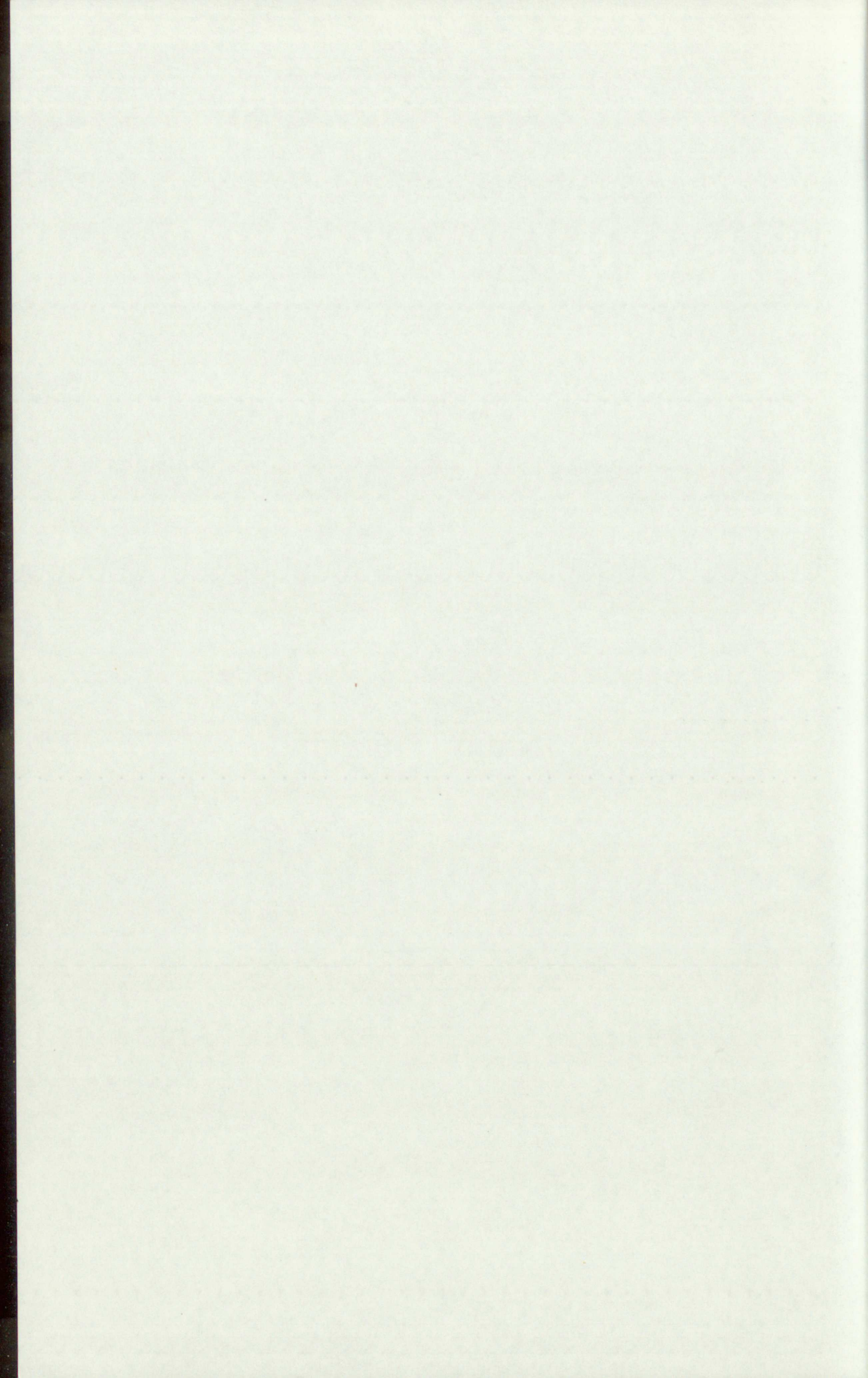


# PŘÍRUČKA ZABEZPEČOVACÍ TECHNIKY

Stanislav Křeček a kol.

- ✓ elektronické zabezpečovací systémy
- ✓ právní a regulativní aspekty oboru
- ✓ mechanické zábranné systémy
- ✓ montáž poplachových systémů
- ✓ elektrická požární signalizace
- ✓ návrh poplachových systémů
- ✓ systémy průmyslové televize
- ✓ IP - kamerové systémy
- ✓ další systémy ...





# **Příručka zabezpečovací techniky**

**Ing. Stanislav Křeček a kolektiv**

Ing. Stanislav Křeček a kolektiv

## **Příručka zabezpečovací techniky**

Názvy produktů, firem apod. použité v knize mohou být ochrannými známkami nebo registrovanými ochrannými známkami příslušných vlastníků.

© cricetus – Ing. Stanislav Křeček

ISBN 80-902938-2-4

## Předmluva

Dostáváte do rukou knihu, která navazuje na I. a II. Vydání publikace „Příručka zabezpečovací techniky“. Poprvé publikace vyšla v roce 2002 a její celý náklad byl během krátké doby vyprodán. Podobný osud stihlo i II. Vydání. Publikace se stala za dobu své distribuce standardem pro vzdělávání žáků na středních školách studujících specializovaný obor „Bezpečnostní systémy“. Vývoj technologií v tomto oboru si vynutil přepracování a doplnění nových informací. To je hlavním cílem tohoto III. vydání.

Pokrývá svým obsahem problematiku Elektronické zabezpečovací signalizace (EZS), Systémů průmyslové televize (CCTV), IP-kamerových systémů, Elektrické požární signalizace (EPS). V omezené míře se věnuje problematice Mechanických zábranných systémů (MZS).

Prioritně je určena jako učebnice pro 14 středních odborných škol zapojených do projektu výuky předmětu „Bezpečnostní systémy“ na středních odborných školách a učilištích vyučujících maturitní předmět „Mechanik elektronik“, kde je školám ponechán v 3 – 4 ročníku v osnovách prostor pro zařazení specializovaných předmětů. Příručka ctí doporučenou osnovu výuky tohoto předmětu. Svým záběrem však základní potřeby výuky na středních školách překračuje a může sloužit i ve školství vyšším. Vzhledem k náplni je však kniha vhodná i pro potřeby profesního vzdělávání pracovníků projekčních, montážních a servisních firem působících v oboru technického zabezpečení objektů.

Vychází z historického vývoje oboru a vysvětlení fyzikálních principů prvků jednotlivých systémů. Zahrnuje rovněž přehled platných předpisů a norem k oboru se vztahujících. Z praktického hlediska se zabývá činnostmi od koncepčního návrhu až po servis těchto systémů.

Autorský tým je složen z odborníků, kteří v oboru prakticky působí či působili, a pedagogů – zkušených autorů pod vedením **ing. Stanislava Křečka**. Uvedení autoři poskytli podklady pro redakční zpracování, či se sami na textech podíleli.

### **Jiří Bartáček - Střední odborná škola a Střední odborné učiliště, Dubno**

Vystudoval Střední průmyslovou školu spojovací techniky v Praze a doplňkové pedagogické studium. Dnes působí jako zástupce ředitele pro praktické vyučování na SOŠ a SOU Dubno. V oboru poplachových systémů působí cca 8 roky od doby zapojení školy do projektu výuky Poplachových systémů. Podílí se na organizaci odborných seminářů o bezpečnostních systémech od roku 1999 pro učitele a mistry odborného výcviku. Zpracovává podklady pro výuku především v oblastech spjatých s využitím informačních technologií Významně se podílí na projektu sdružení CSE, který v soutěži Grand Prix při příležitosti konání 11. ročníku mezinárodního veletrhu Pragoalarm/Pragosec 2002 a získal zvláštní cenu poroty. Organizuje soutěže pro žáky škol sdružení CSE (Jablotron - cup Lenia - cup a další). Převzal po odchodu ředitele ing. Jaroslava Husáka ze SOŠ a SOU z Ústí/Labem důchodu funkci předsedy rady sdružení škol do projektu výuky poplachových systémů zapojených.

### **Ing. Milan Holas - Jablotron s.r.o.**

Vystudoval Fakultu elektrotechnickou ČVUT, obor sdělovací technika. Celková doba praxe v oboru elektroniky je 25 let. Od r. 1990 se specializoval na poplachové systémy (AVRO Přišovice, Lites). Dnes působí jako vedoucí vývojového pracoviště firmy Jablotron. Z významných úspěchů v oboru lze jmenovat přípravu akreditace zkušební laboratoře LITES na poplachové systémy, předsednictví Technické normalizační komise TNK-124 při Českém normalizačním institutu. Je také zpracovatelem řady norem ze skupiny ČSN EN 5013++.

### **Ing. Jan Klügl – ASTOR - KOMPLEX s.r.o.**

Jeden z významných odborníků působící v oboru zabezpečovací techniky již od r. 1974. Stojí za ním řada výsledků z oblasti publikační (Výukové osnovy ochrany objektů SOŠ MV Pardubice 1992, příručka Montáž EZS 1993, Pravidla montáže EZS CZBS/AGA 1994) a přednáškové činnosti (Konference Bezpečnostní systémy peněžních ústavů 1991, Konference Ochrana kulturního dědictví 1992, Konference Energetika – série 1998, Konference NATO PfP/PWP Bezpečnost a ochrana utajovaných skutečností 2001, Školení ČEZ, ČS, AČR, PČR, Městské policie 1992 – 2001, Přednášky a příspěvky na setkáních a MV, CZBS-AGA, AMBO 1993 – 2000) a řada publikačních a překladatelských aktivit (3 publikace, desítky odborných textů článků a rešerší) v oboru Poplachových systémů. Kromě jiného je majitelem zřejmě nejrozsáhlejší sbírky historických exponátů zařízení zabezpečovací techniky v České republice. O jeho osobnosti snad vypovídá i to, že je uveden v publikaci o nejvýznamnějších Čechách „Who is Who in Czech Republic“.

### **Ing. Stanislav Křeček – OSVČ**

Vystudoval Fakultu elektrotechnickou ČVUT v Praze, obor radiotechnika, specializace audio- a videotechnika. Svou praxi započal v radiokomunikacích specifickou oblastí měření vysokofrekvenčních rušivých polí, poté prošel zkušenostmi z výroby elektronických součástek a zařízení, kde pracoval v oblasti zkušebnictví a poté jako vedoucí odboru řízení jakosti. Po roce 1991 začal působit v oblasti poplachových systémů. Svě zkušenosti sbíral v rámci realizační firmy jako vedoucí projekce a montáže. Dnes působí jako samostatný a nezávislý subjekt (OSVČ), bezpečnostní konzultant, autor odborných článků a publikací, člen Technické normalizační komise při Českém normalizačním institutu, zpracovatel řady ČSN EN pro oblast poplachových systémů. Je koordinátorem projektu výuky poplachových systémů na středních odborných školách a učilištích (CSE).

Jeho druhým oborem je management jakosti, environmentu a bezpečnosti informací, kde působí jako lektor, konzultant a auditor systémů řízení dle norem řady ISO 9001 a BS 7799. Dále je posuzovatelem Českého institutu pro akreditaci.

### **Ing. Jan Merhaut - Telenot elektronika s.r.o.**

V oboru poplachových systémů působí od roku 1993. Je zpracovatelem řady překladů zahraničních norem z oboru z německého i anglického jazyka. Je auditorem Certifikačního Institutu České asociace pojišťoven pro obor Pultů centralizované ochrany. Je členem Technické normalizační komise TNK 124 „Poplachové systémy a EPS“ při Českém normalizačním institutu. Je zástupcem ČR v technické komisi TC 79 při CENELEC. Je technickým tajemníkem Asociace Grémium alarm (AGA), předsedou Odborné komi-

se EZS při AGA, a působí jako zástupce AGA v evropské organizaci sdružující subjekty v oboru poplachových systémů EUROALARM. Je horlivým propagátorem vyššího standardu a kvality v oboru.

#### **Petr Sloup - Střední odborná škola a Střední odborné učiliště, Dubno**

Vystudoval Střední průmyslovou školu elektrotechnickou v Praze. Dnes působí jako mistr praktického vyučování na SOŠ a SOU Dubno. Od roku 1988 montuje EZS. Byl jeden z prvních, kteří za školách začali EZS učit. Od roku 1999 se podílí na přípravě školicích textů a na organizaci odborných seminářů pro učitele a mistry odborného výcviku v rámci projektu výuky Poplachových systémů. Zpracovává podklady pro výuku především v oblastech spjatých s praktickými zkušenostmi z montáže a s připojením systémů EZS na PCO. Významně se každoročně podílí na přípravě prezentace sdružení středních odborných škol CSE v rámci mezinárodních veletrhů Pragoalarm/Pragosec.

#### **d.t. Rostislav Srstka – Security technologies a. s.**

Vystudoval Střední průmyslovou školu elektrotechnickou v Brně. Od roku 1973 pracoval jako konstruktér a projektant elektrických zařízení nízkého napětí. V oblasti poplachových systémů působí od roku 1984. Dnes je vedoucím projekčního oddělení realizační firmy. Od roku 1994 je autorizovaným technikem v oboru technika prostředí staveb – specializace elektronická zařízení. Aktivně spolupracuje při přípravě a realizaci vzdělávacích aktivit CSE. Spolupracuje na zpracování normativních dokumentů v oblasti poplachových systémů.

#### **plk. Ing. Ladislav Toms – emeritní vrchní policejní rada ve výslužbě**

Vyučen přesným mechanikem, absolvoval Fakultu strojní ČVUT v Praze se specializací přesná mechanika a optika. Zámkovou technikou se profesionálně zabývá od roku 1965. Před odchodem do penze zastával funkci ředitele odboru Služby kriminální policie Policejního presidia ČR.

V současné době působí jako soudní znalec v oboru zámková a zabezpečovací technika. Publikuje v řadě odborných časopisů a přednáší na VOŠ Trivis Praha.





## **OBSAH:**

Kapitola 1	
Úvod do oboru zabezpečovací techniky .....	11
Kapitola 2	
Mechanické zábranné prostředky .....	37
Kapitola 3	
Elektronické zabezpečovací systémy (EZS) .....	127
Kapitola 4	
Elektrická požární signalizace (EPS) .....	125
Kapitola 5	
Systémy průmyslové televize (CCTV) .....	161
Kapitola 6	
IP-kamerové systémy .....	237
Kapitola 7	
Přepět'ové ochrany v elektronických systémech .....	291



## Poradenské služby

---

### Nabídka služeb

- **služby pro investory a provozovatele bezpečnostních elektronických systémů**

**v rámci přípravy investiční akce:**

- stanovení cíle projektu
- předběžný návrh specifikace
- analýza rizik objektu
- zadání projektu v souladu s Evropskými normami
- předběžný návrh provozního režimu
- posouzení návrhu systému

**v rámci výběrového řízení:**

- spolupráce při zpracování zadání
- vytipování okruhu možných dodavatelů
- zpracování kritérií hodnocení nabídek
- posouzení nabídek pro potřeby hodnocení
- konzultace technických aspektů smlouvy

**v rámci realizace:**

- příprava a vyhodnocení testů pro přijímací řízení

**v rámci provozu:**

- zpracování postupu pro pravidelné hodnocení funkce systému
- ověření funkčnosti stávajícího systému CCTV pomocí testovacího obrazce ROTAKIN popř. u bankovních systémů dle směrnice ORŮA uplatňované v SRN
- kvalifikační školení pracovníků údržby

- **služby pro dodavatele bezpečnostních elektronických systémů**

- otevřená i podniková školení pro nastupující i stávající pracovníky
- konzultace projektu systému s ohledem na ustanovení Evropských norem
- příprava a realizace přijímacích testů konkrétního systému CCTV dle metodiky Evropských norem

- **služby v oboru managementu jakosti**

- analýza stavu systému řízení firmy podle ISO 9001: 2000, VDA -6.1, VDA - 6.2, ISO TS 16949
- příprava k certifikaci dle ČSN ISO 9001:2000
- návrh harmonogramu bodování systému jakosti
- spolupráce při dokumentování systému jakosti
- školení vrcholového i středního managementu
- provedení rozběhového interního auditu
- specializovaná odborná školení na témata z managementu jakosti

---

blíže informace: tel.: 383 423 202, 603 864 068, e-mail: cricetus@blatna.cz

# Úvod do oboru poplachových systémů

Milan Holas, Jan Klügl, Stanislav Křeček

## OBSAH:

<b>1 Úvod</b> .....	13
1.1 Historie .....	13
1.2 Poplachové systémy v ČR po roce 1989.....	16
1.3 Poplachové systémy – my a svět .....	17
<b>2 Předpisová základna v oboru Poplachových systémů</b> .....	18
2.1 Evropská unie .....	18
2.2 Česká republika .....	18
<b>3 Oborově specifické normy</b> .....	19
3.1 Technická komise CENELEC/TC79 .....	19
3.2 Technická komise CEN/TC 72.....	20
3.3 Normalizační zabezpečení v ČR .....	20
<b>4 Odborná způsobilost</b> .....	31
4.1 Poplachové systémy (EZS, CCTV, ACS..) .....	31
4.2 Elektrická požární signalizace .....	34



# 1 Úvod

## 1.1 Historie

Potřeba ochrany před nebezpečím a s tím spojená potřeba signalizovat nebezpečí, když je bezpečnost ohrožena, provází lidstvo od věků. Hrozba mohla vždy přicházet právě tak od přírodních sil, jako je potopa nebo oheň, jako od nepřátel.

Jak se civilizace vyvíjela, vyvíjely se i systémy vyhlašování poplachu. Ale ať už využívaly křiku, bubnování, trubení či zvonění, vždy se jednalo o výhradně lidskou činnost – snad s výjimkou hlídacích psů.

Průmyslová revoluce, nabírající tempo na přelomu 18. a 19. století, vehnala masy lidí do měst a předhodila je nastupujícímu věku technologie. S koncentrací spoust lidí na malých plochách se koncentrovala i nebezpečí a nejhorším z nich byly požáry. Velká města tyto problémy řešila postupně zdokonalovanými sítěmi hlásek a požárních stanic, které si předávaly signály posly, zvony, trubením nebo světelnými záblesky.

Zásadní přelom v přenosu informací na dálku znamenal vynález telegrafu v roce 1835 a jeho první reálná aplikace v roce 1844 (linka Washington – Balfimore). Poprvé byl v systémech pro signalizaci nebezpečí použit v roce 1847 – hlavní inženýr města New York Cornelius Anderson propojil požární hlásky telegrafem s centrálním stanovištěm, které bylo dále propojeno s jednotlivými požárními stanicemi. Došlo tak k nebývalému zkrácení doby potřebné k přenosu poplachového signálu od místa ohrožení k „záškové skupině“ – tedy na nejbližší požární stanici.

Dalším krokem k prvním „elektrickým zabezpečovacím signalizacím“ tak, jak je chápeme dnes, bylo technické vylepšení systému centralizace hlášení pomocí tzv. „volací skřínky“ – dnes bychom řekli veřejného hlásiče. Při zatažení za páku hlásiče se roztočilo vroubkované kolo a prostřednictvím elektrického kontaktu vyslalo sérii teček a čárek, ve kterých byl obsažen jeho individuální kód. Na centrálním pultu pak primitivní zapisovač zaznamenal zmíněnou sérii, a vytvořil tak záznam o poplachu. Systém byl schválen v Bostonu (stát Massachusetts) v roce 1851 a v roce 1854 ve městě fungovalo již 42 takových hlásičů. Zajímavé je, že v podstatě stejný systém byl vybudován v Hamburku koncem 19. století a vydržel ve službě až do roku 1976.

První známý elektrický zabezpečovací systém, podstatně vylepšující předchozí ryze mechanickou kombinaci nástražného drátu a pastičky na myši, si nechal patentovat v roce 1853 pan Augustus Pope ze Sommerville (opět stát Massachusetts). Používal kombinaci kontaktů instalovaných na dveřích a oknech s baterií a zvonkem. Svůj patent v roce 1857 prodal Edwinovi T. Holmesovi, novoanglickému obchodníkovi s galanterií a šicími potřebami a výrobcí krinolín.

Edwin T. Holmes to jako všichni průkopníci to neměl lehké – i když už se začínala vyrábět elektrická zařízení, v té době ještě neexistovali dodavatelé elektrických drátů a příslušenství. Naštěstí pár kroků od jeho bostonského obchodu sídlil první elektrikářský obchod v zemi – Hinds & Williams. Holmes se spřátelil s Williamsem, který pro něho začal vyrábět zvonky a kontakty. Musel také začít vyrábět izolované dráty, přičemž využil své zkušenosti z výroby krinolín, vymyslel mnoho dalších základních elektrických součástí, které si patentoval a později se staly základem telefonních systémů. Elektrická zabezpečovací signalizace byla na světě – dvacet let před telefonem a čtvrt století před žárovkou.

Nebylo to snadné – nikdo nechtěl v té době věřit, že při otevření okna v přízemí může začít zvonit zvonek v patře. Holmes se tedy přesunul do New Yorku, kde byl potenciální trh přece jen perspektivnější než v tehdejší Bostonu, vyrobil model domu s fungujícím poplašným zařízením a objížděl nebohatší obyvatele Manhattanu. Uspěl a za vydělané peníze vylepšoval svůj systém – v krátké době byl schopen pomocí barevných klapkek vytvořit „adresný“ systém indikující stav každého zabezpečeného okna nebo dveří, přidáním hodin systém „programovat“ na zapínání a vypínání ve stanovenou dobu a později i na ovládání domovního osvětlení.

Holmes samozřejmě využil již známé myšlenky centralizovaných pultů a v roce 1858 uvedl do provozu první centrály elektrické ochrany v Bostonu a v New Yorku, které brzy sloužily jako působivý seznam prominentních zákazníků – Bowery Bank, Montreal Bank, Equitable Life, Phelps Dodge & Comp., John Jacob Astor, Tiffany a spousta dalších. Roku 1872 Holmes vyvinul „elektrický sekretář“ pro ukládání klenotů – úložní objekt se stěnami propletenými průběžnou vodivou fólií a s dveřmi opatřenými kontakty, připojený na centrální stanoviště se 24hodinovou službou schopnou kdykoli zakročít.

Když Graham Bell v roce 1873 přemýšlel, kde vyzkoušet svoji myšlenku přenosu lidského hlasu na velkou vzdálenost, přišel za Edwinem Holmesem, na stávající síti objektových zabezpečovacích linek si ověřil její reálnost a v roce 1876 ohlásil vynález telefonu. Demonstrace byly tak úspěšné, že E. T. Holmes byl požádán o vybudování první komerční telefonní ústředny, kterou dokončil v New Yorku v roce 1877 Holmes Central Station se stala první telefonní ústřednou a současně prvním účastníkem, Holmes prvním prezidentem Bell Telephone Company a jedním z prvních ředitelů Bell Telephone Association, předchůdcem známé ATT (American Telephone and Telegraph Comp.)

Po dlouhá desítiletí byla elektrická zabezpečovací signalizace ryze kontaktní záležitostí. Používaly se různé druhy kontaktů spínacích i rozpínacích, často ve spojení s nástražným drátem, a od počátku destruktivní čidla, to znamená pevně zabudované vodiče, které byly při pokusu o proražení překážky přerušeny – to vše jsou dodnes používané principy, i když přece jen v sofistikovanější podobě). Zřejmě teprve začátkem 20. století se objevují elektromechanická čidla založená na principu setrvačnosti, případně kyvadla. Jsou to speciální kyvadlová čidla pro ochranu trezorových místností, nejrůznější typy vibračních kontaktů, používaných až do začátku 80. let, a inerciální senzory, používané občas i v současných zařízeních pro ochranu vozidel (reagují na jejich rozhoupání).

Zabezpečovací ústředny byly až do 50. let 20. století zásadně reléovou záležitostí. S objevem polarizovaného relé, které umožnilo používání vyvážených smyček, podstatně narostla odolnost zabezpečovacích systémů. Pro signalizaci se používaly převážně zvonky, což přetrvalo dodnes zejména v anglosaských zemích.

Teprve rozvoj elektroniky za druhé světové války a po ní, zejména pak průmyslová výroba tranzistorů, následná miniaturizace elektronických zařízení a posléze boom nových technologií vyvinutých pro potřeby kosmického průzkumu a v souvislosti s vietnamskou válkou umožnily vznik nových druhů čidel, jejich elektronizaci a posléze komputerizaci. Právě výpočetní technika dosáhla v poslední době úrovně dovolující technickými prostředky nahrazovat některé činnosti, které dosud bylo možné zajišťovat výlučně lid-

skou silou (tedy vnímáním a myšlením), a po téměř třicetileté přestávce se opět objevují v zabezpečovací technice skutečně nové prostředky a z nich vyplývající možnosti.

Postupné vnitrospolečenské změny v demokratických zemích měly za následek decentralizaci bezpečnostních činností, což znamenalo další rozvoj pultů centralizované ochrany a s tím souvisejících bezpečnostních služeb, a na rozdíl od systémů požární ochrany, vázaných na požární sbory, výraznou komercializaci této oblasti.

V padesátých letech 20. století se objevují elektronická čidla. Jsou to zejména tzv. trezorové kontakty – akustické snímače připevňované na chráněný objekt (stěnu trezorové skříně nebo komory) a vyhodnocující hluky šířící se materiálem. Vzhledem k jednoduché pásmové filtraci snímaných akustických frekvencí byly dost náchylné k planým signalizacím způsobovaným přenosem chvění z jiných konstrukčních struktur (topení, vodovody, armatury atp.). Dále se jednalo o kapacitní čidla vyhodnocující kapacitu chráněného objektu proti zemi. Tato zařízení již byla značně spolehlivá a vysoce účinná, vyžadovala však (a dodnes vyžadují) velmi pečlivou přípravu a montáž. Konečně šlo o první aktivní prostorová čidla na principu vyhodnocování a principu při šíření ultrazvuku v uzavřeném prostoru. Jejich klíčovým problémem byla stabilizace vysílaného kmitočtu a opět pečlivá příprava a montáž. V této době začínají také být postupně vytlačovány mechanické kontakty magnetickými snímači s kontaktem jazýčkovým.

V šedesátých letech se zvyšující se úrovní polovodičových součástek mohla přijít VKV prostorová čidla. Fungují na principu pokrytí chráněného prostoru nemodulovaným signálem o frekvenci řádu stovek MHz a vyhodnocování změn elektromagnetického pole. Ve své době doznaly značného rozšíření. Vyráběly se v různých provedeních, jako jednoválcové i víceanténové, s tyčovými i Yagiho anténami. Jejich hlavní výhodou byla možnost pokrytí více místností jednou soupravou, ovšem právě vzhledem k této vlastnosti vyžadovaly velké zkušenosti techniků při nastavování a ladění v konkrétních podmínkách.

Zahájení průmyslové výroby Gunnových diod jako komerčně i technicky využitelných generátorů gigahertzových frekvencí znamenalo nástup mikrovlnných čidel. Na přelomu šedesátých a sedmdesátých let se tak na zabezpečovacím trhu se objevil prostředek umožňující poměrně snadné cílené pokrytí střeženého prostoru prakticky neodstíratelným signálem, a tedy téměř nepřekonatelnou spolehlivostí detekce. Dodnes patří mikrovlnná čidla mezi nejúčinnější zabezpečovací technologie, ovšem s podmínkou jejich perfektního zvládnutí a velkých zkušeností z praktického využívání. Proto se s nimi v praxi setkáváme poměrně zřídka – získávání potřebných zkušeností je při komerčních aplikacích značně nákladná a riziková záležitost.

Zhruba ve stejné době se do popředí zájmu dostávají i „světelné závory“. Princip byl ovšem využíván již dávno, ale teprve dostupnost účinných miniaturních zdrojů infračerveného světla a dalších potřebných polovodičových součástek umožnila jejich kvalifikované využívání v zabezpečovací technice.

Ve druhé polovině sedmdesátých let se na trhu objevuje dodnes nejúspěšnější zabezpečovací prvek – pasivní infračervené čidlo (Passive Infrared Detector – PIR). Pochází z hlavic samonaváděcích protiletadlových a protitankových raket a brzy z komerčních aplikací vytlačilo aplikačně i energeticky náročná mikrovlnná čidla. Ačkoliv PIR čidla nedosahují bezpečnostní spolehlivosti čidel fungujících na Dopplerově principu, jejich spolehlivost, láce a relativní jednoduchost používání měly brzy za následek vytlačení ostatních typů prostorových čidel na okraj zájmu.

### 1.2 Poplachové systémy v ČR po roce 1989

Se změnou společenského zřízení směrem k demokratizaci celé společnosti se uvolnily podmínky pro rozvoj i tohoto oboru. Přestože není obor Poplachových systémů mladý, stál po roce 1989 vlastně na úplném začátku. Bez dostatečného množství kvalifikovaných pracovníků, bez odborné literatury v české řeči, bez učebnic a žáků na odborných školách a s výjimkou jediné normy ČSN 334590 prakticky bez normativní základny.

Na druhé straně stály nové podmínky, které rozvoji oboru Poplachových systémů velice přály. Jednou z nich byl i nechtěný průvodní jev demokratizace - růst trestné činnosti a to především majetkové.

Dále lze jmenovat faktory jako:

- privatizace,
- restituce,
- rozvoj investiční výstavby,
- rozvoj bankovního sektoru,
- rozvoj pojišťovnictví,
- uvolnění mezinárodního obchodu,
- umožnění volného pohybu osob,
- růst obecné kriminality,
- nová bezpečnostní rizika konce tisíciletí.

Aktivita dovozců, tuzemských výrobců, instalačních firem a koneckonců i zákazníků vyzdvihla obor EZS na plnoprávný slaboproudý obor se svými pravidly. Na druhou stranu vytvořil masivní příliv zahraničních výrobků, ke kterému po otevření Českého trhu došlo, podmínky pro řadu zlatokopů, kteří využívali neznalost zákazníků ze soukromé i veřejné sféry. Významnou roli směřující ke stanovování a dodržování pravidel v oboru v počátcích porevolučního rozvoje sehrál Odbor nástrahové a zabezpečovací techniky Ministerstva vnitra, který přechodně nahradil absenci zkušebnictví a výrokové certifikace produktů v ČR. Tato regulativní bariéra se ukázala být nanajvýše účelnou zvláště zpočátku. S růstem kompetence zákazníků se stala nadbytečnou a při restrukturalizaci Ministerstva vnitra došlo k zrušení tohoto útvaru. Jeho úlohu převzaly oficiálně akreditované zkušebny a certifikační orgány. Na dnešním trhu působí v dané oblasti především akreditovaná zkušebna Trezortest, která v rozsahu své činnosti má vedle poplachových systémů i Mechanické zábranné systémy. Svoji roli v oboru hraje dnes i Certifikační institut České asociace pojišťoven (CI ČAP), který po vzoru německé VdS (svazu zřizovatelů) nastartoval systém regulace v oboru Poplachových systémů. Pojišťovny mají totiž ze zákona možnost stanovovat dodatečné technické požadavky na základě tzv. „blokové výjimky“. Tato výjimka kopíruje pravidla Evropských společenství v oboru Poplachových systémů. Další zkušebna – Vojenský technický ústav elektroniky zřízený při Armádě České republiky ukončil svoji činnost pro veřejnost a dnes působí pod hlavičkou Agentury pro rozvoj elektroniky především pro sektor Armády.

Díky těmto začátkům se v ČR vyvinul v určitém slova smyslu v Evropských měřítkách výjimečný systém regulace kterou požadují sami zákazníci jako důkaz splnění vlastností komponent pro jejich použití v objektech s ohledem na rizika zabezpečovaných provozů a objektů.



### 1.3 Poplachové systémy – my a svět

Díky masivnímu rozvoji tohoto oboru po roce 1989 lze říci, že jsme bez nadsázky dohonili a v mnohém i předhonili svět. Oblasti společnosti, které dříve nebyly vůbec pokryty Poplachovými systémy jsou dnes vybaveny progresivní technikou a např. v oblasti bankovníctví došlo od roku 89 již ke dvěma skokovým inovačním změnám.

Dnes stojí celý obor jak u nás, tak i ve světě před obrovskou koncepční změnou a tou je integrace Poplachových systémů v rámci sítí informačních technologií.

Integrace slaboproudých elektronických systémů do digitálních přenosových sítí v rámci objektů se nevyhnula ani Poplachovým systémům a tak aplikacemi, které konzervativně lpí na existenci vlastní přenosové sítě zůstávají vlastně již jen systémy EZS a EPS. Zde je však existence vlastní přenosové sítě dána spíše koncepcí historicky svázanou s oprávněnými požadavky norem a předpisů, než technickými možnostmi těchto systémů.

U některých poplachových systémů (např. CCTV) byl tento do určité míry konzervativní přístup způsoben limitami danými specifickými vlastnostmi přenášených signálů - hlavně požadavky na šířku pásma a požadavky na přenos v reálném čase. Díky pokroku v oblasti rychlosti zpracování signálu v digitálních systémech, vývoji kompresních algoritmů, zvyšování rychlosti přenosových sítí a v neposlední řadě v oblasti zvyšování kapacity paměťových médií padla i tato poslední bariéra. Do budoucna budeme muset zřejmě přehodnotit svůj postoj k současně platným pravidlům aplikovaným v oboru Poplachových systémů.

Mění se rovněž filosofie návrhu od výhradně hvězdicové konfigurace systémů k otevřené síťové konfiguraci, kde je možné prakticky kdykoli při změně požadavků uživatele prostřednictvím příslušných rozhraní přidat (či ubrat) systémový prvek a softwareově překonfigurovat přístupová práva. Rovněž přístup k datům a ovládání je možno řešit ne jako dříve prostřednictvím fyzického zařízení, ale virtuálně prostřednictvím softwareového oprávnění přístupu k serveru či k samostatnému diskovému poli, sloužícímu jako archiv událostí.

Zde přibývají otázky týkající se správy dat - to znamená že se tím dostáváme do oblasti bezpečnosti informačních systémů a je možno aplikovat např. posouzení s ohledem na plnění požadavků ČSN BS 7799 Informační technologie - Soubor postupů pro řízení informační bezpečnosti. Jedná se o posouzení otázek vztahujících se k ochraně všech částí IS - hardware, operačních systémů a programového vybavení, dat, aplikací, prvků datové komunikace proti chybám a výpadkům, úmyslným i neúmyslným zásahům zevnitř i zvenčí, náhodným i předvídatelným chybám a poruchám s cílem minimalizace pravděpodobnosti jejich výskytu a účinku.

### 1.4 Poplachové systémy - budoucnost

V poslední době se prudce rozvíjejí biometrické systémy využívající některých anatomických fyziologických vlastností člověka k jeho identifikaci. Zatím byly využívány pouze v přístupových systémech (Access Control Systems), ale s vývojem výpočetní techniky se jejich možnosti rozšiřují a objevily se již produkty dovolující jejich bezpečnostní aplikace. Dá se oprávněně očekávat, že zejména systémy průmyslové televize (CCTV), po padesát let využívané téměř výlučně jako monitorovací a dokumentační prostředek

(s výjimkou aplikace tzv. videosenzorů čili detektorů pohybu), zaznamenají v blízké době kvalitativní skok do zcela nových dimenzí a bezpečnostních aplikací.

V současné době lze konstatovat, že úroveň techniky užívaná v oboru Poplachových systémů v ČR kopíruje prakticky bez zpoždění vývoj vědy a techniky ve světě. Globalizace se projevila i zde. Díky celosvětovým informačním sítím není žádný problém ani pro zákazníky dozvědět se co je nového ve světě v tomto oboru a logicky to po svých dodavatelích požadovat. To samozřejmě vytváří tlak na obchodní, projekční i montážní organizace a i oni musí sledovat neustále světové trendy a reagovat na ně ve svých nabídkách.

## 2 Předpisová základna v oboru poplachových systémů

### 2.1 Evropská unie

V Evropských společenstvích spadá Zabezpečovací technika (zařízení používaná v poplachových systémech) pod působnost **směrnic Evropských společenství**. Směrnice Evropských společenství je druh dokumentu, který vydává Evropská komise (EC) (dříve Evropská hospodářská komise - EEC). Tento typ dokumentu stanovuje základní požadavky. Nemá přímou právní platnost v rámci členských zemí. Po jejich projednání a schválení jsou směrnice vyhlášovány v Úředním věstníku Evropských společenství (Official Journal of European Union). Povinností členských zemí je zásady uvedené ve směrnicích zpracovat do národní legislativy v termínu stanoveném přímo ve směrnicích. Povinnosti ze směrnic technického charakteru jsou pak **závazné pro výrobce, dovozce a distributory** výrobků spadajících pod působnost příslušného národního legislativního předpisu.

Pro podporu splnění požadavků směrnic jsou vyhlášovány v Úředním věstníku EU **Evropské harmonizované normy**. Tyto **harmonizované normy nejsou závazné**, nicméně jejich splnění je po právní stránce chápáno jako precedens splnění právních požadavků stanovených na daný okruh výrobků. Evropské normy jsou zpracovávány Evropskými normalizačními organizacemi CEN a CENELEC (**CEN - Evropský výbor pro normalizaci European Committee for Standardization a Evropský výbor pro normalizaci v elektrotechnice - European Committee for Electrotechnical Standardization**).

### 2.2 Česká republika

V České republice jsou technické směrnice EC přejímány formou Nařízení vlády České republiky. S ohledem na to, že ČR je od roku 2004 plnoprávným členem EU, kopíruje linie základních legislativních požadavků na výrobky pravidla obvyklá v zemích EU.

Základní legislativní rámec je tvořen **Zákonem 22/97Sb. o technických požadavcích na výrobky**. Tento zákon byl schválen 24.1.1997 a nabyl účinnosti 1.9.1997. Zákon byl s ohledem na proces sbližování právních předpisů ČR s právními předpisy ES v předvstupním období již několikrát novelizován zákonem 71/2000Sb., 102/2001 Sb. a 205/2002 Sb., 226/2003 Sb. a 277/2003 Sb. Pracovní úplné znění zákona s ustanoveními platnými od 1.5.2004 je k dispozici na internetových stránkách Úřadu pro normalizaci metrologii a státní zkušebnictví ([www.unmz.cz](http://www.unmz.cz)). Dále je nutno v tomto oboru počítat s působností základních souvisejících technických předpisů - Nařízení vlády č. 17/2003

Sb., kterým se stanoví technické požadavky na elektrická zařízení nízkého napětí (73/23/EHS), Nařízení vlády č. 18/2003 Sb., kterým se stanoví technické požadavky na výrobky z hlediska jejich **elektromagnetické kompatibility** (89/336/EHS). Ve specifických případech je nutno počítat i s působností Nařízení vlády č. 23/2003 Sb., kterým se stanoví technické požadavky na zařízení a ochranné systémy určené **pro použití v prostředí s nebezpečím výbuchu** (94/9/EHS). Pro oblast EPS navíc přichází v úvahu i Nařízení vlády č. 190/2002 Sb., kterým se stanoví technické požadavky na **stavební výrobky označované CE**, ve znění Nařízení vlády č. 251/2003 Sb. a Nařízení vlády č. 128/2004 Sb. (89/106/EHS). Pro přenosové systémy využívajícími veřejnou telekomunikační síť a případně elektromagnetického spektra je nutno aplikovat požadavky Telekomunikačního zákona a Nařízení vlády č. 426/2000 Sb., kterým se stanoví technické požadavky na **rádiová a na telekomunikační koncová zařízení**, ve znění Nařízení vlády č. 483/2002 Sb. a Nařízení vlády č. 251/2003 Sb. (1999/5/ES). ([www.ctu.cz](http://www.ctu.cz)).

### 3 Oborově specifické normy

Technické normy jsou předpokladem technického pořádku v daném oboru na příslušné úrovni, tedy např. celosvětově, mezinárodně, národně, v rámci určitého sdružení zájemců, podnikově apod. V oboru poplachových systémů začaly v posledním desetiletí 20. století vznikat na půdě evropských (CENELEC - Evropský výbor pro normalizaci v elektrotechnice) a světových (IEC - Mezinárodní výbor pro elektrotechniku) normalizačních organizací oborové standardy nabízející pro jednotlivé skupiny zařízení z oboru poplachových systémů:

- řešení funkčních požadavků na jednotlivá zařízení,
- dále uvádějící metody zkoušení prokazující splnění těchto funkčních požadavků,\*)
- požadavky na vlastnosti vztahující se k vlivům prostředí (klimatické odolnosti),\*)
- metody zkoušení prokazující splnění klimatické odolnosti,\*)
- systémové požadavky vztahující se k podmínkám nasazení těchto systémů,\*)
- návody a doporučení na aplikaci poplachových systémů.

\*) Poznámka - tyto požadavky a metody zkoušení jsou obsahem tzv. výrobních norem

Evropské normy (EN) jsou produktem evropských normalizačních organizací. V případě poplachových systémů je to konkrétně technická komise CLC/TC79 a její pracovní skupiny. V případě EPS je to CEN/TC72 a její pracovní skupiny.

#### 3.1 Technická komise CENELEC/TC79

TC79 je technická komise - poplachové systémy (Alarm Systems) při Evropském výboru pro normalizaci v elektrotechnice (CENELEC). Pole působnosti této komise je velmi široké a to jak do šíře odborného záběru, tak do počtu zpracovávaných norem. Pokrývá nejen klasickou EZS, ale komplexně celou oblast zabezpečení jako je CCTV, kontrola vstupů, systémy přivolání pomoci, přenosové systémy pro hlášení poplachu a integrované systémy. Zasedání komise CLC/TC79 je zpravidla dvakrát ročně. Za ČR zabezpečuje mezinárodní spolupráci s CENELEC TC79 Asociace bezpečnostních služeb Grémium Alarm jejíž zástupce se pravidelně zúčastňuje zasedání TC 79.

### 3.2 Technická komise CEN/TC 72

TC 72 je technická komise - elektrická požární signalizace (fire detection and fire alarm systems) při Evropském výboru pro normalizaci (CEN). Komise normalizuje požadavky a zkušební metody pro prvky elektrické požární signalizace. Výsledkem práce technické komise je tvorba norem řady EN 54. Komise se schází od roku 1973 na jarním a podzimním zasedání. Za ČR zabezpečuje mezinárodní spolupráci s CEN / TC72 LITES Liberec.

EPS je zařazena ve všeobecné normalizaci (CEN) a poplachové systémy do elektrotechnické normalizace (CENELEC, zkráceně CLC). Přitom oba systémy jsou si velice blízké a vývoj směřuje k integraci těchto systémů. Zatím je normalizační rámec odlišný a i způsob uvádění těchto systémů na trh se liší.

### 3.3 Normalizační zabezpečení v ČR

V ČR je organizací ze zákona pověřenou odpovědností za proces zavádění EN do ČSN Český normalizační institut (ČNI). Česká republika je prostřednictvím ČNI řádným členem obou výborů (CEN i CENELEC). ČNI na základě návrhu zainteresovaných zájmových sfér společnosti zřizuje technické normalizační komise (TNK). TNK jsou tedy odbornými normalizačními orgány s celostátní působností, registrovanými, řízenými a koordinovanými ČNI. Jejich působnost je ve svém oboru navrhovat normalizační práce, posuzovat, projednávat a zpracovávat náměty, sledovat a spolupracovat v mezinárodní normalizaci apod. Podle naznačených zásad vznikla při ČNI TNK 124 „EPS a poplachové systémy“. TNK 124 vznikla na základě iniciativy průmyslu a obdobným způsobem se rozšiřovala o nové členy, kterých je dnes více než 25. Příslušní zástupci jsou odborníky (nikoliv normalizační pracovníci) ve svých oborech a jsou i jazykově vybaveni, takže jsou vesměs schopni posuzovat i projednávat anglické originály norem. TNK 124 se maximálně snaží EN do ČSN zavádět komplexně a v rámci možností navazovat na dřívější systém.

Tabulka 1-1: Struktura norem v působnosti CLC/TC79 a CEN/TC72

<b>Všeobecně</b> EN 50 130 +	Elektronické zabezpečovací systémy (EVS) EN 50 131+	Systémy uzavřených televizních okruhů (CCTV) EN 50 132 +
Systémy kontroly a řízení vstupu (ACS) EN 50 133 +	<b>Systémy přivolání pomoci (SAS)</b> EN 50 134 +	
<b>Přenosová zařízení (ATS)</b> EN 50 136 +	Systémy kombinované nebo integrované (IAS) EN 50 137 +	Elektrická požární signalizace (EPS) EN 54 +

Tabulka 1-2: Jednotlivé normy mají v rámci svých nadřazených tematických celků (kromě řady EN 50130 a EN 50137) stejnou strukturu:

ČSN EN 50 13X - 1 Systémové požadavky	Systémová norma - co má umět systém, jaké plní funkce, většinou jen všeobecné požadavky na jednotlivé typy výrobků, definice kategorizace.
ČSN EN 50 13X - Y Produktové normy	Obsahují konkrétní a detailní požadavky na konkrétní typy výrobků (například PIR čidla, černobílé monitory apod.) a to včetně požadovaných zkoušek.
ČSN EN 50 13X - 7 Aplikační směrnice	Definují, jak má být systém navržen namontován a udržován, z jakých fází se návrh a montáž skládá, co je třeba vzít v úvahu, atd.

V CLC/TC79 jsou naplánovány jednotlivé normy tak, že budou v jednotlivých skupinách postupně zpracovávány. Podle pravidel členství v CENELEC nemůže ČR u těchto naplánovaných norem vydávat svoje národní normy které by byly v rozporu s plánovanými či vydanými normami EN. Vzhledem k tomu, že ČNI podle pravidel členství v CENELEC organizuje převzetí evropských norem do soustavy ČSN buď překladem nebo převzetím originálu, lze v jednotlivých částech uvedené tabulky považovat i za systém, který bude plně odpovídat systému ČSN pro obor poplachových systémů. Aktuální seznam norem vydaných jako ČSN viz webová adresa ČSNI ([www.cni.cz](http://www.cni.cz)).

### 3.3.1 Skupina norem na Elektrické zabezpečovací systémy (EZS)

Tabulka 1-3: Skupina norem na Elektronické zabezpečovací systémy (EN 50131)

Číslo normy	Zjednodušený název	Vydána jako ČSN
EN 50131-1	Všeobecné požadavky	červenec 1999
EN 50131-2-1	Společné požadavky pro detektory (čidla)	
CLC/TS 50131-2-2	Detektory (čidla) pasivní	prosinec 2005
CLC/TS 50131-2-3	Detektory (čidla) MW	prosinec 2005
CLC/TS 50131-2-4	Detektory (čidla) kombinovaná PIR/MW	prosinec 2005
CLC/TS 50131-2-5	Detektory (čidla) kombinovaná UZ/PIR	prosinec 2005
EN 50131-2-6	Detektory (čidla) otevření	srpen 2005
CLC/TS 50131-3	Ústředny	květen 2005
EN 50131-4	Výstražná zařízení	
EN 50131-5-1	Společné požadavky pro propojovací zařízení	
prEN 50131-5-3	Propojovací zařízení využívající vyhrazené drátové spoje	březen 2006
EN 50131-5-4	Propojovací zařízení využívající VF techniku	
EN 50131-5-5	Propojovací zařízení využívající IČ techniku	
EN 50131-6	Napájecí zdroje	září 1999
CLC/TS 50131-7	Pokyny pro aplikace	květen 2005

\*) Poznámka - K této normě jsou vydány tři Technické normalizační informace (TNI), které poskytují návod k aplikaci normy v podmínkách ČR.

Tabulka 1-4: Technické normalizační informace

Číslo normy	Zjednodušený název	Vydání v ČSNI
TNI 334590-1	Elektrická zabezpečovací signalizace - Pokyny pro aplikace – Část 1: Návrh systémů EZS	srpen 2005
TNI 334590-2	Elektrická zabezpečovací signalizace - Pokyny pro aplikace – Část 2: Montáž systémů EZS	říjen 2005
TNI 334590-3	Elektrická zabezpečovací signalizace - Pokyny pro aplikace – Část 3: Kontrola EZS po montáži, výchozí a pravidelné revize EZS, funkční zkoušky a měření	říjen 2005

### **Anotace TNI:**

Tyto technická informace (dále jen TNI) jsou určeny pro používání spolu s platnou ČSN CLC/TS 50131-7:2004 (33 4591) Poplachové systémy – Elektrické zabezpečovací systémy - Část 7 Pokyny pro aplikace. Byly vypracovány pro usnadnění orientace v předmětné oblasti a pro uplatnění některých technických řešení, která nejsou v ČSN CLC/TS 50131-7:2004 obsažena.

### **3.3.2 Skupina norem na Elektrickou požární signalizaci (EPS)**

Tento obor díky úzké vazbě na legislativu byl i v dobách před rokem 89 velice silně normalizačně zabezpečen. Dnes tvoří legislativní rámec zřizování EPS Zákon č. 67/2001 Sb. o požární ochraně a z řady vyhlášek především č. 246/2001 Sb. o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru a stavební zákon. Systémy používané na území ČR musí být certifikovány. Certifikační orgány (autorizované osoby) pro schvalování zařízení EPS k provozu na území ČR jsou v současné době tři: **PAVUS a.s.**, **TZUS s.p.** a **EZÚ s.p.** V současné době je v republice certifikováno cca 15 systémů EPS. Certifikovaný musí být vždy systém EPS jako celek, nebo pokud se skládá z ústředny a jednotlivých prvků jiných výrobců, musí být certifikovány tyto prvky jako použitelné s danou ústřednou.

Dále je nutno v tomto oboru počítat s působností Zákona 22/97Sb. o technických požadavcích na výrobky ve znění pozdějších předpisů a souvisejících technických předpisů - Nařízení vlády č. 17/2003 Sb., kterým se stanoví technické požadavky na **elektrická zařízení** nízkého napětí (73/23/EHS), Nařízení vlády č. 18/2003 Sb., kterým se stanoví technické požadavky na výrobky z hlediska jejich **elektromagnetické kompatibility** (89/336/EHS) a Nařízení vlády č. 190/2002 Sb., kterým se stanoví technické požadavky na **stavební výrobky označované CE**, ve znění nařízení vlády č. 251/2003 Sb. a nařízení vlády č. 128/2004 Sb. (89/106/EHS) ve znění platných změn. Úplný přehled související legislativy lze získat na [www.cecheps.cz](http://www.cecheps.cz) Normativní základem pro obor EPS jsou normy řady EN 54, které jsou postupně přejímány do systému Českých technických norem. Tvorba těchto norem je výsledkem práce technické komise CEN/TC 72. Evropské normy řady EN 54 jsou ve stavu rozpracování a dnes jsou z celé skupiny známé následující části:

Tabulka 1-5: Evropské normy na EPS

Číslo normy	Název	Vydána jako ČSN
EN 54-1	Elektrická požární signalizace - Část 1: Úvod	září 1997
EN 54-2 (norma je určená)	Elektrická požární signalizace - Část 2: Ústředna	únor 1999
EN 54-3 (norma je harmonizovaná)	Elektrická požární signalizace - Část 3: Požární poplachová zařízení - Sirény	duben 2002
EN 54-4 norma je harmonizovaná)	Elektrická požární signalizace - Část 4: Napájecí zdroj	únor 1999 A1 9.03
EN 54-5 (norma je harmonizovaná)	Elektrická požární signalizace - Část 5: Hlásiče teplot - Bodové hlásiče	prosinec 2001 A1 6.03
EN 54-7 (norma je harmonizovaná)	Elektrická požární signalizace - Část 7: Hlásiče kouře - Hlásiče bodové využívající rozptýleného světla, vysílaného světla a ionizace	říjen 2001 A1 6.03
EN 54-10	Elektrická požární signalizace - Část 10: Hlásiče plamene - Bodové hlásiče .	prosinec 2002
EN 54-11	Elektrická požární signalizace - Část 11: Tlačítkové hlásiče	březen 2002
EN 54-12 (norma je harmonizovaná)	Elektrická požární signalizace - Část 12: Hlásiče kouře - Hlásiče lineární využívající optického světelného paprsku	červenec 2003
EN 54-13	Systémové požadavky (zatím nevyšla)	prosinec 2005
TS 54-14	Aplikační návody	prosinec 2005
EN 54-15	Hlásiče multisenzorové a hlásiče plynu	
EN 54-16	Ústředny pro hlasové poplachové systémy	
EN 54-17	Izolátory	červenec 2006
EN 54-18	Vstupně-výstupní zařízení	červen 2006
EN 54-19	neobsazeno	
EN 54-20	Nasávací hlásiče	
EN 54-21	Přenosová zařízení	
EN 54-22	Lineární tepelné hlásiče	
EN 54-23	Optická poplachová zařízení	
EN 54-24	Reproduktory pro hlasové zdroje zvuku	
EN 54-25	Komponenty využívající rádiové linky	

*Poznámka - Zde je třeba podotknout, že řada evropských norem na EPS vychází nikoli jako EN, ale jako Technická specifikace (TS) z důvodu neschválení na úrovni CEN. Neschválení je způsobeno nekompatibilitou těchto norem s národními systémy, které jsou navázány na konkrétní zákonné předpisy pro oblast požární ochrany v jednotlivých zemích.*

Vedle těchto norem je nutno počítat s existencí norem z mezinárodního systému pod ISO a s dosud platnými národními normami především ze skupiny ČSN 7308XX - Požární

bezpečnost staveb, z nichž některé jsou vyhlášeny jako normy harmonizované případně určené (viz [www.csni.cz](http://www.csni.cz)).

Pro výrobu a provoz zařízení EPS platí norma ČSN 34 2710 - Předpisy pro zařízení elektrické požární signalizace. (účinnost: 1979-05-01 Změny a opravy: a 12.79, b 7.85 3.90, 4 10.94, 5 9.97, 6 2.99, Z7 10.01, Z8 12.01)

Pro navrhování a projektování EPS platí ČSN 73 0875 z roku 1991. Obě normy jsou postupně nahrazovány jednotlivými oddíly EN 54 tak, jak jsou schvalovány a vydávány.

Pro navrhování systémů EPS se využívá norma ČSN 73 0875 - Požární bezpečnost staveb. Navrhování elektrické požární signalizace (účinnost: 1992-03-01) U jednotlivých typů objektů je ovšem nutné vzít v úvahu i ustanovení dalších norem řady ČSN 73 08xx – Požární bezpečnost staveb. Přehled Českých technických norem souvisejících se zřizováním EPS je uveden dále.

Tabulka 1-6: České technické normy na EPS

Název normy	Název	Účinnost/ Změny
ČSN 73 0802	Požární bezpečnost staveb - Nevýrobní objekty	2001-01-01
ČSN 73 0804	Požární bezpečnost staveb - Výrobní objekty	2002-11-01
ČSN 73 0810	Požární bezpečnost staveb. Požadavky na požární odolnost stavebních konstrukcí	1996-10-01 Z1 5.04
ČSN 73 0818	Požární bezpečnost staveb - Obsazení objektů	1997-08-01 Z1 10.02
ČSN 73 0821	Požární bezpečnost staveb. Požární odolnost stavebních konstrukcí	1974-10-01 a 3.80, b 6.83
ČSN 73 0822	Požárně technické vlastnosti hmot. Šíření plamene po povrchu stavebních hmot	1987-09-01
ČSN 73 0823	Požárně technické vlastnosti hmot. Stupeň hořlavosti stavebních hmot	1984-04-01 Z1 7.03
ČSN 73 0824	Požární bezpečnost staveb. Výhřevnost hořlavých látek	1993-01-01
ČSN 73 0831	Požární bezpečnost staveb – Shromažďovací prostory	2002-01-01
ČSN 73 0833	Požární bezpečnost staveb. Budovy pro bydlení a ubytování	1996-02-01 Z1 12.00
ČSN 73 0834	Požární bezpečnost staveb – Změny staveb	2000-08-01
ČSN 73 0835	Požární bezpečnost staveb. Budovy zdravotnických zařízení	1996-05-01
ČSN 73 0842	Požární bezpečnost staveb. Objekty pro zemědělskou výrobu	1996-05-01 Z1 10.04
ČSN 73 0843	Požární bezpečnost staveb - Objekty spojů a poštovních provozů	2001-08-01
ČSN 73 0845	Požární bezpečnost staveb – Sklady	1997-03-01 Z1 2.99
ČSN 73 0856	Stanovení požární odolnosti zavěšených podhledů	1988-01-01 a 8.91
ČSN 73 0863	Požárně technické vlastnosti hmot. Stanovení šíření plamene po povrchu stavebních hmot	1992-01-01
ČSN 73 0865	Požární bezpečnost staveb. Hodnocení odkapávání hmot z podhledů stropů a střech	1988-01-01
ČSN 73 0872	Požární bezpečnost staveb. Ochrana staveb proti šíření požáru vzduchotechnickým zařízením	1996-02-01
ČSN 73 0873	Požární bezpečnost staveb - Zásobování požární vodou	2003-07-01



Další normy související s navrhováním a projektování systémů EPS, zkouškami, revizemi a instalací v různých prostředích atd.

Tabulka 1-7: České elektrotechnické normy související s EPS

Název normy	Název	Účinnost/ Změny
ČSN 34 1390	Elektrotechnické předpisy ČSN. Předpisy pro ochranu před bleskem	1970-04-01 a 12.79, b 5.85, c 1.88, 4 12.96
ČSN 34 1391	Elektrotechnické předpisy ČSN. Ochrana před bleskem část1.instalace s optickými kabely.	2001-08-01
ČSN 34 2100	Elektrotechnické předpisy ČSN. Předpisy pro nadzemní sdělovací vedení	1977-03-10
ČSN 34 2300	Elektrotechnické předpisy ČSN. Předpisy pro vnitřní rozvody sdělovacích vedení	1965-04-07
ČSN 34 3100	Elektrotechnické předpisy ČSN. Bezpečnostní předpisy pro obsluhu a práci na elektrických zařízeních	1967-10-01 a 5.68, b 1.70, c 7.76, d 2.79, e 9.85, f 3.89, 4.93, 8 9.94, Z9 11.03, 1 12.04
ČSN EN 50265-1	Společné metody zkoušek pro kabely v podmínkách požáru - Zkouška odolnosti proti svislému šíření plamene pro vodiče nebo kabely s jednou izolací - Část 1: Zkušební postupy	1999-09-01 Z1 5.05
ČSN EN 50265-2-1	- Společné metody zkoušek pro kabely v podmínkách požáru - Zkouška odolnosti proti svislému šíření plamene pro vodiče nebo kabely s jednou izolací - Část 2-1: Postupy - 1 kW směsný plamen	1999-09-01 Z1 4.05
ČSN EN 50265-2-2	Společné metody zkoušek pro kabely v podmínkách požáru - Zkouška odolnosti proti svislému šíření plamene pro vodiče nebo kabely s jednou izolací - Část 2-2: Postupy - Svitivý plamen	1999-09-01 Z1 4.05
ČSN EN 50266-1 až 5	Společné zkušební metody pro kabely za podmínek požáru - Zkouška vertikálního šíření plamene na vertikálně namontovaných svazcích vodičů nebo kabelů	2001-12-01 Z: 1 8.02
ČSN 33 1500	Elektrotechnické předpisy. Revize elektrických zařízení .	1991-06-01 Z1 8.96, Z2 4.00, Z3 4.00
ČSN 33 2000-4-41	Elektrotechnické předpisy - Elektrická zařízení - Část 4: Bezpečnost - Kapitola 41: Ochrana před úrazem elektrickým proudem .	2000-03-01 Z:1 9.00, Z1 11.02 Z2 8.03
ČSN 33 2000-5-51	- Elektrotechnické předpisy - Elektrická zařízení - Část 5: Výběr a stavba elektrických zařízení - Kapitola 51: Všeobecné předpisy .	2000-05-01

Tabulka 1-8: České elektrotechnické normy související s EPS

Název normy	Název	Účinnost/ Změny
ČSN 33 2000-6-61 ed. 2	Elektrické instalace budov - Část 6-61: Revize - Výchozí revize	2004-05-01
ČSN 33 2340	Elektrotechnické předpisy. Elektrická zařízení v prostředích s nebezpečím požáru nebo výbuchu výbušnin	1980-09-01 a 10.82, b 12.87
ČSN 33 2312	Elektrotechnické předpisy. Elektrická zařízení v hořlavých látkách a na nich.	1986-09-01
ČSN EN 50014	Nevýbušná elektrická zařízení - Všeobecné požadavky .	1998-11-01 A1 9.99, A2 9.99, Z1 12.04
ČSN EN 50039	- Nevýbušná elektrická zařízení. Jiskrově bezpečné elektrické zařízení.	1993-11-01 Z1 9.04
ČSN EN 50020 ed. 3	- Nevýbušná elektrická zařízení - Jiskrová bezpečnost“	2003-04-01

*Poznámka - Počet norem, související s problematikou návrhu a instalace systémů EPS budí respekt. Nesmíme však zapomenout na skutečnost, že se jedná o vysoce zodpovědnou preventivní činnost. vždyť k zahoření dojde v rámci republiky ročně v každém čtvrtém objektu !!!*

### **3.3.3 Skupina norem na CCTV sledovací systémy pro použití v bezpečnostních aplikacích**

CCTV systémy jsou v EN pojaty jako doplňková zařízení poplachových systémů a nejsou na ně stanoveny kritéria na stupně zabezpečení, tak jako u klasických poplachových systémů dle ČSN EN 50131-1. Proto je z ohledem na aplikaci rozhodující především konstatování skutečnosti, zda zařízení splňuje nebo nesplňuje požadavky dané příslušnou normou a tudíž zda je lze použít v aplikacích poplachových systémů.

Požadavky na poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích jsou nebo budou uvedeny v těchto skupinách evropských technických norem řady EN50132-x:

Tabulka 1-9: Skupina norem na CCTV

Číslo normy	Zjednodušený název	Vydána jako ČSN
EN 50132-1	Systémové požadavky	
EN 50132-2-1	Černobílé kamery	červenec 1999
EN 50132-2-2	Barevné kamery	
EN 50132-2-3	Objektivy	
EN 50132-2-4	Příslušenství	
EN 50132-3	Místní a hlavní řídicí jednotka	
EN 50132-4-1	Černobílé monitory	duben 2002
EN 50132-4-2	Barevné monitory	
EN 50132-4-2	Barevné monitory	
EN 50132-4-3	Záznamová zařízení	
EN 50132-4-4	Zařízení pro okamžitý výtisk obrazu	
EN 50132-4-5	Videodetektor pohybu	
EN 50132-5	Přenos videosignálu	duben 2002
EN 50132-6	(Volná)	
EN 50132-7	Pokyny pro aplikace	duben 1999

### 3.3.4 Skupina norem na systémy kontroly vstupu pro použití v bezpečnostních aplikacích (ACS)

Do rodiny poplachových systémů jsou zařazeny i systémy kontroly a řízení vstupy (ACS - Acces Control Systems). Aplikace požadavků těchto norem je vymezeno úlohou nasazení ACS v konkrétním objektu. V této oblasti probíhá neustálý vývoj na úrovni stále bezpečnějších a jednodušeji použitelných médi, jež jsou nositeli přístupového oprávnění. Principiálně je nutno počítat s aplikací požadavků vztahujících se obecně na informační systémy, rozhraní a začlenění ACS jako subsystému pracujícího na bázi přenosové sítě informačního systému nejen na úrovni hardware, ale i na úrovni software. Dále je nutno zahrnout i požadavky na požární bezpečnost v případě nutnosti evakuace tímto systémem vybaveného objektu. Na koncové akční prvky (el. zámky, turnikety, brány, propusti a další) je nutno aplikovat požadavky ošetřené normami pod působností CEN/TC 33). Základní požadavky jsou nebo budou uvedeny v následující skupině evropských norem řady EN50133+:

Tabulka 1-10: Skupina norem na ACS

Číslo normy	Zjednodušený název	Vydána jako ČSN
EN 50133-1	Systémové požadavky	březen 2001
EN 50133-2-1	Identifikační zařízení - Všeobecné požadavky na komponenty	březen 2001
EN 50133-3	Vyhodnocovací zařízení	
EN 50133-4	Výstupní ovládací prvek přístupového místa	
EN 50133-5	Komunikace	
EN 50133-6	Volná	
EN 50133-7	Pokyny pro aplikace	listopad 2000

### 3.3.5 Skupina norem na Systémy přivolání pomoci (SAS)

Do rodiny poplachových systémů byl zařazen i Systém přivolání pomoci (SAS – Social Alarm Systems). Tento systém zajišťuje 24 hodinovou pohotovost pro aktivování poplachu, identifikaci, přenosu signálu, přijetí poplachu, záznam a obousměrnou hlasovou komunikaci k poskytnutí jistoty a pomoci lidem žijícím v domácnosti v ohrožení. Zde se jedná spíše o rizika zdravotní a použití je zvláště v oblasti péče o seniory.

Tabulka 1-11: Skupina norem na SAS

Číslo normy	Zjednodušený název	Vydána jako ČSN
EN 50134-1	Systémové požadavky	březen 2003
EN 50134-2	Aktivační zařízení	duben 2001
EN 50134-3	Místní jednotka a kontrolér	březen 2002
EN 50134-4	(volná)	
EN 50134-5	Propojení a komunikace	červenec 2005
EN 50134-6	(volná)	
EN 50134-7	Pokyny pro aplikace	březen 2006

### 3.3.6 Skupina norem na poplachové přenosové systémy a zařízení (ATS)

Tato skupina norem stanovuje požadavky na provedení, spolehlivost a bezpečnostní charakteristické znaky poplachových přenosových systémů a zařízení pro použití v různých typech poplachových systémů a využívajících různé přenosové cesty.

Použití EN 50136 se vyžaduje pro přenos všech typů poplachů; požár, vloupání, řízení přístupu, přivolání pomoci atd.

Je-li využívána veřejná telefonní síť, musí být aplikovány důležité evropské telekomunikační normy (ETS) ETSI a doporučení CCITT, CCIR a CEPT. Tam, kde je to vhodné, musí zařízení splňovat místní, národní a evropské požadavky a směrnice pro zřizování a ukončování spojení a přenosu prostřednictvím veřejné telefonní sítě a datové a/nebo směrnice pro radiový přenos, přenos prostřednictvím energetické rozvodné sítě a systémů televizních kabelových rozvodů.

V závislosti na požadovaném stupni spolehlivosti a provozních parametrech poplachových přijímacích center, je přípustné použít různé systémové konfigurace včetně po-

užití více než jedné poplachové přenosové cesty mezi poplachovým systémem a jedním nebo více poplachovými přijímacími centry.

Pro potřeby přenosové redundance musí být možné propojit poplachový systém ve střežených prostorech se vzdáleným centrem více než jednou formou přenosu, např. vyhrazenou poplachovou přenosovou cestou a digitálními komunikátory, které využívají veřejnou telefonní síť.

Tam, kde je použita přenosová síť, může poplachová přenosová cesta existovat pouze na dobu, kdy je zřízeno spojení.

Tabulka 1-12: Skupina norem na ATS

Číslo normy	Zjednodušený název	Vydána jako ČSN
EN 50136-1-1 + A1:2002	Všeobecné požadavky na poplachové přenosové systémy	červen 1999 + A1:2002
EN 50136-1-2	Požadavky na systémy využívající vyhrazené poplachové přenosové cesty	červen 1999
EN 50136-1-3	Požadavky na systémy s digitálními komunikátory využívajícími veřejnou komutovanou telefonní síť	červen 1999
EN 50136-1-4	Požadavky na systémy s hlasovými komunikátory využívajícími veřejnou komutovanou telefonní síť	červen 1999
EN 50136-2-1 + A1:2002	Všeobecné požadavky na poplachová přenosová zařízení	červen 1999 + A1:2002
EN 50136-2-2	Požadavky na zařízení v systémech využívajících vyhrazené poplachové přenosové cesty	červen 1999
EN 50136-2-3	Požadavky na zařízení v systémech s digitálními komunikátory využívajícími veřejnou komutovanou telefonní síť	červen 1999
EN 50136-2-4	Požadavky na zařízení v systémech s hlasovými komunikátory, které používají veřejnou telefonní síť	červen 1999
EN 50136-3	Poplachové přenosové protokoly	
EN 50136-4	Ovládací a indikační zařízení	listopad 2005
EN 50136-5	(volná)	
EN 50136-6	(volná)	
EN 50136-7	Pokyny pro aplikace	listopad 2005

### 3.3.7 Související elektrotechnické normy

V následující tabulce jsou uvedeny základní elektrotechnické normy související s návrhem, montáží, technickými prohlídkami a revizemi poplachových systémů. Tyto normy jsou uvedeny jako související v rámci Technických normalizačních informací k ČSN CLC TS 50131-7. V případě aplikace konkrétního systému je možné identifikovat další související normy např. s ohledem na vliv prostředí apod. viz [www.csni.cz](http://www.csni.cz).

Poznámka - Seznam norem aplikovaných na konkrétní zakázku je vhodné **přesně** specifikovat jako součást či přílohu smlouvy na realizaci poplachového systému. Rozhodně by však být konkrétní seznam aplikovaných norem součástí projektové dokumentace na poplachový systém s důrazem na normy harmonizované případně určené.

Tabulka 1-13: Související elektrotechnické normy

Číslo normy	název normy	Třídící znak
ČSN 33 2000-1:1995	Elektrotechnické předpisy - Elektrická zařízení - Část 1: Rozsah platnosti, účel a základní hlediska	(332000)
ČSN 33 2000-3:1995	Elektrotechnické předpisy - Elektrická zařízení - Část 3: Stanovení základních charakteristik	(332000)
ČSN 33 2000-4-41:2000	Elektrotechnické předpisy - Elektrická zařízení - Část 4: Bezpečnost - Kapitola 41: Ochrana před úrazem elektrickým proudem	(332000)
ČSN 332000-4-43:1994	Elektrotechnické předpisy - Elektrická zařízení - Část 4: Bezpečnost - Kapitola 43: Ochrana proti nadproudům	(332000)
ČSN 33 2000-5-51:2000	Elektrotechnické předpisy - Elektrická zařízení - Část 5: Výběr a stavba elektrických zařízení - Kapitola 51: Všeobecné předpisy	(332000)
ČSN EN 332000-5-52:1998	Elektrotechnické předpisy - Elektrická zařízení - Část 5: Výběr a stavba elektrických zařízení - Kapitola 52: Výběr soustav a stavba vedení	(332000)
ČSN 33 2000-6-61:2000	Elektrotechnické předpisy - Elektrická zařízení - Část 6: Revize. Kapitola 61: Revize elektrických zařízení	(332000)
ČSN EN 60529:1993	Stupně ochrany krytem (krytí - IP kód)	(33 0330)
ČSN 330165:1992, tisková změna 1:1998, tisková změna Z2:2002	Elektrotechnické předpisy. Značení vodičů barvami nebo číslicemi. Prováděcí ustanovení	(330165)
ČSN 33 0420-1:1998	Elektrotechnické předpisy - Koordinace izolace elektrických zařízení nízkého napětí - Část 1: Zásady, požadavky a zkoušky	(330420)
ČSN 33 0420-1:1998	Elektrotechnické předpisy - Koordinace izolace elektrických zařízení nízkého napětí - Část 1: Zásady, požadavky a zkoušky	(330420)
ČSN 33 1500: 1989	Elektrotechnické předpisy. Revize elektrických zařízení	(331500)
ČSN 332130:1985, tisková změna a: 1988, tisková změna 2: 1994	Elektrotechnické předpisy. Vnitřní elektrické rozvody	(332130)

## 4 Odborná způsobilost

Odborná způsobilost potřebná pro podnikání v oblasti poplachových systémů je vymezena Živnostenským zákonem ve smyslu přílohy č.3 k Nařízení vlády č. 469/2000 Sb. Obsahově náplně koncesovaných živností ve znění změny 324/2006 Sb.

### 4.1 Poplachové systémy (EZS, CCTV, ACS..)

Základní živností pro obor poplachových systémů je:

#### **Skupina 314: Ostatní – Poskytování technických služeb k ochraně majetku a osob**

Projektování, montáž, kontrola, údržba a opravy elektronických poplachových systémů (zejména systémů zabezpečovacích, tísňových, protipožárních, kontroly vstupu, povolání pomoci, integrovaných a kamerových), určených k ochraně majetku a osob před neoprávněnými zásahy, včetně poplachových systémů a zařízení umožňujících sledování pohybu a projevů osob v objektech a jejich okolí. Montáž, údržba, revize a správa mechanických zábranných systémů, dodatečně zvyšujících účinnost běžných standardů zabezpečení majetku a osob.

Požadována je **odborná a jiná zvláštní způsobilost** podle § 27 odst. 1 a 2 živnostenského zákona ve znění zákona č. 356/1999Sb. a 167/2004Sb.:

- a) vysokoškolské vzdělání v příslušné oblasti nebo v příbuzné oblasti a 1 rok praxe v oboru nebo
- b) úplné střední odborné vzdělání v oboru nebo příbuzném oboru a 2 roky praxe v oboru nebo
- c) vyučení v tříletém učebním oboru v oboru nebo v příbuzném oboru a 3 roky praxe v oboru.

Podmínkou, jejichž splnění se vyžaduje podle § 27 odst. 3 živnostenského zákona ve znění z. č. 356/1999Sb. a 167/2004Sb. je **bezúhonnost** všech zaměstnanců (§ 6 odst. 2) zákona č. 455/1991 Sb. ve znění zákona č. 286/1995 Sb., 356/1999 Sb. a 167/2004 Sb.

#### 4.1.1 Projektování (návrh poplachových systémů)

Při projektování se mohou uplatnit specifické požadavky na způsobilost osob v souvislosti s ustanovením Stavebního zákona. Projektovou dokumentaci v tomto případě mohou zpracovávat fyzické nebo právnické osoby, které mají níže uvedenou živnost.

#### 4.1.2 Projektová činnost ve výstavbě

Jedná se o vázanou živnost dle zákona č.455/1991 Sb. ve znění platných předpisů – skupina 213 - Stavebnictví. Tuto živnost je možné u poplachových systémů provozovat v souvislosti se základní koncesovanou živností dle.

Podmínkou je odborná způsobilost – Autorizace v příslušném oboru podle zákona č.360/1992 Sb., o výkonu povolání autorizovaných architektů a o výkonu povolání autorizovaných inženýrů a techniků činných ve výstavbě ve znění platných předpisů, nebo splnění podmínek stanovených v § 34 téhož zákona. V oboru poplachových systémů se jedná o autorizaci v oboru „Technika prostředí staveb – specializace elektrotechnická zařízení“.

Předpokladem získání autorizace je příslušné odborné elektrotechnické vzdělání, předepsaná praxe a způsobilost v elektrotechnice, tj. §10 vyhlášky 50/78 Sb ve znění platných předpisů – samostatné projektování, nebo řízení projektování.

Fyzická osoba vykonává tuto živnost přímo, právnická osoba vykonává tuto živnost prostřednictvím takto kvalifikované osoby, která musí být v pracovně-právním vztahu s touto právnickou osobou.

Takto kvalifikovaná fyzická nebo právnická osoba může sama zpracovávat projektovou dokumentaci ve stupni **územního plánování, stavebního řízení i realizace stavby** v investiční výstavbě. Pokud autorizovaná osoba nemá příslušnou specializaci, musí ke zpracování projektové dokumentace přizvat autorizovanou osobu s příslušnou specializací.

Takto kvalifikovaná osoba může samozřejmě zpracovávat projektovou dokumentaci i u staveb, které nepotřebují dle § 56 zákona 50/1976 Sb. ve znění platných předpisů stavební povolení a nemají ani ohlašovací povinnost vůči stavebnímu úřadu (opravy vnitřních instalací).

Pokud se jedná o opravu v objektu, který je kulturní památkou - je i zde ohlašovací povinnost. Pokud je ale oprava instalací prováděna v rámci změny užívání stavby a je kvalifikována jako změna stavby dle §55 zákona 50/1976 Sb. ve znění platných předpisů – je zde dokonce povinnost povolení stavby ve stavebním řízení.

*Poznámka - Při zpracovávání projektové dokumentace systému EZS je v podmínkách ČR obvykle požadováno navíc prokázání znalosti konkrétní techniky prostřednictvím potvrzení o absolvování školení u výrobce nebo distributora techniky, která je navržena v projektovaném systému. Potřeba na absolvování školení u výrobce nebo distributora je logický důsledek rychlého rozvoje techniky EZS a potřeby prokázat schopnosti projektanta nejen v obecné poloze, ale i znalosti konkrétně vázané k předmětu díla. Toto prokázání může zadavatel či investor smluvně požadovat jako nezbytný kvalifikační předpoklad.*

### 4.1.3 Montáž

Montáž systému EZS mohou provádět fyzické nebo právnické osoby splňující uvedená ustanovení Živnostenského zákona, za podmínek plnění požadavků souvisejících právních předpisů na odbornou způsobilost pracovníků v elektrotechnice a zvláštních právních předpisů. Vedle základní živnosti **Skupina 314: Ostatní – Poskytování technických služeb k ochraně majetku a osob** je možné uplatnit pro specifické činnosti montáže v oboru poplachových systémů další požadavky na způsobilost:

#### 4.1.3.1 Montáž, údržba a servis telekomunikačních zařízení

Skupina 205: Elektrické stroje a přístroje - Montáž, údržba a servis telekomunikačních zařízení

Montáž, údržba a servis zařízení pro vysílání, přenos a příjem informací jakéhokoli druhu po vedení radiovými, optickými či jinými prostředky využívajícími elektromagnetických vln. Základními skupinami telekomunikačních zařízení jsou zejména....., speciální telekomunikační zařízení (*klasické signálové rozvody a zařízení, komunikátory pro popla-*



chové systémy), vysílací a přijímací rádiová zařízení (... ,rádiová přenosová zařízení pro poplachové systémy, ..)

Požadována je **odborná způsobilost** podle § 27 odst. 1 a 2 živnostenského zákona ve znění zákona č. 356/1999Sb. a 167/2004Sb. dle **§ 8 vyhl. č. 50/1978 Sb.**, o odborné způsobilosti v elektrotechnice, nebo doklady podle § 19 odst. 1 písm. a zákona č. 18/2004 Sb. o uznávání odborné způsobilosti.

### 4.1.3.2 Revize, údržba, servis

Činnosti související s prováděním prohlídek, funkčních zkoušek a revizí mohou provádět fyzické nebo právnické osoby, které mají některou z níže uvedených živností při splnění požadavků souvisejících právních předpisů na kvalifikaci pracovníků v elektrotechnice. Vedle základní živnosti **Skupina 314: Ostatní – Poskytování technických služeb k ochraně majetku a osob** je možné uplatnit pro specifické činnosti při servisu a údržbě v oboru poplachových systémů další požadavky na způsobilost:

### 4.1.3.3 Montáž, údržba a servis telekomunikačních zařízení

Navazující živností je dle přílohy č.3 k nařízení vlády č. 469/2000 Sb. Obsahově náplně vázaných živností:

**Skupina 205: Elektrické stroje a přístroje - Montáž, údržba a servis telekomunikačních zařízení**

Montáž, údržba a servis zařízení pro vysílání, přenos a příjem informací jakéhokoli druhu po vedení radiovými, optickými či jinými prostředky využívajícími elektromagnetických vln. Základními skupinami telekomunikačních zařízení jsou zejména....., speciální telekomunikační zařízení (*klasické signálové rozvody a zařízení, komunikátory pro poplachové systémy*), vysílací a přijímací rádiová zařízení (... ,rádiová přenosová zařízení pro poplachové systémy, ..)

Požadována je **odborná způsobilost** podle § 27 odst. 1 a 2 živnostenského zákona ve znění zákona č. 356/1999Sb. a 167/2004Sb. dle **§ 8 vyhl. č. 50/1978 Sb.**, o odborné způsobilosti v elektrotechnice, nebo doklady podle § 19 odst. 1 písm. a zákona č. 18/2004 Sb. o uznávání odborné způsobilosti.

### 4.1.3.4 Montáž, opravy, revize a zkoušky vyhrazených elektrických zařízení

Skupina 205: Elektrické stroje a přístroje - Montáž, opravy, revize a zkoušky vyhrazených elektrických zařízení

Montáž, opravy, zkoušky a veškeré revize elektrických zařízení (provozovaných na napětí od 50V) občanské, průmyslové a zemědělské výstavby.....a pevných zařízení elektrické trakce. Provádění elektroinstalací, montážní dozor a ověřovací zkoušky navržených soustav, sítí, obvodů a instalací. Údržba veřejného osvětlení.

Požadovaná **odborná způsobilost** - Oprávnění [§ 6c odst. 1 písm. b) zákona č. 174/1968 Sb., ve znění pozdějších předpisů, nebo § 8a odst. 6 písm. a) zákona č. 61/1988 Sb., ve znění pozdějších předpisů]

*Poznámka - Tato živnost připadá v úvahu v souvislosti s prováděním výchozí a pravidelných revizí elektrických instalací. Podmínkou je základní koncesovaná živnost dle 4.1 nebo spolupráce s držitelem koncesované živnosti dle 4.1.*

### 4.2 Elektrická požární signalizace

#### 4.2.1 Projektování EPS

Projektovou dokumentaci mohou zpracovávat fyzické nebo právnické osoby, které mají některou z následujících živností:

##### 4.2.1.1 Projektová činnost ve výstavbě

– jedná se o vázanou živnost dle zákona č.455/1991 Sb. ve znění pozdějších oprav a novel – skupina 213 - Stavebnictví

Podmínkou je odborná způsobilost - Autorizace v příslušném oboru podle zákona č.360/1992 Sb., o výkonu povolání autorizovaných architektů a o výkonu povolání autorizovaných inženýrů a techniků činných ve výstavbě v platném znění, nebo splnění podmínek stanovených v § 34 téhož zákona. V našem případě se jedná o autorizaci v oboru „Technika prostředí staveb – specializace elektrotechnická zařízení“.

Předpokladem získání autorizace je samozřejmě příslušné odborné elektrotechnické vzdělání, předepsaná praxe a způsobilost v elektrotechnice, tj. §10 vyhl.50/78 Sb – samostatné projektování, nebo řízení projektování.

Fyzická osoba vykonává tuto živnost přímo, právnická osoba vykonává tuto živnost prostřednictvím takto kvalifikované osoby, která musí být pracovně-právním vztahu s touto právnickou osobou.

Takto kvalifikovaná fyzická nebo právnická osoba může sama zpracovávat projektovou dokumentaci ve stupni **územního plánování, stavebního řízení i realizace stavby** v investiční výstavbě. Pokud autorizovaná osoba nemá příslušnou specializaci, musí ke zpracování projektové dokumentace přizvat autorizovanou osobu s příslušnou specializací.

Takto kvalifikovaná osoba může samozřejmě zpracovávat projektovou dokumentaci i u staveb, které nepotřebují dle § 56 zákona 50/1976 Sb. stavební povolení a nemají ani ohlašovací povinnost vůči stavebnímu úřadu. (opravy vnitřních instalací).

##### 4.2.1.2 Projektování elektrických zařízení

– jedná se o volnou živnost dle zákona č.455/1991 Sb. ve znění pozdějších oprav a novel .

Předpokladem je samozřejmě příslušné odborné elektrotechnické vzdělání a způsobilost v elektrotechnice, tj. §10 vyhl.50/78 Sb – samostatné projektování, nebo řízení projektování.

Takto kvalifikovaná osoba může zpracovávat projektovou dokumentaci u staveb, které nepotřebují dle § 56 zákona 50/1976 Sb. stavební povolení a nemají ani ohlašovací povinnost vůči stavebnímu úřadu (opravy vnitřních instalací).

Ovšem pozor! Pokud se jedná o opravu v objektu, který je kulturní památkou - je i zde ohlašovací povinnost. Pokud je ale oprava instalací prováděna v rámci změny uží-

vání stavby a je kvalifikována jako změna stavby dle §55 zákona 50/1976 Sb. – je zde dokonce povinnost povolení stavby ve stavebním řízení.

V takových případech, jakož i u všech dalších případů staveb v investiční výstavbě, může takto kvalifikovaná osoba zpracovávat jen dílčí části projektové dokumentace jako subdodávku pro osobu autorizovanou, nebo si autorizovanou osobu s příslušnou kvalifikací může přizvat ke zpracování takové dokumentace.

Při zpracovávání projektu EPS osobami, kvalifikovanými dle 4.2.1.1 a 4.2.1.2 je rovněž vyžadováno potvrzení o absolvování školení u výrobce nebo distributora techniky, která je navržena v projektovaném systému. Požadavek na absolvování školení u výrobce nebo distributora vyplývá z rychlého rozvoje techniky EPS.

Při projektování systémů EPS, jejich následující montáži a uvádění do provozu musíme mít na paměti zejména následující ustanovení vyhlášky 246/2001 Sb. a musí být splněny v nich uvedené požadavky. Vyhláška vymezuje pojem **vyhrazené požárně bezpečnostní zařízení**. - Za vyhrazené požárně bezpečnostní zařízení se považuje i **Elektrická požární signalizace** (§4 odst. 3, písmeno a).

Požadavky na projektování, montáž, kontrolu, údržbu a opravy požárně bezpečnostních zařízení (ve smyslu jmenované vyhlášky) jsou uvedeny dále:

### **4.2.2 Projektování požárně bezpečnostních zařízení**

§5 odst. 1 – Při **projektování** požárně bezpečnostních zařízení se postupuje podle normativních požadavků (**například ČSN 73 0875 pro navrhování elektrické požární signalizace**. - příslušné normy jsou tedy dle legislativního požadavku závazné).

§5 odst.5 – **Projektování** vyhrazených požárně bezpečnostních zařízení podle odst.1 se zabezpečuje prostřednictvím osoby způsobilé pro tuto činnost, která získala oprávnění k projektování podle **zvláštního předpisu (zákon č. 360/1992 Sb. o výkonu povolání autorizovaných inženýrů a techniků ve výstavbě)**.

§5 odst.6 Je-li podmínkami stavebního povolení stanoveno předložení **podrobnější dokumentace** podle zvláštního předpisu, musí být splněny požadavky uvedené v§10 odst.2.

§5 odst. 7 – V případě souběhu dvou a více vzájemně se ovlivňujících bezpečnostních zařízení **zabezpečuje koordinaci zpracovatel požárně bezpečnostního řešení stavby**.

#### **4.2.2.1 Montáž požárně bezpečnostních zařízení**

§6 odst. 1 – Při montáži zařízení EPS musí **být dodrženy podmínky vyplývající z ověřené projektové dokumentace**, popřípadě podrobnější dokumentace a **postupy stanovené v průvodní dokumentaci výrobce**.

§6 odst. 2 – **Osoba, která provedla montáž požárně bezpečnostního zařízení potvrzuje písemně splnění požadavků uvedených v odstavci č. 1.**

#### **4.2.2.2 Provoz, kontrola, údržba a opravy požárně bezpečnostních zařízení**

Musí vždy probíhat v souladu s ustanoveními §7 a §8 vyhlášky. Doklad o kontrole provozuschopnosti zařízení dle **§7 odst.8** je možné spojit s písemným vyjádřením dle **§6 odst.2** – viz příloha 1a.

#### **4.2.2.3 Společné požadavky na projektování, montáž a kontrolu provozuschopnosti**

§10 odst1 – Při projektování, montáži a kontrole provozuschopnosti vyhrazených požárně bezpečnostních zařízení, jakož i při provádění kontrol, údržbě a opravách **musí osoba, která tuto činnost provádí splnit podmínky stanovené právními předpisy, normativními požadavky a provodní dokumentací výrobce konkrétního typu požárně bezpečnostního zařízení.**

§10 odst. 2 – osoba, která příslušnou činnost podle odstavce 1 provedla, **odpovídá za kvalitu provedené činnosti a písemně potvrzuje, že při tom splnila podmínky stanovené právními předpisy, normativními požadavky a průvodní dokumentací výrobce konkrétního typu požárně bezpečnostního zařízení.** – např. viz příkloha č.1b

# ***Mechanické zábranné systémy***

*Ladislav Toms*

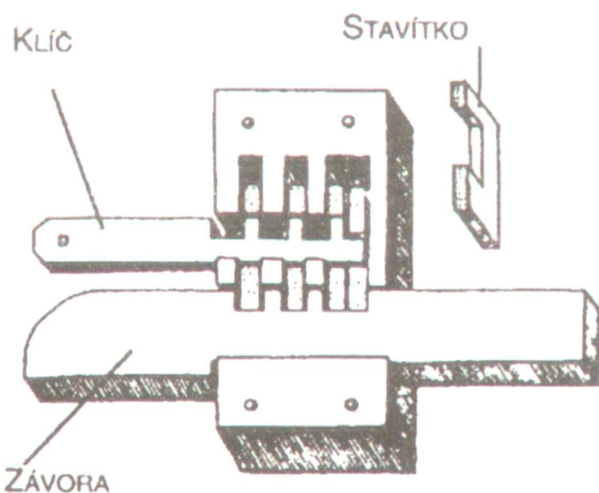
## **OBSAH:**

<b>1 Stručný historický úvod .....</b>	<b>39</b>
<b>2 Charakteristika mechanických zábranných systémů (MZS) .....</b>	<b>40</b>
2.1 Stupeň pasivní (průlomové) odolnosti .....	40
<b>3 Rozdělení mechanických zábranných systémů (MZS) .....</b>	<b>43</b>
3.1 Prostředky obvodové ochrany .....	43
3.2 Prostředky objektové ochrany .....	48
3.3 Prostředky individuální ochrany.....	55

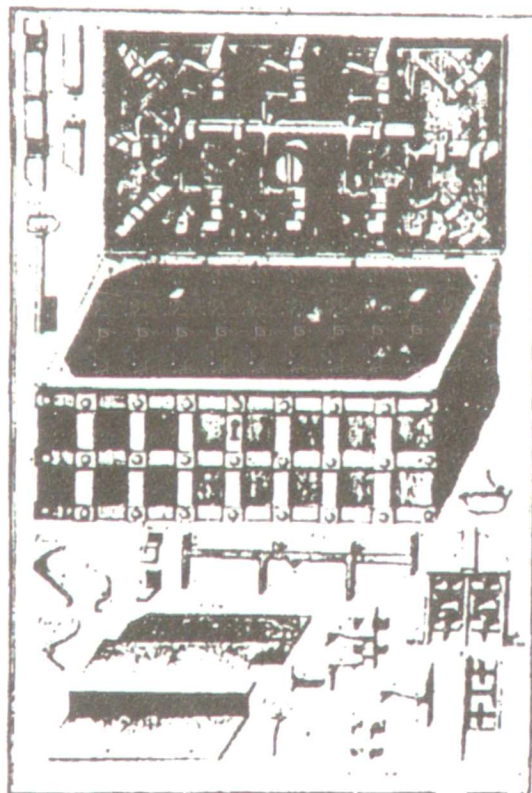


## 1 Stručný historický úvod

Prioritní postavení mechanických zábranných systémů vyplývá logicky z historického vývoje světové techniky. Zcela nepochybně vládly světu napřed mechanické principy jako je páka, zarážka apod., využívající tehdejší technologické materiály a to především dřevo a kámen a teprve později nalezené a zpracované kovové materiály. Využívání principů elektřiny a jiných fyzikálních jevů uskutečnilo lidstvo až v novověku, kdy dovedlo používat zařízení na principech elektřiny, eventuálně jiných fyzikálních principů jako např. magnetismu, optiky a dalších. Mechanické pomůcky a zařízení se postupně objevovaly nejprve v centrech světových kultur, tak jak historicky vznikaly a zanikaly a z nich se pomalu šířily do ostatních civilizovaných částí světa. Vznik mechanických zábran byl vynucen silnými požadavky na ochranu nejprve vlastního života a později i majetku. Tak vznikala a vyvíjela se ochrana osad a obydlí: ploty, ohrady, příkopy, hradby, ochrana vstupů – dveře, ochrana okenních otvorů, skříně, truhlice a konečně zámků a klíčů. Svědky těchto skutečností jsou jednak písemné zmínky ve starých záznamech ale i archeologické nálezy, i když se jich zachovalo velice málo (díky základnímu výrobnímu materiálu – dřevu). Pro profesi bezpečnostních zábran je důležitý vývoj zámkařské techniky, datované od dob řecké a římské kultury. Nejbouřlivější vývoj nastal až v 18. a 19. století, vývojem precizních zámků a úschovných objektů a ve 20. století, kdy se k mechanice připojila i elektronika. V průběhu vývoje zabezpečovací techniky vznikl samostatný obor zabezpečovací techniky, združující tři sektory: výrobu a rozvoj prostředků, montáž a instalaci, údržbu. Vývoj mechanických zábranných systémů (používá se zkratka MZS) nám ozřejmí názorná ukázka uzamykacích mechanismů od zásuvných (většinou dřevěných) zámků až po klíčové otočné systémy:



Obr. 2-1: Dřevěný zámek egyptského typu se zásuvným klíčem z let 1500 př.n.l. (ještě dnes tento typ zámku můžeme spatřit v Evropě na dveřích zemědělských usedlostí).



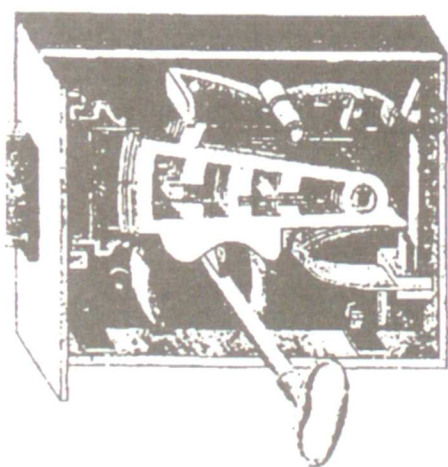
Obr. 2-2: Zabezpečovací souprava středověké železné pokladnice asi ze 16. století – obdobně lze spatřit v depozitářích některých českých hradů a zámků.

## 2 Charakteristika mechanických zábranných systémů (MZS)

### 2.1 Stupeň pasivní (průlomové) odolnosti

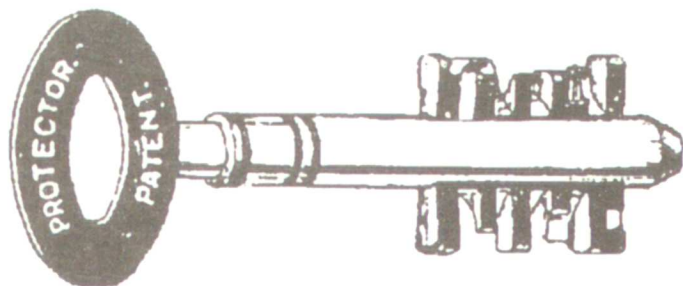
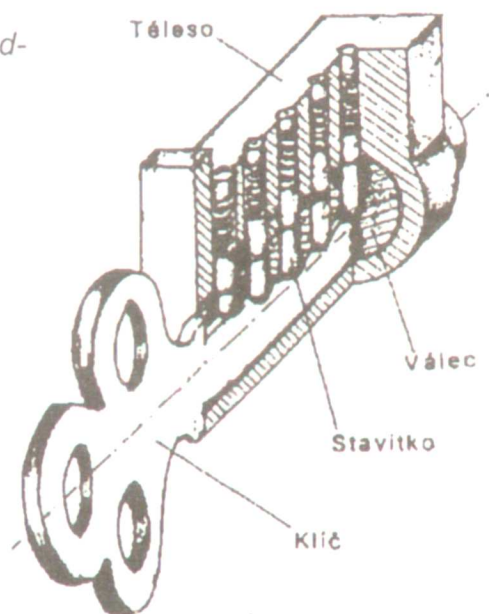
Každý mechanický zábranný systém je překonatelný v určitém reálném čase. Úkolem zabezpečovací techniky je posunout tento časový termín do pásma bezpečnosti, tzn. do doby, kdy ohrožený zábranný systém je již pod další, například fyzickou kontrolou. Hodnota času pro překonání MZS záleží na několika parametrech:

- kvalitě MZS,
- znalosti konstrukce překonávaného zařízení,
- umístění (instalace) MZS,
- druhu a kvalitě použité techniky (nástrojů) pro překonání MZS,
- možnost použití vedlejších energetických zdrojů (zásuvky el. proudu apod.).



Obr. 2-3: Kovový vícestavítkový zámek s otočným klíčem z roku 1820 – konstrukce Chubb vychází z původní konstrukce zámku typu Barron z r. 1780.

Obr. 2-4: Bezpečnostní dveřní cylindrická vložka typu AYLE z roku 1850.



Obr. 2-5: Klíč k bezpečnostnímu trezorovému zámku typu KROMER z r. 1870.



Vlastní stupeň pasivní odolnosti (což je vyjádření příslušné výše bezpečnostní úrovně objektu) vyjadřuje vztah maximálního prodloužení časového intervalu  $t$ , který je potřebný pro překonání bezpečnostního zařízení (používá se rovněž výraz: průnik do oblasti chráněného zájmu).

$$\Delta t = t_2 - t_1 \quad [\text{min.}], \quad \text{kde } \Delta t - \text{časový interval potřebný k překonání překážky} = \text{odporový čas,}$$

$t_2$  – čas zahájení práce na překonání zábrany,  
 $t_1$  – čas ukončení překonání zábrany.

### 2.1.1 Stanovení doby průlomové odolnosti

Jedná se o stanovení minimální doby průlomové odolnosti, podle charakteru MZS, zda se jedná o otvorové výplně nebo úschovné objekty.

#### a) minimální doba průlomové odolnosti pro otvorové výplně

Jedná se o dveře, okna, balkónové dveře, mříže, vrata apod. Minimální čas potřebný pro překonání je uveden v tabulce 2-1, podle norem ČSN P ENV 1627 a ČSN P ENV 1630. Tento čas je přiřazen podle bezpečnostních tříd (BT) a stanoven empiricky podle předpokládaného způsobu napadení.

Tabulka 2-1: Bezpečnostní třídy a odporový čas otvorových výplní

Bezpečnostní třída	Kategorie nářadí	Předpokládaný způsob napadení	Odporový čas (min)
1	nepoužívá se	Příležitostný zloděj zkouší rozbít okno, dveře nebo okenice užitím fyzického násilí, např. kopáním, naražením ramenem, zdviháním, vytrháváním.	Neměřen
2	A	Příležitostný zloděj dále zkouší rozbít okno, dveře nebo okenice užitím jednoduchých nástrojů, např. šroubováku, kleští, klínu.	3
3	B	Zloděj zkouší zajistit přístup použitím dalšího šroubováku a páčidla.	5
4	C	Zkušený zloděj dále používá pily, kladiva, sekery, sekáče a přenosné akumulátorové vrtačky.	10
5	D	Zkušený zloděj dále používá elektrické nářadí, např. vrtačku, přímočarou pilu, úhlovou brusku o průměru kotouče maximálně 125 mm.	15
6	E	Zkušený zloděj dále používá výkonné elektrické nářadí např. vrtačku, přímočarou pilu a úhlovou brusku o průměru kotouče max. 230 mm.	20

#### b) minimální doba průlomové odolnosti pro úschovné objekty

Zde se jedná o plechové skříně, mobilní i stabilní trezory, přenosné objekty apod. Minimální doba průlomové odolnosti se stanoví výpočtem při použití bezpečnostních tříd pro klasifikaci skříňových trezorů a hodnot průlomové odolnosti (v odporových

jednotkách RU, stanovených zkouškami typového výrobku) – viz tabulka 2-2, podle ČSN EN 1143-1. Minimální doba průlomové odolnosti je dána vztahem:

$$T = [(V_R - B_V) : C_1 > 1]$$

$T$  – doba min. průlomové odolnosti  
 $V_R$  – hodnota průlomové odolnosti v RU, dle charakteru částečného nebo úplného průlomu,  
 $B_V$  – základní ohodnocení použitého nářadí  
 $C_1$  – koeficient – viz tabulku 2-3

Pro stanovení **optimální doby průlomové odolnosti** je nutné výslednou hodnotu  $T$  násobit koeficientem (2 až 3) – koeficient praktického navýšení  $T_{opt} = T \cdot (2-3)$

Tabulka 2-2: Minimální požadavky pro klasifikaci skříňových trezorů do BT

Bezpečnostní třída	Zkouška napadení		Pevnost ukotvení <sup>1)</sup>	Zámky		Doplňkový požadavek pro označení EX <sup>3)</sup>
	Hodnoty průlomové odolnosti		Požadovaná síla	Množství	Třída podle EN 1300	Hodnota průlomové odolnosti po výbuchu
	částečný průlom	úplný průlom				
	RU	RU	kN			RU
0	30	30	50	1	A	2)
I	30	50	50	1	A	2)
II	50	80	50	1	A	4
III	80	120	50	1	B	6
IV	120	180	100	2	B	9
V	180	270	100	2	B	14
VI	270	400	100	2	C	30
VII	400	600	100	2	C	30
VIII	550	825	100	2	C	41
IX	700	1050	10	2	C	53
X	900	1350	100	2	C	68

<sup>1)</sup> použitelné pouze pro mobilní trezory o hmotnosti menší než 1000 kg

<sup>2)</sup> označení EX není možné pro třídy 0 a I

<sup>3)</sup> pro označení EX musí skříňové trezory, trezorové dveře a komorové trezory (s dveřmi nebo bez nich) odpovídat hodnotě průlomové odolnosti v souladu s uvedenými tabulkami. Jejich prostupy pro kabely musí být konstruovány takovým způsobem, aby jimi nebylo možné zavést výbušninu (např. rozbušku nebo nálož) do vnitřních prostorů.

Tabulka 2-3: Koeficienty průlomové odolnosti  $C_1$ 

Bezpečnostní třída úschovného objektu podle ČSN EN 1143-1	Koeficient RU/min $C_1$
0 - I	5
II - III	7,5
IV - VII	10
VIII - XI	15
XII - XIII	35

**Identifikace BT v praxi:**

Současná normová základna rozlišuje dva druhy bezpečnostních tříd (BT) a navíc se připojuje i klasifikace Národního bezpečnostního úřadu (NBÚ).

- **úschovné objekty** – bezpečnostní třídy jsou označovány římskými číslicemi **BT 0 – X (resp. XIII)**
- **ostatní MZS** – bezpečnostní třídy jsou označeny arabskými číslicemi **BT 1 – 6**
- **stupně utajení NBÚ: vyhrazené – důvěrné – tajné – přísně tajné**

**3 Rozdělení mechanických zábranných systémů (MZS)**

Mechanickými zábrannými prostředky se rozumí zejména prostředky pro ohraničení prostor, vstupní bezpečnostní systémy dveří a oken, mříže, bezpečnostní skla a fólie a vlastní uzamykací systémy.

Vzhledem ke skutečnosti že MZS patří do širší problematiky bezpečnostního zabezpečení, můžeme MZS rozdělit zhruba do tří oblastí:

- 1) **Prostředky obvodové ochrany** – jedná se o prostředky zajišťující bezpečnost vyhrazeného území a prostor kolem chráněného objektu.
- 2) **Prostředky objektové ochrany** – tyto prostředky zabraňují nepovolanému přístupu do objektů. Někdy se používá i názvů plášťová či obvodová ochrana.
- 3) **Prostředky individuální ochrany** – tím se míní přenosné i nepřenosné technické prostředky používané v předchozích dvou oblastí, ale i další prostředky jako jsou vlastní zámky, trezory, přenosové prostředky apod.

**3.1 Prostředky obvodové ochrany**

Jedná se o skupinu vnějších mechanických zábran, které nejsou přímou součástí vlastního objektu (budova, místnost, dveře apod.), ale naopak jsou od něho prostorově vzdálené. Jsou na volné ploše, většinou na parcele objektu, a mnohdy vytvářejí nejen fyzickou, ale i právní hranici pozemku.

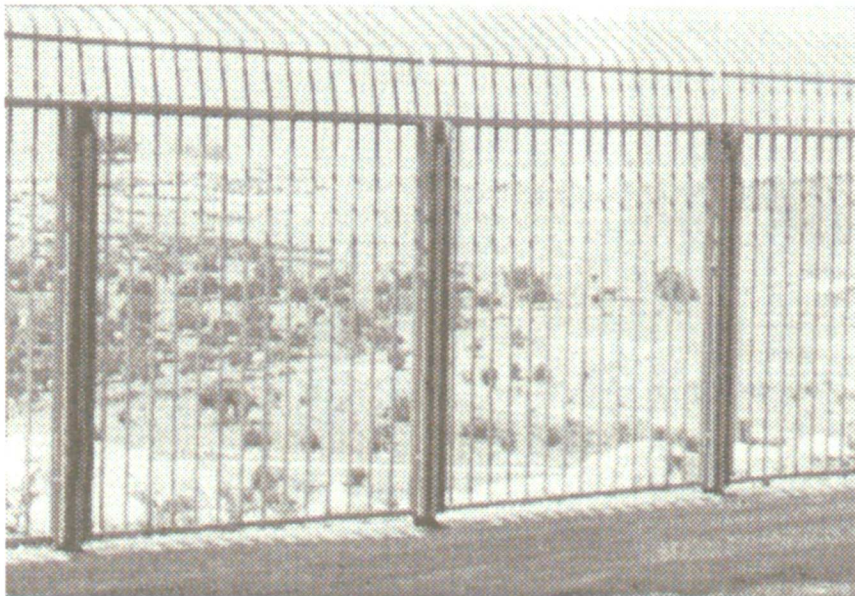
Hlavními představiteli těchto ochranných zábran jsou ochranné zdi a ploty. S oběma souvisí používání dalších prvků, které musí být zabezpečeny: dveře, vrata, branky a v některých případech i závory, průchody a turnikety. Všechny tyto prvky jsou stabilně uloženy, ale mohou se použít i přenosné zábrany – zátarasy.

### 3.1.1 Zdi

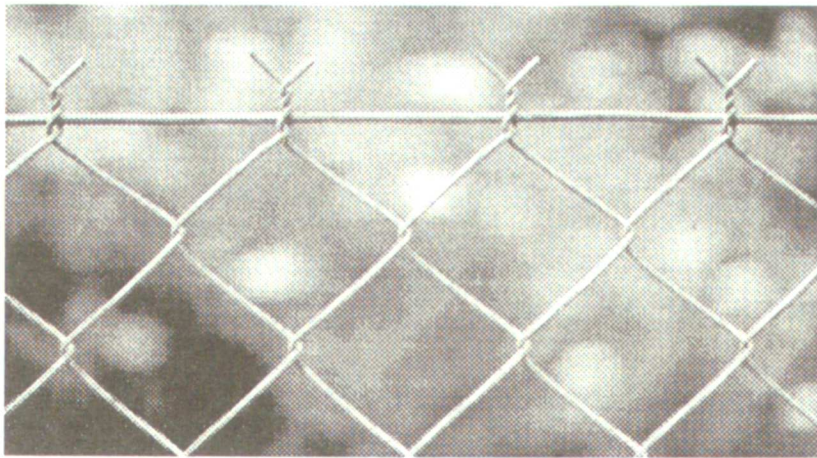
Aby zeď jako bariéra čelila průniku do chráněné zóny musí znesnadnit, ne-li zabránit přezení, podlezení, eventuálně podhrabání. Zeď musí být pevná, bytelná, s minimální výškou 2,5m a musí stát na podezdívce.

### 3.1.2 Ploty

Jsou proti zdím většinou s volnými mezerami („průhledné“) a když pomíneme dřívější ohrady z prken, jsou moderní ploty tvořeny pevnou nosnou konstrukcí se sloupky zajištěnými proti vyvrácení a s výplní většinou z drátěného pletiva. Pletivo, nosná železná konstrukce, napínací dráty a ostatní kovové prvky musí být povrchově ošetřeny proti působení povětrnosti. Dráty mohou být opatřeny i potahem z umělé hmoty. Pokud se při montáži použije řezání či svařování dílů, musí být tyto plochy dodatečně natřeny antikorozním nátěrem. Pletivo musí být ze silného drátu – průměr bývá minimálně 3 mm a velikost ok je 40 až 50 mm. Rozteč nosných sloupků je odvislá od výšky plotu, např. pro pletivo o výšce 3 m se doporučuje rozteč 3 m, přičemž sloupky na konci jednotlivých zón musí být podepřeny výztuhami.



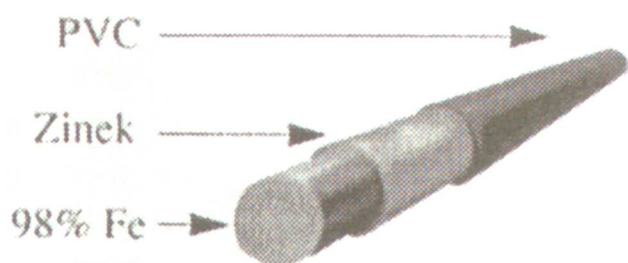
Obr. 2-6: Plot z profilovaného železa.



Obr. 2-7: Detail drátěného pletiva.



Obr. 2-8: Napínací element plotu.

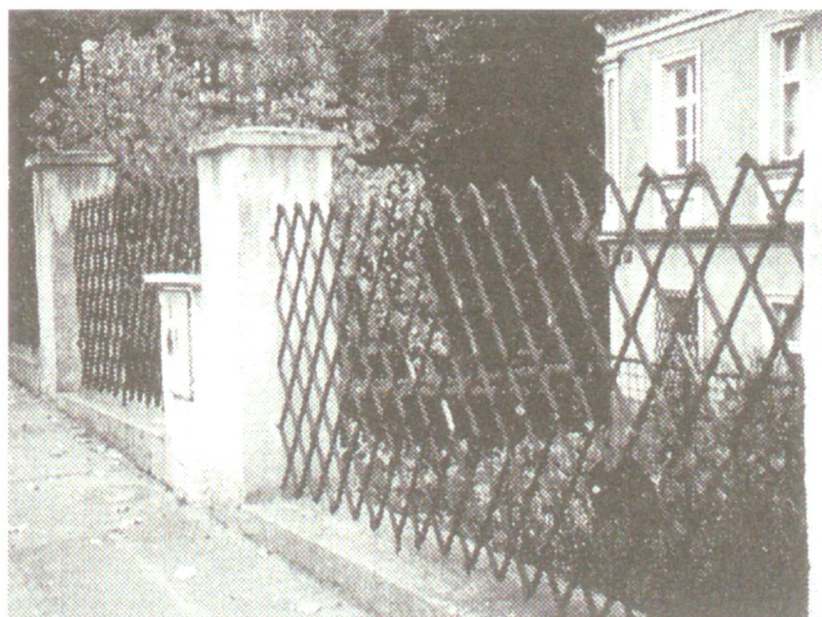


Obr. 2-9: Průřez drátu plotu s umělým povlakem.

### 3.1.3 Průchozí prvky zdí a plotů

Mezi nejdůležitější patří **dveře, vrata, branky**. Tyto prvky musí být pevně a bezpečně usazeny do zdí a plotů. To znamená, že musí mít tuhou konstrukci, pevné uchycení a bezpečný uzamykací systém. Zásady pro jejich konstrukci a uchycení platí podle specifikace vstupních dveří uvedené v další kapitole. Jistým specifíkem jsou vrata, hlavně dvoukřídlá, která se musí zajišťovat proti vyvrácení a tzv. vyháčkování. Platí to i pro garážová vrata, i když moderní mají konstrukci jednokřídlovou s vyklápěním směrem nahoru. Ke speciálním propustím patří **turnikety a závory**, ale ty většinou nedosahují takového stupně bezpečnosti.

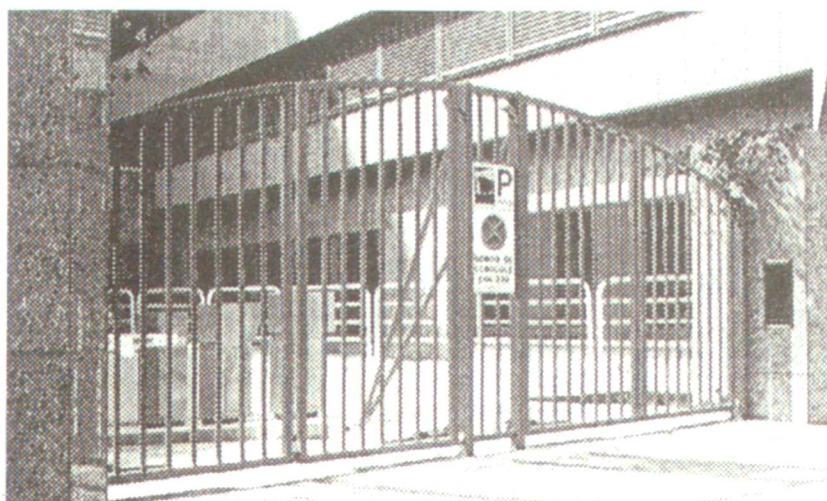
Obr. 2-10: Plot ze železných profilů.



### 3.1.4 Vrcholová ochrana

Představuje ochranu na vrcholu zdi či plotu. Mezi takovou ochranu patří

- a) konstrukce z ostnatého drátu,
- b) konstrukce z tzv. žiletkového drátu,
- c) pevné hroty na vrcholu plotů či zdí.



Obr. 2-11: Otočná skládací vrata.



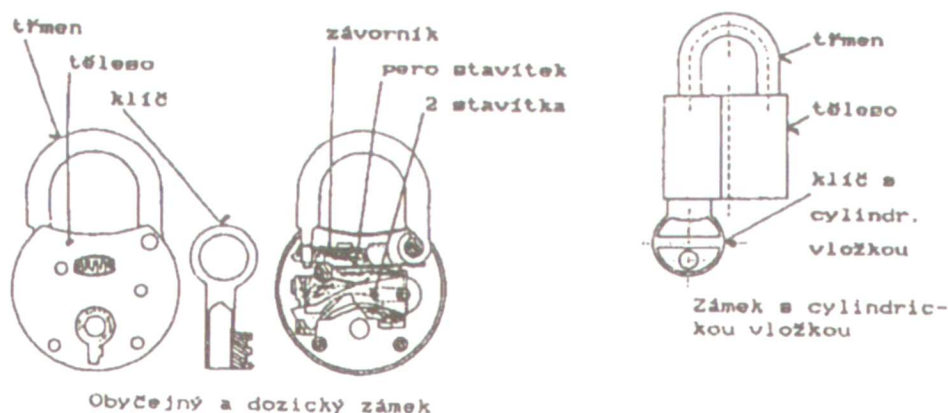
Obr. 2-12: Vrcholová zábrana žiletkovým drátem.

### 3.1.5 Visací zámky a petlice

I když se jedná o samostatné zabezpečovací prostředky, patří nejméně z poloviny do souboru zabezpečení prostorové ochrany, protože řada dveří vrat a branek je opatřena právě visacím zámekem a petlicí. Používají se však i k uzavírání skříní, jízdních kol apod. Visacím zámekům se rovněž říká zámky závěsné a řidčeji přenosné. Visací zámky se rozdělují podle funkčního hlediska na **zámky se zásuvným klíčem** (klíč zasunutím uvolní zábranu závory) a **zámky s otočným klíčem** (klíč po zasunutí do zámku se otáčí kolem své osy buď částečně – uvolní závorník a nebo celou otáčkou – posouvá závoru). Další rozdělení je podle závěsného dílu a pak se visací zámky dělí na zámky **se svorníkem** a zámky **se třmenem**. Svorník se při otevřeném zámku vždy vyjímá ale třmen se může buď také vyjmout a nebo povytáhnout a pootočit.

První dochované visací zámky jsou staré zhruba 2000 let. V českých zemích se objevují okolo 12. století. Tyto konstrukce byly římské a teprve kolem 18. století se objevují nové konstrukce z Francie a Německa. V 19. století se objevují konstrukce z Anglie a posléze i z USA s bezpečnostními uzamykacími mechanismy. Z hlediska použitého otevíracího elementu – klíče, rozeznáváme visací zámky:

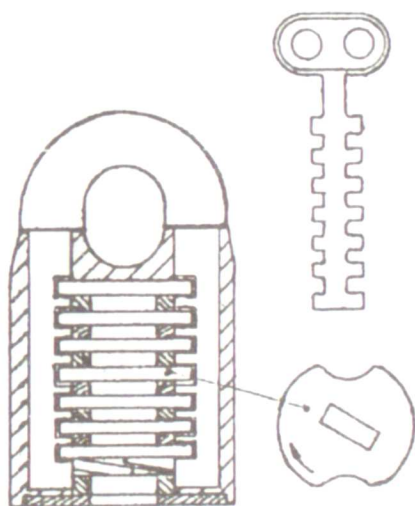
- **obyčejné** – jsou vybavené odpruženou závorkou a mohou být doplněny zábranami. Klíč má 1 plný zub a může být profilovaný.
- **dozické** – mimo závorku mají ještě plochá stavítka. Klíč má na svém zubu radiální zářezy, které odpovídají jednotlivým stavítkům. Jejich základem je Chubbova konstrukce.
- **motýlkové** – zámek obsahuje závorku a stavítka, uzpůsobená pro oboustranné vedení zubem klíče. Klíč má tedy zub na obou stranách – tvarem vytváří křídélko motýla. Samozřejmě má na obou křídélkách zářezy pro stavítka.
- **cylindrické** – správný název je s cylindrickou vložkou. Zámky mají buď válcová odpružená stavítka nad sebou nebo lamelová (kotoučová) stavítka vedle sebe. Do konstrukce zámku lze zabudovat jakoukoliv cylindrickou vložku, tzn. i vložku s magnetickými stavítky.



Obr. 2-13: Popis jednotlivých dílů visacích zámků.

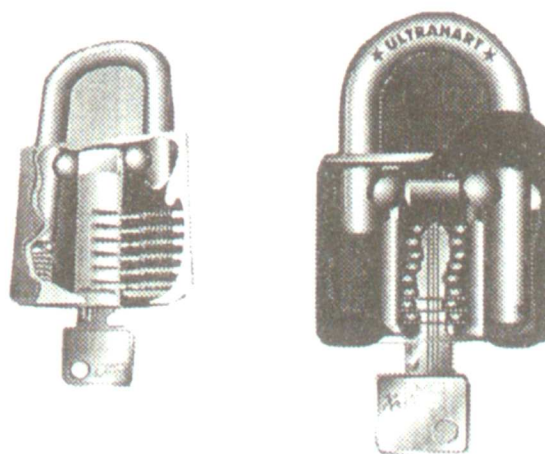
- **heslové – (kódové)** – ovládání uzamykacího systému se provádí bez klíče, natáčením heslových kotoučků umístěných z boku či zespoda zámku.

U visacích zámků je velice důležitá, ale zároveň dost obtížně splnitelná, ochrana proti násilnému napadení. Jedná se o bytelnost skříně zámku, aby odolala úderům kladiva. To platí i pro svorník nebo třmen, ale ty musí ještě odolávat řezání a štípání, musí tedy být přiměřeně silné a povrchově tvrzené. Rovněž tak je důležité zabránit nedovolenému přístupu ke třmenu, což se děje úpravou tvaru skříně zámku, anebo častěji tvarem použitých petlic.

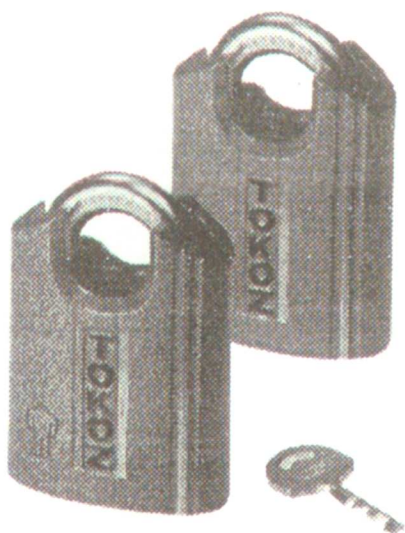


Obr. 2-14: Visací zámek s kotoučovými stavítky.

Obr. 2-15: Zámky s cylindrickou vložkou  
a) válcová stavítka  
b) lamelová stavítka.



Obr. 2-16: Bezpečnostní visací zámek s ochranou třmenu.



**Petlice** – je nezbytnou součástí většiny uzamykacích systémů, kde je použit visací zámek. Bezpečné petlice jsou vyráběny z kvalitní legované oceli a plní mimo funkce spojení pohyblivé části dveří nebo okna s nepohyblivou částí rovněž funkci ochrany visacího zámku. Pokud se týká přichycení petlic, je lepší z hlediska vypáčení petlice přichycovat ji pomocí průchozích šroubů než pouhými vruty do dřeva.

### 3.2 Prostředky objektové ochrany

Jedná se o zabezpečení vstupu do všech stavebních otvorů v objektu: dveří, oken, balkónových oken, sklepních oken, vikýřů, zásobovacích a energetických šachet apod.

#### 3.2.1 Dveře

Dveřní prostor je nejdůležitějším stavebním otvorem a je tvořen dvěma celky s doplňky: zárubní a dveřním křídlem. **Zárubeň** neboli rám dveří je buď dřevěný a nebo v současné době se zhotovuje z ocelových profilů a tím je bezpečnější. Důležité je správné usazení zárubně do ostění a jedna jeho stojina musí být opatřena závěsy pro nasazení a kyvný pohyb dveřního křídla. Protější stojina zárubně je opatřena zapadacím plechem (tzv. protiplechem), což je přišroubovaný díl sloužící pro zasouvání závory včetně střelky uzamykacího zámku při zamykání. U železné zárubně jsou výřezy pro závoru a střelku součástí stojiny.

**Dveřní křídlo** je nejdůležitější součástí dveřního prostoru a je tvořeno pevnou rovnou deskou, která se nesmí prohýbat. Je buď celodřevěné nebo s dřevěným rámem a překližkovým zakrytím, nebo s rámem a kazetovou výplní. Dveře vnitřních místností mohou být i prosklená, naopak dveře sklepní a dílenská mohou být oplechovaná nebo celokovová. Pro zabezpečení je důležité umístění dveří v budově a jejich funkce. Z hlediska bezpečnosti jsou nejdůležitější **vstupní dveře**.

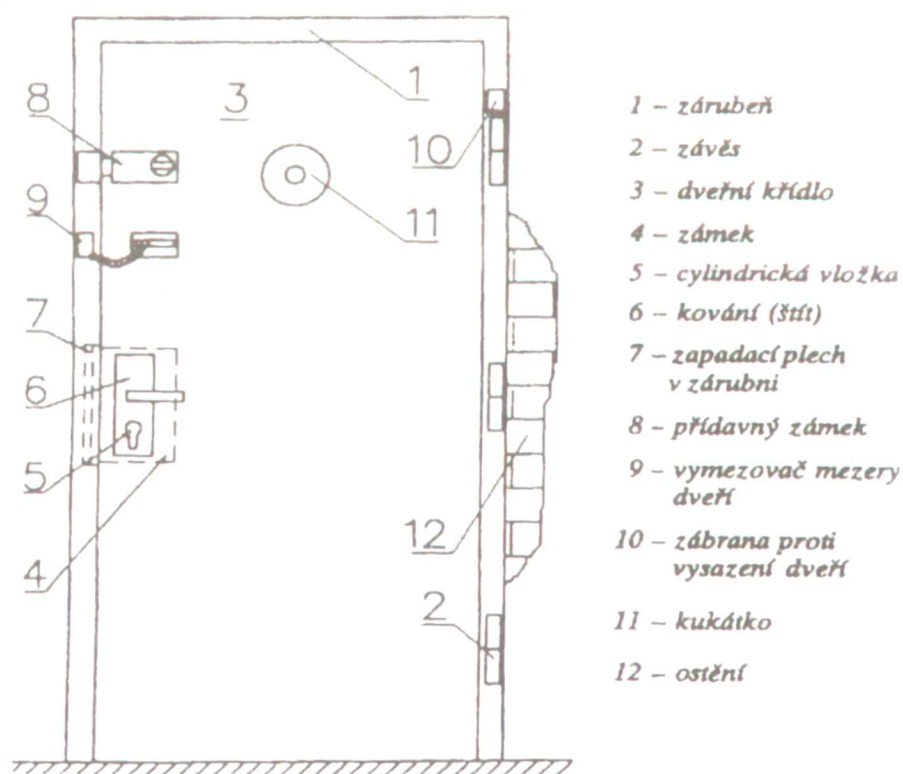
Jejich bytelnost musí zaručovat, že plochu dveří nelze prokopnout či vyvrátit. Musí být opatřeny nejlépe třemi závěsy, zajištěnými navíc tak, aby se dveřní křídlo nedalo násilně "vysadit" ze zárubně. Dalším dílem je uzamykací systém, tvořený zadlabacím zámkem s bezpečnou klíčovou sestavou a chráněný kováním. U dveří mohou být ještě přídavná zařízení jako je druhý – přídavný zámek (většinou vrchní-nezadlabaný), kukátko, vymezovač mezery pootevřených dveří, příčná závora apod. Dvoukřídlové dveře musí být zajištěné proti vyvrácení a tzv. vyháčkování.

**Dveřní zámek** – z hlediska umístění zámku na dveřním křídle rozeznáváme 2 druhy zámků:

- **zadlabací** – nejvíce používaná montáž. Zámek je ukryt uvnitř a nepřečnivá přes plochu desky křídla

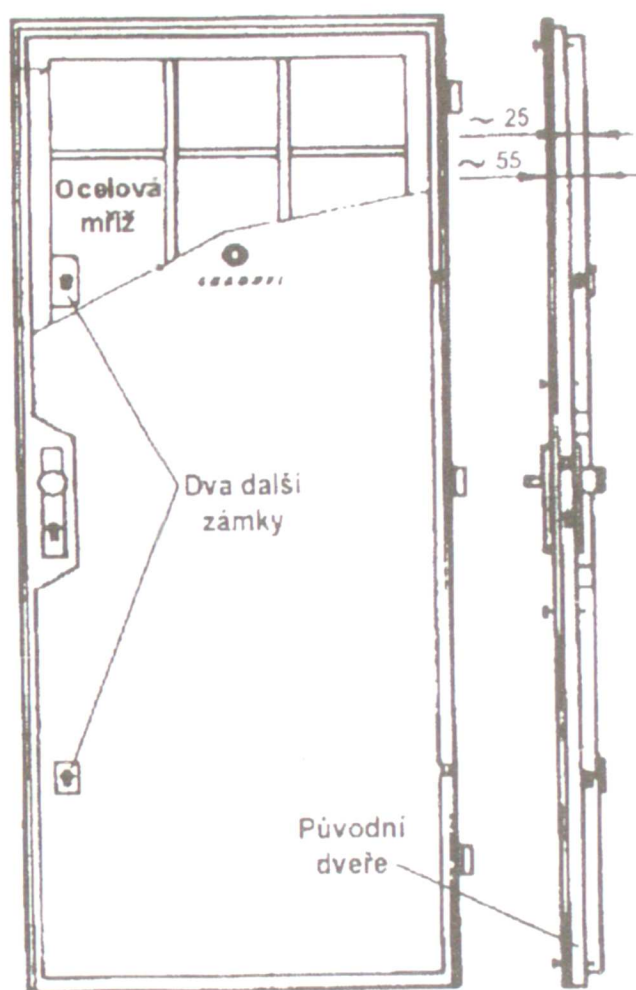
- **vrchní** – montáž se provádí na vnitřní stranu dveří a nezslabuje tloušťku dveřního křídla.

Z hlediska bezpečnosti lze zámkové systémy dělit na obyčejné a bezpečnostní. Obyčejné mají jednoduchý mechanismus, kdy klíčem s plným zubem posunujeme závoru.



Obr. 2-17: Obecný popis dveřního prostoru.





Obr. 2-18: Princip bezpečnostních dveří.

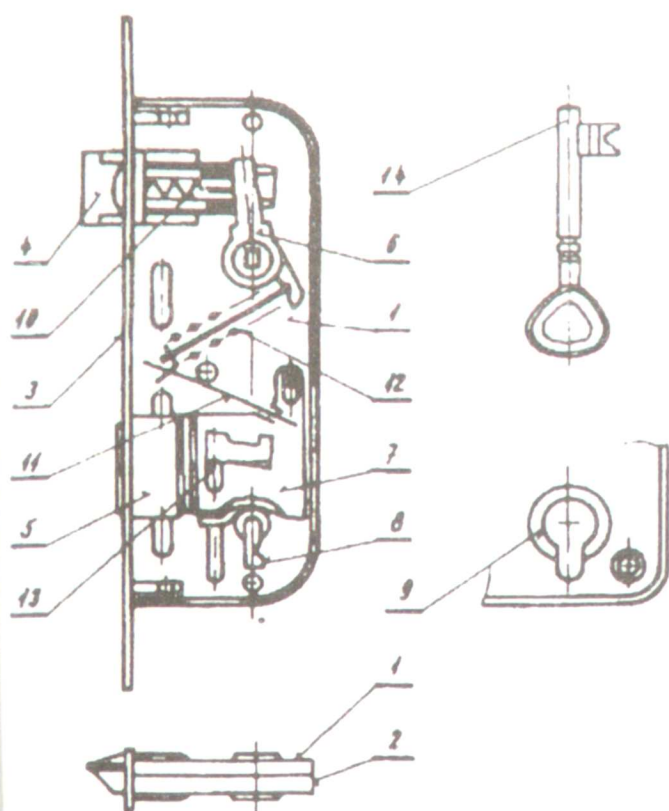
Používá se u mezipokojových dveří a dveří příslušenství. Bezpečnostní zámky mají mechanismus pro klíče dozické, motýlková ale hlavně s cylindrickou vložkou.

Ochránit dveřní zámek a jeho klíčový vstup má za úkol bezpečnostní štít odborně zvaný **vnější dveřní kování**. Pro bezpečnost je důležité, aby kování bylo na dveřní křídlo přichyceno šrouby zevnitř objektu – aby nešlo odšroubovat nebo vylomit. Pokud je použit zámek s cylindrickou vložkou, musí se vložka ochránit proti rozlomení, a to tak, že nesmí přesahovat čelní stěnu kování o více než 3 mm!

**Bezpečnostní dveře** – proti klasickému dveřnímu křídlu mají následující zvýšené bezpečnostní úpravy:

1) zvýšenou odolnost proti proražení, prořezání a páčení – konstrukce je většinou sendvičová s pevným kovovým rámem a různými výplněmi (i protipožárními),

- 2) nejméně tři bytelné závěsy,
- 3) rozšířený počet uzamykacích a zajišťujících míst po celém obvodu dveřního křídla – použitím rozvorového systému,
- 4) nejméně dva uzamykací zámky (hlavní a přídavný) vybavené všemi způsoby ochrany proti násilnému napadení,



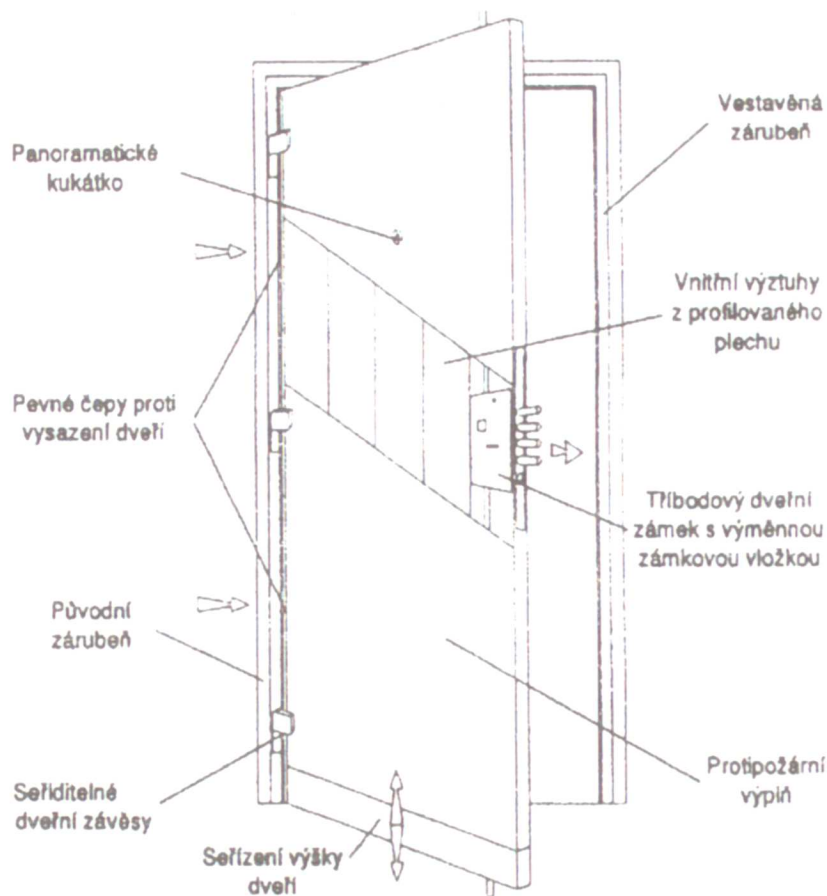
- 1 - základová deska
- 2 - krycí deska
- 3 - čelo
- 4 - stěpka
- 5 - závora
- 6 - ořech
- 7 - stavítko, závorník nebo zábrana
- 8 - otvor pro klíč
- 9 - otvor pro cylindrickou vložku
- 10 - pružina stěpky
- 11 - pružina stavítek nebo závorníku
- 12 - pružina ořechu
- 13 - čep závory
- 14 - dozický klíč

5) většina bezpečnostních dveří používá i vlastní zesílenou bezpečnostní zárubeň.

### Cylindrická vložka

Nejznámější bezpečnostní uzávěra světě má počátky již ve starém Egyptě, ale moderní podobu mu dal v roce 1865 američan Linus Yale. Od těch dob se vložka rychle rozšířila po celém světě vzhledem k malým rozměrům a velké odolnosti proti paklíčům.

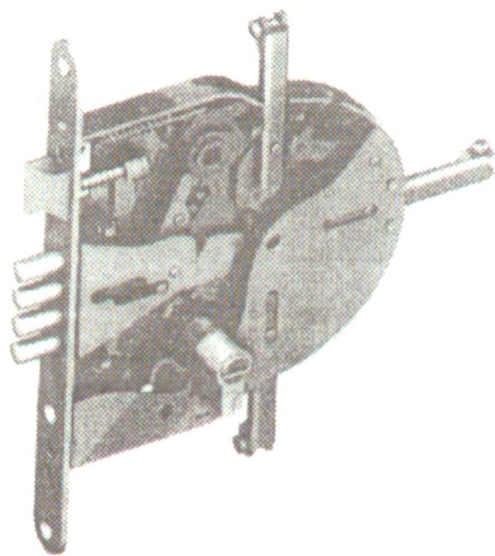
Obr. 2-19: Jednoduchý zadlabací zámek s variantou klíčového vstupu na dozický klíč nebo cylindrickou vložku.



Obr. 2-20: Základní vybavení bezpečnostních dveří.

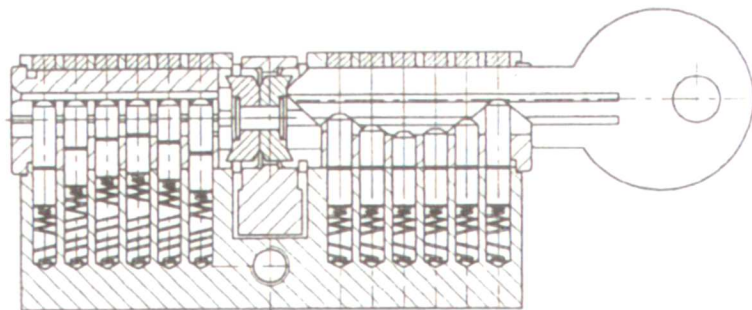
Cylindrická vložka je vlastně náhradou za klíč, protože ve své konstrukci musí mít ozub, který teprve svým otáčením posouvá vlastní závoru zámku. Celou tuto funkci nám znázorňuje obrázek 2-23: zasunutý klíč napřed umožní dosednutí stavitelky do zářezů v klíči a zároveň svou špičkou zasune spojku do otvoru v ozubu. Tím je celá sestava tuhá a při otáčení klíče se pohybuje cylinder, spojka i ozub. Ten svýmnosem posouvá vlastní závoru zámku.

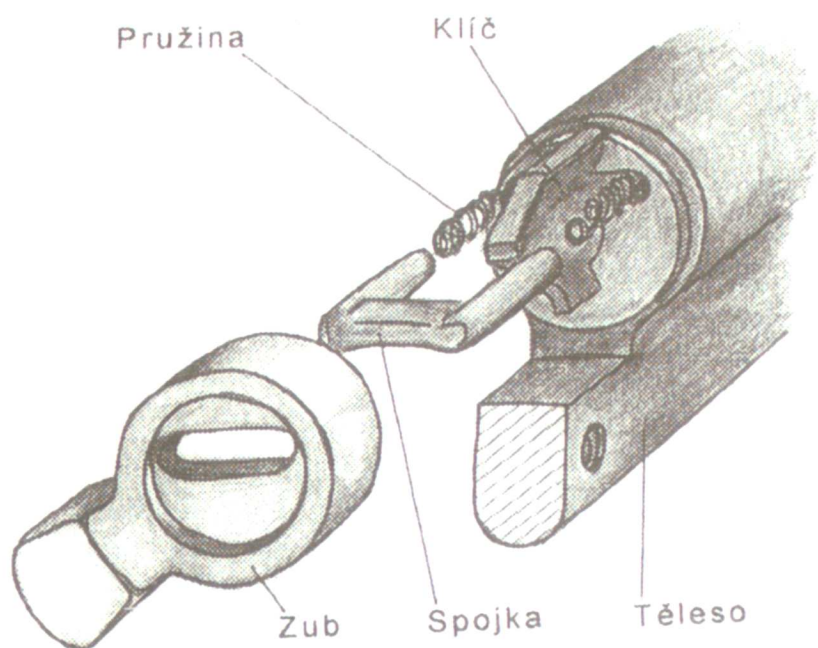
Cylindrické vložky se dělí podle mnoha hledisek. Podle tvaru tělesa vložky rozeznáváme vložky profilové (nejrozšířenější u oboustranných vložek), kruhové (používané jako jednostranné vložky), oválné, osmičkové (USA) a různé speciální profily podle způsobu použití. Podle délky vložky rozeznáváme vložky oboustranné – jdou otevírat zvenčí i zevnitř dveří a jednostranné – ote-



Obr. 2-21: Rozvorový zadlabací zámek s vysunutím závor do všech čtyř stran.

Obr. 2-22: Řez a základní názvy cylindrické vložky.

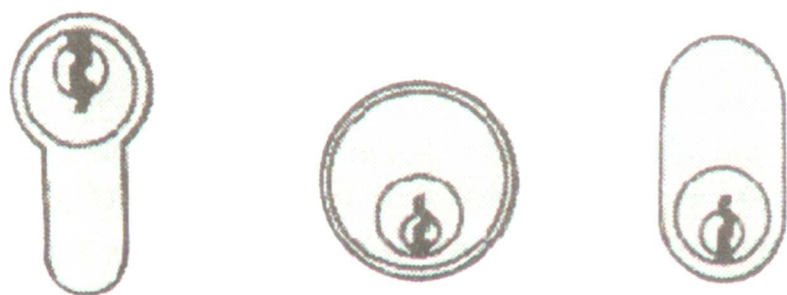




Obr. 2-23: Funkce klíče, spojky a ozubu.

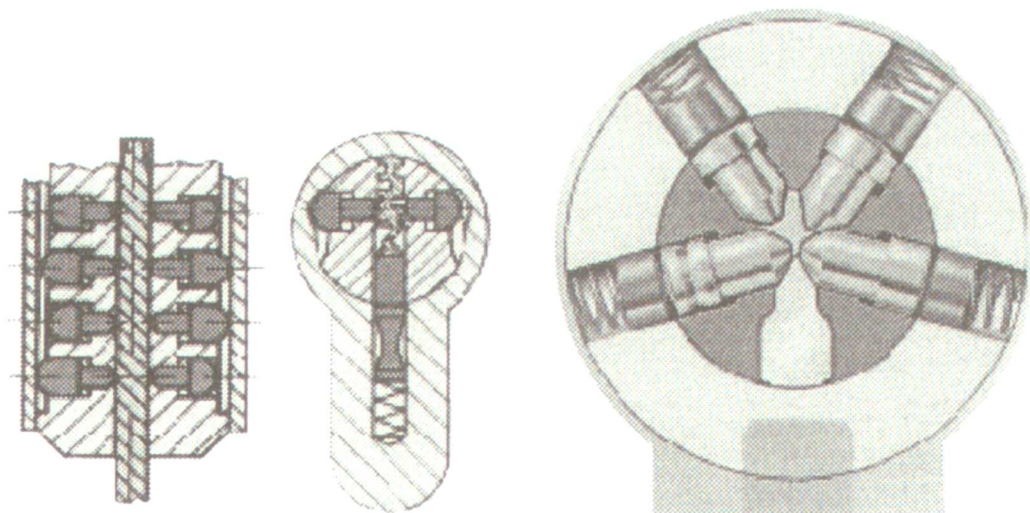
víratelné pouze z jedné strany. Podle tloušťky dveřního křídla rozeznáváme vložky symetrické a nesymetrické, které mají jednu stranu delší podle výplně dveřního křídla. Podle systému vnitřních stavítek rozeznáváme vložky mechanické (profilovaný nebo plochý klíč), magnetické a elektronické (mimo mechanického systému je pro ovládání zábrany použit elektronický čip znemožňující otáčení cylindru). Podle počtu stavítek v řadě za sebou rozeznáváme cylindrické vložky 3, 4, 5, 6 a vícestavítkové. Podle počtu řad se dělí na jednořadé, dvouřadé, třířadé a čtyřřadé.

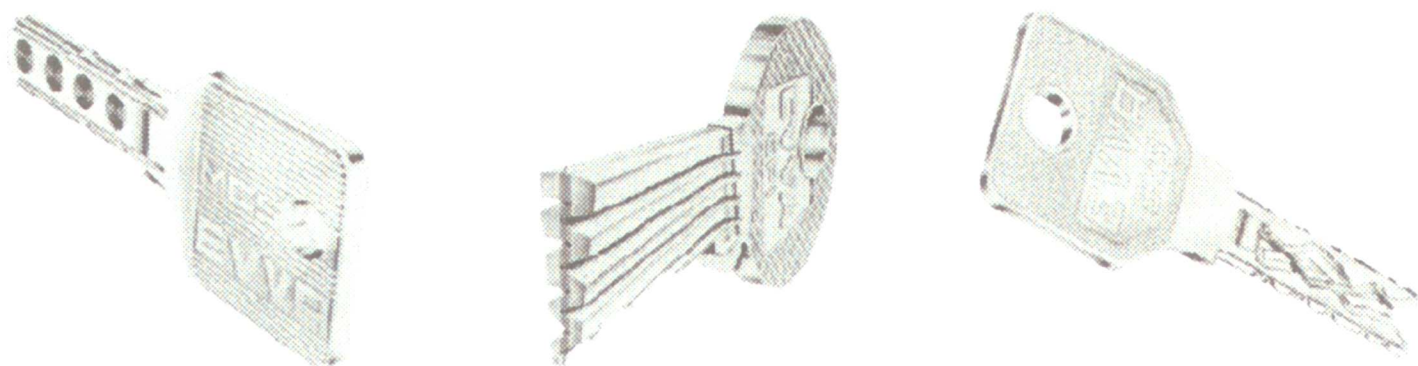
Současný stav vývoje a výroby cylindrických vložek již nemá nic společného s klasickým zámečnictvím a je na úrovni přesné mechaniky, čemuž odpovídají i tolerance funkčních částí, které se řádově pohybují v setinách milimetru. Zároveň se čím dál více prosazuje v sestavě cylindrické vložky elektronika ve funkci ovládání otáčení ozubu (elektromotorické vložky) nebo ve funkci ovládání blokování otáčení cylindru (vložky s ovládacím elektronickým čipem).



Obr. 2-24: Nejčastější tvary cylindrických vložek.

Obr. 2-25: Příkladů víceřadých cylindrických vložek.



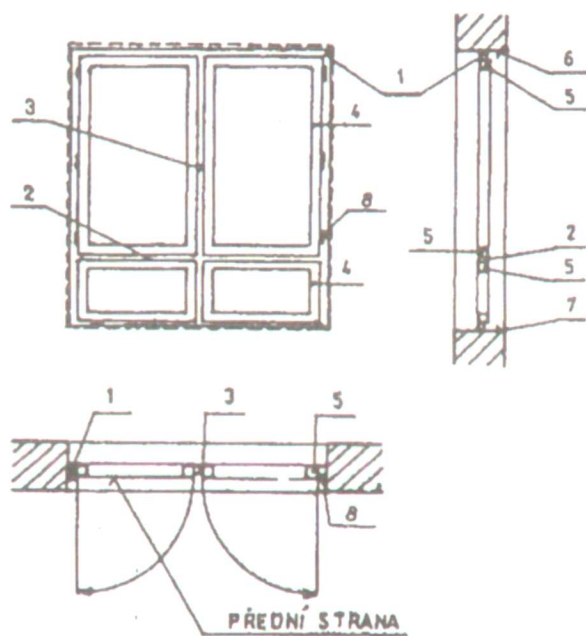


Obr. 2-26: Klíče k různým druhům cylindrických vložek.



Obr. 2-27: Elekromotorická cylindrická vložka s ovládací jednotkou.

### 3.2.2 Okna



**Schéma okenní konstrukce**

- 1 - okenní rám
- 2 - poutec
- 3 - sloupek
- 4 - okenní křídlo
- 5 - vlys křídla
- 6 - okenní překlad (nadpražl)
- 7 - parapet
- 8 - okenní závěs (pant)

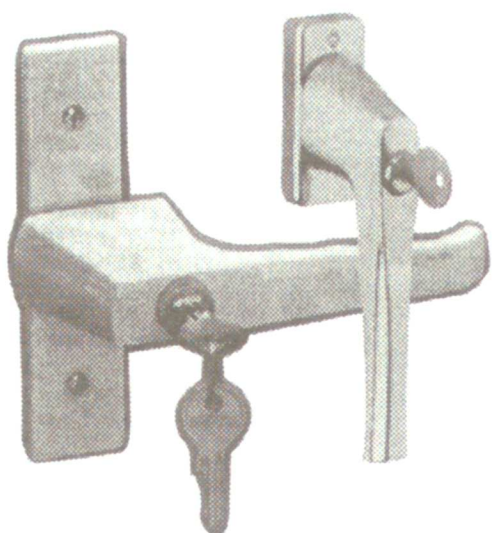
Obr. 2-28: Schéma okna a popis jednotlivých částí.

Okna, resp. všechny zasklené prostory stavebních otvorů, jsou hned na druhém místě zájmu o ochranu. Jedná se o bytová okna, balkonová okna a dveře, sklepní a garážová okna, vikýře, větrací a násypné otvory, ale i výlohy, prosklené stěny apod. Okno je rámová konstrukce s průhlednou nebo průsvitnou výplní, osazovaná obvykle do obvodové stěny budov, protože jeho hlavní funkcí je denní osvětlení a eventuální možnost větrání místností. Konstrukce oken může být **otevíratelná** nebo **neotevíratelná**. Otevíratelných konstrukcí je řada typů podle způsobu otevírání okenních křídel.

Z hlediska bezpečnosti musí být **rám okna** pevný a musí být do zdi (ostění) řádně ukotven. Rovněž **závěsy** musí být pevné a bezpečně připevněné k rámu (musí odolávat páčení). Okenní křídlo musí být při otevírání a zavírání pevně v krutu, aby skleněná výplň nepraskla. Pokud se jedná o velkou zasklenou otevíratelnou plochu, dělí se její konstrukce na menší díly pomocí sloupků a poutců. Pro okenní závěsy platí stejné zásady jako pro rám okna.

Tabulka 2-4: Přehled způsobů otevírání okenních křídel

Způsob otevírání křídla	Osa otáčení (směr) posunu	Schematické zobrazení	Označení	
			písmenné	grafické
vyjímatelné			J	
otevíravé	svislá boční		O	
sklápěcí	vodorovná dole		S	
vyklápěcí	vodorovná nahoře		V	
kyvné	vodorovná uprostřed		K	
otočné	svislá uprostřed		T	
posuvné (posouvací)	vodorovná		H	
výsuvné (vysouvací)	nahoru		N	
Zásuvné (zasouvací)	dolů		Z	
okno neotevíratelné (pevně zasklené)	–		P	
Kombinované způsoby - příklady				
otevíravá a sklápěcí	svislá boční a vodorovná dolní		OS	

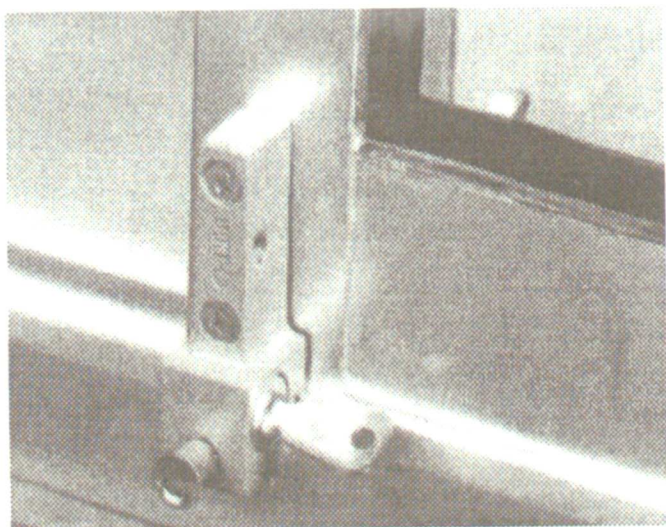


Obr. 2-29: Uzamykatelná okenní klika s vymezovačem pootevření okna.

**Uzávěry a kování** oken musí být hlavně u přízemních oken kvalitní a bezpečné. Nejlepší je používat tyto uzávěry uzamykatelné.

Okna sklepní, garážová, koupelnová a dílenská je nejlépe opatřit mříží stejně jako větrací šachty a technologické otvory. Pro zvýšení bezpečnosti oken se místo výplně tabulového skla používají skla tvrzená, skla s bezpečnostní fólií např. ALLFOLIE, BRUXSAFOL (polyesterový film silný 50 až 400 mikrometrů) a skla vrstvená např. CONNEX, ALLSTOP (jedná se o sendvičovou technologii lepených vrstev většinou sklo-fólie-sklo a tloušťkách 3-0,8-3 mm. Lze vytvořit lepené sklo odolné i střelným zbraním.

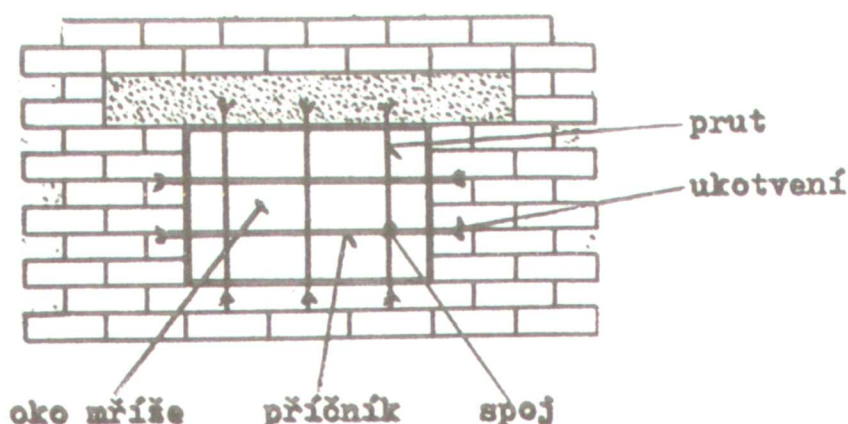
Druhotným zabezpečením stavebních otvorů jsou mříže, rolety, žaluzie a posuvné panely.



Obr. 2-30: Univerzální uzamykací uzávěr okna nebo balkonových dveří.

### 3.2.3 Mříže

Patří k nejstarším mechanickým zábránám. Nemají normativní podklad, při jejich výrobě a instalaci se vychází z empirických zkušeností.



Obr. 2-31: Základní názvosloví klasické mříže.

Tabulka 2-5: Druhy mříží – rozdělení

<p><b>Konstrukce</b></p> <ul style="list-style-type: none"> <li>- pevně kotvené</li> <li>- odejímatelné</li> <li>- otevírací:               <ul style="list-style-type: none"> <li>a) otočné</li> <li>b) sklopné</li> <li>c) posuvné:                   <ul style="list-style-type: none"> <li>pevné</li> <li>nůžkové</li> </ul> </li> </ul> </li> <li>- navíjecí:               <ul style="list-style-type: none"> <li>a) s průhledným výpletem</li> <li>b) s neprůhledným výpletem</li> </ul> </li> </ul>
<p><b>Montáž</b></p> <ul style="list-style-type: none"> <li>- vnější               <ul style="list-style-type: none"> <li>a) ploché</li> <li>b) předsazené</li> </ul> </li> <li>- vnitřní</li> <li>- meziokenní</li> </ul>
<p><b>Materiál</b></p> <ul style="list-style-type: none"> <li>- ocelové</li> <li>- hliníkové (tvrzený a šlechtěný hliník)</li> </ul>

U mříží je důležitá velikost ok a průřez použitého materiálu. Tyto hodnoty jsou opět stanoveny podle zkušeností výrobců a poznatků pojišťoven. **Velikost mřížového oka** má být maximálně **10 x 20 cm**.

Rozměry použitých kovových tyčí mají být minimálně

pro **kruhový průřez 20 mm**,

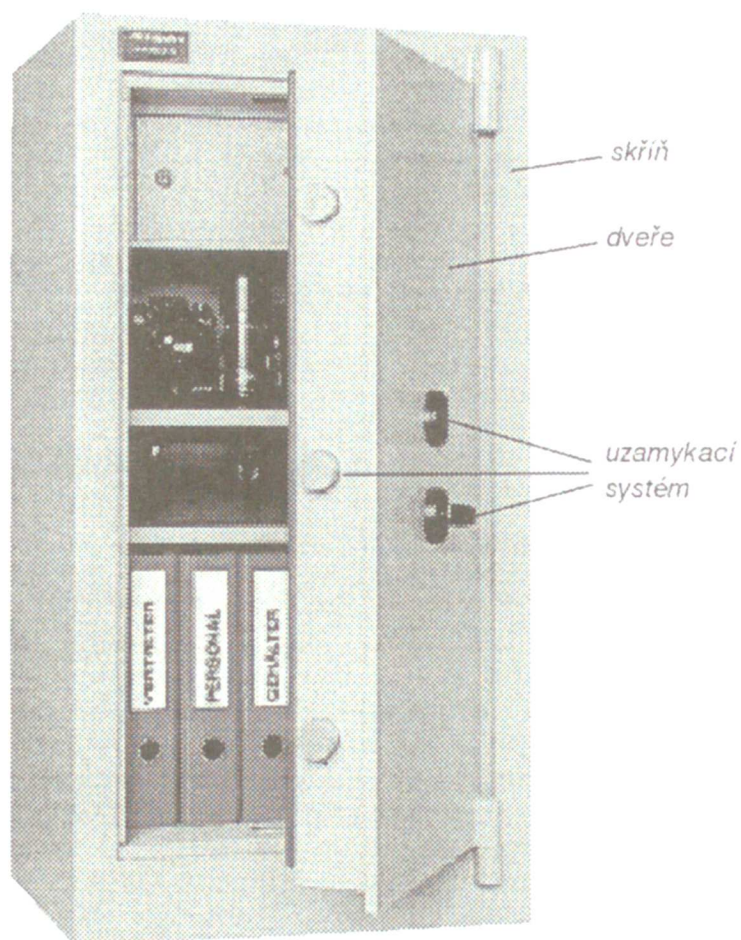
pro **čtvercový průřez 18 x 18 mm**,

pro **obdélníkový průřez 16 x 20 mm**.

**Hloubka ukotvení** prutů a příčníků záleží na druhu zdiva a má být minimálně **14 cm**.

### 3.3 Prostředky individuální ochrany

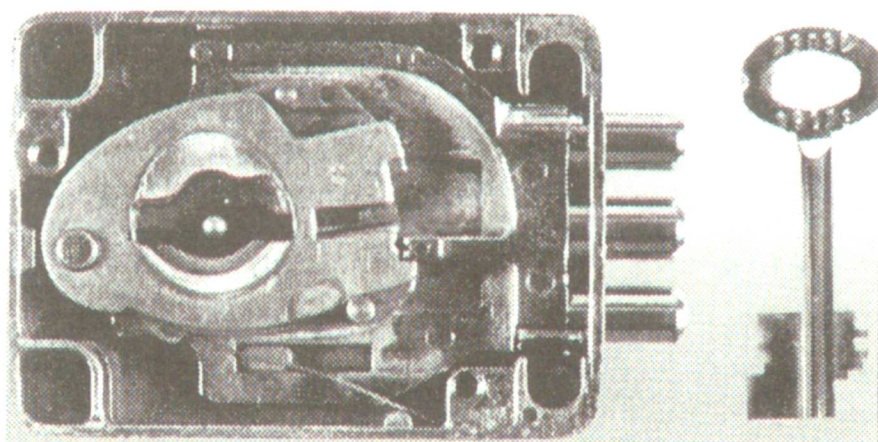
Jedná se o prostředky, které mohou sloužit samostatně, převážně jako úschovné objekty, ale mohou být zařazeny i do předchozích systémů ochrany. Tyto prostředky jsou konečným místem pro úschovu finančních hotovostí, šperků, cenností, sbírek, cenných papírů a dokumentů. Musejí být proto na nejvyšším stupni bezpečnosti. Patří sem především mobilní i stabilní trezory, trezorové skříně, ohnivzdorné skříně, příruční pokladny, manipulační schránky, přenosné kontejnery a kufry.



Obr. 2-32: Základní části trezoru.

Samozřejmě všechny tyto prostředky musí být opatřeny zámkovou technikou a vzhledem k účelu těchto prostředků, musí být instalována zámková technika na nejvyšší úrovni, mnohdy je kombinována nebo zdvojená elektronickou zabezpečovací technikou.

Uzamykací zařízení trezorů a trezorových skříní je ukryto uvnitř dveří trezoru a je tvořeno závorovým systémem a vlastním zámkem. U kvalitních trezorů má závorový systém výsuvné závory do všech stran a jsou buď ploché, nebo častěji válcové o průměrech 15 až 80mm (i více). Zámky se používají buď klíčové (motýlkový typ) nebo heslové (bez klíče).

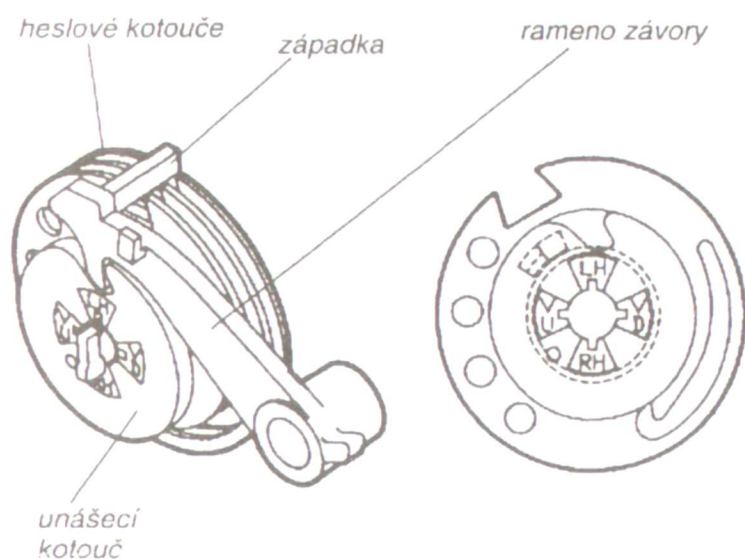


Obr. 2-33 Klíčový stavítkový zámek Mauer.

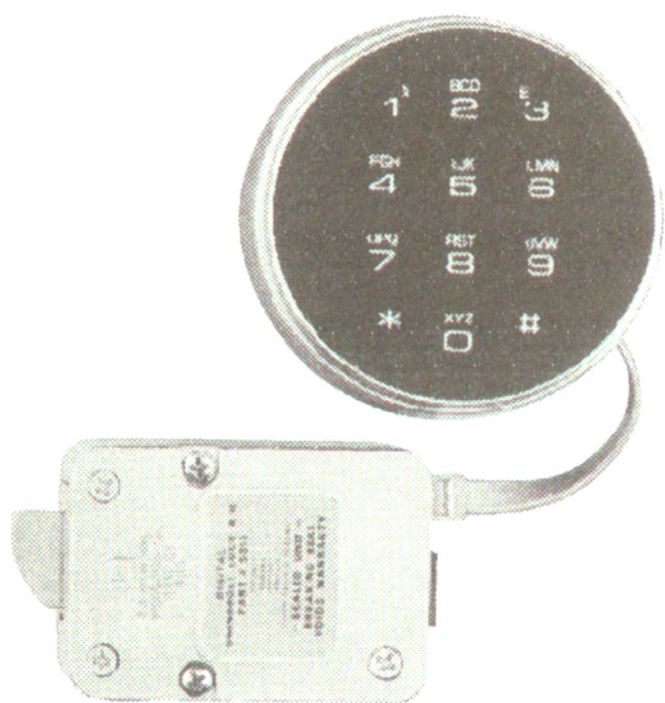
Klíčové zámky se prezentují vysokou přesností výroby stavítek a montáže, tak aby se při otáčení klíče zasouval závorový kolík do výřezů stavítek s minimální vůlí. U heslových zámků mohou nastat dvě varianty: heslový zámek mechanický, kde nastavení zvoleného kódu se provádí otáčením heslového kotouče umístěného na čelní stěně dveří



Obr. 2-34: Schéma funkce heslového zámku a jeho realizace.



trezoru, a heslový zámek elektronický, kde nastavení kódu se provádí klávesnicí. Mnohdy se používají u trezorů zámky dva; děje se tak hlavně u bankovních sejfů, kde jeden klíč má pracovník banky a druhý klíč klient – jeden bez druhého nemůže samostatně sejf otevřít, protože závora zámku je blokována. V takovém případě se používá většinou kombinace dvou klíčových zámků a druhá varianta, kombinace klíčového a heslového zámku, se používá u podnikových nebo soukromých trezorů.



Obr. 2-35: Příklad elektronické zámku s klávesnicí.

### Použitá literatura:

1. Skřivan, Z. a kol.: Nebojte se zlodějů. Praha: Grada, 1994
2. Koktan, P. – Švancar, S.: Bariéry proti zlodějům. Praha: Práce, 1992
3. Švancar, S.: Bezpečnostní uzamykací systémy. Praha: VÚSSZ, 1989
4. Toms, L. – Koniček, T. – Kocábek, P.: Zabezpečení dveří a oken. Praha: THEMIS, 1997
5. Koktan, P.: Mechanické zábranné systémy č. IV. Praha: TREZOR TEST, s. r. o., 2000
6. Toms, L.: Mechanické zábranné systémy – seriál článků. Praha: Security Magazin, 1998 - 2001
7. Uhlář, J.: Technická ochrana objektů, I. díl Mechanické zábranné systémy. Praha: Vydavatelství Policejní akademie ČR, 2000
8. Večeř, Fr.: Zámkařství. Praha, 1893
9. Pankofer, H.: Schlüssel and Schloß. München, 1977
10. Mohr, J – Rasl, Z.: Černé řemeslo v průběhu století - katalog výstavy. Praha, 1984
11. Mohr, J.: Zámky 15. – 18. století ze sbírek Sč. muzea v Liberci. Liberec, 1985

# Elektronické zabezpečovací systémy EZS

Stanislav Křeček, Jan Merhaut

## OBSAH:

<b>1 Názvosloví EZS</b> .....	61
1.2 Tržní rozdělení EZS.....	68
1.3 Stupeň zabezpečení.....	68
1.4 Rozdělení prvků EZS.....	69
<b>2 Prvky plášťové ochrany</b> .....	70
2.1 Magnetické kontakty (čidla otevření).....	70
2.2 Čidla na ochranu skleněných ploch.....	72
2.3 Mechanické kontakty.....	75
2.4 Vibrační čidla.....	75
2.5 Poplachové fólie, tapety, polepy a poplachová skla.....	75
2.6 Drátová čidla.....	76
2.7 Rozpěrné tyče.....	76
<b>3 Prvky prostorové ochrany (čidla prostorová)</b> .....	76
3.1 Pasivní infračervená čidla.....	78
3.2 Ultrazvuková čidla.....	82
3.3 Mikrovlnná čidla.....	84
3.4 Kombinovaná (duální) čidla.....	85
<b>4 Prvky tísňového hlášení</b> .....	86
4.1 Veřejné tísňové hlásiče.....	86
4.2 Speciální tísňové hlásiče.....	87
4.3 Automatické tísňové hlásiče.....	89
4.4 Osobní tísňové hlásiče.....	90
<b>5 Prvky předmětové ochrany</b> .....	91
5.2 Čidla na ochranu uměleckých předmětů.....	96
5.3 Kapacitní čidla.....	98
<b>6 Prvky venkovní obvodové (perimetrické) ochrany</b> .....	99
6.1 Mikrofonické kabely.....	100
6.2 Infračervené závory a bariéry.....	101
6.3 Mikrovlnné bariéry.....	102
6.5 Zemní tlakové hadice.....	104

6.6 Perimetrická pasivní infračervená čidla (infrateleskopy) .....	105
6.7 Další systémy venkovního zabezpečení .....	106
<b>7 Ústředny EZS</b> .....	<b>107</b>
7.1 Základní funkce a rozdělení ústředen EZS .....	107
7.2 Kritéria výběru ústředny EZS.....	112
7.3 Vstupní vyhodnocovací obvody .....	112
<b>8 Ovládací a indikační zařízení</b> .....	<b>119</b>
8.1 Funkce a varianty ovládání .....	119
<b>9 Doplnková zařízení ústředen EZS</b> .....	<b>123</b>
9.1 Akustická signalizace.....	123
9.2 Optická signalizace.....	124
9.3 Grafická tablo .....	124
9.4 Tiskárny .....	125
9.5 Poplachová přenosová zařízení (komunikátory) .....	125

## 1 Názvosloví EZS

Jedinou normou zabývající se problematikou EZS byla dlouhá léta v našem systému norem ČSN 334590. Český normalizační úřad vydal v roce 1999 jako ČSN EN 50131-1 evropskou normu EN 50131-1 zahrnující všeobecné požadavky na EZS, která normu ČSN 334590 nahrazuje. Oficiální zrušení normy bylo odsouhlaseno na základě hlasování v TNK 124 dne 14. května 2001 a ve věstníku ÚNMZ 3/2002 vyšlo oficiální oznámení o zrušení této normy.

Dalším zdrojem terminologie je dnes norma ČSN EN 50131/Z1 vydaná v roce 2000, která do systému českých technických norem zapracovává normy z oblasti EZS, jež na evropské úrovni existují zatím pouze jako návrhy evropských norem (prEN).

Z důvodů zachování terminologické kontinuity v oboru jsou v textu zachovány původní definice pojmů ze zrušené normy ČSN 334590, a současně tam, kde existují ekvivalentní nebo související pojmy a definice v normě ČSN EN 50131-1:1999, ČSN EN 50131-1/Z1:2000 či dalších norem řady ČSN EN 50 13++, jsou uvedeny paralelně i ony. Pro rozlišení jsou tyto pojmy a definice uvedeny kurzivou včetně originálního anglického výrazu. Následující seznam pojmů není úplným výčtem, uvádí pouze pojmy frekventované, a v jednotlivých případech je vždy vhodné využít příslušné normy vztahující se ke konkrétnímu tématu.

**Zařízení elektrické zabezpečovací signalizace** (zařízení EZS): je soubor čidel, tísňových hlásičů, ústředen, prostředků poplachové signalizace, přenosových zařízení, zapisovacích zařízení a ovládacích zařízení, jejichž prostřednictvím je opticky nebo akusticky signalizováno na určeném místě narušení střeženého objektu nebo prostoru.

**poplachový systém** (*alarm system*): elektrická instalace, která reaguje na ruční nebo automatickou detekci přítomnosti nebezpečí

**elektronický zabezpečovací systém (zkratka EZS)** (*intruder alarm system*): poplachový systém pro detekci a indikaci přítomnosti, vstupu nebo pokusu o vstup narušitele do střežených objektů

*Poznámka – oficiální název v normě je „elektrický“, nicméně vzhledem k EZS začíná převažovat pojem „elektronický“.*

**subsystém** (*subsystem*): ta část EZS, která je umístěna v jasně definované části střežených objektů a je schopna samostatného provozu

**komponenty systému** (*system components*): jednotlivá zařízení, která, pokud jsou uspořádána, tvoří EZS

**Čidlo EZS**: je zařízení reagující na jevy související s narušením střeženého objektu nebo prostoru nebo s nežádoucí manipulací se střeženým předmětem vytvořením předem určeného výstupního elektrického signálu.

**Čidlo EZS destrukční**: čidlo schopné pouze jednorázové funkce. Při vyhlášení poplachu se samo zničí.

**Čidlo EZS napájené**: čidlo vyžadující ke svému provozu napájení elektrickou energií.

**Čidlo EZS nenapájené:** čidlo nevyžadující ke svému provozu napájení elektrickou energií.

**Čidlo prostorové:** reaguje na jevy související s narušením střeženého prostoru.

**čidlo směrové:** reaguje na jevy související s narušením v definovaném směru.

**čidlo (detector):** zařízení určené k vysílání poplachového signálu nebo zprávy jako odezvy na zaznamenání abnormální podmínky, indikující přítomnost nebezpečí

**aktivní (active):** stav čidla při přítomnosti nebezpečí

**senzor (sensor):** ta část čidla, která snímá změnu stavu

*Poznámka – pojem čidlo je v nových normách nahrazen ekvivalentním pojmem detektor. Doporučuje se preferovat pojem detektor.*

**Tísňové hlásiče EZS:** zařízení určená k manuálnímu vyhlášení poplachu osobami, které jsou obeznámeny s jejich použitím.

**Veřejný tíšňový hlásič:** tíšňový hlásič instalovaný zjevně, k jehož ovládání je třeba překonat určitou překážku zabraňující nahodilému zneužití.

**Speciální tíšňový hlásič:** tíšňový hlásič instalovaný skrytě, ovládaný stanoveným způsobem obsluhou obeznámenou s jeho použitím.

**Ústředna EZS:** zařízení určené k příjmu a vyhodnocení výstupních elektrických signálů čidel nebo tíšňových hlásičů a k vytvoření signálu o narušení.

**ústředna (control and indicating equipment):** zařízení pro příjem, zpracování, ovládání, indikaci a iniciace následného přenosu informací

**Signalizační zařízení EZS:** zařízení, které opticky a akusticky, nebo opticky, nebo akusticky signalizuje výstupní informace ústředny

**Signalizační panel EZS:** zařízení, které souběžně signalizuje některé, nebo všechny stavy ústředny.

**signalizační (výstražné) zařízení (warning device):** zařízení, které vyhláší poplach nebo výstrahu

*Poznámka – vžitá názvy pro akustickou signalizaci – siréna, pro optickou signalizaci – světelný maják. Dnes se prosazuje v návrzích na převzetí evropských norem překladem pojem „výstražná zařízení“.*

**Orientační tablo EZS:** zařízení, které opticky znázorňuje místo narušení ve schematicém plánu střeženého objektu.

**Informační jednotka:** zařízení, které poskytuje informaci o místě poplachu, případně další informace navazující na provoz zařízení EZS.

**Tablo obsluhy:** zařízení, jehož prostřednictvím lze získávat informace o výstupních stavech zařízení EZS a které umožňuje jeho zpětné ovládání

**pomocné ovládací zařízení** (ancillary control equipment): zařízení použité pro doplňkové ovládací účely

Poznámka – vžitě názvy – integrovaný ovládací díl popř. ovládací díl s alfanumerickým displejem, ovládací klávesnice ...

**akce** (při nastavování stavu střežení a klidu) (action): jakákoliv záměrná činnost nebo jednání uživatele, které je součástí postupu nastavování stavu střežení a klidu

**přístupová úroveň** (access level): úroveň přístupu k jednotlivým funkcím EZS

**Přenosové zařízení EZS**: zařízení, které umožňuje samočinné předávání výstupních informací do určeného místa po lince jednotné telekomunikační sítě nebo po samostatném vedení nebo po síťovém vedení nebo bezdrátově.

**komunikátor poplachového systému** (alarm system transceiver): přenosové poplachové zařízení, které je umístěno ve střežených prostorách nebo na satelitní stanici

Poznámka – V některých systémech může být komunikátor schopný vysílání, ale ne příjmu.

**poplachové přenosové zařízení** (alarm transmission equipment): Zařízení, které je především určené k přenosu poplachových hlášení na rozhraní poplachového systému ve střežených prostorech k rozhraní poplachového přenosového zařízení v poplachovém přijímacím centru a dále k ovládacímu a indikačnímu zařízení v poplachovém přijímacím centru

Poznámka – Může také přenášet informace nebo povely z poplachového přijímacího centra k jednomu nebo několika poplachovým systémům.

Poznámka – Nezahrnuje zařízení sloužící uživatelům veřejné telefonní sítě nebo další otevřené nosiče, které jsou součástí veřejného přenosového systému pro všeobecné účely, ale obsahuje všeobecná telekomunikační zařízení (např. modemy), která jsou přednostně použité pro přenos poplachu.

Poznámka – vžitý název – telefonní volič, komunikátor (po JTS či GSM), nebo objektové zařízení (je-li systém připojen na PCO/PPC).

**Pult centralizované ochrany (PCO)**: zařízení, které umožňuje přenos i vyhodnocení signalizace narušení ze zabezpečených objektů do místa centrálního vyhodnocení pomocí linek jednotné telekomunikační sítě (JTS).

**poplachové přijímací centrum/pult centralizované ochrany (zkratka PPC/PCO)** (alarm receiving centre): trvale obsluhované vzdálené středisko, do kterého se předávají informace týkající se stavů jednoho nebo více EZS

Poznámka – dvojí pojem PPC/PCO má vyjadřovat odlišného provozovatele centra (PCO – Policie, PPC – soukromý subjekt). V praxi je však převážně užíván pojem PCO, nezávisle na statutu provozovatele.

**monitorovací centrum** (monitoring centre): člověkem na dálku obsluhované centrum, kterým je monitorován jeden nebo více poplachových přenosových systémů

*Poznámka – Monitorovací centrum může být samostatným centrem nebo částí poplachového přijímacího centra.*

**vzdálené centrum** (*remote centre*): lokalita vzdálená od střežených prostor, ve které jsou zpracovávány informace týkající se stavu jednoho nebo více poplachových systémů pro hlášení (tj. do poplachového přijímacího centra) nebo pro následný přenos (retranslaci)

**poplachový přenosový systém** (*alarm transmission system*): zařízení a síť, používané pro přenos informací, týkající se stavů jednoho nebo více EZS do jednoho nebo více PPC/PCO

**Zapisovací zařízení EZS:** zařízení, které umožňuje automatické provedení písemného zápisu výstupních informací ústředny s doplněním identifikačních a časových údajů.

*Poznámka – v dřívějších dobách se jednalo o přímo připojenou tiskárnu, dnes se jedná o interní či externí paměť událostí (dějů) s možností vytisknout historii v rozsahu daném velikostí paměti buď přímo na tiskárnu, nebo stáhnout na počítač přes sběrnici či přes fyzické médium, a posléze vytisknout na běžné tiskárně stolního počítače.*

**událost** (*event*): změna stavu indikovaná EZS, například stav střežení, stav klidu, poplachový stav

**záznam událostí** (*event recording*): shromažďování událostí vyplývajících z činnosti EZS, například pro analýzu

**Ovládací zařízení EZS:** zařízení, které umožňuje ovládat samočinně nebo pomocí obsluhy zařízení EZS, jeho části nebo jednotlivá čidla (vžitý název – ovládací díl).

**oprávnění** (*authorization*): povolení k získání přístupu k různým funkcím EZS

**Propouštěcí zámek EZS:** zařízení, které umožňuje s použitím kódu vyřazení a opětovné uvedení do funkce jednotlivých prvků EZS bez signalizace poplachu.

*Poznámka – tento pojem díky softwareovým možnostem ovládání moderních ústředn prakticky vymizel.*

**Propustný stav:** stav propouštěcího zámku, při kterém jsou vyřazeny z provozu propouštěcím zámek ovládaná zařízení.

**odpojení** (*isolation*): stav části EZS, ve kterém není možné ohlásit poplachový stav; tento stav zůstává tak dlouho, dokud není záměrně zrušen

*Poznámka – zde se spíše užívá originálního anglického výrazu „bypass“ či českého „přemostění“, z němčiny také „částečné střežení“. Bypass je však asi nejmýšlivější s ohledem na skutečný význam akce.*

**Řídicí jednotka EZS:** část ústředny, která umožňuje automaticky podle předem nastaveného programu ovládat zařízení EZS v nastavitelném časovém intervalu.



**Základní zdroj:** zdroj elektrické energie pro trvalé napájení zařízení EZS.

**napájecí zdroj** (*power supply*): ta část EZS, která zajišťuje energii pro EZS nebo pro kterýkoliv jeho komponent.

**základní napájecí zdroj** (*prime power source*): zdroj napájející EZS nebo jeho komponenty při normálních provozních podmínkách

**napájecí jednotka** (*power unit /PU/*): zařízení, které poskytuje a také mění nebo odděluje (elektrickou) energii pro EZS nebo jeho komponenty a v případě potřeby také pro záložní zdroj

**napájecí zdroj** (*power supply /PS/*): zařízení, které shromažďuje, poskytuje, a také mění nebo odděluje (elektrickou) energii pro EZS nebo jeho komponenty; napájecí zdroj se skládá ze dvou základních částí: napájecí jednotky a záložního zdroje (např. akumulátoru)

**Náhradní zdroj:** zdroj elektrické energie pro napájení zařízení EZS při výpadku základního zdroje.

**náhradní napájecí zdroj** (*alternative power source /APS/*): napájecí zdroj energie, který je schopen napájet EZS po předem určenou dobu v případě výpadku základního napájecího zdroje

**Zajišťovací smyčka:** vedení spojující elektricky zajištěné kryty nebo skříně nebo víka skříní zařízení EZS nebo zajišťovací kontakty zařízení EZS s příslušným vstupem ústředny EZS (vžitý název sabotážní – smyčka).

**sabotáž** (*tamper*): úmyslné zasahování s nedovolenou manipulací do EZS nebo jeho části

**sabotážní poplach** (*tamper alarm*): poplach způsobený detekcí sabotáže

**stav sabotáže** (*tamper condition*): stav EZS, ve kterém byla detekována sabotáž

**detekce sabotáže** (*tamper detection*): detekce úmyslného zasahování do EZS nebo jeho komponentů

**Napájecí linka:** vedení pro přivedení napájecího napětí k zařízení EZS.

**výkonový výstup** (*power output*): výstup napájecího zdroje, který dodává energii EZS

**nezávislé napájecí výstupy** (*independent power outputs*): napájecí zdroj mající více než jeden výstup; každý výstup má svou vlastní ochranu proti zkratu a přetížení (např. pojistky); každý výstup může mít několikanásobné svorky

**Signalizační linka:** vedení spojující výstupy ústředny se všemi zařízeními přiřazenými těmto výstupům.

**Zajišťovací kontakt:** kontakt vytvářející elektrické zajištění mechanického sestavení čidel nebo ostatních zařízení EZS před nežádoucí manipulací (vžitý název – sabotážní kontakt, „tamper“).

**Elektricky zajištěný kryt** (skříň, víko skříně): zajištění, při němž nežádoucí manipulace nebo otevření nebo destrukce způsobí signalizaci poplachu.

**ochrana proti sabotáži** (*tamper protection*): metody nebo prostředky ochrany EZS nebo jeho komponentů proti úmyslnému zasahování

**zabezpečení proti sabotáži** (*tamper security*): metody nebo prostředky ochrany EZS nebo jeho komponentů proti úmyslnému zasahování a detekce úmyslného zasahování do EZS nebo jeho komponentů

**Pohotovostní stav čidla**: funkční stav čidla charakterizovaný jeho pohotovostí reagovat na poplachový podnět.

**aktivní čidlo** (*active detector*): čidlo schopné porovnávat vstupní signály s předem definovanými kritérii (rychlost, frekvence, amplituda, směr) před vysláním poplachového signálu nebo zprávy

**Poplachový stav čidla**: funkční stav čidla, při kterém se vytvoří předepsaný elektrický signál na jeho výstupu.

**signál nebo zpráva narušení** (*intruder signal or message*): informace vyslaná čidlem narušení

**Falešný poplach**: poplachový signál, který vznikne, přestože nedošlo k narušení střeženého objektu nebo předmětu. Způsobí jej:

- a) nahodilá aktivace tísňového hlásiče,
- b) odezva čidel na jiný stav než na takový, který má být zjišťován,
- c) vadná funkce nebo porucha části EZS,
- d) chyba operátora.

**Narušení objektu**: je nežádoucí vniknutí nebo pokus o vniknutí do střeženého objektu.

**poplachový stav narušení** (*intruder alarm condition*): stav EZS nebo jeho komponentů, kterým EZS reaguje na přítomnost narušitele

**Klid objektu**: stav vylučující signalizaci poplachu.

**Základní signalizace poplachu**: signalizace poplachu bez určení místa narušení

**poplach** (*alarm*): výstraha o přítomnosti nebezpečí pro život, majetek nebo okolní prostředí

**hlášení poplachu** (*alarm notification*): předání poplachového stavu na signalizační zařízení, případně do poplachových přenosových systémů

**Signalizace místa poplachu**: signalizace poplachu s určením místa narušení.

**Spouštěcí úroveň**: nejnižší úroveň signálu nebo změna v jeho úrovni, která vede k signalizaci poplachového stavu.

**Provozní kniha EZS**: dokument pro vedení záznamů o činnosti, poruchách, prohlídkách, údržbě a opravách zařízení EZS.

**Garantovaný zdroj:** zdroj, který má zaručenou maximální dobu výpadku.

**Klasická ochrana objektu:** zabezpečuje objekty, prostory a předměty svou mechanickou pevností. Na její překonání je potřeba použít různé nástroje a vynaložit značnou sílu.

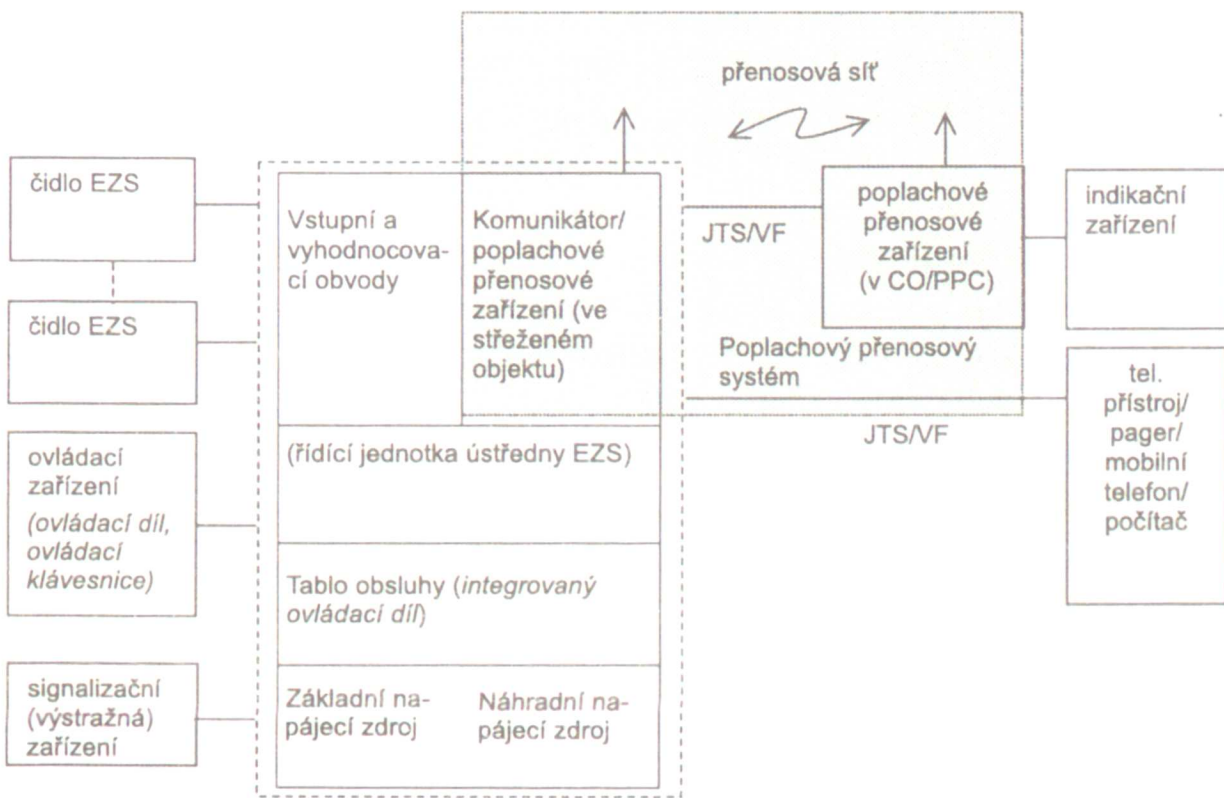
**Technická ochrana objektu:** EZS

**Režimová ochrana objektu:** soustava organizačně administrativních opatření, která vymezují pohyb osob, materiálu a informací vně i uvnitř objektu.

**Fyzická ochrana objektu**

**Zpětná signalizace:** signalizace v místě narušení využívaná ke kontrole signalizace poplachu ve smyčce.

Pro lepší představu o významu jednotlivých pojmů je na následujícím obrázku symbolicky znázorněn systém EZS s vyznačením nejvíce užívaných pojmů.



Obr. 3-1: Schematické znázornění systému EZS.

### 1.2 Tržní rozdělení EZS

Techniku EZS lze rozřadit do určitých úrovní z hlediska aplikace i z hlediska nároků na kvalifikaci instalační firmy či uživatele:

Tabulka 3-1: Systémová pyramida techniky EZS.

	Kvalifikace zřizovatelů:		úroveň techniky:
I.	<ul style="list-style-type: none"> <li>speciální znalosti</li> <li>montáž výhradně prokazatelně proškolenými firmami</li> <li>vysoké nároky na vybavení při montáži a údržbě</li> </ul>		Profesionální technika (vyšší cena)
II.	<ul style="list-style-type: none"> <li>všeobecné znalosti</li> <li>montáž všeobecně znalými firmami</li> <li>standardní vybavení pro montáž údržbu</li> </ul>		Standardní systémové produkty (nižší cena)
III.	<ul style="list-style-type: none"> <li>není nutná odborná kvalifikace</li> <li>montáž může provést uživatel sám</li> <li>minimální nároky na vybavení a údržbu</li> </ul>		Zařízení pro širokou veřejnost (nízká cena)

Prvky zmiňované v rámci následujícího textu patří převážně do úrovně II. Pro zvládnutí techniky úrovně I. je nutné specifické školení na konkrétní výrobky, jež se realizačními firmám v oblasti tzv. profesionální techniky nabízí.

### 1.3 Stupeň zabezpečení

Nejdůležitějším kritériem pro zařazení příslušného prvku EZS jsou tzv. stupně zabezpečení, které jsou definovány v ČSN EN 50131-1 a stanovují kritéria na vybavení a funkce jednotlivých komponentů popř. i systému z hlediska:

- přístupové úrovně,
- provozování,
- vyhodnocení,
- detekci,
- napájení,
- zabezpečení proti sabotáži,
- monitorování,
- propojení,
- záznamu událostí.

Tabulka 3-2: Stupně zabezpečení

Stupeň	Míra rizika	Předpokládaný typ narušitele
1	nízké	narušitel má malou znalost EZS; omezený sortiment snadno dostupných nástrojů
2	nízké až střední	narušitel má určité znalosti o EZS; omezený sortiment základních přenosných přístrojů (například multimetr)
3	střední až vysoké	narušitel je obeznámen s EZS; úplný sortiment základních přenosných přístrojů a elektronických zařízení
4	vysoké	narušitel je schopen nebo má možnost zpracovat podrobný plán vniknutí; kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících prvků EZS

## 1.4 Rozdělení prvků EZS

Tabulka 3-3: Prvky systémů EZS

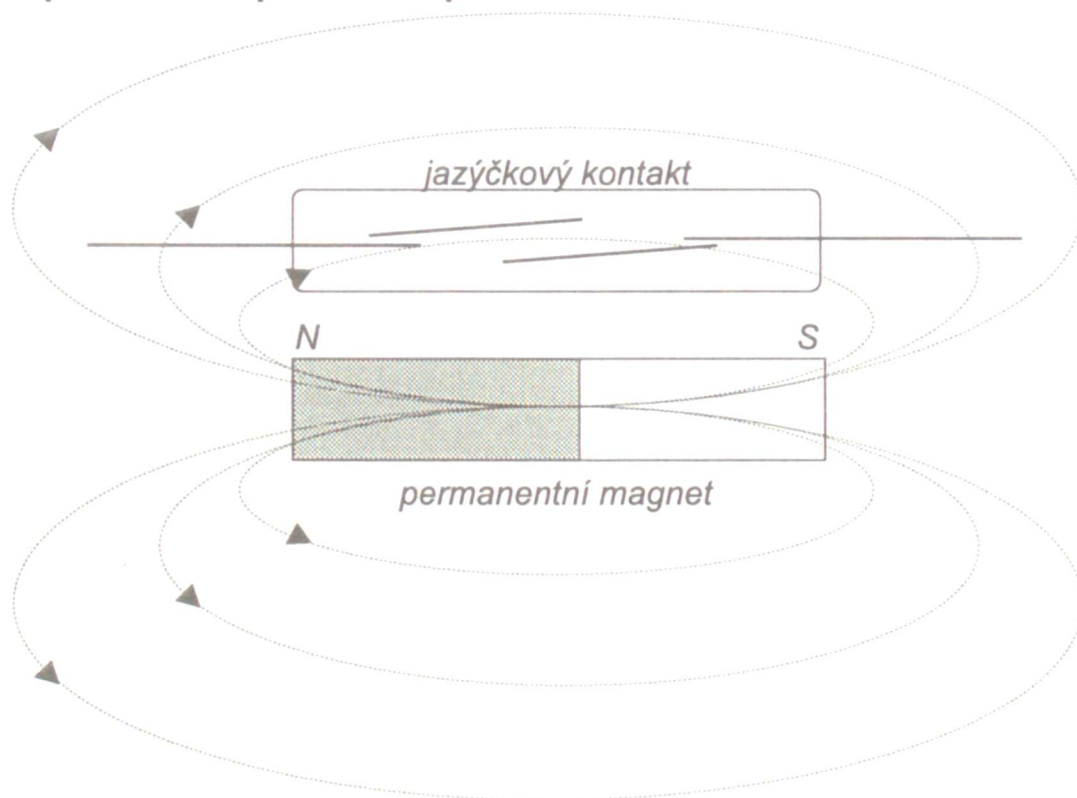
<b>PRVKY PLÁŠŤOVĚ OCHRANY</b>	<b>PRVKY PROSTOROVÉ OCHRANY</b>
<ul style="list-style-type: none"> <li>• magnetické kontakty,</li> <li>• čidla na ochranu prosklených ploch,</li> <li>• mechanické kontakty,</li> <li>• vibrační čidla,</li> <li>• poplachové fólie, tapety, polepy a poplachová skla,</li> <li>• drátová čidla,</li> <li>• rozpěrné tyče.</li> </ul>	<ul style="list-style-type: none"> <li>• pasivní infračervená čidla,</li> <li>• aktivní infračervená čidla,</li> <li>• ultrazvuková čidla,</li> <li>• mikrovlnná čidla,</li> <li>• kombinovaná duální čidla.</li> </ul>
<b>PRVKY TÍSŇOVÉ OCHRANY</b>	<b>PRVKY PŘEDMĚTOVÉ OCHRANY</b>
<ul style="list-style-type: none"> <li>• veřejné tísňové hlásiče,</li> <li>• skryté tísňové hlásiče,</li> <li>• osobní tísňové hlásiče.</li> </ul>	<ul style="list-style-type: none"> <li>• otřesová čidla,</li> <li>• čidla na ochranu zavěšených předmětů,</li> <li>• kapacitní čidla.</li> </ul>
<b>OVLÁDACÍ ZAŘÍZENÍ</b>	<b>ČIDLA SPECIÁLNÍ</b>
<ul style="list-style-type: none"> <li>• blokovací zámky,</li> <li>• spínací a propouštěcí zámky,</li> <li>• kódové klávesnice,</li> <li>• ovládací a indikační díly,</li> <li>• kartové ovládání.</li> </ul>	<ul style="list-style-type: none"> <li>• tlaková čidla,</li> <li>• nášlapné koberce.</li> </ul>
<b>POPLACHOVÉ ÚSTŘEDNY EZS</b>	<b>PRVKY VENKOVNÍ OBVODOVÉ (PERIMETRICKÉ) OCHRANY</b>
<ul style="list-style-type: none"> <li>• klasické smyčkové ústředny,</li> <li>• ústředny s přímou adresací,</li> <li>• ústředny smíšeného typu,</li> <li>• ústředny s bezdrátovým přenosem signálu od čidel.</li> </ul>	<ul style="list-style-type: none"> <li>• mikrofonické kabely,</li> <li>• infračervené závory a bariéry,</li> <li>• mikrovlnné bariéry,</li> <li>• štěrbinové kabely,</li> <li>• zemní tlakové hadice,</li> <li>• perimetrická pasivní infračervená čidla.</li> </ul>
<b>SIGNALIZAČNÍ (VÝSTRAŽNÁ) ZAŘÍZENÍ</b>	<b>PŘENOSOVÁ ZAŘÍZENÍ</b>
<p>zábleskový maják, siréna.</p>	<p>automatické telefonní hlásiče a voliče, bezdrátová přenosová zařízení.</p>

## 2 Prvky plášťové ochrany

Prvky plášťové ochrany slouží, jak už sám jejich název napovídá, k hlídání otevření, popř. destrukce vstupů pláště budovy (oken, vrat, dveří).

### 2.1 Magnetické kontakty (čidla otevření)

#### 2.1.1 Princip funkce a praktické provedení



Obr. 3-2: Princip funkce magnetického kontaktu.

Magnetické kontakty tvoří vždy dvojice dílů – jazýčkový kontakt a permanentní magnet.

**Jazýčkový kontakt** je tvořen zatavenou skleněnou trubičkou naplněnou ochrannou atmosférou, v níž jsou umístěny dva ferromagnetické kontakty.

**Permanentní magnet** je nejčastěji zmagnetovaný váleček z feritu (ALNICO).

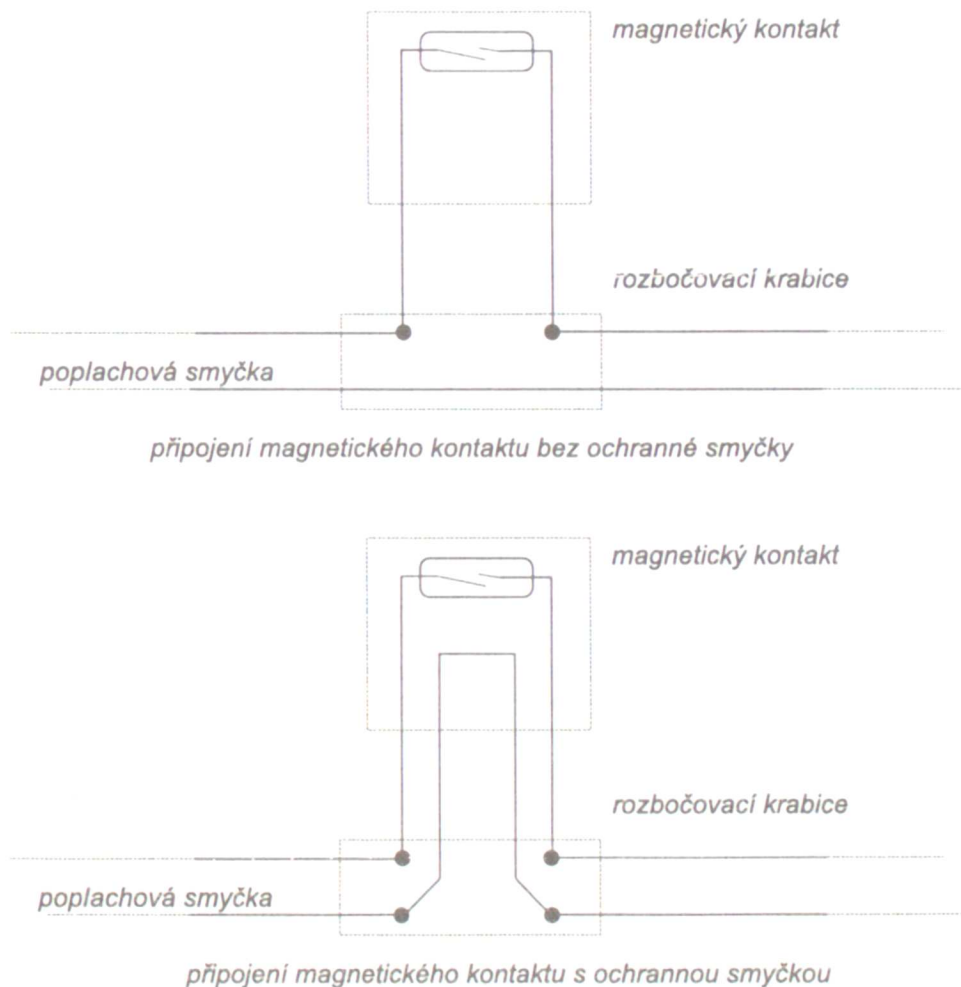
V klidovém stavu je kontakt jazýčkového relé sepnut magnetickým polem permanentního magnetu. Při aktivaci oddálením magnetu se kontakt rozezne, a tím způsobí poplachové hlášení.

Jazýčkový kontakt i permanentní magnet jsou samostatně zapouzdřeny do různě konstruovaných krytů z nemagnetického materiálu (plastu či hliníkové slitiny).

Různé provedení magnetických kontaktů umožňuje povrchovou nebo skrytou montáž přímo do tělesa dveří či oken. Pro střežení vstupů opatřených roletami je určen magnetický kontakt v těžkém, mechanicky i klimaticky odolném provedení. Pro speciální aplikace s velmi vysokými riziky (např. věznice) existují magnetické kontakty odolné proti cizímu magnetickému poli. Jakýkoliv pokus o odstavení magnetického kontaktu přilože-

ním cizího magnetu vyvolá automaticky poplachové hlášení. Tyto magnetické kontakty obsahují buď polarizovaný jazýčkový kontakt, nebo je kontakt tvořen sérioparalelní kombinací více kontaktů (3 – 7 jazýčkových kontaktů), z nichž některé jsou spínací a jiné rozpínací.

### 2.1.2 Elektrické připojení



Obr. 3-3: Elektrické připojení magnetických kontaktů.

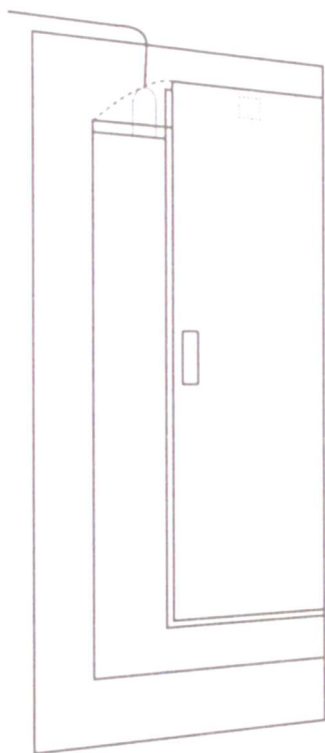
### 2.1.3 Použití a montáž

Magnetické kontakty jsou vhodné ke střežení všech stavebních otvorů – prostupů (oken, dveří, vrat, rolet) proti otevření.

Magnet se montuje na pohyblivou část osazení prostupu, jazýčkový kontakt se montuje na rám. Při montáži je nutné dodržovat instrukce výrobce. Mezi ně patří především následující požadavky:

- dodržujte stanovené max. (popř. i min.) vzdálenosti permanentního magnetu od jazýčkového relé v klidové poloze,
- dodržujte orientaci a polohu magnetu, jsou-li výrobcem stanoveny,
- pro montáž používejte zásadně šrouby z nemagnetického materiálu,
- pro montáž na magnetický materiál použijte pouze takové magnetické kontakty, jejichž výrobce to výslovně povoluje, popř. stanoví konkrétní opatření (např. použití distančních podložek z nemagnetického materiálu stanovené tloušťky), u dvoukřídlých oken a dveří osazujte vždy obě křídla,
- kontakt montujte vždy na stranu křídla proti pantům,

- přívodní vodič ved'te skrytě v elektroinstalačních trubkách či lištách přímo do pojovací krabice,
- neprovádějte nechráněná propojení vodičů pod bužírkou.



Obr. 3-4: Příklad umístění magnetického kontaktu.

### 2.1.4 Kritéria falešných poplachů

Magnetický kontakt je nenapájené čidlo s minimálním počtem konstrukčních dílů. Je to vysoce spolehlivý prvek s dlouhou životností a s vysokou odolností proti vnějším vlivům. Zdrojem planých a falešných poplachů mohou být následující příčiny:

- nedodržení pokynů výrobce při montáži,
- špatně doléhající dveře a okna (nová, vyrobená z nevyzrálého dřeva),
- omylem nezajištěná dveře či okna.

### 2.1.5 Nastavení, údržba

Vlastní nastavení magnetického kontaktu spočívá především ve správné montáži, u některých typů i ve správné orientaci permanentního magnetu. Před definitivním zakrytím či zatmelením při skryté montáži je nutné ověřit správnou funkci magnetického kontaktu nejlépe pomocí zvukového návěští při měření odporu digitálním multimetrem. U magnetických kontaktů se zajišťovací smyčkou je nutné ověřit i stav této smyčky. Nejčastější závady jsou mechanické poškození přívodního relativně tenkého kablíku při zatahování do nejbližší rozbočovací krabice během montáže. V provozu bývá při povrchové montáži častou závadou ztráta či zcizení permanentního magnetu. Magnetický kontakt je sám o sobě bezúdržbový, v případě ztráty funkce je nutné jej celý vyměnit.

## 2.2 Čidla na ochranu skleněných ploch

### 2.2.1 Principy funkce a praktické provedení

Tříštění skla vyvolává charakteristický zvuk, který se hmotou skla šíří jako vlnění v pevném tělese. Toto vlnění zachycuje čidlo pevně spojené s plochou skla – přilepené s důrazem na co nejmenší ztráty při přenosu zvuku. Taková čidla se nazývají kontaktní. Při narušení skleněné plochy je vlnění vyhodnoceno elektronikou čidla a čidlo způsobí hlášení. Podle konstrukce čidla se jedná buď o rozepnutí bezpotenciálového kontaktu relé, který je zapojen v poplachové smyčce, nebo o prudký vzrůst odběru čidla napájeného přímo z poplachové smyčky. Praktický dosah těchto čidel bývá 1,5 – 3 m dle typu.

Čidla na ochranu skleněných ploch staršího provedení obsahovala jednoduchý systém s předepnutým pružinovým kontaktem či rtuťovým prasátkem, jejichž funkce byla závislá na skutečné destrukci skla i v bodě připevnění a reagovala na změnu polohy tělesa čidla.

Pro nejvyšší úroveň rizik jsou určena **aktivní čidla na ochranu skleněných ploch**. Obsahují vysílací a přijímací část. Elektronika vyhodnocuje změny přenosu oproti nor-

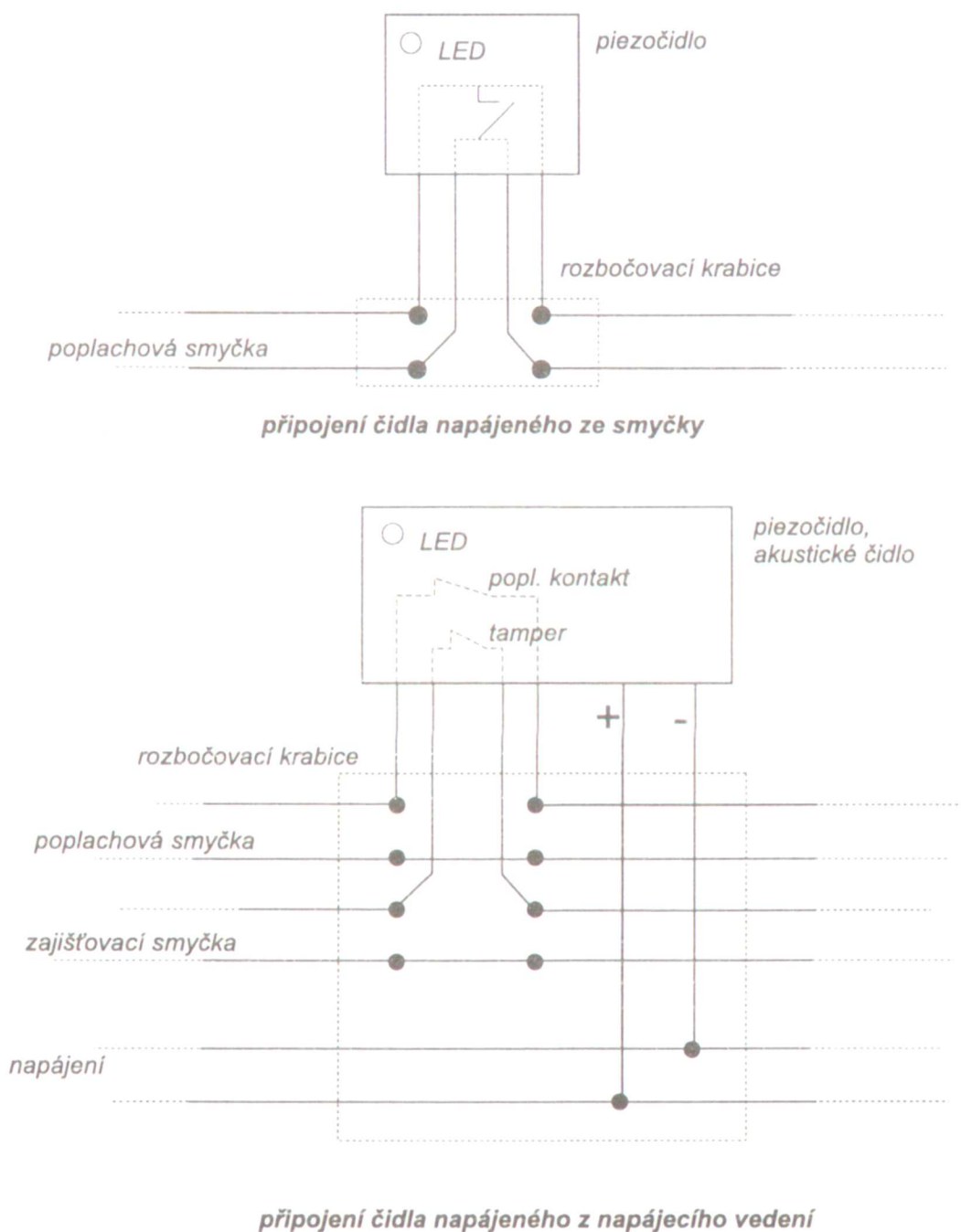


málnímu stavu, jenž je uložen v paměti čidla. Tato čidla mají velký dosah a mohou střežit až 25 m plochy (podle typu čidla a druhu skla).

Velice rozšířené jsou u nás **akustická čidla rozbití skleněných ploch**. Nevyhodnocují vlnění v tělese skla, ale následný akustický efekt při tříštění skla, jenž je naprosto charakteristický. Elektronika vyhodnocuje akustické vlnění přijaté elektretovým mikrofonem. Dále následuje pásmová propust propouštějící pouze část spektra typickou pro tříštění skla. Kvalitnější typy mají těchto propustí více a vyhodnocují přítomnost zvuku ve více částech zvukového spektra, čímž snižují možnost vyhodnocení podobných zvuků, a tím vyvolání falešných poplachů.

Nejnovější typy vyhodnocují zvukové spektrum ve více diskretních bodech a vyvolají hlášení teprve poté, když jsou všechny tyto diskretní kmitočty ve zvuku v určitém časovém intervalu obsaženy. Jedná se o přítomnost tříštivého zvuku skla o vysoké frekvenci a přítomnost rázové vlny vyvolané v oblasti nízkých kmitočtů borcením skleněné plochy.

### 2.2.2 Elektrické připojení



Obr. 3-5: Elektrické připojení čidel na ochranu skleněných ploch.

### 2.2.3 Použití a montáž

Kontaktní čidla se užívají především ke střežení neotevratelných prosklených ploch v plášti střeženého prostoru proti rozbití. Z hlediska montáže je podstatné zvláště u větších ploch dodržení odstupů místa montáže od hrany rámu cca **50 mm**. Rovněž se doporučuje montáž u spodní hrany plochy s kabelovým příchodem dolů či na stranu tak, aby porušení pružného spoje se skleněnou plochou bylo na první pohled patrné. Důležitým krokem při aplikaci je důkladné odmaštění plochy. Pro lepení jsou doporučována kyanoakrylátová lepidla nebo speciální lepidla na bázi silikonových tmelů (podobná lepidlům na lepení akvárií). Od těchto čidel se v poslední době upouští pro vysokou ekonomickou náročnost – jedno čidlo je schopno pokrýt maximálně jednu skleněnou plochu vstupního otvoru. Dalším aspektem pro ústup od tohoto druhu čidel je i vysoká náročnost na řemeslné provedení montáže.

Dnes nejvíce rozšířená akustická čidla rozbití skleněných ploch se montují proti chráněné ploše (plochám). Při montáži je nutné dbát instrukcí výrobce ohledně směřování snímacího prvku čidla a garantovaný dosah čidla s ohledem na konkrétní provedení skleněné plochy (různé tloušťky a různé provedení – lepené sklo, kalené sklo, laminované sklo, drátové sklo...).

### 2.2.4 Kritéria falešných poplachů

Kontaktní čidla mohou být citlivá na silný dopravní ruch v okolí zajištěné skleněné plochy a na úmyslné vytváření skřípavých zvuků poblíž kontaktních čidel. U akustických čidel zvláště s jednopásmovým vyhodnocováním je nutné pečlivě zvažovat možné negativní vlivy okolního prostředí. Zde je třeba brát v úvahu:

- technické vybavení prostor – zvonky, telefony, faxy, počítače...,
- dostupnost skleněných ploch zvenčí,
- okolní dopravní provoz se skřípavými zvuky tramvají, vlaků či brzd autobusů,
- blízkost kontejneru nočního podniku, kam se v noci mohou vysypávat prázdné láhve,
- přítomnost drobné zvěře v objektu (ptáci, hlodavci, hmyz – hlavně cvrčci).

Kvalitní utěsnění oken a pevné osazení skel tak, aby nemohla vibrovat např. ve větru, je nezbytnou podmínkou spolehlivého provozu.

### 2.2.5 Nastavení, údržba

Z hlediska nasazení jednotlivých typů musíme vycházet z charakteru provozu zabezpečovaného prostoru, provedení a velikosti ploch ke střežení a dosahu garantovaného v návodu výrobcem.

U čidel s možností nastavení dosahu se při testování nastaví minimální dosah pro ještě spolehlivou detekci poplachového podnětu. Snižuje se tím náchylnost na plané poplachy. Je-li to možné provozně i ekonomicky, je vhodné skutečnou funkci akustického čidla ověřit v reálných podmínkách nasazení. K tomuto účelu nabízejí výrobci speciální akustické testery, které obsahují digitální paměťový modul s navzorkovaným zvukem tříštěného skla. Při aplikaci akustických čidel tříštění skla je třeba brát v úvahu i možné snížení účinnosti čidel při zastínění záclonami, závěsy a vertikálními žaluziemi. To platí i při aplikaci bezpečnostních fólií na sklo. Zde je nutné počítat s tlumením typického tříštivého zvuku, a na tyto podmínky je nezbytné funkci čidel ověřit.

Testery je vhodné využívat při nastavování citlivosti a při kontrole funkce akustických čidel v provozu. Je-li na smyčku připojen větší počet čidel, je vhodné používat čidla s optickou indikací aktivace (LED), a pro usnadnění údržby i s pamětí poplachu.

Funkci kontaktních čidel můžeme ověřit poklepem šroubováku, úderem ocelového pera poblíž čidla či pohybem navlhčeného kousku pěnového polystyrenu po chráněné ploše.

Při kontrole funkce akustických čidel tříštění skla je nutné ověřit, zda není zvuk příliš tlumen zařízením interiéru, které při instalaci akustického čidla v interiéru nebylo (závěsy, záclony, obložení stěn a stropu...).

### 2.3 Mechanické kontakty

Jsou to mikrosplínače konstrukčně uzpůsobené pro zabudování do rámu proti západce zámku. Střeží uzamčený stav prostupů. Při vhodném zapojení k ústředně EZS zabrání uvedení do stavu střežení v případě, že některý z prostupů není uzamčen. Užívají se především v případech, má-li střežený prostor více možných vstupů.

Mezi mechanické kontakty patří i nájezdy, jež umožňují uzavření elektrického obvodu v případech, když je třeba přivést proud do čidla na posuvný či otočný díl osazení stavebního otvoru. Nájezd současně střeží daný prostup na jeho otevření.

U nás se mechanické kontakty příliš nevyužívají. Jsou doménou ve starších systémech EZS budovaných podle pravidel VdS\*) v SRN.

\*) *Verband der Sachversicherer e. V. – svaz pojišťoven v SRN*

### 2.4 Vibrační čidla

K prvkům střežení pláště budov dále patří vibrační čidla pro hlídání průrazu stěn a stavebních konstrukcí. Základem je zde elektromechanický měnič doplněný vyhodnocovací elektronikou. Tato čidla mají větší šířku pásma vyhodnocovaných kmitočtů, nastavitelnou citlivost a optickou indikaci s pamětí. Osazují se podle konstrukčního provedení na riziková místa možného průchodu zdí, luxfery či na rámy dveří a oken. Vzhledem ke své konstrukci nejsou určena pro střežení trezorových skříní a komorových trezorů.

### 2.5 Poplachové fólie, tapety, polepy a poplachová skla

Tato čidla pracují na principu přerušení vodivého média, nejčastěji jemného drátku uvnitř zmiňovaného nosiče (fólie, tapety, skla), či pásků vodivé fólie aplikovaných samostatně na povrch hlídané plochy (polepy). Polepy jsou dostatečně známy z dřívější éry zabezpečování, neboť byly nejužívanější a viditelnou formou střežení skleněných ploch výkladních skříní a oken obchodů. Dnes jsou neprávem opomíjeny, a zvláště plošné aplikace meandru na vnitřní straně dveří vstupu do střeženého prostoru jsou hodny vzkříšení. Při montáži je důležité orientovat přípojný místo vždy k horní hraně plochy tak, aby bylo chráněno před možnou kondenzací páry, jež by mohla snížit životnost a spolehlivost spojení.

Podstatným problémem zůstává vysoká náročnost vlastního řemeslného provedení všech variant střežení pláště objektů uvedených v této části.

### 2.6 Drátová čidla

Jedná se o jemná ocelová lanka propojená s citlivým mikrospínačem. Jsou vhodná pro střežení velkých prostupů ventilace a prostupů inženýrských sítí do objektu. Pro usnadnění montáže nabízejí výrobci rozsáhlé příslušenství prostředků k jejich upevnění, a dokonce i převodové kladky. Správně instalovaná drátová čidla reagují již na malé zvýšení mechanického napětí.

### 2.7 Rozpěrné tyče

Tento typ čidla je vlastně miniaturní mechanický spínač, jehož klidový stav je mechanicky aretován tyčí. Rozpěrné tyče mohou chránit vstupní otvory objektu z inženýrských sítí a prostupy ventilace v rámci objektu podobně jako drátová čidla.

## 3 Prvky prostorové ochrany (čidla prostorová)

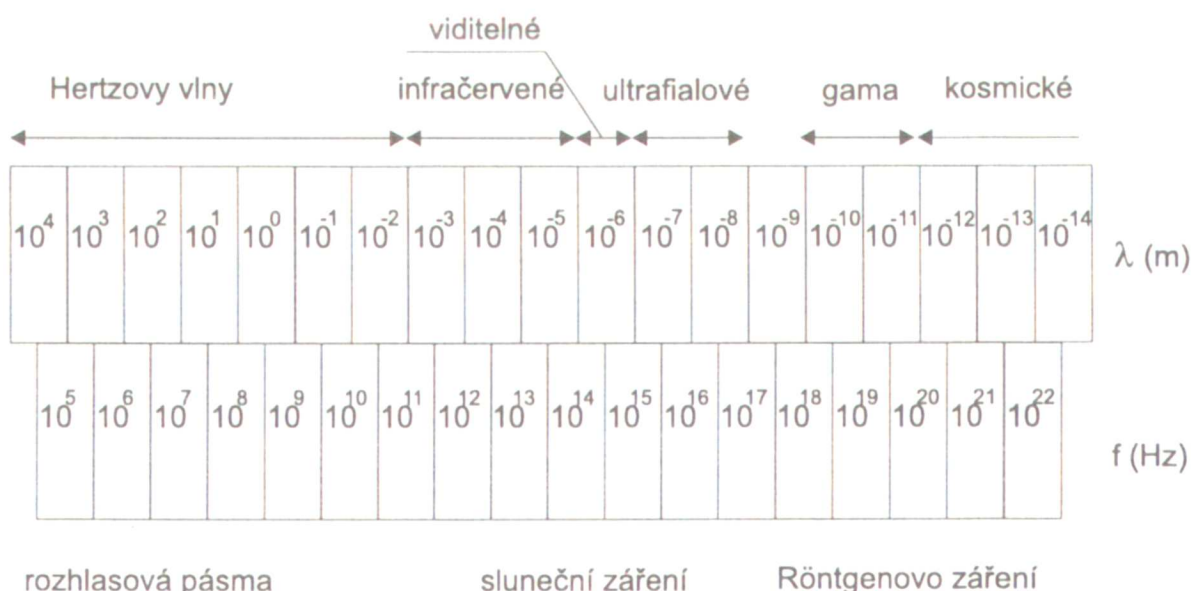
Prostorová ochrana tvoří velice dobrou alternativu, popř. doplnění k současně nejlepší formě střežení - plášťové ochraně. Základní dělení je na **čidla pasivní a čidla aktivní**.

- **Čidla pasivní** – při zjišťování charakteristických rysů napadení pouze registrují fyzikální změny ve svém okolí.
- **Čidla aktivní** – při zjišťování charakteristických rysů napadení vytvářejí své pracovní prostředí aktivním působením na své okolí a detekují změnu takto vytvořeného fyzikálního prostředí.

V praxi je možné se setkat s několika druhy **čidel pohybu**. Jedná se o:

- pasivní infračervená čidla (Passive Infra Red – PIR),
- aktivní ultrazvuková čidla (Ultrasonic – US),
- aktivní mikrovlnná čidla (Microwave – MW),
- duální (kombinovaná) čidla (PIR – US, PIR – MW).

Každé z těchto čidel využívá ke své funkci odlišnou část kmitočtového spektra elektromagnetického vlnění. Ultrazvuková čidla využívají vlnění mechanické.



Obr. 3-6: Spektrum elektromagnetického vlnění.

Každý druh čidla má určité vlastnosti, jež jsou výsledkem úrovně vývoje zpracování signálu a výsledkem úrovně technologie daného výrobce. V rámci trhu se proto objevují vedle základních typů i různé modifikace využívající stejné fyzikální principy, ale doplněné o další speciální funkce z hlediska zpracování signálu. Zde se velice často objevují v sortimentu PIR čidel funkce počítání impulsů nutných k vyhlášení poplachu, dále jsou často aplikovány pyrosenzory v dvojitém či čtyřnásobném provedení a k vyhodnocení dochází paralelně. Při vlastní aplikaci přinášejí tyto funkce vyšší odolnost proti falešným poplachům způsobeným vlivem okolí (proudění vzduchu, osvětlení atd.). Obecně lze však říci, že nepřinášejí vyšší úroveň bezpečnosti z hlediska napadení. Správně aplikované čidlo jednoduššího technologického provedení může uživateli sloužit stejně spolehlivě při nižších nákladech na zařízení. Existují však objekty, kde se bez čidel dražších, ale spolehlivějších a odolnějších proti vlivům okolí, neobejdeme.

Z hlediska aplikace nabízejí některé typy čidel (nezávisle na užitém fyzikálním principu) další luxusní funkce. Jsou to:

- **Dálkové odpínání indikační LED**, které usnadní montážní organizaci i uživateli testování funkce a dosahu čidel v provozu, při servisních zásazích a při pravidelných kontrolách a revizích.
- **Odpínání mikrovlnné či ultrazvukové vysílací části čidel**, neboť u citlivějších osob může při dlouhodobém pobytu v prostorech s ultrazvukovým či mikrovlnným polem dojít ke zdravotním potížím.
- **Paměť poplachu** a dálkový reset této paměti, které umožní identifikaci narušení prostoru či poruchu čidla v případech, je-li na jedinou smyčku připojeno těchto čidel více.

Další doplňkovou funkcí, která oproti předcházejícím přináší vyšší úroveň bezpečnosti, je funkce **ochrany proti zastínění** (tzv. antimasking). Tato funkce je aktivní i v době klidu objektu a slouží k indikaci zastínění čidla. Čidla s touto funkcí se aplikují v prostorech veřejně přístupných, kde je riziko sabotáže systému s cílem připravit si objekt na vloupání ve stavu střežení. Výstup této indikace bývá projektován podle použitého typu ústředny a režimu objektu buď na samostatnou smyčku, popř. bývá funkčně spjat s příslušnou poplachovou smyčkou, do níž je dané čidlo připojeno.

Důvody pro nasazení čidel s funkcí antimasking mohou být dva:

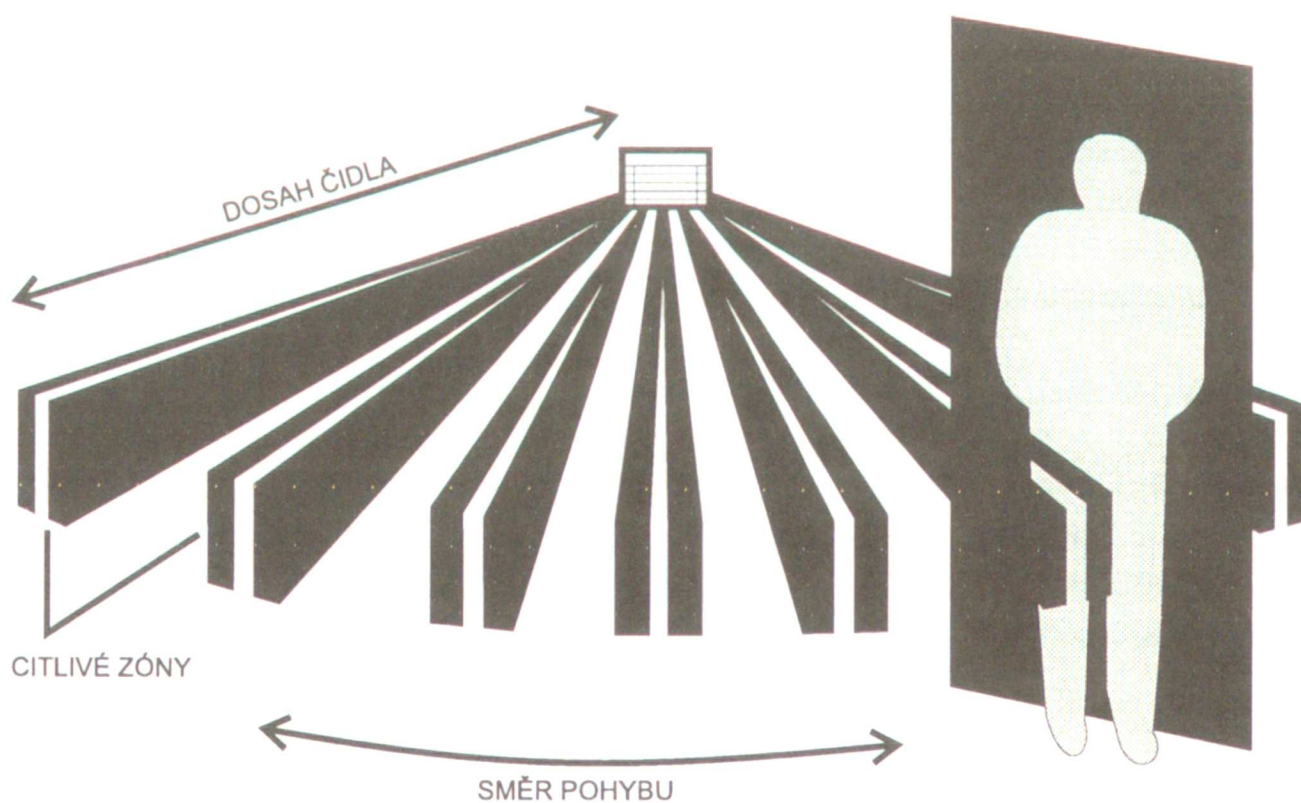
- V objektu se strážní (stálou či denní) službou – požadavek okamžité indikace zastínění čidla či jeho přestříkání barvou.
- V objektu bez strážní služby – požadavek zabránění uvedení do stavu střežení, je-li některé z čidel vybavených funkcí antimasking zastíněno.

### 3.1 Pasivní infračervená čidla

#### 3.1.1 Princip funkce a praktické provedení

Obvykle jsou tato čidla označována jako PIR čidla (Passive infra red sensor). Jsou založena na principu zachycení změn vyzařování v infračerveném pásmu kmitočtového spektra elektromagnetického vlnění. Využívají skutečnosti, že každé těleso, jehož teplota je vyšší než  $-273\text{ }^{\circ}\text{C}$  (absolutní nula) a nižší než  $560\text{ }^{\circ}\text{C}$ , je zdrojem vyzařování vlnění v infrapásmu odpovídacím teplotě tělesa. Směrem k vyšším teplotám se posouvá spektrum ke kratším vlnovým délkám, tedy k oblasti viditelného spektra. Takové vlnění přestáváme vnímat jako teplo a začínáme je vnímat jako světlo. Pro teplotu lidského těla cca  $35\text{ }^{\circ}\text{C}$  je charakteristická vlnová délka  $9,4\text{ mm}$ . Tohoto jevu je využito k zachycení pohybu těles, jež mají odlišnou teplotu od teploty okolí. Jako detektor je užit materiál vykazující pyroelektrický jev. Detekční prvek je měnič gradientní povahy, to znamená, že není schopen z principu detekovat stálou úroveň záření, ale jen změny záření na detektor dopadajícího. Obraz střeženého prostoru v infračerveném pásmu je transformován prostřednictvím optiky na plochu senzoru. Zorné pole je rozděleno na aktivní a neaktivní zóny, které si můžeme představit v analogii optického zobrazení jako viditelné a zakryté části obrazu střeženého prostoru. Pohybuje-li se tedy těleso, jehož teplota je odlišná od teploty okolí (pozadí) v zorném poli čidla PIR, zachycuje čidlo změny při přechodu cíle z aktivní do neaktivní zóny a naopak. Elektronika vyhodnotí signál těmito změnami vyvolaný a způsobí vyhlášení poplachu.

Tvar zorného pole je závislý na provedení optiky, dosah je závislý na kvalitě optiky čidla, citlivosti použitého senzoru a způsobu vyhodnocení. Volbou odpovídající optiky je možné střežit prostor do vzdálenosti cca  $15\text{ m}$  od čidla či dlouhé prostory do cca  $60\text{ m}$ . U čidel pro stropní montáž lze kruhovým uspořádáním optiky obsáhnout velkou plochu v rozsahu  $360^{\circ}$ .

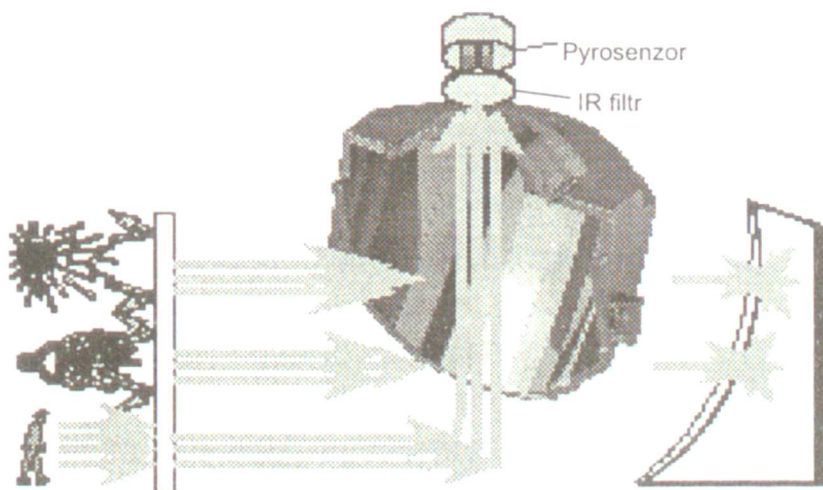


Obr. 3-7: Princip zachycení pohybu PIR čidlem.

V praxi je možné se setkat s optikou dvojího druhu: buď se jedná o zobrazení pomocí soustavy **Fresnelových čoček**, nebo je optika vytvořena soustavou křivých zrcadel. Optika vždy transformuje obraz zorného pole do podoby, jež dalšímu elektrickému zpracování výstupního signálu pyrosenzoru vyhovuje nejlépe.

Porovnáním těchto dvou druhů optiky lze říci, že užití Fresnelových čoček je řešení velice ekonomické, i přes určité nedostatky způsobené tím, že zobrazení pomocí Fresnelových čoček nedává ideální optický obraz skutečnosti. Naproti tomu optický obraz vytvořený pomocí soustavy křivých zrcadel je prakticky zobrazení bez kompromisu. Výroba křivých zrcadel je však v porovnání s Fresnelovými čočkami náročnější na návrh a technologii výroby. Z tohoto důvodu je možné se setkat se zrcadlovou optikou především u čidel tradičních značkových výrobců. Rovněž dosah čidel garantovaný výrobcem je zde díky lepšímu optickému zobrazení větší v porovnání s čidly srovnatelného tvaru detekční charakteristiky s Fresnelovou čočkou.

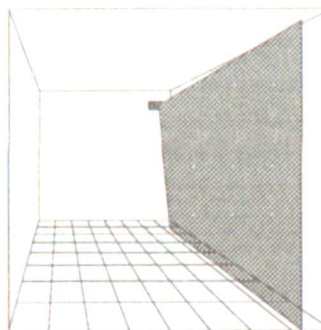
Někteří výrobci nabízejí alternativu tzv. **černých zrcadel**, která principiálně omezují odrazivost v oblastech mimo požadované infračervené spektrum. Toto koncepční řešení podstatně snižuje náchylnost čidel k planým poplachům vyvolaný vlivem záření o vysoké energii ve viditelném spektru (odlesky slunce, reflektory automobilů apod.).



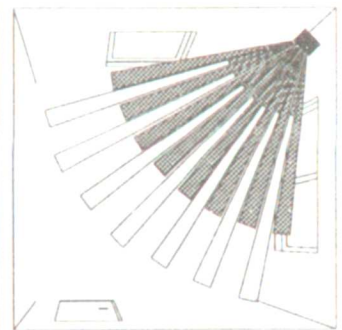
Obr. 3-8: Princip funkce černého zrcadla.

Obr. 3-9: Varianty detekčních charakteristik PIR čidel pohybu.

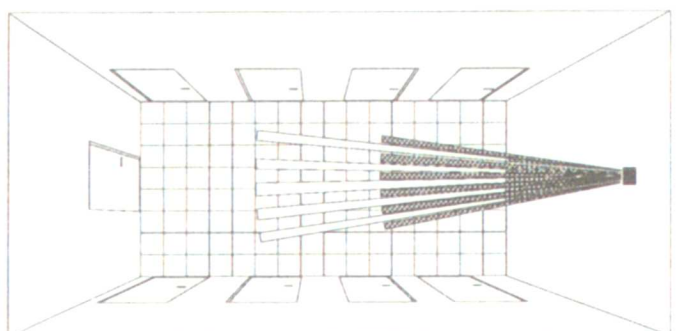
TYP ZÁVĚS



TYP VĚJÍŘ



TYP CHODBA



### 3.1.2 Použití a montáž

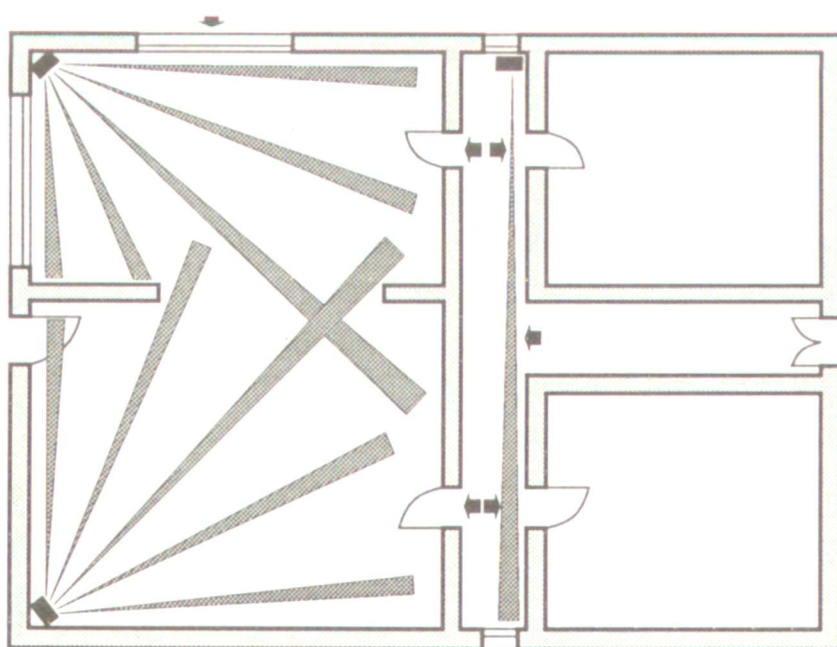
Těžištěm prostorové ochrany jsou centrální body budovy – schodišťové přístupy či výstupy, haly, spojovací chodby a vnitřní komunikační uzly.

Díky nižší náročnosti na montáž mnohdy supluje prostorová ochrana ochranu pláštěvovou. V odůvodněných případech, zvláště v objektech s nízkými riziky napadení a při umístění čidel v takových místech, aby skutečně pokrývala nejpravděpodobnější místa vniknutí z vnitřní strany pláště objektu, lze tento především ekonomický argument připustit. Nahradit pláštěvovou ochranu však nikdy nemůže, neboť pláštěvová ochrana je na rozdíl od ochrany prostorové schopna detekovat vniknutí pachatele s minimální časovou prodlevou. Zůstává pak delší čas na intervenci (zásah).

*Poznámka – Skutečností ale zůstává, že kvalitní montáž pláštěvové ochrany je základem ochrany objektů, přestože řemeslně precizní zvládnutí montáže magnetických kontaktů a čidel na ochranu skleněných ploch je výrazně náročnější než montáž prostorových čidel.*

Zásady instalace PIR čidel lze shrnout do několika bodů:

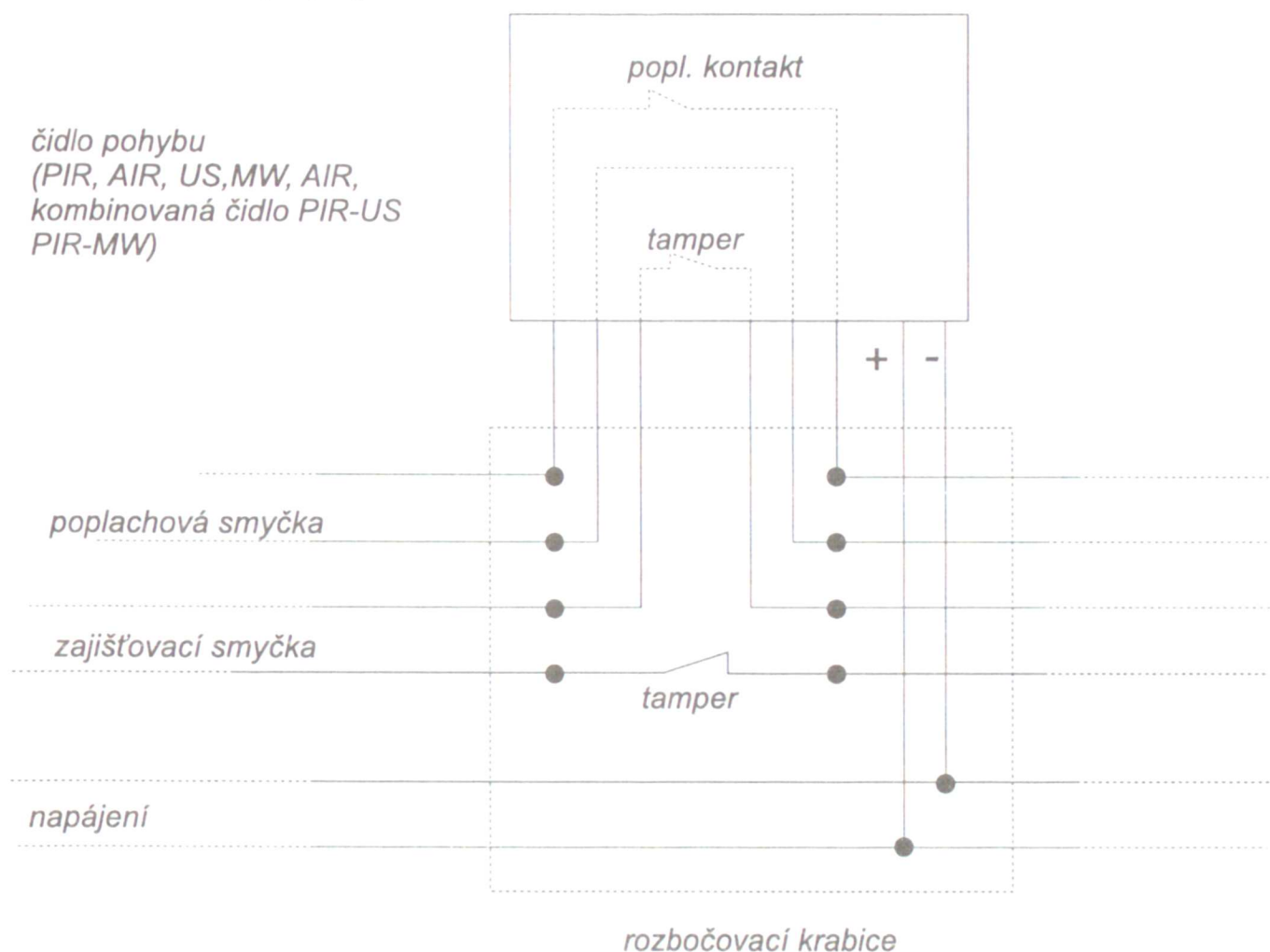
- PIR čidla se mají instalovat tak, aby pravděpodobný směr pohybu pachatele byl kolmý (tangenciální) na myšlený průmět aktivní či neaktivní zóny do půdorysu střeženého prostoru (viz Obr. 3-10).
- Umístění na stavebně pevném podkladu bez vibrací je předpokladem spolehlivé funkce všech druhů prostorových čidel.
- Více PIR čidel je možné instalovat do jednoho prostoru bez nebezpečí vzájemného ovlivňování, neboť nevyzařují žádnou energii.
- Jelikož je PIR čidlo aktivováno pouze tangenciální složkou pohybu pachatele ve vztahu k rozložení aktivních a neaktivních zón, doporučuje se v případě nutnosti úplného vykrytí prostoru instalace více čidel k vzájemnému překrytí zón.
- U prostor s podlahovým vytápěním se od nasazení PIR čidel upouští
- PIR čidla nesmějí být nasměrována na okna, vnější dveře a vrata.



Obr. 3-10: Příklad správného umístění PIR čidel.



### 3.1.3 Elektrické připojení



Obr. 3-11: Elektrické zapojení čidel pohybu.

### 3.1.4 Kritéria falešných poplachů

- PIR čidla nesmějí být vystavena následujícím vlivům:
- ventilace – vstupy a výstupy, průvan,
- přímé nebo nepřímé vyzařování světla (slunce, reflektory),
- proměnné zdroje tepla (topení, komíny),
- spínané rušivé IR zdroje (žárovky).

### 3.1.5 Nastavení, údržba

Nastavování vychází z instalačních manuálů výrobců jednotlivých typů PIR čidel. Obecně lze říci, že většina PIR čidel nemá z principu funkce jemné dostavování dosahu čidla. Často však je možné přizpůsobit snímací charakteristiku výšce montáže čidla. Technicky je potom naklápění snímací charakteristiky v rozmezí jednotek stupňů (cca +/- 5°) řešeno vertikálním posuvem celé desky elektroniky v krytu čidla nebo naklápěním soustavy křivých zrcadel.

V rámci pravidelné údržby je nutné kontrolovat, zda není čidlo zastíněno např. změnami v interiéru (záclony, závěsy, žaluzie, skříně, kontejnery, bedny apod.), pravidelně ověřovat dosah čidla z důvodu zašpinění či zaprášení Fresnelovy čočky či zrcadlové optiky snímacího systému. K pravidelné kontrole patří samozřejmě i funkce zajišťovacího kontaktu krytu čidla.

### 3.2 Ultrazvuková čidla

#### 3.2.1 Princip funkce a praktické provedení

Ultrazvuková čidla (Ultrasonic sensor – US) využívají část spektra mechanického vlnění nad pásmem kmitočtu slyšitelných lidským uchem (pozor při aplikaci, některá zvířata jej slyší – pes, netopýr, komár). Jsou aktivní – to znamená, že do prostoru vysílají energii.

Vysílač vysílá vlnění o stálém (konstantním) kmitočtu. Přijímač přijímá vlnění odražené od překážek v uzavřeném prostoru. V klidovém stavu elektronika vyhodnotí přijatou vlnu ve stále stejném vztahu k vlně vyslané. Pohybuje-li se v prostoru libovolné těleso, mění se fáze přijatého vlnění. Tato změna fáze je vyhodnocena elektronikou a vede k vyhlášení poplachu. Jedná se v podstatě o aplikaci Dopplerova jevu v pásmu ultrazvukových kmitočtů. Dopplerův efekt lze matematicky interpretovat následujícím vztahem:

$$f_1 = \frac{f}{1 - \left(\frac{v}{c}\right)}$$

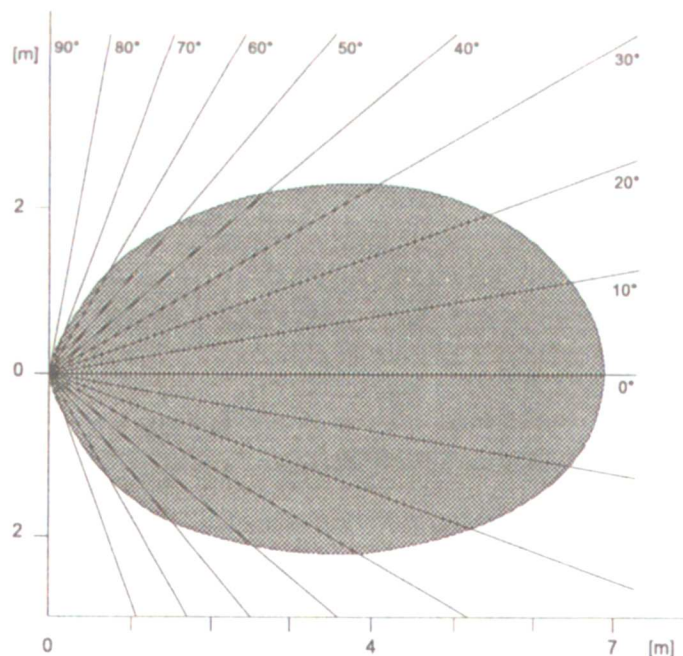
kde  $f$  je kmitočet přijatý přijímačem

$f$  je kmitočet vyslaný vysílačem

$v$  je rychlost pohybu odrazné plochy (v našem případě pachatele)

$c$  je rychlost pohybu vlnění užitého k detekci (rychlost zvuku u US čidla, rychlost pohybu elektromagnetického vlnění u MW čidla)

Tento jev lze demonstrovat v oblasti slyšitelného spektra na známém školním příkladu houkajícího vlaku blížícího se k železničnímu přejezdu. Při přibližování vlaku se posluchači stojícímu u přejezdu zdá, jako by kmitočet zvuku rostl, při odjezdu jako by klesal. U ultrazvukových čidel nás nezajímá absolutní velikost této odchylky, ale pouhá přítomnost této odchylky větší než je nestabilita systému.



Obr. 3-12: Typický příklad charakteristiky US čidla ve volném prostředí.

### 3.2.2 Elektrické připojení

Elektrické připojení je stejné jako na obr. 3-11. Připojení řízení doplňkových funkcí je specifické a liší se podle konkrétního typu.

### 3.2.3 Použití a montáž

Z hlediska aplikace US čidel je nutné znát následující pravidla:

- US čidla pohybu mají být instalována tak, že pravděpodobný pohyb pachatele směřuje k čidlu či od něj (radiálně) – typický dosah je cca do 10 m.
- Prostor musí být uzavřený, aby dosah čidla nemohl přesahovat mimo prostor určený ke střežení.
- V prostorech, kde jsou uloženy předměty absorbující ultrazvuk (koberce, pěnové materiály), musíme mít na zřeteli, že se citlivost čidel může značně změnit oddálením či přiblížením těchto předmětů. Zde se nachází nebezpečí, že čidlo bude po změně buď citlivé příliš, nebo málo.
- Předměty umístěné do blízkosti čidel až po jejich instalaci a nastavení mohou způsobit falešné poplachy ovlivněním citlivosti čidel.
- U prostor s často se měnícím stavem interiéru (sklady) by se mělo od užití US čidel upustit.

### 3.2.4 Kritéria falešných poplachů

Více ultrazvukových čidel pohybu se smí v jednom prostoru instalovat pouze tehdy, jsou-li vysílače synchronizovány nebo kmitočtově tak stálé, že není možné vzájemné negativní ovlivňování. US čidla pohybu se nesmějí instalovat:

- na zavěšené montážní konstrukce,
- nad topná tělesa,
- v prostorách s teplovzdušným topením,
- v blízkosti zdrojů zvuku se širokým kmitočtovým spektrem (telefon),
- v prostorách s volně zavěšenými tělesy (lampy, reklamní štíty),
- v prostorách, kde se pohybují v době střežení zvířata (hlodavci, holubi...).

### 3.2.5 Nastavení, údržba

Nastavování vychází z instalačních manuálů výrobců jednotlivých typů ultrazvukových čidel. Obecně lze říci, že všechna ultrazvuková čidla mají možnost jemného dostavování dosahu. Při nastavování postupujeme od nejmenšího dosahu. V okamžiku, kdy dosáhneme požadovaného pokrytí, již výkon ultrazvukového měniče nezvyšujeme. V takovém stavu má čidlo optimální dosah při minimální náchylnosti k falešným poplachům.

V rámci pravidelné údržby je nutné kontrolovat, zda se nezměnily akustické vlastnosti prostoru, v němž je čidlo nasazeno. Ty mohou být ovlivněny např. změnami v interiéru – obklady stěn či stropu, novými záclonami, závěsy, žaluziemi, jiným uspořádáním skříní, kontejnery, bednami atd. Při jakékoli změně v interiéru je pak třeba dosah čidel znovu nastavit. K pravidelné kontrole patří samozřejmě i kontrola funkce zajišťovacího kontaktu krytu čidla.

### 3.3 Mikrovlnná čidla

#### 3.3.1 Princip funkce a praktické provedení

Mikrovlnná čidla (Microwave sensors – MW) Vycházejí ze stejného fyzikální principu jako ultrazvuková čidla, ale v kmitočtovém pásmu elektromagnetického vlnění. Tentokrát se jedná většinou o pásma 2,5 GHz, 10 GHz a nebo 24 GHz. Je to opět aktivní systém zachycení pohybu, principiálně shodný s ultrazvukovými čidly, ale technologicky uzpůsobený danému kmitočtovému pásmu. Výrobci přešli dnes již výhradně od použití technologie vlnodů, která je nákladná na výrobu a nastavení, k realizaci v podobě mikropáskového vedení integrovaného do desky plošných spojů. Toto řešení výrazně snížilo ceny mikrovlnných čidel v hromadné výrobě, a tím zvýšilo jejich dostupnost.

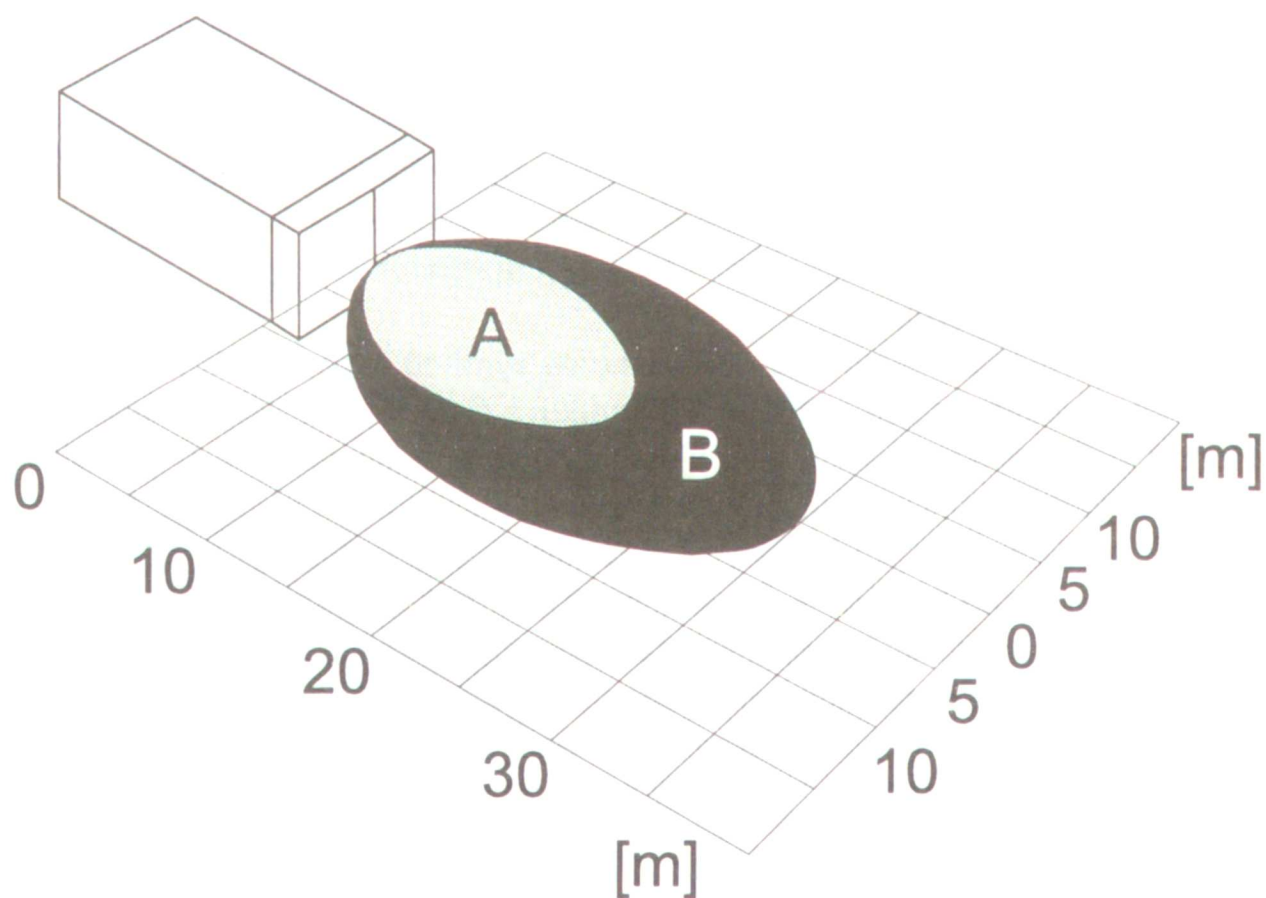
Nejčastěji užívané pásmo X je shodné např. s pásmem družicové televize. Zde nás ovšem nezajímá modulační obsah či absolutní velikost odchylky kmitočtu, ale pouze její přítomnost.

#### 3.3.2 Elektrické připojení

Elektrické připojení je obdobné jako na obr. 3-11. Připojení řízení doplňkových funkcí je specifické a liší se podle konkrétního typu.

#### 3.3.3 Použití a montáž

Mikrovlnná čidla pohybu se mají instalovat tak, aby pravděpodobné směry pohybu pachatele vedly ve směru k čidlu či od čidla – radiálně (obdobně jako u ultrazvukového čidla).



Obr. 3-13: Typické charakteristiky mikrovlnných čidel ve volném prostředí (A, B varianty s nižším a vyšším dosahem).

Mikrovlnná čidla pohybu se musí instalovat tak, aby podněty mimo střežený prostor neovlivňovaly činnost čidla. Protože mikrovlny pronikají skleněnými plochami tenkými stěnami a např. ze dřeva, tvrzeného papíru, plastické hmoty mohou též pohyby mimo střežený prostor vést k aktivaci mikrovlnného čidla (např. projíždějící vozidla, výtahy, voda protékající v plastových trubkách...).

### 3.3.4 Kritéria falešných poplachů

- V blízkosti mikrovlnných čidel se nesmí nacházet žádné velké objekty z kovu. Zvláště kritické jsou objekty s rovinným povrchem, od kterého se mikrovlny odrážejí a mění tím výrazně detekční charakteristiku.
- Mikrovlnná čidla se nemohou aplikovat v prostorách, v nichž může ve stavu střežení objektu docházet ke spínání zářivkového osvětlení.
- V jednom prostoru se smí použít více mikrovlnných čidel jen tehdy, pracují-li na jiné vysílací frekvenci nebo jsou-li aplikovány tak, že je vyloučeno jejich vzájemné negativní ovlivňování.

### 3.3.5 Nastavení, údržba

Nastavování vychází z instalačních manuálů výrobců jednotlivých typů MW čidel. Obecně lze říci, že všechna mikrovlnná čidla mají možnost jemného dostavování dosahu čidla. Při nastavování postupujeme od nejmenšího dosahu. V okamžiku, kdy dosáhneme požadovaného pokrytí, již výkon mikrovlnného měniče nezvyšujeme. V takovém stavu má čidlo optimální dosah při minimální náchylnosti k falešným poplachům. Zde je třeba uvažovat i o teoretické možnosti cílené detekce přítomnosti mikrovlnného čidla a jeho zarušení elektromagnetickým polem.

V rámci pravidelné údržby je třeba kontrolovat, zda se nezměnily elektromagnetické vlastnosti prostoru, v němž je čidlo nasazeno. Ty mohou být ovlivněny např. změnami v interiéru jako jsou velké kovové předměty (sítě, mříže, oplechované dveře). Při podstatné změně v interiéru je vždy nutné dosah čidel znovu nastavit.

K pravidelné kontrole patří samozřejmě i funkce zajišťovacího kontaktu krytu čidla.

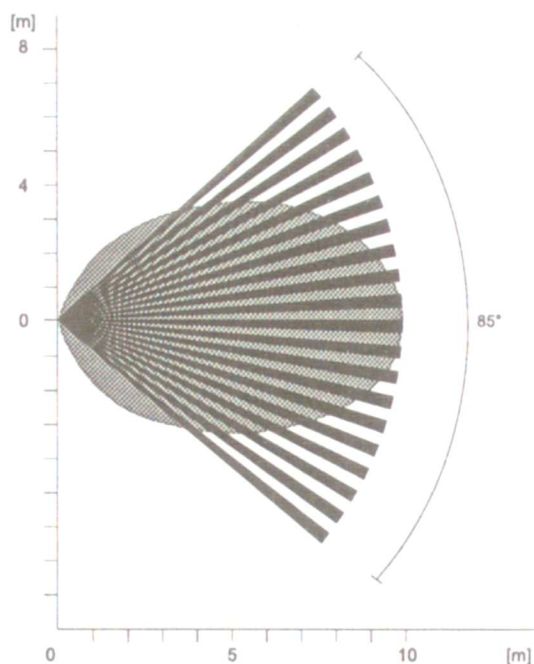
## 3.4 Kombinovaná (duální) čidla

V prostorách s obtížnými podmínkami nasazení, s výrazným negativním vlivem okolního prostředí, se nabízí využití kombinovaných čidel PIR - US či PIR - MW. Vlastní myšlenka pro vývoj kombinovaných (duálních) čidel vychází ze zásady, že je zanedbatelná pravděpodobnost současného vzniku jevů, které by mohly vyvolat planý poplach u více čidel pracujících na různých fyzikálních principech. Aplikace dvou odlišných fyzikálních principů v konjunkci snižuje rizika falešných poplachů vlivem prostředí známá u jednosystémových čidel, neboť rizikové faktory falešných poplachů se pro jednotlivé systémy liší.

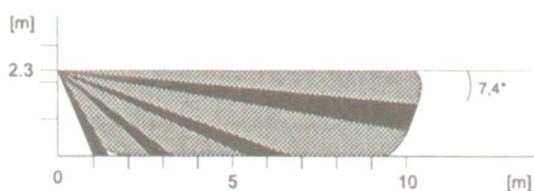
### 3.4.1 Použití a montáž

Pro instalaci kombinovaných (duálních) čidel je nutné v zásadě vycházet z pravidel, která jsou platná pro jednotlivé systémy v čidlech užitých. K jejich nasazení přistupujeme teprve při velice nepříznivých podmínkách s ohledem na vyhlašování planých poplachů.

Je třeba si uvědomit, že práh detekce je u těchto čidel díky použitému principu posunut poněkud výše oproti jednosystémovým čidlům.



Obr. 3-14: Typická charakteristika kombinovaného čidla (PIR – US).



## 4 Prvky tísňového hlášení

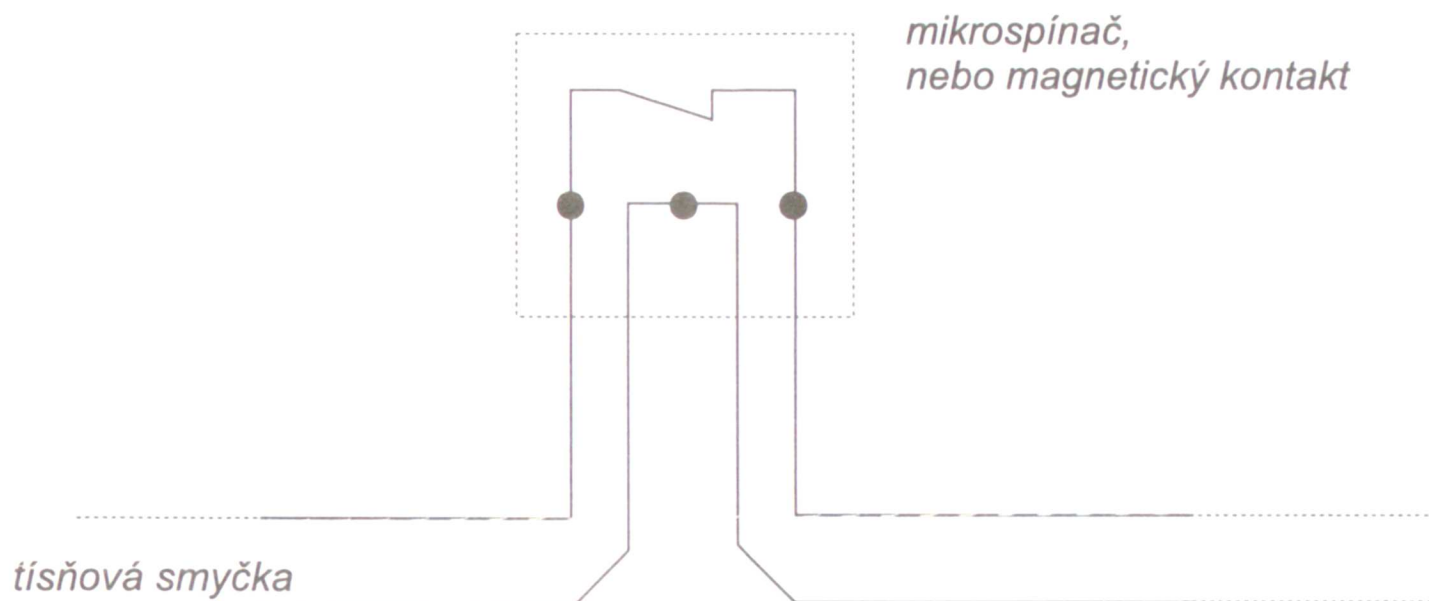
Slouží k ochraně zaměstnanců a veřejnosti v případě přímého ohrožení. Hlášení do místa, odkud může být poskytnuta pomoc, je vyvoláno buď přímým manuálním aktem, nebo zprostředkovaně při definovaném způsobu manipulace, popř. automaticky bez jakéhokoli příspěvní obsluhy či nositele.

### 4.1 Veřejné tísňové hlásiče

#### 4.1.1 Funkce a praktické provedení

Jsou to magnetické kontakty či mikrospínače zapouzdřené do podoby tlačítka. Slouží veřejnosti (popř. klientele) k vyvolání tísňového hlášení.

### 4.1.2 Elektrické připojení



Obr. 3-15: Elektrické připojení tísňových hlásičů.

### 4.1.3 Použití a montáž

Mají být aplikovány na viditelných místech objektu – při schodištích, v chodbách a v halách tak, aby je mohl použít každý, kdo je v nouzové situaci nebo je takové situace svědkem. Může sloužit rovněž k přivolání pomoci při občůzkové službě strážných.

Pokud není hlásič přímo adresován, je účelné užít typ s mechanickou nebo elektronickou pamětí, aby bylo možné při analýze poplachové události zpětně zjistit, který hlásič na smyčce byl aktivován. Kritéria falešných poplachů

Veřejné tísňové hlásiče jsou většinou opatřeny krycím sklem, které je při vědomé aktivaci třeba rozbít. Sklo slouží jako ochrana před náhodným použitím, popř. má zneškodnit zneužití. Falešné poplachu jsou tím eliminovány na minimum.

### 4.1.4 Nastavení, údržba, servis

Vzhledem k jednoduchému provedení není třeba veřejné tísňové hlásiče nijak nastavovat. Během provozu je však nutné pravidelně kontrolovat jejich funkci. Podle provedení hlásiče dodává výrobce přípravky pro testování, aniž by se poškodilo ochranné sklo či plomba. Při testování dbáme též na funkci zpětné signalizace a mechanické či elektrické paměti vyvolání poplachu, jsou-li v systému využity.

## 4.2 Speciální tísňové hlásiče

### 4.2.1 Princip funkce a praktické provedení

Jsou to opět magnetické kontakty či mikrospínače zapouzdřené do podoby vhodné tvarovaného tlačítka či nožní spínací lišty (viz obr. 3-16). Slouží zaměstnancům k nepozorovanému vyvolání tísňového hlášení v případě přímého ohrožení.

### 4.2.2 Elektrické připojení

Je shodné se zapojením na obr. 3-15. Má-li hlásič elektronickou paměť, je k němu nutné přivést od poplachové ústředny napájecí napětí 12 V s možností odpinání při nulování paměti poplachu.

### 4.2.3 Použití a montáž

Mají být aplikovány tak, aby nebyly ze strany zákazníka viditelné. Tzn. tlačítka umístujeme nejčastěji pod horní hranu stolu či pultu, nožní spínací lišty na trnože stolu zespodu či na můstky, peněžní svorky či optická peněžní čidla do peněžních přihrádek.

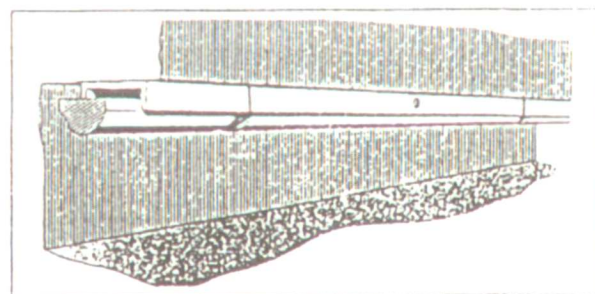
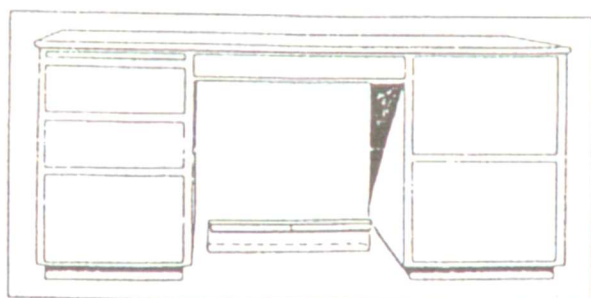
V případě zapojení většího počtu tísňových hlásičů na jednu smyčku je účelné použít prvky s optickou signalizací pro potřeby identifikace planých poplachů způsobených chybou obsluhy i pro zpětnou analýzu poplachové události. V každém případě je důležité dostatečné proškolení obsluhy a pravidelný nácvik chování v kritických situacích.

### 4.2.4 Kritéria falešných poplachů

Skryté tísňové hlásiče nemají ochranu před nechtěným vyhlášením poplachu. Vyhlásování falešných poplachů musíme předejít při návrhu správného umístění těchto prvků tak, aby nedocházelo k nechtěnému vyhlášení poplachu bezděčným pohybem těla (nohy, ruky) či vybavení (např. kancelářská židle) na pracovním místě.

### 4.2.5 Nastavení, údržba, servis

Vzhledem k jednoduchému provedení není třeba skryté tísňové hlásiče nijak nastavovat. Během provozu je však nutné pravidelně kontrolovat funkci skrytých tísňových hlásičů. Při testování dbáme též na funkci zpětné signalizace a mechanické či elektrické paměti vyvolání poplachu, jsou-li v systému využity.



Obr. 3-16: Příklady aplikace nožní spínací lišty.



### 4.3 Automatické tísňové hlásiče

Svým provedením umožňují vyhlášení tísňového poplachu nezávisle na vůli obsluhy – pouze respektováním požadavků případného útočníka.

#### 4.3.1 Princip funkce a praktické provedení

Speciální druh tísňových hlásičů tvoří tzv. čidla poslední bankovky. Vyrábějí se ve dvojitým provedení:

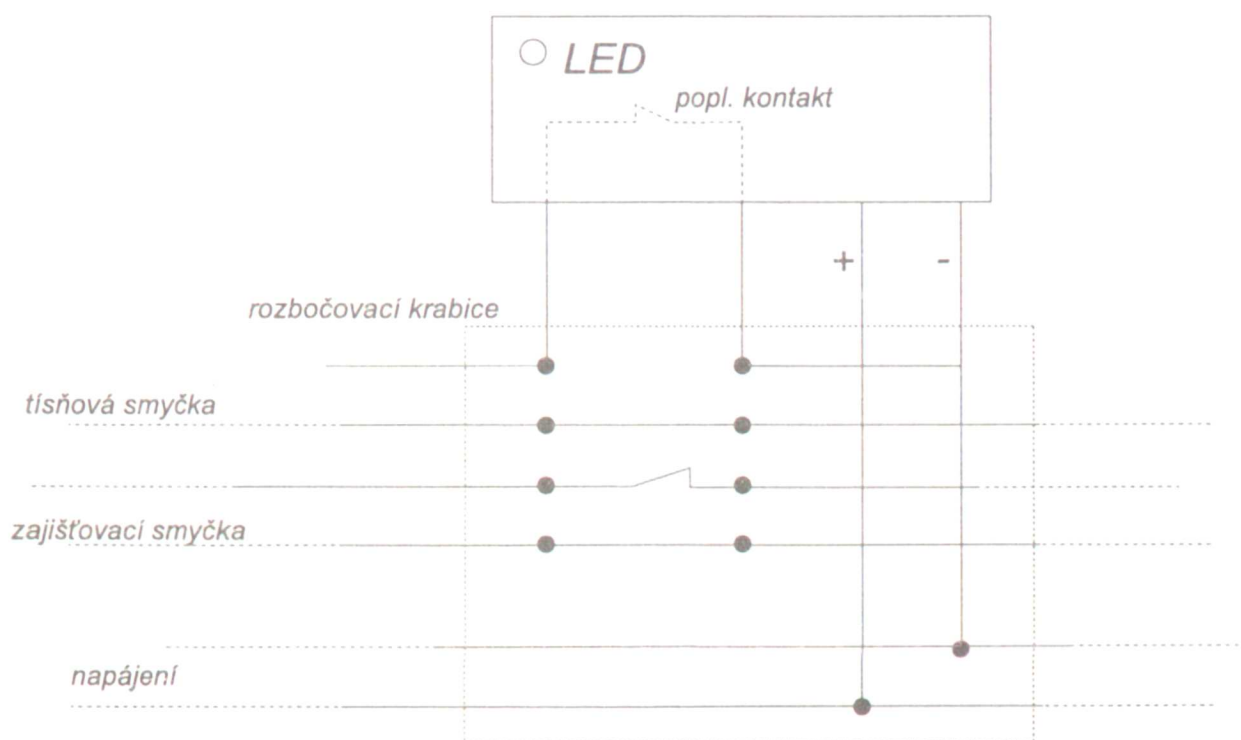
- kontaktní (mechanická) čidla
- bezkontaktní (optoelektronická čidla)

Mechanické kontakty jsou uzpůsobené k zasunutí bankovky do tělesa pouzdra, optická čidla pracují na principu reflexního optoelektronického vazebního členu (optokopleru), tedy bezkontaktně, což je zárukou dlouhodobě spolehlivé funkce.

Optická čidla se vyrábějí ve 3 variantách:

- základní,
- s optickou identifikací a s nastavitelným zpožděním poplachu.

#### 4.3.2 Elektrické připojení



Obr. 3-17: Elektrické připojení optoelektronických reflexních čidel.

#### 4.3.3 Použití a montáž

Mají být aplikována tak, aby nebyla jejich montáž na první pohled patrná. Při aplikaci v peněžních ústavech se umísťují se do peněžních přihrádek a slouží k nepozorovanému vyvolání tísňového hlášení při přepadení. Přes optické čidlo je nutné položit alespoň 10 bankovek kvůli dostatečnému zastínění a k zabránění průniku světla plochou bankovky. Nepatrné rozměry umožňují umístění prakticky do všech používaných typů peněžních přihrádek.

### **4.3.4 Kritéria falešných poplachů**

Pracovní režim elektroniky čidla je nejčastěji pulsní, čímž je docíleno odolnosti proti osvětlení od cizích světelných zdrojů. Čidla jsou odolná proti cizím zdrojům světla do intenzity osvětlení cca 500 lx. Spínací vzdálenost od reflexního optokopleru je 8 – 10 mm. Při montáži je třeba zajistit, aby nemohlo dojít k přímému průniku silného světelného paprsku do prostoru umístění optoelektronických reflexních čidel.

### **4.3.5 Nastavení, údržba, servis**

Během provozu je nutné pravidelně kontrolovat funkci optoelektronických reflexních čidel. Při testování revidujeme též funkci zpětné signalizace a mechanické či elektrické paměti vyvolání poplachu, jsou-li v systému využity. Při provozu je třeba dát pozor na možnost znečištění či zaprášení čelní plochy optokopleru. V rámci pravidelné údržby je také důležité preventivně čistit čelní plochy optokopleru jemným štětečkem na fotografickou optiku.

## **4.4 Osobní tísňové hlásiče**

### **4.4.1 Princip funkce a praktické provedení**

Pracují bezdrátově, výstupní signál vysílaný do prostoru je modulován kódem nastaveným shodně s přijímací stranou. Využívají podle typu různá kmitočtová pásma, nejčastěji pásmo 27 MHz, popř. pásmo 300 MHz či 400 MHz. Existují i varianty pracující na ultrazvukovém principu. Svým provedením jsou podobny buď dálkovému ovládání autoalarmů, či malým pagerům. Dále se vyrábějí bezdrátové tísňové hlásiče v podobě přívěsků, náhrdelníků a náramků.

### **4.4.2 Elektrické připojení**

Vysílač pracuje autonomně bez pevného připojení k systému EZS a je napájen z vlastní baterie či akumulátorku. Přijímač se nejčastěji připojuje svým reléovým výstupem do samostatné poplachové smyčky naprogramované jako smyčka tísňová (aktivní nezávisle na stavu střežení či stavu klidu systému). Přijímač je také možné umístit do skříňe ústředny – pak musíme vyvést přijímací anténu mimo skříň. Při montáži přijímače jinde v objektu je nutné většinou doplnit kryt přijímače o zajišťovací kontakt a zvolit umístění s ohledem na požadovaný dosah. V každém případě by přijímač měl být umístěn tak, aby nebyl náhodnými pozorovateli identifikovatelný a napadnutelný.

### **4.4.3 Použití a montáž**

Osobní tísňové hlásiče se používají v aplikacích, kde je třeba zajistit ochranu osob, jež nejsou vázány na stálé pracovní místo v rámci objektu. Jsou tedy vhodné pro ochranu pracovníků hlídací služby během pochůzky, pro pracovníky v peněžních ústavech při dotaci peněz a pro pracovníky dozorčí služby v rizikových objektech, jako jsou věznice apod. Dosah bezdrátových tísňových hlásičů závisí na použitém typu – zvoleném principu, výkonu a pracovním kmitočtu, na provedení vysílací a přijímací části (příp. antény) a na stavebním provedení objektu. Pro hlásiče pracující s elektromagnetickým vlněním není stavební ohraničení prostoru překážkou, a hlášení je tedy možné přiřadit přímo nositeli bezdrátového tísňového hlásiče.

Zvláštním druhem osobního tísňového hlásiče je hlásič typu „mrtvý muž“. Je to osobní tísňový hlásič používaný v prostředí s vysokými riziky ohrožení personálu. Nejčastěji se s ním lze setkat ve věznicích. Tento hlásič umožňuje kromě cíleného vyhlášení tísňového poplachu i automatický režim v případě pádu. Díky použitému principu přenosu poplachového signálu v pásmu ultrazvukových vln je možné v rámci objektu identifikovat místo vyhlášení tísně či napadení dané omezeným dosahem přijímače ultrazvukových tísňových hlásičů v rámci jediného stavebně ohraničeného prostoru.

#### **4.4.4 Kritéria falešných poplachů**

Poplachové hlášení je vázáno na kódovanou zprávu v pásmu VF či US vlnění. Aktivace přijímače jiným podnětem je málo pravděpodobná s výjimkou překonání hranice odolnosti zařízení proti silným elektromagnetickým, elektrostatickým či v případě US tísňových hlásičů zvukovým polím. Tyto situace jsou málo pravděpodobné a lze jim kvalifikovaným návrhem systému předejít.

#### **4.4.5 Nastavení, údržba**

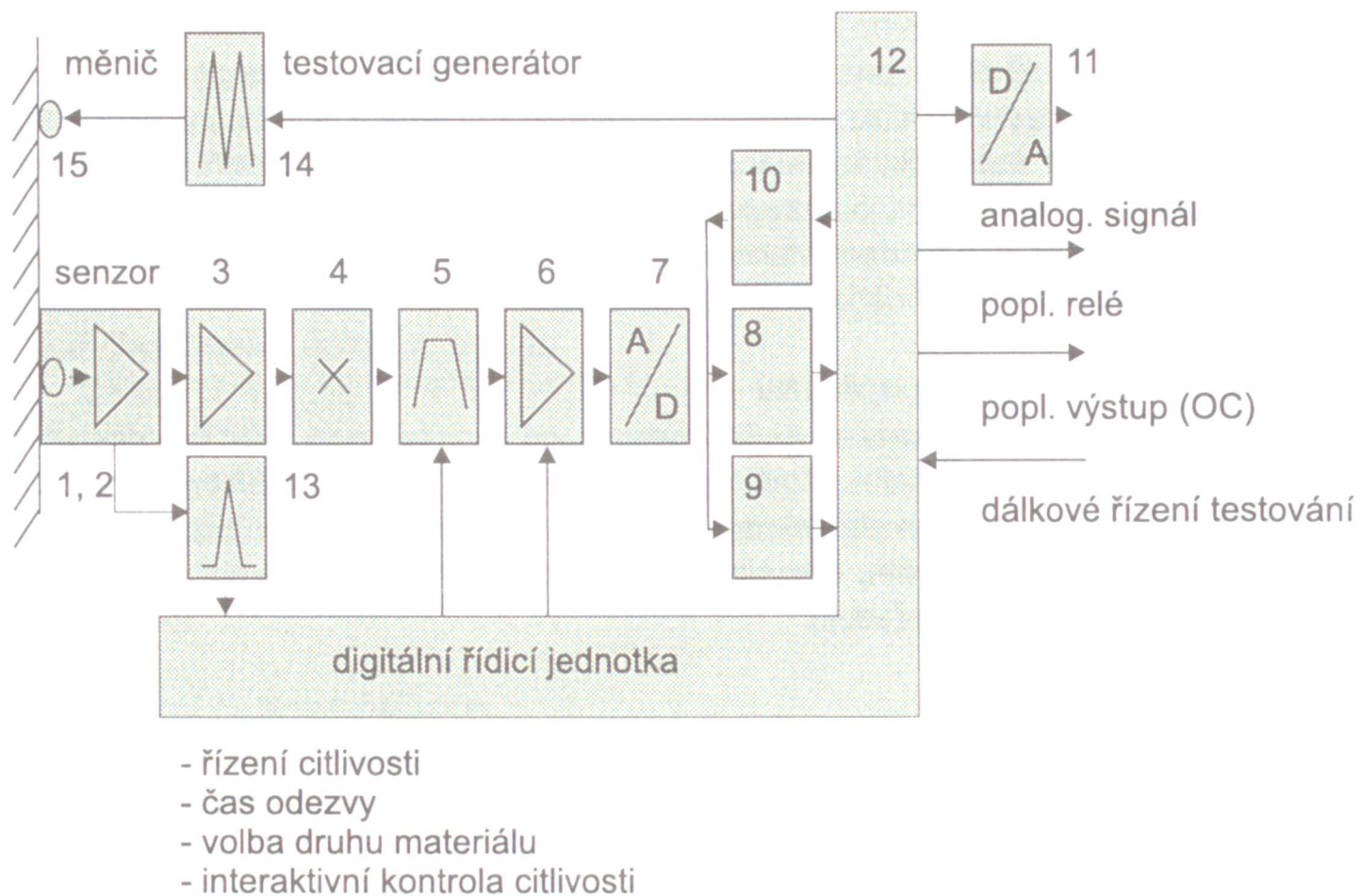
Při oživování systému je nutné pečlivě přetestovat dosah osobních tísňových hlásičů ze všech uvažovaných rizikových prostor. Dosah je vhodné vyznačit v projektu a popsat v uživatelském manuálu. Vzhledem k tomu, že vysílač má svůj autonomní zdroj (baterii), je nezbytné pravidelné testování dosahu a periodická výměna baterií. Především z tohoto důvodu jsou osobní tísňové hlásiče aplikovatelné pouze jako doplňkový prvek tísňové ochrany vedle prvků pevně spojených se systémem (tísňová tlačítka, nožní spínací lišty...).

### **5 Prvky předmětové ochrany**

Pro předmětovou ochranu je možno využít řadu prvků určených původně pro jiné účely např. magnetické kontakty, PIR čidla s charakteristikou záclona, mikrovlnná čidla, infračervené závory, optoelektronická reflexní čidla atd. Speciálně pro vlastní střežení trezorových skříní a komorových trezorů byla vyvinuta tzv. seismická čidla. Dříve se pro tuto úlohu využívala i čidla kapacitní jež však v dnešní době ustupují do pozadí z důvodů náročné montáže, složitého nastavování a náchylnosti k planým poplachům. Další specifickou skupinu předmětových čidel tvoří závěsová a polohová čidla na ochranu uměleckých předmětů.

#### **5.1.1 Princip funkce a praktické provedení**

Jsou to otřesová (seizmická) čidla pracující na principu selektivního zpracování vlnění, jež se šíří pevnými tělesy při jejich mechanickém či termickém opracování. Nejnovější typy využívají při své činnosti digitálního zpracování signálu.



Obr. 3-18: Blokové schéma zapojení otřesového čidla.

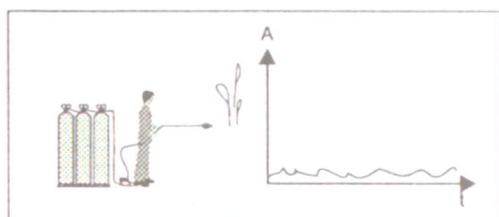
Princip funkce takového otřesového čidla s digitálním zpracováním signálu lze popsat následovně:

Citlivý seizmický detektor (1) snímá vlnění z tělesa, na něž je čidlo připevněné, a elektronika selektivně zpracovává a vyhodnocuje podněty z okolí. Po impedančním působení mikrofону (2) je signál veden do předzesilovače (3), poté je ve směšovači (4) převeden na mezifrekvenční signál, vyfiltrován v pásmové propusti (5), zesílen v zesilovači (6) a převeden v převodníku (7) na digitální signál. Další zpracování je čistě v digitální podobě: digitální integrátor (8), digitální úroňový analyzátor (9) a digitální regulátor (10). Všechny tyto operace jsou řízeny mikroprocesorovou jednotkou (12). Digitální výstup je převeden v převodníku (11) do analogové podoby a je využit k řízení standardních výstupů (poplachové relé, výstup otevřeného kolektoru, analogový výstup pro kontrolu snímání apod.). Pro podněty velké amplitudy slouží samostatný kanál (13), jehož výstup je přímo analyzován digitální řídicí jednotkou. Pro testování funkce čidla slouží zabudovaný testovací generátor (14) a testovací elektroakustický měnič (15). Podstatnou výhodou použití otřesových čidel je skutečnost, že dojde k vyhlášení poplachu dříve, než se pachatel zmocní cenných předmětů umístěných v chráněném prostoru.

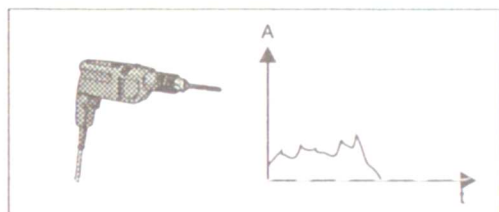
Otřesová čidla jsou schopna reagovat na všechny dnes známé druhy napadení skříňových trezorů, nočních trezorů, peněžních automatů a těžkých trezorových místností. Jsou schopna zareagovat na mechanické i termické napadení, jako je:

- užití hrubého mechanického nářadí,
- vrtání včetně užití vrtáku s diamantovou korunkou,

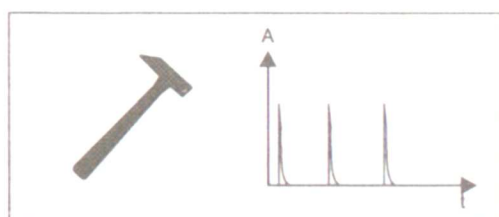
- užití hydraulického tlakového nářadí,
- řezání kyslíko-vodíkovým plamenem,
- užití plastických a jiných trhavin.



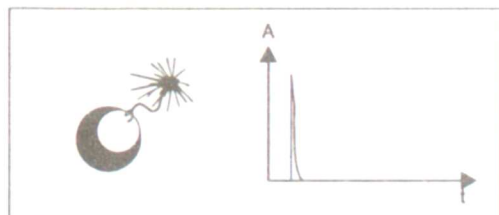
nízká amplituda signálu  
vysoká frekvence  
dlouhá doba trvání



střední amplituda signálu  
široké spektrum frekvencí  
dlouhá doba trvání



vysoká amplituda signálu  
nízká frekvence  
krátká doba trvání

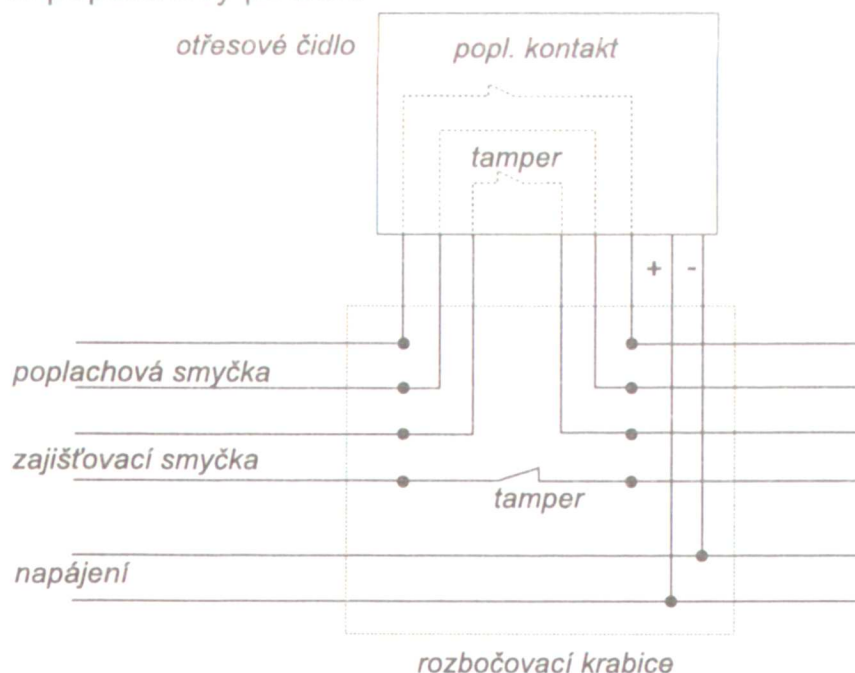


extrémně vysoká amplituda signálu  
široké spektrum frekvencí  
krátká doba trvání (jednorázový děj)

Obr. 3-19: Odezva na různé způsoby napadení.

### 5.1.2 Elektrické připojení

Elektrické připojení je shodné s ostatními čidly používanými v EZS. Typický je navíc paralelní poplachový výstup pro řízení indikačního a testovacího tabla v případě aplikace více otřesových čidel na jedné smyčce a testovací výstup pro měření napěťové odezvy na poplachový podnět.



Obr. 3-20: Elektrické připojení otřesových čidel.

### 5.1.3 Použití a montáž

Mohou být nasazena ke střežení výdejních automatů na lístky, parkovacích automatů, peněžních automatů, pancéřových skříní na peníze, těžkých trezorových místností – trezorových dveří, zdí, stropů a podlahových ploch. S otřesovými čidly můžeme střežit následující materiály:

- kov,
- beton,
- kámen (omezeně).

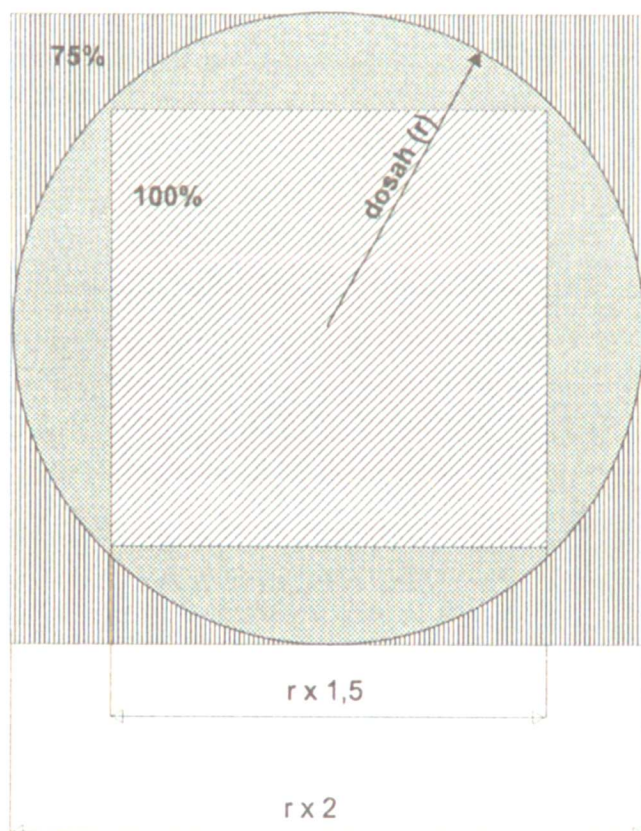
Střežit nelze:

- sklo,
- dřevo,
- gumu,
- vláknité desky,
- pěnové materiály.

Předpokladem spolehlivé funkce je montáž na rovnou plochu střeženého předmětu očištěnou od všech zvuk tlumících materiálů (oškrábání laku v místě montáže apod.).

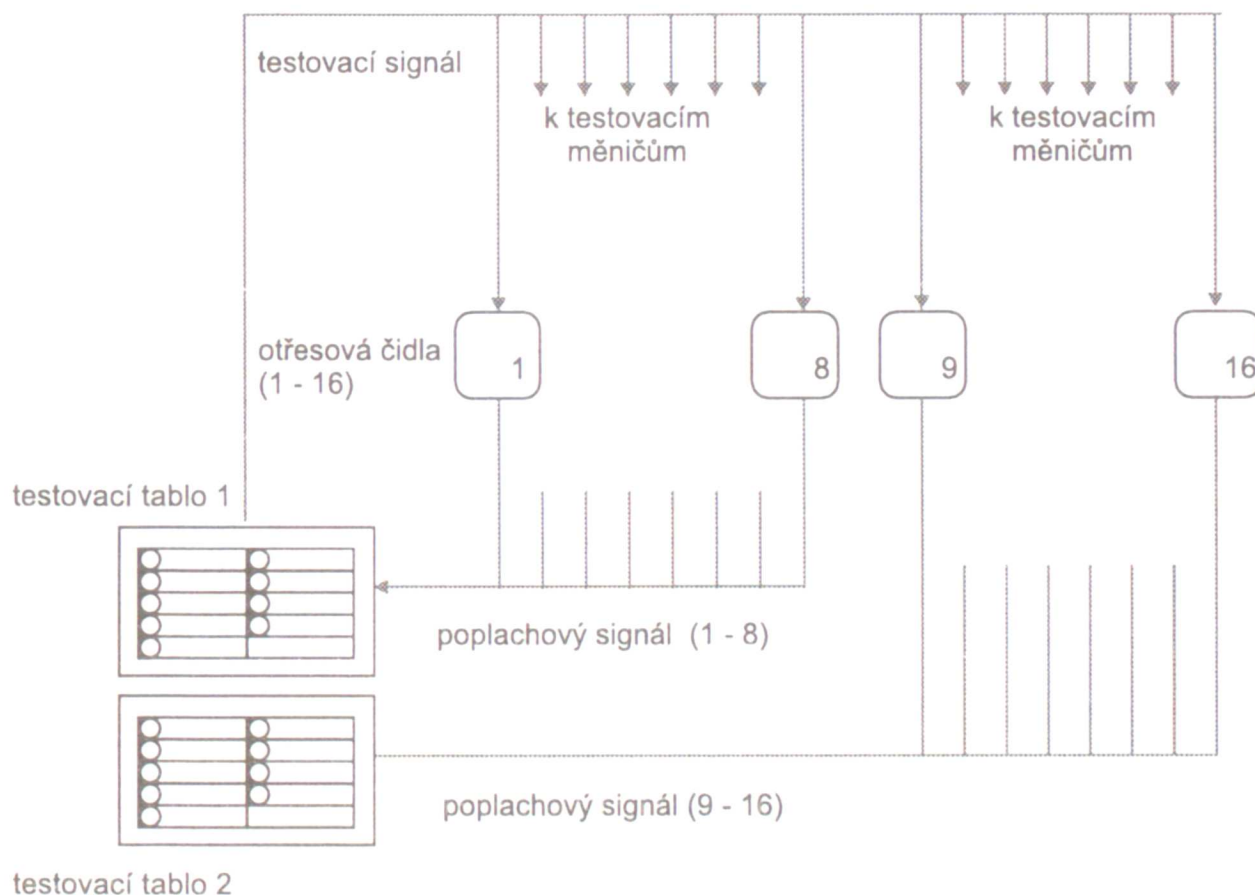
Při střežení zdí, stropů a podlah se musí před montáží pevně stanovit, o jakou stavbu se jedná (beton, kámen). Poté se přezkoušejí všechny plochy z hlediska trhlin a dilatačních mezer. Doporučuje se vyšetřit před montáží čidel přenos zvuku ploch pomocí vhodného měřicího přístroje.

Při nové výstavbě prostor, které mají být otřesovými čidly střeženy, je nutné připravit montážní místa, prostupy a trasy pro kabely během projekce stavební části a výstavby. Pozdější montáž je pak možná bez rizika narušení mechanické celistvosti úschovného místa pouze jako povrchová.



Obr. 3-21: Dvě varianty pokrytí střežených ploch.

Jsou-li prostory nebo části prostorů střeženy otřesovými čidly, musejí se čidla instalovat uvnitř těchto prostor. Otřesová čidla musejí být připojena k bezpečnostnímu zařízení tak, že je možná jejich jednotlivá identifikace. To znamená buď každé čidlo na samostatnou smyčku (či adresu u adresovatelných systémů), nebo použití přídavného indikačního a testovacího tabla. Tablo nám kromě identifikace poplachu umožní autonomní testování funkce všech čidel k němu připojených.



Obr. 3-22: Testovací tablo pro připojení otřesových čidel.

#### 5.1.4 Kritéria falešných poplachů

Při volbě otřesových čidel musí být brán ohled na eventuální okolní vlivy, s nimiž je třeba počítat (např. vozidla, ventilace, provoz metra v blízkosti apod.). Plochy, jež jsou přístupné z nestřeženého prostoru (např. vnější dveře) včetně trezorových prostor a peněžních automatů, nesmějí být střeženy otřesovými čidly. U otřesových čidel instalovaných ve zdech a podlahách může funkci ovlivnit vlhkost (např. zkondenzovaná voda). Čidla se potom musí chránit před vlhkostí pomocí vhodných opatření.

#### 5.1.5 Nastavení, údržba, servis

Má-li otřesové čidlo nastavovací prvky, nastavujeme citlivost na minimální hodnotu nutnou pro spolehlivé pokrytí střeženého předmětu či střežené plochy. Při instalaci otřesových čidel musíme dále mít na zřeteli, aby po zabudování, popř. změně vnitřního zařízení (např. zákaznické schránky), zůstala přístupná pro potřeby servisu. Nezbytnou činností je pravidelné testování jejich funkce.

## 5.2 Čidla na ochranu uměleckých předmětů

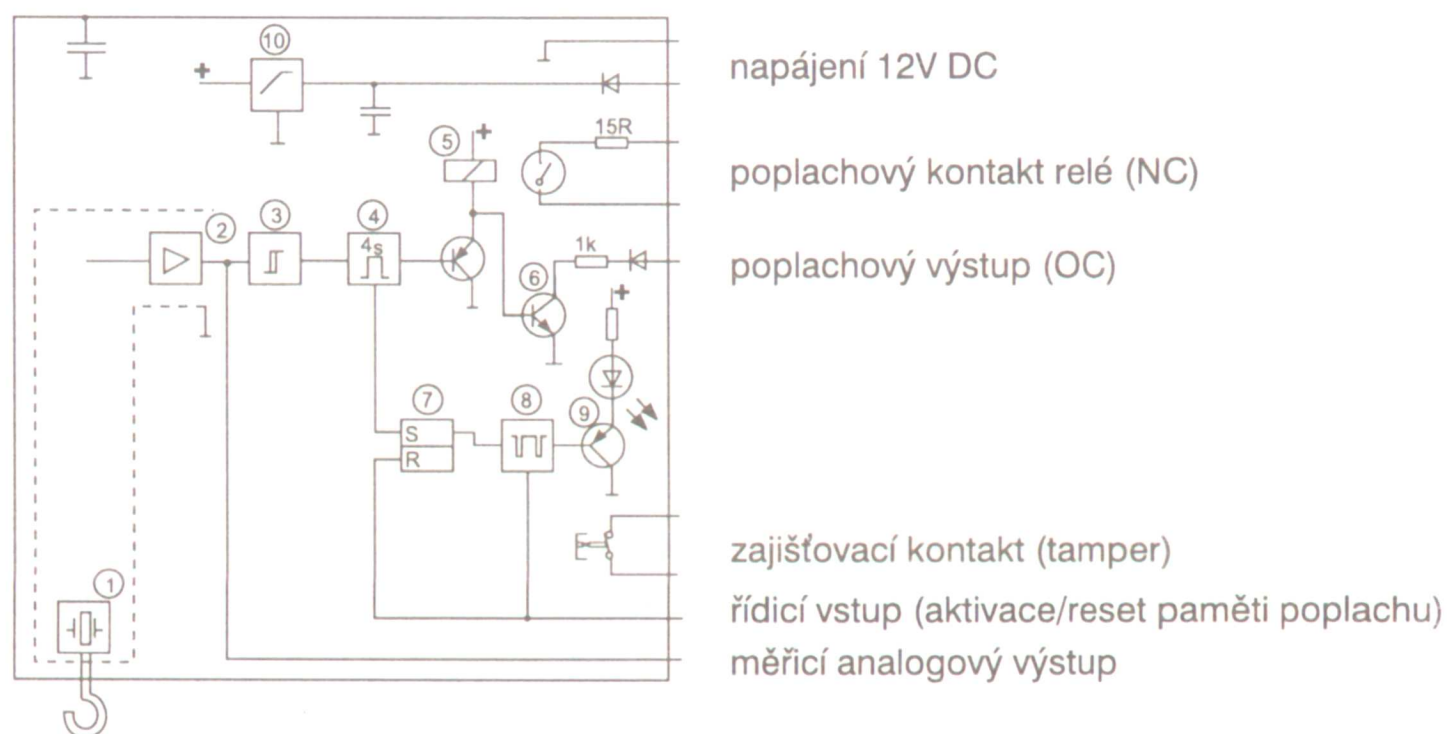
### 5.2.1 Principy funkce a praktické provedení

Jsou určena pro střežení uměleckých předmětů (obrazy, masky, koberce...) zavěšených ve výstavních síních, galeriích, muzeích apod. Princip činnosti umožňuje trvalý provoz střežení, tedy i v době provozu pro veřejnost. V zásadě můžeme tato čidla rozdělit do dvou skupin:

- závěsová čidla,
- polohová čidla.

#### Závěsová čidla:

Střežený předmět je zavěšen pomocí závěsného lanka na hák čidla. Čidlo vyhodnocuje síly působící na hák a podle nastavení citlivosti vyhodnotí elektronika i velmi malé pohyby střeženého předmětu, pokus o jeho sejmutí či pouhý dotek. Principiálně se jedná opět o elektromechanický měnič doplněný vyhodnocovací elektronikou s nastavitelnou citlivostí. Háček je propojen s piezokeramickým měničem (1), signál narušení je zesílen v zesilovači (2), tvarován a filtrován (3), dále ovládá monostabilní klopný obvod (4) a výkonovou elektroniku relé (8). Další podpůrné obvody slouží k filtraci napájení (10), řízení indikace a paměti poplachu (6, 7, 8, 9).



Obr. 3-23: Blokové schéma elektronického čidla na obrazy.

#### Polohová čidla:

Jedná se o elektromagnetická či kontaktní čidla, která velmi citlivě reagují na změnu polohy střeženého předmětu. Vychýlením „praporku“ čidla, jež se přímo dotýká části střeženého předmětu (plátna, obrazu či gobelínu), mimo stanovený rozsah se aktivuje magnetický kontakt a elektronikou čidla je vyhlášen poplach. Tento typ čidla je zvláště vhodný v případech, kdy nelze použít pro střežený předmět čidla závěsová.

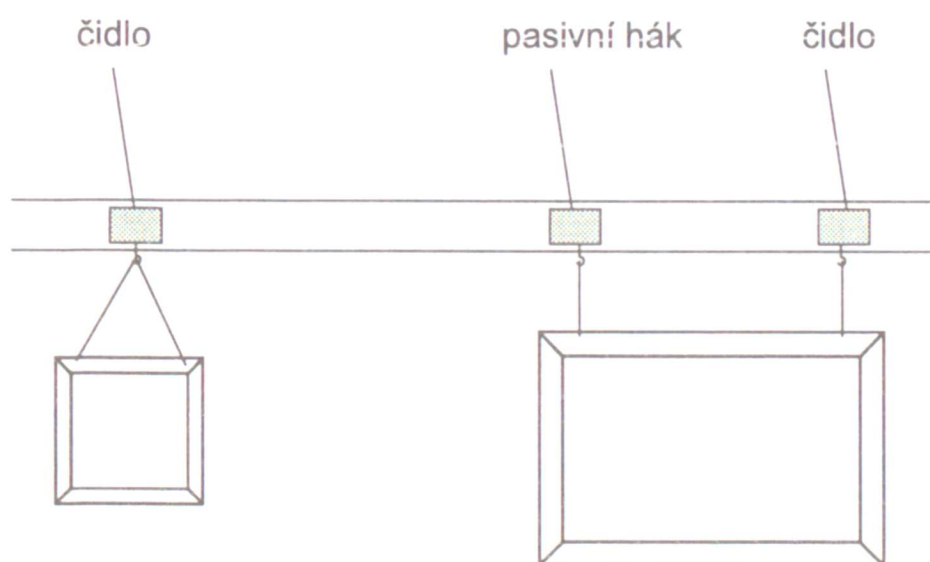


### 5.2.2 Elektrické připojení

Elektrické připojení je shodné s ostatními čidly používanými v EZS. Typický je navíc paralelní poplachový výstup pro řízení indikačního tabla pro případ aplikace více čidel na jedné smyčce, vstup pro řízení indikační LED paměti poplachu a testovací výstup pro měření napěťové odezvy na poplachový podnět.

### 5.2.3 Použití a montáž

Rozsah použitelnosti u závěsových čidel je podle zvoleného typu a způsobu montáže pro předměty od 1kg do cca 100 kg. Montují se na kolmé stěny s dostatečnou mechanickou odolností, tj. min. 30 cm silné, 50 až 200 cm nad zavěšený předmět.



Obr. 3-24: Příklad aplikace závěsových čidel.

### 5.2.4 Kritéria falešných poplachů

Teoreticky mohou k falešným poplachům vést následující faktory:

- nedodržení doporučení výrobce pro montáž (kolmost závěsů, izolace proti vibracím stěny),
- nastavení příliš vysoké citlivosti neodpovídající hmotnosti střeženého předmětu,
- obecně mohou být důvodem falešných poplachů vnější vlivy jako vibrace a otřesy vlivem okolního provozu či přírodních sil, silný průvan.

### 5.2.5 Nastavení, údržba a servis

Nastavení musí odpovídat hmotnosti střeženého předmětu. I zde se doporučuje využívat minimální hodnoty, jež vede ke spolehlivé detekci pokusu o krádež. V provozu je rovněž nutné pravidelně ověřovat funkci obrazových čidel, neporušenost závěsných lan a umístění tlumicích izolačních podložky pod rohy obrazů.

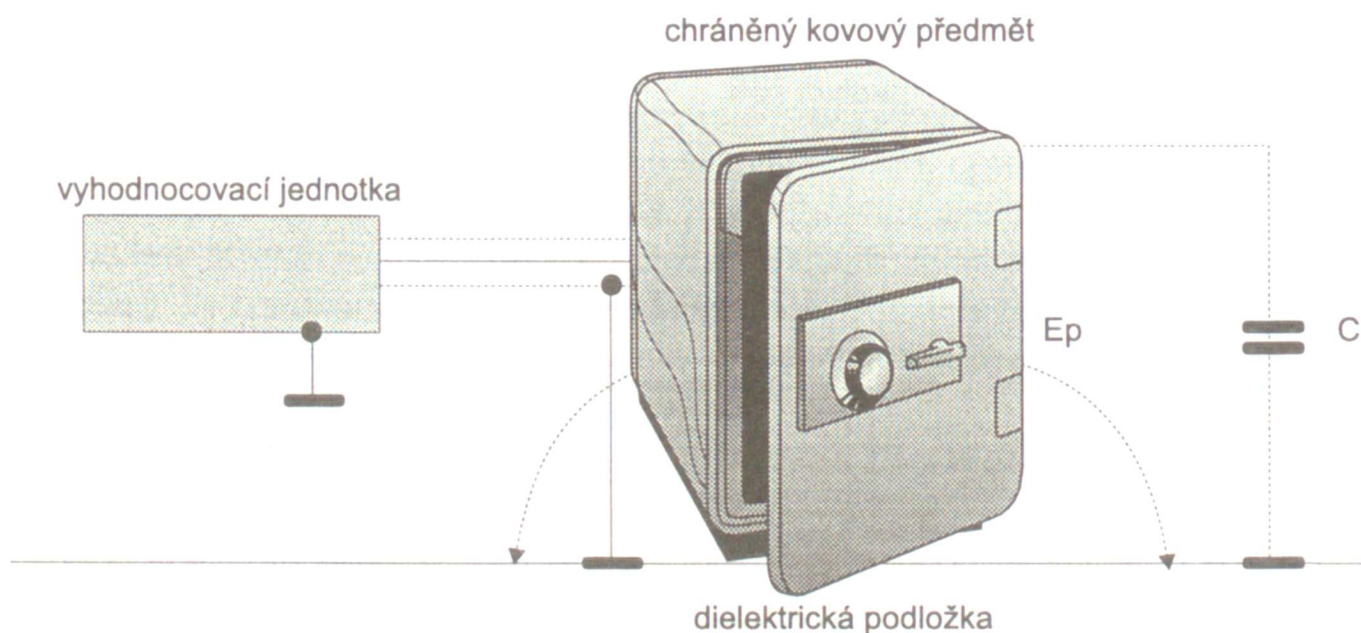
*Poznámka – Pro ochranu zavěšených obrazů se nabízejí další varianty mechanických kontaktů, popř. magnetických kontaktů. Řady zavěšených předmětů je možné dále střežit podle interiérového řešení objektu také infrazávorami či PIR čidly s charakteristikou typu závěs.*

### 5.3 Kapacitní čidla

Jsou určena k indikaci přiblížení či doteku chráněného předmětu. Mohou být užita k ochraně obrazů, volně stojících předmětů a skříní kovových i nekovových.

#### 5.3.1 Princip funkce a praktické provedení

Střežený předmět je umístěn v elektrickém poli čidla ( $E_p$ ) nebo je přímou součástí elektrod. Osoba v elektrickém poli kondenzátoru tvořeného střeženým předmětem a polepy mění parametry dielektrika (jímž je v tomto případě okolní vzduch), a tím i kmitočet oscilátoru, jehož je kondenzátor součástí. Fázový detektor tyto změny vyhodnocuje a dává povel k vyhlášení poplachu.



Obr. 3-25: Princip funkce kapacitního čidla.

#### 5.3.2 Použití a montáž

Vlastní montáž a nastavení kapacitního čidla jsou velice náročné, a proto nepatří v současné době mezi příliš užívané prvky a jen málo světových výrobců ho má dodnes ve svém sortimentu. Jeho podstatnou výhodou však je, že může být nastaveno tak, že dojde k vyhlášení poplachu ještě před započítím jakékoliv činnosti střeženého předmětu, tedy před jeho fyzickým poškozením.

#### 5.3.3 Kritéria falešných poplachů

Nastavování příliš vysoké citlivosti však může vést k výskytu falešných poplachů. Limitujícím faktorem může být celková velikost kapacity chráněného předmětu vůči uzemnění. Nelze tedy jedním kapacitním čidlem chránit celou řadu trezorových skříní, ale jako vhodná aplikace se jeví použití pro samostatné trezorové skříně, popř. pro střežení kovových exponátů v muzeích apod.

#### 5.3.4 Nastavení, údržba, servis

Vlastní nastavování je specifická činnost popsaná detailně v instalačním manuálu výrobce. V podstatě se jedná o nastavení pracovního kmitočtu, na nějž jsou pak naladěny vstupní filtry vyhodnocovací jednotky. Důležité je odizolování střeženého předmětu od parazitních zemních svodů pomocí dielektrických podložek.

## 6 Prvky venkovní obvodové (perimetrické) ochrany

Jsou to čidla, která chrání, resp. signalizují narušení vnějších částí u rozlehlých objektů, komplexů budov nebo továren na samostatném pozemku.

Existuje řada druhů čidel na různých fyzikálních principech, z nichž každé je určeno pro odlišnou povahu chráněného pozemku. Zařízení se liší podle účelu nasazení a podle stupně důležitosti zabezpečení.

Konstrukce vnějších čidel, zejména mechanické a klimatické krytí, odpovídá vnějšímu prostředí, a tak se samozřejmě odlišuje od částí zabezpečovacího systému, které jsou umístěny uvnitř budov. Vnější prostředí má však vliv i na projekci a způsob montáže prvků venkovní obvodové ochrany.

Vzhledem k dimenzím venkovních prostor se liší od čidel pro vnitřní použití především v dosahu. Jsou-li funkční dosahy vnitřních čidel řádově 10 metrů, u venkovních se jedná řádově o 100 metrů. Dalším rozdílem je tvar zabezpečovaného prostoru. Je-li možno přiblížit se k objektu z více stran, bylo by nejvhodnější chránit celý plošný rozměr parcely, a zároveň mít možnost přímé adresace pro každý bod chráněné plochy. Z technických i ekonomických důvodů však nelze tento požadavek důsledně splnit. Proto se vytvářejí nejčastěji přímkové koridory u hranice pozemku popř. křivky kopírující terén a hranici pozemku.

Naprostou podmínkou při užívání venkovní obvodové ochrany, aby bylo vůbec možno definovat narušení, je existence oplocení. Bez mechanické zábrany na hranici pozemku by mohlo docházet k nechtěnému vstupu nepovolaných osob na zabezpečený pozemek a po signalizaci poplachu by byl zákrok a postih z právního hlediska velmi problematický.

Dalším problémem venkovního zabezpečení je velké množství podnětů, na které by neměla čidla reagovat. Jsou to následující vlivy:

- vlnění travního porostu,
- pohyb listí a větví stromů a keřů,
- vibrace oplocení ve větru,
- proudění vzduchu,
- vítr,
- sníh a déšť,
- pohyby různých druhů zvířete,
- dopravní ruch v blízkosti hranice pozemku.

To vše jsou vlivy, které mohou způsobovat falešné poplachu. Výběr vhodné varianty střežení venkovního perimetru tedy musí vycházet z důkladné znalosti zabezpečovaného objektu. Podněty, které se svým charakterem přibližují situaci narušení, nelze nikdy zcela eliminovat. Nejen z tohoto důvodu se často kombinuje systém venkovní perimetrické ochrany se systémem průmyslové televize (CCTV).

Základním požadavkem na prvky venkovní perimetrické ochrany je nezávislost funkce na klimatických podmínkách. Proto bývají venkovní čidla, je-li to z hlediska funkce nutné, obvykle vybavena vnitřním vyhříváním. Krytí čidel či vyhodnocovací elektroniky musejí být dokonale utěsněny a opatřeny kontakty zapojenými do zajišťovací smyčky. Rovněž přívodní kabely musí být kvalitně utěsněny v průchodkách do krytů čidel či vyhodnocovací elektronické jednotky.

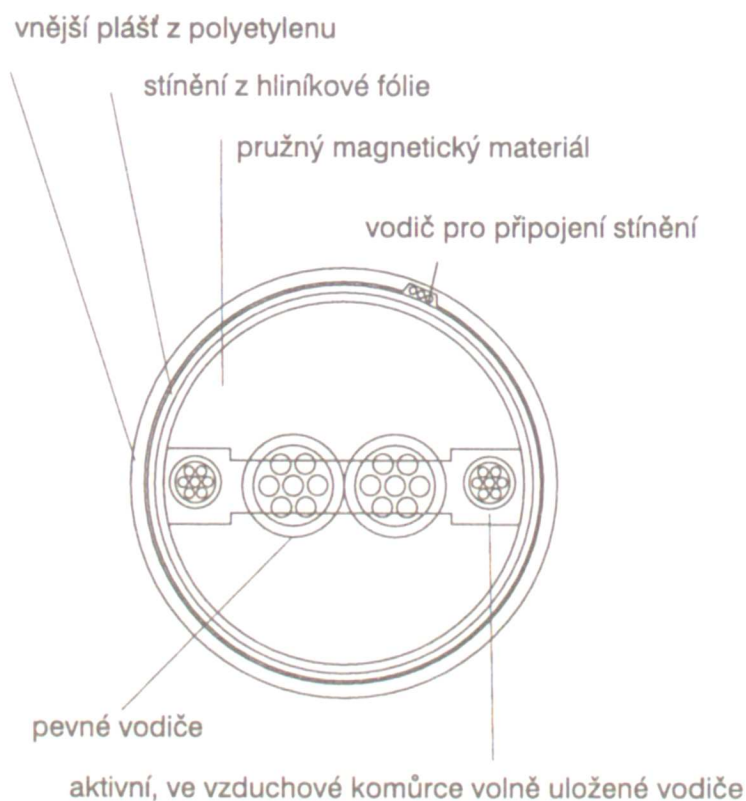
Pro aplikace v praxi zabezpečovací techniky se v současné době nabízí rozsáhlý sortiment prvků venkovní perimetrické ochrany. Každý z nich má podle použitého fyzikálního principu své výhody a nevýhody. Volba vhodného typu pro konkrétní úlohu zabezpečení závisí proto na zkušenostech a odborných znalostech projektanta.

V dalším textu jsou popsány příklady užívaných prvků venkovní perimetrické ochrany.

### 6.1 Mikrofonické kabely

#### 6.1.1 Princip funkce a praktické provedení

Mechanické namáhání nebo záchvěvy citlivého mikrofonického kabelu se převádějí na elektrický signál, který je dále zpracováván ve vyhodnocovací jednotce. Akustický odposlech slouží k rozpoznání charakteru narušení, úroveň odezvy odpovídající vyhlášení poplachu je nastavitelná.



Obr. 3-26: Příklad provedení mikrofonického kabelu.

#### 6.1.2 Elektrické připojení

Elektrické připojení je specifické a vychází z instalačních manuálů konkrétního výrobku. Zásady ochrany proti sabotáži i velikost napájecího napětí bývají standardní.

#### 6.1.3 Použití a montáž

Slouží k ochraně drátěných plotů. Některé typy lze aplikovat i pod omítku či pro zardění a zabetonování. Nejčastěji se aplikuje vpletením do osnovy drátěného plotu. Montáž předpokládá dostatečnou mechanickou tuhost oplocení. Nejlepší je budovat tento typ ochrany spolu s novým plotem. Délka jednoho úseku může být až 300 m. Výhodou jsou nízké náklady na montáž s minimem zemních prací.

#### 6.1.4 Kritéria falešných poplachů

Rizikové faktory falešných poplachů jsou silný déšť, krupobití, silný vítr, přítomnost zvířete. Rovněž indukce silného elektrického či elektromagnetického pole může kompli-

kovat funkci zařízení. Po zaškolení obsluhy lze díky akustickému odposlechu rozpoznat charakter narušení, což napomáhá správnému rozhodnutí o případném protiopatření.

### 6.1.5 Nastavení, údržba a servis

Jedná se o specifické činnosti vyplývající z konkrétních doporučení výrobce. Zásada periodického ověřování správné funkce zůstává zachována. Je nutné uvažovat také o životnosti kabelů vystavených klimatickým vlivům.

## 6.2 Infračervené závory a bariéry

### 6.2.1 Princip funkce a praktické provedení

Nejrozšířenějším druhem venkovních obvodových čidel jsou infračervené závory (infrazávory). Mezi přijímací a vysílací stranou probíhá jeden či více infračervených paprsků. Při přerušení některého z nich (nebo více s koincidenční logikou) dochází na přijímací straně k vyhodnocení a vyhlášení poplachového stavu. Pro zvýšení odolnosti proti cizím zdrojům světla pracují infrazávory v pulsním režimu. Infrazávory bývají vybaveny vyhříváním, aby nedošlo k orosení optiky nebo nánosů vlhkosti z vnější strany. Prakticky použitelný dosah je 50 až 150 metrů, i když někteří výrobci inzerují dosah až do 250 m.

*Poznámka – Zvyšování dosahu venkovních čidel nad tuto mez, i když by bylo technicky možné, není opodstatněné z důvodu požadavku zachování informace o přibližném místě překonání hranice pozemku.*

### 6.2.2 Elektrické připojení

Elektrické připojení je specifické a vychází z instalačních manuálů konkrétního výrobku. Zásady ochrany proti sabotáži i velikost napájecího napětí bývají standardní. Výstup bývá řešen jako bezpotenciálový kontakt relé pro připojení do poplachové smyčky ústředny elektrické zabezpečovací signalizace.

### 6.2.3 Použití a montáž

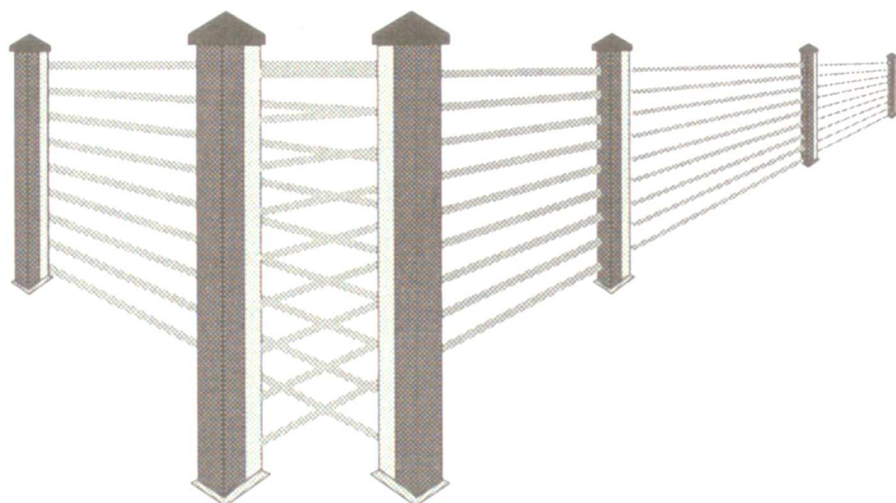
Nevýhodou tohoto typu je pracná montáž. Výhodou bývá relativně nižší cena oproti jiným druhům venkovních obvodových čidel. nutnost vybudování stabilních montážních míst a zemní výkopové práce pro kabely cenu vyrovnají. Při návrhu kabeláže je nutné počítat s nezanedbatelným příkonem vytápění pouzder či montážních sloupů infrazávor. Při použití více souprav na obvodu pozemku, kdy na sebe úseky navazují, se musí částečně překrývat, aby nedocházelo k vytváření mrtvých koridorů, tj. míst, kde by narušení nebylo detekováno. Další nutnou podmínkou aplikace je naprosto rovný terén mezi vysílačem a přijímačem.

### 6.2.4 Kritéria falešných poplachů

Rizikové faktory falešných poplachů jsou mlha, padající sníh, popř. přímý sluneční svit. Někteří výrobci doplňují infrazávory automatikou snímající optickou propustnost prostoru mezi přijímačem a vysílačem. Při poklesu viditelnosti (např. za silné mlhy) automatika vyřadí čidla z provozu a poplach není vyhlášován.

### 6.2.5 Nastavení, údržba a servis

Vlastní nastavení infrazávor vyžaduje poměrně velkou trpělivost a praxi. Výrobci dnes usnadňují montážním pracovníkům nastavování optické osy infračerveného paprsku dodávkou speciálního zaměřovacího přípravku jako příslušenství. V každém případě je nastavování zvláště u systémů vícepaprskových záležitost časově velice náročná. Zásada periodického ověřování správné funkce zůstává zachována.



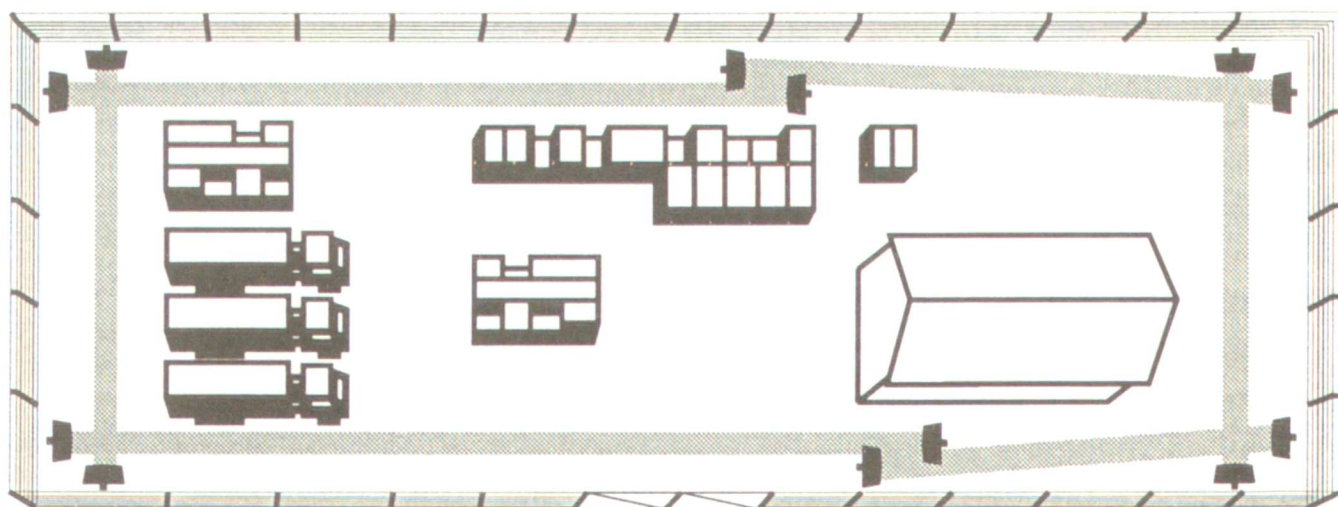
Obr. 3-27: Uspořádání IR bariér s překrytím paprsků.

## 6.3 Mikrovlnné bariéry

### 6.3.1 Princip funkce a praktické provedení

Dalším prvkem venkovní perimetrické ochrany je mikrovlnná bariéra. Jedná se o vytvoření elektromagnetického pole mezi vysílačem a přijímačem. Vnik osoby do detekční zóny způsobí porušení elektromagnetického pole. Tato změna je detekována a vyhodnocována přijímačem. Mikrovlnný svazek je zde rovněž modulován pro zvýšení odolnosti proti rušení cizími zdroji elektromagnetického vlnění.

Typický tvar mikrovlnného svazku je elipsoid s výrazným poměrem velké a malé osy, kdy tento poměr vzrůstá se zvětšením vzdálenosti mezi vysílačem a přijímačem. Vyzařovací diagram čidla má tedy typický doutníkový tvar. Výhodou mikrovlnných bariér je značný dosah, cca 200 až 300 metrů, při relativně vysoké odolnosti vůči povětrnostním vlivům. Kromě provedení pro stabilní montáž jsou vyráběna čidla i pro mobilní použití (na stativu).



Obr. 3-28: Příklad aplikace MW bariér.

### 6.3.2 Elektrické připojení

Elektrické připojení je specifické a vychází z instalačních manuálů konkrétního výrobku. Zásady ochrany proti sabotáži i velikost napájecího napětí bývají standardní. Výstup bývá řešen jako bezpotenciálový kontakt relé pro připojení do poplachové smyčky ústředny elektrické zabezpečovací signalizace.

### 6.3.3 Použití a montáž

Pro nasazování tohoto čidla je nutné dodržet několik zásad, které respektují vyzařovací diagram čidla. Důležité je dodržení správné výšky instalace čidla nad zemí, aby nebylo možné úsek podplazit, rovněž je důležité, aby nebyly v zabezpečovaném prostoru příčné terénní vlny, jimiž by byl možný nekontrolovatelný průchod. Při montáži podél oplocení musí být dodržena zásada minimálního poměru vzdálenosti od plotu vůči výšce plotu minimálně 1:1.

### 6.3.4 Kritéria falešných poplachů

Vyzařovací diagram čidla by se neměl dotýkat oplocení (drátěného), neboť i pohyby tohoto oplocení vyvolávají falešné poplachy nebo může čidlo reagovat na pohyb i za plotem. V zabezpečovaném prostoru se nesmějí vyskytovat pohybující se předměty, traviny a keře, větve stromů apod.

### 6.3.5 Nastavení, údržba a servis

Jedná se o specifické činnosti vyplývající z konkrétních doporučení výrobce. Zásada periodického ověřování správné funkce zůstává zachována.

## 6.4 Štěrbinové kabely

### 6.4.1 Princip funkce a praktické provedení

Jiným druhem venkovní perimetrické ochrany je položený koaxiální kabel (většinou v páru v definovaném odstupu). Stínění má snížené krytím (stínění má definované štěrbinu). Jeden kabel tedy vyzařuje a vytváří elektromagnetické pole, jehož změny jsou druhým kabelem vyhodnocovány. Při narušení tohoto pole osobou dochází k vyhlášení poplachu.

### 6.4.2 Elektrické připojení

Elektrické připojení je specifické a vychází z instalačních manuálů konkrétního výrobku. Zásady ochrany proti sabotáži i velikost napájecího napětí bývají standardní.

### 6.4.3 Použití a montáž

Výhodou je možnost kopírování terénu výškově i půdorysně, štěrbinové kabely se položí podél obvodu pozemku bez nutnosti vytvářet přímé úseky s rovným povrchem. Délka jednoho úseku může být podle typu 100 – 200 m. Určitou nevýhodou je nutnost zemních prací po celé délce zabezpečovaného perimetru, což poněkud zvyšuje náklady na instalaci. Existuje i mobilní verze štěrbinových kabelů, kdy jsou kabely zavěšeny na nosnících v určitém odstupu nad povrchem země.

### 6.4.4 Kritéria falešných poplachů

Indukce silného elektrického či elektromagnetického pole může komplikovat funkci zařízení. Rovněž pohyb zvěře v zabezpečeném prostoru může vyvolávat falešné poplachy. Odolnost proti falešným poplachům je otázkou správné montáže a správného nastavení systému.

### 6.4.5 Nastavení, údržba a servis

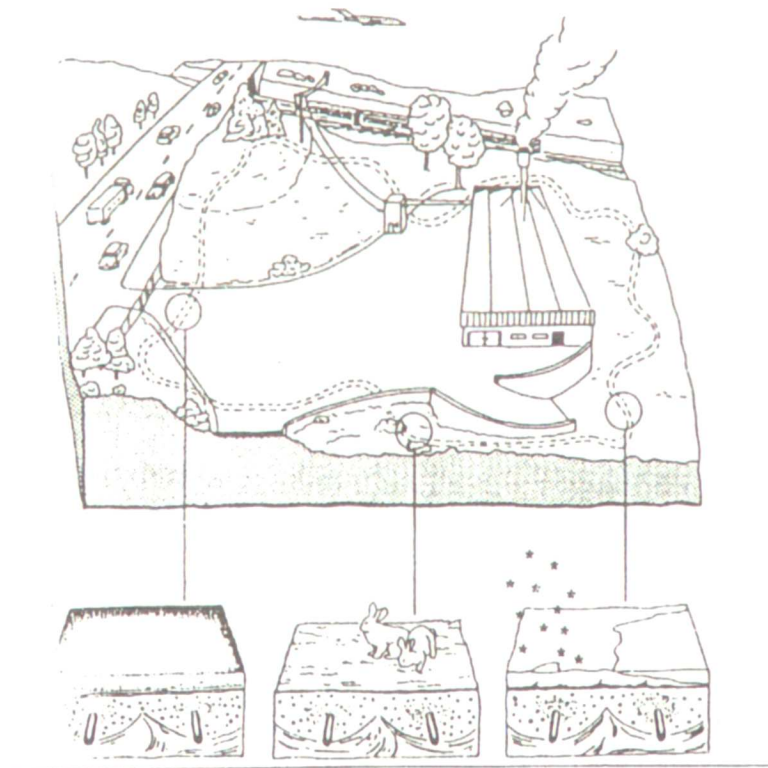
Jedná se o specifické činnosti vyplývající z konkrétních doporučení výrobce. Zásada periodického ověřování správné funkce zůstává zachována. Je nutné rovněž uvažovat o životnosti kabelů uložených v zemi.

## 6.5 Zemní tlakové hadice

### 6.5.1 Princip funkce a praktické provedení

Dalším druhem venkovních čidel je hydraulické podzemní čidlo známé pod názvem GPS (Ground Perimeter System). Jedná se o diferenciální tlakové čidlo, jehož základem jsou paralelně položené dvě pružné hadice v rozteči cca 1 metr po celém obvodu pozemku. Tyto hadice napuštěné nemrznoucí kapalinou působí jako prostředí pro přenos změn tlaku, vyvolaného vnějším podnětem z okolí, až do místa vyhodnocení. Změny tlaku jsou vyhodnocovány v diferenciálním tlakovém čidle a převáděny na elektrický signál. Další elektronické vyhodnocování signálů účinně omezuje falešné poplachy způsobované hluky z okolí mimo koridor, např. silniční dopravou, vlaky, letadly, drobnou zvěří. Délka jednoho úseku může být až 200 m.

Obr. 3-29: Příklad aplikace zemních tlakových hadic.





### 6.5.2 Elektrické připojení

Elektrické připojení je specifické a vychází z instalačních manuálů konkrétního výrobku. Zásady ochrany proti sabotáži i velikost napájecího napětí bývají standardní.

### 6.5.3 Použití a montáž

Výhodou čidla je možnost výškového i půdorysného kopírování jakkoliv členitého terénu na obvodu pozemku. Nemusejí být vytvářeny přímé úseky, po montáži je čidlo po zatrvnění neviditelné, může se pokládat i pod tvrdé povrchy vozovek. Nevýhodou jsou poněkud vyšší náklady na montáž a na pravidelnou údržbu, kde je kladen důraz na kontrolu těsnosti hydraulického systému.

### 6.5.4 Kritéria falešných poplachů

Systém vyhodnocování eliminuje falešné poplachy na minimum a je schopen rozoznat i charakter průniku chráněným územím. Díky hydraulickému médiu není systém citlivý na elektrické a elektromagnetické pole.

### 6.5.5 Nastavení, údržba a servis

Jedná se o specifické činnosti vyplývající z konkrétních doporučení výrobce. Zásada periodického ověřování správné funkce zůstává zachována. V tomto případě se jedná o velice kritické činnosti, neboť díky použitému médiu by únik z netěsného nebo porušeného systému mohl způsobit ekologické škody. Z tohoto pohledu je nutné rovněž uvažovat o životnosti hadic, membrán a těles převodníků uložených v zemi.

## 6.6 Perimetrická pasivní infračervená čidla (infrateleskopy)

### 6.6.1 Princip funkce a praktické provedení

Dalším venkovním čidlem je venkovní infrapasivní čidlo. Několik málo výrobců modifikovalo známý princip infrapasivního čidla (PIR) pro venkovní prostory. Je zde použita jiná optika, vyhodnocovací obvody jsou složitější a mechanicky je použita robustní, klimaticky odolná konstrukce s vytápěným pouzdem. Typický dosah infrateleskopů je cca 150 m.

### 6.6.2 Elektrické připojení

Připojení je typické jako u vnitřních PIR čidel – poplachový výstup je tvořen bezpotenciálovým kontaktem relé, paralelně je k dispozici výstup otevřeného kolektoru tranzistoru. Kryt je proti neoprávněné manipulaci chráněn zajišťovacím kontaktem. Navíc je nutné uvažovat o potřebném příkonu pro napájení topení.

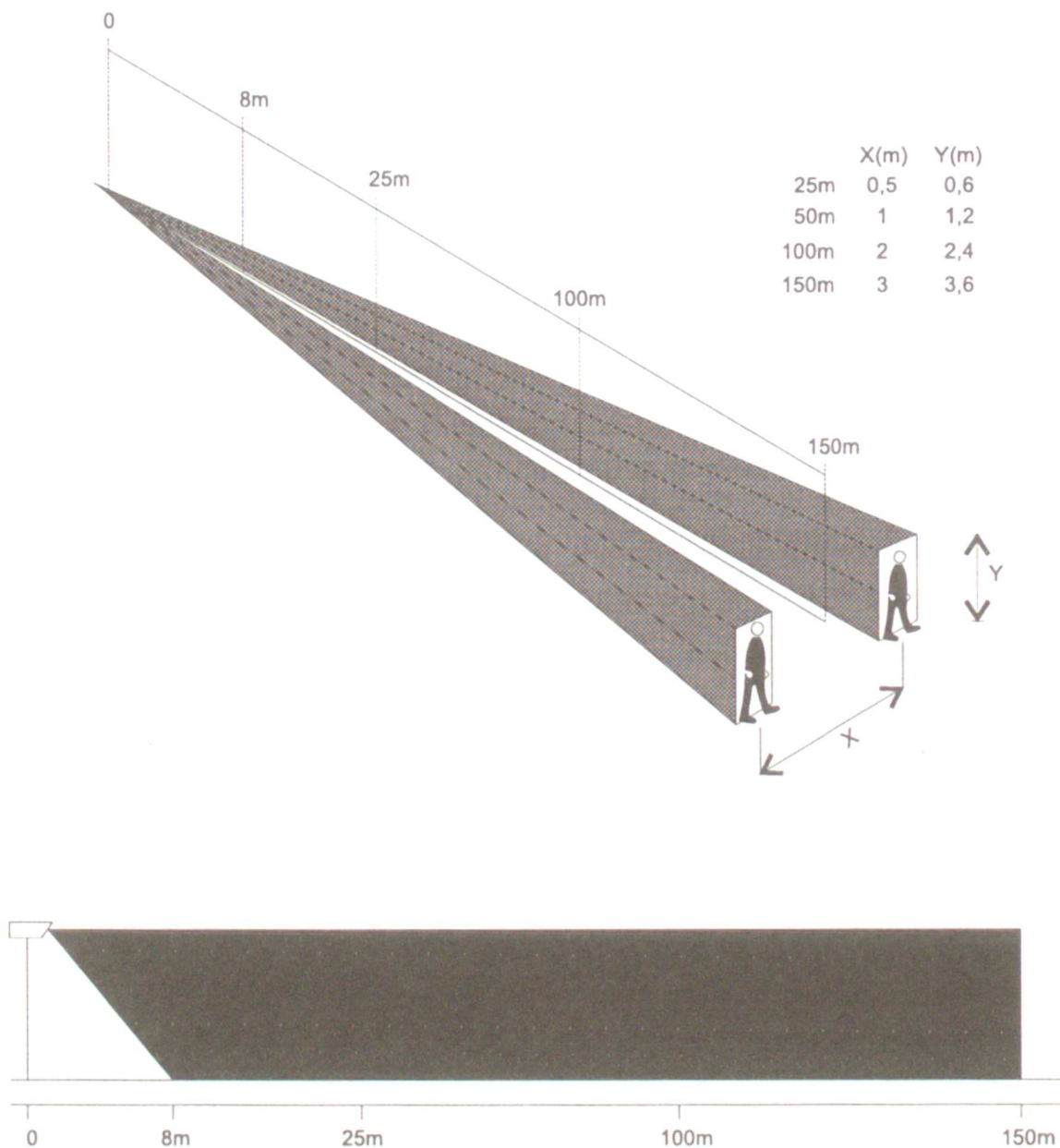
### 6.6.3 Použití a montáž

Infrateleskopy se využívají jako doplněk kamerových systémů pro spínání poplachového monitoringu či záznamu. Montážní místo musí být mechanicky stabilní. Možná je montáž na stěnu či na sloupky.

### 6.6.4 Kritéria falešných poplachů

Díky použití diferenciálních vícenásobných pyrosenzorů a speciálních vyhodnocovacích obvodů je vliv typických kritérií falešných poplachů PIR čidel (víření vzduchu,

pohyb rostlin, dopadající svit slunce či reflektorů automobilů) eliminován na minimum. Schopnost detekce se snižuje při nízkých rozdílech teploty pozadí a pachatele. Vzhledem k tomu, že není fyzikálně nijak omezen dosah, je vhodné infrateleskopy instalovat tak, aby „neviděly“ za hranice střeženého prostoru.



Obr. 3-30: Typická charakteristika infrateleskopu.

### 6.6.5 Nastavení, údržba a servis

Jedná se o specifické činnosti vyplývající z konkrétních doporučení výrobce. V tomto smyslu je nutné zvláště upozornit na čištění a kontrolu průhledu krytu čidla. Zásada periodického ověřování správné funkce zůstává zachována. Důraz musí být kladen na ověřování funkce vytápění a kontrolu těsnosti.

### 6.7 Další systémy venkovního zabezpečení

Vývoj techniky se řítí nezadržitelně vpřed a každoročně se zvláště v oblasti venkovní perimetrické ochrany objevují novinky využívající nových principů či modifikující principy stávající. Z těchto nových systémů lze zmínit plošnou ochranu použitím **rotujících laserů** či využití **optických vláken** přímo do osnovy pletiva. V dnešní době se rozšiřuje nabídka **videosenzorů s počítačovým vyhodnocením a archivací záběrů**, které v kombinaci

s kamerovými systémy částečně přebírají funkci zabezpečení venkovního perimetru. Výhodou těchto systémů je přídatná optická informace o dění v místě vyhlášení poplachu. Obsluha může okamžitě poznat, zda se jedná o falešný poplach či zda jde o skutečné napadení objektu a může rozhodnout o způsobu řešení vzniklé situace. Takové systémy však nesplňují kritéria na EZS ve smyslu zálohování a ochrany vedení proti sabotáži. Vhodným návrhem a výběrem použité techniky však lze částečně eliminovat i tyto nedostatky. Normativně však nejsou tyto případy nijak ošetřeny. Rovněž praxe ukazuje, že videosenzory, jakkoli technicky dokonalé, nemohou za daného stavu techniky zatím převzít úlohu EZS pro venkovní zabezpečení.

## 7 Ústředny EZS

### 7.1 Základní funkce a rozdělení ústředn EZS

Ústředna elektrické zabezpečovací signalizace je zařízení, které:

- přijímá a vyhodnocuje výstupní elektrické signály od čidel EZS,
- ovládá signalizační, přenosová, zapisovací a jiná zařízení, která indikují narušení,
- napájí čidla a další prvky EZS elektrickou energií,
- pomocí elektromechanických nebo kódových zámků, popřípadě vlastních ovládacích klávesnic, umožňuje uvedení celého systému EZS nebo jeho částí do stavu střežení a do stavu klidu,
- umožňuje diagnostiku systému EZS.

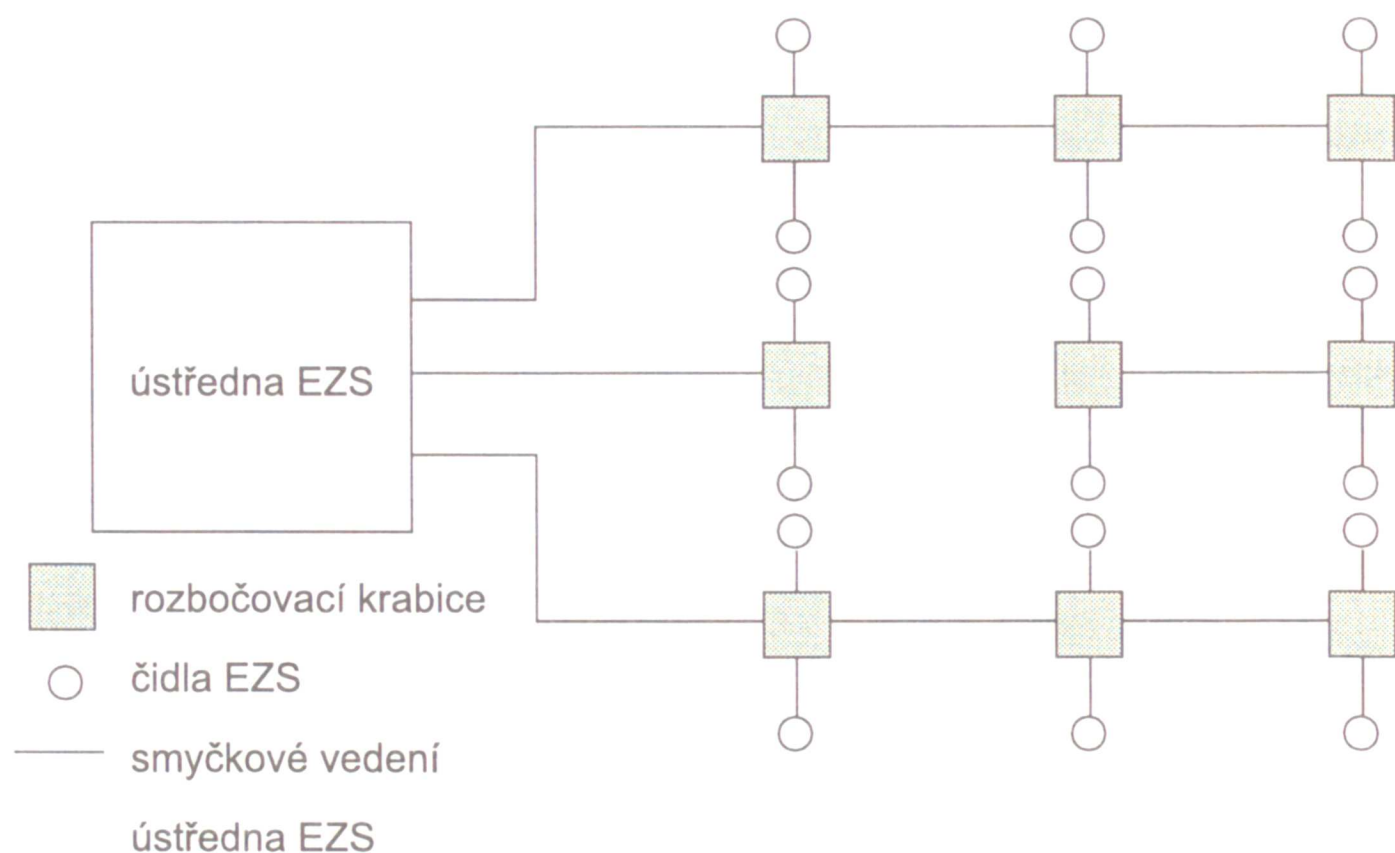
V zásadě lze ústředny EZS rozdělit do čtyř hlavních skupin, a to na:

- ústředny smyčkové,
- ústředny s přímou adresací čidel,
- ústředny smíšeného typu,
- ústředny s bezdrátovým přenosem poplachového signálu od čidel.

#### 7.1.1 Smyčková ústředna

Tato ústředna má pro každou poplachovou smyčku vstupní vyhodnocovací obvod. Obvod je řešen pro připojení proudových smyček o definované hodnotě a toleranci (viz obr. 3-34). Smyčka je zakončena zakončovacím odporem tak, aby vykazovala předepsanou hodnotu odporu pro příslušný typ ústředny. Změna odporu smyčky, způsobená aktivací některého z čidel smyčky nebo sabotáží na smyčce, vede k vyhlášení poplachového stavu systému EZS. Poplachové smyčky systému EZS jsou tvořeny nejčastěji sériovým zapojením rozpínacích kontaktů čidel.

*Poznámka – Zahraniční pravidla pro montáž EZS kladou na počet prvků ve smyčce určitá omezení. Např podle VdS (platné v SRN) je maximální počet prvků v poplachové smyčce 20 kusů.*



Obr. 3-31: Příklad zapojení systému EZS se smyčkovou ústřednou.

Systém EZS se smyčkovou ústřednou má poměrně rozsáhlou kabelovou síť, neboť ke každému čidlu musí být přiveden kabel příslušné smyčky, kabel musí obsahovat dva vodiče pro napájení čidla (u napájených čidel), dva vodiče pro poplachový kontakt čidla, dva vodiče pro sabotážní kontakt čidla a dále vodiče dodatkových funkcí typu paměť poplachu, test chůzí, odpojení vysílače ultrazvuku či mikrovlnného výkonu, indikace překrytí čidla (antimasking) apod.

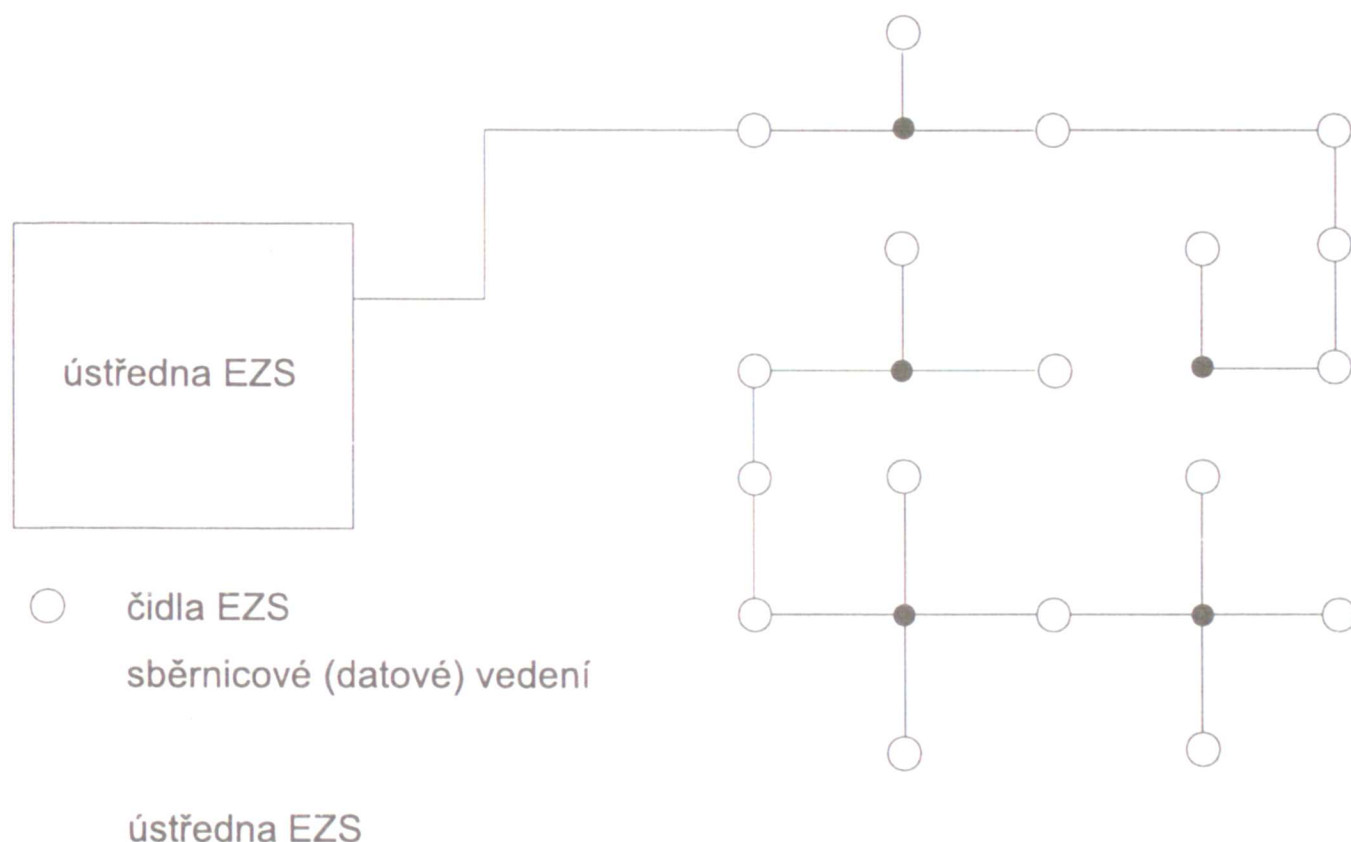
### 7.1.2 Ústředna s přímou adresací čidel

Tato ústředna pracuje na principu komunikace po datové sběrnici ústředna – čidla. Ústředna periodicky generuje adresy jednotlivých čidel a přijímá příslušné odezvy. Každé čidlo je vybaveno komunikačním modulem. Kabelová síť tohoto systému je minimální neboť je tvořena prakticky libovolnou konfigurací kabelové sítě (s max. délkou řádově stovky metrů), jednotlivá čidla jsou připojena v libovolném pořadí na zpravidla čtyřvodičové vedení, kde dva vodiče slouží pro napájení čidla a dva jako datová sběrnice. Velkou výhodou tohoto systému je, že při narušení objektu ústředna oznámí, které konkrétní čidlo bylo aktivované a jaký je druh narušení (poplachový kontakt, sabotážní kontakt dále indikují zkrat na lince, případně další stavy).

Tento systém přináší výhody uživateli v případě, že je v objektu místo trvalé obsluhy nebo je-li přenos na PCO či monitorovací pult hlídací služby realizován jako mnohokanálový. V jiném případě výhody přímé adresace ocení především instalační firma při servisu těchto systémů.

Jednoduchost kabelové sítě je však vykoupena nemožností realizovat po datové sběrnici dodatkové funkce čidel. Rovněž konfigurace kabelové sítě má svá omezení. Jedním z nich je celková délka vedení, dále je nutné vyvarovat se uzavřených okruhů přes nezanedbatelnou plochu, do nichž by se mohlo indukovat elektromagnetické rušení.

Při projekci musíme pečlivě zvažovat odběr jednotlivých částí systému a počítat úbytky na napájecích vodičích. Typický počet přímo adresovatelných čidel se u systémů tohoto typu pohybuje řádově v desítkách.

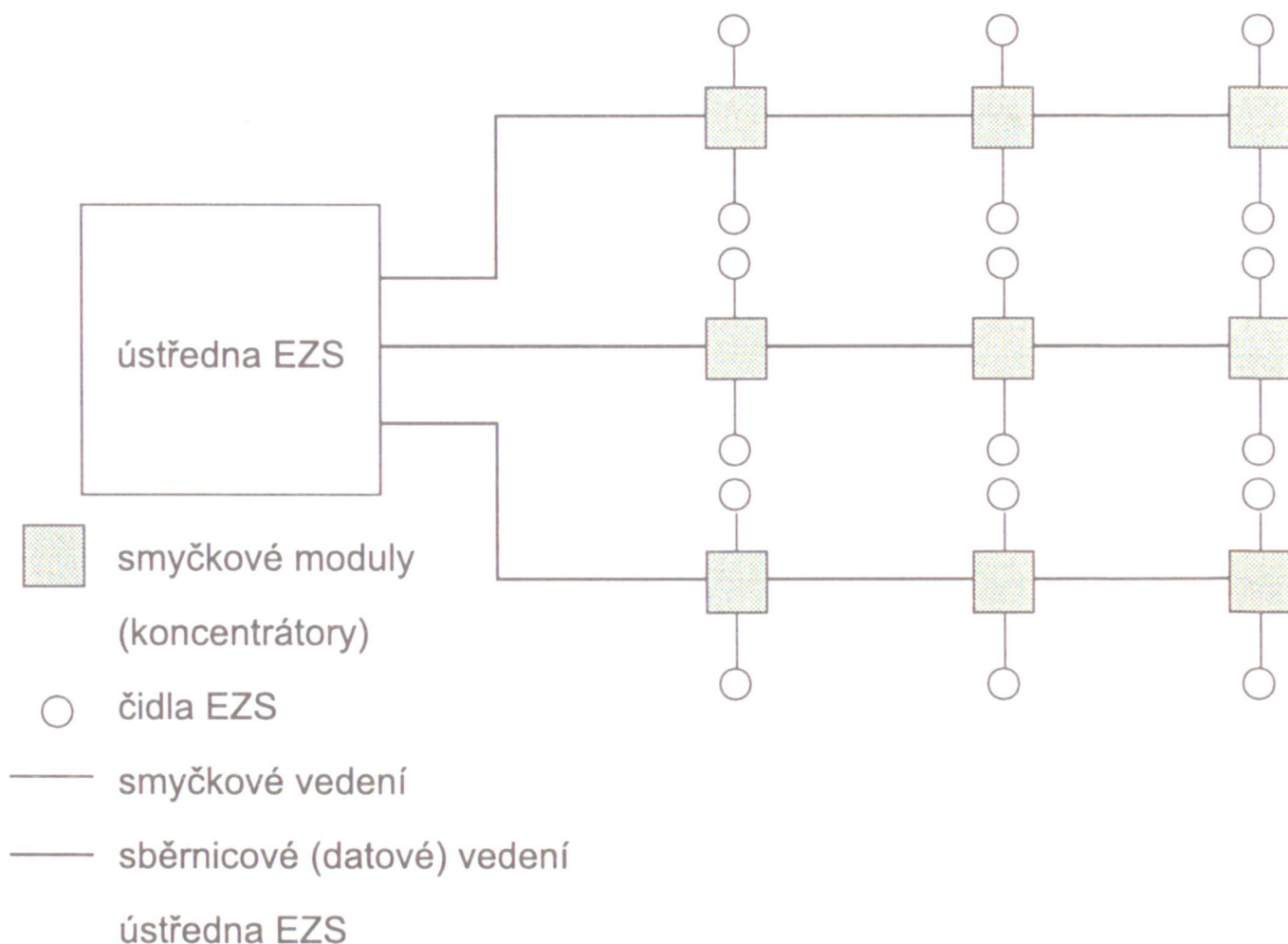


Obr. 3-32: Příklad zapojení systému EZS s ústřednou s přímou adresací čidel.

### 7.1.3 Ústředny smíšeného typu

Tato ústředna pracuje na principu datové komunikace ústředna – koncentrátor (sběrníkový modul smyček). Komunikace mezi ústřednou a koncentrátory probíhá pomocí datové či analogové sběrnice. Na koncentrátory jsou čidla připojena pomocí smyček jako u smyčkových ústředien. Vlastní vyhodnocování probíhá podle typu ústředny různě. Jednou z variant je analogový multiplex, kdy se připojují na sběrnici postupně jednotlivé smyčky a vyhodnocení impedance smyčky s příslušnou odezvou provádí ústředna. Další možností je integrace vyhodnocovací logiky včetně vyrovnávací paměti přímo do koncentrátoru. Komunikace pak probíhá čistě v datové podobě.

Pokud je kapacita ústředny dostatečná, lze na jednotlivé vstupy koncentrátorů připojit přímo jednotlivá čidla. Tím přechází tento typ ústředny na ústřednu s přímou adresací čidel se všemi jejími výhodami. Limitujícím faktorem zde však většinou budou celkové náklady na takto vybudovaný systém. Z tohoto důvodu je potřebné navrhnout optimální rozdělení čidel do smyček tak, aby byla zachována z hlediska uživatele účelná úroveň adresace. Důležitým aspektem návrhu systému zůstává, obdobně jako u předešlé skupiny ústředien, dostatečné dimenzování napájecích i datových vodičů zvláště u rozsáhlých systémů (délka jedné datové sběrnice až do 1 km, s opakovači i více). Navíc tato skupina většinou umožňuje realizaci dodatkových funkcí přímo přes datovou sběrnici.



Obr. 3-33: Zapojení systému EZS s ústřednou smíšeného typu.

#### 7.1.4 Ústředny s bezdrátovým přenosem od čidel

Je to skupina ústřed, které se začínají rozvíjet teprve v poslední době. Nejčastěji pracují v pásmu telemetrie (433 MHz) s výkony okolo 10 mW. Jedná se tedy o vysílací zařízení, které spadá pod působnost legislativy (viz úvodní kapitola).

Přenos poplachového signálu od čidel je nejčastěji 8bitový, kódovaný a adresa čidla je 4bitová. Vhodným návrhem je dosaženo minimálního klidového odběru (cca 10–20  $\mu\text{A}$ ).

Vlastní dosah je ve volném prostředí 100 – 200 m. V objektu je třeba počítat se vzdálenostmi menšími. Čidla jsou napájena buď lithiovou baterií, nebo 9V destičkovým článkem. Napětí baterie je hlídáno a podle provedení buď dojde při poklesu napětí k místní akustické signalizaci interním bzučákem, což upozorní obsluhu na nutnost výměny, nebo je tato informace přenášena do poplachové ústředny.

Obecně lze identifikovat u bezdrátových systémů následující výhody:

- rychlá a snadná instalace,
- možnost instalace do hotových objektů s minimalizací stavebních zásahů,
- snadné rozšíření systému doplněním dalších prvků,
- snadná změna konfigurace (možnost jednoduchého přemístění detektorů při přestavení nábytku).

### 7.1.4.1 Systémy s jednosměrnou komunikací

Jednodušší systémy pracují jednosměrně, tzn., že v čidle je vysílač a v ústředně přijímač. Starší systémy tohoto řešení neměly žádnou kontrolu funkčnosti jednotlivých detektorů (s výjimkou výše popsané indikace poklesu napájecího napětí pod stanovenou mez). Jestliže tedy došlo k poruše prvku nebo jeho násilnému poškození či odcizení, nedostala o tom ústředna žádnou informaci. Modernější systémy pracují na principu pravidelné kontroly přenosové cesty vysíláním kontrolních telegramů. Problémem zde je rozpor mezi požadavkem na co nejvyšší četnost kontrol a požadavkem na velkou trvanlivost baterii napájejících jednotlivé prvky. V praxi se proto obvykle pracuje s četností jednou za několik hodin. To ovšem znamená, že je ústředna o nefunkčnosti prvku informována s určitým (někdy značným) zpožděním. Jestliže u takového systému pachatel poškodí detektor, může uživatel systém zapnout s přesvědčením, že bude mít objekt během své nepřítomnosti náležitě chráněn. Vzhledem k tomu, že je nutné vyloučit nebo alespoň omezit plané poplachy vzniklé následkem náhodných výpadků signálu, způsobené nejrozličnějšími příčinami, vyhodnocuje se obvykle stav jako poruchový nebo poplachový až tehdy nedojde-li několik po sobě jdoucích kontrolních relací (nejméně dvě). Tím se ovšem dále prodlužuje doba během níž systém nemusí zaznamenat poplach nebo poruchu. Jednosměrný systém má značnou nevýhodu také tam, kde je velký pohyb osob (například veřejné budovy). Vzhledem k tomu, že jednotlivé prvky nemají informaci o tom, zda je systém v klidu nebo ve střežení, musejí vždy v okamžiku zjištění poplachového stavu (tedy pohybu v dosahu detektoru) vyslat signál ústředně. Ta sice v klidovém stavu takovou informaci jako poplach nevyhodnotí, ale každé takovéto vysílání vyčerpává energii napájecího zdroje. V praxi se to řeší obvykle tak, že je detektor vybaven časovačem blokujícím po odeslání zprávy po dobu několika minut vysílání. To sice šetří energii zdroje, ale zároveň to ztěžuje následné vyhodnocení pohybu pachatele, protože jeho pohyb po první aktivaci není v dalších minutách monitorován.

Jednou z nevýhod bezdrátových systémů je nebezpečí rušení. To může vést jak ke vzniku falešných poplachů, tak ke ztrátě přenosu. U jednosměrných systémů je relativně snadné zjistit, na jakém kmitočtu a s jakou modulací systém pracuje. Lze jej pak poměrně jednoduše vyřadit z činnosti zahlcením přijímače stejným kmitočtem o podstatně vyšší intenzitě.

### 7.1.4.2 Systémy s obousměrnou komunikací

Nejnovější typy bezdrátových systémů pracují duplexně a každý prvek systému je vybaven jak vysílací, tak přijímací elektronikou – modulem vysílač/přijímač. Tyto inteligentní moduly jsou dokonce schopny si najít ve vyhrazeném kmitočtovém pásmu dva volné kanály pro přenos a automaticky se na ně naladit. V případě rušení těchto kanálů jsou schopny přeladit se na jiné, nezarušené. Zavedení obousměrné komunikace mezi ústřednou a všemi prvky zabezpečovacího systému odstraňuje jmenované nedostatky jednosměrných systémů. Přednosti systémů s obousměrnou komunikací:

- při zapínání systému si ústředna ověří stav všech prvků,
- čidla v klidovém stavu nevysílají, a neplývají proto energií, navíc nemusejí být vybavena blokováním dalšího vysílání po vyslaném poplachu,
- dálkově lze zapnout test chůzí,

- lze uskutečnit funkci automatického přeladění při rušení jako významný faktor zvýšení odolnosti proti úmyslnému i neúmyslnému přerušení přenosu,
- ústředna si může ověřit, zda je došlá poplachová informace skutečný poplach, což umožní vyloučit plané poplachy způsobené rušením.

Jako díly bezdrátových systémů existují bezdrátová čidla pohybu (většinou PIR), bezdrátová tísňová tlačítka, bezdrátové magnetické kontakty, univerzální bezdrátové moduly pro připojení libovolných čidel, stabilní bezdrátové ovládací díly, mobilní bezdrátové ovládací díly, bezdrátové sirény atd.

Bezdrátové systémy jsou vhodné pro dodatečnou instalaci do objektu s minimalizací kabelové sítě a hrubých montážních prací. Rovněž u historických objektů se vzácnými malbami na omítce či s kamennými zdmi, jež neumožňují vedení kabelů, je bezdrátový systém prakticky jediná alternativa. Při provozu je třeba počítat se zvýšenými nároky na pravidelnou kontrolu stavu a výměnu baterií zvláště za nízkých okolních teplot.

### **7.1.4.3 Kódování přenosu a prvků**

Samozřejmým požadavkem u bezdrátových prvků je kódování komunikace mezi jednotlivými prvky systému. To znemožňuje zkreslení během přenosu a znesnadňuje neoprávněné proniknutí do systému s cílem jeho vyřazení z provozu. Kromě toho je nutné jednotlivé prvky v systému identifikovat. U jednodušších systémů se kódování prvků uskutečňuje obvykle naprogramováním mechanickými přepínači binárním způsobem (tzv. DIP – switch), případně programováním pomocí připojeného počítače. U sofistikovaných systémů mají prvky kód pevně přidělen již při výrobě a jejich čísla se programují do ústředny při instalaci systému. Tím je znesnadněno cílené nahrazení (substituce) prvku s konkrétní adresou při pokusu o kvalifikované nabourání systému.

## **7.2 Kritéria výběru ústředny EZS**

Každá z uvedených čtyř skupin ústředen má své opodstatnění na trhu techniky EZS a je věcí projektanta zvolit pro danou aplikaci nejvhodnější řešení. Zde vystupují v rozhodovacím procesu do popředí tři následující aspekty:

- požadovaný stupeň zabezpečení (dle ČSN EN 50131-1) do kterého na základě bezpečnostního posouzení a následné analýzy rizik svým provozem objekt spadá,
- fyzický rozsah objektu, jež má být střežen, a jeho stavební provedení,
- finanční možnosti investora

## **7.3 Vstupní vyhodnocovací obvody**

Jednotlivá čidla EZS (napájená i nenapájená) jsou pomocí vícežilového stíněného kabelu zapojena do poplachové nebo tísňové a zajišťovací (sabotážní) smyčky. Elektrické parametry všech druhů smyček jsou shodné, liší se pouze způsobem hlášení svého narušení. Počet vstupů smyček je dán typem ústředny a může se prakticky pohybovat od čtyř až po stovky smyček.

Vstupní obvody nejjednodušších ústředen bývají obvykle velmi primitivní a jsou schopny vyhodnotit dva základní stavy, a to „smyčka uzavřená“, nebo „smyčka rozpojená“. Jako správný funkční stav se volí stav „smyčka uzavřená“, neboť pak každý de-



struktivní zásah do čidla nebo kabelové sítě vede k poplachovému stavu „smyčka rozpojená“.

Vstupní vyhodnocovací obvody ústředen vyššího standardu (stupně zabezpečení dle ČSN EN 50131-1) jsou dokonalejší a pracují jako přesné odporové děliče nebo jako vyvážené měřicí můstky, u kterých je napětí na děliči nebo v diagonále můstku úměrné velikosti rozvážení děliče nebo můstku. Toto „chybové“ napětí je přiváděno na obvod napětového komparátoru, který při překročení určité meze překlopí svůj výstup, a způsobí tak odpovídající reakci v logických obvodech ústředny. Z uvedeného vyplývá, že takový vstupní obvod ústředny musí být zakončen odporem o definované hodnotě a toleranci. Velikosti zakončovacích odporů jsou pro různé typy ústředen různé (odpory zpravidla dodává výrobce spolu s ústřednou) a pohybují se v rozmezí od 1 k do 12 kΩ. Ústředny pracují s rozvážením vstupního odporu v rozmezí +/- 30 % až +/- 2 %.

Na vstup ústředny je připojena smyčka, která je tvořena kontakty poplachových relé čidel, kabeláží a zakončovacím odporem. Je zřejmé, že výsledná hodnota odporu smyčky je dána hodnotou vlastního zakončovacího odporu zvýšenou o odpor vedení a o hodnoty přechodových odporů kontaktů výstupních relé čidel. Přechodové odpory kontaktů výstupních relé čidel lze v praxi zanedbat, neboť jsou řádově ve srovnání s hodnotou zakončovacích odporů velmi malé. Výrobci však často osazují do čidel sériový odpor kontaktu relé řádově 10Ω. Při zapojení většího počtu čidel do jedné smyčky je pak třeba s těmito odpory počítat!

Výsledná hodnota odporu smyčky je pak dána součtem:

$$R_c = R_z + R_v + R_s$$

kde:

**$R_c$**  je celkový odpor smyčky,

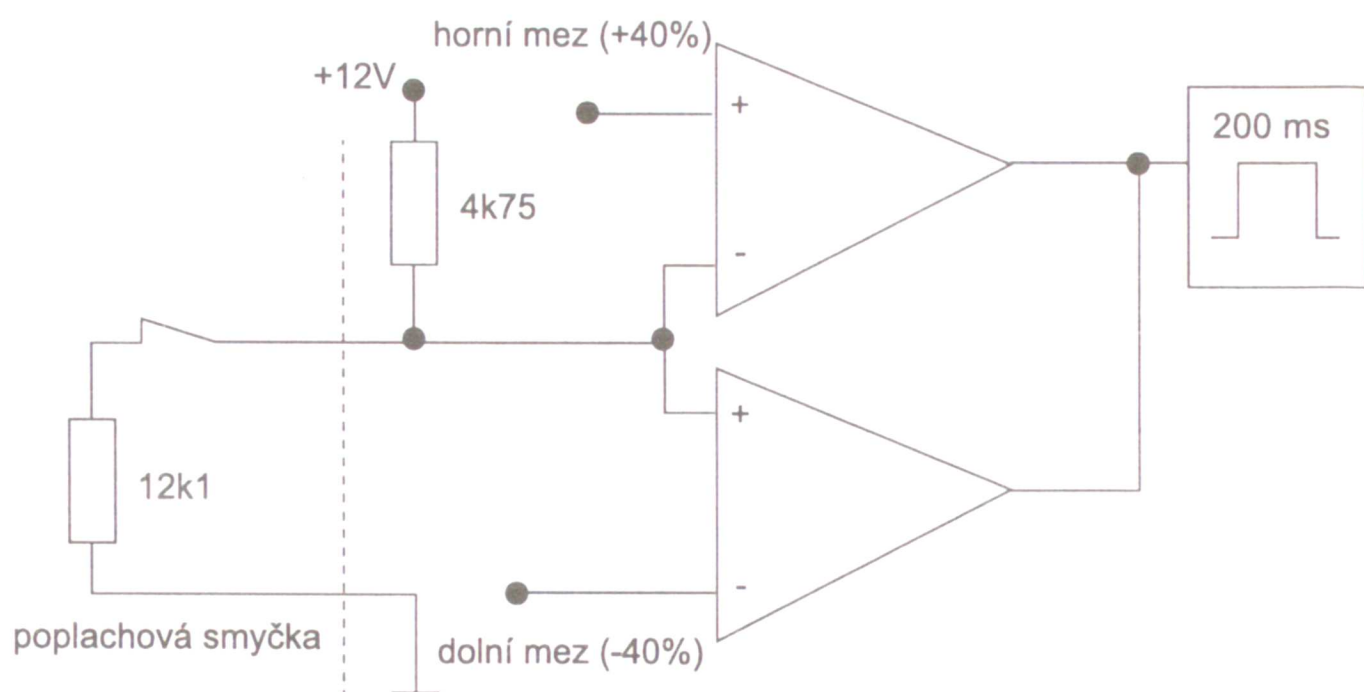
**$R_z$**  je hodnoty zakončovacího odporu,

**$R_v$**  je hodnoty odporu spojovacího vedení,

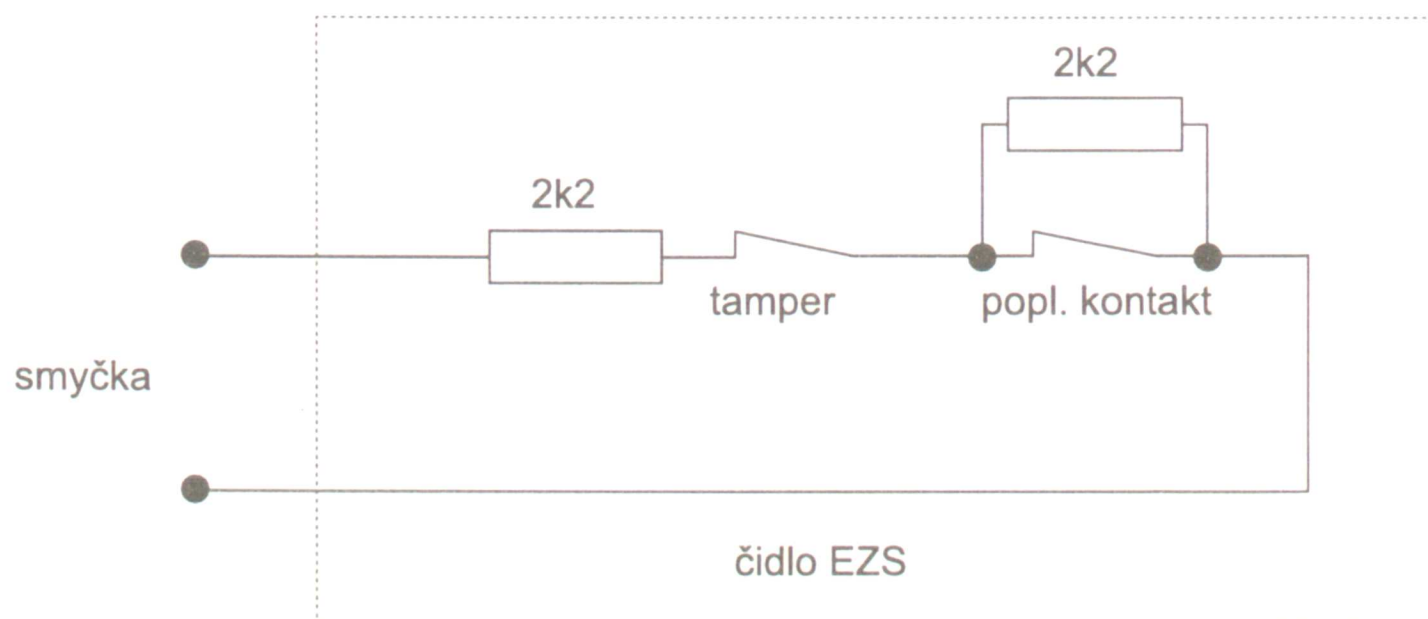
**$R_s$**  je hodnota sériových odporů poplachových kontaktů jednotlivých čidel.

Z tohoto hlediska je nezbytné pro rozsáhlé systémy používat kabely s dostatečným průřezem žil nebo volit ústředny pracující s vyššími hodnotami zakončovacích odporů. V obou případech se tím dosáhne toho, že hodnota odporu spojovacího vedení bude relativně malá proti hodnotě zakončovacího odporu, a vejde se tak do jeho povolené tolerance. Pokud tohoto stavu není možné dosáhnout, pak je nezbytné zvolit takový zakončovací odpor, aby výsledný odpor celé smyčky byl v povolené toleranci. Některé ústředny mají vstupní obvody zdokonaleny do té míry, že si ústředna po spuštění změří skutečné hodnoty odporů smyček a vykompenzuje své vstupy tak, aby chybové napětí vstupního měřicího můstku bylo blízké nule. Od takto získané hodnoty odporu smyčky pak odvozuje všechny změny odporu smyčky.

Vedle klasické vyvážené diferenciální smyčky se s rozvojem techniky A/D převodníků objevují i systémy s tzv. dvojitě vyváženou smyčkou, kdy je možné pomocí jediného smyčkového vedení vyhodnotit jak poplachové hlášení, tak i neoprávněný zásah do čidla či přerušení smyčkového vedení (viz obr. 3-35).



Obr. 3-34: Technické řešení vstupního obvodu vyvážené diferenciální smyčky.



Obr. 3-35: Zapojení tzv. dvojitě vyvážené smyčky.

Tabulka 3-4: Příklad interpretace stavů na dvojitě vyvážená smyčce

	Zajišťovací kontakt	Poplachový kontakt	Odpor smyčky	Příklad interpretace v číselném vyjádření displeje ústředny		
				min.	typ	max.
Sabotáž (otevření čidla)	x	o	nekonečno	64	72	89
Sabotáž (zkrat)	o	o	0	0	3	14
Poplach	o	x	4k4	39	42	51
Klid objektu	o	o	2k2	24	28	37

*Poznámka – Tato varianta provedení vstupních obvodů je hojně užívaná zvláště u ústředen anglosaské provenience, ale díky svým technickoekonomickým výhodám se začíná objevovat i u tak konzervativních výrobců, jako jsou výrobci ze SRN.*

Vstupní obvody ústředen jsou citlivé na změny vstupních elektrických parametrů, a mohou tedy být citlivé i na elektromagnetické rušení, které u rozsáhlých kabelových sítí, a zvláště v průmyslových objektech, může dosáhnout takové výše, že zkomplikuje, popř. zcela znemožní spolehlivou funkci celého systému EZS. Nejen z tohoto důvodu je prakticky nezbytné provádět všechny rozvody smyček stíněnými vodiči.

**Stínění jednotlivých kabelů je třeba dobře propojit, a to tak, že nesmí tvořit uzavřenou zemní smyčku.** V praxi to znamená, že stromovitě propojíme stínění všech kabelových větví a stínění připojíme na svorku PE sítě v ústředně EZS.

Vstupní obvody bývají obvykle vybaveny ochrannými prvky (jiskřiště, varistory) pro ochranu před účinky elektromagnetického rušení vnikajícího indukci do kabelové sítě nebo účinky atmosférické elektřiny.

Funkční vlastnosti jednotlivých vstupních obvodů ústředen z hlediska hlášení v rámci systému jsou buď pevně dané (tíseň, sabotáž, vloupání, poplachové smyčky zpožděné, poplachové smyčky okamžité), nebo programovatelné. Pak je možné podle konkrétní aplikace měnit vlastnosti jednotlivých smyček z hlediska funkce systému EZS. Požadavky na indikaci a hlášení jednotlivých provozních, poplachových a poruchových stavů jsou závislé na stupni zabezpečení a jsou taxativně stanoveny v ČSN EN 50131-1.

#### 7.4 Výstupní obvody ústředen

Výstupní obvody ústředen EZS umožňují aktivovat výstupní signalizační a indikační obvody a prvky systému EZS. Patří sem zejména tyto výstupy:

- **Výstup pro akustickou signalizaci**, kterou je zpravidla pasivní nebo aktivní siréna. Výstup pro akustickou signalizaci bývá obvykle programovatelný a umožňuje volit dobu funkce sirény (podle ČSN EN 50131-1/Z1), dobu zpoždění sirény, přerušování zvuku sirény, modulaci zvuku sirény, popřípadě volit chování výstupu podle toho, jakým typem smyčky byl poplachový stav aktivován.
- **Výstup pro optickou signalizaci**, kterou je zpravidla zábleskový maják. Tento výstup se obvykle spíná současně s výstupem pro akustickou signalizaci, ale zůstává aktivní i po jejím doznění, a to až do doby vynulování ústředny. Někdy bývá též programovatelný.
- **Výstup telefonního voliče** je uzpůsoben pro připojení k JTS. Tento výstup buď kódem, nebo hlasově oznámí na zvolená telefonní čísla předem naprogramované údaje nebo předem namluvenou zprávu. Umožňuje tak přivolání pomoci i v případě, kdy pachatel zneškodní sirénu a maják nebo když na jejich činnost nikdo nereaguje. Je-li ústředna připojena na pult centralizované ochrany, sdělí pak pomocí kódovaného přenosu zprávy v příslušném formátu o jaký typ narušení objektu se jedná, případně která část objektu je narušena. U tohoto typu spojení se často využívá tzv. tichý poplach, tedy poplach bez aktivace sirény a majáku. Požadavky na formu hlášení jednotlivých provozních, poplachových a poruchových stavů jsou závislé na stupni zabezpečení a jsou taxativně stanoveny v ČSN EN 50131-1.

- **Programovatelné výstupy** umožňují vytvořit potřebné výstupní signály ať již impulsní (např. pro resetování čidel s pamětí), nebo definovaných úrovní pro různé periferie (inteligentní sirény, přenosy pro diagnostiku systému EZS atd.).
- **Pomocné zvukové výstupy** slouží pro připojení jednoho nebo více reproduktorů, umožňují zvukové indikace například otevření dveří (dveřní gong), náběhu odchodového intervalu (zpoždění zapnutí smyčky), náběhu vstupního intervalu (zpoždění poplachu), narušení sabotážní smyčky v režimu klidu objektu (denní režim) bez aktivování sirény, interní poplach při odbočení z odchodové trasy, indikaci neuzavřeného obvodu poplachové smyčky při odchodu atd.
- **Výstupy pro periferie** jsou k dispozici zejména u ústředn vyšší kategorie. Jsou to především výstupní porty pro napojení registračních zařízení (tiskáren), signalizačních tablo, dále sériové přenosové kanály (obvykle s rozhraním RS 232) pro připojení PC či programovacích modulů.
- **Bezpotenciálové výstupy** jsou tvořeny obvykle přepínacími kontakty relé. Počet relé bývá omezený a podle typu se pohybuje do počtu 32. Pomocí těchto výstupů lze vytvářet atypické funkční vazby mezi systémem EZS a dalšími doplňkovými bezpečnostními systémy, jako jsou např. uzavřené televizní okruhy (CCTV), systémy kontroly a řízení vstupu osob do objektu nebo systém aktivace osvětlení objektu poplachovým signálem.

### 7.5 Napájecí obvody

Napájecí obvody slouží k napájení elektronických obvodů vlastní ústředny a k napájení všech návazných prvků systému EZS. Protože systém EZS musí být funkční i při výpadku napájecího napětí sítě, je napájecí zdroj ústředny zálohován náhradním zdrojem napětí. Ten je tvořen bezúdržbovými plynotěsnými olověnými akumulátory. Lze z nich vytvořit náhradní zdroj s kapacitou 1,2 Ah až řádově 100 Ah. podle rozsahu systému EZS a podle předepsaného režimu zálohování (viz ČSN EN 50131-1 čl. 9.2, tab. 16 a norma ČSN EN 50131-6 tab. 2).

Síťový napájecí zdroj dodává stabilizované napětí +13,8V se zatížitelností odpovídající rozsahu systému EZS 1 A až 5A. Pokud je systém EZS rozsáhlejší, pak je nezbytné použít přídatný síťový napájecí zdroj s vlastním náhradním zdrojem napětí. Přídatné síťové napájecí zdroje se dodávají se zatížitelností od 1 A do 10 A.

*POZNÁMKA – U rozsáhlých systémů je z hlediska úbytku na dlouhých vedeních výhodné používat více zdrojů s menší zatížitelností umístěných na různých místech objektu (tzv. decentralizované napájení systému EZS).*

Ústředna EZS tedy obsahuje vždy dva zdroje – základní a náhradní.

- Základní napájecí zdroj – zdroj elektrické energie pro trvalé napájení zařízení EZS.
- Náhradní napájecí zdroj – zdroj elektrické energie pro napájení zařízení EZS při výpadku základního zdroje.

Jaké jsou požadavky na tyto zdroje?

**Základní napájecí zdroj** musí být schopen dodat potřebný proud, jenž je součtem proudových odběrů všech prvků systému na daný zdroj připojených včetně ústředny.

Dále musí být základní zdroj dimenzován tak, aby po skončení nejdelšího výpadku sítě byl schopen dodat potřebný proud nejen pro všechny prvky na zdroj připojené, ale i proud potřebný k dobíjení připojeného akumulátoru či akumulátorů během doby stanovené v ČSN EN 50131-1 (ČSN EN 50131-6).

**Náhradní napájecí zdroj** musí být dimenzován tak, aby byl schopen překlenout nejdelší výpadek základního zdroje dle požadavků normy ČSN 50131-1 (ČSN EN 50131-6), odlišný pro jednotlivé stupně zabezpečení vztažený k úrovni rizik objektu.

Tabulka 3-5: Požadované doby zálohování systému EZS

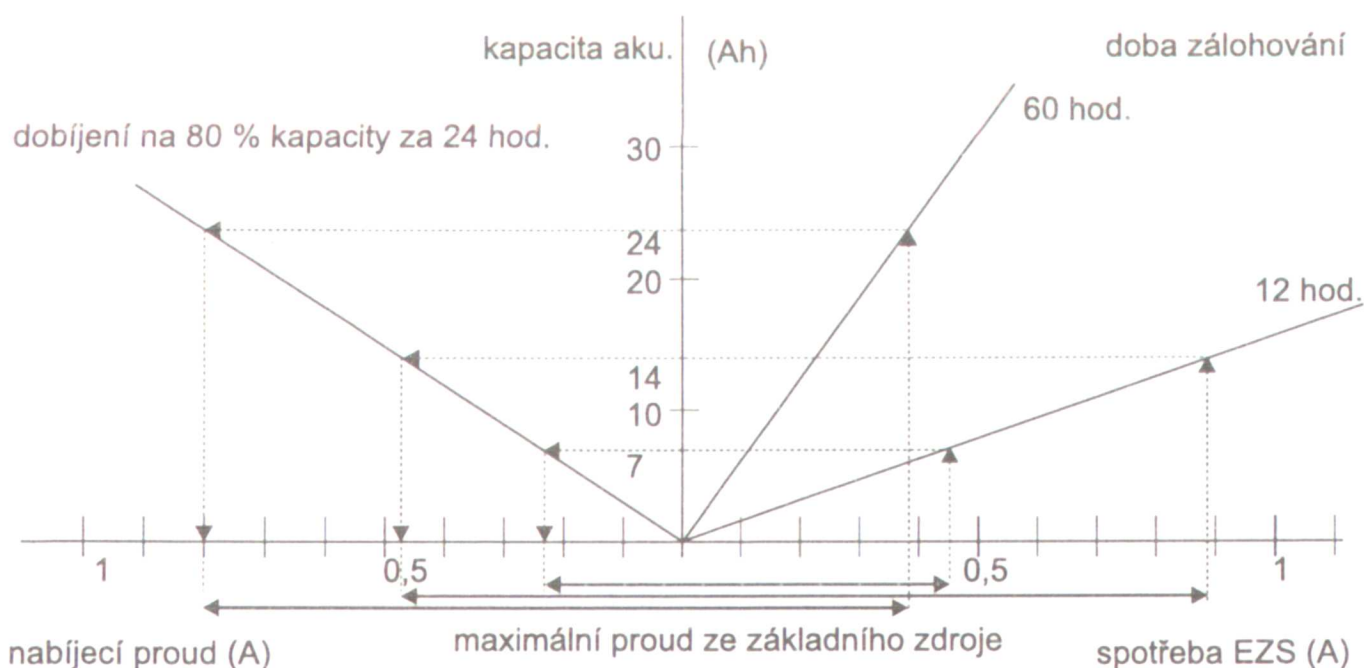
	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Minimální doba pohotovosti (hod.) (dle ČSN EN 50131-1)	12	12	60	60
Minimální doba pohotovosti (hod.) (dle ČSN EN 50131-6)	8	15	24	24

Poznámka (ČSN EN 50131-1): Je-li stav napájecího zdroje přenášen do PCO/PPC, je možno snížit u stupňů zabezpečení 3 a 4 dobu zálohování na 50% stanovené doby. Pro EZS stupně 2, 3, 4 vybavené doplňkovým základním napájecím zdrojem s automatickým přepínáním (např. síť zálohovaná dieselagregátem) je možné dobu zálohování snížit na 4 hod. <R>Poznámka (ČSN EN 50131-6): Je-li napájecí zdroj instalován jako součást EZS musí doby pohotovosti odpovídat ČSN EN 50131-1.

Tabulka 3-6: Požadované doby nabíjení

	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Maximální doba dobíjení na min. 80% kapacity	72	72	24	24

Vyneseme-li tabulkové hodnoty do grafu (obr. 3-36), můžeme určit ze známého odběru systému v závislosti na požadované době zálohování potřebnou kapacitu akumulátoru potřebnou pro stanovený stupeň zabezpečení.

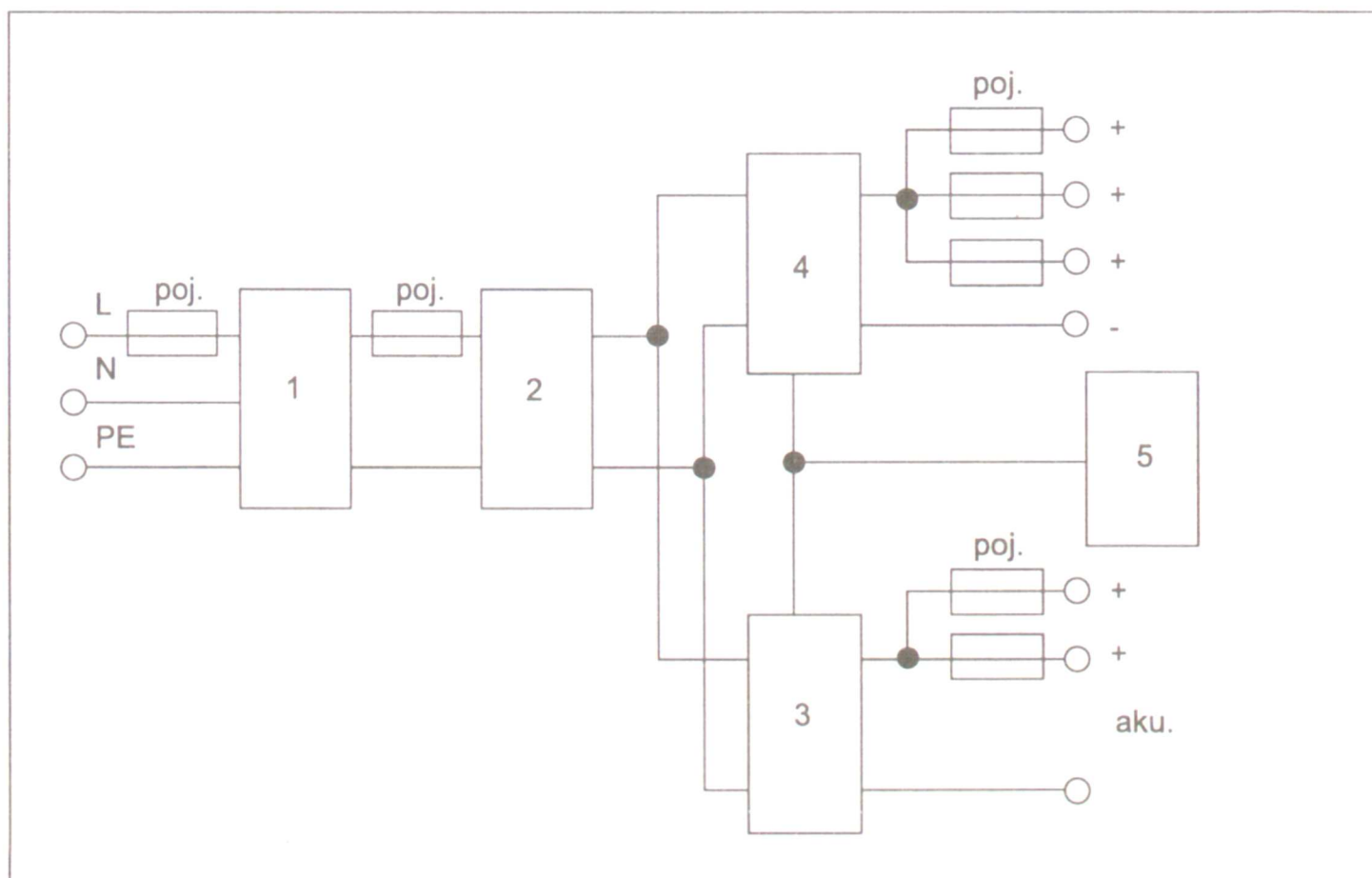


Obr. 3-36: Graf pro určení kapacity základního a náhradního zdroje.

Dále zde můžeme ze součtu požadovaného dobíjecího proudu a odběru systému stanovit celkové požadované proudové dimenzování zdroje.

Z prostého součtu uvedených proudů stanovíme sice požadovaný výkon zdroje, nejde však o prostý součet proudů. Je nutné si uvědomit, že např. akumulátor o jmenovité kapacitě 7 Ah při vybití na 50% v režimu dobíjení konstantním napětím bez proudového omezení je schopen odebrat ze zdroje proud 3,4 A a proud poklesne na hodnotu vypočtenou z výše uvedených kritérií cca po 4 hod. dobíjení! Tentýž zcela vybitý akumulátor odbírá v počátcích nabíjení dokonce 4,3 A! Z těchto údajů je jasné, že konstrukčně musí být zdroj vybaven minimálně dvěma nezávislými výstupy. Jeden s požadovaným proudovým omezením pro dobíjení akumulátoru a druhý dimenzovaný na celkový odběr systému EZS či jeho část z daného zdroje napájené.

Volbě vhodného zdroje je třeba věnovat při návrhu systému EZS dostatečnou pozornost. Jak by měl takový zdroj vypadat a jaké funkce by měl plnit je uvedeno dále.



Obr. 3-37: Blokové schéma napájecího zdroje ústředna EZS.

- BLOK 1 Síťová část je řešena jako elektrický předmět třídy I. Svorkovnice je určena pro připojení pevného třížilového přívodu. Na vstupu síťové části je zařazen odrušovací člen a přepět'ový filtr. Primární obvod má vlastní jištění tavnou pojistkou. Síťové napětí je sníženo na potřebnou hodnotu pomocí bezpečnostního oddělovacího transformátoru. Sekundární obvod má rovněž samostatné jištění tavnou pojistkou.
- BLOK 2 Tento blok obsahuje dostatečně proudově dimenzovaný usměrňovač a vyhlazovací kondenzátor vhodné kapacity. Poté se napětí dělí do dvou paralelních větví.

- BLOK 3 Slouží k zajištění teplotně kompenzovaného stabilizovaného napětí s proudovým omezením k zajištění optimálního dobíjení náhradního zdroje (bezúdržbového olověného akumulátoru). Teplotní kompenzace vychází z doporučení výrobců bezúdržbových akumulátorů a jejím akceptováním se životnost akumulátorů zvyšuje.
- BLOK 4 Zajišťuje stabilizaci napětí potřebného k napájení ústředny a prvků systému EZS. Tento výstup na výstupu je opatřen přepětovou ochranou sloužící k ochraně připojených zařízení v případě hrubé poruchy zdroje. Napájecí výstup je rozdělen do několika samostatně jištěných větví.
- BLOK 5 Zahrnuje hlídací logiku zdroje včetně indikačních výstupů. Hlídání pohotovosti náhradního zdroje je zajištěno cyklickým odpojením (každých 6 min.) napájení ze síťové větve zdroje (BLOK 4) a připojením systému na náhradní zdroj (po dobu 8 s). V tomto okamžiku logika porovnává napětí náhradního zdroje s referenční hodnotou a rozhoduje o vyhlášení indikace "porucha náhradního zdroje". Úlohou logiky je i odpojení náhradního zdroje při vybití pod určitou předem stanovenou mez. Tato funkce slouží k ochraně relativně drahých akumulátorů před úplným vybitím.

## 8 Ovládací a indikační zařízení

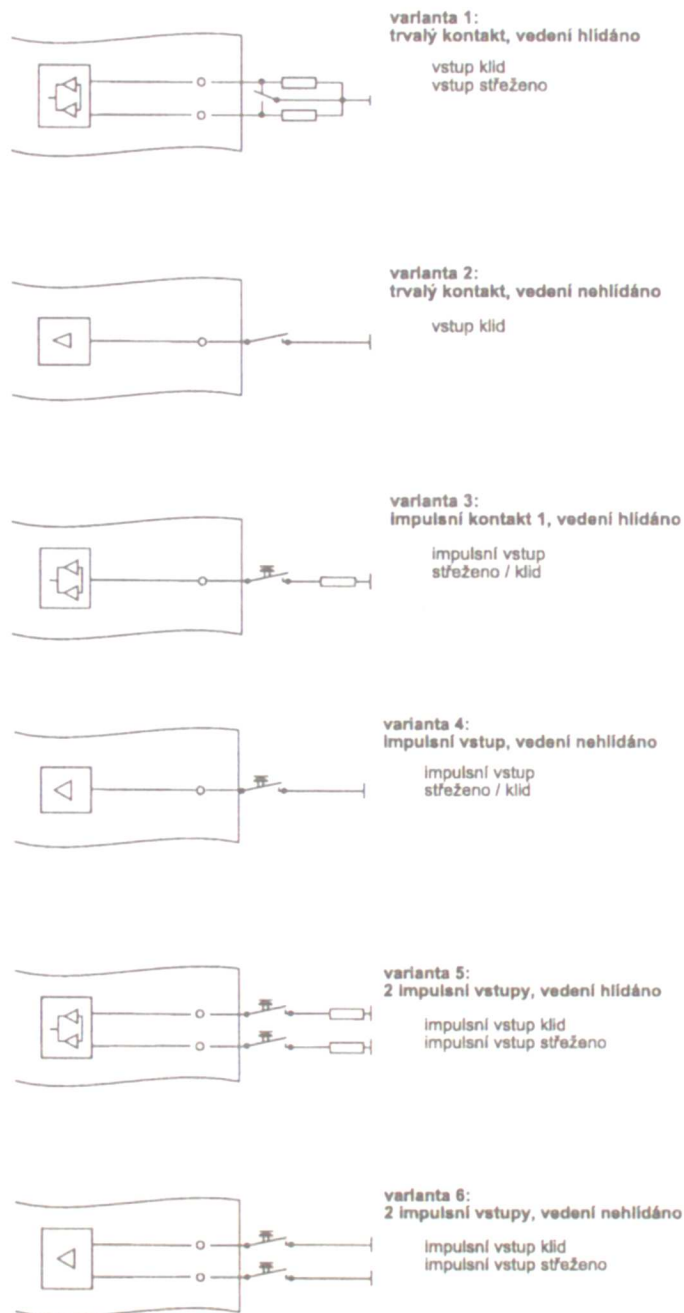
### 8.1 Funkce a varianty ovládání

Aby mohl systém EZS plnit svou funkci, musí být možno uvádět jej do stavu střežení a naopak do stavu klidu. K tomuto účelu jsou určena ovládací zařízení. Vhodný typ ovládacího zařízení se volí podle úrovně rizik (stupně zabezpečení) a požadavků zákazníka. Cílem je jednoduchá obsluha s minimalizací možnosti vyvolat při manipulaci s ovládacím zařízením planý poplach za současně dostatečné ochrany proti kvalifikovanému překonání.

Ústředny umožňují realizovat přepínání do stavu střežení a zpět do stavu klidu různými způsoby. Na Obr. 3-38 jsou uvedeny možné varianty provedení vstupních obvodů pro kontaktní ovládání ústředen EZS.

Ovládací a indikační zařízení kromě základní funkce slouží k:

- odpínání a připínání smyček (pro případ částečného střežení),
- volbě speciálních funkcí (např. tísňové hlášení z klávesnice, testování funkce čidel, vyvolání paměti dějů apod.),
- zadávání uživatelských kódů pro ovládání systému,
- programování instalačních parametrů systému,
- odstavení a resetování poplachů atd.



Obr. 3-38: Varianty ovládání ústředí EZS.

Indikační prvky informují o provozních stavech ústředny a celého systému, a to buď opticky pomocí LED, nebo pomocí akustické signalizace, popř. kombinací akustické a optické signalizace. U ústředí s vyšším ovládacím komfortem probíhá komunikace s uživatelem pomocí alfanumerického displeje. Úroveň indikačních prvků do značné míry podmiňuje úroveň systému diagnostiky. Diagnostika umožňuje selekci závad v systému EZS i ve vlastní ústředně EZS, a usnadňuje tak servisním technikům případné opravy. V zásadě lze říci, že u všech ovládacích dílů různých výrobců nalezneme společné znaky v okruhu hlášení základních provozních stavů.

Jsou to především:

- hlášení stavu střežení/klid systému EZS,
- hlášení připravenosti k uvádění do stavu střežení,
- hlášení poruchy (základního či náhradního zdroje),



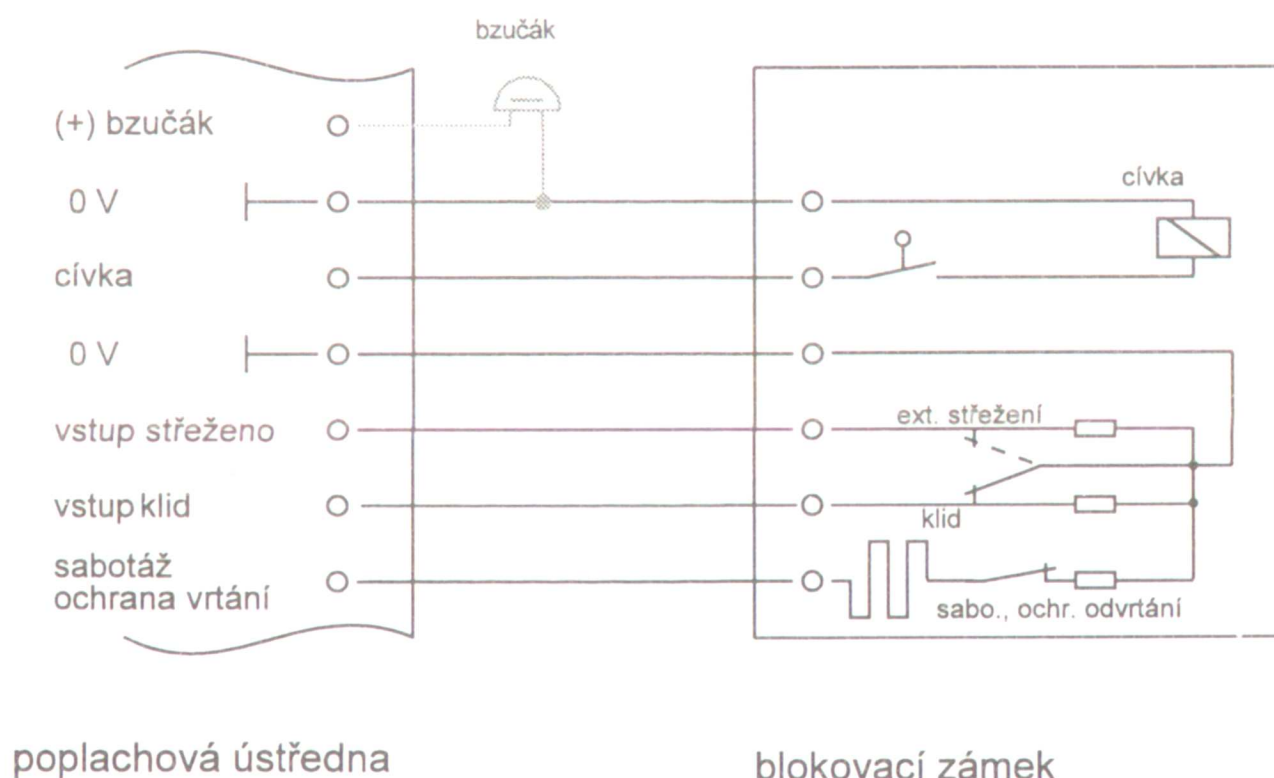
- hlášení narušení smyček,
- hlášení tísně (přepadení),
- hlášení poplachu.

### 8.1.1 Blokovací zámek

Blokovací zámek kombinuje prvek mechanického zabezpečení vstupních dveří spolu s ovládáním systému EZS. Montuje se jako přidavný zámek vstupních dveří. Je to nejbezpečnější, a zároveň z hlediska uživatele nejjednodušší druh ovládacího zařízení. Vlastní konstrukcí je zajištěno spolehlivé uvádění do stavu střežení a naopak. Zámek lze uzamknout jedině tehdy, je-li systém v normálním stavu. V případě poruchy či opomenutí obsluhy (např. otevřené okno) elektromagnetická západka znemožní uzamčení blokovacího zámku, a tím i uvedení systému do stavu střežení. Jde-li zámek uzamknout, má uživatel jistotu, že je systém v pořádku.

Naopak při vstupu do objektu má uživatel jistotu, že je systém odblokován, neboť nejdříve musí odemknout, aby mohl vstoupit. Odemknutím blokovacího zámku přejde systém automaticky do stavu klidu objektu.

Užití blokovacího zámku je nejpřirozenější a nejlepší způsob ovládní systému. Je však také nejnákladnější. Podle provedení blokovacího zámku jej lze osadit buď cylindrickou vložkou, nebo je jeho součástí motýlkový či křížový zámek odolný proti vyhatání a rozlomení. Vlastní zámek je rovněž chráněn proti odvrtání celoplošným vodivým meandrem zapojeným do samostatné zajišťovací (sabotážní) smyčky. Ovládací vedení je rovněž elektricky střeženo, popř. podle typu ústředny je chráněno sabotážní smyčkou.



Obr. 3-39: Zapojení blokovacího zámku.

### 8.1.2 Spínací zámek

Je to ovládací zařízení podobné blokovacímu zámku, ovšem bez blokovací elektromagnetické západky.

Lze jej využít k **odpojování smyček** (umožňuje-li to ústředna) či k ovládání ústředny EZS.

Odpínání smyček spínacím zámekem by mělo být z hlediska uživatele doplněno zpětnou optickou či akustickou indikací otevřené smyčky, jež byla odpojena.

**Při ovládání celého systému EZS** pomocí spínacího zámku je třeba nejprve na displeji ovládacího dílu ústředny ověřit, že není v systému žádný problém či porucha, které by znemožnily přechod systému EZS do stavu střežení. Možné je umístit v blízkosti zámku paralelní optickou indikaci, která nás utvrdí v jistotě, že systém skutečně přeše do stavu střežení.

### 8.1.3 Kódové klávesnice

Funkčně mohou být využity jako spínací zámky. Pro využití jako ovládacího dílu ústředny EZS je však nezbytné, aby elektronika klávesnice byla v samostatné skříni a byla umístěna ve střežených prostorech. Mimo střežené prostory je pak možné umístit pouze tlačítkové pole a indikace. Z hlediska uživatele přinášejí kódové klávesnice nutnost zapamatování si správného kódu. Další problém je nutnost občasné změny kódu (opět nároky na uživatele). Trvalý provoz se stejným kódem vede vedle rizika vyzrazení i k fyzickému opotřebení užívaných tlačítek, což sníží počet možných variant pro tipaře či lupiče. Mezi výhody patří u většiny používaných typů možnost využití tísňového kódu v rizikovém okamžiku vstupu do objektu. Některé typy vybavené více výstupy relé lze využít pro ovládání elektrického vrátného, pro spínání osvětlení apod.

### 8.1.4 Kombinované indikační a ovládací díly

Umožňují spolu s ovládáním systému indikovat informace o systému. Kombinované indikační a ovládací díly jsou používány i pro nejvyšší úroveň rizik. Lze je užít i jako vnitřní indikační tablo pro potřeby uživatele či najaté hlídací služby. Vlastní připojení k ústředně je řešeno většinou prostřednictvím datové sběrnice, která je u systémů pro vyšší rizika elektronicky hlídána proti napadení.

### 8.1.5 Ovládání kartou

Zvláště v poslední době se začínají objevovat na trhu poplachové ústředny EZS, jež umožňují spolupráci se čtečkou identifikačních karet (kontaktních, bezkontaktních). Tento trend je prosazován zvláště u integrovaných systémů, kde v rámci celého komplexu musí spolu korespondovat EZS, CCTV, přístupový systém, EPS a další slaboproudé systémy.

Cílem takových snažení je, aby ve finále uživatel pomocí jediného média (karty) vjel do garáží, ohlásil svou přítomnost v práci, dostal se do výtahu, navolil své patro, odpojil ze střežení svou kancelář, vstoupil do ní, pohyboval se po areálu podniku, přes den na kartu nakupoval v kantýně, platil výkony závodního lékaře, vybíral obědy v jídelně atd...

## 9 Doplnková zařízení ústředn EZS

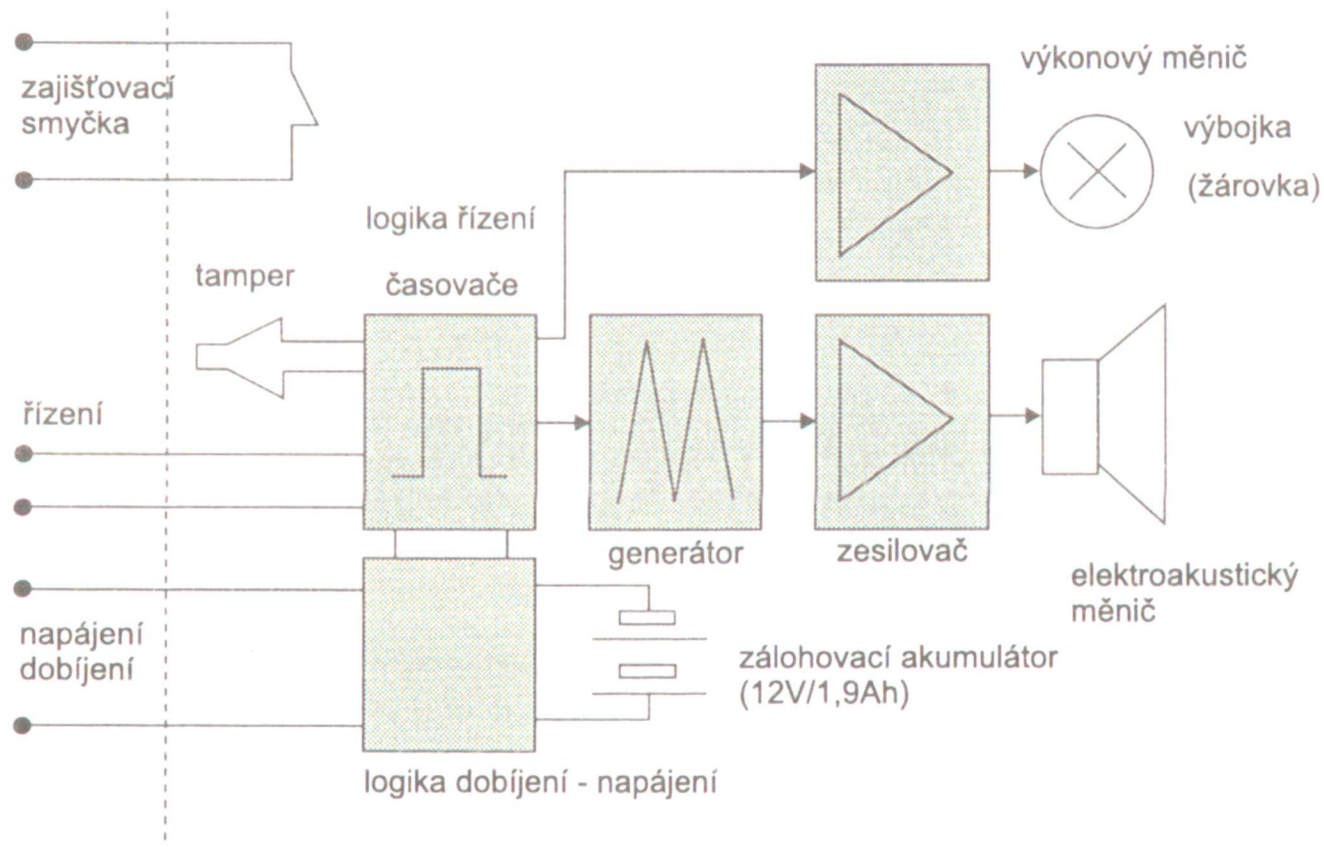
Pod pojmem doplnková zařízení ústředn EZS rozumíme všechna samostatná zařízení, jež jsou umístěna buď v krytu ústředny, nebo mimo ni, a jsou řízena řídicími výstupy ústředny.

*Poznámka – Některá ze jmenovaných zařízení mohou být přímo součástí ústředny, jiná jsou vždy řešena jako externí. Závisí to na výrobci, na technickém provedení ústředny – jejím typu, míře rizik, a také na ceně.*

### 9.1 Akustická signalizace

Nejčastěji instalovaným doplnkovým zařízením je akustická signalizace (siréna). Podle provedení může být určena pro vnitřní či venkovní prostředí. Základem je vždy akustický měnič (piezoelektrický či dynamický) doplněný generátorem kolísavého tónu a výkonovým zesilovačem. Méně časté je využití sirén s motorovým pohonem. Akustický výkon je stanoven v technických požadavcích na zařízení. Doba aktivace by měla být omezena (norma ČSN EN 50131-1 stanovuje dobu min. 90 s a max. 15 min. s odkazem na národní předpisy).

Nejčastěji se umísťují sirény na průčelí střeženého objektu do výšky, která je pokud možno nedostupná bez použití žebříku, štaflí či montážní plošiny. V dnešní době jsou nejrozšířenější tzv. „inteligentní“ sirény s vlastním zálohováním.



Obr. 3-40: Blokové schéma inteligentní sirény.

Siréna je pak propojena a poplachovou ústřednou vícežilovým kabelem, který slouží k ovládání řídicího vstupu sirény rozpínacím kontaktem bezpotenciálového relé ústředny, popř. výstupem otevřeného kolektoru spínacího tranzistoru, dále slouží k dobíjení zálohovacího akumulátoru a k přivedení sabotážní smyčky sirény. Inteligentní siréna je pak aktivována ve více případech. Jsou to:

- regulérní poplach systému EZS,
- přerušení kabelového propojení ústředna – siréna,
- pokus o odstranění pláště sirény,
- pokus o sejmutí sirény se zdi.

Některé sirény mají uvnitř dokonce optoelektronický hlídací modul, který aktivuje poplach při pokusu o odstavení sirény zapněním vnitřku krytu skrz akustickou mřížku, jiné řeší tento problém pomocí dvojitého krytu speciální konstrukce.

*Poznámka – Ze statistik vyplývá velice nízké procento policejních zásahů na základě hlášení veřejnosti o aktivaci sirény. Použití sirén lze tedy v dnešní době chápat především jako psychologický prostředek odstrašující potenciálního pachatele či pachatele v akci.*

### 9.2 Optická signalizace

Optická signalizace (světelný maják) je u venkovních sirén nejčastěji součástí jejich krytu. Technicky se jedná o výkonovou 12V žárovku buzenou přes elektronický přerušovač, nebo lépe o výbojku buzenou z vlastní elektroniky. Doporučená barva optické signalizace je oranžová. Z hlediska vlastní funkce je účelné, aby řízení umožňovalo časově neomezenou aktivaci v případě vyhlášení poplachu. Smysl tohoto opatření spočívá v možnosti identifikace narušeného objektu i po doznění sirény v případě umístění více střežených objektů nedaleko od sebe.

### 9.3 Grafická tablo

U rozsáhlých objektů slouží grafická tablo k usnadnění orientace obsluhy při ovládání systému, a samozřejmě hlavně v případě vyhlášení poplachu. Tato tablo jsou v podstatě panely s vyznačeným plánem objektu doplněné o indikační žárovky či LED a prosvětlené symboly.

*Poznámka – V dnešní době jsou grafická tablo nahrazována obrazovkou počítače s implementovaným speciálním ovládacím a grafickým softwarem. Uživatelé z oboru vězeňské služby a armády, historicky zvyklí na tuto formu znázornění situace ve střeženém objektu, však i dnes vedle obrazovky řídicího počítače požadují grafická tablo pro jejich podstatné výhody. Hlavním argumentem je rozměr grafických tablo, který umožňuje snadnou orientaci a sledování situace současně více osobami při řízení akce při vzniku mimořádných situací.*

## 9.4 Tiskárny

Pro potřebu pozdější analýzy událostí, k nimž došlo ve střeženém objektu, ale i pro případnou kontrolu činnosti obsluhy spojenou s ovládáním rozsáhlých systémů EZS, bývaly ústředny vybaveny zabudovanými tiskárnami. Tiskárna zpravidla zaznamenávala čas a událost (místo napadení, přepínání ústředny EZS, odpinání smyček, poruchy, odstavení a resetování poplachů atd.

S rozvojem mikroelektroniky, se zavedením mikropočítačů do řídicích jednotek ústředny EZS, a hlavně s poklesem ceny polovodičových pamětí je archiv událostí většinou řešen v elektronické podobě, má dostatečnou kapacitu (řádově 10 – 1000 událostí) a možnost připojení tiskárny zůstává jen pro případy výpisu dějů v případě potřeby zpětné analýzy poplachových událostí.

U rozsáhlých systémů EZS vybavených řídicím počítačem je jako archiv událostí využit pevný disk. Výtisk je pak běžnou funkcí softwarové podpory.

## 9.5 Poplachová přenosová zařízení (komunikátory)

S rozvojem komerčních služeb soukromých hlídacích agentur přejímají úlohu vyhlášení poplachu od sirén přenosová zařízení. Přenosové zařízení zprostředkuje po zvoleném médiu (JTS, vzduchem, po privátní komunikační síti) informaci o stavu systému či narušení objektu majiteli nebo na monitorovací pracoviště hlídací služby. Přenos poplachových signálů je samostatná úloha vymezená funkcí poplachového přenosového systému. Tato oblast je normalizačně popsána souborem norem řady ČSN EN 50136++ (viz úvodní kapitolu knihy). Samozřejmě všechna tato zařízení spadají pod působnost legislativy vztahované k provozu koncových rádiových a telekomunikačních zařízení.

### 9.5.1 Zařízení určená pro informování majitele objektu

Mezi nejjednodušší patří tzv. automatické telefonní hlásiče (ATH), které umožňují na naprogramované telefonní číslo po vyhlášení poplachu automaticky zavolat a předat zprávu o trvání 20 – 30 s uloženou v paměťovém digitálním řečovém modulu. Volbu telefonního čísla lze vícekrát opakovat, některá zařízení mají možnost volit více různých čísel, jiná mají doplněk pro kontrolu stavu telefonní linky. Moderní typy umožňují v součinnosti s digitální ústřednou JTS uvolnit obsazené telefonní číslo apod.

Existují přenosová zařízení umožňující poslat prostřednictvím JTS krátkou textovou zprávu (SMS) na mobilní telefon nebo pagerovou službu. V objektech bez telefonní linky (JTS) je možné aplikovat komunikátor v podobě GSM brány, která vedle vyslání poplachové zprávy umožňuje případné dálkové ovládání elektrických zařízení nainstalovaných v objektu. Problém poplachové komunikace prostřednictvím GSM je ten, že mobilní operátoři nerozlišují priority jednotlivých zpráv, a tak poplachové hlášení může přijít v extrémních případech i se zpožděním několika hodin.

### 9.5.2 Zařízení určená pro komunikaci s PCO/PPC

Jsou to zařízení sloužící k předávání informací o systému EZS monitorovacím pracovištím hlídacích služeb (PCO/PPC).

Zařízení na principu automatické telefonní volby (ATV) komunikují s obsluhou PCO již nikoliv hlasitým vzkazem, ale s vyhodnocovacím zařízením pomocí určitého kódu, který obsahuje adresu objektu a druh předávané zprávy. Jsou závislá na přítomnosti JTS,

což v současné době rozvoje sítí JTS již není žádný problém. Dříve diskutovaný problém možnosti napadení především nadzemních a povrchových telefonních vedení je již minulostí. V odůvodněných případech však je žádoucí použít dvě nezávislé přenosové cesty. Jedna z nich může být JTS, druhá pak elektromagnetické pole. Jsou však i případy, kdy z různých důvodů není JTS k dispozici. Pro takové případy slouží přenosová zařízení s datovou komunikací ve vyhrazených pásmech elektromagnetického spektra. Jedná se v podstatě o vysílače s výkony řádově 1 – 10 W uzpůsobené pro přenos datových informací přímo z datových výstupů ústředěn EZS či konvertovaných do datové podoby z jiných výstupů ústředěn (výstupní relé, výstupy otevřených kolektorů tranzistorů apod.). Nejdokonalejší systémy umožňují oboustrannou komunikaci, a tím také možnost monitorování stavu přenosové trasy.

Použité formáty přenosu po JTS jsou normalizovány. V závislosti na použitém vyhodnocovacím zařízení (PCO) je zvolen správný formát přenosu tak, aby si ústředna EZS s monitorovacím pultem „rozuměla“. Rovněž u bezdrátových systémů používají výrobci standardizované formáty.

### **Použitá literatura:**

1. Rehborn, K.: Praxis der Alarmanlagen. München, Karamanolis Verlag 1985
2. Siemens, E.: Handbuch Sicherungstechnik. Heidelberg, Kriminalistik Verlag 1993
3. Toms, L., Koniček, T., Kocábek, P.: Zabezpečení dveří a oken. Praha, THEMIS, 1997
4. Skřivan Z. a kol.: Nebojte se zlodějů, Praha, GRADA, 1994
5. Lošťáková, A.: Technická zařízení na ochranu osob a majetku, Ústí nad Labem, ISS a COP, 1994
6. ČSN EN 50 131-1 Poplachové systémy – Elektrické zabezpečovací systémy – Všeobecné požadavky
7. ČSN EN 50 131-6 Poplachové systémy – Elektrické zabezpečovací systémy – Část 6: Napájecí zdroje
8. ČSN EN 50 131-1/Z1 Poplachové systémy – Elektrické zabezpečovací systémy – Všeobecné požadavky – Změna Z1
9. prEN 50131-7 Poplachové systémy – Elektrické zabezpečovací systémy – Pokyny pro aplikaci

# **Elektrická požární signalizace – EPS**

*Petr Sloup, Rostislav Srstka*

## **OBSAH:**

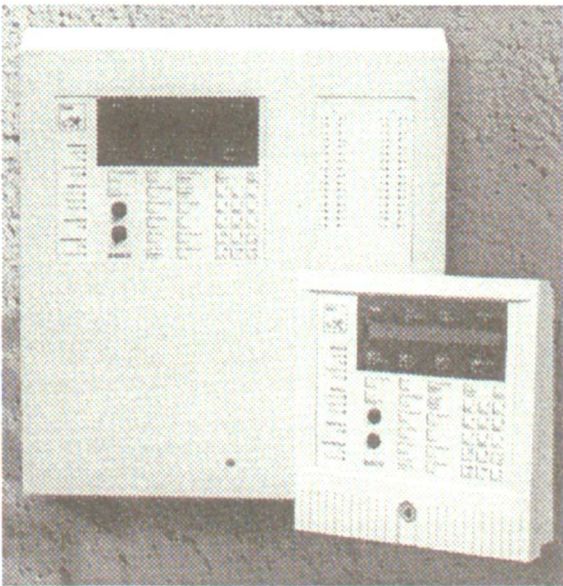
<b>1 Elektrická požární signalizace</b> .....	129
<b>2 Nejdůležitější normy zabývající se problematikou EPS</b> .....	129
<b>3 Blokové schéma systému elektrické požární signalizace</b> .....	129
<b>5 Požární hlásiče</b> .....	130
5.1 Manuální - tlačítkové .....	130
5.2 Požární hlásiče automatické ( <b>samočinné</b> ) .....	<b>131</b>
<b>6 Ústředny elektrické požární signalizace</b> .....	137
6.1 Ústředny EPS konvenční neadresné .....	137
6.2 Ústředny EPS konvenční adresné .....	138
6.3 Analogové ústředny EPS .....	138
6.4 Ústředny EPS Interaktivní .....	138
<b>7 Požární poplachová zařízení</b> .....	138
7.1 Akustická poplachová zařízení .....	138
7.2 Optická poplachová zařízení .....	139
7.3 Vstupní/výstupní jednotky .....	139
<b>8 Zařízení pro dálkový přenos požárního poplachu (ZDP)</b> .....	140
<b>9 Samočinná zařízení požární ochrany</b> .....	140
9.1 Přidržené magnety .....	141
<b>10 Obslužné pole požární ochrany (OPPO)</b> .....	141
<b>11 Klíčový trezor požární ochrany (KTPO)</b> .....	142
<b>12 Zřizování systémů elektrické požární signalizace (EPS)</b> .....	144
12.1 Etapa I. – zadání zakázky .....	144
12.2 Etapa II. – návrh .....	145
12.3 Etapa III. – přezkoumání návrhu a příprava realizace .....	150
12.4 Etapa IV. – realizace (montáž) .....	152
12.5 Etapa V. – provoz .....	158





## 1 Elektrická požární signalizace

Elektrická požární signalizace je soubor technických zařízení, skládajících se z ústředny EPS, hlásičů požáru a doplňujících zařízení. Tato zařízení tvoří systém, jehož úkolem je zaznamenávat a vyhodnocovat požár, již při jeho vzniku a požár signalizuje opticky i akusticky na ústředně EPS. Signalizace bývá v místě stálé služby, která může na signalizaci zareagovat. Je např. schopná začínající požár zlikvidovat nebo přivolat další pomoc, (např. jednotky HZS). Mezi hlavní úkoly elektrické požární signalizace (zkratka EPS) patří rychlé a spolehlivé určení místa požáru již v samém počátku zahoření, vyhlášení poplachu, aktivace a řízení evakuačního systému v zasažených oblastech a v neposlední řadě je to ovládání a signalizace stavu dalších požárně bezpečnostních zařízení. V některých případech také realizuje automatickou komunikaci s hasičským záchranným sborem prostřednictvím zařízení dálkového přenosu (ZDP). Elektrická požární signalizace tvoří základní součást systémů požárně bezpečnostních zařízení. Její význam ve většině případů převyšuje ostatní zabezpečovací systémy, jak z hlediska hodnot chráněného majetku, také její základní, nenahraditelnou úlohou ochrany života a zdraví osob. Při odborné instalaci tak včasnou informací přispívá EPS k minimalizaci škod vzniklých požárem.



Obr. 4-1: Ústředna a klávesnice EPS (Bosch Telecom).

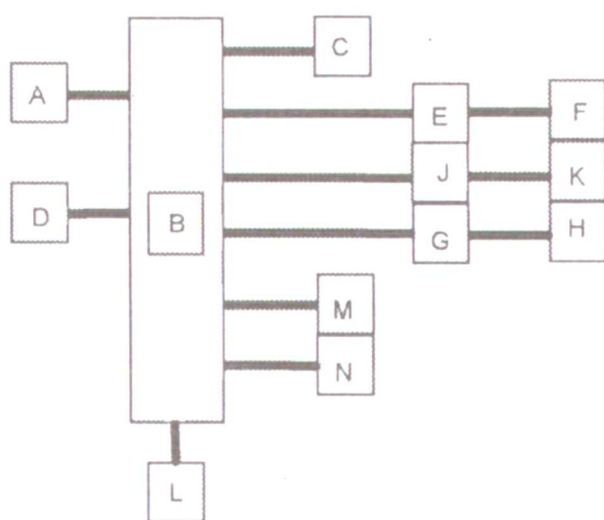
## 2 Nejdůležitější normy zabývající se problematikou EPS

Přehled norem na EPS je uveden v kapitole 1.

## 3 Blokové schéma systému elektrické požární signalizace

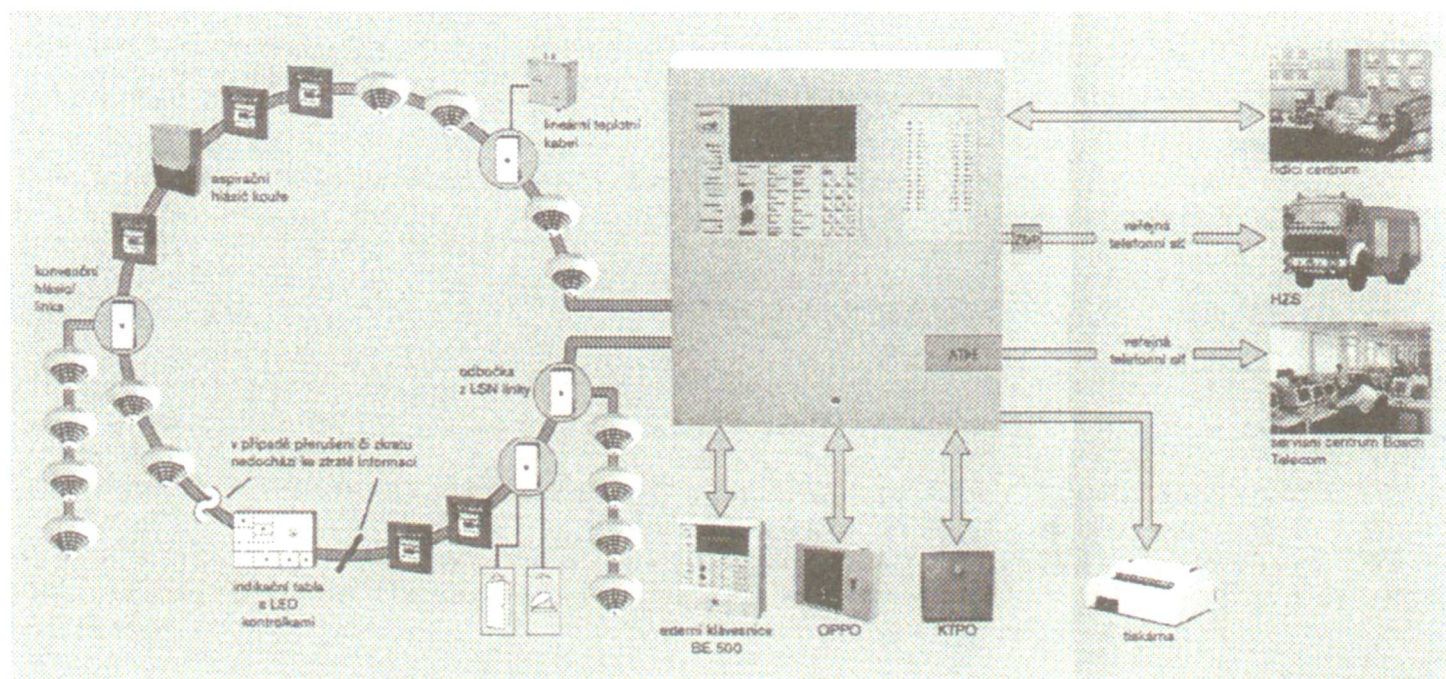
Spojnice propojující různé komponenty zobrazují tok informací, nikoli fyzické propojení.

- A Hlásiče požáru
- B Ústředna EPS
- C Požární poplachové zařízení
- D Hlásiče tlačítkové
- E Zařízení přenosu poplachu



- F Ohlašovna požáru
  - G Řídicí jednotka samočinného zařízení
  - H Samočinné zařízení požární ochrany
  - J Zařízení přenosu poruchových stavů
  - K Přijímací místo hlášení poruchových stavů
  - L Napájecí zařízení
  - M Obslužné pole požární ochrany
  - N Klíčový trezor požární ochrany
- Bloky G a H mohou mít samostatný napájecí zdroj.

Obr. 4-2: Blokové schéma systému EPS.



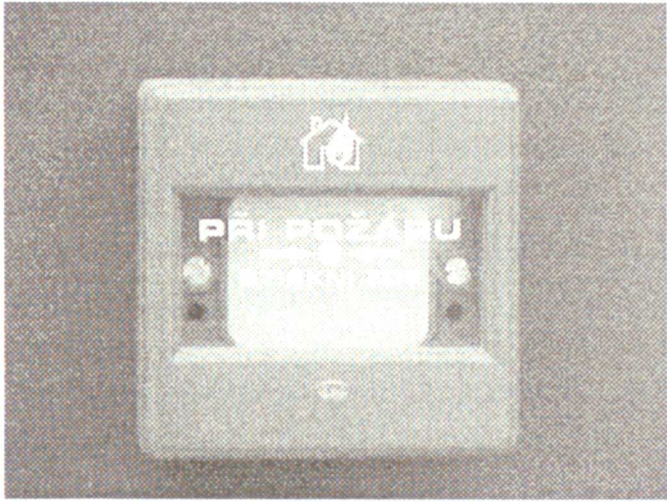
Obr. 4-3: Systém EPS (Bosch Telecom).

## 5 Požární hlásiče

### 5.1 Manuální - tlačítkové

Slouží k vyhlášení poplachu osobou, která zjistí požár, nebo jiný nebezpečný jev. Tlačítkové požární hlásiče jsou **vždy** červené barvy. Obsahují mikrospínač a zakončovací rezistor, nebo elektroniku, v závislosti na tom, zda se jedná o tlačítkový hlásič určený do systému neadresného, nebo do systému s adresací hlásičů. Tlačítkové hlásiče musí být uzpůsobeny tak, aby nemohlo dojít k samovolné, nebo náhodné aktivaci. Musí být možné zjistit, který hlásič poplach vyhlásil. Často je toto řešeno tím, že k aktivaci hlásiče je zapotřebí rozbít sklíčko. To je naříznuté a překryté průhlednou fólií, aby nedošlo k poranění o střepey . Dále musí být také možné provést test správné funkce tlačítkového hlásiče, aniž by bylo nutné sklíčko rozbít. K tomuto účelu slouží speciální přípravek. Tlačítkové hlásiče se instalují především na únikových cestách a u výstupů z těchto cest do volného prostoru a dále nejčastěji do míst se stálou obsluhou ( vrátnice, strojovny,

atd.), nebo do míst pohybu osob ( dílny, chodby, atd.), ale také tam, kde nelze použít jiné hlásiče, nebo, tam, kde je použití jiných hlásičů málo účinné. U systémů EPS kde lze volit takzvané zpoždění reakce na poplachový signál od hlásiče (ověřování), se tlačítkové hlásiče definují tak, aby vyvolaly poplach okamžitě bez jakéhokoli zpoždění.



Obr. 4-4: Tlačítkový hlásič (Kac).



Obr. 4-5: Tlačítkový hlásič (Bosch).

## 5.2 Požární hlásiče automatické (samočinné)

Jsou to zařízení, která monitorují určitý fyzikální nebo chemický jev, reagují na něj a informaci předávají prostřednictvím vedení do požární ústředny. Tyto hlásiče reagují na průvodní jevy požáru jako je kouř, nárůst teploty, plameny nebo jejich kombinace. Umístění hlásičů se řídí odpovídajícími normami, předpisy výrobce hlásiče a pokyny pro projekci a montáž. Typ hlásiče musí odpovídat předpokládanému druhu a rychlosti šíření požáru. Nejvíce jsou používány takzvané BODOVÉ HLÁSIČE. Ty se nejčastěji montují na strop, nebo do určité vzdálenosti pod něj. Vlastní hlásič je zpravidla instalován do patice. Ta je trvale připevněna ke stropu, či držáku a pomocí vodičů je propojena s ústřednou EPS. Hlásič je do patice upevněn pomocí bajonetového uzávěru. Typ použitého hlásiče v daném prostoru závisí na proudění vzduchu, potencionálních příčinách vzniku požáru, na teplotách a na přítomnosti vlivů, které mohou u jednotlivých typů detektorů způsobovat plané poplachy. Plocha pokrytí hlásičem je omezená. Ve větších místnostech je proto zapotřebí použít hlásičů více tak, aby pokrytí prostoru odpovídalo stanoveným požadavkům.

Principy funkce automatických požárních hlásičů:

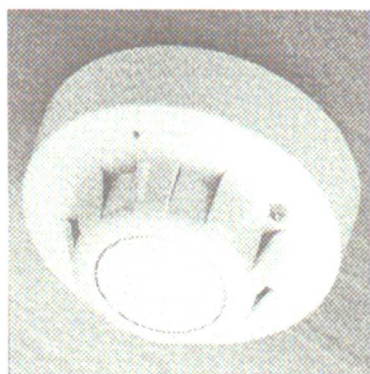
- hlásiče ionizační,
- hlásiče optické,
- hlásiče teplotní,
- hlásiče tlakové,
- hlásiče odporové a
- hlásiče kombinované (multisenzorové).

### 5.2.1 Hlásiče teplotní

Každý oheň způsobuje zvýšení okolní teploty. Tohoto jevu můžeme využít při identifikaci požáru pomocí teplotních požárních detektorů. Ty pracují na tom principu, že v při-

padě překročení určité teploty předají odpovídající elektrický signál ústředně EPS a ta vyhlásí poplach. Tento druh se nazývá STATICKÝ.

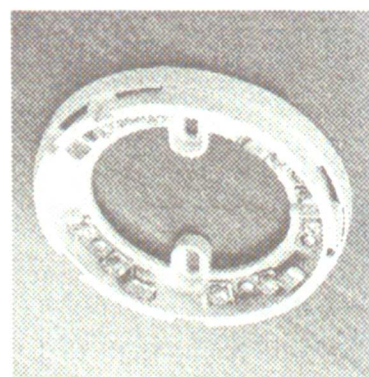
Vyrábí se pro různé teploty např. 60°C, 75°C, 90°C, 100°C atd. Nevýhodou je, že pokud je prahová teplota nízká, dochází často k falešným poplachům, a to tehdy, jestliže teplota vzroste z jiných důvodů než je požár. Pokud je naopak prahová teplota zvolena příliš vysoko, dochází k vyhlášení poplachu pozdě, až když už je požár příliš velký. Lepších výsledků lze dosáhnout pomocí DIFERENCIÁLNÍCH hlásičů teplot. Tyto hlásiče nereagují na konkrétní teplotu, ale na RYCHLOST ZMĚNY TEPLITY. Hlásič obsahuje dva stejné termistory. Jeden z nich je na povrchu hlásiče přímo vystavený okolní teplotě, druhý je zalitý v ochranném krytu uvnitř hlásiče. Pokud začne v blízkosti hlásiče vzrůstat teplota, zaregistruje tuto změnu jako první vnější termistor. Vnitřní termistor díky tepelné setrvačnosti zaregistruje tuto změnu s určitým zpožděním. Tím dojde k nerovnováze průchodu elektrického proudu termistory. Pokud nerovnováha překročí určitou mez, hlásič vyhlásí poplach. Nejlepší vlastností z hlediska toho, aby nedocházelo k planým poplachům, ale aby byl případný požár identifikován včas, mají TEPLITNÍ HLÁSIČE KOMBINOVANÉ, které využívají principu jak statického tak diferenciálního hlásiče. To znamená, že k vyhlášení poplachu dojde když teplota přesáhne prahovou hodnotu, ale i tehdy, když nastane rychlý nárůst teploty v okolí hlásiče.



Obr. 4-6: Ionizační hlásič (Apollo).



Obr. 4-7: Teplotní hlásič (Apollo).



Obr. 4-8: Patice (Apollo).

### 5.2.2 Ionizační hlásiče kouře

Při vzniku požáru se do ovzduší uvolňují plyny a kouř na bázi uhlíku. Tohoto jevu lze využít při identifikaci požáru v ionizačním požárním hlásiči. Ionizační hlásiče ke své funkci využívají dvě komory - otevřenou vnější komoru a vnitřní polouzavřenou referenční komoru. V komoře se nachází fólie s malým množstvím radioaktivního americia 241, touto fólií prochází elektrický proud. Jakmile do komory hlásiče vnikne kouř dojde ke změně proudu ve vnější komoře a následkem toho vzroste napětí mezi vnější a vnitřní komorou.

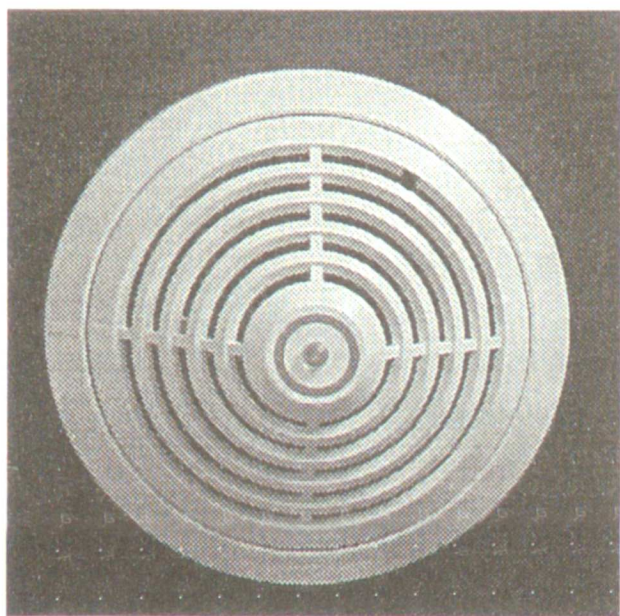
Elektronika hlásiče porovnává rozdílové napětí mezi komorami a při překročení určité hodnoty reaguje předáním poplachové informace. Hlásič je schopný reagovat na poměrně malé koncentrace ionizovaných částic ve vzduchu, proto jsou tyto hlásiče dosti citlivé. Ionizační detektory jsou citlivé i na takové kouře, které jsou lidským okem neviditelné. Reagují velice rychle. To je výhodné tehdy, když začnou hořet snadno vznětlivé materiály, které vyvíjí pouze malé množství viditelného kouře. K aktivaci těchto hlásičů však někdy dochází i v jiných případech než při vzniku požáru. Díky své citlivosti mohou být aktivovány například výpary a plyny které běžně vznikají při přípravě jídel v kuchyních.

Rizikovým faktorem pro vznik falešného poplachu v některých případech může být také změna atmosférického tlaku, vlhkosti a teploty.

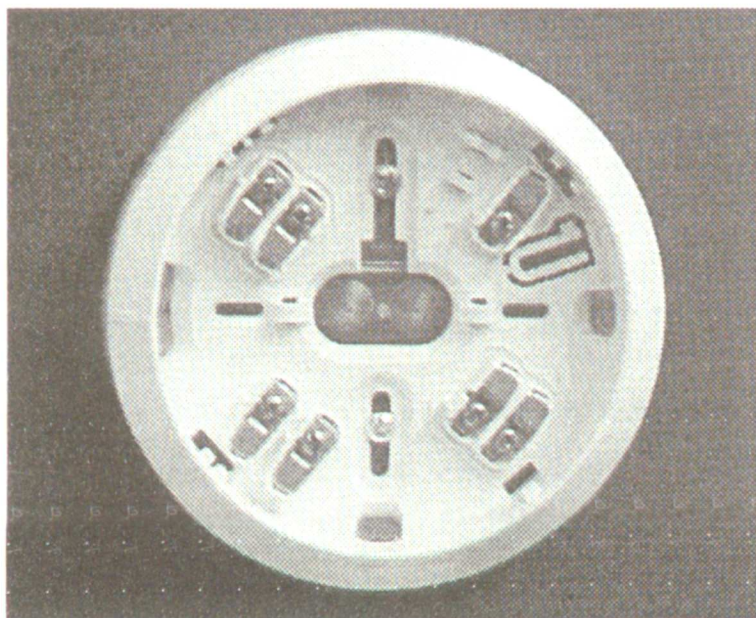
Hlavní výhodou těchto hlásičů je relativně jednoduchá výroba a nízká cena. Naopak nevýhoda spočívá v přítomnosti radioaktivního materiálu a s tím spojené problémy se skladováním, evidencí a likvidací těchto detektorů. Proto velká část výrobců od výroby detektorů pracujících na tomto principu ustupuje.

### 5.2.3 Optické hlásiče kouře

Tyto hlásiče využívají ke své činnosti optickou vazbu mezi pulzující infra LED diodou a fotodiodou. Ty jsou umístěny proti sobě v komoře, do níž nemůže vniknout světlo z žádného cizího zdroje. Do této komory však může proniknout kouř. Částice kouře způsobí zeslabení intenzity infra paprsku vyzařovaného LED diodou, tuto změnu zaregistruje fotodioda. V případě, že fotodioda zaznamená kouř u dvou po sobě jdoucích pulsů, zareaguje hlásič předáním poplachové informace. V současné době se však častěji setkáme s hlásiči u nichž infra paprsek emitovaný LED diodou nedopadá na fotodiodu přímo. Pouze pokud do komůrky vnikne kouř, paprsek se od jeho částic odrazí a dopadne na fotodiodu, v té době ke zvýšení procházejícího proudu. Tato elektrická informace je dále zpracována elektronickými obvody detektoru, vyhodnocena a předána ústředně EPS jako poplachová informace. Bodové optické hlásiče jsou v současné době nejpoužívanější (až 95% aplikací). Rizikovým faktorem pro tento druh hlásičů je přítomnost různých výparů a tvorba orosení.



Obr. 4-9: Optický hlásič (Bosch Telecom).



Obr. 4-10: Patice (Bosch Telecom).

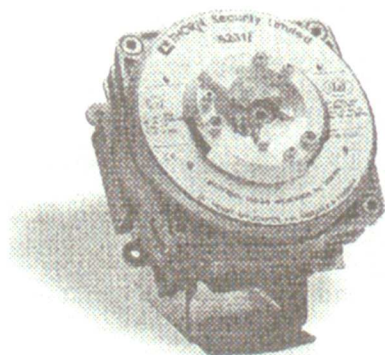
### 5.2.4 Hlásiče multisenzorové s využitím plynové detekce (CO)

Kombinují optický, teplotní a chemický senzor s inteligentní vyhodnocovací elektronikou a stanovují tak zcela novou úroveň technologie detekce požárů. Jedná se o nejnovější generaci mezi bodovými hlásiči požáru. Tyto hlásiče nabízejí mimořádnou odolnost vůči falešným poplachům. Použití chemického senzoru plynů, vznikajících při hoření, přináší klíčovou výhodu před „klasickou“ multisenzorovou technologií. Dříve byly k detekci požáru používány v jednom hlásiči současně nejvýše dva způsoby detekce (charakteristické produkty hoření) – teplo a kouř. V těchto chemosenzorických hlásičích je počet charakteristik, podle nichž se rozhoduje, zda spustit poplach, rozšířen na tři. Rozšiřuje

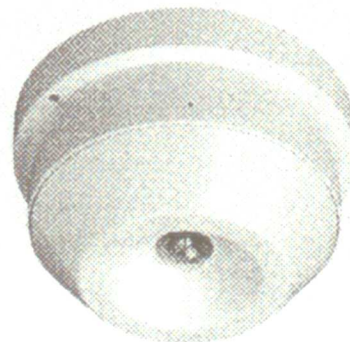
se tak oblast citlivosti pro detekci požáru, snižuje se počet falešných poplachů, spotřeba proudu je velmi nízká. Rychlá detekce a vysoká přesnost činí bez nadsázky tyto chemosenzorické hlásiče nejlepším požárně-detekčním systémem současnosti.

### 5.2.5 Optické hlásiče plamene

Tyto hlásiče pracují na principu identifikace ultra fialového a (nebo) infra červeného záření, které vydává plamen. Tento druh požárních hlásičů se montuje buďto na strop nebo na stěnu. Při montáži těchto hlásičů je nutné aby z místa, kde je hlásič namontován, byla přímá viditelnost na místa, kde lze předpokládat výskyt plamene. Plamenné hlásiče se využívají spíše jako doplňková ochrana v prostorách monitorovaných optickými, ionizačními, nebo teplotními hlásiči. Jejich hlavní nasazení je však hlídání velkých venkovních nádrží a stáječích míst hořavých kapalin a plynů a letištních hangárů.



Obr. 4-11: Hlásič plamene IR (Thorn).



Obr. 4-11: Hlásič plamene UV (Hochiki).

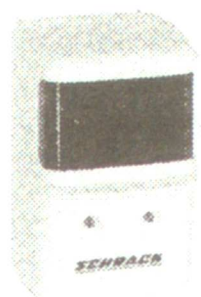
### 5.2.6 Lineární optický hlásič

Jedná se o samočinný hlásič, který slouží k indikaci vznikajícího požáru na principu zeslabení intenzity infračerveného paprsku částicemi kouře.

Nejčastěji se tyto hlásiče využívají v různých halách a rozsáhlých prostorách. Hlásič se instaluje pod strop do míst předpokládaného výskytu a soustředění kouře. Lineární hlásič kouře je tvořen vysílačem a přijímačem (popřípadě samostatnou vyhodnocovací jednotkou). Vysílač a přijímač může být instalován, buď proti sobě na stabilní plochy chráněného prostoru. V tomto případě může být mezi vysílačem a přijímačem až 100 metrová vzdálenost s šířkou monitorovaného prostoru až kolem 7,5m na každou stranu od osy. Nebo v takzvaném RETRO režimu, kdy je vysílač i přijímač vedle sebe a na protilehlé straně monitorovaného prostoru je upevněn odrazový hranol. Rizikovým faktorem pro lineární hlásiče je změna vzájemné polohy vysílače a přijímače, nebo odrazového hranolu. K této změně může například dojít vlivem tepelné roztažnosti konstrukce. Dále pak je nutné dbát aby nebyl paprsek přerušen nějakým předmětem (něco v cestě).

### 5.2.7 Lineární tepelný detektor - teplotní kabel

Lineární teplotní kabel se skládá z vlastního teplocitlivého kabelu a z vyhodnocovací jednotky, popřípadě kabelu, který je mezi teplotním kabelem a vyhodnocovací jednotkou. Vlastní detekci provádí speciální teplocitlivý dvou vodičový kabel zakončený vyvažovacím rezistorem. Vodiče kabelu jsou z pružného odporového materiálu a jsou vzájemně zkroucené a izolovány speciální izolací. Ta při určité teplotě změkne a vodiče se v daném místě



Obr. 4-13: Lineární hlásič (Schrack).



Obr. 4-14: Lineární hlásič (Fireray).

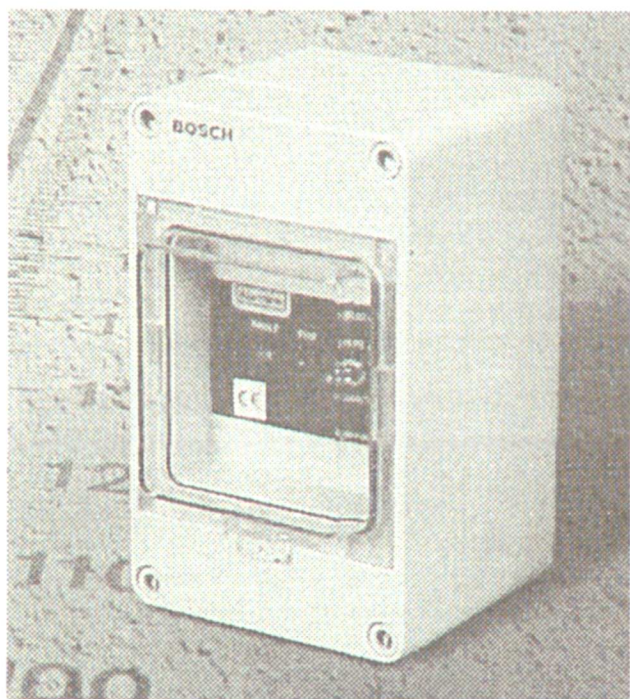


Obr. 4-15: Lineární hlásič EEXD (Fireray).



Obr. 4-16: Lineární hlásič (Fireray).

díky zkroucení dotknou a zkratují. Tím se změní celkový odpor tohoto kabelu (čím blíže od vyhodnocovací jednotky dojde k vyzkratování, tím je odpor kabelu nižší), vyhodnocovací jednotka podle naměřeného odporu určí v kterém místě došlo k překročení teploty. Kabely jsou vyráběny pro různé teploty např. 68 °C, 87 °C, 137 °C atd. a jsou dle teploty barevně rozlišeny. Poškozený teplotní kabel lze vystříhnout a nasvorkovat. Po nasvorkování je nutné kabel zkalibrovat. Jiný způsob detekce je teplocitlivým kabelem s vodiči ze speciální slitiny reagující velkou změnou odporu v závislosti na změně teploty. Další způsob detekce je speciálním kabelem s optickými vlákny spirálově stočenými kolem měkké duše (voskové), změnou teploty dochází k narušení duše kabelu a tím ke změně intenzity procházejícího laserového paprsku. Tyto dva typy teplocitlivých kabelů jsou dražší, ale jejich funkce je vratná pokud teplota nepřekročí cca 260 °C, kdy nastává trvalé poškození a kabel musí být vyměněn.

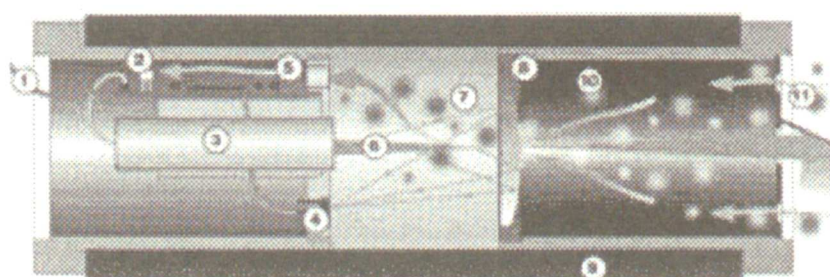


Obr. 4-17: Řídící jednotka teplotního kabelu (Bosch Telecom).

Lineární teplotní kabel je určený jako hlásič EPS především do průmyslových prostředí a aplikací. Například kabelové kanály, kolektory, elektrické rozvaděče, ale i detekce požáru v nádržích na hořlaviny, ochrana mrazíren, leteckých hangárů, v dolech a vysoce prašných prostředích, ve venkovních a výbušných prostředích. Lze jej úspěšně použít také k signalizaci přehřátí určitých zařízení, kabelů, ale i mechanických částí jako např. ložisek u pásových dopravníků na uhlí atd.. Tak lze mnohdy zamezit požáru dříve, než vůbec vznikne.

### 5.2.8 Aspirační (nasávací) požární hlásiče

V objektech nebo místech, kde jsou vyžadovány vysoce citlivé hlásiče, je vhodné namísto mnoha levnějších a relativně málo citlivých hlásičů použít aspirační hlásič kouře. Tento hlásič signalizuje požár již v nejrannějším stádiu a tím minimalizuje následky požáru. Skládají se z vyhodnocovací jednotky s vestavěným ventilátorem nebo kompresorem a z jednoho či více nasávacích potrubí s otvory. Nasávání vzduchu pomocí sacích trubek do vyhodnocovací jednotky je účinnější způsob sbírání kouře než způsob, jakým se dostane kouř do komory bodového hlásiče. Navíc sací dírky se dají mnohem snáze umístit na strategická místa, například do míst předpokládaného vrstvení kouře. Jestliže se v nasávaném vzduchu nacházejí kouřové částice, je po dosažení reakční hodnoty vyvolán požární poplach. Vlastní snímání vzorků vzduchu se provádí na optickém principu. Zjišťuje se množství rozptýleného světla ve vzduchu procházejícím optickou komorou. Rozptyl světla je úměrný množství částic obsažených ve vzorku vzduchu v komoře. Jako zdroj světla může sloužit XENONOVÁ výbojka, POLOVODIČOVÝ LASER nebo LED dioda. Nasávací systém je zvláště vhodný pro použití v historických objektech, kostelech, muzeích, ve věžeňských celách, v prostorách s dřevěnými stropy, či konstrukcemi atd.



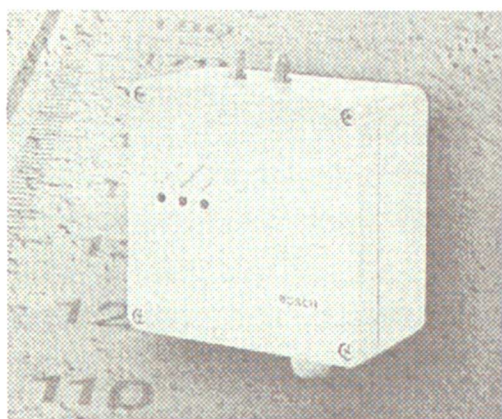
Obr. 4-18: Princip funkce laserové detekční komory.

- |                                      |                          |
|--------------------------------------|--------------------------|
| 1. Kabel k řídicí jednotce           | 7. Rozptýlené paprsky    |
| 2. Snímač rychlosti proudění vzduchu | 8. polopropustné zrcadlo |
| 3. Laser                             | 9. Kryt hlásiče          |
| 4. Přijímač odražených paprsků       | 10. Kouřové částice      |
| 5. Proud vzduchu                     | 11. Děrovaný kotouč      |
| 6. Laserový paprsek                  |                          |

### 5.2.9 Hlásiče tlakové

Tlakové hlásiče se skládají z vyhodnocovací jednotky a snímací trubice. Kompresor uvnitř vyhodnocovací jednotky vytváří v pravidelných intervalech přesně definovaný přetlak v snímací trubici. Poplach je vyvolán na základě změny tlaku vzduchu ve snímací trubici, způsobeným zvýšením okolní teploty. Vlastnosti systému lze programově přizpůsobit požadavkům, daným vlastnostmi prostoru, ve kterém je systém nasazen. Změny tlaku vyvolané například poškozením snímací trubice jsou signalizovány jako porucha. Použití těchto hlásičů je velice často jako ochrana konkrétních zařízení (např. elektrické rozvaděče), nebo tam, kde klasické bodové požární hlásiče nelze z nejrůznějších důvodů použít. Výhodou tohoto hlásiče je, že jeho detekční trubice lze umístit téměř kamkoli. Kromě teploty není téměř ničím negativně ovlivňován, to znamená, že v jeho detekční části mu nevadí vlhko, prach, hmyz a další faktory, které u klasických bodových hlásičů vyvolávají plané poplachy.





Obr. 4-19: Tlakový hlásič (Bosch Telecom).

## 6 Ústředny elektrické požární signalizace

Ústředna EPS je zařízení, které soustřeďuje informace ze všech hlásičů k systému připojených (jak automatických tak tlačítkových). Informace z nich dle nastavení zpracovává a reaguje na ně odpovídající odezvou (vyhlášení poplachu, signalizace poruchy, přenos signálu na PCO, aktivace samočinných hasících zařízení, uzavření požárních dveří atd.).

Ústředna umožňuje programování, ovládání a diagnostiku systému. Dále zprostředkovává napájení celého systému EPS. Ústředny EPS jsou rozděleny podle komunikace s hlásiči a podle jejich vzájemného propojení, na ústředny KONVENČNÍ NEADRESNÉ, KONVENČNÍ ADRESNÉ, ANALOGOVÉ a INTERAKTIVNÍ stejně jako systémy EPS. Různé ústředny se dále liší podle počtu smyček. Tím je určeno kolik hlásičů lze k dané ústředně připojit a pro jak rozsáhlé aplikace je ústředna použitelná.

### 6.1 Ústředny EPS konvenční neadresné

U konvenčních ústředn jsou hlásiče připojeny k ústředně proudově vyváženou hlásicí linkou (smyčkou). Pokud je na smyčce více jak jeden hlásič, při vyhlášení poplachu nelze z ústředny zjistit, který konkrétní hlásič jej způsobil. Na jedné hlásicí lince může být zapojeno bez možnosti jejich rozlišení až 20 (32) hlásičů. Mohou být odlišné konstrukce a typu (ionizační, optické...).



Obr. 4-20: Centralizovaný / decentralizovaný analogový adresovatelný systém EPS „Delta“ (ELTEK).

U některých konvenčních systémů nelze kombinovat na jedné hlásicí lince automatické a manuální hlásiče. Poplach v systému je aktivován hlásičem díky změně jeho impedance (impedance se sníží). Hlásiče mají pouze dva stavy (klid - poplach). Parametry jsou nastaveny z výroby a nelze je měnit.

### **6.2 Ústředny EPS konvenční adresné**

V aplikacích s konvenčními adresnými ústřednami mají jednotlivé hlásiče konkrétní adresu, díky tomu lze na ústředně zjistit který hlásič vyvolal poplach. K vyhodnocování poplachu dochází v ústředně EPS. Hlásiče mají pouze dva stavy ( klid - poplach ), jejich parametry jsou nastaveny z výroby a zpravidla je nelze měnit. Na jedné smyčce lze kombinovat různé typy automatických i tlačítkových hlásičů. Často se využívají tzv. kruhové smyčky s oddělovacími izolátory. Ty se instalují do kruhové smyčky vždy po určitém počtu hlásičů. V případě poruchy hlásiče, nebo poškození vedení, izolátory automaticky vyřadí vadnou část systému mezi dvěma izolátory a zbylá část systému funguje dále.

### **6.3 Analogové ústředny EPS**

V systémech s analogovou ústřednou a hlásiči, hlásiče monitorují prostor v němž jsou nainstalovány a předávají analogové (více stavové) údaje ústředně. Ta na základě dodaných informací, podle určitých algoritmů, rozhodne o tom zda se jedná o normální stav, poruchu, nebo takzvaný předpoplach či poplach. Každý hlásič v tomto systému má svoji adresu. Díky tomu lze na ústředně zjistit z kterého hlásiče přišla informace. Tyto systémy jsou schopné v určitém rozsahu kompenzovat změny způsobené např. zaprášením detektorů. K propojení hlásičů s ústřednou se nejčastěji využívá kruhové sběrnice. Díky velkému objemu dat přenášených do ústředny tyto systémy kladou vyšší nároky na kvalitu kabeláže.

### **6.4 Ústředny EPS Interaktivní**

V systémech s těmito ústřednami se využívají takzvané interaktivní hlásiče. Interaktivní hlásič rozlišuje úroveň jednotlivých signálů ze svého okolí a jejich změnu v čase. Každý hlásič obsahuje mikroprocesor který podle určitého algoritmu zpracovává a vyhodnocuje informace ze svého okolí. Detektor poté vytváří definovaný elektrický signál, který odpovídá určité požární situaci (klid, předpoplach, poplach). Ten je předáván ústředně EPS. Jednotlivé hlásiče jsou adresné, takže na ústředně je zobrazeno který hlásič danou situaci vyvolal.

Mezi přednosti interaktivních systémů patří především to, že v porovnání s klasickým analogovým systémem jsou mnohem méně zatěžovány přenosové cesty mezi hlásiči a ústřednou. Díky tomu jsou tyto systémy výrazně odolnější vůči negativním jevům jako je například elektromagnetická indukce způsobená souběhem vedení kabeláže atd..

## **7 Požární poplachová zařízení**

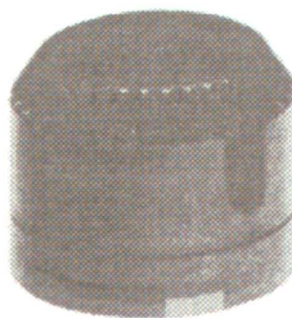
Jsou to takové komponenty nebo jejich soubory, které přijímají elektrický poplachový signál z ústředny EPS a převedou jej do vhodné formy tak, aby byla poplachová informace srozumitelná osobám, jimž je určena. Vhodnou formou rozumíme AKUSTICKOU a (nebo) OPTICKOU podobu.

### **7.1 Akustická poplachová zařízení**

Mezi akustická poplachová signalizační zařízení patří vzdálená signalizační tabla ústředně různé typy sirén, akustických piezo-měničů, bzučáků a také různé druhy požárních zvonů.



Obr. 4-21: Siréna  
(Fulleon).



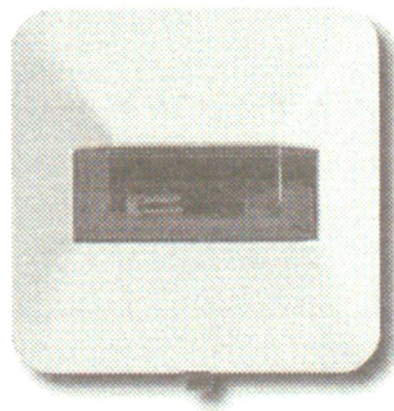
Obr. 4-22: Maják  
(Fulleon).

## 7.2 Optická poplachová zařízení

Mezi optická poplachová zařízení patří různé druhy majáků, jak žárovkových i výboj-  
kových, různé typy signálek a kontrolky, ale i displeje.



Obr. 4-23: Požární zvonek (Fulleon).



Obr. 4-24: Optická signalizace.

## 7.3 Vstupní/výstupní jednotky

Nedílnou součástí systémů EPS jsou také vstupní a výstupní jednotky. Mohou být  
součástí ústředny EPS (malé systémy), nebo mohou být v provedení adresných jedno-  
tek, umístěných na hlásicích linkách.

**Výstupní jednotky** slouží například k ovládání signalizačních zařízení a dále k ovlá-  
dání jiných požárně bezpečnostních zařízení. Jejich součinnost je dána požadavky po-  
žárně bezpečnostního řešení. Jsou to například:

- ovládání ZOKT – zařízení pro odtažení kouře a tepla,
- vypnutí ventilace a vzduchotechniky,
- uzavření průchodů mezi požárními úseky (přidržené magnety),
- otevření dveří na únikových cestách,
- ovládání evakuačního rozhlasu
- vypnutí plynu,
- vypnutí přívodu el. energie,
- uzavření požárních klapek a
- spuštění SHZ (stabilní hasící zařízení).

**Vstupní jednotky** slouží k signalizaci stavu ovládaných zařízení a stavu prvků, kte-  
ré jsou z požárně bezpečnostního hlediska důležité, ale nemají například dálkové ovlá-  
dání:

- stav větracích klapek,
- stav funkce SHZ,
- stav požárních klapek,
- stav požárních předělů (dveří).

*Poznámka - Funkci vstupních a výstupních jednotek může zahrnovat také rozhraní pro připojení na PC. V případě vazby EPS na počítač ( monitorovací software nebo PULT CENTRALIZOVANÉ OCHRANY) poslouží jako optické signální zařízením monitor počítače.*

### **8 Zařízení pro dálkový přenos požárního poplachu (ZDP)**

Jedná se o zařízení, které zprostředkuje přenos poplachového signálu z ústředny elektrické požární signalizace do ohlašovny požáru. Přenos může být buď místní, nebo dálkový. Systém elektrické požární signalizace má význam pouze tehdy, když na případnou poplachovou informaci někdo v krátkém čase odpovídajícím způsobem zareaguje. Toho lze dosáhnout tím, že bude v místě stálá obsluha, která v případě požárního poplachu učiní patřičné kroky. V tomto případě se jedná o požární systém s místní signalizací. V případě místního přenosu se využívá pro přenos informací mezi ústřednou a místem signalizace nejčastěji kabelů s metalickým vedením nebo kabelů s optickými vlákny.

Pokud v objektu monitorovaném systémem EPS není stálá obsluha, využívá se dálkového přenosu na pulty centralizované ochrany u hasičských záchranných sborů. Zde je možné došlé informace z jednotlivých ústředn EPS vyhodnotit a poté organizovat účinný zákrok. Zařízení se skládá z účastnického dílu umožňujícího připojení ústředny EPS k zařízení dálkového přenosu (zkratka ZDP), přenosové cesty a vyhodnocovací části, kterou je pult centralizované ochrany. Jako přenosová cesta se využívá přenos informací v nadhovorovém pásmu po telefonním vedení, přenos po samostatném kabelu nebo přenos radiový. Pokud je použit samostatný kabel může být buď s metalickým vedením, nebo s optickými vlákny. V případě využití dálkového přenosu na požární pult centralizované ochrany je požadavek, aby spojení mezi jednotlivými ústřednami a pultem bylo stálé, nebo aby byla splněna podmínka že nejméně každé tři minuty musí na pult přijít informace o stavu každé ústředny k pultu připojené.

Základní požadavky na ZDP a jeho funkci ve vazbě na EPS jsou stanoveny v ČSN 34 2710 „Předpisy pro zařízení elektrické požární signalizace“ kap. F., čl.210 – 214, ČSN 73 0875 „Navrhování elektrické požární signalizace“, čl. 73 a Sbírce pokynů ředitelství Hasičského záchranného sboru ČR „Zařízení dálkového přenosu informací ve vazbě na elektrickou požární signalizaci“. Systém EPS (ústředna EPS) je nepřetržitě - 24 h denně připojena prostřednictvím ZDP na pult PCO dispečinku HZS. Toto zařízení vždy pracuje spolu s OPPO a KTPO.

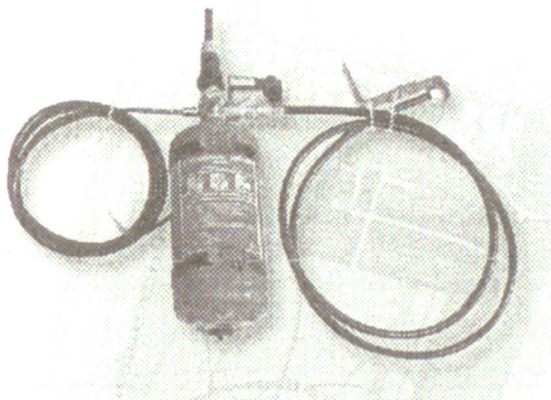
### **9 Samočinná zařízení požární ochrany**

Jedná se o samočinný řídicí systém nebo požárně technické **bezpečnostní** zařízení.

Patří sem především nejrůznější typy **SHZ (stabilní hasící zařízení)** - automatických hasících zařízení, jak těch které využívají jako hasivo vodu **či inertní plyn**, tak využívajících různé druhy dálkově ovládaných hasících přístrojů. Dále různé druhy požárních

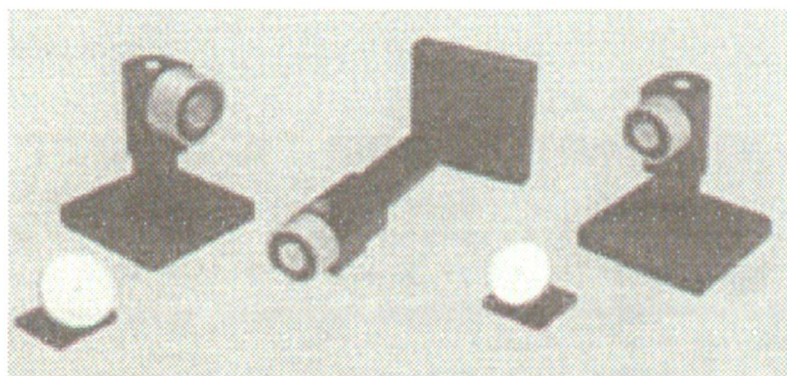
uzávěr jako jsou požární rolety, vrata, samočinně se uzavírající požární dveře. Elektromechanické zámky umožňující odjištění dveří v případě potřeby evakuace z hořícího objektu a tak dále. Patří sem také technika zajišťující odvětrávání kouře **a tepla** při případném požáru, dále pak zařízení, které zajistí, že v případě požáru automaticky výtahy sjedou do přízemí a mnoho dalších přístrojů a zařízení umožňujících realizovat nejrůznější funkce a činnosti důležité při minimalizaci nebezpečí a škod v případě vzniku požáru.

Obr. 4-24: Systém dálkově ovládaného hasicího přístroje (Argonite).



### 9.1 Přídržné magnety

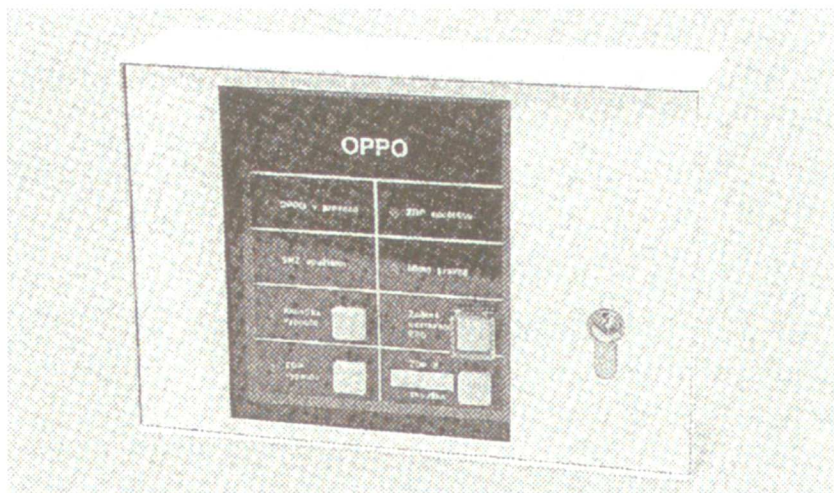
Je to speciální zařízení, které díky elektromagnetické síle udržuje otevřené požární dveře. V případě požáru řídicí jednotka, nebo relé ovládané ústřednou elektrickou požární signalizací, přeruší přívod proudu do požárních magnetů, tím přestanou působit elektromagnetické síly a dveře se díky zavíracímu systému (brano) automaticky zavřou. Tím, že se dveře zavřou se omezí přísun kyslíku do místa požáru a omezí se možnost šíření ohně do dalších prostor.



Obr. 4-25: Přídržné magnety (CSA-Menvier).

## 10 Obslužné pole požární ochrany (OPPO)

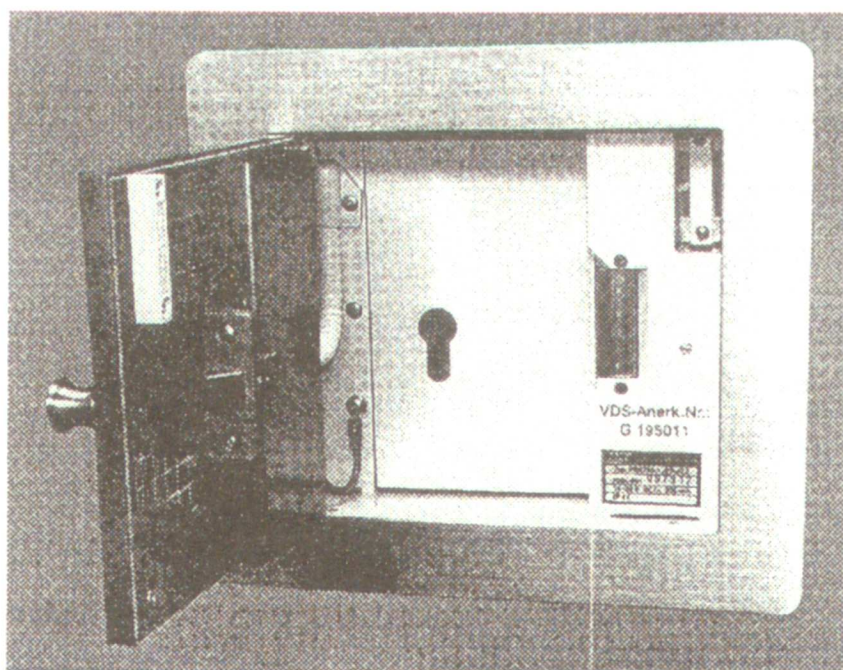
Obslužné pole požární ochrany je univerzální typizovaný ovladač, jednotný pro všechny u nás používané ústředny elektrické požární signalizace. Obslužná pole různých výrobců jsou vzhledem ke své typizaci vzhledově a funkčně téměř stejná. Obslužné pole bylo vyvinuto pro hasičské záchranné sbory. Jeho potřeba vznikla z nutnosti aby hasiči byli schopni snadno a rychle ovládat velký počet u nás používaných druhů ústřednů elektrické požární signalizace. Pomocí obslužného pole hasiči kteří přijedou na objekt, který je v poplachovém stavu, ať již je tento vybaven kteroukoliv ústřednou EPS, mohou ovládat některé důležité funkce ústředny a zároveň získat důležité informace týkající se stavu jednotlivých částí systému, což jim výrazně usnadňuje práci při vlastním zásahu.



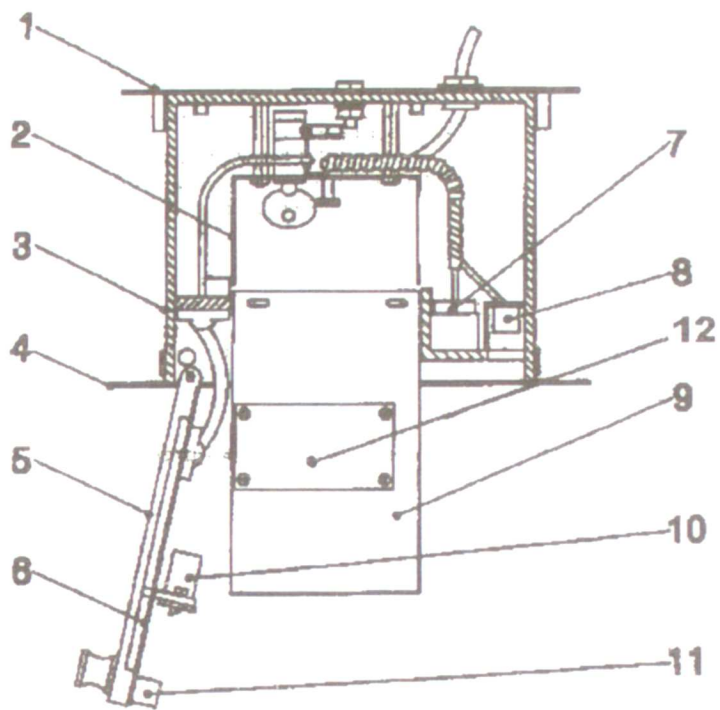
Obr. 4-26: OPPO.

## 11 Klíčový trezor požární ochrany (KTPO)

Klíčový trezor je speciální úschovná schránka do které se ukládají klíče od dveří objektu. Použitím klíčového trezoru se výrazně zrychlí vstup hasičů do hořícího domu a tím umožní jejich včasný zásah. Instalace KTPO má význam především v objektech, kde není stálá obsluha. Trezor se umísťuje do vnější zdi budovy v blízkosti vstupu. Je řízen ústřednou EPS a ve většině případů zajištěn proti neoprávněnému otevření systémem EZS. V klidovém (bezpoplachovém) stavu systému EPS jsou jeho vnější dveře zavřeny a zajištěny tak, aby nebylo možné je otevřít. Vznikne-li na objektu požární poplach, aktivuje se zařízení dálkového přenosu a zároveň se odjistí vnější dveře trezoru, které je pak možno lehkým tahem za madlo otevřít. Takto otevřený trezor však ještě neumožní provést jakýkoli zásah, nebo manipulaci s klíči uloženými v trezoru. Teprve když přijedou na objekt hasiči, odemknou si vnitřní dveře trezoru klíčem (hasičský univerzál) a otevřou je. Teprve potom se dostanou k zámku kterým je možné ovládat jednu požadovanou funkci (např. vypnout akustickou signalizaci). V tomtéž prostoru trezoru jsou uloženy klíče od objektu, pomocí kterých se hasiči dostanou do objektu aniž by se zdržovali a museli ničit vchodové dveře nebo jiné zařízení.



Obr. 4-27: KTPO.



Obr. 4-28: KTPO.

1. Montážní deska
2. Konsole zámku klíčů do objektu
3. Vlastní skříň klíčového trezoru
4. Limcový rámeček trezoru
5. Vnější dvířka
6. Ochrana proti odvrtání + vytápění
7. Elektrický zámek vnějších dveří
8. Kontakt mg. spínače vnějších dveří
9. Vnitřní dvířka
10. Západka vnějších dveří
11. Magnet mg. kontaktu dveří
12. Zámek vnitřních dveří (univerzál)

## 12 Zřizování systémů elektrické požární signalizace (EPS)

Zřizování EPS je komplexní služba zahrnující v sobě všechny fáze od prvního kontaktu se zákazníkem až po provádění servisu.

Předpokládá dostatečnou úroveň znalostí a zkušeností z oboru EPS a oproti ostatním poplachovým systémům (EZS, CCTV, ACS...) navíc ještě specifické kvalifikační předpoklady vymezené právními předpisy.

Poznámka – požadavky na kvalifikaci při zřizování poplachových systémů jsou souhrnně uvedeny v kapitole 1.

Tabulka 4-1: Etapy zřizování EPS

Etapy procesu	Činnost	Dokumentace a záznamy
I. zadání zakázky	<ul style="list-style-type: none"> <li>analýza potřeb zákazníka,</li> <li>bezpečnostní a technická analýza objektu.</li> </ul>	<ul style="list-style-type: none"> <li>zápis z jednání se zákazníkem,</li> <li>projekt požární ochrany*).</li> </ul>
II. zadání	<ul style="list-style-type: none"> <li>zpracování technické specifikace systému.</li> </ul>	<ul style="list-style-type: none"> <li>nabídka s konkrétním technickým řešením (systémový návrh),</li> <li>návrh smlouvy.</li> </ul>
III. Přezkoumání návrhu a příprava realizace	<ul style="list-style-type: none"> <li>ověření úplnosti a realizovatelnosti,</li> <li>odsouhlasení zákazníkem,</li> <li>zpracování změn: projekce.</li> </ul>	<ul style="list-style-type: none"> <li>odsouhlasená smlouva,</li> <li>změny ve smlouvě,</li> <li>upravený systémový návrh,</li> <li>výkresová dokumentace a soupis použitého materiálu.</li> </ul>
IV. realizace	<ul style="list-style-type: none"> <li>montáž,</li> <li>oživení,</li> <li>výchozí revize,</li> <li>předání,</li> <li>zkušební provoz,</li> <li>předání do trvalého provozu.</li> </ul>	<ul style="list-style-type: none"> <li>protokol o předání a převzetí staveniště</li> <li>stavební/montážní deník,</li> <li>zpráva o výchozí revizi,</li> <li>protokol o funkčních zkouškách,</li> <li>předávací protokol,</li> <li>projekt skutečného provedení,</li> <li>návody k obsluze,</li> <li>zápis o vyhodnocení zkušebního provozu.</li> </ul>
V. provoz	<ul style="list-style-type: none"> <li>běžná údržba,</li> <li>periodické prohlídky,</li> <li>pohotovostní servis.</li> </ul>	<ul style="list-style-type: none"> <li>provozní kniha,</li> <li>pokyny pro údržbu,</li> <li>protokol o funkčních zkouškách,</li> <li>revizní zpráva,</li> <li>revizní zpráva,</li> <li>smlouva o provádění servisní činnosti,</li> <li>protokol o provedení servisu.</li> </ul>

\*) Toto posouzení provádí osoba kvalifikovaná ve smyslu vyhlášky 263/2002Sb.

### 12.1 Etapa I. – zadání zakázky

Tato etapa zahrnuje činnosti při kontaktu se zákazníkem. Důležité jsou zde jak formální, tak konkrétní informace a jejich strukturovaný záznam, který může později v rámci nabídkového řízení sloužit pro zpracování koncepce zabezpečení objektu (systémový návrh), aby bylo možné zpracovat nabídkovou cenu. Strategický význam zde má posouzení objektu z hlediska potřeby instalace systému EPS. Toto posouzení provádí osoba



kvalifikovaná ve smyslu vyhlášky 263/2002Sb. a jejím výstupem je dokument s názvem Projekt požární ochrany.

## 12.2 Etapa II. – návrh

### 12.2.1 Všeobecné požadavky

Požadavek na instalaci systému EPS v objektu je dán:

- projektem požární ochrany u nových a rekonstruovaných objektů. Zde je dán rozsah jednak podle technických norem pro příslušné objekty, nebo podle výpočtu dle ČSN 730875. Samočinné hlásiče EPS se nemusí instalovat do těch požárních úseků nebo jejich částí, které jsou bez požárního rizika podle ČSN 73 0802 (požární zatížení nejvýš 7,5 kg/m<sup>2</sup> a součinitel menší než 1). Jsou to například volné chodby a sociální zařízení. Pozor, toto neplatí u shromažďovacích prostorů.
- požadavkem investora na zvýšení protipožárního zabezpečení objektu, případně zvýšení komfortu objektu (hotely, penziony) s ohledem na bezpečnost hostů. EPS na žádost investora, tj. nad rámec požadavku požárně bezpečnostního řešení (bez vývodu na PCO HZS) – nemusí být certifikovaným systémem. Používá se často i tzv. systém EPH (elektrické požární hlášení), kdy jsou čidla detekce požáru připojena na jinou ústřednu než EPS, například na ústřednu EZS.
- požadavky pojišťoven v objektech s nenahraditelnými historickými hodnotami dalšími hledisky vyplývajícími z požárního rizika objektu. Například pokud podle požárně bezpečnostního řešení je EPS vyžadována jen v místnosti serveru, je vhodné zabezpečit i všechny místnosti s touto místností sousedící. Dojde tak k výraznému zkrácení času zjištění nebezpečí požáru v zájmové místnosti, a tak ke snížení případných škod. Je statisticky dokázáno, že pokud není požár zjištěn do 10 minut, jsou škody již nenávratné.

Základním požadavkem na EPS je, aby byla funkčně účelná, hospodárná ve vztahu k nákladům na požární ochranu i k hodnotě chráněných cenností a pravděpodobnosti požáru.

Nutnost střežení požárního úseku se určí hodnotou  $N$  dle výpočtu v odst.18 normy ČSN 73 0875

$$N = (j \cdot a_n + o_s \cdot o_h) \cdot o_v$$

$j$  - je součinitel charakteru posuzovaného prostoru

$a_n$  - je součinitel pro nahodilé požární zatížení

$o_s$  - je součinitel ohrožení osob

$o_h$  - je součinitel ohrožení hodnot

$o_v$  - je součinitel provozních vlivů

Instalace EPS je pak závislá na hodnotě nutnosti střežení  $N$  takto :

$N$  je menší než 3

EPS nemusí být instalována

$N$  je větší než 3 a menší než 3,5

doporučuje se, aby EPS byla instalována

$N$  je větší než 3,5

EPS musí být instalována

Součinitel pro výpočet se určuje dle tabulek v ČSN 730802 a ČSN 73 08 75. Naštěstí samotné výpočty nemusíme provádět často. Dobře zpracovaná zpráva požárně

bezpečnostního řešení objektu již sama určuje, kde je třeba hlásiče EPS nainstalovat a kde ne.

**Při samotném navrhování EPS se musí vycházet:**

- z hodnoty požárního zatížení,
- z počtu osob v objektu, jejich schopnosti pohybu, směrů úniku a dispozice únikových cest,
- z výšky objektu,
- z rozdělení na požární úseky,
- z určení vnějších vlivů v jednotlivých úsecích,
- z úvahy o předpokládaných škodách na majetku,
- z požadavku na ovládaná požárně bezpečnostní zařízení,
- z dalších vlivů působících specificky (proudění vzduchu, tvar stropu, rozmístění svítidel, umístění vzduchotechniky, elektrorozvody apod.)

**EPS musí být navržena tak, aby:**

- všechny vznikající požáry byly signalizovány samočinnými hlásiči již v počátečním stadiu,
- bylo zajištěno co nejrovnoměrnější účinné střežení kteréhokoliv požárního úseku,
- umístění jednotlivých prvků EPS vylučovalo snížení jejich provozuschopnosti,
- byla vyloučena nežádoucí funkce hlásiče (planý poplach),
- byl zajištěn přístup k hlásičům pro jejich údržbu,
- byla provedena dle ČSN 34 2710.

### 12.2.2 Výběr vhodného hlásiče požáru

**Ionizační hlásič kouřový** – detekuje dobře požár, při kterém vzniká při počátečním stadiu jakýkoliv kouř. Nehodí se tam, kde technologické procesy mohou vytvářet zplodiny hoření nebo aerosoly, které způsobí nežádoucí reakci hlásiče.

**Opticko-kouřový hlásič** – lze použít tam, kde v počátečním stadiu hoření vzniká světlý kouř. Nelze ho použít tam, kde technologické procesy mohou vytvářet zplodiny hoření nebo aerosoly světlé barvy, které způsobí nežádoucí reakci hlásiče.

**Lineární hlásiče** – se používají tam, kde je třeba detekovat kouř v počátečním stadiu požáru v prostorách, kde nelze použít klasický bodový hlásič.

**Hlásič vyzařování plamene** – se použije v prostorách, kde se předpokládá rychlé hoření bez vývinu kouře.

**Tepelný hlásič** – se používá tam, kde se předpokládá v počátečním stadiu hoření rychlá nárůst teploty, a zpravidla tam, kde technologie provozu nedovolí nasazení kouřových nebo plamenných hlásičů (údržbářské dílny, svařovny, kuchyně atd.) Při stanovení max. povolené teploty hlásiče nebo hranice diferenciálního navýšení teploty se musí přihlížet k provozní teplotě prostředí, aby byla zaručena správná funkce hlásiče. Tepelné hlásiče se nesmějí umísťovat tam, kde by mohly být zahřívány jinými zdroji tepla (slunce, parovod, přímotop atd.).

**Kombinovaný hlásič** – se používá tam, kde je třeba využít (vzhledem k vlastnostem předpokládaných hořících látek) vlastností několika dříve uvedených hlásičů.

Kombinované hlásiče se v současné době dělí na hlásiče:

MULTISENZOROVÉ – tj. hlásiče, kde k vyhlášení poplachu (nebo i předpoplachu) dojde při součtu hodnot jednotlivých použitých technologií vyhodnocení požáru);

DUÁLNÍ – kde pracují technologie samostatně a k vyhlášení poplachu dojde již při překročení kalibrované hodnoty u jedné z použitých technologií.

Volba správného druhu hlásiče a jeho umístění je nejdůležitější částí návrhu, neboť na tom závisí správná funkce celého systému. Druh hlásiče a jeho umístění se řídí jednak charakterem objektu, předpokládanými průvodními jevy vzniku požáru, provozovanou technologií, a také charakterem střežených hodnot. Rovněž je důležité při umísťování hlásičů zhodnotit jejich přístupnost pro servis a údržbu, opravy a zkoušky, a to i z pohledu ekonomického provozu (příkladem je náhrada bodových hlásičů lineárními hlásiči ve vysokých technologických halách).

### 12.2.3 Umístění ústředny EPS

Ústředny EPS musí být vždy umístěny v požárním úseku, který má součinitel menší než 1.1. Ústředna (hlavní) se umísťuje v ohlašově požáru u stálé služby. Místnost musí být dostupná z volného prostranství nebo z chráněné únikové cesty. Pokud přístupová cesta není chráněná, musí být max. 5 m od hranice objektu. Pokud to není možné dodržet, umísťuje se u vchodu rovnocenný signalizační a ovládací panel.

Vždy se ústředna nebo panel umísťují blízko místa, ze kterého se provádí požární zásah a to do výšky 150 až 160 cm nad podlahou..

Pokud není v objektu stálá služba, musí být zajištěn dálkový přenos informací (ZDP) do místa, kde stálá služba je. Z místa, kde je umístěna ústředna, musí být možnost ovládat protipožární zařízení ručně, pokud je ústředna neovládá automaticky.

### 12.2.4 Řízení ovládaných zařízení

Ovládání nebo signalizace stavu dalších zařízení protipožární ochrany se provádí pomocí vstupních a výstupních modulů (jednotek). Tyto mohou být součástí ústředny EPS (malé systémy) nebo mohou být v provedení adresných jednotek umístěných na hlásicích linkách.

**Výstupní jednotky** – slouží například k ovládání signalizačních zařízení a dále k ovládání jiných požárně bezpečnostních zařízení, jejich součinnost je dána požadavky požárně bezpečnostního řešení. Jsou to například:

- ovládání ZOKT – zařízení pro odtah kouře a tepla
- vypnutí ventilace a vzduchotechniky
- uzavření průchodů mezi požárními úseky
- otevření dveří na únikových cestách
- ovládání evakuačního rozhlasu
- vypnutí plynu
- vypnutí přívodu el. energie
- uzavření požárních klapek
- spuštění SHZ

**Vstupní jednotky** – slouží k signalizaci stavu ovládaných zařízení a stavu prvků, které jsou z požárně bezpečnostního hlediska důležité, ale nemají například dálkové ovládání:

- stav větracích klapek

- stav funkce SHZ
- stav požárních klapek
- stav požárních předělů (dveří) viz odstavec v přehledu EPS – výstupní jednotky

Pokud ústředna EPS vypíná přívod elektrické energie pro zařízení, kde jsou osoby mimo dosah únikových cest (např. jeřáby, dopravníky, výtahy, zakladače atd.), musí být elektrický proud vypnut vždy až po dojezdu zařízení do výchozí polohy.

U protipožárních zařízení, která nejsou ovládána EPS, ale pracují samostatně nebo jsou ovládána ručně (požární klapky, vzduchotechnická zařízení, ZOKT apod.), se doporučuje, aby byl na ústředně EPS signalizován jejich stav.

### 12.2.5 Signalizace poplachu

Poplach se signalizuje jako úsekový (skupinový), všeobecný nebo jako dálkový přenos na HZS. Signalizace se provádí jednostupňově nebo dvoustupňově.

**Jednostupňová signalizace** – ústředna signalizuje všeobecný poplach do prostorů ohrožených vznikajícím požárem (sirény, evak. rozhlas) a podle potřeby provádí ovládní protipožárních zařízení, případně dálkový přenos informací. Tato signalizace funguje vždy při použití tlačítkových hlásičů.

**Dvoustupňová signalizace** – ústředna signalizuje úsekový a všeobecný poplach, přičemž dle ČSN zajišťuje tzv. dva režimy a to DEN a NOC. Nové systémy neznají pojem DEN a NOC, nicméně tyto funkce jsou na ústřednách individuálně programovatelné.

Režim DEN – ústředna signalizuje na podnět samočinných hlásičů úsekový poplach, po uplynutí času T1, případně T2, pak samočinně všeobecný poplach, případně dálkový přenos. Při signalizaci z tlačítek se ústředna chová jako při jednostupňové signalizaci.

Režim NOC – ústředna signalizuje na podnět samočinných i tlačítkových hlásičů hned úsekový i všeobecný poplach, případně provádí dálkový přenos.

Čas T1 (většinou 1–3 minuty) je čas, kdy po vyhlášení úsekového poplachu musí obsluha provést předepsaný úkon, jinak dojde k vyhlášení všeobecného poplachu, případně přenosu dálkového poplachu. Pokud předepsaný úkon provede, naběhne automaticky čas T2.

Čas T2 – je časový interval, ve kterém musí obsluha zjistit skutečný stav v místě signalizovaného požáru, a pokud nehoří, provést následně předepsaný úkon na ústředně EPS. Tak se čas T2 zastaví anedojde k signalizaci všeobecného poplachu či přenosu dálkové signalizace. Pokud se čas T2 překročí nebo po zjištění požáru obsluha aktivuje tlačítkový hlásič, signalizace poplachu pokračuje vyhlášením všeobecného poplachu a případným dálkovým přenosem poplachu ke stálé službě.

Použití dvoustupňové signalizace:

- budova obsahuje více než 50 % osob, které neznají prostředí (administrativní budovy)
- shromažďovací prostory (více než 300 lidí)
- objekt je vyšší než 45 m
- jsou v něm osoby se sníženou pohyblivostí
- jedná se o prostor pro osoby spící
- je-li systém napojen na ZDP
- v jiných případech, požaduje-li to norma

### 12.2.6 Dálkový přenos informací

Základní požadavky na ZDP (zařízení dálkového přenosu) a jeho funkci ve vazbě na EPS jsou uvedeny v přehledu EPS. Toto zařízení se doporučuje z objektů s dvoustupňovou signalizací, tam, kde jsou zapojeny hlásiče do závislostí, kde není vlastní zásahová jednotka a kde není stálá služba. Zejména se jedná o objekty:

- objekty vyšší než 45 m
- shromažďovací prostory
- zdravotnická zařízení s lůžkovými odděleními a výškou nad 8 podlaží
- hotely nad 8 podlaží
- objekty, kde alespoň 10 % má index požárního zatížení vyšší než 1,4

### 12.2.7 Napájení a zálohování systému EPS

Napájení ústředny je ze sítě 230V/50Hz TN-S, rozvody hlásicích linek většinou 24Vdc. Existují ale i zahraniční systémy pracující na bázi 12Vdc. Zálohování a náhradní zdroj dle ČSN EN 54-4, Elektrická požární signalizace - část 4:

Ústředna musí zůstat v provozu na náhradní zdroj 24 hodin, z toho 15 minut ve stavu signalizace požáru.

Kapacitu náhradního zdroje vypočítáme dle vztahu :

$KC = (T-0,25)(I_s+I_o+I_{hs})+0,25(I_p+I_{omax}+I_{hp})$  kde:

K [ - ]	- konstanta v rozsahu 0,8 – 1	
C [ Ah ]	- doba provozu na náhradní zdroj	
$I_s$ [ A ]	- spotřeba ústředny ve střežícím stavu	
$I_o$ [ A ]	- proud odebíraný z ústředny pro jiná zařízení (ve stavu střežení)	
$I_{hs}$ [ A ]	- proud odebíraný hlásicemi prvky ve stavu střežení	$I_p$ [ A ]
	- spotřeba ústředny ve stavu signalizace požáru	
$I_{hp}$ [ A ]	- maximální možný proud odebíraný hlásicemi prvky ve stavu poplachu	
$I_{omax}$ [ A ]	- proud odebíraný z ústředny na jiné zařízení (ve stavu signalizace požáru)	

Pokud je systém napojen na náhradní zdroj, který není součástí systému (UPS, agregát apod.), který zajistí minimálně stejné podmínky zálohování jako zdroj vlastní, může být tento zdroj považován za náhradní zdroj EPS.

Při návrhu systému EPS je třeba provést i kontrolní výpočty hlásicích linek, při kterých se posoudí celková spotřeba zařízení EPS (hlásiče, doplňková zařízení) na lince ve vztahu na průřez a délku vedení tak, aby byly splněny technické požadavky výrobce. K tomu nám pomohou jednoduché výpočty vedení a hlásicích linek.

Tabulka 4-2: Dimenzování vodičů

Průměr Ø [mm]		Poloměr r [mm]	Průřez S [mm <sup>2</sup> ]	Odpor na metr ΔR [Ω/m]	Délka L [m]	Odpor vodiče celkem R [Ω]	Proud I [mA]	Úbytek napětí ΔU [V]
<b>Příklady*):</b>								
1,5	→	0,75	1,76625	0,009738146	75	0,730360934	1,25	0,001825902
0,51	→	0,255	0,204179	0,084240015	100	8,424001548	20	0,336960062
4	→	2	12,56	0,001369427	100	0,136942675	20	0,005477707

\*) uvedené příklady platí pro případ užití měděných vodičů

Zjištěný odpor linky a vypočtený úbytek se porovnává s povoleným odporem a úbytkem dle technických podmínek výrobce. Stejně tak je možné kontrolovat odebíraný proud všech prvků instalovaných na lince s povoleným proudovým zatížením linky dle technických parametrů výrobce. Tyto podmínky i doporučené postupy se u jednotlivých výrobců liší, a proto je třeba před návrhem systému projít odpovídajícím školením.

### 12.3 Etapa III. – přezkoumání návrhu a příprava realizace

Cílem této etapy je připravit podmínky pro bezproblémovou montáž uvedení do provozu a vlastní dlouhodobě spolehlivý provoz systému. V případě odsouhlasení nabídky na realizaci je nutno ještě před uzavřením smlouvy či objednávky na realizaci buď potvrdit skutečnosti uvedené v systémovém návrhu, či navrhnout případné změny a dodatky.

#### 12.3.1 Doporučený obsah projektové dokumentace

##### 12.3.1.1 Dokumentace pro územní rozhodnutí

###### Souhrnná zpráva – průvodní část

V této části se uvádí identifikace investora, identifikace objektu, identifikace zpracovatele dokumentace, předmět územního rozhodnutí, dotčení účastníci řízení.

Souhrnná zpráva – technická část obsahuje stručný popis stavby a její účel, základní technické údaje, bilanci spotřeby, vazby na jiné stavby a soubory, popis zajištění ochrany životního prostředí, požární ochrany a bezpečnosti provozu.

###### Výkresová část

Půdorysné výkresy v měřítku dle zadání investora se zakreslením prvků použité technologie (u slaboproudých systémů včetně EPS se v tomto stupni dokumentace výkresová část zpravidla nevypracovává).

###### Doklady

Zápisy z jednání, stanoviska, souhlasy nebo posouzení dotčených účastníků řízení.

##### 12.3.1.2 Dokumentace pro stavební řízení

###### Souhrnná zpráva – průvodní část

V této části se uvádí identifikace investora, identifikace objektu, identifikace zpracovatele dokumentace, předmět územního rozhodnutí, dotčení účastníci řízení. Dále musí obsahovat údaje o splnění požadavků dotčených orgánů státní správy, způsob provedení stavby, předpokládanou dobu provedení stavby a termín dokončení a orientační náklady na provedení stavby.

**Souhrnná zpráva – technická část**

obsahuje popis stavby a její účel, podrobné technické údaje, bilanci spotřeby a zajištění zdrojů, vazby na jiné stavby a soubory, popis zajištění ochrany životního prostředí, požární ochrany a bezpečnosti provozu.

**Technické řešení**

obsahuje popis řešení s vazbou na jiné soubory, stručný popis funkce zařízení, popis rozmístění zařízení, popis provedení hlavních tras rozvodů včetně způsobu uzemnění .

**Výkresová část**

Půdorysné výkresy v měřítku zpravidla 1:50 zahrnující dispozice a rozmístění zařízení a zakreslení hlavních tras slaboproudých rozvodů.

**Doklady**

Zápisy z jednání, stanoviska, souhlasy nebo posouzení dotčených účastníků řízení, zejména orgánů státní správy.

**12.3.1.3 Dokumentace prováděcí**

Rozsah a způsob provedení této dokumentace se stanoví dohodou mezi objednatelem a zhotovitelem dokumentace. Touto dokumentací nesmějí být měněny nebo upravovány technické parametry a požadavky obsažené v dokumentaci pro stavební řízení. Pokud je taková změna v odůvodněných případech nutná, lze ji učinit výhradně se souhlasem zpracovatele dokumentace pro stavební řízení.

Touto dokumentací se rozšiřuje a prohlubuje vypovídací schopnost dokumentace ke stavebnímu řízení a upřesňují se zde jmenovité dodávky, respektive provedené práce. Tato dokumentace obsahuje například:

Ve smyslu ustanovení normy ČSN 73 0875 v návaznosti na projektovou dokumentaci vyššího stupně (projekt pro stavební řízení), která stanoví nutnost vybavení objektu EPS a dále stanoví druh EPS a přibližný počet hlásičů, návaznosti na ovládaná zařízení a způsob signalizace poplachu, je vypracována realizační projektová dokumentace. Tato dokumentace s konečnou platností posoudí nutnost instalace EPS (většinou v návaznosti na požárně bezpečnostní řešení stavby) a stanoví rozsah EPS pro jednotlivé požární úseky nebo jejich části :

- a) druh, typ, počet, rozmístění hlásičů, popř. dalších prvků systému, jejich zapojení do linek, případně přiřazení adres,
- b) způsob údržby a periodu čištění hlásičů,
- c) umístění ústředěn EPS, doplňujících zařízení a jejich vzájemné propojení,
- d) návaznost ovládaného zařízení podle požadavků požárně bezpečnostního řešení stavby,
- e) způsob přístupu k hlásičům,
- f) vybavení systému pohotovostními díly,
- g) druh EPS,
- h) signalizaci poplachu,
- i) požadavky na pracovní síly nutné pro zajištění údržby a obsluhy.

V dokladové části přikládá tato dokumentace certifikáty použitého zařízení a prohlášení o shodě dle zák. č. 22/97 Sb.

Nad rámec této dokumentace si dodavatel (zhotovitel) v případě potřeby zajišťuje dodavatelskou dokumentaci.

### 12.3.1.4 Dokumentace pro výběr dodavatele

Tato dokumentace slouží jako materiál pro vyhledání dodavatele stavby, jako podklad pro výběrové řízení na dodávku stavby. Je na úvaze investora, v návaznosti na který stupeň dokumentace bude dokumentace pro výběr dodavatele vypracována a jaké podrobnosti bude obsahovat. Tato dokumentace však musí vždy obsahovat výkaz, výměr. Tento podklad nemusí být zpracován autorizovanou osobou.

### 12.3.2 Zásady kreslení a značení prvků EPS v projektech

Ve výkresové dokumentaci je vhodné dodržovat určitá pravidla označování a kreslení hlásičů požáru. Příklad takových pravidel je uveden dále.

Hlásiče a prvky s adresací se označují: XX YY ZZ / xx, kde:

- XX - pořadové číslo ústředny
- XX - pořadové číslo linky na ústředna
- ZZ - pořadové číslo hlásiče nebo prvku v hlásicí lince
- xx - číslo skupiny hlásičů

Hlásiče a prvky bez adresace se označují: XX YY ZZ, kde:

- XX - pořadové číslo ústředny
- XX - pořadové číslo linky na ústřednu
- ZZ - pořadové číslo hlásiče nebo prvku v hlásicí lince
- xx - číslo skupiny hlásičů

U tlačítkových hlásičů se před číslo dává ještě písmeno T. Takto se značí prvky EPS dle ČSN 73 0875. V praxi je to ale dnes velice pracné a nevýhodné značení. Většina systémů je adresných, a jak na LCD displejích, tak na grafické nadstavbě se hlásiče a další prvky zobrazují pod čísly skutečných adres systému. To znamená doplnit ve výkresech označení hlásiče ještě o adresu nebo celé označení nahradit číslem adresy.

Prvky a zařízení EPS se zakreslují do výkresů značkami dle ČSN 01 3378. V případě použití nových nebo jiných značek je třeba výkres doplnit legendou značek.

## 12.4 Etapa IV. – realizace (montáž)

Do této etapy jsou zahrnuty všechny činnosti od převzetí staveniště po předání fungujícího systému do trvalého provozu. Vstupem je zákazníkem odsouhlasený systémový návrh včetně výkresové dokumentace a rozpisu materiálu.

### 12.4.1 Všeobecné požadavky

Ve smyslu normy ČSN 34 2710 čl.400 může montáž provádět pouze montážní organizace výrobce, montážní organizace výrobcem pověřená nebo montážní organizace, která má na tuto činnost proškolené pracovníky.

Montáž v zásadě probíhá dle odsouhlaseného systémového návrhu a výkresové dokumentace. Při montáži vycházíme z projektových zásad.

#### 12.4.1.1 Zásady umístování hlásičů

Hlásiče se umísťují na stropy nebo nejvyšší místa střežených prostorů dle předpisů výrobce s přihlédnutím ke specifikům tohoto prostoru (viz obr. příloha). Pokrytá plocha u současných hlásičů opticko-kouřových a ionizačních je cca 100 m<sup>2</sup>. Pokud si představíme tuto plochu jako kruh a střežené plochy přiložíme k sobě tak, aby nevznikla místa bez pokrytí, dojde k částečnému překrytí úsečí a reálná pokrytá plocha jednoho hlásiče bude



cca 75 m<sup>2</sup>. To odpovídá 6m vzdálenosti hlásičů mezi sebou, a splňuje tak podmínky tabulky v příloze č. 2 normy ČSN 73 0875 pro jednopodlažní objekt s výškou do 12 m a indexem požárního zatížení kolem 1 celé. (většina objektů). Pokud bude index požárního zatížení vyšší nebo menší a bude se výrazně lišit i výška místnosti, je třeba postupovat vždy podle diagramu v příloze č. 2 normy. Tento diagram platí pro prostory až do výšky 20 m. U prostorů vyšších je nutné kombinovat různé druhy samočinných hlásičů a přihlížet k pokynům výrobce.

Povolená vzdálenost hlásiče od boční stěny je polovina vypočtené vzdálenosti mezi hlásiči. Povolený odstup od vyústění vzduchotechniky je 90 cm.

Největší povolená plocha střežená samočinným **tepelným** hlásičem je podle ČSN 20 m<sup>2</sup>, s maximální výškou 8 m a maximální vzdáleností mezi hlásiči 6,5 m. V současné době se však již vyrábějí hlásiče, které podle technických parametrů výrobce pokryjí plochu až 40 m<sup>2</sup>.

**Lineární hlásiče, nasávací systémy, lineární tepelné hlásiče a hlásiče vyzarování plamene** se umísťují vždy jen podle pokynů výrobce. Například většina infralineárních hlásičů dokáže pokrýt plochu 12 x 100 m. To znamená, že hlásič pokrývá 6m prostor na každou stranu od infrapaprsku. Paprsek se nastavuje pod strop místnosti ve vzdálenosti 0,6 až 1 m. Nasávací systémy kryjí plochu v závislosti na počtu ramen trubkového systému a na počtu nasávacích otvorů. Vzdálenost mezi nasávacími otvory je u většiny systémů 8m (tj. plocha cca 50 m<sup>2</sup>). Poslední novinkou na trhu jsou nasávací hlásiče s laserovým vyhodnocením.

Lineární tepelné hlásiče (kabely) pokryjí prostor o šířce cca 3 m – v závislosti na výšce nad střeženým předmětem. Jsou-li hlásiče umístěny:

- v uzavřených nebo oddělených prostorách,
- nad mezistropem nebo podhledem,
- pod zvýšenou podlahou,
- v nepřehledných prostorách,
- uvnitř technologických zařízení nebo uvnitř potrubí vzduchotechniky,

musí k nim být zapojena signální svítidla umístěná na dobře viditelném místě pro službu konající obsluhu. Toto platí nejen pro hlásiče konvenční, ale i pro hlásiče adresné, pokud se jedná o umístění v nepřehledném prostoru nebo uvnitř technologie. Umístění hlásičů nad podhled je dobré s ohledem na servis označit na podhledu například červeným bodem.

Umísťování samočinných čidel v prostorách, jako jsou například regálové sklady, se řídí přímo ustanoveními příslušné normy a normy ČSN 73 0875.

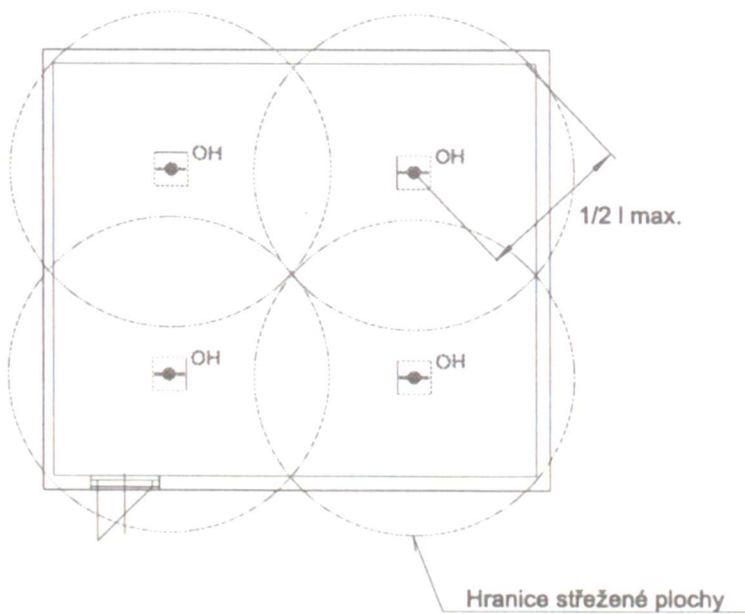
**Tlačítkové hlásiče požáru** se umísťují ve výšce 140 cm od podlahy v místech snadno dosažitelných unikajícími osobami.

- u východů z nechráněných únikových cest do cest chráněných, a to ve všech podlažích objektu
- u východů z únikových cest na volné prostranství, nejdále 3m od východu a do zorného pole unikající osoby.
- v místech obsluhy technologického zařízení
- v místech trasy občůzky osoby konající ostrahu objektu

Při umísťování hlásičů do jednotlivých prostor a objektů je třeba respektovat protokoly o vnějších vlivech (prostředí) ve vztahu na provedení (krytí) hlásičů. Samostatným

oddílem jsou zde hlásiče v provedení do prostředí s nebezpečím výbuchu. Téměř všechny systémy mají tyto hlásiče v sortimentu z důvodu střežení např. plynových zařízení nebo jiných těžkých provozů. Hlásiče v ex. provedení jsou vesměs konvenční a do adresných systémů se připojují přes oddělovací obvody. Tato zařízení, tj. hlásiče i oddělovací obvody, musí splňovat podmínky ČSN EN 50020 – Nevýbušná elektrická zařízení - Jiskrová bezpečnost.

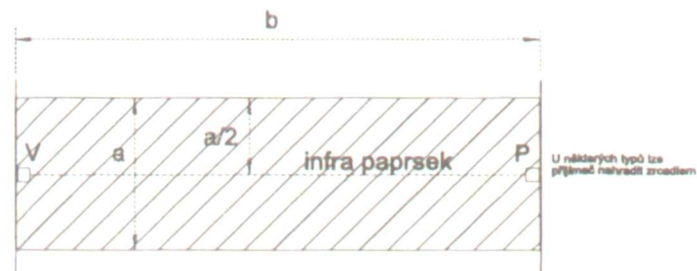
$I_{max}$  - maximální povolená vzdálenost mezi hlásiči



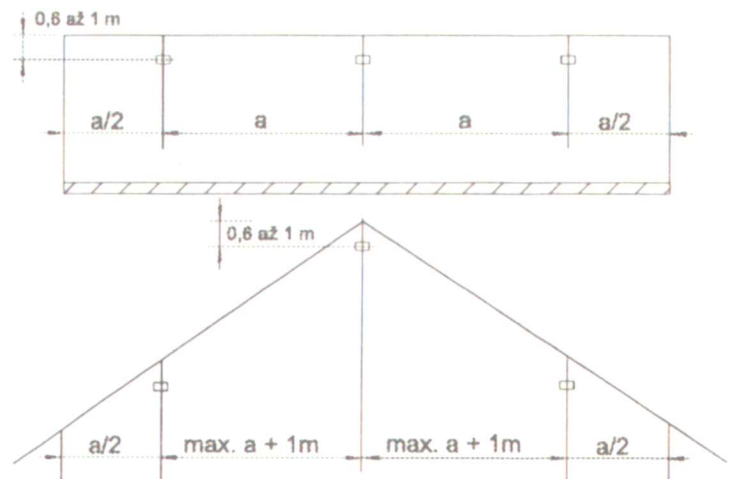
Obr. 4-29: Příklad pokrytí plochy samočinnými hlásiči.

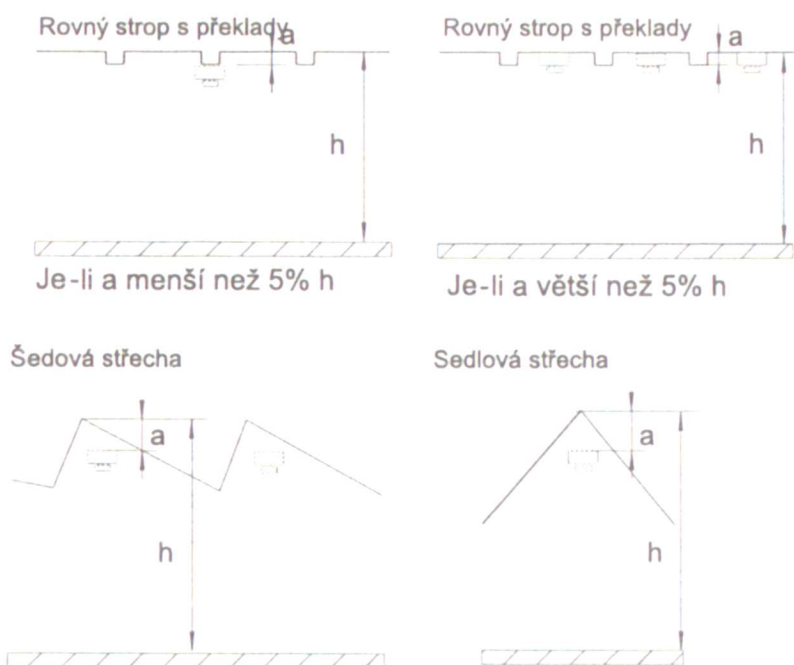
Obr. 4-30: Příklad pokrytí plochy lineárním hlásičem.

- a - maximální šířka pokryté plochy (6 až 7,5 m dle výrobce)
- b - maximální délka pokryté plochy (až 100 m)



Příklad umístění lineárních hlásičů

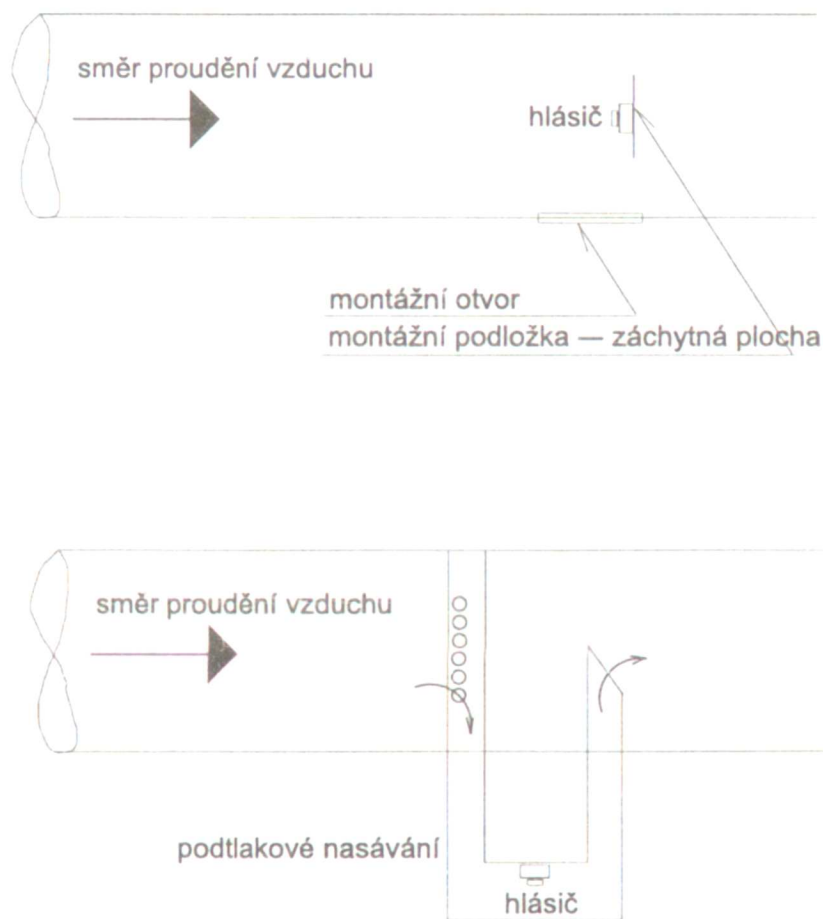




Obr. 4-31: Příklad umístění hlásičů v závislosti na tvaru stropu nebo střechy.

Je-li  $h$  menší než 5 m, bude  $a = 0$   
 Je-li  $h$  5 až 10 m, bude  $a = 0,4$  m  
 Je-li  $h$  větší než 10 m, postupujeme dle pokynů výrobce.

Obr. 4-32: Příklad umístění čidel v potrubí vzduchotechniky.



### 12.4.1.2 Propojování hlásičů

Požární hlásiče se spojují do hlásicích linek, adresné hlásiče se přiřazují do skupin hlásičů. Do jedné hlásicí linky nebo v jedné skupině se řadí hlásiče zejména:

- z jednoho prostoru nebo z prostor sousedních či dispozičně blízkých, přičemž tyto prostory nemusí být v jednom požárním úseku (pokud ČSN nestanoví jinak).
- z prostorů, které jsou podobné z hlediska vzniku požáru, mají stejné nebo podobné charakteristiky a požár se v nich hasí stejným hasivem.

V případech, kdy zjištění skutečného stavu po signalizaci požáru je časově náročné (např. kabelové kanály), musí být hlásiče zapojeny na výstup ústředny umožňující opakované nulování a doporučuje se jejich zapojení do závislosti více linek nebo hlásičů. Stejně tak musí být zapojeny do závislosti linek nebo hlásičů samočinné hlásiče systému EPS, který např. vypíná energetický přívod, ovládá spouštění stabilního hasicího zařízení apod., což by mohlo způsobit následné ekonomické škody v případě planého hlášení (jistota je v zapojení člověka do procesu spouštění HZS).

Tlačítkové hlásiče se zapojují do jedné hlásicí linky nebo jedné skupiny u hlásičů s adresací:

- nejvýše ze dvou navazujících podlaží,
- v přehledném prostoru nejvýše 100 m od sebe,
- v nepřehledném prostoru nejvýše 50 m od sebe.

Tlačítkové a samočinné hlásiče se nesmějí zapojovat do jedné hlásicí linky s výjimkou adresných hlásičů, kde jsou tlačítkové hlásiče přiřazeny do jiné skupiny než hlásiče samočinné. Skupina samočinných hlásičů musí v tom případě umožňovat dvoustupňovou signalizaci (viz ústředna EPS).

Do jedné hlásicí linky nebo skupiny nemají být zařazovány hlásiče:

- uvnitř technologických zařízení společně s hlásiči střežícími okolní prostor,
- nad podhledem nebo pod zvýšenou podlahou společně s hlásiči střežícími hlavní prostor,
- nad podhledem společně s hlásiči pod zvýšenou podlahou.

Řazení hlásicích linek na ústředně by mělo odpovídat prostorovému uspořádání objektu (pokud je to možné).

Na jednu linku konvenční neadresné ústředny je možné zapojit max. 32 hlásičů.

Na jednu linku adresné ústředny je možné zapojit max. 32 adres. Pokud je adresná linka kruhová, je max. počet adres 127. Doporučuje se dělit kruhovou linku izolátory minimálně na dvě poloviny, výhodnější je však podle skupin a dispozic objektu. Pokud je do kruhového vedení zapojen adresný vstupní modul pro konvenční hlásiče, je jejich počet za vstupním modulem opět max. 32 ks.

### **12.4.2 Instalace kabelových rozvodů**

Propojování hlásičů a dalších prvků EPS se provádí vodiči a kabely s měděnými jádry. Ve věci typu a technických parametrů propojovacích kabelů je nutno přihlížet k doporučením výrobce, předpisům a normám pro vnitřní a venkovní slaboproudé rozvody, a zejména dle stanoviska Čechu EPS.

Stanovisko vychází z požadavků na kabely EPS dle ČSN 73 0875 a z požadavků v části 6.11 Kabely a propojení normy CLC/TS 54 –14.

#### **Běžné plamen nešířící (samozhášecí) kabely s izolací PVC dle ČSN EN 50265 (IEC 332-1)**

1. vedení hlásicích linek (požárních smyček) EPS s kolektivní adresací v jednom požárním úseku, pro které hlásicí linka slouží, vedené po povrchu.
2. vedení k hlásičům od adresovací (vstupní) jednotky nebo od master hlásiče v jednom požárním úseku (prostoru), pro který hlásiče slouží, vedené po povrchu.

3. vedení k adresovatelným hlásičům, vstupním či výstupním jednotkám na kruhovém i přímém vedení, slouží-li toto vedení pouze pro jeden požární úsek, vedené po povrchu.
4. vedení vedená pod omítkou s krytím nejméně 10 mm.
5. vedení vedená v samostatně požárně oddělených uzavřených truhlících, šachtách a kanálech, přičemž jejich konstrukce mají vykazovat požární odolnost nejméně EI 30D1.

#### **Bezhalogenové kabely se zvýšenou odolností proti šíření plamene dle ČSN EN 50266 (IEC 332-3)**

1. vedení vedená v prostorách chráněných únikových cest, vedená po povrchu,
2. vedení v prostorách budov pro bydlení a ubytování, budov zdravotnických zařízení a ve shromažďovacích prostorách, vedená po povrchu,
3. tam, kde to požaduje samostatná norma.

#### **Ohniodolné bezhalogenové kabely se zvýšenou odolností proti šíření plamene dle ČSN EN 50266 ( IEC 332-3 a IEC 331)**

1. vedení hlásicích linek (požárních smyček) EPS s kolektivní adresací vedená požárními úseky s požárním rizikem, jimiž pouze procházejí, vedená na povrchu.
2. vedení k adresovatelným hlásičům, vstupním či výstupním jednotkám na kruhovém i přímém vedení, je-li toto vedení vedeno více požárními úseky s požárním rizikem, vedená na povrchu.
3. pokud následující vedení není vedeno pod omítkou s krytím nejméně 10mm nebo není vedeno v samostatných požárně oddělených uzavřených truhlících, šachtách a kanálech, přičemž jejich konstrukce mají vykazovat požární odolnost nejméně EI 30 D1:
  - vedení propojující více ústředí EPS, ovládacích a signalizačních panelů nebo výstupních reléových jednotek zapojených v jedné komunikační síti
  - vedení propojující ústřednu EPS umístěnou mimo ohlašovnu požáru s ovládacím a signalizačním panelem této ústředny umístěným v ohlašovně požáru.
  - vedení propojující ústřednu EPS se zařízením dálkového přenosu informací (ZDP. KTPO.OPPO).
  - vedení propojující ústřednu EPS (její vstupy a výstupy) s požárně bezpečnostními zařízeními (SHZ samočinné odvětrání, požární klapky ve VZT nebo jiné ovládní).

#### **12.4.3 Výchozí revize EPS a funkční zkoušky**

Provedení výchozí revize zařízení EPS se zajišťuje po zkouškách podle čl. 411 ČSN 34 2710. Výchozí revizi zařízení EPS provádí revizní technik podle ČSN 33 1500 a podle dále uvedených ustanovení čl.413 ČSN 34 2710 – tj. min. jednou ročně.

Spolu s předáním systému musí být předán uživateli protokol o výchozí revizi systému EPS. Revizi musí provádět pracovník s potřebnou kvalifikací § 9 vyhl. 50/78 Sb., ve znění pozdějších předpisů. Vzhledem k tomu, že pojetí revize vymezené zákonnými požadavky směřuje k prokázání **bezpečnosti elektrického zařízení** a nevymezuje konkrétní úlohy pro ověřování funkčnosti elektronických systémů a zařízení, je velice účelné, aby instalační firmy měly pro tyto potřeby pracovníka s § 9 vyhl. 50/78 Sb., proškoleného na své systémy EPS, který bude schopen provést jak revizi silové části, tak ověření funkce

systému. Jinou alternativou je provedení silové revize samostatným revizním technikem za přítomnosti techniků montážní firmy, kteří mohou provést funkční zkoušky systému EPS. Zápis o provedení funkční zkoušky je pak v příloze revizní zprávy.

### 12.4.4 Funkční zkoušky

Zkoušky zařízení EPS před uvedením do provozu viz ČSN 34 2710 čl. 410. Před uvedením zařízení EPS do provozu se zjišťuje zejména:

- zda zařízení EPS jako celek má požadované vlastnosti,
- zda je montáž zařízení EPS provedena podle platné dokumentace doplněné o změny vzniklé v průběhu výstavby,
- zda je zařízení EPS vybaveno předepsanou průvodní dokumentací – zda je zařízení EPS vybaveno předepsanými bezpečnostními tabulkami a nátěry – zda izolační odpory jsou v souladu s příslušnými ustanoveními ČSN 34 27 10.

### 12.4.5 Předání uživateli

Jedná se o protokolární akt, kde dodavatelská organizace oficiálně předává zákazníkovi nainstalovaný systém EPS. V rámci předání musí být provedeno kompletní předvedení činnosti systému a funkce komponent včetně případného přenosu požárního poplachu na PCO.

Předávací protokol potvrzuje funkční a úplné předání předmětu smlouvy, stanovuje termíny odstranění případných nedostatků, stanovuje termín vypršení záruční lhůty XX měsíců, stanovuje pracovníka uživatele zodpovědného za provoz EPS a osoby zmocněné k hlášení závady na systému, a dále potvrzuje řádné zaškolení obsluhy. Přílohou přijímacího protokolu může být:

Požadavky na předání a převzetí EPS **stanovuje** ČSN 34 2710 čl. 420 – 423.

Předání a převzetí zařízení EPS musí být provedeno neprodleně po dokončené montáži a po vykonání výchozí revize zařízení EPS podle čl. 411 až 414. O předání a převzetí zařízení EPS je nutno sepsat zápis.

**Při předání zařízení bude předána uživateli následující dokumentace:**

- projektová dokumentace skutečného stavu,
- předávací protokol,
- výchozí revizní zpráva,
- kniha provozu,
- návod k obsluze v českém jazyce.

### 12.5 Etapa V. – provoz

Uživatel určuje v dostatečném předstihu osobu zodpovědnou za provoz zařízení EPS, osoby pověřené údržbou zařízení EPS a osoby pověřené obsluhou zařízení EPS tak, aby při předávacím a přijímacím řízení mohly být proškoleny ze svých činností. Zároveň zajišťuje organizační a technickou návaznost zařízení EPS na systém požární ochrany.

Požadavky na zodpovědné osoby jsou vymezeny ČSN 34 27 10 čl. 430 – 432

**Osoba zodpovědná za provoz zařízení EPS má tyto povinnosti:**

- odpovídá za bezporuchový provoz zařízení EPS,
- kontroluje činnost osob pověřených obsluhou zařízení EPS,

- zajišťuje, aby osoby pověřené údržbou prováděly údržbu dle pokynů výrobce a udržovaly zařízení EPS v trvalém provozu,
- zajišťuje neprodlené provedení všech oprav včetně provedení opravy servisní organizací,
- odpovídá za řádné vedení provozní knihy zařízení EPS a svoji činnost do této knihy podchycuje,
- kontroluje provádění zkoušek činnosti zařízení EPS během provozu a zodpovídá za provedení předepsaných revizí v průběhu provozu,
- udržuje průvodní dokumentaci v pořádku, zaznamenává změny a ukládá ji na místech k tomu určených,
- při vyřazení zařízení EPS nebo jeho části z činnosti zajišťuje potřebná náhradní opatření z hlediska požární bezpečnosti objektu.

### **Osoba pověřená obsluhou zařízení**

- musí být prokazatelně proškolená předávající organizací,
- musí být alespoň poučena dle ČSN 34 3100,
- vede záznamy v provozní knize zařízení EPS a podle situace po signalizaci požáru podle požární poplachové směrnice objektu,
- zjištěné závady neprodleně hlásí osobě zodpovědné za provoz zařízení EPS.

### **Osoba pověřená údržbou**

- musí být znalá dle ČSN 34 31 00 a **prokazatelně** zaškolená dodavatelem zařízení,
- provádí prohlídky a údržbu zařízení EPS podle pokynů výrobce,
- provádí předepsaným způsobem kontrolu zařízení EPS podle čl. 434 ČSN 34 2710,
- provádí opravy v rozsahu stanoveném výrobcem,
- zjištěné závady, které není schopna nebo oprávněna opravit, neprodleně hlásit osobě zodpovědné za provoz zařízení EPS – o všech kontrolách, údržbě a opravách zařízení EPS musí provést záznam do provozní knihy zařízení EPS.

Náhradní díly předepsané v rozpisu materiálu budou uloženy u uživatele zařízení EPS, skladovací prostory musí být v rozmezí teplot -20 °C až +70 °C.





# **Systemy průmyslové televize (CCTV)**

Stanislav Křeček

## **OBSAH:**

<b>1. Teoretické základy videotechniky</b> .....	163
1.1 Fyziologie lidského oka .....	163
1.2 Základní parametry přenosových soustav televize.....	165
<b>2. Stručný přehled vývoje snímací techniky v datech</b> .....	169
<b>3. Snímání obrazu – CCD kamera</b> .....	172
3.1 Princip snímání CCD čipem .....	172
3.2 Formát čip.....	173
3.3 Rozlišovací schopnost.....	173
3.4 Citlivost.....	174
3.5 Odstup signál/šum (S/N - signal/noise) .....	176
3.6 Synchronizace .....	177
3.7 Napájení kamer .....	178
3.8 Připojení objektivu .....	178
3.9 Řídící výstupy kamery .....	178
3.10 Doplnkové funkce.....	178
3.11 Volba vhodného typu kamer .....	181
<b>4. Objektivy</b> .....	182
4.1 Ohnisková vzdálenost .....	182
4.2 Clona .....	183
4.3 Optická ostrost.....	184
4.4 Kritéria výběru vhodného objektivu .....	187
4.5 Uchycení objektivu .....	188
<b>5. Příslušenství kamer</b> .....	189
5.1 Kamerové kryty.....	189
5.2 Polohovací hlavice.....	191
5.3 Systémy dálkového ovládání .....	192
<b>6. Přenos videosignálu</b> .....	194
6.1 Přenos po koaxiálním vedení .....	194
6.2 Přenos po symetrickém vedení .....	196
6.3 Další možnosti přenosu videosignálu (bezdrátové).....	197

6.4 Přenos digitalizovaného videosignálu .....	199
<b>7. Zařízení na zpracování videosignálu .....</b>	<b>199</b>
7.1 Monitory .....	199
7.2 Kamerové přepínače .....	202
7.3 Děliče obrazu, kvadrantový selektor.....	203
7.4 Multiplexery .....	204
7.5 Křížové přepojovací <b>pole</b> .....	<b>207</b>
7.6 Videodetektor .....	209
<b>8. Záznam obrazu .....</b>	<b>210</b>
8.1 Videorekordér s dlouhou dobou záznamu .....	210
8.2 Videotiskárna .....	211
8.3 Digitální záznam obrazu .....	211
8.4 Snímkovací fotokamera .....	212
<b>9 Zřizování systémů CCTV .....</b>	<b>213</b>
9.1 Etapa I. - zadání zakázky .....	214
9.2 Etapa II – Návrh.....	216
9.3 Etapa III. – Přezkoumání návrhu a příprava realizace .....	224
9.4 Etapa IV. – Realizace .....	225
9.5 Etapa V. – Provoz systému CCTV.....	234

## 1. Teoretické základy videotechniky

### 1.1 Fyziologie lidského oka

Vzhledem ke značné analogii konstrukce lidského oka a konstrukce kamery s objektivem jsou v této kapitole uvedeny základní fyziologické vlastnosti lidského oka. Znalost alespoň základních principů nám později pomůže lépe pochopit proces snímání reality kamerou a vytváření elektronického obrazu.

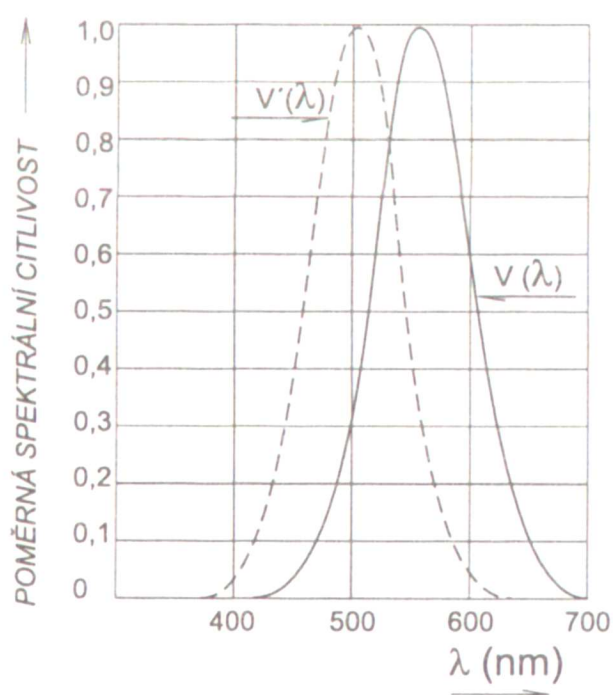
Co je to vlastně vidění?

Je to složitý systém propojení a vazeb mezi nervovými buňkami zrakového systému na různých úrovních včetně vazeb zpětných. Nejde jen o samotné zrakové vnímání, ale i o další fyziologické a biologické funkce lidského organismu s přímým vlivem na psychický stav a kvalitu pracovního výkonu.

Vlastní lidské oko je tvořeno dvěma systémy:

**Optický systém** umožňuje vytvořit na sítnici převrácený, zmenšený a neskutečný (virtuální) obraz vnějšího světa.

**Nervový systém** slouží k příjmu, výběru a zachování zrakové informace. Základním kamenem nervového systému je sítnice tvořená 11 vrstvami buněk. Pro zrakový vjem jsou podstatné dva typy fotoreceptorů, a to **tyčinky** a **čípky**. Denní, tzv. fotopické barevné vidění zprostředkovávají čípky. V oku jich je 6,5 mil. Jejich rozměr se pohybuje od průměru 0,005 do 0,006 mm. Nej hustěji je fotoreceptory osazena centrální jamka sloužící pro přímé vidění. Obsahuje pouze čípky a je jich zde umístěno 800 tis. Noční, tzv. skotopické vidění nám zprostředkovávají fotoreceptory zvané tyčinky. V oku jich je 125 mil. Jsou citlivější než čípky a mají rozměr cca 0,002 mm. Na obr. 5-1 je graf poměrné spektrální citlivosti pro fotopické a skotopické vidění. Z průběhu křivek je patrná nejvyšší citlivost fotopického vidění v oblasti cca 555 nm, což odpovídá žlutozelené barvě. Spektrální křivka poměrné citlivosti skotopického vidění je poněkud posunuta do oblasti kratších vlnových délek, což vysvětluje namodralý zrakový vjem při pozorování scény s nízkou úrovní osvětlení, např. za soumraku.



Fyziologické vlastnosti oka a pojmy, jichž se využívá, popř. nacházejí analogii v televizní technice, jsou:

- akomodace oka
- adaptace oka
- rychlost vnímání (setrvačnost lidského oka)
- zorné pole
- obhledové pole
- rozlišovací schopnost
- zraková ostrost
- prostorové vidění,
- stálost vnímání barevných tónů.

Obr. 5-1: Graf spektrální citlivosti lidského oka.

**Akomodace oka** je schopnost ostře zobrazit na sítnici blízké předměty (ve vzdálenosti menší

než 6 m). Oko nedovede současně stejně ostře zobrazit na sítnici předměty nacházející se v různých vzdálenostech. Normální oko bez optických vad dokáže při pohledu do dálky zaostřit od 6 m do nekonečna. Pro kratší vzdálenosti nastupuje proces akomodace. Nejbližší bod, který je plně akomodované oko schopno ostře zobrazit, se nazývá **blízký bod**. Jeho umístění je individuální a je závislé na věku člověka. Typické hodnoty blízkého bodu jsou uvedeny v tabulce 5-1.

Tabulka 5-1: Hodnota blízkého bodu v závislosti na lidském věku.

Věk provozovatele (roky)	Blízký bod (cm)
15	9 - 10
30	13
50	50

**Adaptace oka** je schopnost přizpůsobit se různým intenzitám osvětlení. Vlastní dynamický rozsah adaptace oka je typicky  $0,25 - 10^5$  lx, což odpovídá prakticky rozsahu 6 řádů! Vnímání je schopno oko ještě při intenzitě osvětlení  $2 \cdot 10^{-9}$  lx. Budeme-li počítat s touto hodnotou, znamená to dynamický rozsah 14 řádů!

*Poznámka – Později uvidíme, že dosáhnout podobného dynamického rozsahu u kamery s řízeným objektivem je technicky velice náročné, ne-li nemožné.*

Takto vynikajících parametrů dosahuje oko dvěma mechanismy. První je jeho schopnost měnit průměr otvoru zornice v typickém rozmezí 1,8 – 7,5 mm, což odpovídá poměru ploch 1:17 až 1:20 s dobou reakce cca 370 ms, v ideálním případě až 100 ms.

*Poznámka – Srovnej s objektivem s řízenou clonou typu autoiris!*

Druhým mechanismem je schopnost fotoreceptorů měnit pomocí fotochemického děje citlivost.

*Poznámka – Srovnej se smyčkou automatického řízení citlivosti kamery (AGC).*

**Rychlost vnímání** neboli setrvačnost lidského oka je jednou z vlastností, která vůbec umožnila vznik kinematografie a později i televizní techniky. Typickým příkladem je vnímání atmosférického výboje o trvání řádově mikrosekundy, jenž vyvolá zrakový vjem trvající cca 0,3 s. Rychlost vnímání je závislá na celkovém jasu a na kontrastu jasů detailu a pozadí. Z těchto poznatků vychází tzv. Talbottův zákon určující frekvenci splývání. Jeho obsahem je tvrzení, že při periodické změně světelného podnětu (světelný tok, jas) je nad frekvencí splývání zrakový vjem stejný jako při světelném podnětu s intenzitou danou střední hodnotou intenzit periodického podnětu.

Matematicky platí pro frekvenci splývání tento empirický vztah:

$$f_s = a \cdot \log L_a + b$$

kde  $L_a$  je z intervalu 2 – 300 cd.m<sup>-2</sup>,  
 $a = 12$  Hz,  
 $b = 33$  Hz

**Zorné pole** je část prostoru ohraničená jak vertikálně, tak horizontálně, kterou může pozorovatel postřehnout upřeným pohledem bez zapojení očních svalů a pohybu hlavy.

Typické hodnoty odpovídají 8° horizontálně a 6° vertikálně. Největší ostrost se pohybuje v rozmezí 1,5°.

**Obhledové pole** je část prostoru, kterou může pozorovatel obsáhnout při zapojení očních svalů i pohybu hlavy.

**Rozlišovací schopnost** je schopnost oka zhodnotit jasnost odlišovaných detailů. Kritický detail je detail stejné barvy na stejném pozadí jiného jasu.

**Zraková ostrost** je schopnost oka rozeznat vůči danému pozadí dva blízké detaily. Normální oko odliší dva detaily vzdálené úhlově 1'. Tato rozlišovací schopnost je nejvyšší v centrální jamce a klesá ke krajům oka.

**Prostorové vidění** je stereoskopický mechanismus binokulárního vidění. Je velice individuální. Typické hodnoty odlišení vzdálenosti dvou předmětů jsou uvedeny v tab. 5-2.

Tabulka 5-2: Hodnoty rozpoznání odlišné vzdálenosti dvou předmětů

Celková vzdálenost (m)	Vzdálenost mezi dvěma předměty (m)
1 000	275
100	3,7
10	0,04
1	0,004

*Poznámka – Tato vlastnost vidění není v TV technice zatím využita. Dvojměrný obraz vnímá lidské oko na základě zkušenosti jako prostorový. Různé pokusy o zprostředkování stereoskopického obrazu zatím nedošly velkého rozšíření. Snad jen v oblasti počítačových her a virtuální reality se taková zařízení – většinou v podobě polarizačních či barevně filtrujících brýlí objevují.*

## 1.2 Základní parametry přenosových soustav televize

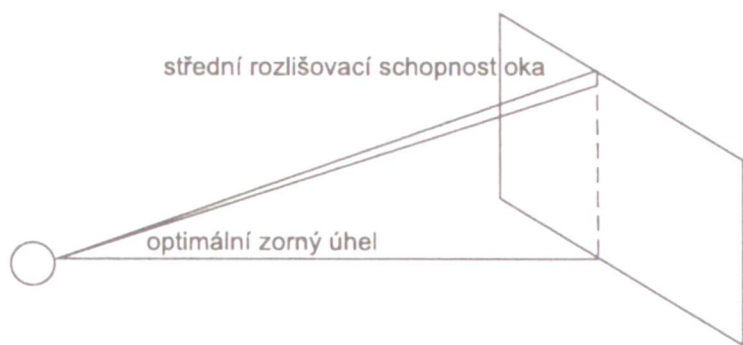
V současné době lze nalézt ve světě řadu TV standardů. Přes jejich konkrétní odlišnosti vycházejí všechny z několika základních myšlenek, které v minulosti umožnily vznik a rozvoj snímání, přenosu a zobrazování obrazu elektronickou cestou.

Tyto základní principy lze shrnout do hesel:

- fyziologická podstata vidění
- princip řádkového rozkladu
- opakování obrazů
- oddělený přenos barvy a jasu (u barevných systémů).

Se znalostí základů fyziologie lidského zraku můžeme přistoupit k odvození základních parametrů TV systémů.

Vydeme-li tedy ze střední rozlišovací schopnosti oka 1' a optimálního zorného úhlu pro přímé vidění cca 10°, lze stanovit optimální počet řádků obrazu. Z optimálního zorného úhlu pro přímé vidění v horizontálním i vertikálním směru vychází rovněž stanovení poměru stran obrazu v TV soustavě. Na obr. 5-2 je vidět grafické a matematické odvození optimálního počtu řádků. Ve skutečnosti „nekulatá“ čísla vycházejí z možností kmitočtových děličů a násobičů používaných v raných dobách televize v synchronizačních generátorech.



$$\text{optimální počet řádků} = \frac{\text{optimální zorný úhel}}{\text{střední rozlišovací schopnost oka}} = \frac{10'}{1'}$$

Obr. 5-2: Odvození optimálního počtu řádků TV soustavy.

Z frekvence splývání  $f_s = 50 \text{ Hz}$  pro zrakový vjem bez blikání vychází stanovení minimálního počtu obrazů za sekundu. V začátcích televize byla zařízení pro rozklad obrazu vybavena synchronními síťovými motory (Nipkowův kotouč, Weillerovo zrcadlo, filmový snímač); odtud vychází obrazový kmitočet stejný jako kmitočet sítě. Ve své době to mělo kromě jiného i výhodu ukrytí brumových pásů, vznikajících nedokonalostí technologie, do zatemňovacího intervalu.

Snímkový kmitočet 50 Hz ve spojení s počtem řádků 625 zabírá v kmitočtové oblasti šířku pásma 13 MHz. To bylo pro další rozvoj s ohledem na úsporu energetického spektra, technologii a cenu TV vysílačů nepřijatelné. Pomocí geniálního triku (F. Schröter 1927) se zmenšily nároky na šířku pásma na polovinu. Tento trik spočíval v zavedení prokládaného řádkování. Snímek byl rozdělen na dva půlsnímky. V prvním půlsnímku se přenášely řádky liché a v druhém řádky sudé. Celkový počet „obrázků“ (v tomto případě již půlsnímků) za sekundu byl zachován (z důvodů hranice blikání) a počet snímků za sekundu klesl na 1/2.

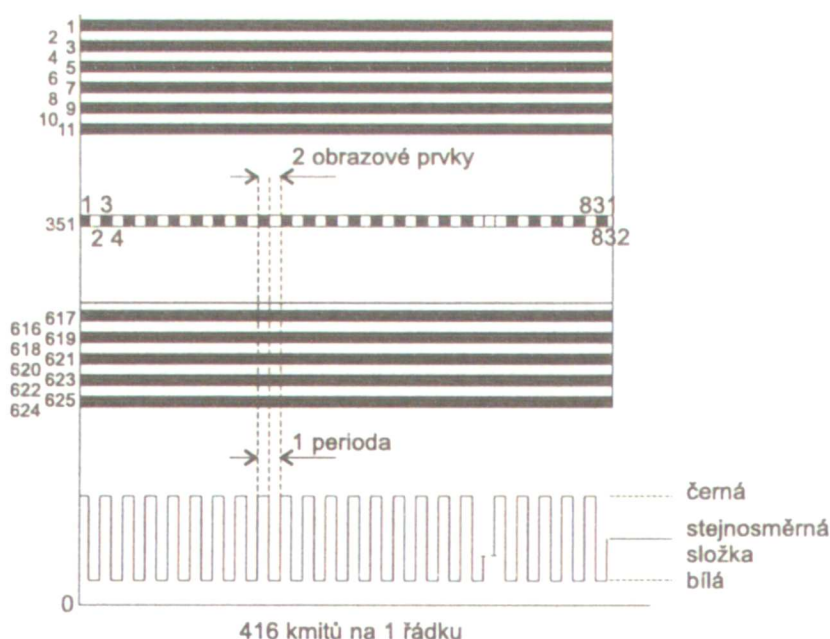
Budeme-li se nadále zabývat pouze normou CCIR, vypadá popsaná operace matematicky takto:

počet řádků úplného TV snímku:	625
počet řádků TV půlsnímku:	312,5
počet půlsnímků přenesených za sekundu:	50

Ze znalosti uvedených parametrů lze odvodit počet řádků přenesených za sekundu:  $50 \times 625 \times 1/2 = 15\,625$ .

Řádkový kmitočet u normy CCIR je tedy 15 625 Hz.

Teoretickou mezní rozlišovací schopnost systému CCIR lze odvodit z počtu řádků a stanoveného formátu obrazu 4:3. Na obr. 5-3 je názorně vidět grafickou konstrukci obrazu s maximální rozlišovací schopností.



Obr. 5-3: Principiální znázornění maximální rozlišovací schopnosti systému.

Pro stejnou rozlišovací schopnost ve vertikálním i horizontálním směru by bylo nutné podél řádku vytvořit

$$4/3 \times 625 = 832$$

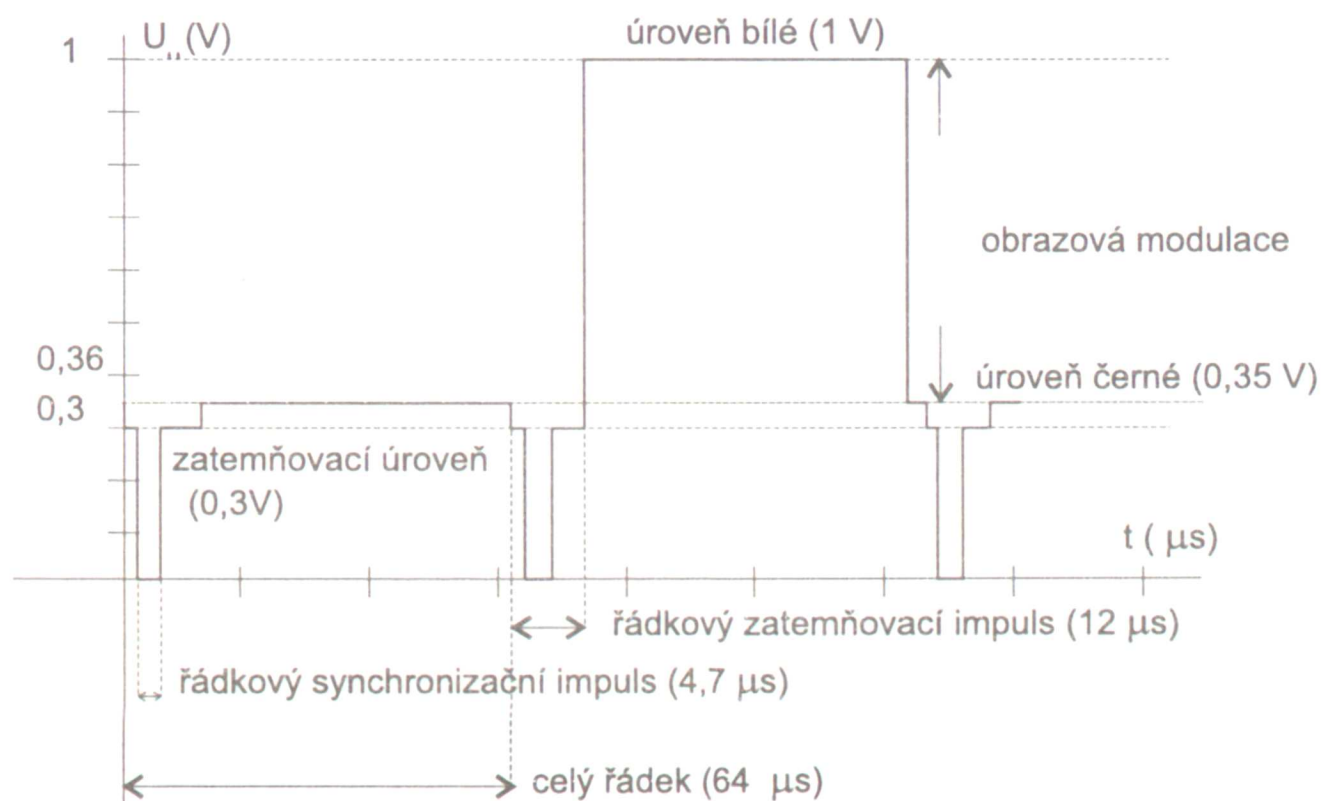
obrazových bodů. To odpovídá 416 periodám střídavého signálu v rozkmitu černá - bílá podél řádku.

Odtud lze odvodit požadovanou šířku pásma pro přenos s maximální rozlišovací schopností:  $50 \times 625 \times 1/2 \times 416 = 6\,500\,000$

Potřebná šíře pásma pro nezkreslený obraz s plnou rozlišovací schopností je tedy 6,5 MHz. V praxi je šíře přenosového kanálu jasového signálu omezena do 5,5 MHz.

Pro potřeby průmyslové televize však v případě přenosu v základním pásmu (bez namodulování na vyšší kmitočty) není nutné pásmo nijak uměle omezovat, neboť nejde o sdílení elektromagnetického spektra s jinými přenosovými kanály, jako je tomu při vysílání TV signálu, a hlavně spektrum videosignálu ze zdrojů používaných v CCTV je užší.

Kromě uvedených základních parametrů musí z hlediska kompatibility zařízení průmyslové televize od různých výrobců být standardizovány ještě další parametry signálu. Mezi tyto patří časové a úrovně rozložení signálu podél řádku. Normalizované hodnoty jsou uvedeny na obr. 5-4.



Obr. 5-4: Úrovnňový diagram videosignálu v závislosti na čase.

V tab. 5-3 jsou uvedeny hlavní parametry nejužívanějších světových TV standardů. Zvýrazněný je standard (CCIR) užívaný v oblasti průmyslové televize v Evropě. To znamená, že všechna zařízení (i dovážená z USA či Japonska) by měla z hlediska vzájemné kompatibility funkce v jednom systému odpovídat standardu CCIR.

Tabulka 5-3: Standardy používané pro přenosové soustavy televize

Standard	B/G (CCIR)	D/K (OIRT)	M (FCC)	I (Velká Británie)	A (Velká Británie)	L (Francie)	E (Francie)
počet řádků na snímek	625	625	525	625	405	625	819
pulsníkový kmitočet (Hz)	50	50	60	50	50	50	50
řádkový kmitočet (Hz)	15 625	15 625	15 750	15 625	10 125	15 625	20 475
trvání řádkového synchronizačního pulsu (us)	4,7	4,7	5	4,7	8...10	4,7	2,5
trvání řádkového zatemňovacího pulsu (us)	12	12	10,8	12	18	12	9,5
doba přední prodlevy (us)	1,5	1,5	1,9	1,5	1,75	1,5	1,1
snímkový zatemňovací puls (počet řádek)	25	25	19...21	25	13...15,5	25	33
šířka pásma videosignálu (MHz)	5	6	4,2	5,5	3	6	10
šířka VF kanálu (MHz)	7(B) / 8 (G)	8	6	8	5	8	14
šířka postranního pásma (MHz)	0,75	0,75	0,75	1,25	0,75	1,25	2
odstup nosné obrazu od počátku pásma (MHz)	1,25	1,25	1,25	1,25	3,75	1,25	2,83
odstup zvuk/obraz (MHz)	5,5	6,5	4,5	6	-3,5	+/-6,5	+/-11,15
VF úroveň synchronizace (%)	100	100	100	100	3	6	3
VF úroveň zatemňování (%)	73	75	75	73	30	30	30
VF úroveň bílé (%)	10	12,5	10	10	100	100	100
modulace obrazu	C3F neg.	C3F neg.	C3F neg.	C3F neg.	C3F pos.	C3F pos.	C3F pos.
modulace zvuku	F3E, F3EH	F3E	F3E	F3E	A3E	A3E	A3E
frekvence zdvih (kHz)	+/-50 kHz	+/-50 kHz	+/- 25	+/-50 kHz	-	-	-
preemfáze (us)	50	50	75	50	-	-	-
výkonový poměr obraz / zvuk (-)	10:1	10:1...5:1	10:1 ...5:1	10:1	4:1	10:1	10:1

Bez ohledu na použitý typ normy byly postupně vyvinuty tři základní systémy pro přenos barevného signálu:

- NTSC (National Television System Committee) USA 1954
- SECAM (Sequentiel á memoire ) Francie 1957
- PAL (Phase Alternatin Line) SRN 1961

Jasový signál je z důvodu kompatibility se stávajícími černobílými systémy zachován v nezměněné podobě. Tři barevné výtažky jsou (se zúženou šířkou pásma) přenášeny v podobě rozdílových signálů spolu s jasovou složkou. Pro zachování úplného informačního obsahu stačí přenášet dvě rozdílové složky a třetí je možné při využití matematických poznatků vektorové algebry zrekonstruovat na straně přijímače.

Oběma rozdílovými složkami je v systému NTSC současně amplitudově modulována barvonosná vlna. U systému PAL jde o kvadrurní modulaci jedné barvonosné vlny, u systému SECAM je rozdílovými složkami postupně frekvenčně modulována pomocná nosná frekvence barvy.

Pro barevnou CCTV se v Evropě užívá systém PAL.

*Poznámka – Uvedené informace slouží k oživení znalostí o základech TV techniky. Případné zájemce o hlubší teoretické informace o přenosových parametrech a soustavách jak černobílé, tak barevné televize lze odkázat na literaturu uvedenou na konci kapitoly.*

Dodržování mezinárodních standardů je nezbytné především z těchto důvodů:

- mezinárodní výměna programů
- vývoj TV vysílačů, převaděčů a satelitní techniky
- výroba TV přijímačů satelitních přijímačů



- vybavení videomagnetofonů
- projektování měřicích přístrojů a systémů
- návrh a výroba prvků systémů průmyslové televize.

## 2. Stručný přehled vývoje snímací techniky v datech

1878

První záznamy o pokusech přenést obraz elektronickou cestou. Šlo o pokusy s telegrafickým přenosem obrazu.

1881

První dokumentovaný přenos obrazu elektrickou cestou se uskutečnil v Londýně.

1884

Patent **Nipkowova kotouče**. Paul Nipkow (Američan polského původu) vynalezl princip řádkového rozkladu používaného v TV technice dodnes.

1934

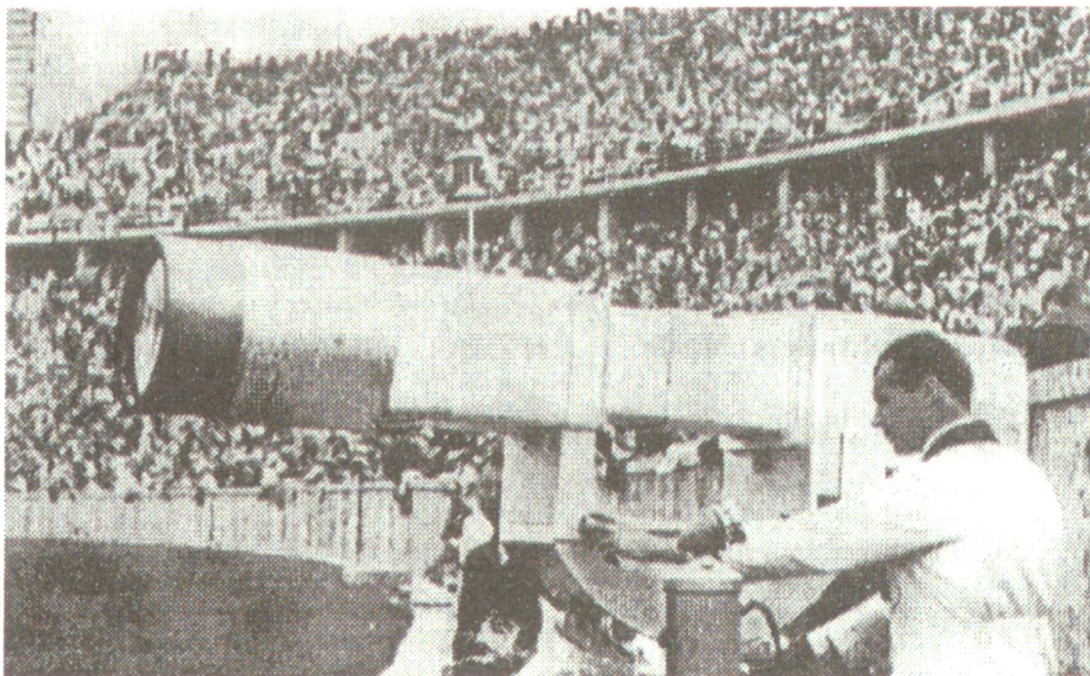
V. N. Zvorykin (Američan ruského původu) – vynález snímací elektronky **Ikonoskop**.

1936

V pondělí 2. listopadu v 15.30 hod. zahájila stanice BBC pravidelné televizní vysílání. Sledovalo je 300 prvních majitelů TV přijímačů.

1940

Zdokonalení snímací elektronky **Ikonoskop** na nový typ s názvem **Super-ikonoskop** s životností řádově stovky hodin.



Obr. 5-5: TV kamera s ikonoskopem (Olympijské hry Berlín 1936).

### 1941

První průmyslově vyrobená kamera se superikonoskopem pro střežicí účely.

Technicko-ekonomické parametry:

- citlivost: 50 lx,
- optika: 2,8/35 mm,
- rozměry: 200 x 200 x 400 (mm) cena: 32 tis. RM (odpovídá dnešní kupní síle cca 350 tis. DM).

Pro další vývoj se ukázaly jako důležité tyto parametry snímacích elektronek:

- malá setrvačnost odezvy na pohyb ve snímaném obraze,
- lineární převodní charakteristika,
- nízký proud za tmy – nízká úroveň rušivých signálů,
- dostatečná rozlišovací schopnost,
- vyhovující spektrální citlivost,
- prodloužení životnosti.

### polovina 50. let

Varianty **Image-ortikon**, **Super-ortikon**. Pro své velké rozměry nenašly v CCTV využití. Až šedesátá léta díky masovému rozvoji tranzistorové techniky umožnila vyrábět kamery akceptovatelné v CCTV jak rozměry, tak cenou.

### polovina 60. let

Objevuje se zdokonalená snímací elektronka **Vidikon** (RCA). Citlivou vrstvu tvoří sirič antimonitý  $Sb_2S_3$ . Cenově relativně dostupná snímací elektronka i pro aplikace v CCTV, dobrá rozlišovací schopnost, při slabém osvětlení vysoký proud za tmy, silný závoj u pohybujících se objektů, citlivá na vypalování, životnost 1,5 roku, ale při slabém osvětlení jen několik měsíců.

**Plumbikon** (Philips) s citlivou vrstvou tvořenou oxidem olovnatým PbO je další v řadě pokusů o vylepšení technických parametrů dosavadních snímacích elektronek. Je určena především pro profesionální použití, má vysokou citlivost, minimální závoj, nepatrný proud za tmy, cena je 2,5x nižší než u konkurenčního Newiconu. V CCTV se užívala jen pro speciální účely.

### 1967

První pokusy vytvořit citlivou vrstvu z mozaiky jednotlivých Si diod. Tato elektronka s akumulací elektrodou měla své klady – vysokou citlivost, dlouhou životnost, odolnost na přesvětlení, vysokou citlivost v IR oblasti, nižší setrvačnost než klasický vidikon. Měla však i své nevýhody – vysoký proud za tmy a možnost vzniku skvrn v obraze při výpadku některých prvků matice. V oblasti CCTV se používaly ovšem výhradně s objektivy a řízenou clonou.

### 1972

Vyvinuta elektronka s akumulací elektrodou tvořenou heterogenním přechodem PN s názvem **Chalnicon** (Toshiba)

1973

Vyvinuta elektronka s akumulací elektrodou tvořenou amorfním selenem s názvem **Satikon** (Hitachi)

1974

Konkurent Vidikonu - elektronka **Newicon** (Matsushita) byla ve světě cenově cca 5x výhodnější (u nás však v době své aplikace v CCTV 10x dražší - roku 1981 Vidikon 700 Kčs, Newicon 7000 Kčs), má 10x vyšší citlivost, je vhodná pro venkovní aplikace pouze s objektivem s řízenou clonou, spektrální citlivost sahá až do oblasti blízké infračervenému záření, méně citlivá na vypalování, životnost dva roky.

80. léta

Počátek vývoje CCD obrazového snímáčiho prvku. (CCD zkratka z anglického názvu Charge Coupled Device, jež vyjadřuje podstatu tohoto prvku. Česky - nábojově vázaná struktura).

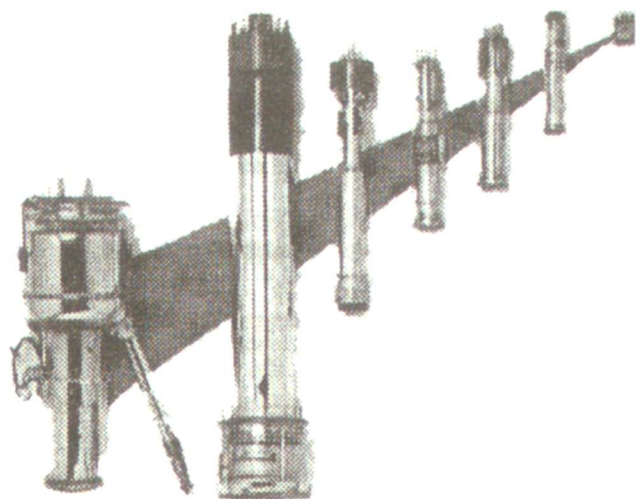
Co si firmy, které stály u zrodu CCD prvku, od vývoje slibovaly?

- miniaturizaci
- dlouhou životnost
- vysokou citlivost
- nízké výrobní i provozní náklady.

1985

Tento rok znamenal uvedením první komerční CCD kamery na trh absolutní převrat ve vývoji obrazových snímáčiho prvků a svými přednostmi umožnil kromě jiného i rozvoj oboru CCTV. Náročnost technologie výroby CCD prvků dokazuje fakt, že do dnešní doby se výrobou CCD snímáčiho prvků zabývá jen několik málo špičkových technologických firem především v Japonsku (SONY, Fuji, Hitachi, NEC, Toshiba, Sharp), v USA (RCA, General Electric, Tektronix, Texas Instruments) v Evropě (Philips, Valvo, Thomson, CDS, EEV).

*Poznámka – V této kapitole byly uvedeny hlavní mezníky s důrazem na snímáčiho techniku, což je stěžejní prvek CCTV, která za dobu existence TV techniky udělala patrně největší pokrok. Podobně bouřlivý vývoj bychom mohli zaznamenat v oboru*



Obr. 5-6: Vývoj rozměrů snímáčiho prvků.

*záznamové techniky, pouze časový interval by byl kratší. U reprodukční techniky, tedy monitorů, se neobjevil za dobu existence TV techniky žádný převrat. Přes všechna technická vylepšení a progresivní obvodová řešení řídicích obvodů monitorů (či TV přijímačů) nejužívanějším zobrazovacím prvkem zůstala vakuová elektronka – TV obrazovka, která v roce 1997 oslavila 100 let od svého vynalezení. Použití zobrazovacích prvků na bázi LCD displejů, které bylo doménou přenosných počítačů a kapesních TV přijímačů se postupně začíná prosazovat i v oboru CCTV.*

*Nové princípy zobrazovacích zařízení jako např. plazmový zobrazovač zůstává zatím v oblasti komerčních TV přijímačů.*

### **3. Snímání obrazu – CCD kamera**

Scéna v zorném poli objektivu je opticky transformována do roviny světlocitlivé plochy snímacího prvku a musí být převedena na elektrický signál. Tento převod se uskutečňuje v polovodičové struktuře CCD čipu. Dříve se využívaly pro tuto úlohu snímací elektronky. CCD kamery téměř vytlačily svými technickými i ekonomickými parametry z trhu CCTV kamery se snímacími elektronkami. Existují však určité speciální aplikace, které zůstávají dodnes jejich doménou. Sem je možné zařadit primární zónu jaderných elektráren, kde běžná CCD kamera má díky úrovni okolní radiace životnost sníženou prakticky na 1 rok! Další aplikací je snímání za extrémně nízkých úrovni osvětlení (ve zbytkovém světle). Zde dominují snímací elektronky typu SIT a ISIT, které vykazují oproti CCD především vyšší rozlišovací schopnost, vyšší citlivost a lepší poměr signál/šum.

V běžných aplikacích CCD kamera přináší oproti kamerám se snímacími elektronkami tyto výhody:

- zcela vyhovuje pro všechny bezpečnostní a kontrolní aplikace,
- vysoká životnost a spolehlivost v trvalém provozu,
- nízké provozní náklady,
- vysoká stálost optických a elektrických parametrů,
- vyloučení rizika vypálení či poškození při přesvětlení,
- snímání pohyblivých objektů bez závoje,
- nepřítomnost geometrických zkreslení,
- odolnost proti magnetickému a elektrickému poli,
- vysoká odolnost proti vibracím a rázům,
- dobrá citlivost v oblasti blízkého infraspéktra.

Kritériem volby konkrétního typu CCD kamery jsou dva základní parametry – rozlišovací schopnost a citlivost kamery. Tyto dva parametry (vedle kvality zobrazení na monitoru) nejvíce ovlivňují hodnocení kvality systému subjektivně vnímané zákazníkem.

#### **3.1 Princip snímání CCD čipem**

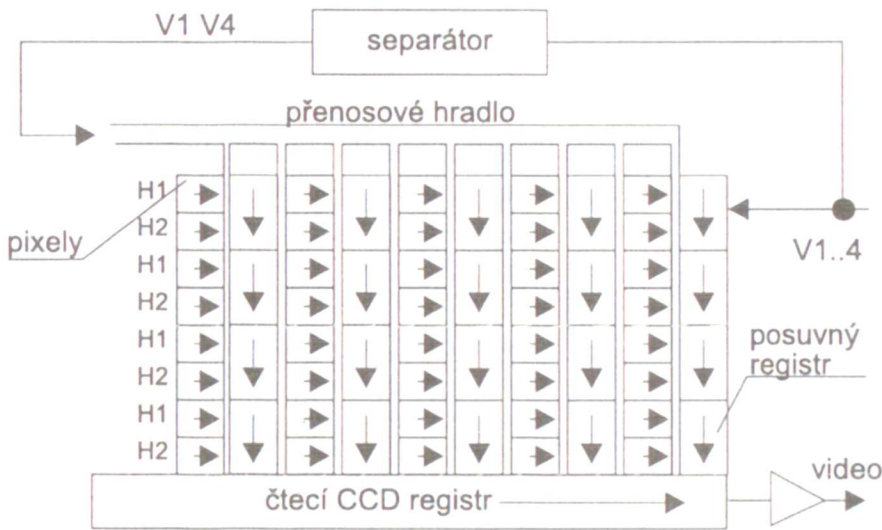
Dominující technologií výroby čipů CCD pro kamery CCTV je IT (interline-transfer image sensor).

Organizace čipu je patrná z obr. 5-6. Čip CCD IT obsahuje sloupcově organizované světlocitlivé elementy (pixely), jež slouží zároveň jako integrační prvky k akumulaci světlem vyvolaného náboje. Každý sloupec je spojen s vertikálně orientovaným posuvným registrem pomocí přenosového hradla (transfergate). Vertikálně orientovaný posuvný registr je řízen čtyřtaktím pulsem (V1 až 4). Počet CCD buněk v posuvném registru je stejný jako počet řádků v jednom pulsnímku, což je polovina počtu světlocitlivých elementů v jednom sloupci. Buňky posuvného registru jsou přiřazeny ke dvěma různým pulsnímkům (H1, H2). Vhodnou volbou napětí na příslušných elektrodách v jednotlivých fázích taktu řídicího vertikální CCD registr je umožněno vyčítání obrazu do horizontálního čtecího CCD registru. Spojením sekvenčních obrazových signálů na výstupní struktuře CCD čipu se vytváří z pulsnímků obrazový signál. Technologicky je CCD IT čip výhodný

redukci počtu buněk vertikálního posuvného registru na polovinu oproti počtu světlocitlivých buněk.

### 3.2 Formát čip

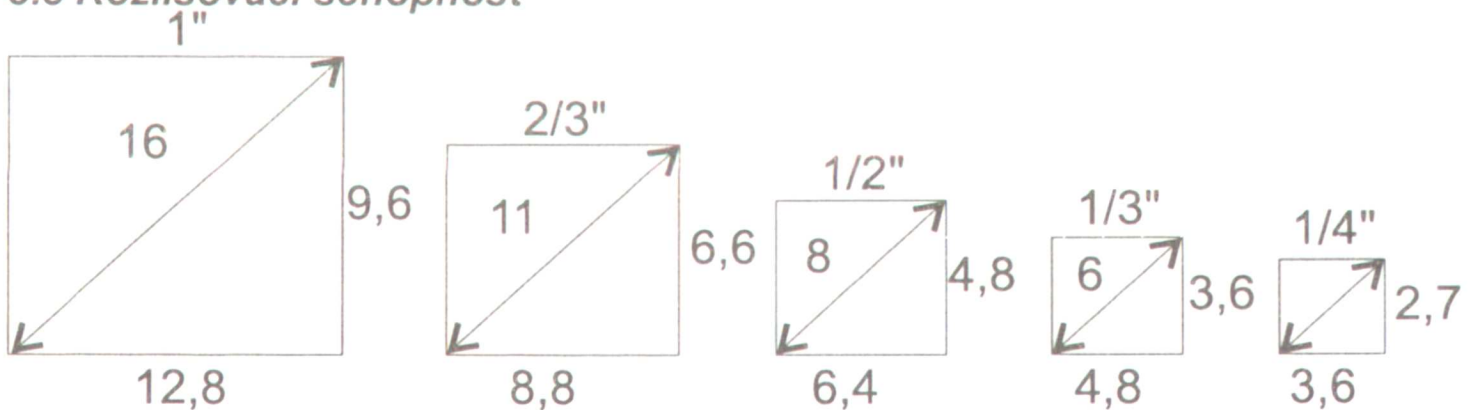
Souvisí s úrovní technologie výroby čipů jednotlivých výrobců. Konečná hodnota je



Obr. 5-7: Organizace čipu CCD – IT.

zřejmě na formátu 1/4". Je to dáno neúprosnými zákony optiky – čím menší čip, tím potřebujeme pro stejnou velikost zorného pole menší ohniskovou vzdálenost ( $f$ ) použitého objektivu. Tím se však začnou více projevovat optické nedostatky levnějších objektivů a dochází ke geometrickému i barevnému zkreslení kvůli odlišnému lomu světla jednotlivých spektrálních složek. Vyrobít kvalitní objektiv s malou ohniskovou vzdáleností je totiž náročnější a objektiv je dražší. Tím je efekt použití levnější kamery s menším čipem eliminován nutností použít dražší objektiv pro stejnou kvalitu zobrazení jako u kamery dražší, s větším čipem a levnějším objektivem. Nejrozšířenější je dnes formát 1/3".

### 3.3 Rozlišovací schopnost



Obr. 5-8: Vývojová řada formátů CCD čipů (rozměry jsou v mm).

Rozlišovací schopnost je hranice ostrosti snímané scény. Přitom je nutné vzít v úvahu, kolik řádků je v horizontálním směru kamera schopna ještě sejmout. Rozlišovací schopnost je závislá na počtu aktivních obrazových bodů snímacího čipu CCD (pixel), méně závislá na jeho formátu.

Je tedy dána konstrukcí CCD čipu, a dále kvalitou zpracování videosignálu v kameře. Udává se v počtu TV řádek nebo alternativně v počtech obrazových prvků (pixelech) snímacího prvku. Technicko-ekonomická hranice se posunula pro oblast běžných aplikací na 570 ř. u čb a 480 ř. u barevné kamery. Technicky je zde s ohledem na používaný standard CCIR ještě rezerva až do teoreticky maximální rozlišovací schopnosti dané normou, a to je 767 ř. (počítáno pro skutečně viditelnou část snímku).

U kamer CCTV platí pro rozlišovací schopnost z hlediska aplikace dále uvedená kritéria:

Rozlišovací schopnost čb kamer 370 – 380 řádků je používána u nenáročných aplikací, ve kterých mají být pro blízké a střední vzdálenosti objekty a osoby dobře rozlišitelné. U barevných kamer těmto aplikacím odpovídá rozlišovací schopnost 320 – 330 řádků.

Rozlišovací schopnost čb kamer 560 – 580 řádků je perspektivní pro všechny běžné aplikace a nezbytná všude tam, kde se požaduje vysoké rozlišení detailů v rámci snímání scény. Doporučuje se v případě dalšího digitálního zpracování obrazu. U barevných kamer těmto aplikacím odpovídá rozlišovací schopnost 460 – 480 řádků.

*Poznámka – Zde je nutné si uvědomit, že daným požadavkům musí vyhovovat všechny prvky konkrétního videořetězce. I nejslabší článek řetězce musí mít přinejmenším rozlišovací schopnost, jež je požadována. Tímto nejslabším článkem řetězce bývá zpravidla záznamové zařízení – je-li užit analogový videomagnetofon.*

Rozdíl rozlišovací schopnosti čb a barevných kamer CCTV je dán odlišným provedením snímacího systému.

Subjektivní vnímání ovlivňují vlastnosti lidského oka. Pozorovatel vyhodnotí při stejné rozlišovací schopnosti vždy jako lepší obraz barevný.

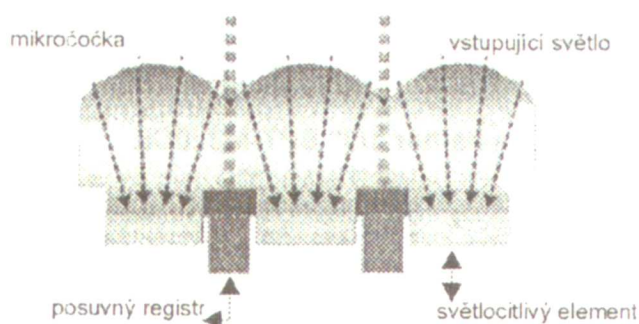
### 3.4 Citlivost

V technických specifikacích kamer je uvedeno minimální osvětlení v luxech (lx). Při této hodnotě intenzity osvětlení je na výstupu kamery signál o amplitudě rovné 50 % jmenovité hodnoty. Toto osvětlení odpovídá hodnotě intenzity světla odraženého od snímaného objektu, měřeného na objektivu kamery.

*Poznámka - intenzitou osvětlení není intenzita osvětlení scény ale intenzita osvětlené odražená do kamery měřená v rovině objektivu!*

Stěžejní parametry byly průběžně zlepšovány v posledním desetiletí u čb kamer od úrovně citlivosti okolo 1 lx/F1,2 na hodnoty okolo 0,1 lx/F1,2 a u barevných od hodnot okolo 4 lx/F1,2 na dnešních 0,8 lx/F1,2 u běžných CCTV kamer a u speciálních řešení čipů (např. Exwavehad, Hyperhad - SONY) až na 0,04 lx/F1,2 u čb a 0,4 lx/F1,2 u barevných kamer.

Tabulka č. 5-4 ilustruje vliv clonového čísla objektivu na citlivost kamery s objektivem. Je možné ji použít pro přepočítání citlivosti



Obr. 5-9: Kamera a řešení čipu ExwaveHAD.

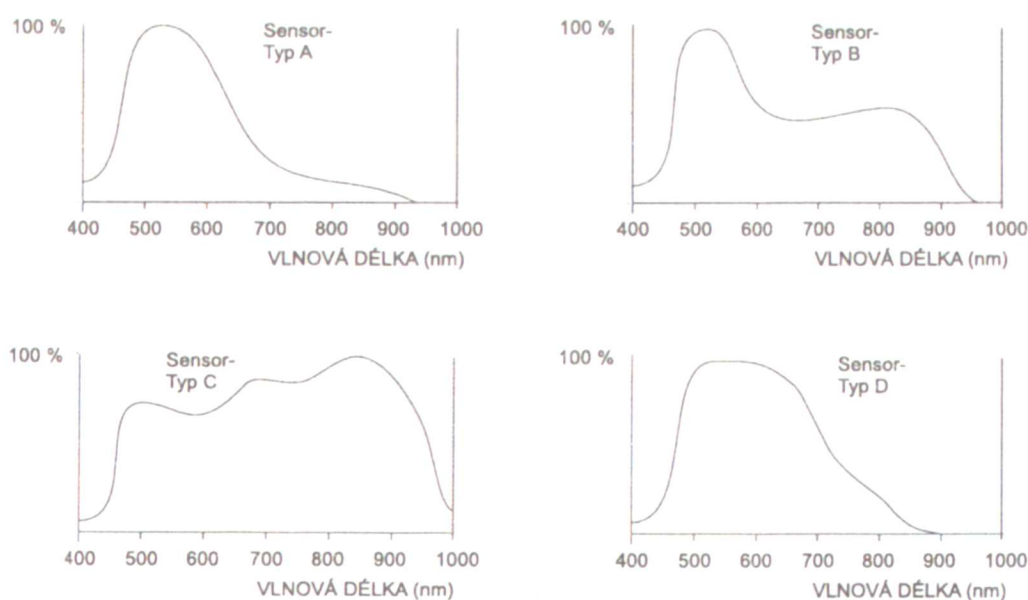
kamery s objektivem o jiné světelnosti, než je uvedeno v technické specifikaci, což nám udává prakticky minimální ještě použitelnou intenzitu osvětlení měřenou na kameře. Zde je třeba mít se na pozoru před kouzlením s čísly, neboť uvedená čísla mohou být podezřele pozitivní. Někteří výrobci neuvádějí totiž ve svých technických specifikacích podmínky, za kterých byla citlivost měřena, a tím o uvedené hodnotě říci, zda je parametr skutečně tak dobrý, jak to na první pohled ve specifikaci vypadá.

Tabulka 5-4: Citlivost kamery s objektivem daného clonového čísla

Clona	na	F 0,95	F 1,4	F 2,0	F 2,8	F 4,0	F 5,6	F 8,0
	čipu							
relativní otvor	-	1:0,95	1:1,4	1:2,0	1:2,8	1:4,0	1:5,6	1:8
multiplikační faktor	0,1	0,5	1	2	4	8	16	32
minimální osvětlení (lx) (typická černá kamera)	0,03	0,15	0,3	0,6	1,2	2,4	4,8	9,6
minimální osvětlení (lx) (typická barevná kamera)	0,15	0,75	1,5	3	6	12	24	48

Při nasazení kamer ve venkovním prostředí jsou požadavky na citlivost podstatným kritériem volby typu kamery a připojeného objektivu především v případech použití za nízké úrovně osvětlení snímané scény.

Specifickým problémem je nasazení kamer pro noční snímání spolu s infraflektory. V běžných technických popisech kamer není údaj o citlivosti v IR spektru uváděn. Neexistuje žádný technický předpis či norma, které by uváděly konkrétní kritérium pro přímé srovnání citlivosti kamer v IR spektru. Jedinou možností je tedy prakticky ověřit společný provoz dané kamery a daného infraflektoru dříve, než soupravu do systému navrhne a instalujeme. Důležitá je zde i volba správného objektivu. Použití běžného objektivu nekorigovaného v IR pásmu může přinést rozčarování a totální neúspěch. Na obr. 5-10 jsou průběhy citlivosti pro čtyři varianty technologického provedení CCD čipů.



Obr. 5-10: Grafy relativní spektrální citlivosti pro CCD čipy.

Tabulka 5-5: Typické hodnoty intenzity osvětlení ve venkovním prostředí a v interiéru.

Přirozené světlo		
		intenzita osvětlení
sluneční svit při jasné obloze	v červenci v poledne	100 000 lx
	v prosinci v poledne	9 000 lx
denní světlo při zatažené obloze	v červenci v poledne	20 000 lx
	v prosinci v poledne	2 000 lx
Umělé osvětlení		
hlavní ulice ve velkých městech		7,5 - 30 lx
ulice, skladovací plochy		1 - 7,5 lx
vedlejší ulice		0,5 - 1,5 lx
schodiště, nástupiště		7,5 - 15 lx
Pracovní osvětlení		
hrubá práce		40 - 60 lx
střední jemná práce		80 - 120 lx
jemná práce		150 - 250 lx
velmi jemná práce		300 - 600 lx

### 3.5 Odstup signál/šum (S/N - signal/noise)

Každý elektronický obvod pracující při teplotě vyšší, než je teplota odpovídající absolutní nule (-273 °C) je zdrojem šumového napětí. Toto šumové napětí se superponuje na užitečný signál a při zpracování videosignálu se nám projeví jako „zrnitost“ nebo „sníh“ na obrazovce. Vedle tohoto teplotního šumu se mohou v obraze projevit další externí interference – například z kabelů elektrického vedení nebo počítačových kabelů, které mohou obraz znehodnotit. Odstup S/N reflektuje pouze interní zdroje šumu.

Pod určitou úrovní intenzity osvětlení se začne počet elektronů produkovaných v důsledku světelných impulsů vyrovnávat s počtem elektronů produkovaných jinými zdroji. Tyto jiné elektrony si elektronika kamery interpretuje jako platné signály a v důsledku toho začne na obraze vznikat interference – zpočátku jako zrnitost obrazu. Když úroveň světla dále klesá, zrnitost se zvyšuje a na obraze se projeví jako sněžení. Nakonec, když kamera dosáhne mezí své funkčnosti, začne sníh „padat“ tak hustě, že je výsledný obraz zcela nepoužitelný.

Účinky šumu na obrazovce závisí na poměru hladiny šumu k hladině videosignálu

Odstup signál/šum je uváděn v dB:

$$B = 20 \times \log (\text{videosignál/signál šumu}) \text{ (dB)}$$

U většiny běžných kamer nebude odstup S/N větší než 60 dB, tj. v poměru 1000:1. To znamená, že signál je tisíckrát větší než šum, a při tomto poměru je šum neznatelný. Následující pravidla interpretují některé poměry signálu k šumu vzhledem k subjektivní kvalitě obrazu (viz tab. 5-6).



Tabulka 5-6: Kvality obrazu v závislosti na odstupu signál/šum

Odstup S/N (v dB)	Poměr užitečného a šumového signálu	Popis kvality obrazu
60 dB	1000:1	Kvalita obrazu výborná, není znatelný žádný šum
50 dB	316:1	Malý objem šumu, ale kvalita obrazu je dobrá
40 dB	100:1	Na obrazu je jemné zrnění nebo sníh, ztrácejí se jemné detaily
30 dB	32:1	Špatný obraz s velkým množstvím šumu
20 dB	10:1	Nepoužitelný obra

### 3.6 Synchronizace

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

#### 3.6.1 Interní synchronizace

Nejlevnější typy kamer mají pouze interní synchronizaci. To znamená, že kamera obsahuje ve své elektronické části stabilní oscilátor, od něhož se odvozují všechny časové signály v tolerancích daných příslušnou TV normou (v našem případě CCIR a u barevných kamer CCIR a PAL). Vzhledem k tolerancím jednotlivých oscilátorů nelze v systému žádným způsobem zajistit synchronizaci s ostatními kamerami. Jsou-li takovéto kamery připojeny k analogovému zařízení (např. běžný sekvenční přepínač, ale i křížové přepojovací pole), dochází při přepnutí z jedné kamery na druhou k vyrovnávání fáze nesynchronních signálů, a tím k „poskočení obrazu“ obvykle o jeden pulsnímek. Tento jev je zvýrazněn v případě záznamu na videorekordér a výsledkem je záznam s výpadky obrazu na malý časový okamžik po přepnutí kamer.

V případě aplikace takovýchto kamer spolu se zařízením na zpracování signálu vybaveným obvodem korekce časové základny (TBC) se problém neprojeví. Tedy kamery s interní synchronizací je možné použít pouze u autonomních systémů kamera – monitor, popř. kamera – videorekordér – monitor, nebo u multiplexních systémů založených na digitalizaci obrazu a zpětném převodu do analogové podoby.

#### 3.6.2 Externí synchronizace

Je to běžný způsob založený na existenci jediného referenčního zdroje synchronizačního signálu a rozvedení tohoto signálu ke všem kamerám v systému zapojeným. Běžně se používá ve studiové technice. V oblasti CCTV prakticky nenalézá uplatnění vzhledem k nárokům na zdvojenou kabeláž, nutnosti použít relativně dražší komponenty a obtížnému sfázování synchronizace všech kamer při oživování danému rozdílnými délkami kabelů. Aplikovatelný je tento způsob synchronizace v některých poloprofesionálních aplikacích (pro sledování laboratorních procesů apod.).

### 3.6.3 Synchronizace od napájecí sítě (linelock)

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

### 3.7 Napájení kamer

Napájení do značné míry souvisí se synchronizací popsanou v předcházejícím od-  
díle. Obecně existují čtyři varianty napájení:

- stejnosměrné napájení (nejčastěji 12 V ss z externího zdroje)
- střídavé nízkovoltové napájení (většinou 16 – 24 V st)
- střídavé napájení ze sítě (230 V st)
- napájení po koaxiálním kabelu ze speciální napájecí jednotky či připojeného systémového monitoru.

### 3.8 Připojení objektivu

Jde o velice důležitý parametr kamery, neboť na trhu objektivů existují dva standardy připojení:

- **C-mount** normalizovaný odstup roviny čipu od roviny zadní čočky objektivu 17,526 mm (0,69').
- **CS-mount** normalizovaný odstup roviny čipu od roviny zadní čočky objektivu 12,497 mm (0,492').

Některé kamery jsou proto vybaveny přestavitelnou kulisou CCD čipu. Umožňují připojit objektiv libovolného standardu a jemně dostavit jeho správnou polohu. U kamer v provedení CS je možné pro připojení objektivů provedení C použít mezikroužek prodlužující závit o 5 mm. Druhá varianta je využití standardu CS a připojení objektivů typu C pomocí adaptéru C-CS (mezikroužek o tloušťce 5 mm).

### 3.9 Řídicí výstupy kamery

Opět jde o důležitou funkci. V některých případech potřebujeme ke kameře připojit objektiv s řízenou clonou. Existují dva typy řízení:

- řízení videosignálem (AI),
- řízení stejnosměrným napětím (DC).

Z hlediska návrhu, montáže i servisu je vhodné používat kamery, které jsou vybaveny oběma řídicími výstupy. Užití DC objektivů má i svůj ekonomický aspekt, neboť tyto objektivy jsou zpravidla levnější.

### 3.10 Doplnkové funkce

Jde o technickou výbavu kamery, která je závislá na třídě dané kamery, tedy hlavně na její ceně.

### Elektronická závěrky (shutter)

Mezi funkce prakticky standardní i v nižší cenové třídě se vypracoval systém ESC (popř. ECS, SCS, EI nebo ES). Nezávisle na použitém názvu, lišícím se od výrobce k výrobci, je to funkce elektronické závěrky (tzv. shutter).

Tato funkce umožňuje regulovat plynule nebo skokově množství akumulovaného náboje na CCD čipu v závislosti na intenzitě osvětlení, a tím umožňuje v určitém omezeném rozsahu změn světelných podmínek použít levnější objektiv s clonou nastavitelnou ručně, popř. bez clony. Není-li však tato funkce odpínatelná, nelze použít objektiv řízený videosignálem. Regulační rozsah se pohybuje od 1/50 s do 1/100 000 s. Regulační rozsah moderních kamer se pohybuje dokonce od 1/50 s do 1/1 000 000 s.

Jaké přednosti nám funkce shutter nabízí?

- automatika neobsahuje žádné pohyblivé díly, čímž jsou odstraněny kritické prvky z hlediska dlouhodobé spolehlivosti,
- hloubka ostrosti zůstává neustále stejná, neboť nedochází ke změně pevně nastavené clony,
- značně se redukuje náklady na údržbu a servis,
- při výměně objektivů nedochází k problémům s konektory,
- automatika není citlivá na mechanické vlivy prostředí (vibrace, rázy, zrychlení, extrémní kolísání teplot).

Vezmeme-li jako příklad regulační rozsah funkce shutter 7000, a vezmeme-li v úvahu ještě rozsah AGC např. 1:15, dostáváme celkový rozsah regulace 105 000. Tento regulační rozsah odpovídá změně clonového čísla v rozsahu větším než 15 jednotek. Tento skok je schopna elektronika překlenout během 3 sekund; klasickému objektivu s automatickým řízením clony stejný skok trvá 6 až 10 s, objektivu s DC řízením 2 až 3 s.

Z popsaného příkladu vidíme, že kvalitní funkce „shutter“ může značně zjednodušit a zlevnit systém CCTV tím, že prakticky není nutné používat objektivy s řízenou clonou.

### Kompenzace protisvětla (BLC)

Další častou funkcí je obvod k eliminaci protisvětla (BLC). Tento obvod dokáže částečně vyloučit důsledky nevhodného umístění kamery se silným zdrojem světla v jejím zorném poli. Principiálně zůstávají zdroje světla přesvětlené a zájmové objekty umístěné v poli, pro něž je funkce BLC určena, budou kontrastnější. Složitější obvody omezení protisvětla (s různými názvy, např. Eclipser) umožňují nahradit ve snímané scéně jasné části od určité úrovně bílé černou či zvoleným odstínem šedé.

### Automatické řízení citlivosti (AGC)

Další funkcí je automatické řízení citlivosti (AGC), které zvyšuje citlivost kamery při nízkých úrovních osvětlení. Efektu se docílí pomocí automatického řízení zisku videozesilovače (AGC). Při nasazení funkce AGC je však nutné počítat s mírným zhoršením odstupu signál/šum odpovídajícím zisku funkce AGC.

### Gama korekce

V podstatě se jedná o korekci převodní charakteristiky vakuové obrazovky. Některé kamery jsou vybaveny také přepínačem gama korekce (obvykle v hodnotách 0,45 a 1). Podle charakteru snímané scény lze tímto přepínačem zlepšit podání gradace obrazu. Dnes tato doplňková funkce není výrobcí preferována.

### Nastavení vyrovnání bílé

U barevných kamer nalezneme navíc vyrovnání bílé (White balance) jako standardní funkci řešenou většinou jako přepínatelnou s možností automatického či ručního řízení v jedné nebo dvou barevných osách (R – B či R – B a G – Mg).

### Další doplňkové funkce

Řada výrobců již v minulosti uváděla na trh kamery s marketingovým přívlastkem "digitální kamera". Ve skutečnosti se však jednalo především o digitální optimalizaci parametrů zpracování signálu v kameře, a na videovýstupu máme zase – logicky, jak jinak – normalizovaný kompozitní videosignál (dle standardu CCIR a PAL).

Jedná se tedy o možnost řízení parametrů z PC přes port RS 232, popř. RS 485, na obrazovkovém menu videomonitoru prostřednictvím ovládacích tlačítek na kameře, popř. ovládání prostřednictvím nastavovací jednotky přes přenosovou cestu (koaxiální videokabel).

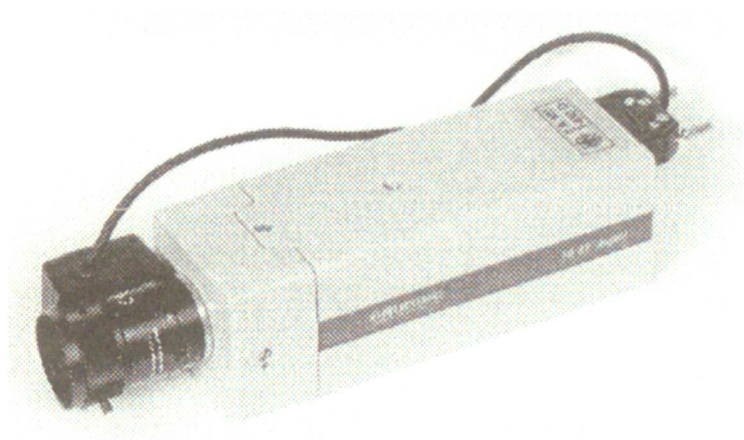
Tyto kamery umožňují dálkové ovládání prakticky všech parametrů kamery a mají-li v sobě skutečně digitální zpracování obrazového signálu, jsou schopny uspět i tam, kde s klasickou analogovou technikou narazíme na fyzikální hranice.

Z množství doplňkových funkcí digitálních kamer lze jmenovat alespoň tyto:

- shutter v rozsahu 1/50 – 1/1 000 000,
- nastavitelná konstanta integrace,
- vymaskování přesvětlených bodů či ploch snímané scény,
- ořezávání světelných špiček,
- nastavení aperturové korekce,
- nastavení referenční úrovně černé,
- nastavení gama korekce a lokální světelné adaptace,
- nastavení sytosti barev,
- nastavení synchronizace (int./ext./line-lock) včetně dostavení fáze,
- generování textu do obrazového signálu,
- volba videovýstupu (symetrický/nesymetrický),
- nastavení parametrů videodetekce,
- nastavení parametrů ukládání poplachových snímků přímo do paměti kamery.

Mezi nejvýznamnější doplňkové funkce, které jsou umožněny digitálním zpracováním videosignálu v kameře patří funkce **lokální světelné adaptace**, která podstatným způsobem rozšiřuje využití kamer při aplikacích ve složitých světelných podmínkách, zvláště kdy není možno s ohledem na místní podmínky instalace dodržet zásady montáže a kdy se v zorném poli vyskytují silné zdroje protisvětla. Tato funkce je vlastně skokovým vylepšením funkce kompenzace protisvětla (tzv BLC) která se vyskytovala i u vyšších modelů ryze analogových kamer.

Další významné funkce, které aplikace digitálního zpracování videosignálu v kameře umožnilo jsou funkce ke zvýraznění kontur, kontrastu a dynamického rozsahu, které výrazně zlepšují kvalitu obrazu a identifikaci detailů za mlhy deště a nízké úrovně osvětlení. Sem lze zařadit i možnost automatického přechodu do černobílého módu při poklesu intenzity osvětlení a tím při snížení odstupů signál – šum (S/Š) v komplexním videosignálu. Všechny tyto funkce mají své specifické názvy a jsou jednotlivými výrobci patentově chráněny a zkratky jsou oficiálně registrovány.



Obr. 5-11: Jedna z prvních kamer s integrovanou pamětí na 16 snímků (Grundig).

### 3.11 Volba vhodného typu kamer

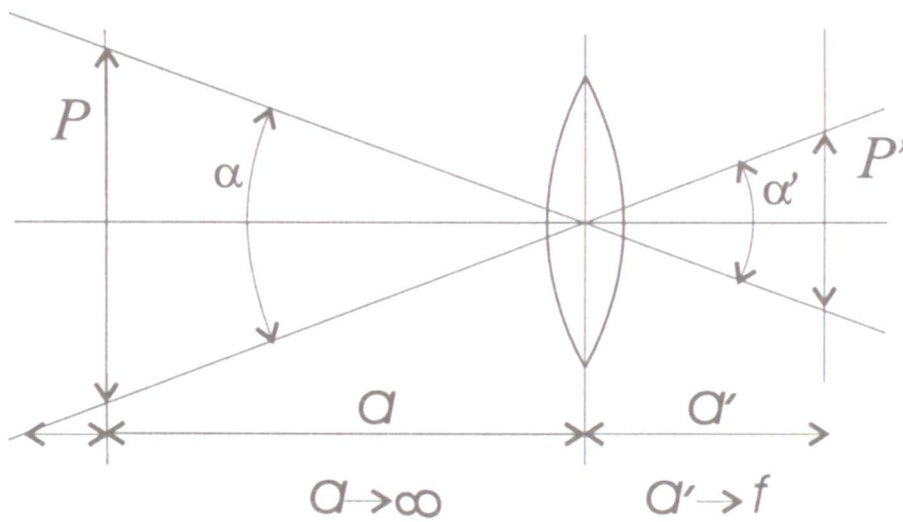
Volba vhodného typu by měla vycházet z technických požadavků na konkrétní použití. Jde především o tato rozhodnutí:

- analogovou či digitální,
- černobílou či barevnou,
- standardní či s vysokou rozlišovací schopností,
- napájení síťové, nízkovoltové st, nízkovoltové ss,
- synchronizaci interní, externí či line-lock,
- dodatkové či speciální funkce.

Ne vždy je však nutné vyžadovat od kamery všechny vlastnosti popsané v jednotlivých částech, ale základním kritériem – tak, jak bylo řečeno v úvodu kapitoly, je splnění představ zákazníka v daném ekonomickém rámci.

## 4. Objektivy

Objektiv zobrazuje zorné pole na svetlocitlivou plochu snímací elektronky nebo CCD čipu. Měřítko zobrazení, tj. poměr velikosti snímaného předmětu a jeho obrazu, a tím i snímací úhel jsou dány **ohniskovou vzdáleností** objektivu.



Obr. 5-13: Optické zobrazení.

### 4.1 Ohnisková vzdálenost

Vztah mezi velikostí snímaného předmětu  $P$  a vzdáleností od objektivu  $a$ , velikostí obrazu snímaného předmětu  $P'$  na citlivé ploše snímacího prvku vzdáleností obrazu  $a'$ , zorným úhlem a ohniskovou vzdáleností objektivu  $f$  je možno vyjádřit rovnicemi:

$$\frac{P}{P'} = \frac{a'}{a}; \quad \frac{1}{a} + \frac{1}{a'} = \frac{1}{f}; \quad \tan \alpha = \frac{P}{2f}$$

Potřebnou ohniskovou vzdálenost pro dané zobrazení lze určit ze vztahu:

$$f = D_R \cdot \frac{a}{P} \cdot \frac{P_M}{1,1 \cdot D_M}$$

kde:

- $f$  je ohnisková vzdálenost (mm),
- $D_R$  je průměr snímacího čipu (mm),
- $a$  je vzdálenost snímaného objektu (m),
- $P$  je výška snímaného předmětu (m),
- $D_M$  je úhlopříčka monitoru (cm),
- $P_M$  je požadovaná výška obrazu na monitoru (cm).

Naopak je možné ze vztahu určit velikost obrazu snímaného předmětu při užití objektivu s danou ohniskovou vzdáleností:

$$P_M = 1,1 \cdot D_M \cdot \frac{P}{a} \cdot \frac{f}{D_R}$$

Předcházející poměrně pracné výpočty lze nahradit tabulkou, jež značně urychlí návrh správné ohniskové vzdálenosti objektivu. Pro daný účel existují kromě tabulek rovněž různé nomogramy, a také posuvná pravítka, a objevují se dokonce i jednoduché výpočetní softwary.

Z těchto pomocných prostředků uvádíme prakticky ten nejprehlednější v tabulce 5-8.



Obr. 5-14: Různé druhy objektivů (TOKINA).

Objektivy se dodávají kromě pevné ohniskové vzdálenosti také v provedení s ručně nastavitelnou ohniskovou vzdáleností v malém rozmezí (2 – 3x). Tyto objektivy značně usnadňují práci montážním organizacím při definitivním nastavování zorného pole před předáním systému. Dále existují objektivy s dálkově řízenou proměnnou ohniskovou vzdáleností s velkým rozsahem (tzv. motorzoomy až 27x).

#### 4.2 Clona

Dalším parametrem objektivů je rozsah nastavení clony. Nastavit ji můžeme ručně nebo motoricky. Změnou vstupního průměru otvoru clony je možné regulovat množství světla, jež dopadá na světlocitlivou plochu snímacího prvku, a tím přizpůsobit objektiv různým světelným podmínkám nasazení.

Clonové číslo  $k$  je pak dáno podílem ohniskové vzdálenosti  $f$  k průměru vstupního otvoru clony  $d$ :

$$k = \frac{f}{d}$$

Clonová čísla jsou řazena do geometrické řady se součinitelem 1,41, kde každé vyšší clonové číslo způsobí, že na snímací prvek dopadá poloviční množství světla. Číslo uvedené na objektivu výrobcem značí obvykle clonové číslo při cloně otevřené na maximum. Čím kvalitnější objektiv, tím menší clonové číslo.

Mezinárodní normalizovaná řada clonových čísel je:

1    1,4    2    2,8    4    5,6    8    11    16    22    32

Má-li být zaručen široký rozsah snímání od úrovně přímého slunečního svitu (viz tabulka 5-5, odd. 3) do úrovně limitované vlastní citlivostí kamery a clonovým číslem použitého objektivu, je třeba použít objektiv s automatickým řízením clony nebo kameru s dostatečným regulačním rozsahem elektronické závěrky (shutter).

Objektivy se dodávají v těchto variantách:

- bez clony,
- s ručně nastavitelnou clonou,
- s videosignálem řízenou clonou (AI),
- s clonou řízenou ss napětím (DC - galvanometrický princip clony),
- pro extrémně velký dynamický rozsah s řízenou clonou (AI nebo DC) a s neutrálním šedým filtrem (tzv. ND provedení).



Obr. 5-15: Objektiv s clonou řízenou videosignálem (COMPUTAR).

### 4.3 Optická ostrost

Hloubka ostrosti je subjektivně definovaný rozsah, v němž jsou předměty zobrazeny s ještě přijatelnou ztrátou rozlišení detailů – jsou tedy ostré. Tento parametr je závislý na technickém provedení optiky, na ohniskové vzdálenosti a na stavu otevření clony. S výjimkou širokoúhlých objektivů s velmi malou ohniskovou vzdáleností je možné nastavit ostrost obrazu ručně nebo motoricky. Pro motoricky ovládané ostření je nutné užít ovládací díl spojený s objektivem řídicím kabelem. Hloubka ostrosti je uváděna pro aplikace v CCTV od minimální vzdálenosti uvedené ve specifikaci do nekonečna. U nejlevnějších objektivů silně klesá hloubka ostrosti se vzdáleností od optické osy. Prakticky se to projevuje na obrazovce vytvořením kruhové plochy s přijatelnou ostroší obrazu a okraje jsou neostře.

Problémy s ostroší mohou nastat také při změně spektrálního složení osvětlení scény. Běžné objektivy nastavené při denním světle mohou při umělém osvětlení způsobit rozostření obrazu. Nejvýrazněji se tento jev projevuje při nočním snímání za přisvětlení scény IR reflektory. Nejsou-li objektivy dálkově ovladatelné (motorzoom), dosáhneme



Tabulka 5-8: Určování potřebných ohniskových vzdáleností objektivů

f (mm)	formát čipu	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
4	1/4"	0,6	0,9	1,2	1,8	2,4	2,9	3,6	4,2	4,7	5,5	6	9	12	15	18	23,5	29,5	47,5	59,5	118,5
		0,8	1,2	1,6	2,4	3,2	3,9	4,7	5,5	6,5	7	8	12	16	20	23,5	31,5	39,5	63,5	79	158
	1/3"	0,8	1,2	1,6	2,4	3,2	3,8	4,7	5,5	6,5	7	8	12	16	20	24	32	38,5	63,5	78,5	159
6	1/2"	1	1,6	2,1	3,2	4,3	5,5	6,5	7,5	8,5	9,5	10,5	16	21	26,5	32	42,5	53	85	106	212
		1,2	1,8	2,4	3,6	4,7	5,9	7,1	8,3	9,5	11	12	18	24	30	36	47	59	95	119	237
	1/4"	1,6	2,4	3,2	4,7	6,3	7,9	9,5	11	13	14	16	24	32	40	47	63	79	127	158	316
8	1/2"	0,4	0,6	0,8	1,2	1,6	2	2,4	2,7	3,2	3,6	4	6	8	10	12	16	20	32	40	80
		0,6	0,8	1,1	1,6	2,1	2,6	3,2	3,8	4,2	4,8	5,5	8	10,5	14	16	21,5	26,5	44	55	110
	1/3"	0,5	0,8	1,1	1,6	2,2	2,8	3,3	3,7	4,5	5,9	6,5	8,5	11	14	16,5	22	27,5	44	55	110
12		0,7	1,1	1,4	2,2	2,9	3,6	4,4	5	6	6,5	7,5	11	14,5	19	22	29,5	36,5	60	75	150
	1/2"	0,8	1,2	1,6	2,4	3,2	4	4,8	5,6	6,4	7,2	8	12	16	20	24	32	40	64	80	160
	1/4"	1,1	1,6	2,1	3,2	4,3	5,3	6,4	7,5	8,5	9,6	11	16	21	28	32	43	53	88	110	220
12		0,3	0,4	0,6	0,9	1,2	1,5	1,8	2,1	2,3	2,7	3	4,4	6	7,5	9	12	15	23,5	29,5	59,5
		0,4	0,6	0,8	1,2	1,6	2	2,3	2,8	3,2	3,5	3,9	6	8	10	12	16	20	31,5	39,5	79
	1/3"	0,4	0,6	0,8	1,2	1,6	2	2,4	2,8	3,2	3,5	3,9	6	8	10	12	16	20	32	39,5	79,5
12		0,5	0,8	1,5	1,6	2,1	2,6	3,2	3,7	4,2	4,7	5,5	8	10,5	13	16	21	26	47	53	106
	1/2"	0,6	0,9	1,2	1,8	2,4	3	3,6	4,2	4,7	5,3	5,9	8,9	12	15	18	24	30	47	59	119
		0,8	1,2	1,6	2,4	3,2	4	4,7	5,5	6,3	7,1	7,9	12	16	20	24	32	40	63	79	158
12	1/4"	0,2	0,3	0,4	0,6	0,7	1	1,1	1,4	1,5	1,7	1,8	2,8	3,8	4,7	5,5	7,5	9,5	15	19	38
		0,25	0,4	0,5	0,7	1	1,2	1,5	1,7	2	2,3	2,5	3,8	5	6,5	7,5	10	12,5	20	25,5	50,5
	1/3"	0,25	0,4	0,5	0,7	1	1,3	1,5	1,8	2	2,3	2,5	3,8	5	6,5	7,5	10	12,5	20,5	25,5	51
12		0,35	0,5	0,7	1	1,4	2	2,4	2,7	3	3,4	5	7	8,5	10	13,5	17	27	34	68	68
	1/2"	0,4	0,6	0,8	1,1	1,5	1,9	2,3	2,7	3	3,4	3,8	5,7	7,6	9,5	11	15	19	30	38	76
		0,5	0,8	1	1,5	2	2,5	3	3,5	4	4,6	5,1	7,6	10	13	15	20	25	40	51	101

Tabulka 5-8: Určování potřebných ohniskových vzdáleností objektivů (pokračování)

f (mm)	formát čipu	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		
16	1/4"	1	0,1	0,2	0,3	0,4	0,6	0,7	0,9	1	1,2	1,3	1,5	2,2	2,9	3,7	4,5	6	7,5	12	15	30	
		5	0,2	0,3	0,4	0,6	0,8	1	1,2	1,4	1,6	1,8	2	2,9	3,9	4,9	6	8	10	16	20	40	
		1/3"	1	0,1	0,3	0,4	0,6	0,8	1	1,2	1,4	1,6	1,8	2	3	4	5	6	8	10	16	20	40
		5	0,2	0,4	0,5	0,8	1	1,3	1,6	1,8	2,1	2,4	2,6	4	5,5	6,5	8	10,5	13	21	27	53	
		1/2"	0,3	0,4	0,6	0,9	1,2	1,5	1,8	2,1	2,4	2,7	3	4,4	5,9	7,4	8,9	12	15	24	30	59	
25	1/4"	0,4	0,6	0,8	1,2	1,6	2	2,4	2,8	3,2	3,6	4	5,9	7,9	9,9	12	16	20	32	40	79		
		0,1	0,15	0,2	0,3	0,25	0,4	0,5	0,6	0,7	0,8	1	1,4	1,9	2,3	2,8	3,8	4,8	7,5	10	19		
		5	0,1	0,2	0,25	0,4	0,5	0,6	0,7	0,9	1	1,1	1,3	1,9	2,5	3,2	3,8	5	6,5	10	12,5	25	
		1/3"	0,1	0,2	0,25	0,4	0,5	0,7	0,8	0,9	1	1,2	1,3	1,9	2,5	3,2	3,8	5	6,5	10	12,5	25,5	
		5	0,1	0,25	0,35	0,5	0,7	0,9	1	1,2	1,4	1,5	1,7	2,5	3,4	4,3	5	7	8,5	13,5	17	34	
50	1/2"	0,2	0,3	0,4	0,6	0,8	0,9	1,1	1,3	1,5	1,7	1,9	2,8	3,8	4,7	5,7	7,6	9,5	15	19	38		
		0,3	0,4	0,5	0,8	1	1,3	1,5	1,8	2	2,3	2,5	3,8	5,1	6,3	7,6	10	13	20	25	51		
		-	-	-	0,15	0,15	0,2	0,3	0,4	0,45	0,4	0,5	0,7	1	1,2	1,4	1,9	2,3	3,8	5	10		
		-	-	-	0,2	0,25	0,3	0,4	0,45	0,5	0,6	0,65	0,9	1,2	1,6	1,9	2,6	3,2	5	6,5	12,5		
		-	-	0,15	0,2	0,25	0,3	0,4	0,45	0,5	0,6	0,65	1	1,3	1,6	1,9	2,5	3,2	5	6,5	12,5		
100	1/2"	-	-	0,2	0,25	0,35	0,4	0,5	0,6	0,7	0,75	0,85	1,3	1,7	2,1	2,5	3,4	4,3	7	8,5	17		
		-	-	0,2	0,3	0,35	0,4	0,6	0,6	0,65	0,8	0,85	1	1,5	2	2,4	2,8	3,8	4,7	7,5	9,8	19	
		-	-	0,3	0,4	0,5	0,6	0,8	0,8	0,9	1	1,1	1,3	1,9	2,5	3,2	3,8	5,1	6,3	10	13	25	
		-	-	-	-	-	-	0,15	0,15	0,2	0,2	0,2	0,2	0,35	0,45	0,6	0,7	0,8	1,2	1,9	2,4	4,8	
		-	-	-	-	-	-	0,2	0,2	0,2	0,25	0,3	0,3	0,5	0,65	0,8	1	1,2	1,6	2,5	3,2	6,5	
1/3"	-	-	-	-	-	0,15	0,2	0,2	0,25	0,3	0,3	0,5	0,65	0,8	0,95	1,25	1,6	2,5	3,2	6,5			
	-	-	-	-	-	0,2	0,25	0,3	0,35	0,4	0,4	0,65	0,85	1	1,25	1,7	2,1	3,4	4,3	8,5			
	-	-	-	-	0,2	0,2	0,3	0,3	0,4	0,4	0,4	0,7	0,9	1,2	1,4	1,9	2,4	3,8	4,7	9,5			
	-	-	-	-	0,2	0,2	0,3	0,3	0,4	0,4	0,4	0,7	0,9	1,2	1,4	1,9	2,4	3,8	4,7	9,5			
	-	-	-	-	0,3	0,3	0,4	0,4	0,5	0,6	0,6	1	1,3	1,6	1,9	2,5	3,2	5,1	6,3	10	13	25	

ostrého obrazu jen při použití objektivů s označením IR. Tyto objektivy mají na povrchu čoček napařenu speciální vrstvu, jež svými optickými vlastnostmi zamezuje pronikání IR záření s vlnovou délkou nad 1000 nm, jež je díky odlišnému lomu v optické soustavě objektivu hlavní příčinou rozostření obrazu snímaného při IR osvětlení oproti osvětlení ve viditelném spektru.

#### 4.4 Kritéria výběru vhodného objektivu

Při volbě vhodného objektivu vycházíme ze vzdálenosti a velikosti snímaného objektu a odtud určíme potřebnou ohniskovou vzdálenost. Ze světelných podmínek vyplynou požadavky na světelnost objektivu, popř. nutnost zvolit objektiv s řízenou clonou. Není-li vzdálenost a velikost snímaných objektů stálá, musíme použít objektiv s proměnnou ohniskovou vzdáleností (tzv. motorzoom). Objektivy typu motorzoom se zpravidla používají na kamerových stanovištích spolu s polohovací hlavicí.

V praxi CCTV se nejvíce využívají objektivy variofocus, ať již s elektronicky řízenou clonou, nebo s clonou ručně nastavitelnou. Předností těchto objektivů je možnost dostavení zorného pole při oživování systému bez nutnosti výměny objektivu za jiný s jinou ohniskovou vzdáleností. S minimálními nároky na montáž se tedy můžeme co nejvíce přiblížit požadavku zákazníka.

Tabulka 5-9: Vybavení objektivů

Ohnisková vzdálenost	Clona	Používaný název
pevná	bez clony	fixfocus bez clony
pevná	nastavitelná (ručně)	fixfocus
nastavitelná (ručně)	nastavitelná (ručně)	variofocus
pevná	proměnná (motoricky)	autoiris (AI)
nastavitelná (ručně)	proměnná (motoricky)	variofocus-autoiris (AI)
pevná	proměnná (galvanometricky)	autoiris (DC)
nastavitelná (ručně)	proměnná (motoricky)	variofocus-autoiris (AI)
proměnná (motoricky)	proměnná (motoricky)	motorzoom
proměnná (motoricky)	proměnná (galvanometricky)	DC motorzoom

*Poznámka – Mimo rámeček výše uvedené tabulky existují i nejlevnější typy objektivů bez ostřicího kroužku. U objektivů typu motorzoom existuje navíc provedení se zpětnovazebními potenciometry, jež snímají polohu čoček pro nastavení ohniskové vzdálenosti a ostření. Tohoto zpětnovazebního signálu lze využít pro automatické nastavení parametrů objektivu, umožňuje-li to připojená řídicí jednotka. Další speciální typ, který se vymyká členění tabulky uvedené výše, je jehlový objektiv – ve specifikacích označován výrazem pinhole. Tento objektiv je díky minimalizovanému rozměru vstupní čočky vhodný jednak pro diskrétní montáž, ale i pro aplikace v průmyslové oblasti, např. v horkých provozech, kde je nežádoucí velká plocha přivrácená ke snímanému žhavému tělesu tak, jak by tomu bylo u běžného objektivu.*

Obr. 5-16: Objektiv typu motorzoom.



### 4.5 Uchycení objektivu

V odd. 3 byly popsány dva standardy uchycení objektivu ke kameře. V technické specifikaci každého objektivu je označením C nebo CS uvedeno, pro jaký standard je objektiv určen. Moderní kamery střední a vyšší třídy mají často přestavitelnou kulisu CCD čipu, a tím i možnost namontovat objektiv obou uvedených standardů, popř. jsou provedeny ve standardu CS s mezikroužkem v příslušenství.

Dalším parametrem uváděným u objektivů je formát, pro který jsou spočteny snímací úhly. V zásadě lze pro kameru menšího formátu vždy použít objektiv určený pro všechny formáty větší. Přehledně to znázorňuje tabulka 5-10.

Tabulka 5-10: Aplikace objektivů a kamer s ohledem na formát čipu

		Objektiv				
		1/4'	1/3'	1/2'	2/3'	1'
Kamera	1/4'	ano	ano	ano	ano	ano
	1/3'	ne	ano	ano	ano	ano
	1/2'	ne	ne	ano	ano	ano
	2/3'	ne	ne	ne	ano	ano
	1'	ne	ne	ne	ne	ano

## 5. Příslušenství kamer

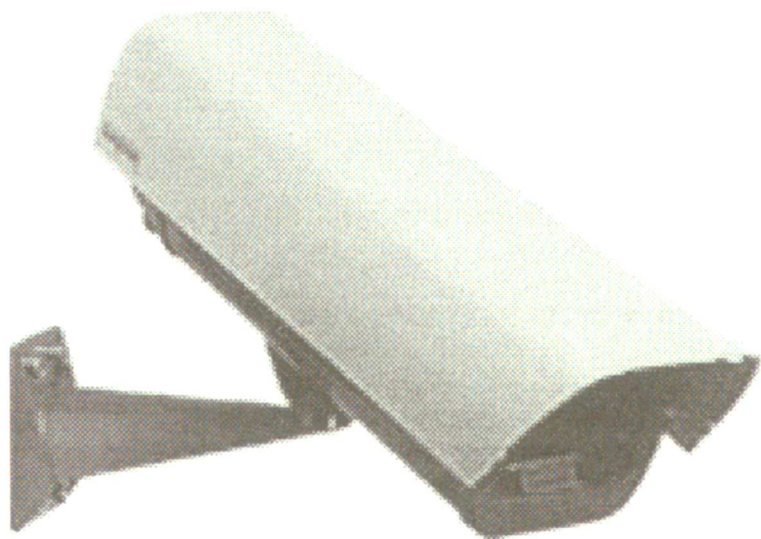
### 5.1 Kamerové kryty

Kamerové kryty jako příslušenství kamer hrají v systémech CCTV podstatnou roli. Nejde jen o estetický dojem zákazníka, ale nevhodný návrh krytu může degradovat celý budovaný systém CCTV.

Nejčastější a logická aplikace je využití kamerových krytů při montáži kamer ve venkovním prostředí. Zde je třeba dbát určitých zásad při výběru a konfiguraci kamerového krytu, a to:

- kamerový kryt musí mít dle elektrotechnických norem příslušnou ochranu představující v mezinárodním značení kategorii minimálně IP - 64;
- vnitřní prostor kamerového krytu musí být tak velký, aby se do něj pohodlně i s ohledem na pozdější servisní zásahy vešla kamera s příslušným objektivem včetně potřebných připojovacích konektorů (pozor na kamery s bočním výstupem pro řízení clony objektivu!);
- součástí kamerového krytu by měla být sluneční stříška jako ochrana před přehříváním v letním období (kamery mají většinou rozsah pracovních teplot omezen shora na 50 – 60 °C);
- naprosto logickou součástí je topení a teplotní spínač, které chrání v zimních měsících kameru před podchlazením a průhled krytu před zamlžením či zamrznutím (kamery mají většinou rozsah pracovních teplot omezen zdola na 5 °C);
- z hlediska elektrotechnických předpisů je důležité ochranné pospojování kovových částí krytu, jež mohou být zvenčí přístupné, a vhodný bezpečný způsob vnitřního propojení topení, termostatu a napájení kamery, jsou-li provedeny na síťové napětí;
- možnost izolované montáže kamery uvnitř krytu tak, aby bylo možné oddělit místní přizemnění krytu (při montáži např. na ocelové konstrukce budov, sloupy osvětlení, mostové jeřáby apod.) od ochranného vodiče třížilového přívodu kamery (kamera se síťovým napájením 230 V je elektrický předmět třídy I.!). Toto opatření slouží k odstranění vlivu vyrovnávacích zemních proudů na kvalitu obrazu. V opačném případě se na obraze objeví 50Hz brumový pás, který často dělá montážním organizacím velké problémy s identifikací místa vzniku a možnostmi jeho odstranění;
- snadný přístup do krytu a jednoduchá demontáž v případě servisních zásahů;
- možnost skrytého vedení napájecího a signálového kabelu z kamerového ramene není podmínka nezbytná, ale takovéto esteticky čisté provedení rozhodně podporuje prestiž montážní organizace.

Obr. 5-17: Kamerový kryt (COMPUTAR).



Kromě venkovního prostředí existuje však celá řada aplikací, kde je účelné kamerový kryt použít rovněž. Jde především o použití v průmyslu. Důvody pro použití krytu jsou dány vlastnostmi prostředí, v němž budou kamery umístěny. Je to např. prostředí prašné, vlhké, s korozní agresivitou, horké, výbušné atd.

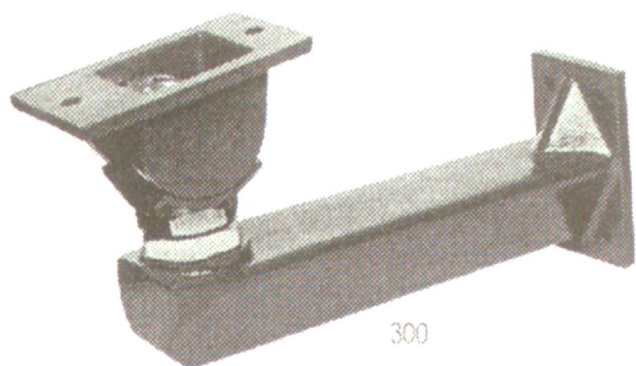
Základní kritéria, platící pro venkovní kryty, zůstávají zachována s určitými dodatky dále. Pro vlhké a prašné prostředí je možno použít běžných venkovních krytů s neúplnou výbavou – tedy bez sluneční stříšky a bez topení. Častým důvodem pro montáž krytu i ve vnitřním prostředí je obava z úmyslného poškození či krádeže kamery. Pro tyto případy nabízejí někteří výrobci kompaktní kamery v provedení s krytím až IP 67. V aplikacích bez požadavků na montáž motorzoomů jsou naprosto vyhovující, mají menší rozměry oproti klasickým krytům a jsou levnější.

V horkém prostředí se se většinou neobejdeme bez chlazení. Kryty jsou pak dvouplášťové a v dutině je zajištěn nucený oběh chladicího média (vzduch, voda). Průhled je vyroben z masivního kaleného skla, je běžného rozměru, nebo je využito objektivů typu „pinhole“ a průhled je minimalizován. U prostředí s nebezpečím výbuchu je nutné dbát na použití kamerového krytu, který je odzkoušen a výrobce prokázal shodu s technickými požadavky na výrobky (zákon č. 22/97 Sb. ve znění pozdějších předpisů).

V posledních dvou případech je nutné ve stadiu návrhu velice pečlivě zkoumat podmínky nasazení a zvažovat výběr vhodného typu krytu. Vzhledem k tomu, že jde o elektrické zařízení, měli bychom vždy vyhledat ustanovení příslušných norem pro krytí elektrických předmětů a druhy prostředí.

Nedílnou součástí návrhu krytů je volba odpovídajícího **kamerového ramena**. Zde je základním technickým kritériem nosnost ramena a estetickým kritériem jeho konstrukční a barevné provedení. Některé druhy ramen umožňují navíc skryté vedení napájecího a signálového kabelu.

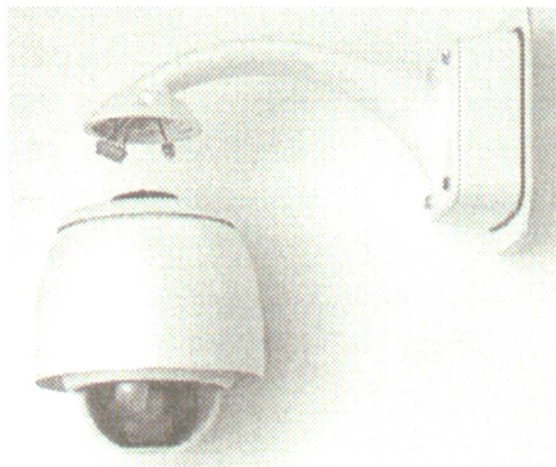
*Poznámka – Jako speciální příslušenství pro náročné aplikace nabízejí některé firmy vysokotlaké ostřikovače okénka kamerového krytu, popř. speciální stěrače. V praxi se však tyto speciální doplňky nevyskytují příliš často.*



Obr. 5-18: Kamerové rameno (COMPUTAR).

## 5.2 Polohovací hlavice

Technicky jde o elektromechanické zařízení vybavené dvěma reverzibilními motory střídavými či stejnosměrnými, nejčastěji z hlediska bezpečnosti na malé napětí. Existují sice i hlavice s motory na síťové napájení, ale jejich aplikaci nelze doporučit právě z hlediska bezpečnosti. Hnací moment je z elektromotorů převáděn přes převodové ústrojí na těleso krytu a nosník kamerového krytu. Celý systém je zapouzdřen v odolném krytu a pro aplikaci ve venkovním prostředí platí podobná kritéria jako pro kamerové kryty. Pouze rozsah pracovních teplot je širší. Není tedy nutné používat pro polohovací hlavice topení. To je však možno jako zvláštní výbavu pro extrémní podmínky doplnit. Krytí pro vnější použití by mělo být rovněž nejméně IP 64.



Obr. 5-19: Integrovaná kamerová jednotka s polohováním a zoomem (PHILIPS).

Nejdůležitější parametry polohovací hlavice jsou:

- nosnost,
- stupeň klimatické odolnosti, krytí elektrického předmětu,
- úhlová rychlost,
- krouticí moment,
- mrtvý chod,
- proudový odběr motorů.

Nosnost a mrtvý chod (spolu s mechanickou tuhostí montážního místa a kamerového ramene) jsou parametry důležité pro stabilní obraz při použití velkých ohniskových vzdáleností za větru. Úhlová rychlost se projeví na operativním přesměrování kamery a odběr motorů ovlivní výpočet potřebného průřezu vodičů při řízení vícežilovým kabelem. Při montáži musíme nastavit správně dorazy hlavice tak, aby nemohlo dojít k poškození připojovací kabeláže a kamerového krytu.

### 5.3 Systémy dálkového ovládání

V praxi je možné se setkat s požadavkem monitorovat rozsáhlý prostor, kde není předem definováno ani umístění snímaného předmětu, ani vzdálenost, ani jeho přesná velikost, popř. pohyb se snímaného předmětu. Zde nezbyvá technicky žádné jiné řešení než aplikace dálkově řízených objektivů (motorzoom) a umístění samotné kamery, popř. kamery v kamerovém krytu, na polohovací hlavici.

Standardní úlohy pro systém dálkového ovládání jsou :

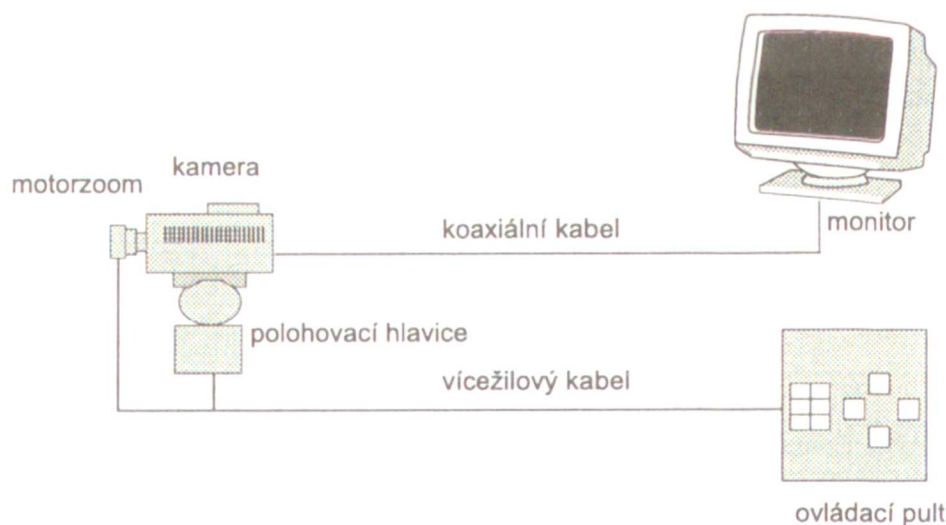
- pohyb kamery v horizontální rovině ( vpravo/vlevo),
- pohyb kamery ve vertikální rovině (nahoru/dolů),
- změna ohniskové vzdálenosti (telezáběr/širokoúhlé snímání),
- změna ostření (blízké/vzdálené).

Některé systémy nabízejí navíc luxusní uživatelské funkce, jako je třeba ovládání ostřikovačů, stěračů, místních reflektorů či infrareflektorů, předvolbu nastavení objektivu a kamerové polohovací hlavice, vstupy poplachového interface pro spolupráci s EZS atd. K realizaci systémů dálkového ovládání se nabízí několik odlišných principů přenosu řídicích signálů. Dále budou probrány jednotlivé možnosti s jejich výhodami, nevýhodami a doporučeními pro aplikaci.

#### 5.3.1 Řízení po vícežilovém kabelu

Tento způsob je technicky nejjednodušší. Ovládací pult obsahuje pouze spínače, popř. posilovací relé, a přes tyto kontakty je přivedeno vícežilovým kabelem řídicí napětí přímo na kontakty motorů motorzoomu a polohovací hlavice. Je to levné řešení, ale má svá omezení. Tím nejpodstatnějším je úbytek napětí na řídicím kabelu daný použitým napětím a průřezem žil použitého kabelu. V praxi má smysl tento způsob použít do vzdálenosti kamerového stanoviště 100m od ovládacího pultu. Použití polohovacích hlavice řízených síťovým napětím 230 V je sice teoreticky možné, ale z hlediska bezpečnosti nepřilíš doporučované. Ideální pro tuto aplikaci jsou hlavice řízené střídavým napětím 24 V.

Obr. 5-20: Řízení po vícežilovém kabelu.

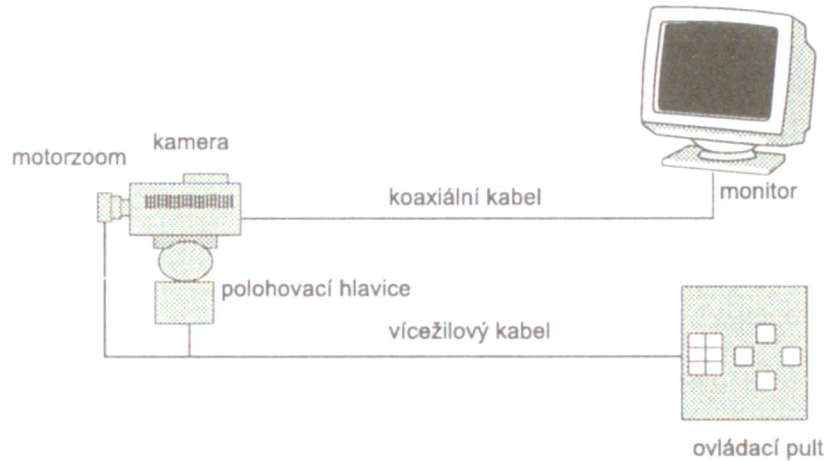




### 5.3.2 Řízení po koaxiálním kabelu

Jde o využití trasy nesymetrického koaxiálního vedení ke zpětnému přenosu řídicích signálů (obr.21). Ovládací pult v tomto případě kóduje do snímkového zatemňovacího impulsu časově synchronizované pulsy, které přijímač umístěný u kamerového stanoviště zpětně rozkóduje a převede na povely ke spínání místních relé, popř. k otevření spínacích tranzistorů.

Obr. 5-21: Řízení po koaxiálním kabelu.

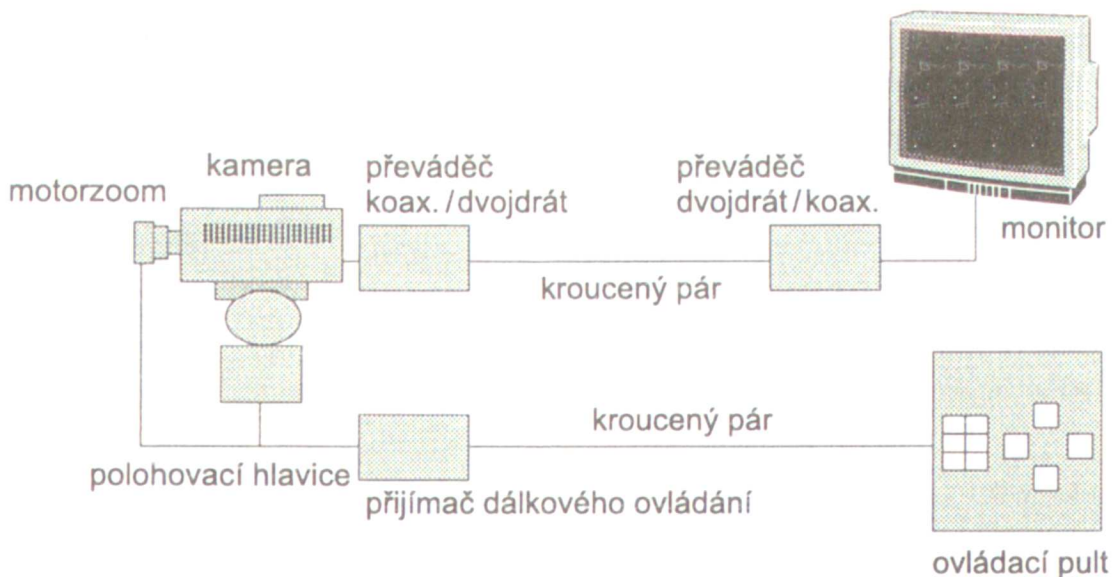


Z tohoto principu vyplývá výhoda ovládání motorzoomu i polohovací hlavice z lokálního napájecího zdroje, čímž odpadá problém úbytků na vedení. Nevýhodou ovšem je omezení vzdálenosti dané vlastnostmi použitého koaxiálního kabelu.

*Upozornění – Vzhledem k využití přenosové trasy pro videesignál jedním směrem a pro řídicí signály směrem druhým není možné zařadit do trasy průběžný videozesilovač.*

### 5.3.3 Řízení po symetrickém vedení

Zde je pro přenos řídicích signálů využit samostatný kroucený pár vodičů (tzv. dvojdrát). Tento způsob umožňuje přenos na největší vzdálenost řádově až 5 km, a tím koresponduje s přenosem videesignálu po symetrickém vedení. Pro přenos řídicích signálů i videesignálu je v tomto případě použit kabel s dvěma páry kroucených vodičů s minimální kapacitou (tzv. datapár).



Obr. 5-22: Řízení po symetrickém vedení.

Vlastní řídicí signál může podle použitého systému řídicího pultu být analogový či digitální. U digitálních systémů je dvojnásobně většinou využito pro normalizovanou sběrnici RS 485. Formát řídicích signálů není ujednocen a každý výrobce má svůj. Z hlediska kompatibility musí tedy řídicí pult i přijímač s dekodérem pracovat na stejném principu. Jedním z využívaných formátů je i telefonní tónová volba. Všechna polohovací stanoviště leží na společné datové sběrnici a každý přijímač má vlastní adresu. Alternativně je možné i hvězdicové zapojení.

## 6. Přenos videosignálu

Zvláště v aplikacích monitorování objektů je často značná vzdálenost kamery a zařízení pro zpracování videosignálu s monitorem. Pro přenos videosignálu jsou k dispozici varianty přenosu za pomoci metalických okruhů, navíc je možné ve speciálních případech užít i bezdrátový přenos videosignálu či přenos po optických vláknech.

Rozhodnutí pro ten který druh přenosu závisí na těchto aspektech:

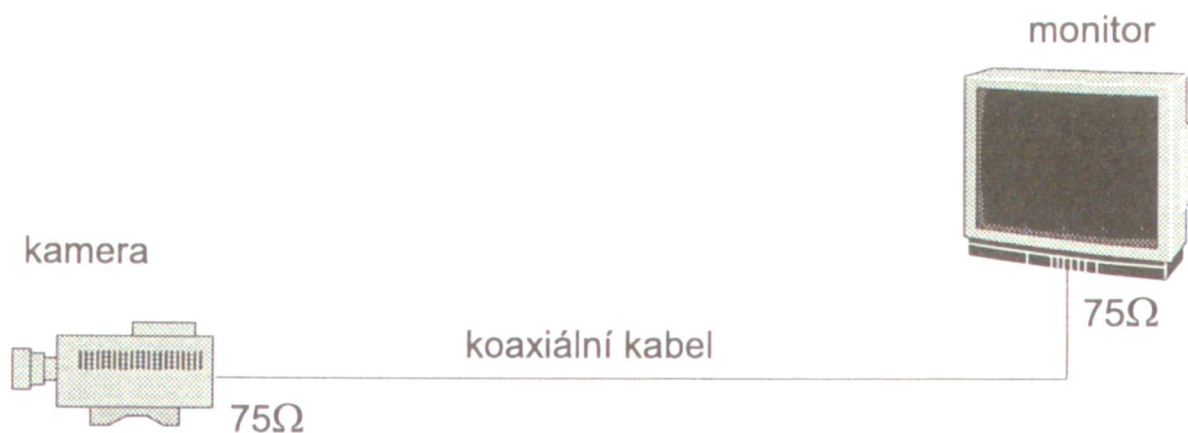
- počet kamer,
- vzdálenosti jednotlivých komponentů videosystému,
- ekonomické porovnání náročnosti jednotlivých variant,
- druh a vliv prostředí, v němž je videosystém nasazován.

### 6.1 Přenos po koaxiálním vedení

Pro přenos videosignálu s plnou rozlišovací schopností je potřebná šířka přenosového pásma 6,5 MHz. Délka vedení je zde omezena úbytkem signálu podél vedení, jenž je dán parametry použitého kabelu. Bez použití dodatečných technických prostředků je přenos videosignálu od kamery k monitoru možný na vzdálenost řádově stovky metrů dle volby typu koaxiálního kabelu.

Pro delší trasy je nutné použít průběžné korekční videozesilovače. Takto lze docílit délky trasy v řádu kilometrů. Průběžný korekční videozesilovač eliminuje útlum použitého kabelu. Tento útlum roste s délkou vedení a s přenášeným kmitočtem.

Každá trasa musí být přizpůsobena - tzn. musí být zakončena vstupem zařízení s charakteristickou impedancí  $75 \Omega$ . Kabelové konektory by měly



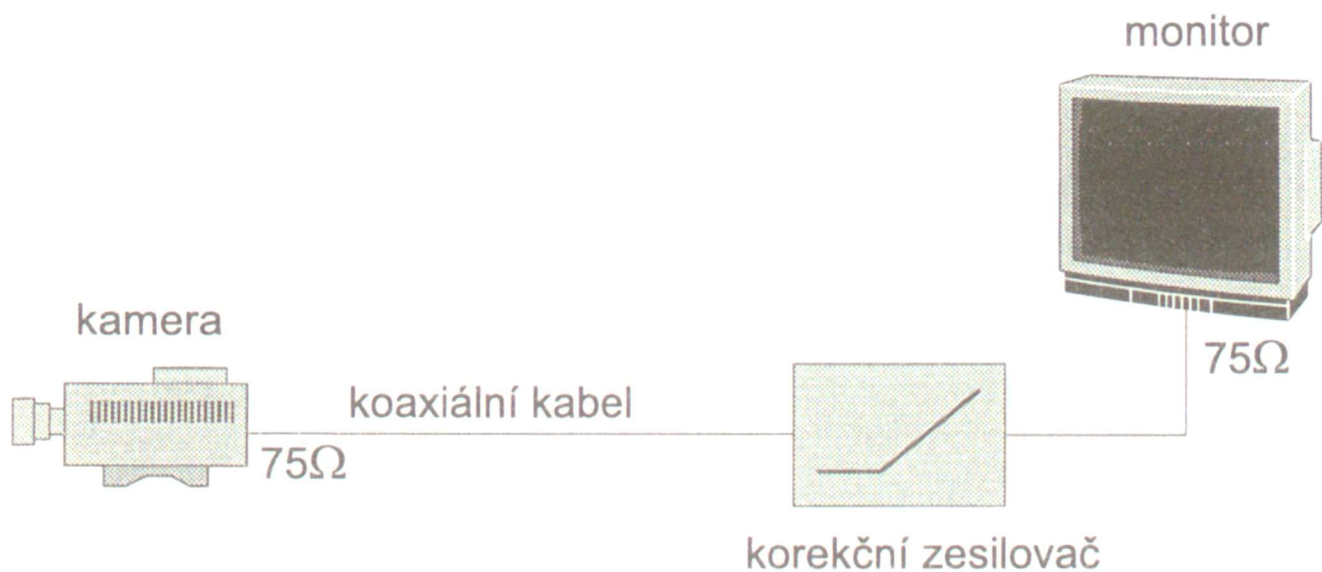
Obr. 5-23: Přenos videosignálu pasivní koaxiální trasou.

mít spolehlivý kontakt jak středního vodiče, tak stínění. K tomuto účelu je nejvhodnější používat speciální kleště, které konektor na konec vedení nalisují tak, že vznikne nerozebíratelný spoj. Nejpoužívanější typ kabelu pro přenos videosignálu je kabel 0,6/3,7 o vnějším průměru 6 mm. Pro delší trasy se používají kabely 1,0/6,6 nebo 1,1/7,3 o vnějším průměru 9 nebo 10,3 mm.

V tabulce 5-11 jsou uvedeny maximální délky koaxiálních kabelů s ohledem na přijatelný útlum videosignálu. Při útlumu 3dB/5MHz je obraz bezvadný, při útlumu 6dB/5MHz je obraz ještě vyhovující.

Tabulka 5-11: Maximální délky pasivní koaxiální přenosové trasy

útlum při 5 MHz (dB)	typ kabelu koax 75 Ω	délka (m)
3	0,6/3,7	115
	1,0/6,6	214
6	0,6/3,7	230
	1,0/6,6	428



Obr. 5-24: Přenos videosignálu se zařazeným korekčním zesilovačem.

Potřebný zisk průběžného zesilovače lze vypočítat ze vztahu:

$$G = l \cdot A$$

- kde  $l$  je délka kabelu (m)  
 $G$  je zisk na 5 MHz (dB) x 100  
 $A$  je útlum kabelu (dB/100m při 5 MHz)

*Poznámka – Při přenosu koaxiálním kabelem musí být vždy zachována zásada přizpůsobení, tzn. že na vstupu i výstupu musí být připojeno zařízení s charakteristickou impedancí 75 Ω. Přípustné je vysokoimpedanční odbočení signálu v případě smyčkování monitorů. Rozbočení signálu při zachování zásad přizpůsobení je možné jedině pomocí aktivních rozbočovacích prvků (zesilovačů). Při nepřizpůsobení vzniknou na kabelu odrazy, což se projeví vznikem vícenásobným obrazům na obrazovce (tzv. duchů).*

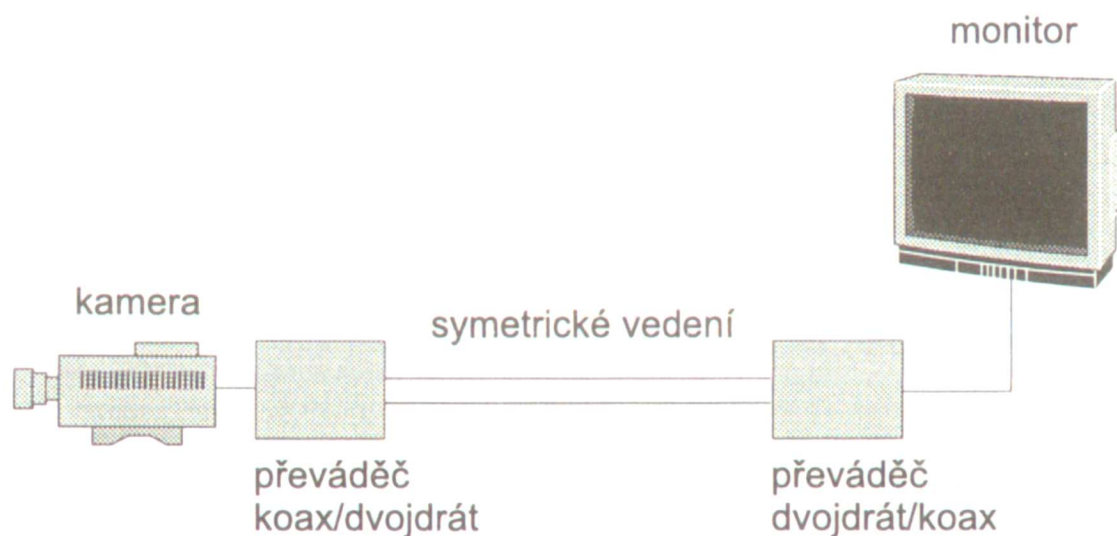
## 6.2 Přenos po symetrickém vedení

Druhá možnost přenosu videosignálu je dvojdřátový systém (obr. 5-25). Pro tento typ přenosu je možné využít párový kabel nebo volné páry ve vícežilových sdělovacích kabelech.

Nevýhodou tohoto řešení je, že neumožňuje přímé propojení kamery a monitoru. Pro připojení kamery (zdroje videosignálu) je nezbytný převáděč, který konvertuje vstup nesymetrický  $75 \Omega$  na výstup symetrický, a u monitoru přijímač, který konvertuje naopak symetrický vstup na nesymetrický výstup  $75 \Omega$ .

*Poznámka – Některé typy kamer, jsou vybaveny jak nesymetrickým, tak symetrickým výstupem. Nárůst ceny takto vybavené kamery je však srovnatelný s náklady na pořízení samostatného konvertoru nesymetrického signálu na symetrický. Nezanedbatelná je však u kamer se zabudovaným konvertorem výrazně jednodušší montáž.*

Velkou předností symetrického vedení na rozdíl od přenosu po koaxiálním vedení je vyšší odolnost proti rušení vnějším elektromagnetickým polem. Výhodou je také podle provedení vysílače a přijímače galvanické oddělení od přenosové trasy, a to buď optočleny, nebo širokopásmovými videotransformátory. Určitou nevýhodou je silná závislost na kapacitě použitého párového kabelu, a proto je vhodné navrhovanou trasu ověřit a zvolit nejvhodnější typ kabelu. Rovněž precizní nastavení vyrovnané kmitočtové charakteristiky je poměrně pracné a vyžaduje přístrojové vybavení, minimálně osciloskop a signální TV generátor. V nouzi musí vystačit místo TV generátoru zkušební obrazce.



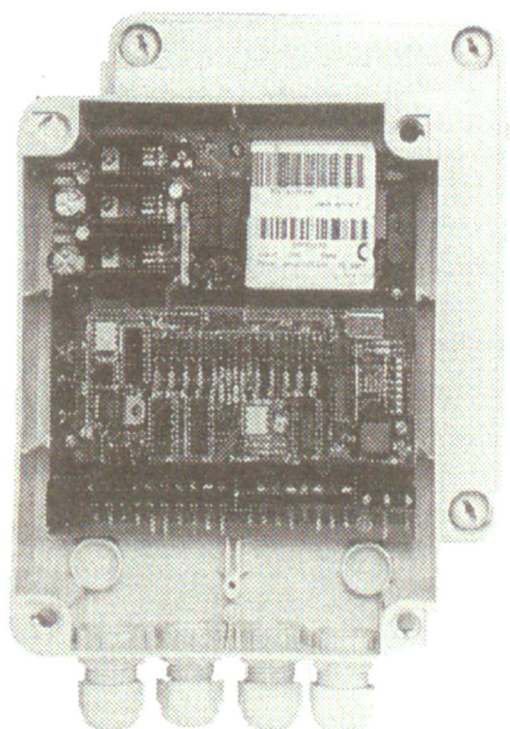
Obr. 5-25: Přenos videosignálu po symetrickém vedení.

Přípustná délka symetrického vedení je opět závislá na parametrech použitých kabelů. Nejvhodnější jsou kabely s garantovaným počtem minimálně 5 zkrutů na metr délky. Pro kabely s izolací PE jsou přípustné v tab. 5-12 uvedené délky přenosové trasy.

Tabulka 5-12: Příпустné délky přenosové trasy symetrického vedení

Průměr vodičů	Délka trasy
2 x 0,4 mm	1000 m
2 x 0,8 mm	2000 m
2 x 1,2 mm	2300 m
2 x 1,4 mm	2600 m

Zařazením průběžných symetrických videozesilovačů je možné dosáhnout délky přenosové trasy řádově až několika desítek km.



Obr. 5-26: Souprava pro přenos videosignálu po symetrickém vedení (COMPUTAR).

### 6.3 Další možnosti přenosu videosignálu (bezdrátové)

Pro současný přenos více signálů po koaxiálním vedení je možné využít **system s modulací signálů na nosné frekvence** v pásmu 30 – 300 MHz. Délka přenosové trasy je závislá na útlumu kabelu a je ji možné prodloužit zařazením průběžných zesilovačů. Tento systém se v rámci PTV příliš nevyužívá a v principu je shodný s řešením sítě kabelové televize.

Variantu **bezdrátového přenosu** je možné realizovat pomocí směrových spojů v pásmu dm a cm vln. Tento způsob přenosu je rozšířen v profesionální praxi pro přenos TV signálu z mobilních stanic (např. přímé přenosy) na stacionární. Vzhledem k použité frekvenci lze i zde využít možnosti **kombinace bezdrátového přenosu se systémem modulace signálů na subnosné frekvence** pro vícekanálový přenos.

Bezdrátový přenos není v rámci PTV příliš využíván (s výjimkou Městských kamerových dohlížecích systémů – MKDS) a vzhledem k vyšším nákladům je určen pro speciální aplikace, ale i tam se musí zřídit a provozovat v souladu s příslušnými předpisy o využívání rádiového spektra.

Vzhledem k tomu, že se režim uvádění koncových telekomunikačních a rádiových zařízení na trh e sjednocením postupů v rámci EU změnil, je nutno v této oblasti věnovat zvýšenou pozornost technickým požadavkům na přenosová zařízení pro aplikace v CCTV a to jak pro širokopásmový přenos videosignálu, tak pro případný digitální přenos ovládacích signálů.

Pro přenosové systémy využívajícími veřejnou telekomunikační síť a případně elektromagnetického spektra je nutno aplikovat požadavky Telekomunikačního zákona a Nařízení vlády č. 426/2000 Sb., kterým se stanoví technické požadavky na rádiová a na telekomunikační koncová zařízení, ve znění nařízení vlády č. 483/2002 Sb. a nařízení vlády č. 251/2003 Sb. (1999/5/ES)..

Zařízení využívají pásma všeobecných oprávnění (dříve generálními licencemi GL) ČTÚ (nezpłatněná pásma). Ani při využití těchto pásem a splnění technických požadavků se nezbavuje výrobce či dovozce povinnosti nechat zařízení schválit pro provoz v ČR a provést posouzení shody se všemi Nařízeními vlády, jež se a ně vztahují.

Bližší informace ve znění všeobecných oprávnění na ([www.ctu.cz](http://www.ctu.cz)).

Základní principy provozu ve sdílených pásmech jsou:

- Provoz vysílacích rádiových stanic nemá zajištěnou ochranu proti rušení způsobenému jinými telekomunikačními a rádiovými zařízeními. Kmitočty jsou sdílené.
- Provoz vysílacích rádiových stanic nesmí rušit zařízení jednotné telekomunikační sítě ani jiná radiokomunikační zařízení nebo telekomunikační služby.

Do kategorie bezdrátového přenosu lze zařadit i optický přenos pomocí modulovaných laserů. Na trhu se vyskytuje řada zařízení pro přenos dat či video- a audiosignálu na vzdálenost řádově stovky metrů. Je to alternativa zvláště pro případy, kdy není možné provést ani závěsné, ani zemní vedení. Může jít např. o překlenutí dálnice, železnice, vodního toku, a také o případy, kdy by budování metalického vedení bylo příliš nákladné.

Varianta přenosu videosignálu, která zvláště v poslední době nabývá na významu, je **přenos videosignálu po optickém vlákně**. Na trhu se dokonce objevují první kamery vybavené přímo optickým výstupem. Na přijímací straně je pak nutné doplnit pouze přijímač optického signálu o konvertor na klasický videosignál. Bez průběžných optických zesilovačů lze počítat s možností max. délky přenosové trasy do 4 km. Pro profesionální aplikace jsou k dispozici i soupravy pro přenos na vzdálenosti až 100 km bez průběžného zesílení. Rovněž se zde nabízí možnost multiplexního přenosu více videosignálů, popř. paralelní přenos audiosignálu či protisměrný přenos řídicích signálů pro ovládání kamerového stanoviště.

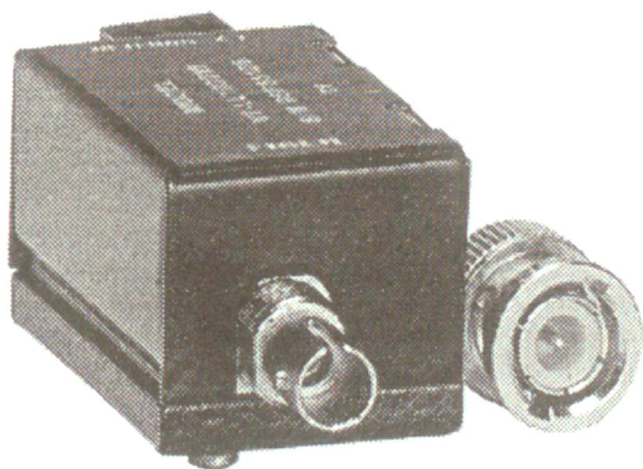
Přenos videosignálu po optických vláknech přináší řadu předností:

- absolutní odolnost vůči vlivům elektromagnetických polí,
- elektricky izolovaný systém nezávislý na rozdílných potenciálech míst spojení, a tím také bezpečný,
- odolnost proti odposlechu, bez rušivého vyzařování,
- mechanické provedení kabelu s malou hmotností – ohebný s malým průměrem.

Nevýhodou zatím zůstává poměrně vyšší cena takto vybudovaného systému, vysoká kvalifikační náročnost na projekci, montáž i servis a vysoká cena montážních i servisních přípravků a přístrojů.

### 6.4 Přenos digitalizovaného videosignálu

Další varianta přenosu, využívaná především v bezpečnostních aplikacích, je **přenos obrazového signálu v datové podobě** po běžných telefonních linkách, po linkách ISDN nebo po datových sítích, ať již uzavřených či veřejných. Principy přenosu videosignálu v datové podobě jsou popsány v **kapitole 6 IP-kamerové systémy**.



Obr. 5-27: Jednoduchý převaděč videosignálu na optické vlákno (Videor Technical).

## 7. Zařízení na zpracování videosignálu

### 7.1 Monitory

Používají se k zobrazení dějů snímaných kamerou nebo zaznamenaných na videorekordér. Nejčastěji se jedná o monitory vybavené poslední elektronkou – klasickou vakuovou obrazovkou, již je dodnes vybaveno prakticky 100% zobrazovacích zařízení u reálných systémů CCTV. I obrazovka monitoru počítače – přes odlišné rozkladové frekvence – je vlastně pouhou přes 100 let starou lampou.

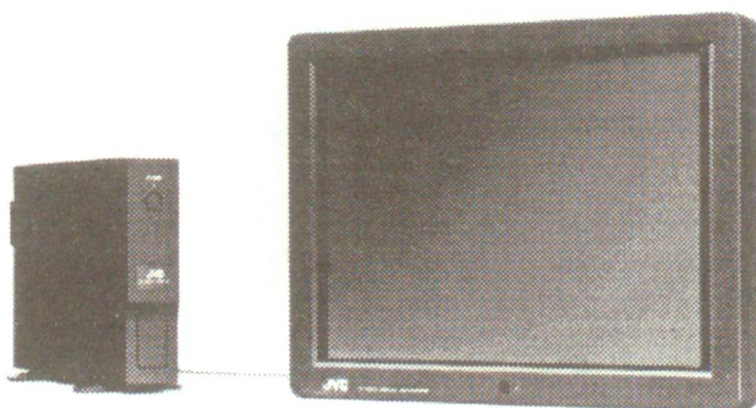
Určitou alternativou je využití zobrazovačů z tekutých krystalů (LCD displejů) obdobně jako u přenosných počítačů. Jejich použití bylo omezeno kvůli velké setrvačnosti zobrazovače především na menší úhlopříčky. Sledování dynamických dějů, což je v CCTV obvyklé, přinášelo v minulosti problémy se závojem pohybujících se předmětů, daným právě vysokou setrvačností zobrazovače LCD. Dnešní zobrazovače LCD mají tento problém prakticky již vyřešen a je možné použít i pro sledování dynamických dějů a dnes soupeří na trhu s plazmovým displejem.

Zřejmě nejpravděpodobnějším nástupcem vakuové obrazovky se stane Plazmový displej (PDP – Plasma Display Panels). Tento panel se poprvé veřejně objevil na výstavě zabezpečovací techniky SECURITY Essen 1996, a to hned na několika stáncích. Neveřejně byl k vidění v zázemí jednoho stánku již dva roky předtím. Technologie výroby je natolik náročná, že zůstává doménou několika výrobců mezi nimiž hrají prim Fujitsu a NEC. Od nich zobrazovače nakupují všichni renomovaní výrobci televizorů. Do oboru CCTV však PDP díky své vysoké ceně zatím nepronikl.

Jak tento panel vlastně funguje?

Luminofor je podobně jako u klasické barevné obrazovky tvořen miniaturními poli luminoforů pro složkové barvy (RGB). Rozdíl je však ve způsobu jejich buzení. Jestliže u klasické vakuové obrazovky jsou luminofony buzeny elektronovými paprsky, u PDP je pod každým luminoforem miniaturní komůrka s plynovou náplní a se samostatně adresovatelnou elektrodou. Přivedením napětí na elektrodu dojde k zážehu plynové náplně a ke vzniku ultrafialového záření, které aktivuje příslušný luminofor. Jak vidíme, je vlastně struktura zobrazovače digitální – je tvořena diskretními komůrkami pod každým luminoforem jednoznačnou adresou v maticové struktuře, pod kterou je identifikována a také buzena.

Obr. 5-29: PDP monitor (JVC).



### Vybavení monitorů

Pro aplikace v CCTV jsou to přístroje velice jednoduché s minimem ovládacích prvků – většinou v kovové skříni nebo uzpůsobené pro montáž do 19" skříně. Rozlišovací schopnost černobílých monitorů je vždy vyšší než rozlišovací schopnost libovolného prvku v řetězci CCTV (kamer, videorekordérů). Uváděny jsou hodnoty okolo 800 řádků.

Monitory mají normalizovaný nesymetrický vstup na konektoru BNC s možností odpojit zakončovací impedanci 75 W v případě prosmyčkování k dalším přístrojům; výstup mají rovněž na konektoru BNC. Z hlediska synchronizace musejí pracovat ve stejné normě (CCIR) jako zdroj videosignálu (kamera, videorekordér).

Barevné monitory mají většinou vybavení vstupy, výstupy a ovládacími prvky poměrně rozsáhlejší. U vyšší třídy barevných monitorů je k dispozici Y/C vstup S-VHS kompatibilní, popř. samostatné vstupy RGB. Zde je velice důležité, zda je monitor schopen pracovat ve stejné normě (PAL, SECAM, NTSC...) jako připojený zdroj videosignálu.

Rozlišovací schopnost u barevných monitorů je parametrem, který je nutno sledovat, neboť na rozdíl od černobílých monitorů díky odlišné konstrukci obrazovky existují rozdíly v rozlišovací schopnosti v závislosti na úhlopříčce, a hlavně na třídě výrobku. Konkrétní hodnoty monitorů používaných v CCTV jsou 320 řádků, 450 řádků, výjimečně i 550 řádků. Monitory s vyšší rozlišovací schopností spadají svým provedením i cenou do oblasti studiové TV techniky.



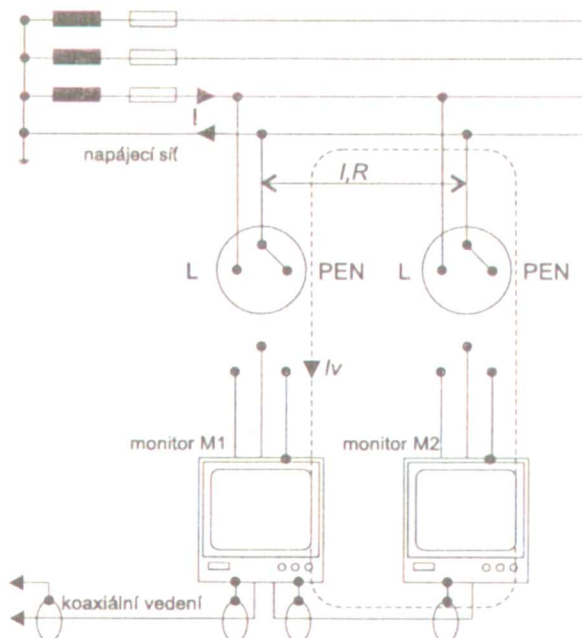
*Poznámka – V případě budování barevného systému CCTV s více monitory na jednom pracovišti se nedoporučuje použití neznačkové techniky. Praxe ukazuje, že dlouhodobě spolehlivý provoz včetně zachování shodného barevného podání u všech monitorů může zajistit pouze technika vyššího standardu.*

Velice důležité je u monitorů provedení videovstupu a videovýstupu. Vzhledem k tomu, že monitory jsou většinou konstruovány jako elektrický předmět třídy I., je stínění BNC konektorů videovstupu a videovýstupu galvanicky spojeno s kostrou přístroje. Při prosmyčkování více monitorů může dojít k vyrovnávání zemních potenciálů nulového vodiče příslušného lokálnímu napájení monitorů. Toto vyrovnávání zemních potenciálů pak vede ke vzniku brumového pásu na obrazovce, a v některých případech může dojít až k rozpadnutí synchronizace. Princip vzniku tohoto efektu je naznačen na obr. 5-34. Proto se při budování nových systémů CCTV provádí samostatné napájení všech prvků v systému zapojených, a to se samostatným jištěním, a zásadně třížilově (dle ČSN 33200-4-41).

Problematiku zemních vyrovnávacích proudů lze bez rekonstrukce síťových rozvodů řešit buď aplikací širokopásmových oddělovacích transformátorů v signálové videocestě, či oddělením pomocí izolačních videozesilovačů (což je relativně drahé řešení), nebo napájením monitoru z bezpečnostního oddělovacího transformátoru 1 : 1. Tím se převede ochrana zemněním na ochranu oddělením obvodů, a pak není kostra monitoru galvanicky spojena s ochranným vodičem sítě. V každém případě je však nutno dbát na dostatečné dimenzování oddělovacího transformátoru. Jeho provedení z hlediska bezpečnosti musí odpovídat příslušným normám. S výhodou lze u dlouhých tras videosignálu využít i videozesilovače s galvanickým oddělením pomocí optoelektronických vazebních členů (optronů).

Vzhledem k tomu, že ochranný vodič je současně vodičem pracovním, uzavírá se přes něj proudový okruh a matematicky lze z toho vyvodit tyto důsledky:

$$I \neq 0, I_v \neq 0, R \neq 0 \Rightarrow \Delta U \neq 0$$



Obr. 5-30: Důvod vzniku brumových pásů u dvojitých rozvodů.

Tento nenulový rozdíl potenciálů se uzavírá přes stínění koaxiálního kabelu mezi monitory a způsobuje vznik vyrovnávacího proudu  $I_v$ . Ten se superponuje na videosignál a podle velikosti rozdílu potenciálů se projeví temným brumovým pásem na obrazovce. Je-li zdroj videosignálu synchronní se sítí, má pás na obrazovce stálou polohu. Při interní či externí synchronizaci může dojít k jevu, že se brumový pás po obrazovce pohybuje. Situace naznačená na obr. 5-30 platí samozřejmě obecně pro libovolná zařízení systému CCTV napájená ze sítě třípólovou vidlicí (kamery, přepínače...).

Volba velikosti monitoru vychází především z optimální pozorovací vzdálenosti obsluhy.

Tabulka 5-15: Pozorovací vzdálenost monitorů

Úhlopříčka	Pozorovací vzdálenost (m)		
	minimální	optimální	maximální
12	0,3	0,5	1
23	0,5	1	2
31	0,7	1,4	2,8
36	0,8	1,6	3,2
43	1	2	4,1

V určitém zjednodušení lze říci, že optimální pozorovací vzdálenost se rovná pětinásobku úhlopříčky sledovaného obrazu. Větší úhlopříčky (44 – 61 cm) se pak používají pro multikamerové systémy se zobrazením záběrů více kamer na jediném monitoru.

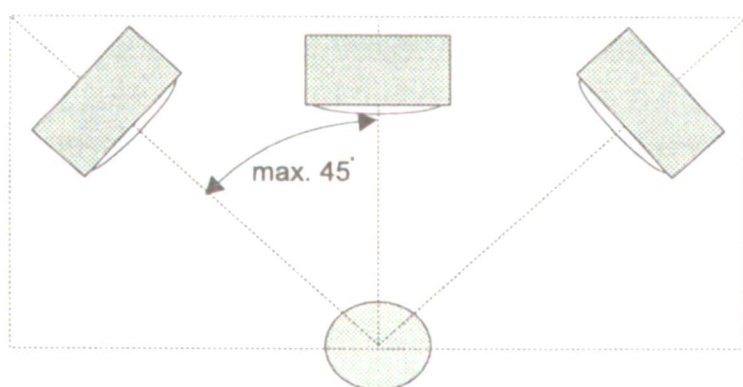
Při navrhování a instalaci monitorových stěn platí dále určité zásady z hlediska ergonomie daného pracoviště.

Obecně by krajní monitor v řadě neměl být z místa pozorovatele vzdálen více, než je vzdálenost tvořící s osou pozorovatele úhel  $45^\circ$ . Ideální je uspořádání na úseku kružnice tak, jak je naznačeno na obr. 5-31.

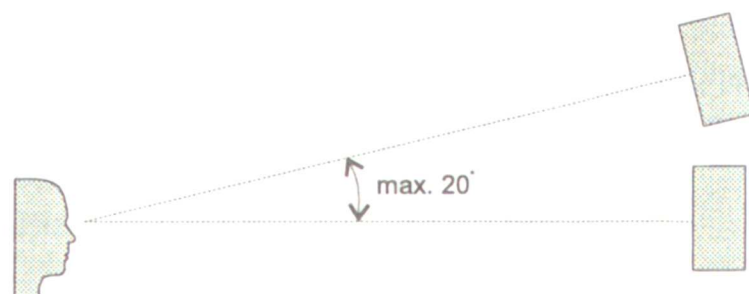
Při instalaci monitorů nad sebou by nejvýše umístěný monitor neměl svírat s vodorovnou osou proloženou ve výši očí pozorovatele více než  $20^\circ$  (obr. 5-32).

### 7.2 Kamerové přepínače

Umožňují zobrazit na jediném monitoru pohled z více kamer, ale nikoli současně. Podle typu lze právě zobrazený vstup volit ručně nebo automaticky s naprogramovanými časy přepínání pro jednotlivé vstupy.



Obr. 5-31: Umístění monitorů v horizontální rovině.

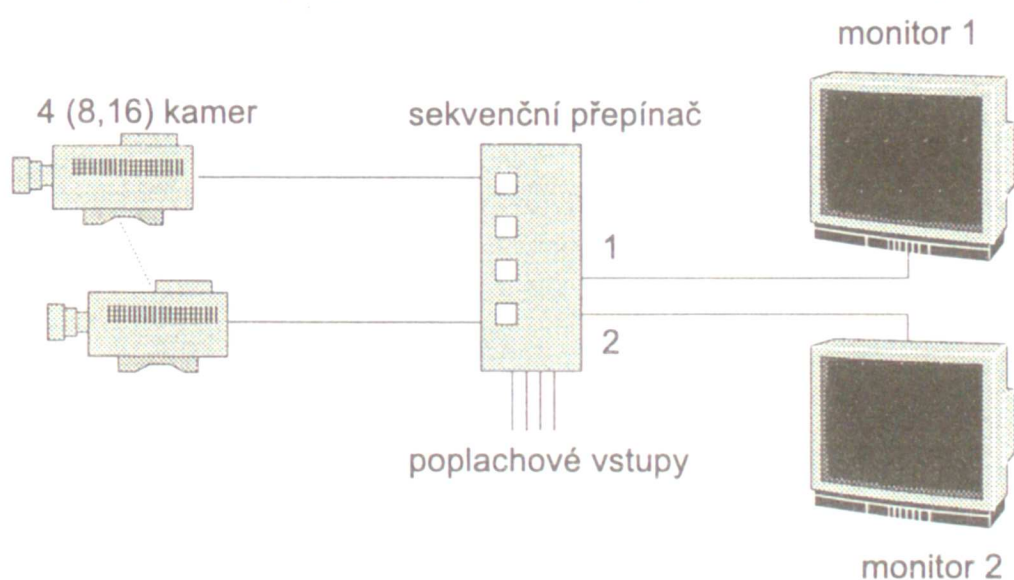


Obr. 5-32: Umístění monitorů ve vertikální rovině.

Nejjednodušší typy mají pouze jeden nastavitelný čas přepínání, jeden výstup a možnost přemostit neosazené vstupy.

Nejrozšířenější jsou typy s poplachovými vstupy, jejichž aktivace na základě vnějšího podnětu způsobí, např. u EZS, automatické zobrazení záběru kamery z prostoru, ve kterém došlo k vyhlášení poplachu. Vyšší typy jsou navíc vybaveny generátorem času a znaků s možností přiřadit každému vstupu název snímaného prostoru, přiřadit poplachové texty atd.

Optimální variantu pro aplikace CCTV bez záznamu tvoří sekvenční přepínače se 4 – 8 – 16 vstupy vybavené dvěma nezávislými výstupy. Pro každý videovstup jsou vybaveny poplachovým kontaktem s jedním sumárním poplachovým výstupním kontaktem s možností programového řízení přepínacích časů pro každý krok sekvence zvlášť



Obr. 5-33: Standardní konfigurace kamerového přepínače.

a s možností opakovaného zařazení daného vstupu do sekvence. Výstup 1. umožňuje sledovat naprogramovanou sekvenci 1 nebo přímou ruční volbu z klávesnice přístroje a výstup 2. umožňuje sledování naprogramované sekvence 2. Při aktivaci libovolného poplachového vstupu se zobrazí na výstupu 2. příslušný signál videovstupu svázaný s poplachem. Zabudovaný bzučák upozorní obsluhu na poplach, systém resetování poplachových událostí podporuje aktivitu obsluhy při řešení poplachových událostí.

*Poznámka: V případě využití jednoho z výstupů jako výstupu pro nahrávání na videomagnetofon s dlouhou dobou záznamu (timelapse) musíme počítat s rušivými jevy v záznamu při přepínání z jedné kamery na druhou (z důvodu synchronizace). Dalším nedostatkem při využití sekvenčního přepínače spolu se záznamem je nárůst mrtvých časů mezi záznamem jedné a téže kamery v rámci sekvence. Přijatelným kompromisem je aplikace max. čtyř systémových kamer napájených a synchronizovaných z kompaktního systémového monitoru se zabudovaným přepínačem a připojení videomagnetofonu v modu max. 24 hod.*

### 7.3 Děliče obrazu, kvadrantový selektor

Obr. 5-34: Kamerový přepínač (Videor Technical).



Tato zařízení slouží k **současnému** zobrazení záběrů více kamer na jediném monitoru. Zařízení mají 2 (4, 8) vstupů a pracují s digitalizací vstupních signálů. Nejde tedy o zobrazení v reálném čase, vstupní signály nemusejí být synchronizovány.

Zařízení kromě své základní funkce může být vybaveno poplachovými vstupy, vkládáním textů, data a času, prosmyčkovanými vstupy, dvěma výstupy s možností odlišného programového řízení. To vše jsou alternativy uživatelského komfortu vícenásobných děličů obrazu.

*Poznámka – Při záznamu takto sloučeného obrazu je třeba si uvědomit, že dochází ke snížení rozlišovací schopnosti. Pro kvadrantový selektor a záznam na úrovni rozlišovací schopnosti systému VHS vychází výsledná rozlišovací schopnost v černobílém režimu 150 řádků, což je citelná ztráta rozlišení. Zvláště v případech požadavku identifikace detailů ve snímané scéně může být toto snížení rozlišovací schopnosti limitujícím faktorem.*

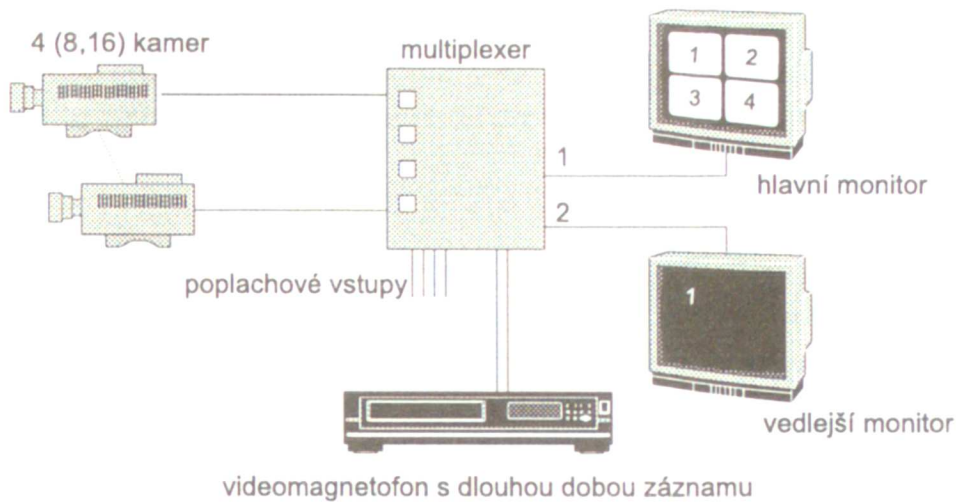


Obr. 5-35: Standardní konfigurace kvadrantového selektoru.

## 7.4 Multiplexery

Tato zařízení umožňují realizaci multikamerových systémů s dokonalým záznamem. Multiplexery jsou vybaveny 4 až 16 vstupy videosignálu. Výhoda multiplexerů se projeví především při požadavku záznamu a následné analýzy záznamu. Multiplexer je přímo propojen s videorekordérem s dlouhou dobou záznamu (timelapse) a spolupracuje s ním jak při záznamu, tak při přehrávání. Umožňuje oproti běžným videopřepínačům zkrátit na minimum mrtvý čas v sekvenci záběrů, tzn. dobu, po kterou není signál od příslušné kamery zaznamenáván.

Zařízení pracuje s digitalizací videosignálu, tzn. nejde o zpracování signálu v reálném čase. Obvody vyrovnání časové základny (TBC) umožňují do systému připojit kamery, které nejsou vzájemně synchronizované. Vlastní záznam se uskutečňuje po snímcích (nebo pulsnímých) od každé kamery v sekvenci spolu s kódem pro každou kameru. Při



Obr. 5-36: Standardní konfigurace pracoviště s multiplexerem.

přehrávání pracuje multiplexer jako dekodér; je schopen jednotlivé obrazy skládat a posílat na monitor v kvazispojité podobě. Příslušnou volbou na klávesnici multiplexeru je možné vybrat jednotlivé kamery, popř. vytvořit na stínítku obrazovky vícenásobný obraz od kamer pro potřebu analýzy poplachových dějů. Vybavení multiplexerů umožňuje navíc i elektronickou paměť obrazů, dvojnásobné zvětšení a možnost prohledávání detailů v tomto zvětšení. Vkládání dat, času, identifikace kamer a poplachové vstupy pro každou kameru zvlášť jsou samozřejmé. Některé typy mají zabudovanou logiku jednoduchého videosenzoru s možností vytvořit v rámci zorného pole aktivní pole, v nichž dochází ke komparaci signálu. Dojde-li ke změně scény např. pohybem osob či vozidel, je automaticky aktivován poplachový režim multiplexeru s preferováním záznamu od kamery, která tento děj vyvolala. Záznamy ostatních kamer zůstávají zachovány pro potřebu širší analýzy dějů v objektu.



Obr. 5-37: Multiplexer (Dedicated Micros).

Princip vzorkování obrazu a digitální zpracování v paměti přístroje jsou vyřešeny tak optimálně, že nedochází ke ztrátě rozlišovací schopnosti. Většinou je uváděna šířka pásma až 10 MHz. Multiplexery jsou nabízeny ve variantě simplex, která obsahuje pouze jeden modul obrazové paměti. Je-li tedy v provozu záznam na videomagnetofonu, není

tento multiplexer schopen v živém modu zobrazovat na jeden monitor pohled více kamer najednou (multiscreen). To umožňuje pouze varianta duplex, která obsahuje dva moduly obrazové paměti. Jeden slouží pro záznam na videorekordér, druhý pro operativní práci obsluhy v živém modu.

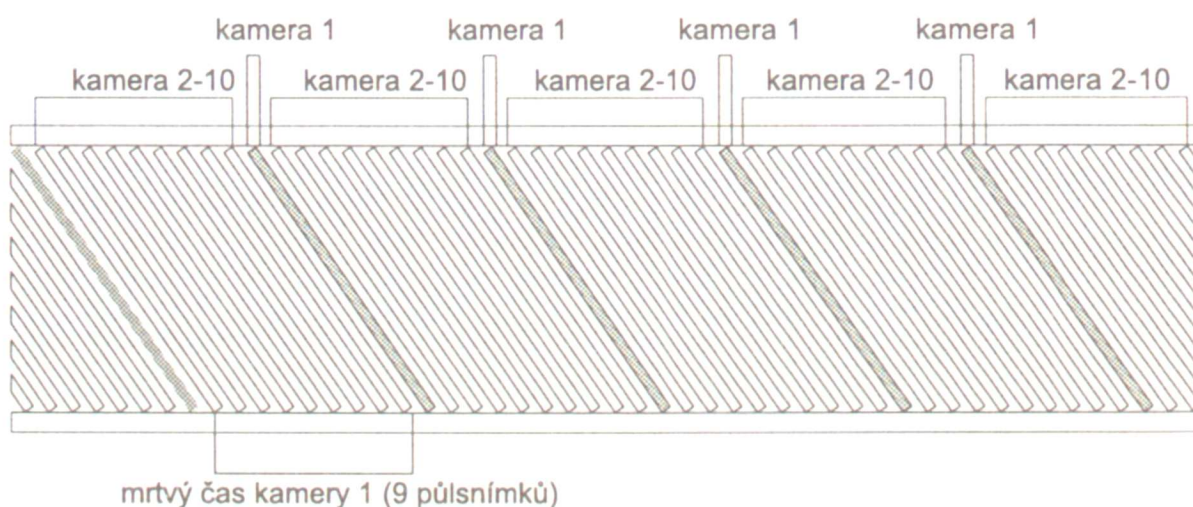
### 7.4.1 Dlouhodobý záznam v multiplexním provozu

Multiplexní zařízení pracující synchronně s videorekordérem (v provedení simplex pro záznam a následné vyhodnocování nebo v provedení duplex s možností současného multiplexního nahrávání a multiplexního zobrazení živých obrazů).

Z pohledu tří stanovených kritérií lze říci:

1. Kvalita obrazu je prakticky shodná s kvalitou reprodukce záznamu jedné kamery.
2. Mrtvý čas, pro náš příklad 120 hod. záznamu a 10 kamer, bude roven  $(10 - 1) \times 20 \text{ ms} \times 40 = 7,2 \text{ s}$ .
3. Vzhledem k možnosti volby zobrazit na monitoru pohled zájmové kamery samostatně, popř. vícenásobné zobrazení, je vyhodnocování velice pohodlné.

Jaký režim záznamu timelapse videorekordéru při multiplexním záznamu zvolit? Podle použitého typu videorekordéru máme k dispozici max. 24 hod., 480. hod.,



Obr. 5-39: Poloha stop při multiplexním záznamu.

či 960. hod. videozáznamu na 3hod. kazetu (E 180). Rozhodnutí pro správný režim nevychází však jen z technických možností timelapse videomagnetofonu, ale i z dynamiky a četnosti sledovaných procesů, popř. předpokládaných dějů, topologie sledovaného prostoru, rozmístění a počtu kamer, a samozřejmě z předpokládaného režimu provozu monitorovacího pracoviště – hlídací služby.

Vyjdeme-li z použití tříhodinové kazety (E 180) s kapacitou 540 000 šikmých stop (pulsů), lze sestavit tabulku 5-16, kde je vidět pro jednotlivé časové režimy čas záznamu jednoho pulsů a počet pulsů sejmutých za 1 s pro systém s jednou kamerou a multiplexní záznam se 4, 8, 9, 10, 16 kamerami.

Tabulka 5-16: Srovnání multiplexního záznamu pro různé časové režimy a různý počet kanálů

Kazeta E 180			9 kamer - 9 kanálů		10 kamer - 10 kanálů		16 kamer - 16 kanálů	
počet stop (půlsnímků)	dnů	časový mód (hod.)	obr./s na kanál	s/obr.	obr./s na kanál	s/obr.	obr./s na kanál	s/obr.
540 000	-	3	5,56	0,18	5	0,2	3,13	0,32
540 000	1	24	0,69	1,44	0,63	1,6	0,39	2,56
540 000	2	48	0,35	2,88	0,31	3,2	0,2	5,12
540 000	3	72	0,23	4,32	0,21	4,8	0,13	7,68
540 000	4	96	0,17	5,76	0,16	6,4	0,1	10,24
540 000	5	120	0,14	7,2	0,13	8	0,08	12,8
540 000	10	240	0,07	14,4	0,06	16	0,04	25,6
540 000	20	480	0,03	28,8	0,03	32	0,02	50,12
540 000	40	960	0,02	57,6	0,02	64	0,01	102,4

Do kapitoly volba režimu provozu patří i režim výměny a archivace nahraných kazet, stanovení jejich životního cyklu a doporučení nejvhodnějšího typu kazety.

Zásadní požadavky na kazetu jsou v podstatě čtyři:

- robustní bezporuchová mechanika kazety,
- dostatečná mechanická odolnost podložky (zesílená rubová strana),
- vlastnosti magnetické vrstvy (odolnost proti oděru),
- délka kazety 180 min.

Magnetická vrstva musí být vhodná pro vícenásobný přepis s minimální ztrátou kvality obrazu; mechanicky musí být pásek stabilní ve vysoce náročném vzorkovacím režimu.

Stanovení počtu kazet pro běžný provoz vychází ze tří kritérií:

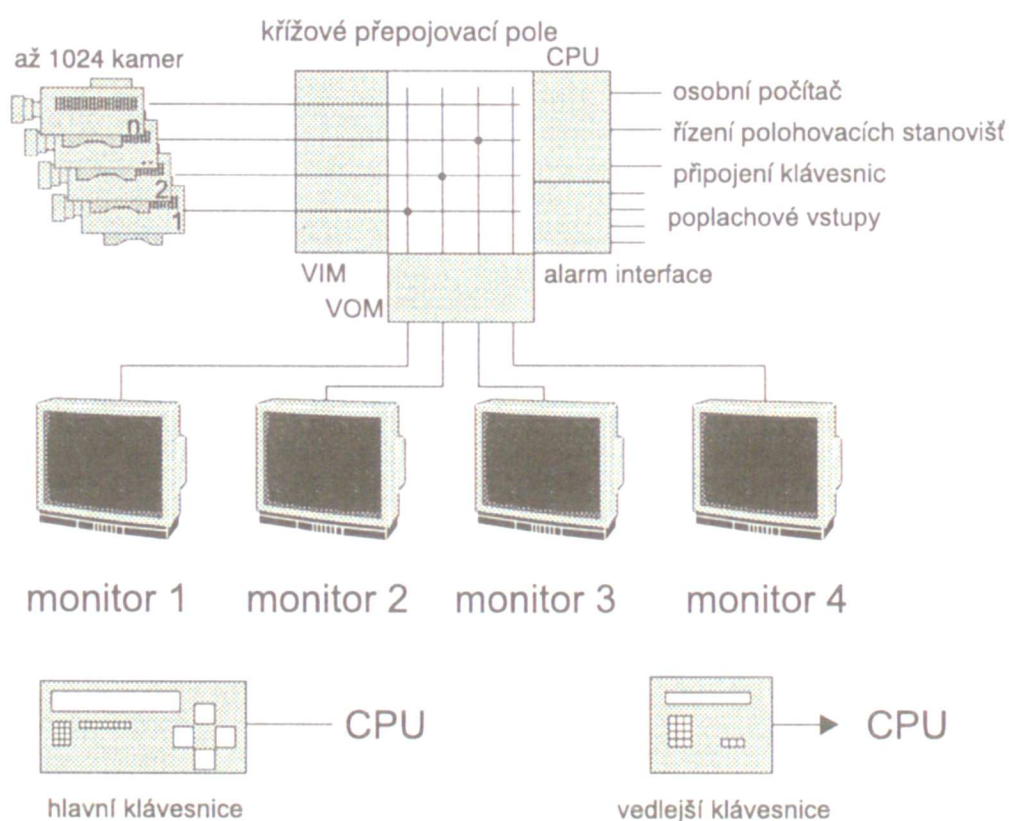
- **navolený timelapse režim** na videomagnetofonu,
- **předepsaná doba archivace**, která se liší podle vnitřních předpisů uživatele videosystému,
- **doporučený počet následných přepisů**, který vychází z požadavku zachování kvality obrazu a pohybuje se podle typu pásku v mezích 10 – 20x.

### 7. 5 Křížové přepojovací pole

Křížové přepojovací pole, jinak též nazývané videoústředna či maticový přepínač, je zařízení určené pro rozsáhlé aplikace s velkým množstvím kamer a monitorů. Jeho základem je matice s analogovými spínači umožňujícími obecně přepojit kteroukoli kameru na kterýkoli monitor. Zařízení pracuje bez digitalizace obrazu, tedy v reálném čase. Způsob, jakým je tato základní funkce řešena, se liší u jednotlivých výrobců v nepodstatných detailech. Do rozsahu cca 32 vstupů na 16 výstupů jsou většinou křížová přepojovací

pole řešena jako kompaktní zařízení s pevně daným hardwarem. Tato zařízení umožňují programování a provoz bez použití nadstavbového PC. Pro větší systémy je vhodné budovat křížové přepojovací pole z modulových komponentů, a tím v rámci požadavků daných zákazníkem optimalizovat i náklady na takto budovaný systém.

Základem je centrální procesorová jednotka (CPU), tj. jednotka, která se stará o programové řízení celého křížového přepojovacího pole. Obvykle je vybavena několika porty RS 232 pro připojení operačních klávesnic, modulů poplachového řízení, expanderů



Obr. 5-40: Konfigurace křížového přepojovacího pole.

portu pro řízení polohovacích stanovišť, a samozřejmě pro připojení osobního počítače pro účely buď nastavování parametrů systému, anebo pro potřeby přímého řízení z nadstavbového softwaru. Implementace konkrétních požadavků uživatele na selektivní přístup k jednotlivým kamerám a monitorům a další uživatelské funkce (texty, sekvence, typ zobrazení, poplachové řízení atd.) je možné operativně měnit pomocí set-up softwaru z PC připojeného na jeden z portů RS 232 řídicí jednotky. Set-up software je chráněn přístupovými právy proti neoprávněnému použití. Samozřejmostí je vkládání alfanumerické identifikace jednotlivých kamer, systémového času a poplachových zpráv.

Kamery jsou připojovány na jednotky vstupů (VIM), jež jsou obvykle řešeny jako sdružené pro 8 nebo 16 vstupů.

Monitory jsou připojovány na jednotky výstupů (VOM), jež jsou obvykle řešeny jako sdružené pro 2 nebo 4 výstupy.

Podle požadované konfigurace systému lze připojit k systému až desítky klávesnic různého typu podle požadavků na uživatelský komfort konkrétního pracoviště.

Klávesnice mohou mít softwarově přiřazeny určité kamery a určité monitory, v případě kolize ovládání z více pracovišť je možné stanovit hierarchie – pořadí, posloupnost podle hodnoty, důležitosti jednotlivých klávesnic.

Některé typy klávesnic umožňují změnu nastavení parametrů systému (hlavní programovací klávesnice). Toto řešení se nedoporučuje, neboť u rozsáhlých systémů se



výrazně jeví tendence oddělit zodpovědnost za ovládání od zodpovědnosti za vlastní provoz, údržbu a aktualizaci nastavení ve vazbě na režimové změny provozu objektu.

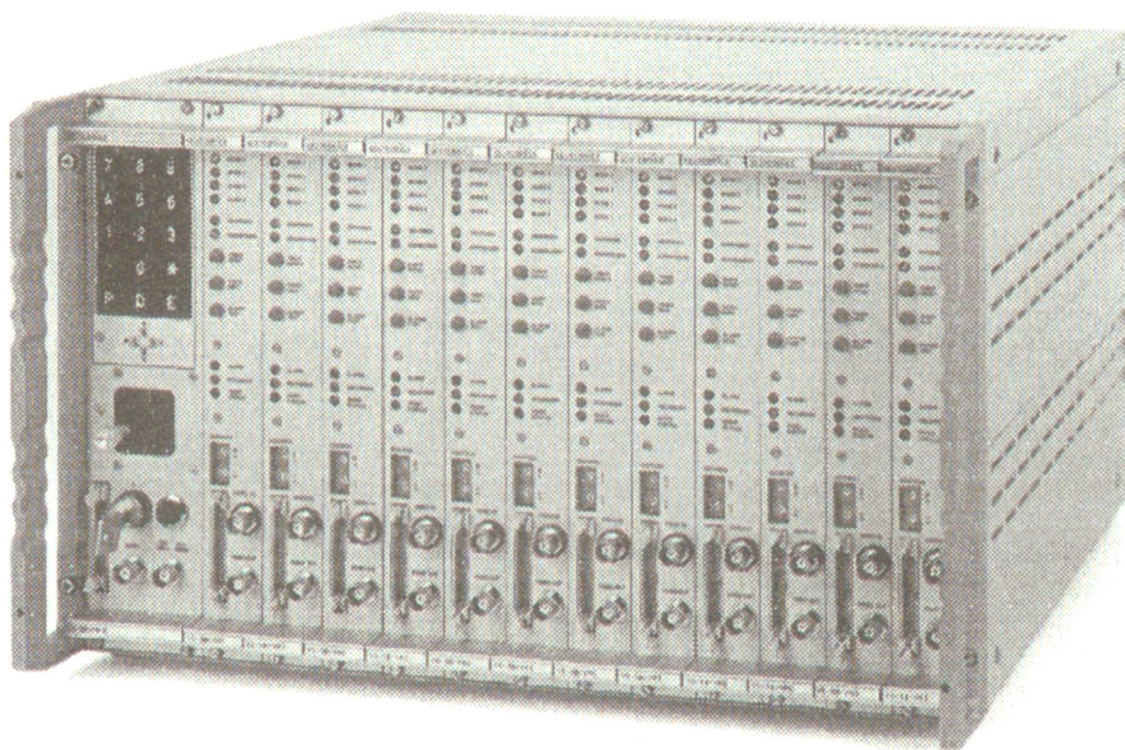
Klávesnice může rovněž umožňovat ovládání polohovacích stanovišť s pamětí nastavení souboru nepoužívanějších pozic. Může dále řídit pomocné příslušenství, jako je např. reflektor, ostřikovač či stěrač okénka kamerového krytu.

### 7. 6 Videodetektor

Videodetektor (jinak též digitální detektor pohybu) je zařízení, které slouží k indikaci narušení snímaného prostoru pomocí porovnávání obrazu zorného pole v klidu a při narušení prostoru jakýmkoli pohybem.

V dnešní době bouřlivého rozvoje digitální a multimediální techniky jsou videosenzory spjaty nejčastěji s multiplexery či se zařízeními na záznam obrazu.

Základní funkcí videosenzoru je především vytvoření aktivních ploch v zorném poli kamery (či všech připojených kamer). V těchto polích dochází k porovnávání obrazu a jakýkoli pohyb je identifikován a následně zpracován jako povel k určité činnosti zařízení (odstartování záznamu, sepnutí relé, změna režimu zařízení...).



Obr. 5-41: Profesionální videodetektor (Geutebrück).

K omezení nechtěných vyhlášení mají videosenzory další funkce:

- **maskování** deaktivuje podněty, které jsou mimo oblast zájmu (veřejné komunikace, pohyb větví stromů vlivem větru, změna odlesků od ploch s velkou odrazivostí při změně sluneční aktivity a počasí během dne atd.);
- **citlivost** stanovuje prahovou úroveň změny při komparaci videosignálu s předchozím obrazem snímané scény;
- **počet narušení** eliminuje, podobně jako u PIR detektorů, možné falešné poplachy;
- **minimální velikost** identifikovaného předmětu eliminuje poplachy způsobené drobným zvířectvem.

Nejdokonalejší zařízení tohoto druhu umějí dokonce rozeznat směr pohybu sledovaného objektu, vyznačit jeho trajektorii na obrazovce, spočítat rychlost pohybu, přepočítat z perspektivy skutečnou velikost a další parametry sledovaného objektu.

Tyto systémy dnes fungují prakticky jako nadstavba běžného PC počítače a jejich vlastnosti určuje především koncepce speciálního, mnohdy velice drahého softwaru. Jejich obliba a úspěšnost na trhu CCTV roste zvláště v aplikacích integrovaných bezpečnostních systémů, kde monitorování všech bezpečnostních funkcí objektu na jediném pracovišti na PC je více než účelné.

## 8. Záznam obrazu

K dokumentování dějů, a to zvláště v případě napadení objektů, je účelné zařadit do videořetězce záznamové zařízení. V současné době jsou pro archivaci záběrů kamer k dispozici 3 technické prostředky – videorekordér, videotiskárna a digitální videorekordér.

### 8.1 Videorekordér s dlouhou dobou záznamu

Tento videorekordér byl vyvinut speciálně pro potřeby záznamu dějů v bezpečnostních aplikacích systémů CCTV. Umožňuje vedle běžného typu záznamu v reálném čase (50 pulsů/s.) nahrávat signál ve vzorkovacím režimu. Vzorkovací režim prodlužuje záznam na běžnou kazetu E 180 (3 hod.) podle nastavení na 24, 48, 72, 120, 168, 240, 480 až 960 hodin. Některé typy videorekordérů umožňují rovněž externí řízení při záznamu s možností nahrávat jednotlivé snímky. Volba vzorkovacího režimu pro konkrétní aplikace závisí na dynamičnosti snímaných dějů a velikosti zorného pole snímané kamery. Na trhu jsou k dispozici tři kategorie: do 24 hod., do 480 hod., do 960 hod. Videorekordér dále umožňuje přes poplachový vstup změnu záznamového režimu na záznam v reál-



Obr. 5-42: Videorekordér s dlouhou dobou záznamu (Mitsubishi).

ném čase (3hod. mod). Tohoto vstupu je možné využít při kombinaci s EZS, kde narušení určitého prostoru či vstup do chráněného prostoru jsou indikovány EZS, a současně je prostor snímán. Přejde-li tedy od EZS řídicí signál, videorekordér přejde do kontinuálního režimu, a tím je zajištěn záznam událostí v daném prostoru bez časových prodlev. V klidovém stavu bez událostí je videorekordér v příslušném vzorkovacím režimu s časovými prodlevami mezi jednotlivými snímky. Tím se šetří záznamový materiál a zkracuje a usnadňuje se zpětná analýza dějů v narušeném prostoru.

Videorekordér obsahuje většinou i poplachový výstup, jímž je možno řídit např. optické či akustické signalizace k upozornění hlídací služby atd.

Standardně jsou tyto videorekordéry vybaveny generátorem data a času. Tyto údaje jsou automaticky vkládány do záznamu a umožňují pozdější detailní analýzu časového průběhu poplachových dějů.

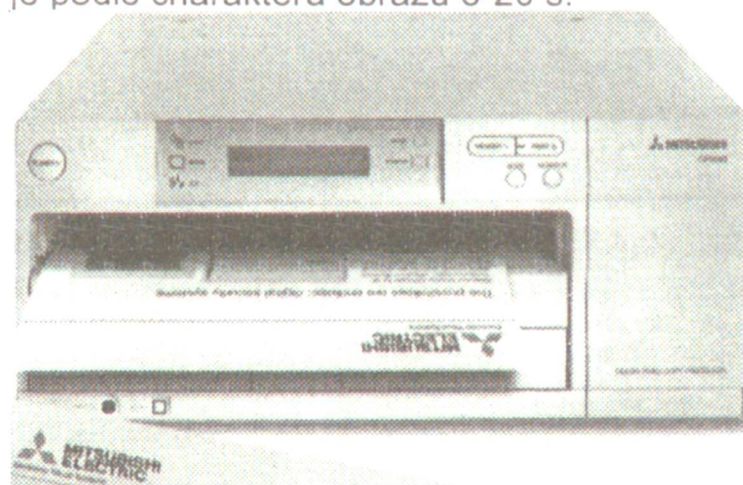
Ke speciální výbavě videorekordérů s dlouhou dobou záznamu patří vkládání tzv. VISS kódu do záznamu. Jeho pomocí je pak možné velice snadno nalézt počátek poplachového záznamu.

*Poznámka – Z dnešního pohledu je využívání analogových videorekordérů s dlouhou dobou záznamu již minulostí a většina aplikací je již dnes nahrazena digitálními systémy záznamu.*

### 8.2 Videotiskárna

Toto zařízení umožňuje převést videosignál do digitální podoby a digitalizovaný obraz vytisknout na termotiskárně. Podle požadavků na celý systém je možné zvolit černobílý či barevný tisk (podle zvoleného typu videotiskárny).

Obvyklé formáty snímků z videotiskárny jsou 100x74 mm a 250x190 mm. Doba tisku je podle charakteru obrazu 6-20 s.



Obr. 5-43: Videotiskárna (Mitsubishi).

*Poznámka – Velkou výhodou termotiskáren je skutečnost, že snímek je prakticky okamžitě k dispozici.*

### 8.3 Digitální záznam obrazu

Zkušenosti s digitalizací obrazu dovedly výrobce multiplexerů logickou cestu až k vývoji digitálních záznamových zařízení a jejich uvedení na trh. Komerční dostupnost

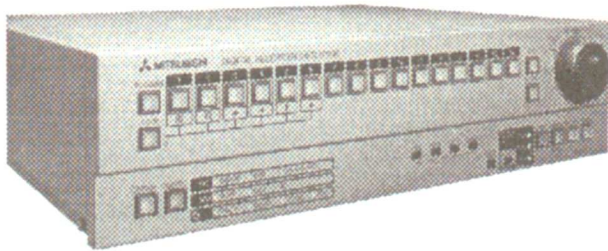
pak byla podmíněna vývojem v oblasti digitální, a částečně i komerční AV techniky, především:

- vývojem nových a zlepšováním parametrů stávajících periférií (DV, DVD, CD-R, ZIP, JAZ, rychlé HD atd.),
- snižováním ceny paměťových médií, a hlavně
- vývojem nových, účinnějších kompresních algoritmů.

Principy digitálního záznamu jsou uvedeny v **kapitole 6 IP-kamerové systémy**.

### 8.4 Snímkovací fotokamera

Svým principem se sice vymyká rámci oboru CCTV, ale s naší tematikou úzce souvisí vzhledem k účelu nasazení. Toto zařízení slouží rovněž k záznamu poplachových dějů. Od ostatních prvků v této kapitole uvedených se odlišuje fyzikálním principem záznamu. Jde o klasický fotografický proces. Elektronická nadstavba umožňuje realizovat vzorkovací režimy a v poplachovém modu kontinuální záznam. Dodatková elektronika umožňuje rovněž vkládat do snímků datum a čas, popř. i další identifikační znaky.



Obr. 5-44: Digitální videorekordér (Mitsubishi).

Dálkové ovládání a možnost propojení s EZS jsou samozřejmé. Určitou nevýhodou je použití poměrně drahých kazet s 35mm filmem a skutečnost, že snímek není okamžitě k dispozici, ale je nutné film nechat zpracovat klasickým fotoprocesem.

*Poznámka – Podstatnou výhodou je však vynikající rozlišovací schopnost až 8 640 000 pixelů (záznam VHS 120 000 a S-VHS 225 000) a výrazně vyšší vypovídací síla v případě použití tohoto typu záznamu v soudním řízení. S tímto způsobem záznamu se můžeme setkat zvláště v bankovní sféře. Obvyklé*



*bývá klasický videosystém v peněžním ústavu doplněn o snímkovací filmovou kameru umístěnou u vstupních dveří a snímající všechny odcházející osoby. Na videozáznamu lze sledovat poplachovou událost v kontextu, na filmovém záznamu pak je možné lépe identifikovat konkrétní účastníky této události.*

Obr. 5-46: Snímkovací fotokamera (Robot).

## 9 Zřizování systémů CCTV

Pomocníkem při návrhu, realizaci a provozování systému CCTV je norma ČSN EN 50132-7, která poskytuje pokyny pro zajištění funkce systémů CCTV a má sloužit všem, kteří jsou odpovědní za zadávání zakázek, výběr dodavatele, stanovení provozních požadavků, formulování specifikací systému, montáž, funkční zkoušky, předání systému a zajištění údržby během provozu.

Celý proces zřizování systému CCTV lze logicky rozdělit do několika etap a tyto etapy jsou dále i názvy jednotlivých částí kapitoly. V rámci částí jsou uvedeny i odkazy na jednotlivé články normy ČSN EN 50132-7 Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích, Část 7: Pokyny pro aplikaci.

Tabulka 5-17: Etapy zřizování systémů CCTV

Etapy procesu	Činnost	Dokumentace/záznamy
I. zadání	<ul style="list-style-type: none"> <li>analýza potřeb zákazníka</li> <li>technická analýza objektu</li> </ul>	<ul style="list-style-type: none"> <li>dotazník zákaznických požadavků</li> <li>topologie objektu</li> <li>rámcová koncepce (studie)</li> </ul>
II. návrh	<ul style="list-style-type: none"> <li>zpracování technické specifikace systému</li> </ul>	<ul style="list-style-type: none"> <li>nabídka s konkrétním technickým řešením (systémový návrh)</li> <li>návrh smlouvy</li> </ul>
III. přezkoumání návrhu a příprava realizace	<ul style="list-style-type: none"> <li>ověření úplnosti a realizovatelnosti</li> <li>odsouhlasení zákazníkem</li> <li>zpracování změn</li> <li>projekce</li> </ul>	<ul style="list-style-type: none"> <li>odsouhlasená smlouva</li> <li>změny ve smlouvě</li> <li>upravený systémový návrh</li> <li>výkresová dokumentace a soupis použitého materiálu</li> </ul>
IV. realizace	<ul style="list-style-type: none"> <li>montáž</li> <li>výchozí revize</li> <li>oživení</li> <li>funkční zkoušky</li> <li>předání</li> <li>zkušební provoz</li> <li>předání do trvalého provozu</li> </ul>	<ul style="list-style-type: none"> <li>protokol o předání a převzetí staveniště</li> <li>stavební/montážní deník</li> <li>zpráva o výchozí revizi</li> <li>protokol o funkčních zkouškách</li> <li>předávací protokol</li> <li>projekt skutečného provedení</li> <li>návody k obsluze</li> <li>zápis o vyhodnocení zkušebního provozu</li> </ul>
V. provoz	<ul style="list-style-type: none"> <li>běžná údržba</li> <li>periodické prohlídky</li> <li>pohotovostní servis</li> <li>pravidelné revize</li> </ul>	<ul style="list-style-type: none"> <li>pokyny k údržbě</li> <li>servisní smlouva</li> <li>servisní protokol</li> <li>revizní zpráva</li> </ul>

### 9.1 Etapa I. - zadání zakázky

Návrh systému průmyslové televize (CCTV) vychází z důkladné **analýzy potřeb zákazníka**. Tato úvodní fáze realizace systému CCTV klade na jednající osobu realizační firmy značné nároky, jež v sobě zahrnují dovednosti úspěšného prodejce spolu s poměrně důkladnými technickými znalostmi o nabízených zařízeních i o možnostech CCTV jako celku.

Všeobecné rozšíření komerčních audiovizuálních médií (videokamery, televizory, videomagnetofony, domácí kino ...) vytváří v zákaznících pocit, že oboru vlastně také rozumí. Snaží se své, často nereálné představy prosazovat, a pak dochází k určitým konfliktům a okamžikům nepochopení při sběru základních informací o účelu navrhovaného videosystému.

V této fázi je vedle ústního rozhovoru účelné používat jednoduché dotazníky, soubory otázek a názorné pomůcky pro ujasnění pojmů a pochopení funkcí základních prvků videosystému. Zvláště účelné je předvést potenciálnímu zákazníkovi rozdíly:

ve snímání	- černobíle/barevně
	- standardní rozlišení/vysoké rozlišení
v záznamu	- VHS/S-VHS/digital

Soubory otázek by měly zákazníkovi pomoci ujasnit cíl a účel využití CCTV v jeho objektu. Otázky „Proč chcete vybudovat CCTV?“, „Jaké výsledky od CCTV očekáváte?“ patří do standardního arzenálu při shromažďování základních informací o požadavcích zákazníka. Již ve fázi analýzy potřeb je nutno udržet vyvážený vztah mezi zjišťováním **funkčních a provozních požadavků** na systém CCTV, které slouží pro zpracování předběžné konfigurace systému, která má stěžejní vliv na stanovení nabídkové ceny.

Funkční požadavky jsou výchozím podkladem pro návrh konfigurace systému CCTV. Zachycují požadavky zákazníka na funkci systému na co? kde? kým? a proč? bude systém použit. Pro upřesnění **funkčních požadavků** může sloužit např. rozvinutá osnova uvedená v článku 5.2 normy ČSN EN 50132-7.

Nejprve se stanoví, o jaký **druh objektu** jde z hlediska úrovně rizika. Výběr techniky, výbavy doplňkovými funkcemi a způsob montáže pak konkrétní úrovni rizik zpravidla odpovídá. Běžné provozní monitorování lze zařadit do úrovně 1 (standardní aplikace). Úroveň 2 v sobě již zahrnuje bezpečnostní aspekt využití CCTV (střední úroveň rizik). Objekty, kde je CCTV využita v rámci integrovaného bezpečnostního systému spolu s EZS, EPS, s kartovými systémy, popř. kde plní CCTV sama o sobě určitou střežící úlohu, spadají do vysokých rizik ohrožení - úroveň 3. Bohužel zde neexistuje opora v oblasti normalizace a tedy není možné ani při certifikaci komponent CCTV stanovovat jakékoli stupně zabezpečení tak, jak je to obvyklé u prvků pro systémy EZS.

Dále spolu se zákazníkem stanovujeme oblasti objektu, které budou systémem CCTV pokryty. S velikostí **zorného pole** úzce souvisí stanovení **požadovaného stupně rozlišení** v rámci sledované scény. Při použití kamer se standardní **rozlišovací schopností** (cca 400 TV řádků) můžeme požadavky zákazníka na rozpoznání detailů v rámci snímané scény pro potřeby návrhu kamerové sestavy (především kamery a objektivu) kategorizovat do čtyř skupin tak, jak je uvedeno v čl. 7.6 ČSN EN 50132-7:

- snímání podrobného detailu – **identifikace** kde by cílový objekt (v normě představovaný standardní osobou) neměl představovat při zobrazení méně než 120 % výšky obrazovky,
- snímání detailu – „**rekognoskace**“ kde by cílový objekt neměl představovat při zobrazení méně než 50 % výšky obrazovky,
- snímání polodetailu – „**detekce**“ kde by cílový objekt neměl představovat při zobrazení méně než 10 % výšky obrazovky,
- přehledové snímání (širokoúhlé) – **monitorování skupiny osob** kde by cílový objekt neměl představovat při zobrazení méně než 5% výšky obrazovky.

Poté spolu se zákazníkem probíráme s ohledem na charakter objektu účel pokrytí jednotlivých předem vydefinovaných oblastí. Z toho vyplyne **počet a provedení kamerových stanovišť** potřebných k pokrytí zájmových scén, počet vnitřních a vnějších stanovišť, požadavky na polohovací stanoviště s objektivy s proměnnou ohniskovou vzdáleností. Dodavatelská firma má logicky zájem zrealizovat v rámci systému kamerových stanovišť co nejvíce, zákazník má naopak spíše tendenci potřebný rozsah systému omezit. Argumentem pro optimální rozsah systému jsou reálná rizika objektu vyjasněná se zákazníkem v úvodu jednání. V této fázi musíme rovněž rozhodnout o provedení systému – jako černobílý, barevný či kombinovaný. Zde se vyjasní s ohledem na požadavek denního či nočního snímání i požadavky na citlivost kamer pro potřeby kvalifikovaného návrhu. Při ověřování **intenzity osvětlení scén** je třeba zjistit pro jednotlivá stanoviště orientaci vzhledem ke světovým stranám, umístění sloupů veřejného či firemního osvětlení, intenzitu osvětlení ve dne, popř. i v noci, možnost přisvětlení v noci, druh přisvětlení - viditelné/infra.

Se stavebním provedením objektu, jeho velikosti a topologií souvisí **způsob přenosu videosignálu** i řídicích signálů.

Další oblastí, na kterou je nutno se zaměřit je otázka monitorovacích pracovišť. Zde je třeba určit počet a umístění **monitorovacích pracovišť**, jejich vztah z hlediska kompetencí (řídící, podružné) a jejich režim (obsluhovaný/bezobslužný, denní/nepřetržitý), předběžnou **konfiguraci monitorů** na pracovišti, **požadavek na záznamová zařízení**.

Pro **volbu režimu** zařízení bereme za základ charakter provozu monitorovacího pracoviště (pracovišť). Prvotní členění rozděluje provoz na:

- obsluhovaný,
- bezobslužný.

Vedle tohoto členění mohou existovat ještě kombinace např. přes den obsluhovaný, v noci bezobslužný nebo naopak či z jiného pohledu jako denní a nepřetržitý provoz. V nepřetržitém provozu monitorovací služby je předmět zájmu pro denní dobu často odlišný od noční doby. Tento rozdíl je možno ctít např. nabídnutím zařízení na zpracování videosignálu, který umožňuje využít programově řízených časovačů v software.

V této fázi uvažujeme i o logických vazbách priorit ovládání v případě existence více monitorovacích stanovišť. Tím je myšleno blokování současného ovládání stejné funkce z více stanovišť. Povolení či zamezení přístupu operátora k jednotlivým funkcím zařízení se pak uskutečňuje prostřednictvím řídicího softwaru.

Rovněž mód záznamu vyplývá z režimu provozu. U objektů s nepřetržitou přítomností hlídací služby je možné poplachový záznam řešit jako cílený záznam z určitého místa. Záznam je možné odstartovat buď ručně, nebo automaticky od EZS či kartového systému.

Někdy je požadován nepřetržitý záznam. To lze prakticky nejelegantněji řešit pomocí multiplexeru a odpovídajícího záznamového zařízení. Zde musí korespondovat počet kamer se zvoleným záznamovým módem. Možné je uskutečnit záznam i při použití sekvenčního přepínače, popř. vícenásobného děliče obrazu, musíme zde však počítat s omezenou využitelností záznamu.

Na vícekamerový záznam lze klást z pohledu provozu 3 základní požadavky:

- **optimální kvalita obrazu** – proti kvalitě při záznamu z jedné kamery se nemá projevit žádné omezení;
- **minimalizace mrtvých časů** – mrtvý čas je doba, ve které není zaznamenáván obraz příslušné kamery;
- **optimální možnosti analýzy** – musí být umožněno sledování záznamu při normální rychlosti reprodukce od libovolné kamery. Pro detailní analýzu musí být k dispozici dobrý obraz v režimu stop záznamového zařízení.

**Součinnost s ostatními systémy** v objektu (EZS, EPS, kartové systémy) je rovněž předmětem této analýzy.

Při zjišťování **podmínek v objektu** je nutno ověřit všechny nepříznivé vlivy prostředí z hlediska vlhkosti, prašnosti, korozní agresivity, nebezpečí výbuchu, teploty, vibrací, elektromagnetických polí, ionizačního záření, riziko úmyslného poškození či odcizení, apod.

**Provozní požadavky** propojují funkční požadavky na prvky systému CCTV s reálnými postupy obsluhy. Zde se ptáme jak budou funkční vlastnosti systému využívány a zda jsme konkrétní provozní požadavky navrhovaným zařízením vůbec splnit. Pro upřesnění **provozních požadavků** vycházíme z předpokládaného režimu objektu a jako pomocník může sloužit např. rozvinutá osnova uvedená v článku 6 normy ČSN EN 50 132-7.

### 9.2 Etapa II – Návrh

Výsledky této **analýzy potřeb zákazníka** je vhodné zaznamenávat do předem připravených tabulek. Vyplněné tabulky slouží technikům jako výchozí materiál pro stanovení předběžných technických specifikací jednotlivých zařízení v systému požadovaných pro potřeby zpracování nabídky. Záznam o analýze potřeb je vhodné nechat zákazníkem podepsat a může být jako předběžná specifikace součástí nabídky. Vyhneme se tím možným nedorozuměním z odlišného vnímání projednávaných skutečností zákazníkem a obchodně-technickým zástupcem dodavatelské organizace. Příklad takových tabulek je uveden dále.



Tabulka 5-18: Základní údaje o zakázce

<b>Zákazník:</b>	Název firmy,, adresa,, kontaktní osoba a spojení (tel. fax,, mail...)
<b>P. č.</b> číslo z podnikové databáze poptávek/nabídek/zakázek	
<b>účel nasazení systému</b>	krátce popsat účel – monitorování vjezdu,, sledování provozu na vrátnici,, hlídání skladových prostor,, nakládací rampy,, monitorování technologie...
<b>předpokládaná rizika objektu/ režimu provozu</b>	krátce popsat rizika – umístění objektu,, možnosti přístupu,, atraktivita materiálu a majetku v objektu,, provoz v objektu...
<b>podmínky v objektu</b>	nepříznivé vlivy prostředí z hlediska vlhkosti,, prašnosti,, korozní agresivity,, nebezpečí výbuchu,, teploty,, vibrací,, elektromagnetických polí,, ionizačního záření,, riziko úmyslného poškození či odcizení apod.
<b>předpokládaný způsob montáže</b>	povrchově,, pod omítkou,, závěsná vedení,, využití stávajících žlabů a můstků...
<b>provedení silových rozvodů</b>	zajistí zákazník – dodavatelská organizace
<b>provedení stavebních prací</b>	zajistí zákazník – dodavatelská organizace
<b>podklady pro nabídku/projekt</b>	aznamenat rozsah předaných podkladů (projekty,, plány,, el. data..)
<b>provedení systému</b>	<ul style="list-style-type: none"> <li>- černobílý – barevný</li> <li>- rozlišení standardní – vysoké</li> <li>- denní/noční snímání</li> <li>- požadavky na přisvětlení</li> <li>- dálkově ovládaná kamerová stanoviště</li> <li>- provedení přenosových tras</li> <li>- požadavky na ovládání</li> <li>- požadavky na záznam</li> <li>- zálohování napájení</li> <li>- ...</li> </ul>
<b>rozsah systému</b>	<ul style="list-style-type: none"> <li>- druh a počet snímaných scén</li> <li>- počet monitorovacích pracovišť</li> </ul>
<b>součinnost s ostatními bezpečnostními systémy v objektu</b>	<ul style="list-style-type: none"> <li>- EZS</li> <li>- EPS</li> <li>- kartový systém</li> <li>- vlastní střežicí funkce (videosenzory)</li> </ul>
<b>specifické požadavky zákazníka</b>	-
<b>předpokládané termíny</b>	<ul style="list-style-type: none"> <li>- nabídky</li> <li>- smlouvy</li> <li>- realizace</li> </ul>
<b>datum a podpisy</b>	<ul style="list-style-type: none"> <li>- datum jednání</li> <li>- podpisy za zákazníka a za dodavatelskou organizaci</li> </ul>

Tabulka 5-19: Údaje o kamerových stanovištích

<b>Kamerové stanoviště:</b>	- umístění
<i>pořadové číslo či umístění</i>	- předmět snímání - orientace vůči světovým stranám (azimut) - ...
<b>podmínky montáže</b>	- dostupnost a umístění montážního místa (zed/strop/podhled/sloup) - riziko úmyslného poškození či odcizení apod.
<b>vzdálenost stanoviště od monitorovacího pracoviště</b>	- vzdušná (pro bezdrátový přenos) - reálná (pro přenos po metalických vedení či optických vláknech)
<b>druh prostředí</b>	- nepříznivé vlivy prostředí z hlediska vlhkosti,, prašnosti,, korozní agresivity,, nebezpečí výbuchu,, teploty,, vibrací,, elektromagnetických polí,, ionizačního záření - protokol o stanovení prostředí
<b>rozpoznání předmětu snímání</b>	- specifikovat dle ČSN EN 50132-7 čl. 7.6
<b>vymezení zorného pole</b>	- např. vzdálenost (či min/max vzdálenost) - šířka - výška
<b>intenzita osvětlení</b>	- den/noc
<b>technická specifikace kamerového stanoviště</b>	-
<b>typ kamery:</b>	-
<b>typ objektivu:</b>	-
<b>typ kamerového krytu:</b>	-
<b>typ kamerového ramena:</b>	-
<b>typ polohovací hlavice:</b>	-
<b>další příslušenství:</b>	-

Tabulka 5-20: Údaje o monitorovacích pracovištích

<b>Monitorovací pracoviště:</b>	- umístění -	
<b>P. č. číslo či umístění</b>		
<b>režim pracoviště</b>	- denní/noční/nepřetržitý - obsluhovaný/bezobslužný - způsob vyhodnocování informací	
<b>počet vstupů (od kamer)</b>	-	
<b>počet výstupů (pro monitory)</b>	-	
<b>požadavek na ovládání</b>	- ovládání či pouhé sledování bez možnosti vstupu do systému - převzetí/priority ovládání - automatizace provozních režimů	
<b>požadavky na záznam</b>	- automatizovaný režim bez možnosti zásahu obsluhy - kompetence obsluhy - nucený záznam od ostatních systémů - nucený záznam od obsluhy	
<b>vyhodnocování záznamu</b>	- kompetence obsluhy - nezávislé vyhodnocování na samostatném pracovišti - nezávislé vyhodnocování během provozu na monitor. pracovišti	
<b>provedení techniky</b>	- stolní - zabudovatelná - 19" rack - ...	
<b>Technická specifikace monitorovacího pracoviště</b>	-	
<b>typ a počet zařízení na zpracování videosignálu:</b>	- (sekvenční přepínač, vícenásobný dělič obrazu, multiplexer,, videomatice,, videosever...)	- počet
<b>typ a počet monitorů:</b>	-	- počet
<b>typ záznamového zařízení:</b>	- videorekordér VHS - videorekordér S-VHS - digitální videorekordér	- počet
<b>další příslušenství</b>	-	

Kritéria návrhu jsou uvedena v kapitole 7 normy ČSN EN 50132-7. V další části jsou uvedeny aspekty návrhu jednotlivých částí kamerového řetězce.

### 9.2.1 Kamerové jednotky

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

Je nutno přiznat, že schopnost barevných kamer uspokojivě pracovat za nízkých úrovní osvětlení a při osvětlení smíšenými zdroje světla se neustále zlepšuje a ceny ta-

kových kamer se stávají přijatelnými. Dnes již tedy nestojíme před dilematem, zda raději preferovat černobílé kamery s dostatečnou citlivostí i s dostatečnou rozlišovací schopností či zda preferovat nižší citlivost a nižší rozlišovací schopnost za cenu pro identifikaci důležité vlastnosti – barvy. I tak však musíme počítat s omezenou schopností věrně zobrazit konkrétní barvu zvláště za umělého osvětlení, jehož spektrální složení je vzdálené dennímu světlu (např. sodíková či rtuťová výbojka)

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

Prisvětlení scény v infračerveném spektru by mělo být až tím posledním řešením – výhodnější je zlepšit běžné osvětlení sledované scény nebo využít kamery s vyšší citlivostí.

Možnost přepínání režimu černobílý/barevný je požadavek rozumný ne však nezbytný – spektrální složení světla umělého osvětlení (ať již sodíkových či rtuťových výbojek) výrazně mění barevné podání obrazu a i při dostatečné intenzitě osvětlení ovlivňuje vypovídací schopnost snímku v oblasti barvy.

**Mezní citlivost kamer** – jsou-li zóny sledování v noci osvětleny umělým osvětlením, měla by být citlivost s ohledem na současně dosažitelné parametry v ekonomických mezích lepší než 1 lx v barevném režimu/popř. lepší než 0,1 lx v černobílém režimu) stanovena s rezervou. Parametr citlivost je vždy vázán na světelnost použitého objektivu a citlivost by měla být uváděna vždy ve spojení se světelností objektivu, ke které je vztažena.

**Rozlišovací schopnost** kamer by pro běžné aplikaci měla být určitě vyšší než 400 řádků, a to jak v černobílém, tak barevném režimu.

Návrh **ohniskové vzdálenosti objektivu** vychází ze specifikace článku 7.6 ČSN EN 50 132.

U **polohovací hlavice a kamerového krytu** je důležitým požadavkem stupeň krytí pro venkovní nasazení v nepřetržitém provozu. Podstatným požadavkem je také rychlost otáčení polohovací hlavice zvláště v horizontálním směru. Je-li kamera umístěna tak, aby bylo možno sledovat prostor v celém rozsahu 360°, potřebuje standardní hlavice s rychlostí otáčení 6°/s k přetočení z jedné mezní polohy do druhé 60 s! Co vše se za tuto dobu může stát mimo zorné pole, je nutno pečlivě zvážit. Nový trend, který se v této oblasti v posledních letech silně prosazuje, je provedení kamerové jednotky jako integrované, zahrnující kromě kamery polohovací hlavici s vysokou rychlostí otáčení, motor-zoom, i ovládací a přenosové zařízení se standardním rozhraním (např. RS 232 či RS 485). Vlastní provedení v integrovaném kulovém krytu pak jednak zlepšuje designovou hodnotu systému CCTV zvláště na objektech, kde je systém pod drobnohledem kromě jiných i pracovníků památkové péče či architekta. Výhody má toto provedení i z hlediska montáže a servisu, a koneckonců ani cena není proti kamerové jednotce poskládané z komponentů výrazně vyšší.

Určitě je nezbytným požadavkem **ochrana proti přepětí** na signálových i napájecích trasách (viz kapitola 7).

### 9.2.2 Přenos

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

#### 9.2.2.1 Přenos videosignálu

##### **Přenos v digitální formě (tzv. slow-scan)**

Signál je přenášen obvykle po komutovaných či vyhrazených linkách jednotné telefonní sítě (JTS) v lepším případě po ISDN linkách popř. po optických datových sítích. Obraz je nespojitý a rozhodně se nehodí za současného stavu techniky ke sledování dynamických dějů. Dále je za tohoto stavu obtížné ovládání kamer (zoomování, ostření, polohování). Tento systém se obvykle používá u systémů dálkového dohledu méně dynamických dějů, kde je přijatelný nespojitý přenos statických obrázků.

##### **Přenos po nesymetrickém vedení (koaxiální kabel)**

Uvedený přenos je doposud nejčastějším způsobem přenosu videosignálu používá ke spojení kamer s ovládací místností. Koaxiální kabel může vést videosignál i ovládací signál jedním kabelem. Přenos je omezen vzdáleností (řádově na stovky metrů), kde v závislosti na útlumu použitého kabelu se zhoršuje rozlišovací schopnost systému jako celku (ztrácí se schopnost zobrazit jemný detail, obrázky vypadají jakoby rozostřené). Samozřejmě lze zařadit do přenosové trasy korekční zesilovače videosignálu, pak ale ztrácíme možnost přenosu řídicích signálů ke kamerové jednotce po jednom kabelu.

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

##### **Symetrické vedení (kroucený pár)**

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

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

##### **Bezdrátový přenos**

Právně přípustný je přenos pomocí přenosových zařízení schválených pro provoz v provozních kmitočtových pásmech stanovených GL 14/R/2000 ČTÚ v pásmu 10 GHz a revidovaného GL 30/R/2000v pásmu 2,4 GHz. Je třeba říci, že se nejedná o vyhrazená pásma, kde by byl garantován nerušený provoz a která by byla zpoplatňována. Jedná se

o pásma sdílená více uživateli na základě zásad uvedených ve všeobecných oprávněních.

Při porovnání obou pásem je nutno říci následující. Z fyzikálního principu má vyšší pásmo (10 GHz) směrové účinky, a tak i když na blízkém kmitočtu pracuje jiné zařízení riziko rušení je minimální. Mikrovlnný přenos je možno realizovat s přijatelnými náklady na řádově jednotky kilometrů s možností pasivní retranslace a až desítky kilometrů s aktivní retranslací. Přenosové vzdálenosti jsou závislé rovněž na použité anténě, která má vzhled běžné satelitní antény na družicový televizní příjem. Praktické omezení vyplývá z potřeby přímé viditelnosti popř. zařazení retranslačních bodů. Antény se obvykle musí umísťovat na nejvyšší budovy nebo věže. Při nepříznivých povětrnostních podmínkách (hustý déšť, sněžení) se může snížit kvalita obrazu.

Nižší používané pásmo (2,4 GHz) je prioritně určeno pro přenos dat s rozprostřeným spektrem což přináší vyšší riziko rušení přenosu a i směrové účinky těchto kmitočtů jsou menší, takže i z fyzikálního principu přenosu vyplývá vyšší náchylnost k rušení. Antény jsou většinou buď směrové - klasické YAGI či anténní řady s reflektorem podobné televizním anténám, či zvláštní dielektrické antény popř. se využívají i všesměrové antény. Cena takového přenosového zařízení je nižší ovšem při výše jmenovaných rizicích že v kritickém okamžiku operátor neuvidí, co vidět má, popř. že záznam bude nepoužitelný. Není možné takové systémy zcela vyloučit, ale je třeba přistupovat k nim opatrně a nasazení podmiňovat dokonalým radiokomunikačním průzkumem.

Jednoznačná výhoda bezdrátových přenosů je galvanické oddělení jednotlivých částí systému a eliminace přenosu přepětových pulsů.

### **Infračervený přenos**

Infračervené spojení je další možností z oblasti bezdrátových technologií, o níž lze uvažovat při přenosu na krátkou vzdálenost. Je to další pomůcka, která se na krátký dosah velice osvědčila, ale povětrnostní podmínky ji ovlivňují daleko výrazněji než mikrovlnné zařízení.

Výhody jsou stejné jako u předcházejícího bezdrátového přenosu.

### **Přenos po optickém vlákně**

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

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

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

### 9.2.2.2 Přenos řídicích signálů

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

### 9.2.3 Monitorovací pracoviště

Je vhodné uvažovat, kde je pracoviště umístěno (např. na služebně hlídací služby v objektu. Je-li k dispozici výkres místnosti s předpokládaným umístěním zřizovacích předmětů, je vhodné ho zahrnout jako podklad pro zpracování návrhu konkrétního řešení monitorovacího pracoviště v rámci projektu. Z počtu pracovníků obsluhy stanoveného v provozních požadavcích může vyplynout při návrhu požadavek paralelního pracoviště např. pouze pro monitorování či pro práci se záznamem nebo archivem snímků.

Návrh zálohování napájení pro případ výpadku napájení zařízení celého monitorovacího pracoviště je rozumné z praktických důvodů omezit pouze na dobu nezbytnou k „úklidu“ dat či ošetření případně použitého software.

#### 9.2.3.1 Monitor

S ohledem na režim provozu nepřetržitý/omezený, organizaci času, počtu pracovníků obsluhy je účelné zvážit požadavky na vybavení monitorovacího pracoviště monitory. S ohledem na zkušenosti z praxe a reálnou schopnost obsluhy, omezenou fyziologickými i psychologickými faktory sledovat dlouhodobě více obrazovek je standardní požadavek alespoň dvou barevných monitorů s dostatečným rozlišením (s ohledem na rozlišovací schopnost kamer, přenosových tras, i zařízení na zpracování videosignálu minimálně však 400 řádků), s možností vícenásobného zobrazení pohledu všech kamer na jednom monitoru (multiscreen), popř. sekvenčního přepínání, a druhý větší monitor pro sledování aktuálně vybrané zóny sledování a paralelního monitoru na pracovišti velitele policie.

Návrh vhodných typů monitorů je důležité přizpůsobit požadavkům na ergonomii, fyziologii, bezpečnost a ochranu zdraví při práci a prostorovým dispozicím pracoviště.

#### 9.2.3.2 Ovládací zařízení

Podobně jako u volby monitorů je s ohledem na režim provozu nepřetržitý/omezený, organizaci času – střídání směn, počtu pracovníků obsluhy účelné zvážit v rámci návrhu požadavky na ovládací zařízení. Je-li součástí provozních požadavků požadavek na předvolbu nastavení sledování oblastí zájmu v rámci sledovaných zón, musí návrh tento požadavek při specifikaci vhodného ovládacího zařízení zohlednit.

Rovněž návrh kapacity ovládacího zařízení by měl korespondovat s cílovým stavem rozsahu systému. Vhodnou volbou zde může být návrh modulové konstrukce ovládacího zařízení.

### 9.2.3.3 Záznamové zařízení

Zde se mohou vyskytnout největší diskuse a odlišné názory i odlišná technická řešení. Tato zařízení zvláště v oblasti digitálního záznamu prožívají dynamický vývoj a my buď musíme smířit s tím, že již v okamžiku návrhu digitálního záznamového existuje daleko dokonalejší zařízení, než je právě to naše, a že to nové se objeví na trhu v dohledné době.

Pro operativní nasazení je někdy vhodné zařazení videotiskárny. Tyto tiskárny mohou vytvářet barevné nebo černobílé snímky, které lze využívat jako trvalý záznam nebo lépe jako operativní prostředek k předávání informací důležitým orgánům (např. policii). U digitálních záznamových zařízení tuto úlohu může převzít PC tiskárna.

Požadavek na dobu archivace by měl vycházet z reálného režimu provozu monitorovacího pracoviště a „hodnoty“ záznamu rizikové události. Jeho hodnota logicky z časem klesá a záznam by měl sloužit prioritně pro okamžitou analýzu situace a přijetí optimálního opatření v řádu jednotek dnů. Určitě existují záznamy, jejichž hodnota je i po uplynutí delší doby, ale procento takových záznamů bude zřejmě malé. Je to zvažování prakticky využitelné doby archivace v rozumném ekonomickém rámci. U digitálních záznamových zařízení lze obvykle kapacitu paměti postupně rozšiřovat pomocí např. diskových polí, připojení externích paměťových médií (např. VXA mechaniky, DAT kazetopáskové jednotky, magnetooptický disk apod.).

Požadavek na minimální rozlišovací schopnosti záznamu (min. 400 televizních řádků) souvisí s požadovanou „frekvencí vzorkování“, to je počet snímků od každé kamery za sekundu. Tento požadavek má rovněž souvislost s požadovanou kapacitou záznamového zařízení. V každém případě by minimální rozlišovací schopnost záznamového zařízení měla být stejná nebo vyšší než u celého systému od kamery přes přenosové trasy až k zobrazovacímu zařízení.

### 9.3 Etapa III. – Přezkoumání návrhu a příprava realizace

Cílem této etapy je připravit podmínky pro bezproblémovou montáž uvedení do provozu a vlastní dlouhodobě spolehlivý provoz systému. V případě odsouhlasení nabídky na realizaci je nutno ještě před uzavřením smlouvy či objednávkou na realizaci buď potvrdit skutečnosti uvedené v systémovém návrhu či navrhnout případné změny a dodatky.

V předcházející části popsané činnosti nám umožní zpracovat a se zákazníkem odsouhlasit popř. upravit konečné znění smlouvy. Ze smlouvy, nebo z její přílohy by měly být jasné jednoznačné závazky zřizovatelské organizace v oblasti provozních požadavků zákazníka i úplné technické specifikace prvků všech prvků systému CCTV. Především k tomuto účelu slouží tabulky uvedené v minulé části.

Úlohou projektanta je přenést stanovené provozní požadavky a technické specifikace do konkrétního návrhu funkčního systému CCTV a připravit výkresové podklady pro kvalifikovanou montáž.

*Poznámka – požadavky na obsah projektové dokumentace se do značné míry kryjí se strukturou popsanou v kapitole 10 Zřizování poplachových systémů, proto nejsou na tomto místě publikace uvedeny.*



## 9.4 Etapa IV. – Realizace

### 9.4.1 Montáž CCTV

Vlastní montáž CCTV se podstatnou měrou podílí na celkovém úspěchu realizace systému CCTV. Je velice důležité mít pracovníky montáže spolehlivé, pečlivé, a hlavně dostatečně proškolené v obecných znalostech o CCTV, a samozřejmě i v konkrétních znalostech o používaných zařízeních.

Na pracovníky montážních čt jsou kladeny i požadavky na základní zásady jednání se zákazníkem. Citlivá je zvláště situace, kdy se rozvody CCTV montují za provozu objektu. V tom případě se pracovníci montážních čt musí snažit, aby svou přítomností neobtěžovali. Základní požadavky lze shrnout do několika zásad:

- dohodnout si časový rozvrh prací s ohledem na provoz objektu, a plán také dodržovat;
- práce, při nichž vzniká hluk, přesunout mimo pracovní dobu uživatele objektu;
- po práci vždy po sobě důkladně uklidit;
- po skončení denních prací předávat pracoviště osobně zpět uživateli objektu (riziko nařčení ze ztráty či poškození zřizovacích předmětů a interiérů).

Kvalifikační předpoklady jsou jedna strana mince, ale důležitější je precizní technické zvládnutí profese. Sem patří nejen technická funkčnost, ale i zvládnutí montáže z estetických hledisek. Křivě usazené kamerové rameno, nezačištěné prostupy zdí, nevhodné umístění kabelových kanálů, krabic a dalších částí instalace CCTV – to je první, čeho si zákazník všimne.

#### 9.4.1.1 Kabelové rozvody

Kabeláž v sobě zahrnuje napájecí trasy, trasy pro přenos videosignálu a trasy pro přenos ovládacích signálů. Alternativy napájení se objevují prakticky jen u kamer (odd. 3). Ostatní prvky CCTV (s výjimkou kontrolních monitorů) se vyskytují výhradně se síťovým napájením. Přenosové trasy mají rovněž několik alternativ (odd. 6). Konkrétní provedení kabelových rozvodů se tedy odvíjí od zvoleného způsobu napájení a přenosu.

##### Napájecí trasy

Ideální situace nastane při budování nového objektu. Vstoupí-li realizační firma do zakázky ve stadiu přípravy celkového projektu na výstavbu daného objektu, má možnost prosadit všechny požadavky na přípravu napájení CCTV v rámci projektu silnoproudých rozvodů.

U varianty síťového napájení kamer se doporučuje provést přívod pro každou kameru samostatným v průběhu trasy nevypínatelným vedením 220 V 3 x 1,5 Cu se samostatným jištěním 1 A.

U varianty napájení kamer ze společného zdroje malého napětí (ss nebo st) je nutné vzít v úvahu odběry kamer a vzdálenosti od napájecího zdroje. Zvolený typ kabelu pak musí vyhovovat z hlediska úbytku napětí podél vedení.

U varianty napájení kamery po koaxiálním vedení se vůbec žádné samostatné napájecí trasy nebudují.

Zařízení na zpracování videosignálu (monitory, multiplexer, videomagnetofon apod.), která jsou instalována na společném stanovišti, mohou mít společný třížilový pří-

vod. Dimenzování a jištění by měly odpovídat instalovanému příkonu. Všechny silové přívody v rámci CCTV by měly být zásadně taženy ze stejné fáze. Provedeny musí být třížilově kabelem s odpovídajícím průřezem, minimálně však CYKY 3 x 1,5 3C. Při realizaci rozvodů je nutné dodržet požadavky ČSN 332000-5-52 Elektrotechnické předpisy – Elektrická zařízení – Část 5: Výběr a stavba elektrických zařízení – Kapitola 52: Výběr soustav a stavba vedení. (nahrazující ČSN 341050 Předpisy pro kladení silových vedení, ČSN 332000-4-41 Elektrotechnické předpisy – Elektrická zařízení – Část 4: Bezpečnost – Kapitola 41: Ochrana před úrazem elektrickým proudem, ČSN 332000-4-43 Elektrotechnické předpisy – Elektrická zařízení – Část 4: Bezpečnost – Kapitola 43: Ochrana proti nadproudům, ČSN 332000-4-473 Elektrotechnické předpisy – Elektrická zařízení – Část 4: Bezpečnost – Kapitola 47: Použití ochranných opatření pro zajištění bezpečnosti. Oddíl 473: Opatření k ochraně proti nadproudům, ČSN 332000-5-523 Elektrotechnické předpisy – Elektrická zařízení – Část 5: Výběr a stavba elektrických zařízení – Kapitola 52: Výběr soustav a stavba vedení. Oddíl 523: Dovolené proudy.

Napájení kontrolních monitorů umístěných mimo monitorovací pracoviště je možné provést z běžného zásuvkového okruhu. V rámci realizace CCTV velice často nic jiného nezbývá, neboť umístění doplňkových zařízení (např. kontrolních monitorů) ve stadiu projekce zpravidla neznáme. Vhodné je, zvláště u starých dvou vodičových rozvodů, doplnění napájení těchto doplňkových zařízení o oddělovací bezpečnostní transformátory 1:1 pro eliminaci vlivu zemních vyrovnávacích proudů na kvalitu obrazu (ekvivalentním opatřením může být oddělení signálových zemí prostřednictvím izolačního videotransformátoru nebo oddělovacího videozesilovače, který může současně sloužit ke kompenzaci ztrát na vedení).

### Signálové trasy

Signálové trasy jsou velice důležitou součástí systému CCTV. Nevhodně zvolené typy kabelů, nesprávně provedená spojení a nespolehlivé připojení konektorů mohou funkci systému CCTV zcela znehodnotit a degradovat jej v očích zákazníka, i když je vybudován z kvalitních a spolehlivých komponentů.

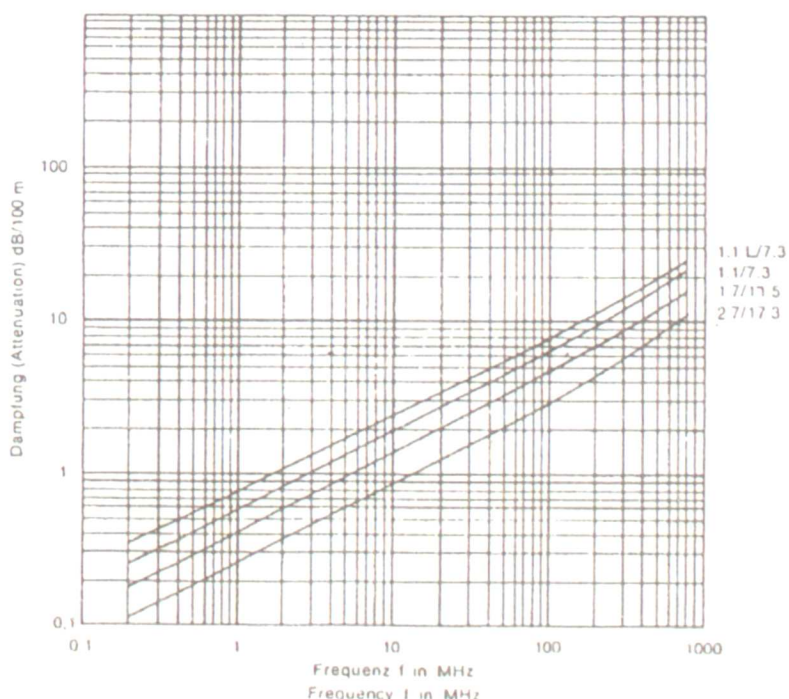
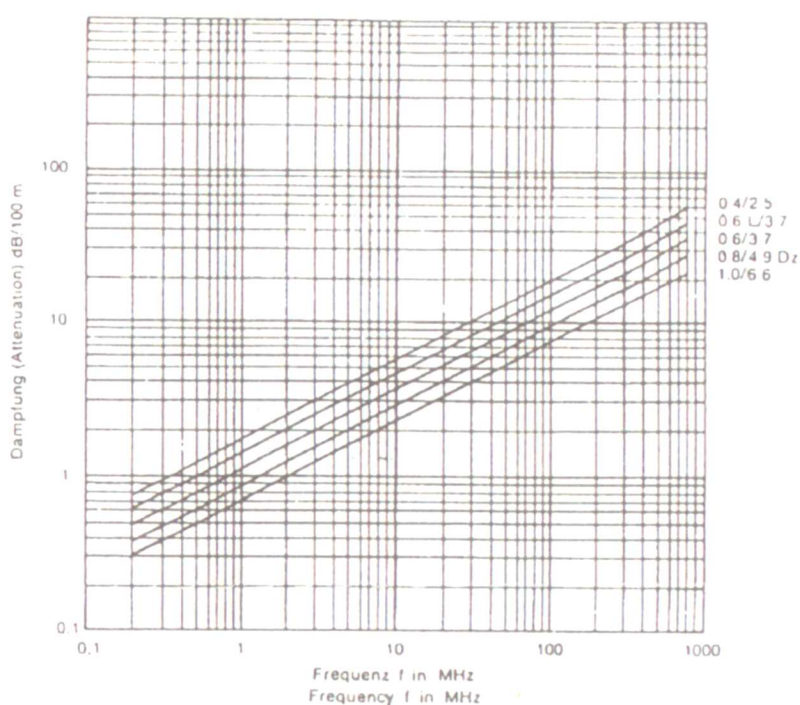
Prvním problémem je volba vhodného koaxiálního kabelu a druhým správné spojování kabelů a připojování k zařízení. Vzhledem ke kmitočtovému rozsahu videosignálu nejsou na kabely kladeny nijak zvláště přísné nároky. Přesto je však třeba zachovávat alespoň elementární zásady při výběru vhodných kabelů.

Základním parametrem popisujícím koaxiální kabel je jeho **charakteristická impedance**. Charakteristická impedance je vysokofrekvenční odpor nekonečně dlouhého vedení. Je to ohmický odpor, jakým musíme zakončit reálné vedení konečné délky, aby na něm nevzniklo stojaté vlnění, a tím i odrazy signálu.

Všeobecně užívaná charakteristická impedance v oboru CCTV je 75  $\Omega$ .

Další parametr, který nás s ohledem na CCTV také zajímá, je **útlum kabelu**. Jsou to vlastně energetické ztráty konkrétního typu kabelu uváděné v dB, jež vznikají na přízpusobeném vedení v závislosti na délce vedení a pracovním kmitočtu. Jsou dány součtem odporových a dielektrických ztrát daného kabelu.

Při návrhu kabelových tras nad 100 m délky bychom vždy měli brát v úvahu útlumové parametry použitého kabelu. Určitým pomocníkem při návrhu tras mohou být tabulky či grafy uvedené v katalogových listech koaxiálních kabelů.



Obr. 5-47: Příklad útlumových charakteristik koaxiálních kabelů.

Je-li nutné garantovat provoz pod  $-25\text{ }^{\circ}\text{C}$ , je nutno používat typy s pláštěm z měkčeho mrazuvzdorného PVC.

Existuje řada dalších parametrů (činitel zkrácení, homogenita, kritický kmitočet, výkonová zatížitelnost, průrazné napětí dielektrika apod.), které charakterizují koaxiální kabel a předurčují ho ke konkrétní aplikaci. V oboru CCTV díky kmitočtovému rozsahu v základním pásmu (0 – 6,5 MHz) se projevují tyto parametry minimálně.

To, co nás v oboru CCTV na kabelech zajímat ale musí, jsou jejich mechanické parametry a klimatická odolnost.

Pro standardní úlohy v CCTV je nejvhodnější např. RG 59 B/U či jeho tuzemský ekvivalent o vnějším průměru 6 mm, s plným středním vodičem a stíněním tvořeným opletením z měděných drátků.

Pro venkovní závěsné vedení je vhodné použít koaxiální kabel se zalisovaným závěsným ocelovým lanem, popř. vytvořit závěs z ocelového lanka a přichytkami k němu aretovat běžný koaxiální kabel.

Pohyblivé aplikace vyžadují kabel co nejohybnější, s vnitřní splétanou žilou.

Nechceme-li zařazovat do tras delších než cca 190 m (odd. 6) průběžný zesilovač, je účelné i z hlediska vyšší mechanické odolnosti použít kabel RG 11 či odpovídající tuzemský ekvivalent.

Základní parametry koaxiálních kabelů vhodných pro CCTV:

impedance:	75 $\Omega$ s tolerancí 3 $\Omega$
dielektrikum:	PE (polyetylen)
kapacita:	67 pF/m
činitel zkrácení:	0,66
izolační odpor:	min. $10^8 \Omega$
min. poloměr ohybu:	5 x D
teplotní rozsah:	PVC od -25 °C do +70 °C PVC-M od -40 °C do +70 °C
stínění:	opletení Cu, krytí 91 %
standard:	ČSN IEC 96-2

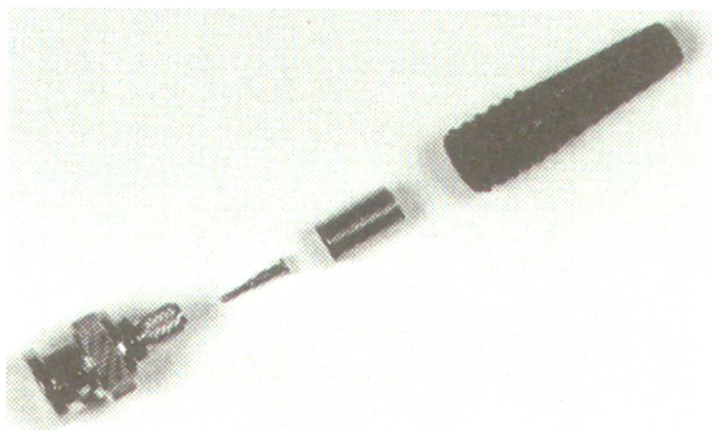
Normami je oblast koaxiálních kabelů u nás i mezinárodně poměrně dobře pokryta. Zahraniční kabely značené RG xx vycházejí ze standardu, jenž vznikl dokonce již v roce 1944, a odpovídají americké vojenské normě MIL 17C. V oboru CCTV připadají v úvahu typy RG 59, RG 11 a RG 12.

Zájemce o bližší informace o technických parametrech koaxiálních kabelů lze odkázat na ČSN IEC 96-2.

### 9.4.1.2 Připojování a spojování

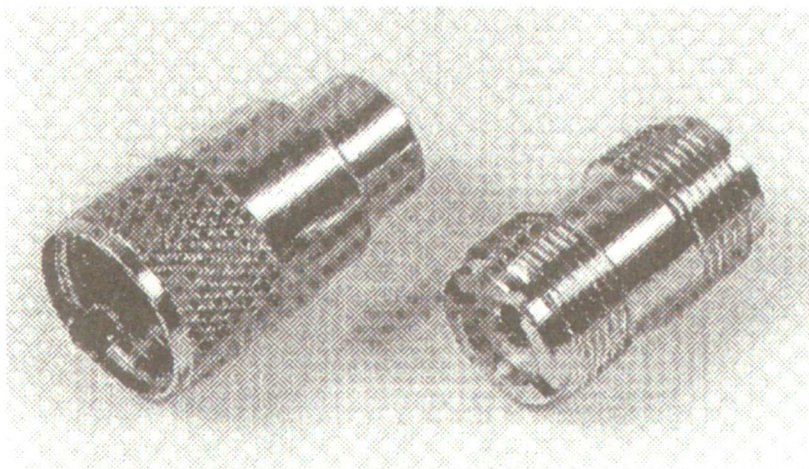
Neužívanějším připojovacím konektorem v oboru CCTV je konektor typu BNC (viz obr. 5-48) o charakteristické impedanci 75  $\Omega$ . Z hlediska montáže existují dvě varianty konektoru - varianta pro pájený spoj (solder type) a varianta pro spoj nalisovaný (crimp type). Označení konektoru BNC vychází z počátečních písmen jmen tvůrců tohoto konektoru – inženýrů Bellových laboratoří, pánů Bayoneta, Neilla, Concelmana. Jde o miniaturní konektor použitelný ve verzi 75  $\Omega$  až do kmitočtu 1 GHz. Normalizované provedení je popsáno v normě IEC 169.

Další používaný typ konektoru PL (viz obr. 5-49) byl vyvinut původně jako UHF konektor počátkem 30. let firmou Amphenol (USA). Jeho využití v oboru CCTV přichází v úvahu spolu se silnými kabely (RG 11 apod.) při venkovních aplikacích a dlouhých přenosových trasách především pro spojování tras tvořených více úseky. Vlastní spoj není vodotěsný! Je nutné před montáží převléci přes kabel smršťovací bužírku v šíři přesahující okraje konektorů zašroubovaných do PL spojky a po ukončení montáže spoj hermetizovat tepelným zdrojem. Méně estetické, ale funkční je využití různých kabelových bandáží určených např. pro telekomunikační kabely.



Obr. 5-48: Konektor BNC v provedení pro nalisování (crimp type).

V oboru CCTV najde uplatnění i konektor typu F (viz obr. 5-50). Tento miniaturní konektor spatřil světlo světa s nástupem satelitní techniky. Je použitelný do kmitočtů přes 2 GHz. Jako střední kolík využívá žílu kabelu. Nabízí se opět ve dvou variantách, z nichž



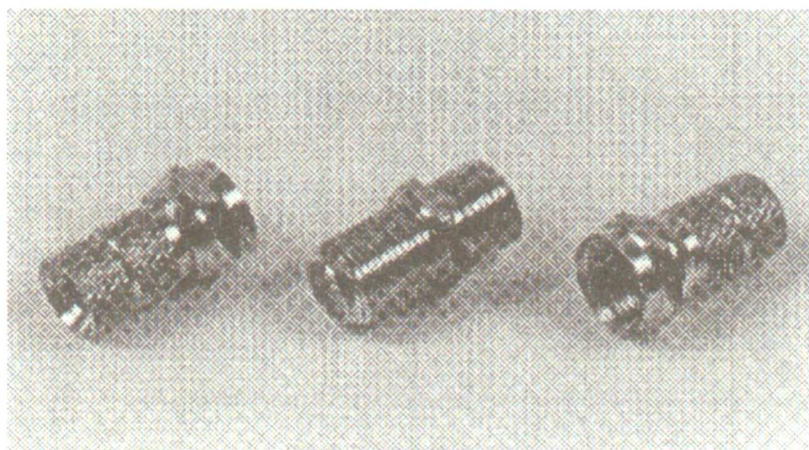
Obr. 5-49: Provedení PL konektoru a PL spojky.

jedna slouží pro později rozebíratelný spoj se šroubovacím tělesem stínění, druhá varianta podobně jako u BNC crimp type slouží k nerozebíratelnému nalisování na kabel.

V oboru CCTV se používá výhradně pro spojování kabelu RG 59 B/U či jeho ekvivalentů o průměru 6 mm. Pro spoje zatahované do elektroinstalačních trubek či pro venkovní aplikace je účelné spoj chránit opět smršťovací bužírkou (podobně jako u PL konektoru).

Pro montáž lze rozhodně doporučit BNC a F konektory v nerozebíratelném provedení, určené k jednorázovému nalisování na konce kabelu pomocí speciálních kleští (crimp type). PL konektor je k dispozici pouze jako pájený (solder type).

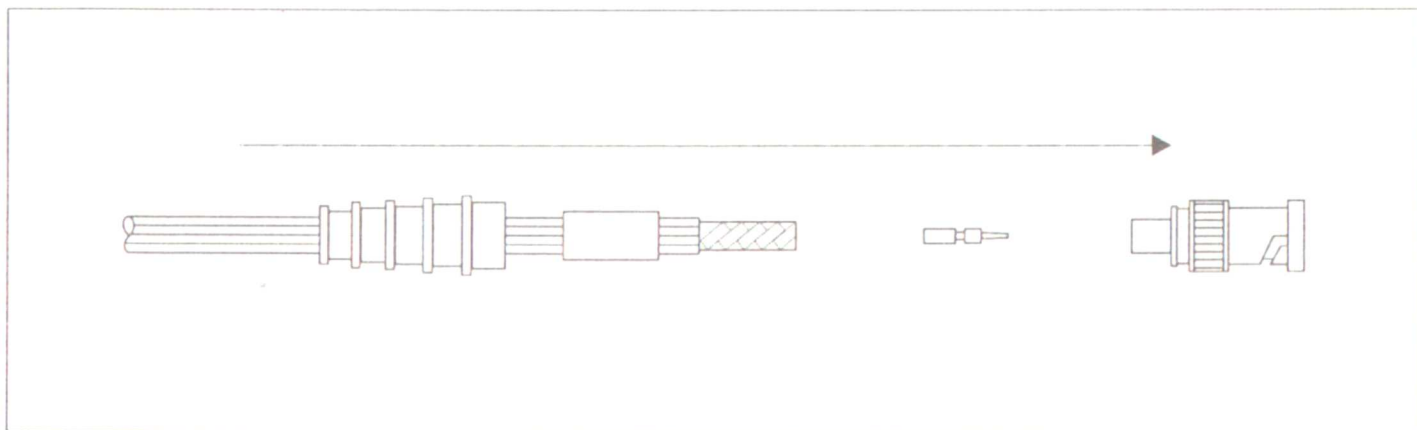
Vlastnímu spojení je třeba věnovat náležitou pozornost. Zkušenosti ukazují, že 90 % problémů se signálovými trasami způsobuje chybná montáž konektorů. Nedostatečně



Obr. 5-50: Provedení F konektoru a F spojky.

nalisovaný střední kontakt může způsobit teplotně závislou nespolehlivost, špatné připojení stínění způsobí zvýšený útlum kabelové trasy či poruchu přizpůsobení, a tím vznik odrazů („duchů“ v obraze). Úplnou ztrátu signálu způsobí přelomený střední vodič, naříznutý částečně při montáži a vlivem manipulace s kabely dolomený, popř. přetržený při necitlivém zatahování do elektroinstalačních trubek při montáži signálových rozvodů.

Každý, kdo má alespoň minimální zkušenosti s montáží konektorů, potvrdí, že investice do běžně dostupných přípravků (crimp – kleště, strip – přípravek) se vyplatí. Vlastní postup při montáži konektoru BNC je naznačen na obr. 5-51.



Obr. 5-51: Montáž BNC crimp konektoru.

Potřebné je správné nastavení nožů strip – přípravku pro úpravu konce kabelu a dokonalé nasunutí lisovacích kleští na jednotlivé díly konektoru při zalisování. Velice důležité je, aby přechod mezi odkrytým stíněním a pláštěm kabelu byl v zóně lisování. Dostane-li se tento konec mimo krycí stínicí trubičku, je zvláště u pohyblivých přívodů riziko přerušení hlavně vnitřního vodiče. Velmi účinnou ochranou kabelů proti mechanickému poškození v místě vyústění z konektoru jsou pryžové kabelové převlečky.

### 9.4.1.3 Značení kabelů

V rámci rozsáhlejších systémů CCTV je nezbytné, v rámci menších (do 8 kamer) účelné a šetří čas při identifikaci správného kabelu. K tomuto účelu realizační firmy používají různé přelepky s alfanumerickým kódem, samolepky apod. Rozhodně se však neosvědčily Dymo kleště, kde kvůli malému průměru kabelů a poměrně velké tuhosti Dymo pásky označení po čase odpadne.

Ideálním a vpravdě profesionálním řešením je zadat si u specializované firmy potisk nebo značení podle projektu na plastové převlečky. Na trhu je již řada firem, jež tyto služby nabízejí pro široký okruh použití v elektromontážních pracích. Cenově se toto značení v rámci celého systému prakticky neprojeví, ale ušetří spoustu práce jak při montáži, tak při pozdějším případném servisu.

K otázce připojování a spojování lze říci, že na trhu existuje tak nepřeberné množství variant a kombinací (spojky, redukce, úhlové provedení atd.) popsaných základních typů konektorů, že skutečně pro každou aplikaci lze nalézt optimální profesionální řešení.

Ve spojování a připojování vedení v CCTV platí více než kdekoli jinde: „Vyhněte se improvizaci a provizorním řešením! Ušetříte ohromné množství práce sobě i těm, kteří přijdou po vás opravovat nefungující zařízení!“

### 9.4.2 Oživování systému CCTV

Systém oživujeme postupně po výchozí revizi silnoproudé části rozvodů. ČSN 332000-6-61, pojednávající o postupech při výchozích revizích, přináší poněkud odlišné pojetí, než jsme byli zvyklí podle ČSN 331500, která stanovuje ověření stavu zařízení z hlediska bezpečnosti, ČSN 332000-6-61 stanoví navíc povinnost před uvedením do provozu zařízení v rámci výchozí revize prohlédnout a vyzkoušet. Norma zahrnuje v podstatě tři činnosti: prohlídku, zkoušení a měření. Zápis či protokol o vlastních funkčních zkouškách je možno přiložit k protokolu o výchozí revizi. Z legislativních důvodů je však vhodné tyto činnosti formálně od revize oddělit. Prakticky by výchozí revizi měl provádět revizní technik montážní organizace, který má vedle odborné kvalifikace § 9 ve smyslu zák. 50/1978 Sb. také dostatečné znalosti o nainstalovaných zařízeních, neboť existuje riziko poškození citlivých obvodů zařízení CCTV při určitých měřeních během praktického provádění revize. V každém případě by měl být při výchozí revizi k dispozici technik realizační firmy, který byl za montáž odpovědný a dokonale zná namontovaný systém.

Při oživování postupujeme ve směru videosignálu od kamer, přes přenosové trasy, zařízení na zpracování videosignálu k monitorům a záznamovým zařízením (jsou-li součástí systému).

#### 9.4.2.1 Oživení kamer

Nejprve nastavíme přepínače umístěné na tělese kamery. Obvykle se jimi nastavují: druh řízeného objektivu, parametry elektronické závěrky (Shutter), kompenzace protisvět-

la, u barevných kamer režim vyrovnání bílé a automatického řízení citlivosti. Mechanicky musíme uvolnit aretaci přestavovací kulisy čipu a namontujeme objektiv v provedení C nebo CS. K řízeným objektivům musíme připojit odpovídající konektory (nejčastěji užívané jsou mini – DIN, mini – square). Připojíme kontrolní monitor, a teprve poté zapneme napájecí napětí.

Na kontrolním monitoru sledujeme snímanou scénu. Nejprve nastavíme správnou polohu čipu vzhledem k použitému typu objektivu (C/CS), u objektivů s proměnnou ohniskovou vzdáleností (variofocus) také přesně dostavíme zorné pole.

Pro objektivy s ručně řízenou clonou nastavíme pro dané světelné podmínky optimální obraz bez přesvětlených ploch, a také bez ztráty detailů v temných plochách.

Pro objektivy s automaticky řízenou clonou nastavujeme úroveň řídicího videosignálu (ovládací prvek Level) pro dané světelné podmínky na optimální obraz bez přesvětlených ploch a také bez ztráty detailů v temných plochách. V případě složitých podmínek s bodovými či plošnými světelnými zdroji je možné při nastavování využít druhého ovládacího prvku objektivu (ALC), jenž ovládá integrační konstantu regulační smyčky objektivu. Krajiní polohy A (*average level*) a P (*peak level*) vyjadřují extrémy v regulačním rozsahu objektivu při reakci na střední hodnotu osvětlení přes plochu snímané scény, či reakci na hodnotu maximálního osvětlení, jež se v zorném poli vyskytuje.

Pro složité světelné podmínky je účelné zapojit paralelně ke kontrolnímu monitoru osciloskop a kameru nastavovat na zkušebních obrazcích. Při nastavování řízených objektivů za vysoké intenzity okolního osvětlení je vhodné použít neutrálně šedý filtr k jejímu snížení. Zabráníme tím jevu rozostření sledovaného předmětu při poklesu intenzity okolního osvětlení. Zde vycházíme ze skutečnosti, že čím více je uzavřena iris clona řízeného objektivu, tím větší je hloubka ostrosti a naopak.

### 9.4.2.2 Oživení polohovacího stanoviště

Polohovací stanoviště je nutné před připojením k řídicí jednotce oživit samostatně. Důležité je nastavení dorazů polohovacích hlavíc a nastavení motorzoomů tak, aby bylo možné zaostřit obraz v celém rozsahu přeladění. Před připojením řídicích vodičů je nezbytné místně přetestovat všechny funkce dálkového ovládání polohovacího stanoviště. U venkovních stanovišť si zaslouží pozornost přetestování funkce termostatických spínačů a topení kamerových krytů. K tomuto účelu lze v běžných podmínkách využít chladicí spreje.

### 9.4.2.3 Oživení přenosových tras

Po nastavení kamery připojíme přenosovou trasu. V místě zakončení trasy na monitorovacím pracovišti připojíme kontrolní monitor, popř. osciloskop. Hrubé závady – přerušení vedení, přerušení středního vodiče či stínění, chybné nalisování konektorů, nepřizpůsobení trasy – se projeví viditelně přímo na kontrolním monitoru. Chceme-li však ověřit, zda má přenosová trasa odpovídající parametry z hlediska útlumu či kmitočtové charakteristiky, musíme využít přenosu signálu zkušebních obrazců nebo využít profesionální generátor měřicích signálů. Minimálně osciloskop je však potřebný při nastavování parametrů kompenzačních zesilovačů a převaděčů signálu nesymetrického na symetrický signál přenášený krouceným párem vodičů a naopak.

### 9.4.2.4 Oživení monitorovacího pracoviště

Jsou-li nastaveny všechny kamery a ověřeny všechny přenosové trasy, můžeme připojit kamery k jednotlivým vstupům zařízení, zkontrolovat a zajistit přizpůsobení vstupů. Připojíme monitor (či příslušný počet monitorů) a ověříme přizpůsobení. Připojíme ovládací díl (či díly), nejsou-li integrovány do skříně vlastního zařízení. Poté zapneme napájení zařízení na zpracování videosignálu. Ověříme existenci a správnost videosignálu na jednotlivých vstupech. Provedeme textovou identifikaci jednotlivých signálů (umožňuje-li to zařízení).

Poté implementujeme příslušný provozní režim systému pomocí specifického softwaru zařízení. Alternativou je nahrání příslušného nastavení z přenosného PC přes port RS 232 zařízení. Naprogramovaný provozní režim přetestujeme na všechny využívané funkce. Existuje-li hierarchie přístupových práv k jednotlivým ovládacím zařízením či k programování, implementujeme ji. Zodpovědnost za provoz systému CCTV musí být u uživatele stanovena zcela jednoznačně.

### 9.4.2.5 Oživení příslušenství

Teprve po přetestování základní funkce zařízení připojíme záznamová zařízení (videomagnetofon, videotiskárna) a řídicí interface ostatních systémů (EZS, přístupové systémy).

### 9.4.6 Oživení podružných monitorovacích pracovišť

Tato pracoviště přicházejí na řadu jako poslední po oživení monitorovacího pracoviště a zajištění součinnosti s jinými, v objektu instalovanými zařízeními.

### 9.4.7 Ověřování funkce systému CCTV

Před vlastním předáním systému by realizační firma měla učinit rozhodně dále uvedené kroky, a to nejlépe prostřednictvím svého revizního technika.

Před předáním či jako součást převímacího řízení systému CCTV do provozu je vhodné provést ověření funkce všech zařízení v systému nainstalovaných. Jde o doporučený rozsah funkčních zkoušek, ověřování činností a dokumentace související s realizací.

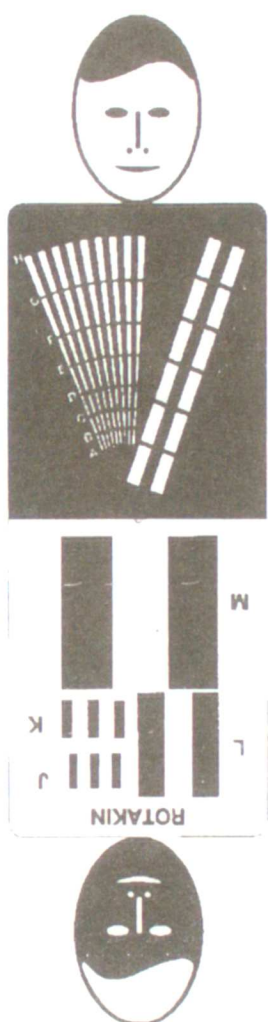
#### **Kontroluje se, zda zařízení jako celek má požadované vlastnosti.**

Zde se především kontroluje soulad s požadavky zákazníka. Systém se koncepčně posoudí, zda jeho vlastnosti odpovídají účelu nasazení. Vizuelním testem se kontroluje splnění funkčních požadavků a shoda se systémovou specifikací. Velkým pomocníkem je zde využití testovací metody ROTAKIN vyvinuté pro převímací zkoušky Městských dohlížecích kamerových systémů ve Velké Británii. Tato metoda je normalizována a popsána v normě ČSN EN 50132-7.

#### **Kontroluje se, zda provedení a úplnost montážních prací je v souladu s platnou projektovou dokumentací doplněnou o změny vzniklé v průběhu výstavby.**

Zde se kontroluje úplnost systému ve vztahu k projektu. Veškeré odsouhlasené změny vzniklé v průběhu výstavby musí být zapracovány do finální verze projektové dokumentace.





Obr. 5-52: Testovací obrazec ROTAKIN.

**Kontroluje se, zda je zařízení vybaveno průvodní dokumentací.**

- **Uživatelský manuál** (návod k obsluze), jenž popisuje obsluhu zařízení a postupy uživatele při preventivní údržbě a zkouškách zařízení během provozu.

- **Prohlášení o shodě** (popř. ujištění o tom, že bylo prohlášení o shodě vydáno) z hlediska splnění zákonných požadavků (viz. kap. 1) pro všechny relevantní komponenty systému.

**Kontroluje se provedení kabeláže napájecích a přenosových tras.**

Napájecí trasy podléhají pravidlům pro provádění revize silnoproudé části. U přenosových tras kontrolujeme jejich provedení, celistvost, spojování kabelů a jejich připojení ke koncovým zařízením. Namátkově lze ověřit delší trasy z hlediska útlumu a ztráty rozlišovací schopnosti.

**Posuzuje se zařízení CCTV vzhledem k umístění v daném prostředí, umístění jednotlivých částí zařízení CCTV a jejich přístupnost.**

Výchozím bodem je zde protokol o určení druhu prostředí ve smyslu (ČSN 332000-3, ČSN 332000-5-51) popř. u prostředí jednoduchých alespoň zápis o určení prostředí.

Zde se kontroluje nasazení jednotlivých prvků z hlediska technických podmínek výrobce. Prvky musejí být umístěny v souladu s doporučením výrobce s ohledem na požadovanou funkci. Jejich umístění musí umožňovat přístup pro potřeby oprav a údržby i pro potřeby preventivních technických prohlídek a pravidelných revizí.

**Zjišťují se funkční vlastnosti jednotlivých částí zařízení CCTV. Při zkouškách se přihlíží k technickým podmínkám, k návodu pro obsluhu a údržbu jednotlivých zařízení CCTV a k pokynům pro obsluhu zařízení CCTV.**

Zde se kontroluje funkčnost jednotlivých prvků dle návodu k obsluze systému.

**Kontroluje se, zda při provozu zařízení nemůže dojít k ohrožení osob nebo okolí.**

Lze sem zařadit kontrolu nasazených prvků z hlediska hygienických předpisů. Zásadně by v místě s trvalým pracovním pobytem osob neměly být nasazeny takové prvky, které jsou zdrojem elektromagnetických polí v takové intenzitě, jež může při dlouhodobém pobytu poškodit zdraví pracovníků. Zde jde o mikrovlnné pole u přenosových zařízení, rentgenové záření obrazovek monitorů, popř. u laserového přenosového zařízení možnost vstupu osoby do přímého paprsku.

**Kontroluje se, zda provoz zařízení není rušen jinými zařízeními nebo zda sám jiná zařízení neruší.**

Zde se kontroluje především kompatibilita zařízení s ostatními sdělovacími a silovými zařízeními, instalovanými v objektu (počítačové sítě, ventilace, osvětlení, reklamní tabule, EZS, EPS, přístupové systémy apod.).

### 9.4.8 Předání systému CCTV

Jedná se o protokolární akt, při němž realizační firma předává **přejímací protokol**, jenž potvrzuje funkční a úplné předání předmětu smlouvy, stanovuje termíny odstranění případných nedostatků, stanovuje termín vypršení záruční lhůty (v měsících), stanovuje pracovníka uživatele zodpovědného za provoz systému CCTV a osoby zmocněné k hlášení závady na systému a dále potvrzuje řádné zaškolení obsluhy. Přílohou přejímacího protokolu jsou následující dokumenty:

- projekt skutečného provedení,
- oboustranně potvrzený soupis skutečně nainstalovaného zařízení s příslušnými prohlášeními o shodě,
- protokol o výchozí revizi,
- protokol o provedení funkčních zkoušek,
- návody k obsluze,
- zápis o vyhodnocení zkušebního provozu (pouze v případě, že je zkušební provoz požadavkem specifikovaným ve smlouvě),
- další smluvně ujednané dokumenty a materiály (např. výrobní certifikáty, náhradní díly, přípravky pro běžnou údržbu apod.).

### 9.5 Etapa V. – Provoz systému CCTV

Systémy CCTV většinou pracují v nepřetržitém režimu 24 hod. denně. Přestože je elektronika dnes vysoce spolehlivá, neobejde se ani systém CCTV bez pravidelné údržby, preventivních technických prohlídek, ověřování funkčnosti a pravidelných revizí elektrických zařízení. Tyto činnosti je vhodné podchytit smluvně s firmou, která systém CCTV v objektu realizovala.

#### 9.5.1 Údržba systémů CCTV

Systémy CCTV většinou pracují v nepřetržitém režimu 24 hod. denně. Přestože je elektronika dnes vysoce spolehlivá, neobejde se ani systém CCTV bez pravidelné údržby.

S ohledem na prostředí, ve kterém je systém CCTV v provozu, je účelné stanovit periodicitu těchto preventivních technických prohlídek. Zvolený interval pravidelné údržby připadá v úvahu od jedné do čtyř prohlídek ročně. Z hlediska vlivu prostředí jsou nejpodstatnějšími faktory prašnost, korozní agresivita, vlhkost a vibrace.

V průmyslovém prostředí tvoří asi největší problém prach. Tabulku kategorizace z pohledu prašnosti lze využít nejen při plánování údržby, ale i při rozhodování o krytí zařízení při návrhu konfigurace systému CCTV.

Tabulka 5-21: Kategorizace prostředí s ohledem na úroveň prašnosti

Prostředí	Nečistota		Odstraňování nebo filtrace nečistoty	Adheze nečistoty	Příklady prostor
	vznikající	z okolních prostor			
velmi čisté (VČ)	žádná	žádná, nebo se do prostoru nedostává	výborné	žádná	operační sály, laboratoře, moderní kanceláře, pracoviště pro mimořádně jemné práce
čisté (Č)	velmi malá	téměř žádná, nebo se do prostoru nedostává	nadprůměrné	malá	rýsovny, ateliéry, dozorny, kanceláře, studovny, učebny, obytné prostory, společenské a kulturní prostory
průměrné (P)	znatelná, ale ne velká	určitá se do prostoru dostává	podprůměrné	viditelná po několika měsících	spotřební průmysl, restaurace, prostory pro pohybovou rekreaci a rekreační sport
špinavé (Š)	rychle se shromažďuje	velké množství se dostává do prostoru	pouze větráky nebo dmychadly	vysoká (pravděpodobně vlivem oleje, vlhkosti či elektrostatických sil)	těžké strojírenství, lakovny, kotelny na tuhá paliva, výroba pneumatik, živočišná výroba, svařovny
velmi špinavé (VŠ)	stálé hromadění	téměř žádná se neodstraňuje	žádné	vysoká	stejně prostory jako špinavé, ale zařízení je instalováno přímo v prostoru znečištění

Jaké činnosti by se měly při pravidelných technických prohlídkách provádět?

- přezkoušet mechanické upevnění kamer,
- překontrolovat jejich správné nastavení,
- vyčistit okénka kamerových krytů či čočky objektivů,
- ověřit správné nastavení clony, popř. rozsah regulace u objektivů s automaticky řízenou clonou,
- přezkoušet konektorové spoje,
- přezkoušet funkci všech v systému používaných zařízení na zpracování signálu včetně všech jejich funkcí a připojení,
- vyčistit vnitřní prostory monitorů od prachu nasátého elektrostatickými účinky vysokonapěťového zdroje,
- přezkoušet ostření monitorů a jejich případné dostavení,
- přezkoušet záznam a reprodukci u videorekordérů (timelapse) a digitálních záznamových zařízení,
- přezkoušet kvalitu tisku u videotiskáren.

### Použitá literatura

1. Vít, V. a kol.: Televizní technika, Praha, SNTL, 1979
2. Košťál, E.: Obrazová a televizní technika II, Praha, Vydavatelství ČVUT, 1993
3. Ptáček, M.: Přenosové soustavy barevné a digitální televize, Nakladatelství dopravy a spojů, 198.
4. Habel, J.: Osvětlování, Praha, Ediční středisko ČVUT, 1991
5. Habel, J.: Světelná technika, Praha, Ediční středisko ČVUT, 1990
6. Schröder, G.: Technická optika, Praha, SNTL, 1981
7. Klimeš, B. – Kracík, J. – Ženíšek, A.: Základy fyziky II., ACADEMIA, 1972
8. Siemens, E.: Handbuch Sicherungstechnik, Heidelberg, Kriminalistik Verlag, 1993
9. Wege, A.: Video Überwachungstechnik, Heidelberg, Hütig GmbH, 1994
10. WS special, Juni 1992, Sondernummer, Heidelberg, Kriminalistik Verlag, 1992
11. Evropský magazín pro bezpečnost, Euro Security Fachverlag, Mettmann, ročník 2001 – 2002
12. Firemní literatura firem Computar, Dallmeier, Dedicated Micros, JVC, Mitsubishi, Panasonic, Philips, Samsung, Sony, Tokina, Videor Technical
13. Gwozdek, M.I.: Lexikon der Videoüberwachungstechnik, Heidelberg, Hütig GmbH, 1997

# **IP - kamerové systémy**

*Jiří Bartáček, Stanislav Křeček*

## **OBSAH:**

<b>1 Digitalizace TV snímku</b> .....	239
1.1 Přenos digitalizovaného videosignálu .....	239
1.2 Uložení digitalizovaného videosignálu .....	240
1.3 Komprese videosignálu .....	240
<b>2 Digitální systémy CCTV</b> .....	243
2.1 Prvky digitálních systémů CCTV .....	246
2.2 Digitální záznamová zařízení .....	248
<b>3 Základy techniky počítačových sítí</b> .....	250
3.1 Rozdělení .....	250
3.2 Architektura .....	250
3.3 Topologie .....	250
3.4 Jednotky a rychlost přenosu .....	252
3.5 Kabely, konektory a jejich zapojení .....	253
3.6 Hardware .....	258
3.7 Software .....	259
3.8 Dálkové napájení .....	268
3.9 Bezdrátové systémy Wi-fi .....	271
<b>4 Plánování</b> .....	276
<b>5 Příklad praktického použití</b> .....	277
<b>6 Popisy konkrétních prvků</b> .....	280
6.1 Nastavení a konfigurace IP kamer .....	281
6.2 Nastavení a konfigurace videoserverů .....	283
<b>7 Nastavení a konfigurace Access Pointu (AP)</b> .....	285
7.1 Základní informace .....	285
7.2 Technické parametry .....	285
7.3 Instalace .....	286
<b>8 Nastavení a konfigurace IP Wi-fi kamery</b> .....	287
8.1 Základní informace .....	287
8.2 Technické parametry .....	288
8.3 Instalace .....	288



## 1 Digitalizace TV snímku

V CCTV v našich zeměpisných šířkách a délkách je užíván přenosový standard CCIR. Ze základních parametrů lze odvodit teoreticky největší rozlišovací schopnost obrazu ve standardu CCIR. Počet viditelných řádků 575 (50 řádků slouží pro snímkové zatemnění – 25 ř. lichý a 25 ř. sudý pulsnímek)

Pro stejnou rozlišovací schopnost viditelného obrazu ve vertikálním i horizontálním směru bychom potřebovali podél řádků rozlišit  $(4:3) \times 575 = 767$  obrazových bodů.

Viditelný obraz lze tedy vyjádřit jako matici  $575 \times 767 = 441\,025$  obrazových bodů. Představme si tento obrazový bod jako paměťovou buňku, která vedle definované polohy v rámci snímku musí být u černobílého signálu nositelem jasu (256 úrovní šedé odpovídá v digitální podobě 8 bitům a 1024 úrovní šedé 10 bitům) a u barevného signálu musí nést ještě informaci o barvě. Prostou matematickou operací – násobením zjistíme potřebnou kapacitu paměti pro jeden obrazový snímek o plné rozlišovací schopnosti dané standardem CCIR.

Tabulka 6-1: Potřebné objemy dat pro digitalizaci obrazového snímku bez komprese

Typ videosignálu	Počet obrazových bodů	Počet stupňů šedé	Počet barevných odstínů	Objem dat (Mbit)
čb videosignál	440 000	256	-	3,5
čb videosignál	440 000	1024	-	4,4
barevný videosignál	440 000	256	256	7
barevný videosignál	440 000	1024	1024	8,8

### 1.1 Přenos digitalizovaného videosignálu

Pokud vyjdeme z počtu 25 snímků za sekundu (což odpovídá ve standardu CCIR 50 pulsnímkům o 312,5 řádcích při prokládaném řádkování), lze spočítat potřebný datový tok pro nezkomprimovaný tv signál v digitální podobě:

$$8,8 \text{ Mbit} \times 25 = 220 \text{ Mbit/s}$$

Tabulka 6-2: Kapacity přenosových sítí

Přenosová síť	Standard	Rychlost přenosu
JTS (jednotná telekomunikační síť)	V 34/V34+	28,8 KBit/s
Euro – ISDN	Standard 1 * S 0	64 – 128 Kbit/s
	Standard 3 * S 0	64 – 384 KBit/s
širokopásmová ISDN		2 MBit/s
síť LAN		100 MBit/s
síť ATM		2 GBit/s

### 1.2 Uložení digitalizovaného videosignálu

Lze odvodit i potřebné kapacity paměti pro uložení příslušného počtu snímků:

U klasického analogového videorekordéru v reálném režimu záznamu při použití videokazety o délce 3 hodiny (E180) je možno uložit 540 000 snímků.

Pokud bychom chtěli obdobným způsobem uložit barevné snímky v digitální podobě s 10 bit vzorkováním v plné rozlišovací schopnosti dané standardem CCIR bez komprimace potřebovali bychom paměť o kapacitě:

$$540\,000 \times 8,8 \text{ Mbit} = 4752000 \text{ Mbit} (4,6 \text{ GB})$$

Pokud bychom tedy použili k uložení videodat pevný disk běžného počítače o kapacitě např 40GB, a byl-li by vyhrazen pouze pro videodata, kapacita by nám nestačila ani na 10 hodin kontinuálního záznamu jedné kamery.

### 1.3 Komprese videosignálu

Bez vývoje kompresních algoritmů by zůstal digitální systém CCTV ještě dlouho pouhou teorií. Všem postupům videokomprese je společné, že odstraňují **nadbytečné** (redundantní) a **zbytečné** (irelevantní) informace z obrazu.

**Nadbytečné informace** se identifikují podle druhu digitalizace obrazu v řádkové rozteči pravouhlé mřížky obrazových bodů. Přitom reprezentují sousední obrazové body velmi často stejný jas a barevný odstín. To znamená, že příslušná informace je již k dispozici, je ale většinou vícenásobně opakována pro popis rozsahu oblasti s daným jasnem a barevným odstínem. Efektivním popisem je možno tyto redundance odstranit, aniž by pozorovatel rozeznal jakýkoliv rozdíl. Příkladem může být přenos obrazu záběru kamery bez pohybů ve snímané scéně. Sled snímků popisuje vždy stejný obraz se stejným informačním obsahem (hodnotou dat). Stačí tedy vyslat na přijímací stranu informaci o tom, že se nic nezměnilo a opakovat na přijímací straně stále první ze sekvence snímků. Tím se značně redukuje datové toky, aniž by pozorovatel zaznamenal jakékoli zhoršení kvality obrazu.

Redukce zbytečných informací, které nemůže pozorovatel postřehnout vychází buď z psychofyzikálních vlastností lidského zraku, nebo jsou to informace mimo oblast zájmu pozorovatele, jako např. barevné odstíny v pozadí scény. Klasifikace rozdílných typů informací však není možné provádět zcela bezchybně, proto také může kódovací zařízení některé relevantní informace zkreslit. Při rekonstrukci kódovaného obrazu se pak mohou objevit tzv. **artefakty – důsledky chyby kódování**.

Vlastní postup komprese lze laicky popsat asi následovně:

- Aktuální obraz předvídej z minulosti pokud možno nejlépe, jak jen to jde.
- Přenášej pouze to, co ještě nebylo přeneseno (redundance) a to, se nedá předpovídat z minulosti (změny) a eliminuj zbytečné informace s co nejmenším zatížením kapacity paměti.
- Odhad zpřesni procesem výpočtu pohybů jednotlivých obrazových bodů v rámci snímku a předvídaním jejich nové polohy.

Na trhu existuje více, mezi sebou nekompatibilních standardů. Každý výrobce zařízení pro digitální zpracování obrazu volí spíše s ohledem na tržní zaměření zařízení některý z existujících standardů. Některé standardy jsou spíše vhodné pro archivaci, jiné pro přenos. Každý má své výhody a nevýhody a záleží pouze na koncepci vývojářů a marke-



tingové strategii firmy, který standard využijí. V oblasti CCTV pro bezpečnostní aplikace v současné době sice převažují kompresní algoritmy, jež pocházejí z oblasti multimédií ale všeobecný konsensus zatím nepanuje. V poslední době se zdá, že v oblasti CCTV zvítězí komprese typu Wavelet, nicméně vývoj kompresních algoritmů jde neustále dále.

Již jsme uvedli, že komprese je jedním z předpokladů aplikace videosystémů v digitálních přenosových sítích. Zde bychom chtěli vysvětlit, proč je vůbec komprese videodat nutná a jaký druh kompresního algoritmu se nejlépe hodí pro určitou aplikaci.

Digitalizace analogového videosignálu (standardu NTSC nebo PAL) se obvykle provádí podle normy CCIR 601. Tato norma zajišťuje reálné a vysoce kvalitní zobrazení videosignálu na úkor požadavků vysoké datové rychlosti. Digitální formát CCIR 601 vyžaduje šířku pásma přibližně 140 Mbit/s. I když má video nižší rozlišení, např. ve formátu Common Intermediate Format (CIF) s 352 pixely (horizontálně) a 288 řádky (vertikálně) a je přenášen pouze každé druhé pulsníkové, není výsledná datová rychlost nižší než přibližně 35 Mbit/s.

Na druhé straně i moderní sítě jako například FastEthernet mají síťovou kapacitu přibližně 40 Mbit/s. Proto by už jediný tok digitalizovaného videosignálu s nízkým rozlišením naprosto vyčerpával kapacitu moderního vysokorychlostního síťového propojení. Porovnáme-li rychlost modemu (běžného starého telefonního) 33,6 kbit/s s požadavky videa a hned nám musí být jasné, proč je nutná komprese a co taková komprese dokáže. Moderní standardy pro videokompresi jako H.263 poskytují kvalitu typu VHS při datových rychlostech přibližně 500 kbit/s. Ani živý videopřenos přes telefonní linky o obnovovací frekvenci přibližně 15 obrázků za sekundu není problém. To vše dokazuje, že dnešní sítě jsou skutečně schopné podporovat mnoho paralelních toků videodat.

Když tedy víme, proč je nutná videokompresse, položme si další otázku: Jakou metodu či algoritmus je nejlepší použít? Podrobné vysvětlení všech v současné době používaných algoritmů a jejich výhod a nevýhod by přesahovalo rámec tohoto materiálu, ale načrtneme alespoň několik obecných přístupů.

Videokamera generuje 50 pulsnímků za sekundu. Pokud aplikace vyžaduje hodně plynulý pohyb a maximální kvalitu videa, je nejlepší použít algoritmus MPEG-2. MPEG-2 se kromě jiného používá i na DVD a při digitálním vysílání satelitní televize, pro které bylo především vyvinuto. O kvalitě tedy nemůže být pochyb. Na druhé straně má MPEG-2 skutečně smysl pouze při datových rychlostech nad 2 Mbit/s (DVD mají rychlost přibližně 6 Mbit/s), a proto se MPEG-2 používá především v prostředí objemných LAN (Local Area Network) nebo při záznamu na pevný disk. Pokud je nejdůležitější datová rychlost, například u aplikací WAN (Wide Area Network) přes ISDN nebo dokonce přes analogové telefonní linky PSTN (Public Service Telephon Network), je lepší omezit počet pulsnímků na maximálně 30 a použít H.323, což je standard pro videokonference na Internetu. Standard H.323 a jeho základní videokódovací schéma H.263 je velmi účinné a vykazuje minimální zpoždění. Co nejmenší zpoždění je důležité pro reálné živé monitorování a rovněž pro dálkové ovládání mechanismů polohovacích zařízení a motorzoomů kamer.

Jaký má toto vše vztah k stále tak populárnímu algoritmu JPEG? JPEG obecně je schéma pro kódování nehybných obrázků. Termín „M-JPEG“, kde „M“ zastupuje „motion“ („pohyb“), se vztahuje k postupné aplikaci metody JPEG na každý z pulsnímků videosignálu. Jelikož statické oblasti nejsou filtrovány, není brán v úvahu pohyb ani časové redundance, je JPEG vždycky méně účinný než jiné uvedené standardy. Jako základní pravidlo

pro jakoukoli danou snímkovou frekvenci a kvalitu obrazu platí, že JPEG nebo M-JPEG vyžadují desetkrát vyšší datovou rychlost. Opačně to znamená, že při pevně dané datové rychlosti zajistí M-JPEG desetinu snímkové frekvence. Metoda Wavelet je o něco účinnější, ale dosud přetrvává totéž základní chování. Jak JPEG, tak i Wavelet jsou vhodné pro aplikace lokálního ukládání, kde je snadná manipulace, jako například volitelný výběr obrázků a zpětné přetáčení po jednotlivých krocích, důležitější než celková účinnost algoritmu. V tabulce 1 jsou porovnány nejvíce používané kompresní algoritmy.

Tabulka 6-3: Porovnání vlastností kompresních algoritmů

standard	M – JPEG	MPEG	H.261	WAVELET
Použití	záznam statických a pohyblivých obrázků	záznam pohyblivých obrázků	přenos pohyblivých obrázků	záznam/přenos pohyblivých obrázků
Princip	stálý časový rozestup snímků	analýza změn obrazu	analýza změn obrazu	analýza změn obrazu
Velikost snímku	15 – 50 kB	25 – 45 kB	max. 50 kB	5 – 45 kB
původ	digitální zpracování fotografií	multimedia (CD – I, DVD)	telekomunikace (videokonference)	CCTV
vnitřní kódování snímků	žádné	vektorové	změny/žádné	změny
zobrazení jednotlivého obrazu	ano	omezené	ano	ano
hodnocení přenos	+	++	++++	+++
hodnocení záznamu	++++	+	+	+++
zvláštní charakteristika	konstantní kvalita obrazu	konstantní kvalita obrazu	konstantní datový tok	konstantní kvalita obrazu + konstantní datový tok

Z velikosti jednoho snímku lze odvodit **kompresní poměr** oproti digitalizovanému videosnímků v plném rozlišení. Tento parametr je často uváděn jako jeden ze základních parametrů digitalizace videosignálu. Nejčastěji je i tento parametr u digitálních záznamových zařízení volitelný v určitém rozmezí. Se zvětšováním kompresního poměru se logicky snižuje schopnost rekonstrukce snímku v původní kvalitě. Dochází k degradaci především v oblasti rozlišovací schopnosti.

Ve skutečnosti je signál, který je digitalizován omezen vlastní **rozlišovací schopností kamery**. Ta je dána především počtem aktivních snímacích prvků (pixelů) CCD čipu. Rozlišovací schopnost kamery je dnes spíše uváděna údajem matice aktivních snímacích prvků (např. 754x256) bodů. Alternativně pro analogové systémy zůstává uvádění rozlišovací schopnosti v tv řádcích, což je vlastně počet černých a bílých pruhů, které je schopna kamera v horizontálním směru v signálu ještě rozlišit na úrovni -3dB (poloviční

rozkmit analogového signálu oproti plnému rozkmitu 1Všš černá-bílá) za předpokladu ještě přijatelného odstupu signál/šum (40dB a více).

Účinnost komprese je navíc dána charakterem snímané scény (množstvím drobných detailů v zorném poli snímané scény a proměnlivostí této scény).

To jsou důvody, proč je těžké jednoznačně stanovit skutečnou **kapacitu digitálních záznamových zařízení** (časovým údajem doby záznamu nebo počtem zaznamenaných snímků) v poměru ke kapacitě záznamového média v GB či TB. Jednoznačné vyjádření tak, jak jsme byli zvyklí u analogového záznamu na videorekordér zde neexistuje! Uváděné kapacity vychází vždy z předpokladu statisticky "normální snímané scény" a z navolené stupně komprese - tedy požadované kvality (rozlišovací schopnosti) obrazu a z obnovovací frekvence (počtu snímků za sekundu).

## 2 Digitální systémy CCTV

Digitální systémy CCTV musí tedy ve svém komplexu vždy řešit prakticky všechny 4 úlohy:

- Digitalizaci videosnímku,
- kompresi digitalizovaného videesignálu,
- přenos digitalizovaného videesignálu,
- uložení digitalizovaného videesignálu.

Vlastní zobrazení pak může být běžnou úlohou dnešní počítačové techniky, která je již relativně zvládnuta, a nebo mohou být videodata převedena (dekódována) zpět do analogového videesignálu standardu PAL.

Základní podmínkou rozvoje digitálních systémů CCTV je vývoj technologií počítačových sítí a především jejich rychlosti.

V minulosti byla většina sítí realizována sběrnicovou topologií, která používala takzvaný Thinwire nebo Thickwire Ethernet. Všechna zařízení byla připojena k síti prostřednictvím připojovací jednotky nebo odbočením ze sběrnice T-konektorem typu BNC. Všechna propojená zařízení měla společnou pásmovou šířku Ethernetu. Pokud došlo k poruše nebo někdo neodborně manipuloval s konektorem, zhroutila se funkce veškerých zařízení připojených k téže sběrnici. Tento druh síťové kabeláže se nazývá 10Base2

V současnosti se už sběrnicová topologie prakticky nepoužívá. Místo ní převládá takzvaná hvězdicová topologie neboli 10BaseT u standardního Ethernetu a 100BaseTX u FastEthernetu: každý výstup je připojen zvlášť k síťovému přepínači (switch) a tvoří takzvané rameno sítě. Každé rameno neboli výstup má k dispozici plnou síťovou rychlost, např. 100 Mbit/s.

Pokud chce některé síťové zařízení poslat data sousednímu zařízení, rozpozná switch lokální povahu přenosu a předá balíčky dat (packets) bez interference jakéhokoli jiného připojeného zařízení přímo příjemci. Pouze když adresovaný přijímač nesídlí na stejném síťovém přepínači, je přenos veden přes páteř. Pro páteř se obvykle vybírá technologie s vyšší rychlostí, např. ATM nebo Gigabit Ethernet, aby nedocházelo k zahlcování této páteřní sítě.

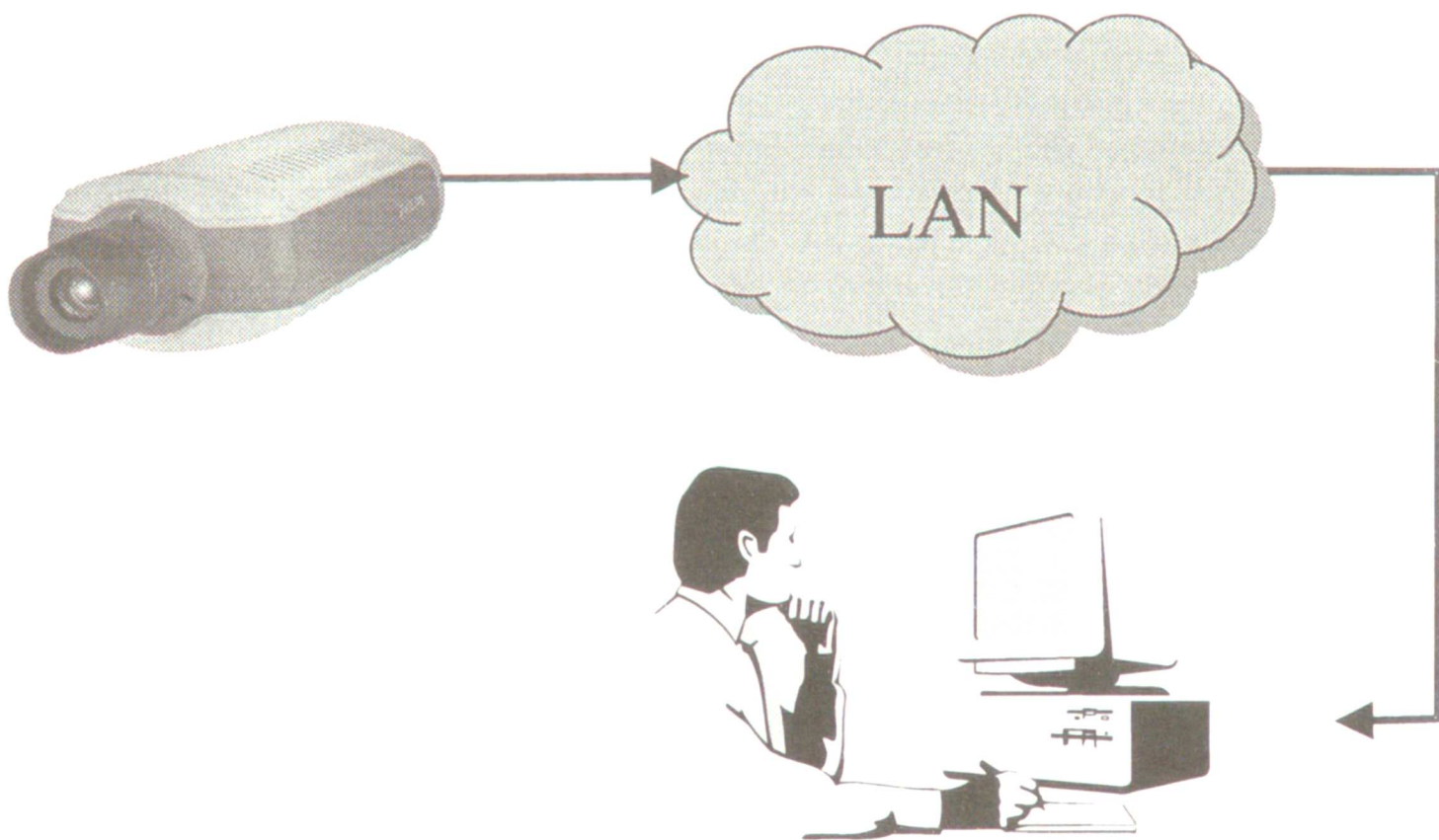
S propojením hvězdicovou topologií již video v síti není nijak na obtíž ostatním uživatelům sítě, dokonce ani v případě velkého počtu kamer. Abychom si byli naprosto jisti, můžeme použít pro videoprovoz jednoúčelový switch, který účinně oddělí videodata od

ostatního provozu na síti, ale přesto zachová využití stávající kabeláže hvězdicové topologie.

V analogovém světě může být videosignál připojen k více než jednomu přijímači. Kamera je obvykle připojena k monitoru za účelem zobrazení a paralelně k VCR za účelem nahrávání. Signál je navíc veden do matice nebo připojen k přenosovému zařízení. Za tímto účelem se používají smyčkové propojení, kde je odbočení videosignálu ve všech jednotkách vysokoimpedanční kromě poslední jednotky v řetězci. Základní požadavek je zachování charakteristické impedance vedení a přizpůsobení na straně zdroje videosignálu i „spotřebiče“. Pro případ ještě obsáhlejší distribuce signálu jsou k dispozici speciální distribuční videozesilovače, které jsou schopny se postarat o více výstupů při zachování normalizovaných parametrů analogového videosignálu.

Ve světě digitálního síťového propojení se simultánní prohlížení nebo záznam síťového videozdroje nazývá „**skupinové adresování**“. Na rozdíl od spojení z bodu do bodu, kterému se rovněž říká „**přímé adresování**“, zajišťuje skupinové adresování současný příjem téhož toku videodat v několika přijímačích. Nejdůležitějším aspektem skupinového adresování je účinnost. Datový tok není duplikován vysílačem, nýbrž replikován uvnitř sítě podle potřeby. Proto se nemůže stát, že by vysílač a síťové spojení s vysílačem byly přetíženy. Bez ohledu na počet přístrojů, které provádějí simultánní prohlížení, je na kamerovém konci tatáž datová rychlost.

Dalším známým mechanismem síťového propojení je všesměrové vysílání. Během síťového vysílání jsou informace, např. datové balíčky, vysílány nevyžádaně ke všem přístrojům na síti. Režimy všesměrového vysílání potenciálně velice zatěžují síť. Proto bychom se měli vyhýbat všesměrovému vysílání digitálního videa a používat i pro větší počet uživatelů videodat vysoce účinný režim skupinového adresování.



Ted', když jsme si vysvětlili hlavní stavební kameny síťového videa, tj. kompresi a síťové propojení, máme přehled o kompletním systému digitálního videa přes-IP. IP je synonymem síťového propojení obecně, díky popularitě Internet Protocolu (IP). Základní hlediska, která jsou zde použita, samozřejmě platí i pro ostatní typy sítí, například pro ATM.

Systém si můžeme představit jako síťový mrak, do nějž jsou připojeny komponenty síťového videa. Síťový mrak obsahuje všechny síťové komponenty nutné pro LAN nebo WAN kontext nebo jejich kombinace. Aby mohl datový balíček cestovat od vysílače k přijímači, může se stát, že bude nutné předat několik síťových prvků s potřebnými vlastnostmi.

Všimněme si, že přestože se počítačová síť v těchto případech používá k přenosu videa, není nutný žádný počítač. Argumenty proti používání počítače zahrnují větší bezpečnost (žádné hroucení systému), snadné používání (žádné operační systémy, žádná manipulace s myší), kompaktnost (videoservery se svými kompaktními rozměry vejdou do kabelovodů) a zvýšenou robustnost (žádný scandisk po výpadku elektřiny).

Na druhé straně jsou k dispozici **aplikace založené pouze na softwaru PC**, které zajišťují širokou škálu funkcí a jsou ekonomické. Počítač je k dispozici prakticky vždy a software je většinou součástí dodávky videoserveru. Z hlediska ceny a snadného použití nabízí nejvýhodnější řešení standardní webový prohlížeč. Specifické softwarové aplikace zajistí pestrou škálu exkluzivních funkcí, od multikanálového prohlížení přes archivování a poplachové řízení po operace založené na plánu topologie objektu, které jsou vhodné pro použití v rámci místa trvalé obsluhy a dozoru objektu nebo dokonce pro dálkový dohled.

Speciální třída těchto aplikací je zaměřena na záznam a příjem poplachových situací. Tento druh záznamu se nazývá **síťový videozáznam (NVR, network video recording)** a kamery zde nejsou připojeny lokálně, nýbrž logicky přes síť. Jakýkoli standardní počítač na síti vybavený tímto záznamovým zařízením může fungovat jako síťový videorekordér. V praxi jsou možnosti a aplikace síťového videa prakticky nekonečné.

Jak již bylo výše uvedeno, nabízí digitální technologie možnost videozáznamu založeného na síti. Jakýkoli standardní počítač je možno transformovat v zařízení pro záznam obrazu na pevný disk pouze s pomocí softwaru. Toky videodat dodávané z videoserverů po celé síti jsou zaznamenávány v předem definovaném režimu. Počítače mohou být umístěny kdekoli v síti, např. v serverové místnosti. Na rozdíl od speciálně vytvořených rekordérů s pevným diskem je síťový videozáznam založen na standardních PC platformách bez nutnosti jakýchkoli dalších přídavných zařízení. Standardní zařízení vždy představuje neekonomičtější a nejrozšířenější řešení. Pro požadavky ukládání ve velkém měřítku jsou k dispozici disková pole RAID, které mohou mít rozsah ukládací kapacity až několik terabytů.

Síťový videozáznam však nikdy nevytlačí lokální záznam. Bylo zjištěno, že přes 99% všech záznamů si již nikdo nikdy neprohliží, nýbrž časem je přepíše. Pro tyto případy je smysluplné aplikovat videoserver vybavený pevným diskem. Lokální záznam nepotřebuje síť a tím eliminuje její zatížení nevyžádaným přenosem toku videodat jako je tomu u koncepce síťového záznamu. Současně je však možno použít síť k archivování nebo ke zvýšení kapacity lokálního pevného disku (= virtual drive). A co víc, pevný disk video-

serveru je možno vybavit přes síť možností přístupu na dálku. Hledání a přehrávání archivovaných videozáznamů se může provádět z kteréhokoli místa v síti, což vlastně smaže hranici mezi lokálním záznamem a záznamem na dálku. Stejně jako Internet, kde uživatel většinou neví ani se nezajímá o to, kde jsou informace uloženy, hlavně když k nim rychle získá přístup, stane se síťové video univerzálním a cenově výhodným řešením pro průmysl CCTV i pro další oblasti.

### 2.1 Prvky digitálních systémů CCTV

V systémech průmyslové televize založených na IP technologiích se vyvinuly postupem času standardní systémové prvky, z nichž každý zastává určitou úlohu, kde lze většinou nalézt analogie s funkcemi systémových prvků „klasických“ analogových systémů CCTV.

Jedná se o:

- IP- kamery,
- IP- videosesvery,
- IP – dekodéry,
- IP – záznamová zařízení.

Mnohdy IP - systémové prvky tyto základní kategorie různě kombinují a navíc se zde užívají i systémové prvky, které standardně slouží k realizaci určitých funkcí na úrovni fyzické struktury počítačové sítě (SWITCH, HUB, počítač).

#### 2.1.1 IP - kamera

Je to základní systémový prvek, často je také nazýván **digitální kamerou**. V nabídkách distributorů je však nutno odlišit skutečně digitální kamery od těch, které mají na sobě toto slovo vytištěno, ale rozhraní k přenosové síti je běžný konektor BNC sloužící pro analogové připojení k běžnému koaxiálnímu vedení o charakteristické impedanci 75 Ohm. V těchto případech slovo „digitální“ vyjadřuje způsob zpracování signálu uvnitř kamery, signál je nakonec převeden do analogového standardu CCIR pro aplikace v běžných analogových sítích CCTV.

Poznámka: Konec konců i analogovou kameru CCD od počátků vývoje je možno v určitém slova smyslu považovat za digitální, neboť CCD snímací prvek je vlastně původně paměťové médium, kde je v aplikaci jako snímací prvek užito světlo (tok fotonů) k vytvoření náboje na jednotlivých aktivních prvcích (pixelech). Velikost tohoto náboje reprezentuje intenzitu osvětlení v místě obrazu transformovaného objektivem na plochu CCD čipu. Struktura CCD čipu je (na rozdíl od předcházející světlocitlivé vrstvy snímacích elektronek) ryze diskrétní a již zde dochází k prvnímu vzorkování obrazu a vlastně digitalizaci. Tento signál je však pracně zpět převeden do analogové podoby odpovídající standardu CCIR, aby bylo možno kameru v rámci CCTV vůbec použít. Pomineme-li zkreslení obrazu dané kvalitou optické soustavy objektivu, dochází již na ploše CCD čipu k první degradaci obrazu danou omezením rozlišovací schopnosti. Převod a zpracování v analogové podobě přináší další degradaci způsobenou superpozicí šumu do obrazového signálu. Ten je pak vyjadřován jako parametr odstup signál/šum uváděný v dB. Každý další prvek analogového kamerového řetězce včetně přenosového média signál již

jen zhoršuje. Pokud přejdeme k přenosu digitalizovaného signálu, je degradace obrazu dána vedle omezení rozlišovací schopnosti snímacího prvku CCD již jen způsobem komprese. Degradace digitálního signálu v přenosových systémech je pak prakticky nulová.

Jistě si můžeme položit otázku proč se nemontují do analogových kamer CCTV lepší čipy, když v oblasti digitální fotografie nejsou na trhu výjimkou fotoaparáty s čipy, které mají 3 milióny pixelů a dokonce se objevují fotoaparáty s čipy 6 - 8 miliónů pixelů. V případě analogové CCTV je hranice smysluplnosti počtu aktivních prvků CCD čipu dána mezní rozlišovací schopností standardu CCIR což je cca 440 000 obrazových bodů. U digitálních systémů CCTV můžeme do budoucna očekávat zlepšení kvality obrazu nad tuto mezní hranici. Současný limit je dán požadavky na kompatibilitu s analogovými komponenty CCTV (např. analogový monitor) ale hlavně neúprosným principem souvislosti rozlišovací schopnosti a šířky pásma přenosového kanálu. S vývojem kompresních a přenosových technologií však lze očekávat úplné odpoutání parametrů digitální CCTV od hodnot blízkých standardu CCIR.

Skutečná IP-kamera obsahuje standardizovaný konektor RJ 45 pro připojení k počítačové síti, napájecí konektor, případně podle typu kamery ještě další rozhraní pro ovládání příslušenství (poplachové vstupy a výstupy na řízení lokálního záznamu či osvětlení apod.). Některé IP-kamery obsahují navíc BNC konektor pro připojení standardního CCIR analogového monitoru pro potřeby nastavení kamery při instalaci. IP-kamera může obsahovat i paměťové médium (lokální disk) pro zajištění časově či počtem snímků omezeného záznamu v případě vyvolání poplachové události.

U ryze digitálních kamer bychom měli odlišovat od sebe tzv. IP - kamery, které je možno připojit přímo k počítačové síti a tzv. Web-kamery, které ke svému připojení k datové síti potřebují počítač. Z pohledu aplikace zůstávají podstatné běžné parametry jako je rozlišovací schopnost, citlivost, formát připojení objektivu, vybavení řídicími vstupy/výstupy a doplňkovými funkcemi. Navíc však přibývají parametry vztahující se k rychlosti obnovení snímku (obnovovací frekvence, která by se pro vnímání obrazu jako spojitého měla v ideálním případě blížit k 50 Hz), použitý algoritmus komprese a možnost nastavení stupně komprese, objem dat na jeden snímek, rozhraní pro připojení k datovým sítím, popř. kapacita vnitřní videopaměti.

### 2.1.2 IP - videosever

Jedná se o zařízení, které slouží pro připojení jedné, či více běžných analogových kamer. Jedná se vlastně o interface, který umožňuje připojit běžné analogové kamery k datové síti. Některé modely náleží z hlediska zařazení mezi IP-kamery i videosevery, neboť vedle kamery obsahují navíc další vstupy pro připojení běžných analogových kamer.

**Videosever** digitalizuje a komprimuje videosignál. Součástí je i rozhraní pro připojení k příslušné síti. Nejdůležitější je, že videosever poskytne IP-adresu, která jednotně identifikuje kameru z kteréhokoli místa v síti. Koncept IP-adres je stejný pro počítače na LAN nebo pro Internet obecně. Všechny funkce a parametry videoseveru jsou dálkově ovládány z prohlížečí strany nebo z kterékoli jiné ovládací jednotky na síti. Kromě videovstupu může mít videosever další rozhraní, která zajistí dvousměrný audiopřenos,

např. u dálkového příposlechu nebo hlášení. Plně duplexní datová rozhraní umožňují například vzdálené ovládání připojených periferních zařízení, například polohovacích hlavíc a motorzoomů. Další populární rozhraní, kterými je vybavena většina videoserverů, jsou ovládací vstupy a reléové výstupy. Zatímco ovládací vstupy umožňují připojení standardních prvků poplachových systémů, jako např. detektorů pohybu IR, magnetických či mechanických kontaktů dveří, usnadňuje reléový výstup dálkové zapínání a vypínání spotřebičů či ovládání technických zařízení vybavení budov (topení, osvětlení, klimatizace apod).

U instalací, kde je několik kamer seskupeno v těsné blízkosti, je někdy hospodárnější použít **multikanálový videoserver** spíše než zvláštní videoserver pro každou kameru. Takový systém například kombinuje čtyřvstupý dělič obrazu (quad) a multiplexer s videoserverem. Alternativně je rovněž možné zkombinovat videoserver se standardními komponenty CCTV, např. analogovými přepínači, děliči obrazu (quad), multiplexery, nebo videomaticemi

### 2.1.3 IP - dekodér

Je to zařízení, které slouží k připojení klasického analogového monitoru CCIR k zobrazení digitalizovaného videosignálu.

**IP-dekodér** konvertuje tok videodat zpět na analogový kompozitní videosignál ve standardu PAL. Aplikace, které používají tento takzvaný přístup „box – to – box“, jsou plně kompatibilní se stávajícími analogovými zařízeními CCTV. Počítačová síť se používá v těchto případech převážně jako náhražka nebo rozšíření analogové koaxiální sítě.

## 2.2 Digitální záznamová zařízení

V zásadě lze digitální záznamové zařízení podle technického řešení rozdělit do tří skupin:

### Čistě softwarové zařízení

Je určeno pro síťové aplikace, kde není k dispozici signál v analogové podobě. Umožňuje v decentralizovaném systému přístup k hardwarovým záznamovým zařízením (např. harddisk digitální videokamery či videoserver) či při filosofii centralizovaného záznamu přístup na server či diskové pole. Je to vlastně software pro práci s daty, uživatelsky přizpůsobený charakteru videodat. Do této skupiny vlastně můžeme zařadit i běžné webové prohlížeče, které umožňují přístup přes pevné či mobilní telefonní sítě k tzv. webovským kamerám.

### PC s interface

Tato zařízení jsou konstruována jako samostatná karta do PC (či externí box) s příslušným softwarem. Karta má podle vybavení příslušný počet analogových videovstupů pro přivedení signálu od kamer a vše ostatní se děje na úrovni ovládání PC. Obrazová kvalita i využití všech možností takového záznamového zařízení je dána jeho konstrukcí a závisí také na konfiguraci hardware použitého počítače.



### Čistě hardwarové záznamové zařízení (digitální videorekordér)

Tato zařízení jsou již konstruována se speciálním zaměřením pro CCTV. Toto zařízení v minulosti realizovalo průlom „digitálu“ do klasických analogových systémů CCTV. Již řadu let je analogový videorekordér pro aplikace v poplachových systémech prakticky mrtvý.

Digitální videorekordér využívá sice periférie i rozhraní, která jsou standardizována v oboru počítačů, ale není to klasické PC. Pokud se v něm vyskytuje základní deska PC jedná se nejčastěji o průmyslové provedení určené pro náročný provoz.

Charakteristické znaky těchto zařízení jsou uvedeny dále:

- Vstupy videosignálu jsou analogové,
- většina zařízení obsahuje multiplexer pro připojení více analogových kamer,
- v zařízení dochází k ke kompresi videosignálu a jeho zaznamenání na HD (popř. jiné médium DVD, DV),
- zařízení umožňují připojit prostřednictvím rozhraní (SCSI, IDE..) externí paměť pro rozšíření kapacity paměti popř. zálohovací médium (diskové pole, Jaz-Drive, CD-ROM, ZIP...),
- jsou vybaveny kontrolním analogovým videovýstupem,
- zařízení umožňují připojení k různým typům přenosové sítě JTS – internet, LAN/WAN/Ethernet, ISDN, GSM...).

Podle koncepce některá zařízení umožňují připojit PC klávesnici a/nebo myš. Pro potřebu systémové integrace jsou téměř všechny typy vybaveny poplachovými vstupy a výstupy a standardní řídicí sběrnici RS 232.

Podle typu a vybavení může zařízení podobně jako u multiplexerů umožňovat duplexní či triplexní režim provozu, což je důležité u systémů CCTV navržených pro trvalý provoz za přítomnosti obsluhy.

Nejvíce se zařízení liší v koncepci zpracování videosignálu – rozlišovací schopnosti, počtu stupňů vzorkování jasu a barvy, kompresní metodě, „záznamové rychlosti“ (což je historicky pojem z analogového záznamu, ve skutečnosti se jedná o rychlost uložení digitalizovaného snímku na paměťové médium, případně jeho vybavení z paměti a uvolnění pro zpracování dalšího snímku), která je závislá na hardwarovém řešení zařízení a hlavně na objemu dat, tedy na použitém kompresním algoritmu, nastaveném stupni komprese a u vícevstupých zařízení i na synchronizaci vstupních analogových signálů), velikosti vnitřního HD vybavení doplňkovými funkcemi.

### 3 Základy techniky počítačových sítí

IP kamery jsou koncipovány tak, aby je bylo možné bez problémů připojit do stávajících počítačových sítí. Proto se nejprve zaměříme na vysvětlení základních pojmů z této oblasti.

#### 3.1 Rozdělení

Pojmem počítačová síť se rozumí zejména spojení dvou a více počítačů tak, aby mohly navzájem sdílet své prostředky. Přitom je jedno zda se jedná o prostředky hardwarové nebo softwarové.

*Lokální síť* – LAN (Local Area Network). Skupina počítačů a dalších zařízení propojená komunikačním spojem na relativně malé geografické oblasti (do několika km), umožňující zařízením vzájemnou komunikaci v rámci určité skupiny (firma, úřad, banka, škola, nebo i domácnost).

*Rozlehlá síť* – WAN (Wide Area Network). Datová komunikační síť, která pokrývá geograficky rozlehlé území a využívá spojení veřejných poskytovatelů přenosových služeb. Typickým příkladem je internet.

*Bezdrátová síť* – WiFi (Wireless Fidelity). Primárně je určena k náhradě kabelového ethernetu bezdrátovým spojením v bezlicenčním pásmu, které je dostupné prakticky v celém civilizovaném světě.

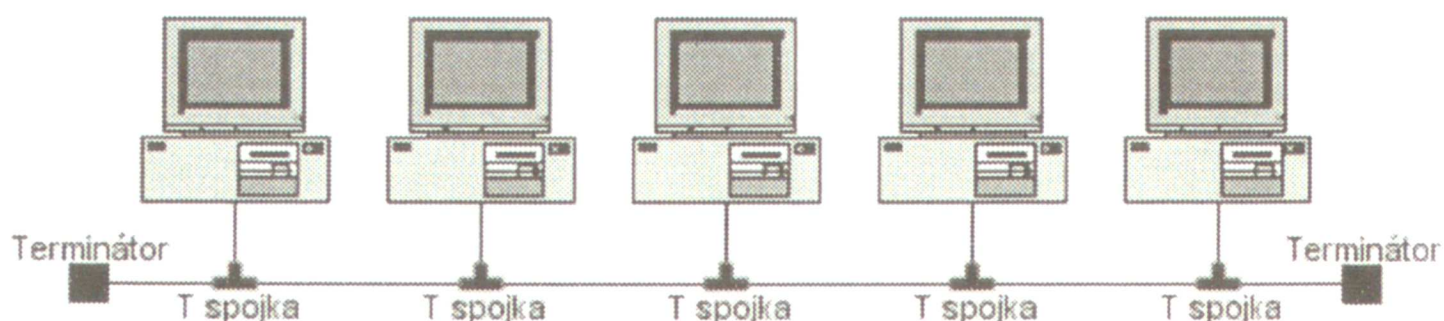
Poznámka: V odborné literatuře se můžeme setkat s dalšími typy sítí (MAN – Metropolitan síť, PAN – Osobní počítačové síť, apod.) nebo s jiným způsobem dělení.

#### 3.2 Architektura

*Client-server* – jednotliví klienti (PC) komunikují vždy s centrálním serverem či servery, prostřednictvím kterého komunikují i s jinými klienty (pokud je to potřeba). Server je samostatný počítač, který řídí předávání dat po síti a umožňuje připojeným stanicím přístup k datům a k perifériím zapojeným v síti. Serverů může být i více a mohou mít specifické významy, jako je např. databázový server, tiskový server atd. *Peer-to-peer* (doslova rovný s rovným) neboli P2P. Je označení architektury počítačových sítí, ve které spolu komunikují přímo jednotliví klienti. Nejjednodušším příkladem je propojení dvou PS nebo PC a IP kamery.

#### 3.3 Topologie

*sběrnice* – je také známa jako lineární sběrnice. Jde o nejjednodušší a dnes již méně používaný způsob zapojení počítačů do sítě. Skládá se z jediného kabelu nazývaného hlavní kabel (také páteř nebo segment), který v jedné řadě propojuje všechny počítače v síti.



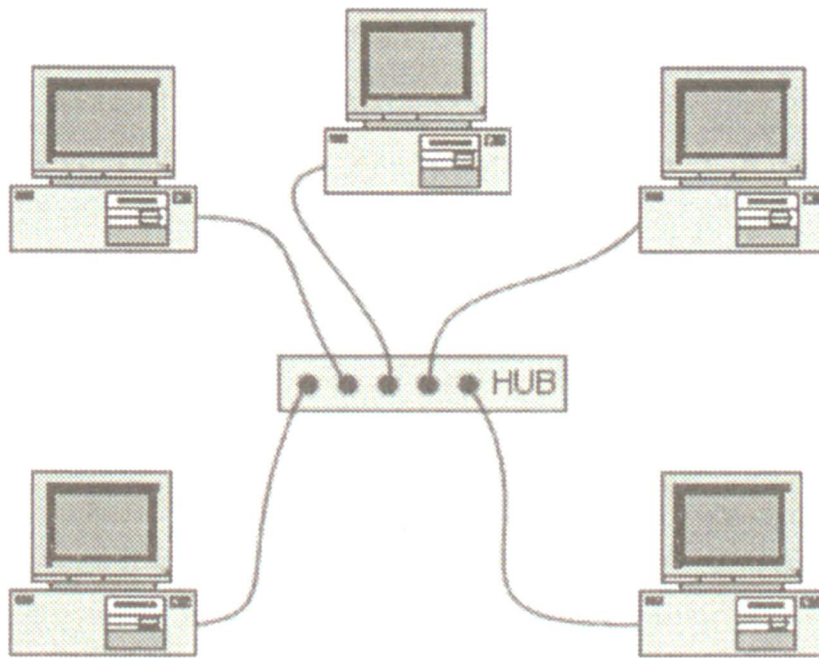
Obr. 6-2: Síť se sběrniceovou technologií.

K propojení se používá koaxiální kabel s impedancí  $50 \Omega$  a BNC konektory. Na konce vedení musí být připojeny zakončovací odpory (terminátory) s impedancí  $50 \Omega$ .



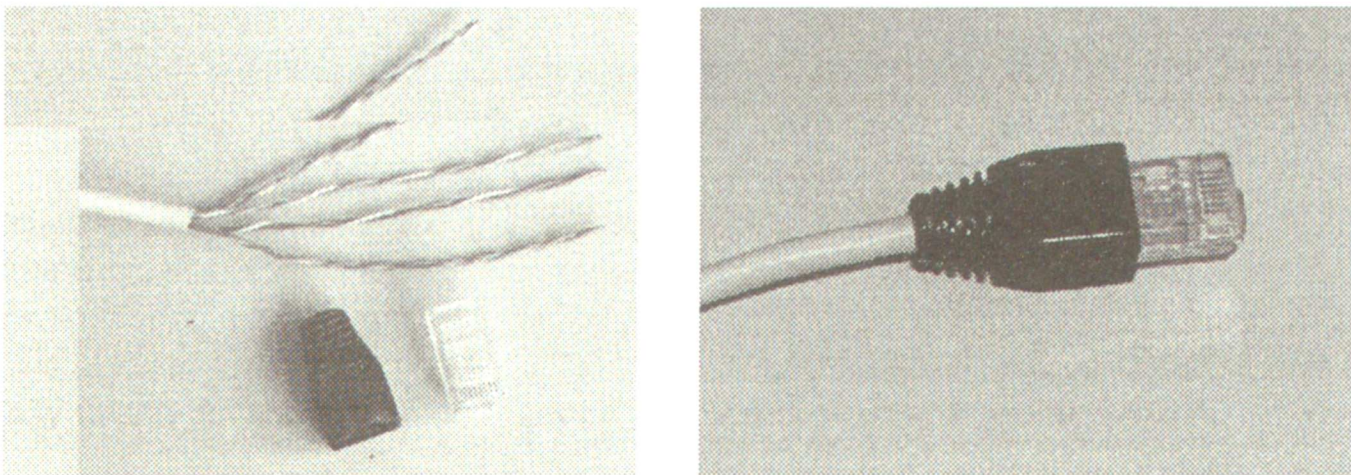
Obr. 6-3: Prvky koaxiální sítě.

*Hvězdicová topologie* – počítače jsou propojeny pomocí kabelových segmentů k centrálnímu prvku sítě, nazývanému přepínač (switch) nebo rozbočovač (HUB). Signály se přenáší z vysílacího počítače přes přepínače nebo rozbočovače do všech počítačů v síti.



Obr. 6-4: Síť s hvězdicovou topologií.

K propojení se používá UTP (Unshielded twisted pair), nestíněná kroucená dvojlinka zakončená konektory RJ 45.



Obr. 6-5: Detail zakončení párových vodičů v připojovacím konektoru RJ 45.

### 3.4 Jednotky a rychlost přenosu

Základní jednotkou informace používanou v číslicové technice je 1 bit (binary digit - dvojková číslice) [b]. Může mít pouze dvě hodnoty (log 0 a log 1). Často se také setkáváme s jednotkou byte (bajt) [B], 1 bajt = 8 bitů. Nabývá hodnot od 0 do 255. Pro vyjádření vyšších hodnot se používají předpony k (kilo), M (mega), G (giga), atd. V mezinárodní soustavě SI, která vychází z decimální soustavy značí předpona kilo značí násobek 1 000, atd. Číslicové systémy však vychází z binární soustavy a předpona kilo znamená násobek  $2^{10}$  tj. 1 024.

Tabulka 6-4: Používané předpony a značky

předpona	značka	decimální (SI)		binární	
		mocnina	převod	mocnina	převod
kilo	k	$10^3$	1 000	$2^{10}$	1 024
mega	M	$10^6$	1 000 00	$2^{20}$	1 048 576
giga	G	$10^9$	1 000 000 000	$2^{30}$	1 073 741 824
tera	T	$10^{12}$	1 000 000 000 000	$2^{40}$	1 099 511 627 776

Protože však řada výrobců nedodržovala výše uvedené zásady a 1 MB počítala jako 1 000 kB, začala se odlišovat značka „k“ jako 1 000 x, „K“ jako 1 024 x „M“ jako 1 000 000 x a „m“ jako 1 048 576 x. Roku 1998 se celosvětová standardizační organizace IEC (International Electrotechnical Commission) rozhodla udělat těmto problémům konec. Zavedla nové předpony, které jsou pro snadnější zapamatování odvozeny od stávajících ze soustavy SI:

Tabulka 6-5: Nově používané předpony a značky

předpona	značka	mocnina	převod
kibi	Ki	$2^{10}$	1 024
mebi	Mi	$2^{20}$	1 048 576
gibi	Gi	$2^{30}$	1 073 741 824
tebi	Ti	$2^{40}$	1 099 511 627 776

Nové jednotky vznikly odvozením z předpon používaných v SI systému jednotek. Druhá část předpony byla nahrazena slabikou bi (ze slova binary).

Přes výše uvedené snahy o sjednocení značení se tento systém příliš neosvědčil a výrobci pamětí nadále používají pro převod mezi kb a Mb násobek 1 024, zatímco výrobci pevných disků násobek 1 000.

Celou situaci dále komplikuje užívání jednotek bit a byte (bajt). Následující příklady uvádí některé vztahy:

$$1 \text{ kib} = 2^{10} \text{ bitů} = 1 024 \text{ bitů} = 128 \text{ bytů}, \text{ tedy } 1 \text{ kib} = 1 024 \text{ b} = 128 \text{ B}$$

$$1 \text{ kiB} = 2^{10} \text{ bytů} = 1024 \text{ bytů} = 8192 \text{ bitů}, \text{ tedy } 1 \text{ kiB} = 1 024 \text{ B} = 8 192 \text{ b}$$

Chceme-li vyjádřit rychlost jakou putují data v síti, sledujeme kolik bitů nebo bajtů projde za 1 sekundu. Používáme tedy jednotky bps (bit per sekund) a jejich násobky kbps, Mbps, Gbps nebo Bps a jejich násobky. Můžeme se také setkat s označením b/s, kb/s Mb/s, Gb/s nebo B/s, kB/s a MB/s.

Na závěr ještě jedna tabulka, která uvádí srovnání starých a nových názvů včetně jejich převodů:

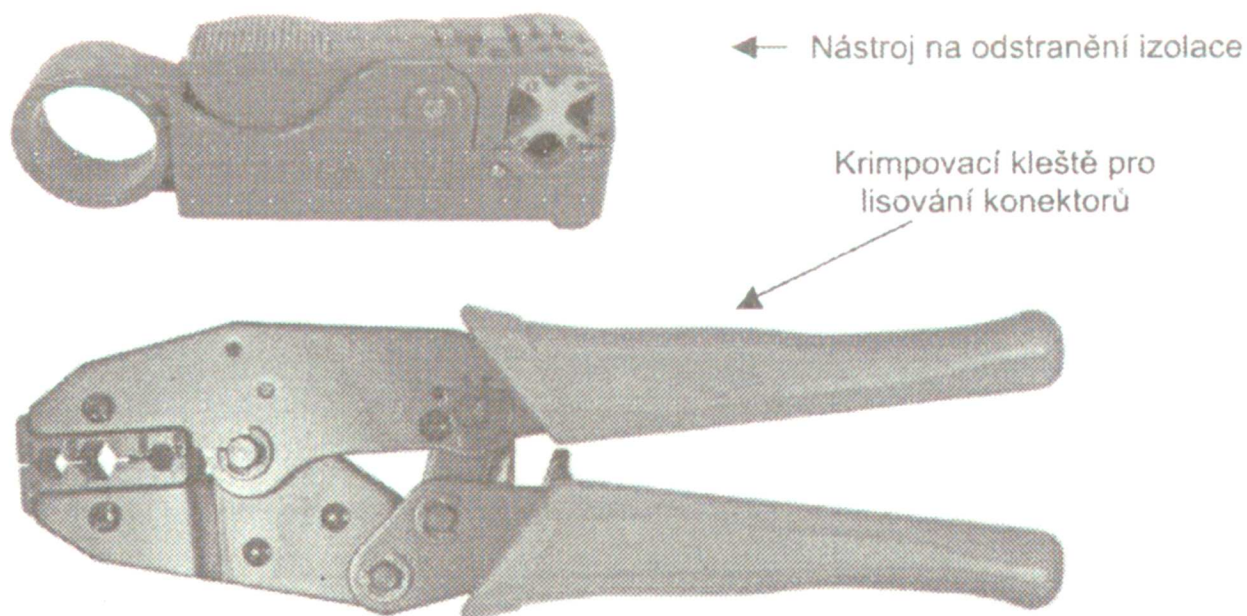
Tabulka 6-6: Převodní tabulka nových a starých jednotek

starý název	nový název	velikost
	1 byte (B)	8 bitů (b)
1 kilobyte (kB)	1 kibibyte (KiB)	1 024 bytů, 8 192 bitů
	1 kilobyte (kB)	1 000 bytů, 8 000 bitů
1 megabyte (MB)	1 mebibite (MiB)	1 048 576 bytů, 8 388 608 bitů
	1 megabyte (MB)	1 000 000 bytů, 8 000 000 bitů
1 gigabyte (GB)	1 gibibyte (GiB)	1 073 741 824 bytů, 8 589 934 592 bitů
	1 gigabyte (GB)	1 000 000 000 bytů, 8 000 000 000 bitů
1 kilobyte za sekundu (KB/s, KBps)	1 kibibyte za sekundu (KiB/s, KiBps)	8 192 bitů za sekundu (b/s, bps)
1 megabyte za sekundu (MB/s, MBps)	1 mebibyte za sekundu (MiB/s, MiBps)	8 388 608 bitů za sekundu (b/s, bps), 8 192 kilobitů (kibibytů) za sekundu (Kb/s, Kib/s, Kbps, Kibps)
1 gigabyte za sekundu (GB/s, GBps)	1 gibibyte za sekundu (GiB/s, GiBps)	8 589 934 592 bitů za sekundu (b/s, bps), 8 388 608 kilobytů (kibibytů) za sekundu (Kb/s, KiB/s), 8 192 megabitů (mebibitů) za sekundu (Mb/s, Mib/s, Mbps, Mibps)
1 kilobit za sekundu (Kb/s, Kbps)		128 bytů za sekundu (B/s, Bps)
1 megabit za sekundu (Mb/s, Mbps)		131 072 bytů za sekundu (B/s, Bps), 128 kilobytů (kibibytů) za sekundu (KB/s, KBps, KiB/s, KiBps)

### 3.5 Kabely, konektory a jejich zapojení

#### - koaxiální kabely a BNC konektory

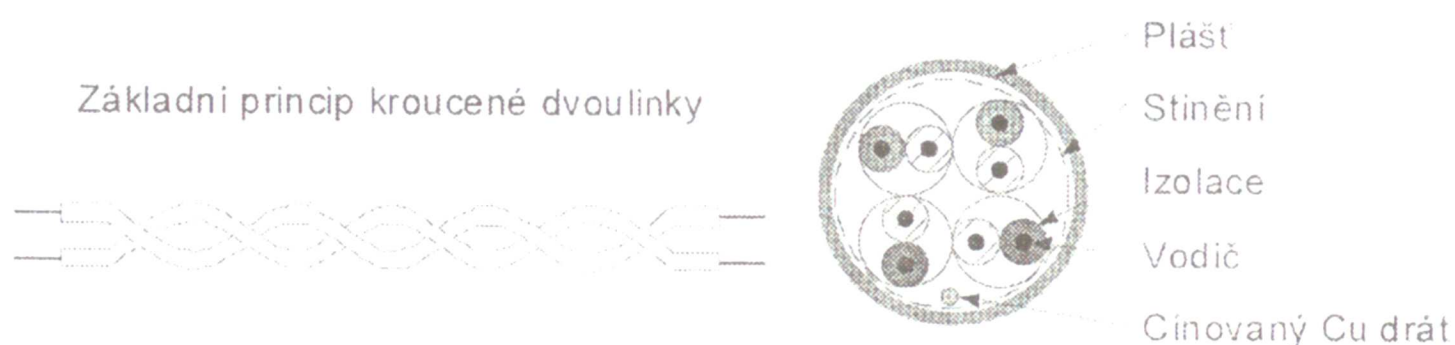
Jedná se o starší, dnes již málo využívané zapojení. Zpravidla se používá koaxiální kabel typu RG-58 s impedancí 50  $\Omega$ . Montáž konektoru se provádí pomocí speciálních nástrojů, tzv. stripovacích a krimpovacích kleští. Kabel se nejprve odizoluje a poté se nalisuje konektor.



Obr. 6-6: Nářadí užívané pro připojování kabelů v počítačových sítích.

### - kroucená dvoulinka a konektory RJ45

Kabel tvoří několik dvojic (párů) izolovaných vodičů v základní barvě (modrá, zelená, oranžová, hnědá) a bílé v kombinaci s příslušnou základní barvou. Kroucení neboli twistování zajišťuje vyšší odolnost proti interferencím s okolními vlivy. Při toku elektronů vodičem se okolo vodiče vytváří magnetické pole. Jsou-li dva vodiče, které jsou součástí stejného elektrického okruhu, dostatečně blízko od sebe, jejich magnetická pole působí proti sobě - tím se vzájemně potlačí. Dojde-li k porušení twistování např. nevhodným způsobem pokládání kabelu nebo jeho ukončení v panelu či zásuvce, mohou se přenosové vlastnosti spoje zhoršit. To se projeví snížením komunikační rychlosti.



Obr. 6-7: Princip krouceného párového vodiče.

Častěji se setkáte s nestíněnými kabely, označovanými jako UTP (Unshielded Twisted Pair). Stíněné kabely bývají označovány jako FTP (Foiled Twisted Pair) nebo ScTP (Screened Twisted Pair). Stínění má své opodstatnění zejména při vyšších přenosových rychlostech, kdy omezuje nejen možné rušení pronikající do kabelu, ale i vyzařování energie z kabelu do okolí. Aby mělo stínění význam, musí být na jednom konci (pouze na jednom) uzemněno!

V této souvislosti se také hovoří o strukturované kabeláži. Základní myšlenkou je vytvořit univerzální kabelový systém, umožňující vícenásobné využití (počítačové sítě, telefonní rozvody, IP kamery, apod.).

Pro běžné sítě s rychlostí 100 MBps se používají kabely kategorie 5, označované jako CAT 5.



Obr. 6-8: Barevné schéma zapojení páru.

Připojení jednotlivých drátů ke kontaktům konektoru je standardizováno. Aby to nebylo tak jednoduché, používá se používá se dvou standardů T568A a T568B, které se odlišují přehozením datových párů (zelený a oranžový). Zapojení jsou funkčně shodná, je však třeba, aby oba konce kabelu byly zapojeny stejně (nechcete-li zhotovit překřížený kabel). Pokud opravujete nebo rozšiřujete existující síť, dodržujte použitý standard. Častěji se používá standard T568B. Jednotlivé páry nejsou zapojeny postupně, ale stylem 1-2, 3-6, 4-5 a 7-8.

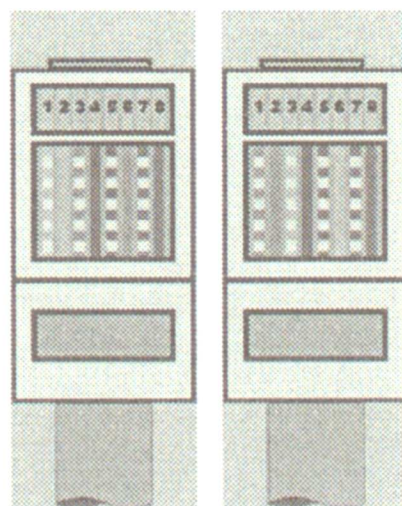
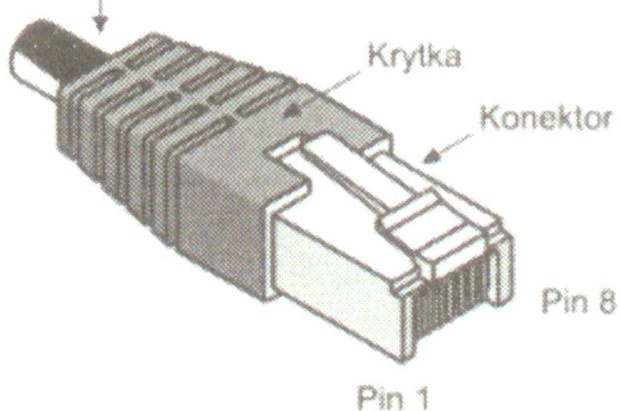
Tabulka 6-7: Možnosti zapojení konektorů

Zapojení podle standardu T568B									
Přímý kabel					Překřížený kabel				
konektor 1		kabel	konektor 2		konektor 1		kabel	konektor 2	
Pin	barva		barva	Pin	Pin	barva		barva	Pin
1	bílo - oranžová		bílo - oranžová	1	1	bílo - oranžová		bílo - zelená	1
2	oranžová		oranžová	2	2	oranžová		zelená	2
3	bílo - zelená		bílo - zelená	3	3	bílo - zelená		bílo - oranžová	3
4	modrá		modrá	4	4	modrá		modrá	4
5	bílo - modrá		bílo - modrá	5	5	bílo - modrá		bílo - modrá	5
6	zelená		zelená	6	6	zelená		oranžová	6
7	bílo - hnědá		bílo - hnědá	7	7	bílo - hnědá		bílo - hnědá	7
8	hnědá		hnědá	8	8	hnědá		hnědá	8

Poznámky:

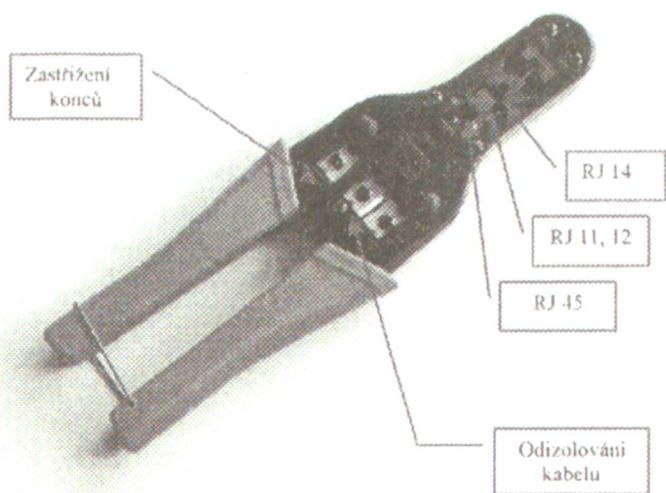
- Pořadí barev podle standardu T568A odpovídá překřížení v předchozí tabulce
- Přímý kabel se používá k propojení mezi počítačem a HUBem (nebo SWIT-CHem)
- Překřížený kabel se používá např. k propojení dvou počítačů v síti Peer-to-peer

Síťový kabel Category 5



Obr. 6-9: Detail provedení konektoru.

Ke spojení kabelu s konektorem se používá krimpování (lisování) pomocí speciálních kleští:



Obr. 6-10: Speciální krimpovací kleště na konektory typu RJ.

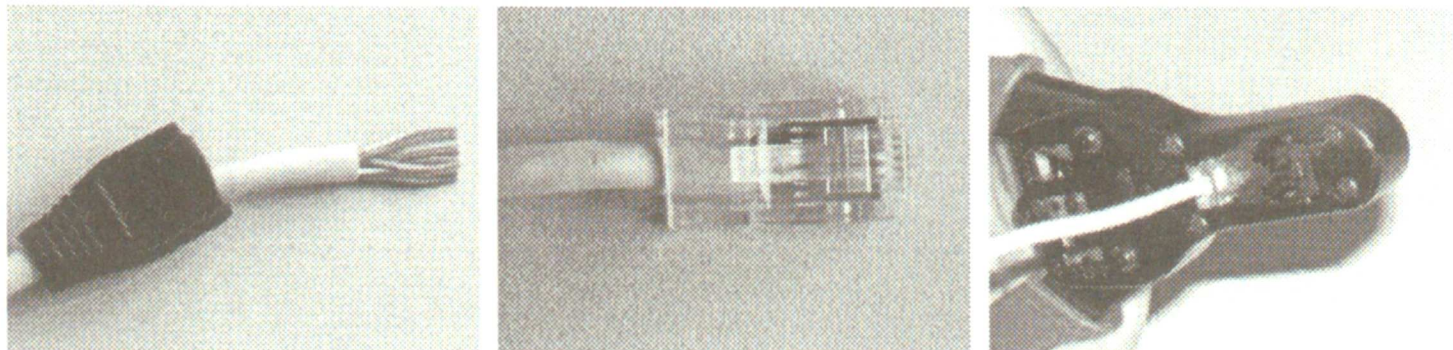
*Postup:*

- zastříhneme konec kabelu,
- nasuneme krytku,
- zasuneme po doraz do části pro odizolování a odstraníme vnější plášť kabelu,



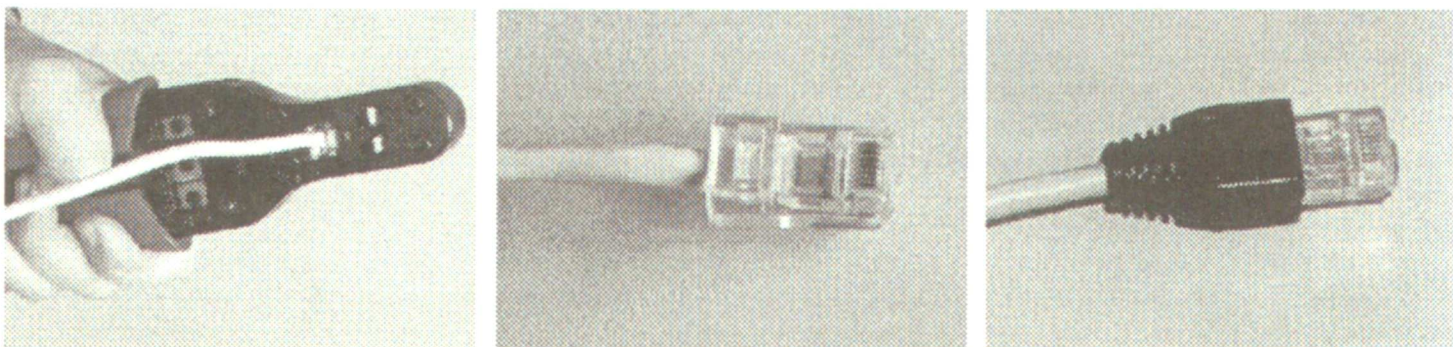
Obr. 6-11: Postup připojování konektoru I.

- jednotlivé páry rozpleteme a vyrovnáme ve správném pořadí,
- zastříhneme konce vodičů do roviny,
- upravený konec kabelu zasuneme do konektoru,
- zkontrolujeme, zdali jsou konce vodičů zasunuty až do konce,
- konektor s nasunutým kabelem vložíme do kleští a krimpujeme,



Obr. 6-12: Postup připojování konektoru II.

- zkontrolujeme výsledek,
- nasuneme krytku,
- hotový kabel proměříme.



Obr. 6-13: Postup připojování konektoru III.



Poznámky:

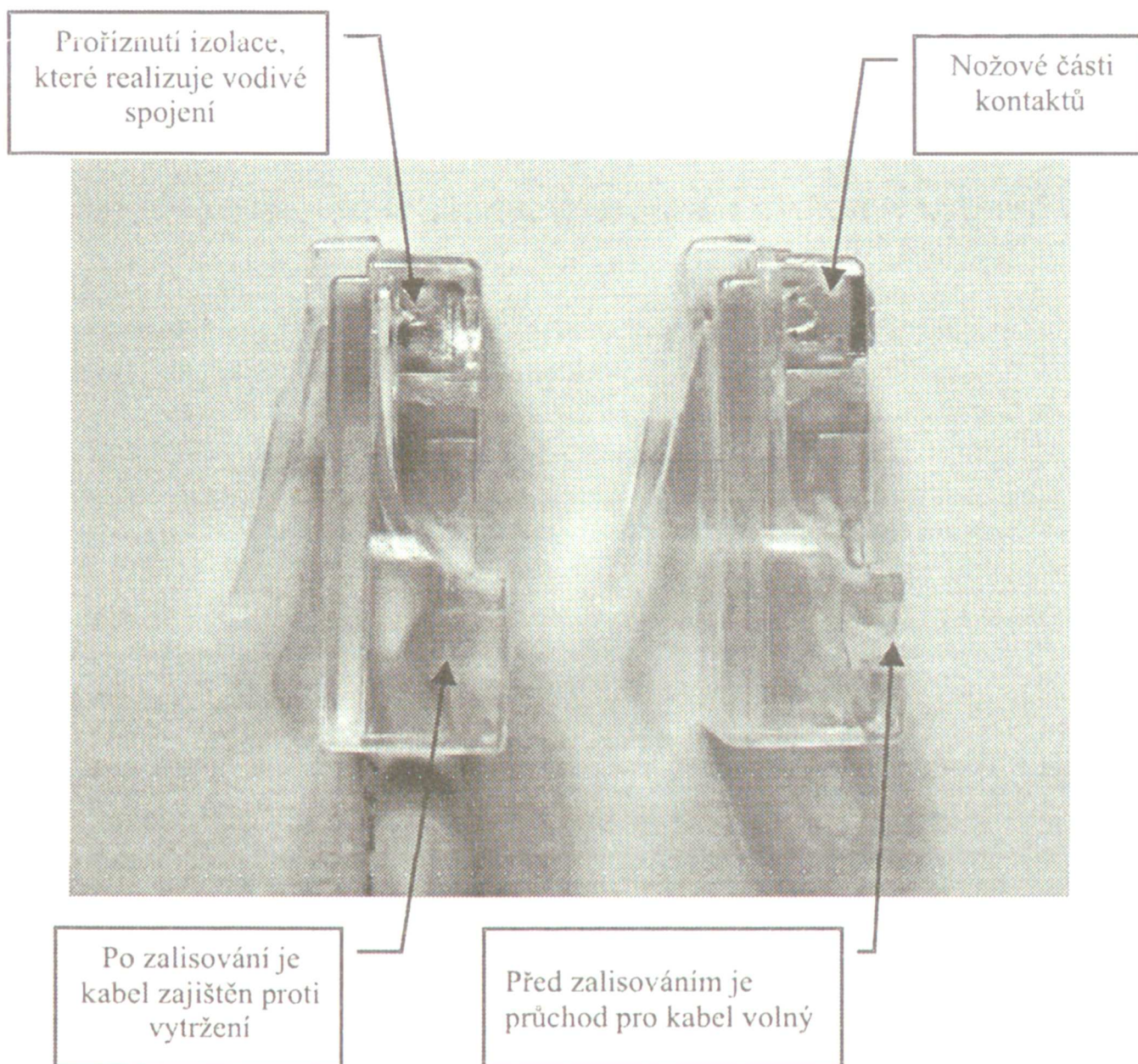
Při odstraňování pláště kabelu nesmíme kleště úplně zmačknout. Došlo by k poškození izolace vodičů nebo jejich ustřížení.

Jednotlivé vodiče se neodizolovávají!

Při práci je třeba postupovat opatrně a svědomitě. Špatně nakrimpovaný konektor nelze opravit. Je třeba jej odstříhnout a začít znovu.

Nejčastější chybou je, že konce vodičů nejsou zasunuty až do konce. Špatně provedený spoj může být příčinou zničení nebo poškození připojených zařízení (zvláště pokud jsou kabelem také napájeny – viz. PoE).

Můžeme také použít již hotových kabelů, které se vyrábí v délkách 2 až 10m jako přímé nebo překřížené. V nabídkách je nalezneme pod označením *UTP Patch kabel*.



Obr. 6-14: Detail zalisování vodičů v konektoru.

### 3.6 Hardware

Každý počítač připojený do sítě musí mít síťovou kartu. Na novějších základních deskách již bývá integrována. Je-li označena jako 10/100 znamená to, že podporuje rychlost 10 i 100 Mbps. Nejvyšší podporovanou rychlostí 1 GBps. Na dražších základních deskách bývají integrovány síťové karty označované také jako GLAN, které uvedenou rychlost podporují.

Maximální délka vedení závisí na kategorii (kategorie 5 pro kabely do 100 MHz s přenosovou rychlostí až 100 Mbps. Jedná se o nejčastěji používanou kabeláž realizovanou čtyřpárovými kabely UTP nebo FTP. Novější verze je označována jako CAT 5e) a třídě (vedení třídy D je specifikováno do 100 MHz). Pro síť 100 Mbps je maximální délka vedení 100 m. Vřazením aktivních prvků je možné tuto vzdálenost prodloužit.

MAC (Media Access Control) – ethernetová adresa je 48 bitové číslo přidělené výrobcem identifikující konkrétní síťovou(ethernetovou) kartu. Vyjadřuje se ve formě dvánáctimístného znakového řetězce nebo se také píše jako šest hexadecimálních dvojic čísel oddělených dvojtečkami nebo pomlčkou (např. 00-00-3C-35-DE-54, 00:00:A4:65:FA:E4).

Aby bylo možné jednotlivé komponenty propojit, zařazují se do sítě aktivní prvky – HUBy nebo SWITChe.

*Hub* (rozbočovač) funguje na principu tzv. opakovače, což znamená že veškerá data okamžitě rozesílá (opakuje) ostatním počítačům a veškerá přenosová kapacita, která je k dispozici, je všemi sdílena. Celková „propustnost“ HUBu zůstává konstantní a nemůže se přizpůsobovat zátěži.

*Switch* (přepínač) se snaží rozpoznat, kdy spolu komunikující nějaké dva uzly mezi sebou a snaží se nezatěžovat jejich vzájemným provozem i ostatní počítače. Lze si představit, že každé komunikující dvojici uzlů se snaží vytvořit samostatný kanál, o maximální možné propustnosti, odpovídající nominální přenosové rychlosti Ethernetu.

Hub si také můžeme představit jako zesilovač, který přijatý signál rozesílá do všech zásuvek, zatímco Switch data rozděljuje podle hlavičky PAKETU a posílá jen tomu počítači, pro který jsou určeny. V zásadě platí, že Switch je schopen nabídnout větší „výkon“ než hub.

*Router* (směrovač) mívá jeden vstup pro připojení k Internetu a jeden nebo více výstupů. Má svou vlastní IP adresu pro připojení zvnějška a druhou, podle které ho najdou počítače na vnitřní síti. Pro návštěvníky z Internetu se chová jako samostatný počítač. Některé Routery mají rovněž v sobě zabudován tzv. Printer server, což umožní přímé připojení tiskárny na vnitřní počítačovou síť.

*Bridge* (most). Síťový most spojuje dva segmenty téže sítě. Přístupové body fungují jako mosty mezi kabelovými a bezdrátovými segmenty sítě. Dalším druhem mostu je bezdrátový most, který se používá ve dvojicích pro spojení segmentů kabelové sítě.

*Access Point* AP (přístupový bod). AP řídí komunikaci mezi Wi-fi zařízeními, která jsou zapojena v infrastrukturním režimu. Přístupové body je možné použít pro poskytování různých služeb pro lokální síť a připojení k internetu. *Gateway* (brána) je zařízení, které funguje jako překladač mezi systémy, které nepoužívají stejné komunikační protokoly, formát dat, struktury, jazyky nebo architekturu. Brány mění uspořádání datových paketů a mění syntaxi tak, aby odpovídala cílovému systému.

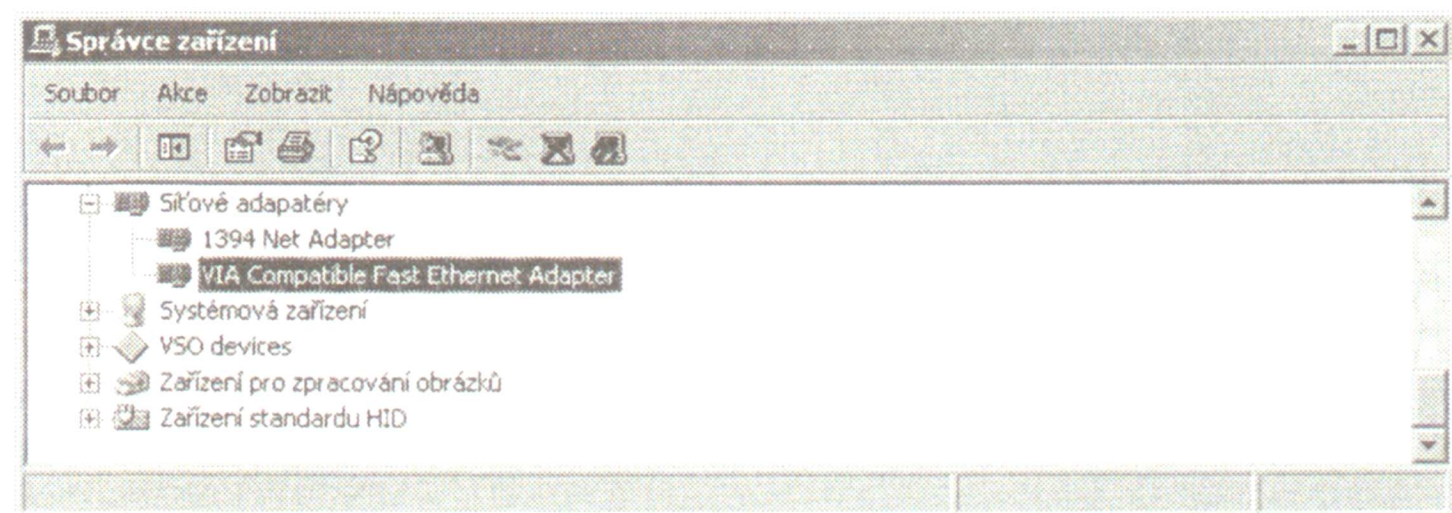
Pokud jsou sítě rozděleny na podsítě, brány jsou potřebné k propojení jedné podsítě z druhou nebo sítě a podsítě.

Všechna další zařízení, která chceme do sítě připojit (tiskárny, IP kamery, AP, IP telefony, apod.) musí být opatřena příslušným rozhraním a konektory RJ45. Většina z nich obsahuje mikroprocesor, který mimo jiné umožňuje konfiguraci prostřednictvím webového serveru. Po zadání IP adresy a případně i instalaci doplňkového modulu jsme zpravidla vyzváni k zadání jména a hesla. Poté se v internetovém prohlížeči zobrazí stránka umožňující konfiguraci a ovládání daného zařízení.

### 3.7 Software

Aby počítač mohl v síti komunikovat, je třeba jej nejprve nastavit. Postup se liší podle použitého operačního systému a další popis bude zaměřen na Windows XP, který patří k nejrozšířenějším. Starší verze (Windows 9x, NT, apod.) nejsou perspektivní a Microsoft postupně ukončuje jejich aktualizace a podporu. Při použití Linuxu můžeme narazit na problémy s kompatibilitou nebo ovladači.

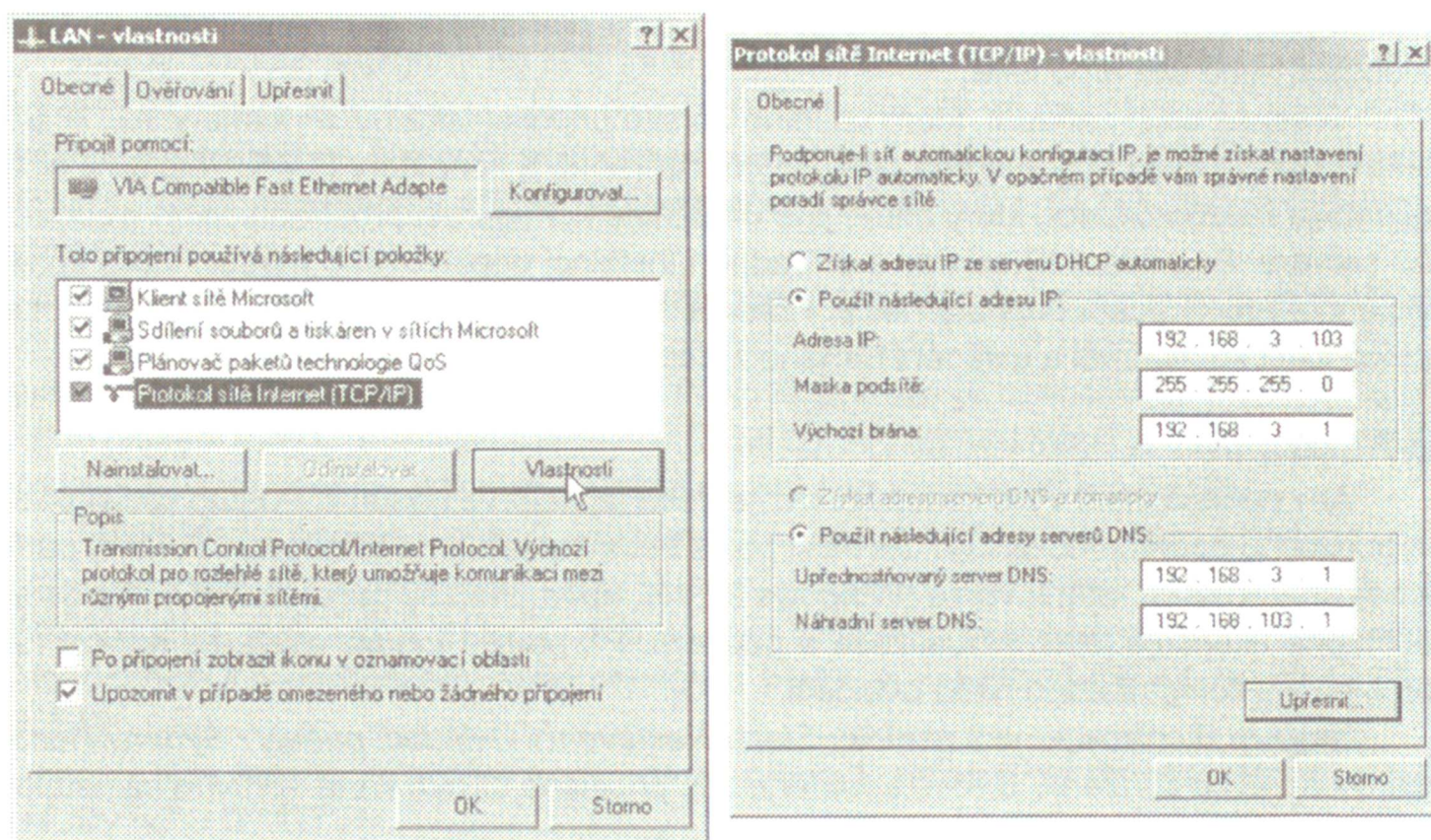
Nejprve zkontrolujeme z nabídky *Start / Nastavení / Ovládací panely / Systém / Hardware / Správce zařízení / Síťové adaptéry*, zda příslušná síťová karta správně nainstalována.



Obr. 6-15: Screenshot 1.

Pokud zařízení chybí nebo je zobrazen žlutý symbol s otazníkem či vykřičníkem, je třeba aktualizovat ovladač, provést novou instalaci s použitím odpovídajících ovladačů nebo odstranit konflikt v přidělených prostředcích. Ovladače nalezneme na CD (disketě) dodané se síťovou kartou nebo základní deskou.

Dále v nabídce *Start / Nastavení / Síťová připojení* zkontrolujeme, zda již bylo vytvořeno připojení k síti a volbou *Vlastnosti* (po stisku pravého tlačítka myši na existujícím připojení) zjistíme jeho konfiguraci.



Obr. 6-16: Screenshot II.

Nebyl-li dosud počítač pro připojení k síti nakonfigurován, přihlaste se jako správce a použijte *Průvodce instalací sítě*. Postupně budete dotazováni na některé důležité údaje, které je nutné správně vyplnit. Jedná se o konfiguraci, která není určena začátečníkům, proto je některých manuálech uvedeno doporučení kontaktovat správce sítě.

V dalším popisu se zaměříme na vysvětlení některých základních pojmů:

*Protokol TCP/IP* (Transmission Control Protocol/Internet Protocol - Protokol řízení přenosu/Protokol Internetu) je sada protokolů, které slouží k definování způsobu, jakým se data předávají síťovým zařízením. Aby se jednotlivá zařízení připojená k síti „domluvíla“ musí dodržovat určitá pravidla (protokoly). TCP/IP patří k nejpoužívanějším.

*Protokol Internetu (IP)* - když jsou informace odesílány do sítě, data jsou rozdělena na malé části (pakety). Pakety jsou odesílány nezávisle. IP směřuje datové pakety v síti a poskytuje nespojitě, nezaručené doručení datových paketů v celé síti. Každému uzlu sítě je přiřazena adresa IP.

*Protokol řízení přenosu (TCP)* se stará o rozdělení dat do paketů a jejich opětovné spojení po přijetí dat příjemcem. Poskytuje spojitě, spolehlivé a zaručené doručení do dalšího uzlu sítě. Jakmile data dorazí na místo určení TCP provede kontrolní součet každého paketu a ověří, zda nejsou data poškozena. Pokud došlo během přenosu k poškození dat v paketu, TCP paket odstraní a paket je posílán znovu.

*DHCP* (Dynamic Host Configuration Protocol - protokol dynamické konfigurace stanice). Umožňuje zařízení na síti získat IP adresu dynamicky při připojení k síti.

*IP adresa* je číslo ve tvaru xxx.xxx.xxx.xxx, kde xxx je dekadické číslo v rozsahu 0 až 255 (8 bitů, tj.  $2^8$ ), které identifikuje počítač v síti. Celkem je tedy k dispozici 32 bitů, tj.  $2^{32} = 4\,294\,967\,296$  kombinací.

Příklad vyjádření IP adresy v dekadickém a binárním tvaru:

151.88.19.103 = 10010111.0111000.00010011.01100111

IP adresa každého zařízení připojeného do sítě musí být jedinečná. To platí také v síti Internet, kde je potřeba jednoznačně přidělovat IP adresy, čísla autonomních systémů a jména domén. Žádná centrální autorita, která by řídila Internet, však neexistuje. Proto bylo založeno několik mezinárodních organizací, které mají za úkol bdít nad celosvětově jednoznačným přidělováním IP adres, čísel autonomních systémů a doménových jmen. Síťové adresy jsou distribuovány organizacím, které zas odpovídají za to, že všechna připojená zařízení nebo hostitelé v síti mají přidělena správná čísla.

V praxi se zpravidla setkáme se třemi základními principy:

- Pole „Získat adresu IP ze serveru DHCP automaticky“ zvolíme v tom případě, že náš provider (poskytovatel připojení) toto podporuje, či dokonce vyžaduje. V principu se jedná o to, že počítače v síti nemají pevnou IP adresu, toto číslo je při připojení propůjčeno na omezenou dobu. Volby „Adresa IP, Masky podsítě a Výchozí brána“ pak nevyplňujeme.
- Za příplatek můžeme od providera získat pevnou IP adresu. Znamená to, že získáme jedinečnou IP adresu a připojené zařízení je z internetu identifikovatelné. To je důležité například pokud chceme provozovat IP telefon. Podobně jako u běžného telefonu je nutné směřovat příchozí volání na konkrétní zařízení. Při konfiguraci vyplníme údaje, které nám stanoví provider.
- V rozsáhlejší lokálních sítích připojených k internetu (např. ve škole) se nejčastěji setkáme s tzv. privátními (soukromými) adresami. Adresami, které nemusí být získány prostřednictvím IP registries, tedy způsobem, který zajišťuje jejich unikátnost. Mohou to být adresy, které jsou již použity někde jinde v internetu. Privátní IP adresy si zřizovatel sítě může zvolit libovolně, aniž by se ohlížel na někoho jiného. Základní podmínkou správné funkce je vřazení takového mechanismu (např. proxy brány), který zabezpečí, že každý uživatel privátní sítě komunikuje pouze prostřednictvím brány a jeho IP adresa není z internetu viditelná. Samotná proxy brána přitom musí být „veřejná“, neboli vybavená unikátní IP adresou a „viditelná“ z obou stran.

Rozsah IP adres, které byly vyčleněny pro použití v roli privátních IP adres, je rozdělen do tzv. tříd A až C. Následující tabulka uvádí rozsah privátních adres a implicitní masky (bez podsítování).

Tabulka 6-8: Rozdělení IP adres

Třída	IP adresa		Implicitní maska podsítě
	od	do	
A	10.0.0.0	10.255.255.255	255.0.0.0
B	172.16.0.0	172.31.255.255	255.255.0.0
C	192.168.0.0	192.168.255.255	255.255.255.0

*Podsítě* - pokud je adresa IP přidělena organizaci, nepočítá se s tím, že na místě může být více než jedna síť. Správci místní sítě používají podsítě k rozdělení sítě do několika oddělených sítí. Rozdělení sítě do podsítí může zvýšit výkon a zlepšit používání omezeného množství adres v síti.

*Maska podsítě* je mechanismus používaný k rozdělení jediné sítě IP do několika různých sítí. Aby bylo možno použít adresu IP v podsíti, musí správce vzít hostitelskou část adresy a přiřadit ji číslům podsítě. Masky podsítě „maskuje“ tuto část hostitelské adresy IP spolu s celou síťovou částí adresy jedničkami a nechává ve zbývající části nuly, které jsou k dispozici pro adresování hostitelů.

*Výchozí brána* je IP adresou zařízení zprostředkujícího připojení k internetu

*Adresa DNS serveru* (Domain Name Server) zajišťuje překlad jmenných (pro člověka snadněji zapamatovatelných) adres počítačů - např. `www.google.com` na číselnou IP adresu (`66.249.85.104`). DNS-server je používán všemi aplikacemi, které pracují s doménovými jmény počítačů. Dotazy pro DNS-server sestavuje a posílá aplikace automaticky a přijímá odpovědi. Uživatelé se jeví, že se na počítače odvolává přes jejich doménová jména, ačkoli ve skutečnosti se pracuje s číselnými IP adresami. Snadno si to můžeme ověřit zapsáním adresy do prohlížeče v číselné formě. Napišeme-li například do prohlížeče adresu `66.249.85.104`, zobrazí se shodná stránka jako bychom napsali `www.google.com`.

### Stručné shrnutí:

Nejlepším řešením je kontaktovat správce vaší sítě, který vám sdělí všechny údaje potřebné pro konfiguraci připojení k síti.

Nezapomeňte, že IP adresa musí být v dané síti jedinečná!

Ostatní údaje bývají v celé síti vyplněny shodně (pokud není rozdělena do více podsítí).

### Kontrola správného nastavení:

Součástí operačního systému je velmi známý příkaz *ping*. Ten zapisujeme do příkazového řádku (*Start / Programy / Příslušenství / Příkazový řádek*). Zobrazí se černé okno do kterého zapišeme příkaz *ping* a IP adresu příslušného zařízení.

a) nejprve zkontrolujeme síťovou kartu. Zapišeme tedy *ping* a IP adresu našeho PC.

```
Microsoft Windows XP [Verze 5.1.2600]
<C> Copyright 1985-2001 Microsoft Corp.

C:\>ping 192.168.3.103
Příkaz PING na 192.168.3.103 s délkou 32 bajtů:
Odpověď od 192.168.3.103: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.3.103: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.3.103: bajty=32 čas < 1ms TTL=128
Odpověď od 192.168.3.103: bajty=32 čas < 1ms TTL=128

Statistika ping pro 192.168.3.103:
Pakety: Odeslané = 4, Přijaté = 4, Ztracené = 0 <ztráta 0%>
Přibližná doba do přijetí odezvy v milisekundách:
    Minimum = 0ms, Maximum = 0ms, Průměr = 0ms
C:\>
```

Pokud se v okně objeví hlášení „*Cílový hostitel není dostupný*“, je třeba zkontrolovat připojení kabelu. To, že je síťová karta správně připojena, poznáme také podle svitu LED diod umístěných poblíž konektoru RJ 45.

b) dále postupuje obdobným způsobem a kontrolujeme další IP adresy výchozí brány a DNS severů.

```
Microsoft Windows XP [Verze 5.1.2600]
<C> Copyright 1985-2001 Microsoft Corp.

C:\>ping 192.168.3.1
Příkaz PING na 192.168.3.1 s délkou 32 bajtů:
Odpověď od 192.168.3.1: bajty=32 čas < 3ms TTL=128
Odpověď od 192.168.3.1: bajty=32 čas < 3ms TTL=128
Odpověď od 192.168.3.1: bajty=32 čas < 3ms TTL=128
Odpověď od 192.168.3.1: bajty=32 čas < 2ms TTL=128

Statistika ping pro 192.168.3.1:
Pakety: Odeslané = 4, Přijaté = 4, Ztracené = 0 <ztráta 0%>
Přibližná doba do přijetí odezvy v milisekundách:
    Minimum = 2ms, Maximum = 3ms, Průměr = 2ms
C:\>
```

V kolonce čas = budou pravděpodobně vyšší hodnoty než v předchozím případě. Konkrétní hodnota je závislá na rychlosti vaší sítě. Setkáte-li se s hlášením „*Cílový hostitel není dostupný*“, zkontrolujte znovu správnost zapsání příslušné IP adresy.

Příkaz ping můžeme použít obecně ke zjišťování dostupnosti a rychlosti odezvy jak v lokální síti, tak i v internetu.

```
Microsoft Windows XP [Verze 5.1.2600]
<C> Copyright 1985-2001 Microsoft Corp.

C:\>ping www.google.com
Příkaz PING na www.google.com [66.249.85.104] s délkou 32
bajtů:
Odpověď od 66.249.85.104: bajty=32 čas < 28ms TTL=128
Odpověď od 66.249.85.104: bajty=32 čas < 31ms TTL=128
Odpověď od 66.249.85.104: bajty=32 čas < 39ms TTL=128
Odpověď od 66.249.85.104: bajty=32 čas < 31ms TTL=128

Statistika ping pro 66.249.85.104:
Pakety: Odeslané = 4, Přijaté = 4, Ztracené = 0 <ztráta 0%>
Přibližná doba do přijetí odezvy v milisekundách:
    Minimum = 28ms, Maximum = 39ms, Průměr = 32ms
C:\>
```

Povšimněte si, že za příkaz ping můžeme také zadat přeloženou IP adresu ve tvaru `www...` a v okně se objeví její číselná hodnota ve formátu `xxx.xxx.xxx.xxx`. K výpisu konfigurace sítě použijeme příkaz `ipconfig`:

```
Microsoft Windows XP [Verze 5.1.2600]
<C> Copyright 1985-2001 Microsoft Corp.

C:\>ipconfig

Adaptér sítě Ethernet LAN:

    Přípona DNS podle připojení      :
    IP adresa                        :192.168.3.103
    Maska podsítě                    :255.255.255.0
    Výchozí brána                    :192.168.3.1

C:\>
```

Pro kompletní výpis konfigurace sítě včetně MAC adresy PC můžete použít příkaz `ipconfig /all`:

```
Microsoft Windows XP [Verze 5.1.2600]
<C> Copyright 1985-2001 Microsoft Corp.

C:\>ipconfig /all

Konfigurace protokolu IP systému Windows

    Název hostitele                  :stanice_1
    Primární přípona DNS              :
    Typ uzlu                          :neznámý
    Povoleno směrování IP            :ne
    WINS Proxy povoleno              :ne

Adaptér sítě Ethernet LAN:

    Přípona DNS podle připojení      :
    Popis                             :NVIDA Norce Networking
                                     Controller
    Fyzická adresa                   :00-13-D4-05-7E-58
    Protokol DHCP povolen            :ne
    IP adresa                         :192.168.3.103
    Maska podsítě                    :255.255.255.0
    Výchozí brána                    :192.168.3.1
    Servery DNS                       :192.168.3.1
                                     192.168.3.103

C:\>
```

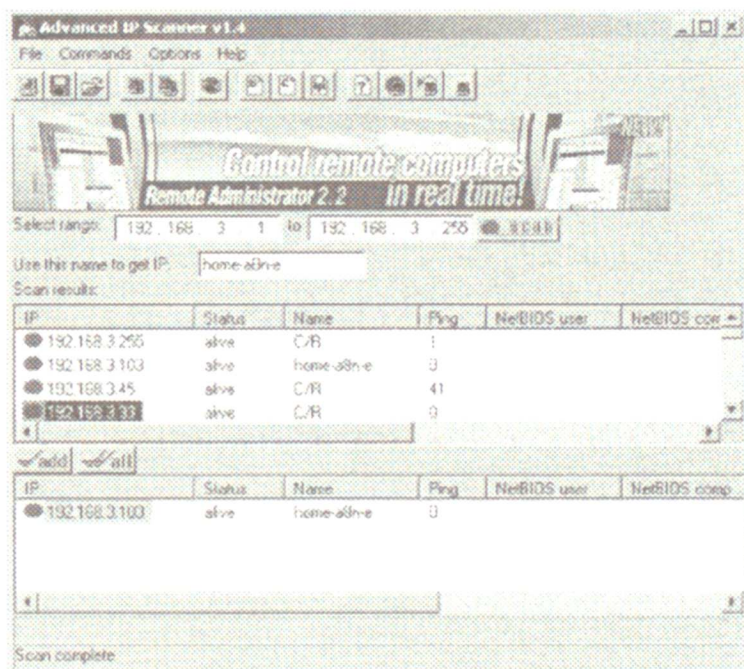
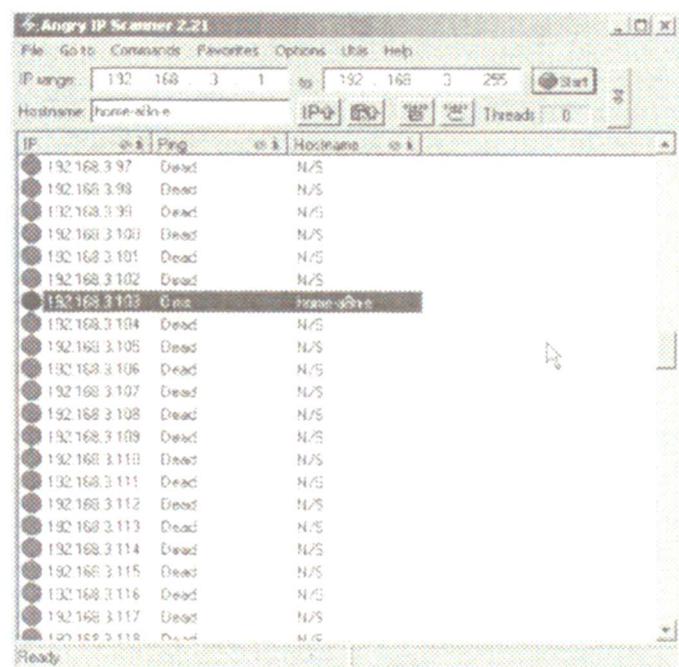


Příkaz ping je vhodný pro zjištění odezvy jednoho zařízení, chceme-li rychle zjistit, stav více zařízení, je lepší použít nějakého specializovaného programu. Z oblasti freewaru můžeme zkusit například:

Check IP Addr <http://www.infojet.cz/download.php?sekce=5> (spustitelný)

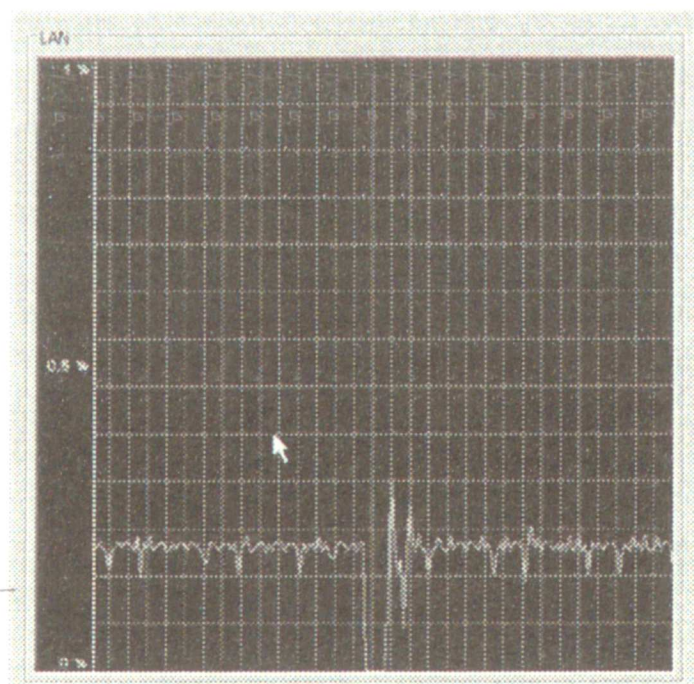
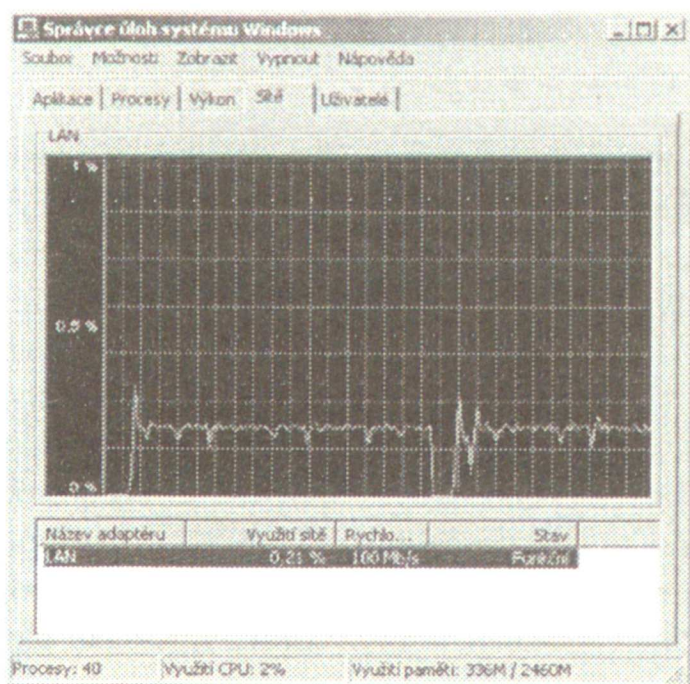
Angry IP Scanner <http://www.angryziber.com/ipscan/> (spustitelný)

Advanced IP scanner <http://www.radmin.com> (nutná instalace).



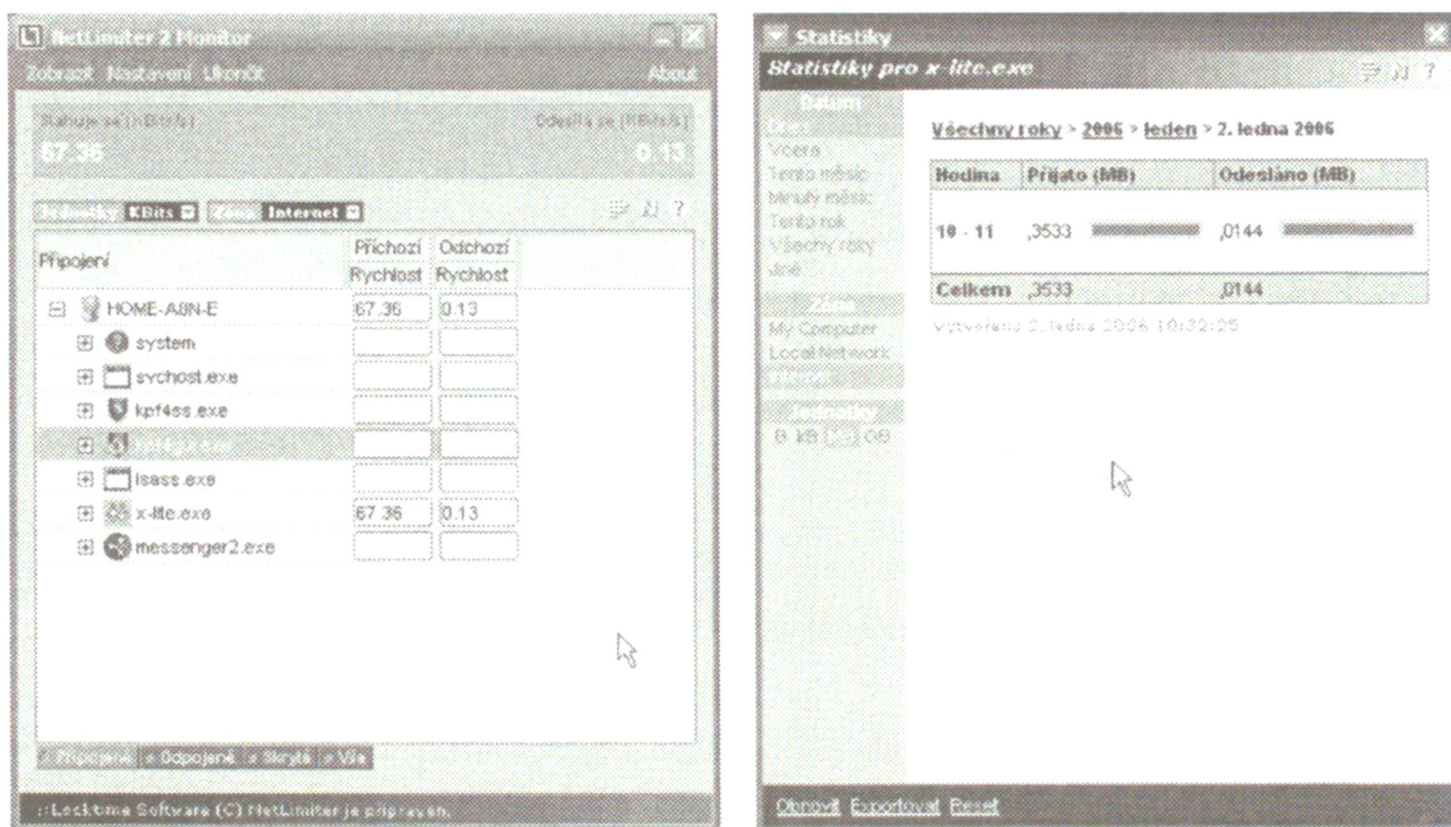
Obr. 6-17: Ukázka programů Angry IP Scanner a Advanced IP scanner.

Nejen při práci s IP kamerami potřebujeme zjistit, omezit nebo limitovat datový tok v síti. Základní informaci můžeme získat stiskem kláves *Ctrl + Alt + Del*. Tím se spustí *Správce úloh systému Windows*. Vybereme-li záložku *Sítě*, objeví se informace o momentálním datovém toku síťového adaptéru.



Obr. 6-18: Monitoring datového toku.

Chceme-li získat podrobnější informace o tom, které aplikace a jakou rychlostí komunikují můžeme použít freeware *NetLimiter Monitor*, který nalezneme na stránce <http://www.netlimiter.com>. Na stejném místě je ke stažení i shareware *NetLimiter*, který navíc umožní přesné určení a nastavení maximálních povolených rychlostí pro každou spuštěnou úlohu v systému.



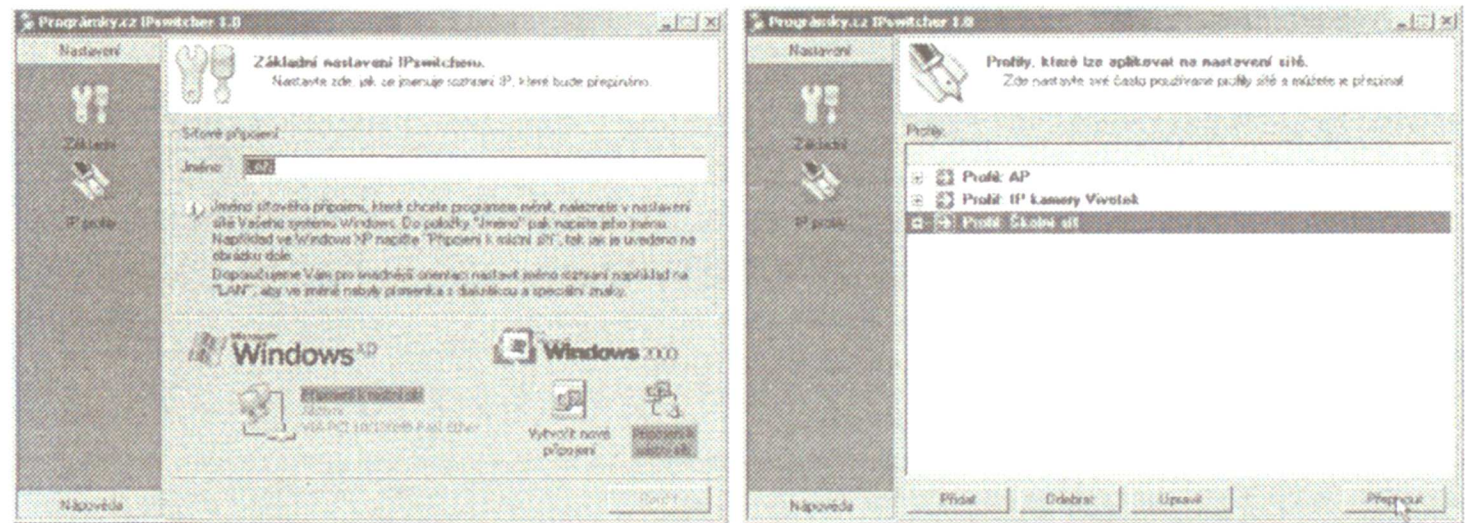
Obr. 6-19: Screenshot IV.

Možnost sledovat datový tok je v případě IP kamer velmi důležitá, protože jeho velikost je závislá na použitém rozlišení, počtu snímků za sekundu a použité kompresi. Při nesprávném nastavení může snadno dojít k zahlcení sítě a tím i omezení všech uživatelů. Datový tok je třeba omezovat také v případě, že signál z kamer bude distribuován prostřednictvím internetu.


Abychom mohli provést základní nastavení IP kamery, videoserveru, AP, nebo i jiných IP zařízení (VoIP telefon, router, apod.) musíme je připojit k PC buď pomocí překříženého kabelu, nebo zapojit nekříženým kabelem do stávající sítě. Výchozí nastavení (do kterého se zařízení také vrací po resetu) IP adresy a masky podsítě bývají různá. Operační systém Windows neumožňuje zapamatovat si různá nastavení a přepínat se mezi nimi. Můžeme použít pouze jedno tzv. alternativní nastavení. Další možností je využití programu dodaného se softwarem. V případě kamer firmy Vivotek je to WebCam Installer nebo Installation Wizard. Zpravidla se však jedná o jednoúčelový software použitelný pouze pro určitá zařízení. Univerzálním řešením je použití specializovaného programu, který umožní přepínání různých předem definovaných nastavení sítě. K tomu lze použít například IP-switcher (<http://www.ip-switcher.com>). Od verze 2.0 je distribuován jako demoverze a cena plné verze je 600 Kč za licenci. Starší, méně propracovaná, ale plně funkční verze 1.0 je freeware.

Ukázka práce s programem:

Nejprve přejmenujte *Připojení k místní síti* tak, aby neobsahovalo znaky s českou diakritikou například LAN. To provedete z nabídky *Start/Nastavení/Síťová připojení* po stisku pravého tlačítka myši na *Připojení k místní síti*. Spustíme program *IPswitcher* (verze 1.0 se neinstaluje), v nabídce *Nastavení* zvolíme *Základní* a vyplníme *Jméno síťového připojení*. Pak přejdeme do nabídky *IP profily* a tlačítkem *Přidat* otevřeme nové okno. Nejprve vyplníme vhodné jméno a pak postupně IP adresu a adresy DNS serverů.



Obr. 6-20: Screenshot V.

Postupně vytvoříme další profily a okno programu minimalizujeme. V systémové liště (tray) přibude ikona , která umožňuje snadno přepínat mezi přednastavenými profily. Během přepínání se objeví okno příkazové řádky, které dokončení skriptu samo zmizí. Program je dobře použitelný také v tom případě, že potřebujeme přenosný počítač připojovat k různým sítím.

### 3.8 Dálkové napájení

Aby nebylo nutné každé IP zařízení napájet (případně i zálohovat) samostatně, byl vypracován standard označovaný jako Power over Ethernet (PoE), který definuje způsob napájení.

Situace poněkud složitější jednak z důvodu jejich různorodého použití a tím i různých požadavků na velikost napájecích napětí a proudů, ale také z důvodu malého průřezu vodičů. Přesto je tato možnost velmi lákavá vzhledem k tomu, že pro přenos dat je většinou využíváno jen dvou párů a zbývající dva nejsou použity (kromě 1000Mbitového ethernetu). Zapojení je rozděleno do dvou částí. Napájené zařízení označuje jako Powered Device (PD), zatímco zdroj energie je Power Sourcing Equipment (PSE). Zdrojem přitom může být koncové zařízení (přepínač nebo rozbočovač) nebo vložené zařízení označované také jako injector. Koncové zařízení pak buď musí vyhovovat podmínkám nově schváleného dodatku normy IEEE802.3af nebo před něj musí být zařazeno zařízení nazývané splitter, které oddělí datový signál od napájecího napětí a upraví jeho velikost. Definována byla také velikost napájecího napětí na 48 V (44 – 57 V) DC a maximální proud na 550 mA. Výkon je odstupňován v 5 třídách:

Tabulka 6-9: Normalizované třídy příkonu

Třída	Identifikační proud	Maximální příkon PD	Maximální výkon PSE	Popis
0	0 – 4 mA	12,95 W	15,4 W	Neznámý příkon, PD se neidentifikoval
1	9 – 12 mA	3,84 W	4 W	Nízký příkon PD
2	17 – 20 mA	6,49 W	7 W	Střední příkon PD
3	26 – 30 mA	12,95 W	15,4 W	Vysoký nebo plný příkon PD
4	36 – 44 mA	12,95 W	15,4 W	Vyhrazeno pro budoucí použití

#### Poznámky:

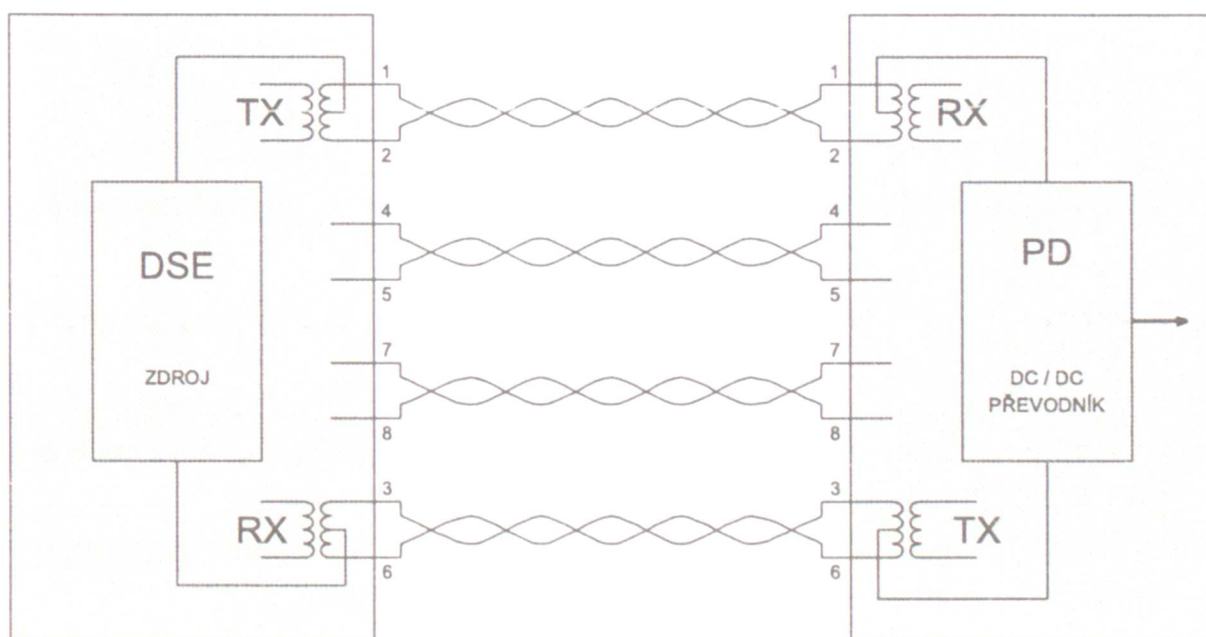
- Napájecí zdroj PSE nejprve pustí do obvodu stejnosměrné napětí v rozmezí 2,8 až 10 V. Je-li na straně spotřebiče detekován terminační (zatěžovací) rezistor v rozmezí 24,1 – 26 k $\Omega$ , je zařízení považováno za odpovídající IEEE802.3af a začíná druhá fáze identifikace napájeného zařízení spočívající v detekci napájecí třídy.
- Třída 0 je výchozí a je nastavena v případě, kdy je detekováno zařízení odpovídající standardu PoE, avšak není známa jeho třída, respektive spotřebič tuto informaci nepodává.
- Třídy 1 až 3 definují konkrétní povolené mezní příkony.
- Třída 4 odpovídá mezním výkonem třídě 3 nebo 0 a je ve specifikaci uváděna jen jako rezerva do budoucnosti.
- Identifikace výkonové třídy spotřebiče probíhá měřením identifikačního proudu tečkou ze zdroje při napětí 15,5 – 20 V.
- Je-li určena výkonová třída spotřebiče, zvýší se napájecí napětí na hodnotu 30 – 44 V označovanou jako UVLO (Under Voltage Lock Out). Ta je signálem pro zdroj v napájeném zařízení, aby uvolnil výstup napájecího napětí.
- Následuje režim aktivace, který může trvat až 50 ms. Tato doba je určena pro nabíjení překlenovacího kondenzátoru. Současně je omezen proudový odběr tak

aby tento stav nebyl vyhodnocen jako zkrat po kterém by bylo napájecí napětí odpojeno.

- Po úspěšném ukončení aktivační fáze poskytně PSE plné napájecí napětí, a které je signálem pro PD k zapnutí (aktivaci) spotřebiče.
- PD by neměl povolit zapnutí spotřebiče, pokud je napájecí napětí nižší než 36 V na PD, resp. 44 V z PSE.

### Varianta A

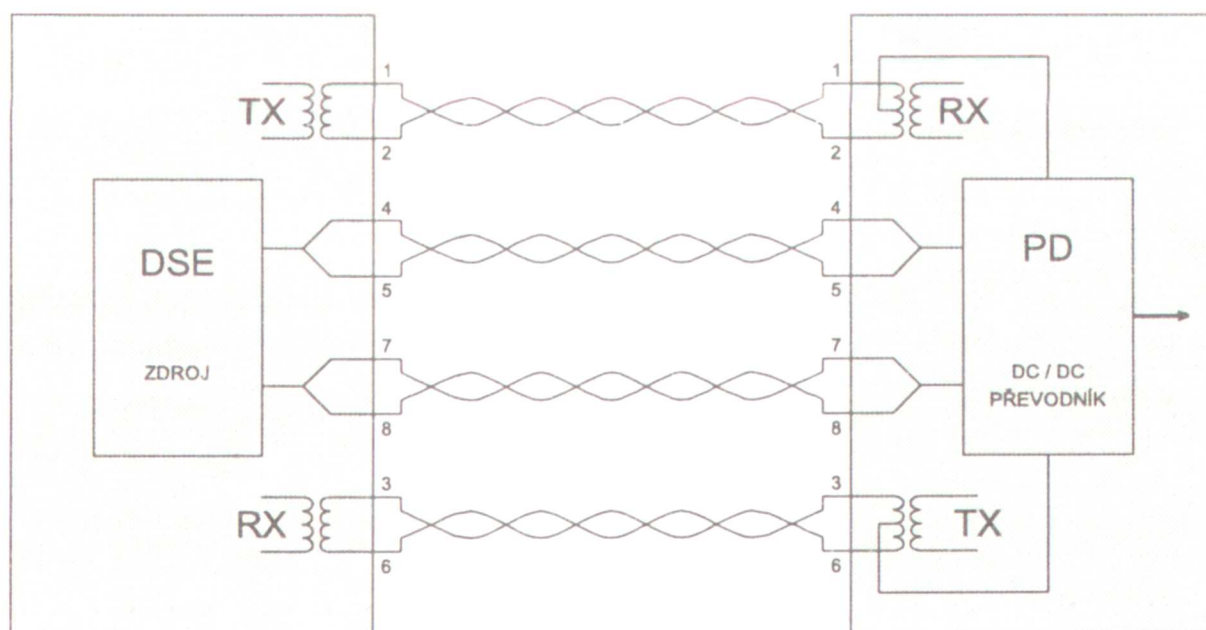
Napájení po datových signálech z aktivních prvků – jsou využívány dva páry vodičů a napájení je připojeno na středy vinutí oddělovacích transformátorů.



Obr. 6-21: Dálkové napájení - varianta A.

### Varianta B

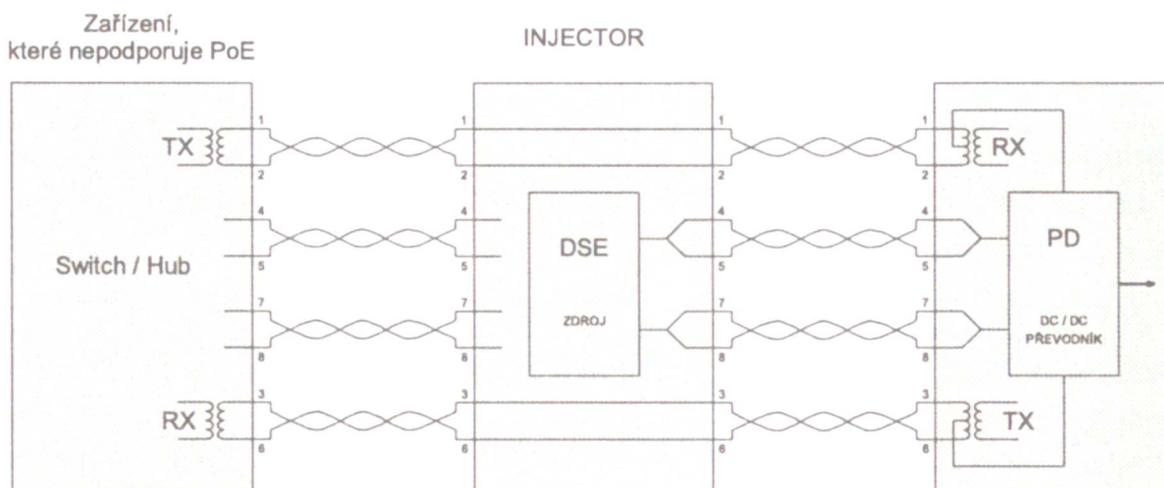
Napájení po volných vodičích z aktivních prvků – kladné i záporné napětí je přenášeno po dvou nevyužívaných párech vodičů, kde jsou vodiče páru vzájemně spojeny v obou koncových zařízeních. Toto zapojení nelze využít v gigabitových sítích využívajících všech 4 párů pro datový přenos.



Obr. 6-22: Dálkové napájení - varianta B.

### Varianta C

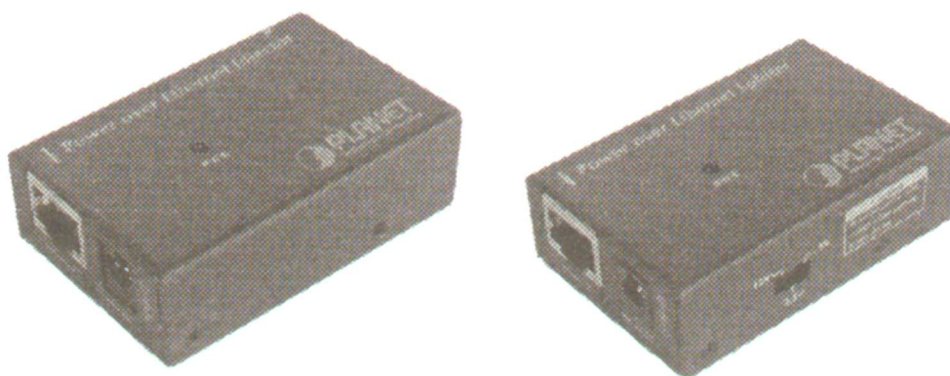
Napájení z vloženého zařízení (jednoportový injektor) – napáječ je vložen do přenosové cesty. Aktivní prvek, který je spojen s napáječem. Doplní napájecí napětí a znovu vyvede všechny vodiče na výstupní konektor.



Obr. 6-23: Dálkové napájení - varianta C.

Napájené zařízení (PD) má na vstupu zapojen můstkový usměrňovač, který zajišťuje správnou polaritu i v případě použití překříženého kabelu. Za usměrňovačem je zapojen rezistor hodnoty 25 kΩ, pro správnou identifikaci zařízení.

V nabídce prodejců se již běžně vyskytují sady injectorů a splitterů s různými výstupními napětími určené pro napájení Wi-fi zařízení nebo IP kamer.



Obr. 6-24: Příklady napájecích prvků.

### Doporučení:

Vyhňte se levným zařízením, která neodpovídají výše uvedenému standardu. Používejte jen taková, která jsou výrobcem koncového zařízení doporučena a odpovídají výkonem i napětím.

### 3.9 Bezdrátové systémy Wi-fi

Bezdrátové sítě dle normy 802.11a/b/g označované zkratkou Wi-Fi (Wireless Fidelity) jsou další možností vytvoření počítačových sítí. Původně byly tyto systémy navrhovány jako náhrada „drátových“ sítí v případech, kdy by instalace kabelů nabyla vhodná nebo ekonomická (podobně jako u bezdrátových EZS). Postupně se rozšířily také pro venkovní propojení na větší vzdálenosti. Jedním z důvodů je nedostupnost nebo stále poměrně vysoké náklady za jiný druh připojení k internetu.

Pro fyzickou přenosovou vrstvu Wi-Fi sítí se nejčastěji používá elektromagnetické rádiové vlnění ve frekvencích 2,4 GHz a 5,4 GHz. Pro nosnou frekvenci 2,4 GHz je maximální teoretická užitečná rychlost přenosu 1,2 GHz (1,2 Gbps). V praxi samozřejmě nelze této rychlosti dosáhnout a spíše se uplatňují užitečné rychlosti výrazně nižší (viz. dále). Vyšší nosná frekvence znamená i vyšší přenosové rychlosti. Také je třeba vzít v úvahu specifické vlastnosti šíření elektromagnetického vlnění na uvedených frekvencích. Pro 2,4 GHz je vlnová délka cca 12,5 cm, vlnění je z 95% pohlcováno vodou a organickými látkami (např. listnaté stromy) a odrazí od jakékoliv překážky větší než délka vlny. Při frekvenci 5,4 GHz je délka vlny cca 6 cm, vlnění není pohlcováno vodou v takové míře jako u 2,4 GHz. V obou případech se šíří podobně jako světlo a jakákoliv překážka mezi vysílačem a přijímačem zhoršuje nebo znemožňuje jejich komunikaci.

#### Pásmo 2,4 GHz

Je limitováno rozsahem 2,4 až 2,4835 GHz, popsáno standardem IEEE 802.11b a rozděleno do 14 kanálů po 22 MHz, které se však vzájemně překrývají (pouze tři z nich se nepřekrývají vůbec). Jedná se o pásmo podléhající tzv. generální licenci umožňující bezplatné (avšak regulované) použití 802.11b zařízení. Maximální rychlost je 11 Mbps, ale užitečná rychlost je nižší, protože 30 až 40% teoretické kapacity tvoří rezie. Dynamicky se mění podle momentálního zarušení na nižší nebo naopak na vyšší (11 Mbps, 5,5 Mbps, 2 Mbps až 1 Mbps). Reálná maximální uživatelská rychlost se udává kolem 6 Mbps.

Norma IEEE 802.11g je zpětně kompatibilní, zvyšuje rychlost oproti 802.11b na 54 Mbps za cenu rozšíření přenosového pásma a tím i zvýšení nebezpečí rušení.

#### Pásmo 5 GHz

Od 1.9.2005 bylo schváleno využívání kmitočtového pásma 5,470 až 5,725 GHz v rámci všeobecného oprávnění VO-R/12/08.2005-34. To řeší odlehčení dnes již velmi přetíženému pásmu 2,4 GHz. Podmínkou je použití zařízení schválených pro tento provoz v ČR.

#### Celkový přehled pásem

**802.11a** pásmo 5,1-5,8GHz ve 3 segmentech, přenosová rychlost až 54Mb/s (72Mb/s, turbo mód 108Mb/s), modulační systém OFDM, dosud není povoleno v EU!

**802.11b** pásmo 2,4GHz, přenosová rychlost až 11Mb/s, DSSS (Direct Sequence Spread Spectrum)

**802.11b+** pásmo 2,4GHz, existují dvě navzájem nekompatibilní řešení od Intersilu a Texas Instruments, přenosová rychlost 22Mb/s a 44Mb/s (na menších rychlostech kompatibilní s 802.11b)

**802.11g** (802.11b+) pásmo 2,4GHz, přenosová rychlost 54Mb/s až 108Mb/s (na menších rychlostech kompatibilní s 802.11b), modulační systém OFDM

**802.11h** pásmo 5,1-5,8GHz ve 3 segmentech, přenosová rychlost až 54Mb/s (72Mb/s, turbo mód 108Mb/s), modulační systém OFDM, tzv. HyperLan určen pro EU, zařízení podporuje dynamickou regulaci výkonu a změnu kmitočtu

### 3.9.1 Hardware

**Přístupový bod** Access Point (AP) obsahuje přijímač a vysílač v pásmu Wi-fi s anténním výstupem vyvedeným na konektor, řídící počítač, minimálně jeden výstupní síťový konektor RJ45 a napájecí konektor. Většina prodávaných zařízení umožňuje více provozních režimů, které je možné konfigurovat pomocí webového rozhraní. Součástí dodávky bývá také napájecí adaptér a malá všesměrová anténa.



Obr. 6-25: Přístupový bod Wi-fi.

#### *Příklad technických parametrů*

Chipset: Realtek 8186

Komunikační porty: 2x RJ-45 (10/100 Mbit/s)

Konfigurace: Web management, SNMP

Pracovní teplota [°C]: 0-60

Rozměry [mm]: 135 x 100 x 26

Hmotnost [g]: 180

EMI: FCC, CE

Anténa: 2 dBi odpojitelná dipólová, konektor RSMA

Přenosové rychlosti: 1/2/5.5/11 Mbit/s, 18 Mbit/s, 24 Mbit/s, 36 Mbit/s, 48 Mbit/s, 54 Mbit/s

Šifrování: WEP 64/128-bit, WPA, WPA 2

Funkce access poitu: Bridge, Client, Repeater

Výstupní výkon [dBm]: 18

2MB Flash, 16MB SDRAM

LED diody Power, LAN, WLAN

Napájení: DC12V, 800mA

**Antény** jsou zařízení, schopná střídavou vysokofrekvenční energii vyzářit do prostoru, ve formě elektromagnetického pole o určité intenzitě (při vysílání). Při příjmu pracují naopak, to znamená, že elektromagnetické pole přemění na elektrickou energii. Základní rozdělení je podle tvaru vyzařovacího diagramu na všesměrové a směrové. Zvláštním typem směrových antén jsou antény sektorové.



# EUROALARM<sup>®</sup>

Zabezpečovací systémy

Specializovaný velkoobchod  
Nejširší nabídka a působnost v ČR

 **Visonic Ltd**

























- \* elektronické zabezpečovací systémy
- \* elektronická požární signalizace
- \* kamerové systémy
- \* přístupové a docházkové systémy
- \* speciální nehořlavé kabely
- \* stabilní hasící zařízení









**PRAHA**  
Hlavní 4  
140 00, Praha  
Tel.: +420 272 770 148  
Mobil: +420 777 705 715  
E-mail: euroalarm@euroalarm.cz

**PLZEŇ**  
Petr Talian  
Zborovská 98  
301 00 Plzeň  
Tel.: +420 377 429 027  
Mobil: +420 777 705 708  
E-mail: plzen@euroalarm.cz

**ČESKÉ BUDĚJOVICE**  
Karel Hlaváč  
Jírovcova 16  
370 01 Č. Budějovice  
Tel.: +420 387 313 295  
Mobil: +420 777 705 706  
E-mail: budejovice@euroalarm.cz

**PARDUBICE**  
David Šrámek  
17. Listopadu 216  
530 02 Pardubice  
Tel.: +420 466 616 474  
Mobil: +420 777 705 709  
E-mail: pardubice@euroalarm.cz

**BRNO**  
Petr Kačur  
Čechyňská 9  
602 00 Brno  
Tel.: +420 541 241 740  
Mobil: +420 777 705 713  
E-mail: brno@euroalarm.cz

**TEPLICE**  
Josef Donát  
Komenského 241  
417 61 Teplice  
Tel.: +420 417 577 552  
Mobil: +420 777 705 703  
E-mail: teplice@euroalarm.cz

**OSTRAVA**  
Ing. Zdeněk Závodný  
Slévárenská 7  
709 00 Ostrava  
Tel.: +420 596 614 880  
Mobil: +420 777 705 714  
E-mail: ostrava@euroalarm.cz

**ZLÍN**  
Marian Višňák  
U Zimního stadionu 4286  
760 01 Zlín  
Tel.: +420 577 217 061  
Mobil: +420 777 705 712  
E-mail: zlin@euroalarm.cz

[www.euroalarm.cz](http://www.euroalarm.cz)

[euroalarm@euroalarm.cz](mailto:euroalarm@euroalarm.cz)



# SALTEK

## ČESKÝ VÝROBCE SVODIČŮ PŘEPĚTÍ



**Komplexní ochrana  
a odrušení:**

- EZS, EPS
- přístupových a docházkových systémů
- kamer a monitorovacích ústředěn



### **Přepětové ochrany:**

**3-stupňový systém, odrušovací filtry nn, ochrana datových,  
analogových, telekomunikačních linek  
a anténních svodů**

SALTEK s.r.o., Arkalycká 1, 149 00 Praha 4  
tel.: 272 942 470, GSM: 602 472 633, fax: 267 913 411  
<http://www.saltek.cz>, e-mail: [obchod@saltek.cz](mailto:obchod@saltek.cz)

# SECURITY

DVOUMĚSÍČNÍK

ČASOPIS PRO VAŠI BEZPEČNOST

## Kamerové systémy

NAŠE  
TĚMA

# EUROSAT CS

Centrum bezpečnostních  
technolog

**P**  **R**  **D O X**  
S E C U R I T Y S Y S T E M



# LG

Kamerové  
systémy

TEL.: 548 216 707

FAX: 548 216 663

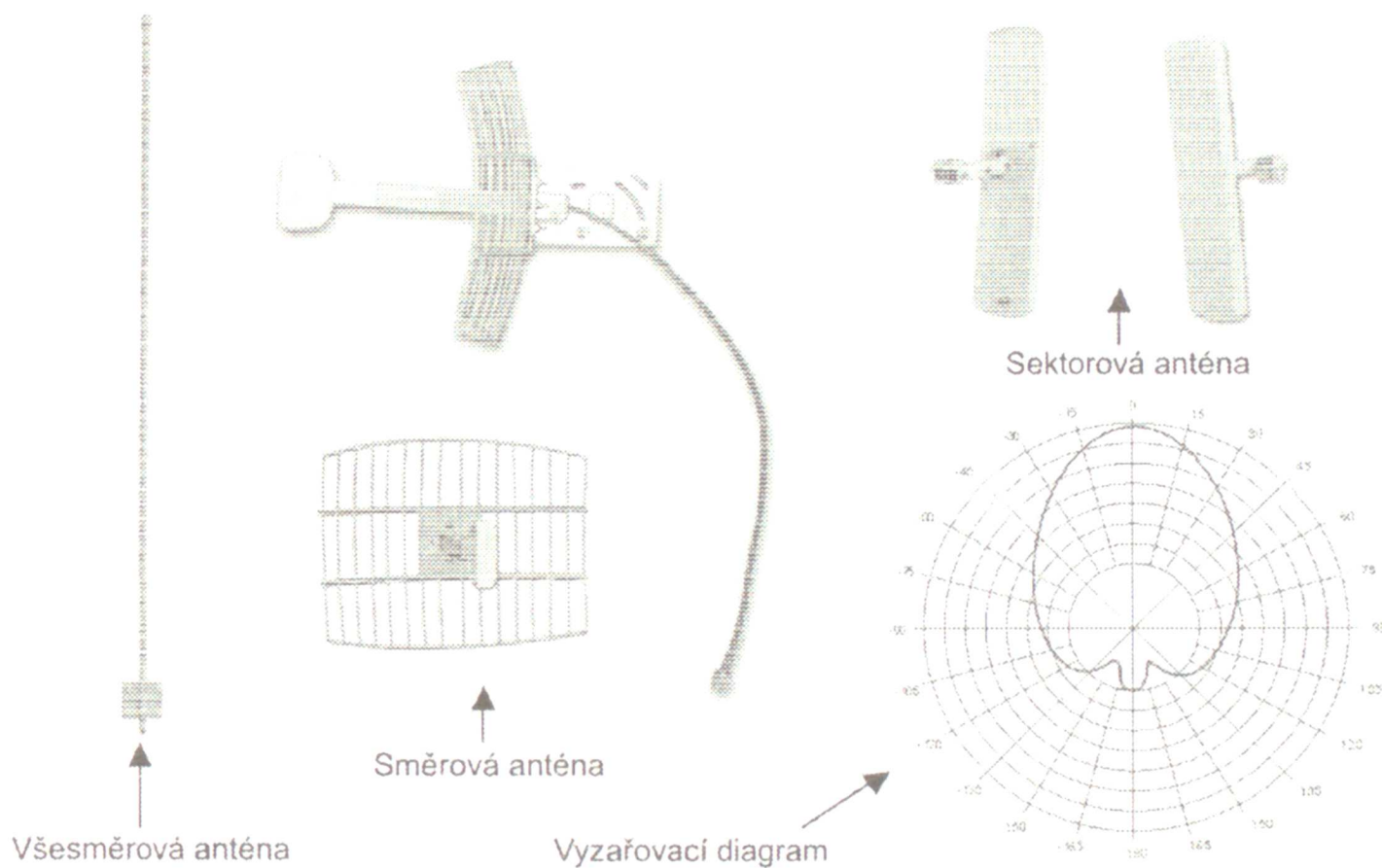
E-mail: [info@eurosat.cz](mailto:info@eurosat.cz)

BRNO - PRAHA - PLZEŇ - TURNOV - OSTRAVA

Č.BUDĚJOVICE - OSTRAVA - K.VARY

HRADEC KRÁLOVÉ - ZLÍN - MĚLNÍK

[www.eurosat.cz](http://www.eurosat.cz)



Obr. 6-26: Anténa Wi-fi.

Všesměrové antény ozařují prostor kolem sebe v úhlu  $360^\circ$ . Vyzařovací úhel v rovině kolmé se pohybuje kolem 10 až 20 stupňů. Na velikosti tohoto úhlu závisí zisk, který ovšem nebývá u těchto antén příliš velký, obvykle je kolem 5 až 12 dBi.

Antény směrové se vyznačují úzkým vyzařovacím paprskem a větším ziskem. Tyto antény se na trhu vyskytují ve velmi širokém sortimentu, takže pro danou aplikaci můžeme prakticky vždy najít a vybrat optimální anténu.

Vyzařovací diagram sektorových antén je přizpůsoben pro ozáření pouze určité části okolního prostoru, tedy sektoru. Jejich zisk proto bývá proti všesměrovým anténám větší.

Antény všesměrové používáme zpravidla pro základnové stanice. Někdy můžeme pro tento účel s výhodou vyššího zisku a zpravidla i nižší ceny použít též antény sektorové. U koncových stanic účastníků bezdrátových sítí, nebo při datových přenosech mezi dvěma stanicemi a zejména při přenosech na větší vzdálenosti se téměř vždy používají antény směrové, soustředí totiž většinu vyzářené energie do úzkého paprsku. Mezi tvarem vyzařovacího diagramu a ziskem antény platí závislost, která se v literatuře uvádí ve formě tabulek, nomogramů nebo grafů.

Směrové vlastnosti antén mají rozhodující vliv na dosažitelnou délku datového spoje. K výhodě většího zisku se současně přidružuje schopnost potlačení rušivých signálů ostatních uživatelů volného pásma, které přichází obecně ze všech směrů.

Při bezdrátovém přenosu Wi-fi signálů se používá lineární horizontální a vertikální polarizace. Rovina polarizace vyzářeného vlnění je dána výhradně konstrukčním uspořádáním antény. Většina prodávaných antén je konstrukčně uspořádána tak, že lze při montáži jednoduchým způsobem měnit jejich polarizaci. Má-li být zajištěna optimální kva-

lita signálu, musí se polarizace antén všech navzájem komunikujících zařízení shodovat. Při nedodržení této zásady dochází k potlačení zisku antén o 16 až 24 dB, což vede ke značnému zhoršení až znemožnění přenosu. Tuto vlastnost využijeme v prostředí se silným rušením, pocházejícím od cizích datových spojů a sítí. Vhodnou volbou polarizace při realizaci vlastní sítě můžeme rušení účinně potlačit.

Antény pro pásmo Wi-fi mají impedanci 50 Ω. Aby nedocházelo k odrazům na vedení, je třeba používat anténní kabely i konektory se shodnou impedancí.

Při instalaci antén musíme mít na mysli, že signály v pásmu 2,4 GHz se šíří podobně jako světlo a jakákoliv překážka mezi nimi má nepříznivý vliv na kvalitu přenosu. Měly by tedy být montovány v přibližně stejné výšce a přímé viditelnosti. Čím vyšší má anténa zisk, tím má také menší vyzařovací úhel a přesné nasměrování je velmi důležité. Také uvnitř budov snižují překážky (např. zdi) použitelný dosah.

### 3.9.2 Kabely a konektory

K propojení mezi anténou a AP se používá koaxiálních kabelů s impedancí 50 Ω, které jsou schopny přenést signál o kmitočtu 2,4 GHz s malým útlumem (ztrátami). Nejčastěji se pro kratší úseky (do 10m) používá typ H155 o průměru 5,4 mm s útlumem 0,5 dB/m. Pro delší úseky je doporučeno použít typ H1000 o průměru 10,3 mm s útlumem 0,22 dB/m.



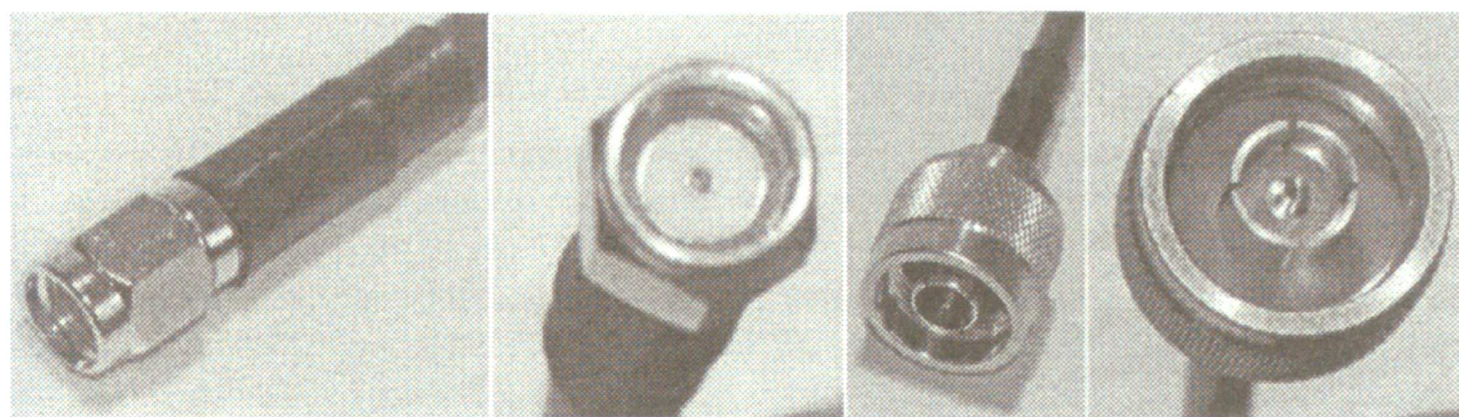
Obr. 6-27: Detail anténních koaxiálních kabelů.

Tabulka 6-10: Parametry koaxiálních kabelů

Příklad technických informací koaxiálních kabelů H155 a H1000			
Parametr	jednotka	H155	H1000
Impedance	Ω	50	50
Tolerance impedance	Ω	± 2	± 2
Kapacita	pF/m	82	80
Činitel zkrácení	-	0,81	0,83
Maximální stejnosměrný odpor ve smyčce	Ω/km	32	11
Útlum při 2,4 GHz	dB/m	0,5	0,22
Průměr vnitřního vodiče	mm	19 x 0,28 Cu	2,62 Cu
Dielektrikum	-	pěna	plné
Vnější vodič - folie	-	Al	Cu
Vnější vodič - opletení	-	pocin. Cu	Cu
Průměr přes plášť	mm	5,4	10,3

Konce kabelů je třeba opatřit příslušnými konektory. U antény je to zpravidla konektor typu N a u AP typ RSMA. Konektory se vyrábí v provedení Male (s kolíkem) nebo

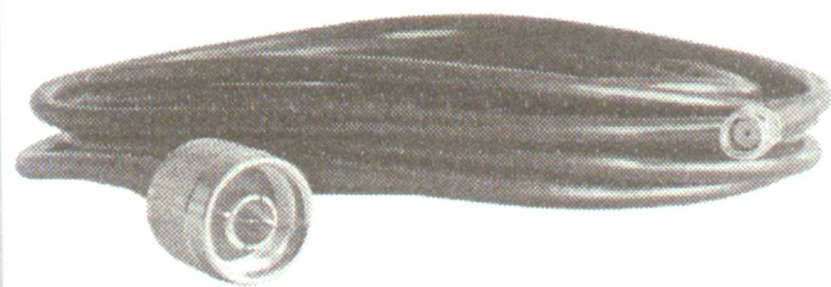
Female (s dutinkou). Liší se také tím, jsou-li určeny pro pájení nebo krimpování a podle průměru kabel, pro který jsou určeny.



Obr. 6-28: Konektory pro Wi-fi.

Potřebujeme-li propojit silný kabel H1000 s AP, musíme použít tzv. Pigtail, protože konektor typu RSMA se pro tak velký průměr kabelu nevyrábí. Pigtail (doslova přeloženo „prasečí ocásek“) je cca 30 cm dlouhá kabelová redukce zakončená různými typy konektorů.

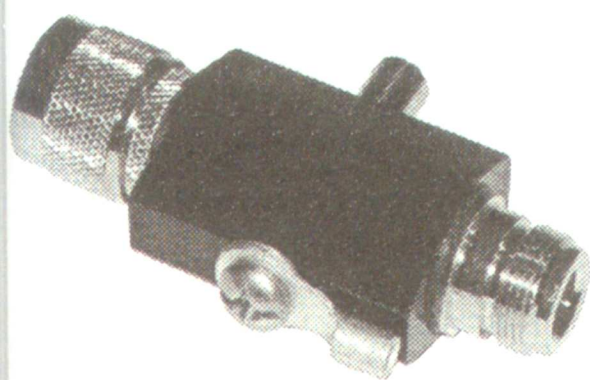
V nabídce prodejců nalezneme již hotové kabely různé délky, určené pro použití s běžnými druhy AP a antén. Jejich nákupem ušetříme čas i další náklady na pořízení speciálních nástrojů pro odizolování a krimpování konektorů (viz. část „Kabely, konektory a jejich zapojení“).



Obr. 6-29: Kabel pro Wi-fi.

### 3.9.3 Přepět'ové ochrany (bleskojistky)

V rozlehlých kabelových systémech nebo u anténních svodů je třeba řešit ochranu proti přepětí. Ta může zamezit poškození připojených zařízení způsobeného průmyslovým rušením, přepětím a atmosférickými výboji.



Obr. 6-30: Přepět'ová ochrana.

U anténních svodů se používá bleskojistek pracujících buď na principu plynové výbojky nebo pásmové propusti s  $\lambda/4$  zkratem naladěné na střed kmitočtového pásma. Bleskojistku je vždy třeba připojit co nejblíže k anténě a uzemnit vodičem dostatečného průřezu (min. 2,5 mm<sup>2</sup>). V žádném případě není možné připojit bleskojistku na ochranný vodič (kolík) zásuvky!

Výše uvedené bleskojistky bývají zařazovány do tzv. hrubé ochrany (hard limiter) na rozdíl od prv-

ků jemné ochrany (fine limiter), jejich základ tvoří varistory, Zenerovy diody a speciální lavinové, tzv. supresorové polovodičové diody. Více o přepětových ochranách v kapitole **7 Přepětové ochrany v elektronických systémech.**

## 4 Plánování

Nejprve se musíme seznámit se stávající konfigurací sítě LAN (doporučuji spolupracovat s vaším administrátorem) a stanovit volnou IP adresu pro provoz AP. Dále je třeba prověřit, jak je v dané lokalitě příslušné pásmo obsazeno. Provoz v bezlicenčních pásmech není nijak regulován a předpokládá se ohleduplnost a vzájemná dohoda mezi uživateli. Vzhledem k přeplněnosti pásem (zejména ve městech) však často dochází k vysílání na shodných nebo sousedních kanálech a překračování maximálního povoleného výkonu. Výsledkem je vzájemné rušení. Dojde-li k uvedenému problému, musí je odstranit ten, který začal pásmo užívat jako poslední (přestat vysílat, nebo přejít na jiný kanál). Problémy mohou způsobovat také Bluetooth zařízení, které pracují ve stejném kmitočtovém pásmu.

Český telekomunikační úřad v souladu s všeobecnými oprávněními ([www.ctu.cz](http://www.ctu.cz)) připouští v pásmu 2 400 až 2 483 MHz celkový vyzářený výkon EIRP (Equivalent Isotropic Radiated Power) jednoho zařízení 100 mW (definuje se také jako 20dBm nebo -10 dBW).

Převodní tabulka		
W	dBW	dBm
1	0	30
0,8	-1	29
0,6	-2	28
0,5	-3	27
0,4	-4	26
0,31	-5	25
0,25	-6	24
0,2	-7	23
0,16	-8	22
0,13	-9	21
0,1	-10	20
0,08	-11	19
0,06	-12	18
0,05	-13	17
0,04	-14	16
0,03	-15	15
0,025	-16	14
0,02	-17	13
0,016	-18	12
0,012	-19	11
0,01	-20	10

Tabulka 6-11: Převodní tabulka výkonových úrovní

Při překročení povoleného výkonu hrozí vysoká pokuta, proto je vhodné skutečný výstupní výkon předem spočítat.

Aby se úrovně, zisky a útlumy snadno počítaly používá se decibelů (dB). Kladná hodnota v dB znamená zisk, záporná hodnota útlum (0 dB odpovídá stejné vstupní i výstupní úrovni).

Vyjadřujeme-li v dB i absolutní úroveň (sílu signálu, pak jsou to vždy dB vztažené k nějaké (dříve hodnuté, standardní) hodnotě.

- dBW - o kolik je napětí vyšší či nižší než 1 W
- dBmW nebo dBm - o kolik je výkon vyšší či nižší než 1 mW

$EIRP \text{ (v dBm)} = \text{výstupní výkon Wi-fi zařízení} + \text{zisk externí antény} - \text{útlum anténního kabelu} - \text{útlum konektorů, bleskojistky, apod.}$

Konkrétní údaje o výstupním výkonu AP (někdy je nastavitelný), zisku antény a útlumu dalších komponent zjistíme např. na webu výrobce nebo prodejce.

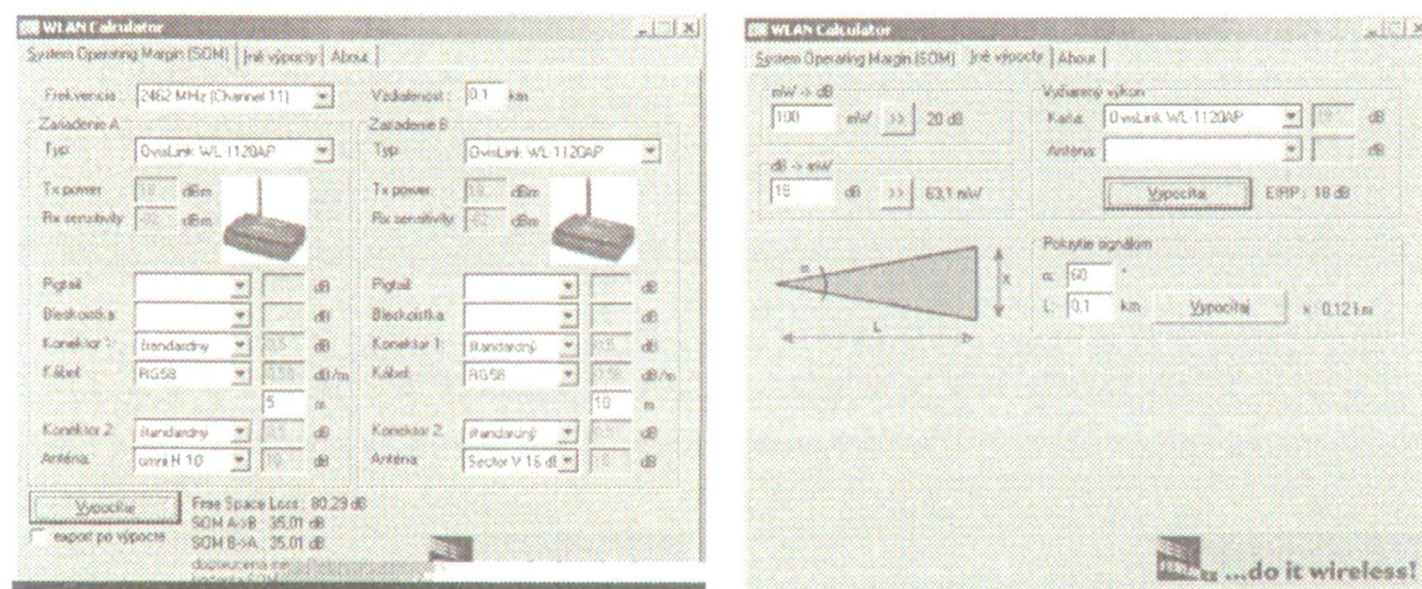


Tabulka 6-12: Kalkulace vysílacího výkonu

Komponent	dBm
Přístupový bod OvisLink AirLive WL-5460AP	18
Externí všesměrová anténa Omni-CZ-08V	8
Anténní kabel Pigtail 10m RSMA-N/m H155	-5,6
Zkratová bleskojistka 2,4 GHz	-0,6
celkem	19,8

Vypočtená hodnota 19,8 dBm je těsně pod maximální povolenou hodnotou EIRP. Některé zdroje uvádějí, že podle dodatků by výsledná hodnota měla být pouze 17 dBm. Tato hodnota vychází ze spektrální hustoty většiny Wi-fi karet. Je proto lepší dodržet nižší hodnotu, tj. 17 dBm. Ve výše uvedeném příkladu by to bylo možné použitím méně výkonné antény nebo nastavením nižšího výkonu AP (funkce - TX power regulation in 4 levels).

K výpočtům důležitých hodnot při zřizování bezdrátových Wi-fi sítí můžete využít program WLAN Calculator, od slovenské firma Ferimex (<http://www.ferimex.com>). Program dovede podle zadaných hodnot určit takzvaný System Operating Margin, což je zisk na trase bezdrátového spoje. Pokud je příliš nízký (doporučeno je minimálně 20 dB), trasa nejspíše nebude provozuschopná a je vhodné zvolit zařízení jiné. Umí také převádět jednotky mW na dB a naopak, počítá vyzářený výkon a pokrytí signálem. Pro výpočet je nejprve nutno zadat parametry Wi-fi zařízení, které chcete používat. Parametry některých na trhu dostupných výrobků jsou v programu již uvedeny, stačí si zařízení vybrat z více-položkového menu.

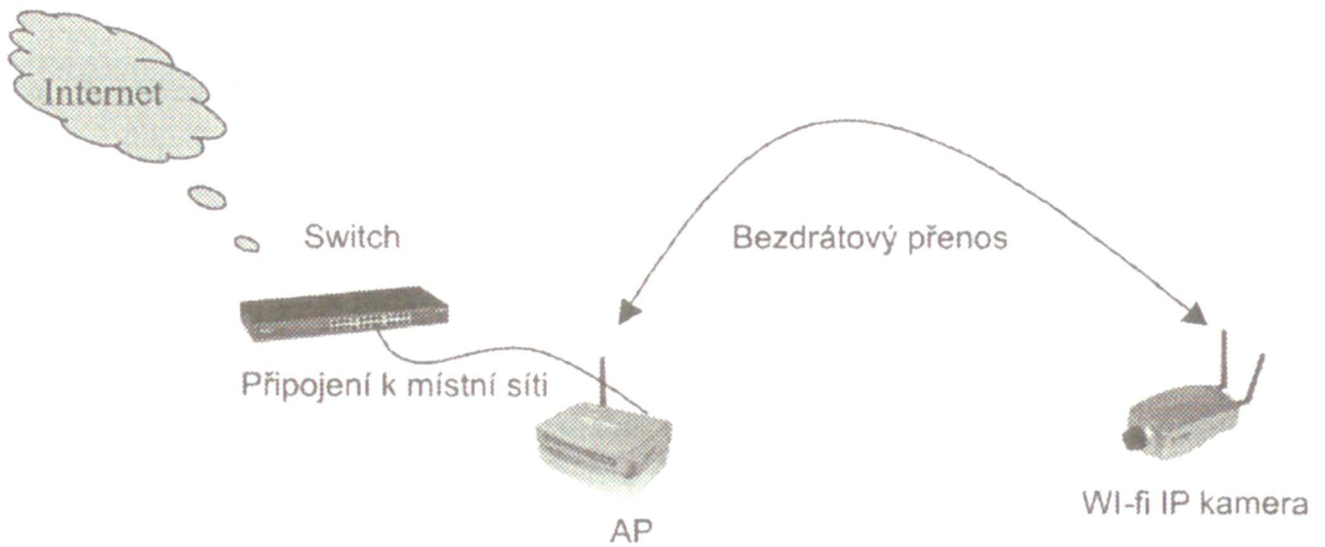


Obr. 6-31: Scren VII.

## 5 Příklad praktického použití

Problém techniky Wi-fi dále zjednodušíme na připojení IP kamer do stávající sítě LAN. Budeme potřebovat přístupový bod dále jen AP (Access Point), který vytvoří rozhraní mezi stávající „drátovou“ sítí LAN a umožní připojení bezdrátové IP kamery. Abychom se i po delším čase dokázali v nastavení rychle zorientovat, je třeba naplánovat

a do tabulky zapsat výchozí i cílové nastavení jednotlivých komponent Wi-fi sítě. Výchozí (defaultní) hodnoty, které jsou přednastaveny a do kterých se zařízení vrátí po restartu zjistíme z manuálu, MAC adresu nalezneme na štítku zařízení nebo zjistíme pomocí vhodného softwaru.



Obr. 6-31: Propojení do sítě prostřednictvím Wi-fi.

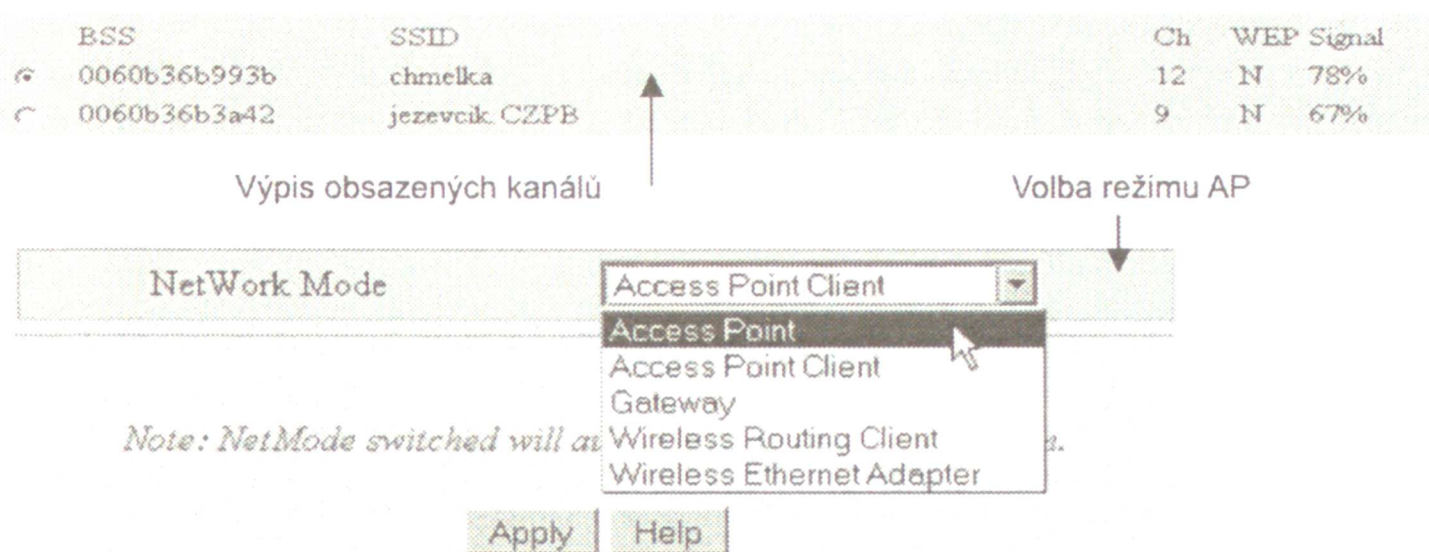
Tabulka 6-13: Parametry nastavení komponent Wi-fi sítě

Parametr	Defaultní hodnota	Požadovaná hodnota	Zařízení
IP adresa	192.168.100.252	10.1.50.151	Přístupový bod WL-1120AP
MAC adresa	00-00-3C-35-DE-54	00-00-3C-35-DE-54	
Submaska sítě	255.255.255.0	255.255.255.0	
SSID	802_11b-SSID	IP_kamery	
Kanál	11	9	
DHCP client	vypnutý	vypnutý	
Mód	AP	AP	
Šifrování	vypnuto	vypnuto	Wi-fi kamera IP 3133
IP adresa	192.168.0.201	10.1.50.152	
MAC adresa	00-00-3C-35-DE-11	00-00-3C-35-DE-11	
Submaska sítě	255.255.255.0	255.255.255.0	
SSID	default	IP_kamery	
Kanál	11	9	
Šifrování	vypnuto	vypnuto	

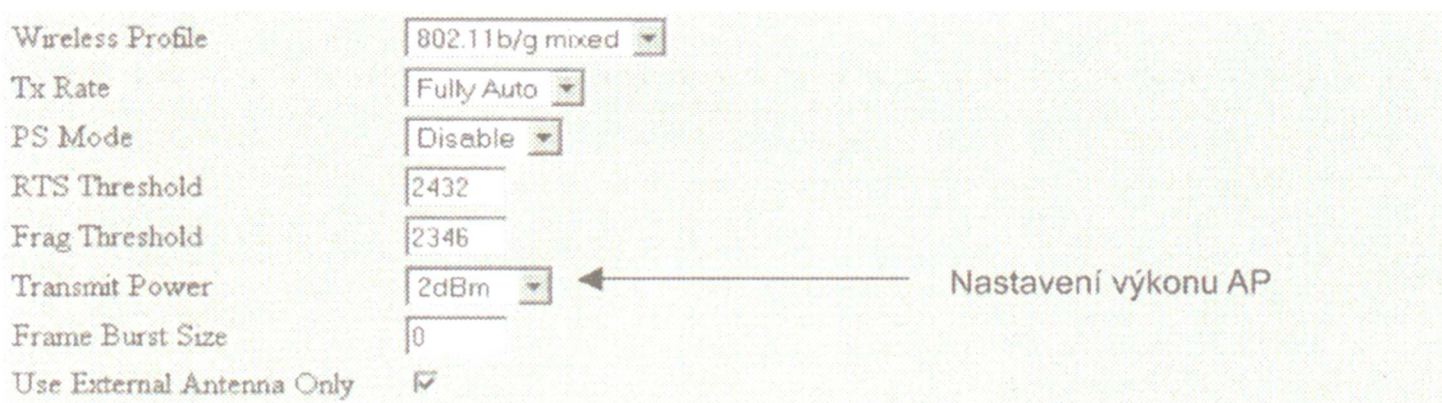
Dále je vhodné poznamenat si výchozí i nastavené přístupové údaje pro jednotlivá zařízení (uživatelské jméno a heslo). Pokud budete využívat připojení k internetu, tak také adresu výchozí brány a DNS serverů.

**Volba kanálu, režimu, nastavení výkonu a konfigurace IP**

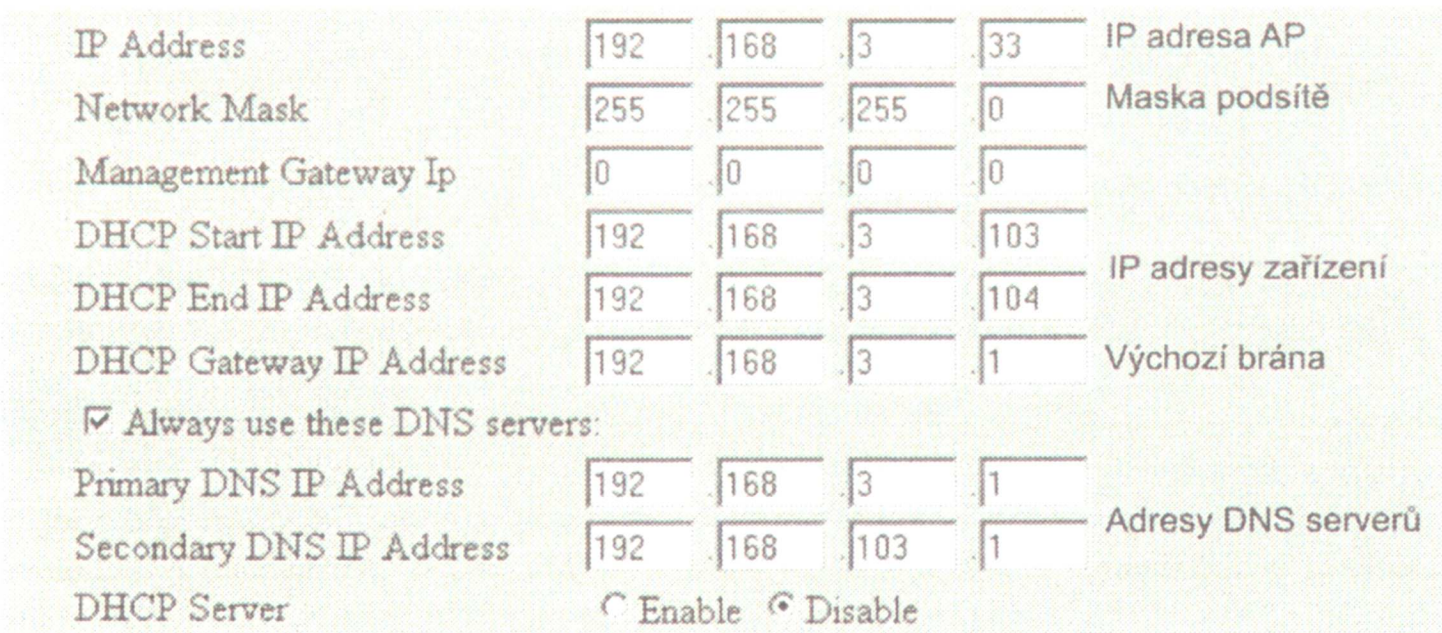
Většina AP umožňuje skenování Wi-fi pásma s výpisem obsazených kanálů. Některé jsou vybaveny automatickou volbou volného kanálu. Abychom zamezili rušení stávajících sítí, je třeba zvolit kanál, který není obsazen. Následující obrázky ukazují příklad konfigurace AP. Konkrétní nastavení a možnosti jsou však u různých AP odlišné a vždy je třeba postupovat podle manuálu.



Obr. 6-32: Screenshot VIII.



Obr. 6-33: Screenshot IX.

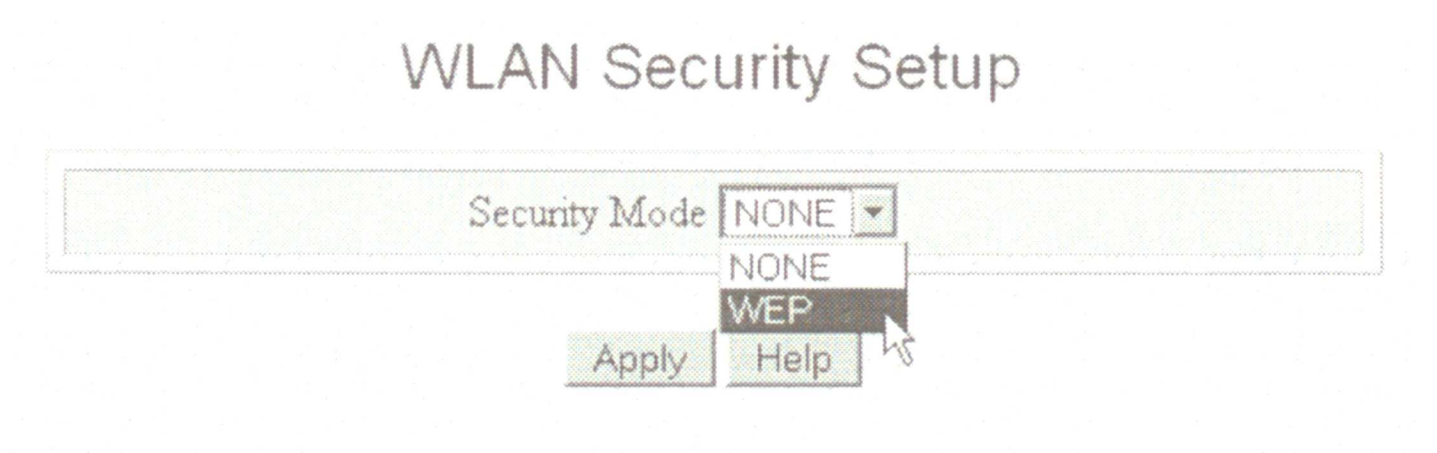


Obr. 6-34: Screenshot X.

### Ochrana dat, šifrování

Bezdrátové sítě Wi-fi jsou daleko snáze napadnutelné než klasické „drátové“, proto je třeba v běžném provozu věnovat pozornost jejich zabezpečení. Po zprovoznění základní komunikace se zaměříme na následující nastavení:

- změna defaultního uživatelského jména a hesla
- změna defaultního SSID
- zrušení vysílání jména sítě (SSID broadcast)
- omezení přístupu k síti podle MAC adres
- aktualizace firmware Wi-fi zařízení
- zapnutí šifrování WEP, WPA nebo WPA2 (nejkvalitnější)



Obr. 6-35: Screenshot XI.

Nezapomeňte, že některá nastavení (např. změna SSID nebo šifrování) je třeba provést nejen na AP, ale také na všech připojených zařízeních a ta je musí podporovat. Dojde-li během nastavování parametrů k chybě a zařízení přestanou správně fungovat, proveďte podle manuálu restart a začněte znovu.

## 6 Popisy konkrétních prvků

**Upozornění:** Než začneme pracovat s kamerami a video servery je nutné si uvědomit, že užití jakýchkoliv kamer a zařízení umožňujících nepozorované snímání přenos a záznam obrazu a zvuku (odposlech) je upravováno zákony, toto se týká i kamer bezpečnostních včetně IP kamer. Před instalací síťové kamery je vždy nutné ověřit, zda její instalace a umístění není v rozporu s platnými zákony.

Síťové kamery a video servery jsou vybavené web serverem ten umožňuje jejich připojení po běžných širokopásmových linkách ISDN a ADSL bezdrátové či kabelové připojení. Zabudovaný web server nabízí uživateli přehledné a jednoduché rozhraní pro sledování, ovládání a nastavování kamery či video serveru a umožňuje uživateli přístup po internetu. Pokud je prvek připojen do ethernetové sítě, k přístupu přes internet musí být povolený přístup do dané ethernetové sítě. Díky připojení kamery či video serveru k internetu je možné obrazovou popřípadě i zvukovou informaci z tohoto prvku sledovat a tento konfigurovat odkudkoli na světě pomocí internetového prohlížeče Microsoft internet Ex-

plorer. Uživatel sleduje audio/video záznam stejným způsobem jako si prohlíží kterékoli jiné stránky na internetu.

Nastavování a práci s IP kamerami i video servery můžeme rozdělit do tří skupin. Do první skupiny patří činnosti společné všem IP prvkům bez ohledu na to, zda jde o video server či IP kameru statickou, či otočnou a od kterého výrobce je. Do druhé skupiny patří takové činnosti které jsou shodné pro určitou část výrobků např. od stejného výrobce. Třetí skupinou činností jsou takové, které jsou specifické pro konkrétní výrobek.

Mezi činnosti společné pro všechny prvky IP kamerových systémů jak kamery tak video servery patří například:

Převzetí komponentů a jejich vybalení. Po otevření balení kamery či video serveru vždy pečlivě zkontrolujte obsah balení podle přiloženého letáku „Obsah balení“. Včetně kontroly výrobních čísel. Poté je nutné prostudovat návod a podle něj postupovat při instalaci. Zabráníte tím problémům při instalaci a provozu, popřípadě riziku poškození, nebo zničení daného zařízení způsobeném nesprávným použitím.

Prvním krokem při vlastní instalaci je nastavení IP adresy. Toto se u všech prvků včetně bezdrátových provádí pomocí překříženého UTP kabelu s konektory RJ 45 pomocí PC nebo notebooku v programu Microsoft internet Explorer (viz. konkrétní popis u jednotlivých zařízení).

Je vhodné poznamenat si výchozí i nastavené přístupové údaje pro jednotlivá zařízení (uživatelské jméno a heslo). Pokud budete využívat připojení k internetu, tak také adresu výchozí brány a DNS serverů.

Dojde-li během nastavování parametrů k chybě a zařízení přestanou správně fungovat, proveďte podle manuálu restart a začněte znovu.

## 6.1 Nastavení a konfigurace IP kamer

IP kamery jsou navrženy pro mnohostranné použití. Nejčastěji jsou využívány pro sdílení videa, v některých případech, ale také mohou posloužit jako účinný zabezpečovací systém, další z možností využití těchto kamer je pro demonstrační účely. Pomocí IP kamer můžeme provádět vzdálený dozor například nad bytem, provozovnou, sledování dopravy atd., lze je také využít při pořádání video konferencí, pro zatraktivnění webových stránek a v mnohých jiných aplikacích.

Dále jsou uvedeny zástupci základních typů IP kamer:



### 6.1.1 Pevná IP kamera typu IP3122

Kamera IP3122 je univerzální síťová kamera osazená CCD čipem 1/4" a s výměnným objektivem. Zabudovaný web server nabízí přehledné a jednoduché rozhraní pro ovládání kamery po síti a umožňuje uživateli vzdálený přístup po internetu. Tuto kameru je možno sledovat a konfigurovat odkudkoli na světě pomocí internetového prohlížeče Microsoft Internet Explorer. Uživatel sleduje audio/video záznam stejným způsobem jako si prohlíží jiné stránky na internetu. Kamera IP3122 je vhodná pro zvýšení atraktivnosti webových stránek, vzdálený dozor, zabezpečení domova či provozovny, pořádání video konferencí a mnoho jiných použití.

Obr. 6-36: IP-kamera (Vivotek).

Základní technické parametry:

- Síť: 10/100BaseT Ethernet
- Podporované protokoly: UPnP, TCP/IP, HTTP, SMTP, FTP, Telnet, NTP, DNS a DHCP
- Max. 30/25 snímků o rozlišení 320x240 nebo 160x120, 25 snímků/s o rozlišení 352x288 nebo 176x144 bodů, 10 snímků/s o rozlišení 704x576 bodů
- Barevný snímací prvek CCD 1/4"
- Citlivost: 1Lux/F2,0
- AGC (automatické řízení zisku), AWB (automatické vyvážení bílé)
- Elektronická závěrka v rozsahu 1/60 až 1/100000 s
- 1x opticky izolovaný vstup pro externí senzor
- 1x reléový výstup pro ovládání externího zařízení
- Záznam zvuku pomocí zabudovaného mikrofону
- Detektor pohybu ve třech nezávislých oknech

### 6.1.2 Otočná IP kamera typu PZ6122



Obr. 6-37: IP-kamera otočná (Vivotek).

Kamera PZ6122 je síťová kamera která má motorizovaný otáčený a naklápěcí objektiv s funkcí ovládané otáčení a naklápění s funkcí ovládané otáčení a naklápění pomocí myši, má také režim automatického otáčení a automatického sledování podle přednastavených pozic. Rozsah naklápění je 135° a otáčení v 270°. Kamera má 10-ti násobný OPTICKÝ ZOOM, plus 10-ti násobný DIGITÁLNÍ ZOOM.

Nabízí volbu mezi dvěma normami výstupního streamu – uživatel si může vybrat mezi kompresí Motion JPEG a MPEG4. Umožňuje přenášet synchronní video společně s obousměrným zvukem (duplexní audio) V kamerě je zabudovaný vysoce citlivý mikrofón (lze připojit také mikrofón externí). Kamera má optimální synchronizaci videa i zvuku, má také audio/video výstup pro sledování na externím analogovém monitoru, nebo pro paralelní připojení do analogového kamerového systému. Dále je vybavena funkcí video detekce pohybu ve třech nezávislých nastavitelných oknech. Umožňuje zasílání snímků před/po alarmové události. Má programovatelný digitální výstup. Komprese obrazu a zvuku umožňuje připojení kamery i po běžných širokopásmových linkách typu ISDN, ADSL, bezdrátového či kabelového připojení. Zabudovaný web server nabízí přehledné a jednoduché rozhraní pro ovládání kamery a umožňuje vzdálený přístup přes Internetu. Kameru PZ6122 lze mimo jiné využít pro zvýšení atraktivnosti webových stránek, vzdálený dozor s možností detailu, zabezpečení domova či provozovny, pořádání video konferencí nebo jako součást více kamerového monitorovacího systému.

Základní technické parametry:

- Síť: 10/100BaseT Ethernet
- Podporované protokoly: UPnP, TCP/IP, HTTP, SMTP, FTP, Telnet, NTP, DNS a DHCP

- 25 snímků/s o rozlišení 352x288 nebo 176x144 bodů, 12 snímků/s o rozlišení 704x576 bodů
- Duplexní audio 8/24/32 kbps, potlačení zpětné vazby
- Barevný snímací prvek CCD 1/4" standardu PAL
- Citlivost 1,5Lux/F1,8 (0,05 Lux/F1,8 – Low Lux Mode)
- AGC (automatické řízení zisku), AWB (automatické vyvážení bílé), AES (automaticky řízená uzávěrka)
- Elektronická uzávěrka v rozsahu 1/60 až 1/120 000 s
- 1× opticky izolovaný vstup pro externí senzor
- 1× reléový výstup pro ovládání externího zařízení.
- Audio/video výstup pro sledování na externím analogovém monitoru
- Externí alarmový vstup
- Napájení stejnosměrné 12V, 1,5A

### 6.1.3 Širokoúhlá IP kamera s vysokým rozlišením



Obr. 6-38: IP-kamera s vysokým rozlišením (IQ eye).

Kamera IQeye3 je zobrazovací systém s vysokým rozlišením, který poskytuje velký počet snímků za sekundu a síťový počítač v jediném kompaktním a robustním pouzdru. Průmyslový design a nízká spotřeba energie umožňují použití i pro aplikace s velmi vzdáleným přístupem. Kamera podporuje široké spektrum protokolů pro jednoduché zprovoznění a volitelně dodávaný IQpoet (napájení po Ethernetu) významně snižuje náročnost a náklady na instalaci.

Kamery IQeye3 nabízí 4x více bodů než běžná CCTV kamera. Kamera IQeye3 je vybavena i možností digitálního přiblížení a pohybu v obraze. Typickou aplikací je například použití kamery s extrémně širokoúhlým objektivem, což umožňuje dokonalé otáčení, naklápění a digitální zoom v obraze - a to bez jediné pohyblivé části!

Základní technické parametry:

- Síť: 10/100BaseT Ethernet
- Podporované protokoly: IP, TCP, UDP, ICMP, 802.11b, ARP, FTP, SMTP, DHCP, HTTP, RARP, BOOTP, SNMP, Telnet, TFTP
- Barevný snímací prvek CCD 1/2"
- Max. rozlišení 1280 x 1024 bodů (1,3 Mega pixelů)
- Citlivost 0.3 lux
- AGC (automatické řízení zisku), AWB (automatické vyvážení bílé), AES (automaticky řízená uzávěrka)
- Podporované objektivy C-Mount nebo CS-Mount

## 6.2 Nastavení a konfigurace videoseverů

Mezi jedny ze základních prvků moderních kamerových sledovacích a monitorovacích systémů patří tzv. videosevery. Jejich funkce spočívá v tom, že umožňují zpracování

signálu z klasických analogových video zařízení a jeho přenos do Ethernet sítě. Video servery se vyrábějí v provedení s jedním, nebo více analogovými video a audio vstupy.

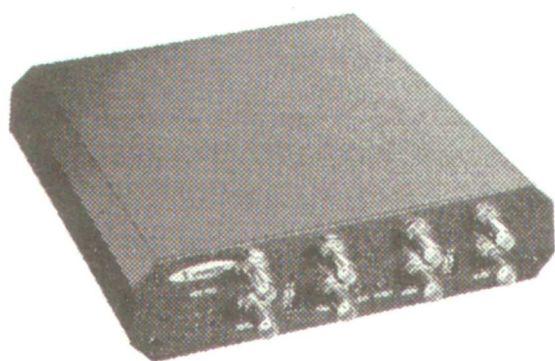
Využití videoserverů je především ve třech oblastech.

První z nich je tam, kde v je zapotřebí modernizovat zastaralý kamerový systém ve kterém k záznamu obrazové informace slouží pomaloběžný videorekordér. Pokud je tento systém v objektu, kde je instalovaná strukturovaná kabeláž a eternitová síť je velice dobrým a ne příliš nákladným řešením, způsob kdy v rámci modernizace je z původního systému zachována část s kamerami a nesymetrickým vedením, kamerový přepínač nebo kvadrátor popřípadě multiplexer spolu s pomaloběžným videorekordérem a analogovým video monitorem jsou ze systému odstraněny a nahrazeny vícevstupovým videoserverem. Poté se s obrazovými informacemi z připojených kamer pracuje stejně jako kdyby byly pořízeny pomocí IP kamer připojených k ethernetové síti se všemi výhodami které tento způsob připojení přináší. Umožňuje záznam, dohled a prohlížení z kteréhokoliv počítače vybaveného patřičným programem a připojeným k této síti popřípadě odkud kdokoliv pomocí internetu. V závislosti na užitém programu je možné použít takové funkce jako je detekce pohybu v obraze, záznam po detekci pohybu, ale i určitou dobu před detekcí pohybu. Další výhodou tohoto řešení je relativně snadná možnost rozšíření tohoto kamerového monitorovacího systému pomocí připojení IP kamer.

Další možností využití videoserverů v kombinaci s analogovým kamerovým systémem je možnost kdy některá, nebo některé kamery z funkčního analogového kamerového systému jsou pomocí vřazeného videoserveru navíc současně připojeny do eternitové sítě, což umožňuje jejich vzdálený dohled a zpracování informací na síti pomocí některého ze specializovaných počítačových programů.

Další oblastí kde jsou v praxi využívané video servery je připojení některých speciálních analogových video kamer do IP monitorovacího kamerového systému. Jedná se především o analogové video kamery s výjimečnými parametry jejichž ekvivalent se v provedení IP kamer nevyrábí, nebo je příliš drahý (podvodní kamery, infra kamery, kamery pro noční vidění, miniaturní kamery, kamery do specifických prostředí).

Video servery mohou být také jako součást digitálních záznamových zařízení, zde umožňují vzdálený přístup pomocí eternitové sítě k video záznamu popřípadě k exportování video souborů nebo obrázků formou E-mailů.



Obr. 6-39: Videoserver (Vivotek).



## 7 Nastavení a konfigurace Access Pointu (AP)

### 7.1 Základní informace

Bezdrátové síťové prvky – WLAN zařízení – jsou produkty, které přenášejí data bez vzájemného fyzického propojení. Pro přenos signálu používají jednu nebo více nosných frekvencí, na kterých je namodulován vlastní signál v zakódované podobě. Cílem WLAN zařízení je zajistit síťové propojení bez využití kabeláže.

WLAN zařízení jsou PC komponenty citlivé na mechanické poškození a výskyt elektrostatické elektřiny, zejména pak zařízení v interním provedení. Vlastní instalaci může provádět pouze odborník a pro jeho zapojení je vyžadována odborná způsobilost v elektrotechnice minimálně na úrovni §4 vyhlášky číslo 50/1978 Sb. Samotnou instalaci mohou provádět tedy pouze pracovníci poučení. Je také doporučena znalost minimálně základní technické angličtiny a pokročilejší orientace v prostředí příslušných operačních systémů. Nutná je také znalost problematiky síťových technologií – protokolu TCP/IP – minimálně na úrovni základní administrace systému.

### 7.2 Technické parametry

V dalším popisu se budeme zabývat AP typu **AirLive WL – 1120AP**.



Základní parametry:

- Defaultní IP adresa je 192.168.100.252
- Defaultní submaska sítě je 255.255.255.0
- Defaultní SSID je 802\_11b-SSID
- Defaultní kanál je 11
- DHCP client je defaultně vypnutý
- Zařízení je defaultně nastaveno v módu AP
- Bezdrátová přístupová bod podporuje čtyři módy AP, Client, Bridge, Repeater (WDS)

Obr. 6-40: IP-přístupový bod.

Tabulka 6-14: Funkce indikačních LED diod na předním panelu

LED		Status	
Indikace	Barva	Svítlí	Bliká
Power	•	Signalizuje připojení napájecího kabelu	N/A
ErrStatus	•	Signalizuje komunikační chybu	Self test
Link/Act.	•	Signalizuje připojení klienta	Přijímá / odesílá data
WEP	•	Funkce je zapnuta	N/A
MAC Ctrl	•	Funkce je zapnuta	N/A
Bridge	•	Zařízení je v módu WDS	N/A
LAN 1	•	Je připojená místní síť	Přijímá / odesílá data
LAN 2			

### 7.3 Instalace

K instalaci budeme potřebovat počítač (notebook). Přišroubujte anténu do příslušného konektoru AP, připojte napájecí kabel a LAN kabel do AP.

#### Reset AP

K tomuto kroku se možná budete několikrát vracet. AP lze resetovat dvěma způsoby:

*Tvrký reset* - při něm se vymažou vaše nastavení a obnoví tovární konfigurace. Tento reset je například potřeba, když se spletete v nastavení a AP se s vámi přestane bavit. Proveďte se tak, že stisknete (vhodným párátkem apod.) tlačítko RESET na AP, a podržíte jej stisknuté alespoň 10 sekund.

*Obyčejný reset* - zůstanou zachována nastavení. Je potřeba, pokud se při běžném provozu AP „zakousne“. Proveďte se tak, že stisknete RESET a podržíte cca 4 sekundy.

Pokud by se AP z nějakého důvodu nepovedlo zresetovat ani tvrdým resetem, zkuste odpojit napájení, znovu ho zapojit, a pak tvrdý reset.

#### Nastavení

Veškerá další konfigurace AP se provádí z počítače pomocí webového prohlížeče. AP v sobě obsahuje malý webový server se stránkami plnými různých nastavení. Po prvním zapnutí a po tvrdém resetu je tento server (a celé AP obecně) dostupný na IP adrese 192.168.100.252. Tuto adresu je zapotřebí změnit na adresu, kterou budete využívat ve vaší síti.

#### Nastavení počítače

Na počítači, který je k AP připojen, nastavte TCP/IP parametry síťového připojení (Ethernetové karty) takto:

IP adresa: 192.168.100.251

Maska sítě: 255.255.255.0

Ostatní parametry nemusíte vyplňovat, nejsou v tuto chvíli potřeba.

Nyní stačí spustit webový prohlížeč a napsat do něj adresu <http://192.168.100.252> a měla by se vám zobrazit úvodní obrazovka konfigurace AP.

#### Nastavení TCP/IP

V menu vyberte TCP/IP a potom Basic. V obrazovce, která se objeví, vyplňte potřebné údaje (viz. kapitola „Bezdrátové systémy Wi-fi/Plánování“).

Potvrďte nastavení.

#### Nastavení počítače ještě jednou

V předchozím kroku jsme změnili výchozí nastavení AP. Proto je nutné vrátit nastavení počítače na původní hodnoty, odpovídající konfiguraci vaší sítě.

#### Základní nastavení WiFi

Opět otevřete prohlížeč a připojte se k AP. Adresa, kterou do prohlížeče zadáte, už ale bude jiná - bude to IP adresa AP, kterou jste nastavili. Opět se objeví úvodní obrazov-

ka AP a menu. Nyní je třeba nastavit parametry bezdrátového připojení. Z menu vyberte *Wireless* a potom *Basic*.

Proveďte (zkontrolujte) následující nastavení:

Mode: Access Point

Network type: Infrastructure

SSID:

*Channel*: Vyplňte příslušné údaje (viz. kapitola „Bezdrátové systémy Wi-fi/Plánování“)

Potvrďte nastavení.

### Další nastavení WiFi

Pokud bude k AP připojena externí anténa s vyšším ziskem, je třeba zkontrolovat, zda nebude překročena maximální povolená hodnota výkonu (EIRP). Obecně platí - *nevysílat výkonem větším, než je pro funkčnost spojení nezbytně nutné*.

Nastavení výkonu se provádí z menu *Wireless / Advanced*:

U položky Tx Power Level vyberte co nejnižší nastavení, při kterém spojení funguje. K dispozici je 5 hodnot od Highest (nejvyšší) po Low (nejnižší). Nejvyšší hodnotu (Highest) nepoužívejte - jednak téměř určitě překročíte limity povolené generální licenci, a také má AP při tomto nastavení tendenci chovat se poněkud ošklivě a rušit ostatní zařízení poněkud více, než je zdravo.

Změny je třeba potvrdit tlačítkem *Apply Change*.

### Uživatelské jméno a heslo

Z menu vyberte *Other / Password*.

Do pole *User Name* zadejte uživatelské jméno. Do pole *Password* zadejte heslo.

Doporučuji ve jménu ani heslu nepoužívat českou diakritiku. Do pole *Confirmed Password* zadejte ještě jednou totéž heslo pro kontrolu. Pak již stačí klepnout na *Apply Change*.

### Uložení nastavení

Nastavení AP si můžete zálohovat do souboru na svém počítači. Stačí v menu zvolit *Other* a *Save/Reload Settings*. Nastavení uložíte tlačítkem *Save*. Uložený soubor s nastavením má název *config.dat*.

Pokud budete někdy potřebovat nastavení obnovit (například po tvrdém resetu), vyberte soubor, do kterého jste nastavení uložili (tlačítko **Browse**) a stiskněte tlačítko **Upload**. Měla by se zobrazit potvrzující zpráva, kterou potvrdíte stisknutím tlačítka OK.

## 8 Nastavení a konfigurace IP Wi-fi kamery

### 8.1 Základní informace

IP Wi-fi kamera v sobě podstatě spojuje dvě již dříve popsaná zařízení – IP kameru a modul bezdrátového přenosu dat standardu Wi-fi. Platí tedy již uvedené základní vlastnosti. V rámci projektu byla vybrána kamera typu IP3133 do firmy Vivotek, která splňuje základní požadavky. Vzhledem ke kvalitě objektivu (který je naštěstí výměnný) však nelze očekávat stejnou kvalitu obrazu jako u profesionálních kamer.

## 8.2 Technické parametry



Důležitá defaultní nastavení:

- Defaultní IP adresa je 192.168.0.99
- Defaultní submaska sítě je 255.255.255.0
- Defaultní router (brána pro připojení k internetu): 0.0.0.0
- Primární DNS: 0.0.0.0
- Sekundární DNS: 0.0.0.0
- SSID - výchozí nastavení je: default
- Režim bezdrátového připojení – Infrastructure (použijte pro připojování kamery k Access Pointu).
- Kanál (Channel): 6
- Pozor! Pokud ponecháte zaškrtnutou volbu  Reset the IP adres at next boot obnoví se po uložení a následném restartu defaultní nastavení a provedené změny se neprojeví.

Obr. 6-41: IP-kamera bezdrátová (Vivotek).

Tabulka 6-15: Funkce indikační LED diody (vpředu vedle objektivu)

Stav LED diody	Status	Doporučení
Bliká červená / zelená	Vnitřní diagnostika po zapnutí	Vyčkat dokončení diagnostiky
Svítil červeně •	Kamera není připojena k síti	Připojit síťový kabel; zapnout AP
Svítil zeleně •	Kamera není správně nastavena	Nastavit parametry sítě (IP)
Jiný stav	Chyba hardware	Vypnout a znovu zapnout

## 8.3 Instalace

K instalaci budeme potřebovat počítač (notebook) a AP. Přišroubujte antény do příslušných konektorů kamery, připojte napájecí kabel a LAN kabel do kamery.

Po připojení napájecího napětí se kamera nejdříve snaží najít připojení k Ethernet kabelem. Pokud se spojení nepodaří, zkusí kamera bezdrátovou síť.

### Reset kamery

K tomuto kroku se možná budete několikrát vracet. Reset provádějte bezprostředně po zapnutí kamery. Stisknete (vhodným párátkem apod.) tlačítko RESET na zadní straně kamery, a podržíte jej krátce stisknuté. Po restartu se vymažou vaše nastavení a obnoví tovární konfigurace.

### Nastavení

Veškerá další konfigurace AP se provádí z počítače pomocí webového prohlížeče. Kamera v sobě obsahuje malý webový server se stránkami plnými různých nastavení. První nastavení je vhodné provádět s připojeným síťovým kabelem. Po zapnutí a resetu

je tento server (kamera) dostupná na IP adrese 192.168.0.99. Tu je potřeba změnit na adresu, kterou budete využívat ve vaší síti.

### Nastavení počítače

Na počítači, který je k AP připojen, nastavte TCP/IP parametry síťového připojení (Ethernetové karty) takto:

IP adresa: 192.168.0.99

Maska sítě: 255.255.255.0

Ostatní parametry nemusíte vyplňovat, nejsou v tuto chvíli potřeba.

Nyní stačí spustit webový prohlížeč a napsat do něj adresu <http://192.168.0.99> a měla by se vám zobrazit úvodní obrazovka. Aby se zobrazil obraz z kamery, je třeba doinstalovat zásuvný modul (plug-in), který slouží pro zobrazení videa a zvuku v internetovém prohlížeči Internet Explorer. V případě, že Váš systém neumožňuje instalaci zásuvných modulů, může být potřeba snížit stupeň zabezpečení Internet Exploreru.

### Nastavení TCP/IP

Otevřete prohlížeč a připojte se k serveru kamery. Nyní je třeba nastavit parametry IP protokolu. V levé části obrazovky vyberte volbu Configuration (nastavení). Dále zvolte Network (síť). Nyní můžete nastavit potřebnou konfiguraci dle vašich požadavků (viz. kapitola „Bezdrátové systémy Wi-fi/Plánování“).

### Nastavení počítače ještě jednou

V předchozím kroku jsme změnili výchozí nastavení AP. Proto je nutné vrátit nastavení počítače na původní hodnoty, odpovídající konfiguraci vaší sítě.

### Základní nastavení kamery

Otevřete prohlížeč a připojte se k serveru kamery. Adresa, kterou do prohlížeče zadáte, už ale bude jiná - bude to IP adresa AP, kterou jste nastavili. Opět se objeví úvodní obrazovka AP a menu. Nastavení je rozděleno do několika nabídek a umožňuje měnit velké množství parametrů. Podrobný popis naleznete v manuálu, které je voně ke stažení na webové stránce <http://www.vivotek.cz>.

### Nastavení WLAN (Wi-fi)

V nabídce Configuration (nastavení)/ Network (síť) nastavte parametry potřebné pro komunikaci v bezdrátové síti Wi-fi. Zejména se jedná o parametry SSID a Channel (kanál).

### Administrace uživatelů

Z důvodu ochrany proti neoprávněnému přístupu je možné nastavit heslo pro administrátora (Root password). Defaultně není nastaveno žádné heslo a přístup k prohlížení i nastavení mají všichni uživatelé, kteří znají IP adresu kamery. Po zadání a potvrzení hesla je nejprve třeba zadat uživatelské jméno *root* a příslušné (nastavené) heslo.

Volbou Add user (přidat uživatele) je možno vytvořit 20 uživatelských účtů.

*Poznámka: Po každé změně nastavení nezapomeňte stisknout tlačítko Uložit (Save) pro uložení nastavení. V opačném případě nedojde k uložení provedených změn.*



# ***Přepět'ové ochrany v elektronických systémech***

*Podklady poskytnuty firmou SALTEK, s.r.o.*

## **OBSAH:**

<b>7 Přepět'ové ochrany v elektronických systémech</b> .....	293
7.1 Zákonné požadavky na elektromagnetickou kompatibilitu .....	293
7.2 Normy související s ochranou proti přepětí a s vf odrušením.....	294
7.3 Základní normy týkající se přepětí.....	294
7.4 Ochrana slaboproudých elektronických systémů před pulsním přepětím .....	298
7.5 Návrh a montáž ochranných prvků.....	301
7.6 Příklady ochrany v poplachových systémech.....	307
7.7 Vzory formulářů pro podporu aplikace ochran.....	311





## 7 Přepětové ochrany v elektronických systémech

### 7.1 Zákoné požadavky na elektromagnetickou kompatibilitu

Přijetím zákona **22/97Sb. o technických požadavcích na výrobky**. Tento zákon byl schválen 24.1.1997 a nabyl účinnosti 1.9.1997. Zákon byl s ohledem na proces sbližování právních předpisů ČR s právními předpisy ES v předvstupním období již několikrát novelizován zákonem 71/2000Sb., 102/2001 Sb., a 205/2002 Sb., 226/2003 Sb. a 277/2003 Sb. Pracovní úplné znění zákona s ustanoveními platnými od 1.5.2004 je k dispozici na internetových stránkách Úřadu pro normalizaci metrologii a státní zkušebnictví ([www.unmz.cz](http://www.unmz.cz)). a Nařízení vlády č. 18/2003 Sb., kterým se stanoví technické požadavky na výrobky z hlediska jejich **elektromagnetické kompatibility** (89/336/EHS). v platném znění se rozšířil problém odolnosti elektronických systémů z roviny technické i do roviny legislativní. Každý výrobce, resp. dovozce, musí ze zákona zajistit dostatečnou odolnost dodávaného výrobku a jeho funkčnost i za přítomnosti rušivých signálů na straně jedné a zajistit, že dodávaný výrobek nebude rušit okolí nad úroveň, kterou povoluje norma, na straně druhé. Cílem zákona a nařízení je zejména:

- 1) Realizovat opatření, která tato rizika eliminují nebo alespoň omezí na minimální nebezpečí, které lze považovat za přijatelné při užívání výrobku vzhledem k odpovídající vysoké úrovni ochrany oprávněného zájmu.
- 2) Zajistit vysokou provozuschopnost zařízení v podmínkách, pro které je určeno.

Oba tyto cíle zajišťují u elektrických a elektronických zařízeních přepětové ochrany a odrušovací filtry. Přepětové ochrany nemají význam pouze pro snížení rizika zničení zařízení, ale mají též podstatný podíl na bezporuchovém chodu zařízení a systémů přesně v duchu definice elektromagnetické kompatibility: zajistit podmínky, aby zařízení v daném prostředí uspokojivě pracovalo. Laciné řešení této problematiky, jak ukazuje praxe, není někdy pouze nedostatečné, ale i nebezpečné.

Problém rušení a odrušení je velice výrazný v průmyslových provozech, kde jsou v těsné blízkosti citlivé řídicí systémy i energetické zdroje rušení. Nejčastějšími zdroji rušivých signálů jsou pulsní přepětí, vznikající při spínání energetických spotřebičů, indukčních zátěží, motorů apod. a vysokofrekvenční rušení, jehož zdrojem jsou především frekvenční měniče dnes běžně používané k napájení motorů. Meze odolnosti i meze rušení stejně jako způsoby měření jsou popsány v harmonizovaných normách, jejichž seznam je přílohou nařízení vlády č.18/2003 Sb. Správné nasazení svodičů přepětí a odrušovacích filtrů vyžaduje nejenom určité znalosti, ale i zkušenosti. Zanedbání této problematiky pak znamená nejenom riziko náhlého kolapsu systému, případně i jeho zničení, ale v případě větších škod i možnost soudního sporu se zákazníkem.

Samo nařízení vlády zavádí kromě jiného tyto definice:

- a) za přístroj se považuje elektrické a elektronické zařízení včetně vybavení a instalací obsahujících elektrické nebo elektronické součásti,
- b) za odolnost se považuje schopnost přístroje nebo systému, ve kterém přístroj pracuje, fungovat bez zhoršení jakosti funkce za přítomnosti elektromagnetického rušení,

- c) za elektromagnetickou kompatibilitu se považuje schopnost přístroje nebo systému, ve kterém přístroj pracuje, fungovat uspokojivě v elektromagnetickém prostředí, aniž by sám přístroj nebo systém způsobovaly nepřipustné elektromagnetické rušení jakéhokoli jiného přístroje v tomto prostředí.

Přístroje (včetně instalací) musejí být podle nařízení provedeny tak, aby pokud jsou řádně udržovány a využívány pro účely, pro které jsou určeny, měly odpovídající odolnost vůči elektromagnetickému rušení, která jim umožňuje provoz v souladu se zamýšleným účelem.

Použitím externích ochranných a odrušovacích prvků se značně zjednoduší návrh, zvýší odolnost systému a zkrátí se doba potřebná na jeho realizaci. Tyto prvky jsou již odzkoušené pro určité úrovně rušení a umožňují bez zásahu do konstrukce použitých přístrojů zvýšit odolnost, resp. snížit míru jejich vyzařování na požadovanou úroveň.

### **7.2 Normy související s ochranou proti přepětí a s vf odrušením**

V České republice se postupně přijímají v rámci harmonizace s technickými předpisy ES také normy EN týkající se EMC (*Electro Magnetic Compatibility*). Elektromagnetická kompatibilita je schopnost elektrických a elektronických zařízení bez vzájemného ovlivňování současně fungovat. Je dána úrovní nežádoucího vyzařování zařízení na jedné straně a odolností proti rušení na straně druhé. Mezi tyto normy patří i normy týkající se přepětí: rozčleňují elektrická zařízení do tříd podle odolnosti a doporučují ochranu proti přepětí v jednotlivých případech i všeobecně. Zatímco třídy odolnosti jsou určeny přesně, technické řešení ochrany proti přepětí stanoveny není. Norma popisující konkrétní technické řešení by rychle zastarala a neumožňovala by technické inovace. Technické řešení ochrany tedy vychází z požadavků normy na úroveň omezení přepětí, z požadavků investora a projektanta na odolnost zařízení používaných v komplexních elektrických a elektronických systémech s požadovanou úrovní bezpečnosti a z ekonomických možností investora – nesmí však být porušen základní princip realizovat opatření, která rizika eliminují, nebo alespoň minimalizují na úroveň, kterou lze považovat za přijatelnou při užívání výrobku vzhledem k odpovídající vysoké úrovni ochrany oprávněného zájmu.

Základní seznam norem ČSN harmonizovaných s NV ČR č. 18/2003 Sb. o elektromagnetické kompatibilitě jsou uvedeny v příloze tohoto nařízení. Harmonizované ČSN, rušení norem, změny i normy nově vydané k příslušným nařízením vlády jsou průběžně vyhlášovány ve Věstníku Úřadu pro normalizaci, metrologii a státní zkušebnictví. Aktuální seznam je k dispozici na webovské stránce Českého normalizačního institutu ([www.csni.cz](http://www.csni.cz)).

### **7.3 Základní normy týkající se přepětí:**

#### **7.3.1 České normy**

##### **ČSN 332000-1 Základní ustanovení pro elektrická zařízení**

Instalaci svodičů přepětí lze zdůvodnit těmito články:

čl. 1.1: Elektrické zařízení jako celek a jeho jednotlivé části (stroje, přístroje, spotřebiče, vodiče a jiné elektrické předměty) musí být navrženo a provedeno hospodárně tak, aby:

- a) nebylo nebezpečné osobám, užitkovým zvířatům a majetku,
- b) neohrožovalo okolí,
- c) nerušilo provoz jiných zařízení, a naopak provozováním jiných zařízení nebylo rušeno,
- d) správně, spolehlivě a hospodárně pracovalo.

čl. 2.3: Všechna elektrická zařízení musí být zabezpečena proti působení možných poruchových stavů, které lze předpokládat (např. přetížení, zkraty a přepětí), přičemž prvky sloužící k tomuto účelu musí být voleny tak, aby při poruchovém stavu elektrického zařízení spolehlivě působily.

Z této normy vyplývá plná odpovědnost projektanta a zřizovatele za správný a spolehlivý provoz elektrického zařízení a jeho povinnost zajistit přiměřenou ochranu před přepětím.

čl. 131.6.2: Osoby, hospodářská zvířata i majetek musí být chráněny před poškozením v důsledku nadměrného napětí, které může vzniknout z jiných příčin (např. atmosférickými jevy, spínacími přepětími, statickou elektřinou).

Norma stanovuje požadavky k ochraně zařízení a elektrických rozvodů proti přepětí.

### **ČSN 341390 Předpisy pro ochranu budov před bleskem**

Tato norma obsahuje několik doporučení vztahujících se k vnitřní ochraně před bleskem. Důležité jsou údaje o pospojování, resp. oddálení kovových konstrukcí od jímacích vedení a svodů. Kvalitní vnější ochrana před bleskem samozřejmě přispívá ke snížení ohrožení elektronických zařízení uvnitř budovy a dnes již nic nebrání jejímu zkvalitnění a doplnění o vnitřní ochranu podle IEC 1024-1 a 1312-1. Pro odhad ohrožení elektronických zařízení v budovách je vhodné doporučení ČES 34.01.95 k ČSN 34 1390, vypracované na základě materiálů IEC-TC 81 k normě IEC 1662. Může být velice důležitým argumentem pro zřízení ochrany.

### **ČSN 332000-4-41 Elektrická zařízení. Bezpečnost. Ochrana před úrazem elektrickým proudem**

Principy pro hlavní a doplňkové pospojování uvádí článek 413.1.2 Pospojování. Průřezy ochranných vodičů a vodičů pospojování pro sítě TN, TT a IT uvádí následující články 413.1.3 a 413.1.6.

### **ČSN 332000-5-54 Výběr a stavba elektrických zařízení. Uzemnění a ochranné vodiče**

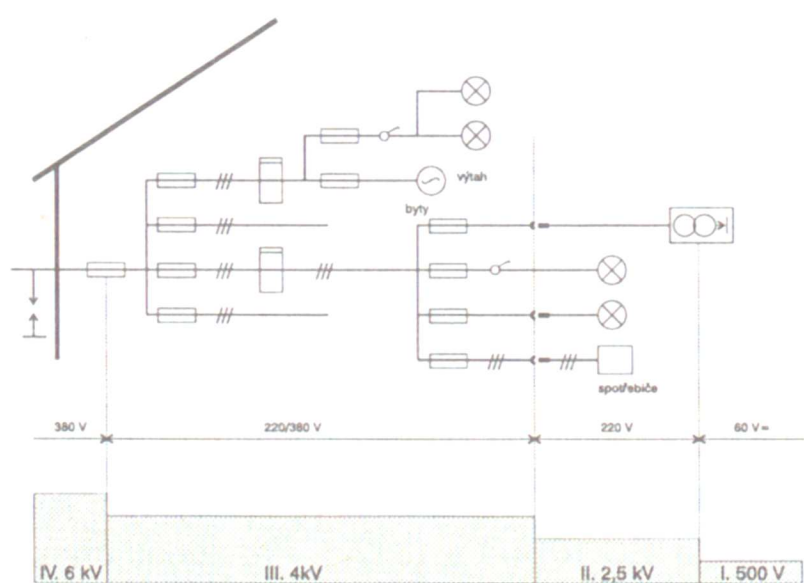
Uvádějí se základní zásady pro zřizování uzemnění, využití náhodných a strojených zemničů a pospojování. V článku 542.5.6 Uzemnění svodičů přepětí přímo uvádí: Pracovní uzemnění svodičů přepětí se spojuje s ochranným uzemněním zařízení, která jsou svodičem přepětí chráněna.

Pro problémy související s elektronickými zařízeními je vhodné řídit se zásadami uvedenými v resortním technickém předpisu (bývalého Federálního ministerstva spojů) TA 116 Uzemnění telekomunikačního zařízení z r. 1991, kde nalezneme mnoho užitečných zásad a zároveň vztah uzemnění a sítí TN-S, které jsou zde předepsány.

### ČSN 330420-1 Koordinace izolace elektrických zařízení nízkého napětí část 1 Zásady, požadavky a zkoušky

(Ekvivalent IEC 664:1980 + Změna A:1981) je velmi důležitým argumentem pro zdůvodnění zapojování ochran před přepětím a rovněž podkladem pro návrh tzv. kaskádové ochrany před přepětím (tj. koordinace požadovaná v IEC 1312-1) v sítích nn.

Obr. 7-1 z ČSN 330420 uvádí příklad výdržných jmenovitých impulsních napětí pro soustavu 230V/400V. Vzhledem k tomu, že systém požadavků na ochrany před přepětím v distribučních sítích nn podle čl. 6 ČSN 38 0810 nezaručuje při přímých úderech blesku do vedení nebo budovy snížení hodnoty přepětí při vstupu do budovy pod hodnotu 6 kV, je prakticky vždy nutné – zejména při instalaci citlivých elektronických zařízení uvnitř budovy – postupně snižovat přepětí na hodnoty bezpečné jak pro izolaci v instalaci, tak pro připojené zařízení.



Obr. 7-1: Příklad jmenovitých impulsních napětí pro soustavu 230V/400V.

### ČSN 334010 Ochrana sdělovacích vedení a zařízení proti přepětí a nadproudu atmosférického původu

Určuje minimální požadavky na jisticí soupravy na konci vnějších sdělovacích vedení. Slouží jako orientační návod pro nutnost nasazení přepět'ových ochran. Podstatně lepším předpisem pro odůvodnění nasazení jemných ochran a ochrany na sítě nn je ovšem technický předpis SPT Telecom TA 9a (1994, doplněk 1 – Ochrana telekomunikačních zařízení v účastnické síti před přepětím). S ohledem na důležitost provozu chráněného zařízení nebo objektu se doporučuje kvalitnější ochrana (v souladu s IEC 1312-1).

### ČSN 332160 Předpisy pro ochranu sdělovacích vedení a zařízení před nebezpečnými vlivy trojfázových vedení vn, vvn a zvn

a obdobná norma pro železniční elektrickou trakci ČSN 342040 mohou posloužit jako podklad pro výpočet nebezpečných vlivů (přepětí) na sdělovacích vedeních zavedených do elektrických stanic nebo v souběhu se silovými vedeními vn až zvn a elektrické

trakce i jako podklad pro zřízení ochrany při překročení dovolených mezí nebezpečných vlivů.

**ČSN 334000 Požadavky na odolnost oznamovacích zařízení proti přepětí a nadproudu**

**ČSN 354870 Ventilové bleskojistky na střídavé napětí**

**ČSN 380810 Použití ochran před přepětím v silových zařízeních**

### 7.3.2 Mezinárodní normy

#### IEC 1024-1 Ochrana budov před bleskem – Obecné zásady

Tato norma definuje některé důležité pojmy:

Vnější ochrana před bleskem – klasická hromosvodní ochrana; norma ovšem požaduje její vyvedení dovnitř budovy pro potřeby potenciálového vyrovnání na ekvipotenciální přípojnicí.

Vnitřní ochrana před bleskem – soubor opatření uvnitř budovy k zabránění nekontrolovanému vzniku přeskoků a průrazů (včetně uvnitř připojených elektrických zařízení).

Potenciálové vyrovnání – součást vnitřní ochrany před bleskem, zahrnující jednak přímé pospojování neživých kovových částí, jednak připojení „živých“ vodičů přes svodiče přepětí. Stejně jako vodiče a svorky i svodiče přepětí v hlavním potenciálovém vyrovnání (v suterénu nebo přizemí budovy na ekvipotenciální přípojnicí) musejí být podle této normy dimenzovány na parametry části bleskového proudu, to znamená, že musejí být zkoušeny vlnou 10/350 ( $\mu\text{s}/\mu\text{s}$ ).

#### IEC 1312-1 Ochrana před elektromagnetickým impulsem způsobeným bleskem (LEMP)

Určuje obecné zásady. Je to nejdůležitější opora při zřizování vnitřní ochrany před bleskem (a přepětím obecně). Opírá se o parametry bleskového výboje definovaného v IEC 1024-1 (uvažuje i následné výboje v kanálu blesku) a zavádí další důležitý pojem, totiž zóny bleskové ochrany (ZBO), umožňující rozčlenění prostoru s chráněnými zařízeními na oblasti s různými nároky na ochranu před LEMP a určující místa ochranného pospojování (vyrovnání potenciálů) na rozhraní zón. Definuje zóny:

LPZ 0A: možnost přímého úderu blesku, netlumený LEMP,

LPZ 0B: ochrana před přímým úderem, avšak též netlumený LEMP,

LPZ 1: vyloučený přímý úder, tlumený LEMP ve srovnání s 0B (v závislosti na stínících opatřeních),

LPZ 2 a další: vyjadřují další útlum LEMP, zavádějí se v souladu s praktickými možnostmi odstínění a vyrovnání potenciálů.

Na všech rozhraních zón bleskové ochrany se musí ošetřit veškeré průniky kovových konstrukcí (včetně elektrických vedení).

V normě je též zdůrazněn požadavek na koordinaci svodičů přepětí v systému zón bleskové ochrany. Z něho prakticky vyplývá požadavek, aby svodič na rozhraní ZBO 0/1 zkracoval vlnu přepětí tak, aby na dalších přechodech mohly být použity svodiče přepětí dimenzované na vlnu 8/20 $\mu\text{s}$ . Při současném stavu technologie výroby svodičů toho lze dosáhnout pouze jiskřišťovými svodiči bleskového proudu.

### **IEC 364, oddíl 534 Elektrické instalace v budovách. Zařízení pro ochranu před přepětím**

Upravuje předpisově nasazení přepět'ových ochran v různých silových instalacích (TN-S, TN-C, IT, TT) a definuje požadavky na kvalitu přepět'ových ochran. Z této normy mj. vyplývá, že přepět'ové ochrany musejí být instalovány tak, že při poruše (a samozřejmě též činnosti) ochrany nesmí dojít k významnému nebezpečí exploze nebo požáru. Přepět'ové ochrany musejí mít vnější nebo zabudované vnitřní ochranné zařízení proti přílišnému zahřátí pouzder. K tomu vysvětlení: Odvádějí-li varistory ve svodičích často přepětí, mění se jejich polykrystalická struktura, a tím stárnou, přičemž se může zvyšovat svodový proud i za provozního napětí z mikroampérů na miliampéry. Tím dochází ke stále většímu zahřívání. Překročí-li zahřátí nebezpečný stupeň, svodič se musí odpojit ochranného okruhu a přerušit i klidový proud. Ani pouzdro ze samozhášitelného materiálu není postačující, poněvadž při vyhřívání zevnitř se plamen nepřeruší. Použití svodičů bez této ochrany je nebezpečné.

### **IEC 1000-4-5 Požadavky na odolnost vůči impulsnímu přepětí (dříve IEC 801-5)**

Stanovuje metodiku zkoušení a vyhodnocování výsledků umožňující na základě úrovní zkoušek charakterizovat odolnost zařízení proti přepětí nejen atmosférického původu.

Pro telekomunikační zařízení je též důležitá znalost, nakolik vyhovují příslušným Doporučením UIT (CCITT) řady K, nebo ČSN 33 4000 Požadavky na odolnost sdělovacích zařízení proti přepětí a nadproudu, která shrnuje požadavky doporučení a aplikuje je v širším měřítku.

### **IEC 61643-1 Přepět'ové ochrany připojené k rozvodům nízkého napětí Část 1: Požadavky na funkčnost a zkušební metody**

Popisuje požadavky a zkušební metody svodičů rozdělených do tříd I, II a III, což odpovídá našemu dělení na 1., 2. a 3. stupeň.

V současné době probíhá proces harmonizace norem ČSN a EN. V průběhu několika let budou do soustavy ČSN přijaty všechny normy EN nebo jejich ekvivalenty.

Nakonec jedno důležité upozornění: IEC 1024-1 konstatuje hned v úvodu, že dnešními prostředky není dosažitelná stoprocentní ochrana před bleskem. Při kvalitně zřízené ochraně však dochází k poškození chráněných systémů nebo svodičů přepětí jen zcela výjimečně a katastrofální škody jsou vyloučeny.

## **7.4 Ochrana slaboproudých elektronických systémů před pulsním přepětím**

### **7.4.1 Odolnost systémů – EMC**

Od 1. 1. 1996 platí v zemích EU Směrnice o elektromagnetické kompatibilitě (EMC) Ta vyžaduje, aby provozované zařízení nebylo zdrojem rušení a bylo odolné proti elektromagnetickým vlivům okolí.

Odolnost je normou IEC 1000-4-4 a IEC 1000-4-5 definována do 4 tříd. V případě integrované ochrany podle IEC 1000-4-5 v nejvyšší třídě se uvažuje se zkušebním proudem 2 kA (ve vlně 8/20), což nepostačuje pro případ přechodu části bleskového proudu

V zařízeních a systémech poskytuje pouze základní odolnost a nepokrývá všechny možné druhy přepětí, zejména ty případy, které jsou spojeny s přímým či vzdáleným úderem blesku. Tento stav je dán zejména ekonomickými důvody.

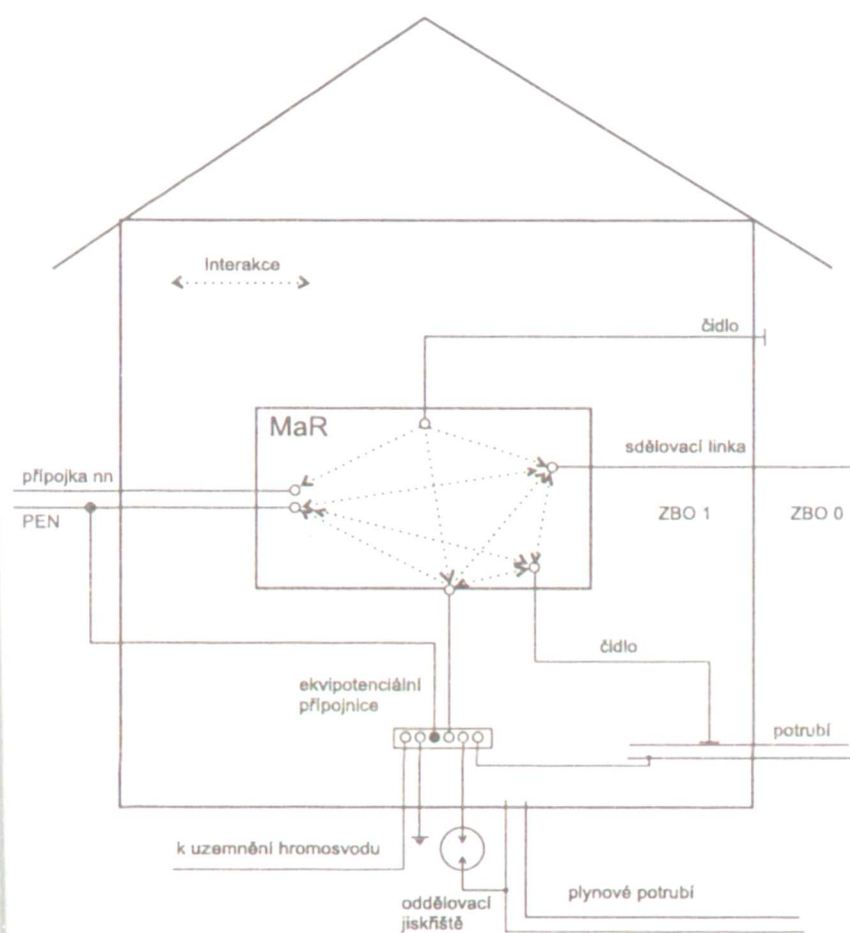
### 7.4.2 Způsoby pronikání přepětových pulsů do zařízení a systémů a interakce jednotlivých částí

Přepětí má vysokofrekvenční charakter a proniká do systémů:

napájecím vedením nn, přes napájecí transformátory a obvody zařízení, přes řídicí, měřicí, datové a telekomunikační vedení a linky čidel, zejména jsou-li umístěny vně budovy nebo na potrubí, kolejišti apod., z hromosvodové soustavy a z uzemňovací soustavy přes všechna vedení opouštějící budovu.

V případě ataku např. systému měření a regulace (MaR) přepětovým pulsem se jednotlivé části nechovají izolovaně, ale vzájemně se ovlivňují, a to i přesto, že nemusí být galvanicky spojeny. Přepětí si vždy hledá cestu směrem k uzemněným částem nebo do dalších vedení představujících vzdálenou zem. Čárkované spoje v Obr. 7-2 představují interakce částí systémů MaR.

Obr 7-2: Pronikání přepětí do zařízení MaR a interakce jednotlivých obvodů.



### 7.4.3 Hlavní zásady řešení ochrany před pulsním přepětím

Vnější ochrana před bleskem – hromosvodová soustava.

Vyrovnání potenciálů na hlavní přípojnici propojení všech vodivých konstrukcí:

- přímá propojení se zřizují tam, kde je to možné: hromosvodová soustava, ochranné uzemnění (PE), vodovod, kovové obaly kabelů, topení apod.,

- nepřímé propojení pomocí oddělovacích jiskřišť vždy tam, kde přímé propojení není možné z bezpečnostních důvodů, např. plynová potrubí nebo funkční katódicky chráněné kovové části,
- nepřímé propojení pomocí tzv. svodičů bleskových proudů a přepětových ochranných všech „živých“ vodičů napájecích i sdělovacích vedení.

### 7.4.4 Prvky a zařízení na ochranu před přepětím ze slaboproudých vedení

#### 7.4.4.1 Výbojková bleskojistka

Výbojková bleskojistka je jiskřiště, ve kterém je prostor pro výboj vyplněn inertním plynem. Toto řešení odstraňuje nevýhody vzduchového nebo uhlíkového jiskřiště umístěním elektrod do hermeticky uzavřeného obalu, čímž je eliminován vliv okolního prostředí. Plynová náplň umožňuje lepší řízení hoření oblouku, a tím omezení následného přepětí vlivem jeho přerušení v okamžiku průchodu proudu nulou. Většinou se používá směs argonu a vodíku, která je plněna pod tlakem kolem 10 kPa. Bleskojistky se vyrábějí od statického zápalného napětí 75 V až do 1500 V, s impulsním proudem až desítky kA ve vlně 8/20. Nevýhodou je dlouhá doba zapálení – řádově 100 ns a poměrně vysoké dynamické zápalné napětí od 600 V do 2500 V. Udržovací napětí oblouku je velmi nízké – řádově desítky. Tím je omezeno přímé použití bleskojistik v napájecích vedeních napětí nad 10 kV. Plynové výbojkové bleskojistky se vyrábějí ve dvou modifikacích se dvěma nebo třemi elektrodami; to podle toho, zda jsou určeny pro ochranu jedné či dvou žil.

#### 7.4.4.2 Varistor

Varistor je napětově závislý odpor s nelineární charakteristikou. Jde o polovodičovou součástku vyráběnou z kysličníků kovů, většinou z oxidu zinku s přísadami vizmutu, kobaltu a dalších kovů. Je schopen svést energeticky bohatší puls než supresorová dioda při stejných rozměrech obou součástek. Odezva je kratší než u bleskojistik – asi 25 ns. Nevýhodou je, že při častém zatížení přepětím nebo působením dlouhotrvajícího přepětí nízké amplitudy se u varistorů může změnit V-A charakteristika a může dojít ke spontánnímu proražení varistoru. Varistory se proto musejí opatřit vhodným předřazeným odporníkem jako ochranným prvkem pro případ jejich přetížení. Varistory se používají zejména k ochraně silových zařízení a přístrojů.

#### 7.4.4.3 Supresorové diody

Supresorové diody jsou rychlé Zenerovy diody zapojené protisměrně (back-to-back), které mají tu vlastnost, že při určitém závěrném napětí se závěrný proud rychle zvětší, takže voltampérová charakteristika těchto diod má v závěrném směru velmi strmý průběh. Pokud přepětí dosáhne průrazného napětí diody, ta se stane vodivou a svede přepětový impuls do země. Této vlastnosti se využívá pro omezování přepětí v chráněných obvodech. Supresorové diody mají velmi rychlou odezvu (řádově ns) na přichozící přepětovou vlnu a jejich V-A charakteristika se časem nemění jako u varistorů. Maximální impulsní proud je od 100 A do několika kA.



## 7.5 Návrh a montáž ochranných prvků

### 7.5.1 Koordinace ochranných prvků

Požadavek na snížení přepětí u slaboproudých vedení bývá velmi striktní. Zbytkové přepětí musíme snížit na úroveň jmenovitého napětí či maximálně jeho násobku. Odolnost ochranných zařízení a rychlost reakce musí být velká. Jednotlivé prvky, které byly doposud uvedeny, samy zpravidla nestačí k dostatečnému zabezpečení zařízení před přepětím. Většinou se používá kombinace více ochranných prvků k dosažení žádané funkce přepětové ochrany. Používají se součástky, které jsou schopny svést velké proudy při pomalé reakci, v kombinaci s takovými, které pracují velmi rychle, ale zase nejsou schopny svést takové množství energie. Tímto řešením se dosahuje omezení přepětových pulsů na hodnotu, která již neohrozí funkci chráněného zařízení. Jako hrubý stupeň se zpravidla používá výbojková bleskojistka. Jemnou ochranu tvoří supresorová dioda, varistor nebo Zenerova dioda.

### 7.5.2 Principy návrhu ochrany

Při návrhu přepětové ochrany systémů MaR, EZS apod. musíme respektovat konkrétní uspořádání systému.

Napájecí vedení, vstupy do datových sítí, sdělovacích vedení, vstupy pro připojení měřicích převodníků a vedení k akčním členům jsou místa, kudy může proniknout přepětí či rušení do výpočetního nebo řídicího systému. Toto nebezpečí se extrémně zvětšuje, jsou-li propojovací linky vedeny mimo budovu, kde je nebezpečí úderu blesku.

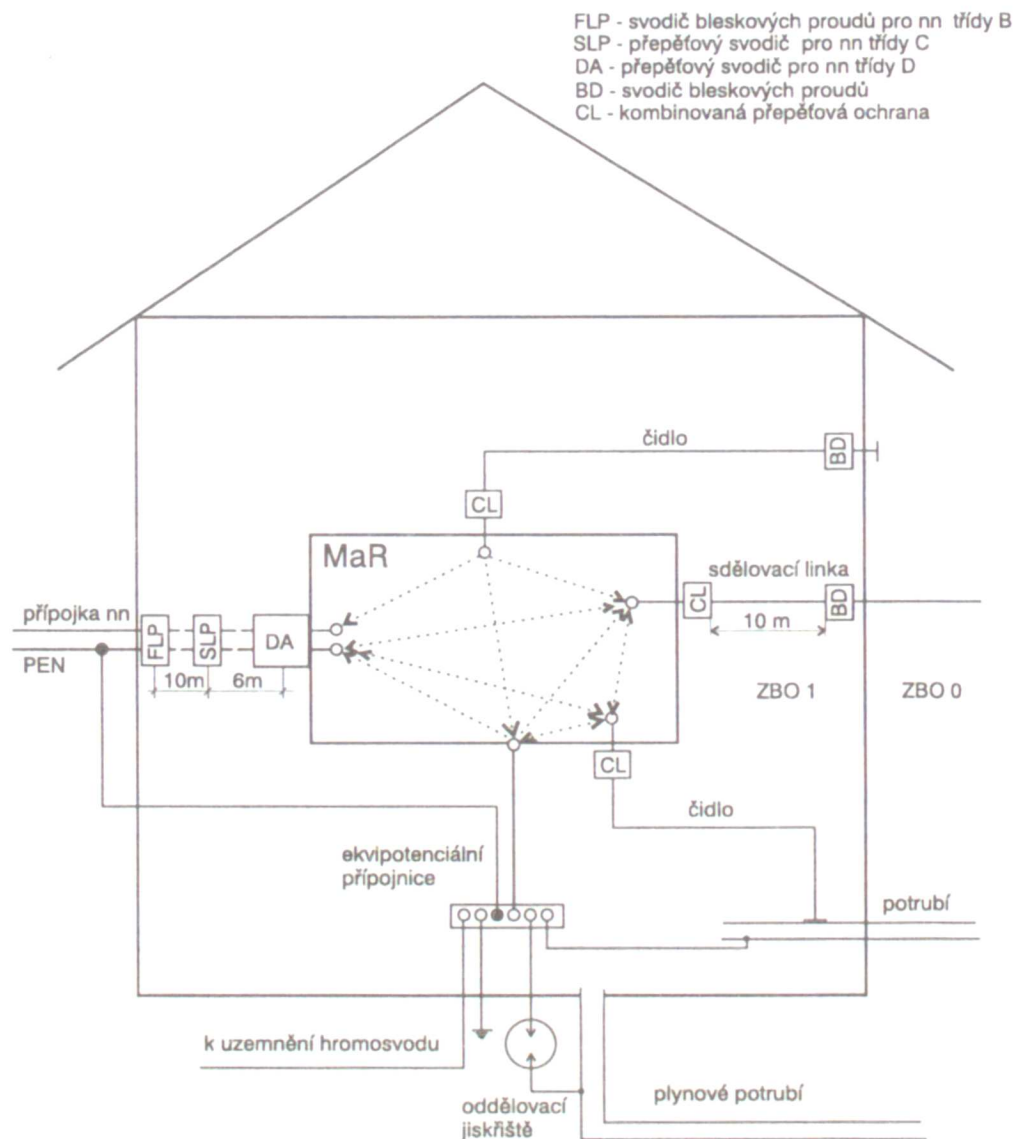
Další nebezpečí představují silná elektromagnetická pole, která vždy obsahují rušivé *vf* složky. V těchto případech je nutné instalovat i vhodné *vf* filtry, popř. kombinace filtru s přepětovou ochranou do napájecích vedení. Potlačení *vf* rušení signálových, měřicích či sdělovacích linek je velmi obtížné. Výskyt těchto jevů obvykle signalizuje špatnou projektovou přípravu či nekvalitní provedení montáže.

Za dostatečnou ochranu linek bývá považováno galvanické oddělení signálu. Je třeba zdůraznit, že galvanické oddělení datové linky má především izolovat vstup linky od souhlasného napětí. Používané integrované obvody však nemají dostatečnou izolační odolnost, která může být snižována nevhodným návrhem plošného spoje, zbytky tavidla, parazitní kapacitou mezi jednotlivými obvody apod. Při příchodu energeticky obsažného pulsu může dojít k přeskoku či oblouku na vývodech, a tím k zavlečení pulsů do dalších obvodů.

### 7.5.3 Hlavní zásady návrhu ochrany proti přepětí:

- kvalitní projektová příprava,
- správně dimenzované propojení s ekvipotenciální přípojnici (pozor na možné indukční smyčky),
- ochrana vedení vstupujícího do objektu v místě vstupu hrubými ochranami – svodiči bleskových proudů (odolnost až 5 kA ve vlně 10/350 $\mu$ s),
- ochrana zařízení MaR instalací 3. stupně přepětových ochranných prvků,
- vyloučení souběhů vedení linek se silovými vedeními,
- volba správného typu svodiče bleskových proudů a přepětové ochrany musí respektovat: jmenovité napětí, proud a maximální frekvenci.

Základní zásadou při ochraně proti přepětí je komplexnost a koordinace ochran (viz Obr. 7-3). Komplexnost znamená, že jsou chráněny všechny vstupy daného zařízení, tj. napájecí i datová a telekomunikační rozhraní. Koordinace ochran znamená, že ochrany s různým ochranným účinkem se řadí za sebou na vedení tak, aby zařízení bylo bezpečně ochráněno. Koordinaci přepětových ochran v napájecím vedení nn se zabývá např. norma ČSN 330420-1.



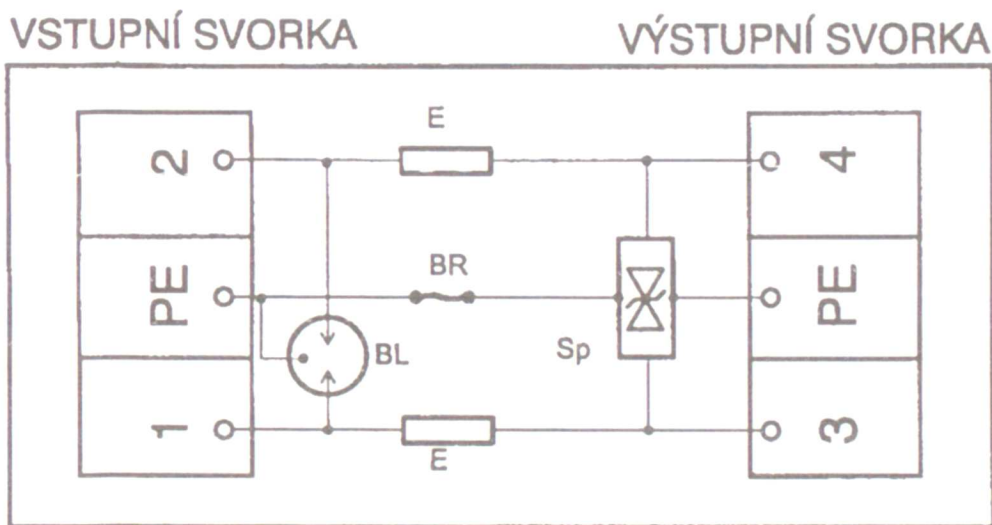
Obr. 7-3: Princip ochrany MaR před bleskovými proudy a přepětím.

*Poznámka – V další části textu vycházíme při vysvětlování zásad návrhu ochrany pro náročnost ze sortimentu českého výrobce – firmy SALTEK. Ekvivalentní prvky lze nalézt i v sortimentu dalších firem působících v této oblasti na našem trhu.*

Svodiče přepětí SALTEK pro sdělovací vedení jsou optimalizovány pro použití při ochraně napájecích vedení, datových a měřicích linek, komunikačních rozhraní proti pulsnímu přepětí, účinkům blesku a atmosférických výbojů i průmyslovému rušení. Použité velmi výkonné prvky zaručují eliminaci opakovaných přepětových pulsů až 10 kA

(žila -zem), resp. 20kA (žila-žila). Jemná ochrana zajišťuje další snížení přepět'ové vlny až na úroveň blízkou jmenovitému napětí.

Ochranný účinek je zajištěn hrubou (Bl - bleskojistka) a jemnou (Sp - supresor) přepět'ovou ochranou. Použity jsou dva typy aktivních prvků – trojpólová neradioaktivní bleskojistka a omezovací velmi rychlé diody (obr. 7-4). Trojpólová bleskojistka zajišťuje hrubou ochranu, diody s extrémně krátkou dobou odezvy (pod 1 ns) ochranu jemnou. Modul chrání zařízení jak proti příčnému přepětí (mezi vodiči), tak i vůči podélnému mezi vodiči a zemí.



Obr. 7-4: Zapojení přepět'ové ochrany typové řady CL-xx.

Hrubá i jemná přepět'ová ochrana jsou vzájemně provázány ohmickou nebo indukční vazební impedancí (E). Použití ohmické vazby zvýší impedanci chráněného vedení asi o 6,8 Ω (typy označené CL-xx/R). Max. proud ve smyčce je omezen na 60 mA. Pokud by zvýšení impedance bylo na závadu, lze místo sériového odporu použít moduly vybavené tlumivkou. V tomto případě se zvýší impedance vedení asi o 1 Ω; jedná se o typy s příponou L – max. proud ve smyčce 370 mA, nebo L2 – max. proud ve smyčce 2 A, resp. L5 – max. 5 A. Jeden modul chrání vždy jeden pár vodičů linky.

Moduly jsou vyráběny v zapojení se společnou ochrannou PE a signálovou GND zemí. Je-li signálová (číslicová) zem GND napájení „plovoucí“, tj. oddělená od ochranné země PE, je možné propojení zemí odstranit. Této vlastnosti lze s výhodou využít při ochraně vedení linek, kde není ochranná a signálová zem propojena.

Svodiče bleskových proudů SALTEK pro datová vedení jsou vyráběny ve dvou typových řadách BD pro běžné linky a kabely a FX pro koaxiální vedení s konektory BNC, F, IEC. Svodiče obsahují speciálně upravené jiskřiště schopné svádět parciální bleskové proudy a jsou určeny pro montáž na rozhraní LPZ 0<sub>B</sub> a LPZ 1, tj. na vstup venkovních vedení do objektů.

Datové ochrany firmy SALTEK typu CL, DM, DL, VL jsou dvoustupňové s menovitým svedeným proudem 10 kA (8/20). Tato hodnota postačuje pro většinu aplikací. Pokud je však dané vedení vedeno venkovním prostředím (vzduchem, po fasádě apod.), resp. zemním kabelem, doporučujeme předřadit výše uvedeným ochranám ještě hrubou ochranu – svodič bleskových proudů – typu BD-xx, resp. FX-xx dimenzovanou na svedený bleskový proud 5 kA (10/350μs), resp. 20kA (8/20μs). Doporučujeme osadit tyto svodiče bleskových proudů těsně za vstupem venkovního vedení, resp. kabelu, do budovy.

Řazením ochran typu BD, resp. FX a typu CL, DM, DL, resp. VL, vytvoříme alternativu k 3stupňové ochraně rozvodů nn:

a) 1. stupeň – svodič bleskových proudů SALTEK typ BD, resp.FX pro koaxiální vedení,

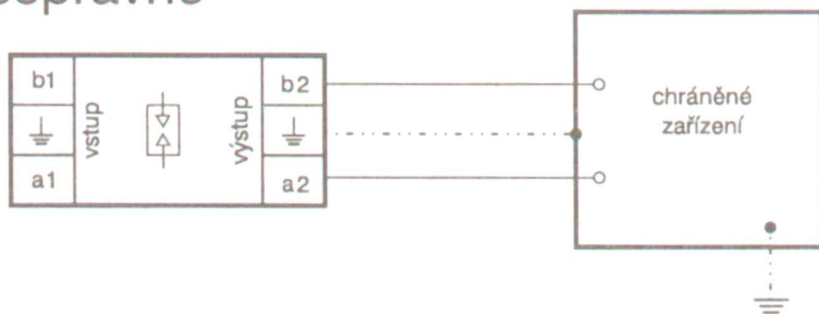
b) 2. a 3. stupeň integrovaný do jednoho svodiče SALTEK typu CL-xx, DM-xx, VL-xx, a DL-xx.

Minimální vzdálenost mezi tzv. hrubou ochranou (typ BD-xx) a tzv. kombinovanou střední a jemnou ochranou (typy CL, DM apod.) by měla být 5 až 10 m. V případě, že to nejde zajistit, musí být koordinace ochran zajištěna jiným způsobem – použitím svodiče bleskových proudů se zabudovanou vazbovou impedancí.

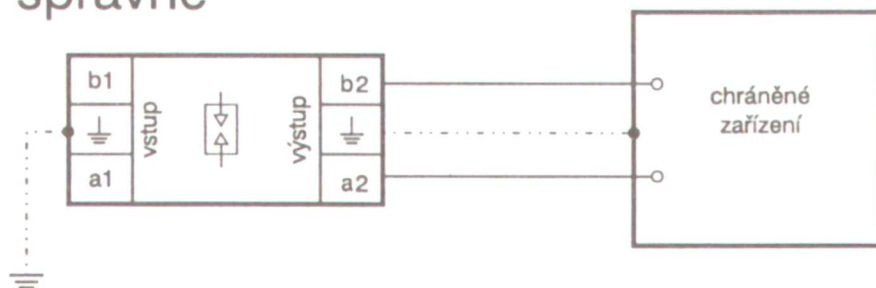
Podmínkou správné funkce přepětové ochrany je správné uzemnění ochran. Svorku označenou PE je nutné připojit na vhodný zemnicí bod žlutozeleným vodičem o průřezu alespoň 2,5 mm<sup>2</sup>. Pro uzemnění ochranných prvků se používá ochranná země chráněného zařízení, která musí vyhovovat platným normám ČSN. V případě, že chráněné zařízení není připojeno k síti nn, použije se jiné uzemnění vyhovující předpisům platných ČSN spojené s kosterou (stíněním apod.) chráněného zařízení. Zemní odpor tohoto uzemnění by neměl překročit 5 Ω, deklarované parametry ochranných prvků jsou však splněny při hodnotách nepřesahujících 2 Ω.

Vstupní a výstupní svorky ochranných modulů jsou určeny pro připojení vodičů o průřezu 0,35 až 2,5 mm<sup>2</sup>. Svorku PE připojte na ochrannou zemi chráněného zařízení pomocí žlutozeleného vodiče o průřezu min. 2,5 mm<sup>2</sup>. Správný a nesprávný způsob uzemnění ochrany a chráněného zařízení je znázorněn na Obr. 7-5.

nesprávně

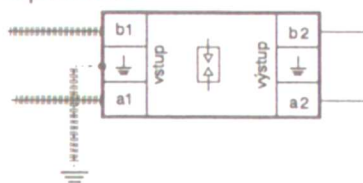


správně



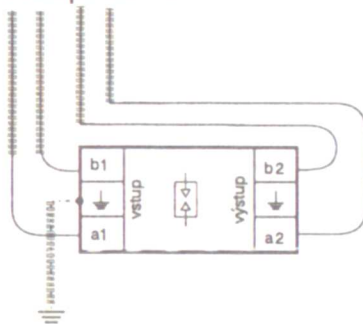
Obr. 7-5: Způsoby uzemnění přepětových ochran.

správně

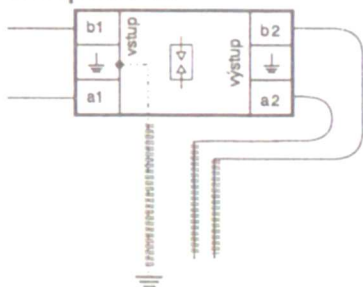


Obr. 7-6: Vazby mezi vstupním a výstupním vedením a uzemněním.

nesprávně



nesprávně



Při instalaci dbáme na to, aby neošetřené vstupní vedení bylo co nejvíce oddáleno od ošetřeného (čistého) výstupního vedení (obr. 7-6).

Způsob uzemnění stínění v sítích se stíněným kabelem není instalací ochranných prvků ovlivněn. Neuzemněný konec stínění však musí být ošetřen proti účinkům pulsního přepětí pomocí bleskojistky (SALTEK DS-B90). U ochran s připojením pomocí konektoru (typy VL, DL apod.) je toto ošetření provedeno – stínění je proti ochranné zemi chráněno plnohodnotnou přepět'ovou ochranou.

Ochranné moduly umísťujeme zásadně tak, aby výstupní vedení k chráněnému zařízení bylo co nejkratší. Zásadně dodržujte směr zapojení ochrany: vstup – ke straně vedení, výstup – k chráněnému zařízení. V případě nedodržení správné orientace přepět'ové ochrany neplní deklarované parametry a může dojít k jejich zničení.

#### 7.5.4 Výběr ochrany podle parametrů chráněného rozhraní

Jmenovité napětí – amplituda přenášeného signálu – nesmí převyšovat jmenovité napětí ochranného prvku o víc než o cca 10%; v opačném případě může dojít k omezení užitečného signálu, případně u tvrdých zdrojů i k poškození ochranného prvku. Volíme tedy co nejmenší jmenovité napětí, při kterém ještě nedochází k omezení užitečného signálu. Zajistíme tak minimální zbytkové přepětí na vstupu chráněného zařízení.

Maximální proud ve smyčce nesmí trvale překračovat hodnotu uvedenou v tabulce technických parametrů.

Mezní frekvence – pokud frekvence přenášeného signálu překročí mezní frekvenci použitého ochranného prvku, dochází k nadměrnému útlumu přenášeného signálu (>2 dB).

Tabulka 7-1: Doporučené typy ochran s ohledem na rozhraní

Typ rozhraní	Doporučený typ ochrany
proudová smyčka 0 - 20 mA, resp. 4 - 20 mA, zdroj 24 V	CL-24/nR(nL), DM-24/nR(nL)
proudová smyčka 0 - 20 mA, resp. 4 - 20 mA, zdroj 48 V	CL-48/nR(nL), DM-48/nR(nL)
rozhraní RS 232	CL-12/nR, DM-12/nR
rozhraní RS 485	CL-6/nR, DM-6/nR
rozhraní RS 422	CL-6/nR, DM-6/nR
100baseT - ethernet kabel UTP	DL-100 ETH, DL-RACK PANEL
čidla a vstupy ústředěn EZS a EPS	CL-xx/nR, DM-xx/nR
rozvody napájení EZS a EPS	CL-xx/nL2 (L5), DM-xx/nL2, DP-xx
telefonní linka, ADSL	DL-TLF, DM240/1RDJ
malá telefonní ústředna	DM-240/n
Střední a velká telefonní ústředna	CLSA-TLF
videopřenos	VL VIDEO BNC, VL B75 F/F
videopřenos + napájení	VL xx BNC SV, VL B75 DJ
anténní systémy	FX-xx, SX-xx, HX-xx
Bezdrátový internet	ZX xx
Měření a regulace	CLSA xx

### 7.5.5 Bezpečnostní opatření při montáži ochran

Instalaci přepětových ochran smí provádět pouze osoba s příslušnou kvalifikací. Při instalaci prvku je nutné dodržet platné technické normy ČSN.

Používání ochran je přípustné pouze v rozsahu podmínek uvedených v montážním návodu. Při použití ochran mimo uvedených podmínek (překročení nominálního napětí, nominálního proudu apod.), resp. při zatížení nad uvedený rámec (např. při přímém zásahu blesku do vedení), může dojít ke zničení ochrany, případně i připojeného zařízení.

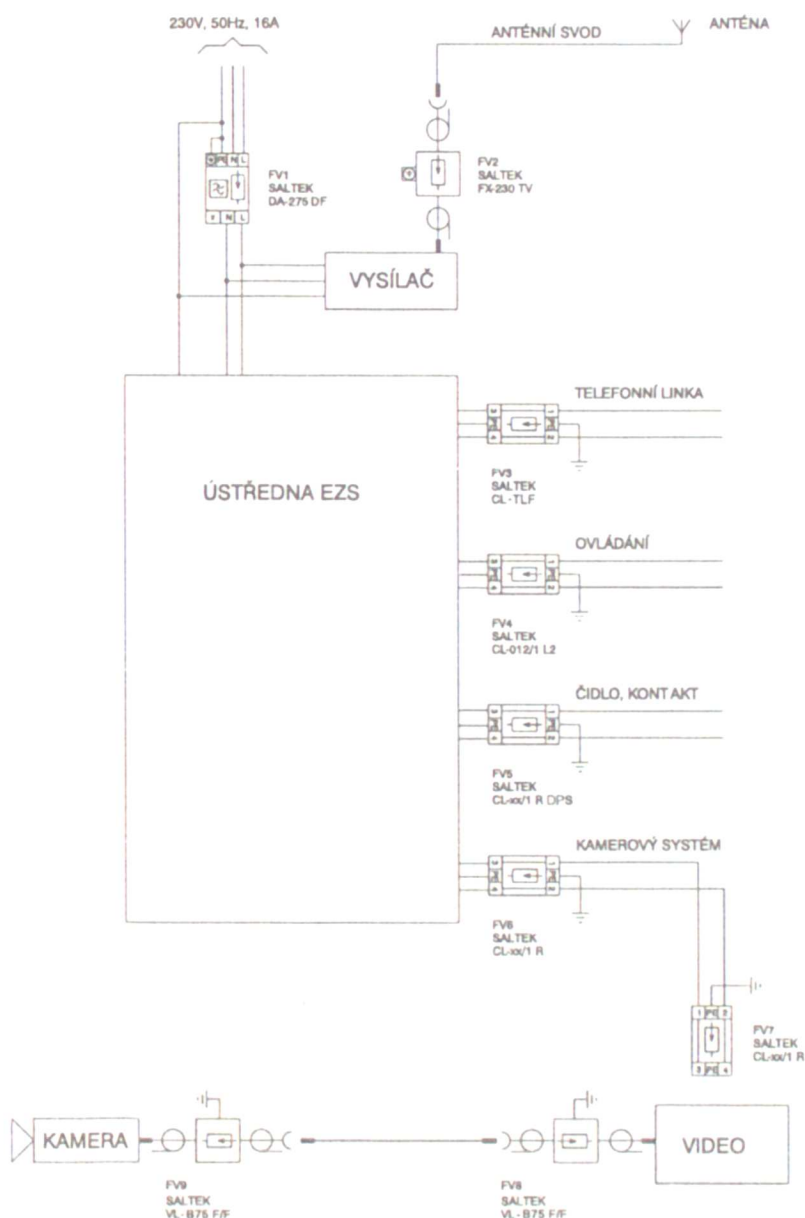
Nikdy neinstalujte mechanicky poškozený ochranný prvek. Zašlete jej k revizi a opravě výrobci. Prvek nikdy neotvírejte. Při jakémkoliv zásahu do prvku může dojít k jeho zničení. Zasahování do prvku vede ke ztrátě záruky.

### 7.5.6 Údržba ochran

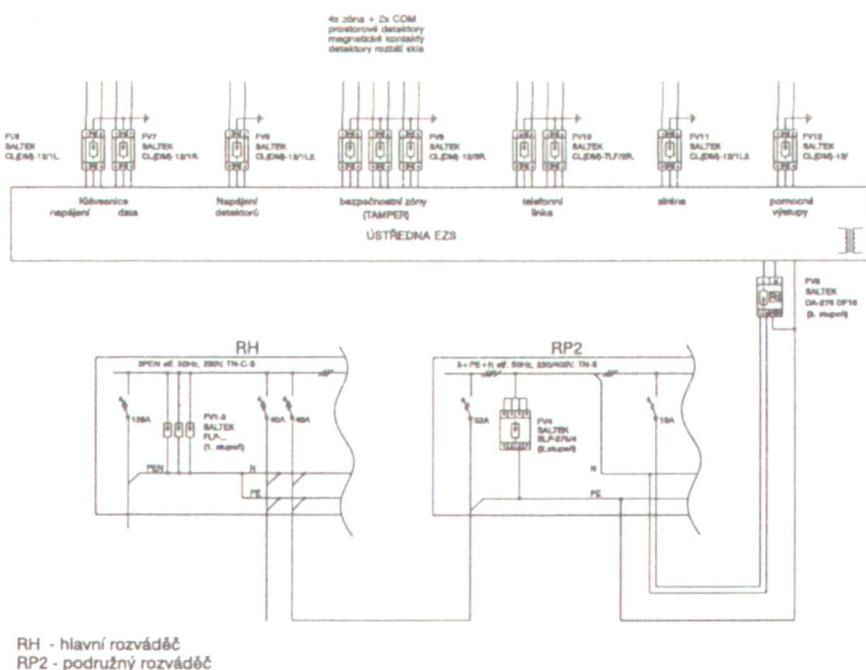
Prvky na ochranu proti přepětí jsou bezúdržbová zařízení. Pokud nedojde k jejich přetížení, dosahuje jejich životnost 10 až 20 let. Při pravidelných kontrolách (revizích) zařízení kontrolujeme celistvost a vodivost zemnicích vodičů a podle typu provozu a použitých vodičů i utažení šroubů ve svorkovnicích.

Poškození ochrany při přetížení se projeví zpravidla jako zkrat, někdy i jako přerušení vedení. Poškozená ochrana se nikdy neopravuje, ale vyměňuje se za novou. Autorizované servisní organizace mohou na vyžádání provádět revizi funkčnosti ochran periodicky.

7.6 Příklady ochrany v poplachových systémech



Obr. 7-7: Schematické znázornění umístění ochrany v systému EZS a CCTV.



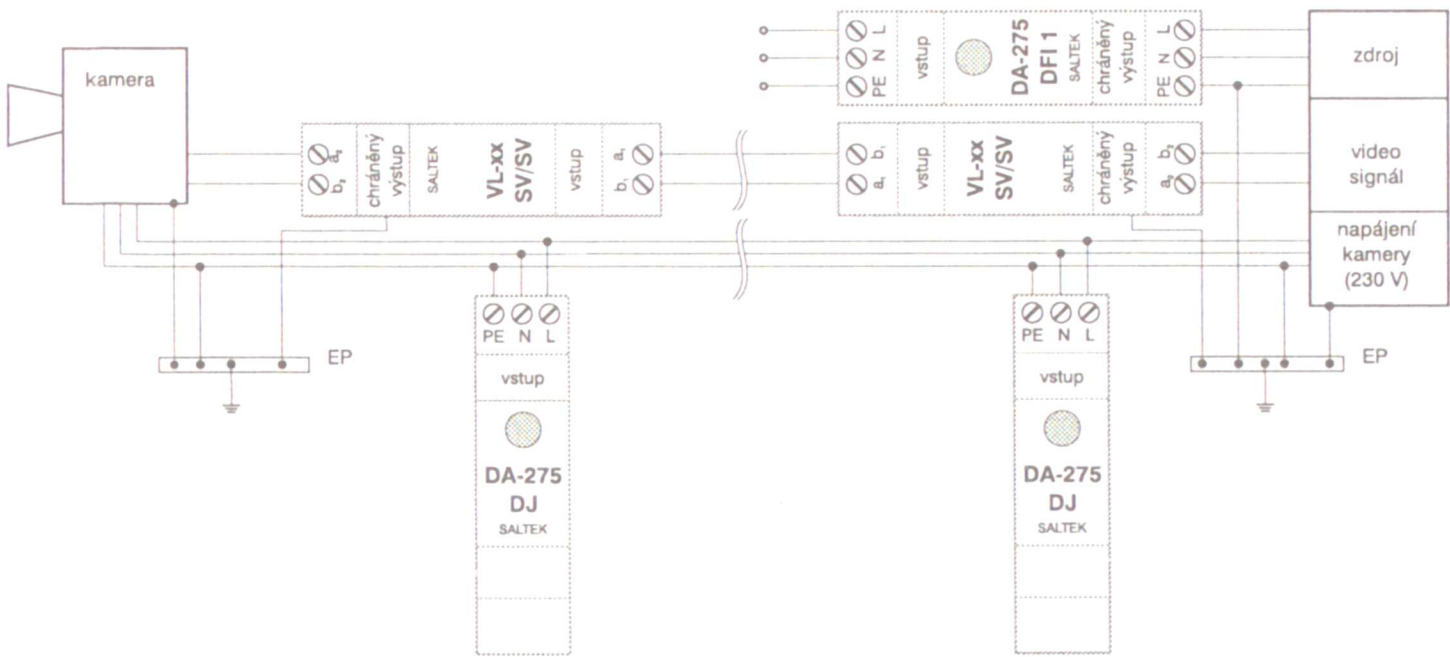
Elektrická zabezpečovací signalizace  
standardní poplachová ústředna (DSC spot)

RH - hlavní rozváděč  
RP2 - podružný rozváděč

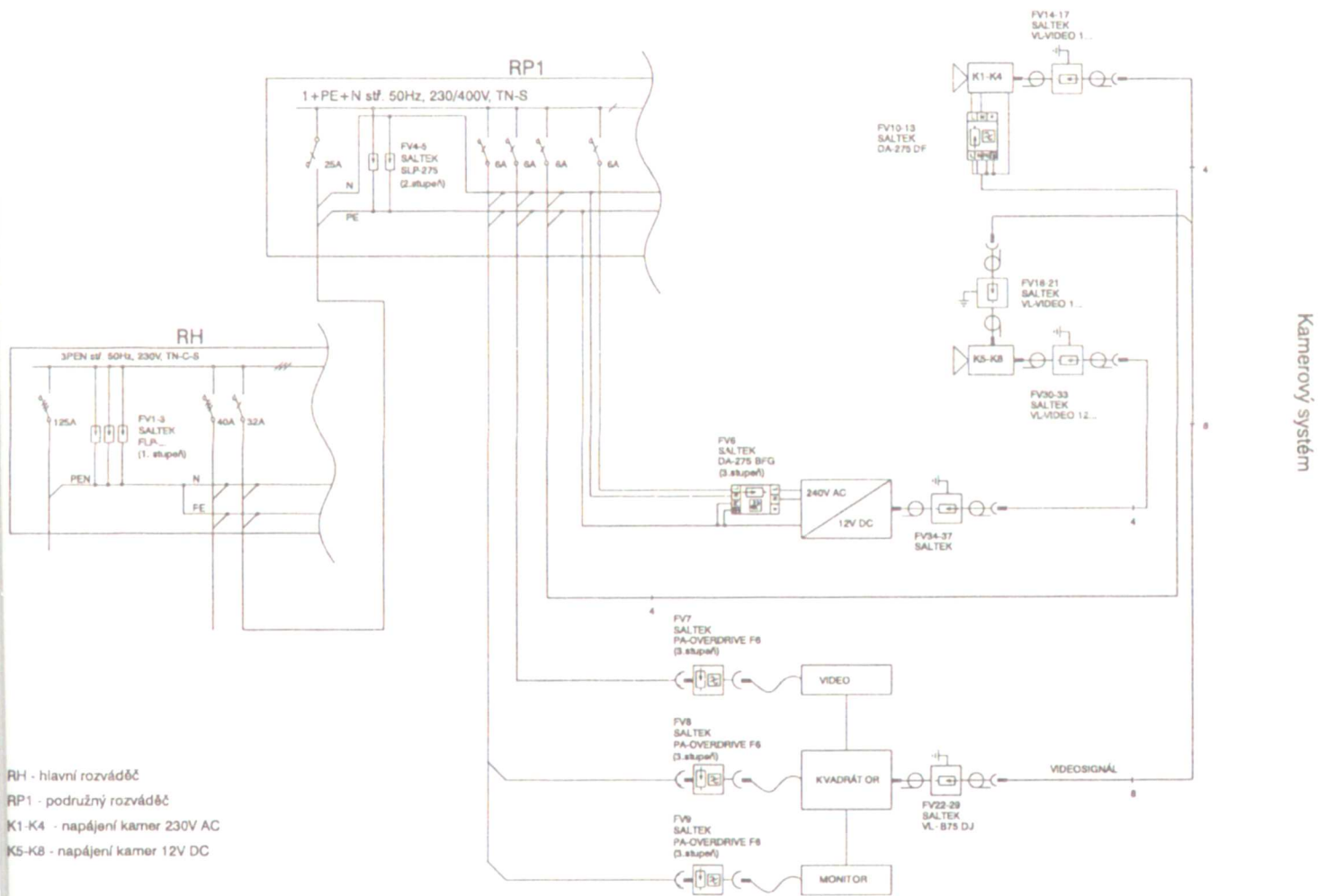
Obr. 7-8: Příklad aplikace ochrany v systému s malou smyčkovou ústřednou EZS.





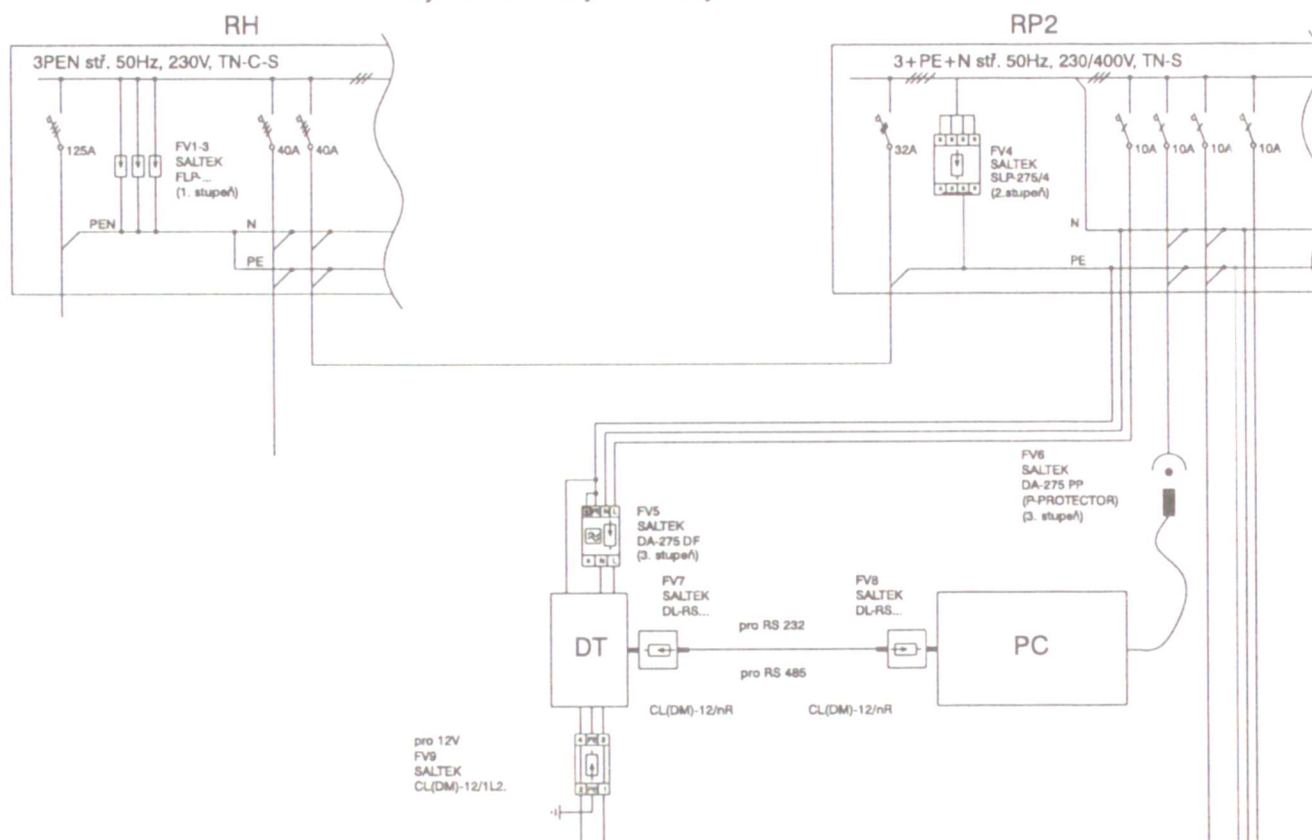


Obr. 7-11: Příklad aplikace ochrany na kamerovém stanovišti CCTV.

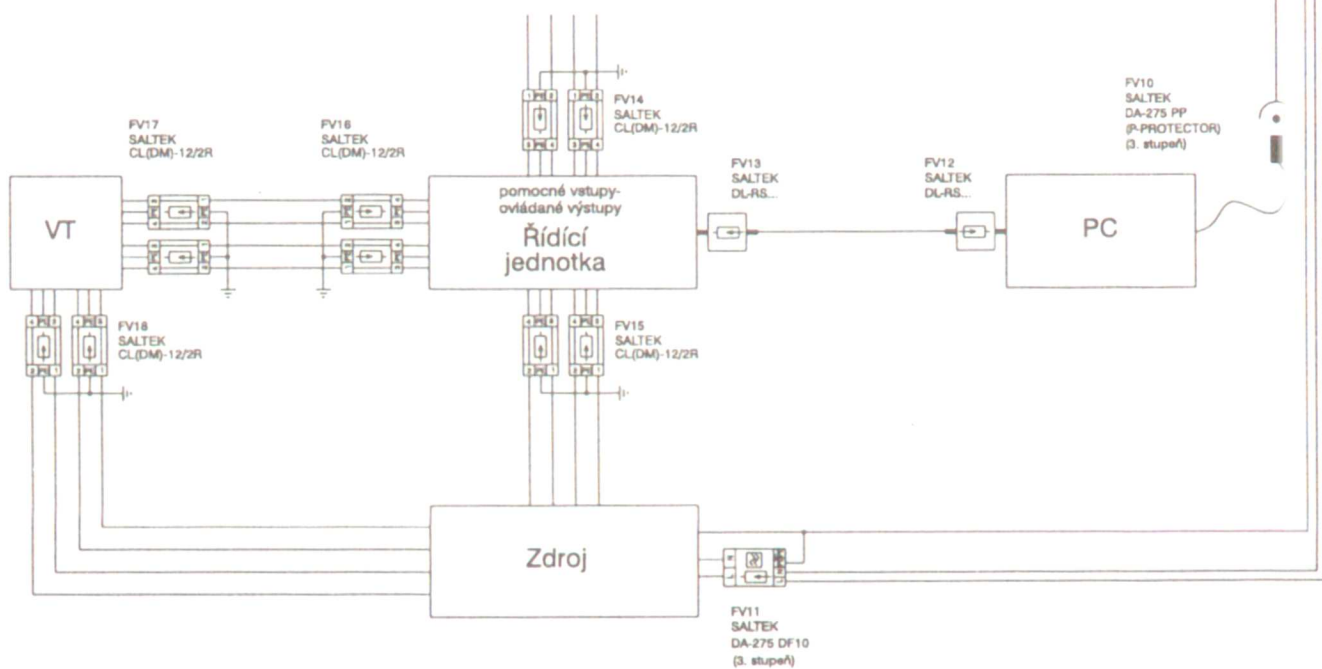


Obr. 7-12: Příklad aplikace ochrany v systému CCTV.

System kontroly docházky



System kontroly vstupu



- RH - hlavní rozváděč
- RP2 - podružný rozváděč
- DT - docházkový terminál
- VT - vstupní terminál

Obr. 7-13: Příklad aplikace ochran v přístupovém/docházkovém systému.

## 7.7 Vzory formulářů pro podporu aplikace ochran

### Doporučení revizního technika

Příloha k revizní zprávě č. .... z .....

Doporučení revizního technika do - periodické - výchozí revize

Doporučuji provést ochranu před účinky nadměrného napětí podle ČSN 33 2000-1-131.6.2 (osoby, hospodářská zvířata i majetek musí být chráněny před poškozením v důsledku nadměrného napětí, které může vzniknout z jiných příčin, např. atmosférickými jevy, spínacími přepětími, statickou elektřinou) a pro použití elektrických předmětů z hlediska kategorie přepětí podle ČSN 330420/2.2 v tomto rozsahu:

Ochranu silových elektrických rozvodů nízkého napětí včetně následujících instalovaných citlivých elektronických zařízení:

- počítače a tiskárny
- záložní zdroje pro počítače
- kopírky
- faxy
- telefonní přístroje
- pokladny
- televizory, videorekordéry a přehrávače
- telefonní ústředny
- ústředny EZS a EPS

Ochranu slaboproudých rozvodů:

- datové rozvody
- počítačové sítě
- telefonní rozvody státních i vnitřních linek
- rozvody EZS
- rozvody EPS
- anténní, satelitní a televizní rozvody

V ..... dne .....

Komplexní ochranu a její prvky před pulzním přepětím projektuje, dodává, instaluje, a technickou podporu zprostředkovává firma:

**Příloha k projektu**

Příloha k projektu č. ....

Věc: Zápis projektanta a investora (objednavatele) o projednání aplikace přepětové ochrany do projektové dokumentace elektro arch. č. ....

Projektant : .....

Investor : .....  
(objednavatel)

Objekt : .....

Investor (objednavatel) byl na základě jednání s projektantem seznámen s principem a účelností aplikace ochrany před účinky nadměrného napětí podle ČSN 33 20 00 -1-131.6.2 (osoby a hospodářská zvířata i majetek musí být chráněny před poškozením v důsledku nadměrného napětí, které může vzniknout z jiných příčin, např. atmosférickými jevy, spínacími přepětími, statickou elektřinou a použitím elektrických předmětů z hlediska kategorie přepětí podle ČSN 3304 20/2.2)

Přepětová ochrana zajišťuje ochranu elektrických rozvodů, připojených citlivých elektronických zařízení, např. počítačů, tiskáren, kopírek, faxů, drahých telefonních přístrojů, pokladen, záložních zdrojů pro počítače, televizorů, videomagnetofonů, telefonních ústředen, ústředen EPS, ústředen EZS.

Dále zajišťuje ochranu slaboproudých rozvodů: např. datové rozvody, počítačové sítě, telefonní rozvody, rozvody EPS a EZS, anténní, televizní a satelitní rozvody.

Investor prohlašuje, že byl seznámen a upozorněn na možné nebezpečí při pomnutí aplikace této ochrany. Případné hmotné škody, které vznikly vlivem a následkem přepětí, nese na své vlastní nebezpečí a náklady.

Vyjádření investora :

Požaduji návrh ochrany před pulsním přepětím v tomto rozsahu:

.....  
.....

Nepožaduji návrh ochrany před pulsním přepětím z důvodu:

.....

Podpis investora: .....

Podpis projektanta: .....

V ..... dne: .....

Komplexní ochranu a její prvky před účinky pulsního přepětí projektuje, dodává, instaluje, a technickou podporu zprostředkovává firma :

Vzor 2: Příloha k projektu

**Použitá literatura:**

1. Zákon 22/1997 Sb., o technických požadavcích na výrobky
2. Nařízení vlády 18/2003 Sb., kterým se stanoví technické požadavky na výrobky z hlediska elektromagnetické kompatibility
3. Aplikační brožura a katalog firmy SALTEK, s. r. o.
4. Dvořáček, K. – Csirik, V.: Projektování elektrických zařízení, Praha, IN-EL, 1999

# Technologie pro Váš úspěch



360,-  
Kč 420,00