BPC-ZSY 2022

Otázky na zkoušku

Informační bezpečnost, FEKT VUT

https://github.com/VUT-FEKT-IBE/FEKT.tex

Bořax

4. ledna 2023
FEKT.tex 2.0

Obsah

1 Systémy PZS 1

2 Předmětové a překážkové detektory PZS 4

3 Objemové a hraniční detektory PZS 10

4 Dohledové videosystémy 14

5 Systémy EPS a hlásiče EPS 18

6 Systémy EKV 23

7 Biometrické přístupové systémy 28

8 Systémy na ochranu zboží 32

9 Elektronické platební systémy 36

10 Ochrany digitálních děl 40

1 Systémy PZS

- Poplachové zabezpečovací systémy
- Elektronický systém určený k detekci a signalizaci vzniku nežádoucích událostí
- Jiné označení toho stejného – Elektronická zabezpečovací signalizace
- Definice podle ČSN EN 50131: „poplachový systém pro detekci a indikaci přítomnosti, vstupu nebo pokusu o vstup narušitele do střežených objektů“
- Další funkce podle normy závisí pouze na detektorech
- „Intruder Alarm System“, „Burglar Alarm“, „Security Alarm“

1.1 Účel PZS

- Detekce a signalizace vzniku **nežádoucích událostí**
  - Incidenty
  - Vniknutí osoby do kontrolované oblasti
  - Uniknutí osoby z kontrolované oblasti
  - Neoprávněná manipulace se střeženým předmětem
  - Vznik nebezpečného prostředí v kontrolované oblasti (zatopení, únik plynu)
  - Vznik požáru (to ale dělají hlavně EPS)
  - Vznik tísňové situace
- Provádění **akcí**
  - Řízení přístupu
  - aktivace jiných zařízení a systémů (domácí automatizace – topení, světla)

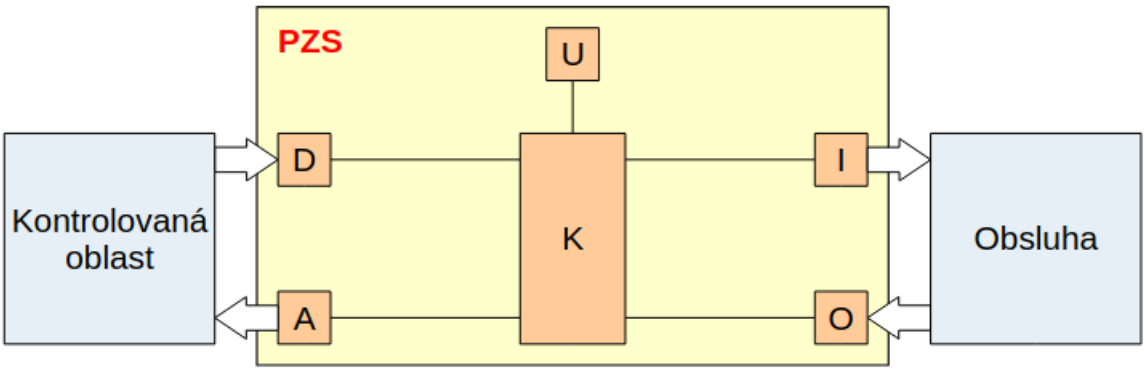
1.2 Architektura PZS

- Ústředna – řídí systém (V diagramu 1 označená U)
- Detektory – detekce incidentů, hlášení ústředně (D)
- Informační zařízení – informace pro obsluhu (I)
- Ovládací zařízení – obsluha skrze ně ovládá systém (O)
- Akční zařízení – vykonávají určené akce v kontrolované oblasti (A)
- Komunikační systém – zajišťuje komunikaci mezi prvky systému (K)

1.3 Prvky PZS

1.3.1 Detektory

- Podávají ústředně hlášení. Typy hlášení:
  - Klid – v dosahu detektoru nenastal incident
  - Poplach – incident byl zjištěn detektorem
  - Sabotáž – neoprávněný pokus o úpravu detektoru



Obrázek 1: Architektura PZS

1.3.2 Ústředna

- Oznamuje hlášení *poplach* a *sabotáž* pomocí informačních zařízení
- Aktivuje akční zařízení, která mají být při poplachu nebo sabotáži daného detektoru aktivována (např. zamlžovací zařízení)
- Obsluha ji řídí pomocí ovládacích zařízení
- Základní stavy:
  - Zastřeženo – oznamován je jak poplach, tak i sabotáž všech detektorů
  - Odstřeženo – jsou ignorovány hlášení o vniknutí. Ostatní typy poplachu jsou oznamovány (požár, tíseň). Oznamována je i sabotáž všech detektorů
- Prakticky řídící počítače, periferie jsou informační, ovládací a akční zařízení
- Zálohované napájení dobíjeným akumulátorem
- Rozhraní k perifériím:
  - Svorky smyček – smyčkové detektory
  - Svorky sběrnice – klávesnice, sběrnicová zařízení
  - Svorky výstupů – informační a akční zařízení s připojením proudovou smyčkou
  - Rádiový modul – bezdrátová zařízení
  - USB rozhraní – správní počítač
  - GSM modul – GSM síť
  - RJ-45 – IP síť

1.3.3 Detektory

- Detekce incidentů
- Měří fyzikální jevy, které doprovázejí incidenty (příznaky)
- Klasifikace
  - Intruzní – detekce neoprávněné aktivity osob, povinné v PZS, měří mechanické síly a elektromagnetiscké jevy
  - Požární – detekce požárů

- Tísňové – detekce tísňové situace
- Substanční – detekce nežádoucí látky

1.3.4 Informační zařízení

- Prezentace informací
- Stav v kontrolované oblast + stav systému
- Obvykle autonomní napájení, nezávislé na ústředně
- Nejstarší: signalizační zařízení (siréna, maják)
  - Komunikace po sběrnici (aktivační příkaz s adresou zařízení) nebo proudové smyčce (klidový proud, jeho zánik -> spuštění signalizace)
- Nové: datová koncová zařízení
  - Počítač, smartphone
  - Vyžadují komunikační rozhraní ústředny (RJ-45, Wi-Fi, GSM...)
  - Aktivace: zasláním dat s adresou zařízení
  - Reprezentace informace na displeji, akustické upozornění

1.3.5 Ovládací zařízení PZS

- Ovládací klávesnice
  - Sběrnice (např. RS-232)
  - Numerická klávesnice, LCD displej nebo dotykový displej
  - Zadávání číselných kódů
- Datová zařízení (počítač, smartphone)

1.3.6 Akční zařízení

- Ovládání proudovými smyčkami (spínání, rozepínání relé)
- Domácí automatizace (topení, světla, vrata garáže...)
- Světla – rozsvítí se, odradí útočníka
- Zamlžovací zařízení – rychle zamlží prostor, útočník ztratí orientaci, ale aktivuje kouřové detektory

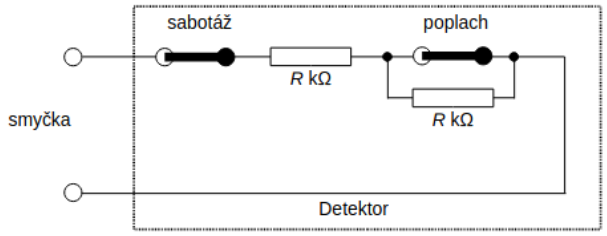
1.4 Typy systémů PZS podle komunikace

- Kabelové – vyšší spolehlivost, nízká variabilita rozmístění čidel, vysoká cena rozvodů
  - Smyčkové – typy:
    - Jednoduchá smyčka
    - Jednoduše vyvážená smyčka
    - Dvojitě vyvážená smyčka
    - Trojitě vyvážená smyčka

- Sběrnicové
  - Obvykle standard RS-485 (čtyřžilový kabel)
  - Protokol typu dotaz-odpověď (dotazy od ústředny)
  - Jednodušší kabeláž, lze po sběrnici připojit vše, dražší a komplikovanější zařízení, maximální počet zařízení na sběrnici (typicky 100 ks)
- Kombinované
  - Expandery – sběrnicí spojené s ústřednou, smyčkou s detektory
- Rádiové
  - Frekvence: 434, 868 nebo 2400 MHz
  - Poloduplexní komunikace
  - Možnost rušení, klamného vysílání, potřeba autonomního napájení
- Hybridní

1.5 Dvojitě vyvážená smyčka

- Poplachový i sabotážní vypínač jsou v jedné smyčce
- Napájení detektorů



Stav	spínač poplach	spínač sabotáž	odpor smyčky
klidový stav	sepnuto	sepnuto	R kΩ
poplach	rozepnuto	sepnuto	$2 \cdot R$ kΩ
přerušení smyčky / sabotáž detektoru	sepnuto	sepnuto / rozepnuto	∞
zkrat smyčky	sepnuto	sepnuto	0

Obrázek 2: Dvojitě vyvážená smyčka

2 Předmětové a překážkové detektory PZS

Detektory viz výše.

2.1 Typy detektorů z hlediska vícevrstvé ochrany

- Vícevrstvá ochrana: aktiva jsou obklopena několika liniemi překážek a detektorů (Plot, pozemek, plášť budovy, interiér, vitrína, vzetí předmětu – vše možno střežit detektory)
- **Objektové**

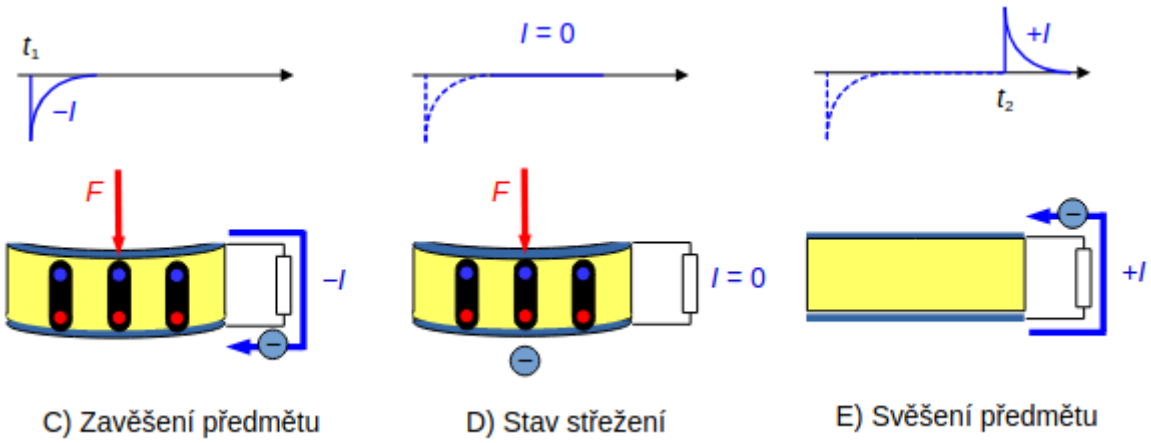
- Detekce manipulace útočníka s objekty – to můžou být střežené předměty nebo překážky
- Dělí se na:
  - Předmětové detektory – neoprávněná manipulace se střeženým předmětem
  - Překážkové detektory – neoprávněná manipulace s překážkou (překážka je pevná materiálová struktura, má útočníkovi znemožnit přístup do prostoru za překážkou)
  - Překážky: ploty, hraniční zdi pozemků, pláště budov (vnější zdi, střecha, dveře, okna), pláště úložišť (úložiště jsou trezory, skříně, vitríny... Plášť úložiště jsou vnější hranice úložiště)

– **Prostorové**
- Detekce pohybu útočníka kontrolovanou oblastí
- Charakteristika: detekční diagram – část prostoru, ve které mže detektor detekovat incident
- Dělení:
  - Objemové – detekční diagram v podobě trojrozměrného geometrického útvaru. Vyhlášení poplachu, když se v útvaru pohybuje útočník
  - Hraniční – detekční diagram v podobě plochy nebo linie, tvoří virtuální hranice. Vyhlášení poplachu, když útočník hranici překročí

2.2 Typy předmětových detektorů — účel a jejich fyzikální princip

– Tíhové
- Tíha je síla, kterou těleso působí v tíhovém poli na závěs nebo na podložku
- **Závěsové detektory**
  - Např. pro obraz
  - Předmět působí na jejich táhlo
  - Typicky piezoelektrické snímače – piezoelektrická destička s elektrodami na opačných stranách, ty jsou spojeny rezistorem (viz část 2.4.1)
  - Zavěšením předmětu je piezoelektrická destička namáhána a polarizuje se, rezistorem krátce poteče proud, který vyrovná potenciály elektrod
  - V klidovém stavu rezistorem proud neteče, piezoelektrická destička je polarizovaná
  - Svěšením předmětu poteče rezistorem krátce proud opačného směru
- **podložkové detektory**
  - Např. pro vázu
  - Kdysi mikrospínač, dnes piezoelektrický snímač nebo tenzometr
- Detekce ztráty tíhy, kterou chráněný předmět působí na detektor
- $F = m \cdot g$
- Piezoelektrické senzory, tenzometry

– Akcelerační



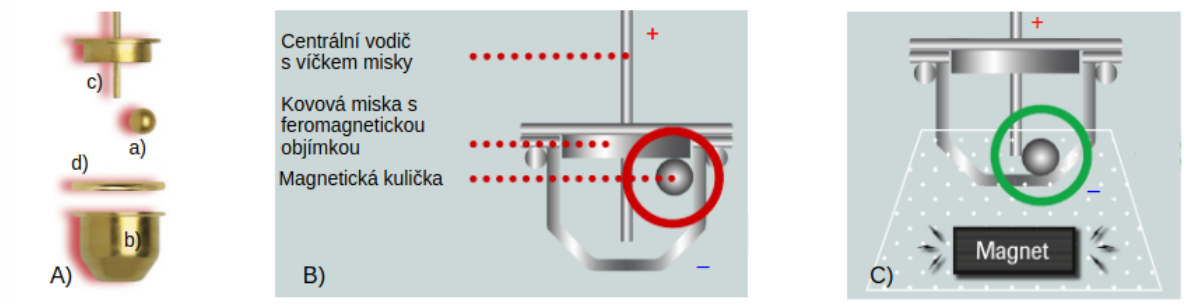
Obrázek 3: Schéma závěsového detektoru

- 2. Newtonův zákon: $a = F/m$
- Manipulace s předmětem vyžaduje sílu, bude ho tedy doprovázet zrychlení předmětu
- Předmětové – translační (detekce pohybu), obvykle umístěné na předmětu, bezdrátové
- Překážkové – otřesové (vrtání zámku trezoru...)

– Instalované externě – detektor je mimo střežený předmět (visí na něm, stojí na něm)
– Instalované interně – detektor je součástí předmětu (je s ním slepený)

2.3 Typy překážkových detektorů – účel a jejich fyzikální princip

– Detekce neoprávněné manipulace s překážkou (přelézání zdi, stříhání plotu, bouránání, otevření okna...)
– Detektor otevření
  - Detekce otevření otevíratelných výplní stavebních otvorů (dveře, okna)
  - Magnet (na dveře/okno) a jazýčkový nebo kuličkový magnetický spínač (na rám)
  - Klidový stav – magnet je v blízkosti spínače, ten je sepnutý, smyčkou prochází proud
  - Jazýčkový
    · Magneticky měkké vodiče – ploché jazýčky v trubičce s inertním plynem, bez magnetu rozepnuté
    · Magnet je magnetizuje, stanou se opačnými póly a spojí se
    · Náchylné na útok přídavným magnetem
  - Kuličkový
    · Zmagnetizovaná vodivá kulička v kovové misce, která je jedním kontaktem. Kulička je přitahovaná k feromagnetickému příklopu misky, skrz který vede elektroda blízko ke dnu misky
    · Magnet musí být v úzké zóně, aby byl spínač sepnut
– Detektor tříštění skla



Obrázek 4: Kuličkový spínač

- Detekce rozbití skleněných ploch tvořících překážky
- Rozbití skla provází akustický ráz a zvuky o frekvenci 4 kHz
- Zachycuje otřesy okenní tabule nebo zvuky v místnosti – spektrální analýza
- Kontaktní – piezoelektrický snímač na skle
- Bezkontaktní – mikrofon – velký rozsah

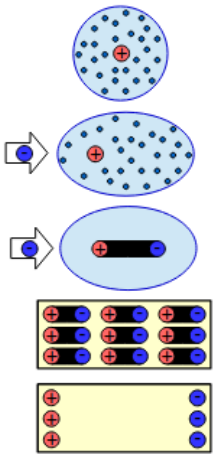
– Otřesový detektor
  - Detekce pokusů o překonání překážky
  - Lokální
    - Dosah metry, ochrana trezorů a stěn místností
    - Kapacitní akcelerometry, piezoelektrické akcelerometry
  - Distribuované
    - Dosah desítek metrů a více, ochrana rozsáhlých překážek jako ploty nebo stěny budov
    - Plotové kabely
      – Detekce překonávání hraničních zdí, plotů a plášťů budov – přelezávání, přestřihávání, podhrabávání
      – Elektromagnetická nebo elektrostatická indukce
      – Pulsní nebo spojitý režim
      – Elektretový kabel – Koaxiální, polarizované dielektrikum (elektret), otřesy indukují náboj ve vodičích díky pohybu vodičů oproti elektretu
      – Elektromagnetický plotový kabel s kontinuálním režimem provozu – Budící vodiče a pohyblivé vodiče v dřážce (vše ve výplni z magnetického polymeru) + stínění – pohyb indukuje napětí
      – Elektromagnetický plotový kabel pro pulzní režim provozu – koaxiální kabel (budící vodiče) s volnými snímacími vodiči v dielektriku – vytvoří střední úrovně indukovaného napětí pro daný okamžik, při větší změně oproti očekávané hodnotě vyhlásí poplach
    - Plotový bezdrátový otřesový systém
      – RFID čipy s akcelerometry MEMS, předávají si informace od jednoho ke druhému až do ústředny

· Plotový tahový systém – dráty jsou nataženy mezi kotvícím sloupkem a sloupkem se snímači tahu, využití tenzometrů nebo piezoelektrických snímačů nebo jazýčkový snímač, který je ovlivňovaný magnetem na konci drátu, který drží pružina

2.4 Fungování piezoelektrického snímače, akcelerometru a tenzometru

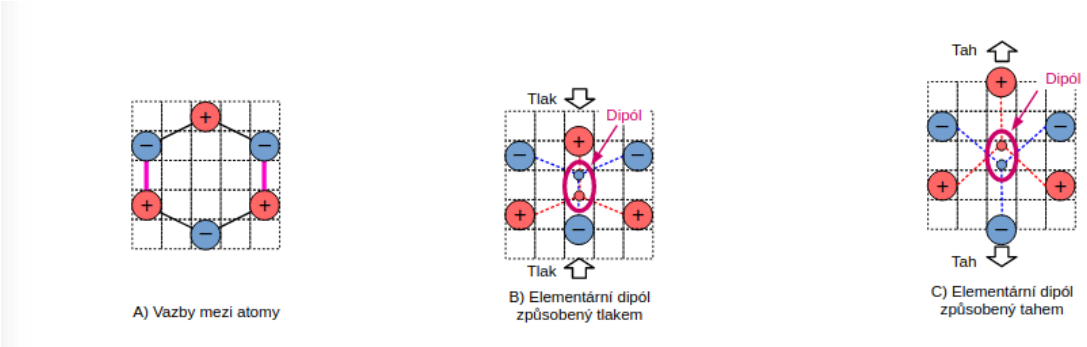
2.4.1 Piezoelektrický snímač

- Dielektrikum – materiál bez volných nosičů elektrického náboje, schopný polarizace
- Polarizace dielektrika – vlivem lokálního posunu vázaných nosičů nábojů se na protilehlých stranách dielektrika objeví opačné náboje
- Atomová polarizace:
  - V klidovém stavu je oblak elektronu kruhového tvaru
  - Blízkým vnějším nábojem se oblak elektronů deformuje na tvar elipsoidu, těžiště záporných a kladných nábojů neleží ve stejném bodě
  - Elektrické síly opačných nábojů se vzájemně ruší uvnitř dielektrika, u povrchu však ne (měřitelná elektrická síla u povrchu)



Obrázek 5: Atomová polarizace dielektrika

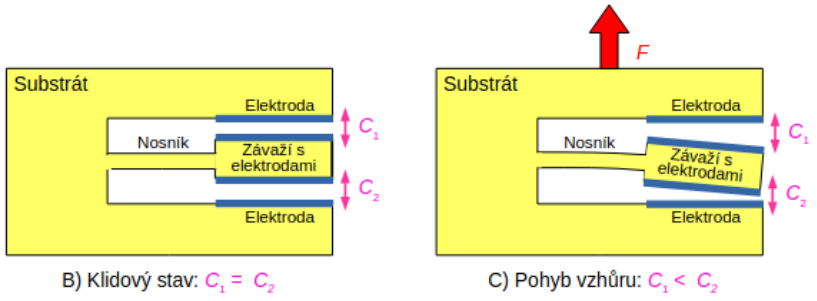
- Piezoelektrika se při mechanickém namáhání elektricky polarizují
- Piezoelektrika jsou krystaly (křemen) nebo keramika
- Krystalická mřížka ve tvaru např. šestiúhelníku se střídajícími se náboji ve vrcholech
- Náboje na opačných stranách krystalické mřížky mohou měnit svou vzájemnou polohu více než sousední částice (ty jsou drženy na místě vazebnými silami)
- Posuvem částic v opačných stranách krystalu dojde k posunu těžišť kladných a záporných nábojů v elementární buňce krystalu



Obrázek 6: Piezoelektrický jev

2.4.2 Akcelerometr

- Obsahují závaží a fyzikální vazbu, která umožňuje měřit sílu působící na závaží
- Typy: piezoelektrické, kapacitní
- Jednoosé (v jednom směru) nebo tříosé (v prostoru)
- Piezoelektrické
  - Piezoelektrická destička je umístěna mezi závaží a sledovaný předmět
  - Pro napětí platí $U = k \cdot F$, kde k je materiálová konstanta piezoelektrika
- Kapacitní
  - Technologie MEMS (Micro-Electro-Mechanical System)
  - Vyrobené ze substrátu SiO_2, vyleptaná struktura
  - Tvoří dvojici kondenzátorů, od každého je jedna elektroda umístěna na tenkém nosníku, který se při pohnutí mírně ohně díky setrvačnosti
  - Změní se kapacita kondenzátorů

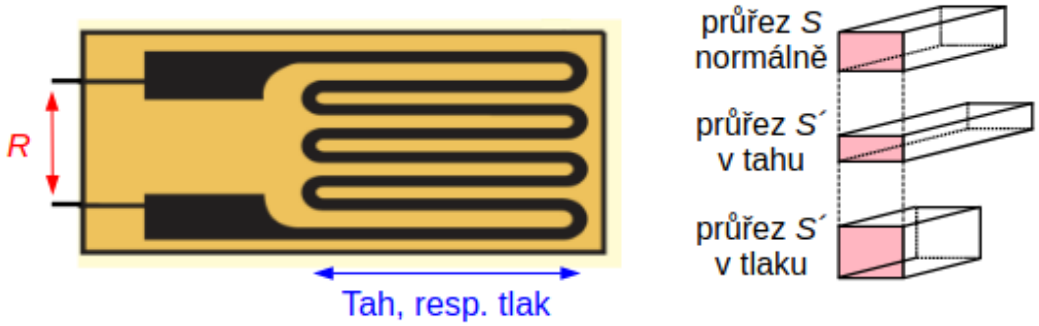


Obrázek 7: Kapacitní akcelerometr

2.4.3 Tenzometr

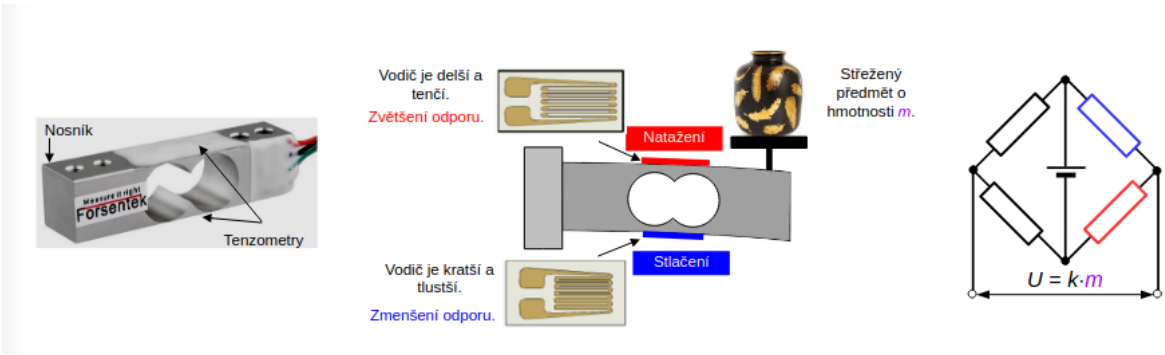
- Pružná fólie, na které je nanesen kovový materiál v tenké vrstvě, do tvaru meandrů
- Mechanickým namáháním se mění elektrický odpor kovového materiálu (mění se totiž průřez a délka vodiče)

– Původní odpor: $R = \rho \cdot L/S$, po namáhání $R' = \rho \cdot L'/S'$, kde L je délka, S průřez vodiče a ρ je měrný odpor materiálu



Obrázek 8: Tenzometr, schéma a změny vodiče

– Často se umisťují na vetknuté nosníky (jeden konec volný), ty se tíhou předmětu ohýbají
– Tenzometry jsou umístěny na horní a dolní straně nosníku, takže na ně působí ohyb
– Zapojí se pomocí Wheatstoneova můstku, na kterém je měřené napětí přímo úměrné hmotnosti předmětu



Obrázek 9: Tenzometry na nosníku, Wheatstoneův můstek

3 Objemové a hraniční detektory PZS

– Rozdělení na objektové a prostorové
– Prostorové – detekce pohybu útočníka kontrolovanou oblastí, objemové, hraniční

3.1 Typy objemových detektorů – účel a jejich fyzikální princip

– Zejména v interiérech, kde se nacházejí aktiva
– **Pasivní infračervené detektory**
  ◦ Neemitují energii
  ◦ Příznak – infračervené záření
  ◦ Pyroelektrický snímač – pyroelektrický jev

- 9,4 μm vlnová délka
- Fresnelovy čočky (soustava)
- Detekce objektů o teplotě lidského těla
- Citlivý na tangenciální směr, málo citlivé na radiální směr
- Potřeba přímého výhledu

– **Mikrovlnné detektory**
- Dopplerův jev – při pohybu zdroje a pozorovatele vlnění
- $f' = f \cdot \left(\frac{c}{c \pm v}\right)$, kde c je rychlost šíření vlnění a v je vzájemná rychlost zdroje a pozorovatele
- 10 GHz
- Generátor vysílá do prostoru signál o frekvenci f_v, ty se odrážejí od objektů. Podle pohybu objektu může mít odražené vlnění jinou frekvenci, odražené signály zachytává anténa
- Generovaný a zachycený signál jsou vstupy do směšovače signálu, dolní propustí se vybírá signál $|f_o - f_v| = \epsilon$. Pokud $\epsilon \neq 0$, pak poplach
- Všechny pohybující se objekty jsou detekovány
- Citlivý na radiální směr, necitlivý na tangenciální
- Falešné poplachy dosahem ze střežené zóny ven nebo blízkostí 2 MW detektorů

– **Duální detektory**
- Kombinace PIR a MW, eliminuje jejich slabiny
- Vyhlášení poplachu – součinová (AND) nebo součtová (OR) logika

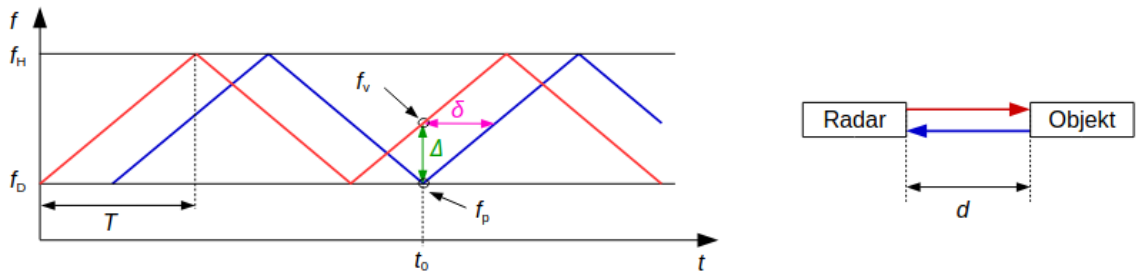
– Kamerový systém s analýzou obrazu – virtuální hranice

3.2 Typy hraničních detektorů – účel a jejich fyzikální princip

– Plošné
- Jeden rozměr detekčního diagramu lze oproti dvěma ostatním zanedbat
- Hranice budov, místností, předmětů
- PIR detektory se záclonovou čočkou
- Lidarové detektory
  · Light Detection And Ranging – 2D laserový skener
  · Analog k radaru v IR nebo optickém pásmu (laser)
  · Vyšle pulz, měří čas do přijetí odraženého záření, $d = c \cdot T/2$
  · Vysílač cyklicky mění směr v určitém úhlovém rozsahu – monitorování v rovině
  · Hraniční rovina často vertikální mezi střeženým objektem a prostorem, odkud může přijít útočník
  · I v exteriéru – vertikální (přes plot nic nesmí projít) nebo horizontální (nad úrovní plotu nic nesmí být) hranice

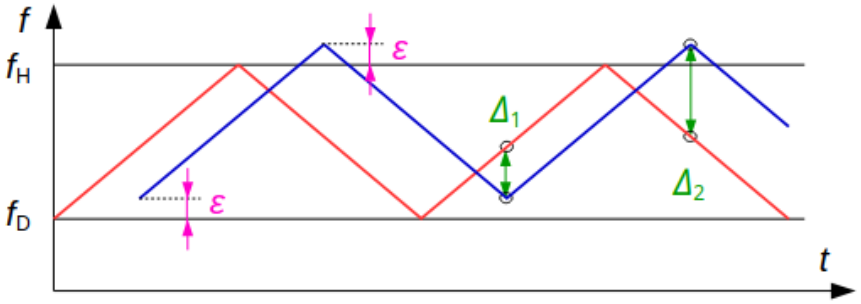
– Liniové

- Dva z jeho rozměrů lze oproti jednomu zanedbat
- Typicky pro hranice pozemku
- Zemní
  - Štěrbinové kabely
    - Koaxiální se štěrbinami v plášti, 1 koax. přijímací, druhý vysílací
    - Vysokofrekvenční pole se šíří štěrbinami mezi nimi a objekt v poli ho naruší
    - Kontinuální nebo pulzní (podle času lze určit, kde se proud naindukoval a když je zjištěna změna oproti normálu, lze nalézt místo, kde byl poplach vyhlášen)
  - Zemní optovláknové kabely
    - meandry jednovidového optického kabelu v zemi, dlouhá střežená linie
    - Krátké pulzy fotonů, část se srazí s nehomogenitami ve vlákně, vznikne Rayleighův rozptyl, část z rozptýlených fotonů se vrací zpět ke zdroji
    - Tlakem se zmenší průřez flákna a na daném místě bude větší pravděpodobnost pohlcení fotonu nehomogenitou
    - Metrová přesnost
  - Seizmické detektory
    - Akcelerometry snímající otřesy země
    - Magnet, pružně zavěšená cívka -> indukce napětí
    - Kolíky s nimi se zapichují do země několik metrů od sebe, připojení k centrální jednotce
- Nadzemní
  - Mikrovlnné
    - Direktivní, vysílač, přijímač, 5, 10 nebo 24 GHz
    - Energie v úzkém elipsoidu – Fresnelova zóna
    - Útočník sníží úroveň přijímaného signálu, až stovky m
  - Infračervené
    - Direktivní, vysílač, přijímač
    - Fototranzistor
    - Čočka, tvoří úzký paprsek
    - Více svazků mezi vysílačem a přijímačem, různé uspořádání
    - Moderní – digitální modulace (pro automatickou regulaci vysílaného výkonu, např. v mlze), multiplexování, adresace – přenos bitů pro vyhodnocení, jestli byl do správného modulu přijímače včas doručen paprsek z modulu vysílače
  - Radarové
    - Zvýšená intenzita odraženého záření
    - FM-CW radar (kmitočtově modulovaný, spojitě vysílající)
    - Kmitočet se spojitě mění podle pilovitého průběhu
    - $d = (c \cdot \Delta)/(2 \cdot v)$, kde v je rychlost přeladování radaru ($v = (f_H - f_D)/T$), T je doba přeladění pásma, $\Delta = f_v - f_p$



Obrázek 10: FM-CW radar

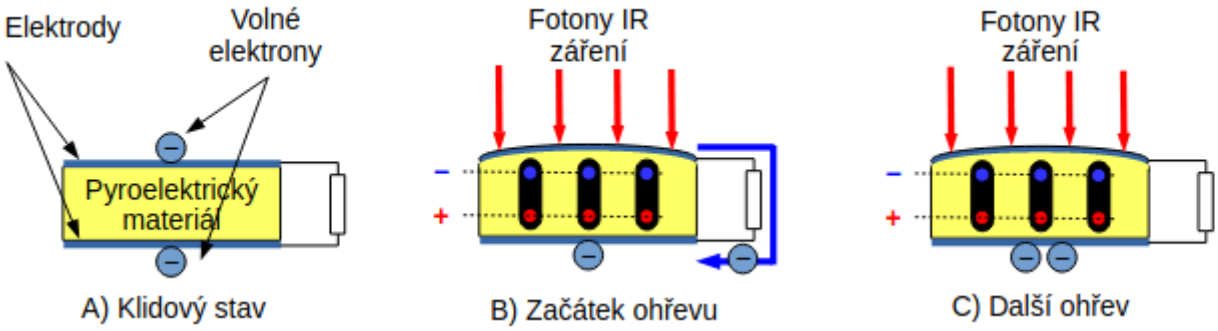
- Dopplerovský FM-CW radar
- $\epsilon = (\Delta_2 - \Delta_1)/2$, $\Delta = (\Delta_2 + \Delta_1)/2$, $d = (c \cdot \Delta)/(2 \cdot v)$, lze určit vzdálenost i rychlost vzdalování nebo přibližování



Obrázek 11: Dopplerovský FM-CW

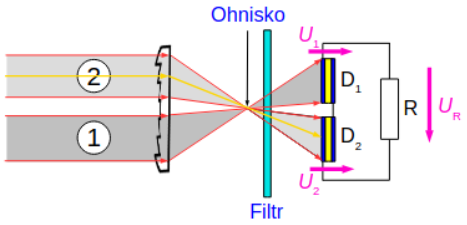
3.3 Fungování pyroelektrického snímače

- Pyroelektrický jev
- Pyroelektrika jsou množina piezoelektrik
- Dopad IR záření -> zahřátí -> vyboulení -> mechanický tah -> nabití záporným nábojem
- Fresnelova čočka – konvexní čočka zborcená po mezikružích



Obrázek 12: Pyroelektrický jev

– PIR detektor jich má celou soustavu
– PIR obsahuje 2 pyroelektrické destičky v rozdílovém zapojení – eliminace změn teplot a chování jako akcelerometr
– Záření ze zóny je rozděleno na 2 laloky a slepou zónu mezi nimi. Z každého laloku dopadají paprsky jen na jednu pyroelektrickou destičku
– Pokud je intenzita záření z laloků stejná, napětí na rezistoru rozdílového zapojení je nulové



Obrázek 13: PIR detektor – laloky

– Soustava Fresnelových čoček vytváří více jemnějších laloků v prostor (např soustava 11 čoček vytvoří 22 laloků)
– Laloky bývají uspořádány do vrstev
– Čočky
  ◦ Klasická – detekční diagram jsou šikmo sklopené, široké vějíře
  ◦ Chodbová – detekční diagram tvoří úzké a dlouhé vějíře
  ◦ Záclonová – 2 úzké, vertikálně postavené vějíře
– Imunita proti zvířatům
  ◦ Zvířecí čočka – Detekční zóny několik desítek cm nad zemí
  ◦ Detektor se 2 snímači – Jeden v nižší vrstvě, druhý ve vyšší, poplach jen při detekcí oběma snímači

4 Dohledové videosystémy

4.1 Účel

– DVS – elektronický systém, oprávněné osobě umožňuje vizuálně a na dálku sledovat dění v kontrolované oblasti
– Oprávněná osoba = pozorovatel – v dohledovém centru
– Dění v zónách (části kontrolované oblasti) se pomocí zařízení snímá a převádí na elektrický signál. Ten je přenášen do dohledového centra
– Signál z kamer je analogový nebo digitální (analogový/digitální systém)
– První VDS využit pro testování německé rakety V2 v roce 1942

– CCTV – *Closed-circuit television* – televizní signál je kabelovým rozvodem přenášen k pozorovatelům, dnes *Video surveillance systems*

4.2 Základní prvky

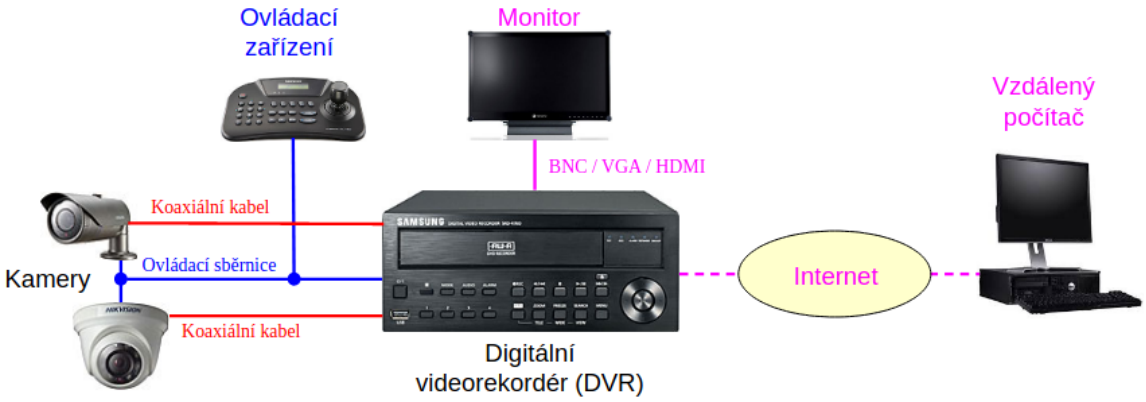
– Kamery
  ◦ Ke snímání sledovaného obrazu
  ◦ Obraz převeden na elektrický signál, odeslán přenosovým zařízením k dalšímu užití
  ◦ Analogové – PAL, NTSC, HD
  ◦ Digitální – H.264, MJPEG
  ◦ Venkovní, vnitřní
  ◦ Dohledové – majitel ji využívá ke zjevnému sledování dění v prostoru
  ◦ Skryté – štěnice – majitel ji používá ke skrytému sledování dění v prostoru
  ◦ Statické kamery – snímají obraz v daném směru bez možnosti přibližování
  ◦ Ovládané kamery – mění záběr podle potřeby, mohou být směrově statické (PTZ kamery – Pan, Tilt, Zoom) nebo směrově statické (lze měnit ohniskovou vzdálenost, větší ohn. v. -> užší výhled)
– Videorekordér
  ◦ Jádro DVS
  ◦ Mají rozhraní pro připojení ostatních zařízení DVS (kamery, ovládací zařízení, vzdálené monitory)
  ◦ Zasílá signál z kamer do monitorů a ukládá je do úložiště
  ◦ Umožňuje přehrrávat uložená data
  ◦ Digitální (DVR) – kamery připojeny koaxiálním kabelem
  ◦ Síťové (NVR) – kamery připojeny počítačovou sítí
– Ovládací zařízení
  ◦ Ovládání ovládaných kamer
  ◦ Natáčení, naklápění, přibližování, vzdalování scény
  ◦ Provádění některých funkcí videorekordéru
  ◦ V digitálních systémech – komunikace protokolem IP
  ◦ V analogových systémech – komunikace po samostatné sběrnici (PAL, NTSC) nebo po koaxiálním kabelu vedoucím ke kameře
– Monitory
  ◦ LCD s LED podsvícením, 4:3, 16:9
  ◦ Rozhraní BNC, VGA, HDMI
– Kabelové rozvody
  ◦ Málokdy nahrazeny bezdrát. přenosem
  ◦ Koaxiální konektory s BNC konektory (kabelový rozvod)
  ◦ UTP s RJ-45 pro digitální signál

- Analogové přenosy neustoupily díky technologii HD, ale více a více se bude používat TCP/IP přenos

4.3 Schéma hybridního a digitálního systému

Hybridní

- Kamery – analogový obrazový signál
- Digitální videorekordér digitalizuje obraz, ukládá na pevný disk
- DVR generuje signál pro monitor a případně i pro vzdálený počítač
- DVR zprostředkovává ovládání kamer pomocí ovládacího zařízení



Obrázek 14: Hybridní DVS

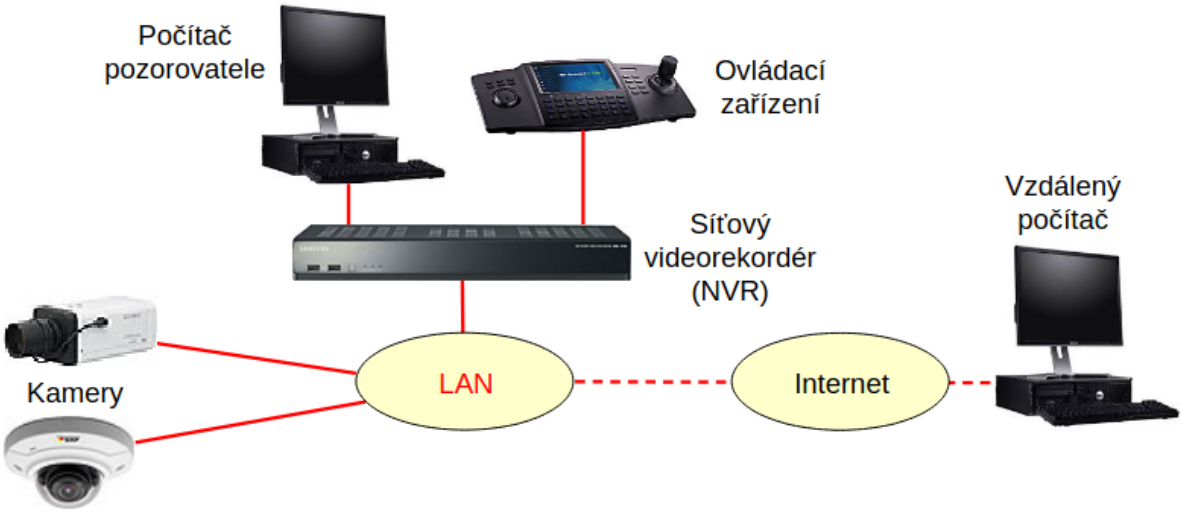
- Analogové kamery vyžadují napájecí pár, koaxiální kabel a u SD ovládací sběrnici RS-485 (u HD lze pro ovládání využít koax a umí přenést i zvuk)

Digitální

- Network Video Recorder – ukládá záznamy na pevný disk, řídí kamery
- Veškerá komunikace protokolem IP
- 100BASE-TX, PoE (Využité 2 páry pro data, 2 pro napájení, 1 pár jako 1 napájecí vodič)
- Obraz – RTSP (port 554, ovládání relace), RTP (přenos obrazových a zvukových dat)
- Iniciativa ONVIF – pro standardizaci IP zabezpečovacích systémů

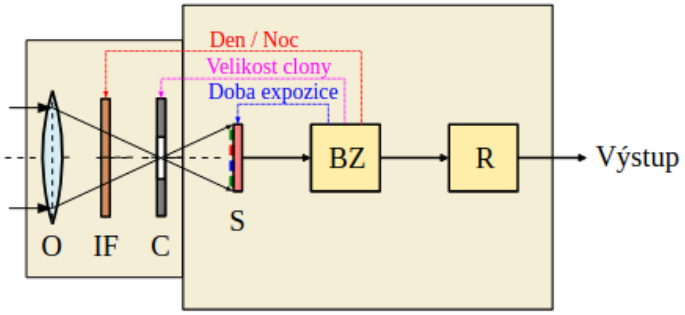
4.4 Architektura kamery

- Objektiv (O) – soustřeďuje světelné záření na snímač
- Infračervený filtr (IF) – Ve dne znemožňuje průchod IR fotonů, předchází zkreslení
- Clona (C) – Regulace množství světla
- Obrazový snímač (S) – Dopadající záření -> signál



Obrázek 15: Digitální videosystém

– Blok zpracování obrazu (BZ) – signál ze snímače převede na obraz, upraví, zkomprimuje. Ovládá clonu, IR filtr a dobu expozice
– Komunikační rozhraní (R) – Obraz převede na signál vhodný pro přenos do dohledového centra



Obrázek 16: Architektura kamery

– Snímače – CCD, CMOS, mění dopadající záření na elektrický náboj, Bayerovo schéma
– CMOS
  ◦ Každý pixel – tranzistory, fotodioda (fotoelektrický jev), filtr a malá čočka

4.5 Kalkulace záběru

Veličiny:

– h – šířka obrazového čipu
– f – ohnisková vzdálenost objektivu (tedy i vzdálenost snímače od čočky)
– D – Vzdálenost objektu od kamery
– H – Šířka záběru ve vzdálenosti D

– Podobnost trojúhelníků: $H/D = h/f$
– Záleží tedy na formátu snímače, ohniskové vzdálenosti a vzdálenosti od objektu
– Potřeba stanovit, jestli je potřeba přehled nebo detaily
– Varifokální kamery – obsluha nastaví podle potřeby
– Příblížení (zoom) $z = f_{\max}/f_{\min}$
– Pokud chceme předmět přes celou šířku monitoru (šířku záběru), musíme správně zvolit ohniskovou vzdálenost, velikost snímače a umístění kamery

4.6 Techniky zpracování signálu (integrace snímků, BLC, WDR, HLC)

Integrace snímku

– Zkvalitnění obrazu ve špatných světelných podmínkách
– Jeden snímek je vypočten součtem více snímků (desítky až stovky)
– Rozmaže pohyby

BLC

– Kompenzace protisvětla
– Místo průměrování jasu z celého obrazu se doba expozice vypočte z určité části obrazu, kterou určí správce kamery
– Místo siluet bude viditelný člověk, ale okno za ním bude přeexponované

WDR

– Široký dynamický rozsah
– Snímky jsou kombinací přeexponovaného a podexponovaného snímku
– Z přeexponovaného snímku se použijí tmavé části, z podexponované ty světlé
– Současně zobrazeny světlé i tmavé části

HLC

– Kompenzace přesvícení
– V obrazu jsou začerněny bodové zdroje světla
– Doba expozice vypočítaná z obrazu, kde jsou zdroje začerněny
– SPZ auta bude viditelná

5 Systémy EPS a hlásiče EPS

5.1 Účel, architektura, základní prvky

Účel

- Detekce a reakce na vznik požáru ve střeženém prostoru (požár je hoření, při kterém jsou ohroženy životy a majetek)
- Reakce:
  - Vyhlášení poplachu
  - Oznámení požáru hasičům
  - Spuštění automatizovaných protiopatření k minimalizaci škod (otevření dveří pro evakuaci, spuštění stabilního hasícího systému...)

Architektura

- Prakticky stejná jako u PZS, všechny části spojeny s ústřednou pomocí spojů
- Smyčkové (konvenční) – analogová signalizace na základě velikosti protékajícího proudu
- Sběrnicové – nejčastěji dvoudrátová sběrnice s kruhovou topologií

Základní prvky:

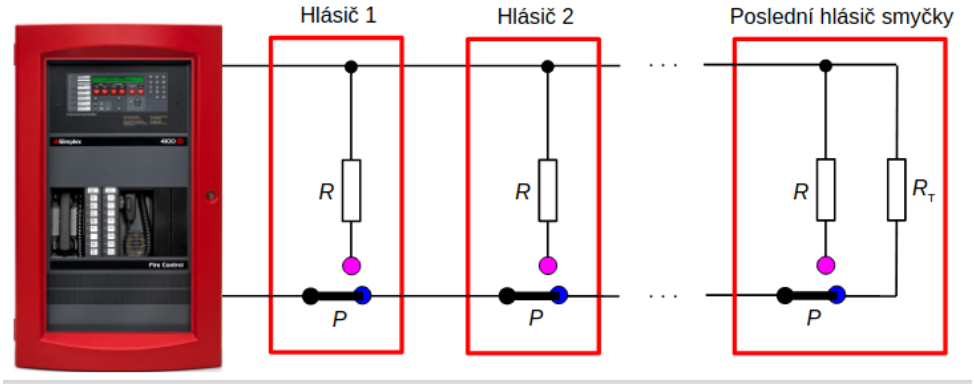
- Hlásiče
  - Sledují příznaky požáru (např. kouř)
  - Klasifikace na detektory (vyhlašují poplach na základě příznaků) a měřiče (také analogové hlásiče, zasílají měřené parametry ústředně, ta rozhoduje o poplachu)
  - Tlačítkové a automatické (hlásiče kouře, hlásiče teploty, hlásiče plamene)
  - Hlásiče mohou být kombinované
  - Automatické hlásiče jsou bodové, lineární, prostorové
- Ústředna
  - Řídí EPS
  - Všechny ostatní prvky jsou k ní připojeny
  - Většinou kabelové spoje
- Informační zařízení – informují osoby o vzniku požáru
- Akční zařízení
  - Uskutečňují akce k minimalizaci škod
  - Stabilní hasící zařízení – hasí požár
  - Ventilátory – vypnutí -> dušení požáru, zapnutí v únikových cestách
  - Požární dveře – Zpomalení šíření požáru do prostoru za nimi
  - Požární klapky – Zpomalení šíření požáru vzduchotechnikou
  - Klíčový trezor požární ochrany – Zpřístupnění hasičům klíče do objektu (dvoje dvířka, vnitřní se odemknou univerzálním klíčem hasičů, vnější odemkne ústředna)
- Ovládací zařízení
  - Umožňují obsluze ovládat EPS
  - Řídící konzola ústředny
  - Obslužné pole požární ochrany (jednotné pro všechny typy ústředen, pro hasiče)

– Spoje
  ◦ Umožňují komunikaci ústředny s ostatními prvky EPS
  ◦ Ohnivzdorné kabely, bezhalogenové směsi (neprodukují jedovaté dýmy)
  ◦ Bezdrátové spoje (hlásiče, akční, informační zařízení)
– Zařízení datového přenosu – informace z ústředny na pult centrální ochrany hasičů
– Pult centrální ochrany – dálkové monitorování systémů EPS

5.2 Schéma a princip fungování smyčkového a sběrnicového systému

Smyčkový

– Smyčka = pár vodičů, hlásiče připojovány za sebou
– V každém hlásiči je přepínač, ve výchozí poloze proud protéká zakončovacím rezistorem na konci smyčky. Při přepnutí proud protéká rezistorem v hlásiči
– Přepnutí odpojí ostatní hlásiče, odpor v hlásiči je menší než ukončovací rezistor, při poplachu se proud zvýší



Obrázek 17: Smyčkový EPS

– Nízká cena, jednoduchost
– Nelze určit, který hlásič na smyčce vyvolal poplach -> více smyček pro určení zóny, ve které je požár
– Pro informační prvky je potřeba oddělené smyčky

Sběrnicový

– Dvoudrátové sběrnice
– Topologie kruh nebo linie
– Sběrnice často zajišťují i napájení, jinak souběžně se sběrnicí dvoužilový napájecí rozvod
– Adresy, výzva – odpověď (ústředna zasílá výzvy cyklicky)
– Detektory sdělují stav (klid/poplach), měřiče sdělují velikost měřené veličiny
– Přesné informace o hlásiči, který poplach vyhlásil, jednodušší rozvody (hlásiče a informační prvky mohou být na stejné sběrnici)

Obrázek 18: Sběrnicový EPS

5.3 Bodové hlásiče a jejich fyzikální principy

- Měří příznaky v okolí svého umístění
- Příznaky plamene:
  - Horké CO_2 – záření v IR pásmu 4,3 μm
  - Wienův posunovací zákon: $\lambda_{max} = \frac{b}{T}$, kde b je Wienova konstanta, $2{,}898 \cdot 10^{-3}$ $[m \cdot K]$
  - Citlivost detektoru na vlnovou délku se nastavuje materiálem okénka nad pyroelektrickou destičkou
  - Pokud snímač detekoval signál 3 až 30 Hz (mihotání), vyhlásí poplach
- Hlásiče teploty
  - Termistor (rezistor, odpor závislý na teplotě)
  - Okolní vzduch teplejší než stanovená mez -> poplach
  - Mohou být použity 2 termistory – jeden vystavený vzduchu, druhý izolovaný. Při změně teploty jsou měření různá, vyhlásí poplach (diferenciální metoda)
- Hlásiče kouře
  - Ionizační hlásiče
    - Pokles elektrického proudu v ionizační komoře (americium-241 – alfa zářič)
    - Kouř vytlačí část plynu z komory, vážou na sebe ionty, ale pohybují se pomalu
  - Optické hlásiče
    - Přerušení paprsku – na fotodiodu svítí IRED, při poklesu intenzity poplach
    - Rozptýlení paprsku – IRED svítí mimo fotodiodu, od aerosolu se paprsky odrazí i na fotodiodu
- Multisenzorové hlásiče – kombinace (kouřový + teplotní), méně falešných poplachů
- Senzor plynů

5.4 Lineární hlásiče a jejich fyzikální principy

- Infračervené
  - Paprskové:

- Přerušení paprsku kouřem
- Přímé nebo s odrazem (vysílač a příjímač na stejné straně, naproti nim je odrazná plocha)
- Snímací:
- Analýza IR spektra – signál 1 až 10 Hz, 4,3 μm vlnová délka záření
- Až di 50 m

– Kabelové
- Zkratové
  - Kroucený pár, izolace taje při nízké teplotě, na konci ukončovací rezistor
  - Podle odporu lze ze vztahu $R = 2 \cdot L \cdot \rho$ vypočítat vzdálenost
  - 1500 m, vyhodnocovací jednota nepřetržitě měří odpor
- Izolační
  - 2 páry kroucených vodičů, na konci páry spojené ukončovacím odporem, izolace kabelů má negativní teplotní koeficient (v teple vede proud), měřící jednotka měří odpor
  - Stačil by jeden pár, druhý je pro kontrolu celistvosti kabelu
  - Po zchlazení se vrátí do pův. stavu
- Optovláknové
  - Rozptylové záření – přechod elektronu mezi energetickými hladinami
  - Ramanův rozptyl – záření s jinou vlnovou délkou než je excitační záření (přechod o 1 úroveň, když byl excitován o 2, přechod o 2 úrovně, když byl excitován o 1)
  - Čím více částice kmitají (vyšší teplota), tím větší pravděpodobnost srážky s fotonem
  - Pulsní laser, polopropustné zrcadlo, rozptylové záření je polopropustným zrcadlem odraženo do přijímače
  - Měří teplotu v okolí vlákna, podle času lze určit vzdálenost

5.5 Prostorové hlásiče a jejich fyzikální principy

– Nasávací
- Využívá se optický detektor po nasátí vzduchu z prostoru – v památkově chráněných objektech

– Kamerový
- Kamera + vyhodnocovací jednotka, sleduje výskyt plamene a kouře
- Např. v tunelu

6 Systémy EKV

6.1 Účel, prvky a architektura systému EKV

- Přístupový systém, elektronická kontrola vstupu
- EACS (Electronic Access Control System), PACS (Physical Access COntrol System)
- Příbuzný je docházkový systém – bez vstupů, pro evidenci (vstup je průchod s pevnou uzavíratelnou výplní, průchod je prvek v překážce, umožňuje pohyb do prostoru za překážkou)
- Určený k automatizovanému řízení vstupů v kontrolované oblasti
- Řízení přístupu
  - Přístupová politika – kdo kdy může v zóně pobývat
  - Autorita – osoba, která stanovuje přístupovou politiku organizace
  - Autorizace – Jednorázové přiřazení identity, práv a autentizačních faktorů, v rámci autorizace se osobě přiřazuje:
    - Identifikátor
    - Dokazovací faktor – něco, čím bude osoba dokazovat svoji identitu
    - Ověřovací faktor – data, s jejichž pomocí bude přístupový systém ověřovat skutečnost,že osoba disponuje dokazovacím faktorem
  - Potřeba přístupového (ID, práva) a ověřovacího seznamu (ID, ověřovací faktor)
  - Identifikace – zjištění ID osoby
  - Autentizace – ověření ID osoby

Základní prvky

- Kontrolér – řídící jednotka přístupového systému
- Vstup
  - Uzavíratelný průchod, elektricky ovládán kontrolérem
  - Výplň se krátkodobě odblokuje
  - Dveře, turnikety (průchod jednotlivě), závory a zásuvné sloupy u aut
- Terminál – zařízení pro komunikaci osoby s přístupovým systémem
- Správní jednotka – zařízení pro správu přístupového systému
- Detektor otevření – kontrolér vyhlásí poplach, pokud má být průchod zablokován, ale není zavřený
- Odchozí tlačítko – Může být nahrazeno MW nebo PIR detektorem, vyžádání krátkodobého odblokování pro opuštění zóny

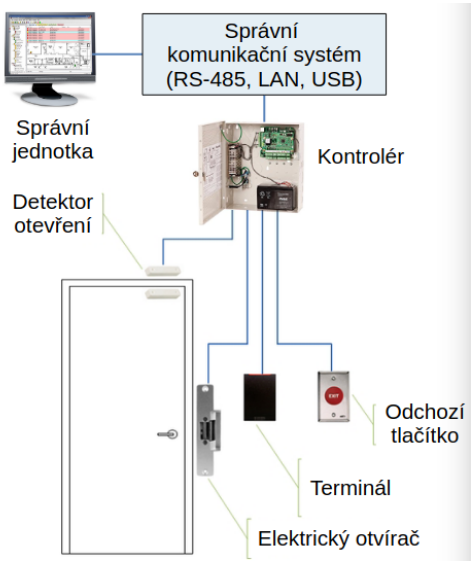
Architektura

- Všechny prvky spojeny s kontrolérem

– Správní jednotka se ke kontroléru připojuje lokálně přes USB nebo RS-232 a vzdáleně přes LAN nebo RS-485
– Autentizaci provádí terminál, ne kontrolér, ověřovací seznam je potřeba aktualizovat v něm
– Terminál a kontrolér se připojují rozhraním Wiegand (5 žil, napájení, zem, high (5 V, přerušení = 1), low (přerušení = 0), ovládání), ostatní prvky dvoudrátovou smyčkou

Fungování

– Před zahájením – autorita vloží správní jednotkou přístupový a ověřovací seznam
– Autentizace pomocí terminálu
– Kontrolér vyhledá práva pro ID
– Odemkne nebo nechá zamčený vstup
– Detektor otevření detekuje násilné otevření nebo nezavření
– Odchozí tlačítko pro otevření při odchodu
– Kontrolér – 2 vstupy. Pokud je potřeba více, každý autonomní kontrolér se připojí ke stejné správní jednotce



Obrázek 19: Architektura EKV

6.2 Typy autentizace – princip a vlastnosti

S oznámením

– Osoba uvede svůj identifikátor
– Nalezení ověřovacího faktoru -> přístupová test
– V počítačích

S rozpoznáním

– Osoba ID neuvádí, podle seznamu se zkouší ověřovací faktory, uživatel se považuje za tu osobu, s jejímž ID je ověřovací test úspěšný
– V EKV

Rozdělení podle dokazovacího faktoru a nosiče dokazovacího faktoru

– Nosičem DF je osoba:
  ◦ DF = tajná data (heslo)
  ◦ DF = biometrika osoby
– Nosičem DF je předmět:
  ◦ DF = tajná data (hardwarem)
  ◦ DF = nepadělatelné rysy předmětu (průkaz)

Biometrika

– Morfologie nebo chování
– DF = biometrika
– OF = datový záznam DF (dokazovací data – DD)
– Záznam nebude s realitou naprosto shodný
– Osoby neuvádějí ID, rozpoznávání (vyhledávání v seznamu)
– V terminálech se provádí autentizace
– Do kontroléru se zašle ID (Wiegandovo slovo)
– Ověřovací seznamy pomocí kryptograficky zabezpečeného spojení IP sítí
– DF má uživatel vždy s sebou
– Dokazovací faktory nejsou tajné, lze vytvořit padělek

Autentizace heslem

– Zapamatovaný řetězec znaků: PIN
– DF = PIN = OF = DD (dokazovací data) = ID
– Autentizaci provádí kontrolér
– Vyžaduje tabulku jen ID a práv
– Jednoduché, laciné
– Možnost zapomenout PIN, malá variabilita (slovníkový útok), odpozorování hesla parazitním kanálem (teplé otisky na klávesnici)

Autentizace průkazem

– Nepadělatelný průkaz
– Ověřovatel zkontroluje, jestli není průkaz padělán
– DF = ochranné prvky průkazu
– OF = znalost ochranných prvků

– Kritérium – průkaz není modifikovaný ani padělaný
– Ověřovatel může být člověk, není potřeba technika
– Možnost ztráty nebo ukradení průkazu, drahé kvůli ochranným prvkům a nepoužitelné pro elektronickou autentizaci
– Dvoufaktorová autentizace – průkaz a biometrika (fotka na průkazu)

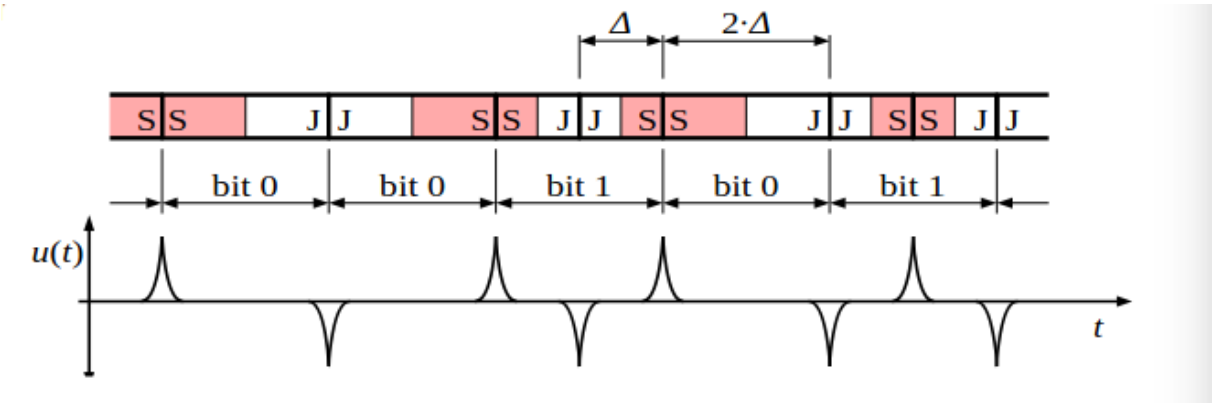
Autentizace hardwarem

– Komunikace bezdrátovým rozhraním
– Paměťové úložiště
  ◦ Tajná data uložená na předmětu, nezapamatovatelná délka
  ◦ Wiegandovo slovo (WS) – 26 b
  ◦ WS = DF = OF = ID = DD
  ◦ Laciné
  ◦ Uživatel může DF ztratit nebo mu může být ukraden
– Mikropočítač
  ◦ Symetrická i asymetrická kryptografie
  ◦ DF = tajný klíč K = OF (u symetrické)
  ◦ DF = SK, OF = VK u asymetrické
  ◦ Symetrická:
    · Terminál vygeneruje náhodný relační klíč, odešle ho zašifrovaný tajným klíčem (CR = E(RK, K))
    · Karta dešifruje, získá RK (RK = D(CR, K)), zašifruje pomocí RK svoje ID a odešle. Terminál odešle ID kontroléru
  ◦ Asymetrická:
    · Karta/telefon/předmět oznámí ID, podle toho si terminál najde VK
    · Terminál odešle náhodnou výzvu
    · Předmět zašifruje výzvu
    · Terminál ověří, jestli dešifrováním veřejným klíčem obdrží výzvu

6.3 Karty s magnetickým páskem – princip a vlastnosti

– Laciné, spolehlivé, ale málo bezpečné (klonovatelné)
– 3 stopy:
  1. 79 alfanumer. znaků, 7 b/znak
  2. 40 numer. znaků, 5 b/znak
  3. 107 numer. znaků, 5 b/znak
– Magnetizace po úsecích Δ a $2 \cdot \Delta$, v nich je materiál zmagnetizovaný jedním směrem
– Sousedící magnety – opačné směry magnetizace
– Každý bit má délku $2 \cdot \Delta$ – bitový úsek

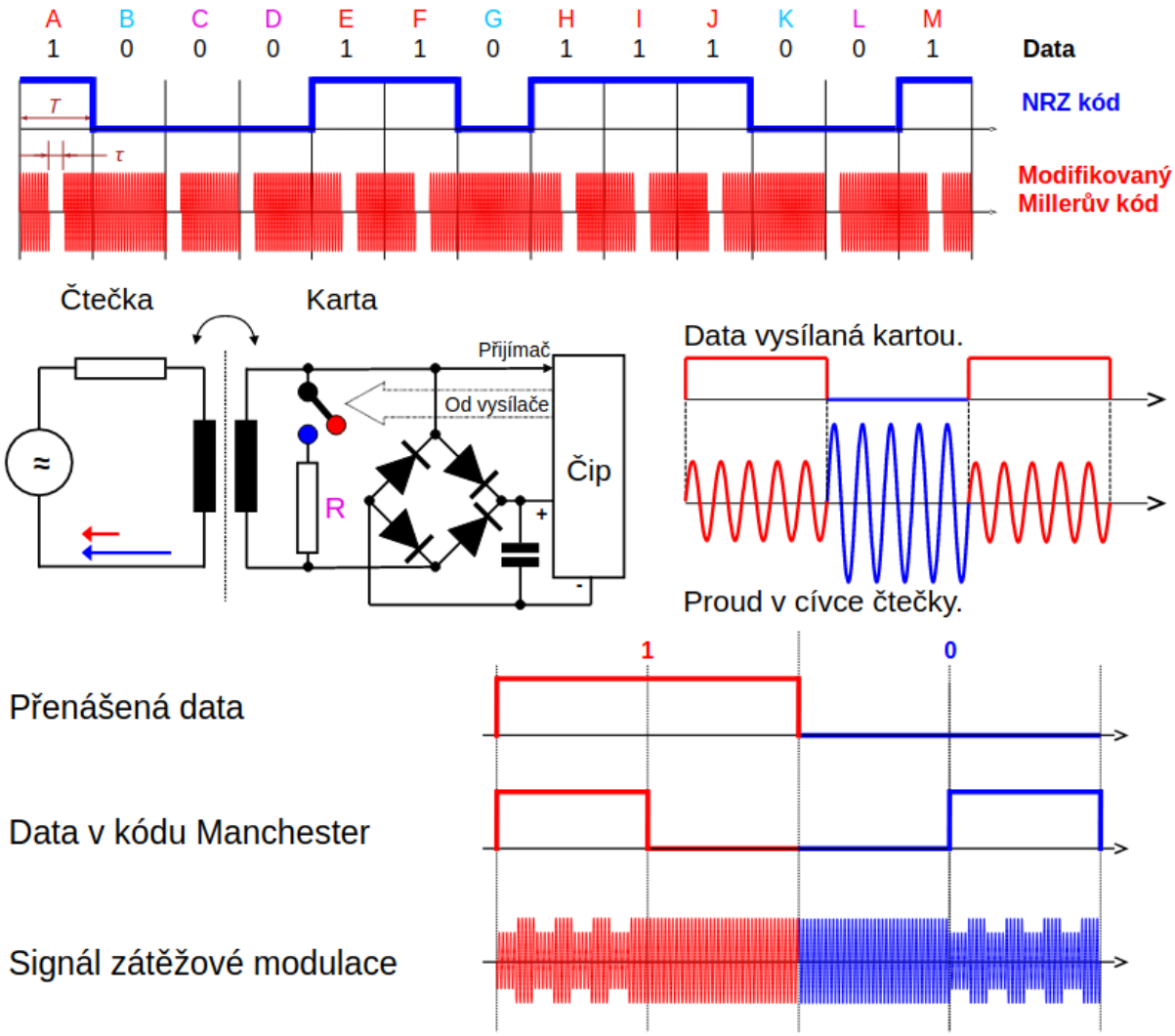
– Nulový bit = 1 magnet délky $2 \cdot \Delta$, jedničkový bit = 2 magnety délky Δ
– Při protahování budou vznikat napěťové špičky na hranách magnetů



Obrázek 20: Magnetický proužek

6.4 Bezkontaktní karty podle ISO 14443 – princip a vlastnosti

– RFID karty (Proximity Card) – 125 kHz
– Mikroprocesorové karty (Smart Card) – 13,56 MHz
– Princip transformátoru (primární je cívka čtečky, sekundární po obvodu karty)
– Čtečka generuje signál, indukuje se v cívce karty, nabíjí se jím kondenzátor – zdroj energie pro čip v kartě
– Komunikace čtečka -> karta: Modifikovaný Millerův kód (H – generování nosné, L – negenerování nosné), 1 – v polovině bitového intervalu se na krátký okamžik přepne H na L, 0 – na začátku bitového intervalu se na krátký okamžik přepne H na L, pokud předcházející bit nebyla 1
– Krátké intervaly L jsou překlenuty napájením z kondenzátoru
– Komunikace karta -> čtečka: zátěžová modulace (čtečka nepřetržitě generuje nosnou), v kartě je připojován k cívce karty a odpojován zátěžový rezistor, L – odpojení rezistoru, H – připojení rezistoru, u H vzroste proud na primární cívce
– 4krát L-H střídání v první polovině bitového signálu = 1, 4krát L-H střídání v druhé polovině bitového signálu = 0
– RFID karty – tajné Wiegandovo slovo – EEPROM paměť, náchylné na odposlech (Některé lze číst jen se znalostí hesla)
– Mikroprocesorové karty – samostatné počítače s dokazovacím faktorem, mají kryptoprocesor
– Smartphone – NFC – rozšíření ISO 14443 nebo Bluetooth



Obrázek 21: Komunikace ISO 14443

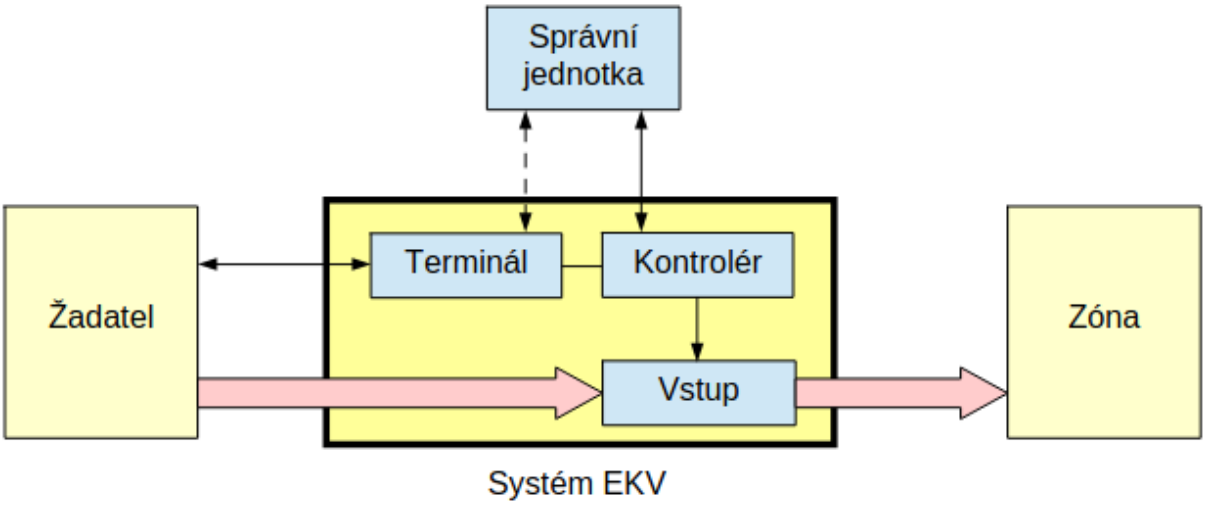
7 Biometrické přístupové systémy

- Morfologická (otisk prstu, cévní řečiště prstu, dlaně, geometrie ruky, geometrie obličeje, skvrny oční duhovky, cévní řečiště sítnice)
- Behaviorální (hlas, psaný podpis, psaní na klávesnici)
- Využívají se výhradně morfologické
- Nejednoznačnost, nenulové hodnoty False rejection rate a False acceptance rate

7.1 Architektura a správa biometrického systému EKV

- Kontrolér
  - Řídící jednotka EKV systému
- Vstup
  - Uzavíratelný průchod ovládaný elektrickým kontrolérem

– Terminál
  ◦ Zařízení pro komunikaci osoby se systémem EKV – čtečka
– Správní jednotka
  ◦ Zařízení pro správu EKV (počítač se specializovaným softwarem)
  ◦ Komunikace s kontrolérem a terminálem



Obrázek 22: Architektura EKV

– Autentizace v terminálu
– Potřeba vytvoření šablony podle změřené biometriky žadatele
– Šablona je OF v terminálu (rozpoznávací autentizace) nebo digitálně podepsaná autoritou v hardware osob (oznamovací autentizace, lze přidat hardwarovou autentizaci -> dvoufaktorová)
– Porovnávání dokazovacích dat (změřená biometrika) a šablony
– Terminál po úspěšné autentizaci odešle ID do kontroléru

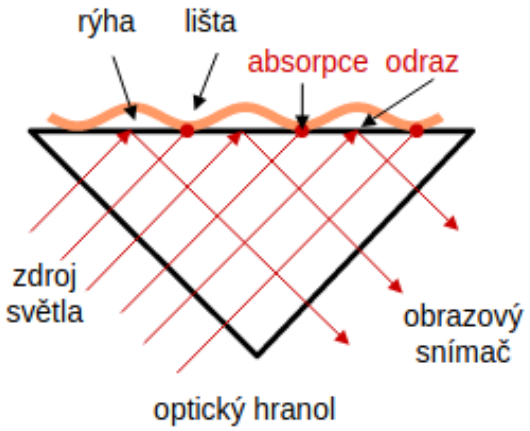
Správa

– Kontroléry z historických důvodů spravovány sběrnicí RS-485 – po ní přístupové seznamy
– Terminály vyžadují ověřovací seznamy, přes IP síť

7.2 Otisky prstů – princip a vlastnosti

– Papilární linie – lišty a rýhy
– Obrazová čtečka
  ◦ Optický hranol, světelný zdroj, CCD nebo CMOS snímač
  ◦ Lišty se hranolu dotýkají a záření pohltí. Tam, kde jsou rýhy, se světlo odrazí k snímači

- Nízká cena, odolnost proti statické elektřině
- Nutnost čištění snímací stěny hranolu, prst nesmí být umazaný
- Moderní – stačí máchnout, více prstů naráz



Obrázek 23: Obrazová čtečka otisků prstů

– Kapacitní čtečka
  - Maticový snímač – velké množství vodivé plošky zalité v izolační destičce
  - Prst je uzemněn kovovým rámečkem, měří se kapacita proti prstu (zemi)
  - Pokud je nad ploškou lišta, má větší kapacitu, než když je nad ní rýha
  - Z matice bodů se vytvoří matice obrazových bodů
  - Není potřeba čistit, může být umazaný prst
  - Dají se poškodit
– Ultrazvuková čtečka
  - Princip sonaru
  - Matice piezoelektrických měničů (vysílač i přijímač)
  - Na rozhraních se vlnění částečně odráží a částečně pokračuje
  - Pokud je nad bodem rýha, přijímač obdrží odraz od dolní strany snímací desky, horní strany a prstu (3 odrazy)
  - Pokud je nad bodem lišta, přijímač obdrží odraz od 2 stran desky, zbytek je prstem pohlcen
  - Drahý, ale odolný proti umazání i statické elektřině
– V otiscích se vyhledávají specifické útvary (markanty) – do šablony se zapisuje typ a souřadnice
– Porovnávání při ověřování – statistické metody na podobnost
– Sledované markanty: konec lišty, rozdvojení lišty, přechod nebo roztrojení lišty (vychází lišty do 4 směrů), jiné
– Ochrana před padělkem: Pulsování krve v prstu, pomocí Rayleighova záření
  - Čtečka s pulzním oxymetrem

        - Rayleighovo záření závisí na tom, jestli je krev okysličená nebo ne
        - V pásmu 660 nm – nižší úroveň záření u odkysličené krve, 940 nm – nižší u okysličené krve
        - Oběma částmi spektra prst ozařován, sledování změn v čase (hledání pulzů)
    - Multispektrální čtečka
        - Snímky různými barvami nasvícení, výsledek se integruje (různé vlnové délky – různá prostupnost)
        - Měření pulzu absorpcí červeného světla

7.3 Cévní řečiště prstu a dlaně – princip a vlastnosti

- Prst
    - Prosvěcování IR zářením (pohlcené hemoglobinem -> cévy tmavé), zachycování kamerou na druhé straně
    - Cévní řečiště není běžně dostupné – bezpečnost
- Dlaň
    - Hemoglobin pohlcuje fotony v IR pásmu 760 nm. Nasvícení -> Rayleighův rozptyl -> tmavé žíly -> zvýšení kontrastu -> extrahování mapy cévního řečiště

7.4 Obličej – princip a vlastnosti

- 2D
    - Fotografování -> obličejové metriky (nalezení významných bodů, vzdálenosti mezi nimi)
    - Nespolehlivá, nepřesná metoda, lze oklamat fotografií nebo videem
- 3D
    - Odrážení fotonů na zakřiveném objektu – fotony se odrážím různými úhly
    - Nasvícení pravidelným rastrem (desetitisíce bodů)
    - na zakřiveném objekt (obličeji) nebudou body stejně daleko
    - Vyhodnocení nepravidelností -> 3D model obličeje -> významné body -> jejich vzdálenosti

7.5 Duhovka – princip a vlastnosti

- Rozmístění a tvary skvrn na duhovce – individuální
- Snímání kamerou, převedení z polárních souřadnic do kartézských (mezikruží mapované na obdélník)
- 8 řádků, 256 sloupců (2048 plošek)
- Každá ploška – průměr pixelů

– Vlnková transformace – každý prvek transformované matice závisí na každém prvku původní matice
– Z transformované matice se vytvoří nová matice, která přiřadí 1 kladným hodnotám transformované matice a 0 ostatním. Lze tedy reprezentovat jako 2048 b.
– Zkoumá se dostatečná podobnost těchto 2048 b

8 Systémy na ochranu zboží

8.1 Účel a klasifikace

– Systémy určené k ochraně zboží před jeho krádeží v obchodech
– Bezprostřední ochranu zboží zajišťuje personál
– Systémy na ochranu zboží buď fyzicky znemožňují krádež (vitríny) nebo personálu umožňují sledovat chování zákazníků v prodejně (DVS) nebo signalizují případnou krádež personálu (stojany u východu)

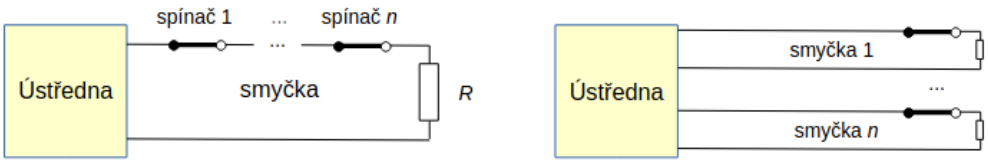
Klasifikace

– Zábranové systémy
  ◦ Úchyt (zamknutý laptop)
  ◦ Vitrína
– Dohledové systémy
  ◦ Systém zrcadel
  ◦ Dohledový videosystém
– Poplachové (elektronické) systémy
  ◦ Kontaktní (smyčkové) – spínač, rozepnutí smyčky spustí poplach
  ◦ Bezkontaktní – magnetické nebo elektromagnetické jevy, etiketa, která je neodstranitelná nebo odstranitelná speciálním přípravkem, na pokladně je odstraněna nebo deaktivována (detektory detekují jen aktivované tikety)
    · EM (elektromagnetické)
    · AM (akustomagnetické)
    · RF (rádiové)
  ◦ Na zboží se připevní generující prvek, který generuje příznaky incidentu (krádeže)
  ◦ V prodejně je detektor příznaků incidentů, zjištění předává ústředně, ta vyhlašuje poplach

8.2 Kabelové systémy – princip a vlastnosti

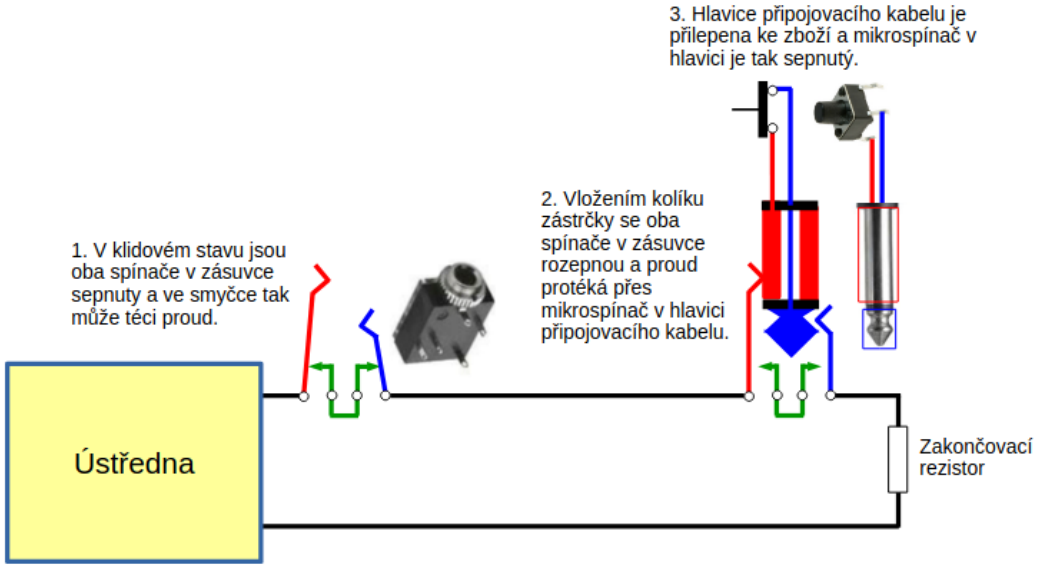
– Jednoduše vyvážená smyčka
– Mikrospínač, přilepený na zboží, tlakem sepnutý

– Při sepnutí smyčkou protéká proud daný nastavovacím rezistorem R
– Odlepením se spínač rozepne
– Poplach vyhlášen i při přerušení nebo vyzkratování smyčky
– 1 smyčka, do které se zapojuje veškeré zboží: starší
– K ústředně připojeno více smyček, na každé jiný výrobek: novější



Obrázek 24: Smyčkové systémy pro ochranu zboží

– Prvky:
  ◦ Ústředna
  ◦ Smyčky zakončené hlavicí s mikrospínačem
– Připojování: konektory typu Jack

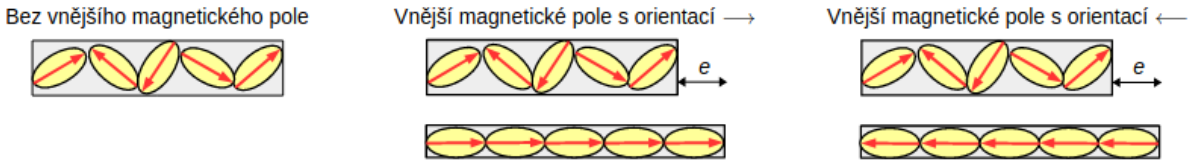


Obrázek 25: Smyčkový systém ochrany zboží

– Hlavice:
  ◦ Přilepovací, smyčkové, kleštinové
  ◦ Zásuvkové moduly (připojení antény televize v prodejně)
– Systémy s více smyčkami:
  ◦ Často pro připojení elektroniky
  ◦ USB, napájecí vodiče napájí vystavená zařízení, datové střeží (detekční smyčka), ale při ztrátě napájení je poplach také vyhlášen

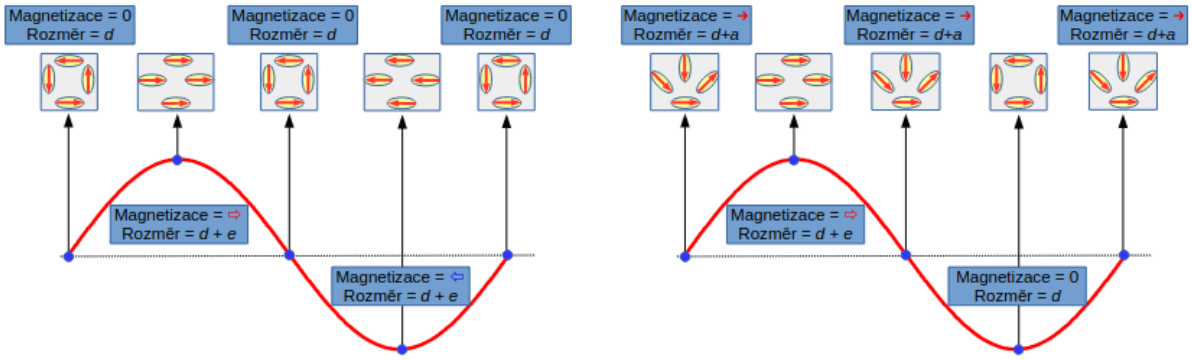
8.3 AM systémy – princip a vlastnosti

- Magnetostrikční jev
  - Magnetizace -> změna rozměrů magnetostrikčního materiálu (a magnetizace změnou rozměrů)
  - Elementární magnetické domény jsou mírně podélné (ve směru magnetizace delší)
  - Srovnání domén vnější magnetickým polem -> prodloužení materiálu
  - Typická etiketa má 40 mm, prodlužuje se asi o 25 μm



Obrázek 26: Magnetostrikční jev

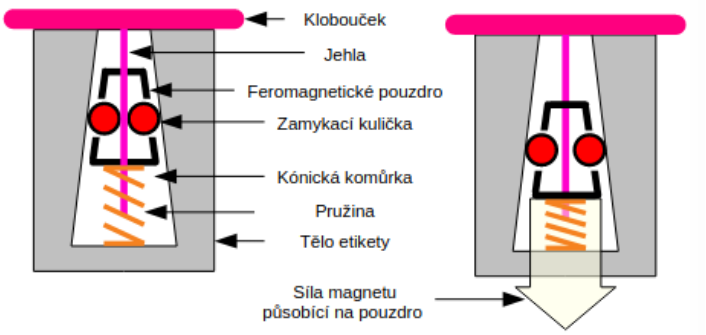
- Etiketa má magnetostrikční (nebo více než 1) a nastavovací proužek
- Detekce – budící magnetické pole
- Pokud je nastavovací proužek odmagnetovaný, domény se budou přetáčet podle magnetického pole, nekumulují mechanickou energii
- Pokud je nastavovací proužek aktivovaný, magnetostrikční proužek je mírně natažený i při absenci magnetického pole mimo etiketu, domény se ve vnějším harmonickém magnetickém poli kývají a kumulují mechanickou energii, po zániku vnějšího pole se ještě krátkou dobu setrvačností kývají a generují magnetické pole



Obrázek 27: Magnetostrikční jev v deaktivované a aktivované AM etiketě

- 58 kHz signál, 2 ms pulzy o odstupu 20 ms je budící
- V aktivovaném stavu nastane rezonance, po skončení budícího signálu asi 5 ms generuje aktivovaná etiketa vlastní pole o stejném kmitočtu
- Jeden stojan je vysílací, druhý přijímací

– Při deaktivaci proužek má rezonanční frekvenci dvojnásobnou (během cyklu bude dvakrát maximálně prodloužen, aktivovaný jen jednou, protože v jednom směru působí proti vnějšímu poli aktivační proužek)
– Deaktivace odmagnetováním (postupný přechod do středu hysterzní smyčky zmenšováním amplitudy magnetického pole)
– Etikety mohou být nalepovací nebo snímatelné
– Další etikety – na zátce láhve, na obalu CD a DVD, etiketa s inkoustovou náplní
– Snímání etiket
  ◦ Magnetický zámek – Jehla, kuličky (často 3), kónická komůrka, feromagnetická klec, pružina, kterou silný magnet přetlačí působením na klec



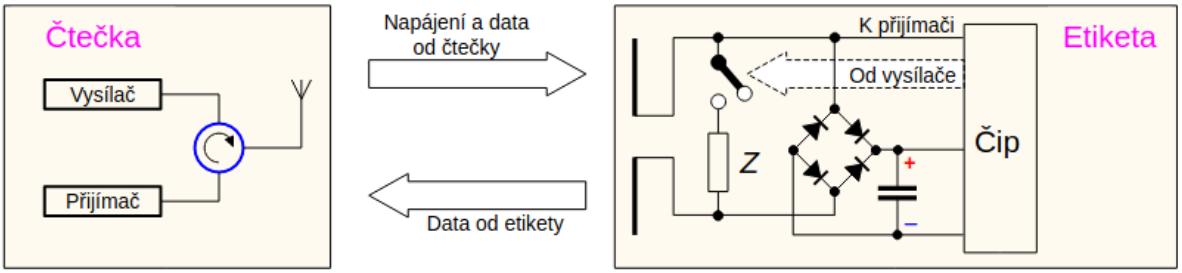
Obrázek 28: Snímatelná etiketa

– 3 až 5 m dosah
– Možnost fungování s jednou anténou (vysílač i přijímač v jednom, střídá se v čase)
– Vysoká spolehlivost detekce, odolné proti falešně pozitivním
– Možnost rušení rušičkou se stejnou frekvencí

8.4 RF systémy – princip a vlastnosti

– LC obvod
– Typy:
  ◦ RF s rozmítáním – starší, jednodušší
    · Vysílací anténa rozmítá elektromagnetický signál (nejčastěji 7,4 až 8,8 MHz)
    · Přijímací anténa přijímá signál o přibližně konstantní úrovni
    · LC obvod má rezonanční frekvenci 8,2 MHz, mezi vysílačem a přijímačem bude fungovat jako další vysílač, zvýší se úroveň signálu na přijímači
    · Etikety snímatelné nebo nalepovací, deaktivace probíhá proražením kondenzátoru
    · Nízká cena
    · Možnost odstínění a rušení – proti tomu detektor kovů
  ◦ RF s čipy RFID (typu EPC)
    · Radio Frequency Identification
    · 96 b EPC (Electronic Product Code)

- Etiketa má dipólovou anténu a čip
- Čtečka generuje harmonický signál 860 až 960 MHz
- Od čtečky k čipu – amplitudové klíčování (Amplitude Shift Keying)
- Od etikety ke čtečce – modulace zpětného rozptylu
  - Elmag. signál indukuje v anténě elektrický proud, který do okolí generuje vlastní elmag. pole (zpětný rozptyl)
  - Modulace dvou stavů: dvojí připojení čipu k dipólové anténě
  - Nejmenší zpětný rozptyl nastane, pokud je vstupní impedance rovna impedanci antény
  - Možnost připojení impedance Z, odráží energii do antény a intenzita zpětného rozptylu je maximální
  - Čtečka vysílá harmonický signál, pomocí cirkulátoru přepíná anténu mezi vysíláním a přijímáním (měří intenzitu zpětného rozptylu)



Obrázek 29: RFID etiketa

- Deaktivace zničením LC obvodu (rezonanční frekvence, vysoké napětí v obvodu, bum)
- Jedna anténa, individuální identifikátory etikety
- Možnost odstínění, rušení – proti tomu detektory kovů
- Integrace do platebního systému? Problém s deaktivací etiket útočníkem před pokladnou

9 Elektronické platební systémy

9.1 Účel

- Provádění plateb a jiných bankovních transakcí elektronickými prostředky na dálku
- Na transakci se podílí majitel účtu (klient) a banka (server)
- Důvěrnost dat
- Autentičnost dat
- Autentičnost stran
- Dosahuje se toho kryptografickými a autentizačními technikami

– Kryptografie -> bezpečný přenosový kanál, v něm se strany autentizují
– Autentizace serveru certifikátem, klienta heslem, biometrikou nebo hardwarem

9.2 Typy a jejich charakteristika

Podle typu terminálu:

– Telefonní
  ◦ Pevná linka i mobilní telefony
  ◦ V bankovnictví
  ◦ Autentizace telefonním číslem volajícího, případně doplnění heslem
  ◦ Přenášená data nebývají šifrována
  ◦ Techniky:
    · Hlasové – Klient zavolá na číslo banky, pomocí stisků kláves volí provádění operací, postupně se ruší
    · SMS – obchodník si sjedná smlouvu s operátorem, klient pošle operátorovi zprávu s kódem prodejce, zboží a případně prodejního místa, operátor převede částku z účtu klienta na účet prodejce a zašle příkaz k výdeji zboží (káva z automatu, jízdenka)
    · Datové – Elektronická platební karta je aplikace na telefonu, možnost použití kryptografie. Rozhraní GSM i NFC (modifikované ISO 14443), platby v obchodě nebo při vstupu do tramvaje. Další možnost je elektronické bankovnictví přes telefon
– Počítačové
  ◦ Webový prohlížeč
  ◦ Internetové bankovnictví, internetové nakupování
  ◦ Autentizace klientů heslem nebo certifikátem. Případně ještě zaslání jednorázového kódu platební operace mTAN na mobil
  ◦ TLS
  ◦ 3D Secure – HTTPS
    · Doména klienta: klient + jeho banka
    · Doména bank: banka klienta, platební brána, banka obchodníka
    · Doména obchodníka: obchodník + banka obchodníka
    · Algoritmus:
      – Klient na stránkách obchodníka objedná zboží. Když chce klient zaplatit, je přesměrován na platební bránu s potřebnými údaji (HTTP 303)
      – Na platební bráně doplní údaje, stiskne zaplatit
      – Platební brána zjistí přes chráněnou síť bank banku klienta
      – Klient se připojí k serveru banky klienta, autentizuje se
      – Banka rezervuje částku, přesměruje na platební bránu
      – Platební brána potvrdí klientovi platbu, přesměruje na stránky obchodníka, potvrdí obchodníkovi provedenou platbu

      - Přes bankovní síť se provede mezibankovní vyrovnání
    - PayPal
- Bankomatové
    - Výdej a vklad hotovosti
    - Terminály – bankomaty, ty sdílejí se svojí bankou tajný klíč
    - Autentizace klienta znalostí a vlastnictvím předmětu (platební karta, PIN)
    - Po zadání PINu klient zadá požadavek na transakci
    - Data o transakci jsou šifrovaná tajným klíčem bankomatu
    - Banka dešifruje, ověří PIN a zašle příkaz k provedení nebo neprovedení transakce
    - Útoky – získání údajů na magnetickém proužku karty a PIN (skrytá čtečka, falešná klávesnice, skrytá kamera)
- Obchodní platební systémy
    - Platba klientů v místě koupi zboží nebo služeb
    - Terminál – čtečka karet
    - Přiložení nebo vložení karty, případně PIN
    - Čip karty zkontroluje PIN, buď platbu potvrdí offline nebo přes terminál zašle dotaz do banky a po potvrzení bankou potvrdí platbu terminálu
    - Obchodník potvrzení karty zašle bance, ta provede převod z účtu klienta
    - Platební karta
        · S mikropočítačem (Smart Card)
        · Zpětná kompatibilita – reliéfní znaky, magnetický proužek
        · Číselný identifikátor
        · Podpis, CVV2 (Visa) nebo CVC2 (MasterCard)
    - Strany: Karta klienta, terminál obchodníka, banky klienta a obchodníka, platební brána
    - Standardy EMV (Europay, MasterCard, Visa) – primitiva a parametry pro platební protokoly karet
    - Banky si sestavují vlastní protokoly
    - Certifikáty – CA konsorcia EMV, v každém terminálu je uložen certifikát této CA
    - Spřažený (online, bezpečnější) a nespřažený platební protokol (offline, méně bezpečný)

9.3 Vysvětlit protokol TLS

- Transport Layer Security
- Verze 1.2:
    - Klient zašle unikát U_K a seznam kryptografických primitiv, které dokáže provádět
    - Server zašle unikát U_S, primitiva a certifikát CRT(VK_S)
    - Klient ověří VK_S, zvolí náhodné semeno R a zašle kryptogram $C = E(R, VK_S)$

- Server dešifruje R, z něj pomocí odvozovací funkce získají klíč $K = F(R, U_K||U_S)$
- Klient se později autentizuje heslem, server se autentizoval certifikátem

– Nad ním: 3D Secure (doména klienta, doména bank, doména obchodníka)

9.4 Vysvětlit nespřažený platební protokol

– Offline
– Bez účasti banky klienta, méně bezpečné, malé částky
– Karta je nabita finanční částkou, čerpání kontroluje čip
– Bezkontaktní, bez PINu
– K_C = klíč karty
– VK_C, SK_C veřejný a soukromý klíč karty
– VK_{BK}, SK_{BK} – podepisovací klíče banky klienta
– DC – data karty, identifikátor karty, banky, doba platnosti...
– DP – data platby (částka, měna, ID obchodníka, účet obchodníka...)
– Autentizace:
  - $CRT_{CA}(VK_{BK})$ – certifikát, veřejný klíč banky klienta (podepsaný CA)
  - $CRT_{BK}(VK_C)$ – certifikát o datech karty a veřejném klíči karty, podepsané bankou
– Terminál ověří certifikáty pomocí uloženého certifikátu CA, pokud důvěřuje, přijme
– Průběh:
  - Terminál předá kartě data platby
  - Karta předá certifikáty, terminál ověří a získá tím veřejný klíč karty
  - Terminál pošle náhodné číslo N
  - Karta podepíše N
  - Terminál ověří podpis, pošle kartě žádost o platební závazek
  - Pokud je v kartě dost prostředků, platební závazek se odešle. Je to podpis dat k platbě podepsaný kartou
  - Obchodník si hromadně nárokuje u platební brány nárok pomocí dat karty, dat platby a platebního závazku
  - Platební brána pošle data příslušným bankám, ty ověří správnost podpisu a převedou platbu na účet obchodníka
– Útoky:
  - Nevyžaduje aktivní účast majitele karty -> propojení čtečky karet s cizí platební bránou -> zaplacení útraty někým jiným
  - Relizace: Čtečka karet nevědomky u karty, připojená ke komunikačnímu rozhraní, které je v kartě útočníka
  - Provedení objednávky komunikačním rozhraním, ale karta, se kterou se bude komunikovat, patří oběti

10 Ochrany digitálních děl

10.1 Účel a klasifikace ochran

– Účel – vynucení kopírování a prezentaci autorských dat (což jsou data, v nichž jsou zakódovaná autorská díla) v souladu s omezeními, která stanovil auto těchto dat
– Pravidla – počet prezentací nebo počet pořízených kopií

Ochrany DRM (digital rights management)

– Metody digitálního vodoznaku
  ◦ Digitální vodoznak – data vložená do chráněných dat takovým způsobem, že je z těchto dat nelze odstranit
  ◦ Identifikační vodoznak – dokazuje vlastnictví
  ◦ Zamítající vodoznak – řídí přístup
  ◦ Zjevné vodoznaky (zpravidla identifikační), pozorovatel je snadno detekuje (např. změna jasu a barvy obrazových bodů, které vytvoří vodoznak, komentář rozhlasového moderátora v úvodu skladby)
  ◦ Skryté vodoznaky – nedetekovatelné, neodstranitelné, využití redundance
  ◦ Příklad skrytého: DCT vodoznak (Diskrétní kosínová transformace, u jpeg formátu, 8×8 pixelů, DCT převede matici A na jinou matici B, všechny prvky nové závisí na všech prvcích původní matice. Některé prvky nové matice se zkombinují s čísly vodoznaku $V = \{v_{ij}\}$, kde $v_{ij} \in \{-1, 1\}$, výsledná matice C, $c_{ij} = b_{ij} + g \cdot v_{ij}$ se zkomprimuje a uloží. g je zvolená konstanta.)
  ◦ Kontrola skrytého vodoznaku typu DCT (diskrétní kosinová transformace)
    · Autor zná matici B, vodoznak v_{ij} a konstantu g.
    · Dekompresí lze získat matici C', která je aproximací C.
    · Extrakce vodoznaku: $v'_{ij} = \left(c'_{ij} - b_{ij}\right)/g$
    · Statistický test, zda V je statisticky shodné s V'
    · Útočník nemá k dispozici pův. obrázek, nezná způsob vložení vodoznaku
    · Při pokusu o skrytí vodoznaku šumem zkreslí obrázek získaný inverzní kosínovou transformací
– Metody řízení přístupu
– Kryptografické metody
  ◦ Šifrování
  ◦ CSS:
    · Content-Scramble System
    · 1996, DVD
    · 1999 – DeCSS – CSS šifrovaný obsah na Linuxu
    · 40 b klíč proudové šifry

        - Správa klíčů – vyzrazení jednoho kompromituje celý systém
    - AACS:
        - Advanced Access Content System
        - AES, 128 b
        - Dynamický skupinový klíč
        - Každý přehrávač má unikátní sadu značek, klíč k dešifrování média je zašifrován, dešifrovat lze s užitím značek
        - Přehrávač v minulosti prozrazené lze vyloučit z přehrávání nových děl v budoucnu vytvořených
- Kombinace těchto metod

Klasifikace ochran DRM

- DRM ochrany vzdálené
    - S prodejem – přehrávač dílo prezentuje po elektronické platbě serveru
    - S povolením přehrávač dílo prezentuje po povolení serverem
- DRM ochrany lokální
    - S identifikací – autora nebo kupce lze dohledat pomocí vodoznaků
    - S řízením přístupu – přehrávač dílo prezentuje po splnění stanovených podmínek
        - Podmínky = vlastnosti média
        - Podmínky = vlastnosti přehrávače (typ nebo znalost tajného klíče)
        - Podmínky = znalost uživatele (znalost hesla)
- Kombinace

10.2 Vzdálené DRM ochrany – typy, principy a vlastnosti

- Prezentaci zajišťuje přehrávač, DRM ochranu vzdálený server
- Server může:
    - Autorská práva poskytovat (systém se vzdáleným úložištěm – např. prodejci hudby, data jsou odeslána po platbě)
    - Prezentaci autorských dat povolovat (systém dálkového dohledu – např. licencovaný software, přehrávač požádá server o prezentaci dat a autentizuje se. Při splnění licenčních podmínek, vydá server přehrávači povolení)
-

10.3 Lokální DRM ochrany – typy, principy a vlastnosti

- Bez síťového připojení, ochrana práv pouze přehrávač
- Kombinace typu média a přehrávače:
    - Běžné médium

- Univerzální přehrávač
  - Identifikační vodoznak
  - Identifikační údaje vlastníka práv nebo uživatele kupujícího data
- Speciální přehrávač
  - Řízení přístupu, využívá se znalost uživatele (vložení hesla -> dešifrování) nebo vlastnost přehrávače (jeho typ nebo tajný klíč v přehrávači, autentizační předmět – HW klíč, pro ochranu specializovaného software)
  - Přehrávač data přehraje jen při splnění podmínek
  - Speciální přehrávač může být z výroby nebo modifikaný univerzání přehrávač (např. PC, do kterého se vloží médium se speciálním programem, který ho modifikuje. Pak je potřeba splnění podmínek pro přehrání)
  - CD Cops – specializovaný přehrávač nepřečte z vypalovaného disku (pozná podle rychlosti čtení)
  - MediaMax – jiné chování při nalezení vodoznaku. Ve Windows Media Playeru driver fungoval správně, WMP přitom omezil počet pořízených kopií. V jiných přehrávačích driver zpožďoval a trhal stream
- Speciální médium a speciální přehrávač
  - Nintendo GameCube – DVD s čárovým kódem vypáleným speciálním laserem (BAC = Burst Cutting Area), kód se kontroluje, nedovolí čtení z disku bez kódu
  - Starší speciální médium – cartridge (ROM v kazetě)
- Speciální médium na běžném přehrávači nebude fungovat