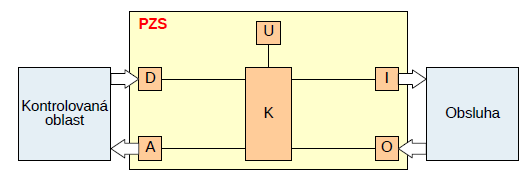
# Systém PZS

## Účel PZS

* Poplachový zabezpečovací systém = elektronický systém určený k detekci a signalizaci vzniku nežádoucích událostí – incidentů.
* Možné incidenty:
  + vnik / únik osoby z / do kontrolované oblasti
  + neoprávněná manipulace so stráženým předmětem
  + vznik nebezpečného prostředí v kontrolované oblasti (voda, oheň)
  + vznik požáru / tísňové situace

## Architektura PZS

* Ústředna U – řídí systém
* Detektory D – detekují incidenty a hlásí je ústředně
* Informační zařízení I – prezentují obsluze informace o stavu v kontrolované oblasti a o stavu systému
* Ovládací zařízení O – umožňuje obsluze systém ovládat
* Akční zařízení A – vykonává určené akce v kontrolované oblasti
* Komunikační systém K – umožňuje komunikaci mezi ostatními komponenty systému
* Detektory podávají ústředně hlášení. K základnímu hlášení náleží:
  + Klid – detektor je v pořádku a zatím nenastal incident
  + Poplach – detektor zjistil incident
  + Sabotáž – je detekovaný pokus o neoprávněnou úpravu chování detektoru

### Ústředna hlášení Poplach a Sabotáž oznamuje prostřednictvím informačních zařízení (siréna, smartfon) obsluze. Případně aktivuje akční zařízení, které mají být při Poplachu anebo Sabotáži aktivované (zamlžovací zařízení)

* Ústředna může být v různých stavech, jako například:
  + Zastřeženo: v tomto stavu se v kontrolované oblasti nemá nacházet žádná osoba. Ústředna v tomto případě obsluze oznamuje každé hlášení Poplach, resp. Sabotáž kteréhokoliv ze svých detektorů.
  + Odstřeženo: v tomto stavu se v kontrolované oblasti nacházejí oprávněné osoby. Ústředna proto hlášení Poplach od detektorů vniknutí ignoruje. Od ostatních typů detektorů (např. detektor požáru) je Poplach oznamovaný. Hlášení Sabotáž je oznamované vždy, a to od všech detektorů bez výjimky

## Prvky PZS

### Detektory PZS

* Detektory slouží k detekci incidentů (alias nežádoucích událostí)
* Využívá sa skutečnost, že sledovaný incident je doprovázen specifickými fyzikálními jevy, tzv. příznaky. Příznakem je například u přelézání plotu otřesy plotu, příznakem přítomnosti osoby je její tepelné záření apod.
* Detektory můžeme klasifikovat na:
  + Intruzní: slouží k detekci neoprávněných aktivit osob (vnik, manipulace s předměty)
  + Požární: slouží k detekci požáru
  + Tísňové: slouží k detekci tísňové situace
  + Substanční: slouží k detekci nežádoucí látky (voda, plyn)
* Vzhledem k primárnímu účelu PZS jsou intruzní detektory povinné a ostatní typy detektorů jsou volitelné
* Intruzní detektory jako příznaky zpravidla využívají projevy mechanických sil. (změna intenzity elmag. záření, zánik mag. pole apod.)

### Informační zařízení PZS

* Informační zařízení jsou určené pro obsluhu k prezentaci o stavu v kontrolované oblasti a o stavu systému.
* Informační zařízení jsou z bezpečnostních důvodů obvykle vybavená autonomním napájením, které je na ústředně nezávislé.
* Historicky nejstarší signalizační zařízení jsou například siréna anebo světelný maják. V případě incidentu je ústředna aktivuje, čímž obsluze dává tuto skutečnost na vědomí.
* Komunikace se signalizačními zařízeními je v proudové smyčce anebo po sběrnici.
* U proudové smyčky v klidovém stavu obvykle protéká smyčkou klidový proud. Signalizační zařízení ústředna aktivuje rozpojením smyčky. Zánik klidového proudu je pro signalizační zařízení příkaz k jeho spuštění.
* Při sběrnici je signalizační zařízení aktivované zasláním aktivačního příkazu s adresou signalizačního zařízení.
* V současné době jsou stále více než informační zařízení používaná datová zařízení jako je například počítač anebo smartfón.
* Ústředny musí být v takovém případě vybavené vhodným komunikačním rozhraním (např. RJ-45, Wi-Fi, GSM, RS-232 apod.)
* Aktivaci datového zařízení ústředna uskutečňuje zasláním aktivačního příkazu z datového zařízení.
* Datové zařízení informaci pro obsluhu prezentuje obvykle na displeji. Prezentace je provázena akustickým upozorněním

### Ovládací zařízení PZS

* K ovládání PZS sa používají ovládací klávesnice a opět datové zařízení – PC anebo smartfón.
* Ovládací klávesnice jsou k ústředně připojené obvykle pomocí sběrnice – např. RS-485
* Ovládací klávesnice je zpravidla kombinace numerické klávesnice a LCD displeje. Obsluha systém ovládá zadáváním číselného kódu a informace z ústředny zjišťuje z textových hlášení na LCD displeji.
* Modernější ovládací klávesnice mají grafický dotykový displej.

### Akční zařízení PZS

* K ovlivněni situace v kontrolované oblasti se používají akční zařízení. K jejich ovládaní sa používají proudové smyčky, ty spínají, resp. rozepínají relé.
* V praxi se typicky jedná o domácí automatizaci (např. zapnutí topení / otevření garáže)
* Z hlediska zabezpečení jsou nejvíc používaná světla a zamlžovací zařízení.
* Světla ústředna spíná při detekci incidentu, aby sa osvětlil prostor, a tak se mohlo hlášení o incidente pořádně vyšetřit.
* Zamlžovací zařízení je prakticky generátor mlhy, tj. drobných kapiček. Dokáže řádově v sekundách zamlžit prostor stovek metrů kubických v takové hustotě, že útočník ztratí orientaci a nemůže pokračovat v útoku

### Ústředna PZS

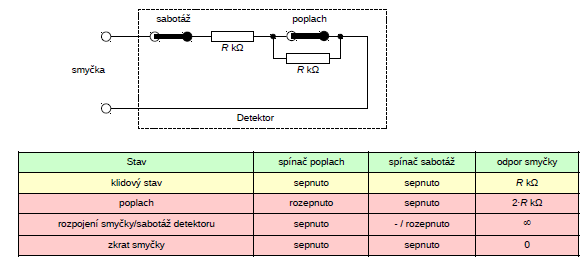
* Současné ústředny PZS jsou prakticky řídící počítače so specifickými perifériemi – informační, ovládací a akční zařízení a detektory.
* Z bezpečnostních důvodů je napájení systému zálohované průběžně dobíjeným akumulátorem. Výdrž akumulátoru je až několik desítek hodin.
* Typické rozhraní k perifériím:
  + svorky smyček k detektorům
  + svorky sběrnice – ku klávesnici
  + svorky výstupu – signalizační a akční zařízení
  + rádiový modul
  + USB rozhraní – spravující PC
  + GSM modul – připojení do GSM sítě
  + RJ-45 rozhraní – připojení do IP sítě

## Typy systémů PZS podle komunikace

### Kabelové systémy PZS

* Mají svoje prvky propojené pomocí metalických kabelů
* Vlastnosti:
  + (+) vyšší spolehlivost, jednoduchost
  + (-) nízká variabilita rozmístění čidel, vysoká cena kabelových rozvodů
* Kabelové systémy dělíme na:

1. **Smyčkové systémy**

* Jednotlivá zařízení jsou připojená k ústředně za pomoci proudových smyček. Výjimkou jsou ovládací klávesnice a datové zařízení, které se k ústředně připojují datovými spoji, či sítěmi (sběrnice RS-232, GSM síť apod.)
* Původně byly detektory připojované k ústředně v **jednoduchých smyčkách**. V detektoru bol poplachový spínač, který byl v klidovém stavu zapnutý. Smyčkou trvale protékal proud. V případě poplachu došlo k rozepnuti spínače, čímž proud v smyčce zanikl a ústředna vyhlásila poplach. Jednoduchá smyčka má 2 stavy a teda klidový proud a žádný proud. Pokud byla smyčka přerušená (sabotáž), tak klidový proud zanikl a byl vyhlášený poplach. Možný útok byl zkrat smyčky – proto sa začali používat vyvážené smyčky.
* V **jednoduše vyvážené smyčce** je v detektoru do série s poplachovým spínačem zařazen rezistor o hodnotě R. Ústředna průběžně měří odpor smyčky, takže klidový stav reprezentuje hodnota R. Při poplachu dojde k rozepnutí spínače a odpor vyroste na nekonečno – vyhlášení poplachu. Při sabotáži zkratem smyčky ústředna naměří odpor o velikosti nula – vyhlásí Sabotáž. Při útoku přerušením smyčky ústředna naměří nekonečný R a vyhlásí signál Poplach. Možný útok je sejmutí krytu a přemostění jeho poplachového spínače – ochrana sabotážní spínač. V tomto případě musí vést 2 vyvážené smyčky k detektoru – Poplachová a sabotážní smyčka. Jednoduše vyvážená smyčka je 3 stavová – klid, poplach/sabotáž, zkrat
* Pro snížení počtu vodičů pro zapojení detektorů se používá **dvojitě vyvážená smyčka –** tento způsob je v praxi nejrozšířenější. U některých výrobců detektorů se používá i k napájení detektoru.
* Někteří výrobci nabízejí trojitě vyváženou smyčku. K poplachovému a sabotážnímu spínači je doplněn poruchový spínač – možná signalizace poruchy na detektoru.

1. **Sběrnicové systémy**

* Často označované jako systémy s přímou adresací zařízení
* Z ústředny společná datová sběrnice, ke které se připojují zařízení
* Využívaný standard RS 485
* Sběrnice je nejčastěji realizovaná kroucenými páry, přenášené bity jsou reprezentované polaritou napětí mezi vodiči krouceného páru
* Komunikační protokol: Dotaz(ústředna) – odpověď(detektor)
* Každý detektor má svoji unikátní adresu, a tak nedochází ke kolizím
* Omezený počet detektorů – 32 je kompromis
* Výhody: jednoduchá kabeláž
* Nevýhody: detektory jsou komplikovanější a dražší

1. **Kombinované systémy**

* Kombinace sběrnicového a smyčkového systému
* Na společnou sběrnici ústředny jsou připojené tzv. expandéry – ty komunikují s ústřednou po sběrnici
* Na expandéry se smyčkami sa připojují detektory
* Každý expandér nepřetržitě monitoruje stav svých detektorů
* Ústředna cyklicky zasílá výzvy jednotlivým expandérům a ty zasílají odpověď o stavu připojených detektorů
* Dobrý kompromis z hlediska složitosti kabeláže a nákladů na systém

1. **Rádiové ústředny PZS**

* Jsou ústředny sběrnicového typu
* Rádiové pásmo 434, 868 anebo 2400 MHz
* Přenos je poloduplexní, takže ústředna vyšle dotaz a adresované zařízení na stejné frekvenci odešle odpověď
* Dosah ve volném prostoru až stovky metrů
* Výhody: žádné kabelové rozvody
* Nevýhody: možnost rušení, útoky falešnými signály, napájení bateriemi

# Předmětové a překážkové detektory

## Typy detektorů z hlediska vícevrstvé ochrany

* **Vícevrstvová ochrana** je nejvíc používaná strategie pro rozmístění detektorů, kde strážená aktiva jsou obklopena několika liniemi překážek a detektorů. Příklad: Nejprve se musí útočník dostat přes plot P areálu (1.linia), dále musí projít přes pozemek Z k plášti budovy B (2.linia), proniknout pláštěm do vnitřku budovy (3.linie), následně sa dostat interiérem I budovy až k vitríně V (4.linie), proniknout do vitríny (5.linie), zmocnit sa předmětu A (6.linie) a nakonec areál opustit.
* **Předmětové** – detekuje útoky na určený předmět
* **Interiérové** – detekuje nositele hrozby uvnitř
* **Plášťové** – detekuje útoky na plášť budov
* **Exteriérové** – detekuje nositele hrozby venku
* **Překážkové** – detekuje útoky na hranici areálu

### Objektové detektory

* Objektové detektory můžeme dále klasifikovat na : Předmětové a Překážkové detektory
* Předmětové detektory jsou určené k detekci neoprávněné manipulace se střeženým předmětem.
* Překážkové detektory jsou určené k detekci neoprávněné manipulace s překážkou.
* Překážkou budeme rozumět pevnou materiálovou strukturu, která má útočníkovi znemožnit přístup do prostoru za překážkou. Překážkami jsou nejčastěji ploty, hraniční zdi pozemků, pláště budov a pláště úložišť.
* Pojmem plášť budovy sa zpravidla označuje venkovní hranice budovy, tj. jej venkovní zdi, střecha, a venkovní stavební výplně (dveře, okna)
* Úložištěm budeme rozumět například trezory, skříně, anebo vitríny a pláštěm úložiště budeme rozumět venkovní hranice okolo tohoto úložiště.

### Prostorové detektory

* Prostorové detektory jsou určené k detekci pohybu útočníka kontrolovanou oblastí.
* Důležitá charakteristika prostorových detektorů je tzv. detekční diagram. Ten představuje část prostoru, v kterém může daný detektor případný incident detekovat.
* Podle tvaru detekčního diagramu budeme prostorové detektory klasifikovat na:
  + objemové detektory
  + hraniční detektory
* Objemové detektory mají detekční diagram v podobě trojrozměrného geometrického útvaru. Pokud se útočník začne vevnitř tohoto útvaru pohybovat, tak způsobí poplach.
* Hraniční detektory mají detekční diagram v podobě plochy anebo linie, kterými se v kontrolované oblasti definují virtuální hranice. Pokud útočník tuto hranici překročí tak dojde k vyhlášení poplachu.

## Typy předmětových detektorů – účel a jejich fyzikální princip

* Jsou určené k detekci neoprávněné manipulace se střeženým předmětem např. obraz, socha váza ...
* K nejrozšířenějším předmětovým detektorům patří:
  + Tíhové detektory: příznakem incidentu je změna tíže, kterou předmět působí na detektor
  + Akcelerační detektory: příznakem je zrychlení detektoru spojeného s předmětem.
* Podle typu vazby předmětového detektoru se stráženým předmětem můžeme rozlišovat externí a interní instalaci.
* V případě externí instalace se detektor nachází mimo střežený předmět. Předmět na detektoru obyčejně visí či na něm stojí.
* Při interní instalaci je detektor zase naopak součástí předmětu. Často jsou navzájem slepené

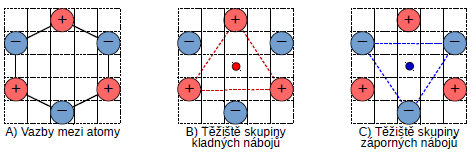
### Tíhové detektory

* Tíha je síla, kterou působí těleso v tíhovém poli na závěs anebo na podložku
* Tíhové detektory detekují neoprávněné přemístění chráněného předmětu ztrátou tíže, kterou na ně tento předmět za normálních okolností působí
* Jako senzory tíže sa obvykle používají piezoelektrické senzory a tenzometry.
* Typy tíhových detektorů:
  + závěsové detektory: sledují tíhu, kterou zavěšený předmět působí na detektor v podobě závěsu (obraz)
  + podložkové detektory, sledují tíhu, kterou předmět působí na detektor v podobě podložky (sošky, vázy apod.)

1. **Závěsové detektory**

* Sledují tíhu, kterou zavěšený předmět působí na táhlo. Příklad háček na zavěšení předmětu.
* Jako senzory tahu sa obvykle používají piezoelektrické snímače. Po zavěšení vyvine předmět na piezoelektrický snímač silu F. Ta způsobí deformaci piezoelektrické destičky a její polarizaci. Přes rezistor spojující elektrody proto následně poteče proud **-I**, čím dojde k vyrovnání potenciálů elektrod a detektor přejde do stavu hlídání.
* Sundáním předmětu dojde ke ztrátě síly F a následně k zániku polarizace destičky. Vyrovnáním potenciálů obou elektrod je spojené se vznikem proudu **+I**, což je zároveň příznakem k vyhlášení poplachu.

**Piezoelektrický jev:**

Pokud jsou určité látky, piezoelektrika, mechanicky namáhané (tlakem), tak se elektricky polarizují. V praxi se používají piezoelektrické krystaly (křemen) a speciální keramika. Máme šestiúhelníkovou piezoelektrickou mřížku. Těžiště kladných a záporných atomů. Atomy ve vertikálních vazbách krystalu se v důsledku odpudivých sil mezi svými jádry mohou pohybovat velmi omezeně. Horní kladný atom a dolní záporný atom jsou však vázané se sousedními atomy šikmými vazbami. V krystalu se tak můžou vertikálně posouvat na větší vzdálenosti. Vnějším tlakem dojde k posunu atomu. Vrcholové atomy jsou zatlačené do hloubky krystalu a tím se změní těžiště obou skupin nábojů. Z krystalu vznikne elementární dipól. Účinkem všech elementárních dipólů v materiálu se na horní straně piezoelektrika objeví záporný náboj a na dolní straně kladný náboj. Analogicky dojde k polarizaci i tahům.

1. **Podložkové detektory**

* Nejčastěji sa používají na ochranu cenných stojících předmětů, jako například vázy, sochy ...
* Předtím se používaly detektory s mikrospínačem. Předmět svou váhou spočíval na mikrospínači a zajištoval tak zapnutý stav mikrospínače. Odebráním předmětu se mikrospínač rozepnul a byl vyhlášený poplach.
* Modernější a mnohem bezpečnější sú detektory s piezoelektrickým snímačem, anebo tenzometrem. Ich principem je měření tíhy předmětu postaveného na detektor a reakce na změny této tíže.
* Moderní podložkové detektory se vyrábějí v řadách, které můžou chránit předměty o hmotnosti v rozsahu desítek gramů až desítek kilogramů. Reagují na změnu hmotnosti už od 10 gramů.

**Tenzometry:**

Tenzometr je snímač k měření mechanického napětí na povrchu předmětu. V bezpečnostních aplikacích se obvykle používají fóliové tenzometry. V tomto případě je kovový materiál nanesený v tenké vrstvě do tvaru protáhlých meandrů na pružný plátek. Plátek tenzometru se přilepí vhodným lepidlem na povrch předmětu tak , aby podélně rovnoběžné vodiče byly ve směru měřeného mechanického napětí. V důsledku tahu, resp. tlaku na předmět dojde i k natáhnutí, resp. zkrácení podélně rovnoběžných vodičů tenzometru. Dojde tedy k prodloužení, resp. zkrácení délky vodiče L na délku L´ a zároveň k zmenšeni, resp. zvětšení kolmého průřezu S vodiče na průřez S´. Při měrném odporu ró následně dojde k změně odporu tenzometru R=ró x L / S na R´=ró x L´ / S´. K měření hmotnosti předmětů se obvykle používají tenzometry umístněné v nosníku. Jeden konec nosníku je pevně ukotvený a druhý konec je volný. Zatažením volného konce nosníku stráženým předmětem dojde k ohybu nosníku. Vzniknuté mechanické napětí se v našem příkladě měří dvěma tenzometry zapojenými do Wheatstoneova můstku. Napětí U závisí přímo úměrně na hmotnosti stráženého předmětu, tj. platí, že U =k.m, kde je k konstanta.

1. **Akcelerační detektory**

* Manipulace s předmětem vyžaduje vždy sílu, a tak podle 2. Newtonova zákona je manipulace spojená so zrychlením předmětu. K detekci neoprávněné manipulace s předmětem tedy můžeme využít měření zrychlení předmětu.
* Ke stráženému předmětu sa jednoduše připevní detektor s akceleračním snímačem a v případě, kdy je změřené nenulové zrychlení, je vyhlášen poplach.
* Akcelerační snímače se mimo předmětových detektorů používají i u překážkových detektorů.
* Z předmětových jsou nejznámější translační detektory – detekce pohybu předmětu
* Z překážkových jsou nejčastější otřesové detektory – detekce překonávaní překážky
* Translační detektor – obsahuje akcelerometr. Připevní se k předmětu a v případě pohybu akcelerometr změří nenulové zrychlení a vyhlásí poplach. Pásmo 434 a 868MHz. Nadějný trend je univerzální detektor typu RFID – obsahuje i jiné snímače. Vysílají periodicky teplotu, vlhkost a polohu.

**Akcelerometr**:

Jsou to zařízení na měření zrychlení. Jádro akcelerometru je závaží, které je so zbytkem akcelerometru spojené fyzikální vazbou, která umožňuje sílu F, která působí na závaží, změřit. V detektorech se obvykle používají akcelerometry: piezoelektrické a kapacitní. Používané akcelerometry jsou obvykle jednoosé anebo trojosé.

## Typy překážkových detektorů – účel a jejich fyzikální princip

* Souží k detekci neoprávněné manipulace s překážkou.
* Příkladem neoprávněné manipulace s překážkou je přelézání hraničních zdí, přestřihnutí pletiva plotu, bourání otvoru ve stěně, vyrážení dveří, otevření nezajištěného okna či přeřezávání pláště trezoru pomocí plamenu.
* Nejčastější typy překážkových detektorů:
  + detektor otevření: detekce otevření dveří anebo oken
  + detektor tříštěni skla: detekce rozbití skleněné tabule
  + otřesový detektor: detekce pokusu o překonání překážky
* překážkový detektor můžeme chápat i jako předmětový detektor. Umožňuje detekovat neoprávněnou manipulaci s předměty jako jsou dveře, okna, stěny ploty apod. Tyto předměty však nejsou primárně chráněná aktiva. Proto budeme předmětové a překážkové detektory rozlišovat, i když z technického hlediska jsou často řešené podobně.

### Detektor otevření

* Jsou určené k detekci otevření otevíracích výplní stavěných otvorů, jako dveře a okna
* Detektory otevření jsou z technického hlediska direktní detektory, a jejich generátorem budící energie je permanentní magnet a snímač jazýčkový, resp. kuličkový magnetický spínač.
* Magnetický spínač se instaluje na rám dveří, resp. oken a magnet sa připevňuje na křídlo dveří, resp. oken. Z hlediska montáže jsou povrchové a zápustné spínače.
* V klidovém stave jsou dveře, resp. okno zavřené, magnet se nachází v těsné blízkosti magnetického spínače, a tak je tento spínač zapnutý. Magnetický spínač plní v smyčce k ústředně funkci poplachového spínače a ústředna proto interpretuje stav ve smyčce jako klid.
* Pokud někdo dveře otevře, resp. okno otevře, tak se magnet na křídle dveří vzdálí od spínače. Ten sa proto rozepne a vyhlásí poplach.

### Detektor tříštění skla

* Slouží k detekci rozbití skleněné tabule
* Snímač zachytává otřesy okenní tabule anebo zvuky v místnosti. Zachycené signály jsou spektrálně analyzované k nalezení příznaku tříštění skla (Signál o velmi nízké frekvenci následovaný signálem o frekvenci okolo 4kHz)
* Poznáme:
  + kontaktní: piezoelektrický snímač přilepený na sklo
  + bezkontaktní: mikrofonní snímač umístněný v místnosti
* U kontaktních detektorů tříštěni skla je potřebné umístit detektor na každou skleněnou tabuli. Výhodou mikrofonních detektorů je, že jeden detekuje vše v rámci jeho rozsahu cca 5 až 10 metrů.

### Otřesové detektory

* Slouží k detekci pokusu o překonáni překážky
* Podle rozsahu dělíme:
  + lokální
  + distribuované
* Lokální otřesové detektory slouží na ochranu trezorů a stěn místností
* Distribuované otřesové detektory se používají na ochranu rozsáhlých překážek jako jsou ploty anebo stěny budov

1. **Lokální otřesové detektory**

* Detekce pokusu o průraz dveřmi, stěnami, podlahami a stropy... mechanické poškozeni pláště budovy
* Snímačem je nějaká varianta akcelerometru.
* Poznáme:
  + s kapacitním, piezoelektrickým akcelerometrem
  + s kuličkovým indikátorem akcelerace

1. **Distribuované otřesové detektory**

* Nejvíc se používají plotové kabely
* Slouží k detekci překonávání plotu, hraničních zdí...
* Plotové kabely sa připevňují na plot
* Typy otřesových kabelů:
  + kabely založené na elektrostatické indukci
  + kabely založené na elektromagnetické indukci
    - V spojitém režimu provozu
    - V pulzním režimu provozu

# Objemové a hraniční detektory PZS

**OBJEMOVÉ DETEKTORY**

* Mají detekční diagram v podobě trojrozměrného geometrického útvaru. Pokud se útočník začne pohybovat vevnitř tohoto útvaru, tak způsobí vyhlášení poplachu.
* Jedná sa asi o nejrozšířenější třídu ze všech detektorů.
* Výhodou je ich nízká cena a dobrá pravděpodobnost detekce útočníka
* Umisťují se hlavně v interiérech, kde sa nacházejí aktiva, tak i na přístupech k těmto prostorům
* Typy:
  + pasivní infračervené (PIR) detektory
  + mikrovlnné (MW) detektory
  + duální (PIR+MW) detektory

**HRANIČNÍ DETEKTORY**

* Jsou to prostorové detektory a ich detekční diagram má podobu plochy anebo linie
* Pomocí těchto plach a linií se v kontrolované oblasti definují virtuální hranice a pokud tyto hranice útočník překročí, tak dojde k vyhlášení poplachu
* Detekční diagram je prostorový útvar, v kterém detektor může incident detekovat
* každý útvar má tři rozměry x y z
* Typy:
  + plošné: detekční diagram má podobu plochy
  + liniové: detekční diagram má podobu linie

## Typy objemových detektorů – účel a ich fyzikální princip

### Detektory PIR

* V pravém slova smyslu nedetekuji osoby, ale pohybující se objekty o teplotě lidského těla
* V případě pohybu objektu směrem k detektoru anebo od něho je detektor citlivý nejméně. Pomalým přibližováním útočníka sa napětí U na destičkách zvyšuje pomalu. Proud I rezistorem R je a útočník nemusí být detekovaný.
* Nejcitlivější je detektor pro tzv. tangenciální směr pohybu, tj. kolmo na detektor, kdy pyroelektrické destičky zachytávají záření objektu střídavě a jejich napětí, a i proud I se rychle a významně mění.
* U detektoru PIR je potřebné zajistit přímý výhled do stráženého prostoru.
* Není vhodné ho umisťovat proti oknům a zdrojům tepla. Záření slunce, anebo reflektorů přes okna a zapnuté topené můžou být zdrojem falešných poplachů.
* Jsou pasivní, takže můžeme umístit i více detektorů v jednom prostoru a nebudou sa ovlivňovat

1. **Princip:**

* Infračervené záření, které se šíří ze stráženého prostoru je pomocí soustavy Fresnelových čoček soustředěné na pyroelektrický snímač
* Spektrum záření je okolo 9,4 mikrometru – v něm tělo září nejvíc
* Pyroelektrický snímač převádí změny intenzity toku IR záření na změny elektrického napětí. Změny napětí jsou analyzované a pokud intenzita a velikost těchto změn překročí hraniční hodnoty tak je vyhlášený poplach.
* Fresnelova čočka slouží ke zvýšení dosahu detektoru. Detektory jsou obyčejně vybavené soustavou čoček, které jsou nalisované z teflonu a vhodně tvarované. Na PIR snímač dopadá IR záření z různých směrů, čímž se zvětšuje detekční prostor.
* Jádrem PIR detektoru je pyroelektrický snímač, v kterém se nacházejí dvě pyroelektrické destičky v rozdílovém zapojení. Tím sa eliminují rušivé jevy jako je například změna teploty vzduchu v místnosti a mechanické otřesy. Každá čočka před snímačem rozdělí snímanou oblast na dva laloky a slepou zóny mezi laloky. Jestliže se intenzita IR záření na obou destičkách rovná, tak napětí se rovná nule – klid.

Pokud se v druhém laloku objeví útočník tak dojde k rozdílu napětí a je vyhlášený poplach.

1. **Typy čoček pro PIR:**

* Soustava Fresnelových čoček se v praxi nazývá jen čočka
* Nejčastěji používáme:
  + klasická čočka – detekční diagram tvoří šikmo sklopené vějíře
  + chodbová čočka – detekční diagram tvoří velmi úzké a dlouhé vějíře
  + záclonová čočka – detekční diagram tvoří dva úzké a vertikálně postavené vějíře
* Obvykle sa používají klasické čočky. Chodbové na dlouhé chodby a záclonová na detekci průniku útočníka dveřmi anebo okny
* Detektory PIR imunní vůči zvířatům: zvířecí čočka je konstruovaná tak, aby detekční diagram končil několik cm nad zemí; detektor s dvěma snímači (jeden nahoře, jeden dole) – k vyhlášení poplachu je potřebná detekce útočníka oběma snímači.

### Mikrovlnné detektory

* Fungují na základě Dopplerova jevu
* Využívá se rádiové záření obvykle okolo 10GHz
* Generátor G generuje signál o kmitočtu, který je vysílací anténou vyzařovaný do prostoru. Signál odrazený od pohybujícího sa objektu je zachycený přijímací anténou, přičemž jeho kmitočet se rovná vysílaná frekvence plus mínus dopplerovský posun.
* Přijatý a vysílaný signál jsou přivedené na vstupy zmiešavača S a na jeho výstupu se vybírá signál s rozdílovým kmitočtem Fp-Fv=e. Pokud e se nerovná 0, tak je vyhlášený poplach.

1. **Vlastnosti:**

* MW detektory nedetekuji osoby ale pohybující sa objekty
* Pokud je pohyb objektu směrem k detektoru anebo od něho, tak dopplerovský posun e je maximální a detektor je nejcitlivější. Při směru kolmém k radiálnímu je hodnota e rovna nule a pohybující se objekt nelze detekovat.
* Nastaveni MW detektorů je složitější a může dojít často k falešnému poplachu, protože detektor při špatném nastavení sleduje stav aj mimo střeženou zónu (například rádiové vlnění prochází i okny).
* MW detektory je nutné umístit tak, aby nebyly ve vzájemném dosahu.

### Duální detektory

* jsou obvykle kombinace detektoru PIR a MW
* touto kombinací se eliminuje slabina každého z nich pomocí předností toho druhého
* K vyhlášení poplachu se dá obyčejně zvolit buď součinovou logiku (jen když oba detekují) anebo součtovou logikou (stačí když jeden z nich detekuje)

## Typy hraničních detektorů – účel a jejich fyzikální princip

### Hraniční liniové

* Jsou prostorové detektory s detekčním diagramem v podobě linie, tj. jeden z rozměrů je dominantní a ostatní jsou zanedbatelné
* Klasifikujeme na:

**Zemní:** (jejich snímače jsou zakopané v zemi)

1. Štěrbinové kabely s kontinuálním režimem
   * + Základem je speciální koaxiální kabel se štěrbinami v plášti
     + Zakopaný vysílací kabel štěrbinami v plášti kontinuálně vyzařuje vf. energii do okolí a souběžně vedený přijímací kabel svými štěrbinami vyzařovanou energii přijímá
     + Vstupem útočníka do pole mezi kabely dojde k změnám parametrů tohoto pole (obvykle jeho amplitudy a fáze), což způsobí vyhlášení poplachu
     + Nevýhoda je, že sa nedá přesněji určit místo
2. Štěrbinové kabely s pulzním režimem
   * + Dva štěrbinové kabely – vysílací a přijímací
     + Vysilač vysílá periodicky velmi krátké vf pulzy. Pulz se šíří vysílacím kabelem, a přitom část jeho energie je ve formě elmg. pole vyzařovaná do okolí
     + Energie elmg. pole se přes štěrbiny indukuje do přijímacího kabelu a indukované pulzy sa šíří k přijímači
     + Podle okamžiku přijetí pulzu se dá na základě rychlosti šířeni signálu odvodit, v jaké vzdálenosti došlo k přenosu energie mezi vysilačem a přijímacím kabelem
     + Amplitudy přijatých pulzů pro různé vzdálenosti se statisticky vyhodnocují
     + Pokud útočník kabely překročí ve vzdálenosti d, tak se v tomto místě ovlivní šíření elmg. pole mezi kabely. Amplituda pulzu z této vzdálenosti tak bude významně odlišná od statistického průměru a detektor vyhlásí poplach.
3. Zemní optovláknové kabely
   * + Kabel s běžným jednovidovým opt. vláknem je zakopaný v několika meandrech do země. Snímače jsou však natolik citlivé, že jsou použitelné i jako plotové detektory.
     + Opt. vlákno funguje jako liniový snímač, který po celé svojí délce snímá mechanické otřesy ze svého okolí.
     + Analýzou zachycených otřesů se dá ve vzdálenosti jednotek až desítky metrů od kabelu detekovat kráčející osoba, jedoucí vozidlo anebo přelet lehkého letadla.
     + Výhodou těchto senzorů je délka střežené linie – až desítky km. Určit, která část kabelu otřesy zachytila, se dá s přesností na metry
     + Kabel je reflexní detektor, využívá se Rayleighův rozptyl a skutečnost, že tlakem na vlákno ve vzdálenosti d, se v tomto místě zmenší průměr, a tedy se tu zvětší i hustota nehomogenit. To sa projeví vyšším počtem fotonů navrácených z vlákna ve vzdálenosti d.
     + V praxi sa dosahuje metrová přesnost u kabelu i několik desítek km dlouhého.
4. Seizmické detektory
   * + Jedná se prakticky o akcelerometry, které snímají akceleraci spojenou s otřesy země
     + Obvykle jsou tvořené silným magnetem, po jeho obvodě je pružně zavěšená cívka.
     + Otřesy země způsobují pohyb magnetu uvnitř zavěšené cívky a v cívce se indukuje napětí. Časový průběh napětí a spektrum signálu sa analyzuje
     + Každý kolík obsahuje akcelerometr, který je spojený kabelem s centrální jednotkou. Kolíky sa zapichují do země po několika metrech od sebe v požadované linii. Centrální jednotka amplitudově a spektrálně vyhodnocuje otřesy zachycené z okolí jednotlivých kolíků. Při detekci příznaku incidentu vyhlásí poplach.

**Nadzemní:**

1. Mikrovlnné liniové detektory (MW bariéry)
   * + Jsou direktním typem detektoru
     + Vysílač V vysílá směrem k přijímači P signál v pásmech 5, 10 anebo 24GHz. Prakticky všechna vysílaná energie je sestředěná do úzkého elipsoidu mezi V a P
     + Útočník při vstupu do elipsoidu působí jako překážka, takže dojde k poklesu úrovně přijímaného signálu
     + Dosah MW závor může být až stovky metrů
2. Infračervené liniové detektory (IR závory)
   * + Jsou direktním typem detektoru, který se skládá z vysilače a přijímače – většinou podoba stojanu
     + Zdroj záření je IR dioda LED a snímač fototranzistor. Před diodou i tranzistorem je čočka. Jejich účelem je soustředit IR záření do podoby co nejužšího svazku. Dosahuje tak stovky metrů.
     + Svazky můžou být uspořádané různými způsoby.
3. Radarové
4. Kmitočtově modulovaný a spojitě vysílající radar (FM-CW radar)
   * + Vysílá rádiový signál nepřetržitě a detekuje časově posunutý pilovitý signál odrazený od objektu. Pokud dojde ke změně doby šíření signálu, tak sa vyhlásí poplach.
5. FM-CW radar Dopplerovský
   * + Bere do úvahy i Dopplerův jev způsobený pohybem objektu. Radar je výrazně složitější ale výsledky měření jsou informačně bohatší, protože kromě azimutu a vzdálenosti je známý i směr a rychlost pohybu objektu, což umožňuje přesnější vyhodnocování výsledku

### Hraničné plošné

1. PIR detektory se záclonovou čočkou
2. Lidarové detektory
   * + Alias 2D laserový skener
     + Lidar je prakticky optický analog radaru
     + Vysílač v určeném směru vyšle pulz IR laserového záření a měří dobru T do přijetí IR energie odražené od nejbližšího objektu v daném směru
     + Vysílač cyklicky mění směr vysíláni v určitém uhlovém rozsahu, takže se dá monitorovat výskyt objektů v rovině vymezené tímto úhlem
     + Mohou být použité i k ochraně předmětů – hraniční rovina je vertikální a je umístěná mezi stráženým předmětem a prostorem, odkud může přijít útočník. Pokud útočník svým tělem naruší hraniční rovinu, tak je vyhlášený poplach. Moderní detektory umožňuji přesně definovat oblast strážení.
3. Kamerový systém s analýzou obrazu

# Dohledové video systémy

* Slouží ke vzdálenému sledování stráženého prostoru

## Účel

* Je určený k snímáni, prezentaci a ukládání obrazových dat o dění ve střežené oblasti
* Dění ve vybraných částech kontrolovaných oblastí se pomocí vhodného zařízení snímá a následně převádí na elektrický signál, který je potom přenášený do dohledového centra. Tam jsou signály z jednotlivých zón prezentované ve formě videa.
* Typy systémů podle přenášeného signálu
  + Analogové – signál z kamer je analogový
  + Digitální – signál z kamer je digitální

## Základní prvky

### Kamery

* Slouží k snímáni obrazu sledovaného prostoru
* V současnosti se nepoužívají analogové, ale digitální kamery:
  + Analogové – pracuji s obrazovým signálem v analogové podobě (PAL,NTSC,HD)
  + Digitální – signál v digitálně komprimované podobě (H.264,JPEG)
  + Dohledové – majitel kamery je používá ke sledování událostí ve vlastním prostoru
  + Skryté (štěnice) – majitel kamery ji používá ke sledováni událostí v cizím prostoru
  + Statické – snímají obraz v předem určeném směru
  + Ovládané – umožňuji měnit záběr podle aktuální potřeby
    - * Směrově statické – obraz můžeme vzdalovat, resp. přibližovat, avšak jen v předem určeném směru
      * Směrově dynamické – obraz můžeme nejen vzdalovat a přibližovat, ale současně i natáčet a naklánět kameru (horizont/vertikál) tzv. PTZ kamery („Pan, Tilt, Zoom“)

### Videorekordér

* Jádrem každého DVS je zařízení, které se sice trochu nepřesně, ale skoro výhradně nazývá videorekordér
* Umožňuje připojit kamery, ovládací zařízení a lokální i vzdálené monitory
* Získané signály jsou videorekordérem zasílané do monitorů k jejich zobrazení, a ukládá je do úložišť, odkud je možné záznamy přehrávat
* Klasifikace videorekordérů:
  + Digitální videorekordéry (DVR) – kamery jsou k videorekordéru připojené koaxiálními kabely
  + Síťové videorekordéry (NVR) – kamery jsou k videorekordéru připojené přes PC síť (switch)

### Ovládací zařízení

* Umožňuje zvolenou kameru natáčet či naklánět a přibližovat anebo vzdalovat zobrazovanou scénu, a také disponuje i některými funkcemi videorekordéru
* V digitálních systémech komunikace probíhá pomocí IP protokolu
* V analogových systémech probíhá komunikace po samostatné sběrnici (RS-485) anebo po koaxiálním kabelu vedeném k dané kameře (HD kamery)

### Monitory

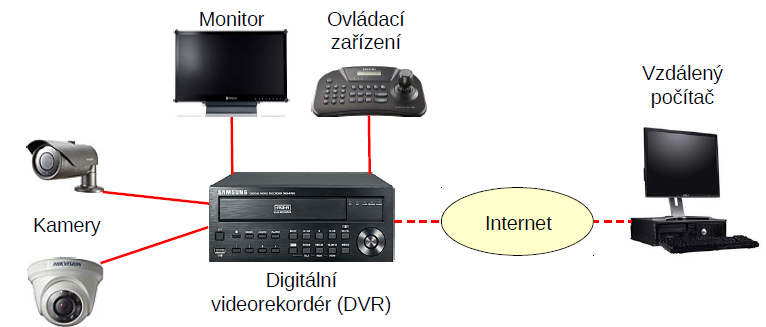
* Slouží k zobrazení signálu z kamer
* V současnosti se používají převážně LCD monitory s LED podsvícením a poměrem stran 4:3 (z historického důvodu) – rozhraní VGA, HDMI, BNC

### Přenos signálů

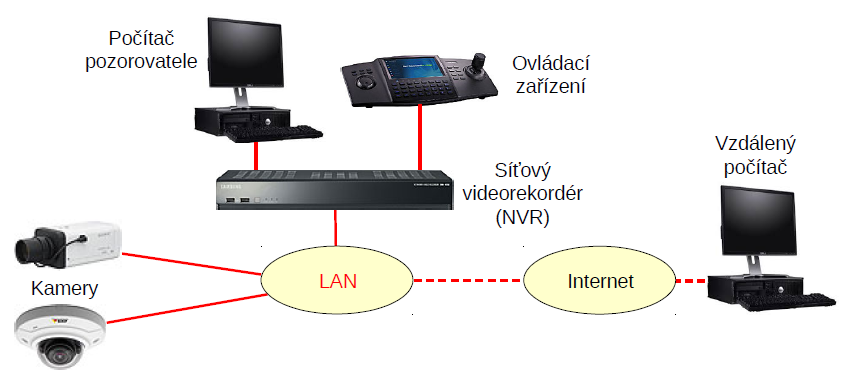
* Zpravidla se používají kabelové rozvody anebo rádiové přenosy (malé prosazené)
  + pro analogové přenosy – koaxiál a BNC konektory
  + pro digitální přenosy – 2linka UTP a RJ-45 konektory
* Dnes vítězí digitální technologie díky univerzálnosti a možnosti integrace do informačních systémů

## Schéma hybridního a digitálního systému

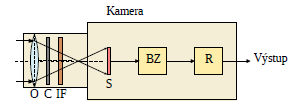
### Schéma hybridního DVS

* Kamery vysílají analogový obrazový signál po koaxiálním kabelu
* Jádrem systému je DVR, který disponuje rozhraními ke všem prvkům systému.
* Signály z kamer digitalizuje a ukládá na pevný disk
* Dále generuje obrazový signál pro monitor ostrahy a volitelně i pro vzdálený PC.
  + Často taktéž zprostředkovává ovládaní kamer pomocí ovládacího zařízení.

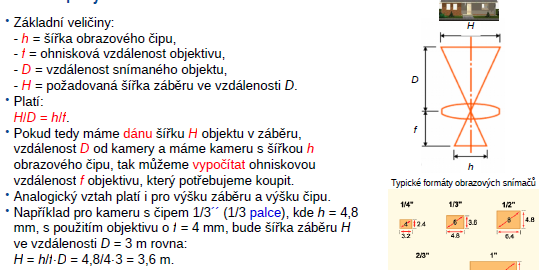
### Schéma digitálního DVS

* Kamery odesílají obraz přes přenosový protokol IP do síťového rekordéru a případně i jiným vzdáleným PC
* Videorekordér ukládá záznamy kamer na pevný disk a umožňuje řízení kamer. Ovládací příkazy a případně i jiná data jako zvuk se odesílají skrz IP protokol
* Digitální DVS
  + zařízení na připojení kamer, typicky ethernetové porty 100base-tx s POE technologií – takže i data i napájení (2 nevyužité páry jsou použité na napájení)
  + přenos obrazu přes technologie RTP (pracuje na UDP, samotný přenos obrazu a zvuku) a RTSP (TCP 554, řídí relaci, jako navázání a ukončeni spojení)

## Architektura kamery

* Kamera převádí obraz snímaného prostoru na elektrický signál
* Architektura kamery:
  + Objektiv O: soustřeďuje světelné záření na obrazový snímač S
  + Clona C: reguluje množství světla dopadajícího na snímač S
  + Infračervený filtr IF: v denním režimu znemožňuje průchod fotonů IR záření a tím zabraňuje barevnému zkreslení obrazu
  + Obrazový snímač S: převádí světelné záření na elektrický signál
  + Blok zpracování obrazu BZ: signál ze snímače převede na obraz a podle potřeby ho upraví a zkomprimuje. Ovládá i Clonu, Filtr a expozici.
  +  Komunikační rozhraní R: obraz z BZ převede do podoby signálu vhodného pro přenos do Dohledového centra
* Obrazové snímače DVS kamer jsou matice světlocitlivých prvků (pixelů) – na základě fotoelektrického jevu převádějí energii fotonů na elektrický náboj
  + dříve byly CCD snímače, ale nyní CMOS
  + CMOS snímač – 3 tranzistory a fotodioda (nad ní barevný filtr a čočka)
  + dopadem fotonů na fotodiodu se uvolní elektrony a vznikne U v závěrném směru, zesilovač s tranzistorem T2 má velký vstupní odpor a U zesiluje, potom na konci expozice se zapne T3 čtení a výstup T2 je připojený na výstup. Nakonec se dá reset

## Kalkulace záběru



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

### Integrace snímků

* Umožňuje zkvalitnit obraz ve špatných světelných podmínkách
* Postupuje se tak, že jeden snímek se vypočítá součtem více snímků, což zvyšuje kvalitu obrazu, avšak nevýhodou jsou rozmazané pohyby

### BLC – kompenzace protisvětla

* Kompenzuje protisvětlo
* Funguje tak, že pokud ve stanovené zóně scény není dostatečná úroveň jasu, tak správce kamery určí, z které časti obrazu se bude určovat doba expozice
* Některé časti obrazu budou přeexponované

### WDR – široký dynamický rozsah

* Umožňuje současně zobrazovat velmi tmavé ale i velmi světlé oblasti scény
* Kamera vytváří snímky kombinací jednoho podexponovaného (vybere světlou část) a druhého přeexponovaného snímku (vybere tmavou část)

### HLC – kompenzace přesvětlení

* Kamera dokáže v obraze detekovat intenzivní bodový zdroj světla
* Kamera si ponechá dostatečný expoziční čas, aby zachytila tmavší část scény
* Pixely zdroje světla následně zamaskuje a sníží se tak rozsah jasu v obraze

# Systémy EPS a hlásiče EPS

## Účel

* Požár – forma hoření, při které jsou ohrožené životy a majetek
* Hoření – chemická reakce paliva a oxidantu, která sa vyznačuje intenzivním světelným a IR zářením
* EPS – systém, který stanoveným způsobem reaguje na vznik požáru ve střeženém prostoru
* Reakce na vznik požáru:
  + Vyhlášení poplachu
  + Oznámení požáru hasičům
  + Spuštění automatizovaných protiopatření k minimalizaci škod

## Architektura

* Architektura EPS je prakticky stejná jako u PZS
* Základní prvky EPS:
  + hlásiče: sledují příznaky požáru
  + ústředna: zajišťuje řízení EPS
  + informační zařízení: informuje osoby o vzniku požáru – siréna
  + akční zařízení: uskutečňuje akce k minimalizaci škod – stabilní hasicí zařízení
  + ovládací zařízení: umožňuje obsluze ovládat EPS – panel OPPO
  + spoje: umožňují komunikaci s ostatními prvky EPS

## Základní prvky

### Hlásiče

* Sledují příznaky požáru
  + Detektory – na základě příznaků vyhlásí poplach
  + Měřiče – pouze měří příznaky, poplachy vyhlašuje ústředna
* Typy detektorů:
  + Tlačítkové – příznaky detekuje osoba
  + Automatické – příznaky detekuje sám detektor
* Typy automatických detektorů:
  + Hlásiče kouře – příznakem požáru je výskyt kouřových častíc
  + Hlásič teploty – příznakem požáru je zvýšení okolní teploty
  + Hlásič plamenu – příznakem požáru je výskyt plamenu
* Hlásiče jsou často kombinované

### Ústředna

* Řídí celý systém EPS
* Podle spojů dělíme systémy EPS na:
  + **Smyčkové** (konvenční) – analogová komunikace na základě velikosti proudu protékajícího párem vodičů
    - * V klidovém stavu v dolní poloze protéká proud přes rezistor R, v případě požáru se přepne do horní polohy a vypojí se zakončovací rezistor, čímž se zvýší proud ve smyčce a na ústředně je vyhlášený poplach
      * (+) jednoduchost, nízká cena
      * (-) nedá se určit, který hlásič, pro hlásiče a informační prvky musí být 2 různé smyčky
  + **Sběrnicové** (adresovatelné) - digitální komunikace obvykle po dvojdrátové sběrnici s kruhovou či liniovou topologií, každé zařízení má unikátní adresu a komunikace je typu výzva – odpověď (sdělují svůj stav)
    - * (+) přesná inf., který vyhlásil poplach, můžeme propojit všechna zařízení do jedné sběrnice
      * (-) cena

### Kabeláže EZS

* Jedná sa o ohnivzdorné kabely s izolací bez halogenových směsí
* ČSN 750°C 180min

### Akční zařízení

* Ústředna EPS může ovládat vybrané zařízení s cílem minimalizovat škody způsobené požárem
* Nejčastější typy:
  + stabilní hasicí zařízení (SHZ) – hasí požár
  + ventilátory – jejich vypnutím je omezen přístup vzduchu k požáru, anebo zapnutím je vyháněn dým z únikové cesty
  + požární dveře – zpomalují šíření požáru
  + požární klapky – zpomalují šíření požáru vzduchotechnikou
  + klíčový trezor

### Klíčový trezor požární ochrany (KTPO)

* Je v něm uložený klíč ke vstupu do objektu
* Umisťuje se na vnější straně obvodu budovy při vstupu a v případě poplachu se odemkne – odhalí se další dvířka se zdířkou pro univerzální klič hasičů – potom se můžou dostat do budovy

### Ovládací zařízení

* Umožňuje oprávněným osobám uskutečnit vybrané řídcí zásahy do fungování EPS
* Jedná sa o:
  + řídicí konzoli (panel)
  + obslužné pole požární ochrany (OPPO)
* Dovoluje personálu řídit provoz EPS
* Obslužné pole je jednotné pro všechny typy ústředen – dovoluje hasičům spustit vybrané funkce EPS a indikovat základní stav EPS

### Zařízení datového přenosu (ZDP)

* Umožňuje přenos vyhlášeného poplachu z ústředny na pult centrální ochrany (PCO) hasičům
* ZDP
  + telefonní linka
  + rádiové modemy v pásmu 80 a 400 MHz
  + moduly GPRS

### Pult centrální ochrany

* Zařízení umožňující dálkově sledovat stavy monitorovaných systémů EPS

## Bodové hlásiče a jejich fyzikální principy

* Měří příznaky požáru v okolí bodu svého umístnění
  + k detekci plamenů
  + k detekci zvýšené teploty
  + k detekci kouře
    - Ionizační
    - Optické
  + K detekci plynů
* Příznaky:
  + Plamene:
    - Výskyt hořícího oxidu uhličitého (CO2)
    - Dominantní složkou je IR záření s charakteristickou špičkou 4,3 mikrometrů a teplota přes 400°C (9,4 mikrometrů – člověk) – IR filtry na konkrétní vlnové délce
* **Hlásiče k detekci plamene**
  + využívá se IR snímač (pyroelektrický), v pásmu 4,3 mikrometrů a f = 3-30 Hz
* **Hlásiče teploty**
  + měří teplotu okolí pomocí termistoru
  + pokud dojde k překročeni teploty okolitého vzduchu, tak dojde k vyhlášení poplachu
  + diferenciální princip – 2 termistory – 1 venku a druhý v tepelně izolovaném obale
* **Hlásiče kouře**
  + Ionizační hlásič:
    - K detekci kouře se využívá pokles elektrického proudu mezi elektrodami v ionizační komoře – kyslík a dusík je vytlačený a na zbytek se naváže dým – pokles rychlosti částí, a tedy i proudu
    - Americia-241
  + Optický hlásič
    - Částice kouře ovlivní pohyb fotonů vevnitř hlásiče
    - Varianta s přerušením paprsku anebo rozptylem – IRED a FD a komůrka s labyrintem
  + Multisenzorové hlásiče
    - Zpravidla kombinuje vlastnosti kouřového a tepelného hlásiče
    - Novinka je přidání senzoru plynů – měří koncentraci určitých plynů
    - Výhodou je eliminace falešných poplachů

## Lineární hlásiče a jejich fyzikální principy

* Sledují požáry v okolí určité linie
* **IR paprskové hlásiče**
  + detekce přerušení IR paprsku částicemi kouře
    - Přímé – vysilač – přijímač
    - S odrazem – chytá odraz pomocí odrazové plochy
* **IR snímací hlásiče**
  + detekce ohně analýzou IR spektra v pásmu 4,3 mikrometrů
  + analýza výskytu složek s kmitočtem 1-10 Hz
  + detekuje v dosahu cca 50m
* **Kabelový zkratovací hlásič**
  + základ je speciální kabel z dvou kroucených vodičů zakončených rezistorem
  + zvýšením teploty okolí dojde v místě požáru k roztečení izolace a dojde ke zkratu
* **Optovláknový hlásič**
  + Do optického vlákna se vysílají světelné impulzy
  + V přestávkách mezi pulzy se měří rozptýlené Ramanovo záření
  + Podle jeho frekvence v daném okamžiku je možné zjistit teplotu v určitém místě vlákna

**Ramanův rozptyl:**

* + - Rozptylové záření, jehož vlnová délka je odlišná od excitačního záření, se nazývá Ramanův rozptyl
    - Závisí na teplotě dané látky – čím víc kmitají, tak tím dřív se srazí částice s fotonem

## Prostorové hlásiče a jejich fyzikální principy

* Sledují příznaky požáru v určitém prostoru
* **Nasávací hlásiče**
  + ze střeženého prostoru se nasává vzduch, v kterém se pak vyhodnocuje přítomnost kouře
* **Kamerové hlásiče**
  + kamera sleduje daný prostor a vyhodnocovací jednotka vykonává automatické vyhodnocování obrazu
  + sleduje výskyt plamene a kouře

## Schéma a princip fungování smyčkového a sběrnicového systému



# Systémy EKV

## Účel

* Elektronická kontrola vstupu alias přístupový systém je elektronický systém na automatizované řízení vstupů do kontrolované oblasti
* EKV pomocí ověřovacího seznamu uskuteční autentizaci žadatele a potom z přístupového seznamu zjistí práva žadatele – podle toho je vstup povolený anebo ne
* Příbuzný systém je docházkový systém – ten je určený k evidenci přítomnosti osob v prostorách, jde tedy o speciální případ systému EKV

## Prvky

* **Kontrolér**: řídicí jednotka přístupového systému, na který se připojují všechny ostatní prvky systému
* **Vstup**: uzavíratelný přechod, který je elektricky ovládaný kontrolérem, např. dveře s elektrickým zámkem, turnikety (1 osoba může projít), závory anebo zásuvné sloupy
* **Terminál**: zařízení pro komunikaci osoby s přístupovým systémem, např. čtečka biometriky anebo karet, klávesnice na vloženi hesla... uskutečňuje náročnější autentizaci
* **Správní jednotka:** zařízení určené na spravování přístupového systému, jedná se o PC se specializovaným SW, slouží k aktualizaci přístupového a ověřovacího seznamu, musí být schopná se připojit i k terminálu i kontroléru
* Méně časté, ale též využívané, jsou i detektory otevření dveří anebo tlačítko pro odchod

## Architektura systému EKV

* **Kontrolér:** připojení ostatních prvků EKV
* **Správní jednotka:** ke kontroléru se připojuje lokálně (USB, RS-232) anebo vzdáleně (sběrnice RS-485, LAN)
* **Terminál:** připojení ke kontroléru (Wiegandovo rozhraní – jednosměrné od terminálu ke kontroléru) anebo správnímu PC (LAN)
* **Ostatní prvky:** připojené dvojdrátovou smyčkou

## Typy autentizace – princip a vlastnosti

* Nosič DF je osoba
  + DF – tajný řetězec znaků (**PIN**) heslo
    - Založené na znalosti hesla
    - PIN je DF, ID, OF aj DD
    - Autentizuje kontrolér
    - (+) jednoduché a levné
    - (-) uživatel může zapomenout PIN, variabilita není velká kvůli paměti lidí (slovníkový útok), možné odpozorování hesla anebo tepelná stopa na tlačítkách
  + DF – **biometrika** osoby (otisk prstu)
    - Biometricky analyzuje unikátní rysy osob k autentizaci, otisk prstu
    - Terminál pošle DD kontroléru ve formě WS a rozhodne o vstupu
    - (+) žadatel má vždy při sobě DF
    - (-) snímače jsou drahé, DF nejsou tajné – útočník může vyrobit falzifikát
* Nosič DF je předmět
  + DF – tajná data (**šifrovací klič**)
    - Autentizace je založená na tajných datech uložených v předmětu, data mohou mít větší délku
    - Předmět je buď paměťové úložiště (unikátní číslo) anebo mikropočítač (WS 26b)
    - Předměty komunikují bezdrátovým rozhraním s terminálem
    - (+) velmi bezpečné
    - (-) možnost ztráty anebo odcizení, dražší a technicky složitější
  + DF – rysy předmětu (mikrotext, reliéfy anebo holografické fólie) **průkaz**
    - Identita osoby je uvedená v obtížně modifikovatelném a zfalšovatelném předmětu
    - Využívají se typicky ochranné prvky jako symboly pod UV světlem apod.
    - (+) ověřovatel může být člověk anebo technik
    - (-) možnost ztráty anebo odcizení, drahé kvůli ochranným prvkům

## Karty s magnetickým páskem – princip a vlastnosti

* Autentizační informace se zapisují na magnetický pásek (3 stopy)
* (+) levné a spolehlivé
* (-) slabá bezpečnost
* Magnetický pásek – stopy se magnetizují po úsecích, v těchto úsecích je materiál zmagnetizovaný v jednom směru (ploché permanentní magnety), sousedící magnety mají opačné směry magnetizace (vedle sebe S-J a J-S)
* Magnetický pásek osoba přetáhne v blízkosti čítací hlavy
* Pokud je následující napěťová špička vzdálená úsek 2 delta, tak jde o bit 0
* Pokud sa špička nachází uprostřed intervalu 2 delta, tak jde o bit 1

## Wiegandovy karty – princip a vlastnosti

* Do karty jsou zalisované dvě řady 26 wiegandových drátů
* Na čtečce u horní i spodní řady drátů je samostatná snímací cívka s překlápěcím magnetem
* S jejich pomocí je možné detekovat, v které řadě se nachází drát a pomocí napěťových pulzů cívky dojde k zjištění binární postupnosti karty
* Horní řada 1, dolní 0
* (+) nízká cena, vysoká trvanlivost
* (-) výroba duplikátu je obtížnější, ale není nemožná
* Wiegandův drát je speciálně zpracovaný drát ze slitiny kobaltu, železa a vanadu, za studena se za stanoveného tahu opakovaně kroutí a nazpět vyrovnává, jádro je magneticky měkké a jeho plášť magneticky tvrdý, změny orientace jádra oproti plášti jsou detekovatelné jako velmi krátké a relativně velké napěťové špičky v blízce umístěné cívce –Wiegandův jev

## Bezkontaktní karty podle ISO 14443 – princip a vlastnosti

* Pro bezdrátovou komunikaci mezi terminálem a RFID, či mikroprocesorovou kartou se používá rozhraní ISO 14443
* Komunikace je založená na principu transformátoru – primární vinutí trafa tvoří cívka čtečky v terminálu a sekundární je navinuté v kartě
* Čtečka prakticky trvale generuje signál o dané frekvenci, který se indukuje v cívce karty
* Indukované napětí se usměrní Graetzovým můstkem a jeho pomocí se dobíjí kondenzátor, který pro čip zalisovaný v kartě funguje jako zdroj energie

### RFID karty

* Jsou prakticky paměťová úložiště pro tajné Wiegandovo slovo WS
* Zpravidla obsahují EEPROM paměť, takže kromě čtení umožňují i zápis informací
* Moderní karty poskytují i ochranu před neoprávněným čtením – část paměti s WS je dostupná jen se znalostí tajného hesla na straně čtečky
* Nevýhoda: odposlech bezdrátové komunikace mezi čtečkou a kartou – možnost odhalení WS

### Mikroprocesorové karty

* Jsou prakticky samostatné počítače s dokazovacím faktorem bezpečně uloženým vevnitř (klič sym/asym krypto systému)
* Kryptoprocesor – náročné kryptografické výpočty jako generování dvojice soukromý a veřejný klič – soukromý klič nikdy neopustí kartu
* Používají se v přístupových systémech k zajištěni nejvyšší bezpečnosti – což je výhoda

### Smartfóny

* Hybridy mobilního telefonu a počítače s dotykovým displejem
* Výkonnost smartfónov dovoluje nasadit asymetrickou kryptografii, která je z provozního hlediska výhodnější
* Často sa používá NFC – rozšířeni standardu ISO 14443
* Bluetooth – má větší dosah než NFC, řádově metry, autentizování uživatele před vstupem, terminál může být za překážkou – lze tedy eliminovat sabotáž terminálu
* (+) autentizační HW je předmět, který vlastní a dennodenně používá prakticky každý, smartfón má víc bezdrátových přenosových technologií (NFC, Bluetooth)

# Biometrické přístupové systémy

* Biometrika je číselně vyjádřená morfologická anebo behaviorální charakteristika osoby
  + morfologická = týká sa vzhledu
  + behaviorální = týká sa chováni
* Biometrické systémy EKV – systémy EKV, v kterých jsou osoby autentizované pomocí biometrik
* Biometrická autentizace:
  + alias autentizace žadatelem, je autentizace, v níž je DF biometrika žadatele
  + kvůli výpočtové náročnosti se biometrická autentizace uskutečňuje v terminálu
  + autorita při autorizaci změří žadatelovu biometriku – její záznam tvoří soubor, tzv. šablonu
  + šablona je OF uložený v terminálech, případně v přenosném HW podepsaná autoritou
  + při žádosti o přístup dostane terminál od čtečky aktuálně nasnímanou biometriku žadatele (DD) a tu porovnává se šablonou – podle míry shody rozhoduje terminál o úspešnosti autentizace
  + Když je úspěšná, tak terminál zašle kontroléru ID žadatele a kontrolér podle přístupového seznamu zjistí práva žadatele a podle toho ovládá vstup

## Architektura a správa biometrického systému EKV

* Kontrolér: řídící jednotka systému EKV
* Vstup: uzavíratelný přechod, který je elektricky ovládaný kontrolérem, např. dveře s elektrickým zámkem
* Terminál: zařízení pro komunikaci osoby se systémem EKV, např. čtečka biometriky
* Správní jednotka: zařízení pro správu systému EKV, jedná se o PC se speciálním SW, při biometrické a mikropočítačové autentizaci správní jednotka komunikuje i s terminálem (správa ověřovacího seznamu)

## Otisky prstů – princip a vlastnosti

* Papilární linie jsou souvislé liniové reliéfy na povrchu bříšek prstů – střídání lišt a rýh
* Autentizace otiskem prstu je založená na velmi nízké pravděpodobnosti shody papilárních linií u dvou osob – jsou unikátní a zároveň lehko snímatelné
* V nasnímaných údajích se hledají pomocí SW specifické útvary, tzv. **markanty** – ty se zapíšou při autorizaci do šablony, konkrétně jeho typ a souřadnice
* OCHRANA PRED ÚTOKY!

### Optické snímače

* Papilární linie prstu se snímají maticí optických snímačů
* Osoba přiloží prst na optický hranol ozařovaný světelným zdrojem
* Fotony světla, které dopadnou na místo, kde je rýha, jsou odražené směrem k optickému snímači, a tam, kde je lišta, je světlo pohlcené tkanivem prstu
* (CMOS, CCD snímač) Z odražených fotonů se vytvoří fotografický snímek, který se dále analyzuje
* (+) nízká cena, odolnost vůči elektrostatické elektřině
* (-) třeba čistit snímací stěny hranolu, nekvalitní obraz při zamazaném prstu

### Kapacitní snímače

* Průběh papilárních linií prstu se zjišťuje měřením kapacity
* Kapacitní snímače – velký počet vodivých plošek uspořádaných do matice, jsou zalité do izolační destičky
* Prst je kovovým rámečkem snímače uzemněný – měří se kapacita každé plošky vůči prstu, tj. vůči zemi
* Lišta – větší kapacita
* Rýha – menší kapacita
* (+) není třeba snímací plochu čistit, zaznamenání obrazce prstu i při zamazaném prstě, cena je přijatelná
* (-) možnost poškozeni elektrostatickým nábojem

### Ultrazvukový snímač

* Průběh papilárních linií se zjišťuje na principu sonaru
* V každém snímaném bodě je vygenerovaný krátký pulz akustické energie v ultrazvukovém pásmu – detekují se odrazy ultrazvuku
* 1. odraz – spodní část snímací destičky
* 2. odraz – vrchní část snímací destičky
* 3. odraz – jen když je rýha
* Když je lišta, tak je vlna pohlcená tkanivem
* (+) nevyžaduje údržbu a čistění, odolný vůči elektrostatické elektřině, snímání umazaných prstů
* (-) vyšší cena

## Cévní řečiště prstů a dlaně – princip a vlastnosti

* Cévní řečiště je taktéž unikátní u každého člověka, a proto se používá

### Cévní řečiště prstu

* Princip:
  + prst se prosvěcuje IR zářením
  + část IR fotonů je pohlcená hemoglobinem v krvi, tj. cévy jsou proto na obrázku tmavší barvy
* (+) obraz cévního řečiště není běžně dostupný

### Cévní řečiště dlaně

* I zde se využívá, že hemoglobin pohlcuje IR fotony v pásmu 760nm
* Nasvícením dlaně IR zářením se v důsledku Rayleighova rozptylu objeví na snímku dlaně tmavé čáry, tedy žíly
* SW se obrázek zpracuje a vyextrahuje komplet cévní řečiště
* (+) rychlost cca 2s, malá pravděpodobnost chybné autentizace

## Tvář – princip a vlastnosti

* Autentizace podle tváře se dělí na 2D a 3D autentizaci

### 2D autentizace podle tváře

* Využívá se obyčejná kamera
* Vyhotoví se fotografie zpředu a fotografie se zpracuje = vyhledávají se obličejové metriky, tj. významné body a vzájemné vzdálenosti
* (-) nespolehlivá a nepřesná, možnost oklamat fotkou člověka
* Prakticky nemá výhody

### 3D autentizace podle tváře

* Využívá se jev, kde v důsledku zakřivení objektu se vrácené fotony vracejí pod různými úhly, tedy dojde k deformaci obrazu objektu
* Tvář se nasvítí pravidelným rastrem (IR záření), odrazené paprsky vytvoří na fotografii tváře rastr, jeho body už nejsou stejně vzdálené, tyto nepravidelnosti se vyhodnocují a na jejich základě se vytvoří 3D model tváře
* Tak jako při 2D, i při 3D se vyhledávají vzdálenosti mezi významnými body tváře a na jejich základě se uskutečňuje autentizace
* (+) autentizace ve špatných světelných podmínkách

## Duhovka – princip a vlastnosti

* Metoda je založená na individuálním rozmístění a tvaru skvrn na duhovce lidského oka
* Využívá se obyčejná kamera s dostatečným rozlišením
* Vyhotoví se fotografie očí osoby a ze získaného obrázku se zjistí charakteristické znaky oční duhovky, které se kódují (vlnková transformace) a uloží do paměti.
* Postup:
  + duhovka se černobíle vyfotí a údaj o barvě pixelů se převede z polárních do kartézských souřadnic. Obraz duhovky je převedený z podoby mezikruží do obdélníka
  + obdélník obrazu je rozdělený na 8 řádků a 256 sloupců, tedy 2048 plošek
  + hodnoty každé plošky jsou zprůměrované
  + Aplikuje sa vlnková transformace
* (+) velmi spolehlivé
* (-) je patentově chráněné

# Systémy na ochranu tovaru

## Účel a klasifikace

* Jsou to systémy určené na ochranu tovaru před jeho odcizením v obchodech
* Bezprostřední ochranu zabezpečuje personál prodejny
* Tyto systémy zlodějovi ztěžují fyzickou realizaci krádeže anebo personálu prodejny umožňuji efektivní a rychlou detekci krádeže
* Klasifikujeme na:
  + Zábranné systémy – mechanické zábrany, např. zamknutá vitrína
  + Sledovací systémy – dávají obsluze přehled o dění v objektu
    - Systém zrcadel
    - Kamerový systém
  + Poplachové (elektronické) systémy
    - Kontaktní (smyčkové) – zboží je do systému připojeno kabelem
    - Bezkontaktní – zboží je připojeno pomocí negalvanické vazby
      * Elektromagnetické (EM
      * Akustomagnetické (AM)
      * Rádiové (RF)

## Kabelové systémy – princip a vlastnosti

* Jsou to prakticky systémy PZS s jednoduchou vyváženou smyčkou, detektorem je spínač připevněný na zboží
* V klidovém stavu je spínač zapnutý a smyčkou teče proud o velikosti daného nastavovacího rezistoru
* Strhnutím spínače se spínač rozepne, tedy přestane téct proud a dojde k vyhlášení poplachu
* Při zkratování dojde k překročení klidového proudu a je opět vyhlášený poplach
* V moderních systémech se používá víc smyček
* Jádro kabelového systému tvoří ústředna, ke které jsou připojené smyčky zakončené hlavicí mikrospínače
* Často sa používají konektory typu Jack, ale i přilepovací anebo zásuvkové (TV signál)

### Systémy s více smyčkami

* Každá smyčka kontroluje jedno konkrétní zboží
* Používají se USB porty
* Datový pár – detekční smyčka
* Napájecí pár – napájení např. mobilu, tabletu ... ztráta napájení – vyhlášení poplachu

## AM systémy – princip a vlastnosti

### Magnetostrikční jev

* Vlivem magnetizace dochází ke změně geometrických rozměrů pásku z magnetostrikčního materiálu (v praxi bzučení trafa)
* V AM systémech sa využívá skutečnost, že magnetostrikční jev je inverzní, a tak při změně geometrických rozměrů vzniká magnetické pole

### AM etiketa

* Skládá se z magnetostrikčního a nastavovacího proužku, jehož nastavováním ovlivňujeme pracovní bod generujícího proužku
* K detekci je potřebné budící magnetické pole, díky kterému dojde k mechanické rezonanci proužku
* I po zániku budícího pole mění svoje rozměry a generuje vlastní magnetické pole a tato skutečnost se využívá k detekci

### AM systém

* Anténa vysílá v cca 20 ms dlouhých cyklech krátké pulzy 2 ms budícího signálu (58 kHz)
* Změny rozměru mají rezonanční kmitočet f a proužek kumuluje energii. V důsledku inverze etiketa generuje vlastní magnetické pole, které přijímač zachytí
* Deaktivace se vykonává odmagnetováním nastavovacího proužku přesunem pracovního bodu na začátek hysterezní slučky, potom negeneruje žádné vlastní mag. pole
* Snímatelné etikety – k upevnění se využívá magnetický zámek – vysoké třeni
* (+) velký dosah (3–5 m), možnost fungování s jednou anténou, vysoká spolehlivost
* (-) možnost rušení

## RF systémy – princip a vlastnosti

* Etikety RF systémů obsahují LC obvod, který dovoluje jejich detekci v elektromagnetickém poli

### RF systém s rozmítáním

* Vysílací anténa rozmítá budící elektromagnetický signál v určitém pásmu (nejčastější 7,4 a 8,8 MHz)
* V klidovém stavu přijímací anténa zachytává signál s přibližně konstantní úrovní
* LC obvod rezonuje 8,2MHz, pokud se mezi anténami objeví RF etiketa, tak v okolí tohoto kmitočtu funguje etiketa jako další vysílač – přijímač tedy detekuje zvýšenou úroveň přijímaného signálu a vyhlásí poplach
* Etikety
  + snímatelná – klasický LC obvod, plastový obal, magnetický zámek
  + nalepovací – LC obvod z hliníkové fólie, při pokladně se silným signálem přerazí kondík LC obvodu – deaktivace

### RF systém s čipy RFID

* RFID čip
  + Čip vybavený komunikačním rozhraním – paměťové čipy s identifikátorem EPC – 96bitov (dá se nastavit podle potřeby)
  + každá etiketa obsahuje dipólovou anténu a čip
  + čtečka generuje harmonický signál 860 až 960 MHz
  + přenos dát
    - čtečka – čip = amplitudové klíčování ASK
    - čip – čtečka = modulace zpětného rozptylu
  + EPC RFID komunikuje na vzdálenost několika metrů
  + deaktivace etikety jako při LC etiketě – přeražení kondíka
  + Možná integrace do platebního systému – každá etiketa má svůj identifikátor, problém, pokud se deaktivuje etiketa před pokladnou

# Elektronické platební systémy

## Účel

* Systémy, které umožňují realizovat platby a bankovní transakce elektronickými prostředky vzdáleně
* Základem bezpečnosti je
  + důvěrnost přenesených dat
  + autentičnost přenesených dat
  + autentičnost komunikujících stran
* Používají sa kryptografické a autentizační techniky
* Autentizace
  + vědomostí
  + biometrika
  + předmětem – např. autentizační kalkulátor

## Typy a jejich charakteristika

### Telefonní platební systémy

* Terminálem jsou telefony, jak pevná linka, tak i mobilní telefony
* Nejvíc se používá v bankovnictví, kde se podle telefonního čísla ověřuje doplňková autentizace v podobě hesla anebo kódu (nešifrovaná data)
* Typy:
  + Hlasové – klient zavolá na speciální číslo a podle menu se realizuje příslušná operace
  + SMS – klient komunikuje s bankou pomocí SMS správ
  + Datové – moderní telefony obsahuji i počítač s připojením na internet skrz mobilní síť – internetové bankovnictví
* Možnost přímých plateb pomocí SMS – obchod má smlouvu s operátorem, operátor inkasuje z účtu klienta
* Perspektivní rozšíření integrace elektronické platební karty – pomocí NFC – přiložení telefonu ke čtečce – využívání kryptografických technik

### Počítačové platební systémy

* Používají klienti, běžný PC s web prohlížečem
* Slouží k internetovému bankovnictví a k internetovému nakupováni
* Autentizace klientů prostřednictvím technik autentizačního kódu (heslo anebo certifikát) a případně doplnění o jednorázový kód mTAN
* Důvěrnost a autentičnost dat pomocí kryptografických protokolů – nejčastější TLS

### Bankomatové platební systémy

* Slouží klientům k výdaji a vkládaní hotovosti
* Jsou tvořené sítí terminálů (bankomatů) – neveřejná síť s bankou – bankomaty sdílejí se svojí bankou tajný klič
* Autentizace klienta – kombinace znalosti a vlastnictví předmětu
* Bankomat komunikuje s bankou šifrovaně, banka dešifruje kryptogram a ověří PIN
* Útoky
  + kamery
  + falešná klávesnice

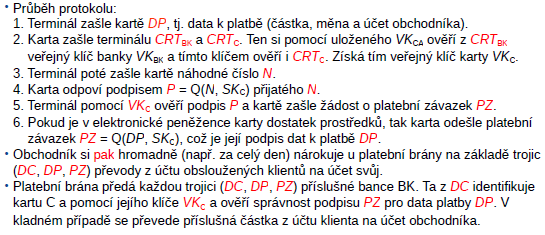
### Obchodní platební systémy

* Slouží k elektronické platbě klientů v obchodech
* Terminál – čtečka karet s LCD displejem a klávesnicí
* Při platbě klient přiloží kartu k čtečce anebo vloží do čtečky v terminálu a zadá svůj PIN
* Čip platbu ověří a potvrdí (off-line) anebo pošle dotaz do banky (online)

## Vysvětlit protokol TLS

* K zabezpečeni webového protokolu http se používá kryptografický protokol TLS
* Kombinace HTTP a TLS se označuje HTTPS
* Vytvoření zabezpečeného kanálu:
  + Klient zašle náhodné číslo (unikát) a seznam kryptografických primitiv, které zná
  + Server banky zašle svůj unikát, kryptografická primitiva, která se v transakci použijí a svůj certifikát
  + Klient CRT ověří VK, zvolí náhodné a tajné seed, a to zašifrované pošle jako kryptogram
  + Server dešifruje kryptogram a získá seed. Obě strany znají seed a unikát, z kterých se odvodí derivační funkcí klič pro autentizaci a šifrování přenášených dat.
* Server se autentizoval CRT, klient se autentizuje heslem, které je spolu s ostatními přenášenými daty zašifrované klíčem K.

## Vysvětlit nespřažený platební protokol

* Využívá se na platby malých částek
* Karta je „nabitá“ omezenou finanční částkou (tzv. elektronická peněženka)
* Čerpání částky kontroluje čip
* Platba se realizuje bezkontaktně a nevkládá se ani PIN – urychlení
* Autentizace karty metodou DDA – karta předkládá každému terminálu vždy různá data
* Fungování:
  + Terminál pomocí VK certifikační autority ověří CRT bankovního klienta, čímž se ověří VK bankového klienta.
  +  pomocí VK banky se ověří CRT karty, čímž obchodník získá záruku, že se platí kartou vydanou konkrétní bankou. Pokud této bance důvěřuje, tak výsledky nespřaženého protokolu přijme.
* Útoky:
  + díky tomu, že probíhá bez účasti majitele karty
  + čtečka – bezdrátové připojení na kartu útočníka – útočník provede objednávku a k platebnímu terminálu přiloží „svoji“ kartu – bezdrátové propojení s kartou oběti

# Ochrana digitálních děl

## Účel a klasifikace ochran

* Autorská data jsou uložená na nějakém elektronickém médiu (např. DVD) a cílem ochrany DRM je vynucovat kopírování a prezentaci autorských dat v souladu se stanovenými omezeními
* Ochrany DRM jsou založené:
  + na metodách digitálního vodoznaku
  + na metodách řízení přístupu
  + na kryptografických metodách
  + na kombinaci metod

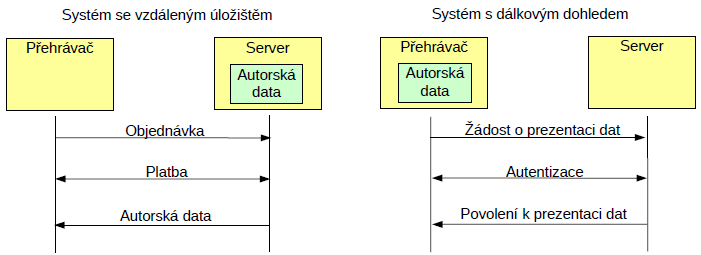
## Vzdálené DRM ochrany – typy, principy a vlastnosti

* Prezentaci autorských dat zajišťuje přehrávač a DRM ochranu zajišťuje virtuální server
* Vzdálený server může
  + autorská data poskytovat – systém se vzdáleným úložištěm
  + prezentaci autorských dat povolovat – systém vzdáleného dohledu

### Systém so vzdáleným úložištěm

* Využívají např. prodejci hudby
* Uživatel si dílo objedná a zaplatí
* Dílo mu je prodané a potom si ho může přehrávat.

### Systémy so vzdáleným dohledem

* Typicky používají poskytovatelé licencovaného SW
* Přehrávač požádá server o prezentaci dat a autentizuje se
* Pokud jsou splněné licenční podmínky, tak server vydá přehrávači povolení na prezentaci dat.

## Lokální DRM ochrany – typy, principy a vlastnosti

* Správa digitálních práv založená na lokálních ochranách nevyžaduje síťové připojení uživatele
* Ochrana práv je v tomto případě realizovaná přehrávačem
* Lokální ochrana může být tříděná podle typu média s chráněnými daty a přehrávačem těchto médií:

### Běžné médium

1. Univerzální přehrávač – jediný ochranný prvek je identifikační vodoznak
2. Speciální přehrávač

* Vložení vodoznaku – umožňuje přehrát médium jen při splnění určitých podmínek
* Autentizace předmětem anebo znalostí – je potřebný HW klič k přehrání dat, případně SW heslo (licenční klič) anebo HW autentizační předmět
* Kombinace – pracuje na principu, kde ochranu zajišťuje speciální program, který modifikuje přehrávač, aby se stal speciálním

### Speciální médium a speciální přehrávač

* Je málo používaná (herní konzoly – Nintendo)
* Využívá standardní DVD disk, na který vypálí čárový kód (BAC) a testuje při přehrávání jeho přítomnost
* Běžné DVD mechaniky nemají takový silný laser pro vypálení čárového kódu – tedy nemožnost vytváření nelegální kopie