

Fyzická bezpečnost

Téma: Elektrická zabezpečovací signalizace,
vstupní systémy, biometrická kontrola vstupu

Ing. Kamil Halouzka, Ph.D.

kamil.halouzka@unob.cz

Učební otázky

1. Úvod
2. Základní prvky EZS
3. Přístupové systémy
4. Biometrie
5. Čtečky otisku prstů
6. Ovládaná zařízení
7. Normativní předpisy

1. Úvod

- Hlavní funkcí **elektrické zabezpečovací signalizace** (EZS) je vyhlášení poplachu v případě napadení prostoru, který EZS střeží.
- Při vyhlášení poplachu se aktivují sirény vně i uvnitř objektu. Informace o poplachu je zpravidla přenášena na **pult centralizované ochrany**, který zajistí okamžitou kontrolu napadeného objektu.
- Uživatel ovládá celý systém pomocí jednoduché klávesnice, bezdrátových klíčenek, pomocí mobilního telefonu nebo internetu.

1. Úvod

- Vedle vyhlášení poplachu při napadení objektu může EZS sloužit také k ochraně osob uvnitř objektu.
- Stisknutím tlačítka je vyhlášen tichý tísňový poplach. EZS může hlídat také vznik požáru, únik plynu, zaplavení a další stavy v objektu.
- Navíc EZS hlídá i sama sebe a poplach je tak vyhlášen i při pokusu o **sabotáž** na jednotlivých komponentech.
- Proti výpadku elektrického proudu je EZS chráněna **záložním zdrojem**.

2. Základní prvky EZS

- EZS je komplexem vnitřních a vnějších technických prostředků, tvořících zabezpečovací řetězec:
 - ústředna,
 - zdroj elektrické energie,
 - poplachové smyčky (primární vedení),
 - zařízení k aktivaci a deaktivaci systému (klávesnice),
 - detektory,
 - signalizační zařízení (akustická a světelná).

2. Základní prvky EZS

- **ústředna** je nejdůležitější částí zařízení,
 - přijímá a hodnotí signály přicházející od jednotlivých detektorů,
 - spouští poplachová zařízení (akustické sirény, optickou signalizaci apod.),
 - předává hlášení na místa, která mohou poskytnout pomoc nebo zajistit zásah,
 - zajišťuje napájení elektrickou energií,
 - oznamuje poruchy, např. na ochranných smyčkách,
 - oznamuje stav zapnuto/vypnuto,

2. Základní prvky EZS

- **zdroj elektrické energie**

- k napájení jsou zpravidla používány dva nezávislé zdroje (jeden ze sítě, druhý ze záložní baterie),

2. Základní prvky EZS

- **poplachové smyčky (primární vedení)**
 - je elektricky střežené spojovací vedení mezi jedním nebo více detektory a poplachovou ústřednou.
 - zároveň je spojovacím vedením mezi ústřednou a poplachovým výstupním zařízením a napájecím zdrojem.
 - podle funkce se primární vedení dělí na:
 - poplachová smyčka vloupání,
 - ochranná smyčka – sabotáž, temper
 - tísňová smyčka – 24h smyčka

2. Základní prvky EZS

- **zařízení k aktivaci systému**

- umožňuje aktivaci poplachových smyček bezpečnostního systému do střežícího stavu.
- na rozdíl od běžných poplachových smyček jsou tzv. **ochranné smyčky** (sabotážní nebo také tamper) a tísňové smyčky (přepadení) označovány za tzv. **24 hodinové smyčky**, neboť jsou trvale ve střežícím stavu.
- aktivace bezpečnostního systému se provádí obvykle pomocí ovládací klávesnice, klíčku, elektrického blokovacího zámku nebo spínacího (propouštěcího) zámku.

2. Základní prvky EZS

- Klávesnice

- Umožňuje programování, ovládání a správu systému. Je dodávána ve třech provedeních:
 - LED klávesnice – indikace stavu systému pomocí **světelných diod**
 - LCD klávesnice – stav systému a jednotlivé akce jsou zobrazovány na **displeji**,
 - **velký LCD displej** zaručuje bezproblémové čtení údajů
 - grafické klávesnice - grafika umožňuje nejen zobrazení vytvořených plánů budovy s detektory, ale zjednodušuje ovládání pomocí grafického menu a navigačních tlačítek. Vnitřní software může obsahovat mnoho řádků zdrojového kódu a je cíleně vytvořen pro maximální komfort cílového uživatele. Programovací software umožňuje plnou konfiguraci, včetně download bitmap a melodií.

2. Základní prvky EZS

- **detektory** (hlásiče, čidla, snímače, senzory)
 - zařízení určené k **detekci vloupání, sabotážního jednání** nebo **technické poruchy** a k předání těchto informací o nebezpečí ústředně.
 - podle fyzikálních vlastností rozlišujeme detektory na elektromechanické, elektroakustické, elektrooptické.
 - lze je však také dělit na **aktivní** (sám vyhodnocuje svůj vyslaný signál, výpadek vysílače nebo přijímače vede k poplachu) a **pasivní** (technickým měřením postihuje určité fyzikální hodnoty, při změně hodnot podá hlášení, ale technický výpadek nevede automaticky k poplachu).

2. Základní prvky EZS

- **detektory** (hlásiče, čidla, snímače, senzory)
 - Problematika detektorů je podrobně rozebrána v přednášce k vlastním detektorům a k perimetrickým systémům.

2. Základní prvky EZS

- **signalizační zařízení**

- zajišťuje převedení předaných informací do vhodné formy (optické akustické či jiné).
- Signalizační výstupy dělíme na:
 - lokální - signalizační výstup (sirénou, zvonkem, světelným blikáčem) je vyveden **na vnější plášť objektu**,
 - autonomní – signalizační výstupy jsou vyvedeny **do místnosti stále služby v objektu**, která provede sama zákrok proti narušiteli nebo přivolá posilu,
 - dálkové – signalizační výstupy jsou vyvedeny **mimo střežený objekt** do místa se stálou službou, která zajistí zákrok (např. PCO).

3. Přístupové systémy

- Přístupový systém (ACS) – systém kontroly vstupů (SKV)
 - soubor opatření k zajištění řízení a evidence přístupu do zabezpečeného objektu nebo prostor na základě jednoznačně přidělených **přístupových práv**.
 - opatření mohou být režimová, fyzická (ostraha) nebo technická (technické prostředky).
 - přístupová práva jsou každému uživateli přidělena na základě personální politiky, stupně oprávnění, časového harmonogramu apod.

3. Přístupové systémy

- Je nutné rozlišovat pojmy „přístupové“ a „docházkové“ systémy.
 - U docházkových systémů je prokázání identity uživatele také nezbytné, ale prvotním cílem není pouze řízení přístupu do objektu, ale především **monitorování času a důvodu průchodu daným místem** (zákonná povinnost zaměstnavatele monitorovat pracovní dobu zaměstnanců, povinné přestávky apod.).

3. Přístupové systémy

- Základní funkce přístupového systému jsou:
 - identifikace,
 - zpracování dat,
 - ovládání přístupového místa,
 - programovatelnost,
 - stavová hlášení,
 - komunikace (s ostatními systémy nebo bloky přístupového systému),
 - styk s uživatelem (optické zobrazování / akustické signály),
 - napájení (systému nebo jednoho přístupového místa),
 - samoochrana (ochrana proti sabotáži, neoprávněné manipulaci, zjištění dat apod.).

3. Přístupové systémy

• Přístupový bod

- Přístupovým bodem v SKV - uspořádání všech prvků, které umožní kontrolovaný přístup (prostup) do prostor/k informacím v daném místě. Přístupový bod je v zásadě tvořen z:
 - místa přístupu (dveře, turnikety..),
 - rozhraní místa přístupu (řídící jednotka - ovládání otevření a zabezpečení místa přístupu),
 - snímače místa přístupu (čtečka, klávesnice, biometrie),
 - APAS (ovládací prvky a senzory přístupového místa).

3. Přístupové systémy

- **místa přístupu** – zařízení, které může být ovládáno k poskytnutí přístupu, dveře, turnikety, brány apod.,
- **rozhraní místa přístupu** – zařízení, které ovládá otevření a zabezpečení místa přístupu,
 - řídicí jednotka/kontrolér – obsahuje řídicí logiku, vstupy/výstupy potřebné k ovládání APAS, zajišťuje převod dat z identifikačního zařízení, komunikaci apod.,

3. Přístupové systémy

- **snímače místa přístupu** – „identifikační zařízení“, čtečka, klávesnice, biometrie,
- **APAS** – ovládací prvky a senzory přístupového místa,
 - vstupní prvky – magnetické kontakty, spínače, optické závory (k signalizaci a zabezpečení místa přístupu),
 - výstupní prvky – otvírač, zámek, motor turniketu apod.

3. Přístupové systémy

- Struktura celého přístupového systému se pak skládá z:
 - jednoho nebo více přístupových bodů,
 - hlavní řídicí jednotky (pokud je v systému nutná),
 - napájení (centrální nebo lokální),
 - komunikační sítě (RS-485, LAN, proudová smyčka, bezdrátová komunikace),
 - řídicího a obslužného pracoviště (PC).

3. Přístupové systémy

• Identifikace

- subjekt se může jednoznačně identifikovat v zásadě třemi způsoby:
 - něčím, co subjekt zná, co si pamatuje – heslo, kód, kontrolní otázka,
 - něčím, co má subjekt fyzicky u sebe – identifikační karta, přívěšek, RF ovladač apod.,
 - sám sebou, svými typickými rysy a chováním – biometrie.

3. Přístupové systémy

- Rozdělení identifikačních prvků
 - **Manuální** – např. vypínače, kódové zámky. Jsou pasivní, vyžadují manuální vstup od člověka.
 - **Čipové** – identifikátor je uložen v integrovaném obvodu (čipu, paměti), je možné čtení i zápis.
 - kontaktní – kontaktní čipové karty (SmartCard), iButton čipy,
 - bezkontaktní – bezkontaktní čipové karty/přívěšky, RFID (Radio Frequency Identification),
 - kombinovaná – kombinace kontaktní i bezkontaktní v jedné kartě, přívěšku, klíči.

3. Přístupové systémy

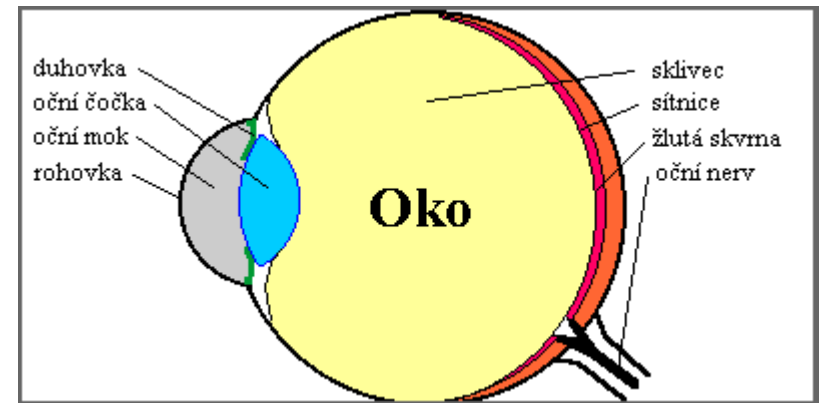
- Rozdělení identifikačních prvků
 - **Magnetické** – karty s magnetickým proužkem, průtažné čtečky.
 - **Optické** – čárovým kód, data matrix (2D) nebo kruhový kód. Laserové nebo CCD čtečky.
 - **Radiofrekvenční** – např. bluetooth identifikace, využití bezlicenčních pásem 434/868 MHz/2,4 GHz.
 - **Biometrické** - papilární linie, oční duhovka, 3D model hlavy, DNA apod.

4. Biometrie

- Biometrická identifikace vychází z předpokladu, že některé fyziologické (anatomické) a behaviorální charakteristiky člověka jsou jedinečné a časem neměnné.

4. Biometrie

- Z fyziologických znaků jsou nejpoužívanější:
 - **Otisk prstů** – papilární linie prstů, v daktyloskopii porovnávání charakteristických vzorů a markantů.
 - **Oční sítnice** – optický systém sejme část sítnice, obraz tvoří krevní cévky osvětlené koherentním zdrojem světla. Systém uživatelsky nepřívětivý, je nutná velmi přesná pozice vůči skeneru.



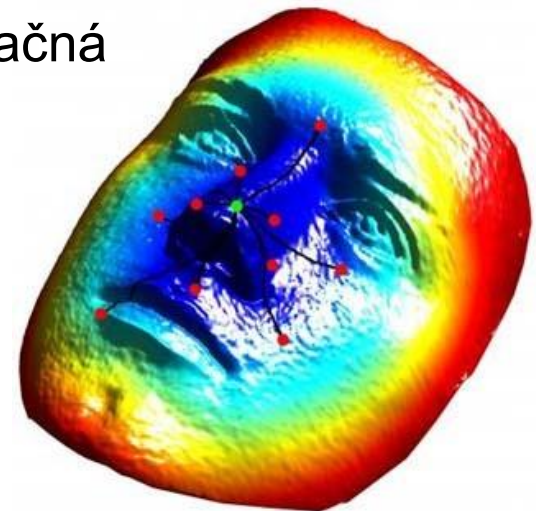
4. Biometrie

- Z fyziologických znaků jsou nejpoužívanější:
 - **Oční duhovka** – oko je snímáno kamerou ve viditelném nebo infračerveném spektru, analýzou kontrastu je „vyseknuta“ oblast duhovky, a pouze ta je navzorkována, normována a zaznamenána.
 - K porovnání jsou použity sofistikované matematické metody.
 - Není nutná nehybnost ani tak přesná pozice uživatele vůči čtečce.



4. Biometrie

- Z fyziologických znaků jsou nejpoužívanější:
 - **Obličej** – porovnávána je geometrie, resp. 3D model tváře.
 - Snímání je prováděno 1 nebo 2 kamerami většinou v IR spektru, porovnávají se charakteristické vzdálenosti a proporce očí, nosu, uší, lícních kostí, čelisti apod.
 - Při dnešních algoritmech je spolehlivost značná ($FAR < 0,0001 \%$), problém nebývá ani u jednovaječných dvojčat.

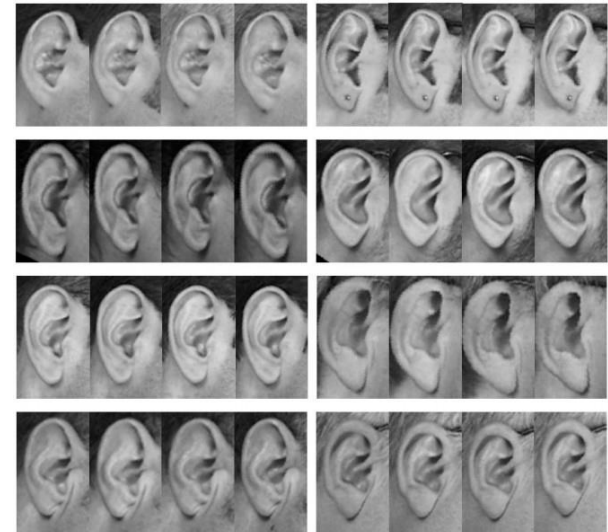
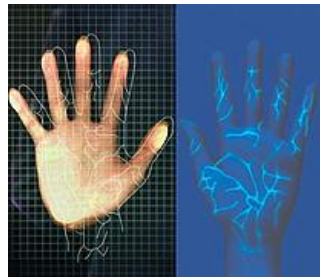


4. Biometrie

- Z fyziologických znaků jsou nejpoužívanější:

- **Další**

- tvar ruky,
- ušnice,
- pach,
- rozložení cév,
- DNA apod.



- Z behaviorálních znaků se používají např. hlas, podpis, stisk kláves, chůzi. Tyto technologie však nejsou příliš rozšířené.

5. Čtečky otisku prstů

- Z pohledu snímacího elementu je dělíme na tyto nejpoužívanější druhy:
 - Optické – vytváření obraz papilárních linií na čip CCD nebo CMOS,
 - kapacitní (CMOS),
 - Ultrazvukové – průnik vysokofrekvenčního ultrazvukového signál do dermální vrstvy prstu,
 - Teplotní – pyrodetektor snímá rozdíl teplot mezi jednotlivými papilárními liniemi a prostoru mezi nimi.

5. Čtečky otisku prstů

- **Optické**

- prst položený na dotykovou vrstvu (sklo) je osvětlen zdrojem viditelného světla (LED), které po odrazu na CCD/CMOS čip vytváří obraz papilárních linií.
- nevýhodou je nutný velký kontrast linií, náchylnost k zašpinění, poškrábání, možnost opticky napodobit

5. Čtečky otisku prstů

• Kapacitní (CMOS)

- zvrásnění papilárních linií je v podstatě kombinací 2 dielektrik (vzduchu a tkáně).
- kapacitní senzory mohou být pasivní nebo aktivní.
- pasivní senzory pouze měří kapacitu záhybů dermální vrstvy pokožky (ta se jeví jako vodivá) vůči mikroelektrodám matice kapacitorů,
- aktivní kapacitní (někdy označované jako RF) budí elektrody matice vysokofrekvenčním signálem a tak jsou schopny měřit kapacitu včetně epidermálních vrstev.

5. Čtečky otisku prstů

• Ultrazvukové

- podobně jako aktivní kapacitní senzory pronikají vysokofrekvenčním ultrazvukovým signálem až do dermální vrstvy prstu, proto je odolnost vůči zašpinění nebo poškrábání velmi dobrá,
- cena je však nejvyšší ze zde uvedených senzorů.
- senzor je tvořen maticí piezoelektrických měničů.

5. Čtečky otisku prstů

- **Teplotní**

- matice pyroelektrického materiálu snímá na povrchu teplotní rozdíly, způsobené vrcholky a prohlubněmi linií.
- funkce je značně ovlivněna okolní teplotou, setrvačností apod.

5. Čtečky otisku prstů

- Podle **způsobu aplikace prstu** na senzor dělíme čtečky, resp. jejich senzory, na:
 - dotykové (touch)
 - posuvné (swipe).
- U dotykových je obraz papilárních linií nasnímán najednou, zatímco u posuvných dochází ke složení výsledného obrazu z několika proužků získaných z užší matice senzoru.

6. Ovládaná zařízení

- Typicky chceme elektronicky řídit prostupy, jakými jsou dveře, turnikety, závory, výtahy, detekční rámy apod.
- Aby mohlo dojít k automatickému odblokování nebo otevření prostupu, musí být tyto prostředky vybaveny akčními prvky.

6. Ovládaná zařízení

- Mezi nejpoužívanější akční prvky patří:
 - elektromagnety
 - elektromagnetické otvírače
 - elektromechanické/elektromotorické zámky
 - elektromotorické/elektrohydraulické otvírače
 - motory
 - přídržné elektromagnety
 - vstupně/výstupní moduly

6. Ovládaná zařízení

- **Elektromagnety**

- Slouží k držení dveří v uzavřeném stavu.
- Přídržná síla elektromagnetu k protikusu bývá až 1000 kg, vyznačují se velkou spolehlivostí a bezúdržbovostí.
- Tam, kde je to potřeba, se kombinují se zámky, často se nasazují na prosklené prostupy.

6. Ovládaná zařízení

- **Elektromagnetické otvírače**

- V závislosti na přivedení napětí je odblokována nebo zablokována západka otvírače, střelka zámku není tedy ničím blokována a dveře umožňují průchod.
- Jedná se o nejběžnější otvírač v instalacích s malými nároky na bezpečnost.
- Instalují se do rámu dveří.

6. Ovládaná zařízení

• **Elektromechanické/elektromotorické zámky**

- Obvykle se jedná o samo-zamykací zámky, kde zjišťovací střelka pozná dovření dveří a následně mechanicky nebo motoricky vysune západku.
- V případě elektromechanických zámků elektromagnet pod proudem aretuje pohyblivý mechanismus v zámku a klika je plně funkční pro otevření dveří, je ji však nutné stisknout, aby došlo k zatažení závory.

6. Ovládaná zařízení

- **Elektromechanické/elektromotorické zámky**

- Bez napětí dochází k blokování funkce kliky.
- U elektromotorických zámků vysouvá a zasouvá západku elektromotor, mají větší množství funkcí a vyšší bezpečnost, obsahují vlastní řídicí jednotku a obecně se využívají v náročnějších aplikacích.
- Oba typy zámků umožňují odemknutí klíčem a vícebodové uzamčení, instalují se do dveří (zadlabací), zatímco protiplech je umístěn v zárubni.

6. Ovládaná zařízení

- **Elektromotorické/elektrohydraulické
otvírače**
 - Slouží k automatizovanému otevírání a zavírání různých typů dveří.
 - Především se používají pro bezbariérové vstupy.
 - Obvyklá je kombinace se zámkem.

6. Ovládaná zařízení

- **Motory**

- Různé typy motorů k ovládání turniketů, vjezdových vrat, závor apod.
- Obvykle mají vlastní řídicí jednotku, které kontrolérem nebo vstupně/výstupním modulem předáme impuls určité délky.

6. Ovládaná zařízení

- **Přidržené elektromagnety**

- Po otevření udržují dveře v otevřeném stavu, bez napětí dojde díky samozavírači k uzavření prostupu.
- Častěji jsou řešeny v rámci EPS.

6. Ovládaná zařízení

- **Vstupně/výstupní moduly**

- Umožňují řízení samostatných celků a přídatných prvků, např. vjezdových zařízení, výtahů, majáků apod.

6. Ovládaná zařízení

- Elektromechanické a elektromotorické zámky a otvírače mohou být podle stavu, v jakém se nacházejí při přivedení napětí, rozděleny do dvou provedení:
 - **běžné** (tzv. fail-secure, pod napětím jsou uvolněny, po odpojení napájení se zablokuje),
 - **reverzní** (tzv. fail-safe, pod napětím zablokovány, po odpojení napájení se uvolní).

7. Normativní předpisy

- Požadavky kladené na systémy kontroly vstupu v bezpečnostních aplikacích jsou stanoveny v souboru norem **ČSN EN 50133**, z kterých je v současné chvíli vypracována pouze
 - „Část 1: Systémové požadavky“,
 - „Část 2-1: Všeobecné požadavky na komponenty“
 - „Část 7: Pokyny pro aplikace“.
- Tyto normy nemají závazný charakter, slouží především jako odkazové pro potřeby certifikace výrobků.

Otázky k samostudiu

1. Jaké jsou směry vývoje biometrických přístupových systémů?

Literatura

- [1] Lukáš L. a kolektiv – Bezpečnostní technologie, systémy a management, 1.vyd., Zlín 2011, ISBN 978-80-87500-05-7
- [2] Uhlář, J. Technická ochrana objektů - 2. Díl (Elektrické zabezpečovací systémy II). Katedra technických prostředků bezpečnostních služeb, Praha: PA ČR, 2005, ISBN 80-7251-189-0.
- [3] Uhlář, J. Technická ochrana objektů - 3. Díl (ostatní zabezpečovací systémy). Katedra technických prostředků bezpečnostních služeb, Praha: PA ČR, 2006, ISBN 80-7251-235-8.
- [4] Normy ČSN