Poplachové zabezpečovací a tísňové systémy a návrh jejich funkčnosti

Alarm Security and Emergency Systems and Designing of their Functionality

Bc. Lukáš Krahulík

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Lukáš KRAHULÍK**
Osobní číslo:	**A10456**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Poplachové zabezpečovací a tísňové systémy a návrh jejich funkčnosti**

Zásady pro vypracování:

1. **Vypracujte literární rešerši zaměřenou na poplachové zabezpečovací a tísňové systémy (PZTS).**
2. **Popište prvky používané v systémech PZTS.**
3. **Analyzujte možnosti ovládání současných systémů PZTS.**
4. **Proveďte průzkum uživatelských požadavků na užívání systému.**
5. **Navrhněte obecnou strukturu uživatelsky komfortního systému.**
6. **Zhodnoťte navrženou strukturu ovládání zabezpečovacího a tísňového systému z pohledu uživatele.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KŘEČEK, S.: Příručka zabezpečovací techniky. Blatná: Cricetus, 2003. ISBN 80-902938-2-4.**
2. **VLČEK, J.: Bezpečnost elektrických zařízení. Praha: BEN, 2007. ISBN 978-80-7300-222-0.**
3. **BASTIAN, P.: Praktická elektrotechnika. Praha: Europa – Sobotáles, 2004. ISBN 80-86706-07-9.**
4. **UHLÁŘ, J.: Technická ochrana objektů: II. díl – EZS II. Praha: PA ČR, 2005. ISBN 80-7251-189-0.**
5. **KINDL, J.: Projektování bezpečnostních systémů I. díl – EPS, EZS. Zlín: UTB, 2004. ISBN 80-7318-165-7.**
6. **ZEMAN, P.: Česká bezpečnostní terminologie. Brno: Masarykova univerzita v Brně, 2002. ISBN 80-210-3037-2.**

Vedoucí diplomové práce: **doc. Mgr. Milan Adámek, Ph.D.**
Ústav bezpečnostního inženýrství

Konzultant: **Ing. Radek Pospíšil**

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

Termín odevzdání diplomové práce: **15. května 2012**

Ve Zlíně dne 24. února 2012

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce je zaměřena na podrobné seznámení s problematikou poplachových zabezpečovacích a tísňových systémů. Jejím cílem je navrhnutí uživatelsky komfortního způsobu ovládání těchto systémů, které shledá v rámci úvodní rešeršní činnosti za chybějící.

Klíčová slova: PZTS, detektor, ústředna, poplachový stav.

ABSTRACT

Thesis is focused on detailed explanation of intrusion and hold up alarm systems. The main objective is to propose a comfortable method of control of these systems, which are classified as missing at the beginning of research.

Keywords: PZTS, detector, control and indicating equipment, alarm condition.

Úvodem chci poděkovat vedoucímu mé diplomové práce doc. Mgr. Milanu Adámkovi, Ph.D. za čas a odborné vedení, které se mi během práce dostávalo. Současně bych chtěl poděkovat Ing. et Ing. Radku Pospíšilovi ze společnosti JIMI CZ, a.s. za cenné rady, připomínky a vstřícnou komunikaci.

Také děkuji svým rodičům za morální a materiální podporu, která mi byla poskytována během psaní diplomové práce a po dobu celého studia.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Technická ochrana objektů se v posledních letech velmi rychle rozvíjí. Stojí za tím vývoj elektronických systémů a stále vyšší nároky uživatelů na kvalitu zabezpečení. Poplachový zabezpečovací systém nezabrání vstupu nepovolané osoby do střeženého prostoru, ale informuje o jeho neoprávněném narušení. Poplachový stav je vyhlášen buď lokálně (akustická signalizace) nebo dálkově předáním zprávy fyzické ostraze.

Instalace těchto systémů se provádí zejména s cílem minimalizovat možnost ztráty hmotného majetku a s tím související ochrana osob. Je možná i kombinace s jinými prostředky ochrany jako jsou mechanické zábranné systémy, systémy kontroly vstupu, kamerové systémy nebo elektrická požární signalizace.

Aby mohl zabezpečovací systém pracovat podle našich představ je nutná dokonalá znalost jeho funkcí a parametrů. Ty pak můžeme programovat a ovládat přes uživatelský terminál (např. klávesnice). Hlavním úkolem této diplomové práce je tedy navrhnutí uživatelsky komfortního systému.

Práce je rozdělena na teoretickou a praktickou část. V úvodu teoretické části se zabývám legislativními požadavky na poplachové zabezpečovací systémy. V následující kapitole popisuji komponenty používané v zabezpečovacích systémech. Poslední kapitolou je způsob ovládání těchto systémů, který je ukázán na čtyřech konkrétních ústřednách.

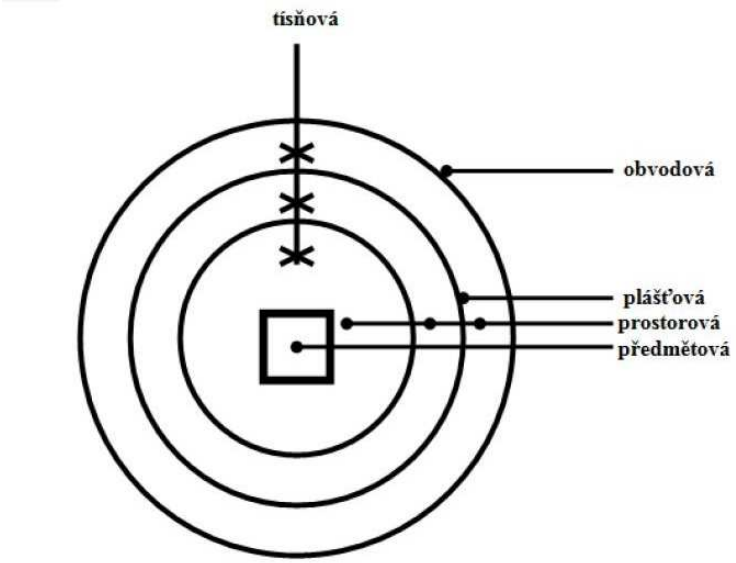
V praktické části jsou uvedeny výsledky uživatelského dotazníku, který je vytvořen pro zjištění nedostatků pří ovládání zabezpečovacích systémů. Na jeho základě je pak navržena obecná struktura komfortního ovládání systému.

I. TEORETICKÁ ČÁST

1 POPLACHOVÉ ZABEZPEČOVACÍ A TÍSŇOVÉ SYSTÉMY

Poplachové zabezpečovací a tísňové systémy (PZTS), dříve nazývané Elektrické zabezpečovací systémy (EZS) slouží k signalizaci nebezpečí ve střeženém objektu. Jedná se o kombinovaný systém určený k detekci poplachu vniknutí a tísňového poplachu. V technických normách se také používá anglická zkratka I&HAS - Intrusion and hold-up alarm system.

Poplachový zabezpečovací systém spadá do kategorie technické ochrany. Ta se dále dle prostoru člení na obvodovou, plášťovou, prostorovou, předmětovou a tísňovou.



Obr. 1: Prostorové členění technické ochrany [5]

Každý PZTS je složen z několika základních prvků:

a) Ústředna - zařízení pro příjem a zpracování informací z detektorů. Umožňuje ovládání, indikaci a inicializaci následného přenosu informace.

b) Čidlo (detektor) - zařízení určené k vyslání poplachového signálu nebo zprávy na základě jevů souvisejících s narušením střeženého objektu či prostoru.

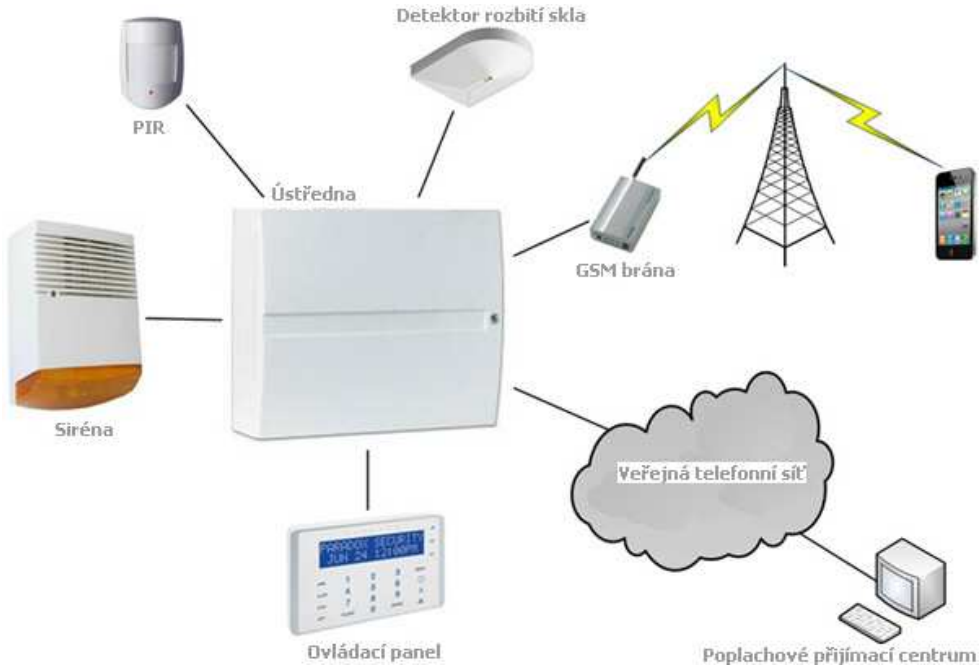
c) Signalizační zařízení - zajišťuje přenos výstupních informací z ústředny a to buď opticky nebo akusticky.

d) Poplachové přenosové prostředky - zajišťují přenos výstupních informací z ústředny k poplachovému přijímacímu centru (PPC) a následné ovládání poplachového systému.

e) Doplňkové ovládací zařízení – slouží pro usnadnění ovládání systému, jeho pomocí je možné zařízení uvádět do stavu střežení nebo klidu.

f) Napájecí zařízení - část PZTS, která zajišťuje energii pro jeho komponenty.

Tyto základní komponenty se kombinují v různých podobách a stupních složitosti. Ty mohou být následně ještě doplněny o tísňové hlásiče a záznamová zařízení. Začlenění jiných prvků je možné pokud nebude ovlivněna funkce komponentů PZTS.



Obr. 2: Schéma zapojení PZTS [8]

1.1 Právní předpisy a normy

Parametry a podmínky poplachových zabezpečovacích a tísňových systémů jsou formulovány v ČSN CLC/TS 50131. Ta byla vypracována evropskou technickou komisí CENELEC/TC79, která se zabývá poplachovými systémy. V České republice tyto normy schvaluje a vydává Úřad pro technickou normalizaci, metrologii a statní zkušebnictví.

Tab. 1: Obecná struktura normy PZTS

Označení normy	Oblast
ČSN EN 50131-1	Systémové požadavky (funkce, typy, definice)
ČSN EN 50131-2-4	Požadavky na konkrétní části systému
ČSN EN 50131-5	Požadavky na propojení zařízení (komunikace)
ČSN EN 50131-6	Napájecí zdroje
ČSN EN 50131-7	Pokyny pro aplikace (návrh, montáž, provoz)

Samotné komponenty PZTS podléhají NV č. 616/2006 Sb., o technických požadavcích na výrobky z hlediska jejich elektromagnetické kompatibility. To znamená, že zařízení bude uspokojivě fungovat v elektromagnetickém prostředí, aniž by samo způsobovalo nepřípustné elektromagnetické rušení jiného zařízení v tomto prostředí.

V souvislosti s poplachovými systémy platí i tyto základní normy:

ČSN CLC/TS 50398 Poplachové systémy - Kombinované a integrované systémy -

Všeobecné požadavky.
ČSN 33 2000-6 Elektrické instalace nízkého napětí - Revize ČSN 33 1500
Elektrotechnické předpisy. Revize elektrických zařízení
ČSN 33 2000-4-41 Elektrické instalace nízkého napětí - Ochranná opatření pro zajištění bezpečnosti - Ochrana před úrazem elektrickým proudem. [10]

1.2 Stupně zabezpečení chráněného objektu

Mezi důležité kritérium pro zařazení komponentů PZTS patří stupně zabezpečení, které jsou uvedeny v normě ČSN 50131-1. Ty jsou rozděleny podle míry rizika do čtyř stupňů. Riziko se stanovuje dle předpokládaných znalostí a vybavenosti narušitele.

Tab. 2: Stupně zabezpečení

Stupeň	Míra rizika	Typ narušitele
1	Nízké	Narušitel má malou znalost PZTS a k dispozici omezený sortiment snadno dostupných nástrojů.
2	Nízké až střední	Narušitel má určité znalosti PZTS a používá základní sortiment nástrojů a přenosných přístrojů.
3	Střední až vysoké	Narušitel je obeznámen s PZTS a má úplný sortiment nástrojů a přenosných elektrických zařízení.
4	Vysoké	Narušitel má možnost zpracovat podrobný plán vniknutí a má kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících prvků v PZTS.

Při návrhu vhodného stupně PZTS je nutné zvážit více aspektů (hodnota majetku, lokalita objektu). Jednoznačně nelze určit kam který objekt spadá, zařazení tedy provede dodavatel na základě požadavků a upřesnění objednavatele.

1.3 Klasifikace prostředí pro zařízení

Při výběru vhodných zařízení je potřeba zvážit v jakém prostředí se budou tyto komponenty nacházet. Proto nám norma určuje čtyři třídy prostředí.

Tab. 3: Klasifikace prostředí [9]

Třída	Název prostředí	Popis prostředí, příklady	Rozsah teplot
I	**vnitřní**	Vytápěná obytná nebo obchodní místa	+5 °C až +40 °C
II	**vnitřní všeobecné**	Přerušovaně vytápěná nebo nevytápěná místa (chodby,schodiště, skladové prostory)	-10 °C až +40 °C
III	**venkovní chráněné**	Prostředí vně budov, kde komponenty nejsou trvale vystaveny vlivům počasí (přístřešky)	-25 °C až +50 °C
IV	**venkovní všeobecné**	Prostředí vně budov, kde komponenty jsou trvale vystaveny vlivům počasí	-25 °C až +60 °C

2 PRVKY POUŽÍVANÉ V SYSTÉMECH PZTS

Technické prostředky bezpečnostního průmyslu, mezi které řadíme právě prvky PZTS slouží k ochraně osob, majetku a informací. Jejich úkolem je podpora a náhrada lidských smyslů, umožňující vnímání požadovaných údajů a informací.

Rozdělení prvků poplachových zabezpečovacích systému:

Prvky plášťové ochrany - slouží k hlídání otevření, destrukce prostorů pláště budovy.

- Magnetické kontakty
- Čidla na ochranu skleněných ploch
- Mechanické kontakty
- Vibrační čidla
- Poplachové fólie a tapety
- Drátová čidla
- Rozpěrné tyče

Prvky tísňové ochrany - slouží k vyvolání tísňového hlášení v případě přímého ohrožení.

- Veřejné tísňové hlásiče
- Skryté tísňové hlásiče
- Osobní tísňové hlásiče

Prvky předmětové ochrany - slouží ke střežení cenných předmětů.

- Otřesová čidla
- Čidla na ochranu závěsných předmětů
- Kapacitní čidla

Prvky prostorové ochrany - identifikují pohyb narušitele uvnitř střeženého prostoru.

- Pasivní IR čidla
- Aktivní IR čidla
- Ultrazvuková čidla
- Mikrovlnná čidla
- Kombinovaná duální čidla

Prvky venkovní obvodové ochrany - signalizují narušení perimetru u rozlehlých objektů.

- Mikrofonické kabely a IR závory a bariéry
- Mikrovlnné bariéry a štěrbinové kabely
- Zemní tlakové hadice
- Perimetrická pasivní infračervená čidla

Poplachové ústředny PZS - centrální část poplachových systémů.

- Klasické smyčkové ústředny
- Ústředny s přímou adresací
- Ústředny smíšeného typu
- Ústředny s bezdrátovým přenosem signálu od čidel

Výstražná zařízení - prostředky upozorňující na vzniklý poplachový stav.

- Sirény a zábleskový maják

Speciální čidla

- Tlaková čidla
- Nášlapné koberce

Ovládací zařízení - umožňují uvádět PZS do stavu střežení nebo klidu.

- Blokovací zámky
- Spínací a propouštěcí zámky
- Kódové klávesnice
- Ovládací a indikační díly

Přenosová zařízení - zprostředkují informace o stavu systému nebo narušení objektu.

- Automatické telefonní hlásiče a voliče
- Bezdrátová přenosová zařízení [1]

2.1 Ústředny

Základní funkcí ústředen poplachových zabezpečovacích systémů je sběr informací o stavu jednotlivých čidel a vyvolání poplachových signálů. Zabezpečovací ústředna je plošný spoj s mikroprocesorem, zdrojovou částí a se vstupy pro zapojení zón s detektory.

Detektory nepřetržitě vyhodnocují snímanou plochu, v případě že dojde k narušení okamžitě informují ústřednu. Následně je na základě rozhodovacího schématu, které je předem vytvořeno obsluhou vyvolán poplachový signál. Tím se rozumí akustická nebo optická signalizace, předání informace o poplachu na přijímací poplachové centrum (PPC) nebo fyzické osobě.

Důležitým prvkem ústředny je klávesnice, která slouží k jejímu ovládání a programování. Pomocí uživatelského kódu pak může uživatel zapínat nebo vypínat střežení zóny (objektu). Pro komunikaci s okolím bývá ústředna vybavena telefonním komunikátorem, s nímž se můžeme napojit například na PPC. Napájení ústředny je prováděno zabudovaným nebo samostatným napájecím zdrojem. Součástí většiny ústředen jsou i programovatelné výstupy PGM. Umožňují přiřadit každému z nich určitou událost, když dojde k jejich sepnutí. (osvětlení, topení).

Ústředna se nesmí montovat v místech, kde má přístup veřejnost. Nejlépe umístit do střeženého prostoru s nejvyšším stupněm zabezpečení.

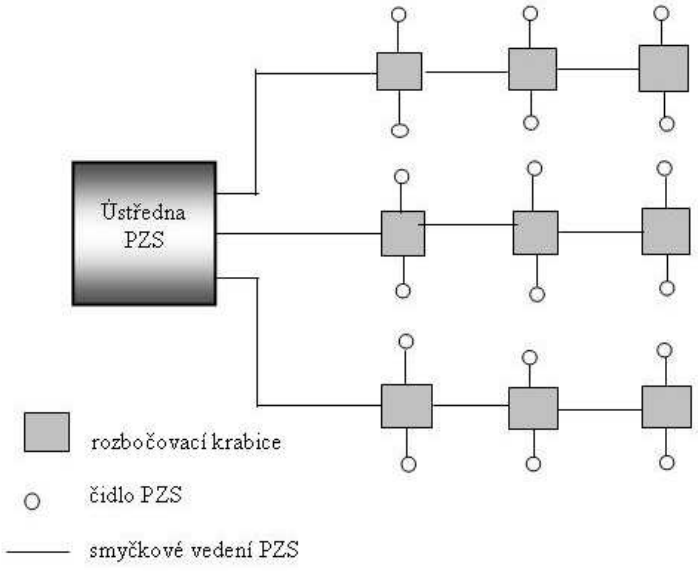
2.1.1 Stupně vybavenosti ústředny

Ústředny dělíme do skupin podle jejich parametrů, komfortu a kvality vybavení. Stupně vybavenosti závisí především na odolnosti ústředny proti jejímu překonání a tím vyřazení celého nebo části zabezpečovacího systému. [3]

- Nízké riziko - stupeň zabezpečení 1
- Nízké až střední riziko - stupeň zabezpečení 2
- Střední až vysoké riziko - stupeň zabezpečení 3
- Vysoké riziko - stupeň zabezpečení 4 (složena ze dvou ústředen)

2.1.2 Ústředny smyčkové

Detektory a tísňové hlásiče jsou k ústředně připojeny pomocí proudových smyček o definované hodnotě a toleranci. Každá smyčka je připojena na vyhodnocovací obvod ústředny a má svůj zakončovaní odpor. Změna tohoto odporu, která je způsobená aktivací čidla nebo sabotáží vede k vyhlášení poplachové stavu. [3]

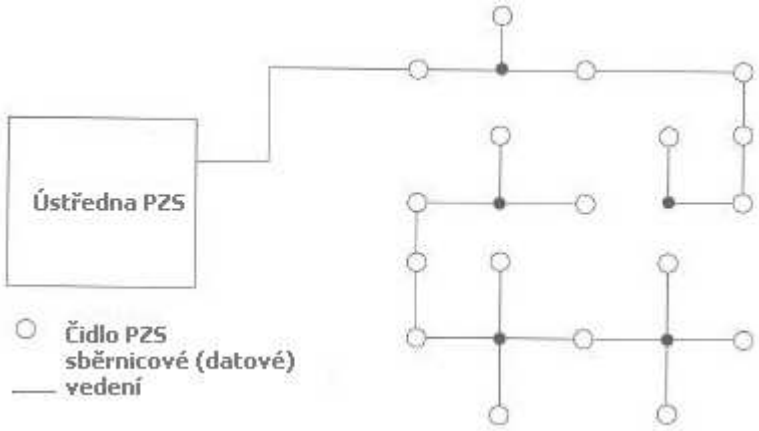


Obr. 3: Schéma zapojení smyčkové ústředny[1]

Nevýhodou tohoto zapojení je poměrně rozsáhlá kabeláž. Ke každému čidlu musí být přiveden kabel o dvou vodičích. Jedná se o kabely pro napájení, poplachový kontakt, sabotážní kontakt a dodatkové funkce (paměť poplachu, průchozí test apod.).

2.1.3 Ústředny s přímou adresací čidel

Komunikace mezi ústřednou a čidly probíhá pomocí datového vedení (sběrnice) v časovém nebo frekvenčním režimu. Ústředna periodicky aktivuje adresy jednotlivých čidel a přijímá jejich odezvy. Součástí každého čidla musí být komunikační modul.



Obr. 4: Schéma zapojení sběrnicové ústředny[1]

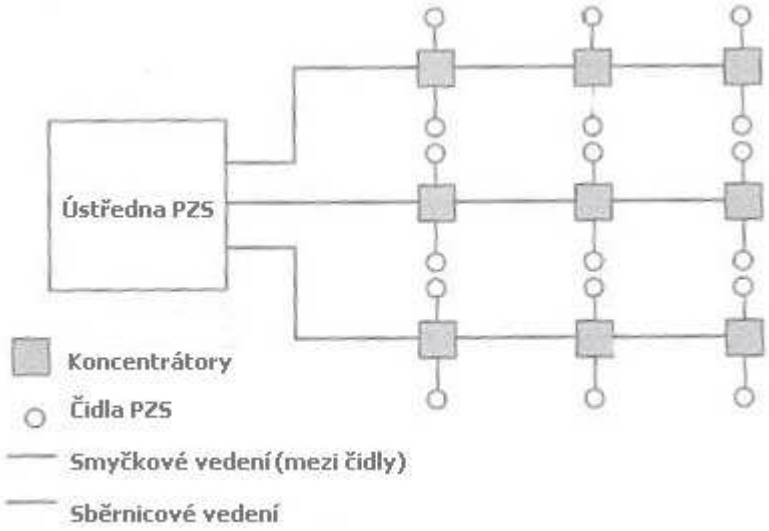
Výhodou tohoto systému je minimální kabeláž, která je tvořena libovolnou konfigurací kabeloví sítě. Čidla jsou připojena libovolně, zpravidla na čtyřvodičovém vedení. Dva vodiče slouží jako napájení čidel a dva datovou sběrnici. Další výhodou je adresovatelnost čidel. To znamená, že ústředna po narušení objektu oznámí, které čidlo bylo aktivováno a jaký je druh narušení (poplachový nebo sabotážní kontakt, zkrat na lince, indikace dalších stavů).

Mezi nevýhody se řadí celková délka vedení. Z důvodu úbytku napětí se musí pečlivě zvažovat odběr jednotlivých komponentů systému PZTS (počet adresovatelných čidel se pohybuje v desítkách). [3]

2.1.4 Ústředny smíšené

Tyto ústředny pracují na principu datové komunikace ústředna - koncentrátor. Komunikace probíhá pomocí datové nebo analogové sběrnice. Koncentrátory slouží jako analogové několika smyčkové podústředny. To znamená, že čidla jsou na koncentrátory připojena pomocí smyček. Jedná se tedy o kombinaci analogových a sběrnicových ústředen.

Systém může přejít i na typ ústředny s přímou adresací čidel a to tak, že na jednotlivé vstupy koncentrátorů se připojí konkrétní čidla. Pro tento návrh je nutná dostatečná kapacita ústředny. [1]



Obr. 5: Schéma zapojení smíšené ústředny[1]

2.1.5 Ústředny s bezdrátovým připojením

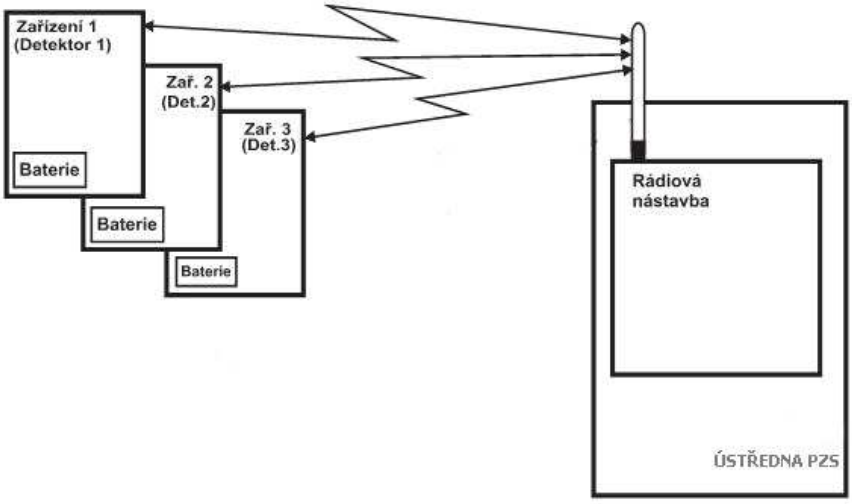
Komunikace mezi ústřednou a čidlem probíhá bezdrátově. Pracují v pásmu 433 MHz nebo 868 MHz. Poplachový signál je nejčastěji 8-bitový, kódovaný a adresa čidla je 4-bitová. Dosah připojení ve volném prostoru je 100 až 500 metrů. Jejich použití je obvykle uvnitř objektu, takže dosah se několikrát zmenší. Čidla jsou napájena baterií nebo 9V článkem. Pokles napětí je indikován akustickým signálem nebo přenesením do ústředny. Tím dojde k upozornění obsluhy na výměnu baterií.

V rámci bezdrátové komunikace mezi ústřednou a čidly se přenos dělí na *jednosměrný* a *obousměrný*.

Základními komponenty bezdrátového zabezpečovacího systému jsou čidla pohybu, magnetické kontakty, čidla pro rozbití skla, snímače kouře, tísňová tlačítka, sirény, univerzální moduly pro připojení čidel, ovládací prvky.

Mezi výhody těchto systému patří zkrácení doby montáže a velká flexibilita. Minimalizuje se kabeláž a nevznikají žádné zásahy do omítky. Dalším plusem je i jednoduchá změna konfigurace v případě potřeby a možnost doplnění dalších komponentů.

Nevýhodou je vlastní napájení a s tím spojená častá výměna baterií. Vznik falešných poplachů nebo ztrátě přenosu vlivem nebezpečného rušení přenosu.



Obr. 6: Bezdrátová komunikace detektorů

a) Systémy s jednosměrnou komunikací

Systémy s jednosměrnou komunikací jsou jednodušší. To znamená, že ústředna slouží jako přijímač a čidlo je vysílačem. Problémem dřívějších systémů s tímto přenosem byla neschopnost ústředny zkontrolovat stav čidel k ní připojených. Když bylo tedy některé čidlo porušeno nebo odcizeno, neměla ústředna o jeho stavu žádnou informaci.

Novější systémy však provádí kontrolu přenosové cesty pomocí kontrolních zpráv. Aby byla kontrola efektivní musela by se provádět s velkou četností. To ovšem není možné k vzhledem trvanlivosti baterií u napájených komponentů. Obvykle se používá četnost kontrol v rámci hodin. Tím dochází k tomu, že ústředna se o vyřazení prvku dozvídá s určitým zpožděním. Aby nedocházelo k planým poplachům vlivem nečekaných výpadků signálu, vyhodnotí situaci jako poplachovou nebo poruchovou až pokud nedojde několik po sobě jdoucích kontrolních intervalů. Doba zaznamenání porušení nebo poplachu se nám tedy opět prodlouží. [1]

Nevýhodou systému je poměrně snadné zjištění kmitočtu a modulace na které pracují. Při použití dané frekvence o vyšší intenzitě dojde k zahlcení přijímače a jeho vyřazení.

b) Systémy s obousměrnou komunikací

Všechny komponenty tohoto systému jsou vybaveny přijímací i vysílacím modulem. Tyto moduly pracují souběžně na dvou vyhrazených kmitočtech. Pokud dojde k narušení kteréhokoliv kanálu, jsou schopny přeladit se na jiné dva nenarušené kanály. Tento typ komunikace se nazývá duplexní a odstraňuje nedostatky stejnosměrné komunikace systému.

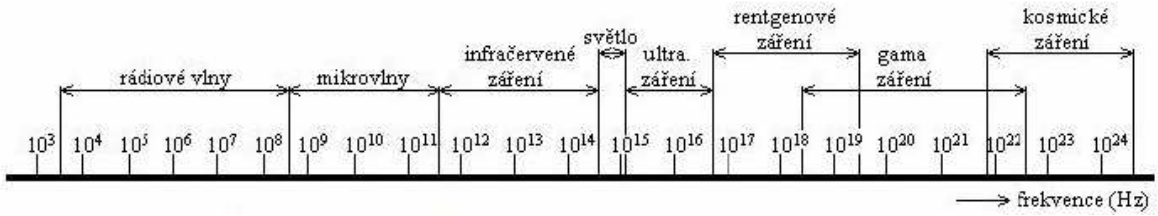
Mezi výhody řadíme ověření ústředny o stavu všech prvků při zapínání systému. Možnost ověření, zda je přijitá poplachová informace skutečným poplachem. Zvýšení odolnosti systému proti úmyslnému i neúmyslnému přerušení přenosu. V klidovém stavu čidla nevysílají a tím šetří baterie.

Poslední skupinou jsou tzv. *hybridní ústředny.* Jde o kombinované připojení pomocí drátových vstupů, tak i bezdrátových prvků. Používají se v různorodých objektech, kde je potřeba instalovat oba uvedené systémy.

2.2 Detektory narušení střeženého prostoru

Patří jsem skupina čidel, které detekují pohyb nebo přítomnost osob ve střeženém prostoru. Takové detektory se nazývají pohybové a jsou použity pro střežení vnitřních prostor i venkovních prostranství.

Čidla detekce pohybu pracují na různých fyzikálních principech. To znamená, že každé z nich využívá odlišnost část kmitového spektra.



Obr. 7: Spektrum elektromagnetického vlnění[3]

Rozdělení detektorů:

- Napájené (aktivní a pasivní)
- Nenapájené

Pasivní čidla - pasivně reagují na fyzikální změny ve svém okolí (PIR detektor, změna teplotního gradientu).

Aktivní čidla – aktivním působením si vytvářejí své vlastní prostředí a detekují jeho změny (Ultrazvukový detektor, snadno se určují tzv. mrtvé zóny).

Způsoby zpracování signálu

Další rozdělení čidel závisí na zpracování získaného analogového signálu. Důležitost tohoto zpracování spočívá ve spolehlivosti detekce a odolnosti proti falešným poplachům.

a) Analogové zpracování signálu - poplachový stav vznikne vlivem překročení vyhodnocené prahové úrovně. K tomu je nutné, aby se tato činnost opakovala několikrát během definovaného časového úseku.

b) Digitální zpracování signálu - zpracovávají signál pomocí softwaru uloženého v mikroprocesoru. Dochází k přesnější selekci poplachového signálu a oddělení od nežádoucího šumu a rušení.

2.2.1 PIR detektory

Pasivní infračervená čidla (Passive infra red sensor) patří mezi nejčastěji používané prvky systému PZTS. Jejich princip je založen na zachycení změn vyzařovaní narušitele v infračerveném pásmu kmitočtového spektra elektromagnetického vlnění. Jsou tedy schopny zachytit pohyb těles, které mají jinou teplotu než dané pozadí. Pro teplotu těla člověka kolem 35 ºC, je dána vlnová délka 9,3 - 9,4 μm. Toto záření je detekováno *pyroelementem.*

Ten je základní součástí čidla, složen ze sloučenin na bázi lithia a tantalu. Pracuje jako měnič gradietní povahy, detekuje tedy jen změny dopadajícího záření. U lepších čidel se používá dvojitého pyroelementu. Další částí čidla je *optika*, která dělí snímaný prostor na detekční zóny. Je určena pro přenos infračerveného záření z detekovaného prostředí na pyroelement. Prostor je rozdělen na tzv. aktivní a neaktivní zóny. V případě, že narušitel vstoupí do aktivní zóny je zaznamenán nárůst infračerveného signálu v opačném případě naopak. Následný průběh je vyhodnocován elektronikou a pokud odpovídá průchodu osoby je vyhlášen poplach. [3]

Optiku tvoří jeden ze dvou základní elementů:

a) Zrcadlová optika - segmentové zrcadlo vyrobené z plastu s napařenou kovovou vrstvou (detekční charakteristika je dána při výrobě).

b) Fresnelova čočka – výlisek z plastické hmoty obsahující soustavu čoček, které rozdělí snímaný prostor na zóny (výměnou čočky můžeme změnit detekční charakteristiku).

Nejčastější typy PIR čidel dle charakteristiky snímaného prostoru na základě tvaru čočky:

- Vějíř (dosah 12 - 15 metrů, šířkový úhel 90º)
- Záclona (dosah 12 - 15 metrů, šířkový úhel 15º)
- Dlouhý dosah (dosah 20 - 35 metrů, šířkový úhel 15º)
- Stropní (dosah 8 - 12 metrů, šířkový úhel 360º)

Obr. 8: Typy PIR detektorů[11]

Dále můžou být detektory konstrukčně rozšířeny o následující funkce:

- **Antimasking -** aktivní ochrana detektoru pomocí infračerveného záření, při zakrytí dojde k vyhlášení poplachového stavu.
- **PET imunita -** ke zvířatům s hmotností do 40 kg.
- **Černé zrcadlo -** snižuje počet planých poplachů vyvolaných vlivem vysokého záření viditelného světla
- **Quad PIR -** zdvojený pyrosensor zvyšující odolnost proti planým polachům.

Aby nedocházelo k častému vyhlášení falešných poplachů, nastavují se impulsní čítače na hodnoty 1 – 2 nebo 3 – 5. To znamená, že poplachový stav bude vyhlášen až po prvním, druhém nebo třetím překročení prahové hodnoty.

Hlavní výhody těchto detektorů jsou snadná montáž a seřízení, vysoká spolehlivost a malá spotřeba elektrické energie. Do prostoru můžeme instalovat více čidel, jelikož nevyzařují žádné vzájemné rušení.

Mezi nevýhody patří rychlé teplotní změny jako podlahové topení, zařízení v místnosti. Dalšími faktory jsou světelná rušení (slunce, světla automobilů) a proudění vzduchu (ventilace, klimatizace, topná tělesa atd.). Uvedené nevýhody zvyšují možnost vzniku falešného poplachu.

2.2.2 MW detektory

Mikrovlnné čidlo (Microwave sensor) je aktivní detektor, který obsahuje přijímač a vysílač mikrovlnného signálu. Pracují v pásmech 2,5 GHz, 10 GHz a 24GHz. Vyhodnocuje se odražená část vyslaného signálu a to na principu Dopplerova jevu. Pokud se narušitel pohybuje, odražená vlna se vrátí se změněnou fází a vyhlásí poplach. Na předměty které se nepohybují nereaguje. Používají se pouze tam, kde není možní instalace infračervených detektorů. Pokud chceme v místnosti instalovat více čidel, je nutné aby každé pracovalo v jiném kmitočtovém pásmu. [11]

Mezi nevýhody řadíme že:

- mikrovlny procházejí skrz stěnu a to může vést k vyvolání falešného poplachu.
- v místnosti se nesmí nacházet pokovené nebo kovové předměty.
- nesmí dojít k rušení zářivkami ani pohybující se kapalinou v plastovém potrubí.

2.2.3 US detektory

Ultrazvukové čidlo (Ultrasonic senzor) pracují na frekvenci v pásmu 20 - 45 kHz. Aktivním prvkem je vysílač, který vysílá vlnění o stálém kmitočtu. Vysílá nad pásmem kmitočtu slyšitelným lidským uchem. V prostoru se vytvoří konstantní vlnění, které poukazuje na klidový stav. Vlnění odražené od překážek se vyhodnocuje v přijímači. Pokud se v prostoru objeví narušitel, přijaté vlnění bude mít jinou hodnotu. Tím dojde k vyhlášení poplachu. Můžeme tedy říct, že se opět jedná o aplikaci Dopplerova jevu.

Dosah těchto detektorů je přibližně 10 metrů a instalace by měla být prováděna ve směru předpokládaného pohybu pachatele. Funkčnost čidla je ovlivněna okolními objekty ve střeženém prostoru (povrch předmětů, zdroje ultrazvukových hluků atd.). Jejich využití je spíše v zabezpečení vnitřního prostoru automobilů. [1]

2.2.4 Kombinované detektory

Pro eliminaci uvedených nedostatků předchozích detektorů se využívá jejich kombinací. Nejčastějším typem duálního čidla je pasivní infračervené s kombinací mikrovlnného (*PIR + MW*). Druhou variantou je spojení *PIR + UZ*. K vyhlášení poplachového stavu dojde, pokud obě vyhodnocovací jednotky zaznamenaly narušení střeženého prostoru. Pro detekci obou části detektoru je vymezen časový interval, který je spuštěn záznamem o prvním narušení prostoru. Hlavním cílem je snížení vzniku falešných poplachů. [11]

V dnešní době se kombinovaná čidla nahrazují PIR detektory s inteligentním zpracováním signálu.

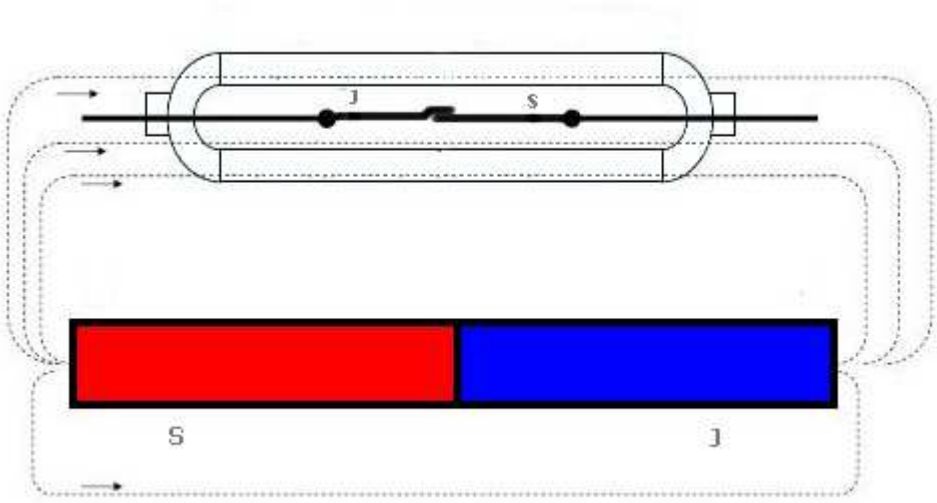
2.3 Detektory otevření

Do této skupiny spadají čidla, která se snaží zabránit násilnému vniknutí do střeženého objektu/prostoru. Při narušení klidového stavu dojde k vyhlášení poplachu. Jedná se o prvek plášťové ochrany.

2.3.1 Magnetické kontakty

Jsou to jednoduché detektory bez vyhodnocovací jednotky a nároků na napájení. Detektor je tvořen jazýčkovým kontaktem a permanentním magnetem. Jazýčkový kontakt složený ze dvou feromagnetických plíšků je zatavený ve skleněné mikrotrubičce a naplněný ochrannou atmosférou. Magnetem je zmagnetizovaný feritový váleček.

Samotný detektor je tedy tvořen ze dvou částí. Část z relé obsahuje vývody s dvěma případně čtyřmi vodiči nebo jednoduchou svorkovnici. Druhou částí je samostatný magnet. V klidovém stavu je jazýčkový kontakt sepnut pomocí magnetu. Pokud dojde k narušení (oddálení magnetu) je kontakt rozepnut a dojde k vyhlášení poplachu. [3]



Obr. 9: Magnetický kontakt (sepnutý)

Při instalaci se magnet upevní na pohyblivou část okna (dveří), jazýčkový kontakt pak na pevnou konstrukci (rám). Důležitým prvkem při aplikaci je stanovení maximální a minimální pracovní vzdálenosti, která je přidělená výrobcem. Provádí se buď povrchová nebo skrytá montáž přímo do dveří (oken).

Provedení dle konstrukčního uspořádání:

- s jedním jazýčkovým kontaktem
- s více jazýčkovými kontakty
- s funkcí spínací nebo rozpínací
- s vestavěnou ochranou smyčkou

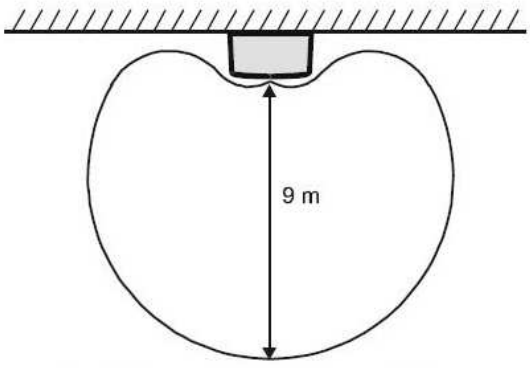
Výhodou je snadná a rychlá montáž s poměrně vysokou životností. Mezi nevýhody se řadí možnost zmagnetizování pomocí přiloženého magnetu. To je však možné jen u jednodušších provedení.

2.4 Detektory narušení skleněných ploch

Patří mezi důležité prvky plášťové ochrany. Používají se pro zabezpečení skleněných ploch a pláště budovy. K vyhlášení poplachu vede již první déle trvající mechanická změna střežené plochy. Detektory jsou vyráběny ve dvou variantách - kontaktní a bezkontaktní.

2.4.1 Akustické detektory tříštění skla

Jde o pasivní bezkontaktní detektor. Vyhodnocují slyšitelnou část zvuku, která je charakteristická pro tříštění skla o rozdílných velikostech a tloušťkách skleněné plochy. Pomocí piezoelektrického nebo elektretového mikrofonu se sledují zvukové signály a tlakové vlny typické pro tříštění skla. Pokud je splněn časový průběh a intenzita u obou složek dojde k vyhlášení poplachového stavu.



Obr. 10: Směrová charakteristika GBS[12]

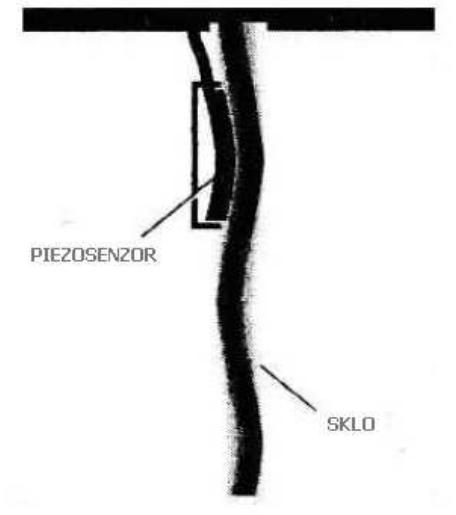
Výhodou je pokrytí všech skleněných ploch v jeho dosahu. Důležité je, aby čidlo na chráněné plochy vidělo. Mezi sklem a detektorem pak musí být volný prostor (žádné závěsy a žaluzie).

Za nevýhodu považujeme vznik falešných poplachů. V okolí detektoru může být mnoho negativních vlivů jako okolní dopravní provoz, kontejner na sklo, technické vybavení prostor nebo přítomnost drobné zvěře. Při instalaci detektoru je nutné zjistit, zda sklo není opatřeno bezpečnostní nebo jinou fólií. Tím se předejde snížení účinnosti detekce.

V praxi se používají dva typy akustických detektorů tříštění skla - *jednopásmová* a *vícepásmová.*

2.4.2 Pasivní detektory tříštění skla

Kontaktní detektor připevněný na skleněnou plochu, který detekuje energii vzniklou při rozbíjení skla. Jde o piezoelektrický senzor obsahující piezokrystal naladěný na rezonanční kmitočet v pásmu 40 -120 kHz. Elektronika ve vyhodnocovací jednotce sleduje jen kmitočty charakteristické pro určitý druh destrukce skla (řezání skla diamantem atd.). Ty se hmotou šíří jako vlnění v pevném tělese. Čidlo je přilepeno na skleněnou tabuli s důrazem na co nejmenší ztráty přenosu zvuku. Vlnění vzniklé při narušení skleněné tabule je vyhodnoceno piezosenzorem a dojde k vyhlášení poplachové stavu.



Obr. 11: Umístění piezosenzoru[3]

Čidlo pracuje bez citlivosti na rušivé hluky v zabezpečeném prostoru. Jako výhodu můžeme uvést i preventivní účinek, protože čidlo svou viditelnou instalací upozorňuje na přítomnost zabezpečovacího zařízení.

K nevýhodám patří nutnost pohyblivého přívodu při instalaci na otevírané plochy. Při aplikaci na dělené skleněné plochy je nutné, aby každá tabule měla svoje vlastní čidlo.

Do této skupiny můžeme zařadit také destrukční čidla - fóliové polepy a poplachové fólie a skla. [3]

2.4.3 Aktivní detektory tříštění skla

Kontaktní detektor rozbití skla, který obsahuje vysílací a přijímací část. Je namontovaný na skleněnou plochu a detekuje změny celistvosti povrchu skla. Následně vysílá, přijímá a zpracovává signály vzniklé při těchto změnách. Používají se pro nejvyšší stupně rizik.

2.5 Detektory prostředí

Do této skupiny řadíme tzv. speciální čidla. Slouží jako doplňkový sortiment k pohybovým detektorům. Jejich základní funkcí je detekování různých veličin a látek uvnitř hlídané plochy.

2.5.1 Požární detektory

Jsou určeny k detekci vzniku požáru v hlídaném prostoru. Používají se v podstatě dva hlavní typy - tepelné a opticko kouřové detektory. Poplach je opět signalizován výstražným znamením zabudované sirény a předáním zprávy ústředně. Ta pak může pomocí sms informovat majitele budovy.

a) Teplotní detektory - dochází k vyhodnocování maximální teploty v místnosti případně rychlosti jejího nárůstu (kombinace s termodiferenciálním detektorem). Aktivační teplota je obvykle nastavena kolem 60 ºC. Za nevýhodu můžeme považovat jejich zpoždění při reakci na vzniklý požár. Aby tedy došlo k vyhlášení poplachu je zapotřebí plamene, který způsobí zvýšení teploty.

b) Opticko kouřové detektory - obsahují vyhodnocovací komoru, která je prosvětlována IR diodou. Pokud se v ní objeví kouř je vyhodnocena světelná ztráta a detektor vyhlásí poplach. Výhodou je, že k detekci není potřeba přímý plamen, ale stačí již doutnání. Nevýhodou je nutnost čistění komory, pokud se detektor nachází v prašném prostředí. [11]

2.5.2 Detektory zaplavení

Čidla se používají v místech, kde může dojít k zatopení nebo úniku vody (koupelny, kuchyně, sklepy atd.). K vyhlášení poplachového stavu dojde, pokud kapalina spojí detekční kontakty. Tím se aktivuje vnitřní siréna detektoru pro místní výstrahu a předá se poplachová zpráva k ústředně.

Při volbě podobných detektorů patří mezi rozhodující parametry pracovní teplota a vlhkost v daném prostředí.

2.5.3 Detektory úniku plynu

Slouží k indikaci a detekci nebezpečných plynů v daném prostoru. Dle typu zařízení detekuje různé druhý plynů - propan, butan, zemní plyn, oxid uhelnatý, vodík atd..

Při instalaci těchto detektorů si musíme dávat pozor na váhu jednotlivých plynů vůči vzduchu. V závislosti na detekovaném plynu se tedy čidla umisťují co nejvýše nebo nejníže v příslušném prostoru.

a) Záplavový detektor b) Opticko kouřový a teplotní detektor (kombinovaný) c) Detektor úniku plynu CO

Obr. 12: Detektory prostředí[13]

2.6 Výstražná zařízení

Zařízení, které na základě vyhlášení poplachového stavu produkuje akustický poplachový signál. Jeho akustický výkon je velký a slouží pro maximální znepříjemnění pobytu narušitele v místnosti nebo výrazné upozornění na poplach. Jejich použití můžeme rozdělit na venkovní a vnitřní. Základem je akustický měnič (většinou piezoelektrický) doplněný o generátor kolísavého tónu a výkonový měnič. Instalují se tak, aby nebyly snadno dostupné a tím napadnutelné.

Tyto zařízení můžou být ještě doplněna o optickou signalizaci (světelný maják).

Obr. 13: Piezoelektrická siréna[12]

2.7 Zamlžovací bezpečnostní zařízení

Systém tvořící řadu samostatných zařízení v odolném krytu, který při aktivaci vyvine hustou mlhu za účelem snížení viditelnosti v chráněném prostoru. Tím dojde k dezorientaci narušitele a eliminuje tak škodu, kterou by mohl napáchat. . Při aktivaci dojde k rozptýlení tekutiny do prostoru během několika sekund. Mlha je naprosto nezávadná a neškodná vůči oděvu, výpočetní technice, dokumentům i zvířatům. Obnovení normální viditelnosti trvá kolem 20 až 30 minut.

Pro velké objekty se můžou používat systémy s výkonem až 800 m^3 za 30 sekund. V prostorech kde se využívá zamlžovací bezpečnostní zařízení je umístěna následující varovná tabule. [7]

Obr. 14: Varovná tabule[7]

3 OVLÁDÁNÍ SOUČASNÝCH PRVKŮ PZTS

Hlavní funkcí ovládacího zařízení současných prvků PZTS je uvedení systému do stavu střežení nebo klidu. To můžeme provádět pomocí uživatelského kódu, kartou, bezdrátovou klíčenkou nebo vzdáleně přes softwarovou nadstavbu. Cílem je tedy jednoduchost ovládání tohoto systému, ale současně i dostatečná ochrana proti překonání.

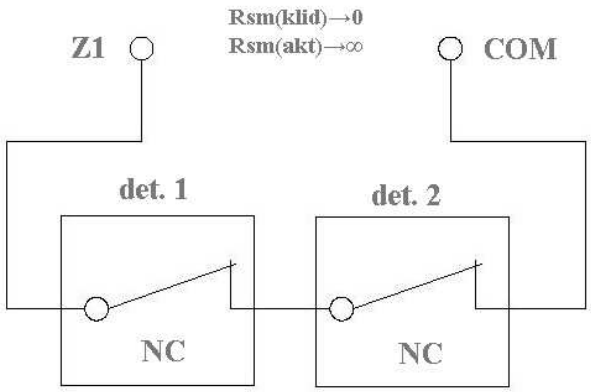
Proto je důležité při výběru zabezpečovacího systému určit vhodnou ústřednu na základě jejích parametrů. Za základní charakteristiku považujeme počet zón, které je schopna sledovat.

3.1 Typy drátových smyček

Drátové ústředny jsou s detektory propojeny formou jednotlivých smyček (zón). Na každou může být připojen jeden i několik detektorů. Ústředna měří a vyhodnocuje odpor smyčky a pokud dojde k jeho změně vyhlásí poplach. Rozlišujeme dva základní typy zapojení - *NC (Normally closed)* a *NO (Normally opened).*

3.1.1 NC - v klidu uzavřená

Zapojení smyčky se vyznačuje tím, že kontakty detektorů jsou v klidovém stavu sepnuty. To znamená, že jí neustále prochází elektrický proud. Pokud se aktivuje některé z čidel dojde k rozpojení kontaktu. Zapojení tedy detekuje pouze dva stavy - klidový a poplachový. Jestliže připojujeme více detektorů, jejich zapojení je sériové.

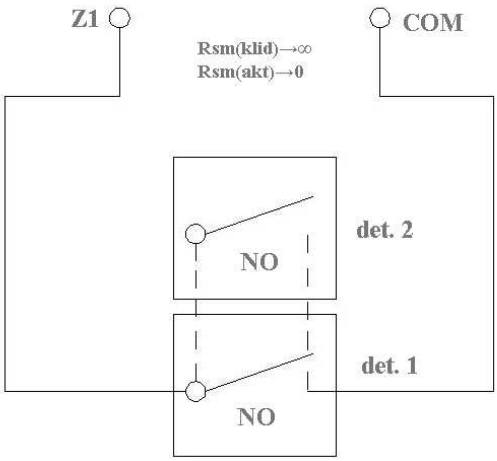


Obr. 15: Smyčka NC(rozpínací)

Nevýhodou je, že smyčka nepozná jestli byla zkratována nebo rozpojena detektorem. Dále zde chybí kontakty tamper (otevření detektoru) a antimasking (zakrytí detektoru).

3.1.2 NO - v klidu otevřená

Jednotlivé kontakty detektorů jsou v klidu otevřené. Když dojde k vyhlášení poplachu dojde k jejich sepnutí. Ústředna opět vyhodnocuje dva stavy a v rámci jedné smyčky nedokážeme určit, který detektor poplach vyvolal. Větší počet čidel se musí zapojovat paralelně.



Obr. 16: Smyčka NO(spínací)

V klidovém stavu smyčkou neprochází žádný proud což můžeme považovat za výhodu. Jestliže ale dojde k přerušení vedení, nedokážeme tuto závadu rozpoznat a smyčka se stává nefunkční. Proto se druh tohoto zapojení příliš nepoužívá.

3.1.3 EOL - odporově vyvažovaná

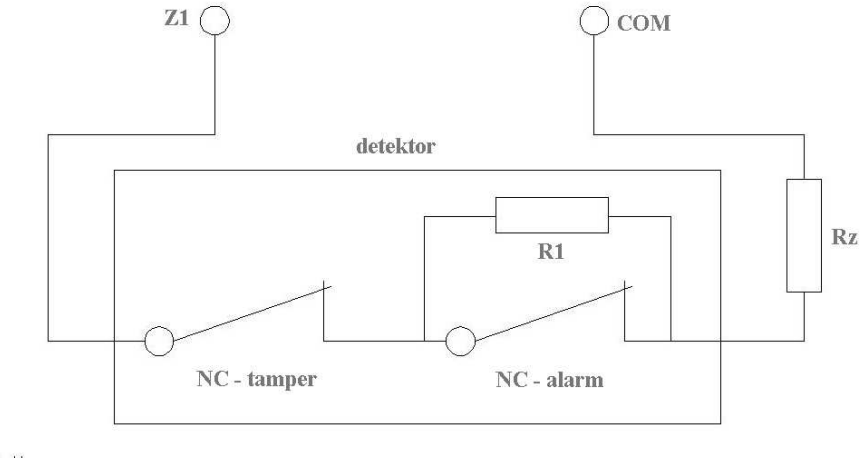
Vedení smyčky je chráněno koncovým odporem, takže můžeme rozpoznat kdy došlo ke zkratování smyčky (sabotáži). Takové zapojení označujeme zkratkou EOL (End of line). Součástí je i kontakt tamper, který se aktivuje při nedovolené manipulaci s krytem detektoru.

Ústředna rozlišuje tři základní stavy - sabotážní, klidový a poplachový. Hodnota koncového odporu je většinou 1k1, 2k2 nebo 2k7. Umísťuje se do nejvzdálenějšího místa od ústředny aby byla hlídána celá délka smyčky.

3.1.4 2EOL - dvou odporově vyvažovaná

K tomuto typu zapojení smyčky je přidán další odpor R_1, který je paralelně připojen ke každému poplachovému kontaktu. Díky němu je ústředna schopna rozlišit rozdíl mezi aktivací poplachového nebo sabotážního kontaktu.

Pokud je smyčka v klidovém stavu, tak se její odpor blíží hodnotě vyvažovacího odporu R_Z. Jakmile se navýší o hodnotu R_1 je vyhlášen poplachový stav vlivem aktivace čidla. Když dojde k sabotáži blíží se odpor ve smyčce k nekonečnu. V případě zkratování smyčky se odpor blíží nule.



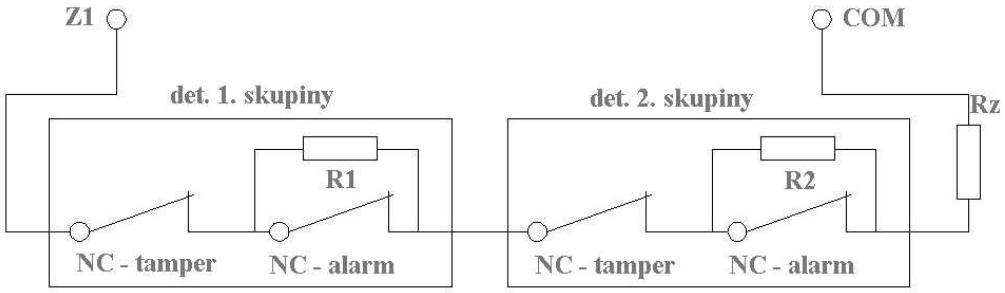
Obr. 17: Smyčka 2EOL(s NC kontakty)

Používá se i smyčka *3EOL - tří odporově vyvažovaná*, kde přibyl kontakt antimasking s paralelně připojeným odporem. Ústředna tedy dokáže detekovat zakrytí čidla.

3.1.5 ATZ - odporově vyvažovaná zdvojená

Na rozdíl od předchozích zapojení dokážeme rozeznat, které čidlo bylo aktivováno. Na jedné smyčce jsou totiž připojeny dvě skupiny detektorů o dvou typech odporu. Jedna skupina detektorů používá k vyhodnocení poplachu hodnotu odporu R_1 a druhá hodnotu R_2. Pokud je ke koncovému odporu přičtena hodnota R_1 je vyhlášen poplachový stav v 1. skupině detektorů. Když dojde k poplachu ve 2. skupině, jedná se o hodnotu R_2. V klidovém stavu se hodnota celkového odporu přibližuje hodnotě zakončovacího odporu R_Z.

Nevýhodou je, že nezjistíme ve které skupině došlo k aktivaci sabotážního kontaktu (tamperu).



Obr. 18: Smyčka ATZ

3.2 Typy poplachových zón

Jednotlivé detektory jsou v systémech PZS zařazeny do předem definovaných zón. Na jejich základě si ústředna zvolí druh reakce na narušení detektoru nebo střeženého prostoru.

Mezi nejčastěji používané režimy poplachový ústředen patří:

- **Okamžitá zóna**

Zastřeženo - při narušení detektoru dojde k vyhlášení poplachového stavu.

Odstřeženo - narušení detektoru není vyhodnoceno jako poplach.

- **Zpožděná zóna**

Zastřeženo - po aktivaci detektoru je spuštěn příchodový čas. Po jeho dobu je nutné systém vypnout pomocí kódu nebo jiného identifikačního prvku, jinak bude vyhlášen poplach.

Odstřeženo - narušení detektoru není vyhodnoceno jako poplach.

- **Plášťová zóna (STAY)**

Zastřeženo - pokud označíme zónu jako STAY, tak je její narušení ignorováno. V opačném případě je při narušení detektoru okamžitě vyhlášen poplach.

Odstřeženo - narušení detektoru není vyhodnoceno jako poplach.

- **24 hodinová zóna**

Zastřeženo/odstřeženo - v obou případech se při narušení detektoru vyhlásí poplach. Je tedy neustále v režimu hlídání.

- **Požární zóna**

Zastřeženo/odstřeženo - vyhodnocuje poplachový stav na stejném principu jako 24 hodinová zóna. Rozdíl je v signalizaci poplachu, který je přerušovaný.[11]

3.3 Ústředny Concept

Systémy Concept 3000 / 4000 Access patří mezi často používané zabezpečovací systémy pro velké objekty s množstvím podsystémů. Výrobcem je australská firma Inner Range. Umožňuje připojení až 2000 smyček a 3800 programovatelných výstupů. To vše můžeme rozdělit až na 240 podsystémů.

Systém nabízí i řadu doplňkových funkcí:

- **docházkový systém** (pomocí komunikačního formátu Wiegand).
- **systém řízení a správy budov** (klimatizace, topení, výtahy).

Ústředna komunikuje s poplachovým přijímacím centrem, GSM telefony, prostředky výpočetní techniky nebo může přenášet data po LAN pomocí internetu. Zpracování informací probíhá paralelně, takže umožní přenášení informací na několik zařízení současně.

Konfigurace a kontrola stavu systému se provádí pomocí softwaru *Insight*. Propojení k počítači je realizováno přes TCP/IP (internet) nebo sériovým rozhraním (RS-232).

Počet jednotlivých prvků systému (zóny, podsystémy, PGM výstupy atd.) závisí na vloženém paměťovém čipu. Ty se dodávají v těchto velikostech - 32 kB, 128 kB a 512 kB. Systém Concept spadá do stupně zabezpečení 4. kategorie (vysoké riziko).

Tab. 4: Základní technické parametry ústředen Concept[14]

	Concept 3000/4000 Access (Paměť 32 kB)	**Concept 3000/4000 Access** (Paměť 128 kB)	**Concept 3000/4000 Access** (Paměť 512 kB)
Podsystémy	24	96	240
Maximální počet zón	až 130	až 600	až 2000
Počet zón na ústředně	16	16	16
PGM výstupy	2 / 130	2 / 600	2 / 3800
Uživatelů	100	2000	4000
LCD klávesnice	8	32	99
Čtečky	16	64	240
Historie událostí	550	2000	6500

3.3.1 Možnosti ovládání systému

Zabezpečovací systém Concept 3000/4000 Access je uživatelem ovládán a programován přes LCD klávesnici, dotykový terminál nebo čtečku karet. Dále nám tyto komponenty ukazují aktuální přehled stavu systémů a podsystémů.

a) LCD klávesnice IRT 3000

Slouží k zapnutí nebo vypnutí hlídaných prostor. Jejich funkčnost nastavíme na základě našich požadavků. A to buď pro práci s celým systémem nebo vybranými podsystémy. V celém systému jich můžeme použít až 99.

K přihlášení do systému použije uživatel svůj PIN kód. Ten jej při správném zadání identifikuje v opačném případě zamítne jeho přístup. Následně se objeví názvy střežených prostorů. Zde si uživatel může vybrat, zda chce daný prostor odstřežit nebo zastřežit. Když vybereme variantu zapnutí střeženého prostoru, systém nejprve otestuje použité prvky v tomto místě a až poté nám ohlásí aktivaci (viz. obr. 20).

K pomoci při ovládání slouží klávesa HELP, která zobrazí nápovědu pro dané téma.

Obr. 19: LCD klávesnice Concept

b) Dotykový terminál Concept 4000

V současné době se používají i dotykové terminály, které mají lepší grafické prostředí než LCD klávesnice. Využívají barevného displeje s úhlopříčkou 3,5 palce. Bez nutnosti přihlášení pomocí PIN kódu můžeme ovládat některé doplňkové funkce (osvětlení, vytápění, žaluzie). Po spuštění se nabídka čísel pro zadání PIN kódu přemisťuje. Tím se má předejít opotřebení displeje na vybraných místech. (viz. obr. 21). [15]

c) Čtečka karet

Jejich zapojení do systému je provedeno přes přístupové moduly. Z hlediska konstrukce se dělí na dva typy - bezdotykové a dotykové. Jako identifikační medium používáme kartu nebo čip. Ověření může být kombinováno i s následným zadáním PIN kódu.

Obr. 20: Dotykový terminál[15]

3.4 Ústředny Galaxy Dimension

Modulární systémy určené k použití pro malé i rozsáhlé objekty. Výrobcem těchto systémů je firma Honeywell Security. Jejich součástí je i komplexní řešení systémů zabezpečení a kontroly vstupu.

Systém umožňuje audio verifikaci. Jde o novou funkci, která dopřeje pracovníkům poplachového přijímacího centra hlasový odposlech. Ten je proveden z mikrofonu umístěného v blízkosti narušení.

Komunikace je zajištěna pomocí telefonní linky, Ethernetu nebo RS-232. Program určený pro monitorování a záznam z ústředen se nazývá *Tegal.* [16]

Zařízení splňuje požadavky na stupeň zabezpečení 3. střední až vysoké riziko. Zároveň spadá do třídy prostředí II. - vnitřní všeobecné.

Tab. 5: Technické parametry ústředen Galaxy Dimension[16]

	GD-48	**GD-96**	**GD-264**	**GD-520**
Podsystémy	8	16	32	32
Maximální počet zón	až 48	až 96	až 264	až 520
Počet zón na ústředně	16	16	16	16
PGM výstupy	8 / 24	8 / 48	8 / 132	8 / 260
Uživatelů	100	250	999	999
LCD klávesnice	8	16	16	32
Čtečky	4	16	16	32
Historie událostí	1000	1500	1500	1500

3.4.1 Možnosti ovládání systému

Systém Galaxy Dimension se ovládá z LCD klávesnice, dotykovým terminálem nebo bezkontaktní čtečkou. Dotykových terminálů můžeme instalovat jen omezené množství a to 1 až 4 podle typu ústředny. Ovládacími prvky systému jsou tedy PIN kódy, karty a klíčenky.

a) LCD klávesnice MK7

Jedná se o jednoduchou dvouřádkovou klávesnici. Přístup do systému provedeme zadáním uživatelského kódu. Zmáčknutí kláves nám odpoví pípnutím. Při správném vložení kódu se zobrazí menu s vlastními podsystémy tzv. grupy. Jednotlivé grupy jsou označeny písmeny:

„*P*“ - připraveno k zapnutí,

„*N*“ - není připraveno k zastřežení,

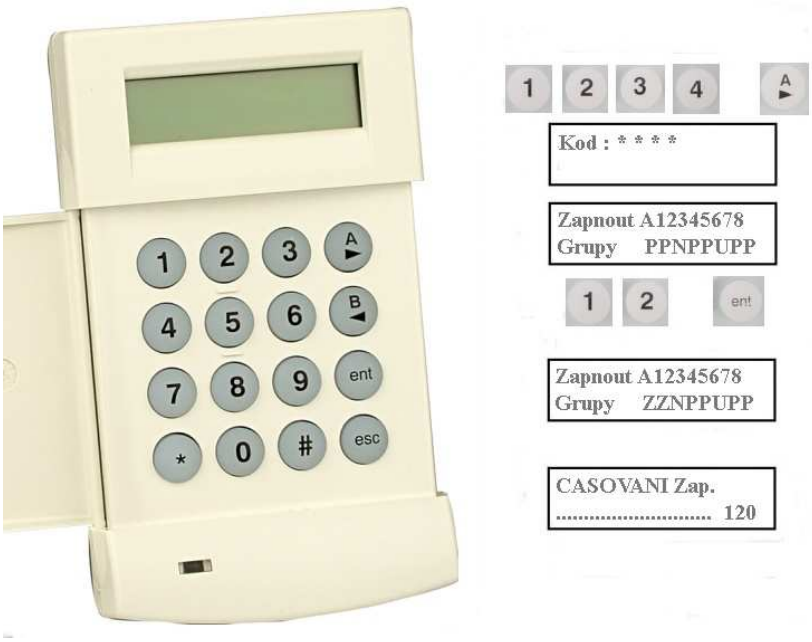
„*Z*“ - zapnuto,

„*U*“ - uzamčeno časovým zámkem,

„-“ - z dané klávesnice není přístup,

„*C*“ - částečně zastřeženo.

Stisknutím čísla příslušné grupy měníme jejich stav (například z „*P*“ na „*Z*“). Poté klávesou potvrdíme zvolené nastavení.



Obr. 21: LCD klávesnice MK7

b) Ovládání systému kartou

Čtečka bezkontaktních karet je vestavěna v klasické LCD klávesnici a slouží pro zjednodušení obsluhy poplachového zabezpečovacího systému. Uživatel tedy kartu může použít pro zastřežení systému. Pokud má nadefinován přístup jen pro jeden podsystém, je jeho aktivace možná pouhým předložením karty před čtečku. To provede v délce asi 3 sekund v pravém dolním rohu klávesnice.

Jestliže má však uživatel na výběr z více podsystémů, musí po podržení karty vybrat systémy k zastřežení na klávesnici. Další funkcí je tzv. dual focus, který má využití v prostorech s vysokými riziky. Jde o kombinaci kódu a karty. Až potom má uživatel povolen přístup do menu.

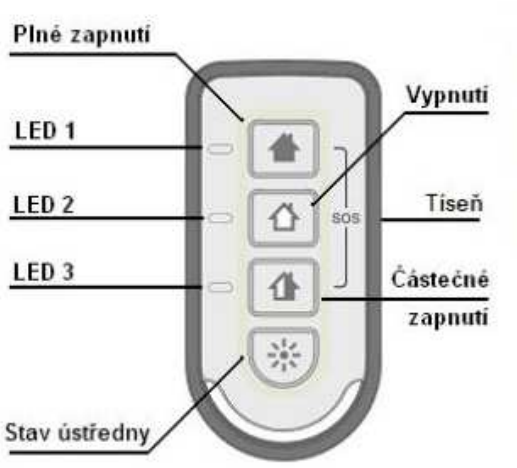
K systému je možno připojit i dotykový terminál s vestavěnou čtečkou karet, který poslouží k vyššímu komfortu ovládání. Další možností je připojení samostatné čtečky a klávesnice, musí být ale navzájem kompatibilní. [17]

Obr. 22: Dotykový terminál Honeywell[17]

c) Ovládání bezdrátovou klíčenkou

Další způsob k ovládání ústředny Galaxy Dimension je bezdrátová klíčenka s obousměrnou komunikací. Je vybavena 4 tlačítky a signalizačními LED diodami. Uvedený dosah na přímou viditelnost je 80 metrů. Pracuje na frekvenci 868 MHz.

Klíčenka umožní zapnutí, vypnutí a kontrolu systému, reset poplachových událostí a vyslání tísňového signálu.



Obr. 23: Klíčenka TCB800[17]

3.5 Ústředny Digiplex EVO

Jedná se o řadu ústředen pro střední a velké objekty se sběrnicovým systémem. Kromě zabezpečení je zde i nadstavba přístupového systému, která dokáže omezit pohyb osob po objektu. Na programovatelné výstupy můžeme přiřadit libovolné události (řízení osvětlení, klimatizace atd.). Ústředna Digiplex EVO 48 se však již pomalu přestává dodávat.

K naprogramování a správě systému Digiplex EVO 48 a 192 se používá softwarová nadstavba WinLoad. Komunikace mezi PC a ústřednou probíhá s pomocí USB adaptéru, IP (internetu) nebo telefonní linky. Systém je zařazen do stupně zabezpečení 3 - riziko střední až vysoké. [13]

Tab. 6: Technické parametry ústředen Digiplex[13]

	Digiplex EVO48	**Digiplex EVO192**
Podsystémy	4	8
Maximální počet zón	až 48	až 192
Počet zón na ústředně	16	16
PGM výstupy	5 / 250	5 / 250
Uživatelů	96	999
LCD klávesnice	127	254
Čtečky	32	32
Historie událostí	1024	2048

3.5.1 Možnosti ovládání systému

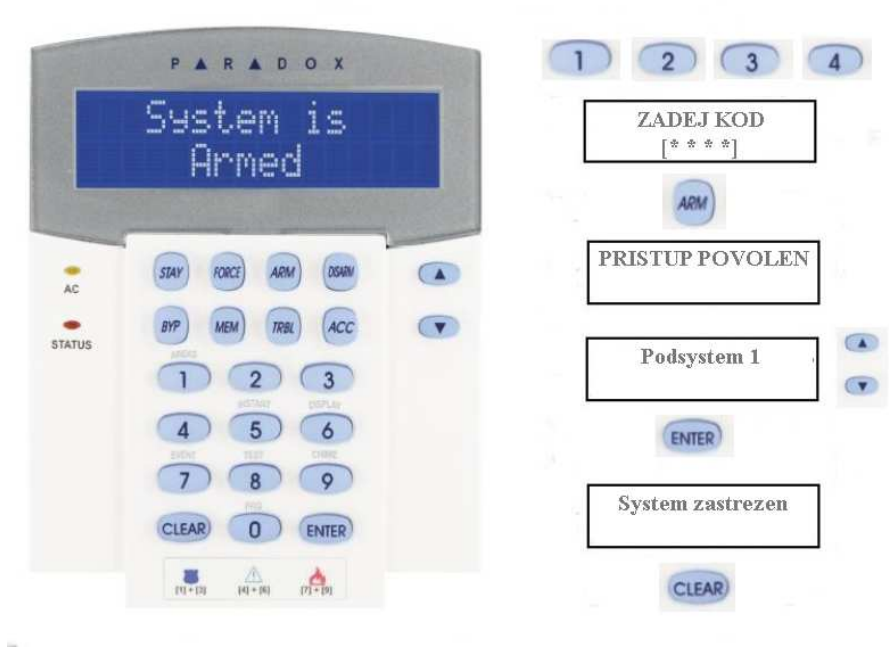
Klávesnice pro systémy Digiplex EVO nám umožní programování, ovládání a přehled o stavech systému. Můžeme si vybrat z několika druhů provedení terminálů (dvouřádkové LCD klávesnice, grafické LCD klávesnice nebo grafické dotykové terminály).

Dle požadavků uživatele můžou být doplněny o zabudovanou čtečku karet nebo LED zobrazovače. Ty slouží k zobrazení stavu jednotlivých zón nebo podsystémů. Nadstavbu tvoří přístupový systém Access, který je schopen zařadit do systému samostatné čtečky karet.

LCD klávesnice s vestavěnou čtečkou karet

K zapnutí nebo vypnutí systému použijeme uživatelský kód, kartu nebo bezdrátovou klíčenku. Klávesnice je vybavena zvukovou signalizací, která při platném příkazu trojitě zapípá v opačném případě se ozve dlouhý tón.

Normální zastřežení je aktivováno po zadání uživatelského kódu a výběru příslušného podsystému. Na klávesnici je i tlačítko pro tzv. nucené zastřežení (FORCE). Systém nezastřeží otevřené zóny, k jejich aktivaci dojde až po uzavření.



Obr. 24: LCD klávesnice Paradox

Druhou možností je zastřežení systému kartou. Aby bylo možné zapnutí, musí být zavřené dveře a zóny v klidu (uživatelé nejsou v objektu). Karta nebo přívěsek se přikládá v oblasti alfanumerických čísel na klávesnici. K zastřežení dojde pokud ji asi během 5 sekund načteme 2x za sebou. Vypnutí provedeme pouze jedním přiložením karty.

Nadstavba přístupového systému je funkční, když jsou uživatelé v objektu a zabezpečení je vypnuté. Pak má uživatel přístup do definovaných dveří dle skupiny přístupu a času. [13]

3.6 Ústředny ATS

Ústředny Aritech ATS 2000/3000/4000 mají využití v malých, středních i rozsáhlých instalacích. Jejich výrobcem je společnost GE Interlogix. Jde o integrovaný zabezpečovací systém a systém kontroly vstupu. Na desce ústředny je 16 dvojitě vyvážených vstupů rozšiřitelných až na 256. Přímo na datovou sběrnici můžeme připojit bezdotykové čtečky a jejich prostřednictvím ovládat zabezpečovací systém.

Jako konfigurační, řídící a monitorovací prostředek se používá softwarová nadstavba *Titan.* Komunikace ústřednou je přes RS-232 port nebo modem. Splňuje požadavky na stupeň zabezpečení 3 - střední až vysoké. [18]

Tab. 7: Technické parametry ústředen ATS[18]

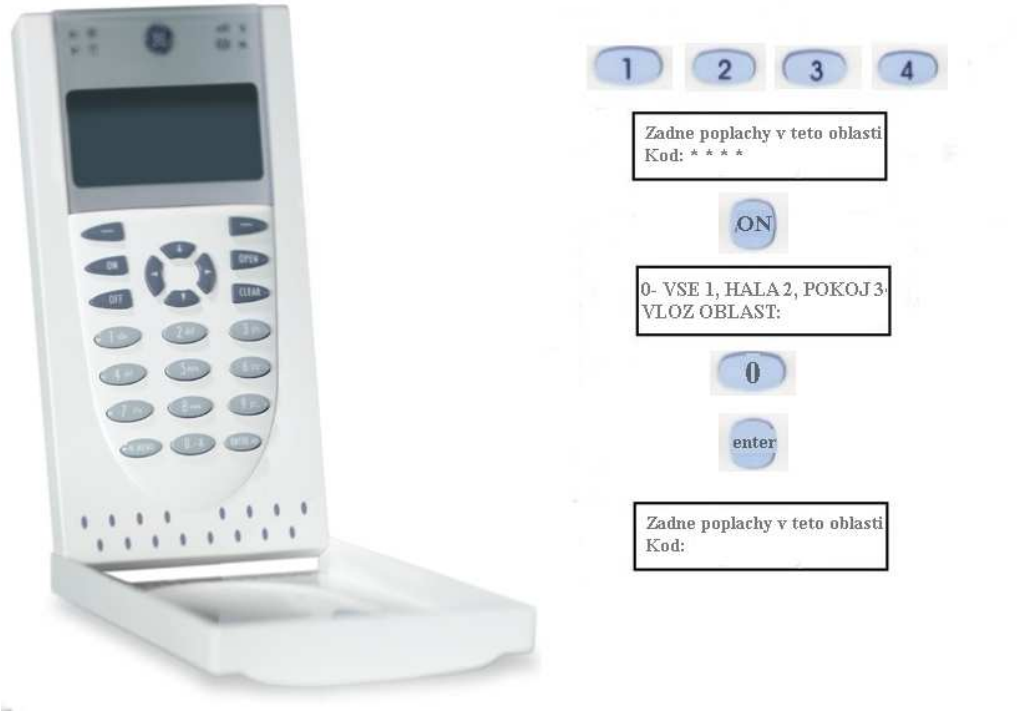
	ATS 2000	**ATS 3000**	**ATS 4000**
Podsystémy	4	8	16
Maximální počet zón	až 32	až 64	až 256
Počet zón na ústředně	8	8	16
PGM výstupy	3 / 255	3 / 255	3 / 255
Uživatelů (karet)	50	200(11466)	200 (11466)
LCD klávesnice	16	16	16
Čtečky	16	16	16
Historie událostí	10	1000	1000

3.6.1 Možnosti ovládání systému

Zabezpečovací systém se ovládá LCD klávesnicí s LED diodami. Ty jsou určeny pro optickou signalizaci stavu systému a podsystému. Jako nadstavbu můžeme připojit bezkontaktní čtečky pro systémy kontrolu a vstupu. Dle požadavků zákazníka se zvolí způsob jejich užití. Buď budou sloužit jen ke kódovému ovládání systému nebo ke kontrole vstupu v objektu.

Zastřežení přes alfanumerickou klávesnici provedeme zadáním uživatelského kódu a zvolením podsystému, který chceme aktivovat.

Pokud chceme objekt zastřežit pomocí karty, tak ji během asi 10 sekund přiložíme 3x ke čtečce. Pak dojde k aktivaci systému a spustí se odchodový čas. Když chceme následně systém odstřežit, stačí už předložit kartu jen jednou. Při pokusu deaktivace systému nedefinovanou kartou dojde k vyhlášení poplachového stavu.



Obr. 25: Klávesnice ATS

II. PRAKTICKÁ ČÁST

4 UŽIVATELSKÉ POŽADAVKY NA UŽÍTÍ SYSTÉMU PZTS

V této části se zaměříme na požadavky uživatelů směrem k ovládání poplachových zabezpečovacích systémů. K zjištění současného stavu je zvolen průzkum trhu formou dotazníku.

4.1 Struktura dotazníku

Pomocí vytvořeného dotazníku provedeme uživatelský průzkum trhu, který je zaměřený na způsob a náročnost ovládání systémů PZTS. Dotazník obsahuje 19 otázek k vyplnění, z toho je 12 povinných a 7 nepovinných.

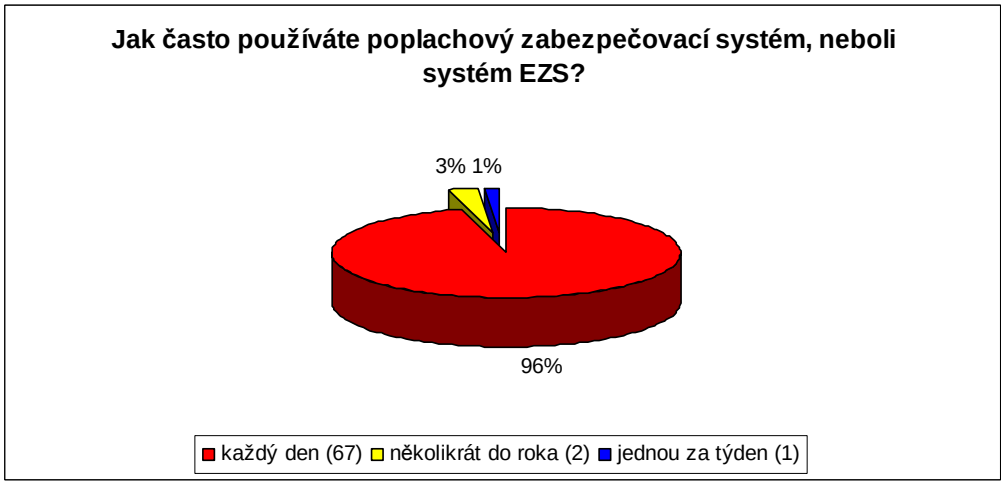
Jako cílovou skupinu jsem si zvolil servisní a dodavatelské firmy na území České republiky. Ty jsem si vybral na základě jejich zkušeností s ovládáním poplachových zabezpečovacích systémů.

4.2 Vyhodnocení dotazníku

Dotazník byl elektronickou formou zaslán do přibližně 200 firem, kde jsem následně získal odpověď od 70 respondentů. Z toho vyplývá, že návratnost dotazníku byla asi 35 %.

Otázka č. 1: *Jak často používáte poplachový zabezpečovací systém, neboli systém EZS?*

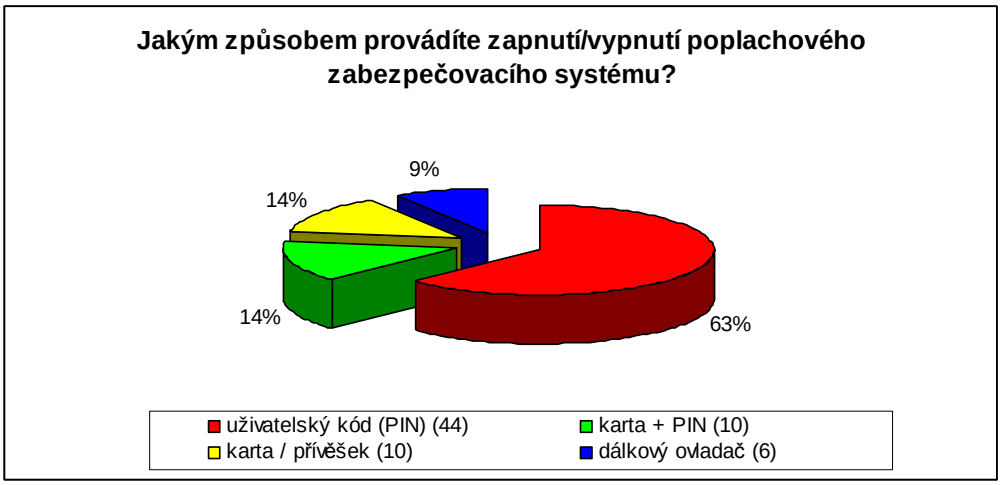
Cílem otázky bylo zjištění, jak často přijdou respondenti do styku s poplachovými zabezpečovacími systémy. Na základě odpovědí můžeme zjistit, že 96 % dotázaných používá systém PZTS každý den.



Graf 1: Četnost použití PZTS

Otázka č. 2: *Jakým způsobem provádíte zapnutí/vypnutí poplachového zabezpečovacího systému?*

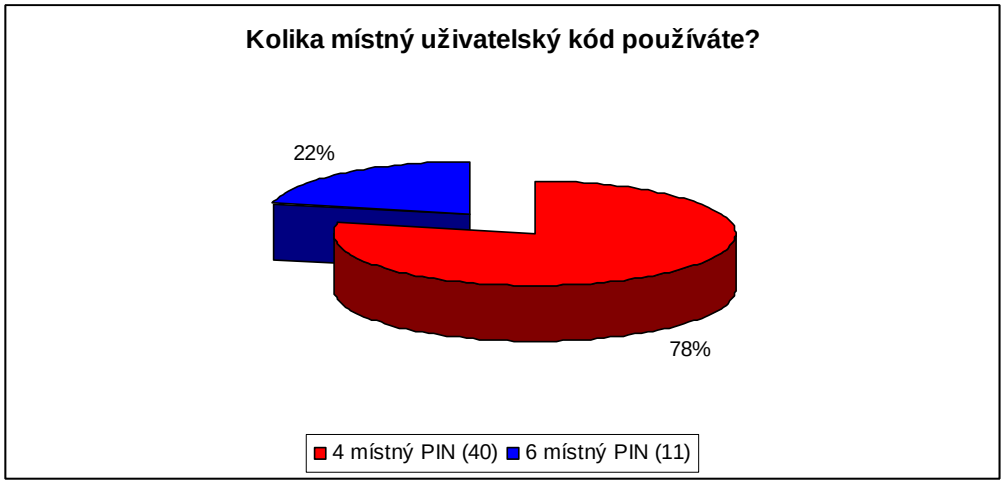
Otázka byla položena za účelem zjištění způsobu odstřežení nebo zastřežení podsystému/systému. Nejvíce se tedy používá uživatelský kód, který označilo 63 % dotázaných. Následující dvě otázky souvisí právě s ovládáním pomocí PIN kódu.



Graf 2: Způsob zapnutí/vypnutí PZTS

Otázka č. 4: *Kolika místný uživatelský kód používáte?*

Tato otázka navazuje na předchozí odpověď a byla určena těm, kteří ovládají poplachové zabezpečovací systémy pomocí PIN kódu zadaného na klávesnici.

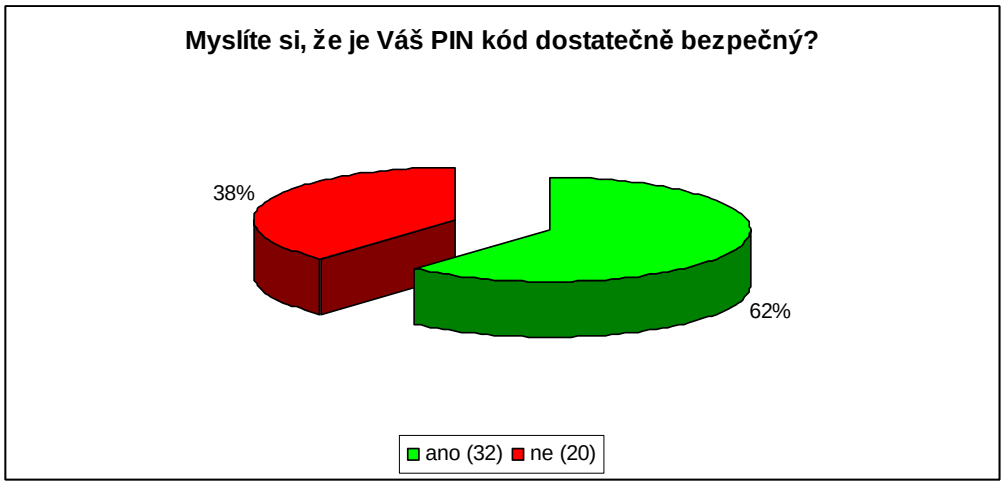


Graf 3: Délka PIN kódu

Zde většina dotázaných používá 4 místný uživatelský kód. Ten se však může zdát jako nepříliš bezpečný. Někteří uživatelé totiž používají pro lepší zapamatování PIN kód s rokem narození nebo založením firmy. Tím pádem se může stát lehce dostupným pro případného narušitele objektu.

Otázka č. 5: *Myslíte si, že je Váš PIN kód dostatečně bezpečný?*

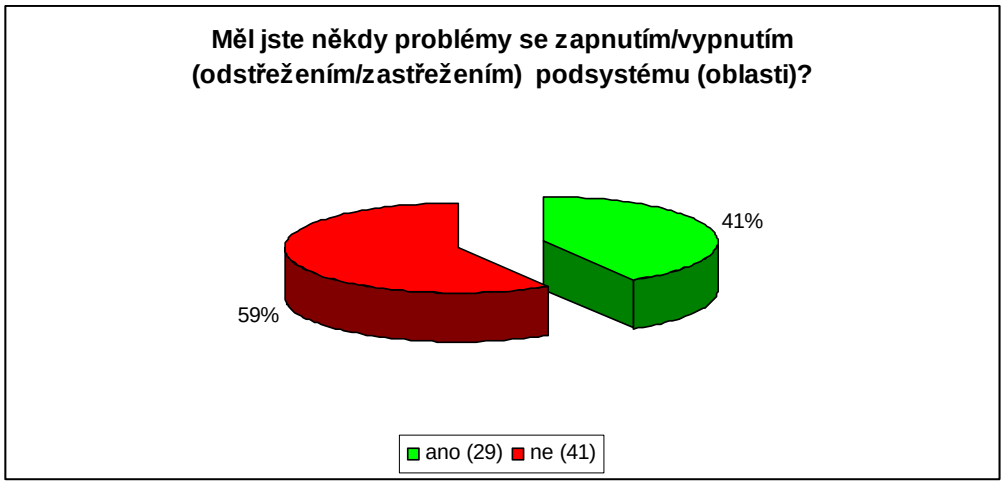
Otázka byla položena za účelem zjištění, zda jsou dotázané osoby přesvědčené o dostatečné bezpečnosti používaného uživatelské kódu. U 4 místného kódu si jsou uživatelé v 57 % jisti, že je bezpečný a u 6 místného má toto číslo hodnotu 73 %. V celkovém výsledku připadá 62 % respondentů jako bezpečný.



Graf 4: Bezpečnost PIN kódu

Otázka č. 6: *Měl jste někdy problémy se zapnutím/vypnutím (odstřežením/zastřežením) podsystému (oblasti)?*

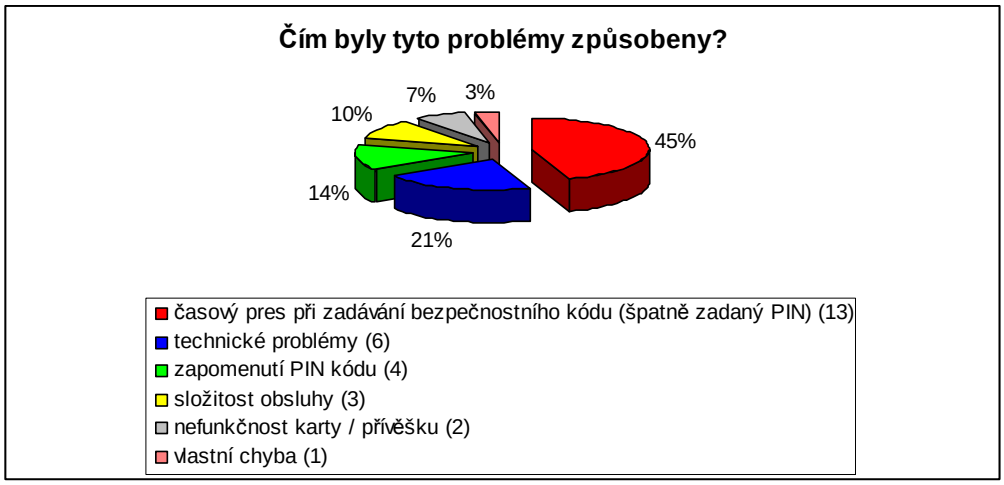
Cílem této otázky bylo zjištění, jak časté jsou problémy vyskytující se při ovládání podsystémů. Na základě odpovědi byla případně přiřazena další podotázka. Problémy se vyskytly u 41 % dotázaných, což je poměrně vysoké číslo.



Graf 5: Četnost problémů při ovládání PZTS

Otázka č. 7: *Čím byly tyto problémy způsobeny?*

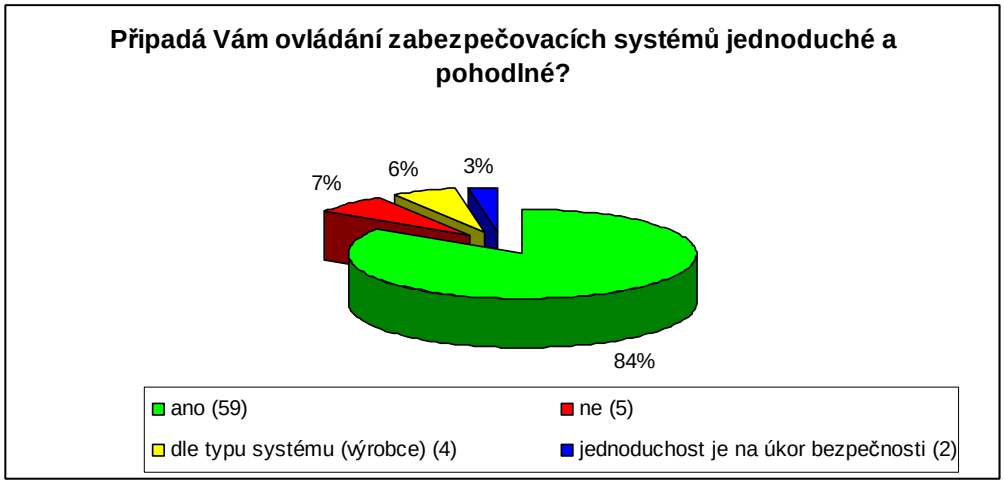
Jedná se o doplňující otázku v reakci na předchozí odpověď. Jde o definování vzniku problému, který nastal při ovládání poplachového zabezpečovacího systému. Téměř polovinu problémů tvoří časový pres při zadávání uživatelského kódu. Ten může být způsobený špatným nastavením příchodového času. Další často vyskytující se problémy jsou technického rázu (nefunkční klávesnice, porucha na detektorech, neuzavřená zóna apod.).



Graf 6: Typy vzniku problémů

Otázka č. 8: *Připadá Vám ovládání zabezpečovacích systémů jednoduché a pohodlné?*

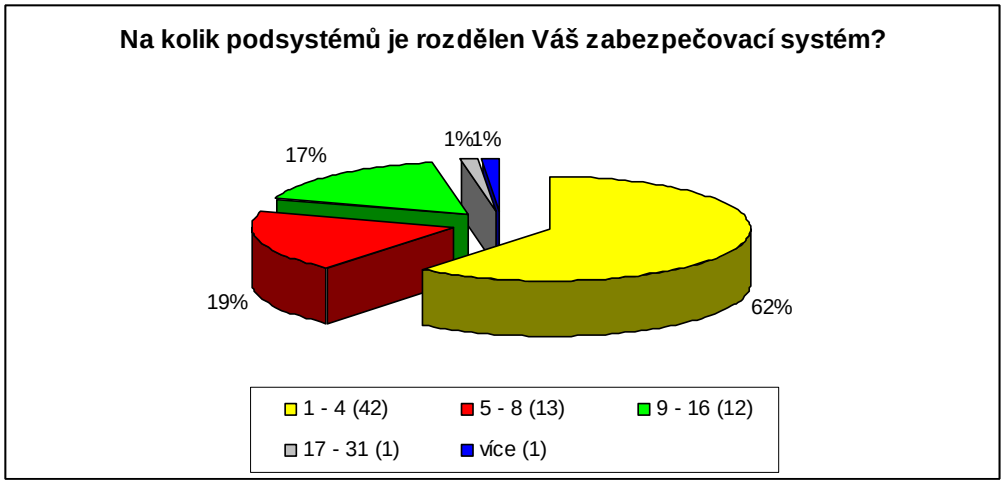
Otázka je zaměřena na zjištění spokojenosti ovládání současných systémů PZTS. Většina dotázaných odpověděla „ano“, takže jim připadá ovládání jednoduché a pohodlné. Výsledek je určitě ovlivněn i tím, že většina respondentů přichází do styku s těmito systémy každý den.



Graf 7: Spokojenost při ovládání PZTS

Otázka č. 9: *Na kolik podsystémů je rozdělen Váš zabezpečovací systém?*

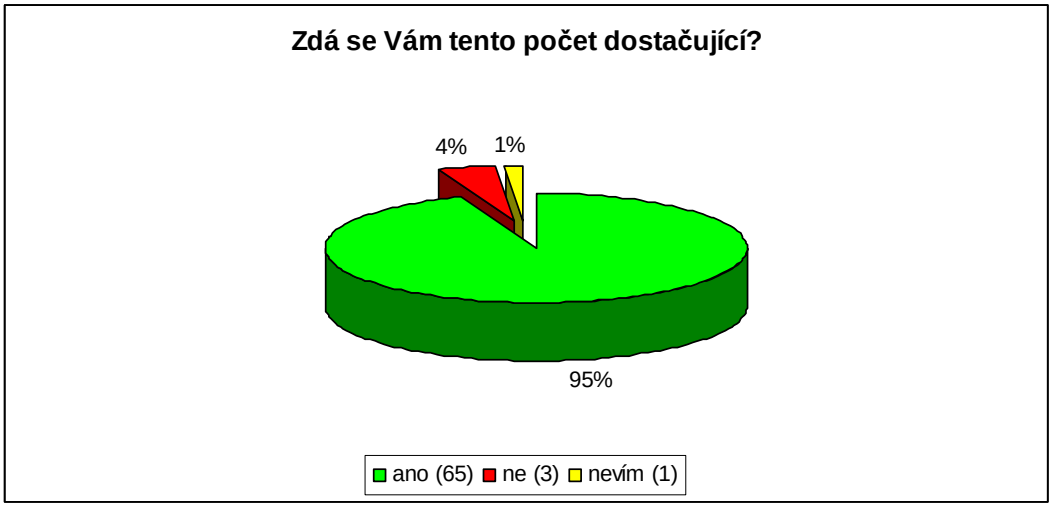
Otázka byla položena s cílem zjistit jak rozsáhlé systémy používají oslovené subjekty. Nejvíce odpovědí bylo s užitím 1 až 4 podsystémů, takže se jedná o zabezpečení menších objektů.



Graf 8: Počet podsystémů

Otázka č. 10: *Zdá se Vám tento počet dostačující?*

Otázka byla položena za účelem zjištění, zda uvedený počet podsystémů dotázaným vyhovuje nebo by potřebovali systém rozšířit. U této otázky odpovědělo 95 %, že je jimi používaný systém dostačující.



Graf 9: Rozšiřitelnost systému

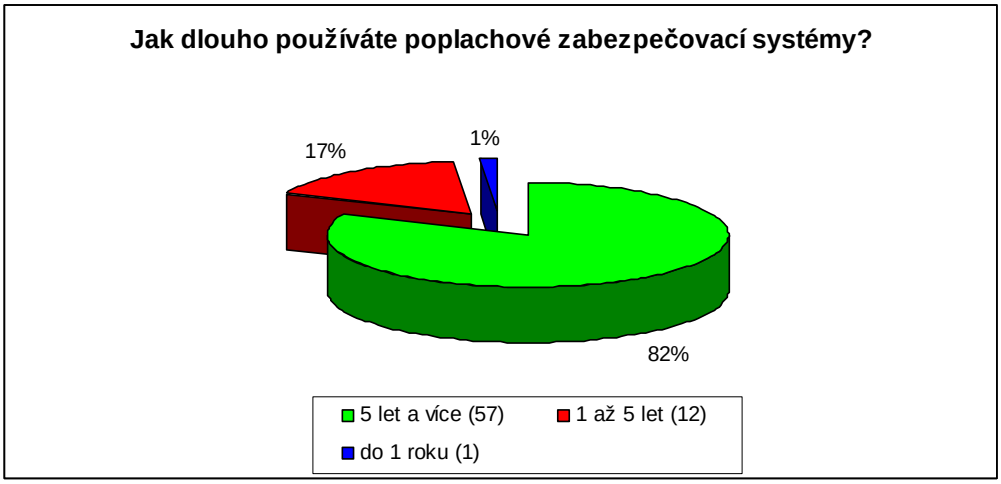
Otázka č. 11:*Napadá Vás nějaká myšlenka (funkce), která by vedla k lepšímu ovládání poplachových zabezpečovacích systému?*

Tuto otázku jsem položil tak, aby respondenti měli možnost vyjádřit svou myšlenku na zlepšení kvality ovládání poplachových zabezpečovacích systémů. V odpovědích se objevovaly i již používané bezdotykové terminály nebo komunikace pomocí smartphonu.

Nejčastěji byla zmiňována kombinace rozpoznání uživatele pomocí obličejového terminálu a hlasové komunikace. Tento návrh se objevoval i v otázce č. 19.

Otázka č. 12: *Jak dlouho používáte poplachové zabezpečovací systémy?*

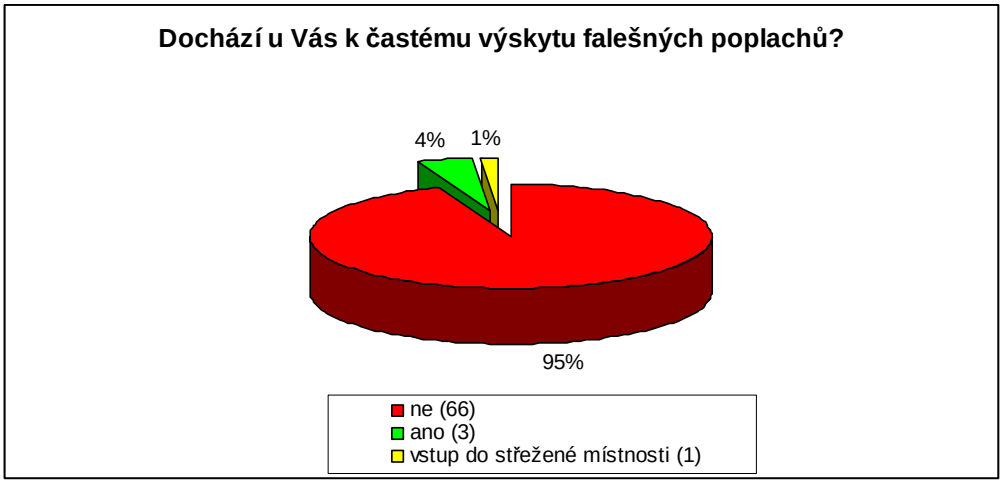
Tato otázka měla za úkol zjistit jak dlouhou dobu se respondenti setkávají se systémy PZTS. Tedy jaké mají zkušenosti s jejich používáním a ovládáním. Z dotazníku plyne, že 82 % dotázaných používá poplachové zabezpečovací systémy více jak 5 let.



Graf 10: Doba užívání PZTS

Otázka č. 13: *Dochází u Vás k častému výskytu falešných poplachů?*

Cílem otázky bylo zjištění, jak často dochází ke spuštění alarmu vlivem falešných poplachů a jaké jsou jejich příčiny. Odpovědi dotázaných nám ukazují, že k výskytu falešných poplachů u nich dochází jen v 5 % míře. Dle mého názoru je toto číslo spíše výjimkou a obvykle se objevuje v mnohem větší míře. Falešné poplachy jsou způsobeny vlivem prostředí a lidským faktorem.

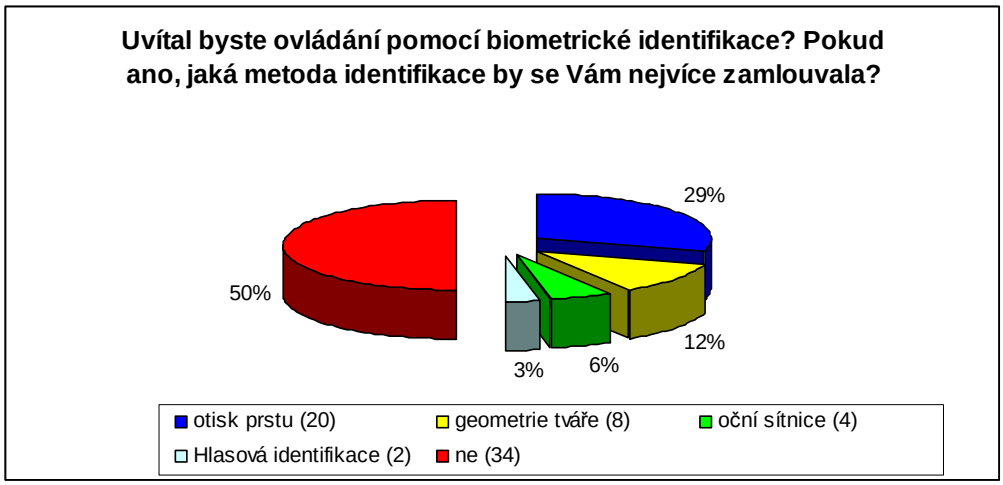


Graf 11: Četnost falešných poplachů

Otázka č. 14: *Uvítal byste ovládání pomocí biometrické identifikace? Pokud ano, jaká metoda identifikace by se Vám nejvíce zamlouvala?*

Otázku jsem směřoval na užití biometrické identifikace při ovládání poplachových zabezpečovacích systémů. Považuji totiž tuto variantu za jednu z možností, kterými se budou PZTS v blízké době ovládat. Součástí otázky bylo také určení metody identifikace.

Přesně polovina dotázaných by biometrickou identifikaci nepoužívalo. Mezi nejčastější metody se však řadí biometrie pomocí otisku prstu, kterou by uvítalo 29 % respondentů. Tyto metody sebou ale nesou i nedostatky, které jsou uvedeny v následujícím bodě.



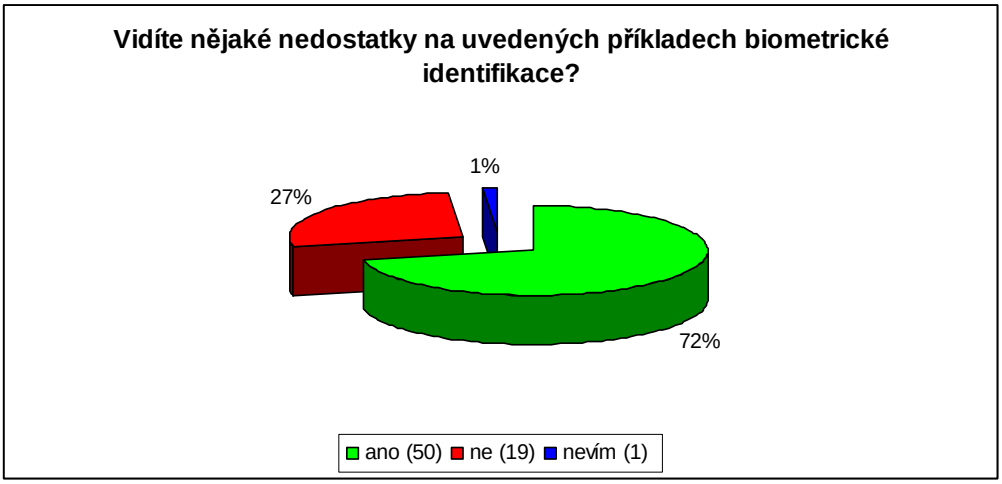
Graf 12: Ovládání pomocí biometrické identifikace

Otázka č. 15: *Vidíte nějaké nedostatky na uvedených příkladech biometrické identifikace?*

Otázka je zaměřena na zjištění nedostatků při používání biometrických metod. V dotazníku uvedlo 72 % respondentů, že shledává v těchto metodách určité nedostatky.

Mezi nejvíce zmiňované nevýhody patří:

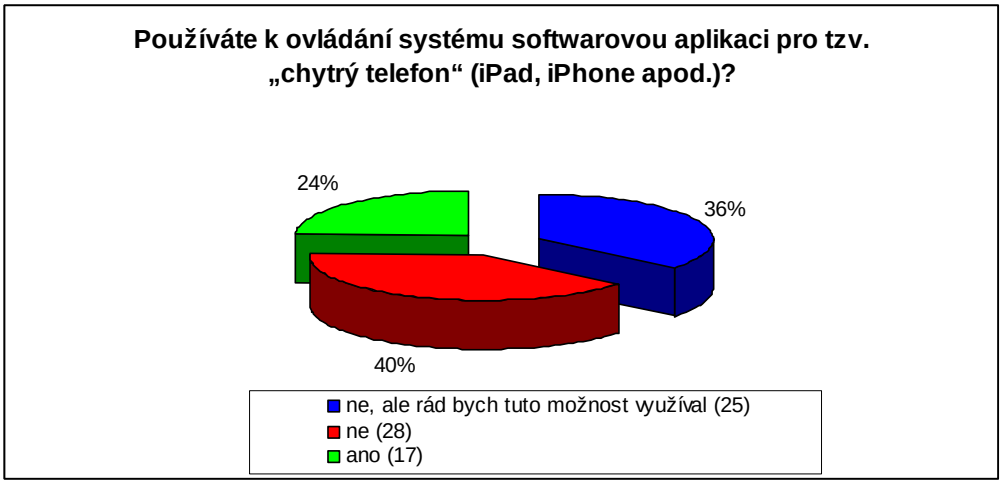
- vysoká pořizovací cena,
- náchylnost na prostředí,
- nefunkčnost při úrazech,
- nedostatečná odolnost proti zfalšování.



Graf 13: Nevýhody biometrické identifikace

Otázka č. 16: *Používáte k ovládání systému softwarovou aplikaci pro tzv. „chytrý telefon“ (iPad, iPhone apod.)?*

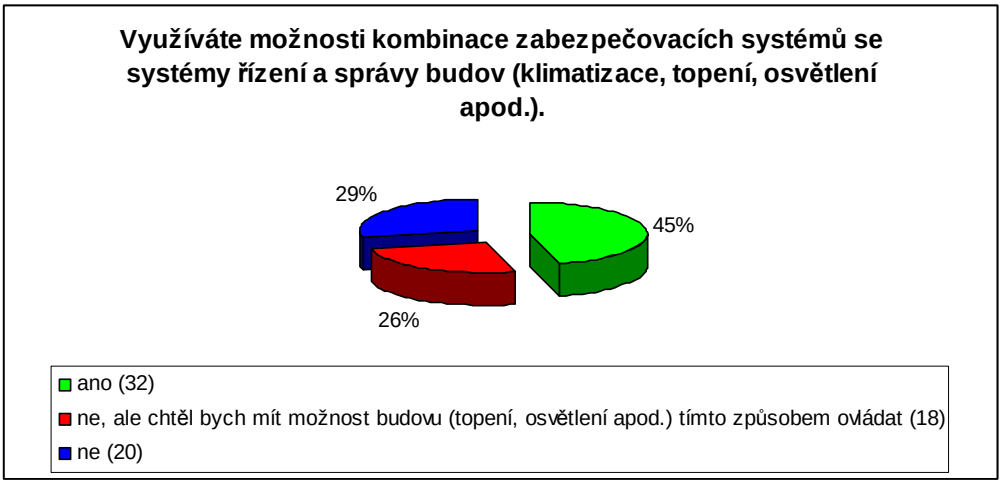
Cílem otázky bylo zjistit, jestli jsou uživatelé seznámeni s touto možností ovládání a v jaké míře ji používají. Průzkum nám ukázal, že 24 % dotázaných tuto aplikaci využívá a dalších 36 % by ji do budoucna použilo.



Graf 14: Ovládání pomocí smartphonu

Otázka č. 17: *Využíváte možnosti kombinace zabezpečovacích systémů se systémy řízení a správy budov (klimatizace, topení, osvětlení apod.).*

Otázka slouží k zjištění, zda uživatelé používají integraci poplachových zabezpečovacích systémů se systémy pro řízení a správu budov. Výsledkem je, že 45 % tuto kombinaci aktivně využívá a dalších 26 % by chtělo mít takovou možnost.



Graf 15: Integrace PZTS se systémy řízení a správy budov

Otázka č. 18: *Seřaďte následující hlediska dle toho, za jak důležitá je považujete (1 = nejdůležitější).*

Otázka byla vytvořena tak, aby při vyplnění ukázala čemu dávají uživatelé při pořizování PZTS přednost. Pořadí podle odpovědí respondentů: (od nejdůležitějšího)

- Kvalita
- Bezporuchový provoz
- Cena
- Intuitivní a jednoduchá obsluha
- Prostředí v českém jazyce

Zde můžeme vidět, že uživatelé kladou největší důraz na kvalitu a bezporuchový provoz. Nejméně důležitou roli hraje prostředí v českém jazyce, což se mně jeví vzhledem k pohodlnosti ovládání jako docela důležitý faktor.

Otázka č. 19: *Jakým směrem se podle Vás budou současné zabezpečovací systémy ubírat?*

Poslední otázka směřovala k myšlence, jak budou zabezpečovací systémy vypadat do budoucna. Zde jsem se setkal se širokou škálou názorů. Mezi nejčastěji formulovanými odpověďmi se objevuje stále větší integrace a automatizace s ostatními systémy. Z toho vyplývá vznik inteligentních instalací (budov). Přechod z LCD klávesnic na dotykové a dosazení biometrických čteček. Používání inteligentních kamer a hlasové identifikace.

4.2.1 Zhodnocení dotazníku

Na začátku dotazníku jsme se dozvěděli, že většina dotázaných používá poplachové zabezpečovací systémy každý den a pracuje s nimi více jak 5 let. Tento ukazatel by měl pomoci ke kvalitě získaných informací. Co se týká velikosti zabezpečených ploch dotázaných, jde spíše o malé aplikace s 1 až 4 zónami. Jak je vidět, současné PZTS se ještě stále nejvíce ovládají zadáváním uživatelského kódu na klávesnici. To však sebou nese i celou řadu problémů. Ať už jsou to 4 místné kódy a jejich bezpečnost nebo časový přes při zadávání a s tím spojená gramotnost obsluhy.

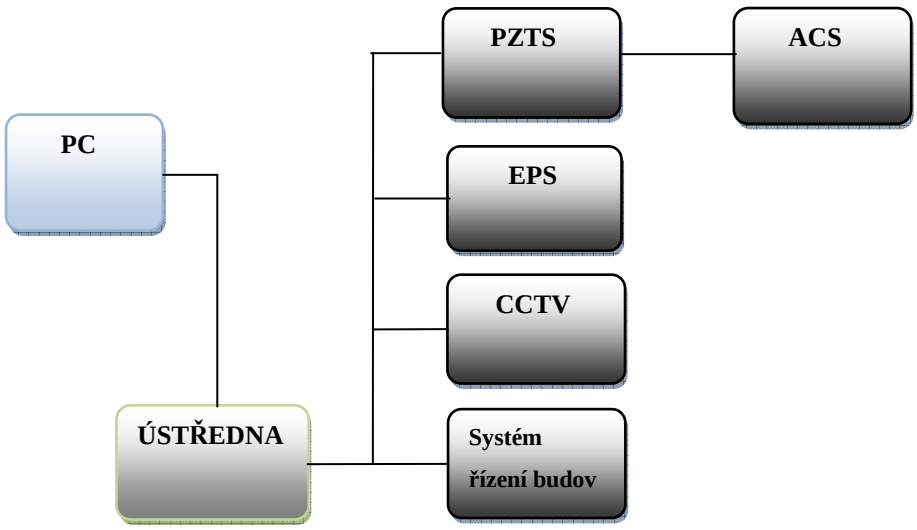
Použitím více místného uživatelského kódu sice můžeme předejít jeho případnému odhalení, ale opět tím zvyšujeme nároky na obsluhu. Proto si myslím, že by bylo vhodné více aplikovat ovládání pomocí karetní čtečky. K vyššímu stupni zabezpečení tedy můžeme přispět použitím kombinace PIN kódu a bezkontaktní karty.

Druhá část dotazníku je věnována možnému komfortu při ovládání současných poplachových zabezpečovacích systémů. Jednou z možností ovládání je přechod na biometrickou identifikaci. U této varianty se však názory dotázaných liší. Část respondentů by tuto možnost uvítala, druhá spíše ne a to zejména kvůli poukazování na její ne úplně 100% funkčnost. Mezi častým argumentem se objevuje i vysoká pořizovací cena. Biometrická identifikace se mně jeví jako nejvyšší možná úroveň zabezpečení, takže bych i přes vyšší náklady na její pořízení doporučoval tuto metodu ovládání. Mezi nejdostupnější a nejlevnější patří otisk prstu, ale nejpřesnější výsledky poskytuje skenování sítnice či snímání duhovky.

Další metodou je ovládání přes softwaru aplikaci v „chytrém telefonu“. Pomocí této aplikace můžeme systém ovládat bez nutnosti být přímo v objektu. Aplikace slouží k vypnutí/zapnutí systému, sledování stavu zón, zobrazení poplachů a poruch nebo ovládání PGM výstupů. Tuto možnost dnes již 60 % dotázaných využívá nebo by ji uvítalo. Pro její lepší účinnost zabezpečení bych uvítal větší návaznost s dohledovým a přijímacím poplachovým centrem.

Respondenti také uvedli, že poměrně často používají kombinaci zabezpečovacího systému se systémem řízení a správy budov. Zde se jedná o správný směr integrace více systémů a usnadňuje tak uživateli ovládání některých domácích zařízení. Hlavní výhodou této integrace je úspora energie. Jako nevýhodu můžeme uvést složitou instalaci do již postavených objektů. Důležité však zůstává, aby tato integrace neprobíhala na úkor bezpečnostních funkcí systému. Je taky nutné připomenout, že systém řízení a správy budov spadá mezi nepoplachové aplikace.

Vývoj současných poplachových zabezpečovacích systémů tedy směřuje k úplné automatizaci. To znamená vznik velkého modulárního systému, který kromě PZTS komponentů obsahuje speciální moduly pro ovládání ACS, EPS, CCTV a systému řízení a správy budov.



Obr. 26: Schéma zapojení modulárního systému

5 NÁVRHNUTÍ OBECNÉ STRUKTURY UŽIVATELSKY KOMFORTNÍHO SYSTÉMU

Úkolem diplomové práce je navrhnout obecnou strukturu ovládání poplachových zabezpečovacích systémů. V následujících bodech jsou tedy popsány možné prostředky, které mohou uživatelům pomoci k jednoduššímu a pohodlnějšímu ovládání.

5.1 Biometrická identifikace

Jelikož při ovládání současných systémů PZTS dochází u uživatelů k zapomenutí hesla nebo ztracení či odcizení karty, jsou tyto prostředky identifikace označovány za nedostatečné a nepraktické. Z těchto důvodů je na snaze přejít na biometrickou identifikaci. Ta získává údaje o určitých jedinečných fyziologických znacích lidského těla. To znamená, že každý uživatel má svůj vlastní identifikační znak stále při sobě (oči, ruce apod.).

V souvislosti s ovládáním poplachových zabezpečovacích systémů by se dalo hovořit o identifikaci pomocí otisku prstu, geometrie tváře nebo sítnicové biometrie. Uživatel by byl tedy schopen zapnout nebo vypnout zabezpečovací systém potvrzením jeho nadefinované identity (např. přiložením prstu na čtečku otisků).

a) otisk prstu - tato metoda se zdá jako finančně nejdostupnější. Její použití je možné kombinovat jak s klávesnicí, tak čtečkou karet. Bohužel i tento způsob identifikace má svoje nedostatky. Čtečky jsou náchylné na prostředí, tudíž tato forma není vhodná pro použití v továrnách. S tím souvisí i nefunkčnost při úrazech. Za nevýhodu můžeme považovat i možnost vymodelování repliky prstu, ale ta je vzhledem k pokroku snímacích zařízeních možná jen se speciální technikou.

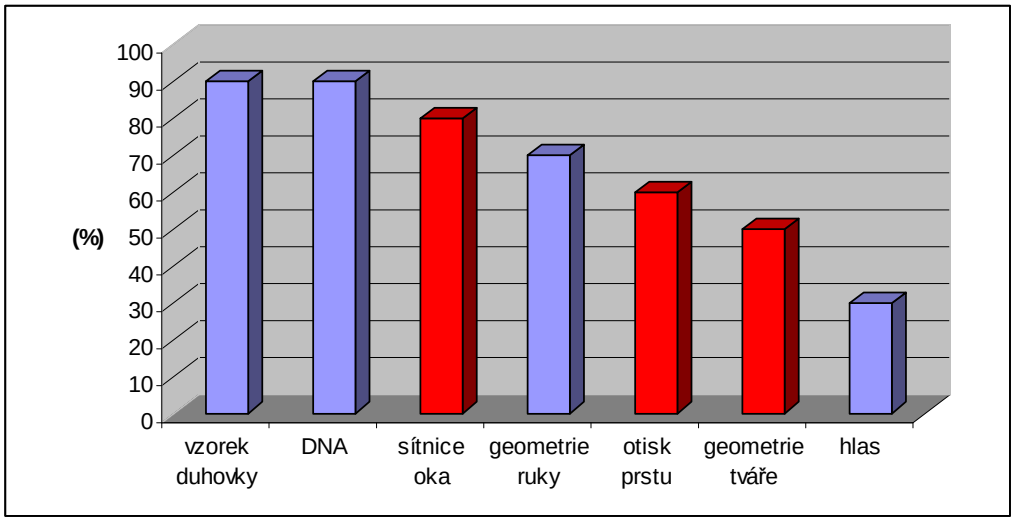
Zadávání otisků do systému probíhá přes sběrnici RS 485, kde je možné pomocí softwaru v PC provádět administraci, mazání a výměnu otisků. Systém je považován za efektivní při správě asi 200 osob. Pro lepší funkčnost je lepší zadat aspoň jeden prst z každé ruky (pro případ zranění).

b) geometrie tváře a sítnicová biometrie - u těchto metod identifikace již hraje finanční stránka poměrně velkou roli. U geometrie tváře je výhodou, že při ověřovaní nemusí uživatel prakticky vůbec nic dělat. Snímaní tváře probíhá pomocí IR kamery zabudované ve čtečce. Díky IR záření je možné identifikovat člověka i v naprosté tmě.

I tak, ale může být některým lidem snímání nebo skenování nepříjemné. U rozpoznání oční sítnice nastávají problémy při očních nemocích (např. šedý zákal).

Identifikace uživatele může probíhat ve dvou variantách. První z nich je tzv. 1:N, kdy uživatel předstoupí před vyhodnocovací jednotku a ta prohledá svou databázi zda se tam daný obličej nachází. Druhým způsobem je verifikace 1:1, kde uživatel zadá kód nebo přiloží kartu a vyhodnocovací jednotka na základě toho porovná šablonu uloženou pod tímto identifikačním číslem.

Důležitou roli hraje i stálost uložených vzorků v databázi. Vlivem stárnutí, opotřebení tkáně nebo úrazu se mohou biometrické vlastnosti člověka měnit. V následujícím grafu jsou uvedeny zmiňované biometrické metody a jejich stálost v závislosti na čase.



Graf 16: Stálost biometrické vlastnosti v závislosti na čase[20]

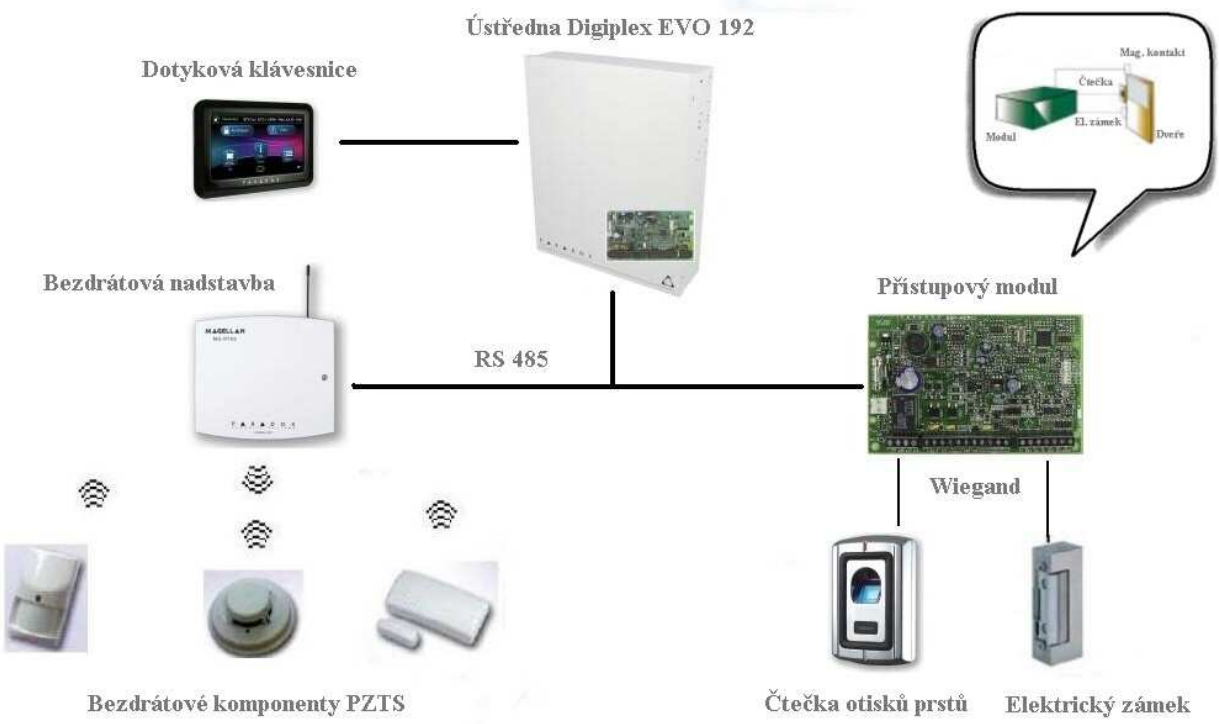
I přes uvedené nedostatky je podle mě biometrická identifikace jednou z možných variant, kterou se bude ovládání zabezpečovacích systémů ubírat. Rozhodujícím faktorem zde však bude finanční náročnost na pořízení těchto systémů.

V současné době se začíná rozšiřovat i behaviometrika, která sleduje vlastnosti a chování typické pro určité úkony člověka (dynamika chůze, pohyb a tvar rtů apod.). Problémem je, že se tyto vlastnosti mění v závislosti na čase a nejsou po dobu života člověka stálé. V oblasti PZTS se zatím tato charakteristika neimplementuje vzhledem k neúplné míře shody.

S aplikací této metody se v blízké době můžeme setkat na zastávkách metra. Systém zde má za úkol odhalit lidi chystající se k sebevraždě. Vychází se z toho, že jejich chování odpovídá určitému typu charakteru.

5.1.1 Návrh ovládání PZTS pomocí čtečky otisků prstů

K návrhu ovládání PZTS tímto způsobem jsem se rozhodnul na základě informací získaných z dotazníku. Uživatelským průzkumem zde bylo zjištěno, že téměř 30% dotázaných by uvítalo tento způsob ovládání poplachových zabezpečovacích systémů. Tato metoda mně přijde jednoduchá a spolehlivá. Na uživatele nejsou kladeny žádné nároky, takže si nemusí pamatovat žádné hesla ani mít u sebe kartu. K identifikaci uživatele slouží pouze otisk jeho prstů.



Obr. 27: Obecná struktura zapojení PZS

Použité komponenty v návrhu obecné struktury ovládání systému:

Pro funkční realizaci je nutné zvolit ústřednu, která umožní připojit nadstavbu pro systémy kontroly vstupu. V mém případě jsem zvolil ústřednu *Digiplex EVO192*, která lze rozdělit na 8 podsystémů a 192 zón. Ústředna je s řídícím PC propojena sériovým rozhraním RS 232 nebo sítí LAN (internet). Uživatelská správa systému je prováděna softwarem NEWARE ACCESS, který umožňuje spravovat, programovat části PZS, zadávat a mazat uživatele nebo sledovat události konkrétních uživatelů nebo dveří.

Systém je dále rozšířen o přístupové moduly, ke kterým jsou připojeny čtečky otisků prstů. Použité komponenty jsou vybrány z nabídky distribuční firmy VARIANT plus, spol. s r.o..

Komunikace mezi ústřednou a přístupovými moduly probíhá pomocí rozhraní RS 485. Mezi čtečkou a modulem je spojení zaručeno protokolem Wiegand.

V návrhu systému není zahrnut popis bezdrátové nadstavby systému RTX3 – 433 a bezdrátových detektorů. Jejich četnost použití je závislá na struktuře objektu a požadavcích zákazníka. Pro komunikaci s ústřednou přes LAN (internet) je potřeba použít modul IP 100.

Přístupový modul ACM12

Slouží k vytvoření bodu, který se chová jako systém kontroly a vstupu. Pomocí této nadstavby můžeme do systému přidávat čtečky, které se následně používají k vypnutí a zapnutí zabezpečovacího systému. Zároveň mají kontrolu nad pohybem osob ve střeženém objektu.

Obr. 28: Přístupový modul ACM12[13]

K funkčnosti systému je ještě potřeba osadit dveře elektromechanickým zámkem. Pro případ výpadku sítě je nutné připojit záložní zdroj. Modulem se můžou ovládat pouze jedny dveře a do celého systému jich můžeme připojit až 32.

Tab. 8: Technické parametry modulu

Vstup pro čtečku:	Ano,1
Rozhraní:	Wiegand
Napájení:	16 V~, 40 VA (jeden transformátor pro více modulů)
Proudový odběr:	max.80 mA
Záložní akumulátor:	12 V, 7 Ah/18 Ah
Počet vstupů:	2, magnetický kontakt, detektor
Pracovní teplota:	0 °C až +50 °C
Rozměry:	š 140 x v 90 x h 30 mm

Čtečka otisků prstů a karet F007-EM

K autentizaci uživatele jsem použil čtečku otisků prstů a karet od firmy Sebury, která je plně kompatibilní s navrženým systémem. Čtečka může pracovat v autonomním i systémovém režimu. V našem případě použijeme systémový, kde se propojí pomocí rozhraní Wiegand 26bit s nadřazenou řídící jednotkou. Součástí terminálu je i integrovaná čtečka EM karet (pracující na frekvenci 125 kHz).

Obr. 29: Čtečka F007-EM[13]

Kapacita paměti je určena pro 160 otisků a 2000 uživatelských karet. Programování čtečky se provádí pomocí IR klávesnice.

Jedná se o kontaktní čtečku otisku prstů, takže je nutné přikládat prst rovnoběžně se čtecí plochou. Není doporučeno čtečku používat v provozech a prostředích, kde se předpokládá špinavé okolí. Zhoršení čtení je možné zaznamenat, i pokud je čtečka osvícena přímým silným zdrojem světla. Tento případ může v praxi nastat, pokud je čtečka umístěna venku a je na přímém slunečním svitu.

Jedno načtení prstu slouží k vypnutí systému PZS, pro zapnutí musí dojít ke dvěma načtením během asi 10 sekund. K identifikaci nelze použít kombinaci bezkontaktní karta + otisk prstu. Ovládání je možné pouze jednou z těchto metod.

Tab. 9: Technické parametry čtečky

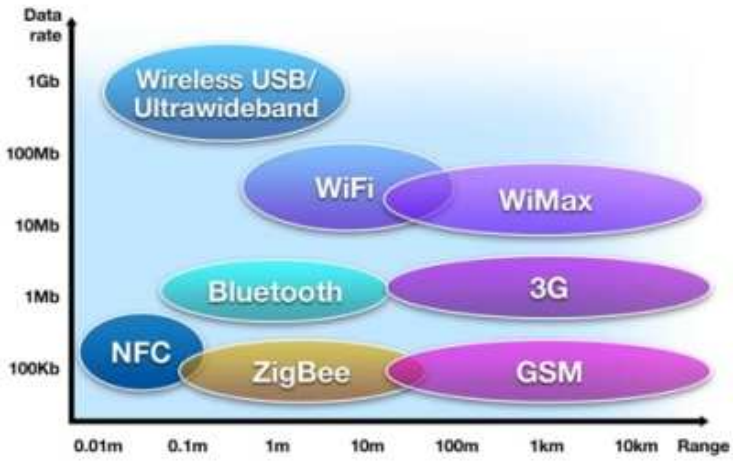
Kompatibilita:	otisk, nebo karta/přívěšek standard EM 125 kHz
Master oprávnění:	ano, 2 master otisky a karty
Rozlišení snímání:	450 dpi
Čas identifikace:	méně než 2 sec
Napájení:	10,5 - 13,5 Vss
Pracovní teplota:	-20 °C až +60 °C
Proudový odběr:	max. 110 mA
Rozměry:	š 70 x v 115 x h 35 mm

5.2 Předpokládaný vývoj ovládání PZTS

5.2.1 Bezdrátová komunikace NFC

Technologie NFC (Near Field Communication) je určena k intuitivní a jednoduché bezdrátové komunikaci mezi elektronickými zařízeními. Tuto funkci můžeme označit jako pokročilý stupeň RFID technologie. Umožňuje komunikaci na velmi krátké vzdálenosti (do 20 cm) pouhým přiblížením nebo přiložením.

Jedná se vlastně o NFC čip, který je zabudovaný přímo v mobilním telefonu. Komunikace probíhá pomocí rádiových vln o frekvenci 13,56 MHz. Maximální přenosová rychlost může být až 848 kbit/s. [19]



Obr. 30: Bezdrátové technologie[19]

V poplachových zabezpečovacích systémech může tato technologie nahradit používání klasických bezkontaktních karet. Tím pádem by uživatel mohl zapnout a vypnout zabezpečovací systém pouhým přiložením mobilního telefonu ke čtečce.

Odpadla by tedy nutnost mít u sebe kartu pomocí níž ovládáme systém nyní. Čtečky jsou k systému připojeny standardně po datové sběrnici pomocí rozhraní RS 485.

NFC čip je provázán se SIM kartou, takže v případě ztráty mobilního telefonu je možné kartu ihned zablokovat. Tato technologie je považována za poměrně bezpečnou díky malé aplikační vzdálenosti při komunikaci se čtečkou (optimálně 4 cm). I přesto ji lze pomocí rádiových zařízení odposlouchávat, proto je lepší použít šifrování. Nevýhodou je, že při vybití akumulátoru telefonu přijdeme o přístup do střeženého objektu.

Komunikace NFC se dělí na dva typy a zahrnuje iniciátor a cíl:

- **Aktivní -** „Peer to Peer“, vzájemně komunikují obě zařízení (vytváří RF pole).
- **Pasivní -** iniciátorem je aktivní přístroj, který sám generuje rádiové vysílání, cíl pak pošle jen svou odpověď(nevytváří RF pole)

Obr. 31: Obslužná aplikace telefonu s NFC čipem

Technologie NFC je teprve na začátku svého rozvoje, ale do budoucna to může být jedna z možností ovládání, která nahradí současné bezkontaktní karty.

5.2.2 Inteligentní systém rozpoznání obličeje

Prozatím jsem uvedl pouze doplňkové funkce a metody pro větší uživatelský komfort. Vývoj budoucích poplachových zabezpečovacích systémů je však zaměřen na inteligentní systém rozpoznání obličeje.

Jde vlastně o inteligentní kamerový systém, který s pomocí softwarové nadstavby umožní identifikovat osoby, které mají do daného objektu přístup. Tento systém může být ještě doplněn o hlasovou verifikaci. Předpokladem je, že celý systém bude ovládán počítačem, který se bude starat o zabezpečení objektu.

V praxi by to mělo vypadat tedy tak, že uživatel přijde ke dveřím domu a na základě rozpoznání obličeje bude do objektu vpuštěn. V případě neshod bude vyzván k hlasovému pokynu, který bude porovnám s uloženým hlasovým otiskem.

Jedná se o vysokou úroveň zabezpečení, kde nejsou kladeny přehnané nároky na gramotnost uživatelů.

6 ZHODNOCENÍ NÁVRHU SYSTÉMU PZTS

Pro zhodnocení návrhu jsem vybral biometrickou identifikaci metodou otisku prstu. Je to hlavně proto, že v současné době je z výše uvedených možností ovládání poplachových zabezpečovacích systémů nejekonomičtější a nejdostupnější. Samozřejmě cenový rozptyl těchto čteček je velký, tak jsem použil aplikaci čtečky s nižší nákupní cenou.

Finanční kalkulace je provedena na modelu firmy s přibližně 50 zaměstnanci. V podniku je již zavedený poplachový zabezpečovací systém, který se ovládá uživatelským kódem v kombinaci s bezkontaktní kartou. Uvažujme, že firma používá 10 terminálů se čtečkou karet. Jelikož jsou čtečky připojeny na stejnou sběrnici cena dalších komponentů nebude brána v potaz. Cena bezkontaktní karty Paradox je 70 Kč bez DPH. Pokud tedy uvažujeme, že každý uživatel dostane svou kartu, tak je pořizovací cena 3500 Kč bez DPH.

Tab. 10: Srovnání cen jednotlivých ovládacích terminálů

	Cena za ks	**Karta/přívěšek**	**Celková cena**
Čtečka karet EM+HID (SEBURY R1-EM+HID)	1 149,-	3500,-	14 990,-
Čtečka karet + klávesnice (SEBURY BC-2011)	1 990,-	3500,-	23 400,-
Snímač otisku prstu + čtečka karet (SEBURY F007-EM)	**2 790,-**	**3500,-**	**31 400,-**
Snímač otisku prstu + klávesnice (SEBURY BC-2018)	3 380,-	-	33 800,-

V tabulce můžeme vidět, že oproti původními návrhu vzrostla cena zhruba o 16 tisíc korun. V ceně jsou ale započteny i náklady na nákup případných bezkontaktních karet, které nejsou nutností. Celkově se mi jeví biometrická metoda otisku prstu jako bezpečnější a pohodlnější. Nemůže dojít ke zneužití jako při odcizení karty nebo uživatelského kódu. I samotnému uživateli odpadne nutnost nosit sebou kartu nebo čip a to přidává na komfortu ovládání PZTS.

Pokud budeme návrh srovnávat s konvenčním řešením ovládání systémů, které je prováděno pomocí zadání uživatelského kódu jsou už náklady na pořízení poměrně vyšší. Nejde totiž o integraci poplachového zabezpečovacího systému se systémem kontroly a vstupu a musí se tedy započíst i náklady na pořízení přístupových modulů. Jeden takový modul přitom stojí 2 599 Kč bez DPH. To znamená, že k modelovému návrhu 10 terminálů by jsme museli ještě připočíst částku 25 990 Kč na nákup nadstavby access. Jak již bylo uvedeno jedním modulem jdou ovládat pouze jedny dveře. Existují ale i řídící jednotky, které umožní připojit až 8 dveří na jeden modul.

Zhodnocení ovládání pomocí otisků prstů oproti současným metodám:

Výhody:

- Otisk prstu nemůžeme zapomenout doma nebo zabouchnout do dveří
- Otisk prstu nelze nikomu zapůjčit
- Snadné použití bez velkých nároků na obsluhu
- Složitost při výrobě falzifikátů

Nevýhody:

- Nefunkčnost v nečistém prostředí
- Výskyt chybných přijetí a odmítnutí (FAR a FRR)
- Nutnost fyzické přítomnosti uživatele při nahrávání otisků do systému
- Nefunkčnost při úrazech

ZÁVĚR

Diplomová práce je zaměřena na poplachové zabezpečovací a tísňové systémy. Obsah této oblasti je však poměrně velký, tak je hlavní důraz kladen na ovládání těchto systémů.

V teoretické části věnuji prostor popisu užívaných komponentů PZTS. S tím souvisí i výběr čtyř ústředen u kterých si ukazujeme současné ovládání poplachových zabezpečovacích systémů. Mezi nejčastější způsob zapínání nebo vypínaní systému patří uživatelský PIN kód. Dalšími používanými prostředky jsou bezkontaktní karty a přívěšky nebo dálkové ovladače. Pro lepší bezpečnost může být použita kombinace PIN kódu a karty.

Pro zjištění aktuální situace ovládání PZTS na českém trhu je použita dotazníková metoda. Dotazník je vytvořen formou otevřených a uzavřených otázek, tak aby došlo k co největšímu objasnění daného tématu. Výstupem práce je návrh obecné struktury jednoduchého a pohodlného ovládání systému. Ten spočívá v čím dál větší integraci stávajících systémů (PZTS, CCTV, EPS, ACS, systém řízení a správy budov) a vzniknutí tzv. inteligentního domu. S tím souvisí i možnost vzniku inteligentního systému rozpoznání obličeje spolu s hlasovou verifikací. To by znamenalo, že uživatel by nepotřeboval žádné hesla ani karty, ale systém by sám rozpoznal zda má do objektu povolený přístup. Ke komfortu ovládání může ale napomoci i použití biometrické identifikace. A to zejména metoda otisku prstu, která je z finančního hlediska nejekonomičtější.

Vzhledem k vývoji technologií mi přijde jako dobrý směr k ovládání těchto systémů i bezdrátová technologie NFC. Ta se sice teprve začíná rozvíjet, ale v budoucnu může nahradit současné bezkontaktní karty.

Uvedené informace by měly sloužit pro získání přehledu o ovládání současných poplachovým zabezpečovacích systémů a jejich možnému vývoji.

ZÁVĚR V ANGLIČTINĚ

The thesis is focused on intrusion and hold up alarm systems. The content of this field is quite large, so the main focus is to operate these systems.

In the theoretical part is devoted to the description of the space used PZTS components. This is related to the selection of four panels which show the simultaneous control of security alarm systems. The most common method of switching on or off the system include the user PIN. Other funds are used contactless cards and pendants or remote controls. For better security can be used in combination card and PIN code.

To determine the actual control of the situation on the Czech market PZTS is used questionnaire method. The questionnaire is developed through open and closed questions, so in order to maximize the explanation of the topic. The output of work is the general structure of a simple and convenient system control. This is a growing integration of existing systems (PZTS, CCTV, EPS, ACS, system management and administration buildings) and created has the intelligent house. This is related to the possibility of intelligent face recognition system with voice verification. This would mean that the user would not need any passwords or cards, but the system itself would recognize whether the object is allowed access. The comfort control can help but the use of biometric identification. A particular method of fingerprint, which is financially economical.

Given the evolution of technology, I find a good direction to control these systems and wireless technology NFC. It is true just starting to develop, but in the future may replace the current contactless cards.

This information should serve as an overview of the current control alarm security systems and their possible development.

SEZNAM POUŽITÉ LITERATURY

[1] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Blatná: Cricetus, 2003, 351 s. ISBN 80-902-9382-4.

[2] BASTIAN, Peter. *Praktická elektrotechnika*. Praha: Europa-Sobotáles, 2004, 295 s. ISBN 80-867-0607-9.

[3] UHLÁŘ, Jan. *Technická ochrana objektů: II. díl - EZS II*. Praha: PA-ČR, 2005, 229 s. ISBN 80-725-1189-0

[4] VLČEK, Jiří. *Bezpečnost elektrických zařízení*. Praha: BEN - technická literatura, 2007, 109 s. ISBN 978-80-7300-222-0

[5] KINDL Jiří. *Projektování bezpečnostních systémů: I. díl – EPS, EZS.* Zlín: UTB, 2004. ISBN 80-7318-165-7.

[6] ZEMAN, Petr. *Česká bezpečnostní terminologie*. Brno: Ústav strategických studií Vojenské akademie v Brně, 2002, 186 s. ISBN 80-210-3037-2.

[7] ČSN CLC/TS 50131. *Poplachové systémy*: *Poplachové zabezpečovací a tísňové systémy*. Praha: Český normalizační institut, 2007.

[8] EZS. *EMPIRE Alarms* [online]. 2007 [cit. 2012-03-10]. Dostupné z: http://www.empirealarms.sk/ezs.html

[9] Podniková norma. *Jablotron* [online]. 2011 [cit. 2012-03-10]. Dostupné z WWW: <http://www.jablotron.cz/upload/File/pnj131.pdf>.

[10] Předpisy související s poskytováním technických služeb k ochraně majetku a osob. *MVČR* [online]. 2010 [cit. 2012-03-20]. Dostupné z WWW: <http://www.mvcr.cz/docDetail.aspx?docid=21527415&doctype=ART&>.

[11] Začínáme s EZS. *Variant* [online]. 2005 [cit. 2012-03-20]. Dostupné z WWW: <http://www.variant.cz/dokumenty-ke-stazeni/>.

[12] Zabezpečení objektu. *Jablotron* [online]. 2012 [cit. 2012-03-25]. Dostupné z WWW: <http://zabezpeceni-objektu.jablotron.cz/cz/sekce/vyrobky/oasisnew/>.

[13] EZS. *Variant* [online]. 2012 [cit. 2012-03-30]. Dostupné z WWW: <http://www.variant.cz/kategorie/ezs/>.

[14] Zabezpečovací ústředna Concept. *Eurosat* [online]. 2012 [cit. 2012-04-10]. Dostupné z WWW: <http://www.eurosat.cz/106-concept-3000-acess-4000.html>.

[15] Touchscreen Terminal. *Inner Range* [online]. 2012 [cit. 2012-04-12]. Dostupné z WWW: <http://www.innerrange.com/products.php?id=17&cid=21&tid=43 >.

[16] Galaxy Dimension. *ADI Global* [online]. 2012 [cit. 2012-04-13]. Dostupné z WWW: <http://www.adiglobal.cz/iiWWW/docs.nsf/all/79C7F3AE4DC3781EC12575130036CF95/$FILE/08039706.pdf >.

[17] Uživatelský manuál ústředen Galaxy Dimension. *ADI Global* [online]. 2010 [cit. 2012-04-13]. Dostupné z WWW: < http://www.adiglobal.cz/iiWWW/docs.nsf/all/DA9B8AC796E15658C12575130036CF8B/$FILE/UM_Galaxy_Dimension_ver1.01.pdf >.

[18] Ústředny EZS. *UTC F&S* [online]. 2012 [cit. 2012-04-17]. Dostupné z WWW: < http://www.utcfssecurityproductspages.eu/CZ/products_cat3.php?cat_2=2&cat_3=1 >.

[19] NFC. *Notebook* [online]. 2011 [cit. 2012-04-27]. Dostupné z WWW: < http://notebook.cz/clanky/technologie/2011/nfc-bezdratova-komunikace-blizke-budoucnosti>.

[20] Biometrické metody identifikace osob. *VŠB TU Ostrava* [online]. 2008 [cit. 2012-05-2]. Dostupné z WWW: < http://www.fbi.vsb.cz/miranda2/export/sites-root/fbi/040/cs/sys/resource/PDF/biometricke_metody.pdf>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PZTS	Poplachové zabezpečovací a tísňové systémy
EZS	Elektrické zabezpečovací systémy
PPC	Poplachové přijímací centrum
I&HAS	Intrusion & Hold-up alarm systems
ČSN	Česká státní norma
PIR	Passive infra red sensor
MW	Microwave sensor
US	Ulrasonic sensor
GBS	Glass break
NC	Normally closed
NO	Normally opened
EOL	End of Line
LAN	Local Area Network
NFC	Near Field Communication

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK

Poplachové zabezpečovací systémy

Konec vyplňování **zítra v 16:00:00**, výsledky budou k dispozici pouze zadavateli.
Počet otázek: 19

Dobrý den,

jsem studentem Univerzity Tomáše Bati ve Zlíně a rád bych Vás požádal o vyplnění tohoto dotazníku. V rámci závěrečné diplomové práce na téma Poplachové zabezpečovací systémy a komfort jejich ovládání provádím uživatelský průzkum, který je zaměřen na způsob a náročnost ovládání těchto systémů.

Předem děkuji za Váš čas a spolupráci.

povinná otázka

1. Jak často používáte poplachový zabezpečovací systém, neboli systém EZS?

- ○ každý den
- ○ jednou za týden
- ○ několikrát do roka
- ○ vůbec

povinná otázka

2. Jakým způsobem provádíte zapnutí/vypnutí poplachového zabezpečovacího systému?

- ○ uživatelský kód (PIN)
- ○ karta / přívěšek
- ○ karta + PIN
- ○ dálkový ovladač
- ○ mobilní telefon (sms příkazy)
- ○ biometrická identifikace
- ○ jiné

nepovinná otázka

3. Jaký způsob tedy používáte pro zapnutí/vypnutí systému?

nepovinná otázka

4. Kolika místný uživatelský kód používáte?

- ○ 4 místný PIN
- ○ 6 místný PIN
- ○ Jiná odpověď:

nepovinná otázka

5. Myslíte si, že je Váš PIN kód dostatečně bezpečný?

- ○ ano
- ○ ne

povinná otázka

6. Měl jste někdy problémy se zapnutím/vypnutím (odstřežením/zastřežením) podsystému (oblasti)?

- ○ ano
- ○ ne

povinná otázka

7. Čím byly tyto problémy způsobeny?

- ○ zapomenutí PIN kódu
- ○ nefunkčnost karty / přívěšku
- ○ složitost obsluhy
- ○ časový pres při zadávání bezpečnostního kódu (špatně zadaný PIN)
- ○ Jiná odpověď:

povinná otázka

8. Připadá Vám ovládání zabezpečovacích systémů jednoduché a pohodlné?

- ○ ano
- ○ ne (můžete uvést důvod do pole jiná odpověď)
- ○ Jiná odpověď:

nepovinná otázka

9. Na kolik podsystémů je rozdělen Váš zabezpečovací systém?

- ○ 1 až 4
- ○ 5 až 8
- ○ 9 až 16
- ○ 17 až 31
- ○ více

nepovinná otázka

10. Zdá se Vám tento počet dostačující?

- ○ ano
- ○ ne (můžete uvést důvod do pole jiná odpověď)
- ○ Jiná odpověď:

nepovinná otázka

11. Napadá Vás nějaká myšlenka (funkce), která by vedla k lepšímu ovládání poplachových zabezpečovacích systému?

povinná otázka

12. Jak dlouho používáte poplachové zabezpečovací systémy?

- ○ do 1 roku
- ○ 1 až 5 let
- ○ 5 let a více

povinná otázka

13. Dochází u Vás k častému výskytu falešných poplachů?

- ○ ano (můžete uvést důvod do pole jiná odpověď)
- ○ ne
- ○ Jiná odpověď:

povinná otázka

14. Uvítal byste ovládání pomocí biometrické identifikace? Pokud ano, jaká metoda identifikace by se Vám nejvíce zamlouvala?

- ○ ne
- ○ ano – otisk prstu
- ○ ano – oční sítnice
- ○ ano – tvar tváře (geometrie)
- ○ Jiná odpověď:

povinná otázka

15. Vidíte nějaké nedostatky na uvedených příkladech biometrické identifikace?

- ○ ano (můžete uvést příklad do pole jiná odpověď)
- ○ ne
- ○ Jiná odpověď:

povinná otázka

16. Používáte k ovládání systému softwarovou aplikaci pro tzv. „chytré telefony“ (iPad, iPhone apod.)?

- ○ ano
- ○ ne, ale rád bych tuto možnost využíval
- ○ ne (můžete uvést důvod do pole jiná odpověď)
- ○ Jiná odpověď:

povinná otázka

17. Využíváte možnosti kombinace zabezpečovacích systémů se systémy řízení a správy budov (klimatizace, topení, osvětlení apod.)

- ○ ano
- ○ ne, ale chtěl bych mít možnost budovu (topení, osvětlení apod.) tímto způsobem ovládat
- ○ ne (můžete uvést důvod do pole jiná odpověď)
- ○ Jiná odpověď:

povinná otázka

18. Seřaďte následující hlediska dle toho, za jak důležitá je považujete (1 = nejdůležitější).

Zvolte prosím u každé odpovědi nějaké (jedinečné) pořadí:

	1.	2.	3.	4.	5.
Kvalita:	○	○	○	○	○
Cena:	○	○	○	○	○
Intuitivní a jednoduchá obsluha:	○	○	○	○	○
Bezporuchový provoz:	○	○	○	○	○
Prostředí v českém jazyce:	○	○	○	○	○

nepovinná otázka

19. Jakým směrem se podle Vás budou současné zabezpečovací systémy ubírat?