Česká zemědělská univerzita v Praze

Technická fakulta

Katedra technologických zařízení staveb

Analýza možností sabotáže elektrických zabezpečovacích systémů (EZS)

Bakalářská práce

Vedoucí bakalářské práce: Ing. Zdeněk Votruba

Vypracoval: Martin Janovský

Praha 2010

Vysoká škola:	Česká zemědělská univerzita v Praze	Fakulta:	technická
Katedra:	**technologických zařízení staveb**	Akademický rok:	2008/2009

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Student: **Janovský Martin**

Studijní obor: Informační a řídicí technika v APK

Název práce: Analýza možností sabotáže elektrických zabezpečovacích systémů (EZS)

Zásady pro vypracování:

Cíl práce: Provézt rozbor a bezpečnostní analýzu obvykle používaných detektorů systémů EZS (smyčkové a bezdrátové ústředny). Rozdělit obvykle používané detektory do skupin podle možného způsobu napadení a prakticky ověřit jejich odolnost. Na základě zjištěných dat doporučit přednostní využívání optimálních detektorů.

Osnova práce:

1. Rozbor smyčkových ústředen EZS
2. Detektory používané ve smyčkových ústřednách
3. Rozbor možného způsobu napadení výše uvedených typů detektorů, praktické ověření
4. Rozbor a ověření bezpečnosti bezdrátových přenosů detektor - ústředna
5. Další rizikové faktory provozu EZS
6. Praktické zkušenosti a doporučení, finanční zhodnocení navrhované koncepce

Metodika práce: Definujte obvykle používané detektory ve smyčkových a bezdrátových systémech EZS. Pro dané skupiny detektorů stanovte bezpečnostní rizika – způsoby napadení a pokuste se je ověřit a na základě zjištěných dat zobecnit. Ověřte odolnost stejného typu detektoru od různých výrobců. Stanovte jednoduchý bezpečnostní manuál pro instalaci vybraných detektorů.

Rozsah práce: 40 stran textu včetně obrázků, grafů a tabulek

Seznam doporučené odborné literatury:

Zdroje Internet

ZAHRÁDKA, J.: Začínáme s EZS. Variant plus s r.o. 2005, 36 s.

KŘEČEK, S.: Příručka zabezpečovací techniky. 2002, Critetus, 313 s. ISBN 80-902938-2-4.

UHLÁŘ, J.: Technická ochrana objektů - 1.díl. Skripta PA ČR Praha, Praha, 2001, 180 s. ISBN 80-7251-172-6

UHLÁŘ, J.: Technická ochrana objektů - 2.díl. Skripta PA ČR Praha, Praha, 2001, 230 s. ISBN 80-7251-189-0

KLUGL, J.:Montáž EZS. 1994, 215 s.

KOKTAN, P. a kol.: Mechanické zábranové systémy. 1998, 268 s.

BEBČÁK, P.: Požárně bezpečnostní zařízení, 2004, SPBI, 226 s. ISBN 80-86634-34-5.

HEŘMAN, J., TRINKEWITZ, Z., a kol.: Elektrotechnické a telekomunikační instalace, 2006, Verlag Dashofer, ISBN 80-86897-06-0

Vedoucí bakalářské práce: Ing. Zdeněk Votruba

Datum zadání bakalářské práce: 7. 12. 2008

Termín odevzdání bakalářské práce: 30. 4. 2010

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE TECHNICKÁ FAKULTA

doc. Ing.Miroslav Přikryl, CSc.
vedoucí katedry

prof. Ing. Jiří Klíma, CSc.
děkan

V Praze dne 10.12.2008

Čestné prohlášení:

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a že jsem uvedl všechny literární zdroje a prameny, ze kterých jsem čerpal.

V Praze dne 23. dubna 2010 …….

Martin Janovský

Poděkování:

Chtěl bych poděkovat vedoucímu své bakalářské práce Ing. Zdeňku Votrubovi za jeho cenné rady a připomínky při psaní této práce.

Abstrakt:

Moje práce se zabývá možnostmi ochrany jednotlivých prvků elektronických zabezpečovacích systémů, kde analyzuji jejich silné a slabé stránky. Pod tím si můžeme představit rozdělení do základních bezpečnostních tříd a také rozdělení podle metod použití jako jsou ústředny, prvky obvodové ochrany, pohybové ochrany, předmětové ochrany a pult centralizované ochrany. Podle tohoto rozdělení popisuji v jednotlivých kapitolách hlavní používané typy a nastiňuji jejich konstrukci a zásady instalace. V poslední části se zabývám srovnáním dvou realizovaných koncepcí EZS, kde první je realizována bezdrátovým připojením a druhá po metalickém vedení. V závěru práce navrhuji použití jednotlivých zabezpečovacích tříd podle charakteru budovy.

Klíčová slova: ústředny EZS, detektory EZS, pult centralizované ochrany

Analysis of the possibilities of sabotage of electrical security systems (ESS)

Sumary:

My work deals with the possibilities of protection of individual elements of electronic security systems, where they analyze their strengths and weaknesses. Beneath that you can imagine the division into basic safety classes and distribution according to the methods used as switches, circuit protection components, physical protection, protection of the subject and the central security panel. According to this division in the various chapters describe the main types used and outline the design and installation principles. The last part is to compare two concepts implemented intrusion detection, where the first wireless is realized, and the second after the metallic lines. In conclusion, I propose the use of various security classes depending on the nature of the building.

Key words: intrusion control, alarm detector, centralized protection

Obsah

Úvod

Každý z nás si přeje žít v prostředí, kde se bude cítit bezpečně a bude si moci užívat svého majetku bez nebezpečí, že bude poškozen anebo odcizen. Toto ohrožení přináší každému z nás pocit nejistoty a strachu. Z toho důvodu se od nepaměti snažili lidé před tímto nebezpečím chránit.

Potřeba chránit sebe je úzce spjata s potřebou informovat o nebezpečí. To platí již od doby, kdy první lidé vyšli z jeskyně a byli nuceni signalizovat ohrožení divou zvěří a později od sousedních kmenů. Signalizace se postupně vyvíjela, přes zapálené ohně používané domorodci a umění praporků používané Římany. V dnešní době používáme ke sdělení informace datový přenos, který je realizován pomocí bezdrátového nebo metalického kabelu. Oba tyto principy se také využívá při přenosu dat v elektronických zabezpečovacích systémech.

Tato práce by měla čtenáři poskytnout základní popis a orientaci v prvcích elektronických zabezpečovacích systému. V první části práce si rozebereme základní prvky a pojmy. Obecně tak získáme přehled o dělení prvků do základních zabezpečovacích tříd a jejich obecných funkcí a použití v praxi. Seznámíme se také s použitím pultu centralizované ochrany, a typech připojení k němu. V druhé části se zaměřím na rozbor funkce a činnosti jednotlivých typů detektorů a ústředen včetně jejich rozdělení podle vhodného použití k ochraně objektů. Pokusím se nastínit vhodnost použití a základní pravidla pro instalaci systémů a jednotlivých prvků EZS. Na závěr se pokusím sepsat slabiny jednotlivých komponent EZS a obecná pravidla pro používání zabezpečovacího systému tak, aby se zabránilo jeho nesprávné činnosti, případné sabotáži. Celkové schopnosti obrany proti základním typům narušení se pak pokusím definovat v koncové tabulce a uvést zde základní přehled o výhodách a nevýhodách těchto systémů.

V poslední kapitole se pokusím nastínit použití zabezpečovacích systému na dvou velmi podobných domech s různým přístupem v realizaci zabezpečovací techniky a demonstrovat zde realizované chyby a možnosti jejich nápravy.

1 Základní pojmy a definice

1.1 Rozbor situace

Majetek, peníze a nápady. Ať se podíváme kamkoliv jsou všude kolem nás. Každá z těchto věcí má svého majitele. Některá patří osobě, jiná zase skupině, ať tak či onak jsou soukromým vlastnictvím a jsou potencionálně ohroženy ať již náhodnými zlodějíčky či profesionálními zloději na zakázku. [1]

Majetek lze poškodit, odcizit či zneužít. Každá taková činnost způsobuje svému majiteli škodu. To je hlavní důvod proč je nutno majetek chránit. Pokud bychom brali ochranu svého majetku na lehkou váhu, musíme počítat nevyhnutelně se škodami. Majetek je nutno chránit uvážlivě, rozhodně, důsledně a s ohledem na legislativu. [1,4]

Ochrana majetku je pradávným problémem. Původně se tento problém řešil tvrdými tresty pro zločince a petlicemi na dveřích. První klíče a zámky jsou běžně známy z 9. a 10. století. Jednalo se o jednoduchá zařízení z bronzu. [1,4]

Vývoj a ochrana majetku je přímo závislý na vývoji lidské společnosti. Byli doby kdy zamykání bytů a domů příliš nikoho nezajímalo. Tato forma ochrany byla spíše symbolická a používalo se zde několik velmi jednoduchých zařízení, která objekt nijak výrazně neochránila. Tento stav byl dán především velmi nízkým počtem vloupání a krádeží. Tato doba je však již nenávratně pryč a trend, zejména z posledních let nám ukazuje jasné směřování k stále dokonalejším zabezpečovacím systémům mechanickým a elektronickým. I když se stát i místní samosprávy snaží těmto deliktům předcházet nasazováním policistů a kamer do ulic, tak se i přes tato opatření nedaří pachatele usvědčovat, neboť demokracie nechrání jen dobré občany, ale také i zločince. §226 trestního řádu říká, stíhat a trestat lze jen tehdy, má-li žalobce dostatek nezpochybnitelných důkazů. Pokud ne, pak je používána zásada in dubio pre reo (v pochybnosti je třeba rozhodnout ve prospěch obžalovaného). Je tedy na každém z nás, ať si to uvědomujeme nebo ne, ochránit svůj majetek a zdraví v našich domovech nebo firmách. Nelze se spoléhat na nikoho, že to udělá za nás. [1,3,4]

1.1.1 Krádeže a pachatelé

Celková kriminalita se v posledních letech zvyšuje. To je vidět zejména v období let 1990 až 1994, kdy počet vloupání kulminoval. Do roku 2001 se čísla držela ve stejných

hodnotách, ale poslední roky nám ukazují nový trend odrážející se v nárůstu trestných činů. Viz (tab. 1)

	1990	1991	1992	1993	1994	2001	2002	2003	2004	2005
Celková Kriminalita	216852	282998	345205	398505	372427	375630	394267	403654	425930	426626
Majetková Kriminalita	166638	231372	287059	327183	300352	289002	301727	304039	314249	306351
Krádeže vloupáním	72885	106943	115779	124365	111914	100098	98472	94603	92029	85631
Z toho Bytů	15238	17432	16818	17632	14804	13936	13538	13068	12752	12445
Krádeže automobilů	11658	10849	20829	25522	25615	25059	27517	29422	27889	27092

Tab. 1 Celková kriminalita na území ČR [1,3]

Další statistika v (tab. 2a) uvádí nejčastější způsoby průniků do bytů a (tab. 2b) průniků do rodinných domků.

Slabá místa v činžovních domech	2009	1992
Okna	19,73%	16,6%
Balkónové Dveře	25,66%	19,8%
Vchodové Dveře	54,65%	63,6%

Tab. 2a Nejčastější narušení (byty) [3]

Slabá místa v rodinných domech	2009	1992
Okna	26,49%	31,3%
Balkónové dveře	52,05%	48,8%
Domovní dveře	13,88%	11%
Sklepní dveře	3,78%	8,5%
Sklepní Okna	3,15%	8,5%
Ostatní	0,62%	0,4%

Tab. 2b Nejčastější narušení (domy) [3]

U pachatele vloupání je třeba pochopit jeho motivaci- zda jde o organizovanou skupinu, která operuje na objednávku, nebo na podnět tipaře či jen náhodného zloděje, kterému se zrovna zlíbí náš byt či dům. Zabezpečovací zařízení proto musíme přizpůsobit pro nejpravděpodobnějšího vetřelce. Z toho vyplívá, že je ekonomicky nepřiměřené

budovat za statisíce korun zabezpečovací systém, když v domě nemáme nic cenného. Proto je potřeba při komponování bezpečnostních prvků brát zřetel na reálie našeho vlastnictví. [1,2,5]

1.2 Základní pojmy

Zabezpečovací systém se z hlediska bezpečnosti dělí do čtyř kategorií, které jsou značeny římskými čísly. Výrobce musí každý svůj výrobek označit, tak aby bylo jasné, do které skupiny patří. Toto dělení nám zavádí technická norma ČSN EN 50131-1. Tato norma uvádí nový termín pro poplachové systémy. Místo staršího značení **elektrická zabezpečovací signalizace (EZS)** nově uvádí termín **elektrické zabezpečovací systémy (EZS)** se stejnou značkou jako jeho předchůdce, zkratkou EZS. Norma dále udává požadavky na elektrické zabezpečovací systémy a přesně popisuje čtyři stupně zabezpečení a čtyři třídy vlivu prostředí a metody testování jednotlivých tříd. [18,15]

Norma je dána jako východisko pro pojišťovací společnosti, dodavatele EZS, uživatele a policii při určení celkové specifikace zabezpečení u konkrétního objektu. Norma nám ale nic neříká o rozsahu a míře detekce. Nemluví ani o počtu a druhu zabezpečení a nemusí ani pokrývat veškeré požadavky systému. Norma pouze odkazuje na minimální požadavky, jež musí být splněny a je nutné brát zřetel při projektování ochrany na specifika objektu a hodnoty majetku v něm, který je třeba střežit, a riziko které představuje vniknutí narušitele. [5,1,18]

Jak jsem již výše psal, tak se pro zajištění úrovně požadovaného zabezpečení používají elektrické zabezpečovací systémy a jeho komponenty. Ty se dělí do čtyř stupňů zabezpečení, které berou v úvahu míru rizika. Ta je závislá na typu objektu, hodnotě majetku a na předpokládaném typu narušitele. Stupeň zabezpečení typu IV. je nejpřísnější a stupeň zabezpečení typu I. nejlehčí na splnění.

1.3 Základní rozděleni EZS

Existuje celá řada typů detektorů použitých v EZS a tím pádem je i velké množství způsobu jejich použití. Toto členění nám blíže specifikují evropské normy (tab. 3).

Poplachové systémy EN 50 (TC 79), EN 54 (TC 72)		
Všeobecné	**Elektronické zabezpečovací systémy (EZS)**	**Systémy uzavřených televizních okruhů (CCTV)**
EN 50130+	EN 50131+	EN 50132+
Systém kontroly a řízení vstupů (ACS)	**Systémy přivolání pomoci (SAS)**	**Systémy tísňové (HUAS)**
EN 50133+	EN 50134+	EN 50135+
Přenosová zařízení (ATS)	**Systémy kombinované nebo integrované (IAS)**	**Elektrická požární signalizace (EPS)**
EN 50136+	EN 50137+	EN 54+

Tab. 3 Normy [18]

Pro nás je zde nejdůležitější norma ČSN EN 50131, podle které můžeme systémy dále dělit do čtyř skupin, v rámci kterých se dále dělí a blíže se s nimi seznámíme v následujících odstavcích.

Prostorové zaměření: *Obvodová ochrana* je signalizací narušení obvodu, tedy ochrana pozemku hranice. *Plášťová ochrana* signalizuje narušení pláště střeženého objektu, například zdi či vstupních dveří. *Prostorová ochrana* má za cíl zajistit bezpečí vnitřního prostoru objektu. Po překonání plášťové ochrany zachytí pohyb vetřelce uvnitř střeženého objektu. *Předmětová ochrana* se vztahuje k určitému střeženému objektu a manipulaci s ním. Jedná se například o trezor či obraz. *Klíčová ochrana* má za cíl chránit klíčová místa objektu, předpokládaná místa vetřelcova pohybu a centrální body jako rozvodny a ústředny. [5,9,15,16]

Hledisko předávání poplachového signálu: *Lokální signál* je předáván jen místně. Nejčastěji je proveden akusticky, kdy signál převedeme na poplachovou sirénu. *Autonomní signál* má výstup přiveden ke stálé službě. Ta vyhodnocuje signál a následně provádí i zákrok. Zpravidla je doplněna o akustickou a optickou signalizaci. *Dálková signalizace* má výstup na vzdáleném pracovišti, nejčastěji se jedná o pult centralizované ochrany. [5,9,15,16]

Kategorie rizikovosti chráněných objektů: Je specifikovaná v normě ČSN 33 4590. Tato kategorie říká, ke kterému objektu mohu použít různá zabezpečovací zařízení a z kterých tříd. Rozdělení v (tab. 4). [5,9,15,16]

Rizika	Druhy Objektů	Kategorie dle ČSN
Nízká (NR)	byty, vilky, malé provozy, obchůdky	4
Průměrná (PR)	obchody, sklady, obchodní centra*	3
Vysoká (VR 1)	velká klenotnictví, banky, galerie	2
Nejvyšší (VR 2)	zbrojovky, atomové elektrárny, centrální úložny, státní pokladny	1

Tab. 4 Kategorie ohrožení objektů [5]

Hledisko stupně zabezpečení chráněného objektu: Je hlavním rozdělením, které se používá pro stanovení třídy bezpečnosti jednotlivých součásti EZS.

Tak jako jsou mechanické zábrany schopny zabránit vloupání, nejsou schopny vyhlásit poplach, ani žádným jiným způsobem neupozorní majitele na přítomnost nebezpečí. To platí i v případě nebezpečí únikem plynu a požáru. K tomu slouží elektronické zabezpečovací systémy. Jak již bylo výše zmíněno, norma definuje rozdělení do čtyř základních tříd. Stupeň I. - nejsnáze překonatelné až stupeň IV. - nejhůře překonatelné (tab. 5). V tabulce vidíme základní předpoklady pro zařazení do jednotlivých tříd. [3,5]

Riziko	Znalosti a vybavení narušitelů	**Stupeň**
Nízké	Malá nebo žádná znalost EZS. S velmi omezeným a snadno dostupnými nástroji.	**I.**
Nízké až střední	Narušitel je obeznámen se základním principem funkce EZS a mají úplný sortiment nástrojů a přenosných přístrojů.	**II.**
Střední až	Předpokládáme, že narušitel má znalosti EZS na vyšší úrovni a má přístup k úplnému sortimentu nástrojů a přenosných zařízení	**III.**

vysoké		
Vysoké	Použití v místech kde má bezpečnost přednost před jakýmkoliv hlediskem. Pachatele mají část a možnost sestavit podrobný plán a disponují kompletní sadou nářadí a mají možnost nahradit členy EZS.	**IV.**

Tab. 5 Kategorie rizik [5]

Pokud systém rozdělujeme do více subsystémů s různou bezpečnostní úrovní, má systém celkovou úroveň bezpečnosti jako jeho subsystém s nejnižší úrovní. Vlastní úroveň zabezpečení subsystému je dána nejnižší hodnotou komponentu zařazeného do subsystému. Pokud jsme zařadili do systému nějaký komponent společný pro více subsystémů, např. ústřednu, pak mají úroveň zabezpečení stejnou jako hodnota nejvyšší úrovně subsystému. [3,5]

1.3.1 Možnosti připojení na pult centralizované ochrany (PCO)

O co se vlastně jedná? Ve stručnosti se dá říci, že jde o monitorovací místo bezpečnostní agentury nebo policie, kam jsou přiváděny výstupy z bezpečnostní ústředny. Zde jsou informace vyhodnocovány a případně řešeny. Jedná se zpravidla o placenou službu. V reálu se tato služba realizuje pomocí několika metod. V zájmu vyšší bezpečnosti je lepší aplikovat více metod na přenos informací na PCO, které popíši v následujících odstavcích.

Připojení po pevné telefonní lince: První a nejstarší metodou předávání informací na PCO je telefonní linka. Dosud je to nejpoužívanější metoda, ale také nejméně bezpečná. Pro bezpečnostní systém není potřeba mít zavedenou nezávislou linku. Komunikátor ústředny pracuje na stejném způsobu jako fax. Při předávání informací na PCO nejprve odpojí všechny jiné členy telefonní sítě a po ukončení přenosů je opět do sítě připojí. Z toho vyplívá, že každé spojení s PCO představuje jeden telefonní impulz. Zpravidla dochází každý den alespoň k jednomu kontrolnímu spojení. Připojení je velice snadno napadnutelné vytrhnutím telefonní přípojky, zničením spojovacího kabelu nebo přetížením linky. Další nevýhodou je také množství impulzů a tudíž i cena služby. [1,5,10]

GSM modulem: Tato metoda je realizovaná pomocí sim karty běžného mobilního operátora. Toto řešení je mnohem spolehlivější než připojení po pevné lince, ale stále

dochází k podstatnému navýšení telefonních poplatků o hovory, které způsobí zabezpečovací zařízení. Většina bezpečnostních služeb však nabízí paušalizované SIM karty za poměrně příznivou cenu, která tento handicap snižuje. Možnosti narušení tohoto systému jsou poměrně malé. Může se jednat buď o rušičku signálu v pásmu přenosu GSM, anebo vyřazení vysílačů GSM v dané oblasti, což je v reálu dosti problematické. Dalším vyskytovaným narušením je odposlech přenosového signálu a jeho následná dešifrace využívaná k získání informací o systému. [1,5,10]

GPRS modemem: Bezpečnostní agentury využívají pro připojení elektronického zabezpečovacího systému k pultu centralizované ochrany modemu GPRS. Stejně jako u GSM se k přenosu použije některá z mobilních sítí, ale místo telefonního hovoru se použije GPRS modem, který informace pošle jako data. Takto realizované spojení je podstatně levnější. Možnosti narušení jsou stejné jako u GSM. [1,5,10]

Bezdrátová sít: Někteří provozovatelé pultů centralizované ochrany mají i vlastní bezdrátové sítě. Jejich výhodou je nezávislost na cizích přenosových zařízeních, trvalá kontrola spojení mezi bezpečnostním systémem a pultem centralizované ochrany a v některých případech i nižší provozní náklady. Většinou je ale nutné si vysílač od provozovatele PCO zakoupit. Problémem je často dostupnost sítě provozovatele PCO. Díky trvalému spojení s PCO je možnost vyřazení takového přenosu dosti problematická a vždy při pokusu o narušení vede k podezření na pultu hlídací společnosti. Vyskytly se případy, kdy za nepříznivého počasí skupiny před vniknutím vyřazovaly celé vysílače bezpečnostní služby tak, aby to vypadalo na poškození vlivem bouřky. Počítali s tím, že agentura nebude mít dost lidí na to zajistit kontrolu všech hlídaných objektů. [1,5,10]

1.3.2 Napájecí zdroje

O bezpečnosti prvků EZS nám vypovídá odolnost napájecích zdrojů. Tu nám specifikuje norma ČSN EN 50131-6, která se vztahuje jak ke komponentům instalovaným uvnitř domu, tak i ve venkovních prostorách. Tato norma stanoví požadavky, zkušební postupy a stupně zabezpečení na napájecí zdroje, které jsou použité v systémech EZS. Norma definuje podmínky, které zdroj musí splnit, včetně těch volitelných. Posuzovanými hodnotami jsou: zajištění monitorování v případě výpadku napájecího zdroje, doba zálohování, po kterou je zdroj schopen fungovat v případě výpadku energie ze sítě, čas

nutný na dobytí hlavního napájecího zdroje, ochrana proti sabotáži a otevření krytu. Souhrn uveden v tab. 6. [15]

Monitorovací signál	Stav	I.	II.	III.	IV.
Porucha vnějšího zdroje energie	Porucha vnějšího zdroje energie	P	P	P	P
Porucha náhradního napájecího zdroje	Nízké napětí	P	P	P	P
	Porucha	V	V	P	P
Porucha výstupu napájení	Nízké výstupní napětí	V	V	P	P
Doba zálohování v případě výpadku napájení		8h	15h	24h	24h
Doba dobíjení hlavního zdroje		72h	72h	24h	24h
Ochrana proti sabotáži. Energie nárazu (Joule)		2	2	5	5
Detekce Sabotáže					
Otevření normálními prostředky		P	P	P	P
Otevření z montážního místa		V	V	P	P
Proražení krytu		V	V	V	P
*Průměr ocelové tyčky v mm (±0,05)		2,5	2,5	1	1

Tab. 6 Podmínky ochrany napájecího zdroje
*Maximální velikost tyčky, kterou se lze dostat k detekci sabotáže. V-Volitelná funkce P-Povinná funkce Poplachové ústředny [17]

Centrem každého poplachového systému je ústředna. Jedná se o plošný spoj s mikroprocesorem, napájecím zdrojem a vstupy pro zapojení zón s detektory. Dnes již je standardem vybavení na GSM, které slouží ke komunikaci na pult centralizované ochrany, nebo pro dálkové ovládání ústředny. Toto zařízení je v podstatě mobilním telefonem fungujícím na telefonní kartu jakéhokoliv operátora. V ústředně je každá zóna definována výrobcem pod nějakým číslem. Podle čísla je pak definováno chování každého detektoru. To může být buď továrně nastaveno, nebo u novějších ústředen, jako je například agility od společnosti Risco, je možné chování definovat. Standardně se vyrábějí ústředny dle realizace obvodů - s drátovými rozvody a bezdrátovými rozvody, nebo ústředny hybridní.

Ústřednu připojujeme do elektrické sítě vždy přes nezávislý jistič. Každá ústředna je vybavena záložní baterií, která by měla vydržet po dobu 12 hodin. Bližší specifikace v (tab. 6). Jednoduché programování ústředny lze zajistit přes funkci Upload/Download, kde lze programovat chování, citlivost, časové zpoždění detektoru a mnohé další funkce. Například máme-li vchodové dveře vybaveny magnetickým kontaktem a za nimi PIR detektor, umožňuje nám ústředna volby nastavení zpožděné reakce. Příjemné jsou také možnosti pojmenování zón, kdy místo nic neříkajícího „zóna 01, poplach“ nám umožňuje nastavit například „vstupní dveře, chodba dole, poplach“, což oceníme nejvíce u rozsáhlých zabezpečovacích systémů.

Hlavní rysy ústředen jsou: počet drátových a bezdrátových zón, což nám udává celkový možný počet připojených detektorů a možnost nastavení všech uživatelských kódů plus master, kde master kód je hlavní správcovské heslo, které nemůže být omezeno na pravomocích a plně ovládá systém. K uživatelským kódům se váže nastavování stupňů oprávnění pro jednotlivá hesla a také možnost proximity tagu pro uživatele. [1,2,11,12]

Z výše zmíněných funkcí vyplívá, že ústředna musí být schopna zpracovávat velké množství signálů. Z toho se dají snadno určit požadavky na ústřednu a zpracování jednotlivých signálů, které jsou: [15]

- poplach narušení (intruder alarm).
- poplach přepadení (hold-up alarm).
- poplach sabotáže (tamper alarm).
- porucha (fault).
- jiné (např. signály, zprávy servisu - nesmí ovlivnit žádné povinné funkce).
- uživatelský přístup (zprávy nebo signály z uživatelského přístupového zařízení např. uživatelské ovládací klávesnice nebo spínače).

Jako každý typ zabezpečovacího zařízení je i ústředna dělena do 4 typů zabezpečení, jak již bylo řečeno výše. Hlavní hlediska pro rozdělení do těchto tříd si zde popíšeme. Základním kamenem je rozlišení chybných kódů (tab. 7).

Chyby kódu nebo klíče	I.	II.	III.	IV.
Indikace (informace o chybě uživateli)	V	V	V	V
Záznam událostí	V	V	P**	P
Blokování uživatelského rozhraní (10 chyb)	V	V	P* 1h	P 10h
Poplach sabotáže (10 chyb v 1 hodině max.)	V	V	P*	P

Tab. 7 Chyby kódu a klíčů

*Pro třetí stupeň je nutno splnit alespoň jeden požadavek. **Není povinné pro jednotlivé chyby, ale nutno blokování pro sabotáže a blokování. V-Volitelná funkce P-Povinná funkce. [17]

Dalším důležitým bodem je indikace různých stavů - ať už formou optickou, nebo akustickou. Tyto stavy jsou: [15]

- poplachy (narušení, sabotáž)
- poruchy
- systém ve střežení/klid
- provoz.

Veškeré funkce musí být jasné a nezaměnitelné. U optické signalizace je doporučováno následující rozdělení.: [15]

- poplachy (narušení, sabotáž) - červená
- poruchy - žlutá
- testování - žlutá
- stav střežení/klid - zelená
- provoz – zelená

Akustická signalizace pak musí splňovat následující. Je spouštěna vždy při vzniku stavu poplachu a poruchy, ale ne při stavu přepadení. Signalizátor musí být umístěn ve skříni ústředny nebo v panelu ovládání. Vypnutím zvukové signalizace se přitom nesmí vypnout žádná jiná funkce. Signalizace poplachu má mít nejmenší zvukové parametry v hodnotě 60db/(A) po dobu jedné minuty. Požadavky na zařazení do bezpečnostních skupin jsou uvedeny v (tab. 8). [2,15]

Indikace Stavů	I.				II.				III.				IV.			
	NS	SS	NK	SK	NS	SS	NK	SK	NS	SS	NK	SK	NS	SS	NK	SK
Blokace Systému	V	V	V	V	P	V	V	V	P	V	V	V	P	V	V	V
EZS střežení	/	V	V	/	/	V	V	/	/	P	V	/	/	P	V	/

Tab. 8 Idikace stavů EZS
V-Volitelná funkce P-Povinná funkce. NS-Nastavení střežení, SS-Stav střežení, NK-Nastavení klidu, SK-Stav klid [17]

Další kriterium je, že za předpokladu decentralizované ústředny bude mít ústředna oddělený indikační a ovládací panel. Musí být monitorovány též spoje mezi jeho decentralizovanými částmi. Podle stupně zabezpečení rozlišujeme monitorovací kanály jako přímo monitorované, nebo s nepřímo odděleným kanálem ve stejném kabelu (Tab. 9). [2,15]

Způsob monitorování	I.	II.	III.	IV.
Přímé-jednoduché vyvážení	V	P		
Přímé-dvojité vyvážení	V	V	P	P
Nepřímé	V	V		
Cyklus monitorování				
Nepřetržité 24h denně	P	P	V	V
Pouze v režimu střežení	P			

Tab. 9 Způsoby monitorování
V-Volitelná funkce P-Povinná funkce. [15]

Jedním z nejdůležitějších požadavků je ochrana proti sabotáži, kde je nutné zajistit robustnost krytu tak, abychom zabránily neautorizovanému přístupu do ústředny a vlastních komponent ústředny bez viditelných stop po násilí. Pro přístup je vyžadováno

otevření pouze adekvátním nástrojem, který otevře pevné uzavření skříně. Stupně ochrany při úderu a nutnost požadavků pro rozdělení do kategorií uvádím v (tab. 10). [7,12,15]

Ochrana proti sabotáži	**I.**	**II.**	**III.**	**IV.**
Energie úderu (J)	2	2	5	5
Detekce sabotáže.				
Otevření krytu normálními prostředky*	P 2,5	P 2,5	P 1	P 1
Oddálení z namontované polohy	V	V	V	P
Proniknutí krytem	V	V	V	P

Tab. 10 Ochrana a detekce proto sabotáži
* Průměr ocelové tyčky v mm (±0,05) V-Volitelná funkce P-Povinná funkce. [15]

K dalším detekčním požadavkům u ústředen patří detekce poruch. Tuto službu musí každá ústředna detekovat dle předpokládaného stupně zabezpečení. To znamená zpracovávat poruchy a chyby z napájení EZS a poplachového přenosového systému (tab. 10). A co je důležité, že programově řízené ústředny musí být schopné monitorovat správné vykonávání programu. Víc v předchozí (tab. 3) kapitola 1.2.1. [15]

1.3.3 Detektory

Pod pojmem detektor si představíme souhrnné označení pro přístroj sloužící k monitorování přidělené oblasti, který při splnění stanovených podmínek nahlásí na ústřednu poplach. Ústředna informaci vyhodnotí, a buď ji ignoruje, nebo vyhlásí poplach. Základní požadavky pro rozdělení do bezpečnostních skupin jsou pro všechny typy detektoru stejné. Rozdělení uvádím v (tab. 11).

Požadavek	I.	II.	III.	IV.
Odolnost Mechanická	P	P	P	P
Odolnost použití nástrojů	V	P	P	P
Přístup otevřením krytu	V	P	P	P
Odolnost na magnetické pole	V	P	P	P
Zabránění sundání z montážní podstavy	V	V	P	P

Odolnost proti hmyzu	P	P	P	P
Blokace vzájemného rušení	P	P	P	P
Režim návěstní	P	P	P	P
Režim místního zkoušení	P	P	P	P
Pohotovostní režim	V	V	V	V
Režim dálkového zkoušení	V	V	V	V

Tab. 11 Požadavky na bezpečnost detektorů
V-Volitelná funkce P-Povinná funkce. [14,16,17]

Dále si povíme něco málo o nejčastěji používaných detektorech a jejich schopnostech. Blíže se s nimi seznámíme v kapitole 2.

Detektor pohybu (IR): Je postaven na bázi pasivního a dnes i aktivního infračerveného snímání pozadí, a pokud dojde k pohybu nějakého teplého předmětu v teplotě odpovídající lidskému tělu, vyhlásí poplach. Základem je snímací čočka, přes kterou prochází IR signál ze senzoru, který čočka rozdělí na laloky. V případě, že někdo vstoupí do laloku, dojde k nárůstu IR signálu a po začátku jeho chůze dojde také k střídavému nárůstu IR signálů v různých lalocích. Tím jsou splněny obě podmínky pro vyhlášení poplachu a pachatel je detekován. Výměnou různých čoček lze tak dosáhnout určitých vlastností, jako například odolnosti proti domácím mazlíčkům. Těmto detektorům říkáme PIR s ochranou PET. Detektory PIR jsou nejběžnějším tipem detektoru. [2,7]

Detektor pohybu (MW): Jedná se o aktivní detektor založený na vysílači a přijímači mikrovlnného signálu pohybujícího se okolo 10 GHZ. Detekce se zakládá na Dopplerově jevu, kdy čidlo vyhodnocuje situaci na základě odraženého signálu. Pokud se objekt pohybuje, tak se signál mění, a to signalizuje narušení. Používá se jen na místech, kde nelze dát detektor IR. Velkou nevýhodou je pronikání záření přes tenké plochy, a tudíž velké ohrožení ze strany falešných poplachů. Signál je navíc zesilován kovovými plochami a přístroje se navzájem mohou rušit. [2,7]

Detektor pohybu (IR+MW): Jedná se o kombinovaný detektor určený do extremních podmínek. Využívá jak infračerveného čidla, tak vysílače a přijímače mikrovln. Vyhlašuje narušení jen v případě splnění obou podmínek. [2,7]

Magnetické kontakty (MK): Magnetický kontakt je nejběžnější a nejlevnější typ detektoru. Princip je postaven na jazýčkovém relé, které po přiložení magnetu ke kontaktu sepne. Používá se zejména na dveřích a oknech. Vyrábějí se hlavně dva typy - zapuštěný do rámu (detektor není vůbec vidět) a povrchový. Instalace je jednoduchá, hlídá se pouze vzdálenost obou částí detektoru od sebe, kterou nám udává výrobce. V praxi je též nutno počítat s určitým zpožděním zaviněným hysterézí a také náchylností jazýčku na mráz a následně špatnému spínání. [2,7]

Detektory tříštění skla: Používáme je v uzavřených prostorách k ochraně velkých zasklených ploch a jejich princip je založen na akustickém sledování prostoru. Většinou analyzují slyšitelnou část zvuku, která vznikne tříštěním skla a tlakovou vlnou, která vzniká v okamžiku rozbíjení skla. Při splnění obou podmínek detektor indikuje narušení. Hlídání podmínek má za úkol mikrofon, který hlídá časoví průběh a intenzitu tříštění skla. Důležité je, abychom nepodceňovali umístění detektoru a aby detektor na hlídanou plochu viděl a byl umístěn v dostatečné vzdálenosti od ní. Důležité je před nákupem zjistit, zda hlídá i okna s fólií, a jaký má zaručený rozsah hlídané plochy. Ideální je při kombinaci s magnetickými kontakty. [2,7]

Otřesové detektory: Používají se všude tam, kde je možno překážku překonat pomocí síly. Pokud máme tento přístroj doma, tak to bude s největší pravděpodobnosti detektor založený na piezo-čidlu, na kterém vzniká v důsledku chvění napětí. Senzor následně vyhodnotí dle velikosti napětí, zda se jedná o narušení chráněné zóny či nikoli. Schopnost detekce se u různých činností napadení liší dle zařazení do skupiny úrovně zabezpečení. Tyto detektory je možné kalibrovat. Proto musíme při instalaci dbát na to, na jaký materiál budeme detektor instalovat. Na materiál lepíme detektor nepružným lepidlem netlumícím rázy. To můžeme otestovat ranami na nejvzdálenějším místě chráněného předmětu. [2,7]

Infrazávory: Jedná se o aktivní hlídací detektor použitelný jak pro venkovní, tak i pro vnitřní prostor. Je složen ze dvou částí - IR vysílače a přijímače. Jeho funkce je založena na principu přerušení paprsku, který je vysílán vysílačem a zachycován přijímačem. V případě, že je paprsek přerušen, je detekován poplach. Infrazávory, zvláště venkovní, jsou dosti náchylné na vliv okolí, zvláště pak na vítr a mráz. [2,7]

1.3.4 Požární detektory

Požární detektory slouží jako doplňková ochrana k EZS. V současné době se nejvíce používají dva principy – tepelné a opticko-kouřové.

Tepelné: Jak již jejich název napovídá, tepelné detektory vyhodnocují maximální teplotu v místnosti a mohou také vyhodnocovat rychlost nárůstu teploty. Pokud je překročena maximální teplota, je vyhlášen poplach. Poplach je vyhlášen rovněž, pokud je nárůst teploty rychlejší, než je povoleno. Tepelné detektory nejsou náchylné na prach a nečistotu. Pro jejich aktivaci je potřeba plamen, který způsobí nárůst teploty. Tyto detektory zpravidla reagují na požár s určitým zpožděním. [8]

Opticko-kouřové: V detektoru je vyhodnocovací komůrka, která je prosvětlována IR diodou a je vyhodnocována světelná ztráta. Pokud se do komůrky dostane kouř, je snížena viditelnost a detektor vyhlásí poplach. Komůrku a vyhodnocovací prvky je potřeba pravidelně čistit, protože v prašném prostředí je zanášení detektorů rychlejší. Výhodou je reakce na kouř, kdy materiály nemusí přímo hořet, ale už jejich doutnání způsobí poplach.[8]

Tepelně-optické: Jedná se o kombinovaný detektor, který používá obě předchozí metody pro detekci požáru. Stačí pouze jedna složka pro vyhlášení poplachu. [8]

Pro kouřové detektory lze v souhrnu použít následující pravidla pro jejich instalaci a testování:

- **Instalace:** Nejlepší umístění je na strop nad materiál, jehož požár se má hlídat. Pokud se hlídá pouze místnost, je nejlepší umístit detektor doprostřed místnosti na strop. Pokud nelze umístit detektor doprostřed stropu, je dobré jej umístit na strop co nejblíže středu, v krajním případě minimálně 20 cm od rohu místnosti. [7,8]
- **Test tepelného detektoru:** Dá se v domácích podmínkách provést pomocí horkého vzduchu z fénu přiváděného na čidlo. Vyhodnocení poplachu však může mít určité zpoždění z důvodu doby nutné pro ohřátí senzoru. [7,8]
- **Test kouřového detektoru:** Nejjednodušším testem je zapálit papír a uhasit jej. Kouřící zbytek papíru přiložte pod detektor. Reakce detektoru může mít opět zpoždění z důvodu průniku kouře do vyhodnocovací komůrky. Pro ukončení poplachu „profoukněte“ detektor, který s jitým zpožděním přejde do klidu. Do

detektoru lze fouknout i cigaretový kouř. Pro větší počet testů je lepší použít speciální aerosolové spreje určené pro simulaci kouře. Na detektor se v tomto případě krátce stříkne aerosol a po chvilce musí detektor vyhlásit poplach. Pro ukončení poplachu je nutno počkat, až plyn vyprchá nebo je nutné číslo profouknout. [7,8]

2 Možnosti narušení a ochrany, rozbor prvků EZS

2.1 Ústředna

Při výběru ústředny musíme dávat pozor na to, že naše ústředna spadá do takové kategorie jako její nejslabší připojený člen a nemá tak smysl kupovat ústřednu kategorie III. pro detektory kategorie I. či II.

Dle připojení členů do zabezpečovacího systému rozlišujeme několik typů ústředen, s čímž i souvisí možnost napadení ústředny. Pro výběr zabezpečovacího systému bychom měli zvláště zohlednit tyto aspekty:

- Riziko způsobené typem provozu v objektu (např. banka).
- Velikost chráněného objektu.
- Finanční možnosti investora.

2.1.1 Základní bezpečností pravidla

U každé z dále uvedených skupin ústředen je možno uplatnit z hlediska umístění a možností narušení obecně platná pravidla tak, abychom snížili bezpečnostní rizika.

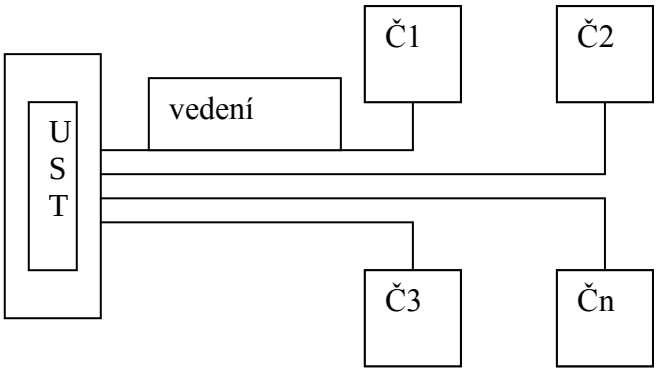
- Ústřednu umísťujeme do chráněného prostoru, mimo dohled a dosah neoprávněných osob tak, aby nebyla snadno a rychle dostupná. [5]
- Moderní mikroprocesorové ústředny jsou provedeny odděleně. Vlastní ústředna může být vhodně skryta a přístupné jsou pouze ovládací panely. To nám umožní dát do zpožděné smyčky pouze ovládací klávesnici. Její vyřazení však nevyřadí z činnosti celý systém. [2,5]
- Uživatel systému by neměl být seznámen s programováním ústředny ani se servisními kódy a postupy. Zabráníme tak neodborným zásahům a změnám funkce

EZS a následným planým poplachům a případně i pojišťovacím podvodům, které se vztahují na špatnou funkci EZS. [5,7]

2.1.2 Analogová (smyčková) ústředna

Analogové smyčky se vyznačují tím, že každá poplachová smyčka je připojena na samostatný vyhodnocovací obvod ústředny (obr. 1).

Převážně se jedná o ústředny III. a IV. stupně, které registrují klidový proud protékající smyčkou, a pokud je větší, než ± 40 % vyhlašují poplach. Klidový proud smyčky určuje jednak parametry ústředny, a jednak odpor smyčky. Současné ústředny běžně používají jediný zatěžovací odpor dané hodnoty, který je zapojen v nejvzdálenějším bodu smyčky. Změna odporu smyčky, způsobená odpojením nějakého čidla nebo sabotáží na smyčce, vede k vyhlášení poplachu na EZS. Smyčky tvoříme nejčastěji sériovým zapojením rozpínacích kontaktů. [5,9]

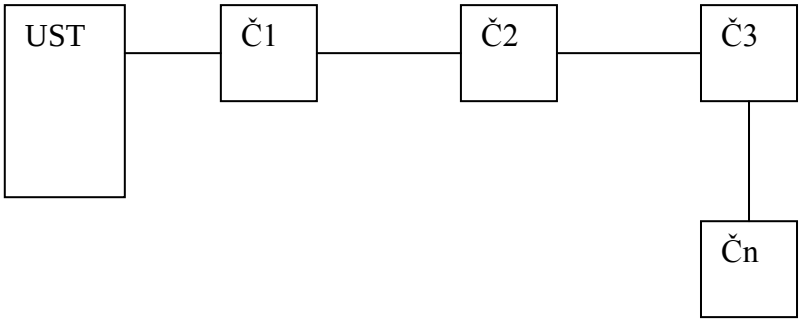


Obr. 1 Princip analogové ústředny
UST-ústředna, Č1..Čn-čidla

2.1.3 Sběrnicová ústředna s přímou adresací čidel

Sběrnicové ústředny pracují na principu digitální adresné komunikace po datovém vedení (sběrnici) mezi čidly a ústřednou v režimu časového eventuálně frekvenčního multiplexu (obr. 2.). Ústředna periodicky volá adresy čidel a následně vyhodnocuje jejich odpovědi. Pro toto připojení je nutné, aby každé čidlo bylo vybaveno komunikačním

modulem.[5,10]



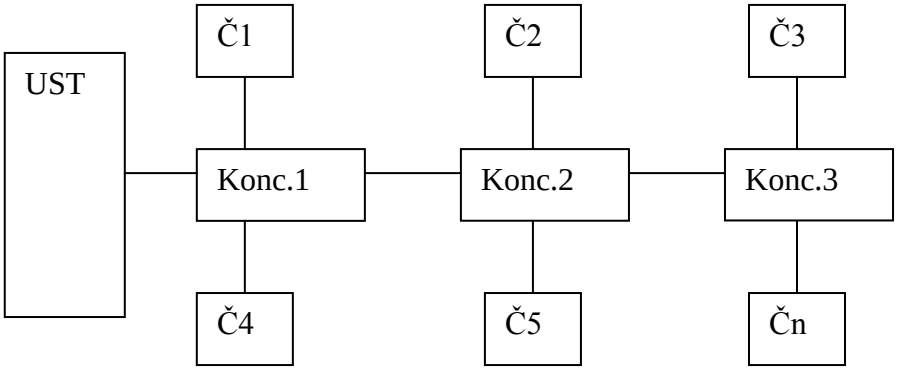
Obr. 2 Princip funkce sběrnicové ústředny
UST-ústředna, Č1..Čn-čidla [5]

Tento systém má výhodu minimální kabeláže, která je tvořena různou kombinací kabelové sítě. Čidla je možno připojit v libovolném pořadí, nejlépe na čtyřvodičové vedení. Dva vodiče zde slouží k napájení a dva pro datový přenos sběrnice. Při napadení nám toto uspořádání umožňuje přesně zjistit, jaké čidlo bylo napadeno a k jakému druhu napadení či poruchy došlo. [5]

Sběrnicové ústředny mají vysokou odolnost přenosových tras proti narušení a umožňují pomocí softwaru selektivní komunikaci s jednotlivými čidly v rámci libovolné smyčky. Počet přímo adresovaných čidel se pohybuje v desítkách. Je možné ho dále dělit do podsystémů. Nevýhodou je nutnost dodržet maximální délku kabeláže z důvodů úbytku napětí na vedení, což může způsobovat nekvalitní přenos informací a vyvolávat tak plané poplachy. [5]

2.1.4 Koncentrátorové ústředny (smíšené)

Jedná se o kombinaci ústředen sběrnicových a smyčkových s připojením desítek čidel do smyčky. Tyto ústředny se používají především do rozsáhlých objektů. Jejich principem je jedna či více sběrnic připojených k ústředně, přes které jsou připojeny koncentrátory, na které jsou pak připojena čidla. Koncentrátory zde zastupují analogové několika-smyčkové pod-ústředny (obr. 3). [5]



Obr. 3 Princip funkce koncentrátorové ústředny
UST-ústředna, Č1…Čn-čidla, Konc.1…Konc.n - Koncetrátory [5]

Výhodou těchto ústředen je nižší nárok na vedení kabelových rozvodů, protože není nutno vést vedení ke každému čidlu zvlášť, ale jen k nejbližšímu koncentrátoru. Na jednotlivé vstupy koncentrátoru pak přímo připojujeme jednotlivá čidla, čímž zachováme vlastnosti ústředen s přímou adresací čidel. Nevýhodou je však cena celého systému EZS. [7,5,9,]

2.1.5 Bezdrátové sítě EZS

Tyto ústředny se zejména uplatňují v objektech, kde je EZS doděláváno dodatečně, nebo na místech kde není možno vést rozvody pomocí kabeláže. Také se hojně používá při zřízení náhradního systému, nebo při dočasném zabezpečení objektu. Přenos je prováděn pomocí dvou způsobů - jednosměrnou či obousměrnou komunikací. [5,12]

- **Výhody:** Vysoká flexibilita. Snadná instalace - ústředna si prvky vyhledá sama. Možnost dočasné instalace. Připojení množství zařízení bez ohledu na dostupnost kabelového připojení. [5]
- **Nevýhody:** Přenos je realizován bezdrátovým přenosem - je zde možnost blokování přenosového signálu a odposlouchávání. Je nutné mít u každého přístroje vlastní napájecí zdroj a díky tomu je i cena za údržbu vyšší. [5]

2.1.5.1 Jednosměrný rádiový přenos

Nedostatek je zde v jejich jednosměrné komunikaci. Spolehlivost nelze kontrolovat na zvláštních či určených frekvencích, nebo pásmu 433 MHz a 868 MHz. Nedoporučuje se

používat tento typ ústředen pro objekty s vysokým rizikem napadení, protože zde není možnost neustálého monitorování detektoru. [5,9]

2.1.5.2 Obousměrný rádiový přenos

Tato komunikace využívá stejný stupeň monitorování jako ústředny spojené po metalickém vedení (sběrnicové rozvody). Pracují zpravidla na 433 MHz a 868 MHz. Systém je adresovatelný - má k dispozici kolem 100 adres a umožňuje dělení na nezávislé subsystémy. Ovládat lze pomocí přenosného ovladače nebo blokovacího zámku. Přenosný ovladač má výhody pro postižené při tísňovém volání a při práci venku monitoruje příchody a odchody na dálku. Systém je také možno vybavit funkcí tzv. mrtvého muže. To znamená, že je ovladač vybaven náklonovým čidlem a infračerveným vysílačem a není tak možno systém uvést do chodu bez přítomnosti obsluhy uvnitř střeženého objektu. [5,12]

Hlavní výhodou obousměrného přenosu je podstatně vyšší zabezpečení přenosového kanálu, kde přijímač a vysílač pracují souběžně na dvou kmitočtech a v případě narušení pásma přenosu, ať již rušením záměrným nebo atmosférickým, si je schopen sám vyhledat jiné pásmo přenosu. Systém je také schopen indikovat intenzitu pole, a podávat uživateli informace o tom, zda pracuje s rezervou nebo na hranici citlivosti. Přenos mezi prvky je digitální a má plavoucí kódování proti odposlechu, což jej činí velmi špatně napadnutelným. [5,12]

2.1.6 Hybridní

Tento typ patří k nejmladším typům ústředen. Jedná se o kombinovanou ústřednu umožňující jak připojení pomocí drátových vstupů tak i bezdrátových adresovatelných prvků.

Ústředny mají všechny nevýhody smyčkových ústředen, ale zároveň mají výhody ústředen bezdrátových. Použití je zejména v oblastech, kde je možné mít částečně připojení metalické, ale zároveň jsou určité prostory nedostupné pro kabeláž. Zvláště v poslední době zažívají tyto ústředny velké rozšíření díky své flexibilitě a schopnosti vytvořit jakékoliv požadované zabezpečení z hlediska rozmístění jednotlivých prvků. [5]

2.2 Pult centralizované ochrany

Pult centralizované ochrany je místem, kde dochází k vyhodnocování signálu přicházejícímu z chráněných objektů. Proto je nebytné zajistit bezproblémový chod těchto

pracovišť tak, aby nedošlo k jejich vyřazení a následnému znemožnění předání informace z ústředny napadeného objektu. Z hlediska funkce jsou pulty centralizované ochrany koncipovány jako autonomní nebo integrované do PC. [3,5]

- Autonomní systém je schopen plného přenosu bez dalších přístrojů. Je možno k nim připojit počítač pro příjemnější práci. V případě výpadku napájení je však schopen samostatné funkce a poskytuje všechny základní informace a reaguje tak na zprávy přicházející z detektorů. [3,5]
- Systémy integrované do PC pro svůj provoz potřebují provoz počítače a jsou jeho nedělitelnou součástí. Je nutná funkce všech částí počítače - například porucha pevného disku s ovládacím softwarem vyřadí celý systém PCO. Totéž platí i při výpadku softwaru realizujícího funkce PCO. Tyto systémy však mají větší požadavky na zajištění bezproblémového chodu, který je obvykle řešen záložními obslužnými místy. [3,5]

V České republice je v současné době v provozu velké množství firem a institucí provozujících pulty centralizované ochrany. Tyto pulty vždy nemusí splňovat kvalitativní požadavky stanovené normou ČSN EN 501131 a 50137. Proto je dobré se při výběru PCO řídit základními kritérii: [5,18]

- Doba přenosu (poplachu)
- Doba hlášení zprávy (kontrolní spojení)
- Dosažitelnost (navázání spojení)
- Zabezpečení proti záměně (objektové stanice)
- Zabezpečení informací (šifrování zpráv)

Rozdíl je zejména v kapacitě připojených objektů softwarovým vybavením, a co je nejdůležitější v realizaci přenosu informací ze zabezpečovaného objektu na pult centralizované ochrany. Ten je realizován jako linkový, bezdrátový, nebo kombinovaný. Podrobněji byly popsány v kapitole 1.3.1. [5]

Důležitou rolí PCO je odlišení planých poplachů od těch reálných. Ve skutečnosti je jen nepatrné procento poplachů nahlášených na PCO skutečných. Největší část planých poplachů (asi 60 %) připadá na uživatele, jedná se tedy o chybu lidského faktoru. Další

význačné procento (35 %) připadá na poruchu na EZS. Všechny tyto přenosy zatěžují přenosové kanály a obsluhu PCO, které musejí na každý takový poplach reagovat. Tyto stavy lze minimalizovat pomocí několika technických a administrativních opatření: [5,6]

- Přísnější stanovení režimu v objektech uživatele.
- Přehodnocení příchodové a odchodové trasy zaměstnanců, optimalizaci doby zpoždění na klávesnici. Vhodné je umístění klávesnice EZS.
- Kvalitnější montáž EZS a montáž prvků pro nejvyšší rizika.
- Volba vhodného typu tísňových hlásičů a optimalizace rozmístění.
- Filtrování poplachů ostrahou objektu u rozsáhlých objektů.
- Nábor vhodných zaměstnanců pro obsluhu EZS.

2.3 Detektory

Stejně jako lze dělit ústředny EZS do mnoha skupin, dělíme i detektory a čidla. Základní dělení je podle toho, zda ke své činnosti potřebují elektrickou energii. Dělí se tedy na čidla napájená a nenapájená.

2.3.1.1 Čidla napájená

Prvním typem napájených čidel jsou *aktivní čidla*, která vytvářejí své pracovní prostředí svojí aktivní činností, jako je například vysílání elektromagnetického vlnění. Z toho důvodu je snadné je detekovat a určit tak jejich mrtvé zóny. Pracují na principu porovnávání vstupních signálů s předem nastavenými kriterii. Riziko změny nastavených parametrů při režimu údržby se však nedá vyloučit i přes snahy výrobců. Z toho důvodu je v našem zájmu nepouštět žádné neoprávněné osoby k našemu zabezpečovacímu systému, a pokud voláme technika na údržbu, je nezbytné si jeho totožnost řádně prověřit. *Pasivní čidla* pak reagují na fyzikální změnu ve svém okolí - pasivní infračervené čidlo registruje změnu teplotního gradientu. Tato čidla jsou obtížně identifikovatelná běžnými prostředky jako je infravizor. [5]

Čidla napájená se dále rozdělují dle charakteru střežené oblasti. *Prostorová čidla* zaznamenávají narušení ve střeženém prostoru. *Směrová čidla* reagují jen ve směru, který je definován, například jsou to infrazávory. *Bariérová čidla* vytvářejí určitý druh bariéry,

při jejímž narušení dochází k detekci poplachu. *Polohová čidla* jsou určená k ochraně předmětu, tedy změně jeho postavení. [3,5]

2.3.1.2 Čidla nenapájená

Destrukční čidla jsou pouze jednorázová - při vyhlášení poplachu dojde k jejich zničení. Jedná se zejména o polepy, folie, nebo nádržky s barvou či případně nějakou dráždivou látkou. *Nedestrukční čidla* - po aktivaci nedochází k trvalým změnám a lze je použít opakovaně. Jedná se tedy především např. o magnetické kontakty. [5,17]

2.3.2 Prvky plášťové ochrany

Mezi prvky plášťové ochrany zahrnujeme všechny typy detektorů věnující se ochraně objektu ještě před narušením vlastního objektu

2.3.2.1 Mikrospínače

Mikrospínač je miniaturní přepínač určený ke kontrole přístupů. Montuje se do zárubně naproti závoře zámku, čímž střeží uzamčený stav objektu. Používá se zejména tam, kde je více vstupů a znemožňuje tak spuštění EZS bez uzavření všech vstupů do objektu. Dnes se používají zejména jako sabotážní kontakty. Problémem je složitá instalace, protože je nutné přesně nastavit pracovní rameno a pevnou aretaci celého kontaktu, jinak hrozí uvolnění a tím i nesepnutí spínače. [5,10]

2.3.2.2 Dveřní a přechodové spínače

Jedná se o starší typ zabezpečovacího systému. Dnes se již vyskytuje zřídka. Jedná se o kontaktní vidlice, které dosedají na protější kontakt či se zasunují mezi dva kontaktní plechy. Montují se na část, která se otevírá, tedy na tzv. zámkovou stranu. Přechodový kontakt má tu výhodu, že na něj lze montovat další prvky ochrany a vytvořit s ním tak smyčku. Připojíme-li ke smyčce například folii a kontakt bude sepnutý, protéká ve smyčce klidový proud. Bude-li se pachatel pokoušet spínač obejít vyříznutím otvoru do dveří, naruší tak folii a tím naruší i klidový proud a bude generován poplach. Nevýhodou je složitá instalace a malá životnost zvláště pak kontaktních plošek, které jsou náchylné ke korozi. Dále pak dochází ke znečištění plošek a jejich ošoupání, a proto je zde nutná častá kontrola. [2,5]

2.3.2.3 Nášlapné kontakty

Jedná se o mechanické kontakty, které se uvádějí v činnost, pokud pachatel vstoupí na jejich plochu. Využívají se zejména ke střežení vstupních či klíčových ploch a jsou umísťovány skrytě pod koberec nebo lino. Nevýhodou je, že jsou v klidovém stavu vždy kontakty rozpojeny a lze je za určitých podmínek oklamat, nebo jednoduše překročit. Jsou citlivé zejména na trvalé zatížení, při kterém se zvyšuje citlivost. Nutností je svědomité umístění vodičů tak, aby byly co nejvíce skryty a co nejméně dostupné, protože jsou náchylné na poškození, pokud nejsou dostatečně kryty. [5,16]

2.3.2.4 Rozpěrné tyče

Rozpěrná tyč je mechanický spínač, jehož klidový stav je aretován tyčí. Jedná se o doplňková čidla používaná například u prostupů ventilace. [5]

2.3.2.5 Magnetické kontakty

Jedná se o nejrozšířenější variantu prvků plášťové ochrany co do počtu provedení i aplikačních variant. Existuje několik skupin dle provedení. Provedení má totiž zásadní vliv na jejich odolnosti vůči napadení a jejich překonání. Tyto skupiny jsou s jedním jazýčkem, s více jazýčky, s vestavěným sériovým či paralelním odporem, s před-magnetizací, bez ochranné smyčky či s vestavěnou ochranou smyčkou. [11]

Ty nejběžnější lze obelstít dostatečně silným magnetem. Jednoduchý jazýček zůstane sepnutý z důvodu nerozpoznání cizího magnetického pole. Magnetické kontakty mohou mít mnohé provedení a obsahovat i řadu kombinací výše uvedených vlastností. Jsou vhodné ke střežení veškerých stavebních otvorů. Magnetický kontakt v těžkém provedení se používá v kombinaci s roletami, kde je pouzdro provedeno z nemagnetického materiálu odolného vůči mechanickému i klimatickému opotřebení. Magnet je umístěn na pohyblivou část a jazýčkový kontakt je umístěn na část pevnou. Je nutné dbát na maximální vzdálenost magnetu od jazýčku, kterou definuje výrobce. Ideální je vzdálenost poloviční mezi maximem a minimem. Tento požadavek se obtížně splňuje zejména u skryté montáže, kde je vzdálenost přímo ovlivňována vlastnostmi materiálu, na kterém je umístěn magnet. Proto se používají při montáži podkladové nemagnetické materiály k potlačení tohoto rušení. [5,11]

Vlastní kontakt je tvořen dvěma jazýčky z magneticky měkkého materiálu. Ty jsou zataveny do trubičky o průměru 2 až 4 milimetrů a délky 15 až 40 milimetrů. Trubička je

zhotovena z olověného skla. Plošky kontaktu jsou umístěny tak, aby se nepatrně překrývaly, v klidovém stavu se však nedotýkají. Trubička je naplněna neutrálním plynem. Plošky jsou pokryty galvanickou vrstvou zlata, někdy se přidává i malé procento niklu. Umístíme-li k jazýčkům dostatečně silný zdroj magnetického pole rovnoběžného s magnetickými siločárami, jazýčky se zmagnetizují a vzniknou na nich opačné magnetické póly a dojde k přitažení jazýčků a sepnutí kontaktu. [5,16]

Z důvodu zlepšení ochrany proti překonání se vyrábějí magnetické kontakty s ochranou proti překonání cizího magnetu. Tato ochrana je tvořena dvěma jazýčkovými kontakty v jednom tělese. Kontakty pracují buď s orientovanými magnety, nebo jako dva nezávisle odstíněné jazýčky, kdy jeden je spínací a druhý rozpínací. Připojují se čtyřmi vodiči - dva pro ochranou smyčku a dva pro spojení s kontakty. Permanentní magnet způsobuje, že jazýček zůstane sepnut. Oddálíme-li magnet, pole slábne a dojde k detekci poplachu. Stejně tak dojde k detekci poplachu, přiložíme-li v klidovém stavu cizí magnet k čidlu. Poplach je pak způsoben kolísáním magnetického pole. [5,15]

Nejlepší magnetické kontakty jsou založeny na principu Hallova jevu. Hallův jev je založen na umístění polovodičové destičky tak, že ve směru nejdelší hrany jím prochází proud do magnetického pole. Vektor, kterým prochází, musí být na destičku kolmý. Pokud je tomu tak, vzniká na stěnách Hallovo napětí. V praxi to znamená několikanásobné rozmístění magnetů a Hallových sond. Z toho vyplívá, že pachatel by musel mít přesnou znalost rozmístění magnetů a jejich indukce, a navíc by musel vše zvládnout na první pokus, což vyžaduje značný um a štěstí. [5,15]

Při instalaci kontaktu dbáme na to, aby nedocházelo k falešným poplachům, a proto umísťujeme kontakty tak, aby nedošlo k aktivaci při normálním pohybu (například nedosedáváním dveří a velké vůli nebo drnčením oken). Kontakt musí spínat při každém způsobu otevření dveří - nejen normálním, ale také při vylomení. Snadnost instalace a vysoká životaschopnost a odolnost vůči okolním vlivům za příznivou pořizovací cenu dělá z magnetických kontaktů nedílnou součást každého EZS, a proto se výrobci snaží neustále zlepšovat odolnost vůči napadení. [5]

2.3.2.6 Destrukční čidla

Tato čidla pracují na principu překážky, kterou musí pachatel překonat. Velkou nevýhodou je jejich jednorázové použití. Čidlo je nutné po vyhlášení poplachu vyměnit nebo opravit. V této kategorii čidla dělíme následovně:

Fóliové polepy vytvářejí na chráněné ploše tenkou vodivou vrstvu. Po narušení chráněné plochy dojde k narušení polepu a tím i ke změně procházejícího proudu. Instalujeme je vždy tak, aby z předpokládané strany narušení nebyly vidět a nebyly dostupné. Tato metoda je spolehlivější než vibrační čidla, která je nutné seřizovat. Přípojné místo orientujeme vždy k horní hraně ploch z důvodů možné kondenzace par, které mohou snižovat přenos. Problém u polepů je v složité a časově náročné instalaci. [5,17]

Vodičové sítě a zátarasy se používají zejména u trezorových místností. Fungují na principu instalace slabého vodivého materiálů na chráněné zdi, který je zakryt omítkou. Pro identifikaci průniku každá stěna reprezentuje jednu smyčku. Před zakrytím je potřeba dbát na dodržení postupů instalace, jelikož vlastní oprava je vzhledem k umístění velice složitá. [5]

Světlovodné zábranné sítě jsou moderním prvkem zabezpečení pláště budov. Na rozdíl od vodičové sítě používají světlovodné trubičky, díky čemuž jsou zde vyloučeny plané poplachy. Při stavbě se aplikují do trezorů již při výrobě panelů. [5]

2.3.2.7 Čidla ochrany proti destrukci

Principem těchto čidel je, že reagují na otřesy při narušení chráněných ploch. V současné době se používají nejvíce otřesová čidla s mechanickým měničem. Jedná se o čidla, která se aktivují při jakémkoliv otřesu. Principiálně jsou založena na setrvačnosti pružně zachyceného závaží. Používají se výhradně u skleněných ploch výkladních skříní. Z důvodů přerušení klidového proudu jen na několik milisekund je potřeba zajistit spojení s ústřednou pomocí rychlých klopných obvodů. Dalším negativem je častá kontrola - měla by být provedena minimálně třikrát do roka. Výhodou je pak jejich nízká poruchovost, která je ale vykoupená velkým počtem planých poplachů. [5]

2.3.2.8 Čidla na ochranu skelných ploch

Používají se ke střežení ploch obvodového pláště vybaveného sklem. Konstrukčně jsou uzpůsobena k vyhlášení poplachu při mechanickém poškození plochy. Jsou známa v provedení aktivním, pasivním kontaktním, nebo bezkontaktním. [7]

Pasivní kontaktní čidla pracují na principu piezoelektřiny. Obsahují piezokrystal naladěný na rezonanční frekvenci v pásmu 40 až 120 kHz. Elektronika v čidle monitoruje spektrum charakteristické pro destrukci skla šířící se jeho povrchem. Čidlo umisťujeme co nejtěsněji na chráněnou plochu s ohledem na co nejmenší ztráty minimálně 50mm od hrany rámu. Při výběru piezočidla je nutné zjistit, pro jaké sklo čidlo požadujeme, protože každý typ čidla je určen pro jiný druh skla. Dosah čidel je přitom maximálně do tří metrů. Výkonnější čidla jsou vybavena počítadlem pulzů, které eliminuje nahodilé pulzy. Výhodou těchto čidel je jejich necitlivost na rušivé zvuky, a proto je lze hlídat po dobu 24 hodin denně. Nevýhodou je pohyblivý přívod a nutnost použití čidla na každou skelnou tabuli zvlášť. [5,7]

Pasivní bezkontaktní čidla akustická jsou nejčastějšími detektory rozbití skla. Fungují na principu následné identifikace akustického jevu po rozbití skla. Charakteristické znaky jsou pro každou tloušťku a typ skla jiné. Tento akustický signál je převáděn do čidla vlněním vzduchu. Elektronika vyhodnocuje získaný signál přes takzvanou pásmovou propust, která propustí jen definovaná pásma signálu. K potlačení planých signálů se instaluje více propustí a signál se vyhodnocuje ve více pásmech spektra. [5,7]

Při instalaci je třeba mít na zřeteli několik základních aspektů k minimalizaci planých poplachů a schopnosti čidla detekovat poplach. Těmito aspekty jsou: dostupnost skelných ploch zvenčí, doprava v okolí (zejména blízkost dopravních zastávek a tras vlaků, kde skřípění brzd může negativně ovlivňovat čidlo), přítomnost nadměrného množství hmyzu. Z těchto důvodů musíme při instalaci dbát také na kvalitní usazení skelných ploch s omezením vibrace. Čidlo umístíme tak, aby vidělo na celou chráněnou plochu, a neumisťujeme mezi čidlo a plochu žádnou záclonu ani žaluzie. Výrobce přesně definuje pro které sklo a na jakou vzdálenost ho umisťujeme. [5,9,10]

Dalším typem čidla jsou *vícepásmová akustická čidla*. Jedná se o vylepšená čidla akustická, která kromě nízkofrekvenčního zvuku rozbití skla analyzují i pozdější zvuk

dopadu skla, při kterém má zvuková vlna vyšší frekvence. Čidlo je vybaveno vícepásmovým analyzátorem pracujícím v reálném čase, který při zachycení obou signálů ve správném pořadí detekuje poplach. Reálné použití je do tloušťky skla mezi 3-12 mm a sledované plochy do $15m^2$. [5]

Pro objekty s nejvyšším požadavkem na ochranu jsou určena *aktivní čidla rozbití skla*. Ta jsou vybavena vysílacím i přijímacím zařízením. Tato zařízení sledují vyslaný signál na svém přijímači, kde hledají ultrazvukové změny ve skle oproti normálnímu stavu, který je v elektronice zaznamenán. [5,12]

2.3.2.9 Bariérová čidla

Tato čidla slouží k vytvoření umělého zátarasu v chráněném objektu pomocí světelné, laserové, nebo infračervené technologie. Obecně existují dvě skupiny, které se dělí dle elektromagnetického spektra, ve kterém pracují viditelné světelné závory a neviditelné světelné závory. Od viditelných závor se upustilo, jelikož viditelné spektrum umožňuje pachatelům snadné překonání. [5]

V současné době se používají pouze neviditelné světelné závory v infračerveném spektru o hodnotách 0,75 Až 10 μm a laserová čidla v oblasti 850 nm. [5,12]

Infračervená závora je tvořena dvěma částmi - vysílačem a přijímačem. Princip je takový, že vysílač generuje infračervené záření, které zpracuje přijímač a při přerušení je detekován poplach. Vysílač je také vybaven modulátorem regulujícímu světelný tok tak, aby šířka pulzu byla úzká a tok malý. Modulátor má zabránit oklamání přijímače nahrazením vysílače jiným vysílačem. Použitelnost infračervené závory se pohybuje kolem 100 metrů. Instalace těchto prvků je však časově náročná. Vyžaduje přesné zaměření osy paprsku do přijímače a pevnou aretaci prvků. Pro menší objekty lze k vícenásobné blokaci použít odrazová zrcadla. Jejich použití ale zvyšuje riziko planých poplachů kvůli ušpinění nebo změně odrazné plochy. [5]

Existují také reflexní infračervené závory, kde vysílač a přijímač je integrován v jednom pouzdře. Vyslaný signál je odražen o reflexní vrstvy a následně navrácen do přijímače, kde je vyhodnocen. Tento systém je jednodušší na instalaci, avšak trpí více na plané poplachy, má kratší dosah a lze ho snáze překonat. [5,16]

Infračervené bariéry jsou tvořeny několika svazky infrazávor umístěnými nad sebe. Vysílače a přijímače jsou umístěny v nezávislých speciálních stojanech, které se instalují tak, aby se paprsky křížily. Vrchní paprsek je pak přijímán spodním přijímačem. Nevýhodou je pracná a zdlouhavá instalace s nutností pravidelných kontrol. [5]

Infračervené záclony zabezpečují chráněnou oblast pomocí optoelektronické záclony. Detektor je tvořen dvěma proti sobě ležícími lištami. Jedna lišta je tvořena řadou vysílačů a přijímačů, které vyhodnocují přijatý signál. Vysílač pracuje s kódovaným signálem okolo 900nm. Přijímač vyhodnocuje pouze paprsky v příslušném kódování, a tím eliminuje rušivé vlivy. Systém je odolný proti pomalému znečišťování i proti krátkodobému zakrytí jednoho vysílacího nebo přijímacího prvku. Odrazná lišta je pak tvořena řadou rovnoběžných hranolů. Malá šířka odrazné plochy způsobuje jen několikacentimetrovou tloušťku střežené plochy, jejíž rozměry se tak pohybují na výšku kolem 80 až 250 cm a na délku 100 až 950 cm. [5]

Při použití a instalaci bariérových čidel bychom měli dodržovat několik zásad pro práci s nimi. Při instalaci dbejme na kvalitu konstrukce v místě, kam detektor umisťujeme a na požadované upevnění vysílače. Čím lépe a pevněji detektor umístíme, tím menší hrozí odchylka signálu, a tím méně planých poplachů bude vznikat. Zásadně neumisťujeme na povrchy pružné nebo tam, kde je velké riziko chvění či posunů. Vychýlení o 1º znamená na vzdálenosti 20 metrů vychýlení na přijímači asi 35cm. Při instalaci infrazávor umisťujeme čidlo do výšky 50 až 60 cm od podlahy, což umožní zachytit přikrčeného narušitele a zároveň zabrání náhodnému překročení. U oken nebo podobných průlezu by se pak mělo jednat o 25 až 30 cm od spodního kraje chráněného průlezu. Pokud budeme vytvářet infrabariéru, umisťujeme paprsky na vzdálenost asi 30 cm od sebe, přičemž závory nesmí být dosažitelné a viditelné z nechráněného prostoru. [5,12]

Nevýhodou těchto systémů je zejména náročnost montáže na přesnost. Optika nesmí být vystavena přímému slunečnímu záření. Je důležité brát zřetel na vlastnosti prostředí a nutnost dodržovat pravidla v chráněném režimu.

Výhodou je, že tyto systémy pracují na vlastní frekvenci a nemůže tak dojít k ovlivnění okolních systémů. Při správné instalaci je nelze obejít ani pomocí jiného vysílače. Při dodržování pravidel v chráněném prostoru je nemusíme vůbec vypínat a na rozdíl od jiných zabezpečovacích prvků není nutné mít chráněný průchod uzavřený. [5]

2.3.3 Prostorová ochrana

Prostorová ochrana má za cíl chránit vnitřní oblasti chráněného objektu a těžištěm její ochrany jsou takzvané klíčové body budovy (chodby, vstupy a schodiště). Předností je zejména nižší pořizovací cena a rychlá instalace.

2.3.3.1 Pohybová čidla

Pohybová čidla je dnes možné na trhu koupit nejen v základním provedení, ale i s celou řadou modifikací. Modifikovaná čidla pracují na stejném principu, ale jsou doplněna o přídavné funkce zpracování signálu. Vesměs se jedná o funkce, které mají zamezit planým poplachům, které způsobí okolní prostředí. Přídavné funkce z pravidla nepřináší při napadení objektu vyšší stupeň bezpečnosti.

Antimasking patří mezi nejdůležitější modifikace základního provedení čidla, kde zajišťuje ochranou proti zakrytí nebo přestříkání čidla. Jedná se o aktivní funkci zvyšující bezpečnost čidla. Tato funkce se používá zejména v místech, kde jsou očekávána vyšší bezpečnostní rizika. Přičemž antimasking pracuje i mimo dobu střežení, kdy vyvádí neustále informace o své činnosti a v případě napadení (například zakrytím čidla pevnou překážkou nebo přestříkání čidla sprejem) pošle zprávu o svém napadení - vyhlásí poplach. [5]

V současné době jsou používány nejčastěji dva principy funkce antimaskingu: Ten jednodušší princip je založen na infadiodě, která před sebe neustále vysílá paprsek. Odrazem paprsku od překážky získává přehled o okolí, a pokud paprsek není detekován přímo přijímací infradiodou je vše v pořádku, ale je-li odražen zpět, vyhlásí čidlo poplach. Druhým principem je vysílání mikrovlnného záření pracujícího stejným způsobem jako infračervené záření. [5,16]

VKV čidla jsou nejstarší pohybová čidla a pracují na frekvenci 420 MHz. Vyrábějí se, jako dělená (dnes se již nevyskytují) a monolitní. Monolitní čidla pracují na vzdálenost 15 metrů na principu Dopplerova efektu. [5,15]

Mikrovlnná čidla patří stejně jako VKV čidla ke starším konstrukcím a označujeme je jako MW. Na rozdíl o čidel VKV pracují na podstatně menším kmitočtu v řádech mikrovln. Mikrovlnná čidla jsou založena stejně jako VKV čidla na Dopplerově efektu, ale na rozdíl od VKV čidel má přijímač vyšší citlivost a vysílač snížený výkon na řády μW.

Toto opatření má za následek zhoršení průchodu vlnění přes zeď, které zlepšuje odolnost vůči planým poplachům. Mikrovlnná čísla se používají pro vysoká rizika a je jen velmi obtížné je překonat. [5,16]

VKV čidla a MW čidla instalujeme tak, aby rušení mimo střeženou zónu nebylo možné, protože reagují na každou změnu pohybujícího se předmětu v závislosti na vzdálenosti, rychlosti, velikosti a reflexi snímaného objektu. Čidla neinstalujeme do míst, kde jsou (tenké stěny, skla, sádrokartonové stěny a podobné materiály), protože vlnění přes tyto materiály snadno proniká. K dalším nebezpečím patří předměty kovové, které odrážejí vlnění a mohou ho šířit velmi daleko. Při použití více čidel v jedné místnosti, musíme dbát na to, aby pracovala na rozdílném kmitočtu, jinak se přístroje budou negativně ovlivňovat. [5,10]

Ultrazvuková čidla (US) stejně jako výše zmíněná čidla pracují na Dopplerově efektu. Jejich princip je založen na práci s ultrazvukovým polem v pásmu 20 kHz až 45 kHz, kde je pole generováno akustickým vysílačem. Vysílač je v podstatě reproduktor vysílající vlnění o stálém kmitočtu nad slyšitelnou úrovní a je li ve střeženém objektu klid, přijímá vlnu ve stejném formátu, jako byla vyslána z vysílače. Pokud tomu tak není, pak čidlo informuje o narušení. [5,2]

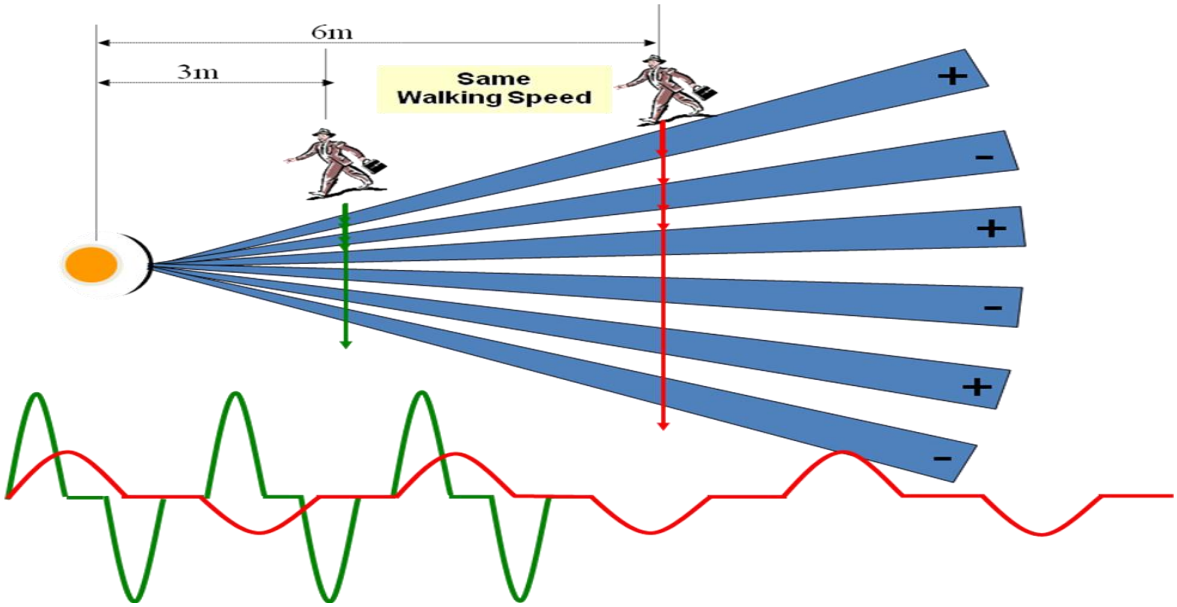
Při instalaci US čidel je dobré zohlednit tyto aspekty: Čidla instalujeme tak, aby předpokládaný pohyb pachatele směřoval k čidlu nebo od něj (čidlo nejcitlivější). Dbáme na dosah garantovaný výrobcem (mají velký útlum způsobený vzduchem). Odrazivost povrchu je lepší, čím je povrch hladší. Neinstalujeme je do větrných míst s velkým prouděním vzduchu (nepříznivě ovlivňuje vlnění a způsobuje nežádoucí plané poplachy). Vlnění nepronikne ani tkaninou proto musí mít dobrý výhled a nakonec neinstalujeme je do místností se zvířaty, která jsou citlivá na vysokofrekvenční zvuk, jako jsou třeba psy, [1,5]

Pasivní infračervéné čidlo je v současné době nejrozšířenější typ pohybových čidel a označujeme ho zkratkou PIR (Pasiv Infra Red detectors).

Výhody těchto čidel jsou: Snadná instalace, nízké nároky na servis a malá spotřeba energie (výhoda u bezdrátových zařízení). Dále jsou spolehlivé, odolné proti falešným poplachům a mohou být instalovány po skupinách v jedné místnosti (bez nutnosti nastavení zvláštního režimu).

Jako nevýhody můžeme brát: Možnost překonání některých jednodušších čidel (například těch bez antimaskingu). Dále je to náchylnost PIR čidel na okolní rušení (sluneční energie dopadající přímo na čočku detektorů nebo vlnící se záclony pohybující se po ohřátí od slunce) a v poslední řadě také proudění vzduchu (teplého nebo studeného), které může způsobit rychlou změnu teploty. Z výše zmíněných důvodů je jasné, že bychom neměli umísťovat PIR detektor naproti proskleným plochám [1,5,15]

PIR detektory fungují na principu detekce infračerveného záření, které vyzařuje narušitel. Tento princip operuje s tím, že každé těleso je zdrojem tepelného záření a leží v teplotách vyšších než absolutní nula a nižších než 560 ºC, kterému říkáme infračervené záření. Čím je teplota vyšší tím je i kratší frekvence, teplo se přibližuje k oblasti viditelného spektra, a protože infračervené záření vydávané živými organizmy má vysokou intenzitu v oblasti vlnových délek (8 μm až 10 μm), můžeme provádět detekci za pomocí pyroelementu. [5,15]



Obr. 4 Detekce pomocí PIR [12]

Jak jsme si již řekly tak součástka na principu *pyroelementu* je základním prvkem PIR čidla a připomíná fototranzistor s citlivostí posunutou do oblasti infračerveného záření. Musíme si uvědomit, že čidlo není citlivé jenom na délky v oblasti infračerveného záření, ale naopak je citlivé na zdroje tepla v celé škále vlnových délek. Z tohoto hlediska je největším znečišťovatelem slunce, které pokrývá všechny vlnové délky. PIR čidlo pracuje,

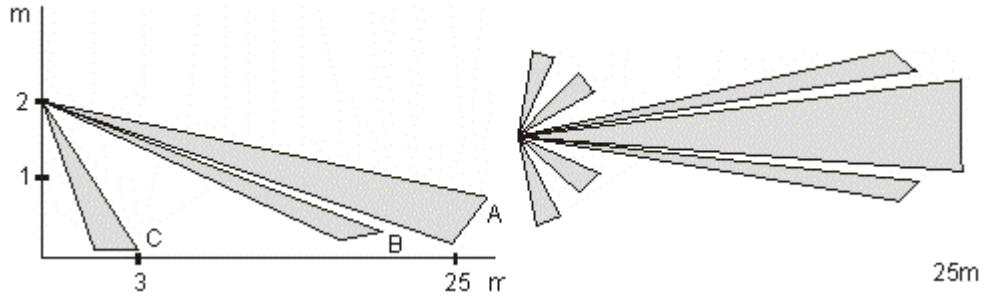
jako měnič gradientní povahy a nedetekuje tak stálou úroveň, ale jen změny dopadajícího záření. Pokud by na čidlo dopadalo záření z celého prostoru, došlo by při vstupu narušitele do oblasti jen k nepatrné a pomalé změně energie. Z těchto důvodů musíme prostor dělit pomocí speciální optiky. Jednoduchá čidla reagují na pohybující se zdroj záření stejně jako na stojící, který dostatečně rychle mění svoji teplotu. Proto kvalitní čidla používají dvě čidla integrovaná do jednoho pouzdra zapojeného do série s opačnou polarizací (obr. 4). [5,15]

V současné době se kromě PIR čidel začínají hojně vyskytovat i *aktivní infračervená čidla*. Jedná se o nejnovější verzi čidla představenou v roce 1994 a označujeme je ho zkratkou AIR. Pracují na principu vysílání kódovaných paprsků v pásmu 850 nm a následnému přijetí odrazu, po kterém je paprsek digitálně vyhodnocen. Rozdělení paprsku se provádí pomocí klasických čoček. Čidlo dokáže detekovat jak pohyb tělesa nevyzařující žádné teplo tak i pohyb libovolně pomalého tělesa. Dále čidlo umožňuje měnit detekční charakteristiku jednoduchým přeprogramováním a elevaci je možné nastavit v rozmezí 84º až 15º při dosahu čidla 12 metrů. Nevýhodou je (oproti PIR), že při instalaci více čidel do stejné místnosti je nutno použít synchronizační elektroniku, ale naproti tomu čidlo není ovlivněno žádným dalším vlivem okolí. Bohužel tyto čidla mají vyšší energetická spotřebu a také takzvaný mrtvý čas (doba, po kterou je čidlo zranitelné). Poslední nevýhodou je možnost detekce vyzařování a prostřednictvím toho detekovat mrtvé zóny detektoru. [5,9,10]

Optika u PIR a AIR čidla zaručuje rozdělení střeženého prostoru do zón a při výběru optiky bychom měli zohlednit vlastnosti chráněné oblasti. Optika totiž soustřeďuje příchozí záření z objektů na povrchu čidla, kde průchod narušitele přes signál procházející optikou má za následek silné kolísání energie dopadajícího na čidlo oproti klidovému stavu. Optika je na trhu dostupná v realizaci jako zrcadlová čočka nebo jako Fresnelova čočka. [5,12]

První realizací čoček je *zrcadlová optika*. Detekční charakteristika zrcadlové optiky je dána geometrii jednotlivých segmentů zrcadla a jeho rozložením. Výhodou oproti Fresnelovým čočkám je, že lze zajistit různou ohniskovou vzdálenost. U čidel se zrcadlovou čočkou je detekční charakteristika (vějíř, záclona nebo dlouhý dosah) dána již při výrobě a nelze jí měnit [5,12]

Druhá realizace je pomocí *Fresnelovy čočky.* Tato čočka využívá lom paprsků a má hned několik výhod: Jednoduchá výroba, nízká cena a snadná změna charakteristik čidla díky jednoduché výměně profilu čočky. Nevýhodou je naproti tomu nemožnost nastavení ohniskové vzdálenosti (detekční zóny nejsou přesně zaostřeny na čidlo), které má za následek pokles amplitudy. Z toho důvodu může pohyb malého živočicha blízko čidla vyvolat poplach, a proto se k zamezení tohoto jevu prostor rozčleňuje do několika samostatných horizontálních vrstev.[5]



Obr. 5 Realizace Fresnelových segmentů [12]

Kombinovaná čidla jsou čidla založená na předpokladu, že nedojde ke kombinaci dvou rozdílných fyzikálních jevů, které by zaznamenalo čidlo ve stejný okamžik. Tím je docíleno minimalizace planých poplachů. K detekci poplachu dojde jen za předpokladu, že je na vyhodnocovací elektroniku přiveden signál z obou částí čidla během definovaného času. Při instalaci tohoto typu musíme zohlednit pravidla platná pro instalaci obou součástí detektoru (v současné době se na trhu vyskytuje nejčastěji kombinace PIR–MW čidel). [9]

Tabulka 12 nám ukazuje citlivost různých druhů čidel v závislosti na zdroji rušení.

Zdroje planých poplachů	Typ čidla		
	PIR	MW	US
Proudění horkého vzduchu	Citlivé	Necitlivé	Citlivé
Chvění, vibrace, otřesy	Necitlivé	Citlivé	Citlivé
Světelné zdroje	Citlivé	Necitlivé	Necitlivé

Tab. 12 citlivost Pohybových čidel [5]

2.3.4 Předmětová ochrana

Hlavním cílem předmětové ochrany je ochrana jednotlivých předmětů před poškozením nebo odcizením. Jedná se tedy o skupinu čidel určených k přímé ochraně určených objektů (například, obrazy, sochy a trezory), kde předmětová ochrana doplňuje zabezpečení plášťové a prostorové. Obvykle jsou realizovány do samostatně ovládané skupiny (skupin), což umožňuje střežení těchto předmětů i v době zvýšeného provozu.

2.3.4.1 Kontaktní čidla

Aplikují se na nižší třídy chráněných předmětů. Jedná se zejména o *tlakové kontakty* - jsou založeny, na principu mikrospínačů popsaných výše s rozdílem, že klidový stav je způsoben trvalým stlačením, *tahové kontakty* - používají se dnes jen velmi málo a *Mikrospínače* - instalují se zejména za obrazy, princip byl popsán výše v kapitole plášťová ochrana.[5]

2.3.4.2 Kapacitní čidla

Kapacitní čidlo je konstruováno jako deskový kondenzátor, kde jednu elektrodu představuje kovová konstrukce chráněného předmětu (pokud chráněný předmět nemá kovovou součást, olepuje se tenkými kovovými pásky) a druhou vlastní čidlo. Výhodou je možnost nastavení citlivosti čidla. [5]

2.3.4.3 Bariérová čidla

Jak název napovídá tak tato čidla vyhlásí poplach v případě narušení bariery. Ta je tvořena buď pomocí infračervené závory založené na principu PIR čidla, anebo AIR čidla s charakteristikou čočky - záclona. Jejich funkci a použití jsem popsal již výše, a proto se zde budu zabývat jenom posledním typem bariérových čidel, což je čidlo laserové.

Laserová čidla mají funkci založenou na laseru o vlnové délce 780 nm, který vysílá v pravém úhlu do tenké nepřerušované roviny ve tvaru záclony, kde se odráží od reflexní pásky o šířce 25 a 50 mm, která je umístěná na konci střežené plochy. (Tuto plochu nelze nahradit žádným jiným odrazným materiálem). Aktivní plochu je možné seřizovat v rozsahu 0º až 180º a použití je tak velmi rozmanité (skříně na zbraně, sochy, malby a trezory). Čidlo detekuje poplach proniknutím jakéhokoliv předmětu skrz bariéru a teplota ani rychlost na detekci nemá žádný vliv. [5]

2.3.4.4 Trezorová čidla

K ochraně trezorů a trezorových místností se s úspěchem používají čidla seizmická, která mají schopnost rozpoznat všechny dnešní způsoby napadení trezoru. Jsou vybavena třemi nezávislými detekčními kanály a díky širokému spektru frekvenčních vln detekují všechny možné druhy nářadí. Jediným jejich nedostatkem je nemožnost detekce útoků založených na bázi kyselin. [2,5]

Pracují na principů vyhodnocování vibračních signálů přicházejících na čidlo, kde je signál následně porovnán s uloženými rozsahy a pokud se nějaký shoduje, vyhlásí se poplach. Čidlo je nastavitelné pro různé typy materiálů a instalace je prováděna na dveře trezoru z vnitřní strany tak aby nebyla přístupná z venkovního prostoru. [2,5]

2.3.4.5 Čidla na ochranu uměleckých předmětů

Tato kategorie čidel se používá na ochranu uměleckých předmětů na výstavách a galeriích, kde nemůže být instalován jiný systém EZS. (ten tam samozřejmě je, ale nemá dostatečnou odolnost proti sabotáži, proto se používají tyto speciální čidla).

Závěsová čidla. Předmět je zavěšen na tenkém nerezovém drátu, jehož čidlo umožňuje nastavovat maximální pohyblivost hlídaného objektu (rozsah použitelnosti je mezi 1 kg a 50 kg), kde poplach je způsoben sílou působící na senzor po překonání této maximální povolené pohyblivosti. [5]

Polohová čidla reagují na pokus o sejmutí obrazu, nebo vyříznutí plátna z rámu přičemž čidlo není vybaveno žádným sabotážním kontaktem, neboť při dobré instalaci zůstává čidlo skryto za obrazem. Výhodou je velikost čidla, které je velmi malé a nenápadné. [5]

Váhová čidla se používají ke střežení statických předmětů nejčastěji soch, kde jsou umísťovány pod střežený předmět. Po umístění střeženého předmětu si čidlo zaznamená jeho váhu a podle nastavené citlivosti je pak detekována odchylka (v horním i dolním rozpětí od původní váhy). Systém je nenáročný, stabilní, bezúdržbový a k ústředně se připojuje šesti-pramenným vodičem. V (tab. 13) je uvedena citlivost čidel pro různé hmotnosti. [5]

Citlivost čidla	Hmotnost předmětu
10 g	0,05 – 5 kg
40 g	0,2 – 20 kg
200 g	1 – 100 kg

Tab. 13 Citlivost váhových čidel

Tab. 13. [5]

2.4 Souhrn bezpečnostních rizik vybraných detektorů

Tato tabulka shrnuje možnosti nejčastěji používaných detektorů odolat vybraným druhům napadení. Typy napadení jsem vybral do tabulky s ohledem na nejčastější způsoby vyřazení prvků EZS z činnosti a s ohledem na jejich reálné použití při ochraně objektu (tab. 14).

Způsob napadení	Typ detektoru	Třída bezpečnosti			
		I.	II.	III.	IV.
Odolnost magnetickému poli	MK	S	O	O	N
	IR-MW,AIR, PIR	O	O	N	N
	DRS, INFRA, OT	N	N	N	N
Magnet od stejného zařízení	MK	S	S	S	O
Přemostění	MK	S	O	N	N
	PIR	S	O	N	N
	IR-MW, AIR	-	O	N	N
	DRS	O	O	O	O
	INFRA	O	O	O	N
Mechanické poškození	MK	S	O	O	O
	INFRA	S	S	O	O
	DRS, OT	O	N	N	N

	PIR,	S	O	O	N
	MW	O	O	N	N
	AIR	_	O	O	O
Vylomení střeženého objektu	MK	O	O	O	N
	OT	O	O	N	N
Proražení střeženého objektu	MK	S	S	S	S
	INFRA	S	S	S	S
	OT	O	N	N	N
Jen skleněné plochy	DTS	O	N	N	N
Pomalí pohyb a snížení siluety	PIR	O	O	N	N
	AIR	_	N	N	N
	MW	_	N	N	N
	IR-MW	_	_	N	N
Umělé snižování tělesné teploty	PIR	S	O	O	N
	AIR	_	N	N	N
	MW	O	N	N	N
	IR-MW	_	_	N	N
	INFRA	N	N	N	N
Zakrytí	PIR	S	S	O	N
	AIR	_	N	N	N
	MW, OT	O	O	N	N
	DTS	S	S	S	O
	IR-MW	_	_	N	N
	INFRA	S	O	N	N

Vyřazení napájení*	PIR, MW, IR-MW	O	O	N	N
	INFRA	O	O	O	O
	MK, OT, DTS	S	O	N	N
	AIR	_	O	N	N
Rušení přenosových pásem Wi.	Veškeré typy Wi.	S	S	S	O
Napadení přenosu cizí informací	Veškeré typy kabelové	O	O	N	N

Tab. 14 Odolnost prvků vůči napadení

*Jedná se o narušení hlavního zdroje i s vyřazením záložního akumulátoru. Zkratky: S-Snadné, O-obtížné, N-Nepravděpodobné, PIR-Pasivní infračervené čidlo, AIR-Aktivní infračervené čidlo, MK-Magnetický kontakt, INFRA-infračervené bariery, DTS-detektor tříštění skla, OT-otřesový detektor, IR-MW-kombinované čidlo mikrovlnné a infračervené, MW-mikrovlnné čidlo, Wi-Bezdrátový přenos.

Z porovnání je na první pohled patrné, že čím vyšší je třída bezpečnosti tím je i složitější překonání takovéhoto zabezpečovacího zařízení, ale zároveň také vidíme při porovnání s (tab. 15.), že vyšší bezpečnost přináší i větší investiční náklady na pořízení.

Z hlediska rozumné míry bezpečnosti se vzhledem i k ceně jeví jako nejvhodnější typ zabezpečovacího zařízení pohybový detektor PIR s drátovým připojením. Při kombinaci s magnetickým kontaktem a otřesovým detektorem dokáže při vhodném rozmístění vytvořit těžko překonatelnou bariéru. Pokud bychom však porovnávali kombinaci výše zmíněných detektorů se stejnou kombinací, provedenou pouze detektory na principu bezdrátového připojení. Dopadl by ve srovnání s metalicky připojenými detektory podstatně hůře. Bezdrátové detektory (kromě možnosti rychlé a snadné instalace) totiž přináší nižší stupeň bezpečnosti a navíc za podstatně vyšší pořizovací cenu. Z tohoto důvodu je třeba se vyvarovat tvorby výhradně bezdrátových EZS.

Typ detektoru	I.	II.	III.	IV.
PIR	N, S*	N, S*	S, V*	S, V*
AIR	_	V, V*	V, V*	V, V*
MK	N, N*	N, N*	S, S*	S, S*

OT	N, S*	N, S*	N, S*	S, V*
DTS	N, S*	N, S*	N, S*	S, V*
MW	_	S, S*	S, V*	V, V*
MW-IR	_	_	S, V*	S, V*
INFRA	S, S*	S, V*	V, V*	V, V*

Tab. 15 Porovnání cen

*-Bezdrátový přenos. N-nízká (Do 1000Kč), S-střední (1000Kč-3000Kč), V-vyšší (3000Kč a více Kč), PIR-Pasivní infračervené čidlo, AIR-Aktivní infračervené čidlo, MK-Magnetický kontakt, INFRA-infračervené bariery, DTS-detektor tříštění skla, OT-otřesový detektor, IR-MW-kombinované čidlo mikrovlnné a infračervené, MW-mikrovlnné čidlo, [11,12,13]

Celkově se dá konstatovat, že každý prvek EZS má své opodstatnění a využití. Při nákupu a instalaci EZS je proto třeba zohlednit množství hledisek (například odolnost, rychlost odezvy) pro výběr každého konkrétního typu a obzvláště pak je třeba se zaměřit na jeho silné a slabé stránky. Pokud na tyto hlediska budeme brát zřetel, můžeme dosáhnout velmi odolných a těžko překonatelných soustav EZS.

3 Praktický návrh

V tomto oddílu provedu srovnání dvou typových rodinných domů stejné stavební konstrukce vybavené EZS. První z domů má EZS z roku 1997 provedený pomocí kabelové (metalické) techniky zatímco druhy z případů má EZS z roku 2009, kde je připojení k ústředně provedeno pomocí bezdrátového připojení. Na obou případech se pokusím zjistit chyby, kterých se plánovač dopustil a ilustrovat možnosti jejich nápravy. Nákres a rozmístění je zobrazen pro oba domy na (obr. 6) první patro a (obr. 7) přízemí domu.

3.1 Bezpečnostní analýza objektů

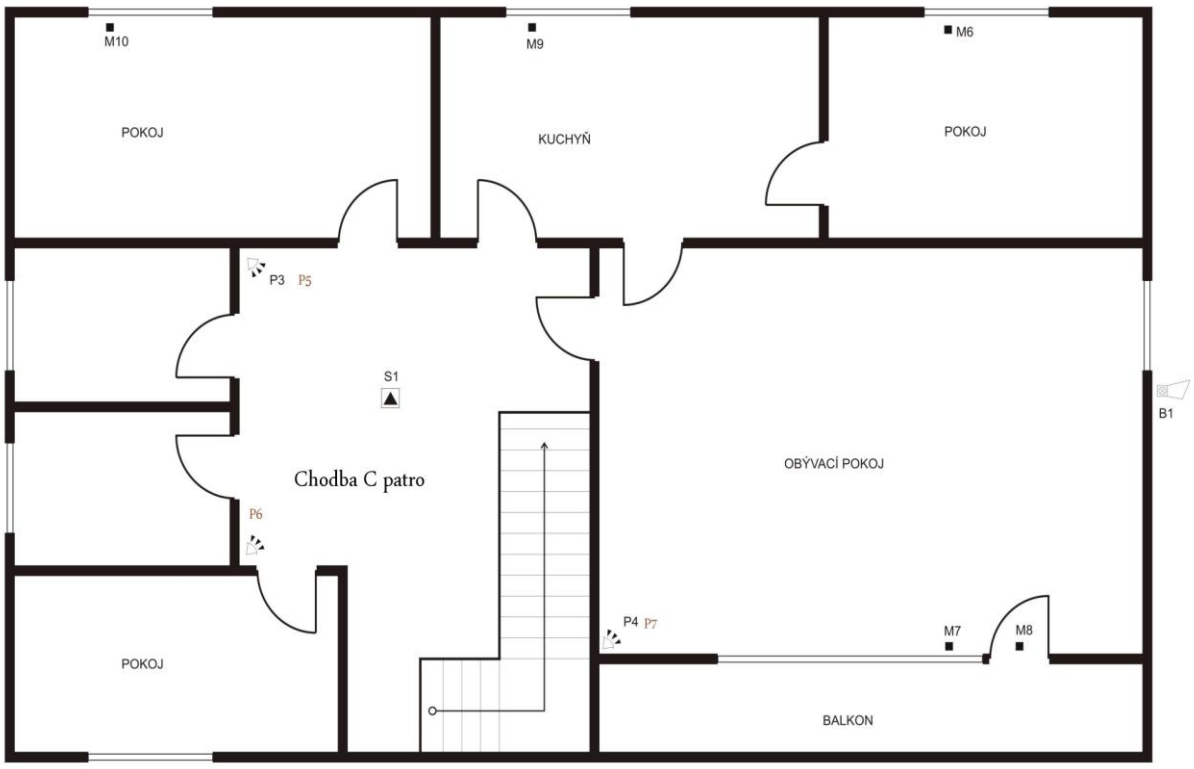
Cílem analýzy je posouzení účinnosti a efektivnosti použitých součástí EZS v objektu protože musíme zajistit, aby prostředky určené zadavatelem byly co nejlépe zúročeny.

3.1.1 Popis chráněného domu 1

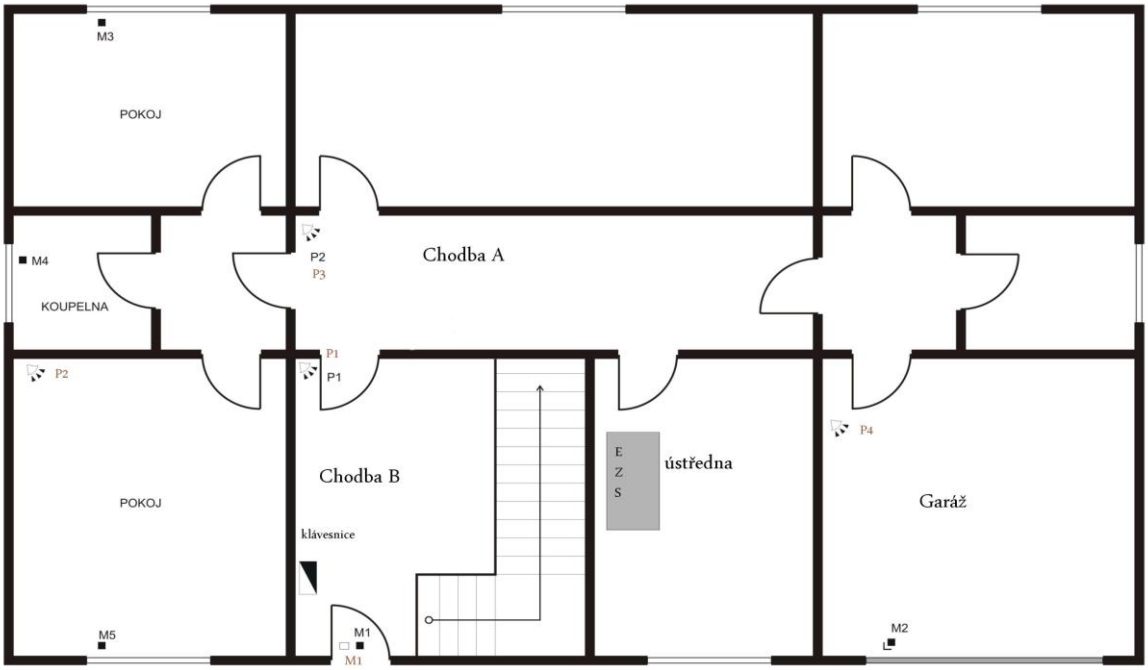
Rodinný domek je situován do klidné příměstské oblasti s nízkou kriminalitou. Je zasazen do zástavby rodinných domů, kde se obyvatele znají a mají přátelské vztahy. Domek byl postaven v polovině 80. let a EZS bylo instalováno v roce 1999. Rozvod je tvořen metalickými kabely vedenými skrze stěny, které jsou přivedeny na sběrnicovou ústřednu.

3.1.2 Popis chráněného domu 2

Tento rodinný domek byl stejně jako první rodinný dům postaven začátkem osmdesátých let ve stejném prostředí. Zadní malá přízemní okénka mají instalovanou ocelovou mříž a veškeré přízemní prostory domu jsou uzamykatelné. EZS zde byl instalován začátkem roku 2009. Vzhledem ke stáří domu se majitel rozhodl provést zabezpečovací systém výhradně pomocí bezdrátových zařízení, u kterých požadoval dva oddělené podsystémy - Jeden na zapnutí plášťové ochrany a druhý na pohybové detektory. Dalším přáním majitele byla instalace detektoru kouře v hlavní chodbě prvního patra.



Obr. 6 První Patro
černě označen dům 2 a hnědě dům 1, siréna společné



Obr. 7 Přízemí domu
černě označen dům 2 a hnědě dům 1, ústředna a klávesnice společné

3.2 Rozbor prvků EZS

V této kapitole si prohlédneme použité prvky v zabezpečení jednotlivých domů a popíšeme si jejich schopnosti a vlastnosti.

3.2.1 Rozbor prvků EZS domu 1

Zabezpečovací systém je vytvořen pomocí prvků kanadské společnosti DSC. Zabezpečovací zařízení bylo uvedeno do provozu roku 1999 a spadá do druhé bezpečnostní třídy.

3.2.1.1 Ústředna

Jako ústředna byla zvolena sběrnicová ústředna PC 1510 od společnosti DSC, kde délka kabelů může být maximálně 300 metrů. Ústředna není vybavena žádným rozšiřujícím modulem a k ovládání slouží jedna klávesnice typu PC 1500RK umístěná v zádveří domu. Ústředna umožňuje i připojení požárních detektorů, ale v našem případě není žádný takový detektor instalován. Samotný řídicí systém je umístěn v kovové krabici s pojistkami a záložní baterii. Systém umožňuje připojení detektorů na 6 sběrnic a vytvoření tak 6 nezávislých okruhů. Signalizace každé sběrnice je prováděna na klávesnici pomocí LED diody. Pokud chceme na sběrnici připojit více prvků ochrany, je pak tato signalizace pro všechny prvky společná. Ústřednu je možno programovat jak z klávesnice,

tak i pomocí softwaru přes PC, kde se propojení vytvoří přes simulátor telefonní linky nebo modemu. Ke vzdálené komunikaci může být použito připojení na PCO o rychlosti 20Bps, ale v našem případě není realizováno. Nesmíme také opomenout nastavení kódů, kde máme možnost kromě master kódu nastavit ještě šest dalších 4 místných kódů [11]

3.2.1.2 Ovládání

K ovládání je zde využita klávesnice PC 1500RK společnosti DSC. Jedná se o jednoduché zařízení bez nároku na uživatelské znalosti. Neobsahuj displeje a nepodporuje ani proximity klíčenky pro rychlou deaktivaci. Informace o připojených detektorech poskytují pouze LED diody signalizující stav v pořádku nebo porucha (narušení). Klávesnice umožňuje programování ústředny, to je bez podrobné znalosti systému a předchozí zkušenosti se systémem poměrně obtížné. Celkově je klávesnice jednoduchá, ale pro svůj účel dostačující. [11]

3.2.1.3 Magnetické kontakty

Jako jediný magnetický kontakt byl na dveře použit magnetický kontakt společnosti DSC POWER 700 bezpečnostní třídy II., který je připojen k ústředně přes ID linku a ta je přivedena přímo na sběrnici ústředny. Jeho pracovní mezera je 13 mm. [13]

3.2.1.4 Detektory pohybu

Jako detektor pohybu byl opět zvolen detektor od společnosti DSC, kde se konkrétně jedná o typ LC-100. LC 100 je PIR detektor s možností nastavení citlivosti čidla a spadá do bezpečnostní třídy II. Rozhled mu zajišťuje Fresnelova čočka dosahující do vzdálenosti 12 metrů. Detektory jsou v domě zapojeny buď samostatně, nebo po dvojicích na sběrnici ústředny, protože je ústředna limitována počtem šesti sběrnic. [13]

3.2.1.5 Siréna

Poplach je systémem vyhlášen pomocí venkovní sirény od společnosti Word Tech, která je umístěna na štítu hlídaného domu. Díky svému výkonnou (125dB) a kovovému boxu (dvojitý s kovovým krytem a majákem) se jedná o velmi účinný zdroj odstrašení pro potencionální pachatele. Siréna je napájena pomocí ID linky a záložní zdroj ji umožňuje funkci až po dobu 7 h při klidovém odběru 4 mA. [13]

3.2.2 Rozbor prvků EZS domu 2

Zde si popíšeme prvky od společnosti Risco použité k zabezpečení druhého domu. Bezpečnostní prvky byly voleny tak aby splňovali bezpečnostní třídu II.

3.2.2.1 Ústředna

Jako ústřednu jsme zde použili systém Agility spadající do druhé bezpečnostní třídy, která je vybavena IP, GSM/GPRS, PSTN, a hlasovým modulem. Ústředna nám umožňuje vytvoření 32 bezdrátových zón s 3 různými podsystémy. Tato ústředna je koncipována jako bezdrátová a principiálně se jedná o ústřednu realizovanou obousměrnou komunikací. Tato ústředna má paměť dostatečně velkou na 250 událostí a umožňuje skrytou komunikaci pomocí SMS nebo telefonního hlasového modulu. Hlasový modul nám umožňuje hovořit skrze reproduktor nebo naopak naslouchat okolí ústředny (to zajisté potěší podezřívavé partnery). Pro uživatele nabízí připojení třech klávesnic a nastavení 32 uživatelských kódů a osmi dálkových ovládání nebo klíčenek. K přednosti ústředny patří zejména její nízká váha a jednoduchá instalace prostřednictvím šroubů na zadní straně krytu. To nám umožnilo vybrat si umístění ústředny podle našich požadavků tak aby se dala oddělit od volně přístupných míst a zároveň nám byla snadno dosažitelná bez větších nároků na čas a práci. Ústřednu jsme nainstalovali v místnosti pod schodištěm, která je uzamykatelná. Vstupní dveře do místnosti s ústřednou jsou pod dozorem PIR čidla. Ústředna je umístěna na vlastním proudovém jističi, který slouží k zamezení možnosti zkratování ústředny prostřednictvím elektrické rozvodné sítě domu. Také samotná instalace prostřednictvím instalačního softwaru v přenosném počítači, s příjemným uživatelským rozhraním, proběhla po umístění všech součástí EZS snadno, (programování je možné provádět i prostřednictvím klávesnice), ústředna si veškeré prvky dokázala sama vyhledat a uživatel si již jen snadno navolil podsystémy a definoval jejich názvy.

3.2.2.2 Ovládání

K ovládání ústředny byla zvolena bezdrátová klávesnice systému Agility, která umožňuje plně ovládat a programovat ústřednu jednoduchými a přehlednými pokyny zobrazovanými na LCD displej. K příjemným vlastnostem klávesnice patří jednoduché získávání informací o systému zmáčknutím jedné klávesy a k jednoduchému ovládání přispívá i možnost přiřazování uživatelských kódů proximity klíčenkám (k rychlému odemykání a zamykání systému).

K dalším ovládacím prvkům patří obousměrný dálkový ovladač s jednoduchým zámkem kláves, kde zámek zabraňuje zneužití při ztrátě.

3.2.2.3 Magnetické kontakty

K zajištění plášťové ochrany jsou použity univerzální bezdrátové magnetické kontakty pro dveře a okna s 470K Ω rezistorem a dosahem 300 m ve volném prostranství. Kontakt má možnost nastavení (pomocí jednoduchých spínačů), citlivosti, rychlosti, a odezvy vysílače. Realizace umístění na okna byla řešena s požadavkem majitele na možnost otevírání ventilace oken při zapnutém systému a také s ohledem na nová umělohmotná okna (nemožnost vrtání). Kontakty byly umístěny do spodních rohů pomocí oboustranné vysoce odolné lepenky. K minimalizaci nákladů byl na dvoukřídlá okna použit vždy jeden magnetický kontakt, kde vysílač je umístěn na levém křídle a magnet na pravém. Vzdálenost mezi vysílačem a magnetem se blíží k maximální citlivosti kontaktu což u tohoto typu činní 15 mm.

K ochraně garážových vrat jsme použili vratový kontakt s mezerou detekce 65mm a kabelem chráněným ocelovými kruhy o délce 0,5m ten je následně připojen k vysílači univerzálního magnetického bezdrátového kontaktu. [12]

Díky těmto zařízením je provedena celková plášťová ochrana objektu, se zaměřením na vylomení dveří, vrat nebo oken.

3.2.2.4 Detektory pohybu

Jako detektor pohybu byl použit bezdrátový PIR detektor s ochranou proti zvířatům (PET) do váhy 36kg. Tento detektor pracuje pomocí obousměrné komunikace, která redukuje bezdrátové přetížení a pomocí které lze detektor vzdáleně ovládat a diagnostikovat. Rozsah střežené plochy je 15 x 15 m kde pokročilý procesor zpracování signálu zajistí kvalitní vyhodnocení přijímaného signálu ze střeženého prostoru. Umístění zadního sabotážního kontaktu nám umožnilo instalaci do rohu místnosti a díky snadné instalaci (pomocí závrtných šroubů), je možné později provést úpravy v umístění detektorů. [12]

3.2.2.5 Detektor kouře

Použit byl bezdrátový fotoelektrický snímač kouře, který funguje neustále a je nezávislý na poplachové ústředně. Stejně jako ostatní detektory má protisabotážní temper a

umožňuje testovací režim. Umístily jsme ho na strop na hlavní chodby, kde má za úkol chránit horní obývací pokoje. Do přízemí nebyl detektor instalován z důvodu občasného zatápění v kotli na uhlí. [12]

3.2.2.6 Siréna

Jedná se o obousměrnou plně bezdrátovou sirénu, která je plně napájená bateriemi, (5 x 3V Lithium baterie). Siréna je umístěna na štít domu a bez výsuvného žebříku je tak nedostupná. Směrována je do oblasti trvalého osídlení. [12]

3.3 Možnosti narušení a nápravy

Každá budova, i přes snahu zabezpečit jí co nejlépe, má svá slabá místa kterými lze systém obejít nebo poškodit tak, že je neschopen splnit své poslání.

3.3.1 Dům 1

Vchodové dveře do domu jsou z masivního dřeva ovšem s poměrně velkou skleněnou výplní. Z pohledu EZS jsou dveře zajištěny jednoduchým magnetickým kontaktem, který lze vyřadit libovolně silným magnetem. Následující vstupní prostor zádveří je zablokován PIR detektorem zaměřeným na vstupní dveře. Tato cesta je tedy dobře zabezpečena.

Další hrozbu představuje velké okno napravo ode dveří, to není vybaveno žádnou samostatnou ochranou a ochranu této místnosti má zajišťovat PIR detektor. Ten je možno spustit jen v případě, že zde není majitel (jedná se o místnost určenou ke spaní). Pokud je tedy majitel doma pak má narušitel volné pole působnosti ve spodní levé části budovy. Jako nápravu bych doporučil okno zabezpečit buď kombinací magnetického kontaktu s detektorem tříštění skla, nebo detektorem se záclonovou charakteristikou.

Hlavní chodba B (obr. 7) je chráněna PIR detektorem, ten je umístěn tak aby chránil chodbu od garáže a z místnosti vlevo je k němu při opatrnosti dobrý přístup a lze ho tak mechanicky vyřadit nebo zastínit jeho čočku (například sprejem). Při cestě do horního patra musí pachatel projít nejprve přes chodbu A (obr. 7). Chodba A je zabezpečena opět PIR detektorem, který je dostupný z chodby B a lze ho tedy snadno vyřadit. K nápravě nedostatků by majitel měl zvolit buď lepší umístění prvků EZS tak, aby

byli hůře dostupné, anebo systém doplnit o další ochranu tak aby se prvky navzájem chránily například dalším PIR detektorem.

Průchod do horního patra je zajištěn (chodba C obr. 6) dvěma PIR detektory s vzájemně se překrývajícími Fresnelovými poli a proto se tento průchod stává nemožný.

Vniknutí přes horní terasu do obývacího pokoje je možné přes velké balkónové dveře. Dveře nejsou vybaveny žádným magnetickým kontaktem a bezpečnost horního patra zajišťuje dvojice PIR detektorů. První se nachází v obývacím pokoji, ten je nasměrován na okna a byl důvodem častých planých poplachů z důvodu pohybu záclon a teplého vzduchu z topení. Proto byla jeho citlivost snížena. Případný pachatel by se mohl pokusit proplížit skrz obvodové stěny pokoje až k čidlu.

Tento dům má jednu velkou chybu, nenabízí majiteli téměř žádnou plášťovou ochranu, proto při užívání domu majitel nemůže využívat svůj systém nebo alespoň jeho části bez rizika spuštění planého poplachu. V praxi je tedy při pobytu majitele v budově zabezpečovací systém vypnut a dovoluje tak pachatelům volný pobyt po objektu. K nápravě tohoto hendikepu bych navrhl doplnit systém o prvky plášťové ochrany a rozdělit systém EZS do odpovídajících podsystémů, tak aby bylo možno zabezpečit dům i během pobytu majitele uvnitř. Prvky EZS v tomto domě jsou provedeny pomocí metalického kabelu se sběrnicovým adresováním, kde kabeláž je zabudována hluboko v omítce a pro osobu neznalou rozmístění je nemožné narušit rozvody a sabotovat tak přenosovou soustavu. Ústředna je umístěna na půdě budovy a je tak bez překonání PIR detektoru na chodbě C nedostupná. Bohužel vyvolání poplachu provádí ústředna pouze místně a to venkovní sirénou, což snižuje rychlost reakce při vloupání a nevylučuje to zde možnost, že se majitel o vloupání dozví až po příjezdu domu (s velkou časovou prodlevou). Pokud by potencionální pachatel umlčel sirénu ještě před započetím průniku, nemusel by se nijak znepokojovat zabezpečovacím systémem, který by nemohl nijak předat informaci o napadení.

Systém je celkově zaměřen na ochranu domu při nepřítomnosti majitele a k zajištění dobré funkce zde chybí kvalitní předání informace o narušení dále někomu, kdo by mohl upozornit bezpečnostní složky. Majitel by měl proto zvážit zakoupení alespoň GSM modulu nebo připojení na PCO. Bez těchto doplnění bude systém pouze

odstrašujícím prvkem bez celkové funkčnosti. Nezbytností se také jeví realizace (alespoň bezdrátově) plášťové ochrany pomocí magnetických kontaktů nebo detektorů tříštění skla.

3.3.2 Dům 2

Hlavním nebezpečím každého domu jsou vstupní dveře. Dveře jsou z masivního dřeva a jsou vybaveny magnetickým kontaktem s časováním a celé dveře pak snímá PIR detektor. Magnetický kontakt lze překonat magnetem o podobné intenzitě přiložený správným pólem do odpovídající vzdálenosti nebo vyříznutím otvoru do dveří, to je v zásadě dosti nepraktické. Uvažujeme li, že pachatel překonal magnetický kontakt, dostane se po otevření dveří přímo do zorného pole PIR detektoru v chodbě A (obr. 7.). Tato varianta průniku do domu bez vyhlášení poplachu není pravděpodobná.

Další variantou je průnik velkým oknem vpravo ode dveří. Okno je plastové, dvojité, vybavené magnetickým kontaktem bez časování. Pachatel zde může použít opět magnet, anebo jednoduše prorazí sklo okna, přes které se dostane do budovy bez vyhlášení poplachu. Zde bych doporučoval umístit detektor tříštění skla, neboť v této místnosti se spí a PIR detektor tu tedy není vhodný.

Chce li se pachatel dostat dále do horního patra, musí projít přes dvě spodní chodby A, B (obr. 7), kde každá z nich je chráněna PIR detektorem. V chodbě B je PIR detektor namířen směrem k průchodu do garáže a zabírá i částečně vstup z postraní místnosti. Přes tyto detektory se může pokusit pachatel projít pomalou přikrčenou chůzi anebo se může pokusit zakrýt čočku detektoru. Obě varianty narušení by odstranil detektor se záclonovou charakteristikou umístěny přímo nad průchod do chodby. Na chodbě A je detektor namířen na vstupní dveře a zabírá průchod z vedlejší chodby jen okrajově. Vzhledem k délce chodby, lze vyloučit, že by se pachatel proplížil a připadá zde v úvahu pouze možnost zakrytí, nebo mechanické sabotáže přímo na čidle.

Přístup do horní chodby C (obr. 6) přes schodiště je chráněn opět detektorem PIR. Detektor míří přímo na schodiště a neumožňuje tak pachateli se z prostor schodiště k němu přiblížit bez vyhlášení poplachu. K zvýšení bezpečnosti bych doporučil instalaci detektoru se záclonovou clonou nad schodiště tak, aby vytvořil přehradu pachateli postupujícímu ze spodního patra. Také je možno zvolit stropní PIR detektor s plošným pokrytím a tím zamezit přístupu přes schodiště. Průchod přes schodiště lze tedy také vyloučit.

Další variantou je vloupání přes balkonové dveře. Zde opět chybí ochrana proti proražení skla, kterou z části kompenzuje přítomnost detektoru PIR. Detektor zde vytváří clonu po celé šíři pokoje a blokuje pohyb pachatele po vyražení okna. Pachatel zde má jedinou možnost pokusit se zamaskovat svojí tepelnou stopu a snížit siluetu tak aby detektor předpokládal, že se jedná o zvíře.

Posledním nebezpečím je, že pachatel vyřadí ústřednu dříve, než vyhlásí poplach. V tomto případě, je ústředna umístěna do uzavřené vnitřní místnosti s jedním vchodem. Vchod je zabezpečen PIR detektorem, které ho má ve svém výhledu. Vyhlášení poplachu realizuje ústředna třemi způsoby: Vnitřní sirénou, venkovní sirénou a SMS zaslanou na tři čísla majitele domu. Venkovní siréna je namontována na cíp střechy a bez velmi dlouhého žebříku je nedostupná.

Koncepce tohoto domu má dvě zásadní chyby. Jedná se v první řadě o spoléhání v plášťové ochraně výhradně na magnetické kontakty, které sice dobře ochrání při otevření okna nebo dveří, ale při rozbití skla v oknech nemají žádnou účinnost a i obecně znalý člověk EZS dokáže magnetický kontakt vyřadit. Druhou a to fatální chybou se zde jeví provedení zabezpečovacího systému pouze pomocí bezdrátového provedení. Bezdrátový přenos lze poměrně snadno vyřadit z provozu rušičkou, kterou lze zakoupit za cenu pohybující se kolem třiceti tisíc korun. Systém má sice možnost reagovat změnou frekvence přenosového signálu, kterou však učiní, až po 15 minutách kdy se daný prvek nehlásí. Tento čas je pro pachatele dostačující k provedení loupeže a následnému odchodu bez vyhlášení poplachu. Z toho důvodu by měl majitel uvažovat o zařazení několika pohybových detektorů v kabelovém provedení a o jejich umístění na klíčová místa objektu.

Celkově se dá říci, že dům při plném střežení je poměrně dobře zabezpečen (mimo ochrany proti rušení přenosového pásma) a pachateli vytvoří účinnou překážku. Podíváme-li se pouze na plášťovou ochranu, tak v tomto případě by bylo záhodno ochranu doplnit (alespoň na místech předpokládaného narušení) detektory tříštění skla.

	Dům 1	Dům 2
Plášťová ochrana	Nedostačující	Dostačující
Pohybová ochrana	Dobré	Dobré

Bezpečnost přenosu dat	Dobré	Dostačující
Schopnost předání informace o poplachu	Dostačující	Dobré
Umístění ústředny	Velmi dobré	Velmi dobré
Účelnost rozmístění prvků	Dobré	Velmi dobré
Zajištění ochrany v přítomnosti majitele	Nedostačující	Dostačující
Zajištění ochrany v nepřítomnosti majitele	Dobré	Dobré
Celkové zhodnocení	Dostačující	Dobré-Dostačující

Tab. 16 Vyhodnocení návrhů obou domů

Známkovaní jako ve škole: 1-výborné, 2-velmi dobré, 3-dobré, 4-dostačující, 5-nedostačující.

Po celkovém zhodnocení základních aspektů obou EZS dojdeme k závěru, že bylo lépe provedeno zabezpečení domu číslo dvě.

Tento dům jsem si také vybral pro cenovou kalkulaci zabezpečovacího zařízení, kde budeme demonstrovat náklady na pořízení bezpečnostního zařízení od české společnosti Jablotron, která není sice nejlevnější a také nepatří k těm nejbezpečnějším. Vybral jsem ji hlavně z důvodu nejčastějšího využití na českém trhu a proto, že se prvky této společnosti nejčastěji objevují v sadách, které tuzemští prodejci nabízí zákazníkům.

Použitý komponent		Realizace v třídě II.	
Typ	Počet kusů	název	Cena za Ks
Ústředna	1 ks	JA 65K (Kombinovaný)	4000 Kč
PIR snímač	2 ks	JA 60P (Wi.)	1400 Kč
	2 ks	JS 20 LARGO	560 Kč
Magnetický kontakt	2 ks	SA 200	90 Kč
	5 ks	JA 81 M (Wi.)	1100 Kč
Siréna	1 ks	JA 80A (Wi)	3000 Kč

Klávesnice	1 ks	JA 63 F (Wi)	2050 Kč
Detektor kouře	1 ks	JA 63 S (Wi)	1200 Kč
Rozvody	30 m	SYKFY 2x2	18 Kč
Cena práce		3000Kč	
Celková cena		23390 Kč	

Tab. 17 Cenová kalkulace pro ilustrační dům

Z cenové kalkulace (Tab. 17) vyplívá, že zabezpečovací zařízení je v současné době ve finančních možnostech většiny z nás a nemělo by chybět v žádném nově stavěném domě, protože i cenově přijatelný zabezpečovací systém může náš majetek ochránit před nenechavými ručičkami zlodějů a co více může nám zachránit i život.

Závěr

Ze statistik policie ČR je jasně vidět stoupající majetková kriminalita v ČR a nejčastější způsoby průniků do domů a bytů. Proto jsem svoji práci zahájil rozborem prvků systému EZS včetně analýzy typu ústředen. Dále se pak se zabývám základním členění kategorii ochrany EZS, tak jak je definuje norma, a rozdělil jsem prvky EZS dle použití a tříd bezpečnosti. Popsal jsem důvody a metodiku napojení EZS na vyšší systém (například PCO).

Jelikož fyzikální principy, na kterých je funkce detektorů založena, je u všech výrobců shodná, neporovnával jsem detektory různých výrobců. Zaměřil jsem se především na principy funkce, nikoliv dodatečného vybavení. V práci jsem jasně definoval hlavní požadavky na součásti EZS, které na ně klade bezpečnostní třída, a přinesl jsem přehlednou tabulku odolnosti jednotlivých tříd detektorů proti základním typům napadení. Z toho se dá také určit, které zabezpečovací třídy jsou vhodné pro komerční použití a které zase k ochraně domácností.

Bezpečnostní systémy použité k zabezpečení komerčních objektů, kde se počítá se zvýšeným rizikem napadení, musí splňovat vyšší nároky na bezpečnost, a proto by se zde měli volit dražší ústředny spadající do bezpečnostní třídy III. a IV., které jsou nejčastěji realizovány jako stavebnicové. Hlavní prvek zde obvykle tvoří sběrnicová

ústředna, která je díky své odolnosti nejvhodnějším typem ústředny pro vysoká rizika. Takovouto ústřednou je například stavebnicová ústředna Dominius Millenium MU3, která spadá do bezpečnostní třídy III. a veze 4.0 je zařazena dokonce do nejpřísnější třídy IV. Realizace takového to integrovaného systému se pak stává otázkou mnoha set tisíc korun a u rozsáhlých zabezpečovacích systémů se může vyšplhat k částkám v řádech miliónů korun. Za tuto cenu dostane klient instalaci řešící napojení na další systémy vykonávající další činnosti, jako jsou výtahy, klimatizace a podobné informační systémy.

K domácímu použití nám dnes nabízí celá řada firem různé balíčky zabezpečovacích prvků v různém provedení, které nejčastěji spadají do II. zabezpečovací třídy. Ve většině případů nabízejí komplet tvořený třemi až čtyřmi zabezpečovacími prvky s bezdrátovým připojením na ústřednu do částky 15 000 Kč. Pořizovatel takového kompletu by si měl uvědomit, že bezpečnostní systém založený výhradně na bezdrátovém připojení je o mnoho zranitelnější než metalický systém jak ukazuji ve svém srovnání.

V poslední řadě by v žádném případě neměl podceňovat předávání informace o napadení třetí osobě (například pultu centralizované ochrany). V dnešní době se, ale PCO přestávají realizovat a dává se přednost přenosu přes GSM operátorů mobilních sítí. V tomto případě je potřeba důkladně zvážit komu bude informace o napadení předána a zda je ta osoba schopná zajistit adekvátní reakci. Rozdíl v realizaci předávání informace demonstruji v poslední kapitole na dvou koncepcích. První dům by měl být bezpečnější než dům druhý, neboť je koncipován po metalickém vedení. Jasně se ukazuje, že i když je výchozí metalická koncepce bezpečnější, tak při špatné koncepci a zejména zanedbání přenosu informace o napadení třetí osobě je možné systém EZS znehodnotit. Proto bych chtěl apelovat na každého, kdo si elektronický zabezpečovací systém pořizuje, aby si řádně promyslel, k jakému účelu mu bude sloužit a zda se mu nevyplatí investovat o něco málo větší částku do provedení. Zabezpečení objektu lze principiálně realizovat relativně levně a přitom spolehlivě. Klíčovým se mi však jeví především způsob a provedení práce včetně výběru vhodných prvků. Proto důrazně doporučuji svěřit odbornou instalaci koncesované firmě. Což má i velice pozitivní aspekt pro jednání s pojišťovnou.

Použitá Literatůra

[1] JELÍNEK, JOZEF: Jak zabezpečit byt, dům, chatu, automobil, Havlíčkův Brod, Grada Publishing, spol. s.r.o., 2000. ISBN: 80-7169-931-4

[2] BISCHOP, OWEN: Zabezpečovací zařízení vhodná i ke stavbě svépomocí, Ostrava, Nakladatelství HEL, 1993. brož

[3] BASTIAN, Hans-Werner: Bezpečný dům a byt, Jihlava, nakladatelství Dobrovský - BETA, 2004. ISBN: 80-7306-171-6

[4] Uhlář, JAN: Technická ochrana objektů I. díl, Praha, Vydavatelství PA ČR, 2004. ISBN: 80-7251-172-6

[5] Uhlář, JAN: Technická ochrana objektů II. díl, Praha, Vydavatelství PA ČR, 2005. ISBN: 80-7251-189-0

[6] Uhlář, JAN: Technická ochrana objektů III. díl, Praha, Vydavatelství PA ČR, 2006. ISBN: 80-7251-235-8

[7] Zahrádka, JÍŘÍ: Začínáme s EZS, Praha, Variant plus s.r.o., 2005. příručka

[8] BEBČÁK, PETR: Požárně bezpečnostní zařízení, Ostrava, SPBI, 2004. ISBN: 80-88634-34-5

[9] ČANDÍK, MAREK: Objektová bezpečnost II. díl, Zlín, UTB-Academia, 2004. ISBN: 80-7318-217-3

[10] LAUCKÝ, VLADIMÍR: Technologie komerční bezpečnosti I. díl, Zlín, UTB-Academia, 2003. ISBN: 80-7318-119-3

[11] KATALOG 1999. Řada klasických a multiplexních ústředen EZS pro komerční aplikace, DSC®

[12] KATALOG 2009-2010. Produktový katalog, Risco®

[13] KATALOG 2001. Řada detektorů pro komerční aplikace EZS, DSC®

WWW stránky

[14] Ing. Ivan Konečný, Ing. Jaroslav Tůma, Ing. Jan Bydžovský CSc.: Podnikové normy PN 50130-5, [cit. 2010-6-3].

Dostupný z URL: <http://www.jablotron.cz/cz/sekce/sluzby+a+informace/legislativa/>

[15] Ing. Ivan Konečný, Ing. Jaroslav Tůma, Ing. Jan Bydžovský CSc.: Podnikové normy PN 50131-1, [cit. 2010-8-3].

Dostupný z URL: http://www.jablotron.cz/cz/sekce/sluzby+a+informace/legislativa/

[16] Ing. Jiří Laifr, Miloš Říha, Zdeněk Juračka, Kateřina Bobková: Podnikové normy PN 50131-6, [cit. 2010-26-2].

Dostupný z URL: <http://www.jablotron.cz/cz/sekce/sluzby+a+informace/legislativa/>

[17] Ing. Milan Holas, Zdeněk Juračka: Podnikové normy PN 131-2-1, [cit. 2010-1-4].

Dostupný z URL: http://www.jablotron.cz/cz/sekce/sluzby+a+informace/legislativa/

[18] JABLOTRON, Současný stav norem na poplachové systémy v ČR [cit. 2010-16-3].

Dostupný z URL: <http://www.jablotron.cz/cz/sekce/sluzby+a+informace/legislativa/>

Seznam použitých zkratek:

EZS		Elektronické zabezpečovací systémy
PIR		Pasivní infračervené čidlo
AIR		Aktivní infračervené čidlo
MK		Magnetický kontakt
INFRA	-	Infračervená bariera
DTS		Detektor tříštění skla
OT		Otřesový detektor
IR-MW		Kombinované čidlo mikrovlnné a infračervené
MW		Mikrovlnné čidlo
Wi		Bezdrátový přenos

US	Ultrazvukové čidlo
ČSN	Česká technická norma
EN	Evropská norma

Seznam tabulek

Seznam použitých obrázků

Příloha

Příloha 1 Slovníček pojmů

- **Úroveň autorizace:** Každý bezpečnostní kód je v ústředně spojen s úrovní autorizace což znamená možnost zasahování a provádění změn na bezpečnostním systému a přístupu do něj v praxi to znamená, čím vyšší oprávnění tím větší možnosti daného systému jsou uživateli otevřeny.
- **Chime:** Jedná se o sérii tří krátkých tónů z klávesnice. Ta signalizuje narušení systému v době jeho deaktivace. Kupříkladu vchodové dveře do prodejny, při každém otevření dveří zazní z klávesnice trojí pípnutí. Poplachová zóna s vlastností „chime“ je definována v programování systému. Signalizaci mění uživatel dle vlastní potřeby.
- **Paměť událostí:** Zde jsou uloženy veškeré důležité informace o činnosti. Ukládají se zde poplachy, deaktivace a aktivace, poruchy to vše je možné zobrazit buď na LCD klávesnici, nebo stáhnout pomocí download do PC.
- **Vstupní / odchodové zpoždění:** Vlastnost sytému nastavit zpoždění různých zabezpečovacích zařízení bez vyhlášení poplachu, tedy s časovou prodlevou. Využívá se v případech, kdy je klávesnice nebo jiný obslužný prvek umístěn uvnitř střežených prostor.
- **Telefon „Následuj mne“:** Funkce umožňující přenášet uživatelem definovaná sdělení ústředny, poplachy, poruchy deaktivace, aktivace a podobné na telefonní přístroje zadané v ústředně pomocí sms, nebo namluveného vzkazu.
- **Skupina:** Skupina detektorů (zón) které se zapínají jedním tlačítkem. Každá zóna může být ve více skupinách.

- **Klíčový ovladač:** Ovládání (aktivace / deaktivace) bezpečnostního systému prostřednictvím elektrického kontaktu (například kontaktem v samostatném zámku). Alternativa ovládání systému z klávesnice.
- **Podsystém:** Skupina zón, kterou je možno samostatně ovládat a kde je možno
- volit přístupová práva pro jednotlivé uživatele. Příklad (Vnější opláštění domu zamkneme okna a vnitřní kdy zapneme pohybové detektory).
- **Proximity:** Jedná se o technologii, která bez použití klávesnice deaktivuje a aktivuje systém, je přiřazena k danému uživatelskému heslu. Jedná se buď o kartu, nebo klíčenku s dálkovým ovládáním.
- **Tamper:** Antisabotážní funkce bezpečnostního systému.
- **Chybové Hlášení:** Ústředna signalizuje veškeré poruchy na všech svých členech docházející baterie, otevřený kryt porušená kabeláž signalizuje jí na klávesnici a případně zasílá na PCO.
- **Upload/Download:** Program umožňující programování a správu systému z PC. Může být připojen kabele nebo pomocí telefonní linky.
- **Uživatelský kód:** Většinou 4 místné, někdy šesti místné, číslo, které uživateli zpřístupní ovládání bezpečnostního systému z klávesnice. Každý uživatel by měl mít přidělen individuální kód.
- **Programovatelný výstup:** Ústředna může být dovybavena množstvím programovatelných výstupů sloužících k připojení zařízení, nebezpečnostního charakteru jako je například poplachová siréna, spínání světel, ovládání topení, otevírání garážových vrat. Výstupy mohou být ovládány automaticky přes plánovač, nebo manuálně z klávesnice.
- **Plánovač:** Bezpečnostní systém je vybaven reálnými hodinami ty umožňují dopředu plánovat určité funkce jako rozsvěcování světel, deaktivace určených zón a podobně
- **Zóna:** Jeden nebo více detektorů, které jsou propojeny s jedním vstupem systému. Zóna je základním prvkem bezpečnostního systému. Pokud je na jedné zóně zapojeno více detektorů (zařízení), bezpečnostní systém je již nedokáže

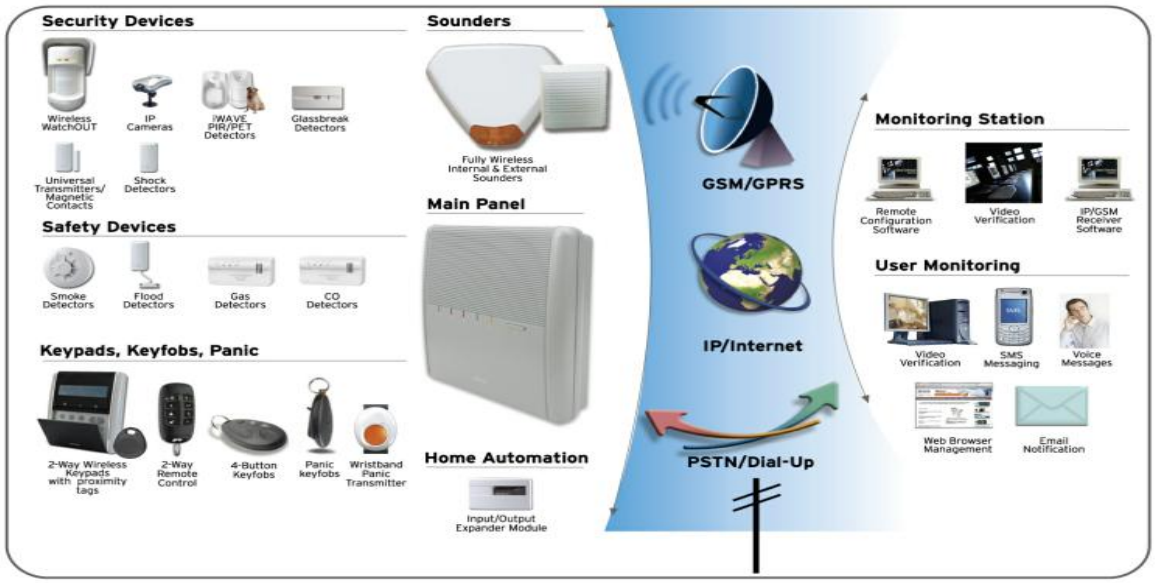
rozlišovat.Má-li zóna např. 5 detektorů, tak v případě poplachu nelze rozlišit, který z těchto detektorů poplach signalizoval.

- **Náhradní napájecí zdroj:***(alternative power source (APS)*)**:** napájecí zdroj energie, který je schopen napájet EZS po předem určenou dobu v případě výpadku základního napájecího zdroje.
- **Ochrana proti hlubokému vybití:** *(deep discharge protection)***:** ochrana, která zamezuje poškození záložního zdroje v případě, kdy míra jeho vybití je pod úrovní definovanou výrobcem ve specifikaci záložního zdroje.
- **Vnější zdroj energie:** *(external power source (EPS))***:** vnější napájení EZS*), které nemusí být nepřetržité, používané jako základní napájecí zdroj pro napájecí zdroj typu A a typu B.
- **Nezávislé napájecí výstupy:** *(independent power outputs)***:** napájecí zdroj, mající více než jeden výstup; každý výstup má svoji vlastní ochranu proti zkratu a přetížení (např. pojistky); každý výstup může mít několikanásobné svorky.
- **Nízké výstupní napětí:** *(low output voltage)***:** napětí nižší než je minimální napájecí výstupní napětí.
- **Nízké napětí záložního zdroje:** *(low voltage from storage device)***:** napětí specifikované výrobcem při kterém je záložní zdroj téměř vybit.
- **Maximální výstupní napětí:** *(maximum power output voltage)***:** maximální výstupní napětí napájecího zdroje specifikované výrobcem pro normální provozní stav.
- **Minimální výstupní napětí:** *(minimum power output voltage)***:** minimální výstupní napětí napájecího zdroje specifikované výrobcem pro normální provozní stav.
- **Normální provozní stav:** *(normal operative condition)***:** stav v rámci specifikace dané třídou prostředí, kdy je napájecí zdroj připojen podle předpisů výrobce; použitý napájecí zdroj a zatížení musí být v rozsahu specifikovaném výrobcem a kapacita záložního zdroje nesmí být nižší než 80%.
- **Přepěťová ochrana:** *(over-voltage protection)***:** ochrana napájecího zdroje případně připojených komponentů proti nadměrnému výstupnímu napětí, včetně napětí naprázdno

- **Výkonový výstup:** *(power output)***:** výstup napájecího zdroje, který dodává energii EZS
- **Napájecí jednotka:** *(power unit (PU))***:** zařízení, které poskytuje a také mění nebo odděluje (elektrickou) energii pro EZS nebo jeho komponenty a v případě potřeby také pro záložní zdroj.

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

Příloha 2 Příslušenství pro systém Agility [12]



Příloha 3 Vnitřní uspořádání ústředny Agility

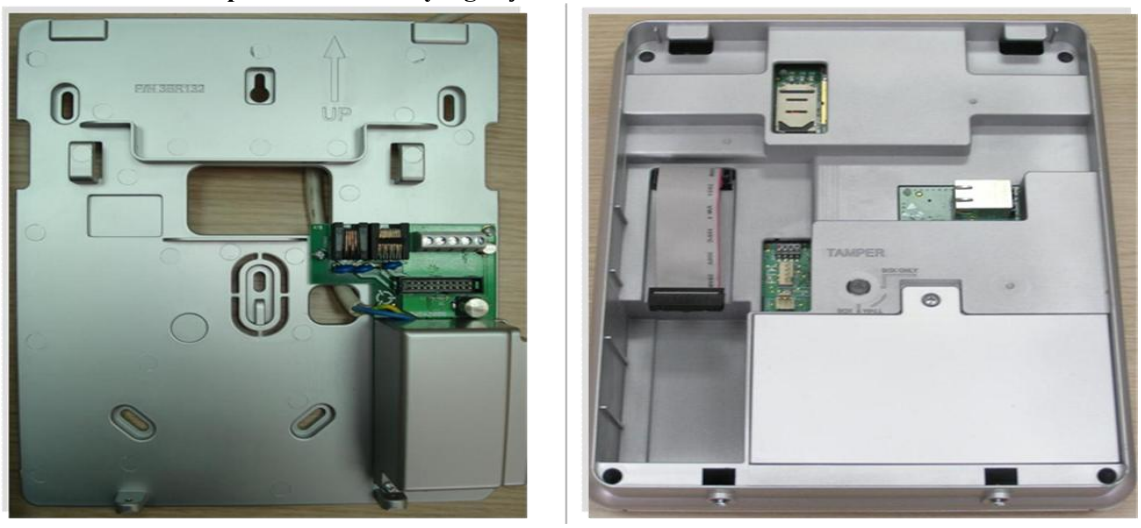


Foto autor

Příloha 4 Možné provedení sestavy pro rozsáhle EZS [13]