

**JIHOČESKÁ UNIVERZITA**  
v Českých Budějovicích

**Pedagogická fakulta**

Katedra fyziky

**Systemy elektrické zabezpečovací signalizace**

Bakalářská práce

Knihovna JU - PF



3 1 1 5 1 7 1 7 0 4

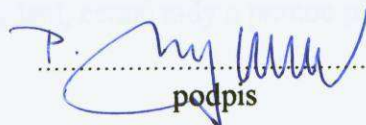
**Petr Maryška**

Vedoucí práce: Doc. PaedDr. Petr Adámek, Ph.D.

České Budějovice 2005

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně na základě uvedené literatury.

V Jindřichově Hradci 1.12.2005

  
.....  
podpis

199	Kořisťové plodiny	21
204	Isoprenylní terpeny	21
209	Ornithin	21
214	Ornithin	21
215	Ornithin	21
216	Ornithin	21
217	Ornithin	21
218	Ornithin	21
219	Ornithin	21
220	Ornithin	21
221	Ornithin	21
222	Ornithin	21
223	Ornithin	21
224	Ornithin	21
225	Ornithin	21
226	Ornithin	21
227	Ornithin	21
228	Ornithin	21
229	Ornithin	21
230	Ornithin	21
231	Ornithin	21
232	Ornithin	21
233	Ornithin	21
234	Ornithin	21
235	Ornithin	21
236	Ornithin	21
237	Ornithin	21
238	Ornithin	21
239	Ornithin	21
240	Ornithin	21
241	Ornithin	21
242	Ornithin	21
243	Ornithin	21
244	Ornithin	21
245	Ornithin	21
246	Ornithin	21
247	Ornithin	21
248	Ornithin	21
249	Ornithin	21
250	Ornithin	21
251	Ornithin	21
252	Ornithin	21
253	Ornithin	21
254	Ornithin	21
255	Ornithin	21
256	Ornithin	21
257	Ornithin	21
258	Ornithin	21
259	Ornithin	21
260	Ornithin	21
261	Ornithin	21
262	Ornithin	21
263	Ornithin	21
264	Ornithin	21
265	Ornithin	21
266	Ornithin	21
267	Ornithin	21
268	Ornithin	21
269	Ornithin	21
270	Ornithin	21
271	Ornithin	21
272	Ornithin	21
273	Ornithin	21
274	Ornithin	21
275	Ornithin	21
276	Ornithin	21
277	Ornithin	21
278	Ornithin	21
279	Ornithin	21
280	Ornithin	21
281	Ornithin	21
282	Ornithin	21
283	Ornithin	21
284	Ornithin	21
285	Ornithin	21
286	Ornithin	21
287	Ornithin	21
288	Ornithin	21
289	Ornithin	21
290	Ornithin	21
291	Ornithin	21
292	Ornithin	21
293	Ornithin	21
294	Ornithin	21
295	Ornithin	21
296	Ornithin	21
297	Ornithin	21
298	Ornithin	21
299	Ornithin	21
300	Ornithin	21
301	Ornithin	21
302	Ornithin	21
303	Ornithin	21
304	Ornithin	21
305	Ornithin	21
306	Ornithin	21
307	Ornithin	21
308	Ornithin	21
309	Ornithin	21
310	Ornithin	21
311	Ornithin	21
312	Ornithin	21
313	Ornithin	21
314	Ornithin	21
315	Ornithin	21
316	Ornithin	21
317	Ornithin	21
318	Ornithin	21
319	Ornithin	21
320	Ornithin	21
321	Ornithin	21
322	Ornithin	21
323	Ornithin	21
324	Ornithin	21
325	Ornithin	21
326	Ornithin	21
327	Ornithin	21
328	Ornithin	21
329	Ornithin	21
330	Ornithin	21
331	Ornithin	21
332	Ornithin	21
333	Ornithin	21
334	Ornithin	21
335	Ornithin	21
336	Ornithin	21
337	Ornithin	21
338	Ornithin	21
339	Ornithin	21
340	Ornithin	21
341	Ornithin	21
342	Ornithin	21
343	Ornithin	21
344	Ornithin	21
345	Ornithin	21
346	Ornithin	21
347	Ornithin	21
348	Ornithin	21
349	Ornithin	21
350	Ornithin	21
351	Ornithin	21
352	Ornithin	21
353	Ornithin	21
354	Ornithin	21
355	Ornithin	21
356	Ornithin	21
357	Ornithin	21
358	Ornithin	21
359	Ornithin	21
360	Ornithin	21
361	Ornithin	21
362	Ornithin	21
363	Ornithin	21
364	Ornithin	21
365	Ornithin	21
366	Ornithin	21
367	Ornithin	21
368	Ornithin	21
369	Ornithin	21
370	Ornithin	21
371	Ornithin	21
372	Ornithin	21
373	Ornithin	21
374	Ornithin	21
375	Ornithin	21
376	Ornithin	21
377	Ornithin	21
378	Ornithin	21
379	Ornithin	21
380	Ornithin	21
381	Ornithin	21
382	Ornithin	21
383	Ornithin	21
384	Ornithin	21
385	Ornithin	21
386	Ornithin	21
387	Ornithin	21
388	Ornithin	21
389	Ornithin	21
390	Ornithin	21
391	Ornithin	21
392	Ornithin	21
393	Ornithin	21
394	Ornithin	21
395	Ornithin	21
396	Ornithin	21
397	Ornithin	21
398	Ornithin	21
399	Ornithin	21
400	Ornithin	21

Děkuji Doc.PaeDr.Petru Adámkovi, Ph.D. za odborné vedení, cenné rady a pomoc při zpracování bakalářské práce.

2.8.3	Kódové klávesnice.....	42
2.8.4	Kombinované indikační a ovládací díly.....	42
2.8.5	Ovládání kartou.....	42
<b>2.9</b>	<b>Doplňková zařízení ústředěn EZS.....</b>	<b>42</b>
2.9.1	Akustická signalizace.....	42
2.9.2	Optická signalizace.....	43
2.9.3	Grafická tabla.....	44
2.9.4	Tiskárny.....	44
2.9.5	Poplachová přenosová zařízení (komunikátory).....	44
2.9.6	Zařízení určená pro informování majitele objektu.....	44
2.9.7	Zařízení určená pro komunikaci s PCO/PPC.....	45
<b>3.</b>	<b>Elektronická zabezpečovací signalizace pro motorová vozidla.....</b>	<b>46</b>
<b>3.1</b>	<b>Systémy EZS pro motorová vozidla.....</b>	<b>46</b>
<b>3.2</b>	<b>Čidla.....</b>	<b>46</b>
3.2.1	Čidla obvodové ochrany.....	46
3.2.1.1	Kontaktní čidla.....	46
3.2.2.	Čidla prostorové ochrany.....	46
3.2.2.1	Ultrazvuková čidla.....	46
3.2.2.2	Mikrovlnná čidla.....	47
3.2.3	Ostatní čidla.....	47
3.2.3.1	Otřesová a náklonová čidla.....	47
3.2.3.2	Čidla rozbití skla.....	47
<b>3.3</b>	<b>Řídící jednotky.....</b>	<b>47</b>
<b>3.4</b>	<b>Ovládací prvky.....</b>	<b>48</b>
<b>3.5</b>	<b>Signalizační zařízení.....</b>	<b>48</b>
3.5.1	Lokální signalizace.....	48
3.5.2	Dálková signalizace.....	49
<b>3.6</b>	<b>Systémy zabráňující nastartování vozidla - imobilizéry.....</b>	<b>49</b>
<b>3.7</b>	<b>Systémy umožňující vyhledání vozidla.....</b>	<b>50</b>
3.7.1	Systémy lokalizace polohy vozidla pomocí rádiové sítě.....	51
3.7.2	Systémy lokalizace polohy vozidla na principu GSM.....	51
3.7.3	Systémy lokalizace polohy vozidla na principu GPS.....	51
3.7.4	Přenos dat.....	51
<b>4.</b>	<b>Závěr.....</b>	<b>52</b>
	<b>Seznam použité literatury.....</b>	<b>54</b>



# Obsah

Úvod.....	5
1. Definice a zkratky.....	10
2. Elektrické zabezpečovací systémy (EZS).....	14
2.1 Rozdělení prvků EZS.....	14
2.2 Prvky plášťové ochrany.....	16
2.2.1 Magnetické kontakty.....	16
2.2.2 Čidla na ochranu skleněných ploch.....	17
2.2.3 Mechanické kontakty.....	19
2.2.4 Vibrační čidla.....	19
2.2.5 Poplachové fólie, tapety, polepy a poplachová skla.....	19
2.2.6 Drátová čidla.....	19
2.2.7 Rozpěrné tyče.....	19
2.3 Prvky prostorové ochrany.....	20
2.3.1 Pasivní infračervená čidla.....	21
2.3.2 Ultrazvuková čidla.....	23
2.3.3 Mikrovlnná čidla.....	24
2.3.4 Kombinovaná (duální) čidla.....	24
2.4 Prvky tísňového hlášení.....	24
2.4.1 Veřejné tísňové hlásiče.....	25
2.4.2 Speciální tísňové hlásiče.....	25
2.4.3 Automatické tísňové hlásiče.....	25
2.4.4 Osobní tísňové hlásiče.....	26
2.5 Prvky předmětové ochrany.....	27
2.5.1 Otřesová (seismická) čidla.....	27
2.5.2 Čidla na ochranu uměleckých předmětů.....	27
2.5.3 Kapacitní čidla.....	28
2.6 Prvky venkovní obvodové (perimetrické) ochrany.....	29
2.6.1 Mikrofonické kabely.....	29
2.6.2 Infračervené závory a bariéry.....	30
2.6.3 Mikrovlnné bariéry.....	30
2.6.4 Štěrbínové kabely.....	31
2.6.5 Zemní tlakové hadice.....	31
2.6.6 Perimetrická pasivní infračervená čidla (infrateleskopy).....	32
2.6.7 Další systémy venkovního zabezpečení.....	32
2.7 Ústředny EZS.....	33
2.7.1 Smyčková ústředna.....	33
2.7.2 Ústředna s přímou adresací čidel.....	34
2.7.3 Ústředna smíšeného typu.....	34
2.7.4 Ústředny s bezdrátovým přenosem od čidel.....	35
2.7.4.1 Systémy s jednosměrnou komunikací.....	35
2.7.4.2 Systémy s obousměrnou komunikací.....	36
2.7.4.3 Kódování přenosu a prvků.....	36
2.7.5 Vstupní vyhodnocovací obvody.....	37
2.7.6 Výstupní obvody.....	38
2.7.7 Napájecí obvody.....	39
2.8 Ovládací a indikační zařízení.....	40
2.8.1 Blokovací zámek.....	41
2.8.2 Spínací zámek.....	41



## Úvod

Každý z nás, když se rozhlédne kolem okolo sebe, první co spatří je majetek. Majetek je prostě všude kolem nás. Každý někomu patří. Některý je osobním vlastnictvím, jiný patří firmám, různým spolkům, obcím, městům či státu. Každý má svou hodnotu, svou cenu. Nemusí jít pouze o peníze, cennosti nebo hmotné věci, může jít také o myšlenky či nápady.

Majetek lze poškodit, odcizit nebo zneužít. Vždy vzniká nějaká škoda a proto je třeba si majetek chránit.

Ochrana majetku je stará jako lidstvo samo. Stavby hradeb, příkopů nebo plotů kolem osad, byly v podstatě zřizováním mechanických zábranných systémů sloužících k ochraně proti napadení nepřítelem a k zabezpečení života a majetku obyvatel.

Jak se lidstvo rozvíjelo, vznikala třídní společnost, rostla potřeba ochrany majetku a začaly vznikat první uzamykací systémy (zámky).

S potřebou ochrany majetku před nebezpečím byla spojena i potřeba toto nebezpečí signalizovat. Nebezpečí nepřicházelo jen od nepřátel, ale také od přírodních sil (potopa, požár..).

S rozvojem civilizace se vyvíjely i systémy vyhlašování poplachu. Ale ať už využívali křiku, bubnování, troubení či zvonění, vždy se jednalo o výhradně lidskou činnost - snad s výjimkou hlídacích psů.

Zásadní přelom v přenosu informací na dálku představoval vynález telegrafu v roce 1835 a jeho první reálná aplikace v roce 1844 (linka Washington - Baltimore). Poprvé byl v systémech pro signalizaci nebezpečí použit v roce 1847 kdy hlavní inženýr města New York Cornelius Anderson propojil požární hlásky telegrafem s centrálním stanovištěm, které bylo dále propojeno s jednotlivými požárními stanicemi. Došlo tak k nebyvalému zkrácení doby potřebné k přenosu poplachového signálu od místa ohrožení k „zámkové skupině“ - tedy na nejbližší požární stanici.

Dalším krokem k prvním „elektrickým zabezpečovacím signalizacím“ tak, jak je chápeme dnes, bylo technické vylepšení systému centralizace hlášení pomocí tzv. „volací skřínky“ - dnes bychom řekli veřejného hlásiče. Při zatažení za páku hlásiče se roztočilo vroubkované kolo a prostřednictvím elektrického kontaktu vyslalo sérii teček a čárek, ve kterých byl obsažen jeho individuální kód. Na centrálním pultu pak primitivní zapisovač zaznamenal zmíněnou sérii a vytvořil tak záznam o poplachu. Systém byl schválen v Bostonu (stát Massachusetts) v roce 1851 a v roce 1854 ve městě fungovalo



již 42 takových hlásičů. Zajímavé je, že v podstatě stejný systém byl vybudován v Hamburku koncem 19. století a vydržel ve službě až do roku 1976.

První známý elektrický zabezpečovací systém, podstatně vylepšující předchozí ryze mechanickou kombinaci nástražného drátu a pastičky na myši, si nechal patentovat v roce 1853 pan Augustus Pope ze Sommerville (opět stát Massachusetts). Používal kombinaci kontaktů instalovaných na dveřích a oknech s baterií a zvonkem. Svůj patent v roce 1857 prodal Edwinovi T. Holmesovi, novoanglickému obchodníkovi s galanterií a šicími potřebami a výrobcí krinolín.

Edwin T. Holmes tak jako všichni průkopníci to neměl jednoduché - i když už se začínala vyrábět elektrická zařízení, v té době ještě neexistovali dodavatelé elektrických drátů a příslušenství. Naštěstí pár kroků od jeho bostonského obchodu sídlil první elektrikářský obchod v zemi - Hinds & Williams. Holmes se spřátelil s Williamsem, který pro něho začal vyrábět zvonky a kontakty. Musel také začít vyrábět izolované dráty, přičemž využil své zkušenosti z výroby krinolín, vymyslel mnoho dalších základních elektrických součástek, které si patentoval a později se staly základem telefonních systémů. Elektrická zabezpečovací signalizace na světě vznikla dvacet let před telefonem a čtvrt století před žárovkou. Nebylo to snadné - nikdo nechtěl v té době věřit, že při otevření okna v přízemí může začít zvonit zvonek v patře. Holmes se tedy přesunul do New Yorku, kde byl potenciální trh přece jen perspektivnější než v tehdejší Bostonu, vyrobil model domu s fungujícím poplašným zařízením a objížděl nejbohatší obyvatele Manhattanu. Uspěl a za vydělané peníze vylepšoval svůj systém - v krátké době byl schopen pomocí barevných klapek vytvořit „adresný“ systém indikující stav každého zabezpečeného okna nebo dveří. Přidáním hodin systém „programoval“ na zapínání a vypínání ve stanovenou dobu a později i na ovládání domovního osvětlení.

Holmes samozřejmě využil již známé myšlenky centralizovaných pultů a v roce 1858 uvedl do provozu první centrály elektrické ochrany v Bostonu a v New Yorku, které brzy sloužily jako působivý seznam prominentních zákazníků - Bowery Bank, Montreal Bank, Equitable Life, Phelps Dodge & Comp., John Jacob Astor, Tiffany a spousta dalších. Roku 1872 Holmes vyvinul „elektrický sekretář“ pro ukládání klenotů - úložní objekt se stěnami propletenými průběžnou vodivou fólií a s dveřmi opatřenými kontakty, připojený na centrální stanoviště se 24hodinovou službou schopnou kdykoli zakročit.

Když Graham Bell v roce 1873 přemýšlel, kde vyzkoušet svoji myšlenku přenosu lidského hlasu na velkou vzdálenost, přišel za Edwinem Holmesem. Na stávající síti objektových zabezpečovacích linek si ověřil její reálnost a v roce 1876 ohlásil vynález



telefonu. Demonstrace byly tak úspěšné, že E. T. Holmes byl požádán o vybudování první komerční telefonní ústředny, kterou dokončil v New Yorku v roce 1877 Holmes Central Station se stala první telefonní ústřednou a současně prvním účastníkem Holmes byl prvním prezidentem Bell Telephone Company a jedním z prvních ředitelů Bell Telephone Association, předchůdcem známé ATT (American Telephone and Telegraph Comp.)

Po dlouhá desetiletí byla elektrická zabezpečovací signalizace ryze kontaktní záležitostí. Používaly se různé druhy spínacích a rozpínacích kontaktů. Často ve spojení s destrukčními čidly, což byly vlastně pevně zabudované vodiče, které byly při pokusu o proražení překážky přerušeny. Zřejmě teprve začátkem 20. století se objevují elektromechanická čidla založená na principu setrvačnosti, případně kyvadla. Jsou to speciální kyvadlová čidla pro ochranu trezorových místností, nejrůznější typy vibračních kontaktů, používaných až do začátku 80. let, a inerciální senzory, používané občas i v současných zařízeních pro ochranu vozidel (reagují na jejich rozhoupání).

Zabezpečovací ústředny byly až do 50. let 20. století zásadně reléovou záležitostí. S objevem polarizovaného relé, které umožnilo používání vyvážených smyček, podstatně narostla odolnost zabezpečovacích systémů. Pro signalizaci se používaly převážně zvonky, což přetrvalo dodnes zejména v anglosaských zemích.

Teprve rozvoj elektroniky za druhé světové války a po ní, zejména pak průmyslová výroba tranzistorů a následná miniaturizace elektronických zařízení, umožnila vznik nových druhů čidel. Následně pak i jejich elektronizaci a posléze i komputelizaci. Právě výpočetní technika dosáhla v poslední době úrovně dovolující technickými prostředky nahrazovat některé činnosti, které dosud bylo možné zajišťovat výlučně lidskou silou (tedy vnímáním a myšlením). A tak po téměř třicetileté přestávce se opět objevují v zabezpečovací technice skutečně nové prostředky a z nich vyplývající možnosti. Postupné vnitro společenské změny v demokratických zemích měly za následek decentralizaci bezpečnostních činností, což znamenalo další rozvoj pultů centralizované ochrany a s tím souvisejících bezpečnostních služeb, a na rozdíl od systémů požární ochrany, vázaných na požární sbory, výraznou komercionalizaci této oblasti.

V padesátých letech 20. století se objevují elektronická čidla. Jsou to zejména tzv. trezorové kontakty - akustické snímače připevňované na chráněný objekt (stěnu trezorové skříně nebo komory) a vyhodnocující hluky šířící se materiálem. Vzhledem k jednoduché pásmové filtraci snímaných akustických frekvencí byly dost náchylné k



planým signalizacím způsobovaným přenosem chvění z jiných konstrukčních struktur (topení, vodovody, armatury atp.). Dále se jednalo o kapacitní čidla vyhodnocující kapacitu chráněného objektu proti zemi. Tato zařízení již byla značně spolehlivá a vysoce účinná, vyžadovala však (a dodnes vyžaduje) velmi pečlivou přípravu a montáž. Konečně šlo o první aktivní prostorová čidla na principu vyhodnocování a principu šíření ultrazvuku v uzavřeném prostoru. Jejich klíčovým problémem však byla stabilizace vysílaného kmitočtu. V této době začínají také být postupně vytlačovány mechanické kontakty magnetickými snímači s jazýčkovým kontaktem.

V šedesátých letech se zvyšující se úrovní polovodičových součástek mohla přijít prostorová čidla využívající principu velmi krátkých vln. Chráněný prostor byl pomocí těchto čidel pokryt nemodulovaným signálem o frekvenci řádu stovek Mhz. Poplachový stav byl vyhodnocován změnou elektromagnetického pole. Ve své době doznaly značného rozšíření. Vyráběly se v různých provedeních, jako jedno i víceanténová. Jejich hlavní výhodou byla možnost pokrytí více místností jednou soupravou, ovšem právě vzhledem k této vlastnosti vyžadovaly velké zkušenosti techniků při nastavování a ladění v konkrétních podmínkách.

Zahájení průmyslové výroby Gunnových diod jako komerčně i technicky využitelných generátorů gigahertzových frekvencí znamenalo nástup mikrovlnných čidel. Na přelomu šedesátých a sedmdesátých let se tak na zabezpečovacím trhu objevil prostředek umožňující poměrně snadné cílené pokrytí střeženého prostoru prakticky neodstíratelným signálem, a tedy téměř nepřekonatelnou spolehlivost detekce. Dodnes patří mikrovlnná čidla mezi nejúčinnější zabezpečovací technologie, ovšem s podmínkou jejich perfektního zvládnutí a velkých zkušeností z praktického využívání. Proto se s nimi v praxi setkáváme poměrně zřídka.

Zhruba ve stejné době se do popředí zájmu dostávají i „světelné závory“. Princip byl ovšem využíván již dávno, ale teprve dostupnost účinných miniaturních zdrojů infračerveného světla a dalších potřebných polovodičových součástek umožnila jejich kvalifikované využívání v zabezpečovací technice.

Ve druhé polovině sedmdesátých let se na trhu objevuje dodnes neúspěšnější zabezpečovací prvek - pasivní infračervené čidlo (Passive Infrared Detector - PIR). Pochází z hlavic samonaváděcích protiletadlových a protitankových raket. Z komerčních důvodů brzy tato čidla vytlačila aplikačně i energeticky náročná mikrovlnná čidla. Ačkoliv PIR čidla nedosahují bezpečnostní spolehlivosti čidel fungujících na Dopplerově principu, jejich spolehlivost a relativní jednoduchost používání měly brzy za následek



vytlačení ostatních typů prostorových čidel na okraj zájmu.

V Československé republice byla první větší aplikace zabezpečovací techniky zaznamenána v roce 1933, kdy byly zřizovány automatické poplašné telefonní hlásiče. Rozmach elektrických zabezpečovacích systémů (EZS) je datován od padesátých let minulého století.

V roce 1958 bylo v podniku Obchodní zařízení a potřeby státního obchodu Praha započato s vývojem prvních zabezpečovacích elektrických prvků a systémů, na kterém se podílelo i Ministerstvo vnitra. Byly položeny základy novému technickému oboru, o jehož výrobní program projevil zájem n. p. TESLA Lanškroun, jenž se tak stal hlavním podnikem pro výrobu elektrických zabezpečovacích zařízení.

V roce 1974 byla ve složkách tehdejší Veřejné bezpečnosti zřízena speciální pracoviště, která se využitím a vývojem těchto prostředků zabývala.

K velkému rozmachu v zavádění EZS docházelo od sedmdesátých let minulého století pod vlivem výrobního programu n. p. TESLA Liberec. Začal se zde vyrábět nový systém, jehož širšímu využívání napomohlo usnesení vlády ČSSR č. 73/1982 Sb., a centralizace zabezpečených objektů. Usnesení určovalo kategorie objektů a z toho vyplývající nároky na složitost EZS. Vznikla řada organizací, zabývajících se projekcí, montáží a servisem.

V roce 1974 byl u Služby ochrany objektů VB v Příbrami zkušebně instalován první pult centralizované ochrany (PCO). Nejprve byly napojeny benzínové čerpací stanice, jeden peněžní ústav a sklady tržavin. Potom objekty obchodní sítě a objekty kulturního a památkového významu. Na základě vyhodnocení byl tento PCO rozšířen postupně do většiny krajských měst. Jednalo se o reléový linkový pult CENTR KM. Umožňoval napojení 120 objektů na teritoriu jedné telefonní ústředny.

Během let přicházely do policejní výzbroje další pulty centralizované ochrany: RONA, TCP 60, TRVZ a GENOVA. V roce 1989 bylo na území Československa provozováno celkem 79 systémů centralizované ochrany se 7724 napojenými objekty.

Po roce 1989 přestalo být využití elektronické zabezpečovací signalizace a pultů centralizované ochrany doménou jenom policie. V oboru ochrany majetku a osob začaly podnikat nejrůznější výrobní, obchodní a montážní firmy a bezpečnostní agentury.

V poslední době se prudce rozvíjí biometrické systémy využívající některých anatomických a fyziologických vlastností člověka k jeho identifikaci. Zatím byly využívány pouze v přístupových systémech (Access Control Systems), ale s vývojem



výpočetní techniky se jejich možnosti rozšiřují a objevily se již produkty dovolující jejich bezpečnostní aplikace.

## 1. DEFINICE A ZKRATKY

Následující seznam pojmů je pouze výčtem nejčastěji používaných pojmů v oboru. Není úplným výčtem všech pojmů vzhledem k velké obsáhlosti. Pro přehlednost a orientaci je také v závorce, za jednotlivými pojmy, kurzívou uveden originální anglický výraz.

V současné době je hlavním zdrojem terminologie pro elektronické zabezpečovací systémy norma ČSN EN 50131-1 a její změna ČSN EN 50131/Z1.

**Jednotka RU:** smluvně dohodnutá mezinárodní jednotka převzatá z německého značení. Vyjadřuje agresivitu určitého nářadí za minutu.

**Zařízení elektrické zabezpečovací signalizace - zařízení EZS:** je soubor čidel, tísňových hlásičů, ústředen, prostředků poplachové signalizace, přenosových zařízení, zapisovacích a ovládacích zařízení, jejichž prostřednictvím je opticky nebo akusticky signalizováno na určeném místě narušení střeženého objektu nebo prostoru.

**Poplachový systém (*alarm systém*):** elektrická instalace, která reaguje na manuální podnět nebo automatickou detekci přítomnosti nebezpečí.

**Elektrický zabezpečovací systém (zkratka EZS) (*intruder alarm systém - IAS*):** poplachový systém pro detekci a indikaci přítomnosti, vstupu nebo pokusu o vstup narušitele do střežených objektů.

*POZNÁMKA – vzhledem k EZS začíná převažovat pojem „elektronický“.*

**Komponenty systému (*system components*):** jednotlivá zařízení, která pokud jsou spolu uspořádána, tvoří EZS.

**Subsystém (*subsystem*):** ta část EZS, která je umístěna v jasně definované části zabezpečených prostorů a je schopna samostatného provozu.

**Čidlo (*detector*):** zařízení určené k vyslání poplachového signálu nebo zprávy jako odezvy na zaznamenání abnormální podmínky, indikující přítomnost nebezpečí.

**Aktivní (*active*):** stav čidla při přítomnosti nebezpečí.

**Aktivní čidlo (*active detector*):** čidlo schopné porovnávat vstupní signály s předem definovanými kritérii (rychlost, frekvence, amplituda, směr) před vysláním poplachového signálu nebo zprávy.

**Senzor (*sensor*):** ta část čidla, která snímá změnu stavu.



**Zakrytí čidla** (*detector masking*): stav, při kterém je detekční schopnost čidla značně snížena.

**Tísňové hlásiče EZS:** zařízení určená k manuálnímu vyhlášení poplachu osobami, které jsou obeznámeny s jejich použitím.

**Ústředna** (*control and indicating equipment - CIE*): zařízení pro příjem, zpracování, ovládání, indikaci a inicializaci následného přenosu informací.

**Provozní program** (*operating programme*): software, firmware případně hardware ústředny, dodávané výrobcem, které poskytuje prostředky s jejichž pomocí může montážní technik nebo uživatel zpracovávat (vyhodnocovat) signály nebo zprávy.

**Signalizační (výstražné) zařízení** (*warning device - WD*): zařízení, které vyhláší poplach nebo výstrahu.

**Akce** (při nastavování stavu střežení a klidu) (*action*): jakákoliv záměrná činnost nebo jednání uživatele, které je součástí postupu nastavování stavu střežení a klidu.

**Přístupová úroveň** - (*access level*): úroveň přístupu k jednotlivým funkcím EZS.

**Poplachové přijímací centrum/pult centralizované ochrany** (zkratka **PPC/PCO**) (*alarm receiving centre - ARC*): trvale obsluhované vzdálené středisko, do kterého se předávají informace týkající se stavů jednoho nebo více EZS.

*POZNÁMKA - dvojí pojem PPC/PCO vyjadřuje odlišného provozovatele centra (PCO – policie, PPC – soukromý subjekt). V praxi se však převážně využívá pojem PCO.*

**Systém přenosu poplachu** (*alarm transmission systém - ATS*): zařízení a síť, používané pro přenos informací, týkající se stavů jednoho nebo více EZS do jednoho nebo více PPC/PCO.

*POZNÁMKA - Přenosové systémy nezahrnují místní přímá spojení, např. propojení mezi komponenty EZS, které nepožaduje rozhraní pro přenos informací do formy vhodné pro přenos.*

**Přenosová cesta** (*transmission path*): komunikační cesta používaná pro přenos ohlašované informace.

**Vyhrazená přenosová cesta** (*dedicated transmission path*): přenosová cesta, která je trvale k dispozici pro spojení poplachového přenosového systému s jeho PPC/PCO a která nevyžaduje spínání nebo nastavování před přenosem jednotlivých poplachových událostí.

**Propojení** (*interconnection*): prostředky s jejichž pomocí jsou zprávy případně signály přenášeny mezi komponenty EZS.

**Místní propojení pro přenos poplachu** (*local interconnection for alarm transmission*): propojení mezi EZS a poplachovým přenosovým systémem a mezi přijímacím zařízením PPC/PCO a signalizačním zařízením.

**Bezdrátové propojení** (*wire-free interconnection*): propojení přenášející informace mezi komponenty EZS bez fyzických médií; toto propojení může přenášet informace příslušející dvěma nebo více aplikacím.

**Komunikace** (*communication*): přenos zpráv či signálů mezi komponenty EZS.

**Porucha komunikace** (*failure of communication*): nemožnost předat zprávu nebo signál mezi komponenty EZS.

**Poruchový stav** (*fault condition*): stav, který znemožňuje EZS nebo jeho komponentům normálně pracovat.

**Normální stav** (*normal condition*): stav EZS, při kterém neexistují žádné podmínky, které by mohly znemožnit nastavování EZS do stavu střežení.

**Zkušební stav** (*test condition*): stav EZS, ve kterém jsou normální funkce modifikovány pro zkušební účely.

**Stav střežení** (*set*): stav EZS nebo jeho komponentů, při kterém může být vyhlášen poplachový stav.

**Poplachový stav** (*alarm condition*): stav EZS nebo jeho komponentů, který je výsledkem odezvy systému na přítomnost nebezpečí.

**Stav klidu** (*unset*): stav EZS nebo jeho komponentů, při kterém nemůže být ohlášen poplachový stav.

**Poplach** (*alarm*): výstraha o přítomnosti nebezpečí pro život, majetek nebo okolní prostředí.

**Planý (falešný) poplach**: omylem vyslaný poplachový signál způsobený náhodným spuštěním tlačítkového detektoru, reakcí automatického zařízení na jiné podmínky než ty, pro jejichž detekci je určen, špatnou funkcí nebo poruchou některého prvku či chybou obsluhy.

**Hlášení poplachu** (*alarm notification*): předání poplachového stavu na signalizační zařízení případně do poplachových přenosových systémů.

**Aktivní doba** (*active period*): doba po kterou trvá poplachový signál.

**Signál nebo zpráva o narušení** (*intruder signal or message*): informace o narušení vyslaná čidlem.

**Sabotáž** (*tamper*): úmyslné zasahování s nedovolenou manipulací do EZS nebo jeho části.



**Sabotážní poplach** (*tamper alarm*): poplach způsobený detekcí sabotáže.

**Zabezpečené prostory** (*supervised premises*): ta část budovy případně území, ve které může být pomocí EZS detekováno nebezpečí.

**Událost** (*event*): změna stavu indikovaná EZS, například stav střežení, stav klidu, poplachový stav.

**Záznam událostí** (*event recording*): shromažďování událostí vyplývajících z činnosti EZS, například pro analýzu.

**Odpojení** (*isolation*): stav části EZS, ve které není možné ohlásit poplachový stav; tento stav zůstává, dokud není záměrně zrušen.

*POZNÁMKA: zde se spíše užívá anglického originálu „bypass“ nebo českého „přemostění“.*

**Hlášení** (*notification*): předání poplachového stavu, stavu sabotáže nebo poruchového stavu na signalizační zařízení případně do poplachových přenosových systémů.

**Poruchový signál/zpráva** (*fault signal/message*): informace vzniklá poruchou.

**Prostor** (*zone*): stanovená oblast, ve které mohou být detekovány abnormální podmínky.

**Napájecí zdroj** (*power supply - PS*): ta část EZS, která zajišťuje energii pro EZS a jeho komponenty.

**Základní napájecí zdroj** (*prime power source*): zdroj napájející EZS a jeho komponenty při normálních provozních podmínkách.

**Náhradní napájecí zdroj** (*alternative power source - APS*): napájecí zdroj schopný napájet systém po předem určenou dobu v případě výpadku základního napájecího zdroje.

**Doplňkový napájecí zdroj** (*supplementary prime power source*): energetický zdroj schopný napájet EZS po rozšířenou dobu, aniž by došlo k ovlivnění doby zálohování náhradního napájecího zdroje.

**Výkonový výstup** (*power output*): výstup napájecího zdroje, který dodává energii EZS.

**Nezávisle napájené zařízení** (*self-powered device*): zařízení, které má svůj vlastní napájecí zdroj.

**Oprávnění** (*authorisation*): povolení k získání přístupu k různým funkcím EZS.

**Kódy oprávnění** (*authorization codes*): fyzické nebo logické klíče, které umožňují přístup k funkcím EZS.



**Pomocné ovládací zařízení - ACE** (*ancillary control equipment*): zařízení použité pro doplňkové ovládací účely.

**Přístupová/výstupová úroveň** (*entry/exit route*): cesta, po které lze docílit oprávněného vstupu nebo výstupu do střeženého prostoru.

**Rušení** (*interference*): zkreslení signálů případně zpráv při jejich předávání mezi komponenty EZS.

**Odpovědná osoba/orgán** (*response authority*): určená osoba, která má odpovědnost za službu ve střežených objektech po vyhlášení poplachu a za přijmutí příslušného opatření.

**Nulování** (*restore*): postup zrušení poplachového stavu, stavu sabotáže, poruchového nebo jiného stavu a návrat EZS do výchozího stavu.

**Signál** (*signal*): proměnné parametry, pomocí kterých jsou přenášeny informace.

## 2. Elektrické zabezpečovací systémy (EZS)

### 2.1 Rozdělení prvků EZS

Nejdůležitějším kritériem pro zatřídění prvků EZS jsou tzv. stupně zabezpečení. Tyto stupně definuje norma ČSN EN 50131-1 a zároveň stanovuje kritéria na výbavu a funkci jednotlivých komponentů i celkového systému EZS.

Tab.1 Stupně zabezpečení

Stupeň	Míra rizika	Předpokládaný typ narušitele
1	nízké	narušitel má malou znalost EZS; omezený sortiment snadno dostupných nástrojů
2	nízké až střední	narušitel je obeznámen s EZS; omezený sortiment základních přenosných přístrojů a elektronických zařízení
3	střední až vysoké	narušitel je obeznámen s EZS; úplný sortiment základních přenosných přístrojů a elektronických zařízení
4	vysoké	narušitel je schopen nebo má možnost zpracovat podrobný plán vniknutí; kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících prvků EZS

Tab. 2 Rozdělení prvků EZS

<b>PRVKY PLÁŠŤOVÉ OCHRANY</b>	<b>PRVKY PROSTOROVÉ OCHRANY</b>
magnetické kontakty, chrana prosklených ploch, mechanické kontakty, vibrační čidla, poplachové fólie, tapety, polepy a poplachová skla, drátová čidla, rozpěrné tyče.	pasivní infračervená čidla aktivní infračervená čidla, ultrazvuková čidla, mikrovlnná čidla, kombinovaná duální čidla.
<b>PRVKY TÍŠŇOVÉ OCHRANY</b>	<b>PRVKY PŘEDMĚTOVÉ OCHRANY</b>
veřejné tísňové hlásiče, skryté tísňové hlásiče, osobní tísňové hlásiče.	otřesová čidla, čidla na ochranu zavěšených předmětů, kapacitní čidla.
<b>OVLÁDACÍ ZAŘÍZENÍ</b>	<b>ČIDLA SPECIÁLNÍ</b>
blokovací zámky, spínací a propouštěcí zámky, kódové klávesnice, ovládací a indikační díly, kartové ovládání.	tlaková čidla, nášlapné koberce.
<b>POPLACHOVÉ ÚSTŘEDNY EZS</b>	<b>PRVKY VENKOVNÍ OBVODOVÉ (PERIMETRICKÉ) OCHRANY</b>
klasické smyčkové ústředny, ústředny s přímou adresací, ústředny smíšeného typu, ústředny s bezdrátovým přenosem signálu od čidel.	mikrofonické kabely, infračervené závory a bariéry, mikrovlnné bariéry, štěrbinové kabely, zemní tlakové hadice, perimetrická pasivní infračervená čidla.
<b>SIGNALIZAČNÍ (VÝSTRAŽNÁ) ZAŘÍZENÍ</b>	<b>PŘENOSOVÁ ZAŘÍZENÍ</b>
zábleskový maják, siréna.	automatické telefonní hlásiče a voliče, bezdrátová přenosová zařízení.

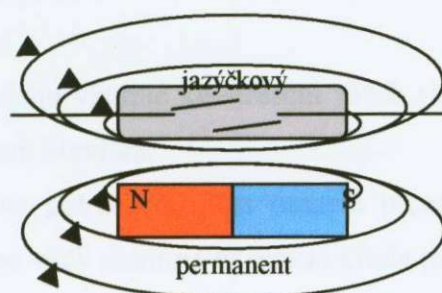


## 2.2 Prvky plášťové ochrany

Prvky plášťové ochrany slouží, jak už sám jejich název napovídá, k hlídání otevření, popř. destrukce prostupů pláště budovy (oken, vrat, dveří).

### 2.2.1 Magnetické kontakty

Magnetický kontakt je nenapájené čidlo s minimálním počtem konstrukčních dílů. Je to vysoce spolehlivý prvek s dlouhou životností a s vysokou odolností proti vnějším vlivům. Je to takzvané čidlo otevření a tvoří jej vždy dvojice dílů - jazýčkový kontakt a permanentní magnet (viz. obr. 1).



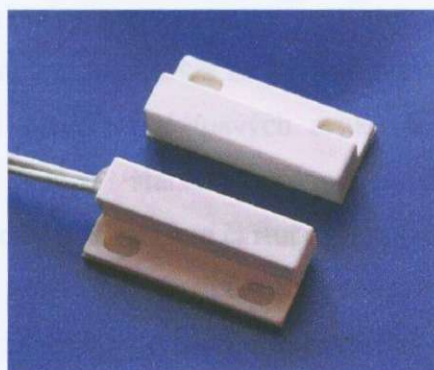
Obr. 1 Princip funkce

**Jazýčkový kontakt** je tvořen zatavenou skleněnou trubičkou naplněnou ochrannou atmosférou, v níž jsou umístěny dva feromagnetické kontakty.

**Permanentní magnet** je nejčastěji zmagnetovaný váleček z feritu.

V klidovém stavu je kontakt jazýčkového relé sepnut magnetickým polem permanentního magnetu. Při aktivaci oddálením magnetu se kontakt rozezne, a tím způsobí poplachové hlášení.

Jazýčkový kontakt i permanentní magnet jsou samostatně zapouzdřeny do různě konstruovaných krytů z nemagnetického materiálu (plastu či hliníkové slitiny) (viz. obr.2).



Obr. 2 Magnetický kontakt.

Různé provedení magnetických kontaktů umožňuje povrchovou nebo skrytou montáž

přímo do tělesa dveří či oken. Pro střežení prostupů opatřených roletami je určen magnetický kontakt v těžkém, mechanicky i klimaticky odolném provedení. Pro speciální aplikace s velmi vysokými riziky (např. věznice) existují magnetické kontakty odolné proti cizímu magnetickému poli. Jakýkoliv pokus o odstavení magnetického kontaktu přiložením cizího magnetu vyvolá automaticky poplachové hlášení. Tyto magnetické kontakty obsahují buď polarizovaný jazýčkový kontakt, nebo je kontakt tvořen sérioparalelní kombinací více kontaktů (3-7 jazýčkových kontaktů), z nichž některé jsou spínací a jiné rozpínací.

Magnetické kontakty jsou vhodné ke střežení všech stavebních otvorů – prostupů (oken, dveří, vrat, rolet) proti otevření.

Magnet se montuje na pohyblivou část osazení prostupu, jazýčkový kontakt se montuje na rám. Kontakt se vždy montuje na stranu křídla proti pantům. U dvoukřídlových oken a dveří se vždy osazují obě křídla.

### 2.2.2 Čidla na ochranu skleněných ploch

Tříštění skla vyvolává charakteristický zvuk, který se hmotou skla šíří jako vlnění v pevném tělese. Toto vlnění zachycuje čidlo pevně spojené s plochou skla – přilepené s důrazem na co nejmenší ztráty při přenosu zvuku. Taková čidla se nazývají **kontaktní**. Užívají se především ke střežení neotevíratelných prosklených ploch v plášti střeženého prostoru proti rozbití. Při narušení skleněné plochy je vlnění vyhodnoceno elektronikou čidla a čidlo způsobí hlášení. Podle konstrukce čidla se jedná buď o rozepnutí bezpotenciálového kontaktu relé, který je zapojen v poplachové smyčce, nebo o prudký vzrůst odběru čidla napájeného přímo z poplachové smyčky. Praktický dosah těchto čidel bývá 1,5m - 3 m.

Kontaktní čidla mohou být citlivá na silný dopravní ruch v okolí zajištěné skleněné plochy a na úmyslné vytváření skřípavých zvuků poblíž kontaktních čidel. Čidla na ochranu skleněných ploch staršího provedení obsahovala jednoduchý systém s předepnutým pružinovým kontaktem či rtuťovým prasátkem, jejichž funkce byla závislá na skutečné destrukci skla i v bodě připevnění a reagovala na změnu polohy tělesa čidla.

Pro nejvyšší úroveň rizik jsou určena **aktivní čidla na ochranu skleněných ploch**. Obsahují vysílací a přijímací část. Elektronika vyhodnocuje změny přenosu oproti normálnímu stavu, jenž je uložen v paměti čidla. Tato čidla mají velký dosah a mohou



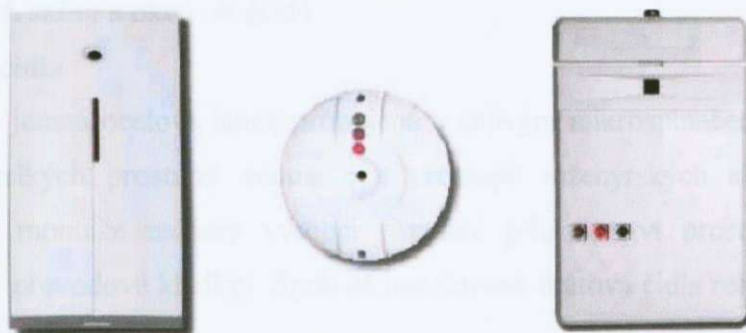
střežit až 25 m<sup>2</sup> plochy (podle typu čidla a druhu skla).

Velice rozšířené jsou u nás **akustická čidla rozbití skleněných ploch** (viz. obr. 5-5). Nevyhodnocují vlnění v tělese skla, ale následný akustický efekt při tříštění skla, jenž je naprosto charakteristický. Elektronika vyhodnocuje akustické vlnění přijaté elektretovým mikrofonem. Dále následuje pásmová propust propouštějící pouze část spektra typickou pro tříštění skla. Kvalitnější typy mají těchto propustí více a vyhodnocují přítomnost zvuku ve více částech zvukového spektra, čímž snižují možnost vyhodnocení podobných zvuků, a tím vyvolání falešných poplachů.

Nejnovější typy vyhodnocují zvukové spektrum ve více diskretních bodech a vyvolají hlášení teprve poté, když jsou všechny tyto diskretní zvukové kmitočty obsaženy v určitém časovém intervalu. Jedná se o přítomnost tříštivého zvuku skla o vysoké frekvenci a přítomnost rázové vlny vyvolané v oblasti nízkých kmitočtů borcením skleněné plochy.

U akustických čidel zvláště s jednopásmovým vyhodnocováním je nutné pečlivě zvažovat možné negativní vlivy okolního prostředí (např. zvonky, telefony, faxy, skřipavý zvuk tramvají, ale také přítomnost drobné zvěře v objektu – hlavně cvrčků).

Je také vhodné skutečnou funkci akustického čidla ověřit v reálných podmínkách nasazení. K tomuto účelu nabízejí výrobci speciální akustické testery, které obsahují digitální paměťový modul s navzorkovaným zvukem tříštěného skla.



Obr. 3 Různá provedení akustických čidel



### **2.2.3 Mechanické kontakty**

Jsou to mikrospínače konstrukčně uzpůsobené pro zabudování do rámu proti západce zámku. Střeží uzamčený stav prostupů. Při vhodném zapojení k ústředně EZS zabrání uvedení do stavu střežení v případě, že některý z prostupů není uzamčen. Užívají se především v případech, má-li střežený prostor více možných vstupů.

Mezi mechanické kontakty patří i nájezdy, jež umožňují uzavření elektrického obvodu v případech, když je třeba přivést proud do čidla na posuvný či otočný díl osazení stavebního otvoru. Nájezd současně střeží daný prostup na jeho otevření.

### **2.2.4 Vibrační čidla**

K prvkům střežení pláště budov dále patří vibrační čidla pro hlídání průrazu stěn a stavebních konstrukcí. Základem je zde elektromechanický měnič doplněný vyhodnocovací elektronikou. Tato čidla mají větší šířku pásma vyhodnocovaných kmitočtů, nastavitelnou citlivost a optickou indikaci s pamětí. Osazují se podle konstrukčního provedení na riziková místa možného průchodu zdí, luxfery či na rámy dveří a oken. Vzhledem ke své konstrukci nejsou určena pro střežení trezorových skříní a komorových trezorů.

### **2.2.5 Poplachové fólie, tapety, polepy a poplachová skla**

Tato čidla pracují na principu přerušení vodivého média, nejčastěji jemného drátku uvnitř zmiňovaného nosiče (fólie, tapety, skla), či pásků vodivé fólie aplikovaných samostatně na povrch hlídané plochy (polepy). Polepy jsou dostatečně známy z dřívější éry zabezpečování, neboť byly nejužívanější a viditelnou formou střežení skleněných ploch výkladních skříní a oken obchodů.

### **2.2.6 Drátová čidla**

Jedná se o jemná ocelová lanka propojená s citlivým mikrospínačem. Jsou vhodná pro střežení velkých prostupů ventilace a prostupů inženýrských sítí do objektu. Pro usnadnění montáže nabízejí výrobci rozsáhlé příslušenství prostředků k jejich upevnění (např. převodové kladky). Správně instalovaná drátová čidla reagují již na malé zvýšení mechanického napětí.

### **2.2.7 Rozpěrné tyče**

Tento typ čidla je vlastně miniaturní mechanický spínač, jehož klidový stav je mechanicky aretován tyčí. Rozpěrné tyče mohou chránit vstupní otvory objektu z inženýrských sítí a prostupy ventilace v rámci objektu podobně jako drátová čidla.



## 2.3 Prvky prostorové ochrany

Na rozdíl od plášťové ochrany, která má za úkol střežit samotný plášť objektu, se prostorovou ochranou střeží samotný prostor objektu. Tyto dva způsoby ochrany se vzájemně doplňují a často se používají dohromady. Mnohdy ochrana prostorová, díky nižší náročnosti na montáž, supluje ochranu plášťovou. Zcela ji nahradit ale nemůže, protože ochrana plášťová je schopna oproti ochraně prostorové detekovat narušitele s co nejmenší časovou prodlevou.

Ve své podstatě se prostorová ochrana rozděluje na **čidla pasivní a čidla aktivní**.

**Čidla pasivní** - při zjišťování charakteristických rysů napadení pouze registrují fyzikální změny ve svém okolí.

**Čidla aktivní** - při zjišťování charakteristických rysů napadení vytvářejí své pracovní prostředí aktivním působením na své okolí a detekují změnu takto vytvořeného fyzikálního prostředí.

V praxi je možné se setkat s několika druhy **čidel pohybu**:

- pasivní infračervená čidla (Passive Infra Red - PIR),
- aktivní ultrazvuková čidla (Ultrasonic - US),
- aktivní mikrovlnná čidla (Microwave - MW),
- duální (kombinovaná) čidla (PIR - US, PIR - MW).

Každý druh čidla má určité vlastnosti, jež jsou výsledkem úrovně vývoje zpracování signálu a výsledkem úrovně technologie daného výrobce. V rámci trhu se proto objevují vedle základních typů i různé modifikace využívající stejné fyzikální principy, ale doplněné o další speciální funkce z hlediska zpracování signálu. Zde se velice často objevují v sortimentu PIR čidel funkce počítání impulsů nutných k vyhlášení poplachu, dále jsou často aplikovány pyrosenzory v dvojitým či čtyřnásobném provedení a k vyhodnocení dochází paralelně. Při vlastní aplikaci přinášejí tyto funkce vyšší odolnost proti falešným poplachům způsobeným vlivem okolí (proudění vzduchu, osvětlení atd.), ale nepřinášejí vyšší úroveň bezpečnosti z hlediska napadení.

Doplňkovou funkcí, která oproti předcházejícím přináší vyšší úroveň bezpečnosti, je funkce **ochrany proti zastínění** (tzv. antimasking). Umožňuje okamžitě indikovat zastínění čidla či jeho přestříkání barvou. Tato funkce je aktivní i v době klidu objektu. Čidla s touto funkcí se aplikují v prostorech veřejně přístupných, kde je riziko sabotáže systému s cílem připravit si objekt na vloupání ve stavu střežení. Čidlo zabrání uvedení systému EZS do stavu střežení, je-li zastíněno.



Tato čidla se používají z různých důvodů, dva nejpoužívanější jsou

- V objektu se tráží službou – požadujeme okamžitou indikaci zastínění čidla, nebo jeho přestříkání barvou.
- V objektu bez strážní služby – požadujeme zabránění uvedení systému do stavu střežení, je-li některé z čidel vybavených funkcí antimasking zastíněno.

### 2.3.1 Pasivní infračervená čidla

Obvykle jsou tato čidla označována jako PIR čidla (*Passive Infra red sensor*).

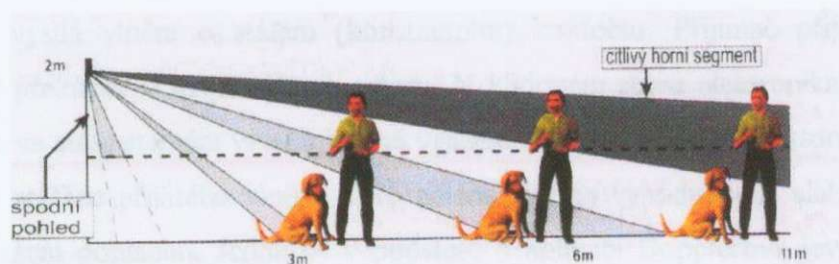


Obr. 4 PIR čidla pohybu

Principiálně jsou založena na zachycení změn vyzařování v infračerveném pásmu kmitočtového spektra elektromagnetického vlnění. Využívají skutečnosti, že každé těleso, jehož teplota je vyšší než  $-273\text{ }^{\circ}\text{C}$  (absolutní nula) a nižší než  $560\text{ }^{\circ}\text{C}$ , je zdrojem vyzařování vlnění v infrapásmu odpovídající teplotě tělesa. Směrem k vyšším teplotám se posouvá spektrum ke kratším vlnovým délkám, tedy k oblasti viditelného spektra. Takové vlnění přestáváme vnímat jako teplo a začínáme je vnímat jako světlo. Pro teplotu lidského těla cca  $35\text{ }^{\circ}\text{C}$  je charakteristická vlnová délka  $9,4\text{ mm}$ . Tohoto jevu je využito k zachycení pohybu těles, jež mají odlišnou teplotu od teploty okolí. Jako detektor je užit materiál vykazující pyroelektrický jev. Detekční prvek je měnič gradientní povahy, to znamená, že není schopen z principu detekovat stálou úroveň záření, ale jen změny záření na detektor dopadajícího. Obraz střeženého prostoru v infračerveném pásmu je transformován prostřednictvím optiky na plochu senzoru. Zorné pole je rozděleno na aktivní a neaktivní zóny, které si můžeme představit v analogii optického zobrazení jako viditelné a zakryté části obrazu střeženého prostoru. Pohybuje-li se tedy těleso, jehož teplota je odlišná od teploty okolí (pozadí) v zorném

poli čidla PIR, zachycuje čidlo změny při přechodu cíle z aktivní do neaktivní zóny a naopak. Elektronika vyhodnotí signál těmito změnami vyvolaný a způsobí vyhlášení poplachu (viz. obr. 4).

Zorné pole čidla závisí na provedení optiky, dosah je závislý na kvalitě optiky čidla, citlivosti použitého senzoru a způsobu vyhodnocení. Pokud vhodně zvolíme odpovídající optiku, můžeme střežit prostor do vzdálenosti cca 15 m od čidla či dlouhé prostory do cca 60 m. U čidel, která jsou určena pro stropní montáž lze kruhovým uspořádáním optiky obsáhnout velkou plochu v rozsahu 360°.



Obr. 5 Detekční charakteristika PIR čidla

V PIR čidlech pohybu je možné se setkat s optikou dvojitího druhu: buď se jedná o zobrazení pomocí soustavy **Fresnelových čoček**, nebo je optika vytvořena **soustavou křivých zrcadel**. Optika vždy transformuje obraz zorného pole do podoby, jež dalšímu elektrickému zpracování výstupního signálu pyrosenzoru vyhovuje nejlépe.

Užití Fresnelových čoček je z pohledu návrhu a technologie výroby řešení výrazně ekonomičtější, i přes určité nedostatky způsobené tím, že zobrazení pomocí Fresnelových čoček nedává ideální optický obraz skutečnosti. Naproti tomu optický obraz vytvořený pomocí soustavy křivých zrcadel je prakticky zobrazení zcela přesné. Z tohoto důvodu je možné se setkat se zrcadlovou optikou především u čidel tradičních značkových výrobců. Rovněž dosah čidel garantovaný výrobcem je zde díky lepšímu optickému zobrazení větší v porovnání s čidly srovnatelného tvaru detekční charakteristiky s Fresnelovou čočkou.

Někteří výrobci nabízejí i tzv. **černá zrcadla**, která principiálně omezují odrazivost v oblastech mimo požadované infračervené spektrum. Toto řešení podstatně snižuje náchylnost čidel k planým poplachům vyvolaným vlivem záření o vysoké energii ve viditelném spektru (odlesky slunce, reflektory automobilů apod.).

Z důvodu eliminace falešných poplachů PIR čidla něsmějí být vystavena následujícím



vlivům

- ventilace – vstupy a výstupy, průvan,
- přímé, nebo nepřímé vyzařování světla (slunce, reflektory),
- proměnné zdroje tepla (topení, komíny),
- spínané rušivé IR zdroje (žárovky).

### 2.3.2 Ultrazvuková čidla

Ultrazvuková čidla (Ultrasonic sensor - US) využívají část spektra mechanického vlnění nad pásmem kmitočtů slyšitelných lidským uchem. Jsou aktivní, to znamená, že do prostoru vysílají energii.

Vysílač vysílá vlnění o stálém (konstantním) kmitočtu. Přijímač přijímá vlnění odražené od překážek v uzavřeném prostoru. V klidovém stavu elektronika vyhodnotí přijatou vlnu ve stále stejném vztahu k vlně vyslané. Pohybuje-li se v prostoru libovolné těleso, mění se fáze přijatého vlnění. Tato změna fáze je vyhodnocena elektronikou a vede k vyhlášení poplachu. Jedná se v podstatě o aplikaci Dopplerova jevu v pásmu ultrazvukových kmitočtů. Dopplerův efekt lze matematicky interpretovat následujícím vztahem (2.1) :

$$f_1 = \frac{f}{1 - \left(\frac{v}{c}\right)^2}$$

- kde
- $f_1$  je kmitočet přijatý přijímačem
  - $f$  je kmitočet vyslaný vysílačem
  - $v$  je rychlost pohybu odrazné plochy (v našem případě pachatele)
  - $c$  je rychlost pohybu vlnění užitého k detekci (rychlost zvuku u US čidla, rychlost pohybu elektromagnetického vlnění u MW čidla)

Tento jev lze demonstrovat v oblasti slyšitelného spektra na známém školním příkladu

houkajícího vlaku blížícího se k železničnímu přejezdu. Při přibližování vlaku se posluchači stojícímu u přejezdu zdá, jako by kmitočet zvuku rostl, při odjezdu jako by klesal. U ultrazvukových čidel nás nezajímá absolutní velikost této odchylky, ale pouhá přítomnost této odchylky větší než je nestabilita systému.

Více ultrazvukových čidel pohybu se smí v jednom prostoru instalovat pouze tehdy, jsou-li vysílače synchronizovány nebo kmitočtově tak stálé, že není možné vzájemné



negativní ovlivňování.

### **2.3.3 Mikrovlnná čidla**

Mikrovlnná čidla (Microwave sensors - MW) vycházejí ze stejného fyzikální principu jako ultrazvuková čidla, ale v kmitočtovém pásmu elektromagnetického vlnění. Tentokrát se jedná většinou o pásma 2,5 GHz, 10 GHz a nebo 24 GHz. Je to opět aktivní systém zachycení pohybu, principiálně shodný s ultrazvukovými čidly, ale technologicky uzpůsobený danému kmitočtovému pásmu. Výrobci přešli dnes již výhradně od použití technologie vlnovodů, která je nákladná na výrobu a nastavení, k realizaci v podobě mikropáskového vedení integrovaného do desky plošných spojů. Toto řešení výrazně snížilo ceny mikrovlnných čidel v hromadné výrobě, a tím zvýšilo jejich dostupnost.

Možnost instalace mikrovlnných čidel je dosti omezená, poněvadž tato čidla se musí instalovat tak, aby podněty mimo střežený prostor neovlivňovaly činnost čidla. Protože mikrovlny pronikají skleněnými plochami a tenkými stěnami např. ze dřeva, tvrzeného papíru, plastické hmoty mohou též pohyby mimo střežený prostor vést k aktivaci mikrovlnného čidla (např. projíždějící vozidla, výtahy, voda protékající v plastových trubkách). Rovněž se v blízkosti těchto čidel nesmí nacházet žádné velké objekty z kovu. Zvláště kritické jsou objekty s rovinným povrchem, od kterého se mikrovlny odrážejí a mění tím výrazně detekční charakteristiku.

### **2.3.4 Kombinovaná (duální) čidla**

V prostorách s obtížnými podmínkami nasazení, s výrazným negativním vlivem okolního prostředí, se nabízí využití kombinovaných čidel PIR - US či PIR - MW. Vlastní myšlenka pro vývoj kombinovaných (duálních) čidel vychází ze zásady, že je zanedbatelná pravděpodobnost současného vzniku jevů, které by mohly vyvolat planý poplach u více čidel pracujících na různých fyzikálních principech.

Negativně se ovšem u těchto čidel projevuje to, že práh jejich detekce je díky použitému principu posunut poněkud výše oproti jednosystémovým čidlům.

## **2.4 Prvky tísňového hlášení**

Slouží k ochraně zaměstnanců a veřejnosti v případě přímého ohrožení. Hlášení do místa, odkud může být poskytnuta pomoc, je vyvoláno buď přímým manuálním aktem, nebo zprostředkované při definovaném způsobu manipulace, popř. automaticky bez jakéhokoli přispění obsluhy či nositele.



#### **2.4.1 Veřejné tísňové hlásiče**

Jsou to magnetické kontakty či mikrospínače zapouzdřené do podoby tlačítka. Slouží veřejnosti k vyvolání tísňového hlášení.

Aplikovány jsou na viditelných místech objektu - při schodištích, v chodbách a v halách tak, aby je mohl použít každý, kdo je v nouzové situaci nebo je takové situace svědkem. Může sloužit rovněž k přivolání pomoci při občůzkové službě strážných.

Veřejné tísňové hlásiče jsou většinou opatřeny krycím sklem, které je při vědomé aktivaci třeba rozbít. Sklo slouží jako ochrana před náhodným použitím, popř. má znesnadnit zneužití. Falešné poplachu jsou tím eliminovány na minimum.

#### **2.4.2 Speciální tísňové hlásiče**

Jsou to opět magnetické kontakty či mikrospínače zapouzdřené do podoby vhodné tvarovaného tlačítka či nožní spínací lišty. Slouží zaměstnancům k nepozorovanému vyvolání tísňového hlášení v případě přímého ohrožení.

Aplikovány jsou tak, aby nebyly ze strany zákazníka viditelné. Tzn. tlačítka se umisťují nejčastěji pod horní hranu stolu či pultu, nožní spínací lišty na trnože stolu zesponu či na můstky, peněžní svorky či optická peněžní čidla do peněžních přihrádek.

V případě zapojení většího počtu tísňových hlásičů na jednu smyčku se souběžně používají prvky s optickou signalizací pro potřeby identifikace planých poplachů způsobených chybou obsluhy i pro zpětnou analýzu poplachové události.

Tyto skryté tísňové hlásiče nemají ochranu před nechtěným vyhlášením poplachu. Vyhlášení falešných poplachů se musí předejít při návrhu správného umístění těchto prvků tak, aby nedocházelo k nechtěnému vyhlášení poplachu bezděčným pohybem těla (nohy, ruky) či vybavení (např. kancelářská židle) na pracovním místě.

#### **2.4.3 Automatické tísňové hlásiče**

Svým provedením umožňují vyhlášení tísňového poplachu nezávisle na vůli obsluhy - pouze respektováním požadavků případného útočníka.

Speciální druh tísňových hlásičů tvoří tzv. čidla poslední bankovky. Vyrábějí se ve dvojím provedení - kontaktní (mechanická) čidla a bezkontaktní (optoelektronická čidla).

Mechanické kontakty jsou uzpůsobené k zasunutí bankovky do tělesa pouzdra. Optická čidla pracují bezkontaktně na principu reflexního optoelektronického vazebního členu (optokopleru).

Optická čidla se vyrábějí ve 3 variantách: základní, s optickou identifikací a s optickou identifikací s nastavitelným zpožděním poplachu.



Aplikována jsou tak, aby nebyla jejich montáž na první pohled patrná. Při aplikaci v peněžních ústavech se umísťují do peněžních přihrádek a slouží k nepozorovanému vyvolání tísňového hlášení při přepadení. Přes optické čidlo je nutné položit alespoň 10 bankovek kvůli dostatečnému zastínění a k zabránění průniku světla plochou bankovky. Nepatrné rozměry umožňují umístění prakticky do všech používaných typů peněžních přihrádek.

Pracovní režim elektroniky čidla je nejčastěji pulsní, čímž je docíleno odolnosti proti osvětlení od cizích světelných zdrojů. Čidla jsou odolná proti cizím zdrojům světla do intenzity osvětlení cca 500 lx. Spínací vzdálenost od reflexního optokopleru je 8 - 10 mm.

#### **2.4.4 Osobní tísňové hlásiče**

Pracují bezdrátově, výstupní signál vysílaný do prostoru je modulován kódem nastaveným shodně s přijímací stranou. Využívají podle typu různá kmitočtová pásma, nejčastěji pásmo 27 MHz, popř. pásmo 300 MHz či 400 MHz. Existují i varianty pracující na ultrazvukovém principu. Svým provedením jsou podobny buď dálkovému ovládání auto-alarmů, či malým pagerům nebo se vyrábějí v podobě přívěsků, náhrdelníků a náramků.

Vysílač pracuje autonomně bez pevného připojení k systému EZS a je napájen z vlastní baterie či akumulátoru. Přijímač se nejčastěji připojuje svým reléovým výstupem do samostatné poplachové smyčky naprogramované jako smyčka tísňová (aktivní nezávisle na stavu střežení či stavu klidu systému).

Osobní tísňové hlásiče se používají v aplikacích, kde je třeba zajistit ochranu osob, jež nejsou vázány na stálé pracovní místo v rámci objektu. Jsou tedy vhodné pro ochranu pracovníků hlídací služby během pochůzky, pro pracovníky v peněžních ústavech při dotaci peněz a pro pracovníky dozorčí služby v rizikových objektech, jako jsou věznice apod. Dosah bezdrátových tísňových hlásičů závisí na použitém typu - zvoleném principu, výkonu a pracovním kmitočtu, na provedení vysílací a přijímací části (příp. antény) na stavebním provedení objektu. Pro hlásiče pracující s elektromagnetickým vlněním není stavební ohraničení prostoru překážkou, a hlášení je tedy možné přiřadit přímo nositeli bezdrátového tísňového hlásiče.

Zvláštním druhem osobního tísňového hlásiče je hlásič typu „mrtvý muž“. Je to osobní tísňový hlásič používaný v prostředí s vysokými riziky ohrožení personálu. Nejčastěji se s ním lze setkat ve věznicích. Tento hlásič umožňuje kromě cíleného vyhlášení tísňového poplachu i automatický režim v případě pádu. Díky použitému



principu přenosu poplachového signálu v pásmu ultrazvukových vln je možné v rámci objektu identifikovat místo vyhlášení tísňe či napadení dané omezeným dosahem přijímače ultrazvukových tísňových hlásičů v rámci jediného stavebně ohraničeného prostoru.

## **2.5 Prvky předmětové ochrany**

Pro předmětovou ochranu je možné využít řadu prvků, která jsou původně určena pro jiné účely, např. magnetické kontakty, PIR čidla s charakteristikou záclona, mikrovlnná čidla, infračervené závory apod. Speciálně pro vlastní střežení trezorových skříní a komorových trezorů byla vyvinuta trezorová čidla tzv. seismická čidla. Dříve se k tomuto účelu využívala i kapacitní čidla, ale vzhledem k náročné montáži, složitého nastavování a náchylnosti k planým poplachům, se od využití těchto čidel ustupuje. Další skupina čidel, jsou čidla závěsová a polohová, která se využívají především na ochranu uměleckých předmětů.

### **2.5.1 Otřesová (seismická) čidla**

Jsou to čidla pracující na principu selektivního zpracování vlnění, které se šíří pevnými tělesy při jejich mechanickém či termickém opracování. Nejnovější typy využívají při své činnosti digitálního zpracování signálu.

Otřesová čidla, jsou schopna reagovat na všechny dnes známé druhy napadení skříňových trezorů, nočních trezorů, bankomatů a těžkých trezorových místností. Velice dobře reagují na mechanické i termické napadení, jako je použití hrubého mechanického náradí, vrtání včetně užití vrtáku s diamantovou korunkou, užití hydraulického tlakového náradí, řezání kyslíko-vodíkovým plamenem a v neposlední řadě i užití plastických a jiných trhavin.

Mohou být použita ke střežení výdejních automatů na lístky, parkovacích a peněžních automatů, pancéřových skříní na peníze.

S otřesovými čidly můžeme střežit předměty z kovu, betonu a omezeně i kamene. Nelze však střežit sklo, dřevo, gumu, vláknité desky a pěnové materiály.

Při instalaci je nutné dbát ohled na eventuální okolní vlivy, s nimiž je třeba počítat (vozidla, ventilace apod.) Nesmíme střežit plochy, které jsou přístupné z nestřeženého prostoru.

### **2.5.2 Čidla na ochranu uměleckých předmětů**

Jsou určena pro střežení uměleckých předmětů (např. obrazů) zavěšených ve výstavních sálích, galeriích, muzeích apod. Princip činnosti umožňuje trvalý provoz



střežení, tedy i v době provozu pro veřejnost. Tato čidla můžeme rozdělit na závěsová a polohová.

#### **Závěsová čidla:**

Střežený předmět je zavěšen pomocí závěsného lanka na hák čidla. Čidlo vyhodnocuje síly působící na hák a podle nastavení citlivosti vyhodnotí elektronika i velmi malé pohyby střeženého předmětu, pokus o jeho sejmutí či pouhý dotek (viz. obr. 5-8). Principiálně se jedná opět o elektromechanický měnič doplněný vyhodnocovací elektronikou s nastavitelnou citlivostí.

Rozsah použitelnosti je podle zvoleného typu a způsobu montáže pro předměty od 1 kg do cca 100 kg. Montují se na kolmé stěny s dostatečnou mechanickou odolností, tj. min. 30 cm silné, 50 až 200 cm nad zavěšený předmět.



Obr. 6 Příklad použití závěsového čidla.

#### **Polohová čidla:**

Jedná se o elektromagnetická či kontaktní čidla, která velmi citlivě reagují na změnu polohy střeženého předmětu. Vychýlením „praporku“ čidla, jež se přímo dotýká části střeženého předmětu, mimo stanovený rozsah se aktivuje magnetický kontakt a elektronikou čidla je vyhlášen poplach. Tento typ čidla je zvláště vhodný v případech, kdy nelze použít pro střežení předmět čidla závěsová.

#### **2.5.3 Kapacitní čidla**

Jsou určena k indikaci přiblížení či doteku chráněného předmětu. Mohou být užita k ochraně obrazů, volně stojících předmětů a skříní kovových i nekovových.

Střežený předmět je umístěn v elektrickém poli čidla nebo je přímou součástí elektrod. Osoba v elektrickém poli kondenzátoru tvořeného střeženým předmětem a polepy mění parametry dielektrika (jímž je v tomto případě okolní vzduch), a tím i kmitočet oscilátoru, jehož je kondenzátor součástí. Fázový detektor tyto změny vyhodnocuje a dává povel k vyhlášení poplachu.

Montáž a nastavení kapacitního čidla jsou velice náročné, a proto nepatří v současné

době mezi příliš užívané prvky a jen málo světových výrobců ho má dodnes ve svém sortimentu. Výhodou však je, že může být nastaveno tak, že dojde k vyhlášení poplachu již při pouhém přiblížení se ke střeženému předmětu.

## **2.6 Prvky venkovní obvodové (perimetrické) ochrany**

Jsou to čidla, která chrání, resp. signalizují narušení vnějších částí u rozlehlých objektů, komplexů budov nebo továren na samostatném pozemku.

Existuje celá řada druhů čidel, pracujících na různých fyzikálních principech, z nichž každé je určeno pro odlišnou povahu chráněného pozemku. Zařízení se liší podle účelu nasazení a podle stupně důležitosti zabezpečení.

Konstrukce vnějších čidel, zejména mechanické a klimatické krytí, odpovídá vnějšímu prostředí, a tak se samozřejmě odlišuje od částí zabezpečovacího systému, které jsou umístěny uvnitř budov. Vzhledem k dimenzím venkovních prostor se liší od čidel pro vnitřní použití především v dosahu. Jsou-li funkční dosahy vnitřních čidel řádově 10 metrů, u venkovních se jedná řádově o 100 metrů. Dalším rozdílem je tvar zabezpečovaného prostoru. Je-li možno přiblížit se k objektu z více stran, bylo by nejvhodnější chránit celý plošný rozměr parcely, a zároveň mít možnost přímé adresace pro každý bod chráněné plochy. Z technických i ekonomických důvodů však nelze tento požadavek důsledně splnit. Proto se vytvářejí nejčastěji přímkové koridory u hranice pozemku popř. křivky kopírující terén a hranici pozemku. Z důvodů zamezení signalizace planých poplachů vzniklých nechtěným vstupem je také nutnou podmínkou oplocení. Avšak podněty, které se svým charakterem přibližují situaci narušení, nelze nikdy zcela eliminovat. Proto se často kombinuje systém venkovní perimetrické ochrany se systémem průmyslové televize.

Základním požadavkem na prvky venkovní perimetrické ochrany je nezávislost funkce na klimatických podmínkách. Proto bývají venkovní čidla, je-li to z hlediska funkce nutné, obvykle vybavena vnitřním vyhříváním. Kryty čidel či vyhodnocovací elektroniky musejí být dokonale utěsněny a opatřeny kontakty zapojenými do zajišťovací smyčky. Rovněž přívodní kabely musí být kvalitně utěsněny v průchodkách do krytů čidel či vyhodnocovací elektronické jednotky.

### **2.6.1 Mikrofonické kabely**

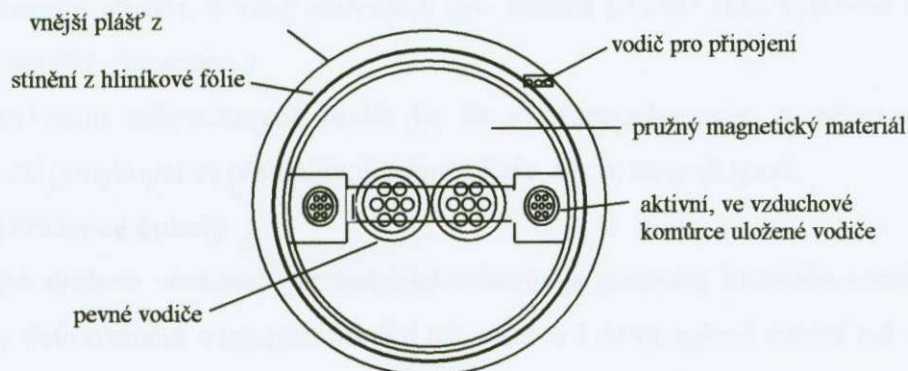
Používají se k ochraně drátěných plotů. Některé typy lze aplikovat i pod omítku či pro zazdění a zabetonování. Nejčastěji se aplikuje vpletením do osnovy drátěného



plotu. Délka jednoho úseku může být až 300 m.

Princip funkce spočívá v tom, že mechanické namáhání nebo záchvěvy citlivého mikrofonického kabelu se převádějí na elektrický signál, který je dále zpracováván ve vyhodnocovací jednotce. Akustický odposlech slouží k rozpoznání charakteru narušení, úroveň odezvy odpovídající vyhlášení poplachu je nastavitelná.

Komplikovat funkci zařízení falešnými poplachu může silný déšť, krupobití, silný vítr či přítomnost zvěře, ale také indukce silného elektrického či elektromagnetického pole.



Obr. 7 Příklad provedení mikrofonického kabelu.

### 2.6.2 Infračervené závory a bariéry

Nejrozšířenějším druhem venkovních obvodových čidel jsou infračervené závory (infrazávory). Mezi přijímací a vysílací stranou probíhá jeden či více infračervených paprsků. Při přerušení některého z nich (nebo více – dle nastavení) dochází na přijímací straně k vyhodnocení a vyhlášení poplachového stavu. Pro zvýšení odolnosti proti cizím zdrojům světla pracují infrazávory v pulsním režimu. Aby nedošlo k orosení optiky nebo nánosu vlhkosti z vnější strany, bývají vybaveny vyhříváním. Prakticky použitelný dosah je 50 až 150 metrů, avšak někteří výrobci inzerují dosah až do 250 m.

Rizikové faktory falešných poplachů jsou mlha, padající sníh, popř. přímý sluneční svit. Někteří výrobci doplňují infrazávory automatikou snímající optickou propustnost prostoru mezi přijímačem a vysílačem. Při poklesu viditelnosti (např. za silné mlhy) automatika vyřadí čidla z provozu a poplach není vyhlášován.

### 2.6.3 Mikrovlnné bariéry

Dalším prvkem venkovní perimetrické ochrany je mikrovlnná bariéra. Jedná se o vytvoření elektromagnetického pole mezi vysílačem a přijímačem. Vnik osoby do



detekční zóny způsobí porušení elektromagnetického pole. Tato změna je detekována a vyhodnocována přijímačem. Mikrovlnný svazek je zde rovněž modulován pro zvýšení odolnosti proti rušení cizími zdroji elektromagnetického vlnění.

Typický tvar mikrovlnného svazku je elipsoid s výrazným poměrem velké a malé osy, kdy tento poměr vzrůstá se zvětšením vzdálenosti mezi vysílačem a přijímačem. Vyzářovací diagram čidla má tedy typický doutníkový tvar. Výhodou mikrovlnných bariér je značný dosah, cca 200 až 300 metrů, při relativně vysoké odolnosti vůči povětrnostním vlivům. Kromě provedení pro stabilní montáž jsou vyráběna čidla i pro mobilní použití (na stativu).

Nevýhodou mikrovlnných bariér je, že v zabezpečeném prostoru se nesmějí vyskytovat pohybující se předměty, traviny a keře, větve stromů apod.

#### **2.6.4 Štěrbinové kabely**

Jiným druhem venkovní perimetrické ochrany je položený koaxiální kabel (většinou v páru v definovaném odstupu). Stínění má snížené krytím, neboli stínění má definované štěrbinové. Jeden kabel vyzářuje a vytváří elektromagnetické pole, jehož změny jsou druhým kabelem vyhodnocovány. Při narušení tohoto pole osobou dochází k vyhlášení poplachu. Výhodou je možnost kopírování terénu výškově i půdorysně, štěrbinové kabely se položí podél obvodu pozemku bez nutnosti vytvářet přímé úseky s rovným povrchem. Délka jednoho úseku může být 100 - 200 m. Existuje i mobilní verze štěrbinových kabelů, kdy jsou kabely zavěšeny na nosících v určitém odstupu nad povrchem země.

Funkci zařízení může falešnými poplasy komplikovat indukce silného elektrického či elektromagnetického pole, nebo také pohyb zvíře v zabezpečeném prostoru.

#### **2.6.5 Zemní tlakové hadice**

Zemní tlaková hadice je hydraulické podzemní čidlo známé pod názvem GPS (Ground Perimeter System). Jedná se o diferenciální tlakové čidlo, jehož základem jsou paralelně položené dvě pružné hadice v rozteči cca 1 metr po celém obvodu pozemku. Tyto hadice napuštěné nemrznoucí kapalinou působí jako prostředí pro přenos změn tlaku, vyvolaného vnějším podnětem z okolí, až do místa vyhodnocení. Změny tlaku jsou vyhodnocovány v diferenciálním tlakovém čidle a převáděny, na elektrický signál. Další elektronické vyhodnocování signálů je schopno rozeznat i charakter průniku chráněným územím, a proto také účinně omezit falešné poplasy způsobované hluky z okolí mimo koridor, např. silniční dopravou, vlaky, letadly, drobnou zvěří. Díky hydraulickému médiu není systém citlivý na elektrické a elektromagnetické pole. Délka jednoho úseku může být až 200 m.



### 2.6.6 Perimetrická pasivní infračervená čidla (infrateleskopy)

Dalším venkovním čidlem je venkovní infrapasivní čidlo. Několik málo výrobců modifikovalo známý princip infrapasivního čidla (PIR) pro venkovní prostory. Je zde použita jiná optika, vyhodnocovací obvody jsou složitější a mechanicky je použita robustní, klimaticky odolná konstrukce s vytápěným pouzdem. Díky použití diferenciálních vícenásobných pyrosenzorů a speciálních vyhodnocovacích obvodů je vliv typických kritérií falešných poplachů PIR čidel (víření vzduchu, pohyb rostlin, dopadající svit slunce či reflektorů automobilů) eliminován na minimum. Schopnost detekce se však snižuje při nízkých rozdílech teploty pozadí a pachatele. Typický dosah infrateleskopů je cca 150 m.

Infrateleskopy se většinou využívají jako doplněk kamerových systémů pro spínání poplachového monitoringu či záznamu.



*Obr. 8 Venkovní provedení čidla PIR*

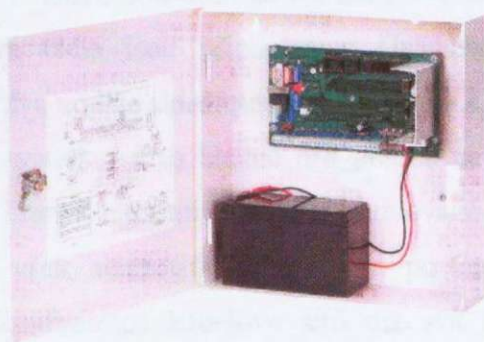
### 2.6.7 Další systémy venkovního zabezpečení

V oblasti venkovní perimetrické ochrany se každoročně objevují novinky využívající nových principů či modifikující principy stávající. Z těchto nových systémů lze zmínit plošnou ochranu použitím rotujících laserů či využití optických vláken vpletených přímo do osnovy pletiva. Stále více se rozšiřuje nabídka videosenzorů s počítačovým vyhodnocením a archivací záběrů, které v kombinaci s kamerovými systémy částečně přebírají funkci zabezpečení venkovního perimetru. Výhodou těchto systémů je přídavná optická informace o dění v místě vyhlášení poplachu. Takové systémy však nesplňují kritéria na EZS ve smyslu zálohování a ochrany vedení proti sabotáži. Vhodným návrhem a výběrem použité techniky však lze částečně eliminovat i tyto nedostatky. Normativně však nejsou tyto případy nijak ošetřeny.

## 2.7 Ústředny EZS

Ústředna elektrické zabezpečovací signalizace je zařízení, které:

- přijímá a vyhodnocuje výstupní elektrické signály od čidel EZS,
- ovládá signalizační, přenosová, zapisovací a jiná zařízení, která indikují narušení,
- napájí čidla a další prvky EZS elektrickou energií,
- pomocí elektromechanických nebo kódových zámků, popřípadě vlastních ovládacích klávesnic, umožňuje uvedení celého systému EZS nebo jeho částí do stavu střežení a do stavu klidu,
- umožňuje diagnostiku systému EZS.



Obr. 9 Ústředna EZS

Ústředny EZS lze rozdělit do čtyř hlavních skupin:

- ústředny smyčkové,
- ústředny s přímou adresací čidel,
- ústředny smíšeného typu,
- ústředny s bezdrátovým přenosem poplachového signálu od čidel.

### 2.7.1 Smyčková ústředna

Tato ústředna má pro každou poplachovou smyčku vstupní vyhodnocovací obvod. Obvod je řešen pro připojení proudových smyček o definované hodnotě a toleranci. Smyčka je zakončena zakončovacím odporem tak, aby vykazovala předepsanou hodnotu odporu pro příslušný typ ústředny. Změna odporu smyčky, způsobená aktivací některého z čidel smyčky nebo sabotáží na smyčce, vede k vyhlášení poplachového stavu systému EZS. Poplachové smyčky systému EZS jsou většinou tvořeny sériovým zapojením rozpínacích kontaktů čidel.



Systém EZS se smyčkovou ústřednou má poměrně rozsáhlou kabelovou síť, neboť ke každému čidlu musí být přiveden kabel příslušné smyčky, kabel musí obsahovat dva vodiče pro napájení čidla (u napájených čidel), dva vodiče pro poplachový kontakt čidla, dva vodiče pro sabotážní kontakt čidla a dále vodiče dodatkových funkcí typu paměť poplachu, test chůzí, odpojení vysílače ultrazvuku či mikrovláknového výkonu, indikace překrytí čidla (antimasking) apod.

### **2.7.2 Ústředna s přímou adresací čidel**

Tato ústředna pracuje na principu komunikace po datové sběrnici ústředna - čidla. Ústředna periodicky generuje adresy jednotlivých čidel a přijímá příslušné odezvy. Každé čidlo je vybaveno komunikačním modulem. Kabelová síť tohoto systému je minimální neboť je tvořena prakticky libovolnou konfigurací kabelové sítě (s max. délkou řádově stovky metrů), jednotlivá čidla jsou připojena v libovolném pořadí na zpravidla čtyřvodičové vedení, kde dva vodiče slouží pro napájení čidla a dva jako datová sběrnice. Velkou výhodou tohoto systému, a to hlavně pro přenos na PCO je, že při narušení objektu ústředna oznámí, které konkrétní čidlo bylo aktivované a jaký je druh narušení.

Tento typ ústředny však neumožňuje realizovat po datové sběrnici dodatečné funkce čidel a rovněž konfigurace kabelové sítě má svá omezení. Jako například celkovou délku vedení, a s tím spojené úbytky na napájecích vodičích pro jednotlivé části systému, a také možnost indukovaní elektromagnetického rušení. Typický počet přímo adresovatelných čidel se u systémů tohoto typu pohybuje řádově v desítkách.

### **2.7.3 Ústředna smíšeného typu**

Tato ústředna pracuje na principu datové komunikace ústředna - koncentrátor (sběrnice modul smyček). Komunikace mezi ústřednou a koncentrátory probíhá pomocí datové či analogové sběrnice. Na koncentrátory jsou čidla připojena pomocí smyček jako u smyčkových ústředen. Vlastní vyhodnocování probíhá podle typu ústředny různě. Jednou z variant je analogový multiplex, kdy se připojují na sběrnici postupně jednotlivé smyčky a vyhodnocení impedance smyčky s příslušnou odezvou provádí ústředna. Další možností je integrace vyhodnocovací logiky včetně vyrovnávací paměti přímo do koncentrátoru. Komunikace pak probíhá čistě v datové podobě.

Pokud je kapacita ústředny dostatečná, lze na jednotlivé vstupy koncentrátorů připojit přímo jednotlivá čidla. Tím přechází tento typ ústředny na ústřednu s přímou adresací čidel. Obdobně jako u předešlé skupiny ústředen, je důležité dostatečné dimenzování napájecích i datových vodičů zvláště u rozsáhlých systémů. Tato skupina většinou umožňuje realizaci dodatkových funkcí přímo přes datovou sběrnici.



## 2.7.4 Ústředny s bezdrátovým přenosem signálu od čidel

Tyto ústředny většinou pracují v pásmu telemetrie (433 MHz) s výkony okolo 10 mW. Přenos poplachového signálu od čidel nejčastěji bývá 8bitový, kódovaný a adresa čidla je 4bitová. Vhodným návrhem je dosaženo minimálního klidového odběru (cca 10-20  $\mu$ A).

Vlastní dosah je ve volném prostředí 100 - 200 m. V objektu jsou to vzdálenosti o něco menší. Čidla jsou napájena buď lithiovou baterií, nebo 9V destičkovým článkem. Napětí baterie je hlídáno a podle provedení buď dojde při poklesu napětí k místní akustické signalizaci interním bzučákem nebo je tato informace přenášena do poplachové ústředny.

Výhodou bezdrátových systémů je rychlá a snadná instalace, možnost instalace do hotových objektů s minimalizací stavebních zásahů, snadné rozšíření systému doplněním dalších prvků a také snadná změna konfigurace (tzn. možnost jednoduchého přemístění detektorů, například při přestavení nábytku).

### 2.7.4.1 Systémy s jednosměrnou komunikací

Jednodušší systémy pracují jednosměrně, tzn., že v čidle je vysílač a v ústředně přijímač. Starší systémy tohoto řešení neměly žádnou kontrolu funkčnosti jednotlivých detektorů (s výjimkou výše popsané indikace poklesu napájecího napětí pod stanovenou mez). Jestliže tedy došlo k poruše prvku nebo jeho násilnému poškození či odcizení, nedostala o tom ústředna žádnou informaci. Modernější systémy pracují na principu pravidelné kontroly přenosové cesty vysíláním kontrolních zpráv. Problémem zde je rozpor mezi požadavkem na co nejvyšší četnost kontrol a požadavkem na velkou trvanlivost baterií napájejících jednotlivé prvky. V praxi se proto obvykle pracuje s četností jednou za několik hodin. To ovšem znamená, že je ústředna o nefunkčnosti prvku informována s určitým zpožděním. Jestliže u takového to systému pachatel poškodí detektor, může uživatel systém zapnout s přesvědčením, že bude mít objekt během své nepřítomnosti náležitě chráněn. Vzhledem k tomu, že je nutné vyloučit nebo alespoň omezit plané poplachy vzniklé následkem náhodných výpadků signálu, způsobené nejrůznějšími příčinami, vyhodnocuje se obvykle stav jako poruchový nebo poplachový až tehdy nedojde-li několik po sobě jdoucích kontrolních relací (nejméně dvě). Tím se ovšem dále prodlužuje doba během níž systém nemusí zaznamenat poplach nebo poruchu. Jednosměrný systém má značnou nevýhodu také tam, kde je velký pohyb osob. Vzhledem k tomu, že jednotlivé prvky nemají informaci o tom, zda je systém v klidu nebo ve střežení, musejí vždy v okamžiku zjištění poplachového stavu vyslat signál



ústředně. Ta sice v klidovém stavu takovou informaci jako poplach nevyhodnotí, ale každé takové to vysílání vyčerpává energii napájecího zdroje. V praxi se to řeší obvykle tak, že je detektor vybaven časovačem blokujícím vysílání po odeslání zprávy po dobu několika minut. To sice šetří energii zdroje, ale zároveň to ztěžuje následné vyhodnocení pohybu pachatele, protože jeho pohyb po první aktivaci není v dalších minutách monitorován.

Jednou z nevýhod bezdrátových systémů je nebezpečí rušení. To může vést jak ke vzniku falešných poplachů, tak ke ztrátě přenosu. U jednosměrných systémů je relativně snadné zjistit, na jakém kmitočtu a s jakou modulací systém pracuje. Lze jej pak poměrně jednoduše vyřadit z činnosti zahlcením přijímače stejným kmitočtem o podstatně vyšší intenzitě.

#### **2.7.4.2 Systémy s obousměrnou komunikací**

Nejnovější typy bezdrátových systémů pracují duplexně a každý prvek systému je vybaven jak vysílací, tak přijímací elektronikou - modulem vysílač/přijímač. Tyto inteligentní moduly jsou schopny si najít ve vyhrazeném kmitočtovém pásmu dva volné kanály pro přenos a automaticky se na ně naladit. V případě rušení těchto kanálů jsou schopny přeladit se na jiné, nezarušené. Zavedení obousměrné komunikace mezi ústřednou a všemi prvky zabezpečovacího systému odstraňuje jmenované nedostatky jednosměrných systémů.

Přednosti systémů s obousměrnou komunikací:

- při zapínání systému si ústředna ověří stav všech prvků,
- čidla v klidovém stavu nevysílají, a neplýtvají proto energií, navíc nemusejí být vybavena blokováním dalšího vysílání po vyslaném poplachu,
- dálkově lze zapnout test chůzí,
- lze uskutečnit funkci automatického přeladění při rušení jako významný faktor zvýšení odolnosti proti úmyslnému i neúmyslnému přerušení přenosu,
- ústředna si může ověřit, zda je došlá poplachová informace skutečný poplach, což umožní vyloučit plané poplavy způsobené rušením.

Jako díly bezdrátových systémů existují bezdrátová čidla pohybu (většinou PIR), bezdrátová tísňová tlačítka, bezdrátové magnetické kontakty, univerzální bezdrátové moduly pro připojení libovolných čidel, stabilní bezdrátové ovládací díly, mobilní bezdrátové ovládací díly, bezdrátové sirény atd.

#### **2.7.4.3 Kódování přenosu a prvků**

Samozřejmým požadavkem u bezdrátových prvků je kódování komunikace mezi



jednotlivými prvky systému. To znemožňuje zkreslení během přenosu a znesnadňuje neoprávněné proniknutí do systému s cílem jeho vyřazení z provozu. Kromě toho je nutné jednotlivé prvky v systému identifikovat. U jednodušších systémů se kódování prvků uskutečňuje obvykle naprogramováním mechanickými přepínači binárním způsobem (tzv. DIP - switch), případně programováním pomocí připojeného počítače. U složitějších systémů mají prvky kód pevně přidělen již při výrobě a jejich čísla se programují do ústředny při instalaci systému. Tím je znesnadněno cílené nahrazení prvku s konkrétní adresou při pokusu o kvalifikované nabourání systému.

### 2.7.5 Vstupní vyhodnocovací obvody

Jednotlivá čidla EZS jsou pomocí vícežilového stíněného kabelu zapojena do poplachové nebo tísňové a sabotážní smyčky. Elektrické parametry všech druhů smyček jsou shodné, liší se pouze způsobem hlášení svého narušení. Počet vstupů smyček je dán typem ústředny a může se prakticky pohybovat od čtyř až po stovky smyček.

Vstupní obvody nejjednodušších ústředen bývají obvykle velmi primitivní a jsou schopny vyhodnotit dva základní stavy, a to „smyčka uzavřená“, nebo „smyčka rozpojená“. Jako správný funkční stav se volí stav „smyčka uzavřená“, neboť pak každý destruktivní zásah do čidla nebo kabelové sítě vede k poplachovému stavu „smyčka rozpojená“.

Vstupní vyhodnocovací obvody ústředen vyššího stupně zabezpečení (dle ČSN EN 50131-1) jsou dokonalejší a pracují jako přesné odporové děliče nebo jako vyvážené měřicí můstky, u kterých je napětí na děliči nebo v diagonále můstku úměrné velikosti rozvážení děliče nebo můstku. Toto „chybové“ napětí je přiváděno na obvod napěťového komparátoru, který při překročení určité meze překlopí svůj výstup, a způsobí tak odpovídající reakci v logických obvodech ústředny. Takový vstupní obvod ústředny musí být zakončen odporem o definované hodnotě a toleranci. Odpory zpravidla dodává výrobce spolu s ústřednou a dle typu ústředny se pohybují v rozmezí od 1 k $\Omega$  do 12 k $\Omega$ . Ústředny pracují s rozvážením vstupního odporu v rozmezí  $\pm 30\%$  až  $\pm 2\%$ .

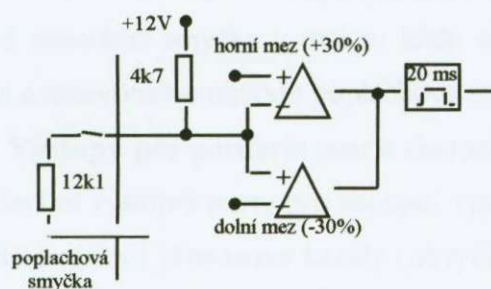
Vedle klasické vyvážené diferenciální smyčky se s rozvojem techniky A/D převodníků objevují i systémy s tzv. dvojitě vyváženou smyčkou, kdy je možné pomocí jediného smyčkového vedení vyhodnotit jak poplachové hlášení, tak i neoprávněný zásah do čidla či přerušení smyčkového vedení.

Vstupní obvody bývají obvykle vybaveny ochrannými prvky (jiskřiště, varistory) pro ochranu před účinky elektromagnetického rušení vnikajícího indukci do kabelové sítě

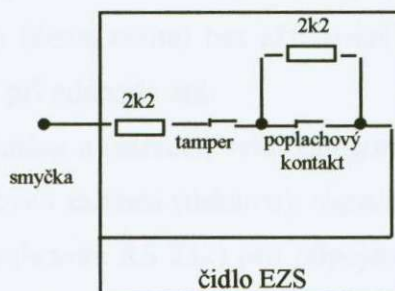


nebo účinky atmosférické elektřiny. Z tohoto důvodu je také nezbytné provádět všechny rozvody smyček stíněnými vodiči. Stínění jednotlivých kabelů je třeba dobře propojit, a to tak, že nesmí tvořit uzavřenou zemní smyčku. V praxi to znamená, že je stromovitě propojeno stínění všech kabelových větví a stínění pak připojeno na svorku PE sítě v ústředně EZS.

Funkční vlastnosti jednotlivých vstupních obvodů ústředen z hlediska hlášení v rámci systému jsou buď pevně dané (tíseň, sabotáž, vloupání, poplachové smyčky zpožděné, poplachové smyčky okamžité), nebo programovatelné. Pak je možné podle konkrétní aplikace měnit vlastnosti jednotlivých smyček z hlediska funkce systému EZS.



Obr. 10 Technické řešení vstupního obvodu vyvážené diferenciální smyčky.



Obr. 11 Zapojení tzv. dvojité vyvážené smyčky.

### 2.7.6 Výstupní obvody

Výstupní obvody ústředen EZS umožňují aktivovat výstupní signalizační a indikační obvody a prvky systému EZS. Patří sem zpravidla tyto výstupy:

- **Výstup pro akustickou signalizaci**, kterou je zpravidla pasivní nebo aktivní siréna. Výstup pro akustickou signalizaci bývá obvykle programovatelný a umožňuje volit dobu funkce sirény (podle ČSN EN 50131-1/Z1), dobu zpoždění sirény, přerušování zvuku sirény, modulaci zvuku sirény, popřípadě volit chování výstupu podle toho, jakým typem smyčky byl poplachový stav aktivován.
- **Výstup pro optickou signalizaci**, kterou je zpravidla zábleskový maják. Tento výstup se obvykle spíná současně s výstupem pro akustickou signalizaci, ale zůstává aktivní i po jejím doznění, a to až do doby vynulování ústředny. Někdy bývá též programovatelný.
- **Výstup telefonního voliče** je uzpůsoben pro připojení k JTS. Tento výstup buď kódem, nebo hlasově oznámí na zvolená telefonní čísla předem naprogramované údaje nebo předem namluvenou zprávu. Umožňuje tak přivolání pomoci i v případě, kdy



pachatel zneškodní sirénu a maják nebo když na jejich činnost nikdo nereaguje. Je-li ústředna připojena na pult centralizované ochrany, sdělí pak pomocí kódovaného přenosu zprávy v příslušném formátu o jaký typ narušení objektu se jedná, případně která část objektu je narušena. U tohoto typu spojení se často využívá tzv. tichý poplach, tedy poplach bez aktivace sirény a majáku.

- **Programovatelné výstupy** umožňují vytvořit potřebné výstupní signály ať již impulsní (např. pro resetování čidel s pamětí), nebo definovaných úrovní pro různé periferie (inteligentní sirény, přenosy pro diagnostiku systému EZS atd.).
- **Pomocné zvukové výstupy** slouží pro připojení jednoho nebo více reproduktorů, umožňují zvukové indikace například otevření dveří (dveřní gong), náběhu odchodového intervalu (zpoždění zapnutí smyčky), náběhu vstupního intervalu (zpoždění poplachu), narušení sabotážní smyčky v režimu klidu objektu (denní režim) bez aktivování sirény, indikaci neuzavřeného obvodu poplachové smyčky při odchodu atd.
- **Výstupy pro periferie** jsou k dispozici zejména u ústředn vyší kategorie. Jsou to především výstupní porty pro napojení registračních zařízení (tiskáren), signalizačních tabel, dále sériové přenosové kanály (obvykle s rozhraním RS 232) pro připojení PC či programovacích modulů.
- **Bezpotenciálové výstupy** jsou tvořeny obvykle přepínacími kontakty relé. Počet relé bývá omezený a podle typu se pohybuje do počtu 32. Pomocí těchto výstupů lze vytvářet atypické funkční vazby mezi systémem EZS a dalšími doplňkovými bezpečnostními systémy, jako jsou např. uzavřené televizní okruhy (CCTV), systémy kontroly a řízení vstupu osob do objektu nebo systém aktivace osvětlení objektu poplachovým signálem.

### 2.7.7 Napájecí obvody

Napájecí obvody slouží k napájení elektronických obvodů vlastní ústředny a k napájení všech návazných prvků systému EZS. Protože systém EZS musí být funkční i při výpadku napájecího napětí sítě, je napájecí zdroj ústředny zálohován náhradním zdrojem napětí. Ten je tvořen bezúdržbovými plynotěsnými olověnými akumulátory. Lze z nich vytvořit náhradní zdroj s kapacitou 1,2 Ah až řádově 100 Ah.

Síťový napájecí zdroj dodává stabilizované napětí +13,8 V se zatížitelností odpovídající rozsahu systému EZS 1 A až 5 A. Pokud je systém EZS rozsáhlejší, pak je nezbytné použít přídavný síťový napájecí zdroj s vlastním náhradním zdrojem napětí. Přídavné síťové napájecí zdroje se dodávají se zatížitelností od 1 A do 10 A.

**Základní napájecí zdroj** - zdroj elektrické energie pro trvalé napájení zařízení



EZS. Musí být schopen dodat potřebný proud, jenž je součtem proudových odběrů všech prvků systému na daný zdroj připojených včetně ústředny. Dále musí být základní zdroj dimenzován tak, aby po skončení nejdějšího výpadku sítě byl schopen dodat potřebný proud nejen pro všechny prvky na zdroj připojené, ale i proud potřebný k dobíjení připojeného akumulátoru či akumulátorů během stanovené doby.

**Náhradní napájecí zdroj** - zdroj elektrické energie pro napájení zařízení EZS při výpadku základního zdroje. Musí být dimenzován tak, aby byl schopen překlenout nejdější výpadek základního zdroje dle požadavků normy ČSN 50131-1 (ČSN EN 50131-6), odlišný pro jednotlivé stupně zabezpečení vztažený k úrovni rizik objektu.

Tab. 3: Požadované doby zálohování a doby nabíjení systému EZS.

	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Minimální doba pohotovosti v hodinách (dle ČSN EN 50131-1)	12	12	60	60
Minimální doba pohotovosti v hodinách (dle ČSN EN 50131-6)	8	15	24	24
Maximální doba dobíjení v hodinách na min. 80% kapacity	72	72	24	24

## 2.8 Ovládací a indikační zařízení

Ovládací zařízení jsou určena k tomu, aby bylo možno uvádět systém EZS do stavu střežení a naopak do stavu klidu. Vhodný typ ovládacího zařízení se volí podle úrovně rizik (stupně zabezpečení). Požadavky jsou na jednoduchou obsluhu s minimalizací možnosti vyvolat při manipulaci s ovládacím zařízením planý poplach za současné dostatečné ochrany proti kvalifikovanému překonání.

Ovládací a indikační zařízení kromě základní funkce slouží také pro:

- odpínání a připínání smyček (pro případ částečného střežení),
- volbě speciálních funkcí (např. tísňové hlášení z klávesnice, testování funkce čidel, vyvolání paměti dějů apod.),
- zadávání uživatelských kódů pro ovládání systému,
- programování instalačních parametrů systému,
- odstavení a resetování poplachů atd.

Indikační prvky informují o provozních stavech ústředny a celého systému, a to buď opticky pomocí LED, nebo pomocí akustické signalizace, popř. kombinací akustické a optické signalizace. U ústředny s vyšším ovládacím komfortem probíhá komunikace s uživatelem pomocí alfanumerického displeje.

V podstatě u všech druhů ovládacích zařízení nalezneme funkce hlášení základních stavů jako je:

- hlášení stavu střežení/klid systému EZS,
- hlášení připravenosti k uvádění do stavu střežení,
- hlášení poruchy (základního či náhradního zdroje),
- hlášení narušení smyček,
- hlášení tísně (přepadení),
- hlášení poplachu.

### **2.8.1 Blokovací zámek**

Blokovací zámek kombinuje prvek mechanického zabezpečení vstupních dveří spolu s ovládním systému EZS. Montuje se jako přídatný zámek vstupních dveří. Je to nejbezpečnější, a zároveň z hlediska uživatele nejjednodušší druh ovládacího zařízení. Vlastní konstrukcí je zajištěno spolehlivé uvádění do stavu střežení a naopak. Zámek lze uzamknout jedině tehdy, je-li systém v normálním stavu. V případě poruchy či opomenutí obsluhy (např. otevřené okno) elektromagnetická západka znemožní uzamčení blokovacího zámku, a tím i uvedení systému do stavu střežení. Jde-li zámek uzamknout, má uživatel jistotu, že je systém v pořádku.

Naopak při vstupu do objektu má uživatel jistotu, že je systém odblokován, neboť nejdříve musí odemknout, aby mohl vstoupit. Odemknutím blokovacího zámku přejde systém automaticky do stavu klidu objektu.

Podle provedení blokovacího zámku jej lze osadit buď cylindrickou vložkou, nebo je jeho součástí motýlkový či křížový zámek odolný proti vyhmatání a rozlomení. Vlastní zámek je rovněž chráněn proti odvrtní celoplošným vodivým meandrem zapojeným do samostatné zajišťovací smyčky. Ovládací vedení je rovněž elektricky střeženo, popř. podle typu ústředny je chráněno sabotážní smyčkou.

### **2.8.2 Spínací zámek**

Je to ovládací zařízení podobné blokovacímu zámku, ovšem bez blokovací elektromagnetické západky.

Lze jej využít k odpojování smyček (umožňuje-li to ústředna) či k ovládní ústředny EZS. Pro kontrolu se spínací zámky doplňují optickou nebo akustickou signalizací.



### **2.8.3 Kódové klávesnice**

Funkčně mohou být využity jako spínací zámky. Pro využití jako ovládacího dílu ústředny EZS je však nezbytné, aby elektronika klávesnice byla v samostatné skříni a byla umístěna ve střežených prostorech. Mimo střežené prostory je pak možné umístit pouze tlačítkové pole a indikace. Některé typy vybavené více výstupy relé lze využít pro ovládání elektrického vrátného, pro spínání osvětlení apod. Pro uživatele však kódové klávesnice přinášejí určité nároky v podobě zapamatování si správného kódu a jeho občasné změny.

### **2.8.4 Kombinované indikační a ovládací díly**

Umožňují spolu s ovládaním systému, také indikovat informace o systému. Jako příklad lze uvést kódovou klávesnici s displayem, na kterém je zobrazován stav systému. Kombinované indikační a ovládací díly jsou používány i pro nejvyšší úroveň rizik. Lze je užít i jako vnitřní indikační tablo pro potřeby uživatele či najaté hlídací služby. Vlastní připojení k ústředně je řešeno většinou prostřednictvím datové sběrnice, která je u systémů pro vyšší rizika elektronicky hlídána proti napadení.

### **2.8.5 Ovládání kartou**

Zvláště v poslední době se začínají objevovat na trhu poplachové ústředny EZS, jež umožňují spolupráci se čtečkou identifikačních karet. Tento trend je prosazován zvláště u integrovaných systémů, kde v rámci celého komplexu musí spolu korespondovat EZS, systém průmyslové televize (CCTV), přístupový systém, elektronický požární systém (EPS) a další slaboproudé systémy.

Cílem takových snažení je, aby ve finále uživatel pomocí jediného média (karty) vjel do garáží, ohlásil svou přítomnost v práci, dostal se do výtahu, navolil své patro, odpojil ze střežení svou kancelář, vstoupil do ní, pohyboval se po areálu podniku, přes den na kartu nakupoval v kantýně, platil výkony závodního lékaře, vybíral obědy v jídelně atd.

## **2.9 Doplnková zařízení ústředen EZS**

Pod pojmem doplnková zařízení ústředen EZS rozumíme všechna samostatná zařízení, jež jsou umístěna buď v krytu ústředny, nebo mimo ni, a jsou řízena řídicími výstupy ústředny.

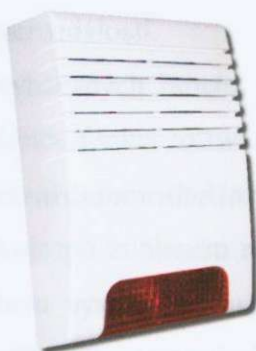
### **2.9.1 Akustická signalizace**

Nejrozšířenějším instalovaným doplnkovým zařízením je akustická signalizace (siréna) (viz. obr. 11). Podle provedení může být určena pro vnitřní či venkovní

prostředí. Základem je vždy akustický měnič (piezoelektrický či dynamický) doplněný generátorem kolísavého tónu a výkonovým zesilovačem . Méně časté je využití sirén s motorovým pohonem. Akustický výkon je stanoven v technických požadavcích na zařízení. Doba aktivace by měla být omezena (viz. norma ČSN EN 50131-1).

Nejčastěji se umisťují sirény na průčelí střeženého objektu do výšky, která je pokud možno nedostupná bez použití žebříku, štaflí či montážní plošiny. V dnešní době jsou nejrozšířenější tzv. „inteligentní“ sirény s vlastním zálohováním.

S poplachovou ústřednou je siréna propojena vícežilovým kabelem, který slouží k ovládní řídicího vstupu sirény rozpínacím kontaktem bezpotenciálového relé ústředny, popř. výstupem otevřeného kolektoru spínacího tranzistoru, a dále také k dobíjení zálohovacího akumulátoru a k přivedení sabotážní smyčky sirény. Inteligentní siréna je pak aktivována nejen regulérním poplachem systému, ale i přerušením kabelového propojení ústředna - siréna, pokusem o odstranění pláště sirény či pokusem o sejmutí sirény se zdi. Některé sirény mají uvnitř také optoelektronický hlídací modul, který aktivuje poplach při pokusu o odstavení sirény zapněním vnitřku krytu skrz akustickou mřížku, jiné řeší tento problém pomocí dvojitého krytu speciální konstrukce.



*Obr. 12 Inteligentní siréna*

### **2.9.2 Optická signalizace**

Optická signalizace (světelný maják) bývá často součástí krytu venkovních sirén. Technicky se jedná o výkonovou 12 V žárovku buzenou přes elektronický přerušovač, nebo o výbojku buzenou z vlastní elektroniky. Doporučená barva optické signalizace je oranžová. Z hlediska vlastní funkce je účelné, aby řízení umožňovalo časově neomezenou aktivaci v případě vyhlášení poplachu. Smysl tohoto opatření spočívá v možnosti identifikace narušeného objektu i po doznění sirény v případě umístění více střežených objektů nedaleko od sebe.



### 2.9.3 Grafická tabla

U rozsáhlých objektů slouží grafická tabla k usnadnění orientace obsluhy při ovládání systému, a hlavně v případě vyhlášení poplachu. Tato tabla jsou v podstatě panely s vyznačeným plánem objektu doplněné o indikační žárovky či LED a prosvětlené symboly.

V dnešní době jsou grafická tabla nahrazována obrazovkou počítače s implementovaným speciálním ovládacím a grafickým softwarem.

### 2.9.4 Tiskárny

Pro potřebu pozdější analýzy událostí, k nimž došlo ve střeženém objektu, ale i pro případnou kontrolu činností obsluhy spojenou s ovládáním rozsáhlých systémů EZS, bývaly ústředny vybaveny zabudovanými tiskárnami. Tiskárna zpravidla zaznamenávala čas a událost (místo napadení, přepínání ústředny EZS, odpínání smyček, poruchy, odstavení a resetování poplachů atd.)

S rozvojem mikroelektroniky, se zavedením mikropočítačů do řídicích jednotek ústředny EZS, a hlavně s poklesem ceny polovodičových pamětí je archiv událostí většinou řešen v elektronické podobě, má dostatečnou kapacitu (řádově 10 - 1000 událostí) a možnost připojení tiskárny zůstává jen pro případy výpisu dějů v případě potřeby zpětné analýzy poplachových událostí.

U rozsáhlých systémů EZS vybavených řídicím počítačem je jako archiv událostí využit pevný disk. Výtisk je pak běžnou funkcí softwarové podpory.

### 2.9.5 Poplachová přenosová zařízení (komunikátory)

Přenosové zařízení zprostředkuje po zvoleném médiu (JTS, vzduchem, po privátní komunikační síti) informaci o stavu systému či narušení objektu majiteli nebo na monitorovací pracoviště hlídací služby. Přenos poplachových signálů je samostatná úloha vymezená funkcí poplachového přenosového systému. Tato oblast je normalizačně popsána souborem norem řady ČSN EN 50136++.

### 2.9.6 Zařízení určená pro informování majitele objektu

Mezi nejjednodušší patří tzv. automatické telefonní hlásiče (ATH), které umožňují na naprogramované telefonní číslo po vyhlášení poplachu automaticky zavolat a předat zprávu o trvání 20 - 30 s uloženou v paměťovém digitálním řečovém modulu. Volbu telefonního čísla lze vícekrát opakovat, některá zařízení mají možnost volit více různých čísel, jiná mají doplněk pro kontrolu stavu telefonní linky. Moderní typy umožňují v součinnosti s digitální ústřednou JTS uvolnit obsazené telefonní číslo nebo poslat prostřednictvím JTS krátkou textovou zprávu (SMS) na mobilní telefon nebo pagerovou



službu. V objektech bez telefonní linky (JTS) je možné aplikovat komunikátor v podobě GSM brány, která vedle vyslání poplachové zprávy umožňuje případné dálkové ovládání elektrických zařízení nainstalovaných v objektu.

### **2.9.7 Zařízení určená pro komunikaci s PCO/PPC**

Jsou to zařízení sloužící k předávání informací o systému EZS monitorovacím pracovištím hlídacích služeb (PCO/PPC).

Zařízení na principu automatické telefonní volby (ATV) komunikují s obsluhou PCO již nikoliv hlasitým vzkazem, ale s vyhodnocovacím zařízením pomocí určitého kódu, který obsahuje adresu objektu a druh předávané zprávy. Jsou závislá na přítomnosti JTS. Dříve diskutovaný problém možnosti napadení především nadzemních a povrchových telefonních vedení je již minulostí. V odůvodněných případech však je žádoucí použít dvě nezávislé přenosové cesty. Jedna z nich může být JTS, druhá pak elektromagnetické pole. Jsou však i případy, kdy z různých důvodů není JTS k dispozici. Pro takové případy slouží přenosová zařízení s datovou komunikací ve vyhrazených pásmech elektromagnetického spektra. Jedná se v podstatě o vysílače s výkony řádově 1 - 10 W uzpůsobené pro přenos datových informací přímo z datových výstupů ústředěn EZS či konvertovaných do datové podoby z jiných výstupů ústředěn (výstupní relé, výstupy otevřených kolektorů tranzistorů apod.). Nejdokonalejší systémy umožňují oboustrannou komunikaci, a tím také možnost monitorování stavu přenosové trasy.

Použité formáty přenosu po JTS jsou normalizovány. V závislosti na použitém vyhodnocovacím zařízení (PCO) je zvolen správný formát přenosu tak, aby si ústředna EZS s monitorovacím pultem „rozuměla“. Rovněž u bezdrátových systémů používají výrobci standardizované formáty.

### **3. Elektronická zabezpečovací zařízení pro motorová vozidla**

Jestliže mechanická zabezpečovací zařízení zabraňují pachateli s vozidlem odjet mechanickým blokováním důležitých systémů vozidla, pak elektronická zabezpečovací zařízení vozidla dokáží signalizovat manipulaci s vozidlem či přímo vstup do vozidla např. v podobě hlasité akustické signalizace, případně vysláním signálu upozorňujícího majitele o vzniklé situaci či mohou přímo znepojídnit vozidlo. Tato zařízení lze rozdělit do tří podskupin na zařízení :

- chránící plášť, vnitřní prostory nebo bezprostřední okolí automobilu
- zabraňující nastartování či umožňující zastavení vozidla
- umožňující jeho vyhledání



### 3.1 Systémy EZS pro motorová vozidla

Autoalarmy patří k nejčastěji nasazovaným systémům v široké škále různých zabezpečovacích zařízení automobilů.

Poskytují široké možnosti uspokojení přání majitele o zabezpečení svého vozidla. Nejjednodušší systémy reagují na pokusy vniknutí do auta otevřením dveří, jiné na otřesy či rozbití oken vozidla, další na pokusy o nastartování vozidla neoprávněnou osobou, případně na pohyb uvnitř vozu nebo v jeho blízkém okolí.

Jednotlivé systémy autoalarmu se skládají ze čtyř základních částí:

- čidla
- řídicí jednotky
- ovládací prvky
- signalizační zařízení

### 3.2 Čidla

Z hlediska způsobu zabezpečení lze čidla pro elektronickou ochranu automobilů rozdělit na čidla obvodové ochrany a čidla prostorové ochrany a další účinná čidla.

#### 3.2.1 Čidla obvodové ochrany

Chrání dveře a víka motoru a zavazadlového prostoru automobilu. Patří sem

##### 3.2.1.1 Kontaktní čidla

U tohoto typu ochrany se v základní sestavě používají "kontaktní čidla" a to buď ta, která jsou ve vozidle již zabudována jako spínače vnitřního osvětlení, a nebo pokud chybí, např. u zadních dveří, kapot, jsou v soupravách autoalarmů dodávány další spínače. Jejich spolehlivost je dobrá a detekce vniku do vozidla jednoznačná.

##### 3.2.2 Čidla prostorové ochrany

V zásadě lze k této ochraně používat čidla ultrazvuková a mikrovlnná

##### 3.2.2.1 Ultrazvuková čidla

Jsou s úspěchem používána pro ochranu vnitřního prostoru vozidla, např. při narušení oken, vykrádání uložených věcí apod. V současné době se vyrábějí ve dvojím provedení a to, jako dělená (vysílač + přijímač) nebo monolitní. V zimním i letním období právě u vozidel vzniká základní problém s tvorbou tepelných kumul (malý interiér vozidla a velké teplotní difference teploty na povrchu a uvnitř vozidla), které po

určité době po odstavení vozidla putují objemovým prostorem a generují falešný poplach simulací pohyblivého předmětu. Dalším častým zdrojem falešných poplachů ultrazvukových čidel bývá hmyz létající v uzavřeném interiéru, případně nedodržení podmínky uzavření všech oken včetně střešního (aktivační pohyb v blízkosti vozidla). Za tímto účelem jsou některé autoalarmy vybaveny možností selektivního zapínání a vypínání ultrazvukového čidla.

#### **3.2.2.2 Mikrovlnná čidla**

Některé problémy ultrazvukových čidel platí v určité formě i pro čidla mikrovlnná. Výhodou mikrovlnných čidel je možnost vhodného zabudování do interiéru vozidla např. pod plastový povrch.

#### **3.2.3 Ostatní čidla**

Ostatní typy čidel pro zabezpečení vozidel.

##### **3.2.3.1 Otřesová a náklonová čidla**

U jednoduchých systémů se používají kontakty zatížené malým závažím, které reaguje na větší či menší náraz, což může být problematické. Stačí, když kolem projede tramvaj nebo těžší vozidlo a může dojít k vyhlášení poplachu, jehož příčinou může být i nesprávné seřízení systému. Modernější čidla používají jako detekční prvek piezokrystal u něhož je jednodušší nastavení citlivosti. Důmyslnější náklonové systémy eliminují plané poplachu tím, že vyhodnocují signál o změně polohy vozidla po určitou dobu a teprve při splnění určitých časových hodnot dojde k vyhlášení poplachu. Do této kategorie patří i gyroskopické, resp. deprezské mechanicky tlumené systémy, které mají mnohem lepší parametry než klasická levná čidla.

##### **3.2.3.2 Čidla rozbití skla**

Výhodou je, že mohou být zapojena trvale, tzn. i v přítomnosti osob ve vozidle a "nevýhodou" vzhledem k tomu, že jsou iniciovány pouze rozbitím oken, musí být kombinovány s dalšími čidly např. reagujícími na otevření dveří či pohyb uvnitř vozidla.

### **3.3 Řídící jednotky**

Řídící jednotka je centrálním prvkem elektronického systému zabezpečení automobilů. Její provedení musí umožňovat snadnou montáž, obsahovat nejen části reagující na signál čidel, ale i vstupy, umožňující majiteli ovládat zařízení, nastavit časovou prodlevu pro aktivaci systému (odchodové a příchodové zpoždění bez vyhlášení poplachu). Složitější systémy mohou plnit i funkce, které se netýkají zabezpečení vozu. Pokud je např. zařízení vybaveno čidlem pro příjem signálu z dálkového ovládače a ten disponuje více kanály, při patřičném vybavení vozu může



řidič díky "autoalarmové ústředně" na dálku ovládat zámky dveří, zapnout nezávislé topení, odpojit prostorové čidlo a ponechat aktivní pouze obvodovou ochranu.

Vyhodnocovací jednotka samozřejmě hlídá veškeré kódování vstupu a výstupů. Pokud jsou kódy pevné, pouze je ověřuje, u plovoucích kódů ústředna sama mění jejich nastavení.

### 3.4 Ovládací prvky

Ovládacím prvkem autoalarmu v levnějším a jednodušším provedení může být **vypínač** (který si z důvodu utajení majitel zpravidla montuje sám na zvolené místo), speciální či běžný **klíč** (je-li napojen na skříňku zapalování), **kódový zámek** či u dražších a složitějších provedení **bezdrátové dálkové ovládání** (infračervené nebo radiové). Hodně se hovoří o ochranách proti tzv. rozkódování autoalarmu. Jde např. o systém "*scanning*" -postupné napodobování kódové informace, kdy během krátkého času lze pomocí scanneru vyslat statisíce signálů. Ve chvíli nalezení kódu má pachatel možnost úspěšně vniknout do automobilu. Ochranu proti rozkódování autoalarmu, tzv. **antiscanning**, lze provést elektronicky nebo programováním. Nové ústředny totiž po přijetí několika nesprávných signálů celý systém na nějaký čas vypnou, nebo se v současné době využívá ovládacích systémů, z kterých nelze odečíst jejich povelový kód. Dalším způsobem odhalování kódu je "*grabing*", což je způsob nahrávání kódu. Vyslaný kód se nahrává a s použitím systému vojenské kryptografie je "hledán" správný kód pro vypnutí autoalarmu. Za další způsob ochrany je považován **systém plovoucího kódu**. Jde o postupnou změnu kódové informace (kód se po každé aktivaci či deaktivaci mění, takže případná nahrávka není aktuální).

### 3.5 Signalizační zařízení

V problematice ochrany automobilů je stěžejním úkolem předání informace o narušení, které lze to provést

- lokálně
- dálkově
- případně kombinací obou způsobů.

#### 3.5.1 Lokální signalizace

U tohoto typu signalizace je spoléháno "na náhodu", že houkající siréna odradí pachatele od dokonání trestného činu, popřípadě upozorní majitele nebo náhodné svědky na páchání trestné činnosti. U levnějších a jednodušších provedení autoalarmů se jako signalizačního zařízení využívá stávající houkačka automobilu, která je snadno překonatelná. Kvalitnější systémy autoalarmů používají vlastní inteligentní zálohované



sirény umístěné na skrytém a špatně přístupném místě, zpravidla v motorovém prostoru automobilu.

Nedovolená manipulace nebo přerušení přívodu sirény vyvolá poplach, který je signalizován houkáním sirény (trvale nebo přerušovaně a nesmí dle předpisu EHK trvat déle než 30 sekund) a zpravidla blikáním přerušovaným rozsvěcováním směrových nebo obrysových světel (optická síť). Doba účinnosti není omezena.

### 3.5.2 Dálková signalizace

Vyhodnocovací zařízení ovládají vysílač, který uvědomí majitele o neoprávněné manipulaci s vozidlem. Jedná se o tzv. pagery, které na frekvenci 27 MHz (občanské pásmo) a nebo na zvláštní, k tomu určené frekvenci (dnes např. 443 MHz apod), předávají z vozidla signál o narušení do miniaturního přijímače, který má majitel u sebe. Takovýto systém má dosah až stovek metrů. Nevýhodou je možné rušení a vzhledem k jednosměrnému spojení absence kontroly úspěšného přenosu poplachové informace. Rádiové signalizace využívají i některé systémy vyhledávací systémy.

Jako jedna z dalších variant spojení se v dnešní době jeví využití sítě GSM, v případě použití mobilního telefonu GSM či modulu instalovanému ve voze.

### 3.6 Systémy zabráňující nastartování - Imobilizéry

Specifickou část ochrany motorových vozidel tvoří tzv. imobilizéry, které zabráňují nastartování vozidla po dobu střežení. Těchto systémů je celá řada od nejjednodušších, které propojují přes zásuvné klíče startovací obvody, až po zařízení, která tyto funkce umožňují pouze přes použití ID karet nebo speciálních kódových mikročipových transpondérů většinou umístěných v klíči zapalování.

Tato zařízení, se zpravidla aktivují automaticky do 10 -30 vteřin, po vypnutí zapalování, kdy rozpojí většinou 3 základní elektrické okruhy nutné pro pohyb vozidla (např. startér, zapalování, palivové čerpadlo, diesel ventil) a tím znemožní jeho nastartování i roztlačení. Tento stav může být signalizován např. dvoubarevnou LED diodou (bliká červeně - aktivace, svítí zeleně -deaktivace, za jízdy nesvítí) umístěnou viditelně na přístrojové desce. Vozidlo je pak možné odcifit pouze odtažením, nebo kvalifikovaným zásahem pachatele přímo na blokačních bodech. V současné době imobilizéry spolupracují s řídicí jednotkou motoru.

Od používaných autoalarmů se imobilizéry liší tím, že *elektronicky zablokuje automobil. Nechrání však vnitřní prostor vozidla a zpravidla neumožňují připojení přenosových zařízení pro signalizaci do místa obsluhy. Možnosti provedení blokace*



Imobilizéry podle stupně složitosti a technického provedení mají řadu možností a variant, kdy mohou např.:

- systém sami uvést do stavu pohotovosti do 30 vteřin po vypnutí zapalování, i v případě, že řidič zapomněl zařízení sám aktivovat. Vypnutí (deaktivace) je poté možná pouze pomocí transpondéru nebo kódu vyslaného z dálkového ovládání
- při tísňové situaci, vyvolané náhlým přepadením a násilným donucením k opuštění vozidla lze odcizené vozidlo zastavit pomocí dálkového ovládání a to těmito způsoby:

- pomocí dálkového ovládače (do cca 50 m), kdy napadený řidič stiskne na dálkovém ovládací tísňové tlačítko (Panic) a tím dosáhne zastavení odcizeného vozidla

- pomocí radiové sítě, pokud je automobil současně s imobilizérem vybaven systémem rádiové komunikace, lze s použitím pozemní radiové sítě zastavit odcizené vozidlo na "dálku" kdekoliv na území ČR i SR.

- pomocí využití technologie GSM, kdy je automobil vybaven příslušným komunikátorem (mobilní telefon, modul).

### 3.7 Systémy umožňující vyhledávání vozidel

V současnosti jsou v naší republice nejznámější tyto systémy:

- systémy lokalizace polohy vozidla pomocí **rádiové sítě**
- systémy lokalizace polohy vozidla na principu **GSM**
- systémy lokalizace polohy vozidla na principu **GPS**

#### 3.7.1 Systémy lokalizace polohy vozidla pomocí rádiové sítě

Jde o velice účinný aktivní zabezpečovací pozemní systém, který spolu s využitím celostátní radiové frekvence umožňuje lokalizaci a následné vyhledání odcizených motorových vozidel, téměř na celém území ČR a sousedních států. Systémy jednotlivých zemí jsou vzájemně kompatibilní.

Systém pracuje na principu minivysílače s vlastním záložním zdrojem energie (na 72 hodin), který vysílá vysokofrekvenční signál (na určené frekvenci, pulzně z důvodu rušení). Po zachycení signálu jej programové vybavení identifikuje a určí odkud signál přichází, případně jakou rychlostí se vysílač (auto) pohybuje. Spouští se po určité

době od ukončení alarmového signálu automobilu (autoalarm), nebo ve chvíli, kdy s vozidlem manipuluje neoprávněná osoba (startování vozu bez klíčku, manipulace s immobilizérem), nebo je vysílač iniciován dálkovou aktivací (při ztrátě či odcizení klíče nebo při násilném odstranění řidiče). Odcizený automobil lze vypátrat do 90 minut od vyslání poplachového kódu, přestože bude ukryt. Vyhledávání je možno vzájemně kombinovat ať již pomocí vlastních firemních prostředků, spoluprací s vozy policie, případně přesnou lokalizací využitím systému GPS. Úspěšnost vyhledání odcizeného vozidla se pohybuje kolem 94%.

### **3.7.2 Systémy lokalizace polohy vozidla na principu GSM**

Vyhledávací systém umožňuje přibližně lokalizovat polohu vozidla na základě identifikace základové stanice, ke které se GSM modul vozidla pravidelně přihlašuje.

### **3.7.3 Systémy lokalizace polohy vozidla na principu GPS**

Ve vozidle je umístěn satelitní přijímač GPS, který z informací získaných od družic vypočítává v určitých periodách polohu vozidla (řádově v metrech). Získané informace jsou vysílačem zabudovaným v automobilu vyslány na centrální dispečerské pracoviště (CDP), kde je pohyb vozidla zaznamenán a zobrazován v reálném čase.

### **3.7.4 Přenos dat**

Klíčovým bodem celého systému je přenos dat z vozidla na CDP. Podle použitých komunikačních prostředků se používají 2 základní typy spojových sítí:

*-lokální* -po interních radiotelekomunikačních sítích s použitím radiostanic pro pozemní pohyblivou službu (sítě pro přenos dat, fonické sítě) s dosahem omezeným na území města, kraje, v případě velkého nebo členitého území jsou potřebné retranslační stanice,

*-globální* -prostřednictvím satelitní komunikace v rámci celé Evropy, případně celého světa (Inmarsat, Iridium) nebo s využitím GSM



## ZÁVĚR

V této bakalářské práci jsem se zaměřil na vytvoření učebních textů pro veřejnost v oblasti elektronické zabezpečovací signalizace. Práce může být využívána jako učební pomůcka, nebo jako pomůcka pro získání širšího přehledu v oblasti EZS.

Text je věnován systémům elektronické zabezpečovací signalizace s doplněním dalších prvků důležitých pro komplexní chod vlastního zabezpečení, přenosu a vyhodnocení poplachu. Jedná se o detektory, ústředny, ovládací, indikační a doplňková zařízení.

Přínos elektronické zabezpečovací signalizace při ochraně majetku a životů osob je neúsporný. Umožňuje včasnou detekci a ohlášení poplachu na příslušná místa a tím možnost zadržet pachatele na místě činu. Je proto důležité seznámit širokou veřejnost s důležitým posláním elektronické zabezpečovací signalizace.

Podstatou zabezpečovacího systému je, zajištění splnění tří úkolů:

1. Vyvolat poplach, dojde-li k poplachové události.
2. Nevyhlašovat poplach, jestliže k poplachové události nedošlo.
3. Poskytnout použitelnou informaci pro toho, kdo monitoruje poplachy a je připraven na ně reagovat.

Systém, který nesplňuje všechna tato kritéria, není optimální. Bohužel v současnosti je velké množství zabezpečovacích systémů nevyhovujících z důvodu četnosti falešných poplachů. Přijímací poplachová centra na celém světě jsou zahrnuta falešnými poplachy. Z celkového pohledu je přibližně 85 % poplachů falešných a to dokonce i v zemích s nejvyspělejší technikou. Výsledkem je požadavek na kvalitnější systémy, lepší montáž a monitorování umožňující filtrovat falešné poplachy. Na základě této skutečnosti výrobci berou v úvahu to, že operátoři přijímacích poplachových center potřebují dříve, než rozběhnou zásah, potvrzení poplachu. Ve většině případů operátor ví pouze to, že byl spuštěn poplach, nepozná ale, zda opilec rozbil okno či výkladní skříň nebo zda se jedná o nájezd organizovaného ozbrojeného gangu.

Veškerá zde popsaná technika buď již k dispozici je, nebo se její uvedení na trh plánuje v nejbližším období, nebo ji lze vyvinout během několika let.

Otázkou však zůstává ochrana soukromí a s tím související skutečnost, jak veřejnost přijme tento způsob využití techniky.

Lze si však jednoduše představit, a také to již v některých městských centrech ve světě funguje, obytná místa s vlastními monitorovacími bezpečnostními systémy provozovanými jejich obyvateli. S inteligentními senzory a internetem není nezbytné, aby

někdo 24 hodin denně sledoval obrazovku monitoru. Poplachy lze generovat z mobilního telefonu bez ohledu na to, kde se právě obsluha nachází.

V zásadě je obor zabezpečovací techniky velice obsáhlý a v rozsahu této práce se nelze věnovat podrobně všem jeho odvětvím.

*Na závěr bych rád uvedl malý dodatek – je potřeba pamatovat na to, že žádná elektronika nedokáže nahradit kvalitní mechanický zábranný systém.*



## Seznam použité literatury

- [1] Křeček, S.: Příručka zabezpečovací techniky, Blatenská tiskárna, 2003
- [2] Klugl, J.: Montáž EZS, Vydavatelství PA ČR, 1993
- [3] Vedral, J., Fischer, J.: Elektronické obvody pro měřicí techniku, Praha, Vydavatelství ČVUT, 1999
- [4] Interní materiály POLICIE ČR
- [5] WWW stránky
- [6] Výběr z norem ČSN