Česká zemědělská univerzita v Praze

Technická fakulta

Katedra technologických zařízení staveb

Vliv spolehlivosti bezdrátových prvků systémů EZS na kvalitu obsluhy systému (ergonometrie systémů EZS)

Diplomová práce

Vedoucí bakalářské práce: Ing. Zdeněk Votruba

Vypracoval: Bc. Martin Janovský

Praha 2012

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra technologických zařízení staveb

Technická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Janovský Martin

Informační a řídící technika v agropotravinářském komplexu

Název práce

Vliv spolehlivosti bezdrátových prvků systémů EZS na kvalitu obsluhy systému (ergonometrie systémů EZS)

Anglický název

Influence the reliability of wireless systems (ESS systems ergonomics)

Cíle práce

Provést rozbor a bezpečnostní analýzu koncepce bezdrátových zabezpečovacích ústředen a detektorů. Prakticky ověřit a srovnat s obdobnou koncepcí sběrnicové typologie a sledovat zde chování uživatele v závislosti na nejčastějším vyvolání planého poplachu. Z výsledných dat měření stanovit opatření k zamezení planých poplachů a definovat slabiny bezdrátové koncepce EZS oproti sběrnicovým systémům EZS

Metodika

Stručně pojednat o rozdílu v bezdrátové koncepci EZS a sběrnicové topologii. Pro vybrané detektory ústředny provést simulaci narušení kde se otestuje odolnost jednotlivých částí na vybrané typy narušení. Na vybraných ústřednách sledovat paměť poplachů a definovat graficky na měřeném vzorku nejčastější plané poplachy a uživatelské problémy při práci s ním. Z těchto dat provést porovnání bezdrátové koncepce a sběrnicové koncepce a následně provést analýzu a stanovte doporučení k odstranění zjištěných nedostatků.

Osnova práce

Osnova:

1. Rozbor Bezdrátové a sběrnicové topologie (EZS)
2. Praktické Testování bezdrátových prvků EZS
3. Praktické Testování Sběrnicových prvků EZS
4. Analýza sledovaných dat z paměti ústředen EZS
5. Porovnání odolnosti testovaných koncepcí
6. Definování problémů a doporučení k jejich odstranění v testovaných systémech EZS zejména v bezdrátové koncepci.

Rozsah textové části

Klíčová slova
EZS, PTZS, bezdrátové přenosy, ergonometrie

Doporučené zdroje informací
Stanislav Kleček, Příručka zabezpečovací techniky, ISBN 80-9029338-2-4
Security Magazín ISSN 1210-8723
Vincenzo de Astis, Bruno Gasparin, Security technologu handbook, March 2006

Vedoucí práce
Votruba Zdeněk, Ing.

Konzultant práce
Ing. Jan Hart

Termín zadání
listopad 2010

Termín odevzdání
duben 2012

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
TECHNICKÁ FAKULTA

doc. Ing. Miroslav Přikryl, CSc.
Vedoucí katedry

prof. Ing. Vladimír Jurča, CSc.
Děkan fakulty

V Praze dne 14.10.2011

Čestné prohlášení:

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

V Praze dne 14 .února 2010 …….

Martin Janovský

Abstrakt

This work deals with the user's ability to control the ESS and aims to map the most common causes of alarms for the current user's system in wireless security systems and their ability to resist disturbance. Further follow their weaknesses in the user network. In this work we set the causes that lead to false alarms and then pointing out the correct solution to their options and avoid similar problems in the future.

Keywords: ESS, PTZS, wireless security systems, ergonomics

Tato práce se zabývá schopností uživatele ovládat EZS a má za cíl zmapovat nejčastější příčiny vzniku poplachů v běžném uživatelském systému v bezdrátových zabezpečovacích systémech a jejich schopnost odolávat narušení. Dále sleduji jejich slabiny v rámci uživatelské sítě. V práci stanovím příčiny, které vedou k planým poplachům a následně poukážu na řešení k jejich napravení a možnosti předcházení podobným problémům v budoucnosti.

Klíčová slova: EZS, PTZS, bezdrátové přenosy, ergonometrie

Obsah

Úvod

Rozvoj a techniky ochrany majetku, kterými rozumíme nástroje patřící do skupiny EZS, je dán překotným vývojem na poli výpočetní techniky, ze které vzešla miniaturizace a masová produkce elektronických součástek. Díky těmto faktorům došlo k podstatnému zlevnění veškeré elektronické techniky, do které patří i EZS. Dnes již tedy prostředky EZS nepatří do kategorie dostupnosti jen pro VIP a vládu, ale jsou široce rozšířeny mezi masovou populaci v různém provedení a kvalitě.

Takovéto rozšíření má, ale i několik záporů. Zatímco dříve pracoval se zabezpečovacím systémem pouze technicky vyškolený personál a instalaci prováděly specializované firmy, dnes tomu již tak není. Celá řada firem dnes nabízí samo-instalační balíčky nevalné kvality pro instalaci do domácnosti bez asistence technika a o proškolení uživatele se zde již nedá vůbec mluvit.

Podomácku instalované systémy nepřinášejí uživateli z pravidla větší bezpečí, ale zato mu přinášejí starosti. Tyto starosti vznikají zejména vlivem planých poplachů, které jsou způsobeny uživatelskou neznalostí nebo špatným použitím jednotlivých detektorů při instalaci. Ty jsou způsobené neznalostí funkcí a principů, na kterém jednotlivé detektory pracují. Takto nepochopená instalace může vyústit v namíření infračerveného pohybového detektoru do okna, kdy detektor snímá i plochu ulice, kde každý průchod nebo i pohyb záclony v kombinaci s teplem slunečního záření má za následek planý poplach. Takto znehodnocený systém je pouhou přítěží, nejen pro svého uživatele, ale i pro okolí.

Takovéto časté plané poplachy způsobují mezi lidmi v okolí netečnost, kde v případě, že posléze dojde v sousedním domě, který má EZS systém zbudovaný profesionálně, k narušení, a bezpečnostní systém zareaguje výstražnou sirénou, vzbudí u okolí nezájem s dojmem, že se jedná opět o planý poplach. Takto dokáže špatně instalovaný jeden systém částečně potlačit funkci všech ostatních systémů v okolí.

Z výše popsaných důvodů se proto v této práci budu zabývat zejména touto problematikou a pokusím se zde přiblížit zásady vedoucí k zamezení těchto neblahých a však v poslední době velice častých jevů. Tyto jevy se pokusím definovat a detekovat zejména na bezdrátových zabezpečovacích systémech a to z důvodu, že v těchto samo instalačních setech bývají zastoupeny nejčastěji.

V první části své práce se budu zabývat teoretickým rozborem jednotlivých prvků EZS a praktickými testy ověřím jejich odolnost na rušivé vlivy, které se v domácnosti nejčastěji vyskytují. Druhá část bude zaměřena na přizpůsobivost uživatele a jeho práci s EZS. Rozebereme si nejčastější plané poplachy, které byly zjištěny při více jak ročním sledování výstupů z měřené ústředny na testovaném vzorku.

V Poslední částí mé práce rozeberu výzkum, který vznikl mezi uživateli zabezpečovacích zařízení, ze kterých vyvodíme obecné předpoklady, které vedou uživatele k nákupu EZS a práci s nimi. V poslední kapitole definuji postupy, které vedou k zamezení planých poplachů a obecné rady při jejich používání.

1 Rozbor bezdrátové a sběrnicové topologie (EZS)

1.1 Rozbor situace

K pochopení problematiky EZS je nutné si říci, z jakého důvodu se používají a proč. K velkému rozšíření EZS dochází v ČR zejména po roce 1993 a to z několika důvodů majetková trestná činnost se začíná stupňovat a ochané prostředky se stávají dostupnější, ať už po stránce technologické, nebo i po stránce finanční. Ze statistiky policie ČR (tab. 1) je patrné, že kriminalita v roce 2011 oproti předchozím rokům poklesla. Tak v hlavní kategorii, která nás z hlediska EZS zajímá, naopak stoupla. V podkategorii krádeže vloupáním, která je pro nás podstatná a kde se EZS vyskytují nejčastěji, je pokles mírný. To je důvod stále většího rozšíření EZS do domácností.

V minulých letech byl trend budovat EZS napojený na pulty centralizované ochrany a zařízení takových systémů bylo přenecháno odborníkům. Tato praxe je postupně opouštěna a to zejména s příchodem samo instalačních setů, které nabízejí mnozí výrobci jako levné alternativy. U takovýchto systémů ovšem chybí dosti často jakákoliv znalost ze strany uživatele, který zde plní i úloho instalačního technika. V předchozích letech takovýto technik uživatele řádně proškolil a zajistil tak určitý stupeň připravenosti

uživatele. Uživateli poté sdělil zásady nutné k užívání takovéhoto systému. Bez takového proškolení není uživatel schopen pochopit nutnost přizpůsobit některé svoje aktivity a zejména pak rozsah možností instalovaného zabezpečovacího systému. V těchto případech dochází k přeceňování systému EZS a jeho nesprávné funkci, která má za následek vznik planých poplachů, které jsou všeobecně nežádoucí a vyvolávají nejen u uživatele ale i v okolí dojem nespolehlivosti.

	1990	1991	1992	1993	1994	2001	2002	2003	2004	2005	2011*
Celková Kriminalita	216852	282998	345205	398505	372427	375630	394267	403654	425930	426626	293202
Majetková Kriminalita	166638	231372	287059	327183	300352	289002	301727	304039	314249	306351	187358
Krádeže vloupáním	72885	106943	115779	124365	111914	100098	98472	94603	92029	85631	75326
Z toho Bytů	15238	17432	16818	17632	14804	13936	13538	13068	12752	12445	11477
Krádeže automobilů	11658	10849	20829	25522	25615	25059	27517	29422	27889	27092	30265

Tab. 1 Kriminalita v ČR * Data k 1.11.2011

1.2 Bezdrátová koncepce

Tyto systémy se zejména uplatňují v objektech, kde je EZS dodělváno dodatečně, nebo na místech kde není možno vést rozvody pomocí kabeláže. Stále hojněji se používá při zřízení náhradního systému, nebo za předpokladu že chceme zabezpečovací systém zřídit dočasně. K přenosu složí dva typy komunikace - jednosměrná nebo obousměrná komunikace. Bezdrátové systémy se z hlediska činnosti vlastního vyhodnocovacího obvodu či senzoru neliší od běžných zabezpečovacích prvků. Jediným rozdíl a to zásadním je realizace spojení s ústřednou, to je prováděno na dvou frekvencích a to je 433 MHz a 868 MHz [1]

- Výhody: Vysoká flexibilita. Snadná instalace - ústředna si prvky vyhledá sama. Možnost dočasné instalace. Připojení množství zařízení bez ohledu na dostupnost kabelového připojení. [5,1]

- Nevýhody: Přenos je realizován bezdrátovým přenosem - je zde možnost blokování přenosového signálu a odposlouchávání. Je nutné mít u každého přístroje vlastní napájecí zdroj a díky tomu je i cena za údržbu vyšší. [5,1]

Jednosměrný rádiový přenos

Nedostatek je zde v jejich jednosměrné komunikaci. Spolehlivost nelze kontrolovat na zvláštních či určených frekvencích, nebo pásmu 433 MHz a 868 MHz. Je určeno pro objekty s naším rizikem napadení. [1]

Obousměrný rádiový přenos

Tato komunikace využívá stejný stupeň monitorování jako ústředny spojené po metalickém vedení (sběrnicové rozvody). Pracují na frekvenčních pásmech 433 MHz a 868 MHz. Systém je zcela adresovatelný - má k dispozici více jak 100 adres a umožňuje dělení na nezávislé subsystémy. Ovládání je možné pomocí přenosného ovladače, nebo blokovacího zámku. Přenosný ovladač má výhody pro postižené při tísňovém volání a při práci venku monitoruje příchody a odchody na dálku. Systém umožňuje instalaci zařízení tzv. mrtvého muže. Mrtvý muž znamená, že je ovladač vybaven náklonovým čidlem a infračerveným vysílačem a není tak možno systém uvést do chodu bez přítomnosti obsluhy uvnitř střeženého objektu. [1]

Hlavní výhodou obousměrného přenosu je podstatně vyšší zabezpečení přenosového kanálu, kde přijímač a vysílač pracují souběžně na dvou kmitočtech a v případě narušení pásma přenosu, ať již rušením záměrným nebo atmosférickým, je ústředna schopna přesunout své vysílací pásmo na jiný kmitočet. Toto se bohužel netýká GSM rušení, ale pouze rušení přenosu komunikace ústředny. Systém je také schopen indikovat intenzitu pole, a podávat uživateli informace o tom, zda pracuje s rezervou nebo na hranici citlivosti. Přenos mezi prvky je digitální a má plavoucí kódování proti odposlechu, což jej činí velmi špatně napadnutelným. [1]

1.3 Základní pojmy

1.3.1 Norma EN 50131

Norma na rozdíl od předchozího vydání rozlišuje poplachové systémy pro detekci vniknutí a poplachové systémy pro detekci přepadení. V souvislosti s tím jsou některé body této normy formulovány odděleně pro tyto dva druhy zabezpečení. V originále této normy se kromě jediné zkratky, IAS (Intruder Alarm System - poplachový systém pro detekci vniknutí), použité v předchozím vydání normy, objevuje zkratka I&HAS (Intruder and Hold-up Alarm System - poplachový systém pro detekci vniknutí a přepadení). Na několika místech normy jsou použity zkratky HAS (Hold-up Alarm System - poplachový systém pro detekci přepadení) tam, kde systém postrádá funkci detekce vniknutí, a IAS tam, kde systém postrádá funkci detekce přepadení. Proto jsou nyní v českém překladu normy místo dosud používané zkratky EZS používány zkratky z originálu - I&HAS "poplachové zabezpečovací a tísňové systémy", IAS pro "poplachové zabezpečovací systémy" a pro HAS "poplachové tísňové systémy". [1;5]

Norma je proti předchozímu vydání přehlednější díky prezentaci velkého množství funkcí formou tabulek. Je v ní také zavedena nová funkce - detekce podstatného snížení dosahu detektorů pohybu. Přesněji jsou definovány podmínky znemožňující uvedení do stavu střežení, je definováno, za jakých podmínek je povoleno tyto podmínky překonat. Podstatně se zkrátila doba ověřování dostupnosti komunikace v okamžiku nastavování střežení (u stupně 2 z dvou hodin na 20 minut, u stupně 3 z jedné hodiny na jednu minutu a u stupně 4 z 15 minut na 10 sekund). Zvýšila se povinná kapacita paměti událostí na dvojnásobek a byly přidány některé povinně zaznamenávané události (například porucha náhradního napájecího zdroje, porucha výstražných zařízení, překonání podmínek znemožňujících nastavit stav střežení). Zcela nově jsou definovány požadavky na přenos poplachu poplachovým přenosovým systémem, zejména pak provozní kritéria těchto systémů v závislosti na stupni zabezpečení. [1;5]

1.3.2 Ústředny EZS

Ústředna EZS je mozkem celého systému EZS. Sleduje stav detektorů (vstupy) a na základě naprogramovaných parametrů vydává povely pro signalizační zařízení (sirény) nebo komunikační zařízení, které informují uživatele o poplachu nebo jiných provozních

stavech (mobil, PCO, e-mail, Internet). Ústředna EZS se ovládá za pomoci ovládací klávesnice (klasický způsob), ale i mobilem, PC přes internet nebo mobilní síť, kartou nebo čipem (pouze změna režimu hlídání - nestřeženém) a dálkovými ovladači. [1]

Ústředna EZS je zálohovaná, aby při výpadku elektrické energie nedošlo ke kolapsu systému. Zpravidla má v sobě zabudovaný telefonní komunikátor pevné linky, za pomoci kterého může předávat naprogramované informace na pult PCO. Při kabelovém provedení poskytuje napájení pro všechny ostatní prvky systému. Má v sobě integrované programovatelné výstupy, které se mohou aktivovat nějakou událostí v systému nebo dálkovým ovládáním, např. zprávou sms mobilním telefonem, přes internet. Takto lze například zapínat topení, saunu, klimatizaci, osvětlení nebo popřípadě lze do systému napojit libovolný elektrický spotřebič. Vyšší řady ústředen mají v sobě integrovaný přístupový systém, tento integrovány systém v sobě zahrnuje možnost definovat různé uživatele a zaznamenávat například jejich docházku. V tomto případě se k systému EZS instalují na požadované dveře čtečky magnetických karet a elektrické dveřní zámky. [1]

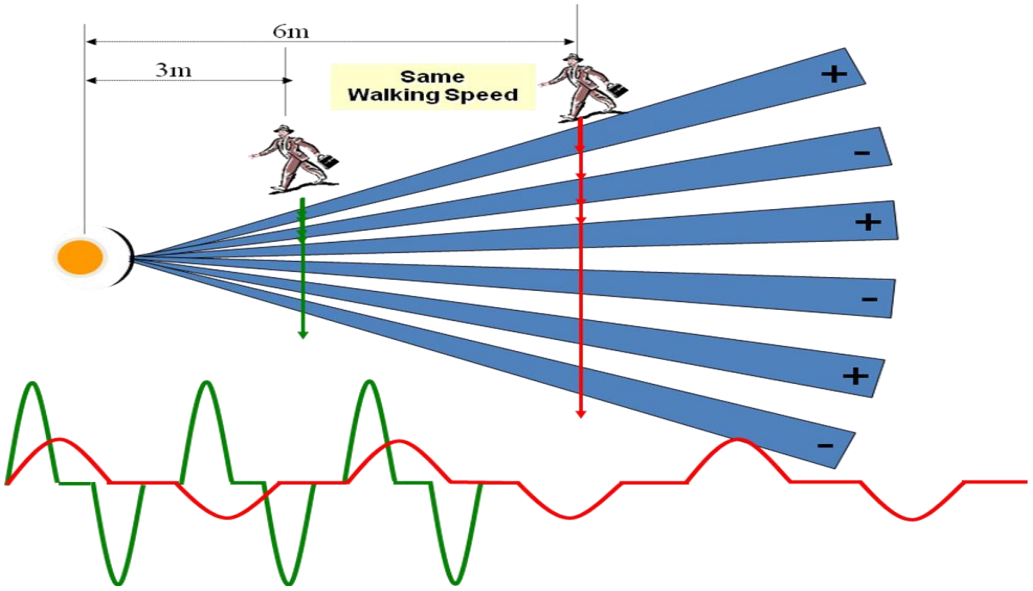
Ústředna EZS se instaluje na skryté a bezpečné místo, aby pachatel nezničil ústřednu dříve, nežli vyhlásí poplach a odešle poplachové informace (siréna, PCO, mobil, internet). Napájení ústředny EZS je řešeno z elektrické sítě napětím 230 V AC, ústředna se připojuje na samostatný proudový jistič.[1]

1.3.3 PIR

Pasivní infračervená čidla (obr 1.1), označována jako "PIR" jsou nejčastěji využívanými detektory ve standardních zapojeních elektrické zabezpečovací signalizace.

Obr 1.1 PIR detektor [21]

Zjednodušeně lze říci, že PIR detektory jsou schopny zachytit pohyb těles, která mají jinou teplotu, než teplotu okolí. Zjednodušeně tedy zaznamenávají změnu teploty u těles, která se pohybují v určitém infračerveném spektru.



Obr 1.2Amplituda signálu (PIR detektoru) v závislosti na pohybu [12;1]

Optika PIR čidla se dá nastavit do tří různých typů snímání- vějíř, záclona a dlouhý dosah.

Typ "vějíř"- Čidlo snímá horizontálně v "širokém vějíři".

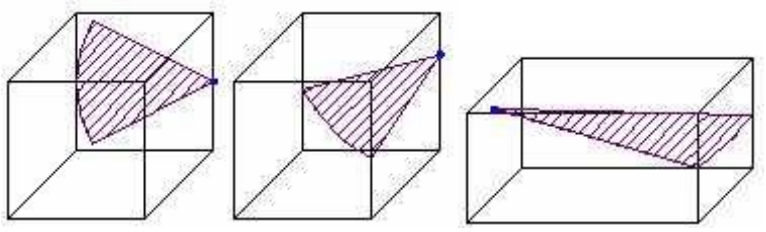
Tato možnost je využívána při klasické prostorové ochraně místností. Dosah čidla je dán výrobcem, pohybuje se okolo 12-15m.Úhel záběru je rovněž dán výrobcem čidla, pohybuje se okolo 90-120stupňů [21]

Typ "záclona"- Čidlo snímá vertikálně v "širokém vějíři".

Tato možnost se využívá při obvodové ochraně, např. v místnostech s velkými okny nebo výkladními skříněmi. Dosah čidla i úhel záběru je shodný jako v minulém případě, snímací charakteristika je však orientována vertikálně. [21]

Typ "dlouhý dosah"-Čidlo snímá horizontálně v "úzkém dlouhém vějíři".

Tato možnost je využívána na úzkých dlouhých chodbách. Dosah čidla je dán výrobcem, pohybuje se okolo 25-30m.Úhel záběru je rovněž dán výrobcem čidla, pohybuje se okolo 45-60stupňů. [21]



Obr 1.3 z leva doprava profil - vějíř, záclona, dlouhý dosah [21]

Pravidla instalace:

Výška montáže od podlahy by měla být v rozmezí 2-2.5m.

Je nutné nastavit snímací charakteristice správný sklon. Proto je detekci nutno vyzkoušet ve všech částech střeženého prostoru a případně provést korekci nastavení dle pokynu v manuálu. To se dělá piny přímo na čidle [21]

Čidlo musí být instalováno tak, aby bylo vyloučeno jakékoli zakrytí vzhledem k provozu v místnosti (zahrnutí závěsu, stažení žaluzií, zastavění nábytkem atd.)

Nejvhodnější umístění PIR čidla vzhledem k včasné detekci je takové, aby směr pohybu pachatele (vstup do střeženého prostoru) byl kolmý, případně tangenciální na snímací charakteristiku detektoru. [21]

U typu "vějíř" je nejvhodnější umístění do rohu místnosti, u typu "dlouhý dosah" do poloviny zadní stěny.

Umístění čidla musí být provedeno dostatečně a na pevném stavebním podkladu. Nesmí docházet k vibracím čidla.

V případě instalace více čidel PIR v jednom prostoru je nutné, aby nebyl vytvořen hluchý prostor a je vhodné, aby se snímací charakteristiky čidel částečně překrývali.

Čeho se vyvarovat:

PIR čidlo se nesmí "dívat" do oken, případně být nasměrováno k vstupním dveřím. Může zde docházet k falešným poplachům vlivem slunečního svitu. [21]

PIR čidlo nesmí být umístěno v blízkosti vzduchotechnických a ventilačních vyústku, kde není zajištěna stálá teplota okolí. [21]

Pozor na místnosti s podlahovým vytápěním. Zde zpravidla nelze eliminovat falešné poplachy a je nutné zvolit jiný druh čidel. [21]

Dále by čidlo nemělo být instalováno na stěně, která sousedí s komínem, teplovodní stupačkou atd. [21]

1.3.4 Magnetické kontakty

Magnetický kontakt je nejběžnější součástí domácích zabezpečovacích systému objevuje se zejména jako součást plášťové ochrany na dveřích a oknech. Jeho funkce je velice jednoduchá kontakt je malí a velice skladný. Funkce je bezproblémová pokud se nejedná o bezdrátový kontakt zde je pak problém s vysílačem a přijímačem signálu, který následně velikost kontaktu zvyšuje několikanásobně. [1]

Nejlepší magnetické kontakty jsou založeny na principu Hallova jevu. Hallův jev je založen na umístění polovodičové destičky tak, že ve směru nejdelší hrany jím prochází proud do magnetického pole. Vektor, kterým prochází, musí být na destičku kolmý. Pokud je tomu tak, vzniká na stěnách Hallovo napětí. V praxi to znamená několikanásobné rozmístění magnetů a Hallových sond. Z toho vyplívá, že pachatel by musel mít přesnou znalost rozmístění magnetů a jejich indukce, a navíc by musel vše zvládnout na první pokus, což vyžaduje značný um a štěstí. [5,15,1]

Při instalaci kontaktu dbáme na to, aby nedocházelo k falešným poplachům, a proto umísťujeme kontakty tak, aby nedošlo k aktivaci při normálním pohybu (například nedosedáváním dveří a velké vůli nebo drnčením oken). Kontakt musí spínat při každém způsobu otevření dveří - nejen normálním, ale také při vylomení. Snadnost instalace a vysoká životaschopnost a odolnost vůči okolním vlivům za příznivou pořizovací cenu dělá z magnetických kontaktů nedílnou součást každého EZS, a proto se výrobci snaží neustále zlepšovat odolnost vůči napadení. [1]

1.3.5 Detektory kouře

Jedná se o detektor, který reaguje na výskyt kouře požárním poplachem. Pro lokální varování má zabudovanou akustickou sirénu. Důležité je detektor kouře nemusí být instalován s ústřednou ale může být nainstalován zcela nezávisle na zbytku zabezpečovacího systému. Detekce kouře je založena na principu ionizační komory. Zařízení je napájeno pomocí vnitřní baterie. Která v čidle vykazuje průměrnou dobu

životnosti 1 rok. Čidla mohou být také napojena na systém EZS odkud probíhá jejich napájení. [1]

Rozměry čidla se pohybují o velikosti 100x80x40 mm. Jejich montáž, např. ke stropní konstrukci, je možná pomocí jednoho či dvou vrutů. Kryty hlásiče bývají plastové většinou bílé barvy. [1,21]

Hlásiče jsou ekologicky nezávadné, i když je jejich součástí radioaktivní součástka, která vykazuje záření maximálně 3Bq, což je hodnota zcela zanedbatelná a neškodná. Někteří výrobci též nabízí možnost drátového i bezdrátového propojení jednotlivých hlásičů s tím, že v případě výstražné reakce jednoho čidla, jsou zapnuta i čidla ostatní. Tento systém je vhodný např. pro rodinné domy, kdy čidlo, reagující na kouř z případného požáru v garáži nebo dílně v podzemí, spustí čidlo v podkrovní ložnici, kde vzbudí spícího uživatele domu a upozorní jej na vzniklé nebezpečí. [1,21]

Aby se informace o poplachu dostala okamžitě i k majiteli bytu, používají se komunikátory využívající buď pevné telefonní linky, nebo sítě mobilních operátorů. Je-li k dispozici pevná linka, lze využít automatické telefonní hlásiče. Tyto přístroje jsou připojeny k telefonní zásuvce a k telefonu. V případě poplachu si automaticky uvolní telefonní linku a začnou vytáčet uživatelem nastavená telefonní čísla. [1,21]

2 Popis měřené studie

V této části se seznámíme s bezdrátovým systémem EZS, na kterém je prováděno měření. Data, která jsou uvedena v této pasáži, jsou získána z níže uvedené ústředny od společnosti Risko ve sledovaném období od 11. října 2010 do 21. Února 2012. Veškerá data byla průběžně stahována z paměti událostí dané ústředny. Instalace celého systému bylo provedeno certifikovaným technikem a po instalaci byl předán majiteli (uživateli) předán certifikát o autorizovaném zapojení číslo certifikátu dle normy EN 50131 No. 32029-2008-PC-NOR.

Celková koncepce sledovaného systému byla zhotovena dle požadavku majitele na ochranu vnitřní i plášťovou v hodnotě do 40 000 Kč. Vzhledem k finančnímu omezení je plášťová ochrana realizována výhradně pomocí magnetických kontaktů, se zaměřením na

vylomení dveří, garážových vrat nebo oken. Vnitřní ochrana je poté provedena pohybovými detektory pracujícími na principu PIR

2.1 Uživatelé

Pro měření a výzkum ergonomie chování uživatele a zabezpečovacího bezdrátového systému jako celku byl zvolen dvoupatrový rodinný dům nacházející se v klidném prostředí na okraji Prahy. Dům pochází z počátku osmdesátých let. Dům je konstruován jako dvougenerační a proto jsou celodenně užívána obě patra. Z hlediska chování uživatele je důležité, abychom mohli náš vzorek roztřídit. Roztřídění vzorku uživatelů, trvale užívající bezpečnostní systém, jsem provedl pomocí vlastního uživatelského hesla pro každého jednotlivce. Pokud tedy takovýto uživatel vytvořil planý poplach nebo jinou nestandardní situaci bylo jeho uživatelské heslo zaznamenáno během deaktivace. Můj měřený vzorek obsahuje pět uživatelů.

2.1.1 Charakteristika uživatele

Uživatel A: Majitel domu vedoucí konstrukčního oddělení, středoškolsky vzdělaný padesátník. Vzhledem ke své práci se dennodenně setkává s počítačem ovšem vzhledem k vyššímu věku a konzervativnosti je schopnost učení již omezená. Také se zde projevuje neochota více proniknout do složitosti celého systému, uživatel byl kompletně proškolen technikem provádějícím instalaci. Uživatel jako jediný pravidelně používá garážová vrata. Uživatel se nejčastěji pohybuje v druhém patře budovy.

Uživatel B: Majitelka domu padesátnice, administrativní bankovní úřednice, středoškolské vzdělání. Její pracovní náplň ji každodenně přivádí se stykem s výpočetní technikou. Rovněž se již před instalací ve svém domě setkala s obsluhou zabezpečující techniky. Uživatelka projevila větší snahu porozumět mechanizmu celého systému během školení uživatelů. Uživatelka se nejčastěji pohybuje v druhém patře budovy.

Uživatel C: Vedoucí konstrukčního oddělení, třicátník, středoškolsky vzdělaný. Pracovní náplň je stejně jako u uživatele A převážně na počítači. Uživatel patří k mladé generaci, kde se předpokládá dobrá schopnost učení a porozumění novým věcem. Uživatel neprodělal školení technikem, informace o užívání mu byly pouze přetlumočeny. Uživatel

neprojevil snahu o bližší seznámení ani o dodatečné školení. Pohyb tohoto uživatele je převážně v prvním patře.

Uživatel D: Informační specialista, vysokoškolské vzdělání, nedosáhl ještě třiceti let. Jako informatik se setkává s celou řadou informačních systému. Uživatel se spolupodílel na zavádění EZS v pozorovaném domě. Zevrubně byl seznámen se systémem EZS a hloubkově porozuměl celkové koncepci a ovládání. Uživatel se pohybuje nejčastěji v druhém patře budovy.

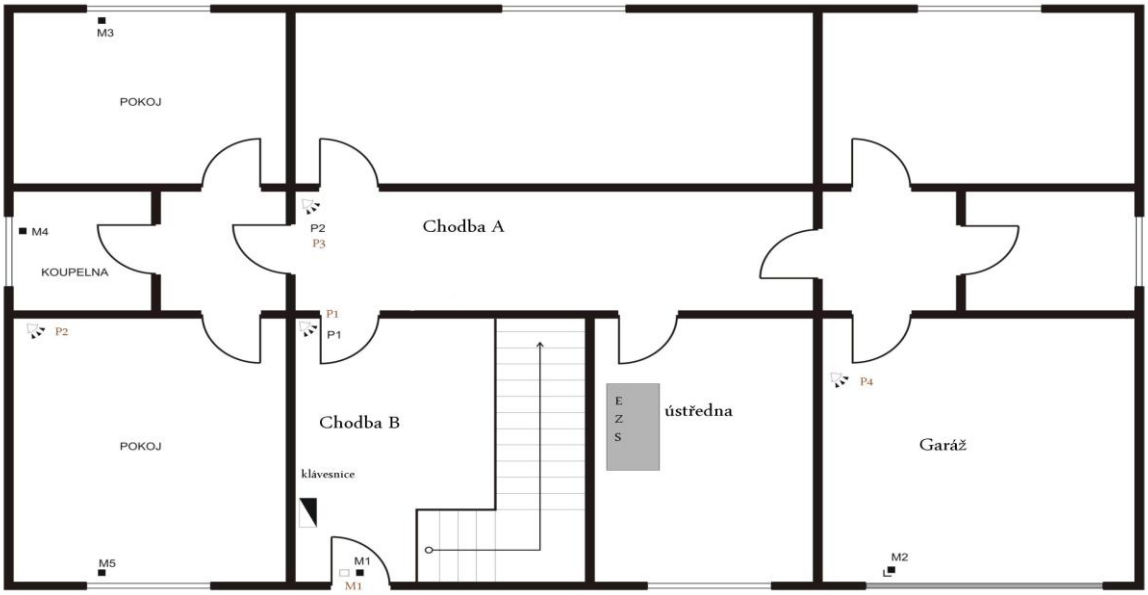
Uživatel E: Vysokoškolsky vzdělaná, administrativní pracovnice pojišťovny, nedosáhla třiceti let. Uživatelka je zdatná v používání zařízení výpočetní techniky. Uživatelka není pevnou součástí domácnosti, ale její výskyt v měřeném časovém etalonu přesahuje více než padesát procent. Z tohoto důvodu byla do měření zahrnuta také. Uživatelka nebyla proškolena technikem.

2.2 Budova

Celková koncepce sledovaného systému byla zhotovena dle požadavku majitele na ochranu vnitřní i plášťovou v hodnotě do 40 000 Kč. Vzhledem k finančnímu omezení je plášťová ochrana realizována výhradně pomocí magnetických kontaktů, se zaměřením na vylomení dveří, garážových vrat nebo oken. Vnitřní ochrana je poté provedena pohybovými detektory pracujícími na principu PIR

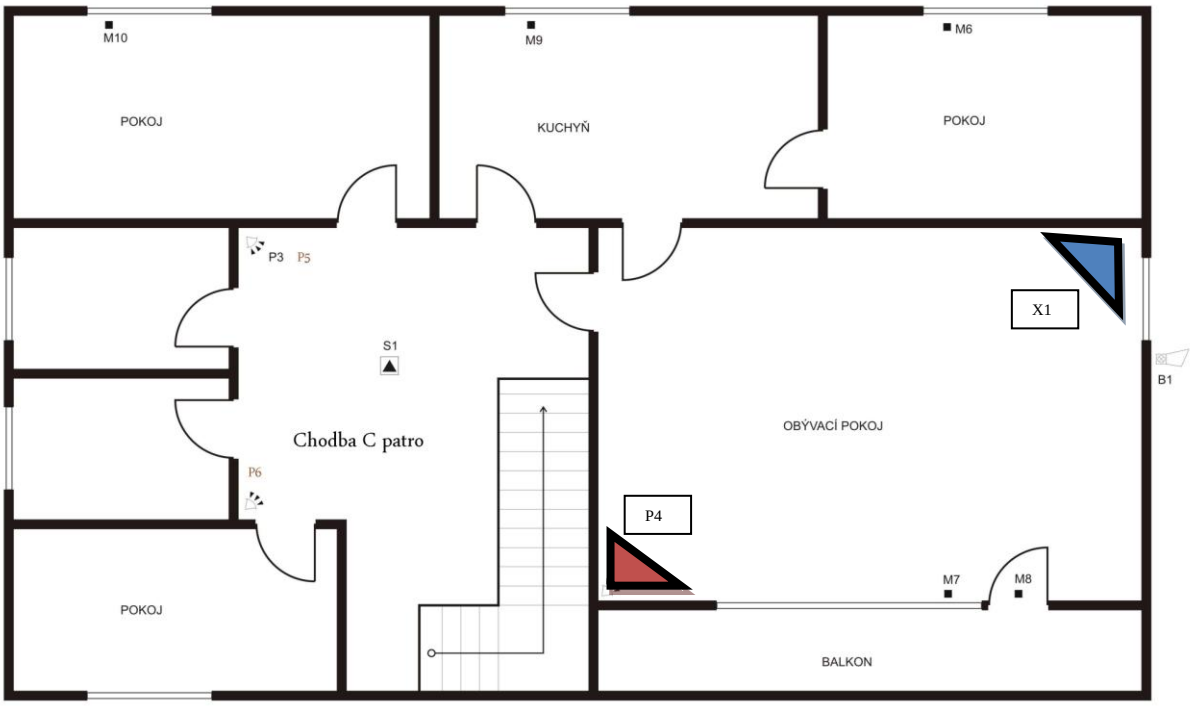
První patro (obr. 2.1): Hlavní vchod je situován k silnici do otevřeného prostoru na jižní stranu, proto je zde nutné brát zřetel na tepelné znečištění při instalaci PIR detektoru. K ochraně vstupních dveří je použit magnetický kontakt M1. Obytná jednotka v prvním patře se nachází v třech místnostech nalevo a ústí do centrální chodby A. V koupelně spodní obývací jednotky byl instalován magnetický kontakt (M4) k sledování změn vlivem působení vlhkosti na zařízení. Místnost položena na jih má velké jednokřídlé okno, na kterém je magnetický kontakt M5. Koupelna a severní místnost jsou osazeny kontaktem M4 a M3. Zdejší okna jsou také chráněna mechanickou mřížovou zábranou. Na pravé straně prvního patra se nacházejí servisní místnosti kotelna, prádelna garáž a sklepy. Garáž je průchozí do hlavní spodní chodby A. Chodba A je centrálním spojovacím uzlem spodní části budovy a je zde v levém rohu instalován PIR detektor (P2), jehož clona zabírá prostor průchodu z části kotelny a garáže. Samotná garážová vrata jsou chráněna pomocí

vratového kontaktu M2, který je napojen na vysílač univerzálního bezdrátového magnetického kontaktu. Mimo chodbu A je pohybový detektor PIR (P1) instalován do vstupní chodby B a směřuje na vstupní dveře a ovládací klávesnici. Maska detektoru je vybavena ochranou PET. Ústředna systému je uložena v místnosti pod průchodovým schodištěm. Tato místnost je dostupná pouze z vnitřku budovy a nevedou do ní žádná okna. Dveře spojující tuto místnost ústí do chodby A, kde jsou chráněny clonou z detektoru P2. Z hlediska ochrany je míst ústředny zvoleno velice výhodně, ovšem je otázka jaký bude mít vliv umístění hluboko do centra budovy na dostupnost signálu.



Obr. 2.1 - 1. Patro budovy

Druhé patro (obr. 2.2): Hlavním vstupem do patra je centrální schodiště ústící do hlavní propojovací chodby C. Schodiště a celá propojovací chodba je zabírána detektorem P3 s maskou typu PET. Chrání tak průchod mezi jednotlivými místnostmi. V centrální chodbě je umístěn fotoelektrický kouřový detektor S1. Jeho činnosti je obsluhována protipožární ochrana horního patra zejména pak kuchyně. Jednotlivé místnosti mají dvoukřídlá skleněná tvrzená okna bez ochranné fólie. Dvoukřídlá okna jsou vybavena magnetickými kontakty M7 až M10. Situace instalace magnetického vysílače na jedno křídlo okna a kontaktu na druhé je výhodné z finančního hlediska, ale nastává situace, kdy kontakt je umístěn na hraně své citlivosti a zejména zde vzniká velká mezera mezi vysílačem a kontaktem do které se dá bez větších problémů vsunout klamný magnet.



Obr. 2. 2 - 2. Patro řešené budovy

2.3 Technická specifikace použité techniky

Technika, která byla použita na pozorovaném systému, byla vyrobena v Izraeli a pochází od společnosti RISCO group. Společnost RISCO patří k dlouholetým výrobcům zabezpečovací techniky a má po světě miliony spokojených uživatelů. Její výrobky patří cenově k dražším, ovšem kvalitativně patří ke špičce. Výrobky, které jsou prodávány v ČR, splňují evropskou normu EN 50 131.

2.3.1 Ústředna

Jako ústřednu jsme zde použili systém Agility spadající do bezpečnostní třídy II., která je vybavena IP, GSM/GPRS, PSTN, a hlasovým modulem. Ústředna nám umožňuje vytvoření 32 bezdrátových zón s 3 podsystémy. Tato ústředna je koncipována jako bezdrátová a principiálně se jedná o ústřednu realizovanou obousměrnou komunikací. Tato ústředna má paměť dostatečně velkou na 250 událostí a umožňuje skrytou komunikaci

pomocí SMS nebo telefonním hlasovým modulem díky kterému máme možnost hovořit skrze reproduktor nebo naopak naslouchat okolí ústředny (to zajisté potěší podezřívavé partnery). Pro uživatele nabízí připojení třech klávesnic a nastavení 32 uživatelských kódů a osmi dálkových ovládání nebo klíčenek k přednosti ústředny patří zejména její nízká váha a jednoduchá instalace prostřednictvím šroubů na zadní straně krytu. To nám umožnilo vybrat si umístění ústředny podle našich požadavků tak aby se dala oddělit od volně přístupných míst a zároveň nám byla snadno dosažitelná bez větších nároků na čas a práci. Ústředna jsme nainstalovali v místnosti pod schodištěm, která je uzamykatelná, a vstupní dveře jsou pod dozorem PIR čidla. Ústředna je umístěna na vlastním proudovém jističi k zamezení možnosti zkratování ústředny prostřednictvím elektrické rozvodné sítě domu. Také samotná instalace prostřednictvím instalačního softwaru v přenosném počítači, s příjemným uživatelským rozhraním, proběhla po umístění všech prvků EZS snadno, (programování je možné provádět i prostřednictvím klávesnice), ústředna si veškeré prvky dokázala sama vyhledat a uživatel si již jen snadno navolil podsystémy a jejich označení. [1]

2.3.2 Ovládání

K ovládání ústředny byla zvolena bezdrátová klávesnice systému Agility, která umožňuje plně ovládat a programovat ústřednu jednoduchými a přehlednými pokyny zobrazovanými na LCD displeji. K příjemným vlastnostem klávesnice patří jednoduché získávání informací o systému zmáčknutím jedné klávesy a k jednoduchému ovládání přispívá i možnost přiřazování uživatelských kódů proximity klíčenkám (k rychlému odemykání a zamykání systému). [1]

K dalším ovládacím prvkům patří obousměrný dálkový ovladač s jednoduchým zámkem kláves, kde zámek zabraňuje zneužití při ztrátě. [1]

2.3.3 Magnetické kontakty

K zajištění plášťové ochrany jsou použity univerzální bezdrátové magnetické kontakty pro dveře a okna s dosahem 300 m ve volném prostranství s 470K Ω rezistorem. Kontakt má možnost 8 nastavení pomocí jednoduchých spínačů, které slouží k nastavení citlivosti, (10ms nebo 500 ms), rychlosti, a odezvy vysílače na kterém se dá nastavit odezva 15 nebo 65 minut. Realizace umístění na okna byla řešena s požadavkem majitele na možnost otevírání ventilace oken při zapnutém systému a také s ohledem na nová

umělohmotná okna (nemožnost vrtání), byly kontakty umístěny do spodních rohů pomocí oboustranné vysoce odolné lepenky. Z důvodů snížení nákladů byl na dvoukřídlá okna použit vždy jeden magnetický kontakt, kde vysílač je umístěn na levém křídle a magnet na pravém. Vzdálenost mezi vysílačem a magnetem se blíží k maximální citlivosti kontaktu což u tohoto typu činní 15 mm. [1]

K ochraně garážových vrat jsme použili vratový kontakt s mezerou detekce 65mm a kabelem chráněným ocelovými kruhy o délce 0,5m ten je následně připojen k vysílači univerzálního magnetického bezdrátového kontaktu. [1]

2.3.4 Detektory pohybu

Jako detektor pohybu byl použit bezdrátový PIR detektor s ochranou proti zvířatům (PET) do váhy 36kg. Tento detektor pracuje pomocí obousměrné komunikace, která redukuje bezdrátové přetížení a pomocí které lze systém vzdáleně ovládat a diagnostikovat. Rozsah střežené plochy je 15 x 15 m kde pokročilý procesor zpracování signálu zajistí kvalitní vyhodnocení přijímaného signálu ze střeženého prostoru. Umístění zadního sabotážního kontaktu nám umožnilo instalaci do rohu místnosti a díky snadné instalaci (pomocí závrtných šroubů), je možné později provést úpravy v umístění detektorů. [1]

2.3.5 Detektor kouře

Použit byl bezdrátový fotoelektrický snímač kouře, který funguje neustále a je nezávislý na poplachové ústředně stejně jako ostatní detektory má protisabotážní temper a umožňuje testovací režim. Umístily jsme ho na strop na hlavní horní chodby, kde má za úkol chránit horní obývací pokoje. Do přízemí nebyl detektor instalován z důvodu občasného zatápění v kotli na uhlí. [1]

2.3.6 Siréna

Je namontovaná na boční zeď rodinného domu ve výši 5 metrů na hlavním štítě. Umístěna je tedy v dostatečné výšce, aby nebyla dostupná bez specializovaného nářadí. Siréna je typově obousměrná bezdrátová, napájená bateriemi, (5 x 3V Lithium baterie, při nízkém napětí se vyšle impuls na ústřednu) s dlouhou životností s Akustickým výkonem 105dBA. Siréna umožňuje nastavit hlasitost akustického výkonu. Na zadním krytu je umístěn temper kontakt zabezpečující ochranu před odstraněním. Má nastavitelný čas stroboskopu a intenzitu optické signalizace. Optická signalizace je oranžové barvy. [1]

3 Praktické Testování prvků EZS

V této kapitole se budu zabývat praktickou aplikací nejrůznějších příčin závad a možností narušení, které vedou k špatné funkci bezdrátových systému a jednotlivých dílčích zařízení. Testy odolnosti jsou vztaženy k případům, které mají vliv na používání systému a mohou se v běžném užívání vyskytnout a snižují tak spolehlivost, udržovatelnost a ovladatelnost celého systému. V této kapitole budu pouze popisovat tyto závady a nebudu zde uvádět možnosti opatření a prevence. Možnosti prevence a opatření budu uvádět v závěru této práce, které budou vycházet z dlouhodobého sledování a zároveň z průzkumu mezi uživateli.

3.1 Magnetické kontakty

3.1.1 Testy odolnosti

Základní test odolnosti jsem zaměřil na odolnost vlivem změny vlhkosti a teploty. Tímto testem jsem podrobil bezdrátový, univerzální kontakt, který byl výše popsán v kapitole 2.1.3

Test odolnosti při výkyvu teploty

Základním testem odolnosti na vlhkost a změnu teploty byl podroben bezdrátoví, univerzální kontakt, který byl výše popsán. První pokus se zaměřil na citlivost jazýčku magnetického kontaktu při změnách teploty v první části, kde byl ohříván a ochlazován na teplotu běžnou působením přírodních vlivů. Pokus byl opakován desetkrát a byla měřena doba reakce kontaktu při otevření a zavření při teplotách -5 °C a + 40 °C. Dalším sledovaným činitelem byla mechanická odolnost krytu zařízení při těchto teplotách. Pro ochlazování byl použit přenosný mrazicí box, kde byla teplota monitorována pomocí rtuťového teploměru. Rozmezí teploty bylo změřeno +2 až -2 stupně. Měření jsem prováděl při nastavení citlivosti odezvy 10 ms a 500 ms (tab. 3.1). Výsledná doba odezvy byla brána z ústředny.

	40°C		-5°C	
	10 ms	500 ms	10 ms	500 ms
1	9,7	531,5	11,7	550,2
2	10,1	521,4	12,4	570,3
3	10	495,5	11,4	601,2
4	10,8	511	12,5	540,5
5	11	530,6	12,4	608,3
6	9,8	498,6	11,8	587,7
7	12	510,3	11,6	604,2
5	10,4	507,6	11,7	578,9
9	13	516,1	12,1	608,2
10	12,5	512,2	13,5	614,7

Tab. 3.1 Tabulka odezvy při změně teploty

Mechanické poškození vlivem teploty nebylo zaznamenáno a odolnost povrchového materiálu vydržela volný pád z výšky 1 a půl metru bez poškození jak při vyšších tak i nižších teplotách. Měření však ukázalo, že nižší teploty mají negativní vliv na odezvu magnetického kontaktu, hodnota rozdílu nebyla při odezvě deset milisekund závratná a pohybovala se kolem 20 ms, což mohlo být způsobeno zhoršeným signálem nebo špatným odečtem. Rozdíl při odezvě 500 ms byl zaznamenán, až v hodnotě jedné sekundy tato hodnota sice není pro funkci zabezpečovacího zařízení ohrožující, avšak může uživateli přinést problémy, zejména jely nastaven tento kontakt na vstupních dveřích. Pokud uživatel v rozmezí 500 ms rozevře a zavře dveře, nestihne vyhodnocovací obvod dát informaci ústředně o opětovném zavření a pro ústřednu se pak jeví jako stále otevřeny a generuje poté planý poplach.

Test odolnosti ve vlhkém prostředí

Praktické testování bylo prováděno na magnetickém kontaktu, jenž byl umístěn do extrémního prostředí okna v prostoru koupelny, kde vzduch dosahuje vlhkosti 90%. Záznam poruch byl monitorován během období 10. 2. 2011 až 10. 2. 2012.

Během sledovaného období se vyskytla celá řada potíží s užíváním tohoto členu plášťové ochrany. Celkem bylo zaznamenáno 37 poruch a jedna výstraha, z čehož více jak 31 krát byla úplná ztráta magnetického kontaktu a nutnost jeho přemostění pro aktivaci celého systému. V těchto 31 případech stala za nefunkčností vlhkost, nebo proniknutí vody do vyhrnovacího obvodu kontaktu. Je nutné vyzdvihnout, že i přes opakované výpadky

vlivem vlhkosti byl kontakt, po jednoduchém vysušení působením topného tělesa a vyjmutí baterie, chopen své funkce.

Dalším zaznamenaným problémem v porovnání s ostatními magnetickými kontakty, které nebyly vystaveny extrémní vlhkosti, byla výdrž baterie. Ve výše popsaném objektu, byly veškeré kontakty umístěny se shodnou baterií SANYO 3V CR13A Lithium dne 16. 9. 2009. U této jediné baterie se projevila snížená životnost a to i přes to, že tento magnetický kontakt byl velmi málo namáhán. V průměru byl spínán dvakrát denně, což je v porovnání se vstupními dveřmi zanedbatelné. Ke dni 16. 12. 2011 začal magnetický kontakt ústředně signalizovat snížené napětí. Ke dni 11. 2. 2012 nebylo u jiných magnetických kontaktů zaznamenáno snížené napětí. Z toho usuzují přímí vliv vlhkosti na životnost baterie.

Dalším patrným jevem, který se vyskytl pouze u tohoto kontaktu, je již vizuálně viditelná koroze, která je patrná jak na plastovém krytu, tak zejména na plošném spoji obvodu. Vzhledem k omezenému časovému období, po které byl experiment prováděn, mohu pouze odhadovat, za jak dlouho by koroze zcela vyřadila toto čidlo z činnosti. Z krátkodobého hlediska je vystavování zabezpečovacího zařízení extrémním vlhkostem zcela nevhodné a zavadí velkou chybovost do zabezpečovacího zařízení a je strůjcem planých poplachů. Kdy kondenzovaná voda v průběhu dne stéká do plošného spoje a vyřazuje ho z činnosti.

Test rušení přenosu

Mimo testu rušičkou pro přenos ve frekvenčním pásmu, kterým se zabývám v podkapitole ústředny, jsem provedl několik pokusů směřujících k ovlivnění přenosu signálu z vysílače magnetického kontaktu na ústřednu.

Test spočíval v obalování vysílače magnetického kontaktu pomocí alumíniové fólie vrstvu po vrstvě samostatně s připojeným magnetem. Celkem jsem testoval přenos pro pět vrstev fólie. Fólie byla o tloušťce 15 μm. Ovlivnění přenosu zachyceno v tabulce 3.2.

Vrstev	Přenos
1	Ne
2	Ne
3	Ne
4	Ne
5	Ano

Tab. 3.2 Rušení aluminiovou fólií

Zajímavou skutečností bylo, že vlivem hliníkové fólie došlo k změně magnetického odporu, který zaznamenal vyhodnocovací obvod a fólie tak bránila k sepnutí. Kontakt se posléze jevil jako rozpojený tudíž v poplachu.

Test narušení cizím magnetem

Tento test se zabýval možností ovlivnění kontaktu působením zdroje cizího magnetického pole a jeho nahrazením, případně okolnostmi, které by mohly v této skutečnosti fungovat.

Nahrazení cizím magnetem kancelářským: Pro tento první test jsem použil tři typy magnetů. Prvním byl typ FMI-A (16x5), druhý FMI-A (26x5), třetí FMA-A (27x10). Všechny tři typy jsou standardními kancelářskými feritovými magnety od společnosti MAGSY. Pokus byl zaměřen na schopnost kontaktu rozeznat cizí magnet od magnetu vlastního. Pokus byl proveden s každým magnetem 10 krát pro severní i jižní orientaci. Z celkového počtu 60 pokusů se zdařilo pouze dvakrát zmást magnetický kontakt natolik, aby zůstal sepnutý. Celkové narušení pomocí tohoto způsobu je velice málo pravděpodobné, neboť i v případě, že magnetický kontakt byl rozpojen, jsem nebyl schopen magnet připevnit tak, aniž bych způsobil rozepnutí systému. Tento způsob narušení bez znalosti síly působící z magnetu na kontakt je velice primitivní metodou a její hrozba pro systém je 3,3% z množiny pokusů.

Pokus č.	FMI-A (16x5)		FMI-A (26x5)		FMA-A (27x10)	
	Sever	Jih	Sever	Jih	Sever	Jih
1	ne	ne	ne	ne	ne	ne
2	ne	ne	ne	ne	ano	ne
3	ne	ne	ne	ne	ne	ne
4	ne	ne	ne	ne	ne	ne
5	ne	ne	ne	ne	ne	ne
6	ne	ne	ne	ne	ne	ne
7	ne	ne	ne	ne	ne	ne
8	ne	ne	ne	ne	ne	ne
9	ne	ne	ne	ne	ne	ne
10	ne	ne	ne	ne	ano	ne

Tab. 3.3 Narušení pomocí permanentních magnetů

Naproti tomu předpokládáme-li, že pachatel bude profesionál a místo narušení bude mít zmapováno například z fotek nacházejících se po různých sociálních sítích a z těchto fotografií si zjistí typ kontaktu. Pak pro něj zajisté nebude problém zajistit si stejný typ magnetu, který posléze použije jako falešný. Při mých pokusech jsem došel k závěru, že takovéto překonaní je velice snadné a jde zde pouze o cvik a hbitost při nahrazování původního kontaktu kontaktem cizím.

3.1.2 PIR Detektor

Hlavním cílem prováděných testů bylo zjistit, jaké jsou možnosti narušení PIR detektoru z hlediska ošálení infračerveného čidla a přenosové soustavy detektor-ústředna. Cílem těchto měření bylo stanovit nebezpečí vyplívající ze špatného měření a definovat protiopatření.

Tepelná citlivost

V rámci sledování ergonomie uživatele jsem zařadil mezi sledované parametry, také vhodnost umístění PIR detektoru vzhledem k nasměrování masky PIR detektoru na potenciální zdroje tepelného záření, jež mohou vyvolávat chybné informace a plané poplachy. Měření bylo prováděno ve dvou typizovaných rodinných domech, oba domy prošly tepelnou rekonstrukcí a mají nová plastová okna s nižší propustností tepla. Rozdíl v měření vzniká u použití detektorů a jeho umístění v rámci místnosti.

V prvním případě se jedná o PIR detektor typ LC-100 společnosti DLC. Jeho umístění a směr clony je patrný z obrázku 2.2 pod označením X1. Kde clona zabírá zřetelně balkónová okna.

V druhém případě se jedná o PIR detektor společnosti RISCO typ iWISE. Jeho umístění je patrné z obr. 2.2 pod označením P4.

Během ročního sledování obou zmíněných případů jsem shledal skutečnost, že zatímco na prvním konceptu byl zaznamenán planý poplach v celkem 6 případech, na druhém nebyl zaznamenán žádný.

Výše zmíněné případy byly zaznamenány v období mezi 17. Červnem a 28. červnem. Během mých úvah proč k tomu začalo docházet zrovna v tomto období, když před touto událostí nebyl zaznamenán problém, jsem vzal v úvahu známý fakt, že nasměrování do oken je vždy problematické. Problém je zde tedy sluneční záření vytvářející teplotu, která nepříznivě ovlivňuje teplotní složku nutnou k spuštění poplachu, ale stále zde nebyla druhá složka pohybová, neboť na oknech nejsou ani záclony či květiny které by mohly pohyb simulovat. Po podrobném přezkoumání problému jsem nad oknem pozoroval klimatizační průduch. Po porovnání času sepnutí klimatizace s časem vyvolání poplachu jsem došel k zajímavému zjištění, který jsem poté prakticky ověřil sérií pěti měření.

Vzduch před okny se vlivem slunečního záření pomalu oteploval a pozvolna vytvářel pomalu pohybující se teplotní masu. To samo osobě k vyvolání falešného poplachu nestačilo, ovšem po sepnutí klimatizační jednotky byl do místnosti prudce vržen studený proud vzduchu, který rychle odvál masu horkého vzduchu, ta začala proudit a v tom okamžiku se pro detektor jevila jako pohybující se narušitel a byla vyhodnocena jako poplach. Z pěti následných pokusů došlo k vyhlášení poplachu celkem třikrát.

Tento pokus jsem na stejném místě poté provedl i s detektorem PIR iWAVE s ochranou PET. Za stejných podmínek, takovýto proud vzduchu nedokázal spustit planý poplach ani v jednom případě.

Tedy z provedených měření a pozorování jsem došel k závěru nevhodnosti umístění detektoru do pozice X1 z hlediska správné funkce detektoru a generování planých poplachů. Při samotné instalaci je třeba dbát na veškeré teplovodní a vzduchové průduchy,

které by mohli v kombinaci s pohybem látky vyvolat planý poplach a snižovat tak dlouhodobě účinnost celého zabezpečovacího systému.

Narušení clonou

Test narušení clonou vychází z nutnosti PIR senzoru reagovat na složku pohybovou a teplotní. Zároveň je tento test aplikovatelný do situace, kdy umístíme detektor do místnosti která je s druhou oddělena tenkou stěnou například sádrokarton a podobné tenké materiály snadno proniknutelné pro vyšší frekvence. Pokud uživatele nerespektují takováto omezení a s vidinou, že budou mít chráněnou chodbu, se tak může stát, že ve vedlejší místnosti, kde budou například spát, se jim v noci po probuzení stane, že je detektor dokáže přes tuto tenkou stěnu zachytit i z vedlejší místnosti. Opět tato situace je častá zejména na chatách. Test spočívá v narušení střeženého prostoru pomocí dřevěné desky a tloušťce 1 cm, za kterou se bude narušitel pokoušet projít skrze střežený prostor. Test byl proveden desetkrát na PIR čidle popsaném v kapitole 2.3.4 s ochranou PET a bez ochrany PET.

Praktický test byl vykonán s 1 cm tlustou překližkovou deskou, kde na vnitřní straně byla umístěna držadla na ruce. Narušitel byl přikrčený a celím objemem se za desku skovával, aby snížil svoji siluetu.

Test dopadl podle očekávání dobře, z deseti pokusů na detektoru bez ochrany PET bylo zaznamenáno celkem 10 narušení. Při Testování s ochranou PET byla spolehlivost osm pokusů z deseti. Snížená úspěšnost u detektoru s ochranou PET ze přisoudit tomu že uživatel se pohyboval na hranici citlivosti z čehož vyplývá, že stínící deska má vliv na citlivost detektoru.

Tepelné zahlcení

Tato situace je poměrně častá a nastává zejména v objektech rekreačního charakteru, kde se často nevětrá budova je vyhřívána prosklenými plochami a přes střechu. V takovém objektu pak vzduch dosahuje vysokých teplot a znečišťuje tak svoji tepelnou stopou měřenou oblast. Detektor v takové oblasti je pak náchylný k přenosu chybných informací. Při tomto testu jsem vycházel z předpokladu, že zahltíme prostor sledovaný pomocí PIR tak pyroelement detektoru nebude schopen rozeznat tepelnou stopu narušitele

od okolního prostředí. Tento test byl prakticky zaměřen na to, jaký má vliv vytápění budovy na činnost zabezpečovacího zařízení, přesněji PIR detektoru.

Samotný pokus jsem provedl na detektoru popsaném v kapitole 2.3.4. Abych dosáhl požadované teploty v místnosti, použil jsem k dosažení požadované teploty 37°C dva 1500W přímotopy. Teplota byla monitorována pomocí digitálního teploměru GTH 1170 s typem měřícího senzoru: termočlánek typu K (NiCr-Ni) při rozlišení 0,1°C. Typ jsem zvolil vzhledem k rychlému zjištění stavu teploty. Vzhledem k nutnosti udržet teplotu v určitém rozmezí jsem zvolil k měření místnost obdélníkového tvaru o rozměrech 2,5x3 metru. Teplota narušitele byla naměřena pomocí rtuťového teploměru, teplota byla 36,7 °C.

Pokus	Teplota	Narušení
1	35,6	Ne
2	35,9	Ne
3	37,4	Ne
4	36,9	Ne
5	36,7	Ne
6	36,4	Ne
7	37,6	Ne
8	37,2	Ne
9	36,1	Ne
10	37,5	Ne
11	36,5	Ne
12	36,8	Ne
13	35,2	Ne
14	34,7	Ne
15	34,6	ANO
16	33,2	ANO
17	32,7	ANO
18	31,5	ANO
19	30,4	ANO
20	29,5	ANO

Tab. 3.5 Citlivost při tepelném zahlcení prostoru

Z naměřených hodnot vychází, že hodnota citlivosti čidla pro rozlišení rozdílu teplot se nachází v hodnotě 2,5 °C v kladném i záporném směru od hodnoty teploty narušitele. V běžných domácích podmínkách je velice nepravděpodobné, že by mohlo dojít k ovlivnění čidla detektoru pomocí běžných výtopných teplot. V případě, že by detektor

byl umístěn do místnosti, kde z nějakého důvodu předpokládáme takovéto teplot, např. skleník, doporučuji zde raději volit duální detektor.

3.1.3 Kouřové detektory

Vzhledem k novele zákona č. 133/1985 Sb. Musí být rodinný dům vybaven zařízením autonomní detekce a signalizace. Toto zařízení musí být umístěno v části vedoucí k východu z bytu nebo u mezonetových bytů a rodinných domů s více byty v nejvyšším místě společné chodby nebo prostoru. Jedná-li se o byt s podlahovou plochou větší než 150 m^2, musí být umístěno další zařízení v jiné vhodné části bytu (viz § 15 odst. 5). Z toho tedy vyplívá, že elektronická signalizace ochrany proti požáru se stává nejrozšířenějším typem zabezpečovací techniky a zákonitě se jí budou dotýkat nejvíce plané poplachy vlivem běžného používaná zejména vlivem kuchyňské činnosti. [21]

Test kouřivosti

Nejčastějším zdrojem planých poplachů na detektorech pracujících na fotoelektrickém a ionizačním principu je pára unikající při vaření. Tato pára je obyčejně nasycena mastnotou, a pokud není řádně odsávána, rozptýlí se do celého sledovaného prostoru. Cílem našeho testu bylo zjistit, jak daleko musí být umístěna varná deska při absenci odsávání od detektoru a zadruhé jak hustá musí být pára. Test jsme prováděli na fotoelektrickém detektoru popsaném v kapitole 2.3.5. Test spočíval v obohacování vody rostlinným olejem uvedeném do varu. Takto odpařovaná voda vytvářela vodní páru, detektor byl umístěn na protilehlé stěně. Místnost o čtvercovém obvodu velikosti 2x2m byla uzavřena bez jakéhokoliv odvodu vzdušných par. Místnost byla prázdná, bez přirozených překážek. Pouze vařič s hrncem o objemu deset litrů. Měření bylo provedeno pro čtyři úrovně par. První úrovní byla destilovaná voda o obejmu 6 litrů. Druhá úroveň bylo pět litrů vody a 250 ml rostlinného oleje. Třetí úroveň byla 4 litry vody na jeden litr oleje. Jako poslední čtvrtou úroveň jsem volil poměr jeden litr vody na jeden litr oleje. Těmito koncentracemi jsem simulovala dým vznikající při vaření. Na dobu odezvy jsem čekal do maximální hodnoty 10 minut od začátku varu. Pokud do této doby poplach nebyl

vyhlášen, pokus jsem ukončil. Mezi jednotlivými pokusnými měření jsem místnost po dobu jedné hodiny odvětrával, abych odstranil případné stopy po předchozím odpařování.

pokus	úroveň 1	úroveň 2	úroveň 3	úroveň 4	
1	ne/10:00	ne/10:00	ano/6:47	ano/5:30	reakce/čas
2	ne/10:00	ano/7:36	ano/8:31	ano/3:11	reakce/čas
3	ne/10:00	ne/10:00	ne/10:01	ano/4:17	reakce/čas

Tab. 3.6 Citlivost požárního detektoru na páry

Výsledné měření přineslo předpokládané výsledky a ukázalo se, že čím je roztok nasycen více tekutinou na bázi oleje tím je jeho hustota a neprůhlednost vyšší a detektor je náchylnější na plané poplachy to samozřejmě vyplívá z toho, že detektor musí být schopen tyto páry s hořícího oleje zachytit a detekovat jako požár. V měřeném rozmezí jsem byl nejméně úspěšný při vytváření planého poplachu s destilovanou vodou ta v měřeném období, nevytvořila poplach ani v jednom s měřených případů. Celkový výsledek je uveden v tabulce Tab. 3.6.

Test plamene

Tento test byl zaměřen na citlivost fotoelektrického bezdrátového zabezpečovacího protipožárního detektoru v závislosti na kouři vznikajícímu při používání běžných domácích potřeb, jako je svíčka, vonné tyčinky a podobné prostředky.

V rámci testu jsem vybral tři zástupce běžných domácích potřeb. Prvním byla svíčka pro použití v interiérech od společnosti Bartek Cannes s vůní cardamonu a kávy. Druhým měřeným předmětem se stala vonná tyčinka s vůní eukalyptu. Posledním pozorovaným předmětem byl doutník Alhambra. Pokus byl zaměřen na to, jak daleko musí být předmět vzdálen při běžném používání, aby nebyl planý poplach vyhlášen, pokud bereme přímočarou vzdálenost zapáleného předmětu od detektoru.

Test jsem provedl na 15 vzdálenostech, kde vodorovná vzdálenost od podlahy sledované místnosti byla vždy 1 metr a 50 centimetrů. K detektoru byla posunována pouze vzdálenost horizontální a to vždy po 20 centimetrech. Z výsledků v Tab. 3.7 je jasně vidět, že plamen nemá valný význam při vyhlašování poplachů na tomto členu. Pokud bychom měli plamen hořící čistě bez jakéhokoliv dýmu, pak můžeme plané poplachy zcela

vyloučit. To reprezentuje plamen u svíčky, avšak zde nastává problém při zhášení knotu, kde vzniká doutnání, pokud toto doutnání je blízko detektoru, jako se to stalo při pokusu mně, detektor samozřejmě zareaguje a vyhlásí poplach. Z měření vyplívá, že pokud máme v domácnosti použit fotoelektrický detektor, měli bychom se vyvarovat v jeho blízkosti používat vonné tyčinky a v žádném případě bychom neměli kouřit. Protože pokud je uživatel vášnivým kuřákem, pak se náchylnost k planým poplachům rapidně zvyšuje, jak ukazuje tab. 3.7.

Vzdálenost (v cm)	Doutník	Svíčka	Vonná tyčinka
300	ne	ne	ne
280	ne	ne	ne
260	ne	ne	ne
240	ne	ne	ne
220	ne	ne	ne
200	ne	ne	ne
180	ano	ne	ne
160	ne	ne	ne
140	ano	ne	ne
120	ano	ne	ne
100	ano	ne	ne
80	ano	ne	ne
60	ano	ne	ano
40	ano	ne	ne
20	ano	ne	ano
0	ano	ne	ano

Tab. 3.7 Ovlivnitelnost detektoru kouře domácími zdroji

Z výše popsaných testů vyplívá, že fotoelektrický detektor je v určitých popsaných situacích náchylný k planým poplachům, ale jen za předpokladu, že mu uživatel bude tyto potencionálně nebezpečné situace vytvářet. Vždyť od mnoha cigaret a vonných svíček v domácnosti vzniklo plno požárů, a proto jsou tyto detektory stavěny tak, aby požárům předcházely. Uživatel by si mněl při domácím využití těchto potřeb uvědomit nebezpečí z nich plynoucí a k tomu právě citlivost detektoru nabádá.

3.1.4 Ústředna

Při testování ústředny jsem zjišťoval možnost zarušení přenosového pásma pomocí rušičky a možnost zablokování vysílání informace o napadení systému pomocí sms za

předpokladu, že s ústřednou komunikujeme pomocí telefonu, tedy sim karta v ústředně je obsazena. Oba testy sice nejsou přímo vztažné k ergonometrii a v domácnosti tento stav v běžné situaci nenastane. Tento test má ovšem do značné míry jistou vypovídací hodnotu o bezpečnosti bezdrátových zabezpečovacích systémů.

Test zarušení pásma

Použití rušiček GSM pásma je v České republice protizákonné a upozorňuji, že tato kapitola neslouží jako návod a každý, kdo rušičku používá, se vystavuje riziku stíhání ze strany státních orgánů a policie České republiky.

Přestože je protizákonné takovéto rušičky používat jsou stále velice oblíbené na poli zločinnosti a to zejména při domácích krádežích a loupežích. Cena takovéhoto zařízení se pohybuje v základu již od 1500 Kč. Pro náš test jsem si vybral zařízení typu JM-110A-6Bb. Toto zařízení dokáže blokovat pásma GSM 900 i GSM 1800 a tím dokážete ochromit jakýkoliv přenos dat z ústředny na uživatele. Je třeba upozornit, že tato pásma neslouží ke komunikaci mezi ústřednou a detektory, ale pouze ke komunikaci s vnějším světem přes kanál systému GSM. GSM rušička je zařízení podobné telefonu a do telefonu ho odlišují pouze výrazné antény. Pro každé pásmo co má rušička blokovat se vyskytuje na přístroji vždy jedna výrazná anténa. Princip funkce GSM rušičky vychází ze vzorce $C=B.\log_2(1+P_s/P_š)$ [20]

Kde C je kapacita kanálu v bit/s, B je šířka kanálu v Hz a P_s a $P_š$ je výkon signálu a šumu. Sítě GSM mají šířku kanálu 200 kHz, přenosovou rychlost 270 kbit/s (na 1 TDMA rámec tedy 8 timeslotů) a jediné, co není dáno je výkon šumu a signálu v dané lokalitě. [20]

Výkon signálu je určen výkonem základnové stanice, přenosovým prostředím (tedy tím jaké prostředí nás obklopuje, zda jsme v domě, sklepě, budova je cihla dřevo, beton) a naší vzdáleností od základnové stanice, tak výkon šumu je za normálních okolností dán výkonem všech zdrojů elektromagnetického rušení v daném pásmu a v daném místě. Takovéto rušení bývá obvykle velice zanedbatelné. [20]

Rušička GSM pásma funguje tak, že začne generovat šumový výkon v pásmech, pro která je určena. To vede k tomu, že šumový výkon v daném bodě přesáhne výkon vysílače a pásmo GSM je tak zarušeno, neboť zde již není možné bezchybně přenést oněch 270 kbit/s potřebných pro komunikaci v síti GSM. [20]

Zařízení je na ovládání velice jednoduché na ovládání. Zařízení jsem spustil ve vzdálenosti od 15m do 5m od ústředny před zahájením průniku do budovy. Po aktivaci zabezpečovacího systému došlo k vyhlášení poplachu, přenosová pásma EZS nebyla narušena. Na každém stanovišti jsem provedl tři měření a bylo zjištěno, že rušička je účinnější, čím blíže je k blokovanému vysílači. Z pokusu je jasně vidět, jak k zarušení pásma došlo zhruba ve vzdálenosti 10m což bohatě postačuje k zarušení ústředny před vstupem do budovy u většiny domácností a budov.

Vzdálenost v (m)	pokus 1	pokus 2	pokus 3
15	Ne	Ne	Ne
14	Ne	Ne	Ne
13	Ano	Ne	Ne
12	Ano	Ne	Ano
11	Ano	Ano	Ano
10	Ano	Ano	Ano
9	Ano	Ano	Ano
8	Ano	Ano	Ano
7	Ano	Ano	Ano
6	Ano	Ano	Ano
5	Ano	Ano	Ano

Tab. 3.8 Narušení bezdrátové ústředny rušičkou frekvence.

Po vzdálení se z oblasti rušení ústředna neprodleně odeslala veškeré do té doby neodeslané informace o napadení. To je ale pozdě a jak se tedy bránit. Nejlepší jak se proti rušení pásma bránit je připojit ústřednu na pevnou datovou základnu tedy připojit jí přes kabel strukturovanou kabeláž například. UTP nebo lepe stínění kabel STP. Pevné připojení může být sice také přerušeno, ale pokud budeme používat kombinaci obou zmíněných provedení tedy bezdrátového přenosu a kabelového přenosu vždy máme jistotu, že se o nestandardní situaci dozvíme včas.

Druhou možností jak těmto rušičkám vzdorovat v místech kde není možné pevné připojení je zajištění komunikace přes systém UMTS běžněji znám jako 3G síť. UMTS nejen že má kanál široký 5Mhz ale zároveň používá kódování CDMA které potřebuje k přenosu pouze 64 kbit/s na rozdíl od GSM jež potřebuje 270 kbit/s. Tato síť naproti

narušení pojatně bezpečnější a zařízení na její blokaci jsou mnohem hůře k sehnání na dnešním trhu.

Test blokování telefonem

Tento test spočívá v jednoduchém zablokování ústředny přes obsazení linky. Test byl proveden v deseti případech s účelem zablokovat ústřednu obsazením linky. Po spojení s ústřednou byl na některém z výstupních detektorů uměle vygenerován poplach a sledovala se reakce ústředny. Ve všech deseti případech ústředna hovor odpojila a odeslala informaci o narušení. Z testu je tedy patrno, že takovýmto způsobem není možno ústřednu narušit.

3.1.5 Shrnutí

V této kapitole jsme se zaobírali testy, které vyplívají ze situací, jež mohou v domácnosti nastat a jsou potencionálně nebezpečné pro správné vyhodnocení signálu na ústředně. V testech se jasně ukázalo, že detektory svoji činnost provádějí dobře, dalo by se i říci, že více než dobře, kdy jejich výborná citlivost dokáže neseznámenému uživateli přinést mnoho překvapení a v tom je právě ten problém. "neseznámenému uživateli" Každý uživatel by se mněl seznámit s obecnou funkcí systému, aby takovýmto situacím zabránil a nedivil se, že když si v domě kouří tak se mu spustí protipožární hlásič anebo, že když bude lít na detektor vodu, že zkratuje a bude vysílat chybné signály. Tyto testy nemohou nikdy suplovat zátěžové testy jednotlivých prostředku EZS, ale mají poukázat na situace, které v domácnosti běžně mohou nastat a na co by si měl dát uživatel ve vztahu k zabezpečovacímu systému pozor, tak aby systém fungoval bez problému a hlavně nezpůsoboval zbytečně plané poplachy. Z toho plyne pro uživatele jasné poučení, že by měli trvat na zevrubném vysvětlení funkce svého zabezpečovacího systému a to samé platí ze strany technika. Kdy technik by měl dostatečně seznámit se všemi aspekty, které s užíváním zabezpečovacího systému vyplívají, neboť systém EZS není hračka a jeho zneužívání ošetřuje zákon a takovému to technikovi ušetří i práci tím, že nebude každou chvíli muset odpovídat na stížnosti uživatelů, že jejich systém EZS je rozbitý.

4 Analýza sledovaných dat - Chování uživatele (ergonometrie)

Uživatel je nejslabším článkem každého zabezpečovacího systému, ale nelze ho vyloučit, neboť právě pro něj je zabezpečovací systém vytvořen. V této kapitole podrobně rozebereme chovaní člověka v závislosti na zabezpečovacím systému.

4.1 Člověk a informace

Z mého pozorování vzešel právě fakt, že nečastěji vznikají plané poplachy na magnetických kontaktech a to zejména kolem 9 hodiny večerní v létě. Při dalším zkoumání jsem došel k závěru, že tento jev je způsoben častějším větráním, kdy dochází k většímu namáhání součástí EZS. Všeobecně z výzkumu vyplývá, že slunečné dny díky tomu i letní měsíce, které mají převahu slunečných dnů, jsou náchylnější na plané poplachy. Samozřejmě člověk není jediným strůjcem poplachů, ovšem z mého sledování vyplívá, že je tím nejčastějším, ať už z příčiny nepochopení funkce systému špatným seznámením s náležitostí jeho obsluhy, nebo jen zapomnětlivostí. Člověk se, ať přímou či nepřímou měrou, podílí na téměř 90% procentech planých poplachů. Níže si rozebereme, jak tyto situace vznikají a v jakém procentu se objevují na měřeném vzorku.

	Uživatel1	Uživatel2	Uživatel3	Uživatel4	Uživatel5	Celkem
Magnetický kontakt	9	6	4	2	1	22
PIR	1	3	2	0	0	6
Požární hlásič	1	5	0	1	0	7
Jiné	1	1	0	0	1	3
CELKEM	12	15	6	3	2	38

Tab. 4.1 Souhrn planých poplachů

Za šestnáctiměsíční sledování systému bylo způsobeno celkem třicet osm planých poplachu, to znamená, že byl průměrně planý poplach způsoben přibližně 2,375 krát do měsíce. (Tab. 4.1)

4.1.1 Špatná obsluha

Pod pojmem špatná obsluha rozumíme souhrn všech planých poplachů, které vylívají z nedodržení aktivace, deaktivace systému přes přístupové porty (klávesnice, klíčenky). Špatná obsluha pramení z nedostatečného proškolení uživatelů, nebo také z nedodržení základních principů, které mnohdy pramení z pouhé zapomnětlivosti.

Typickou modelovou situací, která byla zaznamenána během měření dvakrát, je, že uživatel aktivuje zabezpečovací systém a odejde z domu. Cestou například na autobus či k vozidlu si vzpomene, že něco zapomněl a vrací se zpět, vejde do budovy, která je v procesu aktivace a než by znovu provedl deaktivaci, rozhodne se, že to není potřeba. V tomto momentě aktivace skončí a uživatel je chycen pohybovým detektorem. Tato situace ovšem může pramenit i v případě, že zvukový signál není dostatečně slyšet nebo je vypnut z důvodu zamezení lokalizace ústředny pomocí zvukového vjemu. V prvním případě je zcela na vině uživatel, který nerespektoval zvukovou výstrahu, v dalších případech tomu již tak být nemusí. Předpokládáme-li, že uživatel vchází do střeženého objektu, je zcela zásadní, aby byl uživatel dostatečně upozorněn na nutnost deaktivace zabezpečovacího zařízení. V případě, že se jedná o domácnost, jako v našem případě se dá ještě tolerovat neexistenci výstrahy aktivace a deaktivace za předpokladu, že uživatele budou disciplinovaní, ovšem to se většinou neděje a je tedy třeba hledat jiná řešení.

4.1.2 Stresový faktor

Ať si to uvědomujeme nebo ne je každý poplach, ať se na konci projeví jako planý, velice stresový zejména dojde li k němu v noci. Uživatel pak nereaguje správně a dělá chyby, pokud se chyby kupí a systém nereaguje tak, jak uživatel předpokládá, začíná takový uživatel podléhat panice a to i za předpokladu, že se jedná o planý poplach. K tomu může přispět špatně definovaný výstup z ústředny, samota, či stísněné podmínky. Stresový faktor, ale nemusí nutně být způsoben pouze vyvoláním poplachu, ale třeba i situací kdy odezva ústředny na klávesnici je vlivem zhoršeného přenosu delší než uživatel očekává. Za takových okolnosti pak uživatel neví, zda použil správné klávesy a mačká je nahodile a dostává se do stavu, kdy systém deaktivuje pouze částečně a podobně.

Během pozorování jsem zaznamenal několik takových situací. Prvním problémem uživatele je stisknout klávesy ve správném pořadí. V několika případech, které nastávají z pochopitelného důvodu zejména v ranních hodinách, kdy uživatel vychází z RM spánku a není ještě v plném provozuschopném stavu, uživatel nejprve nedodrží postup a místo deaktivační klávesy začne zadávat kód. To má za následek jediné, nic se nestane a v paměti zůstane uložena klávesa pro zónu dva. Uživatel vidí, že se bezpečnostní systém nedeaktivoval a zmáčkne příslušnou klávesu, poté zadá kód, ale již si nevšiml, že je předvolena pouze zóna dvě a dochází k situaci, že objekt je částečně deaktivován a uživatel otvírá vstupní dveře, s tím dochází k zpožděnému narušení a systém začne hlásit, že je v procesu deaktivace. Uživatel, který by v domnění, že je vše v pořádku neví, co se stalo a začíná podléhat panice, v této situaci nereaguje adekvátně a začíná zadávat kód bez příslušné klávesy a dostává se do spirály nemožnosti deaktivace bezpečnostního systému. Tato situace je vyřešena pomocí jiného uživatele, který není do stresoru zahrnut a reaguje s klidnou hlavou a systém bez problému deaktivuje. Pokud takováto situace nebo ji podobná nastane, je bezprostředně nutné, aby byl z daného problému vyvozen nějaký závěr. Tedy určení chyby a sdělení této chyby uživateli, který reagoval vlivem stresu nesprávně.

Stresu se nedá zabránit, pramení z našeho pudu ohrožení, ale dají se snížit jeho emulátory tedy situace, které umocňují stresovou situaci.

- Zprávy přicházející na mobilní zařízení, ať už je to telefon nebo email musí být co nejjasnější, aby bylo zabráněno zmatečnému chování uživatele, který bude hledat otevřené okno v jiné místnosti.
- Zvukový výstražný signál musí být upozorňující a ne ohlušující vysoké tóny a frekvence umocňují pocit ohrožení a paniky.
- Deaktivace v ranních hodinách přes klávesnici může být nahrazena pomocí bezdrátové klíčenky, kde nehrozí riziko špatné posloupnosti kláves.
- Dobu prodlevy k deaktivaci přizpůsobit potřebě uživatele s nejhorší schopností práce s tímto systémem tak, aby i on měl komfort při deaktivaci.

- Nastavit prodlevu pro všechny detektory, které by mohly překážet pohodlné deaktivaci. Tedy aby uživatel do jejich chráněných zón nemohl vstoupit během deaktivace náhodně.

4.1.3 Špatná koncepce

Problém špatné koncepce není ani tak problémem uživatele jako realizátora samotného systému. U velkých firem a velkých zabezpečovacích systému je projekt přesně zpracován analyticky navržen, na provádění a výstavbě se podílí několik někdy i desítek lidí. Jiná situace je zabezpečovacích zařízení určených pro domácnost, tyto systémy bývají v některých případech realizovány bez jakékoliv koncepce a přítomnosti technika v jiných případech vycházejí z neúplných informací od zadavatele, který opomněl zmínit pro něj nepodstatnou informaci, ale pro činnost systému stěžejní. Dalším důvodem je, že zadavatel trvá na některých požadavcích, ať jsou z technického hlediska chybné anebo, nerespektují zásady instalace. Než aby se poté technik držel zásad, raději zadavateli ustoupí a obejde instalaci ne úplně správnou cestičkou.

4.2 Plané poplachy

Z dlouhodobého sledování jasně vyplynulo, že nejčastějším zdrojem planých poplachů je magnetický kontakt, ať už se jedná o vratový magnetický kontakt nebo kontakt garážových vrat. Jako druhý nejčastější zdroj se umístil kouřový hlásič. Naopak u PIR detektorů dochází k planým poplachům zřídka.

4.2.1 Příčiny

Plejáda příčin planých poplachů je poměrně různorodá a je těžké tak hledat nějaký společný jmenovatel. U některých detektorů to však jde definovat poměrně přesně kupříkladu u detektoru kouře.

Detektor kouře

Ve sledovaném období byl na detektoru kouře planý poplach zaznamenán v sedmi případech (tab. 4.2), z toho čtyřikrát byl způsoben párami unikajícími při vaření a dvakrát prašností. V jednom případě se přesná příčina nepodařila stanovit.

	Kuchyně (páry)	Prašnost	Nezjištěno
Počet	4	2	1

Tab. 4.2 Příčiny poplachů na detektoru kouře

Hlavním důvodem příčin planých poplachů na detektoru kouře je zanedbání údržby a to zejména v případě, že detektor máme umístěny ve velmi prašné oblasti jako je kotelna, uhelna, sklad. V našem případě byl detektor po dobu tří měsíců umístěn ve velmi prašné místnosti mezi uhelnou a kotelnou. Pokud k takovému to umístění dojde je potřeba detektor udržovat, protože detektor kouře pracuje na principu fotoelektrickém, kde je měřena svítivost. v střeženém prostoru. Pokud se do měřící komůrky detektoru dostane kouř, svítivost se sníží a je generován poplach. Výrobce tuto komoru samozřejmě chrání před vnikáním nečistot zvenčí, ale nikdy nemůže zabránit tomuto vnikání úplně. Vlivem proudění vzduchu se prachové částečky poměrně snadno dostávají do této komory a hrozí zde zanesení prostoru prachem. Tyto detektory jsou vysoce citlivé na takováto zanesení a je potřeba pravidelně tento prostor profukovat abychom očistili prostor. Po zavedení pravidelného recirkulačního cyklu vzduchu na senzoru v intervalu jedenkrát za měsíc se problém s tímto planým poplachem zcela vytratil. Pokud víme, že místo, které jsme vybrali na umístění tohoto detektoru je prašné, je třeba profukovat senzor častěji, nebo raději volit jinou variantu umístění do prostor, kde je prašnost nižší.

Je asi samozřejmé, že plané poplachy na detektoru kouře zapříčiňují častěji ženy než muži neboť žena je nejčastěji tím, kdo vaří nebo připravuje pokrmy. Příprava pokrmů v kuchyni má velký vliv na plané poplachy na tomto druhu zabezpečovacího detektoru, zejména mály chránit kuchyni před ohněm. Jak jsme si ukázaly v kapitole testy, jsou protipožární hlásiče náchylné na dým způsobený párou.

V kuchyni totiž vzniká během vaření velké množství vodní páry a v mnoha případech je tato pára nasáklá odpařující se mastnotou. Tato pára velice silně připomíná kouř a její světlost je díky mastnotě podstatně nižší. Takováto pára dostane-li se do

světelné komory, způsobí planý poplach. Během sledování se vyskytl problém s usazováním mastnoty na senzoru, který pak nedával správné údaje o své činnosti. To bylo zapříčeno neexistencí odsávacího systému, tedy digestoře a naprosto nevhodným umístěním detektoru do na boční zeď, která sice nesousedí přim s varným zařízením, ale vzhledem k neexistenci digestoře se pára vlivem teploty vznesla k hornímu okraji místnosti, kde se posléze rozprostřela po celém prostoru a docházelo tak k zanášení senzoru. Po instalaci odsávacího zařízení byl tento problém naprosto odstraněn, neboť mastná pára je odváděna mimo detektor a nehrozí tak zahlcení senzoru falešným signálem.

Elektronická protipožární signalizace je velice důležitá zejména v dnešní době, kdy domácnosti vybavujeme stále větším počtem domácích spotřebičů, kde hrozí jisté riziko vzplanutí zejména tepelné. Kouřové detektory jsou velice citlivé, a proto mohou zachytit i jemné počáteční doutnání a vyhlásit tak poplach před vypuknutím požáru. Mnozí uživatelé si neuvědomují rozdíl mezi kouřovým detektorem a detektorem CO, které pracují na rozdílném principu. Takové to detektory je nutné umístit rozdílně a nepodceňovat nikdy jejich hlášení a je nutné pátrat i po nepatrných náznacích dýmu. Z pozorování jsem zjistil, že uživatelé se při spuštění poplachu prvotně nezajímají o poplach, ale o to jak nejrychleji vypnout zvukovou signalizaci a pokud nikde nevidí oheň signalizaci, ignorují a nehledají možné doutnání, pokud to není do očí bijící.

Magnetický kontakt

Nejčastější příčinou planých poplachů na magnetickém kontaktu jsou výhradně chyby uživatele. Nejčastější příčinou je, že v době zablokování plášťové ochrany uživatel otevře nějaký z hlídacích kontaktů na okně nebo dveřích. Nejčastěji k tomu dochází na oknech a u vrat garáží. V obou případech to na sledovaném objektu bylo v sedmi případech. Dále pak na vstupních dveřích, kde byl planý poplach zaznamenán v šesti případech, nejméně k planým poplachům dochází u balkónových dveří a to pouze ve dvou případech (tab. 4.3).

	Vstupní dveře	Okna	Balkón	garážová vrata
Počet	6	7	2	7

Tab. 4.3 Příčiny poplachů na magnetickém kontaktu

Při dlouhodobém sledování se ukázalo, že magnetické kontakty jsou nejvíce náchylné na plané poplachy. Samotný magnetický kontakt je velice jednoduché zařízení a plané poplachy vlivem jeho poruchy jsou ojedinělé. U bezdrátového kontaktu je jediný problém s přijímačem a vysílačem signálu, který již není tak bezproblémový. Pokud bychom porovnaly magnetický kontakt bezdrátový a drátový bude ten drátový jasně spolehlivější. Ovšem během sledování se problémy s vysílačem projevili jen velice málo a to u frekventovaných vstupních dveří, kde špatně nastavena odezva signálu prodlužovala dobu nutnou nechat otevřené dveře, pokud uživatel tuto dobu nedodržel, vysílač na magnetickém kontaktu neodeslal správnou informaci o poloze kontaktu a ústředna vyhodnocovala systém jako rozepnutý. Ač se to zdá, jako maličkost je při instalaci magnetického kontaktu na dveře nutné dbát toho zda uživatel nemá domácího miláčka, protože vpouští li-ho dovnitř vstupními dveřmi a je tato odezva nastavena na dlouhou dobu pak zvíře například kočka proklouzne dveřmi velice rychle a uživatel okamžitě uzavírá dveře ve zlomku sekundy. To vede k tomu, že nedojde opětovné komunikace vysílače a ústředny a kontakt se jeví jako otevřený a vyhlašuje se tak falešný poplach po zapnutí systému. S tímto jevem jsem se během pozorování setkal několikrát.

Pokud pomineme výše popsaný problém s komunikací je magnetický kontakt jinak velice spolehlivý, problémy na něm vznikají výhradně chybami uživatelů, kteří nerespektují uzavření systému a jeho aktivaci.

Pohybové detektory

Pohybové detektory jsou z hlediska planých poplachů poměrně málo náchylné na plané poplachy za předpokladu, že jsou při instalaci respektována pravidla o jeho umístění. Pokud tyto pravidla technik dodrží, pak jsou plané poplachy na pohybovém detektoru méně časté než na jiných součástech EZS. Tato zkušenost vyplývá i z mého pozorování, kde byli detektory umístěny podle těchto zásad. V době pozorování byla z PIR detektoru odeslána na ústřednu informace o poplachu pouze v šesti případech. Z toho ve čtyřech těchto případech byl příčinnou tohoto planého poplachu domácí miláček a ve dvou uživatel, který se po aktivaci do domu vrátit a prošel do zóny, kde byl detektor již v režimu střežení. (tab. 4.4)

	Domácí zvíře	zachycení uživatele
Počet	4	2

Tab. 4.4 Příčiny poplachů na PIR

Z tohoto sledování vyplívá, že pohybové detektory jsou z hlediska planých poplachů nejvíce citlivá na domácí zvířata a je při instalaci takovéhoto systému nutné s tím počítat. Je samozřejmé, že v některých případech uživatelé ani nepočítají s tím, že budou mít domácího miláčka, ale pokud ho máme, jako v našem případě je velice důležité si uvědomit, že taková kočka se dokáže schovat ve všech možných zákoutí a není možné jí vždy nalézt a přesunout ji do oblasti s ochranou PET, jako uživatelé bychom měli z důvodů prevence raději vybavovat všechny naše pohybové detektory maskou s ochranou PET. Pokud jsem technik je potřeba důkladně s uživateli při sjednávání zakázky prohovořit a sdělit všechna rizika spojená s pohybem domácího zvířectva ve střežené oblasti. Technik by měl také důrazně poučit o nutnosti vybavení takovýchto zón ochranou PET.

Druhý zaznamenaný faktor planých poplachů vzniká z problému, kdy je nutné nechat během aktivace některé součásti zabezpečovacího systému ve zpožděném režimu. Takovéto detektory se po aktivace systému přesunou do stavu standby, kdy detektor setrvá v tomto stavu po zvolenou časovou prodlevu. Uživatel pak má pocit, že je systém celí v takovémto režimu. V našem sledovaném případu pak vznikly právě dva případy, kdy uživatel po aktivaci si vzpomněl, že ve vedlejší místnosti zapomněl nějakou věc a vracel se pro ni, v této místnosti však detektor nebyl zpožděný a uživatel se chytnul do vlastního zabezpečovacího systému. V tomto případě není jiné možnosti než uživatele důkladně seznámit s rozsahem zpožděných zón. Ovšem riziko zapomenutí v této uspěchané době nelze vyloučit a neexistuje tak účinná rada jak bychom se těmto planým poplachům vyvarovali. Pokud nechceme zloděje upozornit vizuální pomůckou na dveře, kde se nachází zabezpečená zóna.

Ústředna

Během sledovaného období nebyl zaznamenán žádný poplach, který by se týkal přímo ústředny. Ústředna sama osobě totiž není aktivní prvek ochrany a tak se nedá divit, že by na něm byl hlášen planý poplach. Ovšem problémy s užíváním se ústřednám nevyhýbají. Problém bezdrátové komunikace je ten, že v určitých případech může být

signál zarušen, jak jsme si ukázali výše a nemusí to být pouze vlivem speciálních rušiče na rušení přenosového pásma. V sledovaném období celkem 32 ústředna hlásila pokles signálů GPS a 5 ztrátu kontaktu s některým ze svých členů. Z toho dvakrát nebyla tato ztráta způsobena poklesem napětí na daném členu. Problém volby umístění ústředny je velice složitý a měl by při instalaci na něj brán veliký důraz. Je potřeba spojit potřebu nedostupnosti ústředny a zároveň dobrého signálu, zvláště pak pokud hlavním přenos informace o napadení je poskytován uživateli pouze formou sms. Uživatel by se měl plně seznámit se signály, které ústředna poskytuje tak aby mohl rychle a efektivně poplach nebo problém identifikovat, tak aby mohl rychle odlišit, zda se jedná s největší pravděpodobností o falešný poplach, anebo zda ústředna opravdu detekuje na svých detektorech pokus o napadení nebo sabotáž.

Před instalací by si měl uživatel ověřit sílu signálu GSM v místě kam se chystá uložit ústřednu. Pokud je signál nedostatečný je potřeba zvolit jiného operátora s tímto také souvisí problém předplacených sim karet. Taková to karta má pouze omezený kredit a je potřeba dbát na pravidelnou kontrolu, zvláště v situacích, kdy jsme měli období několika planých poplachů. V našem sledovaném případě se jednou stalo, že kredit byl vyčerpán a při jednom z planých poplachů se o problému uživatel dozvěděl, až o několik hodin později. Je tedy třeba zvážit, zda raději než předplacenou kartu nevolit tarif, kde se tato situace nemůže stát, anebo zda se napojit na PCO, který poskytuje většinou balíček s výhodnou tarifní kartou.

5 Porovnání odolnosti koncepcí

Abych mohl lépe říci, jak uživatelé pracují se zabezpečovacími systémy, musel jsem provést průzkum v terénu. V rámci svého zaměstnání jsem oslovil databázi našich uživatelů s cílem zjistit pomocí jednoduchého formuláře, zda využívají EZS od jaké společnosti a co bylo důležité při jeho pořízení. Celkem bylo osloveno pomocí automatizovaného systému pro sběr dat 516 lidí, z toho 237 odpovědělo na otázku, zda mají v domácnosti instalovaný bezpečnostní systém. Kladně odpovědělo 33 z dotázaných. Těchto 33 dotázaných vyplnilo přiložený formulář, ze kterého jsou níže formulované výstupy získány.

Hlavním zjištěním průzkumu bylo že 13,9% dotázaných má doma zabezpečovací systém to znamená, jeden zabezpečovací systém připadá na každého desátého dotazovaného. V počtu dotazovaných bylo zajímavé, že lehce převládaly ženy, což se dá odůvodnit tím, že ženy mívají větší starost o své bezpečí a bezpečí svojí rodiny jak ukazuje tab. 5.1 Bereme-li to v procentech pak 59 % žen má ve své domácnosti zabezpečovací systém.

F1. Pohlaví	**Celkem**	**muž**	**žena**
Muž	41%	100%	0%
Žena	59%	0%	100%
počet dotázaných	**32**	**13**	**19**

Tab. 5.1 Profil dotazovaných

Odpovědi mužů a žen se vesměs neliší. Muži jsou spíše aktivnější, pokud se jedná o domácí instalace na rozdíl od žen. Alarmující je ovšem fakt, že 26% (tab. 5.2)dotázaných uvedlo, že si zabezpečovací systém zařídilo doma samo. V tomto případě se jedná převážně o muže, kteří jako hlavní důvod při výběru zabezpečovacího zařízení uvedly cenu a to do 15 000Kč. Je s podivem, kolik lidí se spoléhá na domácí instalace, bez konzultace s odborníkem. Takováto domácí řešení mohou mít velice nepříznivý vliv při nedodržování výše popsaných zásad na vznik planých poplachů.

F4. Instalaci provedena?	Celkem	muž	žena
technik	74%	67%	87%
sám doma	26%	33%	13%
počet dotázaných	33	13	19

Tab. 5.2 Způsob instalace

Mezi zabezpečovacími systémy převládá mezi dotázanými jak u mužů tak žen společnost Jablotron, kterou uvedlo 33% dotázaných jako značku svého zabezpečovacího systému. Jablotron označovali převážně lidé se zabezpečovacím systémem v hodnotě 15 000 Kč a 25 000 Kč v první kategorii byl označován bez dvou výjimek výlučně Jablotron. Jablotron také s převahou převládá mezi lidmi, kteří svůj zabezpečovací systém instalovali bez pomoci technika.

Druhou nejčastěji jmenovanou společností se stala společnost RISCO, ta se umístila na druhém místě, kde jí označilo 24% dotázaných. Převážně mužů, jejichž nejčastější odpovědí bylo, že při pořizování systému hleděli nejčastěji na kvalitu. Hodnota systému od společnosti RISCO se převážně pohybovala v rozmezí od 25 000 Kč až 40 000 Kč. Zbylé společnosti byly zmíněny po jednom či dvou dotázaných a nelze tak lépe říci zda jsou oblíbenější spíše u žen, nebo mužů jak ukazuje tab. 5.3.

F3. Od jaké společnosti?	Celkem	muž	žena
Jablotron	33%	31%	37%
Risco	24%	38%	11%
Crow	6%	0%	11%
Bosch	3%	0%	5%
Honeywell	3%	8%	0%
Alarm absolón	6%	0%	11%
Genesis	9%	0%	16%
jiné	15%	23%	11%
počet dotázaných	**33**	**13**	**19**

Tab. 5.3 Preferované značky

5.1 Důvody pro pořízení

Z hlediska chování uživatele nám velice napoví důvod, pro který se uživatelé rozhodli svůj zabezpečovací systém pořídit. Hlavním důvodem, který byl nejčastěji jmenován, se stala potřeba zabezpečit sebe a svoji rodinu 34% (tab. 5.4). Pokud přiřadíme k důvodu bezpečí, podmínku účasti technika zjistíme, že valná část lidí uvedla, že si svůj systém instalovala sama a tedy i zároveň za nízkou pořizovací cenu. Dá se tedy předpokládat, že mezi obyvateli panuje jistá obava o své bezpečí, ale zároveň nedisponují dostatkem finančních prostředku na složitější a tím pádem také dražší systémy a proto volí levné a ne tak účinné prostředky ochrany, aby alespoň nějak ochránily svoji rodinu a sebe.

Druhou velkou skupinou jsou lidé, kteří udávají, že si svůj zabezpečovací systém pořídily z důvodu nižší pojistky, to uvedlo 31% dotázaných (tab. 5.4). Pokud uživatel udal tento důvod, bral při výběru výrobce systému hlavně na radu technika. Pokud uživatel odpověděl, že systém pořizoval pro nižší pojistku tak to bylo vždy s asistencí technika.

Tento výsledek se dal předpokládat, neboť certifikát pro pojišťovnu zhotovuje právě proškolený technik. Zajímavostí zde je, že pokud lidé udávali, že nepoužívají zabezpečovací systém pravidelně, bylo to právě z této skupiny.

Další velkou skupinou byli uživatelé, kteří uváděli, že si svůj dům musely vybavit zabezpečovacím zařízením (16% tab. 5.4) například, že by nedostaly pojistku, v domě mají drahé vzácné sbírky a podobně. Tato skupina uživatelů volí, draží zabezpečovací systémy většinou v rozmezí 40 000 Kč a více. V této skupině jsou pouze ženy a dá se předpokládat tedy, že tyto ženy v domácnosti podnikají, mají tam při domě sklad s uskladněným zbožím či podobně. Tyto uživatele dále uvedly, že upřednostňovaly při výběru zabezpečovacího systému kvalitu, nad vším ostatním cena zde nehrála žádnou roly.

Poslední skupina uživatelů (13% tab. 5.4)uvedla, že si zabezpečovací systém pořídila po krádeži, ať už to byla krádež u nich doma nebo v jejich přímém okolí. Tato skupina lidí prostupuje všemi směry. Tedy nepřevládají zde ani lidé s drahým zabezpečovacím systémem, nebo že by si volily specifický zabezpečovací systém od konkrétního výrobce.

F5. EZS jsem si pořídil z důvodu?	Celkem	muž	žena
Bezpečí	34%	31%	33%
Slevy na pojištění	31%	38%	28%
musel jsem (kvůli pojišťovně atd.)	16%	0%	28%
po krádeži	13%	15%	11%
jiné	6%	15%	0%
počet dotázaných	**33**	**13**	**19**

Tab. 5.4 Důvod pořízení EZS

Dalším zajímavým zjištěním je, že méně než 50% dotázaných uvedlo, že mají zabezpečovací zařízení připojeno k pultu centralizované ochrany. Pouhých 39% dotázaných uvedlo, že mají systém připojen na PCO. Pokud uživatele uvádějí, že je jejich systém napojen na PCO pak jedná se převážně o dražší systémy přesahující cenu 25 000 Kč a u systému v kategorii 40 000 Kč je tomu tak vždy. Pokud je systém připojen na PCO jedná se vždy o systém, který byl instalován odborným technikem. Tyto uživatelé také udávají, že při instalaci systému daly na radu technika při výběru výrobce a celkového

uspořádání. U levnějších zabezpečovacích systémů se pak připojení na PCO vůbec nevyskytuje a to především kvůli ceně kterou tato služba stojí. Je v celku na zamyšlení zda se v dnešní době PCO vyplatí tedy hlavně od jaké firmy. Vzhledem k tomu, že podle průzkumu mezi zloději bylo zjištěno, že průměrné vloupání není delší než 15 minut [20], stojí za zváženou, zdá pořizovaná služba stihne v tomto krátkém úseku skutečně včas zareagovat na takovýto poplach anebo ne. Pokud se tedy rozhodneme pro zabezpečovací systém napojený na PCO je potřeba si zajistit společnost, která může v reálných podmínkách, při zjištěném narušení skutečně dorazit na místo včas bez zbytečných časových prodlev pokud to společnost není schopna zajistit je pak takováto služba k ničemu a postrádá svůj smysl.

5.2 Parametr pro pořízení

Dalším důležitým ukazatelem o vztahu uživatele a zabezpečovacího zařízení je parametr, který ho vedl investovat do konkrétního systému. Nejvíce uživatelů uvedlo, že při výběru zabezpečovacího zařízení se moc neangažovalo a nezajímalo se o bezpečnostní zařízení před samotnou instalací a nechalo vše na technikovi, to uvedlo 36% dotázaných s mírou převahou žen. U této kategorie konkrétně jsem očekával spíše větší nepoměr mezi ženami a muži, neboť ženy bývají k technickým záležitostem méně všímavé než muži. Celkové zastoupení 36% (tab. 5.5) dotázaných svědčí o tom, že uživatele jsou si vědomi toho, že problematičnost zabezpečovací techniky, by měli nechat na specialistech, ovšem úplné odevzdání do jejich rukou také může mít své následky. Zejména pro nás jako uživatele neboť, nesladíme-li zabezpečovací systém, s našimi potřebami každodenního života stane se systém pouhou přítěží pro svou složitost a po čase se může stát, že mi jako uživatel úplně nebo i částečně přestaneme zabezpečovací systém používat. Pokud se tak stane, z tohoto důvodu, je třeba hledat chybu u technika, který dostatečně neseznámit uživatele se svým domácím systémem. Čas dotázaných dokonce uvedlo, že jim bylo úplně jedno, jaký zabezpečovací systém dostane a plně důvěřoval při výběru zařízení a koncepce celého systému výhradně firmě u které měl zabezpečovací systém objednaný.

Jako druhý důvod dotázaní odpověděli, že při výběru zabezpečovacího zařízení upřednostnilo cenu před vším ostatním, k tomuto stanovisku se přihlásilo 30% (tab. 5.5)

dotázaných uživatelů. Je zajímavé, že jako důvod cenu uváděli spíše ženy nežli muži. Je ale zajímavé, že když uživatele preferovali cenu tak z jejich doplňkových komentářů vyplívá, že se nerozhodovali podle toho, kdo je nejlevnější, ale spíše tím, že mají stanovenou sumu peněz a přes tu nepůjdou a je jim jedno, od jaké firmy to bude. Takže ve finále mohl uživatel za svoji sumu peněz dostat profesionální systém od společnosti Risco. Tato skupina uživatelů samozřejmě také dala na radu specialistů, ovšem vždy cena převládla nad účelností.

Třetím nejčastěji udávaným faktorem, který převládl u uživatelů, při nákupu zabezpečovací techniky byla kvalita (15% tab. 5.5). Uživatelé uváděli, že kvalitu zjišťovali hlavně na internetu z různých diskuzí nebo s rozhovorů s prodejcem. Uživatele dále konstatovali, že chtěli míst systém hlavně spolehlivý a bez nutnosti dlouhodobých zásahů. Tyto lidé volily systémy drátové koncepce vzhledem k větší bezpečnosti a bez nutnosti údržby, tedy bez nutnosti vyměňovat baterie a hlídat kvalitu signálu mezi čidly a ústřednou.

Čtvrtým důvodem bylo doporučení, to uvedlo 12% (tab 5.5) dotázaných. Uživatele konstatovali, že dali na doporučení svého známého nebo kamaráda popřípadě známého, který má s dotyčným zařízením dobrou zkušenost, a proto se rozhodly pro ten daný model a až teprve poté hledaly firmu nebo technika, který jim daný typ systému nainstaluje, popřípadě již dostaly kontakt od známého na tohoto technika. Jako poslední důvod uváděli ho pouze muži (6% dotázaných) uvedli, že při výběru zařízení se rozhodly podle recenzí, tyto recenze hledali daní uživatele převážně na internetu, popřípadě uvádějí, že se snažily nalézt informace v technických magazínech.

F7. při pořizování rozhodovala?	Celkem	muž	žena
cena	30%	23%	37%
kvalita	15%	15%	11%
doporučení	12%	15%	11%
recenze	6%	15%	0%
nechal jsem to na technikovi (nezajímal jsem se)	36%	31%	42%
počet dotázaných	**33**	**13**	**19**

Tab. 5.5 Důvod pro rozhodnutí o výrobci

Uživatele dále několikrát zmiňují, že je velice složité se dostat k bližším informacím o zabezpečovacích systémech a stránky prodejců v české republice jsou velice skoupé a málo obsáhlé parametry jsou neúplné a nic neříkající. Uživatele kolikrát u daného detektoru nezjistily ani výrobce. Dalším velice nepříjemným aspektem, který v souvislosti s touto otázkou uživatelé psali, bylo, že získání ceny jednotlivých výrobku, aby si mohly udělat představu, kolik je bude jejich zabezpečovací systém od různých výrobců stát, byl nadlidský výkon. Je až s podivem proč čeští prodejci tak úzkostlivě tají ceny těchto detektorů, když v zahraničí jsou tyto ceny volně k dispozici.

Pokud tedy shrneme důvody k výběru zabezpečovacího systému, je příjemné vidět, že většina uživatelů se zajímá spíše o kvalitu nežli cenu ovšem 30% není nikterak zanedbatelné číslo a odráží tak tlak na co nejnižší ceny bez ohledu na skutečnou funkčnost systému.

5.3 Náklady na pořízení

Ač jsme se v předchozích částech přímo nebo i nepřímo dotýkali vztahu uživatele a jeho systému v závislosti na ceně v této kapitole si to rozborem více do hloubky s přihlédnutím k doplňujícím textům, které uživatele doplnily k této otázce. Pokud zhodnotíme náklady na pořízení, pak můžeme říci, že ti uživatelé, kteří se rozhodli pro instalaci zabezpečovacího zařízení vlastní silou, pak volili společnost Jablotron a částka kterou, vynaložili na zabezpečovací systém, nepřesáhla ve většině případů pořizovací cenu 15 000 Kč. Tyto levné systémy si uživatele pořizují zejména z důvodu ochrany, ovšem již dále neřeší možnost špatného zapojení a chybovosti, která vzniká z neodborného zapojení. Na druhou stranu je třeba říci, že složitá finanční situace nutí mnohé lidi přející si v neklidné době zlepšit svoje bezpečí volit právě tyto levné kompaktní systémy. Skupina těchto levných systému je zastoupena 21% (tab. 5.7) v našem celku a představuje tak jednu pětinu všech zabezpečovacích systémů. Je však potřeba říci, že do této skupiny patří i uživatelé, kteří si pořizovali detektor určený k ochraně proti ohni a při té příležitosti si svou domácnost nechaly vybavit i několika pohybovými detektory.

Výše zmíněná skupina levných detektorů není nejvíce zastoupena. V měřeném segmentu se jako nejvíce rozšířený systém pohybuje v rozmezí částky od 25 000 Kč do 40 000 Kč a to v 36 % (tab. 5.7) případů diference je zde i v poměru mužů a žen, kdy ženy

zde dominují v poměru 42%, proti, 31% mužů. Dá se tedy říci, že ženy upřednostňují více středně drahá zabezpečovací systémy a vyhýbají se extrémům. Částka 40 000 Kč je částka plně dostačující pro zhotovení sofistikovaného uceleného systému zabezpečující rodinný dům, který bude mít jak plášťovou ochranu, tak i pohybovou složku včetně zabezpečení proti ohni. V tomto finančním rozmezí si dokonce již můžeme volit jakou značku detektorů a ústředny si zvolíme. Do této částky dokáže technik specialista, navrhnou optimální zabezpečovací zařízení pro průměrný dům, a proto je tento finanční limit nejčastěji zmiňován.

Druhou nejčastější kategorií, je kategorie do 25 000 Kč (24% tab. 5.7). S průzkumu vzešlo, že tato kategorie je hojně zastoupena lidmi, kteří si zabezpečovací systém nechávají instalovat do bytů. V poslední době stále více lidí v bytech volí zabezpečovací systém do bytu a to zejména v přízemí, kde nechtějí mít výhled z okna zablokovaný mříží. Uživatele se domnívají, že elektronické zabezpečovací zařízení bude sloužit jako náhrada za pasivní ochranu tedy mříž. To je však velký omyl a EZS nemůže nikdy suplovat pasivní ochranu. V konkrétním případě bytů by uživatelé neměli podceňovat pasivní ochranu a k EZS do oken použít alespoň ochranné fólie.

Poslední kategorií, která je nejméně zastoupena ovšem vyjádřilo se k ní kladně 18% uživatelů je kategorie nad 40 000Kč zde se již jedná o více méně systémy pro velké rodinné domy uceleného systému. Kde jsou zahrnuty všechny složky EZS. U těchto systému se nedá hledat domácí instalace. Systémy si volili hlavně uživatelé, kteří systém volili kvůli pojišťovně, anebo se naopak bály o své bezpečí.

F10. Instalovaný EZS vás stál	Celkem	muž	žena
do 15 000 Kč	21%	23%	21%
do 25 000 Kč	24%	23%	26%
do 40 000 Kč	36%	31%	42%
více jak 40 000 Kč	18%	23%	11%
počet návštěv	**33**	**13**	**19**

Tab. 5.7 Pořizovací náklady na EZS

Celkově lze říci, že více jak polovina uživatelů volila elektronické zabezpečovací zařízení v dražším provedení. To odráží lidskou zkušenost, že nejsou natolik bohatí, aby si kupovali levné věci. Levná domácí zabezpečovací zařízení mnohdy postrádají svůj smysl,

nemají vhodně zvolenou koncepci. Jednotlivé části se navzájem nedoplňují. Při hledání vhodného zabezpečovacího systému musíme brát zřetel na finanční omezení zadavatele, ale je potřeba si uvědomit, že EZS si nepořizujeme na rok, ale je to dlouhodobá investice do našeho bezpečí, a proto bychom si měli uvědomit, co od svého systému chceme a poté teprve stanovit částku, kterou do něj investujeme.

5.4 EZS a uživatel

Jedna věc je sice si elektronický zabezpečovací systém domu pořídit a druhá je ho skutečně využívat. Mnohdy se stane, že zabezpečovací systém je tak složitý a nepříjemný na obsluhu anebo je špatně nastaven tak, že způsobuje neustále plané signály, že uživatele raději i přes značnou investici do něj systém nepoužívají anebo ho používají zřídka.

Je celkem zarážející, že téměř 18% (Tab. 5.8) uživatelů je se svým zabezpečovacím systémem nespokojeno nejčastěji to bývají uživatelé s levným zabezpečovacím systémem. Rozdíl v spokojenosti mezi muži a ženami je zanedbatelný. Uživatelé si nejčastěji stěžují na problém s častými planými poplachy popřípadě, že si koupili zvíře a nemohou ho volně nechat běhat po domě. Takovéto problémy jsou pochopitelné a potýkají se s problémem vhodné optimalizace systému pro danou rodinu. Ta je způsobena samo doma instalací, anebo také špatnou koncepcí, kdy uživatelé nepředpokládali, že budou mít v budoucnu psa a při plánování tak technik s touto eventualitou nepočítal. To odráží i to, že 24% (Tab. 5.8) dotázaných se vyjádřilo, že svůj zabezpečovací systém nepoužívají, pravidelně několik se dokonce vyjádřilo tak, že ho mají doma v nefunkčním stavu a plánují výhledově jeho opětovné znovu zprovoznění. Náš vzorek obyvatel je sice reprezentativní a nemůže nikdy plně suplovat všechny uživatele, ale i jako z reprezentativního vzorku dostáváme poměrně alarmující čísla, kde jedna čtvrtina uživatelů rezignuje na pravidelné použití domácího EZS. Uživatele sice uvádějí různé důvody, proč ho nepoužívají, ale svědčí to o tom, že si lidé plně neuvědomují, co znamená si domu pořídit takovýto systém a neumějí se s ním mnohdy vžít.

otázky ANO/NE	Celkem	muž	žena
F8. Jsem spokojen s EZS?	82%	77%	84%
F9. Instalovaný EZS pravidelně využívám (minimálně 3 týdně)	76%	85%	68%
počet dotázaných	33	13	19

Tab. 5.8 Spokojenost s EZS

5.5 Zhodnocení

Z průzkumu mezi uživateli zabezpečovací techniky vzešlo, že uživatelé upřednostňují kvalitu před cenou a při výběru svého systému dávají na rady technika. Ovšem nemalé procento lidí stále volí podomácku instalované zabezpečovací systémy. Lidé se domnívají, že pokud svěří instalaci profesionálům, dostanou za svoje peníze spolehlivý systém, který bude fungovat naprosto spolehlivě. Nechápou také, proč se s cenovou politikou u zabezpečovacích systémů nadělá takového tajemství. Uživatelé při instalaci nicméně kontrolují průtok svých peněz a nechtějí investovat více než je nutné. Mezi zabezpečovacími systémy je nejvíce rozšířen zabezpečovací systém od společnosti Risco a to pro svoji kvalitu a Jablotron zejména pro výhodnou cenu a největší zastoupení. Zajímavosti je, že pouhá polovina obyvatel si zabezpečovací systém pořizuje kvůli bezpečnosti a že přibývá těch, co chtějí ušetřit na pojistném. Celkově lze na závěr říci, že uživatele jsou vesměs spokojeni a svoje zabezpečovací systémy používají pravidelně.

6 Definování problémů a doporučení k jejich odstranění v testovaných systémech EZS zejména v bezdrátové koncepci.

Pokud chceme minimalizovat plané poplachy, ať už přímo v bezdrátových systémech nebo obecně ve všech elektronických zabezpečovacích systémech je potřeba se řídit určitými zásadami při jejich používání. Z výše zjištěných údajů zde budu definovat zásady a postupy jak minimalizovat plané poplachy a přispět k lepšímu vztahu uživatele k EZS.

V této kapitole se budeme zabírat vhodnými opatřeními, které vzešly z měření a testování jednotlivých kontaktů. Je třeba se zamyslet na zabezpečovací systém v širším

spektru, neboť takové zdánlivě nesouvisející věci pomáhají potencionálním kriminálníčkům uskutečnit svůj cíl a naši chráněnou budovu vykrást.

Všeobecně se dá říci, že zabezpečovací systém je tak dobrý jak se o něj stará jeho obsluha. U zabezpečovacího systému pro firmy je tento aspekt potlačen tím, že se o něj starají profesionální zaměstnanci. U domácnosti tento fakt vychází spíše do popředí. Většina uživatelů si při pořizování takovéhoto systému není vědoma toho, že budou nuceni do jité míry své chování uzpůsobit a před samotnou instalací nemají ani představu co a jak chtějí chránit. Obvyklá představa je taková, že chtějí něco výkonného, aby byli v bezpečí za co nejméně peněz a pokud možno, bez velkých zásahů do struktury domu.

6.1 Člověk

Člověk je tvor komunikativní a družný, sám se rád chlubí a ukazuje co má, kde byl, jak slavil oslavu s rodiči, co postavil. Ovšem z hlediska zabezpečovacího systému je to velice nepříjemná skutečnost. Jak již bylo v kapitole 4 napsáno mnoho lidí má na internetu u svých profilů fotografie ukazující svůj domácí zabezpečovací systém a udává mnoho informací o sobě, kdy nebude doma, kam jde a podobně. Asi neexistuje jednoduší poučky jak tomu zamezit, než říci „Nic nikam nedávat a nic nesdělovat“ bohužel to lidé nechtějí, nebo nemohou. Proto zde definuji pár postojů jak být na internetu opatrný, tak abychom neposkytli nějaké informace, které pachatelům poslouží jako pomocník k narušení našeho domu.

1. Pokud umístíme na internet fotografii, přesvědčíme se, zda na ní není zachycena součást našeho zabezpečovacího systému. V ideálním případě vkládáme fotografie, ze kterých není patrno rozložení místností popřípadě chodeb a vstupních oblastí.
2. Informace o tom, kdy a kde se budeme nacházet, sdělujeme v obecné rovině, například v létě pojedu do Itálie k moři. Z výzkumů společnosti *The Survey Shop and Opinium Research* [20] vyplynulo, že 68% bytařů si shání informace o potencionálním cíly svého vykradení a 12% uvedlo, že hlavním zdrojem informací jsou pro ně Facebook a obdobné sociální sítě.

3. Pokud již informaci někde sdělíme tak ji zděšujeme pouze lidem, ke kterým máme důvěru a sdělujeme jim je tak, aby ji nemohla získat třetí strana.
4. Nikdy nikomu nesdělujme svůj přístupový kód do zabezpečovacího systému, pokud je to nezbytné, sdělujeme ho pouze ústně a tak, aby to slyšela pouze určená osoba. Pokud tento kód sdělujeme jen na omezené období, například dovolená, po návratu z dovolené kód neprodleně změníme.
5. Přihlašovací kód bychom měli měnit alespoň jednou za čtvrt roku, nejlépe však každý měsíc.
6. Nikomu nesdělujeme parametry svého zabezpečovacího systému, ani typ a umístění jednotlivých čidel.
7. Pokud zjistíme závadu na svém zabezpečovacím systému, obrátíme se na svého technika, ke kterému máme důvěru. K systému nepouštíme nikoho cizího.
8. Heslo k zabezpečovacímu systému nikam nezapisujeme. Pokud již si ho někam zapíšeme, píšeme ho tak, aby nebylo poznat, o co se jedná a v žádném případě ho neukládáme do peněženky, kde máme adresu našeho bydlení.
9. Heslo by nemělo být: naše datum, nebo rok narození. Popřípadě nějaký snadno zjistitelný údaj. Nejlépe volíme jako kombinaci různých čísel.
10. Vlastním působením se snažme předcházet situacím, kdy vzniká falešný poplach.

6.2 Magnetický kontakt

Magnetický kontakt je ve své podstatě velice jednoduchým zařízením ovšem při správném používaní je i velice mocným nástrojem. Požadavek na opatření všech potenciálních vstupních míst takovouto základní ochranou je naprosto oprávněný. Ovšem vznikají zde třecí plochy mezi uživatelem a systémem. Z mého pozorování vzešel právě fakt, že nečastěji vznikají plané poplachy na magnetických kontaktech a to zejména kolem 9 hodiny večerní v létě. Jak bylo popsáno v kapitole 4. To vychází ze skutečnosti, že je v létě teplé a dusné počasí a uživatelé chtějí samozřejmě před spaním vyvětrat místnost. Uživatel pak nejčastěji zapomene, že může otevřít okno pouze na vyklápěčku a planý

poplach je na světě, ovšem častější problém je v tom, že jeden uživatel provede aktivaci systému a nepodá o této aktivaci informaci ostatním. Ty bez znalosti této informace okno otevřou.

Tato situace je v celku neuspokojivá a proto je třeba hledat řešení. V celku se zde nabízí dvě podobné varianty jak snížit procento planých poplachů.

1. Systém bude mít nastavenu pevnou hodinu aktivace, po které se samočinně uvede do stavu ochrany. Všichni uživatelé s tímto nastavením musí být seznámeni. Domnívám se, že informace o jednom čase, po kterém již nebude možnost otevření oken, bude snadno zapamatovatelná a uživatel s tím nebude mít problém. Popřípadě, že uživatel nebude chtít aktivaci systému přenést ze svých beder na systém, je potřeba aby se všichni uživatelé dohodly na čase, od kterého časového období se bude systém chodit zapínat. Po tomto časovém rozmezí by bylo jasné, že je systém aktivován.

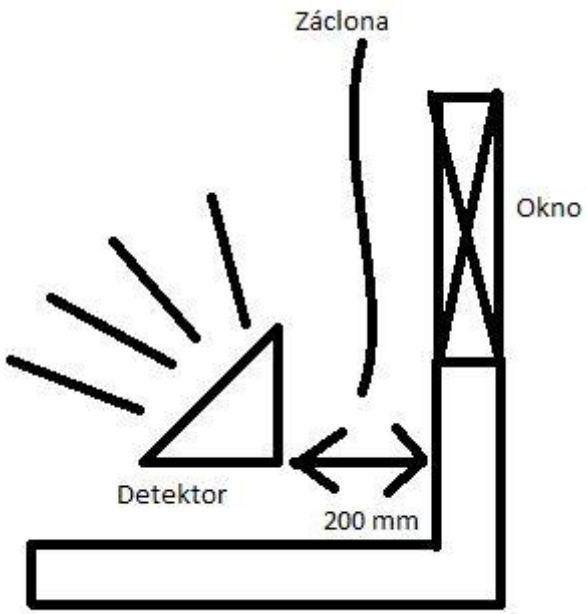
   V tomto řešení předpokládáme, že uživatele se budou chtít domluvit a přizpůsobí své chování systému.

2. Druhým řešením je dokoupení druhé bezdrátové klávesnice a vybavit jím kromě přízemí i druhé patro. Každý uživatel by pak měl možnost nahlédnout na klávesnici a získat tak informaci o tom zda byl systém již aktivován. Tato varianta je dražší a méně účinná jelikož i za předpokladu, že uživatel bude mít klávesnice nablízku tak ho nic nenutí k jejímu použití.

6.3 Detektor pohybu

Při instalaci detektoru pohybu na bázi pyroelementu je nutné dávat velký pozor na vhodné umístění při instalaci. Pokud je vhodně nainstalován jako v testovaném případě tak na něm nevznikají téměř žádné plané poplachy. Pokud ovšem zásady s jeho instalací nedodržíme, jak jsem demonstroval v testovací části, mohou se na něm objevit četné ruchy a detektor pak působí plané poplachy. Detektory pohybu mohou v kombinaci s letním počasím a domácími mazlíčky detekovat množství chyb a proto bychom si při jeho instalaci měli dát pozor na následující problémy, které jsem formuloval na základě zkušeností a pozorování.

1. PIR detektor neinstalujeme tak aby jeho detekční plocha zasahovala do oken, zejména pokud jsou okna směřována na jižní stranu a dochází tak k přímému ohřevu a proudění vzduchu v místnosti. Pokud již máme PIR detektor směřovaný do oken nemněla by být v jeho zorném poli žádná věc (záclony, květiny atd.) jež by mohli být poryvem větru rozpohybována. Detektor by měl mířit nejlépe od oken směrem do střežené místnosti nebo plochy.
2. Je-li detektor instalován k oknu směrem do chráněného prostoru tak ho od zdi odsazujeme alespoň 20 cm, jak je naznačeno na obrázku 6.1, tak aby jeho střežená plocha nezabírala případné záclony.



Obr. 6.1 Vzdálenost PIR od zdi

3. Střežená plocha by měla být ohraničena pevnými plochami a nikoliv takovými druhy materiálů, u kterých hrozí, že detektor bude přes ně nahlížet do vedlejší místnost.
4. Střežená plocha detektorů by se měla částečně překrývat tak aby se detektory navzájem hlídaly.

5. Do blízkosti jednoho metru střežené plochy by neměli být umístěny žádné klimatizační zařízení nebo výpuste u kterých hrozí prudké změny teplot.
6. Žije-li s námi v domácnosti domácí mazlíček je třeba detektory v místnostech výskytu takovéhoto domácího mazlíčka vybavit maskou s ochranou PET. Je-li předpoklad, že domácí zvíře se bude nekontrolovatelně pohybovat po celé střežené ploše, volíme tuto ochranu raději na všech pohybových detektorech.
7. Detektor instalujeme tak, aby byl co nejhůře dosažitelný mimo střeženou oblast, tedy v obě aktivace byl dostupný pouze tak aby se narušitel k němu dostal pouze přes střeženou oblast.
8. Detektor instalujeme tak, aby se k němu například po skříni nemohl dostat domácí mazlíček, mějme na paměti, že čím blíže je domácí mazlíček blíže k senzoru tím se i pro senzor jeví jeho silueta větší a ochrana PET tak ztrácí na své účinnosti.

6.4 Detektor kouře

Ať už si domů chceme pořídit EZS nebo tak by měla mít každá domácnost instalovaný systém pro včasnou protipožární výstrahu. Výhodou těchto detektorů je, že nemusí být napojený na ústřednu a pracují samostatně a mohou nám zachránit život. Ovšem při instalaci je vhodné si dobře rozmyslet, kam ho dáme a řídit se několika poučeními, jež jsem během pozorování zformuloval.

1. Detektor neumísťujeme přímo nad varnou desku nebo nad výpust páry z vaření.
2. Pokud je, detektor umístěn do prašného prostředí provádíme pravidelně kontrolu a zbavujeme ho prachu.
3. Protipožární čidlo umísťujeme nejlépe do středu střeženého prostoru. Nejlépe spojovací chodba, schodiště a podobně.
4. Pokud máme rodinný domek, volíme pro každé patro vždy jeden protipožární člen. Takováto kombinace dvou detektorů je lepší že se nám nemůže stát, že nám případný požár odřízne východové dveře v přízemí.

5. Pokud máme kotelnu, a topíme v ní na pevná paliva, v žádném případě detektor neumísťujeme přímo do kotelny. Volíme vždy sousední místnost, nejlépe přístupovou chodbu v zadním rohu, neboť i pouhé otevření šachty na palivo by mohlo v takovém případě aktivovat protipožární senzor.
6. Pokud byl protipožární senzor aktivován, v žádném případě takovou situaci nepodceňujeme a byt popřípadě dům řádně prohledáme, abychom se ujistili, že nikde nedošlo k zahoření.
7. Po poplachu, tedy před dalším uvedením do pohotovosti profoukneme fotoelektrickou komůrku, abychom případný zůstatek po dýmu z prostoru odstranili.

6.5 Ústředna

Ústředna je srdcem a mozkem každého zabezpečovacího zařízení. Pokud narušitel vyřadí z provozu nějaký detektor, je to špatné, ale pokud se mu podaří vyřadit ústřednu, je celá situace z hlediska ochrany ztracená. Senzor sám o sobě nedokáže předat uživateli informaci o svém napadení, to umí pouze ústředna, a proto je nutné jí co nejlépe chránit a udržovat ji.

1. Ústřednu instalujeme do oblasti nejhůře dosažitelnou běžným pohybem, jako jsou půdy, místnosti bez oken uvnitř budovy. Místnost by se měla dát uzavřít mechanickou zábranou a neměla by být snadno dostupná.
2. Ústřednu musíme vždy zapojovat do nezávislého proudového chrániče.
3. Pokud komunikujeme s ústřednou přes simkartu volíme raději paušál. Pokud máme, ale již dobíjecí kartu, pravidelně provádíme kontrolu stavu kreditu.
4. Veškeré informace, o kterých nás ústředna informuje, bereme vždy vážně a neprodleně se je snažíme odstranit.
5. Před volbou telefonního operátora pro komunikaci s ústřednou zjistíme, zda má operátor v místě uložení ústředny dostatečný signál.
6. Pro komunikaci s ústřednou volíme raději dva kanály, které nelze najednou vyřadit z činnosti.

7. Důkladně se seznámí s možnými zprávami, které nám ústředna může poskytovat, tak abychom byli schopni adekvátně zareagovat.
8. Přístup k ústředně by měl chránit detektor pohybu tak aby případný narušitel musel touto zónou vždy projit na cestě k ústředně.

6.6 Všeobecná opatření

Tato opatření se dají aplikovat na všechny součásti zabezpečovacího zařízení a slouží a měla by napomoci k hladkému chodu zabezpečovacího zařízení jako celku poskytnout několik postupů jak se vyvarovat planým poplachům tak aby zabezpečovací systém sloužil co nejlépe.

1. Instalaci zabezpečovacího zařízení necháváme na specializovaném technikovi vlastnícím certifikát umožňující mu provádět instalaci zabezpečovacích zařízení.
2. Po instalaci vyžadujme certifikát o zařazení do bezpečnostní třídy. S takovýmto certifikátem požadujme na pojišťovně slevu z pojištění. Náklady na pořízení certifikovaného systému se nám posléze snadno vrátí nepřímo na úspoře za pojistku.
3. Nezapomínejme na preventivní návštěvy technika, alespoň jednou za dva roky. Nejlépe však jednou ročně.
4. Do zabezpečovacího systému výrazně sami nezasahujme a změny nechme na specializovaném technikovi. Pokud s ním budeme sami manipulovat, můžeme celý systém úplně rozhodit a jeho správná funkce bude narušena.
5. Detektory sami nerozebírejme ani při výměně baterie. Přenecháme to raději na specialistovi. Při vlastní výměně hrozí poškození citlivého tamper kontaktu a posléze i nemožnosti aktivovat celý systém.
6. K zabezpečovacímu systému nedovolujeme přístup nikomu, koho neznáme.
7. Pokud nejsme zapojeni na PCO tak je lépe se domluvit s někým, kdo bydlí blízko a je neustále doma, aby v případě poplachu přišel skontrovat váš chráněný objekt.

8. Informace o napadení předáváme více uživatelům, abychom zajistili, že informace o napadení bude včas zjištěna.
9. Systém detektorů mějme rozdělen do více logických zón tak, aby bylo možné systém zapínat podle aktuálního požadavku. Minimálně mějme zóny plášťová ochrana a pohybová ochrana.
10. Po zapojení vyžadujme od technika důkladné proškolení v ovládání systému a funkci jednotlivých zón pro všechny uživatele systému. Čím lepší informovanost o funkci tím méně planých poplachů.

7 Závěr

Z výše uvedeného výzkumu a sledování konkrétního zabezpečovacího zařízení trvající rok a půl jsem zjistil mnoho informací o chování uživatele při práci se zabezpečovacím systémem.

Cílem práce bylo přinést informaci o vztahu uživatele a zabezpečovacího zařízení, zjistit motivaci pro jeho pořízení a vlastnosti takových běžných domácích systémů. Dále pak definovat nejčastější problémy, které při jeho užívání vznikají na nejběžnějších v domácnosti vyskytovaných typech, zejména pak bezdrátových systémech, a navrhnout opatření k zamezení planých poplachů v domácnosti.

V první části mé práce jsem rozebral teoreticky nejběžnější prvky domácích zabezpečovacích systému a následně jsem je prakticky otestoval situace, jež mohou v domácnosti nastat, a vytvořit tak planý poplach. Definoval jsem zde možnosti, jak se s těmito situacemi vyrovnat. Z měření vyplynulo, že zabezpečovací systém je zejména náchylný na špatné umístění a vhodná poloha je důležitá pro správnou práci. Zejména jsou na to citlivé protipožární a pohybové detektory. Magnetické kontakty jsou naopak z dlouhodobého měření nejčastějším zdrojem planých poplachů a to zejména pro svůj nejčastější výskyt a princip své funkce. Plané poplachy na detektorech vinou selhání detektoru vznikají minimálně. Hlavním důvodem planých poplachů je v 90% uživatel, který nerespektuje funkci svého zabezpečovacího systému nebo je naopak neproškolen. Ve zbylých 10% je na vině špatně zvolené umístění detektoru. Zajímavostí je, že plané poplachy vznikají častěji v letních měsících, a to závadou vyšší teploty a obvykle větší manipulací se střeženými objekty jako jsou okna.

V druhé části pozorování jsem rozebral příčiny a důvody pořízení EZS uživatelem. Z měřeného vzorku vzešlo, že každá desátá domácnost má doma zabezpečovací zařízení a více jak polovina z nich má zařízení ve vyšší cenové kategorii. Negativním zjištěním bylo, že 26% dotázaných si zabezpečovací systém doma montovalo svépomocí bez asistence specializovaného technika. Motivace lidí k pořízení je naopak velice rozdílná, dva nejčastěji zmiňované důvody jsou bezpečnost a sleva na pojištění. Uživatelé tedy sice upřednostňují bezpečí, ale jsou si vědomi toho, že se jim pořízení vrátí v rámci slevy na pojištění domu. Uživatelé často uváděli, že při nákupu zabezpečovacího zařízení shledávali problém zjistit více informací o jednotlivých typech a jejich cenách. Pokud chtěli získat informace o ceně, museli se obrátit na zahraniční stránky. Smutné je, že 24% dotázaných sdělilo, že zabezpečovací systém používají méně než 3krát do týdne. To znamená, že zabezpečovací systém plně nevyužívají a stává se v domácnosti pouhou zbytečností. Průzkum také potvrdil snižující se zájem o PCO, kde připojení na něj potvrdilo méně jak polovina dotázaných.

Na závěr své práce bych chtěl vzhledem k výše popsaným skutečnostem apelovat na potencionální majitele zabezpečovacích zařízení, aby si pečlivě zvážili umístění jednotlivých detektorů, prošli si s technikem jednotlivé detektory a jejich vlastnosti a podle doporučení technika volili jejich skladbu. Technik ve většině případů má již za sebou mnoho instalací a je si vědom omezení a předností jednotlivých detektorů. Vyšší pořizovací cena u lepších a dražších systému je pak kompenzována větší slevou na pojištění a hlavně méně planými poplachy a omezeními. Je třeba ale také říci, že kvalitní systém a dobrá instalace sama o sobě nikdy nemůže zabránit planým poplachům, může je pouze snížit. Pro eliminaci planých poplachů je nutné, aby uživatel byl důkladně proškolen a respektoval některá omezení, jež mu vznikají při jeho používání.

Seznam obrázků a tabulek

Zdroje

[1] JANOVSKÝ, MARTIN: Bakalářská práce Analýza možnosti sabotáže elektronických zabezpečovacích systémů (EZS), Praha 2010, ČZU

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

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

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

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

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

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

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

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

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

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

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

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

WWW stránky

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

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

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

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

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

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

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

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

[18] JABLOTRON, Současný stav norem na poplachové systémy v ČR [cit. 2012-11-2].

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

[19] Normy.biz cit norma EN 50 131 [cit. 2010-12-2].
Dostupný z URL:

<http://nahledy.normy.biz/nahled.php?i=78248>

[20] Bydlet v panelu, Unikátní průzkum mezi zloději: Jak tipují byty pro vloupání? [cit. 2012-11-2].

Dostupný z URL:

<http://bydletvpanelu.cz/interier/unikatni-pruzkum-mezi-zlodeji-jak-tipuji-byty-pro-vloupani.html>

[21] TZBinfo, Autonomní hlásiče kouře [cit. 2012-11-3].

Dostupný z URL:

<http://www.tzb-info.cz/5011-autonomni-hlasice-koure>

[20] iDNES, Pozor na rušičky mobilu [cit. 2012-15-3].

Dostupný z URL:

<http://mobil.idnes.cz/pozor-na-rusicky-mobilu-oblibenou-zbran-zlodeju-fu8-/mob_tech.aspx?c=A070220_002633_mob_tech_jm>

[21] Elektrika.cz, Detektory PIR - umíte je správně instalovat 1 díl [cit. 2012-15-3].

Dostupný z URL:

<http://elektrika.cz/data/clanky/pujsi1>

Slovníček pojmů

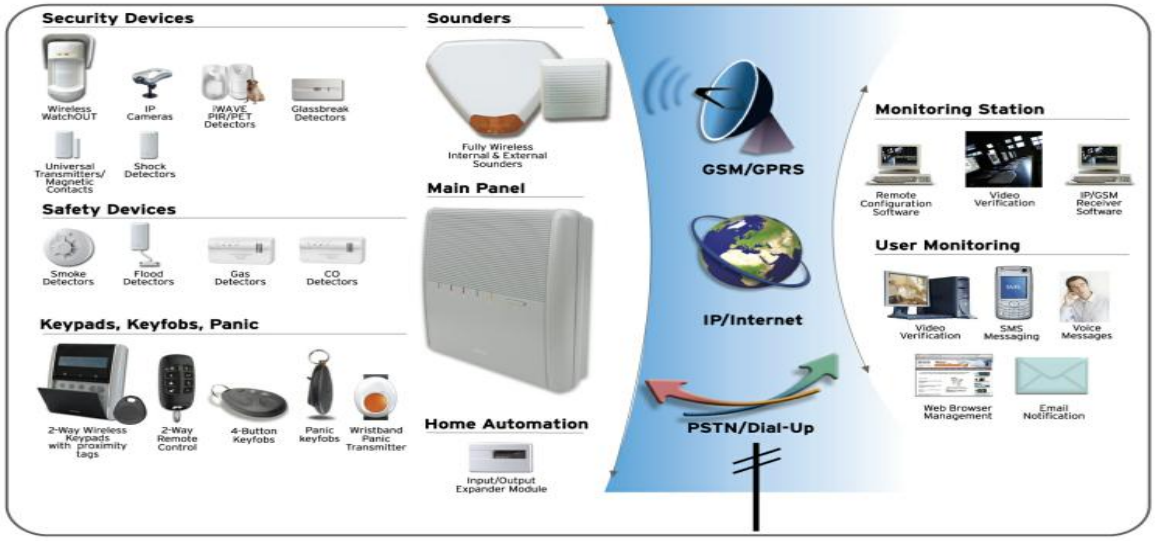
- **Úroveň autorizace:** Každý bezpečnostní kód je v ústředně spojen s úrovní autorizace což znamená možnost zasahování a provádění změn na bezpečnostním systému a přístupu do něj v praxi to znamená, čím vyšší oprávnění tím větší možnosti daného systému jsou uživateli otevřeny.
- **Chime:** Jedná se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

- **Proximity:** Jedná se o technologii, která bez použití klávesnice deaktivuje a aktivuje systém, je přiřazena k danému uživatelskému heslu. Jedná se buď o kartu, nebo klíčenku s dálkovým ovládáním.
- **Tamper:** Antisabotážní funkce bezpečnostního systému.
- **Chybové Hlášení:** Ústředna signalizuje veškeré poruchy na všech svých členech docházející baterie, otevřený kryt porušená kabeláž signalizuje jí na klávesnici a případně zasílá na PCO.
- **Upload/Download:** Program umožňující programování a správu systému z PC. Může být připojen kabele nebo pomocí telefonní linky.
- **Uživatelský kód:** Většinou 4 místné, někdy 6-ti místné, číslo, které uživateli zpřístupní ovládání bezpečnostního systému z klávesnice. Každý uživatel by měl mít přidělen individuální kód.
- **Programovatelný výstup:** Ústředna může být dovybavena množstvím programovatelných výstupů sloužících k připojení zařízení, nebezpečnostního charakteru jako je například poplachová siréna, spínání světel, ovládání topení, otevírání garážových vrat. Výstupy mohou být ovládány automaticky přes plánovač, nebo manuálně z klávesnice.
- **Plánovač:** Bezpečnostní systém je vybaven reálnými hodinami ty umožňují dopředu plánovat určité funkce jako rozsvěcování světel, deaktivace určených zón a podobně
- **Zóna:** Jeden nebo více detektorů, které jsou propojeny s jedním vstupem systému. Zóna je základním prvkem bezpečnostního systému. Pokud je na jedné zóně zapojeno více detektorů (zařízení), bezpečnostní systém je již nedokáže rozlišovat.Má-li zóna např. 5 detektorů, tak v případě poplachu nelze rozlišit, který z těchto detektorů poplach signalizoval.
- **náhradní napájecí zdroj:***(alternative power source (APS)*)**:** napájecí zdroj energie, který je schopen napájet EZS po předem určenou dobu v případě výpadku základního napájecího zdroje.

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

- **výkonový výstup:** *(power output)***:** výstup napájecího zdroje, který dodává energii EZS
- **napájecí jednotka:** *(power unit (PU))***:** zařízení, které poskytuje a také mění nebo odděluje (elektrickou) energii pro EZS nebo jeho komponenty a v případě potřeby také pro záložní zdroj
- **napájecí zdroj:** *(power supply (PS))*: zařízení, které shromažďuje, poskytuje a také mění nebo odděluje (elektrickou) energii pro EZS nebo jeho komponenty; napájecí zdroj se skládá ze dvou základních částí: napájecí jednotky a záložního zdroje (např. akumulátoru).

Přílohy:



[12]

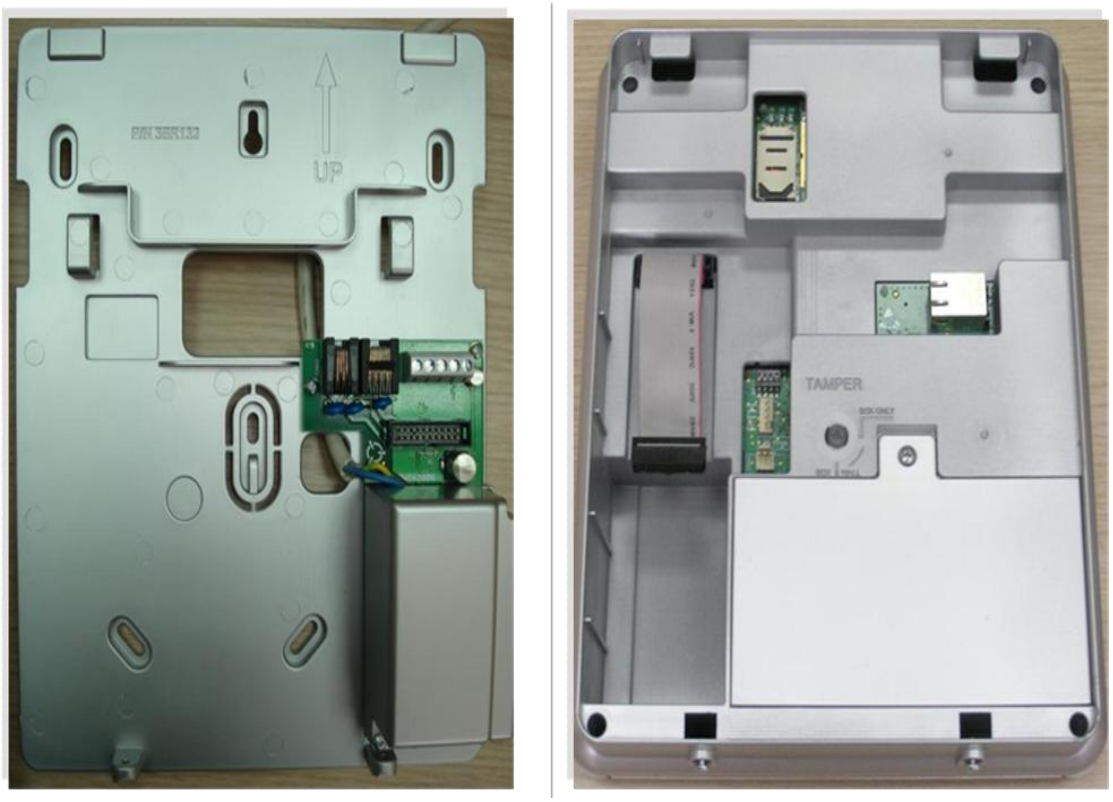
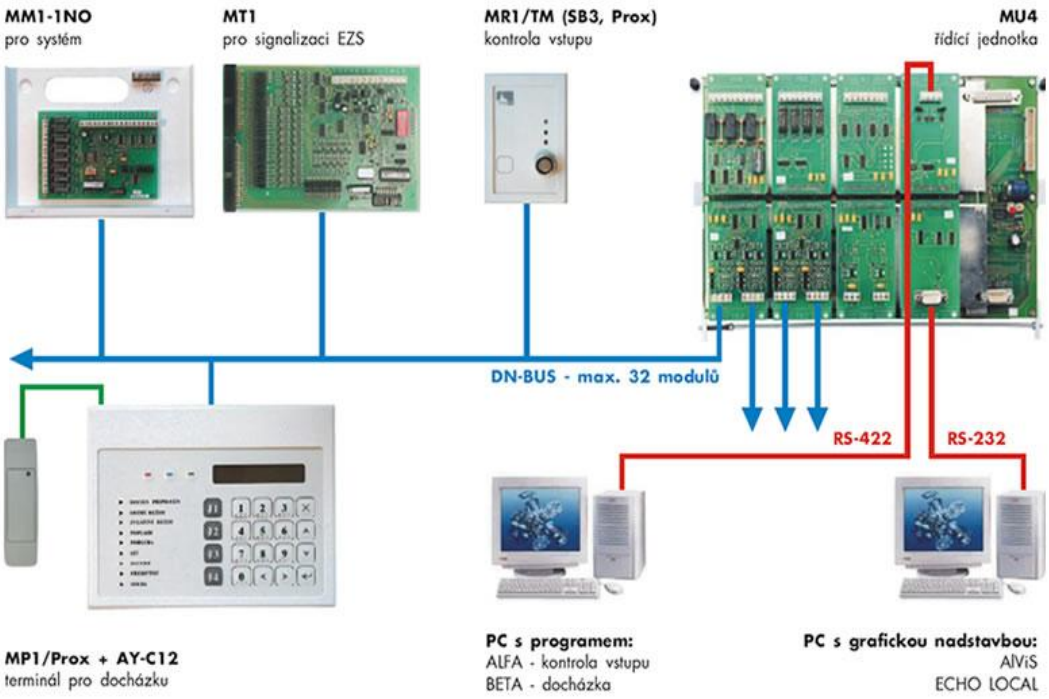


Foto autor



[12]

Foto Autor – test rušení přenosu vysílače magnetického kontaktu hliníkovou fólií

Foto Autor – připojení ústředny přes RS232 a USB převodníku k notebooku

Foto Autor – materiál použitý po test kouřivosti

INFORMACE O EXPORTU

Datum exportu:	11.3.2012
Čas exportu:	12:33
Uživatel:	Martin Janovský
Projekt:	INFORMACE_TEST

HODNOCENÍ FORMULÁŘE

	Body	Maximum	Hodnocení
Celkem			0

INFORMACE

Otázky

F1. Pohlaví	muž žena
F2. Využíváte zabezpečovací systém v domácnosti	ano ne
F3. Od jaké společnosti?	
	jablotron fisco Crow Bosch Honeywell Alarm absolón Genesis jiné
F4. Instalaci provedena?	technik sám doma
F5. EZS jsem si pořídil z důvodu?	
	Bezpečí Slevy na pojištění musel jsem (kvůli pojišťovně atd.) po krádeži jiné
F6. Jsem připojen na pult centralizované ochrany	ano ne
F7. při pořizování rozhodovala?	
	cena kvalita doporučení recenze nechal jsem to na technikovi (nezajímal jsem se)
F8. Jsem spokojen s EZS?	ano ne
F9. Instalovaný EZS pravidelně využívám (minimálně 3 týdně)	ano ne
F10. Instalovaný EZS vás stál	
	do 15 000 Kč do 25 000 kč do 40 000 Kč více jak 40 000 Kč

Ostatní připomínky

Export formuláře část 1.

Export formuláře část 2.