VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

FUNKČNOST A SPOLEHLIVOST POPLACHOVÝCH ZABEZPEČOVACÍCH A TÍSŇOVÝCH SYSTÉMŮ NAPOJENÝCH NA PULT CENTRALIZOVANÉ OCHRANY

Autor práce: Zdeněk Rídl

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2026

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Zdeněk Rídl

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Funkčnost a spolehlivost poplachových zabezpečovacích a tísňových systémů napojených na pult centralizované ochrany

Název bakalářské práce v anglickém jazyce: Functionality and Reliability of Intruder and Hold-Up Alarm Systems Connected to the Alarm Receiving Centre

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce: březen 2025

Cíl bakalářské práce:
Hlavním cílem je vyhodnotit poruchové incidenty jednotlivých součástí poplachových zabezpečovacích a tísňových systémů a posoudit jejich vliv na spolehlivost a funkčnost těchto systémů ve vztahu k prevenci a zabránění protiprávního jednání.
Vedlejším cílem je prostřednictvím respondentů z řad techniků poplachových zabezpečovacích a tísňových systémů posoudit efektivitu jednotlivých prvků ochrany při prevenci kriminality.

Student: Zdeněk Rídl	22.03.2025 *datum*	*podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	22.3.2025 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	7.4.2025 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	7.4.2025 *datum*	*podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	17.4.2025 *datum*	*podpis*

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z.ú. -2- ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí bakalářské práce RNDr. Růženě Ferebauerové za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

RÍDL, Z. *Funkčnost a spolehlivost poplachových zabezpečovacích a tísňových systémů napojených na pult centralizované ochrany: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2026. 83 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová.

Klíčová slova: pachatel, poplach, prevence kriminality, protiprávní jednání, spolehlivost, zabezpečení

Tato bakalářská práce představuje ve své teoretické části poplachové zabezpečovací a tísňové systémy. Jejich hlavním úkolem je ztížit dosažení cíle trestného činu a jsou tak součástí situační prevence kriminality. Dále jsou v práci shrnuty a popsány nejpoužívanější komponenty těchto systémů. Dílčí kapitola pojednává o jejich projektování a plánování. Praktická část zkoumá funkčnost a spolehlivost poplachových zabezpečovacích a tísňových systémů, které se pro zvýšení efektivity napojují na pult centralizované ochrany. Odtud jsou čerpána klíčová výzkumná data ve formě poruchových a poplachových incidentů. Výsledky jsou následně rozšířeny dotazníkovým šetřením mezi techniky, kteří mají přímé zkušenosti s výstavbou a servisem jednotlivých prvků ochrany.

ABSTRACT

RÍDL, Z. Functionality and Reliability of Intruder and Hold-Up Alarm Systems Connected to the Alarm Receiving Centre*: Bachelor Thesis.* České Budějovice: The College of European and Regional Studies, 2026. 83 pgs. Supervisor: RNDr. Růžena Ferebauerová.

Key words: alarm, crime prevention, perpetrator, reliability, security, unlawful act

This bachelor's thesis presents intruder and hold-up alarm systems in its theoretical part. Their primary purpose is to make the achievement of the criminal act's objective more difficult, thus forming part of situational crime prevention. Furthermore, the thesis summarizes and describes the most commonly used components of these systems. A separate chapter focuses on their design and planning. The practical part examines the functionality and reliability of intruder and hold-up alarm systems, which are connected to a alarm receiving centre to enhance their effectiveness. Key research data is collected from here in the form of fault and alarm incidents. The results are further expanded through a questionnaire survey among technicians who have direct experience with the construction and servicing of individual security components.

Obsah

Úvod

Zabezpečování objektů a cenností je dnes bráno za samozřejmost. Cesta k efektivním prostředkům byla však dlouhá a rozšířila se i na ochranu nás samotných. Dala vzniknout propracovanému řetězci neustále se inovujících řešení. Je až s podivem, že poplachové systémy nejsou často zmiňovaným a zkoumaným tématem. U laické veřejnosti se to snad dá pochopit. Bohužel ani ta kvalifikovaná nejeví o problematiku přílišný zájem. O tom ostatně vypovídá i malý rozsah dostupné české odborné literatury, ve které by bylo možné seznámit se s hlubšími informacemi a myšlenkami. Bez nich je představa o fungování těchto složitých soustav pouze povrchní, což neumožňuje správné pochopení smyslu jednotlivých zapojení. To má následný vliv na schopnost nefundované osoby zvážit propojení poplachových systémů do jednoho funkčního celku, který přinese výrazné posílení zabezpečení chráněného zájmu před narušitelem.

S tímto problémem se zcela jistě vypořádá oslovený projektant. I jeho cesta k získání možnosti dalšího rozvoje, ve formě vzdělávacích textů, je odkázána do zahraničních zdrojů. Ani autorem této práce nebyla nalezena jediná kniha českého původu, jež by se plánováním a navrhováním systémů ochrany objektů zabývala. Nejbližším cenným zdrojem informací je tak stále Žilinská univerzita v Žilině. Její vydavatelství nabízí komplexní řadu tematicky zaměřené literatury. Ta pokryje veškeré myslitelné požadavky na zdroj vědomostí. Její výhodou je, že čerpá nejen ze zkušeností tvůrců, ale provádí i citaci technických norem, standardů a právních předpisů. Soustavná redakční činnost navíc produkuje nové tituly, které jsou tak aktuální, což se o jiných přeshraničních říct nedá.

Uvedená problematika je autorovi této bakalářské práce velice blízká nejen ve vztahu k jeho předchozímu vzdělání, jež je elektrotechnické. Zabývá se jí i profesně, což umožňuje prohloubení a doplnění poskytnutého vhledu. Špatná dostupnost edukačních zdrojů byla jen jednou z motivací ke zpracování zvoleného tématu. Podpořilo ji i úzké zaměření písemností na konkrétní součást poplachových systémů. Zrodil se tak dílčí záměr zaznamenat ucelený přehled, který by byl vhodný pro všechny kategorie čtenářů.

Po naplánování, výstavbě a předání nastává provoz. S ním jsou spojeny incidenty ve formě poplachů a poruch. Při jejich vyhodnocování vznikla tvůrčí myšlenka na výzkum spočívající ve faktickém zjištění nejméně spolehlivých prvků poplachových systémů, které pak mají samozřejmý dopad na funkčnost. Jen správně pracující periferie mohou poskytnout spolehlivou ochranu a prevenci.

1 Cíl a metodika bakalářské práce

Význam poplachových zabezpečovacích a tísňových systémů při prevenci kriminality nastává v situačním působení, kdy je zásadní ztížit pachateli dosažení cíle trestné činnosti. Aby se zvýšila funkční efektivita a došlo ke snížení reakční doby, která je potřebná k dopadení narušitele, jsou tyto systémy napojovány na pulty centralizované ochrany. Pomocí nich lze též sledovat provoz dílčích komponent, nevyjímaje poruchové stavy.

Aby bylo možné řádně pochopit veškeré funkční náležitosti, bude se teoretická část této bakalářské práce zabývat poplachovými zabezpečovacími a tísňovými systémy ve svém významovém celku. Autor je čtenáři představí a zmíní jejich stručnou historii. Dále dojde k vysvětlení jejich smyslu při prevenci kriminality s uvedením vybraných trestných činů a přestupků, u kterých se v praxi jejich pozitivní působení využívá. V další kapitole bude následovat výčet jednotlivých zabezpečovacích a tísňových komponent a popis jejich funkce. Poskytnutí vhledu do problematiky projektování a plánování poplachových systémů pak uzavře teoretickou část. Pro splnění zamýšleného komplexního informačního pojetí provede autor nastudování dostupné tematické literatury. Poté pomocí rešerše vybraných kapitol a parafrázování textových pasáží do přehledných celků vytvoří základní pojmový a poznatkový zdroj. Ten je nutný pro pochopení souvislostí ve výzkumné části.

Hlavním cílem této práce je vyhodnotit poruchové incidenty jednotlivých součástí poplachových zabezpečovacích a tísňových systémů a posoudit jejich vliv na spolehlivost a funkčnost těchto systémů ve vztahu k prevenci a zabránění protiprávního jednání. Jeho dosažením se bude zabývat kapitola 5 praktické části. Byla zvolena kvantitativní empirická výzkumná metoda, při níž proběhne sběr dat z dohledového systému pultu centralizované ochrany, a to za období prvního čtvrtletí roku 2025. Po jejich setřídění, analyzování a syntetizování nastane interpretace zjištěných informací. Na základě dohody s rektorem VŠERS a s vedoucí této práce nebudou provozovatel, výrobce ani dodavatel technologií zveřejněni. Anonymizace vyplývá z citlivosti prezentovaných dat, jež by mohla být ve spojení s identifikací připojených objektů zneužita k možnému protiprávnímu jednání. U vybraných součástí poplachových systémů dojde k vyhodnocování incidentů, které zpřehlední strukturované tabulky. Získané výstupy doplní invence autora, jenž ve zkoumaném oboru profesně působí. Zásadní aplikační použitelnost by mělo přinést následné vyhodnocování poruchovosti jednotlivých periferií

a jejich vliv na spolehlivost a funkčnost poplachových zabezpečovacích a tísňových systémů. Tyto části budou doplněny o návrh případných změn, opatření či technických vylepšení.

Vedlejším cílem této bakalářské práce je prostřednictvím respondentů z řad techniků poplachových zabezpečovacích a tísňových systémů posoudit efektivitu jednotlivých prvků ochrany při prevenci kriminality. K tomu poslouží dotazníkové šetření za pomoci nástroje Survio s přímým odkazem na internetovou adresu https://www.survio.com/survey/d/D6N7V8O2I9N2A8N6U. Vzor nevyplněného dotazníku se pak nachází v příloze I. Tento kvantitativní empirický výzkum má za úkol potvrdit či vyvrátit stanovené hypotézy:

- H1: Pohybové čidlo je považováno za funkčně nejefektivnější prvek ochrany, protože si to myslí více než 60 % odpovídajících.
- H2: Nevyhovující umístění je pro respondenty závažnější faktor snižování schopnosti účinného fungování prvků ochrany než stáří/opotřebování.
- H3: Oslovení respondenti se nepřiklání k myšlence, že vyhlášení poplachu odrazuje narušitele od jeho dalšího postupu.

Z podkladů nastudovaných informací, nashromážděných dat, profesních zkušeností autora a odpovědí odborníků dojde v závěru bakalářské práce ke zhodnocení uvedených cílů. Nebude opominuto ani využití získaných poznatků ve vztahu k přínosu a aplikačnímu potenciálu. Odkazy na návrhy náprav možných negativních zjištění výzkumu lze v této části taktéž očekávat.

2 Představení poplachových zabezpečovacích a tísňových systémů

Každý člověk potřebuje ke svému spokojenému životu několik opěrných bodů. Ty jsou přehledně vyjádřeny v Maslowově pyramidě lidských potřeb. Ta řadí na první místo fyziologické potřeby a jako druhá v pořadí se zde objevuje bezpečnost. V souvislosti s tím je však třeba si uvědomit, že tato hodnota není zcela přirozeně dána. Stojí za ní celá řada bezpečnostních opatření, značná práce lidí a techniky. Ve všeobecnosti lze říci, že lidé chrání hlavně život, zdraví, majetek, mír, právo, svobodu a rodinu. Pocit bezpečí narušuje převážně násilná a majetková kriminalita. Tento negativní jev zřejmě nikdy nebude možné z našich životů úplně odstranit, ale lze proti němu účinně bojovat a snažit se ho redukovat. V tomto ohledu je nejdále ochrana majetku.[1]

Pokud se ohlédneme pouhých několik desítek let zpět, tak zjistíme, že lidé chránili svůj majetek i své osobní bezpečí pomocí mechanických systémů. Ty tvořily dveře, zámky, mříže a další zařízení, která měla odradit pachatele v jejich překonávání. Poplachové zabezpečovací a tísňové systémy (dále jen „PZTS") jsou vhodným doplněním mechanických prostředků, kdy dohromady tvoří základní pilíř kvalitní ochrany majetku. PZTS vznikly v důsledku rozvoje elektrotechniky, který umožnil postupné snižování pořizovací ceny. Systémy se tak staly dostupné i pro širokou veřejnost, která zcela přirozeně touží po co nejkvalitnější ochraně svého majetku, života i zdraví.[2] Z významového pojetí slova poplach vyplývá i hlavní určení poplachových systémů. Je jím výstraha, která upozorní na narušení střeženého prostoru a vznik nebezpečí. K aktivaci může sloužit automatická detekce neoprávněného vstupu či jeho pokusu. V takovém případě se použité systémy označují jako poplachové zabezpečovací. Dále může být poplach spuštěn manuální úmyslnou aktivací ze strany uživatele. Tento systém se nazývá poplachový tísňový.[3] PZTS jsou pouze jednou součástí komplexního balíčku nazývaného poplachové systémy. Do celkového výčtu patří:

- poplachové přenosové systémy (dále jen „PPS"),
- dohledové videosystémy (dále jen „VSS"),

[1] LOVEČEK, T., REITŠPÍS, J. *Projektovanie a hodnotenie systémov ochrany objektov*. 1. vydanie. Žilina, 2011, s. 9–10.
[2] BURDA, K. *Základy elektronických zabezpečovacích systémů.* Vydání první. Brno, 2017, s. 4.
[3] LOVEČEK, T., VEĽAS, A., ĎUROVEC, M. *Bezpečnostné systémy: poplachové systémy*. 1. vydanie. Žilina, 2015, s. 21–24.

- elektrická požární signalizace (dále jen „EPS"),
- elektronická kontrola vstupu (dále jen „EKV").[4]

2.1 Historie poplachových zabezpečovacích a tísňových systémů

Potřeba chránit sebe nebo svůj majetek provází lidstvo v podstatě od doby jeho existence. Počátek praktického uplatnění zabezpečení lze hledat v podobě primitivních mechanických prostředků. Jejich výskyt je historicky doložitelný již v počátku středověku. Některé z nich dodnes obdivujeme a hojně navštěvujeme. Hrady, padací mosty, zdi, hradby, valy, příkopy, truhlice nebo mříže sice spadají pod zájem turistického ruchu, ale fakticky se jedná o mechanické zábranné prostředky.[5] Ty byly lidmi dále vylepšovány. Dle nejstarších dochovaných písemností z dávného Řecka a Říma došlo už tehdy k užití mechanického zámku s klíčem. Tato kombinace odolala staletí a dochovala se až do dnešních dnů. Nejčastěji se používá cylindrická zámková vložka. Princip její funkce tkví v uložení odpružených stavítek, které jsou blokovány různě vysokými kolíky. Správný klíč stavítka posouvá do polohy, kdy se dá následně otočit celým cylindrickým válcem vůči pevnému tělu zámku.[6]

Zásadní posun v oblasti ochrany majetku, života a zdraví přinesla průmyslová revoluce. Celé masy lidí se stěhovaly z venkova do velkých měst. Takováto koncentrace obyvatelstva na jednom místě zhoršovala bezpečnostní situaci. Asi největší nebezpečí té doby představoval požár. Z důvodu jeho včasného odhalení a signalizování byla města vybavována systémy hlásek a požárních stanic. Komunikace mezi nimi byla však stále primitivní a skládala se z trumpet, zvonů, světelných záblesků a poslů. Tomu udělal přítrž vynález telegrafu v roce 1835. Jeho reálné nasazení, ve smyslu signalizační techniky, bylo až v roce 1847. Ve městě New York byly pomocí telegrafu propojeny uvedené hlásky a centrální stanoviště. To bylo dále spojeno s dalšími požárními stanicemi města. Tím vším došlo k velké časové úspoře při reakci na požár. Signál se rychleji a přesněji trasoval a dostal se do nejbližší požární stanice od místa události. Systém hlásek byl následně vylepšován a spolu s ním i centralizace. Byl vynalezen veřejný hlásič. V něm se nacházelo ozubené kolo, které se po zatažení páky obsluhou roztočilo a vytvořilo elektrickou zprávu ve formě teček a čárek. Zpráva vyjadřovala unikátní kód hlásky, který doputoval

[4] BOROŠ, M., VEĽAS, A., LENKO, F., KUFFA, R. *Bezpečnostné systémy: elektronické systémy kontroly vstupov*. 1. vydanie. Žilina, 2023, s. 49.
[5] LOVEČEK, T., REITŠPÍS, J. *Projektovanie a hodnotenie systémov ochrany objektov*. 1. vydanie. Žilina, 2011, s. 10.
[6] BOROŠ, M., MACH, V., ĎURICA, J. *Bezpečnostné systémy: mechanické zábranné prostriedky.* 1. vydanie. Žilina, 2022, s. 11–12.

k zapisovači na centrálním pultu. Ten událost zaznamenal na záznam o poplachu. První aktivní nasazení tohoto systému v Bostonu se datuje roku 1851.[7]

Počátky PZTS směřují do Sommerville v USA. Zde si v roce 1853 pan Augustus Pope nechal patentovat svůj elektrický systém na detekci vniknutí zloděje do objektu. Technické řešení bylo velice jednoduché a skládalo se z bzučáku a spínacího kontaktu na okně či dveřích.[8] Patent byl v roce 1857 prodán Edwinovi T. Holmesovi, který ho začal vylepšovat a vyrábět průmyslově. Roku 1858 představil v New Yorku a Bostonu první pult centralizované ochrany. Postava Edwina Holmese se pojí s dalším elektrotechnickým velikánem té doby, který se snažil přenést lidský hlas po drátě. Byl jím Graham Bell, který po úspěšných testech požádal právě Holmese o vybudování první komerčně používané telefonní ústředny. V roce 1877 ji dokončil a první telefonní pobočkou se stala budova Holmes Central Station. Následující období nepřineslo v oblasti zabezpečovací techniky zásadní posun. K detekci byly používány kontakty, nástražné dráty a destrukční čidla. Elektromechanické senzory spatřily světlo světa až počátkem dvacátého století. Patří mezi ně kyvadlová čidla, vibrační kontakty a pohybové senzory. Relé bylo až do poloviny dvacátého století klíčovou součástkou na poli zabezpečovacích ústředen, u kterých se jako signalizace nejčastěji uplatňoval zvonek. Podstatným urychlením rozvoje techniky byla druhá světová válka. Došlo k nástupu výroby tranzistorů a miniaturizaci techniky. Nemalý vliv na rychlém posunu měl kosmický program jednotlivých velmocí. Vše bylo završeno vynálezem a masivním rozšířením výpočetní techniky. První elektronické detektory se objevují v polovině dvacátého století. Měly podobu trezorového kontaktu a snímaly akustický podnět na chráněném zařízení. Následovaly kapacitní a aktivní prostorové detektory na bázi ultrazvuku a velmi krátkých vln. Přelom šedesátých a sedmdesátých let dvacátého století přinesl důležité technické vylepšení v podobě mikrovlnných čidel, která patří do dnešních časů k těm nanejvýš účinným. Ve stejné době byl posunut i vývoj senzorů na principu infračerveného světla. Ten byl ve druhé polovině sedmdesátých let zakončen výrobkem, který se stal nejvíce úspěšným a nejrozšířenějším zabezpečovacím prvkem po celém světě. Dostal název Passive Infrared Detector, což překládáme jako pasivní infračervené čidlo (dále jen „PIR"). Jeho původ se nachází v armádě, kdy bylo využíváno u samonaváděcích

[7] KŘEČEK, S. et al. *Příručka zabezpečovací techniky.* 4. vydání. Blatná, 2021, s. 13.
[8] BURDA, K. *Základy elektronických zabezpečovacích systémů.* Vydání první. Brno, 2017, s. 5.

protitankových a protiletadlových raket. Za zaslouženým úspěchem tohoto zabezpečovacího komponentu stojí spolehlivost, cena a funkční jednoduchost.[9]

2.2 Poplachové zabezpečovací a tísňové systémy jako prevence kriminality

Do širokého povědomí se zapsala poučka, že některým věcem je třeba předcházet, než je později komplikovaně a někdy i draze řešit. To samé jde říct i v případě kriminality. Historicky se ukázalo, že represivní řešení negativních jevů společnosti není příliš funkční. Do popředí se tak dostává preventivní politika. Ta je součástí systému kontroly kriminality a doplňuje trestní politiku, která je vyjádřena soustavou orgánů činných v trestním řízení a realizována trestním zákonodárstvím. Slovo prevence pochází z latinského praevenire, což je možné přeložit jako opatření nebo předcházení. Stejného významu má docílit ve spojení s kriminalitou. Hlavní úlohou je předcházet trestné činnosti a dalším přidruženým záporným projevům, které se nacházejí ve společnosti. Tu i jednotlivce je potřeba efektivně chránit, aby byly minimalizovány škody způsobené případným protiprávním jednáním. Pokud k němu v konečném důsledku dojde, tak přichází na řadu trestní represe. Trest jako takový slouží k ochraně před trestnou činností a dále působí výchovně na pachatele a společnost.[10]

Trestné činy, které jsou uvedeny v části druhé zákona č. 40/2009 Sb., trestní zákoník, mají široký záběr. Pro potřeby této práce je nutné zmínit ty, proti kterým PZTS efektivně působí jakožto prostředky prevence kriminality. Dle zkušeností autora to jsou:

- Loupež dle ustanovení § 173 zákona č. 40/2009 Sb., která je ve svém prvním odstavci spáchána za předpokladu, že je pachatelem proti jinému užito násilí, či je bezprostředním násilím hrozeno v úmyslu zmocnit se cizí věci.[11] Preventivní opatření PZTS zde spočívá hlavně v použití tísňových tlačítek, hlásičů nebo výklopných lišt. Dále se lze setkat s detektory poslední bankovky. Zmíněné technické zařízení je možné nasadit na místech s vysokým předpokladem pokusu nebo dokonání loupeže. Mezi takové objekty řadíme banky, spořitelny, směnárny, zlatnictví, klenotnictví a celkově jakékoliv místo, kde se nachází velká finanční hotovost či cenné předměty. Použití obdobné techniky připadá v úvahu i jako

[9] KŘEČEK, S. et al. *Příručka zabezpečovací techniky.* 4. vydání. Blatná, 2021, s. 13–15.
[10] FIRSTOVÁ, J., ZÁMEK, D. *Prevence kriminality: nedílná součást systému vnitřní bezpečnosti*. Vydání první. Praha, 2021, s. 56–59.
[11] JELÍNEK, J. et al. *Trestní zákoník a trestní řád: s poznámkami a judikaturou.* Vydání sedmé. Praha, 2017, s. 258.

prevence trestných činů proti výkonu pravomoci orgánu veřejné moci a úřední osoby dle ustanovení § 323, 324, 325 a 326 zákona č. 40/2009 Sb. – násilí proti orgánu veřejné moci, vyhrožování s cílem působit na orgán veřejné moci, násilí proti úřední osobě a vyhrožování s cílem působit na úřední osobu.[12] PZTS se zde uplatňují jako ochrana pracovníků, úředních a jiných osob. Při osobním provádění úkonů za přítomnosti klienta, které bývá převážně v místě úřadu, může dojít od protistrany k jednání, které má znaky protiprávního činu. Poškozený má následně možnost přivolat pomoc aktivováním tísňového tlačítka.

- Krádež dle ustanovení § 205 zákona č. 40/2009 Sb., která je ve svém prvním odstavci spáchána přisvojením si cizí věci tím, že se jí pachatel zmocnil a dle písmene a) tím způsobí škodu nikoliv nepatrnou na cizímu majetku.[13] Tato škoda musí činit minimálně 10 000 Kč. Použití poplachových systémů na detekci krádeží cenných předmětů je možné vidět v muzeu, výstavních sálech, prodejnách elektroniky apod. Na ochranu se nasazují hlavně předmětové detektory ve formě tíhových nebo tahových snímačů. Pokud je nějaká část prostoru veřejnosti nepřístupná, lze ji vyjma umístění mechanických bariér zabezpečit pomocí infračervené závory. Jestliže je krádež dle písmene b) páchána vloupáním, PZTS slouží převážně jako preventivní opatření, které má případného pachatele odradit od úmyslu vniknout do uzavřeného prostoru. Když k tomu přeci jen dojde a jsou protiprávně překonány mechanické zábranné prostředky, musí PZTS zareagovat a předat tuto informaci majiteli prostoru či odpovědné osobě. To samé platí i pro případ, při němž se pachatel ukryje ve střeženém místě v době, kdy bylo ještě nezastřeženo. Pakliže je zařízení napojeno na pult centralizované ochrany (dále jen „PCO"), tak je o bezpečnostním incidentu okamžitě informována PČR nebo MP. Toto napojení sníží reakční dobu uvedených složek a zvýší pravděpodobnost zadržení pachatele přímo na místě činu.
- Neoprávněný zásah do práva k domu, bytu nebo k nebytovému prostoru dle ustanovení § 208 zákona č. 40/2009 Sb.[14] Mohou nastat situace, že vyjmenovaná místa jejich majitel delší dobu neužívá. Případně je navštěvuje pouze nepravidelně. Mezi takové objekty se řadí opuštěné domy, chaty, chalupy, sklady, průmyslové objekty apod. Vždy je dobré nasadit do nich poplachové systémy,

[12] ČESKO. *Úplné znění zákona č. 40/2009 Sb., trestní zákoník.* Vydání třinácté. Praha, 2024, s. 146–148.
[13] JELÍNEK, J. et al. *Trestní zákoník a trestní řád: s poznámkami a judikaturou.* Vydání sedmé. Praha, 2017, s. 311–312.
[14] ČESKO. *Úplné znění zákona č. 40/2009 Sb., trestní zákoník.* Vydání třinácté. Praha, 2024, s. 97.

jelikož upozorní na protiprávní vstup nepovolaných osob a ty je možné z místa následně vykázat. V praxi se jedná o bezdomovce, tuláky, squattery, osoby pohřešované nebo v pátrání.

- Poškození cizí věci dle ustanovení § 228 zákona č. 40/2009 Sb. K naplnění skutkové podstaty dle odstavce 1 dojde, pakliže je způsobena na cizím majetku škoda nikoliv nepatrná tím, že někdo zničí, poškodí, eventuálně učiní cizí věc neupotřebitelnou.[15] I u tohoto trestného činu mohou zásadním způsobem pomoci PZTS, které je vhodné doplnit o VSS. Užívají se otřesová čidla, která se vkládají do bankomatů, výdejových boxů atd. Ty jsou mechanicky poškozovány různými údery či kopy. Jakmile dochází k častému rozbíjení okenních výplní vandaly, tak je možné nasazení detektorů rozbití skla. Moderní technologie umožňují i ochranu proti vandalismu ve smyslu neoprávněného posprejování nebo pomalování cizího majetku. V nedávné době šlo spáchání uvedeného trestného činu v jeho druhém odstavci odhalit v podstatě náhodně. Stávalo se to pomocí VSS, svědka či výskytu hlídky PČR nebo MP v místě páchání. Dnes je reálné do vytipovaných lokalit nasadit speciální akustický detektor, který dokáže rozpoznat zvuk stříkání spreje a zareaguje vyhlášením poplachového stavu.

Obdobně PZTS působí i v rámci prevence přestupků, které se nacházejí v zákoně č. 251/2016 Sb., o některých přestupcích. Jsou to zejména tyto:

- Přestupek proti veřejnému pořádku dle ustanovení § 5 odstavce 1 písmene g) zákona č. 251/2016 Sb. Skutková podstata je naplněna pokud je fyzickou osobou neoprávněně zabráno veřejné prostranství, veřejně přístupný objekt či veřejně prospěšné zařízení, případně dojde touto osobou k jejich poškození. Dále musí být splněna podmínka, že případ nejde potrestat podle jiných zákonů. Uvedené platí analogicky pro právnickou nebo podnikající fyzickou osobu. Přestupek je pak dle ustanovení § 5 odstavce 2 písmene c) zákona č. 251/2016 Sb.[16] V situaci, kdy jednání podezřelého naplňuje znaky tohoto přestupku, jsou zásadním pomocníkem VSS. Každé větší město má síť svého kamerového systému, který umožňuje nepřetržitý dohled na veřejná prostranství. V praxi není zcela reálné

[15] JELÍNEK, J. et al. *Trestní zákoník a trestní řád: s poznámkami a judikaturou.* Vydání sedmé. Praha, 2017, s. 359–360.
[16] KUČEROVÁ, H., HORZINKOVÁ, E. *Zákon o odpovědnosti za přestupky a řízení o nich a zákon o některých přestupcích: s komentářem a judikaturou.* Vydání první. Praha, 2017, s. 749–750.

pokrýt takto široký výčet míst, objektů nebo zařízení pomocí zabezpečovací techniky.

- Přestupek proti majetku dle ustanovení § 8 odstavce 1 písmene a) bod 1. zákona č. 251/2016 Sb. Tento přestupek vyžaduje úmyslné zavinění fyzické osoby. Ta na cizím majetku udělá škodu prostřednictvím krádeže.[17] Odcizení nějakého zboží v obchodě se děje prakticky neustále. Vznikla tak potřeba drahé a často kradené zboží nějak ochraňovat. K tomuto účelu se na předměty umísťují radiofrekvenční nebo magnetické ochranné prvky. Jestliže pachatel zboží odcizí a následně projde bezpečnostní bránou, tak je vyvolán poplach. Toto zařízení prakticky spadá pod EKV.

PZTS jsou zahrnuty v situační prevenci kriminality. Ta se nezaobírá důvody a okolnostmi, které pachatele vedly ke spáchání protiprávního jednání. Její směřování cílí k samotnému činu a okolnostem, které ho umožnily nebo učinily snadnější. Tyto faktory se situační prevence snaží omezit a učinit tak páchání trestné činnosti složitější. K tomu ve smyslu této práce slouží:

- opatření znesnadňující přístupnost k samotným prostředkům používaným k trestné činnosti – mříž, zámek, poplachové zařízení, fólie proti rozbití skleněné výplně,
- EKV zabraňující vstup neoprávněné osoby – přístupové karty a další prostředky k identifikaci oprávněného vstupu včetně fyzické kontroly bezpečnostním pracovníkem,
- VSS zvyšující pravděpodobnost odhalení a dopadení podezřelé osoby.

Po použití uvedených opatření může dojít k přesunu cíle kriminality. Pachatel si následně vybere majetek, který není tolik zabezpečen. Volba jiné taktiky je další možností, jak přesunout kriminalitu a obejít preventivní zásahy.[18]

[17] ČESKO. *Úplné znění zákona č. 273/2008 Sb., o Policii České republiky; Úplné znění zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich; Úplné znění zákona č. 251/2016 Sb., o některých přestupcích.* Vydání dvacáté druhé. Praha, 2024, s. 121–122.
[18] FIRSTOVÁ, J., ZÁMEK, D. *Prevence kriminality: nedílná součást systému vnitřní bezpečnosti*. Vydání první. Praha, 2021, s. 65–67.

3 Jednotlivé komponenty poplachových systémů

Přesné vyjmenování dílčích součástí, které tvoří celek v podobě poplachových systémů, určují jednotlivé technické normy. Zde bohužel neexistuje jednota ve výčtu složek. Norma s označení EN 50136-1 pohlíží na tyto systémy ve smyslu detekce nebezpečí. Na něho musí instalované elektrické zařízení zareagovat. Tato reakce se spouští buď automaticky, anebo ručně. Jejím cílem je ochrana majetku, života a zdraví. Další norma EN 50130-4 ED.2 rozlišuje systémy na:

- poplachový zabezpečovací – zjištění a signalizování pokusu nebo dokonání vniknutí pachatele do zastřežené oblasti,
- poplachový tísňový – záměrné spuštění poplachu ze strany uživatele,
- poplachový systém přivolání pomoci – pro lidi žijící v možném stavu ohrožení.

Pro potřeby této práce byly cíleně vybrány následující složky poplachových systémů. U nich je uvedena odpovídající česká technická norma, která je identická s těmi evropskými (dále jen „ČSN EN”):

- PZTS – ČSN EN 50131-1 ED.2,
- PPS – ČSN EN 50136-1,
- VSS – ČSN EN 62676-1-1,
- EKV – ČSN EN 60839-11-1.[19]

Cílenost tkví v představení jednotlivých podskupin a komponentů, které je tvoří. Vzhledem k tomu, že dojde k vyhodnocování jejich funkčnosti a spolehlivosti (vyjma VSS), je podstatné pochopit určení, technické provedení a provozní chování. Uvedený balíček vybraných částí je běžným výčtem u organizace, která je kvalitně zabezpečena poplachovým systémem a zároveň dbá na přehled o pohybu osob nebo vozidel v určeném prostoru. Veškeré technologie se navíc doplňují a společně tvoří opravdu silný řetězec preventivní ochrany před protiprávním jednáním. Pro správné fungování je nutné zachovat vzájemnou kompatibilitu všech prvků, dbát na správné zapojení a provést odborné nastavení. Vyhodnocování provozu přísluší programovému vybavení výrobce nebo dodavatele. Nelze opominout ani pravidelné revize, které se provádí fyzickou kontrolou a měřením v místě instalace.

[19] LOVEČEK, T., MARIŠ, L., ŠISER, A. *Plánovanie a projektovanie systémov ochrany objektov*. 1. vydanie. Žilina, 2018, s. 26–27.

3.1 Poplachové zabezpečovací a tísňové systémy

Svojí podstatou slouží jednoúčelově k odhalení narušení střeženého prostoru či k případnému manuálnímu vyvolání stavu nebezpečí. Zjištěný incident může být doprovázen optickou a akustickou signalizací. PZTS se dělí na autonomní a s dálkovým přenosem. Rozhodujícím faktorem je předávání informace o poplachu. Pokud je indikace pouze centrální v lokálním chráněném místě a je uskutečňována prvky, které jsou součástí zabezpečovací ústředny, tak se jedná o autonomnost. Jakmile je poplachový signál vysílán PPS skrze přenosovou cestu na PCO, mluvíme o dálkovém přenosu.[20]

Komponenty PZTS se navzájem propojují prostřednictvím kabelů, rádiového přenosu či jejich kombinací. Metalické vedení je realizováno žilovými kabely, z nichž se vytvoří páry drátů pro následné zapojení. Rádiové spojení se nejčastěji uskutečňuje na frekvenci 868 MHz. Jeho výhoda tkví v jednoduchosti instalace, jelikož není potřeba náročně rozvádět kabely. Nevýhodou je cena bezdrátových prvků a také nutnost jejich bateriového provozu.[21] Z praktického hlediska se u rozsáhlých objektů a členitých terénů ukázala vhodnost kabelové instalace. V její prospěch mluví dlouhověkost, univerzálnost a stabilita spojení. Ta platí za předpokladu, že je užito stíněné kabeláže a tato je vedena mimo oblast rušení. To typicky představuje souběh s rozvodem elektrické energie. Při nasazení bezdrátové technologie je znatelná absence uspokojujícího dosahu a síly signálu. Tento nedostatek se značně projevuje v městské zástavbě, kde u starších budov bývá větší tloušťka stěn a dochází tak k citelnému útlumu.

Zapojení detektorů do PZTS je nejčastěji provedeno prostřednictvím bezpotenciálových smyček. Rozeznávají se tři jejich základní stavy označené jako klid, poplach a sabotáž. Ta se běžně pojmenovaná jako tamper. Aby je zabezpečovací ústředna mohla rozlišit, tak je nutné smyčku vyvážit zařazením rezistorů do jejího obvodu a nadefinovat systému hodnoty elektrického odporu v ohmech (Ω). Ty jsou měřením vyhodnocovány a dle stanoveného rozmezí dojde k vyhlášení jednoho z uvedených stavů. Příkladem může být vložení dvou rezistorů, které je považováno za dvojité vyvážení. Při identických odporových hodnotách 4,7 kΩ vyhodnotí ústředna jako poplach 9,4 kΩ. Klidový stav bude představovat polovina a sabotáž nejčastěji 0 či nekonečno (∞).[22]

[20] LOVEČEK, T., REITŠPÍS, J. *Projektovanie a hodnotenie systémov ochrany objektov*. 1. vydanie. Žilina, 2011, s. 57–58.
[21] BURDA, K. *Základy elektronických zabezpečovacích systémů.* Vydání první. Brno, 2017, s. 8–14.
[22] HONEY, G. *Intruder Alarms.* Third edition. Oxford, 2007, s. 62–65.

Následuje výčet komponent PZTS, který koresponduje s výzkumem pro praktickou část této práce a zároveň nabízí ucelený přehled nejběžněji užívané technické sestavy těchto systémů. Jsou jimi:

- Zabezpečovací ústředna – je řídící prvek na bázi výpočetní techniky, k němuž se připojují detektory, moduly, klávesnice a další periferie. Z nich dostává informace, které dle programového nastavení vyhodnotí a výsledek předá obsluze formou indikace skrze připojená zařízení. U ústředen existují dva základní provozní stavy. Uživatelsky jsou nejvíce známé jako zastřežení a odstřežení.[23] Propojení komponent se realizuje přes sběrnici, smyčkami, bezdrátově nebo hybridním způsobem. K přenosu dat mezi prvky slouží zvlášť určené metalické vedení. Někdy je však nutné použít i strukturovanou počítačovou kabeláž. Pokud je to vhodné a žádoucí, tak lze zvolit bezdrátový přenos.[24] Ústředna se dá reálně představit jako plechová, případně umělohmotná skříňka kvádrového tvaru. Uvnitř se nachází základní deska s procesorem, pamětí, vstupy, výstupy a komunikačním portem místní počítačové sítě (dále jen „LAN"). K samotné řídící desce se u sofistikovanějších instalací připojuje expandér či linkový modul. Do něj vstupují odporové, eventuálně napěťové smyčky. Dále slouží jako přípojný bod komunikační sběrnice a výstupního napětí. To pochází z napájecího zdroje, který je zapojen na silový rozvod 230 V. Celou sestavu doplňuje akumulátor, o čemž bude dále pojednáno.
- Napájecí, posilovací zdroj – vykonává napájení komponent PZTS včetně zabezpečovací ústředny a je považován za základní. Jeho napětí bývá obvykle okolo 13,8 V stejnosměrně a proudové zatížení se pohybuje v rozmezí 1 až 5 A. Pakliže by provoz veškerých připojených prvků přesahoval horní mez, je nutné použít další zdroj označený jako posilovací. Ten kompenzuje i úbytek napětí u delšího kabelového vedení. Takovýto postup se nazývá napájení decentralizovaným způsobem. Zdroje signalizují ústředně poruchové stavy výpadku 230 V, akumulátoru a také své vlastní. Při přerušení dodávky elektrické energie se využívá náhradní zdroj napětí ve formě olověného akumulátoru poskytujícího 12 V stejnosměrných. Liší se svojí velikostí, která závisí na kapacitě.[25] Označuje se jako sekundární článek, jelikož je možné ho opakovaně

[23] BURDA, K. *Základy elektronických zabezpečovacích systémů.* Vydání první. Brno, 2017, s. 5–6.
[24] LOVEČEK, T., VEĽAS, A., ĎUROVEC, M. *Bezpečnostné systémy: poplachové systémy*. 1. vydanie. Žilina, 2015, s. 46–47.
[25] KŘEČEK, S. et al. *Příručka zabezpečovací techniky.* 4. vydání. Blatná, 2021, s. 116–119.

nabíjet stejnosměrným napětím a vybíjet. U olověných článků nesmí dojít k takzvanému podbití. Způsobí nenávratné poškození vedoucí ke zničení. Při současných instalacích se nasazují akumulátory nevyžadující údržbu doléváním vody. Není u nich nezbytné odvětrávání pro možný únik výbušné směsi kyslíku a vodíku.[26] Z praxe lze skutečně potvrdit nutnost počítat s množstvím zapojených periferií do obvodu, s délkou kabeláže i průměrem vodičů. Jakmile klesne hodnota elektrického napětí pod výrobcem udávanou mez, tak dojde k nestabilní funkčnosti a výpadkům komponentů. Tento jev lze částečně vyrovnat posílením vedení ve formě přidání dalšího vodiče k zápornému i kladnému pólu napájení. Pokud je to nedostačující, nastává nutnost instalace posilovacího zdroje.

- Ovládací klávesnice – patří mezi nejvíce používané zařízení, které je určeno k řízení a indikaci mnoha funkcí. Tou základní je uvedení systému do stavu zastřeženo, nebo odstřeženo. Signalizace, prohlížení a zrušení poplachů spadá též mezi elementární schopnosti. Následují možnosti vypnutí a zapnutí zařízení, nastavení parametrů, změny uživatelských hesel a další dle výrobce. Uvedené je možné po zadání přístupového kódu. To se činí skrze tlačítka. Veškeré dění zobrazuje většinou displej. Klávesnice se umisťuje uvnitř zabezpečené zóny. Z toho důvodu je umožněno aktivování odchodového nebo příchodového zpoždění.[27] Pro potřeby techniků a administrátorů PZTS bývá integrováno skryté menu. K jeho zpřístupnění je zapotřebí zadat speciální heslo. Odryté položky obsahují informace, nastavení a možnosti systému, které vyžadují jeho znalost a odborné proškolení.
- Magnetický kontakt – se řadí k nejvíce používaným čidlům neoprávněného vstupu skrz dveře, okna a podobné prostupy. Skládá se ze dvou kovových jazýčků umístěných v hermeticky uzavřené skleněné trubičce. Ta je vložena do plastového pouzdra a dává se na nepohyblivý otvorový díl. Protikus tvoří permanentní magnet, který se připevňuje na pohyblivý segment prostupů. Pokud je v klidovém stavu, tak jsou oba kusy v těsné blízkosti a díky působení magnetického pole jsou jazýčkové kontakty spojené. Po oddálení se rozpojí, což aktivuje poplachový stav. Montáž se provádí buď povrchově, anebo zápustně.[28] Kabeláž ústí u většiny instalací v blízké rozvodné krabici (dále jen „RKZ"). Zde je provedeno propojení

[26] TKOTZ, K. et al. *Příručka pro elektrotechnika.* 2. doplněné vydání. Haan-Gruiten, 2017, s. 65.
[27] LOVEČEK, T., VEĽAS, A., ĎUROVEC, M. *Bezpečnostné systémy: poplachové systémy*. 1. vydanie. Žilina, 2015, s. 48–49.
[28] HONEY, G. *Intruder Alarms.* Third edition. Oxford, 2007, s. 76–78.

vodičů a odporové vyvážení smyčky. RKZ i magnetický kontakt mohou obsahovat ochranu před sabotáží. Dle nastavení ústředny lze tímto detektorem sledovat stav otevření dveří a nahradit jím případnou absenci spínače u elektronického zámku.

- Pohybové čidlo – slouží k odhalení osoby, která vstoupila do zastřeženého prostoru. Na základě její chůze a aktivity těla dojde k reakci senzorů a vyhlásí se poplach. Užití těchto zabezpečovacích prvků je nejčastější uvnitř budov, kde má jejich detekční diagram objemový trojrozměrný tvar. Dle použité technologie se dělí na pasivní infračervené (PIR), mikrovlnné (dále jen „MW"), ultrazvukové (dále jen „US") a duální, které kombinují uvedené technologie v jednom zařízení.[29] PIR reaguje na změnu záření elektromagnetického vlnění v jeho infračerveném pásmu. Vychází z faktu, že každý objekt s teplotou v rozmezí od -273 °C do 560 °C je původcem takového záření. Člověk představuje v tomto spektru vlnovou délku 9,4 mm a na tuto hodnotu zareaguje pyroelektrický senzor, před kterým je umístěna čočka. Jejím smyslem je rozdělení detekční zóny na část viditelnou a zakrytou. K vyhodnocení stavu se musí objekt pohybovat právě mezi těmito rozdílnými teritorii. Jejich tvar a dosah určuje použitá optika. Umožní vytvořit tenký paprsek, kdy hovoříme o PIR typu záclona. Dále existují stropní provedení s rozsahem 360 stupňů a chodbová, která mají dlouhý dosah. US pracuje na principu Dopplerova jevu. Detekuje změny ultrazvukového vlnění v rozmezí 300 MHz až 300 GHz. Vysílač posílá do střeženého prostoru konstantní frekvenci v pásmu neslyšitelném pro člověka. Po jejím odrazu je přijímačem vyhodnocena změna fáze vlnění. Pokud k ní nedojde, tak se prostorem nic nepohybuje. V opačném případě je vyhlášen poplach. MW používají identický způsob fungování jako US. Liší se v aplikovaném pásmu elektromagnetických vln. Nejčastěji se volí 2,5 GHz, 10 GHz či 24 GHz. Duální detektory velice dobře poslouží v místech, kde dochází k častým falešným poplachům vlivem nežádoucích spouštěčů. K eliminaci poslouží kombinace PIR + MW nebo PIR + US. Díky rozdílné technologii detekce se velice sníží pravděpodobnost aktivace obou v jeden okamžik. Jako další bezpečnostní prvek pohybových čidel se integruje ochrana před zakrytím. V odborné terminologii ji označujeme slovem antimasking a používá se k zjištění sabotáže i v odstřeženém stavu.[30]

[29] BURDA, K. *Základy elektronických zabezpečovacích systémů.* Vydání první. Brno, 2017, s. 32.
[30] KŘEČEK, S. et al. *Příručka zabezpečovací techniky.* 4. vydání. Blatná, 2021, s. 76–86.

- Akustický detektor rozbití skla – rozpoznává, prostřednictvím specifického zvuku tříštění skla a rázové vlny, destrukci okenní či dveřní tabule. Zařízení obsahuje mikrofon, jímž zachycuje a převádí zvuk do podoby elektrické informace. Ta je vyhodnocena vnitřním analyzátorem. Pokud zjistí rázovou vlnu, po které následuje charakteristická frekvence tříštěného skla, tak vyvolá poplach.[31]
- Tísňový hlásič – spouští poplach v případě nebezpečí. Aktivace může být učiněna manuálně obsluhou, která je ohrožena útočníkem. K tomu jsou určena tísňová tlačítka nebo výklopné lišty umístěné na podlaze. Automatické aktivování připadá v úvahu u zařízení k zjištění poslední bankovky. Instaluje se do pokladen jako opatření před loupežným přepadením. Poplach je vyhlášen, pakliže dojde k odstranění peněz umístěných v mechanickém či optoelektronickém detektoru.[32] Posledním typem hlásiče je osobní tísňový. Funguje na bezdrátovém principu přenosu při různých frekvencích rozsahu pásma velmi krátkých vln. Vyrábí se i ultrazvuková provedení. Vysílač má často podobu ovladače vozidlového alarmu, náramku apod. Je napájen baterií a kódován identicky s přijímačem. Ten se zapojuje do zabezpečovací ústředny na smyčku nastavenou jako tísňová.[33] Základním kritériem správného fungování a uživatelsky snadného používání je vhodné umístění. Ideální je ho prokonzultovat s dotyčným pracovníkem. Zároveň tak dojde k jeho proškolení. Touto vzájemnou interakcí se vyloučí budoucí plané poplachy nebo poškození zařízení. Veškeré uvedené hlásiče jsou v praxi nastavené jako tíseň tichá. Pachatel by správně neměl vědět o její aktivaci.
- Otřesové čidlo – se umísťuje na chráněný předmět či překážku. V situaci, kdy na ně dojde k útoku, snímá elektromechanické ústrojí nebo piezoelektrický člen vytvořené vibrace. Je rozpoznávána jejich frekvence a síla. Poplach se vyhlásí při shodě vstupních informací s nastavením daného senzoru. Bohužel se operační rádius řadí k velice malým.[34] U železných povrchů je faktický rozsah detekce maximálně 3 m. Nejběžnější použití je u trezorů a bankomatů. Kvůli planým poplachům se jen málokdy dává na vchodové dveře nebo okna. Pro tyto situace se volí vhodnější detektory, které jsou uvedeny výše ve výčtu.

[31] BURDA, K. *Základy elektronických zabezpečovacích systémů.* Vydání první. Brno, 2017, s. 31–32.
[32] LOVEČEK, T., VEĽAS, A., ĎUROVEC, M. *Bezpečnostné systémy: poplachové systémy*. 1. vydanie. Žilina, 2015, s. 40–41.
[33] KŘEČEK, S. et al. *Příručka zabezpečovací techniky.* 4. vydání. Blatná, 2021, s. 90–91.
[34] HONEY, G. *Intruder Alarms.* Third edition. Oxford, 2007, s. 112–115.

3.2 Poplachové přenosové systémy

Jejich smyslem je zasílání dat o stavech PZTS. Zabezpečovací ústředna zastává prvotní místo vzniklého informačního řetězce. Koncovou destinací pak bývá dohledové a poplachové přijímací centrum (dále jen „DPPC"), případně PCO. PPS jsou tvořeny:

- poplachovou přenosovou cestou (dále jen „PPC"). Tato informační trasa transportuje veškeré určené a nadefinované stavy PZTS do DPPC/PCO. Forma jejího zřízení je skrze pevný přepínaný nebo vyhrazený spoj. Obvyklou dvojici způsobu přenosu tvoří LAN spolu s rádiovou či GSM sítí.
- poplachovým přenosovým zařízením (dále jen „PPZ"). To má primárně za úkol předávání vyhlášených narušení a provozních stavů směrem k DPPC/PCO. Odtud může přijímat další informace a pokyny pro PZTS. Z toho vyplývá, že PPZ je umístěno na obou stranách komunikační trasy. Skládá se z vysílačů, přijímačů a komunikátorů.[35] U nich tkví funkční smysl v předávání signálů, kódů a informací o poplachu oprávněnému místu. Na určené telefonní číslo zašlou SMS, popřípadě tak učiní hlasovou zprávou. Stále častěji se však používá odesílání skrze datové sítě. Rozeznáváme digitální, hlasové, GSM, rádiové, telefonní a internetové typy komunikátorů. Jak již jejich názvy napovídají, tak se liší technologií distribuce.[36]

Zvolené technické řešení PPC s sebou nese jistá specifika, která jsou spojena s řadou výhod i nevýhod. Pro potřeby této práce budou konkretizovány přenosy prostřednictvím metalického vedení, optických kabelů, rádia a GSM sítí.

- Metalické přenosové cesty – se vyznačují svojí stejnorodostí a malou změnou parametrů v průběhu vedení. Nejčastěji používanou je kroucená dvojlinka. Užitý název vychází z faktu, že ji utváří žíly, které jsou v párech smotány k sobě navzájem. Důvodem tohoto řešení je eliminace anténního efektu dvou souběžně jdoucích vodičů, přeslechů, rušení a odporových ztrát. Žíly se skládají z drátu nebo licny. Vodivý materiál bývá z mědi. Nevodivou ochranu kabelu plní pružné umělé hmoty. Jako jejich zástupce lze uvést hojně se vyskytující polyetylen či polyvinylchlorid. Přenos skrze kroucenou dvojlinku nese označení symetrický, jelikož jsou oba vodiče v rovnocenném postavení. Signál vyjadřuje rozdíl jejich

[35] VEĽAS, A. *Poplachové systémy: poplachové prenosové systémy a zariadenia.* 1. vydanie. Žilina, 2015, s. 38–43.
[36] LOVEČEK, T., VEĽAS, A., ĎUROVEC, M. *Bezpečnostné systémy: poplachové systémy*. 1. vydanie. Žilina, 2015, s. 78–82.

potenciálů. Dle volby stínění se tyto kabely rozdělují na Unshielded Twisted Pair (dále jen „UTP"), Foil Twisted Pair (dále jen „FTP") a Shielded Twisted Pair (dále jen „STP"). UTP stínění postrádá a je tak náchylnější na rušení. FTP tento problém odstraňuje aplikací kovové fólie, která obaluje všechny páry naráz. STP jde v tomto ještě dále, jelikož přidává další metalickou fólii okolo každého páru. Mezi výhody uvedených metalických cest patří cena a jednoduchost propojení s koncovými zařízeními. Nevýhodou může být špatná manipulace s STP díky její tloušťce a tvrdosti. UTP se nehodí na dlouhé vzdálenosti. Z důvodu rušení by bylo nutné signál zesílit a vyčistit. Podle rychlosti přenosu se Twisted Pair kabely dělí na kategorie 1 až 8.[37] Při skutečné instalaci musí technik akceptovat plánem určenou kategorii. Je však velice důležité užít stíněné kabeláže tam, kde slouží k vedení linky po sběrnici. Ta je totiž velice náchylná k rušení. U běžných smyčkových detektorů lze sáhnout i po UTP. V dřívějších dobách se pro PPC natahoval i koaxiální kabel. S ním se dnes můžeme potkat při napojení staršího typu VSS a u antén rádiového PPZ. Přenosy na dlouhou vzdálenost převzala optická vlákna.

- Optické přenosové cesty – jsou dobrou volbou pro LAN, ve které vznikne potřeba velkého transportu dat za krátký časový úsek. Často se vyskytují ve struktuře rozlehlé sítě (dále jen „WAN"). Tvoří je optické kabely. Ty nejsou náchylné na elektromagnetické rušení a ani ho nevytvářejí. Umožňují přenos na dlouhé vzdálenosti v řádu jednotek kilometrů. Vděčí za to svému malému útlumu signálu. Další výhodou je nízká možnost odposlouchávání datového provozu. Způsob vysílání je zcela jednoduchý. Na počátku stojí zdroj infračerveného světla. Může to být laser či LED dioda. Ústí do napojených optických vláken kabelu. Pokud svítí, tak vyjadřuje logickou jedničku. Okamžik nesvícení reprezentuje logickou nulu. Užívané vlnové délky jsou 850 nm, 1310 nm a 1550 nm. Toto záření je pro lidské oko neviditelné, ale pohled do aktivního vlákna zapříčiňuje poruchu zraku. Samotný kabel tvoří vnější izolace z polyvinylchloridu, obal proti tahu, plastová protitlaková ochrana a jádro. To bývá skleněné nebo umělohmotné. Okolo něj se nachází další vrstva z obdobného materiálu. Díky její nižší optické hustotě se světelný paprsek odrazí zpět do vlákna. U mnohovidového typu je vysílán pod úhlem. Ideální sklon je takový, že zapříčiní absolutní odraz. Jedině ten garantuje minimální poškození dat. Paprsek v jednovidovém vláknu rovnoběžně kopíruje

[37] ADÁMEK, M., BARČOVÁ, K., BITALA, P., MACH, V., ŠEVČÍK, J. *Dohledové videosystémy v bezpečnostních technologiích.* 1. vydání. Ostrava, 2022, s. 48–51.

podélnou osu kabelu, což mu dovoluje urazit dlouhé vzdálenosti. Na konci trasy se vyskytuje fotodioda, která převádí optický signál na elektrický.[38]

- Rádiové přenosové cesty – využívají elektromagnetické vlny v pásmu 9 kHz až 3000 GHz. V rámci PPS se reálně používá rozsah od 30 MHz do 3 GHz. Toto vlnění se šíří k přijímači směrem od vysílače. Ten převádí digitální či analogový signál na frekvenčně modulovaný. Následně ho vyšle do okolí prostřednictvím antény. Ty existují ve všesměrové formě, kdy mají tvar prutu. Jsou vhodné tam, kde se objekt nachází v blízkosti přijímače. Pokud chceme lepší parametry přenosu, tak zvolíme směrový dipól. Svou kruhovou charakteristikou vyzařuje až do vzdálenosti patnácti kilometrů. A pokud ani to nestačí, instaluje se Yagiho anténa. Její výhoda tkví ve více prvcích, které jsou připevněné na jedné konstrukci. Díky tomu má dosah až 30 km. Při nastavování správné polohy a směru nelze ignorovat, že vlivem nestejnorodosti prostoru, kterým signál proudí, dochází k odrazům, ohybům a útlumu. Na konci rádiové trasy stojí přijímač, jenž přijatá data zesílí a demoduluje.[39] Při výčtu bezdrátových přenosů nelze opomenout mikrovlnné záření. U něho se frekvence pohybuje v rozmezí 0,1 GHz až 300 GHz. Vysílané elektromagnetické vlny mají úzkou charakteristiku a jsou vyzařovány parabolickou anténou. Tu je potřeba nasměrovat přesně k cílovému místu. Trasa nesmí obsahovat překážky.[40] V městské zástavbě je nalezení dokonalého umístění antény problematické. Optimální je samozřejmě přímá viditelnost a co nejnižší vzdálenost k přijímači. Bohužel však dochází k tomu, že pokud nastane jen nepatrná změna v prostředí, tak je síla signálu citelně slabší. K tomu stačí vztyčení stavebního jeřábu, lešení apod. Následuje další měření, při kterém je potřeba nalézt pro anténu novou pozici. Někdy postačuje přesun jen o několik centimetrů.
- GSM přenos – představuje standardizovaný typ rádiových mobilních sítí. Pokryté území je rozděleno na buňky s přidělenými frekvenčními kanály. Ty se nesmí opakovat v rámci vícebuněčného svazku, jehož dosah signálu činí maximálně 3 km. Ve velkých městech se oblasti dělí na mikrobuňky o velikosti až 500 m. Samotná komunikace probíhá mezi základnovou (dále jen „BTS") a mobilní

[38] SPURNÁ, I. *Počítačové sítě: praktická příručka správce sítě.* 1. vydání. Kralice na Hané, 2010, s. 21–24.
[39] VEĽAS, A. *Poplachové systémy: poplachové prenosové systémy a zariadenia.* 1. vydanie. Žilina, 2015, s. 73–78.
[40] ADÁMEK, M., BARČOVÁ, K., BITALA, P., MACH, V., ŠEVČÍK, J. *Dohledové videosystémy v bezpečnostních technologiích.* 1. vydání. Ostrava, 2022, s. 63.

stanicí. Tu reprezentuje telefon nebo modul se SIM kartou. Její význam tkví v jednoznačné identifikaci účastníka v síti. Zařízení je rozeznáno z čísla IMEI, jež má obsaženo ve své paměti. BTS má podobu antén kontrolovaných jejich hlavní řídící jednotkou.[41] GSM přenosová cesta skýtá nejjistější a nejuniverzálnější možnost PPC. Důvodem je značného pokrytí světa těmito sítěmi. Pokud tedy odlehlost nějakého místa neumožňuje spojení poplachových systémů vyjmenovanými cestami, tak GSM bývá volbou k uvážení.

Zařízení, které stojí na rozhraní PPZ a PPC, je nazýváno směrovač. Propojuje mezi sebou navzájem jednotlivé sítě. Ať už se jedná o spojení dvou LAN sítí anebo místní LAN odchází mimo lokalitu do WAN, tak zabezpečuje nejlepší trasu. Směrovač dále nabízí funkce na poli zabezpečení datových informací. Lze na něm nastavit přístup k jednotlivým portům. Také obsahuje integrovaný firewall, který ho chrání před škodlivými útoky.[42]

Přenášená data je nutné šifrovat a zajistit tak jejich celistvost, věrohodnost i utajení. K tomu slouží šifrovací algoritmus a klíč. Původní informaci se říká otevřený text. Transformovat ho dokáže symetrická a asymetrická kryptografie. První způsob vychází z existence klíče, který je oběma komunikačním stranám znám. Následně se použije k šifrovacímu i dešifrovacímu procesu. Nevýhoda tkví ve faktu, že při vzrůstajícím počtu adresátů stoupá i množství nutných klíčů. Takovou šifrou je například 3DES či AES. Asymetrie vychází ze Shamirova algoritmu, který se uplatnil v RSA. Původní zprávu uzamyká klíč odesílatele. Příjemce ho však nezná. Použije vlastní klíč, čímž vznikne dvojí ochrana dat. Následně vše putuje zpět k adresátovi, který zruší svůj zámek a vše opět přepošle příjemci. Ten aplikuje svůj šifrovací klíč, čímž si informace odtajní. Při tomto řešení existují dva typy klíčů. Veřejný bývá umístěn na serveru a má k němu kdokoliv přístup. Odesílatel jím data zašifruje. Privátním pak příjemce zprávu dešifruje.[43]

PCO znamená koncovou destinaci odeslaných dat z PPS. Má formu technických prostředků, které jsou potřeba k práci s přijatými informacemi. Typicky se jedná o počítač, který je spojen s komunikátorem a má v sobě nainstalováno patřičné

[41] VEĽAS, A. *Poplachové systémy: poplachové prenosové systémy a zariadenia.* 1. vydanie. Žilina, 2015, s. 101–106.
[42] LOVEČEK, T., VEĽAS, A., ĎUROVEC, M. *Bezpečnostné systémy: poplachové systémy*. 1. vydanie. Žilina, 2015, s. 158–159.
[43] LOVEČEK, T. *Bezpečnostné systémy: bezpečnosť informačných systémov.* 1. vydanie. Žilina, 2007, s. 196–199.

programové vybavení. Pomocí něho se připojuje na server PCO. Je důležité zdůraznit, že provozovatel poplachových systémů nemá povinnost být napojen, neboť je to služba vyžádaná. Pokud tak učiní, podstatně se tím zvýší šance včasného dopadení pachatele. Vyjma toho plní PCO i další úkoly, mezi něž může patřit:

- příjem a zpracování informací o zabezpečovací ústředně – poplachy, poruchy, režimy či ztráty spojení,
- ovládání podsystémů – zastřežení, odstřežení, přemostění apod.,
- ukládání došlých dat a obsluhou provedených akcí,
- grafické znázornění probíhajících dějů,
- aktualizace prvků.

Pult tvoří součást DPPC, které představuje vzdálené centrální místo. Zde je zajištěna nepřetržitá přítomnost policistů nebo jiných vyškolených osob. Tito mohou okamžitě reagovat na přijaté poplachy a stavy ze střežených objektů. Po patřičném prověření a vyhodnocení předají údaje zakročující jednotce.[44] Operátoři PCO mají k dispozici seznam oprávněných osob a pracovníků objektu. Po vyhlášení poplachu není nutné okamžitě vysílat hlídku k prověření. Pakliže to zabezpečovací instrukce daného místa vyloženě nezakazují, je dohledovým pracovníkem voláno na určené číslo. Pokud se dovolá, tak ověřuje identifikaci volaného a následně řeší důvody incidentu. V případě planého poplachu a přítomnosti autentizované osoby nemusí nikoho vysílat k zakročení. Vše ale záleží na předem stanovených postupech, které mohou být u každého podezření z narušení zcela odlišné.

3.3 Dohledové videosystémy

V rámci ochrany života, zdraví a majetku jsou v hojném počtu využívány i kamery. Zprostředkují možnost sledovat dění ve střeženém prostoru a ověřovat si tak aktuální situaci. Záznam je ukládán a lze ho tudíž využít jako důkazní prostředek. To si uvědomují i pachatelé, čímž VSS značně přispívají k prevenci kriminality. Celý systém kamer doplňují prvky přenosu a záznamu. Nemůže chybět ani ovládací programové vybavení. K Nejstarším dálkovým způsobům přenosu patřila telefonní linka. Dnes se volí internetová cesta sítěmi LAN či WAN. Pokud jsou vzdálenosti lokální, tak jej možné sáhnout i po bezdrátovém provedení. Běžnější však bývá řešení skrze metalický nebo

[44] VEĽAS, A. *Poplachové systémy: poplachové prenosové systémy a zariadenia.* 1. vydanie. Žilina, 2015, s. 117–123.

optický kabel. Velikou výhodou VSS je jejich univerzálnost. Při správné volbě druhu kamery je možné hlídat takřka jakékoliv prostory. Rozmanitost jednotlivých typů je dalším plusem pro provozovatele. Historický přesun od analogového signálu k digitálnímu je zcela samozřejmý. Otevřel větší možnosti práce se záznamy a ulehčil archivaci.[45] S ní se pojí záznamové zařízení, jež se nazývá digitální videorekordér (dále jen „DVR"). Má podobu přístroje s řadou vstupů pro koaxiální kabely, které lze přepínat a vidět na monitoru obraz ze zvolené kamery. Pokud má systém včleněn DVR, tak se nazývá hybridní. Důvodem je přítomnost digitálních i analogových záznamů. Ty v případě potřeby převádí na číslicovou informaci, celek komprimuje a uloží. S rozmachem počítačových sítí zcela klesla obliba těchto aparátů a přenos signálu se přesunul do strukturované kabeláže. Data jsou rozdělena na skupiny bitů nazývající se pakety. Obsahují adresy příjemce a odesílatele, obraz, zvuk, příkazy a další. Jejich přenos zajišťuje klasická počítačová síť LAN či WAN, a to s využitím internetového protokolu IP. Podle něho se označují i kamery, které se v takovémto systému nasazují. Mají výhodu v tom, že obraz přímo komprimují a šifrují. K ukládání slouží vestavěná paměťová karta nebo síťový videorekordér (dále jen „NVR"). Ten nezřídka obsahuje i přepínač s integrovanou funkcí PoE, což umožňuje přes jediný kabel přenášet data i napájet připojené periferie.[46]

Tou nejdůležitější je samotná kamera. Jak již bylo naznačeno výše, jsou analogové modely s koaxiálním kabelem nahrazovány technologií IP a ethernetovým rozhraním. Ve prospěch moderního propojení počítače a kamery v jeden celek hovoří tyto argumenty:

- vysoké rozlišení a ostrost obrazu,
- využívání strukturované kabeláže,
- šifrování přenášených dat,
- univerzálnost,
- integrace zvuku,
- napájení skrze PoE,
- chytré vyhodnocování obrazu a možná implementace do PZTS.[47]

[45] LUKÁŠ, L. et al. *Bezpečnostní technologie, systémy a management II.* 1. vydání. Zlín, 2012, s. 16.
[46] BURDA, K. *Základy elektronických zabezpečovacích systémů.* Vydání první. Brno, 2017, s. 85–88.
[47] ADÁMEK, M., BARČOVÁ, K., BITALA, P., MACH, V., ŠEVČÍK, J. *Dohledové videosystémy v bezpečnostních technologiích.* 1. vydání. Ostrava, 2022, s. 6–7.

Základní konstrukční skladbu každé kamery tvoří soustava čoček ve formě objektivu. Ten většinou umožňuje měnit zaclonění a ohniskovou vzdálenost. Kvalita optiky značně ovlivňuje úroveň výsledného obrazu, který dopadá na světlocitlivý senzor. V něm dojde k převodu na elektrickou informaci. Následuje procesor, jenž provede digitalizaci a komprimaci. Výsledný soubor dat je uložen na paměťovou kartu a přenesen do koncového dohledového místa. Skladba kamery vypadá jednoduše, ale pro lepší pochopení si zaslouží hlubší rozbor s doplněním dalších periferií.[48]

- Objektiv – přes své čočky zobrazuje zmenšenou scénu na fotocitlivý senzor. Veškerá optika je uspořádána v jedné ose a značná část prvků se po ní pohybuje. Při jiném rozložení by nešlo ostřit a aplikovat transfokátor. Ten se stará o změnu ohniskové vzdálenosti. Přibližuje snímanou scénu, čímž však dojde k zúžení zorného pole.[49] K neméně důležitým parametrům objektivu patří i jeho světelnost. Udává, kolik světla u vytváření obrazu projde optickou soustavou až k senzoru. Redukci zajišťuje clona. Činí tak mechanicky pomocí nepropustných lamel, kterými reguluje průměr otvoru pro dopadající světlo. Ovládají se ručně nebo motoricky. Veškeré uvedené nastavení je potřeba provádět s přihlédnutím k hloubce ostrosti, kterou lze upravit manuálně, ale v novějších zařízeních se o vše stará automatické zaostřování.[50]
- Optický senzor – transformuje snímaný obraz do elektrického signálu. Historicky se do těl kamery osazovaly různé typy těchto součástek. Nejstarší CCD mají dobrou světelnou citlivost a hloubku ostrosti. Jejich cena je vyšší. Následoval CMOS, u něhož byl požadavek na snížení výrobní ceny. To s sebou přineslo zhoršení obrazové kvality, ale i energetickou nenáročnost a menší sklony k zahřívání. K novým a nejkvalitnějším technologiím se řadí DPS. Pro každý bod scény obsahuje samostatně pracující převodník, který mění analogový signál na digitální. V rámci jednoho snímku je navíc několikrát vzorkován. Obrazový procesor řídí a nastavuje parametry pro každou buňku snímače odděleně od ostatních. Senzor tedy může pracovat jako obrovské množství nezávislých kamer.[51]

[48] LUKÁŠ, L. et al. *Bezpečnostní technologie, systémy a management II.* 1. vydání. Zlín, 2012, s. 46.
[49] LOVEČEK, T., VEĽAS, A., ĎUROVEC, M. *Bezpečnostné systémy: poplachové systémy*. 1. vydanie. Žilina, 2015, s. 88–90.
[50] KŘEČEK, S. et al. *Příručka zabezpečovací techniky.* 4. vydání. Blatná, 2021, s. 183–187.
[51] LUKÁŠ, L. et al. *Bezpečnostní technologie, systémy a management II.* 1. vydání. Zlín, 2012, s. 51–53.

- Obvody pro zpracování obrazu, kompresi dat, řízení a ukládání – mají zásadní vliv na kvalitu snímků a funkční rychlost. Obrazový procesor nastavuje parametry snímání scény a digitálně ji zpracovává. Například se stará o expozici, stabilizaci, zaostřování, redukování šumu, nastavení bílé barvy a kontrastu. Vzniklý soubor je nutné z kapacitních důvodů zmenšit. Na toto jsou určeny obvodové součásti, které algoritmem kódují informace a snaží se v nich nalézt ty nadbytečné. Jejich odstranění je označováno jako komprese ztrátová nebo bezztrátová. První způsob znamená nemožnost rekonstruovat původní data. Nejčastěji se s ním lze setkat právě u videa či zvuku. Druhý typ zvládne zpětnou obnovu do originální podoby, což je zcela zásadní při přenosech počítačových souborů. Celkové fungování kamery řídí CPU. Svoji centrálnost vyjadřuje tím, že plní roli komunikačního prostředníka s jinými přístroji. U toho potřebuje ukládat a číst určitá data. O to se stará krátkodobá paměť RAM. Dlouhodobé, šifrované a energeticky nenáročné uchování informace obstarává flash paměť.
- Ethernetové komunikační rozhraní a PoE – jsou dnes nejpoužívanějším způsobem zapojení a napájení IP kamer. Na oboje postačí jediný kabel UTP/FTP s koncovkou RJ45. To přineslo obrovskou výhodu ve variabilitě umístění, jelikož odpadla nutnost mít v blízkosti zdroj elektrické energie. PoE je funkce jeho zdrojového zařízení, kterým je v síti LAN povětšinou přepínač. Má větší počet portů a utváří hvězdicové připojení koncových prvků.
- Dělič obrazu – umožňuje rozdělit plochu zobrazovače na více částí a navolit do nich výstupy z kamer. Dle preferencí nabízí různé poměry stran a výřezy.
- DVR – obsahuje pevný disk k uložení digitálního záznamu, který si z analogového sám převede a zkomprimuje. Obraz lze uchovávat i z několika zařízení v jeden okamžik. Tento režim se nazývá multiplexní. Dále přidává volbu časové osy a detekce pohybu. Ústí do něj koaxiální kabely kamerové techniky.
- NVR – je periferie IP kamer sloužící k ukládání nahrávek v digitální podobě. Obvykle bývá umístěn v serverovně. Pro komunikaci v síti mu slouží vlastní IP adresa. Z jakéhokoliv počítače, který je do ní připojen, má oprávněná osoba možnost dostat se k úložišti.[52] NVR nezřídka obsahuje přepínač s funkcí PoE. Vstupují do něj FTP či UTP kabely osazené koncovkou RJ45.

[52] ADÁMEK, M., BARČOVÁ, K., BITALA, P., MACH, V., ŠEVČÍK, J. *Dohledové videosystémy v bezpečnostních technologiích.* 1. vydání. Ostrava, 2022, s. 11–16.

3.4 Elektronická kontrola vstupu

Střežený prostor utváří území, které je skoro vždy ohraničeno nějakou překážkou. Pokud by se chtěl pachatel dostat dovnitř, musí ji překonat. V jeho postavení mu situace nedovoluje jiný než neoprávněný vnik. Existuje však i skupina oprávněných osob. Těm se do zdí, plotů a jiných zábran vytvářejí stavební otvory vyhrazené pro vstoupení. Opatří se dveřmi, závorami, turnikety a zámky. Obdobně se postupuje u průjezdu vozidel. Systém EKV přinesl zásadní změnu v automatizaci řízení a kontrole takových vstupů. Identifikační prvek se stal univerzálním klíčem k přístupu do stanovených zón. Správce oprávnění nastavuje uživatelům konkrétní povolené prostupy do oblasti a přiděluje jim identifikátor. Aby byl skutečně zajištěn pohyb jen určeným lidem či autům, vznikla potřeba řádného zjištění identity prostřednictvím sjednaného ověřovacího faktoru. Zadávání hesla z klávesnice, přiložení karty ke čtečce i biometrické údaje jsou dokazovacím faktorem v držení oprávněného používatele.[53] Pakliže je systém správně nastaven, tak je zcela snadné jím řídit a sledovat pohyb osob. Zaznamená místo, čas a totožnost. Dále nabízí neocenitelnou provázanost s PZTS a EPS. První uvedená spolupráce vyhlásí poplach v době, kdy je vstup proveden neoprávněně, nebo se o něj kdokoliv neúspěšně pokouší. Jestliže nastane požár, je nutné vyvolat odblokování zábranných prostředků, čímž se uvolní úniková cesta. To by bez udaného propojení nebylo možné.[54] EKV je v zásadě o ověření uživatele a jeho přístupových práv. V tomto kontextu pracuje se třemi zásadními pojmy:

- Identifikace – musí bezpečně zjistit návštěvníkovu totožnost. Aby to bylo proveditelné, tak je zapotřebí existence jeho údajů v interní databázi. V ní programové vybavení hledá shodu. Velkým pomocníkem jsou i VSS.
- Autorizace – značí proceduru přiřazení konkrétních oprávnění, a to ztotožněným a autentizovaným používatelům.
- Autentizace – je ověření identity na základě prokázání znalosti (something to know), předložením vlastněného (something to have) nebo měřením unikátních vlastností (something to be). Nejstarším, stále velice aplikovaným ověřením, je zadání kódu na klávesnici. Má výhodu v nekonečné možnosti změnit si heslo. S tím souvisí zásadní nevýhoda spojená s nároky na jeho dlouhodobé uchování v paměti mozku. Jiný druh představuje držení hmotného identifikačního prvku

[53] BURDA, K. *Základy elektronických zabezpečovacích systémů.* Vydání první. Brno, 2017, s. 49–50.
[54] BOROŠ, M., VEĽAS, A., LENKO, F., KUFFA, R. *Bezpečnostné systémy: elektronické systémy kontroly vstupov.* 1. vydanie. Žilina, 2023, s. 15.

neboli tokenu. Reálné využití našla radiofrekvenční, čipová a magnetická karta. Optická cesta skrze čárové a QR kódy nebývá u osob tak častá jako u předmětů. I jejich pohyb v definovaném území zaslouží sledovat. Důvody jsou preventivní ve smyslu předcházení a odhalování trestné činnosti. Poslouží také v logistice či strojovém načítání dokladů. V zásadě nejbezpečnějším typem autentizace jsou biometrické údaje. Jako nejrozšířenější lze označit otisk prstu, sken tváře, snímání oční sítnice a duhovky. Nejlepší volbou ověření identity je kombinace více předložených způsobů.[55]

Z finančních důvodů přetrvává ověřování znalostí a vlastnictvím. Při otevírání vstupů kódovými zámky vzniká několik nešvarů. Jedním z nich je univerzálně nastavené heslo, které používají všichni pracovníci z dané zóny. Systém EKV pak postrádá smysl a navíc je nahráváno na další neduh. Tím jsou nadměrně opotřebovaná či špinavá tlačítka klávesnice. Případný pachatel pak nemusí složitě obhlížet zadávání hesel. Stačí mu zkoušet kombinace znečištěných tlačítek. Je nutné apelovat na administrátora, aby nepřipustil jednotný kód pro všechny. U autentizace kartou, která se čtečkou komunikuje v naprosté většině instalací radiofrekvenčně, existují bohužel také nedostatky v ochraně před neoprávněným vniknutím.

Lidský faktor může představovat zásadního nepřítele správné funkce EKV. Nezáleží na tom, jestli je příčinou slušnost, nevědomost nebo lhostejnost. Následující chování je vždy nežádoucí:

- Nedodržení bezpečné vzdálenosti (tailgating, piggybacking) – znamená porušení bezpečnostních zásad ze strany oprávněného vstupujícího, který ze zdvořilosti vědomě vpustí další osobu bez jejího ověření prostřednictvím EKV. Bohužel nastává i nevědomé umožnění vniku. Má ho za následek nedbalá údržba dveří, jež se příliš pomalu dovírají a v nejhorším případě se ani nezavřou. Umisťování zarážek z lenosti řádných uživatelů znehodnocuje funkčnost celého kontrolního systému. Jako prevence se nasazuje technické opatření umožňující sledovat stav dveří. Při nedovření v nastaveném časovém intervalu vyhlašuje poplach. Účinně působí také otočné propusti, turnikety a VSS.
- Sdílení ověřovacích prostředků (passback) – vytvoří situaci, kdy do zóny systémově vejde stejná osoba několikrát za sebou. Reálně jich však projde

[55] LOVEČEK, T., VEĽAS, A., ĎUROVEC, M. *Bezpečnostné systémy: poplachové systémy*. 1. vydanie. Žilina, 2015, s. 132–137.

několik, protože si mezi sebou jednoduše půjčují jedinou kartu či heslo. I proti tomuto se dá bojovat přiřazením časového úseku. Během něho nepůjde stejný prvek autentizace uplatnit znovu v rámci příchodu. Další modifikace přidá podmínku odchodu, která odblokuje token/kartu ke vstupu. Nejúčinnější prevencí je nasazení biometrie.[56]

Systém EKV nabízí instalaci mnoha součástí a jejich kombinací. Dle autora této bakalářské práce byl vytvořen seznam nejčastějších periferií. Vychází z osobní zkušenosti a z vyhodnocovaných incidentů dohledového počítačového programu PCO.

- Čtečka karet – procházela svým historickým vývojem od načítání magnetických pásků s oxidem kovu. Ten je rozdělen na 3 stopy. Každou z nich má na starosti zvlášť určeny snímač. Některé čtečky jsou pouze jednostopé či dvoustopé. Funkčním principem je změna magnetizace a následná indukce napěťových špiček. Dekódovaná informace má podobu binárního čísla a další přenos se uskutečňuje po sběrnici RS232 nebo skrze USB. Následovalo čtecí zařízení typu Wiegand. Zde hraje hlavní roli elektromagnetická indukce. Karta se skládá ze dvou řad přesně stanovených drátků. Může ji tvořit i děrovaná destička z kovu. Vše je zalito umělou hmotou, což znesnadňuje kopírování. Čtečka vytváří elektromagnetické pole a vložená karta naruší jeho stejnorodost. Dle určeného způsobu toto vyhodnotí a přemění do výsledku v podobě binární informace. Novější technologie přinesla čipová karta s integrovaným procesorem. Dělí se na kontaktní a bezkontaktní. První druh se pozná přítomností plošky s kontakty. Je napájena až ze čtečky a tudíž neobsahuje baterii. U druhého typu se při přiblížení ke čtecímu zařízení indukuje energie do antény karty. Tím dojde k napájení vnitřních obvodů. Princip datového přenosu tkví ve vyhodnocování změny tohoto odběru energie. Dnes nejvíce rozšířeným vývojovým stádiem identifikačních prvků je RFID. Jak již vypovídá samotný název, tak způsob vyčtení i zápisu náleží vlnám rádiové frekvence. Elektronická informace se uchovává v čipu, který je doplněn pamětí a anténou. V takovéto sestavě zařízení samo nevysílá. Je tedy pasivní. Aktivní verze obsahuje baterii a poloaktivní má zdroj pro uschování napětí získaného při posledním načítání. RFID prvek pracuje při několika frekvenčních pásmech. Nízké (LF) má rozsah 125 až 134,2 kHz a dosah 0,5 m.

[56] BOROŠ, M., VEĽAS, A., LENKO, F., KUFFA, R. *Bezpečnostné systémy: elektronické systémy kontroly vstupov.* 1. vydanie. Žilina, 2023, s. 25–27.

Vysoké (HF) funguje při 13,56 MHz a maximální vzdálenost činí 1 m. Velmi vysoké (UHF) je v rozmezí 860 až 960 MHz, kdy může být nejdále 3 m. Mikrovlnné znamená frekvence 2,45 až 5,8 GHz a účinnou komunikační dráhu 10 m. Platí, že čím vyšší pásmo, tím je rychlejší přenos dat.[57] U EKV se v praxi nasazují pouze technologie LF a HF. Do samotné karty se uloží identifikační číslo uživatele. To musí administrátor následně přidělit konkrétní osobě v programové databázi. Po přiložení karty do elektromagnetického pole čtečky je nahrán identifikátor, který je odeslán k vyhodnocení. Pokud je vše v pořádku, přístup projde autorizačním procesem a zápisem do historie. Vstup se buď povolí, anebo zamítne.[58]

Po instalaci nové čtecí hlavy následuje její zanesení do systému a přidělení k již vytvořené skupině osob oprávněných ke vstupu. K tomuto je nutná aktivní a fungující PPC. Čtečky EKV jsou reálně napojeny na zabezpečovací ústřednu a jsou pevnou součástí poplachových systémů. Komunikaci a napájení obstarává k tomu určený modul. Samotná hlava má integrovaný kryptografický klíč. Dle bezpečnostního posouzení, použitých součástí a zadání objednavatele mohou nastat určité kombinace příchodových a odchodových způsobů:

- Prvním z nich je umístění čtečky z obou stran dveří. Ty se osadí koulemi. Z únikové strany musí existovat zabezpečená schránka s klíčem od zámkové vložky. Tato varianta platí u elektronického zámku, který není v klidovém stavu napájen. U inverzního typu se do soustavy EKV přidá nouzové tlačítko. Po jeho stisknutí dojde k odpojení elektrické energie zámků a je umožněn volný průchod.
- Druhá konfigurace dává na stranu odchodu tlačítko s tím, že se předpokládá oprávněnost pobytu daných osoby uvnitř zóny. Není tedy důvod kontrolovat jejich pohyb směrem ven.
- Třetí variantou lze označit užití panikové kliky. Toto řešení se aplikuje do frekventovaných prostor jako je čekárna apod.

[57] LOVEČEK, T., VEĽAS, A., ĎUROVEC, M. *Bezpečnostné systémy: poplachové systémy*. 1. vydanie. Žilina, 2015, s. 140–147.
[58] BOROŠ, M., VEĽAS, A., LENKO, F., KUFFA, R. *Bezpečnostné systémy: elektronické systémy kontroly vstupov.* 1. vydanie. Žilina, 2023, s. 78–80.

U všech popsaných možností a kombinací je důležité detekovat řádné zavření dveří. Není též od věci zvolit vhodný limit jejich otevření. Uvedené poskytuje kontakt zámku, nebo ho může suplovat magnetický senzor PZTS. O následné varování se postará:

- Optická a akustická signalizace – mívá více podob, které jsou poplatné umístění. Do venkovního prostředí přichází v úvahu siréna doplněná o oranžové světlo. Dává se do čela domu ve výšce, jež znemožňuje dosáhnutí bez přistavení podpory. Takto nastavená sestava nachází vhodné použití převážně u klasických poplachů PZTS. Upozorní na napadení objektu, označí ho a značně znepříjemňuje pachateli jeho situaci.[59] U vnitřního provedení se sahá k méně hlučným a viditelným prostředkům. Postačí malé zařízení s LED a zvukovým měničem.

Při nasazení EKV je nutností kontrolované vstupy vybavit elektronickým zámkem. Ten je potřeba propojit kabeláží s ovládacím modulem a přivést do něj napájení buď 12 V anebo 24 V. Záleží na modelu. Systém po úspěšné identifikaci, autentizaci a autorizaci odblokuje západku. Z hlediska typu zádržného mechanismu lze tyto zámky rozdělit na:

- Elektromechanické – poznáme podle zabudování elektrické části do zárubně či křídla dveří, které je statické. Instalační prostor je nutné předem připravit a zavést do něj příslušnou kabeláž. Nezbytnou součástí zapojení je transil. Jde o polovodičovou součástku. Plní ochranu obvodu před napěťovými špičkami.
- Elektromotorické – mají naopak umístění ve dveřním křídle. Jsou to již složitější a dražší zámky s vlastní elektronikou. Blokaci otevření realizuje závora posouvaná motorem. Je důležité uživatele vhodně upozornit na nutnost vyčkat odblokování, jelikož celý proces provází prodleva. Jeho dokončení většinou oznamuje tón.
- Elektromagnetické – tvoří dva fyzické protikusy. Dveřní část z magnetického kovu je nejčastěji k vidění na celoskleněných křídlech. Po dovření přilne k pevně přidělanému elektromagnetu, jímž prochází napětí. U něj technické specifikace stanovují nejvyšší možné hmotnostní zatížení v kilogramech, které ještě udrží.[60]

[59] KŘEČEK, S. et al. *Příručka zabezpečovací techniky.* 4. vydání. Blatná, 2021, s. 123–124.
[60] BOROŠ, M., VEĽAS, A., LENKO, F., KUFFA, R. *Bezpečnostné systémy: elektronické systémy kontroly vstupov.* 1. vydanie. Žilina, 2023, s. 147–150.

Do komplexní sestavy kontroly vstupů spadá historicky i fyzická ochrana. Bezpečnostní pracovník plní nezastupitelnou funkci, kdy k prevenci může přispět:

- v odůvodněných situacích zakázáním vstupu/vjezdu,
- kontrolou osoby, dopravního prostředku nebo zavazadla,
- zápisem do evidence pohybu osob a vozidel,
- zjištěním totožnosti protiprávně se chovajícího jedince,
- zamezením vnášení či vynášení podezřelých předmětů.[61]

Pakliže dotyčný nespolupracuje, je vždy vhodné zavolat na místo hlídku Policie České republiky, která disponuje patřičnými oprávněními. Jednání v nutné obraně, krajní nouzi i zadržení podezřelé osoby dle § 76 odstavce 2 zákona č. 141/1961 Sb. nelze pracovníkovi fyzické ochrany nebo vrátnému upřít. Dle svého právního názoru mohou přistoupit k daným hraničním opatřením. Bude to však na vlastní odpovědnost, jelikož k beztrestnosti takového činu je potřeba splnit řadu zákonných podmínek.

Na pomezí EKV a samostatné kategorie stojí docházkové systémy. I ony evidují čas příchodu a odchodu do místa pracoviště. Toto rozšiřují o další užitečné funkce, které jsou ještě hodnotnější při provázání se mzdovou účtárnou. Jde zaznamenat:

- čerpání dovolené,
- pozdní příchod,
- návštěva lékaře,
- služební cesta,
- obědová pauza aj.

Celý princip spočívá v manuálním stisknutí jedné z předvolených možností. Přiložení identifikačního prostředku ke čtecímu zařízení terminálu se provede záznam do evidence docházky. RFID karta je stále nejrozšířenějším identifikátorem. Pro svoji přenositelnost bohužel svádí k podvodům. Jeden zaměstnanec může odhlásit jiné, kteří již dávno nejsou přítomní. Pro situaci, kdy nastane výpadek elektrické energie, jsou informace ukládány do vnitřní paměti každého jednotlivého terminálu. Po obnově dojde k odeslání na server.[62]

[61] VEĽAS, A., ZVAKOVÁ, Z., BOROŠ, M. *Bezpečnostné systémy: fyzická ochrana objektov.* 1. vydanie. Žilina, 2021, s. 114–116.
[62] BOROŠ, M., VEĽAS, A., LENKO, F., KUFFA, R. *Bezpečnostné systémy: elektronické systémy kontroly vstupov.* 1. vydanie. Žilina, 2023, s. 173–177.

4 Projektování a plánování poplachových systémů

V důsledku požadavku na jednotnost formulace a potřebu zřizovat ochranu objektu, která splní kvalitativní nároky norem i zadavatelů, bylo nutné vytvořit systematiku. Takovou, která naplní komplexnost oboru a zahrne patřičné rozbory. Na tento popud vznikla řada programových nástrojů k měření účinnosti a smysluplnosti jednotlivých prvků ochrany.[63] V nich i uvnitř problematiky se lze setkat s řadou odborných termínů:

- Chráněný zájem – je to, co ohrožuje vzniklá negativní událost (hmotné i nehmotné statky).
- Bezpečnostní incident – jde vyjádřit jako situaci, při které nastane nechtěný sled událostí v podobě krádeže, poškození atd.
- Chráněný objekt – představuje stavba či ohraničené území, kde se nachází všechny její prostory.
- Objektový perimetr – většinou kopíruje katastrální území společnosti.
- Střežený prostor – tvoří hranici perimetru.
- Chráněný prostor – se nachází uvnitř objektu či střeženého prostoru. Obsahuje zájem, jenž se ochraňuje.
- Bezpečnostní zóny – dělí prostor dle jeho stavebního řešení. Nejčastěji se utváří na základě přístupových práv uživatelů.
- Zóna detekce – je území, ve kterém bude narušitel pravděpodobně odhalen.
- Krajní zóna detekce – vysílá prvotní reakci na přítomnost nepovolané osoby.
- Aktivní zóna – značí oblast s plnou funkčností všech zabezpečovacích součástí.
- Ochranné pásmo – znamená prostor, ve kterém pracovník fyzické ostrahy sleduje dění v okolí. Není však ve střeženém prostoru. Nasazuje se zde i VSS.[64]

Je také potřeba definovat další základní termín, kterým je zranitelnost. Při působení ohrožujících vlivů vyjadřuje ztrátu schopností a funkcí objektů, subjektů či prostředků. Tato vlastnost má několik podob. Rozlišuje se zranitelnost fyzická (mechanické zábranné prostředky, cesty apod.), informační (počítačové prvky a programové vybavení), lidská (zaměstnanci) a technická (VSS, telefonní síť aj.). Aby uvedené mohlo nastat, je nutný spouštěč. Odborně se nazývá ohrožení a představuje děj

[63] KAMPOVÁ, K., LOVEČEK, T. *Modelovanie systémov ochrany objektov a ich optimalizácia.* 1. vydanie. Žilina, 2020, s. 9–10.
[64] LOVEČEK, T., REITŠPÍS, J. *Projektovanie a hodnotenie systémov ochrany objektov*. 1. vydanie. Žilina, 2011, s. 36–38.

s následky negativního charakteru, které se projevují v určitém čase a místě. Rozděluje se na úmyslné/neúmyslné, vnější/vnitřní, technologiemi způsobené, sociální (nedbalost, zapomětlivost či nevědomost lidského faktoru) a související s přírodními vlivy. Ve smyslu této kapitoly i práce připadá největší pozornost na úmyslné ohrožení. Málokdy je chráněný prostor napaden náhodou.[65] Útočník vynakládá vědomé úsilí ve formě vloupání, krádeže, sabotáže nebo vandalismu. Činí tak s cílem dosáhnout chráněného zájmu, který chce odcizit, poškodit atd. Úmyslným narušitelem může být i interní pracovník, který neoprávněně vstoupí do zóny, kam nemá přístup. Dle celkové připravenosti k napadení se dělí narušitelé na tyto typy:

- Profesionálně jednající – mají značné povědomí o lokalitě, technologii a fungování ochrany objektu. Disponují plánem. Jednají až po jeho důkladném prostudování. Vybavují se pomůckami na překonání všech mechanických i elektronických ochranných součástí. Často nekonají sami. U práce organizované skupiny se efektivní možnosti útoku dále rozšiřují.
- Informovaní a seznámení – znají oblast a funkci zabezpečovacích prvků. Ke své činnosti nepoužívají speciálních zařízení, ale spokojí se s běžně dostupnými. Z veřejných zdrojů studují patřičné informace. Strategii vymýšlejí tak, aby co nejvíce eliminovali střet s prostředkem znamenajícím překážku, který by byl nad jejich překonávací schopnosti. Významným pomocníkem jsou jim hluchá a slepá místa provedení systému ochrany.
- Náhodní – nečiní své kroky naplánovaně. Spouštěčem je impuls. Jejich vybavení zahrnuje v místě a čase dostupné nástroje. Postupují neorganizovaně a s využitím hrubé síly.

Pakliže jsou bezpečnostní rizika neúmyslná, pak nejsou zatíženy požadavkem konání z vůle člověka. Působit mohou vnitřní vlivy. Do jejich sociální kategorie spadá lidská nedbalost, zapomětlivost a nevědomost. Jiná odnož nastane při nechtěných haváriích technického vybavení uvnitř střeženého prostoru. Neúmyslné vnější ovlivnění má na svědomí přírodní dění (silný vítr, povodně, požáry, zemětřesení aj.). Dále ho může zapříčinit technická havárie či katastrofa vně objektu (požáry, výbuchy, únik radioaktivity, chemické látky v ovzduší, prolomení hrází apod.). I tyto uvedené rizikové elementy vyjadřují značné nebezpečí pro zájem ochrany. Je nutné s nimi počítat a zařadit

[65] KAMPOVÁ, K., LOVEČEK, T. *Modelovanie systémov ochrany objektov a ich optimalizácia.* 1. vydanie. Žilina, 2020, s. 12–17.

je do pracovních etap zpracování poplachových systémů.[66] Ty mají postupné pořadí a jsou následující:

- Plánování – nadchází po ujasnění všech rizik a minimální úrovně ochrany. Určí se cíl, struktura a oblast působnosti.
- Návrh – stanoví typ a umístění ochranných prvků tak, aby se naplnily nároky plánu.
- Instalace – je přímá fyzická realizace navrhovaného zapojení.
- Zprovoznění a ověření funkčnosti – zahájí testovací režim, při kterém se dolaďují instalační vady.
- Schválení protistranou – stvrzuje, že dodaná montáž splňuje poptávané, dohodnuté a objednané vlastnosti.
- Ostrý chod – předává odpovědnost do rukou přebírajícího provozovatele.
- Servis a vylepšování systému – předchází zastarání, nefunkčnosti a zabezpečuje spolehlivý běh, čímž preventivně působí proti narušiteli.[67]

S posledním jmenovanou etapou souvisí zmíněná spolehlivost. Je to pravděpodobnost udávající, že systém bude plnit určené úkoly definované plánem. Jen při zachování tohoto předpokladu lze hovořit o správné funkčnosti. Ta nastává jedině tehdy, když je časový úsek od prvotní detekce narušení delší než dojezdový čas zakročující jednotky. Naplnění této podmínky lze prokázat kvalitativní či kvantitativní cestou. První způsob vychází z neověřitelných odborných odhadů. Druhý si zakládá na nashromáždění měřitelných veličin a následné programové simulaci.[68] Ideální stav je bez poruch. Jakkoliv by to bylo žádoucí, není možné predikovat kdy a kde vznikne závada. Informace od výrobců vycházejí ze všeobecné životnosti zařízení. Pokud jsou ověřovány, děje se tak v ideálním prostoru laboratoře, což výsledek značně zkresluje. Následkem nefunkčnosti dochází k provozním mezerám, které mají vliv na nespolehlivost. Poruchovost se ve sledovaném období počítá jako množství závad za určitý čas. Kromě selhání technického faktoru zasahují do řádného chodu i lidé. Člověk zaostává za strojem převážně v chybovosti svého konání. Nelze předvídat, kdy nastane. Projeví se nepostačující znalostí, nepozorností, nepochopením, fyzickou či duševní nedostatečností,

[66] LOVEČEK, T., REITŠPÍS, J. *Projektovanie a hodnotenie systémov ochrany objektov*. 1. vydanie. Žilina, 2011, s. 39–41.
[67] LOVEČEK, T., MARIŠ, L., ŠISER, A. *Plánovanie a projektovanie systémov ochrany objektov*. 1. vydanie. Žilina, 2018, s. 19.
[68] KAMPOVÁ, K., LOVEČEK, T. *Modelovanie systémov ochrany objektov a ich optimalizácia.* 1. vydanie. Žilina, 2020, s. 17–18.

nedbalostí atd. Hodnocení, jak moc se dá na daného pracovníka spolehnout, nemůže být nikdy úplně uzavřené. Klíčové je poznání jeho povahových vlastností a chování. [69]

Systém sloužící k ochraně majetku musí zcela spolehlivě detekovat neoprávněně vstupující osobu a další vlivy schopné narušit bezpečnost. V jednoduchosti pracuje na principu akce a reakce. Při jeho plánování je podstatné stanovit si zásadní parametr, a to minimální úroveň ochrany. Od ní se odvíjí postup projektanta. Ten ke své práci potřebuje znát požadavky na ochranná opatření, vlastnosti periferií a umístění. Uvedené získá z kombinace těchto zdrojů:

- standardizační normy a obecně závazné právní předpisy,
- vnitrofiremní nařízení,
- smluvní dohoda se zákazníkem nebo účastníkem,
- podmínky pojišťovny.[70]

Například ČSN EN 50131-1 ED.2 rozděluje PZTS do čtyř zabezpečovacích stupňů podle úrovně rizika:

- Nízká – přiznává narušiteli malé vědomosti o nasazené technice. Pro svou protiprávní činnost disponuje běžně dostupným náčiním.
- Nízká až střední – počítá s vyššími znalostmi pachatele a jeho základním vybavením. Má již příruční elektrotechnické pomůcky.
- Střední až vysoká – již znamená úplné seznámení s PZTS a kompletní nástroje pro úspěšné překonání všech bezpečnostních překážek.
- Vysoká – obsahuje prioritu zabezpečenosti, které má přednost před jakýmikoliv ohledy. Protivník má podobu skvěle vybaveného specialisty, jenž koná plánovaně. Vlastní komponenty připravené k záměně prvků PZTS.

Obdobně postupují i další normy. Pro VSS je to ČSN EN 62676-1-1 a u EKV pak ČSN EN 60839-11-1. U nich jsou též 4 stupně zabezpečení a zcela totožné úrovně. Jsou však přidány typové objekty. Proces, při kterém se v kontextu požadavků třetích stran, předpisů, standardů a norem hodnotí zmíněná rizika, se nazývá analýza.[71] Samotné určení

[69] LOVEČEK, T., REITŠPÍS, J. *Projektovanie a hodnotenie systémov ochrany objektov*. 1. vydanie. Žilina, 2011, s. 82–87.
[70] KAMPOVÁ, K., LOVEČEK, T. *Modelovanie systémov ochrany objektov a ich optimalizácia.* 1. vydanie. Žilina, 2020, s. 21–26.
[71] LOVEČEK, T., MARIŠ, L., ŠISER, A. *Plánovanie a projektovanie systémov ochrany objektov*. 1. vydanie. Žilina, 2018, s. 55–63.

rizika se provádí za pomoci výpočtů kombinace pravděpodobnosti vzniku a velikosti způsobených následků. Vstupní informace lze získat induktivně ze statistických údajů obdobných případů nebo expertních odhadů. Z těchto zdrojů se poté pozorováním odvodí obecné závěry. Další možnost představuje dedukce, při které jsou uváženy skutečnosti z minulosti. Z nich se čerpá poučení. Poslední hodnotící technika porovnává shodné dějové znaky, podle kterých se dá předvídat pozdější průběh událostí. Následuje posouzení ke stanovení rizikových úrovní. Metoda kvantitativní je založena na číselném vyjádření existence hrozeb a jejich účinků. Kvalitativní posudek vychází z názorů odborníků. Zde je bohužel nutné počítat s nejednotností výstupů, neboť jsou subjektivní.[72]

Dílčím výsledkem analýzy rizik je stanovení úrovně minimální ochrany. Oba dva procesy přispívají k určení vhodného rozmístění zabezpečovacích prvků. Při něm je potřeba dbát montážních pokynů výrobce, parametrů součástí, norem, standardů a vlivu prostředí. Dále je navrženo technické řešení instalace s možnými variantami. Vznikne bezpečnostní plán či projekt s následujícími částmi, které se však mohou lišit dle požadavků normy příslušného poplachového systému:

- informace o objednavateli i dodavateli,
- popis chráněných zájmů a objektů,
- vyjádření stanovisek z bezpečnostního posouzení,
- charakteristika systému ochrany objektu včetně konfigurace,
- dislokace komponentů a jejich seznam,
- způsob vyhlášení poplachu zahrnující napojení na PCO,
- reakce zakročující jednotky,
- realizace projektu,
- servisní pokyny a údržba,
- návody k obsluze,
- certifikáty nasazených prvků,
- grafické znázornění lokace, budov, vstupů, chráněného prostoru, rozvodů, mechanických zábranných prostředků, PZTS, PPS, VSS, EKV, stanovišť aj.[73]

[72] LOVEČEK, T., REITŠPÍS, J. *Projektovanie a hodnotenie systémov ochrany objektov*. 1. vydanie. Žilina, 2011, s. 192–193.
[73] LOVEČEK, T., MARIŠ, L., ŠISER, A. *Plánovanie a projektovanie systémov ochrany objektov*. 1. vydanie. Žilina, 2018, s. 88–116.

5 Vyhodnocení incidentů vybraných součástí poplachových systémů

Tato kapitola výzkumné části bakalářské práce má za úkol přehledným způsobem znázornit a zhodnotit data, která byla shromážděna z dohledového systému PCO. Za sledované období od 1. 1. 2025 do 31. 3. 2025 bylo u 215 objektů vyhodnoceno 1352 incidentů. Počet posuzovaných prvků poplachových systémů činil 15. Níže uvedené tabulky obsahují roztříděné a statisticky vyjádřené informace, které autor této práce vyhodnotil a dal do empirického kontextu.

Tab. 1: Zabezpečovací ústředna – vyhodnocení incidentů[74]

Identifikace incidentu	Počet případů	Procent z celku			Důvod incidentu	Počet případů	Procent z celku	Řešení incidentu	Počet případů	Procent z celku
Alarm (vyvolaný poruchou)	2	0,9%			Akustický podnět z okolí		0,0%	Elektronická oprava	5	2,1%
Klidový stav (způsobený poruchou)		0,0%			Elektronická závada	1	0,4%	Mechanická oprava	3	1,3%
Neočekávaný restart řídícího procesu	10	4,3%	10		Chyba firmwaru	1	0,4%	Obnova 230 V	17	7,3%
Nepovolené vypnutí	20	8,5%		20	Chyba obsluhy		0,0%	Obnovení spojení	168	71,8%
Osobní identifikace technikem		0,0%			Chybná montáž		0,0%	Odstranění překážky		0,0%
Pokus o neautorizovaný přístup		0,0%			Mechanická závada	3	1,3%	Přehrání firmwaru	3	1,3%
Poplach (vyvolaný uživatelem)		0,0%			Nezjištěn	10	4,3%	Reset zařízení	20	8,5%
Porucha akumulátoru	6	2,6%	5	1	Pachatel		0,0%	Vymazání poplachu	4	1,7%
Porucha integrity databáze ústředny	10	4,3%	10		Překážka (fyzická)		0,0%	Výměna	14	6,0%
Porucha komunikace		0,0%			Sabotáž		0,0%	Změna konfigurace		0,0%
Porucha zdroje	2	0,9%	1	1	Stáří, opotřebování	33	14,1%			
Reset hardwaru (samovolný)		0,0%			Špatná konfigurace		0,0%			
Tamper (sabotážní kontakt/smyčka)	3	1,3%			Teplotní působení		0,0%			
Telefonické nahlášení uživatelem		0,0%			Vliv počasí		0,0%			
Výpadek 230 V	10	4,3%	9	1	Výpadek 230 V	17	7,3%			
Ztráta spojení přes kabelové vedení	101	43,2%	29		Závada na kabelové PPC	98	41,9%			
Ztráta spojení přes rádiový přenos	70	29,9%	10		Závada na rádiové PPC	70	29,9%			
					Závada zdroje	1	0,4%			
					Živočich		0,0%			
Celkem:	**234**	100,0%			**Celkem:**	**234**	100,0%	**Celkem:**	**234**	100,0%
Z toho neporuchových incidentů	**0**									
Z toho poruchových incidentů	**234**									
Z toho s vlivem na nespolehlivost			**74**							
Z toho s vlivem na nefunkčnost				**23**						

V případě zabezpečovací ústředny bylo ve sledovaném období zjištěno 234 incidentů, přičemž všechny spadaly do skupiny poruchových. Největší podíl na nich měla ztráta spojení přes kabelové vedení (101 incidentů, 29 případů s vlivem na nespolehlivost). Na dalším místě se nacházela ztráta spojení přes rádiový přenos (70 incidentů, 10 případů s vlivem na nespolehlivost). Kritériem pro zařazení daného incidentu do nespolehlivostní kategorie poruch bylo stanovení délky ztráty spojení. O spolehlivost se nejedná, jestliže toto komunikační pozbytí probíhalo v řádu hodin

[74] Vlastní zdroj.

a zároveň byla závada pouze na jedné z PPC (hlavní – rádiová, vedlejší – kabelová). Nejčastějším řešením je obnovení spojení. Nepovolené vypnutí (20 incidentů, 20 případů s vlivem na nefunkčnost) je nejzávažnějším druhem incidentu u této periferie. Pokud se objeví, tak vždy znamená nutnost okamžitého servisního zásahu, neboť zabezpečovací ústředna je v podstatě centrálním řídícím počítačem poplachového systému v daném místě. Důvodem tohoto stavu je stáří/opotřebování či dlouhodobý výpadek napětí 230 V, který nepokryje akumulátor. Pakliže nedojde k nápravě obnovením 230 V, je nezbytné sáhnout k výměně zařízení. Neočekávaný restart řídícího procesu (10 incidentů, 10 případů s vlivem na nespolehlivost) značí nežádoucí vnitřní chybu programového vybavení ústředny, která ji činí nespolehlivou, neboť v průběhu restartu neplní svoji funkci. Příčinou bývá stáří/opotřebování, nebo se důvod nezjistí. Když dochází k opakování, je nutná výměna. Porucha integrity databáze ústředny (10 incidentů, 10 případů s vlivem na nespolehlivost) znamená narušení nahraného seznamu uživatelů, bez něhož systém EKV nedokáže rozpoznat oprávněného uživatele. Příčinou této poruchy je opotřebování flash paměti ústředny. Když nepomůže přehrání databáze, je nezbytné úložiště vyměnit. Výpadek 230 V (10 incidentů, 9 případů s vlivem na nespolehlivost, 1 případ s vlivem na nefunkčnost) přináší vždy komplikace pro fungování ústředny. Pokud je akumulátor v pořádku a nedojde k vypnutí, je incident vyhodnocen s vlivem na nespolehlivost. Jakmile je znemožněn přísun síťového napětí na dlouhou dobu a dojde k vybití náhradního zdroje, ústředna se vypne a tento případ je nutné zařadit do kategorie s vlivem na nefunkčnost. Řešením je obnova 230 V, kontrola akumulátoru a jeho případná výměna. S tím souvisí i jeho porucha (6 incidentů, 5 případů s vlivem na nespolehlivost, 1 případ s vlivem na nefunkčnost). Pokud je zdrojem na svorkách akumulátoru zjištěno příliš malé napětí, tak dojde k vyhlášení poruchového stavu. Vždy má vliv na nespolehlivost. Když nastane silné podbití, kdy akumulátor již nedokáže vůbec plnit svoji funkci, má stav v kombinaci s výpadkem 230 V následek v podobě vypnutí ústředny a nefunkčnosti celého systému. Jako prevence těchto situací slouží pravidelné revize, při kterých je náhradní zdroj měřen a případně vyměněn. Porucha zdroje (2 incidenty, 1 případ s vlivem na nespolehlivost, 1 případ s vlivem na funkčnost) nastane, jestliže je na jeho výstupních svorkách naměřeno neadekvátní napětí. Vždy to snižuje spolehlivost daného systému, jelikož zdroj napájí i další periferie. Při výskytu hodnot napájecího napětí, se kterými ústředna a připojené prvky nedokázaly plnit svoji funkci, byl incident zařazen do vlivu na nefunkčnost. Řešením je elektronická oprava nebo výměna. Tamper (3 incidenty) představuje mechanickou závadu kontaktu mikrospínače. Jako náprava postačí jeho přihnutí. Příčina alarmu, který vyvolala porucha

(2 incidenty), bývá bez zásahu servisu výrobce velice špatně diagnostikována. Jako možnost opravy se nabízí přehrání firmware. Pokud se po vymazání poplachu závada znovu objeví, je nutná elektronická oprava. Po vyhodnocení dat z PCO byly u zabezpečovací ústředny jako důvody incidentů, které mají vliv na nespolehlivost či nefunkčnost, zjištěny následující: stáří/opotřebování, výpadek 230 V a závady na PPC.

Tab. 2: Expandér – vyhodnocení incidentů[75]

Identifikace incidentu	Počet případů	Procent z celku			Důvod incidentu	Počet případů	Procent z celku	Řešení incidentu	Počet případů	Procent z celku
Alarm (vyvolaný poruchou)		0,0%			Akustický podnět z okolí		0,0%	Elektronická oprava	7	50,0%
Klidový stav (způsobený poruchou)		0,0%			Elektronická závada		0,0%	Mechanická oprava	1	7,1%
Neočekávaný restart řídícího procesu		0,0%			Chyba firmwaru		0,0%	Obnova 230 V	2	14,3%
Nepovolené vypnutí		0,0%			Chyba obsluhy		0,0%	Obnovení spojení		0,0%
Osobní identifikace technikem		0,0%			Chybná montáž	7	50,0%	Odstranění překážky		0,0%
Pokus o neautorizovaný přístup		0,0%			Mechanická závada	1	7,1%	Přehrání firmwaru		0,0%
Poplach (vyvolaný uživatelem)		0,0%			Nezjištěn	1	7,1%	Reset zařízení	1	7,1%
Porucha akumulátoru		0,0%			Pachatel		0,0%	Vymazání poplachu		0,0%
Porucha integrity databáze ústředny		0,0%			Překážka (fyzická)		0,0%	Výměna		0,0%
Porucha komunikace	13	92,9%	3	10	Sabotáž		0,0%	Změna konfigurace	3	21,4%
Porucha zdroje		0,0%			Stáří, opotřebování		0,0%			
Reset hardwaru (samovolný)		0,0%			Špatná konfigurace	3	21,4%			
Tamper (sabotážní kontakt/smyčka)	1	7,1%			Teplotní působení		0,0%			
Telefonické nahlášení uživatelem		0,0%			Vliv počasí		0,0%			
Výpadek 230 V		0,0%			Výpadek 230 V	2	14,3%			
Ztráta spojení přes kabelové vedení		0,0%			Závada na kabelové PPC		0,0%			
Ztráta spojení přes rádiový přenos		0,0%			Závada na rádiové PPC		0,0%			
					Závada zdroje		0,0%			
					Živočich		0,0%			
Celkem:	**14**	100,0%			**Celkem:**	**14**	100,0%	**Celkem:**	**14**	100,0%
Z toho neporuchových incidentů	**0**									
Z toho poruchových incidentů	**14**									
Z toho s vlivem na nespolehlivost			**3**							
Z toho s vlivem na nefunkčnost				**10**						

U expandéru bylo zjištěno 14 incidentů, z nichž všechny patřily do poruchové kategorie. Nejvíce výskytů měla porucha komunikace (13 incidentů, 3 případy s vlivem na nespolehlivost, 10 případů s vlivem na nefunkčnost). Tato závada je vždy vážná, jelikož dojde k přerušení komunikačního toku mezi modulem a ústřednou. Ta by tak nezaznamenala případné poplachy z detektorů, které jsou na expandér připojeny. Pokud byla porucha přerušovaná v krátkých intervalech (v řádu vteřin) a následně ustala, tak byl incident vyhodnocen s vlivem na nespolehlivost. Pakliže se jednalo o stálý stav, případ se zařadil mezi ty, které mají vliv na nefunkčnost. Příčinami tohoto stavu jsou chybná montáž (uvolněné vodiče ve svorkovnici, neprůchozí linka apod.), špatná konfigurace modulu či výpadek 230 V. K nápravě postačí jeho obnova, úprava konfigurace nebo elektronická oprava. Další možností je provedení resetu v situaci, kdy se důvod nezjistí.

[75] Vlastní zdroj.

Tamper (1 incident) je mechanická porucha sabotážního kontaktu krytu modulu, která se řeší jednoduchým přihnutím plíšku mikrospínače. Po vyhodnocení dat z PCO byly u expandéru jako důvody incidentů, které mají vliv na nespolehlivost či nefunkčnost, zjištěny následující: chybná montáž, špatná konfigurace a výpadek 230 V.

Tab. 3: Posilovací zdroj – vyhodnocení incidentů[76]

Identifikace incidentu	Počet případů	Procent z celku			Důvod incidentu	Počet případů	Procent z celku	Řešení incidentu	Počet případů	Procent z celku
Alarm (vyvolaný poruchou)		0,0%			Akustický podnět z okolí		0,0%	Elektronická oprava		0,0%
Klidový stav (způsobený poruchou)		0,0%			Elektronická závada		0,0%	Mechanická oprava		0,0%
Neočekávaný restart řídícího procesu		0,0%			Chyba firmwaru		0,0%	Obnova 230 V	9	75,0%
Nepovolené vypnutí		0,0%			Chyba obsluhy		0,0%	Obnovení spojení		0,0%
Osobní identifikace technikem		0,0%			Chybná montáž		0,0%	Odstranění překážky		0,0%
Pokus o neautorizovaný přístup		0,0%			Mechanická závada		0,0%	Přehrání firmwaru		0,0%
Poplach (vyvolaný uživatelem)		0,0%			Nezjištěn		0,0%	Reset zařízení		0,0%
Porucha akumulátoru	3	25,0%	3		Pachatel		0,0%	Vymazání poplachu		0,0%
Porucha integrity databáze ústředny		0,0%			Překážka (fyzická)		0,0%	Výměna	3	25,0%
Porucha komunikace		0,0%			Sabotáž		0,0%	Změna konfigurace		0,0%
Porucha zdroje		0,0%			Stáří, opotřebování	3	25,0%			
Reset hardwaru (samovolný)		0,0%			Špatná konfigurace		0,0%			
Tamper (sabotážní kontakt/smyčka)		0,0%			Teplotní působení		0,0%			
Telefonické nahlášení uživatelem		0,0%			Vliv počasí		0,0%			
Výpadek 230 V	9	75,0%	9		Výpadek 230 V	9	75,0%			
Ztráta spojení přes kabelové vedení		0,0%			Závada na kabelové PPC		0,0%			
Ztráta spojení přes rádiový přenos		0,0%			Závada na rádiové PPC		0,0%			
					Závada zdroje		0,0%			
					Živočich		0,0%			
Celkem:	**12**	100,0%			**Celkem:**	**12**	100,0%	**Celkem:**	**12**	100,0%
Z toho neporuchových incidentů	**0**									
Z toho poruchových incidentů	**12**									
Z toho s vlivem na nespolehlivost			**12**							
Z toho s vlivem na nefunkčnost				**0**						

Posilovací zdroj vykazoval ve sledovaném období 12 incidentů. Všechny byly poruchové. Nejčastěji se objevoval výpadek 230 V (9 incidentů, 9 případů s vlivem na nespolehlivost). Pokud nedošlo ke kombinaci s poruchou akumulátoru, byla do jeho vybití ohrožena pouze spolehlivost. Příčinou i řešením je stabilita přísunu elektrické energie v místě instalace. Porucha akumulátoru (3 incidenty, 3 případy s vlivem na nespolehlivost) nastává při jeho opotřebování či vlivem stáří. Opět platí, že když současně nedojde i k výpadku síťového napětí 230 V, jedná se pouze o ohrožení spolehlivosti. Zařízení funguje dál až do úplného vybití. Následně by nastala nefunkčnost. Řešením je výměna za nový náhradní zdroj. Po vyhodnocení dat z PCO byly u posilovacího zdroje jako důvody incidentů, které mají vliv na nespolehlivost, zjištěny následující: stáří/opotřebování a výpadek 230 V.

[76] Vlastní zdroj.

Tab. 4: Ovládací klávesnice – vyhodnocení incidentů[77]

Identifikace incidentu	Počet případů	Procent z celku			Důvod incidentu	Počet případů	Procent z celku	Řešení incidentu	Počet případů	Procent z celku
Alarm (vyvolaný poruchou)		0,0%			Akustický podnět z okolí		0,0%	Elektronická oprava	2	8,7%
Klidový stav (způsobený poruchou)		0,0%			Elektronická závada		0,0%	Mechanická oprava		0,0%
Neočekávaný restart řídícího procesu		0,0%			Chyba firmwaru	2	8,7%	Obnova 230 V		0,0%
Nepovolené vypnutí		0,0%			Chyba obsluhy	8	34,8%	Obnovení spojení		0,0%
Osobní identifikace technikem		0,0%			Chybná montáž		0,0%	Odstranění překážky		0,0%
Pokus o neautorizovaný přístup	9	39,1%			Mechanická závada		0,0%	Přehrání firmwaru	2	8,7%
Poplach (vyvolaný uživatelem)		0,0%			Nezjištěn	10	43,5%	Reset zařízení	1	4,3%
Porucha akumulátoru		0,0%			Pachatel		0,0%	Vymazání poplachu	17	73,9%
Porucha integrity databáze ústředny		0,0%			Překážka (fyzická)		0,0%	Výměna		0,0%
Porucha komunikace	14	60,9%			Sabotáž		0,0%	Změna konfigurace	1	4,3%
Porucha zdroje		0,0%			Stáří, opotřebování		0,0%			
Reset hardwaru (samovolný)		0,0%			Špatná konfigurace	1	4,3%			
Tamper (sabotážní kontakt/smyčka)		0,0%			Teplotní působení		0,0%			
Telefonické nahlášení uživatelem		0,0%			Vliv počasí		0,0%			
Výpadek 230 V		0,0%			Výpadek 230 V		0,0%			
Ztráta spojení přes kabelové vedení		0,0%			Závada na kabelové PPC		0,0%			
Ztráta spojení přes rádiový přenos		0,0%			Závada na rádiové PPC		0,0%			
					Závada zdroje	2	8,7%			
					Živočich		0,0%			
Celkem:	**23**	100,0%			**Celkem:**	**23**	100,0%	**Celkem:**	**23**	100,0%
Z toho neporuchových incidentů	**9**									
Z toho poruchových incidentů	**14**									
Z toho s vlivem na nespolehlivost			**0**							
Z toho s vlivem na nefunkčnost				**0**						

Ovládací klávesnice zaslala na PCO prostřednictvím ústředny a PPZ celkem 23 incidentů. Porucha komunikace (14 incidentů) představovala ve všech výskytech závady. Důvody se buď nepodařilo zjistit, anebo se jednalo o chybu firmwaru, konfigurace či závadu zdroje (respektive veliký úbytek napětí na vedení). Zmíněný výčet zapříčinil, že se klávesnice nesprávně dorozumívala s ústřednou. Řešení poskytuje přehrání programového vybavení klávesnice, reset zařízení, elektronická oprava, posílení průřezů vodičů vedení nebo nasazení posilovacího zdroje. U nezjištěné příčiny se po fyzické kontrole v místě vyhlášení poplach pouze vymaže a sleduje se případné opakování události. Pokus o neautorizovaný přístup (9 incidentů) je správně signalizovaný stav, jenž není poruchový. Způsobí ho chyba obsluhy, která opakovaně zadává špatné autentizační heslo. Po ověření jestli se nejedná o pokus narušitele vniknout do zastřeženého místa, je poplach vymazán. Děje se tak i v situaci, kdy se nepodaří viníka zjistit. Po vyhodnocení dat z PCO nebyly u ovládací klávesnice zjištěny žádné důvody pro zařazení incidentů do kategorie s vlivem na nespolehlivost či nefunkčnost.

[77] Vlastní zdroj.

Tab. 5: Magnetický kontakt – vyhodnocení incidentů[78]

Identifikace incidentu	Počet případů	Procent z celku			Důvod incidentu	Počet případů	Procent z celku	Řešení incidentu	Počet případů	Procent z celku
Alarm (vyvolaný poruchou)	32	18,5%	10	1	Akustický podnět z okolí		0,0%	Elektronická oprava	2	1,2%
Klidový stav (způsobený poruchou)	1	0,6%		1	Elektronická závada	2	1,2%	Mechanická oprava	13	7,5%
Neočekávaný restart řídícího procesu		0,0%			Chyba firmwaru		0,0%	Obnova 230 V		0,0%
Nepovolené vypnutí		0,0%			Chyba obsluhy	138	79,8%	Obnovení spojení		0,0%
Osobní identifikace technikem		0,0%			Chybná montáž	6	3,5%	Odstranění překážky		0,0%
Pokus o neautorizovaný přístup		0,0%			Mechanická závada	6	3,5%	Přehrání firmwaru		0,0%
Poplach (vyvolaný uživatelem)	138	79,8%			Nezjištěn	8	4,6%	Reset zařízení		0,0%
Porucha akumulátoru		0,0%			Pachatel		0,0%	Vymazání poplachu	157	90,8%
Porucha integrity databáze ústředny		0,0%			Překážka (fyzická)		0,0%	Výměna	1	0,6%
Porucha komunikace		0,0%			Sabotáž	1	0,6%	Změna konfigurace		0,0%
Porucha zdroje		0,0%			Stáří, opotřebování	1	0,6%			
Reset hardwaru (samovolný)		0,0%			Špatná konfigurace		0,0%			
Tamper (sabotážní kontakt/smyčka)	2	1,2%		2	Teplotní působení	3	1,7%			
Telefonické nahlášení uživatelem		0,0%			Vliv počasí	8	4,6%			
Výpadek 230 V		0,0%			Výpadek 230 V		0,0%			
Ztráta spojení přes kabelové vedení		0,0%			Závada na kabelové PPC		0,0%			
Ztráta spojení přes rádiový přenos		0,0%			Závada na rádiové PPC		0,0%			
					Závada zdroje		0,0%			
					Živočich		0,0%			
Celkem:	**173**	100,0%			**Celkem:**	**173**	100,0%	**Celkem:**	**173**	100,0%
Z toho neporuchových incidentů	**138**									
Z toho poruchových incidentů	**35**									
Z toho s vlivem na nespolehlivost			**10**							
Z toho s vlivem na nefunkčnost				**4**						

U magnetického kontaktu nastalo 173 incidentů. Celkem 138 z nich bylo vyvoláno uživatelem, který zařízení chybně obsluhoval tím, že daný podsystém před vstupem neodstřežil. Tyto případy značily správnou reakci prvku ochrany a byly zařazeny mezi neporuchové. Po kontrole ze strany PCO se jejich poplachy ze systému pouze vymazaly. Poruchové situace vznikly ve 35 případech. Alarm vyvolaný závadou (32 incidentů, 10 případů s vlivem na nespolehlivost, 1 případ s vlivem na nefunkčnost) značí poplach, který není vyvolaný narušitelem. Způsobuje ho stáří/opotřebování feritu, což snižuje spolehlivost. Je nutná jeho výměna. Pokud je příčinou chybná montáž, kdy vzdálenost obou částí magnetického kontaktu neodpovídá instalačním pokynům, zařízení nefunguje spolehlivě. K vyvolání poplachového stavu pak stačí i malé prohnutí dveří nebo okna. Je nutná mechanická oprava v podobě přemístění. Obdobné může nastat i v případě poškození samotného pouzdra či uchycení. V kombinaci se správnou montáží má vliv také působení počasí a teplot. Průvan a silný vítr způsobují pohyb výplní. Změny teplo/zima působí na materiál (dřevo, plast i kov). Ten má tendence se nepatrně ohýbat, rozpínat nebo naopak smršťovat. Pakliže je vzdálenost protikusů hraniční, může být těmito vlivy rozpojena poplachová smyčka. V tomto případě se jako vhodné řešení nabízí pouhé vymazání vyvolaného stavu ze zařízení a sledování opakování situace. Některé

[78] Vlastní zdroj.

důvody incidentů se nepodaří odhalit. Pokud nedojde k jejich opakování, poplachy se pouze vymažou. Tamper u magnetického kontaktu (2 incidenty, 2 případy s vlivem na nefunkčnost) značí přerušení sabotážní smyčky. Tuto je nutno opětovně propojit. V opačném případě by takovýto prvek ochrany nefungoval. Klidový stav, který způsobila porucha (1 incident, 1 případ s vlivem na nefunkčnost), nastává v případě, kdy u prvku nedojde k řádnému rozpojení poplachové smyčky a tato zůstane nesprávně v sepnutém klidovém stavu. Velice negativní jev skrývá sabotáž. Ze strany oprávněného uživatele nastává tehdy, když vyndá ferit z pohyblivé části výplně a nedovoleně ho přiloží k pevně instalované části magnetického kontaktu. Podsystém je pak možno zastřežit, ačkoliv nejsou všechny smyčky v klidovém stavu. Je vhodné, aby technik takovouto situaci zapsal do knihy provozu PZTS, jelikož má značný vliv na nefunkčnost zabezpečení daného objektu. Oprava je následně mechanického rázu. Po vyhodnocení dat z PCO byly u magnetického kontaktu jako důvody incidentů, které mají vliv na nespolehlivost či nefunkčnost, zjištěny následující: chybná montáž, stáří/opotřebování, sabotáž, mechanická a elektronická závada.

Tab. 6: Rozvodná krabice – vyhodnocení incidentů[79]

Identifikace incidentu	Počet případů	Procent z celku			Důvod incidentu	Počet případů	Procent z celku	Řešení incidentu	Počet případů	Procent z celku
Alarm (vyvolaný poruchou)		0,0%			Akustický podnět z okolí		0,0%	Elektronická oprava		0,0%
Klidový stav (způsobený poruchou)		0,0%			Elektronická závada		0,0%	Mechanická oprava	3	50,0%
Neočekávaný restart řídícího procesu		0,0%			Chyba firmwaru		0,0%	Obnova 230 V		0,0%
Nepovolené vypnutí		0,0%			Chyba obsluhy		0,0%	Obnovení spojení		0,0%
Osobní identifikace technikem		0,0%			Chybná montáž	1	16,7%	Odstranění překážky		0,0%
Pokus o neautorizovaný přístup		0,0%			Mechanická závada	3	50,0%	Přehrání firmwaru		0,0%
Poplach (vyvolaný uživatelem)		0,0%			Nezjištěn	1	16,7%	Reset zařízení		0,0%
Porucha akumulátoru		0,0%			Pachatel		0,0%	Vymazání poplachu	1	16,7%
Porucha integrity databáze ústředny		0,0%			Překážka (fyzická)		0,0%	Výměna	1	16,7%
Porucha komunikace		0,0%			Sabotáž		0,0%	Změna konfigurace	1	16,7%
Porucha zdroje		0,0%			Stáří, opotřebování		0,0%			
Reset hardwaru (samovolný)		0,0%			Špatná konfigurace		0,0%			
Tamper (sabotážní kontakt/smyčka)	6	100,0%		6	Teplotní působení	1	16,7%			
Telefonické nahlášení uživatelem		0,0%			Vliv počasí		0,0%			
Výpadek 230 V		0,0%			Výpadek 230 V		0,0%			
Ztráta spojení přes kabelové vedení		0,0%			Závada na kabelové PPC		0,0%			
Ztráta spojení přes rádiový přenos		0,0%			Závada na rádiové PPC		0,0%			
					Závada zdroje		0,0%			
					Živočich		0,0%			
Celkem:	**6**	100,0%			**Celkem:**	**6**	100,0%	**Celkem:**	**6**	100,0%
Z toho neporuchových incidentů	**0**									
Z toho poruchových incidentů	**6**									
Z toho s vlivem na nespolehlivost				**0**						
Z toho s vlivem na nefunkčnost				**6**						

Ve sledovaném období se u rozvodné krabice vyskytlo 6 incidentů. Veškeré případy byly poruchové a spadaly do kategorie s vlivem na nefunkčnost. RKZ plní funkci

[79] Vlastní zdroj.

propojovacího bodu vodičů. Při použití pro PZTS je chráněna tamperem. Ten je v případě tohoto výzkumu dominující závadou (6 incidentů, 6 případů s vlivem na nefunkčnost). Jakmile dojde k rozpojení sabotážní smyčky, zabezpečovací ústředna již nedokáže vyhodnocovat stavy připojených detektorů, jelikož obvod v té chvíli není uzavřen. Důvody jsou různé. Mechanickou závadu reprezentuje nedostatečně uzavřený kryt krabice. Řešením je řádně dotáhnout jeho šrouby. Tomuto kroku samozřejmě předchází kontrola výskytu mechanické překážky mezi víčkem a spodní částí. Za chybnou montáž lze označit vadný spoj vodiče se svorkovnicí. K vyřešení postačí plošku a drát pečlivě proletovat či utáhnout šroub. Jestliže jsou špatně nastavené hodnoty odporového vyvážení, je nutné provést jejich úpravu formou změny konfigurace. RKZ není vhodné vystavovat přímému slunečnímu svitu. Plast, ze kterého jsou vyrobeny, se dokáže při dlouhodobém působení tepla zkroutit, čímž se horní kryt odchýlí. Tím dojde k aktivaci tamperu. U takovýchto situací je vhodná výměna za nový kus a změna umístění. Poplachy z nezjištěných důvodů se po prověření vymažou a stav se dále sleduje. Po vyhodnocení dat z PCO byly u RKZ jako důvody incidentů, které mají vliv na nefunkčnost, zjištěny následující: mechanická závada, chybná montáž, teplotní působení a nezjištěné příčiny.

Tab. 7: Pohybové čidlo – vyhodnocení incidentů[80]

Identifikace incidentu	Počet případů	Procent z celku			Důvod incidentu	Počet případů	Procent z celku	Řešení incidentu	Počet případů	Procent z celku
Alarm (vyvolaný poruchou)	61	27,2%	10	1	Akustický podnět z okolí		0,0%	Elektronická oprava	6	2,7%
Klidový stav (způsobený poruchou)		0,0%			Elektronická závada	11	4,9%	Mechanická oprava	5	2,2%
Neočekávaný restart řídícího procesu		0,0%			Chyba firmwaru		0,0%	Obnova 230 V		0,0%
Nepovolené vypnutí		0,0%			Chyba obsluhy	159	71,0%	Obnovení spojení		0,0%
Osobní identifikace technikem		0,0%			Chybná montáž	1	0,4%	Odstranění překážky	9	4,0%
Pokus o neautorizovaný přístup		0,0%			Mechanická závada	4	1,8%	Přehrání firmwaru		0,0%
Poplach (vyvolaný uživatelem)	159	71,0%			Nezjištěn	16	7,1%	Reset zařízení	1	0,4%
Porucha akumulátoru		0,0%			Pachatel		0,0%	Vymazání poplachu	194	86,6%
Porucha integrity databáze ústředny		0,0%			Překážka (fyzická)	6	2,7%	Výměna	8	3,6%
Porucha komunikace		0,0%			Sabotáž		0,0%	Změna konfigurace	1	0,4%
Porucha zdroje		0,0%			Stáří, opotřebování	3	1,3%			
Reset hardwaru (samovolný)		0,0%			Špatná konfigurace	1	0,4%			
Tamper (sabotážní kontakt/smyčka)	4	1,8%		4	Teplotní působení	2	0,9%			
Telefonické nahlášení uživatelem		0,0%			Vliv počasí		0,0%			
Výpadek 230 V		0,0%			Výpadek 230 V		0,0%			
Ztráta spojení přes kabelové vedení		0,0%			Závada na kabelové PPC		0,0%			
Ztráta spojení přes rádiový přenos		0,0%			Závada na rádiové PPC		0,0%			
					Závada zdroje		0,0%			
					Živočich	21	9,4%			
Celkem:	**224**	100,0%			**Celkem:**	**224**	100,0%	**Celkem:**	**224**	100,0%
Z toho neporuchových incidentů	**159**									
Z toho poruchových incidentů	**65**									
Z toho s vlivem na nespolehlivost			**10**							
Z toho s vlivem na nefunkčnost				**5**						

[80] Vlastní zdroj.

V 1. čtvrtletí roku 2025 zaznamenal PCO 224 incidentů, které se týkaly pohybového čidla. Celkem 159 z nich vyvolal uživatel chybným obsluhováním, jelikož před vstupem neprovedl odstřežení zabezpečeného podsystému. Tím de facto způsobil nechtěnou zkoušku správné funkčnosti. Takovéto případy jsou neporuchové a poplach je pouze vymazán. Porucha se vyskytla u 65 incidentů. Jejím následkem byl vyvolán alarm (61 incidentů, 10 případů s vlivem na nespolehlivost, 1 případ s vlivem na nefunkčnost). Mezi jeho příčiny se řadí elektronická porucha, která může mít podobu špatného odporového vyvážení, nevyhovující citlivosti či selhání elektroniky. Řešením je elektronická oprava v místě instalace. Případná výměna nastává až po vyčerpání všech variant servisních zásahů, včetně resetu. Chybnou montáž lze napravit mechanickou opravou nebo přemístěním. Špatnou konfiguraci vyřeší technik patřičnou změnou v programu ústředny. U starého/opotřebovaného pohybového čidla je nejlepším řešením jeho výměna. Dalším důvodem alarmu (vyvolaným poruchou) je přítomnost různých živočichů (myš, kočka, nutrie, vydra aj.), kteří v zastřežené zóně nechtěně spustí poplach. Pokud se jedná o ojedinělý výskyt, postačí poplach vymazat a sledovat jeho opakování. Pakliže k němu dojde, je potřeba tento nežádoucí stav řešit změnou citlivosti čidla. Dále je možné zvážit výměnu za duální typ (PIR + MW, PIR + US). Pavouk visící před čočkou tvoří překážku a je nutné ho fyzicky odstranit. Identicky se postupuje i u jiných bariér, které uživatel postaví mezi detektor a prostor, jenž má za úkol zabezpečit. Teplotní působení (přímý sluneční svit, klimatizace, topení apod.) může vyvolat nežádoucí poplach. Tato situace vyjadřuje špatné umístění čidla. Je vhodné ho nainstalovat na jinou pozici. Alternativu nabízí nasazení duální varianty. U neopakovaného výskytu postačí vymazání poplachu a sledování recidivy. Nezjištěné důvody incidentu vyžadují následnou kontrolu v místě události a sledování ze strany technika. Když nedojde k opětovnému poplachu, je možné ho jen vymazat. Aktivace tamperu (4 incidenty, 4 případy s vlivem na nefunkčnost) u pohybového čidla znamená vždy poruchu ovlivňující fungování prvku. Smyčka je tím přerušena a do zabezpečovací ústředny nemohou dorazit změny stavů daného detektoru. Důvod představuje mechanická závada, která se opraví napružením sabotážního kontaktu a důkladným uzavřením krytu. Po vyhodnocení dat z PCO byly u pohybového čidla jako důvody incidentů, které mají vliv na nespolehlivost či nefunkčnost, zjištěny následující: chybná montáž, fyzická překážka, stáří/opotřebování, elektronická a mechanická závada.

Tab. 8: Akustický detektor rozbití skla – vyhodnocení incidentů[81]

Identifikace incidentu	Počet případů	Procent z celku			Důvod incidentu	Počet případů	Procent z celku	Řešení incidentu	Počet případů	Procent z celku
Alarm (vyvolaný poruchou)	30	90,9%	1	1	Akustický podnět z okolí	24	72,7%	Elektronická oprava		0,0%
Klidový stav (způsobený poruchou)		0,0%			Elektronická závada	1	3,0%	Mechanická oprava	1	3,0%
Neočekávaný restart řídícího procesu		0,0%			Chyba firmwaru		0,0%	Obnova 230 V		0,0%
Nepovolené vypnutí		0,0%			Chyba obsluhy	1	3,0%	Obnovení spojení		0,0%
Osobní identifikace technikem		0,0%			Chybná montáž		0,0%	Odstranění překážky		0,0%
Pokus o neautorizovaný přístup		0,0%			Mechanická závada	1	3,0%	Přehrání firmwaru		0,0%
Poplach (vyvolaný uživatelem)	1	3,0%			Nezjištěn	3	9,1%	Reset zařízení		0,0%
Porucha akumulátoru		0,0%			Pachatel		0,0%	Vymazání poplachu	28	84,8%
Porucha integrity databáze ústředny		0,0%			Překážka (fyzická)		0,0%	Výměna	2	6,1%
Porucha komunikace		0,0%			Sabotáž		0,0%	Změna konfigurace	2	6,1%
Porucha zdroje		0,0%			Stáří, opotřebování	1	3,0%			
Reset hardwaru (samovolný)		0,0%			Špatná konfigurace	2	6,1%			
Tamper (sabotážní kontakt/smyčka)	2	6,1%		2	Teplotní působení		0,0%			
Telefonické nahlášení uživatelem		0,0%			Vliv počasí		0,0%			
Výpadek 230 V		0,0%			Výpadek 230 V		0,0%			
Ztráta spojení přes kabelové vedení		0,0%			Závada na kabelové PPC		0,0%			
Ztráta spojení přes rádiový přenos		0,0%			Závada na rádiové PPC		0,0%			
					Závada zdroje		0,0%			
					Živočich		0,0%			
Celkem:	**33**	100,0%			**Celkem:**	**33**	100,0%	**Celkem:**	**33**	100,0%
Z toho neporuchových incidentů	**1**									
Z toho poruchových incidentů	**32**									
Z toho s vlivem na nespolehlivost			**1**							
Z toho s vlivem na nefunkčnost				**3**						

U akustického detektoru rozbití skla bylo zjištěno 33 incidentů. Chyba obsluhy, která vyvolala neporuchový poplach, nastala v jediném případu. Alarm byl PCO zaznamenán u 30 poruch (1 případ s vlivem na nespolehlivost, 1 případ s vlivem na nefunkčnost). Hlavní spouštěč představoval akustický podnět z okolí (zábavní pyrotechnika, stavební práce apod.). Ojedinělý výskyt nepředstavuje problém. Provede se kontrola ze strany pověřené osoby. Jestliže není objeveno narušení, je možné poplach stejně jako u nezjištěných důvodů vymazat. Stav se poté sleduje pro případné nežádoucí opakování. Jakmile by nastalo, je potřeba provést snížení citlivosti mikrofonu ve vztahu k vstupnímu akustickému aktivátoru. Špatně nakonfigurované parametry smyčky vyřeší technik jejich změnou v programovém vybavení zabezpečovací ústředny. Nutnou výměnu značí staré/opotřebované instalace, které cyklicky spouští alarm a servisní zásah nedosáhl žádaného pozitivního účinku. Důvody tamperu (2 incidenty, 2 případy s vlivem na nefunkčnost) lze rozdělit na mechanické (uvolněný kryt, nedostatečné stisknutí sabotážního kontaktu, přerušené vedení atd.) a elektronické (porucha spínače). Následuje pokus o opravu. Pokud tím není příčina odstraněna, je nezbytné přikročit k výměně za nový kus. Po vyhodnocení dat z PCO byly u akustického detektoru rozbití skla jako

[81] Vlastní zdroj.

důvody incidentů, které mají vliv na nespolehlivost či nefunkčnost, zjištěny následující: stáří/opotřebování, špatná konfigurace, elektronická a mechanická závada.

Tab. 9: Tísňový hlásič – vyhodnocení incidentů[82]

Identifikace incidentu	Počet případů	Procent z celku		Důvod incidentu	Počet případů	Procent z celku	Řešení incidentu	Počet případů	Procent z celku
Alarm (vyvolaný poruchou)	4	26,7%	3	Akustický podnět z okolí		0,0%	Elektronická oprava	1	6,7%
Klidový stav (způsobený poruchou)		0,0%		Elektronická závada		0,0%	Mechanická oprava	3	20,0%
Neočekávaný restart řídícího procesu		0,0%		Chyba firmwaru		0,0%	Obnova 230 V		0,0%
Nepovolené vypnutí		0,0%		Chyba obsluhy	10	66,7%	Obnovení spojení		0,0%
Osobní identifikace technikem		0,0%		Chybná montáž	2	13,3%	Odstranění překážky		0,0%
Pokus o neautorizovaný přístup		0,0%		Mechanická závada	2	13,3%	Přehrání firmwaru		0,0%
Poplach (vyvolaný uživatelem)	11	73,3%		Nezjištěn		0,0%	Reset zařízení		0,0%
Porucha akumulátoru		0,0%		Pachatel	1	6,7%	Vymazání poplachu	11	73,3%
Porucha integrity databáze ústředny		0,0%		Překážka (fyzická)		0,0%	Výměna		0,0%
Porucha komunikace		0,0%		Sabotáž		0,0%	Změna konfigurace		0,0%
Porucha zdroje		0,0%		Stáří, opotřebování		0,0%			
Reset hardwaru (samovolný)		0,0%		Špatná konfigurace		0,0%			
Tamper (sabotážní kontakt/smyčka)		0,0%		Teplotní působení		0,0%			
Telefonické nahlášení uživatelem		0,0%		Vliv počasí		0,0%			
Výpadek 230 V		0,0%		Výpadek 230 V		0,0%			
Ztráta spojení přes kabelové vedení		0,0%		Závada na kabelové PPC		0,0%			
Ztráta spojení přes rádiový přenos		0,0%		Závada na rádiové PPC		0,0%			
				Závada zdroje		0,0%			
				Živočich		0,0%			
Celkem:	**15**	100,0%		**Celkem:**	**15**	100,0%	**Celkem:**	**15**	100,0%
Z toho neporuchových incidentů	**11**								
Z toho poruchových incidentů	**4**								
Z toho s vlivem na nespolehlivost			**3**						
Z toho s vlivem na nefunkčnost			**0**						

Tísňový hlásič vykazoval ve sledovaném období 15 incidentů. Z nich bylo 11 neporuchových. Vyvolal je uživatel chybnou obsluhou (nechtěnou aktivací) nebo při konfliktní situaci s osobou, která představovala nebezpečí. Ve všech případech musí nastat okamžitá reakce ze strany PCO. V souvislosti s použitím tísňového hlásiče lze předpokládat ohrožení života či zdraví. Je nutná opravdu důsledná kontrola pověřených pracovníků s přihlédnutím k faktu, že v blízkosti uživatele může stát pachatel. Pokud je vše v pořádku, tak se prvek uvede do klidového stavu spolu s vymazáním poplachu. Poruchové incidenty, které aktivovaly alarm, byly 4 (3 případy s vlivem na nespolehlivost). Mechanická závada aretace spouštěcího táhla zapříčinila jeho nedostatečné udržení ve stavu klidu. To má vždy vliv na spolehlivé fungování tohoto prvku. Je nutná mechanická oprava či výměna. Chybná montáž měla podobu nevhodného umístění a použití původně instalovaného (již poškozeného) kabelu. Řešení spočívalo v následném přemístění a záměně za nové vedení mezi expandérem a tísňovým hlásičem.

[82] Vlastní zdroj.

Po vyhodnocení jeho dat ze systému PCO byly jako důvody incidentů, které mají vliv na nespolehlivost, zjištěny následující: chybná montáž a mechanická závada.

Otřesové čidlo – vyhodnocení incidentů

Daná periferie ve sledovaném období neměla žádný incident, který by zaznamenal dohledový systém PCO. Vzhledem k tomu, že je pravidelnou revizí prováděno ověřování funkčnosti všech zabezpečovacích prvků, lze z absence jakýchkoliv případů usuzovat na:

- vysokou kvalitu výrobků,
- optimální projektování,
- správné provedení montáže a konfigurace,
- nastavení adekvátní citlivosti,
- bezchybnou obsluhu.

S přihlédnutím ke zkušenostem autora této práce a stáří některých exemplářů je třeba konstatovat, že se jedná o překvapující zjištění výzkumu.

Tab. 10: Rádiové poplachové přenosové zařízení – vyhodnocení incidentů[83]

Identifikace incidentu	Počet případů	Procent z celku			Důvod incidentu	Počet případů	Procent z celku	Řešení incidentu	Počet případů	Procent z celku
Alarm (vyvolaný poruchou)		0,0%			Akustický podnět z okolí		0,0%	Elektronická oprava	1	0,2%
Klidový stav (způsobený poruchou)		0,0%			Elektronická závada		0,0%	Mechanická oprava	1	0,2%
Neočekávaný restart řídícího procesu		0,0%			Chyba firmwaru		0,0%	Obnova 230 V	25	4,3%
Nepovolené vypnutí		0,0%			Chyba obsluhy		0,0%	Obnovení spojení	532	90,8%
Osobní identifikace technikem		0,0%			Chybná montáž	1	0,2%	Odstranění překážky		0,0%
Pokus o neautorizovaný přístup		0,0%			Mechanická závada		0,0%	Přehrání firmwaru	3	0,5%
Poplach (vyvolaný uživatelem)		0,0%			Nezjištěn	11	1,9%	Reset zařízení	4	0,7%
Porucha akumulátoru	8	1,4%	8		Pachatel		0,0%	Vymazání poplachu	10	1,7%
Porucha integrity databáze ústředny		0,0%			Překážka (fyzická)		0,0%	Výměna	9	1,5%
Porucha komunikace	11	1,9%			Sabotáž		0,0%	Změna konfigurace	1	0,2%
Porucha zdroje	2	0,3%	2		Stáří, opotřebování	9	1,5%			
Reset hardwaru (samovolný)	1	0,2%	1		Špatná konfigurace		0,0%			
Tamper (sabotážní kontakt/smyčka)		0,0%			Teplotní působení	1	0,2%			
Telefonické nahlášení uživatelem		0,0%			Vliv počasí		0,0%			
Výpadek 230 V	25	4,3%	11		Výpadek 230 V	25	4,3%			
Ztráta spojení přes kabelové vedení	342	58,4%	25	1	Závada na kabelové PPC	341	58,2%			
Ztráta spojení přes rádiový přenos	197	33,6%	44	1	Závada na rádiové PPC	197	33,6%			
					Závada zdroje	1	0,2%			
					Živočich		0,0%			
Celkem:	**586**	100,0%			**Celkem:**	**586**	100,0%	**Celkem:**	**586**	100,0%
Z toho neporuchových incidentů	**0**									
Z toho poruchových incidentů	**586**									
Z toho s vlivem na nespolehlivost			**91**							
Z toho s vlivem na nefunkčnost				**2**						

[83] Vlastní zdroj.

V souvislosti s rádiovým PPZ nastalo v uvedeném období 586 incidentů. Všechny tyto vyhodnocované stavy byly poruchové. Nejčastějším viníkem se ukázala ztráta spojení přes kabelové vedení (342 incidentů, 25 případů s vlivem na nespolehlivost, 1 případ s vlivem na nefunkčnost), které se u autorem sledovaných objektů považuje za vedlejší PPC. V pořadí počtu poruch následovala ztráta spojení přes rádiový přenos (197 incidentů, 44 případů s vlivem na nespolehlivost, 1 případ s vlivem na nefunkčnost). Ten je brán jako hlavní PPC. O zařazení incidentu do nespolehlivostní kategorie poruch rozhodla délka ztráty spojení. Pokud šlo o pozbytí komunikace po více než hodinu, ale zároveň byla závada jen u jedné PPC (rádiová průchozí – kabelová neprůchozí, rádiová neprůchozí – kabelová průchozí), naplnila se kritéria nespolehlivosti. Jakmile vznikl výpadek u obou přenosových cest ve stejný okamžik, nemohlo PPZ žádným způsobem vysílat informace o poplachovém systému směrem ze zabezpečovací ústředny k PCO. Nastala tedy nefunkčnost PZTS jakožto komplexního řetězce, který má zajistit, že dojezdový čas zakročující jednotky bude od prvotní detekce narušení kratší než dokonání protiprávního jednání pachatele a jeho následný únik. Uvedené závady PPC jsou řešeny obnovou spojení. To je automaticky testováno v časových intervalech nastavených v programovém vybavení PPZ. U nezjištěných příčin se prověří, zda skutečně došlo ke ztrátě spojení. Pokud má prověrka negativní výsledek, dojde posléze k vymazání poplachu. Výpadek 230 V (25 incidentů, 11 případů s vlivem na nespolehlivost) vždy prověří stav akumulátoru v zařízení. Jestliže pod zátěží vydrží dodávat předepsanou hodnotu napětí po celou dobu přerušení napájení, je porucha vyhodnocena s vlivem na nespolehlivost. Pokud by byla doba výpadku delší než jsou kapacitní možnosti článků, nastalo by vypnutí PPZ a tedy jeho nefunkčnost. Řešení uvedených poruch přináší včasná obnova přísunu 230 V. Po takovýchto závažných incidentech je vhodné zkontrolovat jednotlivé náhradní zdroje (sekundární články) a případně je vyměnit. To je nevyhnutelné v situaci, kdy se zjistí malé napětí na svorkách bez připojené zátěže. Obdobně se postupuje u prudkého poklesu hodnot napětí akumulátoru při současném připojení na zátěž. Stavy sekundárního článku jsou sledovány zdrojem. Vybočení z výrobcem určených mezí úrovní potenciálu vyvolá samostatný incident v podobě poruchy (8 incidentů, 8 případů s vlivem na nespolehlivost). Příčinou všech výskytů u tohoto výzkumu bylo stáří/opotřebování. Optimálním a správným řešením je pak výměna za nový kus. V soustavě napájecích komponent se nachází i zdroj. S jeho poruchou (2 incidenty, 2 případy s vlivem na nespolehlivost) se pojí neodpovídající naměřené napětí na výstupních svorkách. Stejně jako v případě závady akumulátoru je vždy nutné daný incident zařadit minimálně do kategorie těch, které mají vliv na nespolehlivost.

Důvody v podobě stáří/opotřebování či vadného zdroje jako takového jsou odstraněny jeho výměnou nebo elektronickou opravou. Dalším nežádoucím stavem, který ve sledovaném období přijímal dohledový systém PCO, byla porucha komunikace (11 incidentů). U PPZ se mezi důvody těchto vteřinových výpadků řadila chybná montáž, jež byla uvedena do pořádku mechanickou opravou vodiče ve svorkovnici. Dále je způsobovala nezjištěná příčina, kterou technik preventivně řešil přehráním firmwaru, změnou konfigurace či resetem zařízení. Pakliže se neobjevila možná příčina, byl poplach pouze vymazán a stav se nadále sledoval. Samovolný reset hardwaru (1 incident, 1 případ s vlivem na nespolehlivost) vyvolala teplotní působnost prostředí, ve kterém se zařízení nacházelo. Po provedení nápravy (výpadek klimatizace apod.) se poplach vymazal a následovalo hlídání možného opakování. Jestliže k těmto resetům dochází pravidelně, značí to vážný problém vnitřní elektroniky, který vyžaduje servisní zásah výrobce, jenž disponuje diagnostickým testerem. Zařízení je nutné demontovat, vyměnit a poté zaslat do opravy. Po vyhodnocení dat z PCO byly u rádiového PPZ jako důvody incidentů, které mají vliv na nespolehlivost či nefunkčnost, zjištěny následující: stáří/opotřebování, výpadek 230 V, chybná montáž, teplotní působení a závady na PPC.

Tab. 11: Čtečka karet – vyhodnocení incidentů[84]

Identifikace incidentu	Počet případů	Procent z celku			Důvod incidentu	Počet případů	Procent z celku	Řešení incidentu	Počet případů	Procent z celku
Alarm (vyvolaný poruchou)	1	25,0%			Akustický podnět z okolí		0,0%	Elektronická oprava	2	50,0%
Klidový stav (způsobený poruchou)		0,0%			Elektronická závada		0,0%	Mechanická oprava		0,0%
Neočekávaný restart řídícího procesu		0,0%			Chyba firmwaru		0,0%	Obnova 230 V		0,0%
Nepovolené vypnutí		0,0%			Chyba obsluhy	1	25,0%	Obnovení spojení		0,0%
Osobní identifikace technikem		0,0%			Chybná montáž	2	50,0%	Odstranění překážky		0,0%
Pokus o neautorizovaný přístup		0,0%			Mechanická závada		0,0%	Přehrání firmwaru		0,0%
Poplach (vyvolaný uživatelem)		0,0%			Nezjištěn	1	25,0%	Reset zařízení	1	25,0%
Porucha akumulátoru		0,0%			Pachatel		0,0%	Vymazání poplachu	1	25,0%
Porucha integrity databáze ústředny		0,0%			Překážka (fyzická)		0,0%	Výměna		0,0%
Porucha komunikace	3	75,0%			Sabotáž		0,0%	Změna konfigurace		0,0%
Porucha zdroje		0,0%			Stáří, opotřebování		0,0%			
Reset hardwaru (samovolný)		0,0%			Špatná konfigurace		0,0%			
Tamper (sabotážní kontakt/smyčka)		0,0%			Teplotní působení		0,0%			
Telefonické nahlášení uživatelem		0,0%			Vliv počasí		0,0%			
Výpadek 230 V		0,0%			Výpadek 230 V		0,0%			
Ztráta spojení přes kabelové vedení		0,0%			Závada na kabelové PPC		0,0%			
Ztráta spojení přes rádiový přenos		0,0%			Závada na rádiové PPC		0,0%			
					Závada zdroje		0,0%			
					Živočich		0,0%			
Celkem:	**4**	100,0%			**Celkem:**	**4**	100,0%	**Celkem:**	**4**	100,0%
Z toho neporuchových incidentů	**0**									
Z toho poruchových incidentů	**4**									
Z toho s vlivem na nespolehlivost			**0**							
Z toho s vlivem na nefunkčnost				**0**						

[84] Vlastní zdroj.

U čtečky karet vznikly 4 incidenty, které byly všechny poruchové. Největší zastoupení v nich měla porucha komunikace čtečky s modulem dveří a ústřednou. Vyskytla se celkem ve 3 případech. Chybná montáž způsobila krátkodobé (jednotky vteřin) neprůchodnosti linky. Následná oprava spočívala v úpravě jejího propojení s elektronikou dveřní jednotky. Nezjištěnou příčinu napravil reset čtecí hlavy, který se provádí jejím odpojením od zdroje napájení a opětovným připojením. Alarm (vyvolaný poruchou) nastal vlivem chyby obsluhy, která omylem spustila přístup pod nátlakem. Ten slouží k vyslání znamení od uživatele směrem k PCO v situacích, kdy pachatel nutí oprávněnou osobu autentizovat vstupy. Při řešení je zcela zásadní nepodcenit možné nebezpečí a provést důkladnou kontrolu v místě vyhlášení. Pokud je vše negativní, lze poplach vymazat. Není ke škodě provést i poučení chybujícího o řádném ovládání předmětné periferie. Vyhodnocení dat z PCO neodhalilo u čtečky karet jakékoliv důvody pro zařazení incidentů do kategorie s vlivem na nespolehlivost či nefunkčnost.

Tab. 12: Optická a akustická signalizace – vyhodnocení incidentů[85]

Identifikace incidentu	Počet případů	Procent z celku			Důvod incidentu	Počet případů	Procent z celku	Řešení incidentu	Počet případů	Procent z celku
Alarm (vyvolaný poruchou)		0,0%			Akustický podnět z okolí		0,0%	Elektronická oprava	1	20,0%
Klidový stav (způsobený poruchou)		0,0%			Elektronická závada	3	60,0%	Mechanická oprava		0,0%
Neočekávaný restart řídícího procesu		0,0%			Chyba firmwaru		0,0%	Obnova 230 V		0,0%
Nepovolené vypnutí		0,0%			Chyba obsluhy		0,0%	Obnovení spojení		0,0%
Osobní identifikace technikem	5	100,0%			Chybná montáž		0,0%	Odstranění překážky		0,0%
Pokus o neautorizovaný přístup		0,0%			Mechanická závada		0,0%	Přehrání firmwaru		0,0%
Poplach (vyvolaný uživatelem)		0,0%			Nezjištěn		0,0%	Reset zařízení		0,0%
Porucha akumulátoru		0,0%			Pachatel		0,0%	Vymazání poplachu		0,0%
Porucha integrity databáze ústředny		0,0%			Překážka (fyzická)		0,0%	Výměna	2	40,0%
Porucha komunikace		0,0%			Sabotáž		0,0%	Změna konfigurace	2	40,0%
Porucha zdroje		0,0%			Stáří, opotřebování		0,0%			
Reset hardwaru (samovolný)		0,0%			Špatná konfigurace	2	40,0%			
Tamper (sabotážní kontakt/smyčka)		0,0%			Teplotní působení		0,0%			
Telefonické nahlášení uživatelem		0,0%			Vliv počasí		0,0%			
Výpadek 230 V		0,0%			Výpadek 230 V		0,0%			
Ztráta spojení přes kabelové vedení		0,0%			Závada na kabelové PPC		0,0%			
Ztráta spojení přes rádiový přenos		0,0%			Závada na rádiové PPC		0,0%			
					Závada zdroje		0,0%			
					Živočich		0,0%			
Celkem:	**5**	100,0%			**Celkem:**	**5**	100,0%	**Celkem:**	**5**	100,0%
Z toho neporuchových incidentů	**0**									
Z toho poruchových incidentů	**5**									
Z toho s vlivem na nespolehlivost			**0**							
Z toho s vlivem na nefunkčnost				**0**						

Veškeré incidenty u optické a akustické signalizace byly identifikovány technikem na místě její instalace. Vždy se jednalo o poruchový stav, jehož důvod souvisel ve 3 případech s elektronickou závadou (vadné kontakty desky plošných spojů). Řešením

[85] Vlastní zdroj.

této výrobní vady je pokus o řádné prohřátí vodivých plošek pájkou nebo přemostění cesty na desce plošných spojů. Když se náprava nezdaří, je nutná výměna. Špatná konfigurace nastala ve 2 případech. K vyřešení postačila její změna v programovém vybavení zabezpečovací ústředny. Optická a akustická signalizace neposkytla PCO data rozhodná k přiřazení incidentů do kategorie s vlivem na nespolehlivost či nefunkčnost. Ani autor této práce, který jakožto technik prováděl jednotlivé opravy, neshledal důvody pro takové zařazení.

Tab. 13: Elektronický zámek – vyhodnocení incidentů[86]

Identifikace incidentu	Počet případů	Procent z celku		Důvod incidentu	Počet případů	Procent z celku	Řešení incidentu	Počet případů	Procent z celku
Alarm (vyvolaný poruchou)		0,0%		Akustický podnět z okolí		0,0%	Elektronická oprava	3	15,0%
Klidový stav (způsobený poruchou)		0,0%		Elektronická závada	3	15,0%	Mechanická oprava	5	25,0%
Neočekávaný restart řídícího procesu		0,0%		Chyba firmwaru		0,0%	Obnova 230 V		0,0%
Nepovolené vypnutí		0,0%		Chyba obsluhy		0,0%	Obnovení spojení		0,0%
Osobní identifikace technikem		0,0%		Chybná montáž		0,0%	Odstranění překážky		0,0%
Pokus o neautorizovaný přístup		0,0%		Mechanická závada	7	35,0%	Přehrání firmwaru		0,0%
Poplach (vyvolaný uživatelem)		0,0%		Nezjištěn		0,0%	Reset zařízení		0,0%
Porucha akumulátoru		0,0%		Pachatel		0,0%	Vymazání poplachu		0,0%
Porucha integrity databáze ústředny		0,0%		Překážka (fyzická)		0,0%	Výměna	12	60,0%
Porucha komunikace		0,0%		Sabotáž		0,0%	Změna konfigurace		0,0%
Porucha zdroje		0,0%		Stáří, opotřebování	10	50,0%			
Reset hardwaru (samovolný)		0,0%		Špatná konfigurace		0,0%			
Tamper (sabotážní kontakt/smyčka)		0,0%		Teplotní působení		0,0%			
Telefonické nahlášení uživatelem	20	100,0%	12	Vliv počasí		0,0%			
Výpadek 230 V		0,0%		Výpadek 230 V		0,0%			
Ztráta spojení přes kabelové vedení		0,0%		Závada na kabelové PPC		0,0%			
Ztráta spojení přes rádiový přenos		0,0%		Závada na rádiové PPC		0,0%			
				Závada zdroje		0,0%			
				Živočich		0,0%			
Celkem:	**20**	100,0%		**Celkem:**	**20**	100,0%	**Celkem:**	**20**	100,0%
Z toho neporuchových incidentů	**0**								
Z toho poruchových incidentů	**20**								
Z toho s vlivem na nespolehlivost			**12**						
Z toho s vlivem na nefunkčnost			**0**						

Ve sledovaném období vzniklo u elektronického zámku 20 poruch. Všechny se podařilo identifikovat pomocí telefonického nahlášení uživatelem. Technik následně 12 z nich vyhodnotil s vlivem na nespolehlivost. Jejím nejčastějším důvodem (10 případů, 50 % z celku) bylo stáří/opotřebování, které se projevilo prasklými kovovými částmi zámku. Zde je vždy nutná výměna za nový kus. Mechanická závada zavinila nespolehlivost ve 2 případech tím, že se ulomil kontakt stavu dveří. Řešením je jeho výměna. U zbývajících poruch mechanického rázu postačila oprava ve formě přizpůsobení otvoru západky nebo došlo k jejímu samotnému posunutí. Elektronickou závadu představoval ve 3 případech chybějící transil. Jeho dodání problém vyřeší

[86] Vlastní zdroj.

a prodlouží celkovou životnost. Elektronický zámek neposkytuje PCO řádná data rozhodná k zařazení incidentů do kategorie s vlivem na nespolehlivost či nefunkčnost. U tohoto zabezpečovacího prvku je zásadním kritériem samotné posouzení na místě události. Autorem, který je zároveň i technikem PZTS, byly zjištěny následující důvody incidentů s vlivem na nespolehlivost: stáří/opotřebování a mechanická závada.

Tab. 14: Docházkový terminál – vyhodnocení incidentů[87]

Identifikace incidentu	Počet případů	Procent z celku			Důvod incidentu	Počet případů	Procent z celku	Řešení incidentu	Počet případů	Procent z celku
Alarm (vyvolaný poruchou)		0,0%			Akustický podnět z okolí		0,0%	Elektronická oprava		0,0%
Klidový stav (způsobený poruchou)		0,0%			Elektronická závada		0,0%	Mechanická oprava		0,0%
Neočekávaný restart řídícího procesu		0,0%			Chyba firmwaru		0,0%	Obnova 230 V		0,0%
Nepovolené vypnutí		0,0%			Chyba obsluhy		0,0%	Obnovení spojení	1	33,3%
Osobní identifikace technikem		0,0%			Chybná montáž		0,0%	Odstranění překážky		0,0%
Pokus o neautorizovaný přístup		0,0%			Mechanická závada		0,0%	Přehrání firmwaru		0,0%
Poplach (vyvolaný uživatelem)		0,0%			Nezjištěn	3	100,0%	Reset zařízení	1	33,3%
Porucha akumulátoru		0,0%			Pachatel		0,0%	Vymazání poplachu	1	33,3%
Porucha integrity databáze ústředny		0,0%			Překážka (fyzická)		0,0%	Výměna		0,0%
Porucha komunikace	2	66,7%			Sabotáž		0,0%	Změna konfigurace		0,0%
Porucha zdroje		0,0%			Stáří, opotřebování		0,0%			
Reset hardwaru (samovolný)		0,0%			Špatná konfigurace		0,0%			
Tamper (sabotážní kontakt/smyčka)		0,0%			Teplotní působení		0,0%			
Telefonické nahlášení uživatelem		0,0%			Vliv počasí		0,0%			
Výpadek 230 V		0,0%			Výpadek 230 V		0,0%			
Ztráta spojení přes kabelové vedení	1	33,3%			Závada na kabelové PPC		0,0%			
Ztráta spojení přes rádiový přenos		0,0%			Závada na rádiové PPC		0,0%			
					Závada zdroje		0,0%			
					Živočich		0,0%			
Celkem:	**3**	100,0%			**Celkem:**	**3**	100,0%	**Celkem:**	**3**	100,0%
Z toho neporuchových incidentů	**0**									
Z toho poruchových incidentů	**3**									
Z toho s vlivem na nespolehlivost			**0**							
Z toho s vlivem na nefunkčnost				**0**						

Docházkový terminál vykazoval celkem 3 incidenty. Všechny byly poruchové, avšak neovlivnily spolehlivost či funkčnost. Jednalo se o poruchu komunikace mezi zabezpečovací ústřednou a docházkou. Případně nastala ztráta spojení přes kabelové vedení linky. Důvody těchto vteřinových výpadků se nepodařilo zjistit. Řešení jednotlivých případů však byla rozdílná (samovolné obnovení spojení, reset zařízení a vymazání poplachu). Docházkový terminál je periferie poplachových systémů, která slouží převážně k personálním a mzdovým účelům zaměstnavatele. Jakékoliv její selhání nesmí ohrožovat zabezpečení objektu. Vyhodnocení dat z PCO neodhalilo u docházkového terminálu žádné důvody pro zařazení incidentů do kategorie s vlivem na nespolehlivost či nefunkčnost.

[87] Vlastní zdroj.

Tab. 15: Vyhodnocení incidentů dle jejich identifikace[88]

Identifikace incidentu	Incidentů celkem	Neporuchových	Poruchových	Procentuální vyjádření vlivu incidentu na poruchovost	S vlivem na nespolehlivost	Procentální vyjádření vlivu incidentu na nespolehlivost	S vlivem na nefunkčnost	Procentální vyjádření vlivu incidentu na nefunkčnost
Alarm (vyvolaný poruchou)	130	0	130	12,6%	24	11,1%	3	5,7%
Klidový stav (způsobený poruchou)	1	0	1	0,1%	0	0,0%	1	1,9%
Neočekávaný restart řídícího procesu	10	0	10	1,0%	10	4,6%	0	0,0%
Nepovolené vypnutí	20	0	20	1,9%	0	0,0%	20	37,7%
Osobní identifikace technikem	5	0	5	0,5%	0	0,0%	0	0,0%
Pokus o neautorizovaný přístup	9	9	0	0,0%	0	0,0%	0	0,0%
Poplach (vyvolaný uživatelem)	309	309	0	0,0%	0	0,0%	0	0,0%
Porucha akumulátoru	17	0	17	1,6%	16	7,4%	1	1,9%
Porucha integrity databáze ústředny	10	0	10	1,0%	10	4,6%	0	0,0%
Porucha komunikace	43	0	43	4,2%	3	1,4%	10	18,9%
Porucha zdroje	4	0	4	0,4%	3	1,4%	1	1,9%
Reset hardwaru (samovolný)	1	0	1	0,1%	1	0,5%	0	0,0%
Tamper (sabotážní kontakt/smyčka)	18	0	18	1,7%	0	0,0%	14	26,4%
Telefonické nahlášení uživatelem	20	0	20	1,9%	12	5,6%	0	0,0%
Výpadek 230 V	44	0	44	4,3%	29	13,4%	1	1,9%
Ztráta spojení přes kabelové vedení	444	0	444	42,9%	54	25,0%	1	1,9%
Ztráta spojení přes rádiový přenos	267	0	267	25,8%	54	25,0%	1	1,9%
Celkem:	**1352**	**318**	**1034**	100,0%	**216**	100,0%	**53**	100,0%

Tato tabulka znázorňuje shrnutí výsledků u jednotlivých druhů identifikací incidentů. Vyjadřuje jejich vliv na poruchovost, nespolehlivost a nefunkčnost. Pořadí zde není uvedeno. Hodnoty budou dále využity v následném vyhodnocování periferií.

Tab. 16: Vyhodnocení poruchovosti jednotlivých periferií[89]

Pořadí	Vyhodnocovaná periferie	Počet incidentů	Z celkového počtu incidentů tvoří procent	Počet neporuchových incidentů	Z celkového počtu incidentů dané periferie tvoří procent	Počet poruchových incidentů	Z celkového počtu incidentů dané periferie tvoří procent	Z celkového počtu poruchových incidentů tvoří procent
1.	Rádiové PPZ	586	43,3%	0	0,0%	586	100,0%	56,7%
2.	Zabezpečovací ústředna	234	17,3%	0	0,0%	234	100,0%	22,6%
3.	Pohybové čidlo	224	16,6%	159	71,0%	65	29,0%	6,3%
4.	Magnetický kontakt	173	12,8%	138	79,8%	35	20,2%	3,4%
5.	Akustický detektor rozbití skla	33	2,4%	1	3,0%	32	97,0%	3,1%
6.	Elektronický zámek	20	1,5%	0	0,0%	20	100,0%	1,9%
7.	Ovládací klávesnice	23	1,7%	9	39,1%	14	60,9%	1,4%
	Expandér	14	1,0%	0	0,0%	14	100,0%	1,4%
8.	Posilovací zdroj	12	0,9%	0	0,0%	12	100,0%	1,2%
9.	Rozvodná krabice	6	0,4%	0	0,0%	6	100,0%	0,6%
10.	Optická a akustická signalizace	5	0,4%	0	0,0%	5	100,0%	0,5%
11.	Tísňový hlásič	15	1,1%	11	73,3%	4	26,7%	0,4%
	Čtečka karet	4	0,3%	0	0,0%	4	100,0%	0,4%
12.	Docházkový terminál	3	0,2%	0	0,0%	3	100,0%	0,3%
13.	Otřesové čidlo	0	0,0%	0	nelze vypočítat	0	nelze vypočítat	0,0%
	Celkem:	**1352**	100,0%	**318**		**1034**		100,0%

Tabulka vychází z výše uvedených vyhodnocení jednotlivých součástí poplachových systémů. Zaměřuje se na jejich poruchovost, která je definována jako množství závad v určitém čase. Ten je v případě tohoto výzkumu stanoven na období od

[88] Vlastní zdroj.
[89] Vlastní zdroj.

1. 1. 2025 do 31. 3. 2025. Počet v něm zjištěných incidentů byl ponížen o neporuchové, jež tvořily 23,5 % z celkového množství. Výsledné zastoupení poruchových případů pak činilo 76,5 %. Z hlediska hodnocení poruchovosti vybraných periferií je zajímavé sledovat procentuální vyjádření poruchových incidentů vůči všem případům, které přijal PCO. Ve sledovaném období byly statisticky nejvýraznější 2 periferie. Rádiové PPZ mělo všech 586 incidentů poruchových. Ty tvořily 56,7 % poruchovosti. Zabezpečovací ústředna se na ní podílela též významným vlivem, který dosáhl hodnoty 22,6 %. Veškeré její incidenty (234) byly poruchové. Výsledný součet těchto součástí poplachových systémů tak činil 79,3 % celkové poruchovosti (820 z 1034 případů). Výrazný nepoměr a převaha se ještě prohloubily při vyhodnocení pohybového čidla. Jeho incidenty participovaly na poruchovosti pouhými 6,3 % (65 z 1034 případů). Při jejím posuzování nešlo opominout ani vliv incidentů dle jejich identifikace. Ztráty spojení přes kabelové vedení (444 z 1034 případů) a přes rádiový přenos (267 z 1034 případů) jsou podle tohoto výzkumu záležitostí rádiového PPZ a zabezpečovací ústředny (+1 výskyt u docházkového terminálu). Při svém procentuálním vlivu na poruchovost, který dosahuje hodnot 42,9 % a 25,8 %, jde o zcela dominující závady. Alarm (vyvolaný poruchou) je pak v 130 případech (12,6 %) rozprostřen mezi více zabezpečovacími prvky.

Tab. 17: Vyhodnocení vlivu periferií na nespolehlivost poplachových systémů[90]

Pořadí ve vlivu na nespolehlivost	Vyhodnocovaná periferie	Počet incidentů s vlivem na nespolehlivost	Z celkového počtu incidentů s vlivem na nespolehlivost tvoří procent	Celkový počet poruchových incidentů dané periferie	Z toho s vlivem na nespolehlivost tvoří procent
1.	Rádiové PPZ	91	42,1%	586	15,5%
2.	Zabezpečovací ústředna	74	34,3%	234	31,6%
3.	Elektronický zámek	12	5,6%	20	60,0%
	Posilovací zdroj	12	5,6%	12	100,0%
4.	Magnetický kontakt	10	4,6%	35	28,6%
	Pohybové čidlo	10	4,6%	65	15,4%
5.	Expandér	3	1,4%	14	21,4%
	Tísňový hlásič	3	1,4%	4	75,0%
6.	Akustický detektor rozbití skla	1	0,5%	32	3,1%
7.	Ovládací klávesnice	0	0,0%	14	0,0%
	Rozvodná krabice	0	0,0%	6	0,0%
	Otřesové čidlo	0	0,0%	0	nelze vypočítat
	Čtečka karet	0	0,0%	4	0,0%
	Optická a akustická signalizace	0	0,0%	5	0,0%
	Docházkový terminál	0	0,0%	3	0,0%
	Celkem:	**216**	100,0%	**1034**	

[90] Vlastní zdroj.

Tabulka, která vyhodnocuje vliv periferií na nespolehlivost poplachových systémů, vychází pouze z poruchových incidentů. Spolehlivostí se rozumí předpoklad, že daný systém bude plnit své funkční úkoly, které mu byly naplánovány. Ve sledovaném období nastalo 216 incidentů s vlivem na nespolehlivost (tvoří 20,9 % z 1034 poruch). Stejně jako u poruchovosti, vynikli i zde 2 zástupci periferií, které zároveň tvoří základní technologie poplachových systémů připojených na PCO. Rádiové PPZ mělo negativní dopad na spolehlivost celých 42,1 % (91 z 216 incidentů s vlivem na nespolehlivost). Zabezpečovací ústředna přispěla v tomto duchu též podstatnou měrou a dosáhla 34,3 % (74 z 216 incidentů s vlivem na nespolehlivost). Součet pak tvořil hodnotu 76,4 % (165 z 216 incidentů s vlivem na nespolehlivost). Dominanci těchto periferií opět zvýrazňuje pohled na další pořadí. Od 3. místa je vyjádření vlivu umístěných periferií na nespolehlivost v pouhých jednotkách procent. Premiantů, u kterých se nezaznamenala nespolehlivostní závada, bylo 5 (ovládací klávesnice, rozvodná krabice, otřesové čidlo, čtečka karet, optická/akustická signalizace a docházkový terminál). Zajímavým ukazatelem spolehlivosti jednotlivých zabezpečovacích prvků je také část tabulky, která prezentuje procentuální vyjádření množství incidentů periferie majících vliv na nespolehlivost vůči celkovému počtu poruch této součásti. Zde už bylo pořadí zcela jiné. Posilovací zdroj měl všechny případy s vlivem na nespolehlivost. Tísňový hlásič (3 ze 4 případů) dosáhl u svých poruchových incidentů hodnoty 75 % vlivu na nespolehlivost. U elektronického zámku (12 z 20 případů) spadalo 60 % poruchových incidentů do nespolehlivostní kategorie. Vliv incidentů dle jejich identifikace byl obdobný jako při vyhodnocování poruchovosti. Ztráty spojení přes kabelové vedení (54 z 216 případů) a přes rádiový přenos (54 z 216 případů) zasahovaly do nespolehlivosti u poloviny všech výskytů. Výsledky předchozích vyhodnocení u vybraných součástí poplachových systémů ukázaly jejich přítomnost pouze u zabezpečovací ústředny a rádiového PPZ. Výpadek 230 V a alarm (vyvolaný poruchou) měly též významný podíl, který činil v součtu 24,5 % ze všech incidentů s vlivem na nespolehlivost.

Tato část výzkumu odhalila ve sledovaném období značnou přítomnost incidentů s vlivem na nespolehlivost (216 z 1034). Vzhledem ke zjištěné příčině těchto výsledků je z pohledu autora této práce nutné, aby se techničtí pracovníci PZTS a IT zaměřili na redukci ztrát spojení přes kabelové vedení a rádiový přenos. V prvním případě by bylo prospěšné důkladně proměřit kabelovou trasu, u níž dochází k častým výpadkům a uvážit případnou obměnu síťových prvků (hlavně směrovačů). U frekventovaných výpadků rádiového přenosu v rámci jedné oblasti by bylo zcela na místě prověřit, zda nedošlo ke

změnám majícím negativní vliv na anténu (vychýlení, nové překážky na trase aj.). Pokud nastalo zhoršení kvality signálu, je vhodné provést úpravu nasměrování antény či zvážit její otočení k jinému retranslátoru. Možné zvýšení vysílacího výkonu se též nabízí.

Tab. 18: Vyhodnocení vlivu periferií na nefunkčnost poplachových systémů[91]

Pořadí ve vlivu na nefunkčnost	Vyhodnocovaná periferie	Počet incidentů s vlivem na nefunkčnost	Z celkového počtu incidentů s vlivem na nefunkčnost tvoří procent	Celkový počet poruchových incidentů dané periferie	Z toho s vlivem na nefunkčnost tvoří procent
1.	Zabezpečovací ústředna	23	43,4%	234	9,8%
2.	Expandér	10	18,9%	14	71,4%
3.	Rozvodná krabice	6	11,3%	6	100,0%
4.	Pohybové čidlo	5	9,4%	65	7,7%
5.	Magnetický kontakt	4	7,5%	35	11,4%
6.	Akustický detektor rozbití skla	3	5,7%	32	9,4%
7.	Rádiové PPZ	2	3,8%	586	0,3%
8.	Posilovací zdroj	0	0,0%	12	0,0%
	Ovládací klávesnice	0	0,0%	14	0,0%
	Tísňový hlásič	0	0,0%	4	0,0%
	Otřesové čidlo	0	0,0%	0	nelze vypočítat
	Čtečka karet	0	0,0%	4	0,0%
	Optická a akustická signalizace	0	0,0%	5	0,0%
	Elektronický zámek	0	0,0%	20	0,0%
	Docházkový terminál	0	0,0%	3	0,0%
	Celkem:	**53**	100,0%	**1034**	

Vyhodnocovací tabulka vlivu jednotlivých vybraných součástí poplachových systémů na jejich nefunkčnost bere jako zdroj informací výhradně poruchové incidenty. O funkčnosti se lze bavit jedině za předpokladu, že je časový úsek od prvotní detekce narušení delší než dojezdový čas zakročující jednotky. Některé závady, které byly tímto výzkumem odhaleny, neumožňují v okamžiku incidentu jeho řádnou detekci či odeslání poplachu na PCO. Ve sledovaném období od 1. 1. 2025 do 31. 3. 2025 jich vzniklo 53 (tvořily 5,1 % z 1034 poruch). V pořadí tohoto vyhodnocení vede zabezpečovací ústředna. Její incidenty s vlivem na nefunkčnost představovaly 43,4 % z celkového počtu (23 z 53 případů). Tento základní technický prvek však měl celkem 234 poruchových incidentů. Z nich tedy bylo s vlivem na nefunkčnost jen 9,8 %. Jako druhý v pořadí se umístil expandér. U něho nastalo 10 případů, které znamenaly dosáhnutí hodnoty 18,9 % z celkového počtu 53 incidentů s vlivem na nefunkčnost. Pokud se budou procenta vypočítávat jen z poruchových incidentů dané periferie, tak vznikne již významných 71,4 %. K ještě většímu číslu se dospělo u rozvodné krabice. Všechny její poruchové

[91] Vlastní zdroj.

incidenty znamenaly nefunkčnost. Za zajímavé je možné označit umístění rádiového PPZ. Jen 2 z 586 případů měly vliv na nefunkčnost, což bylo pouhých 0,3 %. Tento výsledek je překvapivý. Vliv incidentů podle jejich identifikace má zcela jiné zástupce, než tomu bylo u nespolehlivostní kategorie. Nepovolené vypnutí nastávalo výhradně u zabezpečovací ústředny (20 případů tvořilo 37,7 % ze všech incidentů s vlivem na nefunkčnost). Tamper měl své výskyty rozprostřeny u více zabezpečovacích součástí (rozvodná krabice, pohybové čidlo, magnetický kontakt a akustický detektor rozbití skla). Jeho 14 případů znamenalo hodnotu 26,4 % z incidentů s negativním vlivem na funkčnost. Posledním významným zástupcem se stala porucha komunikace. Zaznamenána byla pouze u expandéru, kde 10 těchto závad představovalo 18,9 % z incidentů s vlivem na nefunkčnost.

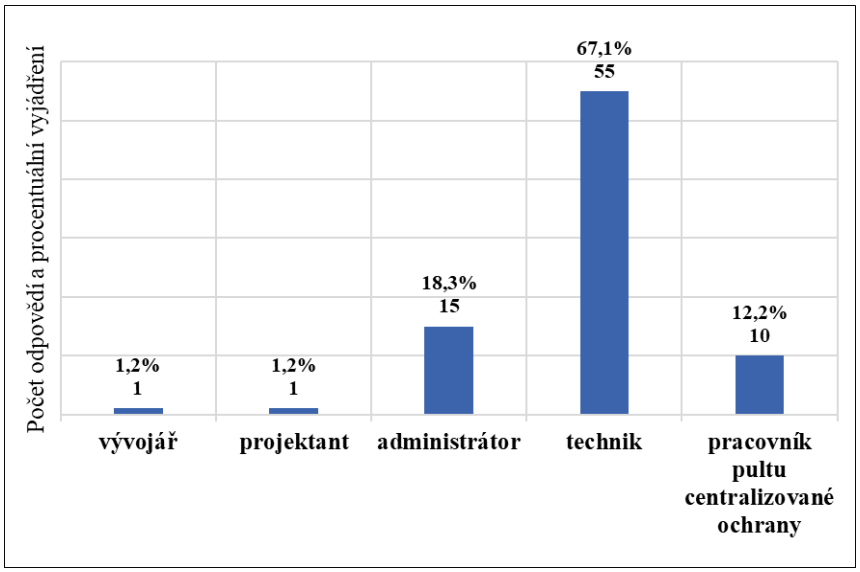
Výsledky této části výzkumu odhalily podstatně menší zastoupení poruch s vlivem na nefunkčnost než těch, které se podílely na nespolehlivosti (53 oproti 216 případů). Hlavní zjištěné příčiny lze z pohledu autora, který je zároveň technikem poplachových systémů, řešit preventivně jen částečně. Stáři/opotřebování zařízení nebo dlouhodobý výpadek 230 V jsou zjištěné důvody nepovoleného vypnutí zabezpečovací ústředny. Odstranění prvního jmenovaného probíhá formou výměny. To bývá značnou ekonomickou zátěží a je tedy žádoucí k němu přikročit, až se nebude jednat o ojedinělý výskyt. Delší výpadek elektrické energie nejde dopředu predikovat. Je však nutné s ním počítat a zásadní technologie připojovat na přívod napětí, který je zálohován např. diesel agregátem. Ten se u malých objektů většinou nevyskytuje. V těchto místech musí technici PZTS řádně revidovat akumulátor ústředny, PPZ a napájecího zdroje. Vyvolání tamperu lze předcházet kvalitní montáží (důsledným uzavřením krytu, napružením sabotážního kontaktu, dotažením šroubků a precizním pájením). Správné umístění prvků je pak vizitkou projektanta. Zde je velice důležitá kooperace s pracovníky montáže, kteří ho mohou v průběhu výstavby upozornit na reálná specifika prostředí. Porucha komunikace si žádá hlubší zjišťování příčiny a je vhodné, aby technik provedl revizi připojení kabelů a případně použil i měření osciloskopem. To může odhalit indukované rušení komunikačního signálu. Kontrola konfigurace, napájecího napětí a firmwaru je samozřejmá.

6 Vyhodnocení dotazníkového šetření

Praktická část této bakalářské práce obsahuje i kvantitativní empirický výzkum ve formě dotazníkového šetření. Cílem je posoudit efektivitu poplachových zabezpečovacích a tísňových prvků ochrany v návaznosti na prevenci kriminality. Respondenty byly výhradně osoby vykonávající odbornou činnost v oblasti výstavby a servisu PZTS. Šetření nástrojem Survio probíhalo od 16. 9. 2025 do 14. 10. 2025. Přímý odkaz na adresu https://www.survio.com/survey/d/D6N7V8O2I9N2A8N6U využilo 51,8 % a vytvořený QR kód 48,2 % oslovených. Distribuce žádosti o vyplnění se uskutečňovala elektronickou poštou ve 4 kolech. Část odpovědí (38) byla získána in natura prostřednictvím mobilního kiosku – telefonu. Počet návštěv na uvedené internetové adrese činil 241. K dokončení došlo v 85 případech. Vyřadily se 3 odpovědi. Celková úspěšná návratnost dosáhla hodnoty 35,3 %. Pro výzkumné účely této části práce byly stanoveny následující hypotézy, které budou dotazníkem potvrzeny či vyvráceny:

- H1: Pohybové čidlo je považováno za funkčně nejefektivnější prvek ochrany, protože si to myslí více než 60 % odpovídajících.
- H2: Nevyhovující umístění je pro respondenty závažnější faktor snižování schopnosti účinného fungování prvků ochrany než stáří/opotřebování.
- H3: Oslovení respondenti se nepřiklání k myšlence, že vyhlášení poplachu odrazuje narušitele od jeho dalšího postupu.

Graf 1: Pracovní pozice respondentů ve vztahu k poplachovým zabezpečovacím a tísňovým systémům[92]

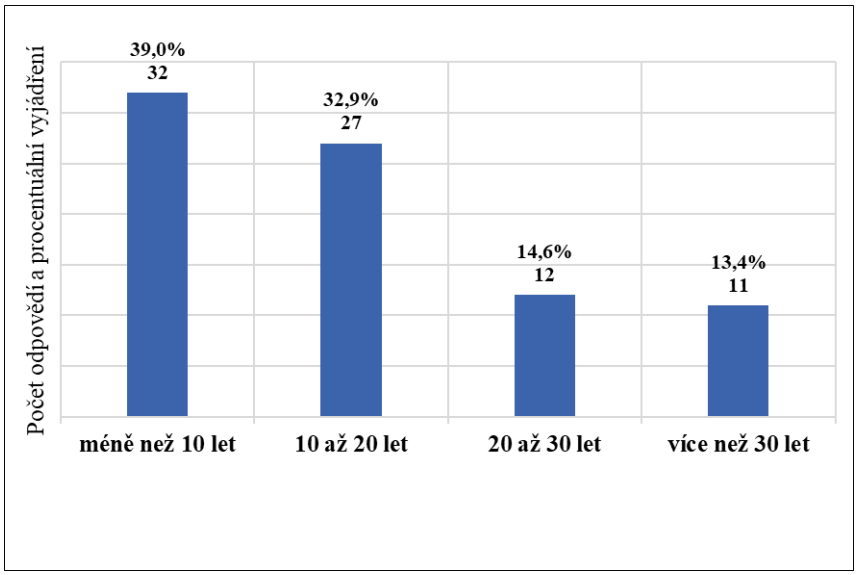


[92] Vlastní zdroj.

Otázka číslo 1 – Jaká je Vaše pracovní pozice ve vztahu k poplachovým zabezpečovacím a tísňovým systémům? Poměr zastoupení odpovědí od techniků, administrátorů a pracovníků PCO, jaký ukazuje graf 1, je pro reliabilitu výzkumu pozitivní. Negativním jevem této otázky se stala neochota projektantů a vývojářů podílet se na dotazníkovém šetření. Jejich celková účast činila pouhých 2,4 % (2 vyplněné dotazníky).

Otázka číslo 2 – Kdo je Vaším současným zaměstnavatelem? Ačkoliv byly osloveny významné soukromé společnosti, které působí na poli PZTS (Trade Fides, Jablotron, Radom, NAM system, Česká pošta Security), reagovaly z jejich strany pouze 2 osoby (2,4 %). Zbylých 80 odpovědí (97,6 %) tvořili zástupci státní správy a PČR. Nikdo z dotázaných se neoznačil jako OSVČ. Výzkum tedy získal stěžejní respondenty z řad zabezpečení státních objektů. Nezájem ze strany výrobců a distributorů poplachových systémů způsobil absenci názorů z jejich strany.

Graf 2: Praxe respondentů ve vztahu k poplachovým zabezpečovacím a tísňovým systémům[93]

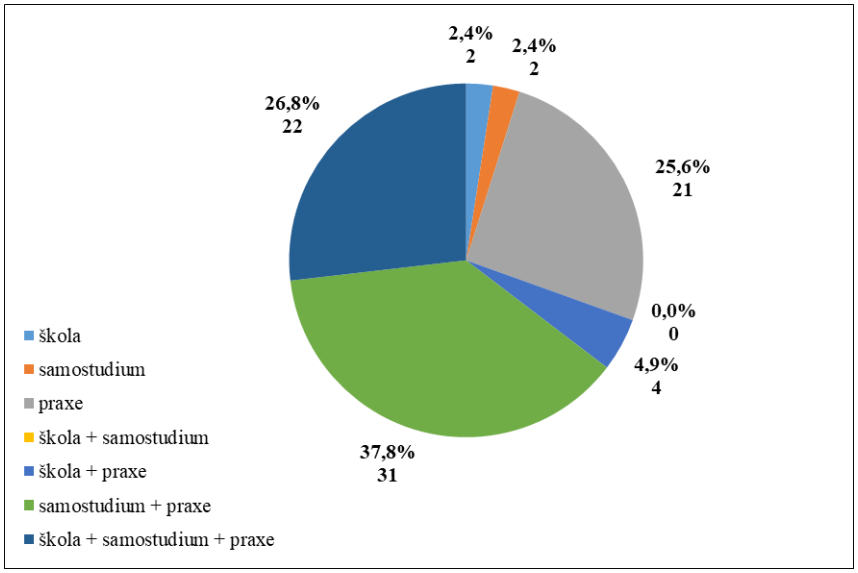


Otázka číslo 3 – Kolik let praxe máte ve vztahu k poplachovým zabezpečovacím a tísňovým systémům? Hodnotným zjištěním z vyhodnocení grafu 2 byl fakt, že 50 vyplňujících pracuje v uvedeném oboru 10 a více let. Jednalo se o 61 % odpovědí, což zvyšuje odbornou i názorovou hodnotu celého dotazníku. Největší ochota dokončit celé dotazníkové šetření vzešla od respondentů, kteří se PZTS věnují méně než 10 let. Ze strany autora této práce jde o předpokládané zjištění. Neočekávanou a velice kladnou

[93] Vlastní zdroj.

skutečností se stalo řádné vyplnění otázek ze strany pracovníků s dobou praxe delší než 20 let (tvořilo 28 % z celku).

Graf 3: Zdroje odborných znalostí respondentů o poplachových zabezpečovacích a tísňových systémech[94]

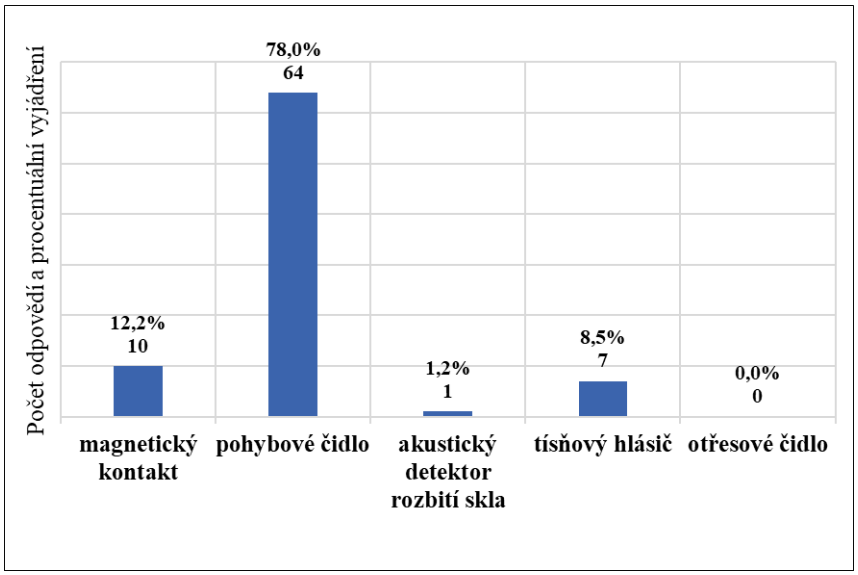


Otázka číslo 4 – Co je zdrojem Vašich odborných znalostí o poplachových zabezpečovacích a tísňových systémech? Zde zvítězilo spojení samostudia a praxe následované stejnou kombinací s přidáním vlivu školy. Na 3. místě se nacházela praxe jakožto jediný zdroj vědomostí. Další volba v pořadí měla již pouze 4,9 % (4 odpovídající). Obsahovala též praxi, která se opírala o školní odborné vědomosti. Graf 3 tedy znázorňuje, že pro řádný výkon technické činnosti v PZTS je nejzásadnější praxe. Její ideální doplnění tvoří samostudium. Význam vzdělávání (škola, samostudium) se ukázal nezanedbatelný pouze v kombinaci s praxí.

Otázka číslo 5 – Vnímáte nasazení poplachových zabezpečovacích a tísňových prvků ochrany jako účinný prostředek prevence kriminality? Pro potřeby tohoto výzkumu byly odpovědi velmi důležité. Zjistit, zda oslovení odborníci z oblasti PZTS daným systémům věří a považují je za efektivní prostředek, jenž působí při předcházení trestné činnosti, se stalo významným v kontextu důvěryhodnosti následných odpovědí. Ověřilo se tak, že 80 odborných respondentů (97,6 %) považuje PZTS za účinný nástroj při prevenci kriminality. Pouhé 2 osoby (2,4 %) si to nemyslely.

[94] Vlastní zdroj.

Graf 4: Funkčně nejefektivnější prvky ochrany dle respondentů[95]

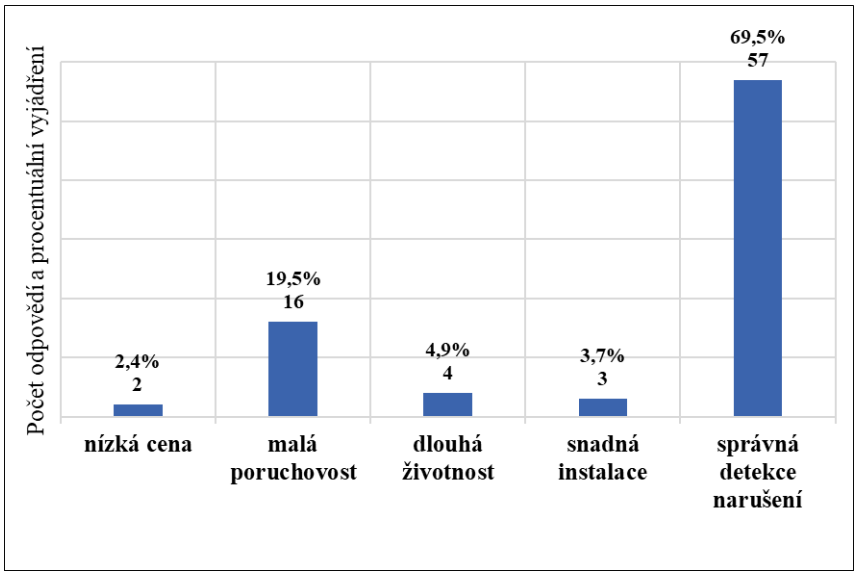


Otázka číslo 6 – Který prvek ochrany považujete za funkčně nejefektivnější? U této otázky měli respondenti na výběr z výzkumné skladby zabezpečovacích periferií (magnetický kontakt, pohybové čidlo, akustický detektor rozbití skla, tísňový hlásič a otřesové čidlo), kterou určil autor této práce. Kritériem výběru byla jeho praktická zkušenost z četnosti užití při realizovaných instalacích. Návaznost na jednotlivá vyhodnocení uskutečněná v kapitole 5 měla též podstatnou roli. Graf 4 ukazuje, že 64 odborných respondentů (78 %) považovalo pohybové čidlo za funkčně nejefektivnější prvek ochrany. Jelikož je to více než 60 % odpovídajících, byla potvrzena hypotéza H1. Za efektivní považovalo 10 odborníků i magnetický kontakt (12,2 %) a dalších 7 zvolilo tísňový hlásič (8,5 %). Nepřítomnost odpovědí u otřesového čidla se však stala překvapující, jelikož byla tato zabezpečovací periferie ve sledovaném období zcela bezporuchová, spolehlivá a funkční.

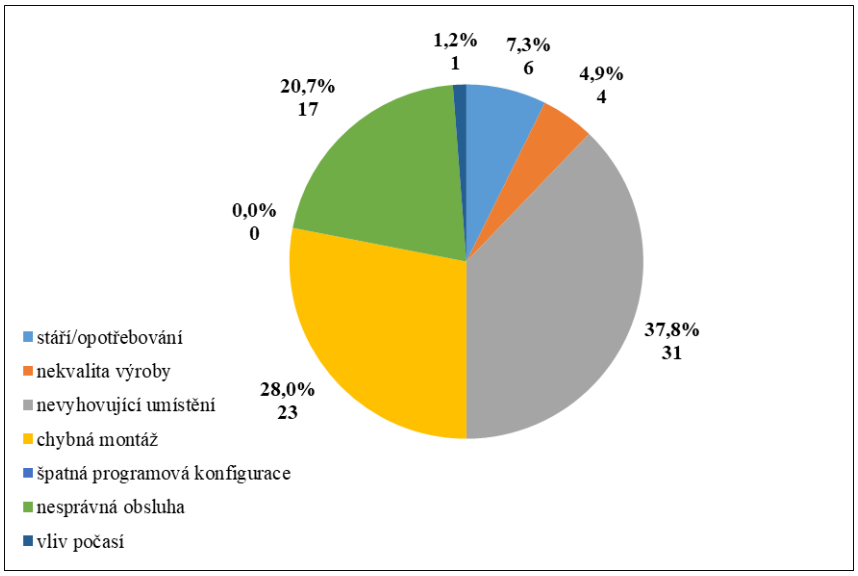
Otázka číslo 7 – Zvolte pozitivní vlastnost, kterou při hodnocení prvků ochrany pokládáte za klíčovou. Respondenti zcela dominantně označili volby, které souvisejí se správnou funkčností/spolehlivostí a nízkou poruchovostí, což je pozitivní zjištění ve vztahu k cílům této práce. Jak ukazuje níže umístěný graf 5, byla nejčastější odpovědí správná detekce narušení (69,5 %). Následovala malá poruchovost. Zvolilo ji 16 odpovídajících (19,5 %). Součet těchto kvalit, jež jsou pro veškeré prvky ochrany stěžejní, dosáhl 89 % podílu z celku. Odpovědělo pro něj 73 z 82 odborníků na poplachové systémy.

[95] Vlastní zdroj.

Graf 5: Klíčové pozitivní vlastnosti při hodnocení prvků ochrany respondenty[96]



Graf 6: Volba faktorů nejvíce snižujících schopnost účinného fungování prvků ochrany[97]

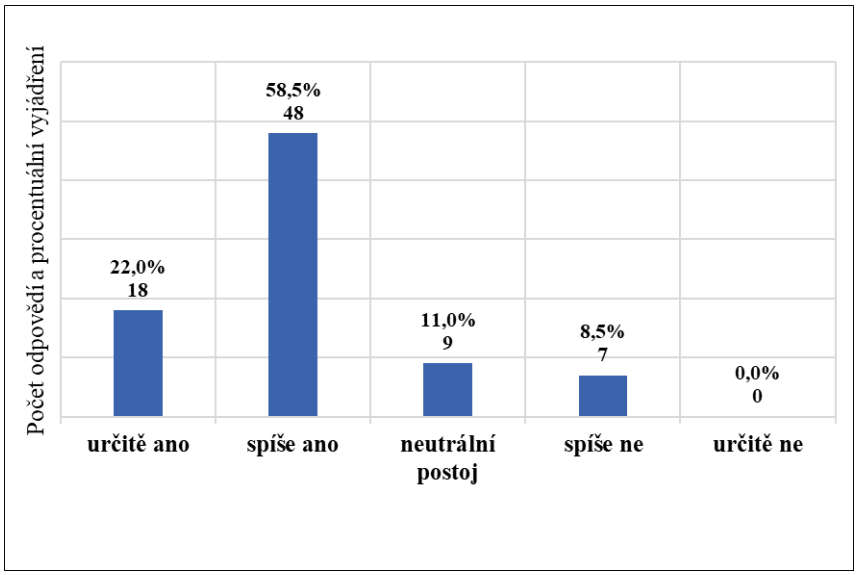


Otázka číslo 8 – Co podle Vás nejvíce snižuje schopnost účinného fungování prvků ochrany? Poměr zastoupení odpovědí vypovídá o tom, že odborní respondenti hodnotili ve vztahu k funkčnosti PZTS především kvalitu práce projektantů, správnost výstavby techniků a následnou úroveň uživatelského chování. Stáří/opotřebování, nekvalita výroby, vliv počasí a špatná programová konfigurace byly zvoleny v součtu 11 oslovených osob (13,4 %). Při pohledu na graf 6 je vidět, že tyto volby nebyly upřednostňovány. Jako vítěz mezi faktory, které nejvíce snižují schopnost účinného fungování prvků ochrany, bylo 31 respondenty (37,8 %) určeno nevyhovující umístění.

[96] Vlastní zdroj.
[97] Vlastní zdroj.

Vzhledem k tomu, že stáří/opotřebování označilo 6 odborníků (7,3 %), byla hypotéza H2 potvrzena.

Graf 7: Účinnost poplachu na odrazení narušitele od dalšího postupu dle respondentů[98]



Otázka číslo 9 – Myslíte si, že vyhlášení poplachu odrazuje narušitele od jeho dalšího postupu? Graf 7 znázorňuje, že odborníci na PZTS věří v účinnost signalizovaného alarmu, který následně zabrání v dokončení protiprávního jednání. Zcela přesvědčeno o tom bylo 18 respondentů (22 %) a spíše ano zvolilo 48 dotázaných (58,5 %). Neutrální názor měl zastoupení u 11 % voleb. Negativních postojů se v součtu nashromáždilo pouze 7 (8,5 %). To je pro autora této práce překvapující, jelikož předpokládal opačný pohled. Ten vyjadřuje i stanovená hypotéza H3, jež byla 66 kladně odpovídajícími respondenty (80,5 %) vyvrácena.

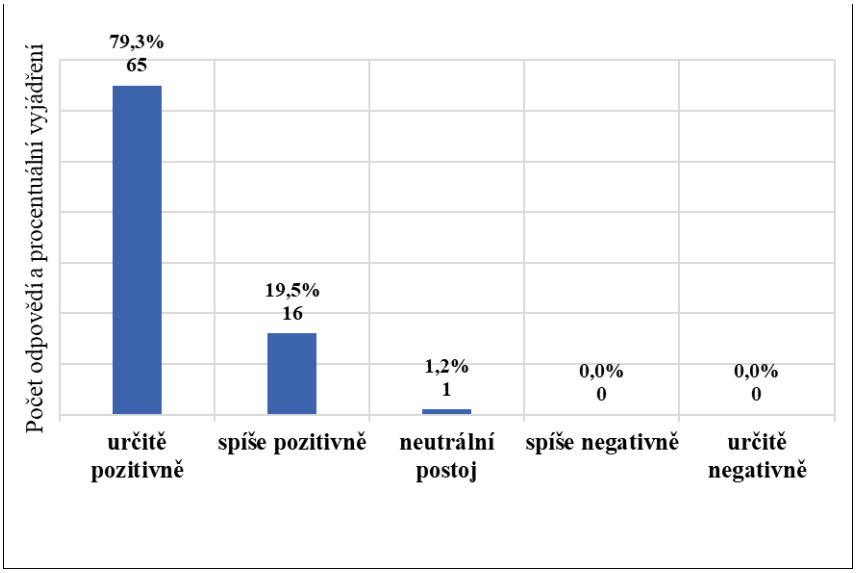
Otázka číslo 10 – Co pokládáte za největší motivaci, která vede k útoku narušitele? U odborníků existovala pouze jediná zásadní odpověď, kterou označilo 80 z nich (97,6 %). Obohacení je jimi považováno za primární hybnou sílu, kvůli které pachatel provádí protiprávní jednání. Tímto dominantním zjištěním se potvrdil smysl existence PZTS ve vztahu k ochraně majetkových hodnot. Další možnosti z výběru (vandalismus a sabotáž) dostaly každá jen 1 hlas. Nikdo z oslovených respondentů nevolil jako svou názorovou preferenci špionáž nebo dobrodružství.

Otázka číslo 11 – Setkal(a) jste se osobně s případem, kdy prvky ochrany detekovaly skutečného pachatele? Smysl jednoduchého dotazu, jenž měl volbu ano/ne,

[98] Vlastní zdroj.

tkvěl v doplnění informací z otázek 5 a 9. V nich bylo u odborníků zjištěno, že PZTS považují za účinný nástroj prevence kriminality, který má schopnost vyhlášením poplachu odradit narušitele od jeho dalšího postupu. Potvrzení funkčnosti a efektivity prvků ochrany bylo uskutečněno 75 respondenty (91,5 %) označením položky ano. Jen 7 odpovídajících osob (8,5 %) nemělo žádnou zkušenost s těmito pozitivními kvalitami PZTS.

Graf 8: Vnímání smyslu investic do pořízení poplachových zabezpečovacích a tísňových systémů dle názorů respondentů[99]



Otázka číslo 12 – Jak hodnotíte smysl investovat do pořízení poplachových zabezpečovacích a tísňových systémů? Zde došlo k jednoznačnému výsledku. Graf 8 ukazuje, že ve prospěch smysluplnosti PZTS jakožto investičního záměru se kladně vyjádřilo 81 odborníků (98,8 %). Pouze jediná odpověď byla neutrální. Negativní volba se nezaznamenala. Jedná se o potvrzení jednotnosti a stálosti názorů většiny respondentů na efektivitu, funkčnost i vhodnost vlastnit poplachový systém.

Dotazníkové šetření proběhlo v souladu se stanoveným vedlejším cílem této bakalářské práce. Jeho výstupy posoudily efektivitu prvků ochrany. Ta byla potvrzena kladnými názory odborných respondentů s dlouholetou praxí ve vztahu k PZTS, přičemž jako funkčně nejefektivnější označili pohybové čidlo. Pozitivní účinnost jednotlivých zabezpečovacích součástí při prevenci kriminality se stala volbou pro 97,6 % odpovídajících, což svědčilo o dominanci tohoto názoru. Hypotézy H1 i H2 byly zjištěními v otázkách číslo 6 a 8 potvrzeny. Výsledky otázky 9 vyvrátily hypotézu H3.

[99] Vlastní zdroj.

Závěr

Tato bakalářská práce se zaměřuje na prostředek situační prevence kriminality, který je autorovi velmi blízký, a to ve vztahu k jeho profesní orientaci a předchozímu elektrotechnickému vzdělání. Ne každý je však osobou znalou v tomto specifickém tématu. Proto se dílčí snahou práce stal vznik uceleného textu, jenž by užitečně posloužil všem kategoriím zájemců o danou problematiku. Teoretická část se tak zaměřuje na představení a historii PZTS. Následuje vysvětlení jejich významu při prevenci kriminality. Zásadní informace čtenáři poskytne výčet vybraných komponent poplachových systémů, který je doplněn o popis jejich funkce. Potřebný teoretický základ uzavírá kapitola o projektování a plánování těchto technických soustav. Ke splnění zamýšleného výsledku bylo nutné nastudovat dostupnou tematickou literaturu, provést rešerši vybraných kapitol a následně textové pasáže parafrázovat do přehledných celků. Takto vytvořený pojmový a poznatkový zdroj zároveň slouží jako podklad pro pochopení souvislostí v praktické části.

Hlavním cílem práce se zabýval kvantitativní empirický výzkum v kapitole 5. Vyhodnocoval poruchové incidenty jednotlivých součástí PZTS a posuzoval jejich vliv na spolehlivost a funkčnost ve vztahu k prevenci a zabránění protiprávního jednání. Prvním nutným krokem se stalo odhalení skutečné poruchovosti vybraných periferií. Během určeného sledovaného období bylo evidováno 1034 poruchových incidentů. Na jejich počtu se nejvýznamněji podílely 2 základní součásti poplachových systémů napojených na PCO. Rádiové PPZ mělo na svědomí 586 (56,7 %) a zabezpečovací ústředna 234 (22,6 %) poruch. Při posuzování poruchovosti byly odhaleny 2 převažující závady, které měly též výhradní spojitost se jmenovanými periferiemi. Ztráta spojení přes kabelové vedení (444 z 1034 případů) či rádiový přenos (267 z 1034 případů) stála v pozadí celkem u 68,7 % závad.

Výzkum dále řešil otázku vlivu periferií na nespolehlivost poplachových systémů. Bylo zjištěno 216 incidentů s tímto nežádoucím účinkem. Nejzásadněji se na nich opět podílely 2 nejporuchovější periferie. Rádiové PPZ mělo negativní dopad na spolehlivost 42,1 % (91 incidentů) a zabezpečovací ústředna přispěla hodnotou 34,3 % (74 incidentů). Dominující závady s vlivem na nespolehlivost byly taktéž stejné. Ztráty spojení přes kabelové vedení a rádiový přenos vykazovaly shodný počet 54 výskytů a měly v součtu přesně poloviční zastoupení u nespolehlivostních závad. Vzhledem k uvedeným faktům

a nezanedbatelnému množství incidentů s vlivem na nespolehlivost (216 z 1034 poruch) bylo z pohledu autora této práce nutné vytvořit opatření, jež vyjádřil na stranách 62–63.

Při vyhodnocení vlivu periferií na nefunkčnost poplachových systémů bylo ve sledovaném období zjištěno 53 závad, které způsobily negativní zásah do správného fungování příslušné části PZTS. Incidenty zabezpečovací ústředny zapříčinily 23 případů. Expandér vyvolal 10 případů. Všech 6 poruch u rozvodné krabice znamenalo vliv na nefunkčnost. Jejím spouštěčem byly primárně 3 druhy incidentů, a to nepovolené vypnutí (výhradně u zabezpečovací ústředny, 20 případů), tamper (14 případů) a porucha komunikace (pouze u expandéru, 10 případů). Výskyt poruch s vlivem na nefunkčnost měl takřka čtvrtinové zastoupení oproti těm, které se podílely na nespolehlivosti. Autor této práce zjistil jejich hlavní příčiny. Navrhnutá řešení a opatření podrobně rozvedl na konci kapitoly 5.

Dotazníkové šetření v kapitole 6 se zabývalo vedlejším cílem této práce. Posuzovalo efektivitu poplachových zabezpečovacích a tísňových prvků ochrany při prevenci kriminality. Prostřednictvím kladných názorů respondentů došlo k jejímu potvrzení. Hodnotu výsledku zvýšila odbornost odpovídajících osob a jejich dlouholetá praxe ve vztahu k PZTS. Reliabilitu posílilo zastoupení odpovědí od techniků, administrátorů i pracovníků PCO. Bylo zjištěno, že pro řádný výkon technické činnosti v PZTS je praxe nejzásadnějším zdrojem odborných znalostí. Respondenti dále označili pohybové čidlo jako funkčně nejefektivnější prvek ochrany, čímž potvrdili hypotézu H1. Dotazník také odhalil, že správná funkčnost, spolehlivost a nízká poruchovost jsou klíčovými pozitivními vlastnostmi při hodnocení prvků ochrany odborníky. Ti se ve vztahu k funkčnosti PZTS zaměřili hlavně na práci projektanta, kvalitu výstavby a obsluhu uživatelů. Při tomto zhodnocení potvrdili hypotézu H2 tím, že považovali nevyhovující umístění za faktor, jenž nejvíce snižuje schopnost účinného fungování prvků ochrany. Poslední hypotéza H3 byla vyvrácena vírou odborníků v to, že vyhlášení poplachu odradí narušitele od jeho dalšího postupu. Podle zjištění motivuje k takovému protiprávnímu chování zásadně obohacení. Význam existence PZTS jakožto prostředku zabezpečení majetkových hodnot byl tímto výzkumem tedy ověřen. Funkčnost a efektivita prvků ochrany byla následně potvrzena kladnou volbou dotázaných (91,5 %). Respondenti zcela dominantně zvolili pozitivní účinnost prvků ochrany při prevenci kriminality a smysluplnost investování do pořízení PZTS.

Práce zaznamenala i překvapivá zjištění. Prvním z nich byl fakt, že ve sledovaném období u otřesového čidla nedošlo k zaznamenání žádného incidentu, což se u jiné součásti nestalo. Dále lze za zajímavé označit vyhodnocování vlivu rádiového PPZ na nefunkčnost poplachových systémů. Do této kategorie u něj šlo zařadit pouze 2 z 586 případů. Dotazníkové šetření přineslo negativní jev v podobě neochoty oslovených projektantů a vývojářů účastnit se výzkumu. To samé platilo i pro výrobce a distributory PZTS. Překvapujícím poznatkem se při volbě nejefektivnějšího prvku ochrany stala absence odpovědí u otřesového čidla, jelikož v kapitole 5 byla zjištěna jeho bezporuchovost, spolehlivost a funkčnost. Autora osobně zaskočilo vyvrácení hypotézy H3, což v kontextu své praxe neočekával.

Tato práce může posloužit široké veřejnosti jako zdroj teoretických a praktických informací, jež doplní již existující tematickou literaturu. Hlavní aplikační potenciál se nalézá v zjištěných výstupech výzkumu. Jedná se o výsledky, které nabízejí možnost hlubšího rozpracování v rámci budoucího bádání. Zaměření na eliminaci hlavních příčin poruch s vlivem na nefunkčnost či nespolehlivost by jistě ocenila nejen odborná technická veřejnost, ale i samotný uživatel.

Seznam použitých zdrojů

Literární zdroje

1. ADÁMEK, M., BARČOVÁ, K., BITALA, P., MACH, V., ŠEVČÍK, J. *Dohledové videosystémy v bezpečnostních technologiích.* 1. vydání. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2022. 158 s. Edice SPBI Spektrum 109. ISBN 978-80-7385-263-4.
2. BOROŠ, M., MACH, V., ĎURICA, J. *Bezpečnostné systémy: mechanické zábranné prostriedky.* 1. vydanie. Žilina: Žilinská univerzita, 2022. 215 s. ISBN 978-80-554-1885-8.
3. BOROŠ, M., VEĽAS, A., LENKO, F., KUFFA, R. *Bezpečnostné systémy: elektronické systémy kontroly vstupov.* 1. vydanie. Žilina: Žilinská univerzita, 2023. 187 s. ISBN 978-80-554-2036-3.
4. BURDA, K. *Základy elektronických zabezpečovacích systémů.* Vydání první. Brno: Akademické nakladatelství CERM, 2017. 124 s. ISBN 978-80-7204-967-7.
5. FIRSTOVÁ, J., ZÁMEK, D. *Prevence kriminality: nedílná součást systému vnitřní bezpečnosti*. Vydání první. Praha: Wolters Kluwer ČR, 2021. 204 s. ISBN 978-80-7676-057-8.
6. HONEY, G. *Intruder Alarms.* Third edition. Oxford: Newnes, 2007. 368 s. ISBN 978-0-7506-8167-4.
7. JELÍNEK, J. et al. *Trestní zákoník a trestní řád: s poznámkami a judikaturou.* Vydání sedmé. Praha: Leges, 2017. 1312 s. Edice Glosátor. ISBN 978-80-7502-230-1.
8. KAMPOVÁ, K., LOVEČEK, T. *Modelovanie systémov ochrany objektov a ich optimalizácia.* 1. vydanie. Žilina: Žilinská univerzita, 2020. 161 s. ISBN 978-80-554-1753-0.
9. KŘEČEK, S. et al. *Příručka zabezpečovací techniky.* 4. vydání. Blatná: Blatenská tiskárna, 2021. 316 s. ISBN 978-80-87603-13-0.
10. KUČEROVÁ, H., HORZINKOVÁ, E. *Zákon o odpovědnosti za přestupky a řízení o nich a zákon o některých přestupcích: s komentářem a judikaturou.* Vydání první. Praha: Leges, 2017. 864 s. Edice Komentátor. ISBN 978-80-7502-211-0.
11. LOVEČEK, T. *Bezpečnostné systémy: bezpečnosť informačných systémov.* 1. vydanie. Žilina: Žilinská univerzita, 2007. 246 s. ISBN 978-80-8070-767-5.

12. LOVEČEK, T., MARIŠ, L., ŠISER, A. *Plánovanie a projektovanie systémov ochrany objektov*. 1. vydanie. Žilina: Žilinská univerzita, 2018. 285 s. ISBN 978-80-554-1482-9.
13. LOVEČEK, T., REITŠPÍS, J. *Projektovanie a hodnotenie systémov ochrany objektov*. 1. vydanie. Žilina: Žilinská univerzita, 2011. 281 s. ISBN 978-80-554-0457-8.
14. LOVEČEK, T., VEĽAS, A., ĎUROVEC, M. *Bezpečnostné systémy: poplachové systémy*. 1. vydanie. Žilina: Žilinská univerzita, 2015. 230 s. ISBN 978-80-554-1144-6.
15. LUKÁŠ, L. et al. *Bezpečnostní technologie, systémy a management II.* 1. vydání. Zlín: VeRBuM, 2012. 387 s. ISBN 978-80-87500-19-4.
16. SPURNÁ, I. *Počítačové sítě: praktická příručka správce sítě.* 1. vydání. Kralice na Hané: Computer Media, 2010. 180 s. ISBN 978-80-7402-036-0.
17. TKOTZ, K. et al. *Příručka pro elektrotechnika.* 2. doplněné vydání. Přeložil Jiří HANDLÍŘ. Haan-Gruiten: Verlag Europa-Lehrmittel, 2017. 624 s. ISBN 978-3-8085-3034-4.
18. VEĽAS, A. *Poplachové systémy: poplachové prenosové systémy a zariadenia.* 1. vydanie. Žilina: Žilinská univerzita, 2015. 137 s. ISBN 978-80-554-1134-7.
19. VEĽAS, A., ZVAKOVÁ, Z., BOROŠ, M. *Bezpečnostné systémy: fyzická ochrana objektov.* 1. vydanie. Žilina: Žilinská univerzita, 2021. 203 s. ISBN 978-80-554-1805-6.

Legislativní dokumenty

1. ČESKO. *Úplné znění zákona č. 40/2009 Sb., trestní zákoník.* Vydání třinácté. Praha: Armex, 2024. 196 s. ISBN 978-80-87451-95-3.
2. ČESKO. *Úplné znění zákona č. 273/2008 Sb., o Policii České republiky; Úplné znění zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich; Úplné znění zákona č. 251/2016 Sb., o některých přestupcích.* Vydání dvacáté druhé. Praha: Armex, 2024. 132 s. ISBN 978-80-87451-97-7.

Seznam zkratek

AES – Advanced Encryption Standard (symetrická bloková šifra)

BTS – Base Transceiver Station (základnová vysílací a přijímací stanice)

CCD – Charge Coupled Devices (obvody vázané nábojem)

CMOS – Complementary Metal-Oxide-Semiconductor (typ polovodičové technologie)

CPU – Central Processing Unit (centrální procesorová jednotka)

ČSN EN – česká technická norma (identická s evropskou)

DPPC – dohledové a poplachové přijímací centrum

DPS – Digital Pixel Sensor (druh CMOS obrazového snímače)

DVR – Digital Video Recorder (digitální videorekordér)

EKV – elektronická kontrola vstupu

EPS – elektrická požární signalizace

FTP – Foil Twisted Pair (kroucená dvojlinka s jedním společným stíněním)

GSM – Global System for Mobile Communications (standard pro digitální mobilní sítě)

HF – High Frequency (vysoká frekvence)

IMEI – International Mobile Equipment Identity (mezinárodní identifikace mobilního zařízení)

IP – Internet Protocol (internetový komunikační protokol)

LAN – Local Area Network (místní počítačová síť)

LED – Light Emitting Diode (dioda vyzařující světlo)

LF – Low Frequency (nízká frekvence)

MW – Microwave Detector (mikrovlnné čidlo)

NVR – Network Video Recorder (síťový videorekordér)

PCO – pult centralizované ochrany

PIR – Passive Infrared Detector (pasivní infračervené čidlo)

PoE – Power over Ethernet (napájení po datovém síťovém kabelu)

PPC – poplachová přenosová cesta

PPS – poplachové přenosové systémy

PPZ – poplachové přenosové zařízení

PZTS – poplachové zabezpečovací a tísňové systémy

QR – Quick Response (rychlá odpověď)

RAM – Random Access Memory (paměť s náhodným přístupem)

RFID – Radio Frequency Identification (identifikace na rádiové frekvenci)

RKZ – rozvodná krabice

RSA – Rivest, Shamir, Adleman (asymetrická šifra s veřejným klíčem)

SIM – Subscriber Identity Module (modul pro identifikaci účastníka)

SMS – Short Message Service (služba krátkých textových zpráv)

STP – Shielded Twisted Pair (stíněná kroucená dvojlinka)

UHF – Ultra High Frequency (velmi vysoká frekvence)

US – Ultrasonic Detector (ultrazvukové čidlo)

USB – Universal Serial Bus (univerzální sériová sběrnice)

UTP – Unshielded Twisted Pair (nestíněná kroucená dvojlinka)

VSS – Video Surveillance Systems (dohledové videosystémy)

WAN – Wide Area Network (rozlehlá počítačová síť)

3DES – Triple Data Encryption Standard (symetrická bloková šifra)

Seznam tabulek a grafů

Seznam příloh

Přílohy

Příloha I: Vzor nevyplněného dotazníku

Dobrý den, vážení respondenti,

dovoluji si Vás požádat o vyplnění krátkého dotazníku. Ten poslouží jako dílčí zdroj dat pro výzkumnou část mojí bakalářské práce. Je určen pouze osobám vykonávajícím odbornou činnost v oblasti výstavby a servisu poplachových zabezpečovacích a tísňových systémů. Odpovědět na všech 12 otázek nezabere více než 5 minut. Zachování anonymity je zaručeno. Děkuji předem za poskytnutí cenných informací. Vážím si jich.

S pozdravem a úctou
Zdeněk Rídl

1. Jaká je Vaše pracovní pozice ve vztahu k poplachovým zabezpečovacím a tísňovým systémům?
   Vyberte jednu odpověď.
   - vývojář
   - projektant
   - administrátor
   - technik
   - pracovník pultu centralizované ochrany

2. Kdo je Vaším současným zaměstnavatelem?
   Vyberte jednu odpověď.
   - stát
   - firma
   - jsem OSVČ

3. Kolik let praxe máte ve vztahu k poplachovým zabezpečovacím a tísňovým systémům?
   Vyberte jednu odpověď.
   - méně než 10 let
   - 10 až 20 let
   - 20 až 30 let
   - více než 30 let

4. Co je zdrojem Vašich odborných znalostí o poplachových zabezpečovacích a tísňových systémech?
   Vyberte jednu nebo více odpovědí.
   - škola
   - samostudium
   - praxe

5. Vnímáte nasazení poplachových zabezpečovacích a tísňových prvků ochrany jako účinný prostředek prevence kriminality?
   Vyberte jednu odpověď.
   - ano
   - ne

6. Který prvek ochrany považujete za funkčně nejefektivnější?
   Vyberte jednu odpověď.
   - magnetický kontakt
   - pohybové čidlo
   - akustický detektor rozbití skla
   - tísňový hlásič
   - otřesové čidlo

7. Zvolte pozitivní vlastnost, kterou při hodnocení prvků ochrany pokládáte za klíčovou.
   Vyberte jednu odpověď.
   - nízká cena
   - malá poruchovost
   - dlouhá životnost
   - snadná instalace
   - správná detekce narušení

8. Co podle Vás nejvíce snižuje schopnost účinného fungování prvků ochrany?
   Vyberte jednu odpověď.
   - stáří/opotřebování
   - nekvalita výroby
   - nevyhovující umístění
   - chybná montáž

- špatná programová konfigurace
- nesprávná obsluha
- vliv počasí

9. Myslíte si, že vyhlášení poplachu odrazuje narušitele od jeho dalšího postupu?
   Vyberte jednu odpověď.
   - určitě ano
   - spíše ano
   - neutrální postoj
   - spíše ne
   - určitě ne

10. Co pokládáte za největší motivaci, která vede k útoku narušitele?
    Vyberte jednu odpověď.
    - obohacení
    - vandalismus
    - špionáž
    - dobrodružství
    - sabotáž

11. Setkal(a) jste se osobně s případem, kdy prvky ochrany detekovaly skutečného pachatele?
    Vyberte jednu odpověď.
    - ano
    - ne

12. Jak hodnotíte smysl investovat do pořízení poplachových zabezpečovacích a tísňových systémů?
    Vyberte jednu odpověď.
    - určitě pozitivně
    - spíše pozitivně
    - neutrální postoj
    - spíše negativně
    - určitě negativně