Zabezpečení komunikačních kanálů poplachového zabezpečovacího a tísňového systému a dozorového a poplachového přijímacího centra

Security of I&HAS and MARC communication channels

Michal Přikryl

Bakalářská práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

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

Jméno a příjmení:	**Michal PŘIKRYL**
Osobní číslo:	**A09628**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Zabezpečení komunikačních kanálů poplachového zabezpečovacího a tísňového systému a dozorového a poplachového přijímacího centra**

Zásady pro vypracování:

1. **Popište dozorové a poplachové přijímací centrum (DPPC) a jeho vývoj.**
2. **Uveďte a popište způsoby propojení DPPC a ústředny poplachového zabezpečovacího a tísňového systému (IHAS), postup při zapojení a druhy komunikačních rozhraní.**
3. **Uveďte a popište možnosti narušení komunikace mezi ústřednou a DPPC.**
4. **Uveďte a popište technické a programové prostředky pro narušení komunikace mezi ústřednou a DPPC.**
5. **Identifikujte a popište možné rezervy v zabezpečení přenosu mezi ústřednou a DPPC.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 2. S.l.: Cricetus, 2003, 351 s. ISBN 80-902-9382-4.**
2. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management III. 1. vyd. Zlín: VeRBuM, 2013, 456 s. ISBN 978-80-87500-35-4.**
3. **KAMENÍK, Jiří a František BRABEC. Komerční bezpečnost: soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. Vyd. 1. Praha: ASPI, 2007, s. 78-79. ISBN 9788073573096.**
4. **DRGA, Rudolf a Vladimír LAUCKÝ. Speciální technologie komerční bezpečnosti. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012, 224 s. ISBN 978-80-7454-146-9.**
5. **VALOUCH, Jan. Projektování bezpečnostních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. ISBN 978-80-7454-230-5.**
6. **IVANKA, Ján. Systemizace bezpečnostního průmyslu. Zlín: Univerzita Tomáše Bati ve Zlíně, 2011. ISBN 978-80-7454-122-3.**
7. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 81 s. ISBN 978-80-7318-889-4.**

Vedoucí bakalářské práce: **Ing. Petr Navrátil, Ph.D.**
Ústav řízení procesů

Datum zadání bakalářské práce: **7. března 2014**

Termín odevzdání bakalářské práce: **10. června 2014**

Ve Zlíně dne 7. března 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Předložená bakalářská práce s názvem „Zabezpečení komunikačních kanálů poplachového zabezpečovacího a tísňového systému a dozorového a poplachového přijímacího centra“ se věnuje zapojení a zabezpečení komunikačních kanálů mezi I&HAS a DPPC a pojednání o odolnosti konkrétních komunikačních rozhraní. Práce je složena ze dvou částí. První část je zaměřena na DPPC a jeho vývoj. Druhá část je věnována propojení DPPC a ústředny I&HAS, postupu při zapojení, druhům komunikačních rozhraní a zabezpečení přenosu. Cílem práce je pojednat o důsledcích při přerušení komunikace nebo alespoň najít rezervy v bezpečnosti přenosu.

Klíčová slova: I&HAS, DPPC

ABSTRACT

The submited bachelor thesis, titled: "Security of I&HAS and MARC communication channels" analyses connection and security of communication channels between I&HAS and MARC and attempts to test and discuss the resistance of specific communication interfaces. The project consists of two chapters. The first chapter describes MARC specification and its evolution. The second part examines the process of linking I&HAS with MARC, the connection procedure, types of communication interfaces and transmission security. The objective of this bachelor thesis is to discuss the results of the disrupting attempts or at least reveal gaps in the transmission security.

Keywords: I&HAS, MARC

Vědět mnoho je nebezpečné, vědět málo také. (Albert Einstein)

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….……

OBSAH

ÚVOD

Už od nepaměti se lidská civilizace potýká s kriminalitou, zloději a krádežemi. Marketingové využití a poptávka po ochraně dala vzniku oboru bezpečnostní technologie za své a díky tomu si tato mladá sféra našla své uplatnění. Trh již v dnešní době silně zastoupen firmami z této oblasti. Například jen na Zlínsku je více než deset firem, nabízejících služby v oblasti bezpečnosti. Ve zkratce řečeno, trh se jeví velmi zaplněn a vznikají pouze otázky ohledně spolehlivosti a kvalit jednotlivých firem, jejich služeb a výrobků. V této bakalářské práci ovšem nebude hlavní náplní srovnávání výrobců a provádění analýz trhu, ale bude se klást důraz na zabezpečení samotného zabezpečovacího systému, který má chránit například dům před vloupáním. Na otázku proč, bych jednoznačně odpověděl tak, že jak postupují kupředu technologie a elektronika, tak se vylepšují a profesionalizují postupy osob při kriminální činnosti. Podle mého názoru je potřeba držet s nimi krok a reagovat inovacemi v technologiích. Bohužel platí pravidlo, že zloděj je o krok napřed před svou překážkou. Ať jde o vloupání, krádež auta, či hackerský útok v jakékoliv formě. Potřeba reagovat je zde na místě a několik let starý systém nebo kód může být kdykoli prolomen a návod do několika okamžiků publikován na internetu.

Jelikož je toto téma velmi obsáhlé, rozhodl jsem se zaměřit na DPPC a na přenos zpráv z poplachových zabezpečovacích systémů (dále I&HAS) na dozorové a poplachové přijímací centrum (dále DPPC) s důrazem na zabezpečení tohoto přenosu. Je známo hned několik způsobů komunikace. Zaměřím se zejména na přenos využívající sítě GSM. Nejenže lze signál GSM snadno sabotovat pomocí pouhé rušičky, ale jak se dá zjistit z různých zdrojů, způsob kódování GSM je dle hackerských kruhů zaostalý a má mnoho bezpečnostních děr.

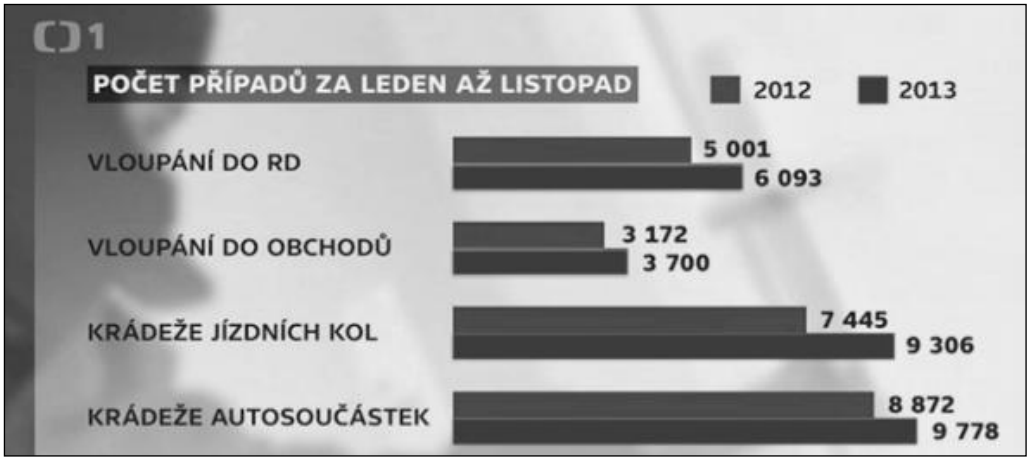
Cílem práce je na základě dostupných informací provést zkoumání právě dostupných technologií a postupů, které umožňují do jisté míry negativně ovlivnit nebo dokonce sabotovat přenos zpráv z I&HAS na DPPC. Na základě osobních schůzek s jednateli firem zjistit, zda jsou si bezpečnostní agentury ve Zlíně vědomy rizika narušení přenosu poplachových zpráv, a zda aktivně využívají vlastní technická protiopatření. Závěrem práce uvedu několik realizovatelných řešení, které minimalizují hrozící rizika sabotáže přenosu zprávy na DPPC.

I. TEORETICKÁ ČÁST

1 DPPC - DOZOROVÁ A POPLACHOVÁ PŘIJÍMACÍ CENTRA

Dozorová a poplachová přijímací centra, dále jen DPPC, jsou významnou složkou bezpečnostních systémů v České republice. Využívá je nejen Policie ČR, ale i Hasičský záchranný sbor, průmyslové podniky a soukromé bezpečnostní služby. Funkce DPPC spočívá v neustálém dohledu a přijímání poplachových zpráv a signálů z lokálních zabezpečovacích zařízení (např.: ústředna ve skladu), jejich následná vyhodnocení a příslušné reakce, například vyslání vlastní zásahové jednotky na dané místo.

Policejní prezídium odhalilo ve své zprávě, která byla zveřejněna v pořadu Otázky Václava Moravce vysílaného dne 15. 12.2013, údaje za rok 2012 a 2013 týkající se případů vloupání a krádeží. Konkrétní data jsou uvedena na následujícím obrázku.[1]



Obr. 1 Statistika případů za leden až listopad 2012 a 2013

Počet vloupání do nemovitostí tedy stále roste. Tyto skutečnosti vyvolávají u občanů stále se zvyšující potřebu chránit sebe i svůj majetek. V tomto negativním důsledku vznikl marketingově velmi lukrativní prostor pro soukromé bezpečnostní agentury, které nabízí z širokého spektra služeb možnost zabezpečení objektů i připojení na DPPC, a tím tuto všeobecnou potřebu naplňují.

1.1 Terminologie

Dozorová a poplachová přijímací centra je nový název pro pult centrální ochrany v platnosti od 1. ledna 2011 dle nové normy **ČSN EN 50518-1**. Celý anglický název je Monitoring and Alarm Receiving Centre (MARC). Světově používaná zkratka je známa pod pojmem ARC (Alarm Receiving Centre). Starý český název pult centrální ochrany

(PCO) se i tak nadále hojně využívá zejména u firem na mnoha internetových portálech při nabídkách svých služeb a ve volných konverzacích lidí z bezpečnostního oboru vyjma akademické půdy, kde se apeluje používat název nový. V této bakalářské práci tedy budu využívat název aktuální a příslušnou zkratku DPPC.

1.2 Historie a vývoj

První známky o vzniku DPPC sahají do zemí dřívějšího východního bloku, kde se začaly vyrábět pod názvem NĚVA Sovětský svaz. Obdobné zařízení na trh uvedlo Bulharsko pod názvem RONA na základě souhlasu k výrobě v rámci RVHP. Do České republiky se tyto výrobky dovážely v letech 1974-1976.

Historicky první DPPC začal používat v tehdejší ČSSR útvar Služby ochrany majetku Veřejné bezpečnosti, který tak zabezpečoval střežení strategicky významných státních institucí a objektů, čerpacích stanic, kulturních objektů, větších poštovních poboček a bank. K přenosu zpráv byla používána telefonní linka v hovorovém pásmu. Střežené objekty byly propojeny s městskou telefonní ústřednou a napojeny na DPPC policie. Samostatné zapínání střežení objektu se prováděla na stanovištích příslušníky Veřejné bezpečnosti, ale pouze mimo provozní dobu objektu, protože zastřežením objektu se přerušila možnost využívání telefonní linky k běžnému hovoru.

DPPC se skládalo pouze ze spínačů a kontrolních žárovek, jež signalizovaly stav zastřežení objektu. Žádné další dělení na podskupiny nebo zóny nebylo možné ani jakákoliv archivace přijatých zpráv.

Ještě v roce 1989 pracovníci Služby ochrany objektů střežili tímto způsobem téměř osm tisíc objektů. Větší pokrok byl zaznamenán koncem osmdesátých let, kdy se vyřešila možnost přenosu zpráv v nad-hovorovém kmitočtovém pásmu 20kHz.

V roce 1991 bylo na první porevoluční výstavě bezpečnostních technologií InterAlarm, která je dnes známa jako veletrh PRAGOALARM, představeno nově vyvinuté nad-hovorové dohledové centrum GENOVA.

Po roce 1989 se DPPC v důsledku zvýšené poptávky nestátních komerčních objektů rozšířily i do oblasti komerční bezpečnosti. Součástí služeb poskytujících DPPC se staly i zásahové jednotky, které zaštitovaly dojezdy v relativně krátkém čase a zajištění napadeného nebo poškozeného objektu.[2]

1.3 Výhody napojení

- Objekt je nepřetržitě pod kontrolou dohledového centra.
- Při narušení objektu je klient ihned informován z dohledového centra a následně je vyslána výjezdová skupina. Na základě druhu vzniklé situace jsou přivolány složky Policie ČR i záchranné složky.
- Do příjezdu Policie ČR zajistí narušený objekt výjezdová skupina DPPC, která v případě úrazu či zranění poskytne na místě postiženým osobám první pomoc, než přijedou záchranné složky.
- Zákazníkem placená agentura, poskytující své služby zajišťuje i veškeré revize, servisy a opravy.
- Objekty napojené na DPPC spadají do kategorie méně rizikových z hlediska pojišťoven.

1.4 Kvalita v poskytování služeb v bezpečnostním sektoru

Kromě chybějícího zákona o soukromých bezpečnostních službách neexistuje v ČR žádná povinná registrační autorita pro pracoviště DPPC a neexistuje tedy žádný ucelený přehled o kvalitě a způsobu poskytování těchto služeb. Jediný přehled má NBÚ, kde je na DPPC napojen objekt podléhající certifikaci NBÚ podle zákona 412/2005 Sb. a ve znění pozdějších předpisů.[3]

V posledních letech panuje v kruzích bezpečnostních služeb snaha tyto nedostatky eliminovat. Zatím bez úspěchu. Důvod proč se zákon nepodařil v roce 2013 prosadit, byl obhájen [Stanovisko komise pro hodnocení dopadů regulace k návrhu zákona o soukromé bezpečnostní činnosti, 4. únor 2013] slovy: „*Spolu s četnými odkazy na zdůvodnění jednotlivých opatření odkazem na konzultace s profesními sdruženími (bez dalších důvodů) však návrh vyvolává otázku, zda nemůže jeho nezamýšleným, či dokonce zamýšleným, účinkem být omezení konkurence na trhu SBS*.“. Zpráva se vyjadřuje k dříve vypracované Zprávě o dopadu regulace, obsahující výčet nedostatků, fakta o negativních poměrech na českém trhu ve sféře bezpečnostních služeb a legislativní návrh zákona pro bezpečnostní služby. Výtah z obou dokumentů je součástí přílohy této bakalářské práce.

Poslední informace o dalším postupu s již vypracovaným a přepracovaným Návrhem zákona o soukromé bezpečnostní činnosti a o změně souvisejících zákonů končí datem 30. května 2013, kdy bylo při zasedání legislativní rady vlády jednání přerušeno.[4]

1.4.1 Kvalita služeb DPPC

Kvalita obsluhy nabízí téma k diskusi a při širokém zastoupení bezpečnostních agentur poskytujících napojení na DPPC v ČR se nabízí otázka, zda není v některých případech nevyhovující. Základní požadavky dle internetových nabídek pro uchazeče o místo dispečera DPPC jsou trestní bezúhonnost, základní znalost PC a středoškolské vzdělání ukončené maturitou nebo střední odborné vyučení.

Některé firmy využívají státem zavedené úlevy na daních při zaměstnávání osob zdravotně znevýhodněných nebo pobírajících invalidní důchod v rozmezí ID 1-3. Existují ale i agentury, které mají ve své nabídce na toto pracovní místo jako základní požadavek právě příjem pouze zdravotně znevýhodněných osob. Je k zamyšlení, zda tento aspekt nemá vliv na kvalitu poskytovaných služeb. Nicméně doposud nebyla publikována žádna studie, která by pojednávala o vztahu těchto skutečností k výsledné kvalitě práce zaměstnance. Je zde zcela na místě podotknout, že na toto téma se negativně zmiňuje i Zpráva o stavu soukromých bezpečnostních služeb vydaná už v roce 2009 Unií SBS České republiky.

Další negativní faktor je skutečnost, že bezpečnostní agentury na své DPPC napojují velký počet objektů, ale k dispozici mají omezený počet zásahových vozidel. V ojedinělých případech, že by došlo k více poplachům v krátkém intervalu, může hrozit, že nebude mít na více místech, kdo zasáhnout.[5]

Na základě schůzky s jednatelem bezpečnostní agentury SG'3 s.r.o. panem Michalem Cíchou musím konstatovat, že i přes předchozí tvrzení, je potřeba si uvědomit, že prakticky nelze na jedno DPPC omezovat počet objektů do takové míry, aby je daná bezpečnostní agentura dokázala při takto vzniklé situaci efektivně obsloužit a neprodleně jednat, protože by daná agentura nedokázala pokrýt finanční náklady spojené s provozem. Tyto případy, že nastane více potvrzených poplachů, ke kterým musí být proveden výjezd v jeden okamžik, jsou velmi nepravděpodobné, nicméně při takto vzniklé situaci se nabízí spolupráce s Policií ČR.

Nemalým měřítkem kvality v poskytování služeb DPPC je platná technická norma **ČSN EN 50518** stanovující požadavky pro DPPC.

1.4.2 Personální podmínky dispečera DPPC a člena zásahové jednotky

Měřítko v kvalitě obsluhy udává platná norma **ČSN EN 50518-3**. Z hlediska personálního obsazení pracovišť DPPC je trvalý požadavek na obsazení odborně vyškoleným personálem. Zejména členové zásahové jednotky musí splňovat náročná kritéria:

- výsledky psychodiagnostického vyšetření odpovídajícího nasazení,
- umět řešit mimořádné situace,
- umět pracovat ve stresu a v časové tísni,
- dokonalá technická znalost DPPC,
- fyzická zdatnost,
- perfektní znalost metodiky zásahu,
- znalost místopisu střežených objektů,
- zběhlost a zkušenost při používání zbraně a ostatních donucovacích prostředků,
- umění komunikace,
- psychická odolnost,
- naprostá disciplinovanost.[6]

1.5 Provozní postupy při práci dispečera s DPPC

Dispečer DPPC se musí řídit danými pravidly, předpisy a dodržovat zásady provozu pro správný a bezchybný chod DPPC.

1.5.1 Dostupnost předpisů pro dispečera

Pro provoz DPPC musí být všem dispečerům dostupné předpisy s obsahem:

- zpracování signálů,
- správa databáze,
- postupy při evakuaci,
- testování,
- vstup a odchod z DPPC,
- průběh provozu a nouzový stav.

1.5.2 Vstup a odchod

Pro všechny osoby bez výjimky platí předpis pro vstup a odchod, který je součástí dokumentovaných postupů a je řízen dispečerem zevnitř DPPC.

1.5.3 Správa databáze

Každoročně je vyžadován audit shody akreditovaným orgánem podle dané normy. Správa databáze je řízena danou normou. Dále musí být vedena dokumentace, která se týká manipulace s údaji a musí být vypracován jasný postup, který se týká údržby, ochrany, přemisťování, ukládání, doby platnosti zabezpečení, zálohování a případné likvidace. Každé DPPC si musí vést záznamy o pravidelných kontrolách a údržbě technického zařízení.

1.5.4 Nouzové stavy

V souladu s **ČSN EN 50518-2** musí existovat plán pro nouzové stavy a výjimečné stavy. V průběhu řešení nouzového stavu musí být umožněn monitoring. V případě dočasného vypadnutí DPPC z provozu musí existovat nouzový plán a musí řešit tyto situace:

- útok zvenčí,
- požár,
- povodeň,
- vodovodní havárie,
- vchod/východ,
- plyn,
- komunikace,
- přepadení,
- monitoring bezpečnosti personálu,
- signály elektronických ochranných systémů,
- CCTV.

1.5.5 Postupy při evakuaci

Musí být vytvořen plán evakuace a v této oblasti musí existovat dokumentovaný výcvik, který není starší než šest měsíců.[3]

1.5.6 Bezpečnost při práci

Dispečerovi musí být předány základní znalosti o ochraně proti úrazu elektrickým proudem či před energetickým nebezpečím. Zejména mu nemůže být povolen přístup k neizolovaným částem obvodů s bezpečným malým napětím (Safety Extra Low Voltage: SELV), obvodům s omezeným proudem a k izolaci vodičů v obvodech malého napětí. Operátorovi DPPC musí být zabráněno v přístupu k neizolovaným obvodům a obvodům s nebezpečným napětím a k jejich funkční nebo základní izolaci. Požadavek na zajištění základních funkcí dispečinku DPPC vyžaduje zvýšenou pozornost, zejména při přechodu na napájení z náhradního zdroje.

DPPC se řadí z hlediska odolnosti zařízení proti přepětí a nadproudu dle **ČSN EN 62305** do 1. kategorie, kde jsou vysoké požadavky na bezpečnost, spolehlivost a nízkou poruchovost provozu. Je zde nutná ochrana proti přepětí bleskojistkami na konci sdělovacího vedení (anténní napáječ, účastnická linka). Bleskojistky mohou být integrovanou částí zařízení. Jejich hlavní úlohou je zamezit vzniku většího rozdílu potenciálů v interních obvodech.[6]

1.6 Základní nabídky služeb DPPC

DPPC disponuje širokým zastoupením nabízených služeb. Mezi základní nabídky, které DPPC poskytuje, patří:

- dálkový monitoring I&HAS,
- dálkový monitoring CCTV,
- zprostředkování výjezdu jednotky ke kontrole stavu objektu,
- zajištění objektu proti dalším škodám,
- kontrola zakódování objektu ve stanoveném čase,
- služba TÍSEŇ sloužící k rychlému přivolání pomoci.

1.6.1 Poskytování služeb v dopravě

Z hlediska poskytování služeb v dopravě DPPC nabízí tři možnosti:

- navigace zásahové jednotky k vozidlu,
- dálkové zastavení vozidla, které je klasifikováno jako odcizené,
- sledování vozidla pomocí GPS.

1.6.2 Další využití a nepoplachové funkce

Kromě poplachového využívání střežených objektů DPPC také nabízí nepoplachové služby:

- dálkové ovládání topení,
- hlídání teplot chladících zařízení,
- monitoring klimatizace, vzduchotechniky, telefonních, elektrických a internetových sítí.
- nouzové stavy a kontinuita pracovního provozu.

1.7 Rozdělení DPPC

Rozdělení DPPC lze chápat ze dvou hledisek. Podle specializace pracovišť, které využívají specifické instituty dle charakteru vlastní potřeby, a podle koncepce.

1.7.1 Rozdělení dle specializace pracovišť

Dle specializace pracovišť se klasifikují DPPC zejména kvůli typu vlastnící instituce:

- pracoviště Policie ČR, kde se soustřeďují informace z technických bezpečnostních systémů,
- pracoviště obecní policie (městské),
- pracoviště Hasičského záchranného sboru, kde se soustřeďují informace o vzniklém požárním nebezpečí získaném z technických prostředků PZTS,
- pracoviště firem podnikajících v průmyslu komerční bezpečnosti, kde je současně organizován represivní zásah a komunikace se zákazníkem i součinnostními složkami (Policie ČR, Hasičský záchranný sbor),
- pracoviště integrovaného záchranného systému.

1.7.2 Rozdělení dle koncepce

DPPC jsou koncipovány dvěma způsoby:

- součást osobního počítače,
- autonomní systém.

Autonomní systém je konstruován tak, aby byl schopen samostatně plnohodnotného provozu. Prvky autonomního systému zahrnují tiskárnu, displej a napájecí zdroj se zálohovaným akumulátorem. Využívají se různé softwarové kombinace pro komfortnější komunikaci obsluhy s počítačem. Přední využití mají softwarové kombinace, které umožňují sledování doplňkových funkcí, především stav akumulátorů, detektorů, napájení a ústředny.

Pro práci operátora DPPC se využívá zobrazování map, trasy a přístupu do místa střeženého objektu. Stejně tak přímo jednotlivých střežených budov, místností a podlaží. V případě výpadku napájení je zařízení mimo tuto signalizaci schopno předat nasbírané informace dispečinku. Při výpadku napájení na dispečinku je zařízení zálohováno z akumulátoru, který umožňuje překlenout bez problému i výpadek delší, jak 24 hodin.

Konstrukce integrovaných systémů do PC vyžaduje k provozu plnou podporu osobního počítače, neboť je jeho integrální součástí. Pro provoz je nezbytné, aby fungovaly všechny části počítače. Při poruše harddisku, na němž je základní software, zkolabuje funkce DPPC. Totéž se stane v případě poruchy softwarového charakteru, který vzhledem ke složitosti operačního systému není zcela vyloučen. Rovněž při výpadku síťového napětí je složitější zajistit bezporuchový provoz. Kromě nákladného napájení existuje i napájení kryjící pouze dobu nastartování benzinového nebo naftového generátoru. Jedná se o velmi složitý a drahý systém.

1.8 Vliv propojení objektu s DPPC při řešení pojistné události

Při vzniku pojistné události v pojištěném objektu, který byl cílem krádeže a je toto připojištění součástí smlouvy, vzniká nárok na pojistné plnění, které nabývá výše dle překonané úrovně zabezpečení v daném objektu nebo uzavřené místnosti. Například ČSOB doplňkové připojištění Pojištění domácnosti má v pojistných podmínkách pevně stanovené výše limitů pro plnění pojistné události dle následujícího obrázku. [7]

Charakter a kvalita konstrukčních prvků zabezpečení uzavřeného prostoru ve smyslu VPP PMO 2014, které pachatel v době vzniku pojistné události překonal		Kód stupně zabezpečení	Limit pojistného plnění v Kč (dále jen „LPP“)		
			LPP bez zabezpečení prostoru místa pojištění EZS	**LPP** s dalším zabezpečením prostoru místa pojištění	
				EZS na plášť nebo **na mobil**	**EZS na PCO**
DVEŘE nebo **BEZPEČNOSTNÍ DVEŘE** nebo **VRATA**	**Dveře** ve sklepních kójích, které jsou uzavřené a uzamčené	**Z1**	**50 000**		
	Dveře nebo **vrata** jsou uzavřena a uzamčena: • zámkem s cylindrickou vložkou nebo • dozickým zámkem nebo • visacím zámkem.	**Z2**	**100 000**	**150 000**	**500 000**
	Dveře nebo **vrata** jsou uzavřena a uzamčena: • bezpečnostním zámkem	**Z3**	**300 000**	**450 000**	**1 500 000**
	Dveře nebo **vrata** jsou uzavřena a uzamčena: • bezpečnostním zámkem a dalším zámkem, který uzamyká dveře v jiném místě než bezpečnostní zámek.	**Z4**	**500 000**	**750 000**	**2 500 000**
	Dveře nebo **vrata** jsou uzavřena a uzamčena: • bezpečnostním zámkem s min. 3-bodovým rozvorovým zámkem nebo • bezpečnostním zámkem a závorou nebo • elektrickým ovládáním - blokací motoru.	**Z5**	**700 000**	**1 000 000**	**3 500 000**
	Bezpečnostní dveře jsou uzavřeny a uzamčeny: • bezpečnostním zámkem s min. 5-bodovým rozvorovým zámkem.	**Z6**	**1 000 000**	**1 500 000**	**5 000 000**
OTVOROVÉ VÝPLNĚ s výjimkou dveří nebo vrat	**Otvorová výplň**, jejíž dolní část je umístěna **níže než 2,5 m** nad okolním terénem nebo nad přiléhajícími a snadno dostupnými konstrukcemi (schodiště, ochoz, přístavky apod.) **bez mechanického zabezpečení otvorových výplní**.	**Z7**	**100 000**	**150 000**	**500 000**
	Otvorová výplň, jejíž dolní část je umístěna **níže než 2,5 m** nad okolním terénem nebo nad přiléhajícími a snadno dostupnými konstrukcemi (schodiště, ochoz, přístavky apod.) **a je dále opatřena mechanickým zabezpečením otvorových výplní** (viz výklad pojmů VPP PMO 2014).	**Z8**	**1 000 000**	**1 500 000**	**5 000 000**
	Otvorová výplň, jejíž dolní část je umístěna **výše než 2,5 m** nad okolním terénem nebo nad přiléhajícími a snadno dostupnými konstrukcemi (schodiště, ochoz, přístavky apod.) **bez mechanického zabezpečení otvorových výplní**.	**Z9**	**1 000 000**	**1 500 000**	**5 000 000**

Obr. 2 Stupně zabezpečení a výše limitů pojistného plnění[7]

Jak je z obrázku patrné, limity pojistných plnění pro objekt, který je napojen na DPPC, jsou několikanásobně vyšší. Ovšem limit pojistného plnění je pouze maximální hodnota a stejně jako ostatní horní limity pojistných plnění mají ať už záměrně nebo nezáměrně pozitivní vliv na žadatele o pojištění. Taktéž slouží jako silný vodící faktor pro pojišťovacího zprostředkovatele při demonstraci kvality nabízené pojistné smlouvy.

2 I&HAS – POPLACHOVÉ ZABEZPEČOVACÍ A TÍSŇOVÉ SYSTÉMY

Pojem I&HAS z anglického názvu Intrusion and Hold-up Alarm System obsahuje soubor systémů určených pro detekci vniknutí a přepadení, aktivaci tísňových prostředků, zpracování informací, vyhlášení poplachů a prostředky k ovládání systému. Patří zde například detektory, tísňové hlásiče, ústředny, prostředky poplachové signalizace, přenosové zařízení, zapisovací zařízení a ovládací zařízení, jejichž prostřednictvím je opticky nebo akusticky signalizováno na určeném místě narušení střeženého objektu nebo prostoru. I&HAS je definován v platné normě **ČSN EN 50131-1 ed. 2**, nabyté účinnosti od roku 2009. Od daného roku uváděn v české odborné literatuře pod zkratkou PZTS. Vedle povinných funkcí je možno I&HAS rozšířit o další volitelné funkce, ale nesmí tak být negativně ovlivněny právě funkce povinné.

Prvky I&HAS jsou vzájemně propojeny přes komunikační rozhraní a případně napojeny na DPPC.

Dle platné normy musí být I&HAS přiřazen danému stupni zabezpečení. Stupeň zabezpečení I&HAS v objektu odpovídá komponentu, který má nejnižší stupeň zabezpečení. Jedno z kritérií je schopnost prvku fungovat v daném prostředí. Norma definuje v rámci systémových požadavků také tzv. třídy prostředí, ve kterých musí být komponenty I&HAS použitelné.

2.1 Třída prostředí 1

V první kategorii se předpokládá s podmínkami uvnitř uzavřených budov a změnám teplot v rozmezí +5 °C až 40 °C. Předpokládá se využití například v obytných nebo obchodních objektech.

2.2 Třída prostředí I

Ve druhé kategorii se předpokládá s vnitřními prostory, kde není stálá teplota nebo vytápění. Zde se předpokládá teplota -10 °C až +40 °C.

2.3 Třída prostředí II

Tato kategorie představuje podmínky v teplotním rozsahu -25 °C až +50 °C ve venkovních prostorech nebo budovách s extrémními podmínkami, kdy ale nedochází k povětrnostním vlivům.

2.4 Třída prostředí IV

Vlivy prostředí, které se vyskytují obvykle vně budov. Předpokládají se teploty -25 °C až +60 °C a povětrnostní vlivy.

Při nasazení I&HAS v podmínkách, pro které není certifikováno, nelze garantovat správnou nebo dlouhodobě spolehlivou funkci při stavu střežení, proto i amatérská instalace zakoupených produktů, které jsou snadno dostupné ke koupi, by měla být pro správnou funkci provedena podle výrobcem přiložených instrukcí.[8]

3 KOMUNIKAČNÍ KANÁLY I&HAS A DPPC

Komunikačními kanály se rozumí přenosová cesta výměny dat mezi prvky. U přenosů signálů a poplachových zpráv mezi I&HAS a DPPC existuje jednosměrná nebo obousměrná komunikace dle využité technologie a technickými parametry komponentů. Každý typ propojení nese své výhody i nevýhody v podobě cenové dostupnosti, spolehlivosti nebo odolnosti vůči sabotáži.

3.1 Přenos kabelem pevné telefonní linky

Technologie přenosu pomocí pevné telefonní linky bývá doporučena z úsporných důvodů u objektů, kde je již zavedena pevná linka a není požadovaná vysoká úroveň zabezpečení. Patří mezi ně například menší kanceláře a obytné domy, kde nemusí být zákazníkem vyžadováno nákladnějšího zabezpečení.

3.2 Přenos pomocí rádiových vln

Nejnákladnější, ale nejspolehlivější varianta komunikace s DPPC je přenos právě přes vyhrazenou rádiovou frekvenci. Bezpečnostními agenturami bývá tato přenosová trasa jednoznačně doporučována jako nejspolehlivější možná varianta zejména u objektů s vyšší potřebou zabezpečení, například banky, sklady zboží a cenných materiálů a různé instituce.

Kromě vysokých pořizovacích nákladů, které jsou spjaty s pořízením vysokofrekvenčního vysílače a instalací, neexistuje více negativ v podobě výdajů v průběhu provozu jako u jiných typů komunikace. Využívaná frekvenční pásma pro rádiový přenos jsou 400 MHz, 160 MHz a 80 MHz. Spolehlivost přenosu spočívá v pravidelném přenosu dat na DPPC v definovaných intervalech a v případě nedoručení dat v této periodě dojde k vyhlášení stavu výpadku na indikačním zařízení. Dosah rádiových připojení je omezený na 20 km.[9]

3.2.1 Jednosměrná rádiová komunikace

Při jednosměrné rádiové komunikaci DPPC pouze přijímá poplachové zprávy a nemá možnost dálkově ovládat ústřednu objektu.

3.2.2 Obousměrná rádiová komunikace

Obousměrná rádiová komunikace je varianta, která vyžaduje i vyšší finanční náklady, ale disponuje možností odesílat z DPPC zprávy na I&HAS v daném střeženém objektu, a tím jej dálkově ovládat a kontrolovat přenosovou trasu.

3.2.3 Decentralizovaná rádiová komunikace

U decentralizovaných rádiových sítí neprobíhá přímá komunikace I&HAS s DPPC, ale využívají se možnosti sběrných stanic. Sběrné stanice mají přidělené zabezpečené objekty, od kterých přijímají zprávy a na DPPC odesílají pouze změnu stavu komunikace. Nevytěžují tolik frekvenční pásma, tudíž díky plošnému nasazení této technologie došlo k menšímu zahlcování rádiové kapacity.

3.2.1 Retranslační stanice

Retranslační stanice slouží k většímu rozsahu pokrytí rádiového signálu. Přenosové zprávy se při průchodu přes retranslační stanice nemění a stanic může být využito více za sebou bez ujmy na kvalitě poplachové zprávy, ale pro funkční retranslaci je nutné zajistit přímou viditelnost mezi anténami koncových bodů spoje. Retranslace se rozděluje na pasivní a aktivní.

Pasivní retranslace je uskutečněna buď odrazem signálu, nebo přesměrováním a neobsahuje žádné prvky pro správu signálu.

Při aktivní retranslaci dojde k přijetí signálu aktivním prvkem, ten zjistí, zda přijatý signál neobsahuje chybu, očistí jej od šumu a posílá dále na další retranslační stanici nebo koncové zařízení. Lze použít jeden nebo dva aktivní prvky. Jeden centrální aktivní prvek zajišťuje menší propustnost než dva aktivní prvky, ale je levnější variantou z hlediska odběru elektrického proudu a má větší rychlost zpracování u velmi malého počtu požadavků.

3.3 Přenos pomocí IP standardu

Využití internetového rozhraní bývá nabízeno velmi často bezpečnostními agenturami z důvodu snadné instalace, relativní spolehlivosti a včasnosti přenosu, nepotřebností telefonního kabelu a nutnosti výdajů poskytovateli telefonních služeb. Využívá se připojení k lokální síti objektu (LAN), připojené do Internetu nebo GPRS připojením

k mobilní síti GSM. Technologie využívá specializované protokoly pro přenos stavových informací z ústředen I&HAS na DPPC.

3.3.1 Protokol IP Contact ID

Jednoduchost a rozšíření protokolu vedlo ke vzniku jeho IP modifikace, která pracuje nad protokolem transportní vrstvy a přenáší formou otevřeného textu sérii číslic, přenášených původním protokolem CID. Úspěšné potvrzení přenosu zprávy na DPPC se provádí odesláním zprávy v původním znění zpět na ústřednu. Protokol neumožňuje žádnou kontrolu přenášených dat ani zajištění důvěrnosti dat.

3.3.2 Protokol SIA IP Events Reporting Protokol

SIA Internet Protocol Events Reporting, často označovaný pouze zkratkou SI, je jednoduchý protokol pro přenos stavových zpráv z ústředen na DPPC Protokol přenáší zprávy třech typů:

- události, informující DPPC o změně stavu zařízení I&HAS,
- kontrolní zprávy, které odesílá zařízení I&HAS a slouží pro kontrolu spojení,
- potvrzení, kterými DPPC potvrzuje přijetí zprávy.

Přenos dat přes protokol SI umožňuje pouze jednosměrnou komunikaci ústředny a DPPC, z toho vyplývá, že DPPC nedokáže dálkově řídit ústřednu.[10]

3.4 Připojení přes GSM

GSM rozhraní má své uplatnění díky snadné dostupnosti a prakticky celkovému pokrytí České republiky sítí mobilních operátorů. Využívá obousměrné komunikace mezi I&HAS a DPPC, díky kterému lze rovněž jako u rádiového využívat dálkového ovládání ze strany dohledového centra. Vzhledem ke snadné instalaci prvků I&HAS s GSM komunikátory a celkového uvedení systému do provozu, jsou takovéto produkty často nabízeny k prodeji i online portály pod záštitou rychlé domácí instalace bez potřeby asistence bezpečnostní agentury. V takovýchto případech, kdy se z různých důvodů napojení na DPPC nevyužije, probíhá přenos poplachových zpráv například na zadaná telefonní čísla uživatelů. Pro úspornější přenos, zpoplatněný mobilními operátory jsou dostupné i SIM karty se speciálním tarifem pro signalizační a zabezpečovací zařízení.

Kontrola spojení u GSM a přenosů se pohybuje v řádech desítek minut až jedna hodina.

3.4.1 Quad-band

Funkce Quad-band představuje možnost přepínání mezi čtyřmi frekvenčními pásmy, které se ve spojení s GSM využívá, patří mezi ně pásma 850, 900, 1800, 1900MHz. Kromě mobilních telefonů tuto funkci obsahují i GSM komunikátory pro minimalizaci rizik spojených s nasazením rušičky, kdy při zarušení jednoho z frekvenčních pásem dojde k automatickému přeladění.[11]

3.4.2 SMS přenos

Přes GSM rozhraní nemusí být využívány pouze hovory, ale i krátké textové zprávy. Komunikace pomocí SMS je obousměrná, tudíž lze dálkově ovládat z dohledového centra. Často používány jsou u zemědělských budov, objektů ve výstavbě a kamenolomů (rypadla, stroje). Dále je formát SMS využíván jako záložní zdroj přenosu poplachové zprávy u I&HAS s funkcí kombinovaných přenosů, který spočívá ve využití náhradní přenosové trasy v případě, že primární komunikace selhala nebo nelze uskutečnit.

3.5 Funkce kombinované komunikace I&HAS a DPPC

Z hlediska vyšší spolehlivosti doručení poplachové zprávy, se využívá právě kombinovaných funkcí přenosu, které jsou na sobě nezávislé. Náhradní komunikace je aktivována v případě selhání primární komunikační trasy. Nastavitelnost kombinovaných přenosů závisí na funkčních dispozicích instalovaného komunikátoru nebo možnostech doplňujících komponentů.

II. PRAKTICKÁ ČÁST

4 POSTUP PŘI ZAPOJENÍ PŘÍJIMAČE DPCC IPR1024 VARIANT PLUS

Pro tuto kapitolu byl použit instalační manuál přijímače IPR1024 firmy Variant plus spol. s r.o. Na základě konzultace, která obsahovala instruktáž o citlivých technických údajích produktu, které nebylo umožněno zveřejnit, bylo zkonstruováno jedinečné osobní povolení využít tento materiál přímo od Variant plus spol. s r.o. Souhlas je součástí přílohy této bakalářské práce.

Přijímač IPR1024 umožňuje hlídání až 1024 objektů s ústřednami Paradox pomocí modulů PCS200, PCS250, IP100 a IP150 schopných přenášet systémové události přes IP sítě. Tyto události jsou pak z přijímače předávány ve formátech Radionics 6500, Sur-Gard MLR2 nebo Ademco 685. Protokol je kryptován formátem AES 256, komunikace je velmi dobře chráněna. Přijímač se vyznačuje nízkou spotřebou energie, snadným programováním a možností záloh na paměťové karty.

Obr. 3 Přijímač IPR1024 Variant plus

4.1 End to end dohled

Celá komunikační linie (kontrolní panel, internetový modul, přijímač a software DPPC) je plně pod dohledem díky patentované šifrované komunikaci Paradox.

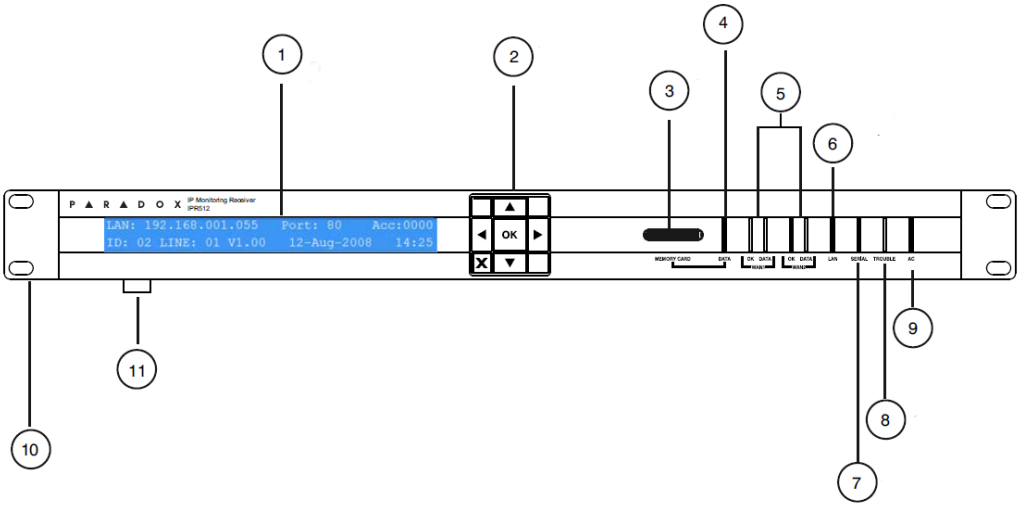
4.2 Software

Monitorovací stanice DPPC podporující datové formáty Radionics 6500, Ademco 685 a Sur-Gard MLR2-DG. Rozhraní v přijímači IPR512 je kompatibilní s těmito DPPC:

- SIS
- SIMS II

- MAXIMUS
- WINSAMM

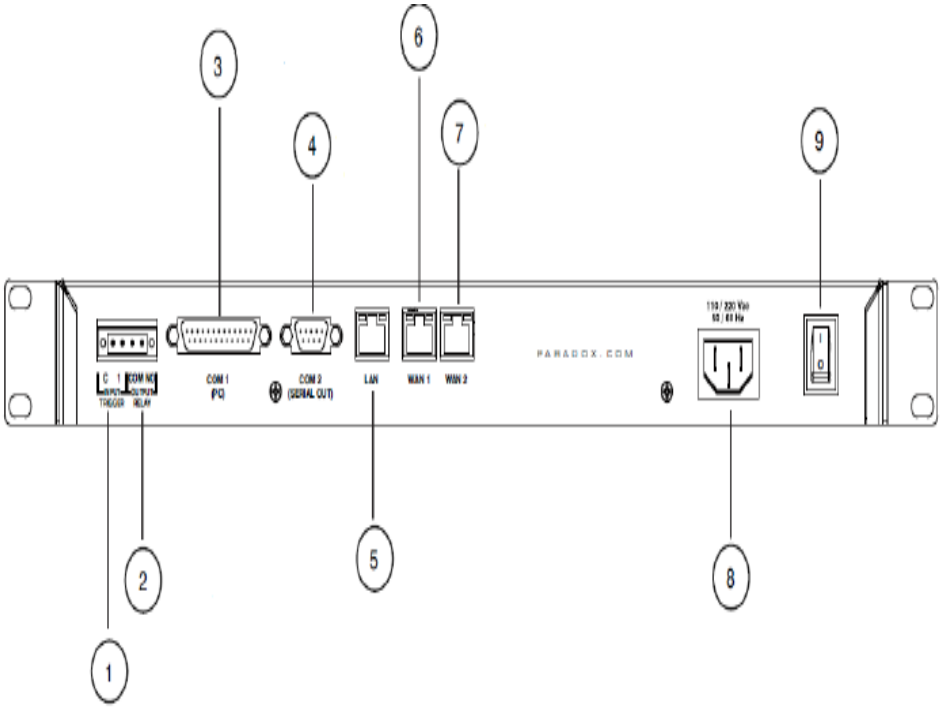
4.3 Ovládací prvky



Obr. 4 Přední strana přijímače IPR1024 Variant plus

1. LCD displej. 2 řádky, 40 znaků. Zobrazuje stav přijímače a umožňuje měnit nastavení systému.
2. Ovládací klávesnice. Slouží k navigaci v menu přijímače.
3. Slot pro paměťové karty. Slouží k připojení karet pro zálohování dat a konfigurace systému.
4. LED dioda. Svítí během přístupu na paměťovou kartu.
5. WAN1 a WAN2 LED dioda. OK LED – svítí, pokud je WAN1 nebo WAN2 rozhraní připojeno k síti. DAT LED svítí při odesílání nebo příjímání dat.
6. LAN LED dioda. Svítí, pokud je LAN rozhraní připojeno k síti.
7. Sériová port LED dioda. Svítí během komunikace přijímače IPR512 se softwarem DPPC.
8. LED dioda. Svit signalizuje problémy.
9. LED dioda. Signalizuje připojení napájecího napětí.

10. Konzole pro montáž do Rack panelů. Volitelný montážní prvek, používá se pro instalaci IPR512 přijímače do standardního rozvaděče.
11. Volitelný montážní prvek. Používá se, pokud se IPR512 přijímač instaluje na stůl.



Obr. 5 Zadní strana přijímače IPR1024 Variant plus

1. Vstupní spoušť. Vstup lze použít pro vygenerování událostí, které mohou být odesílány na software DPPC.
2. Vstupní relé. Aktivuje se při ztrátě komunikace se softwarem DPPC.
3. Port COM1. Sériový port pro připojení k PC s nainstalovaným softwarem pro DPPC.
4. Port COM2. Sériový port určený pro zasílání akcí na tiskárnu nebo k počítači protokolem RS-232.
5. LAN. Port určený pro připojení PC k interní webové stránce pro konfiguraci přijímače.

6. WAN1. Ethernet port určený k příjmu událostí přes internetové připojení.
7. WAN2. Ethernet port určený k příjmu událostí přes internetové připojení.
8. AC vstup. Konektor pro připojení napájecího proudu.
9. Hlavní vypínač přístroje.

4.4 Nastavení systému

Pro přístup k přijímači IPR1024 musí být PC, z kterého se má přijímač konfigurovat, připojeno do stejné sítě. Pro přihlášení do webového rozhraní se řídí těmito kroky:

- spuštění webového prohlížeče,
- zadání LAN IP adresy přijímače IPR1024 do adresného řádku webového prohlížeče. Přístup na přihlašovací stránku přijímače. Domluva se svým správcem sítě ohledně IP adresy a masky podsítě, která umožní přístup k přijímači IPR1024,
- zadání uživatelského jména,
- zadání uživatelského hesla,
- Login.

4.4.1 Registrace přijímače

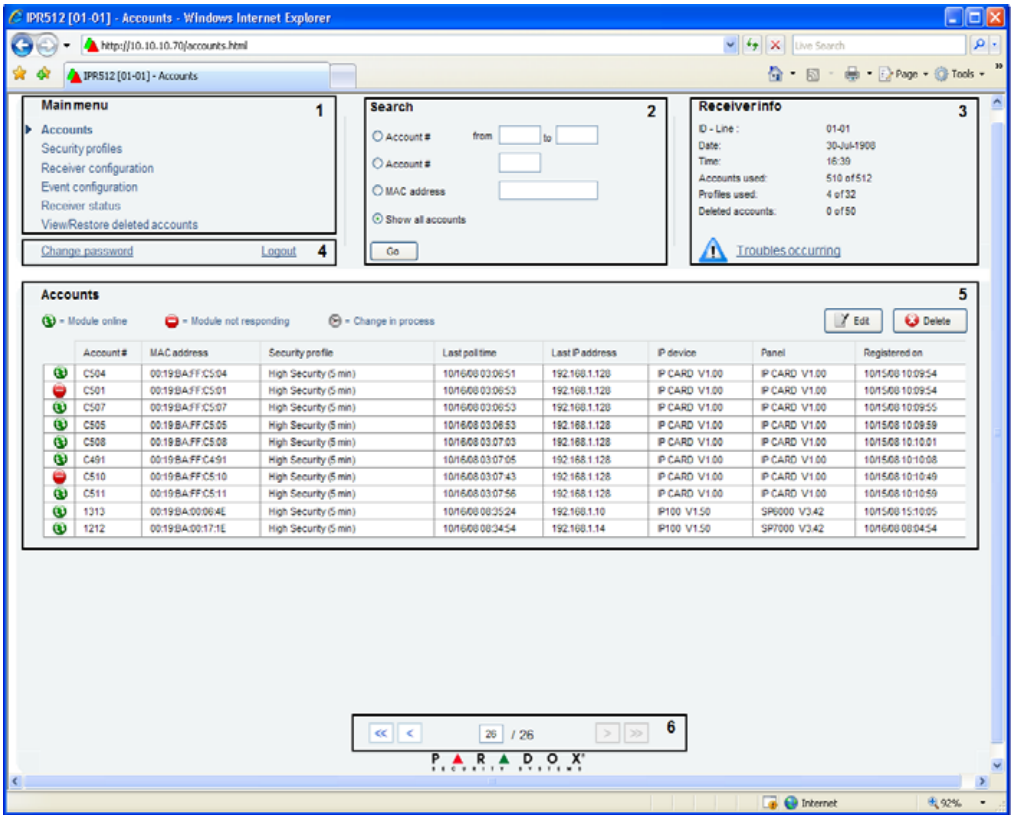
Pro plnou funkci přijímače IPR1024 je po prvním přihlášení na jeho web-rozhraní nutné provést registraci. Přijímač IPR1024 je továrně nastaven do módu, kdy se po deseti přístupech bez zaregistrování stává nedostupným.

4.5 Přístupové web rozhraní

Hlavní okno rozhraní umožňuje nastavit přijímač, upgrade firmware, prohlížet, upravovat a mazat zprávy z registrovaných Paradox ústředen a nastavení bezpečnostních profilů. V horní části se vždy zobrazuje hlavní menu, vyhledávání a informační okno. To umožní snadný přístup k vyhledávání a hlavnímu menu.

4.5.1 Hlavní obrazovka

Hlavní obrazovka, na které probíhá správa připojených zabezpečovacích zařízení, představuje přehledné uživatelské rozhraní.

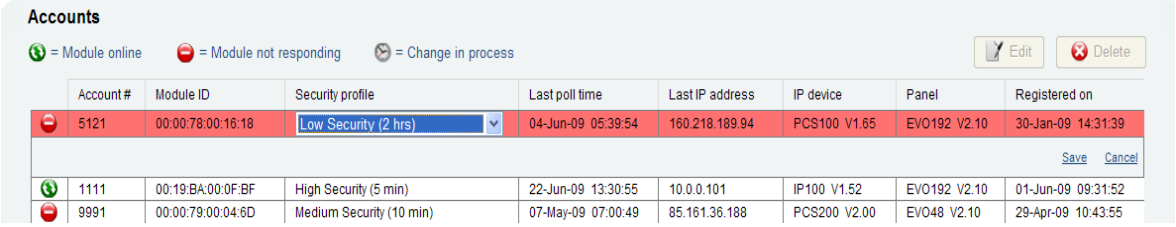


Obr. 6 Hlavní obrazovka

- Main menu. Obsahuje přístupy k účtům, nastavení bezpečnostních profilů, nastavení přijímače, zobrazování stavů a obnov smazaných účtů.
- Search. Umožňuje vyhledávání nebo filtrování účtů prostřednictvím čísla účtu, rozsahu čísel účtů nebo MAC adresy.
- Reciever Info. Zobrazuje ID-Line, datum a čas, počet účtů a profilů v systému a počet smazaných účtů.
- Accounts. Zobrazuje stav účtů a umožňuje přiřadit profil nebo účet vymazat.
- Page browser. Zobrazuje číslo stránky a umožňuje listování. Na jedné straně se zobrazuje maximálně dvacet účtů.

4.5.2 Připojené účty

Záložka Accounts obsahuje seznam připojených účtů, indikaci stavu a adresy, jak je patrno z následujícího obrázku.



Obr. 7 Účty napojených objektů

Následující tabulka podává přehled zobrazovacích funkcí a zapsaných údajů o připojené ústředně.

Ikony stavu	Zobrazuje aktuální stav účtu připojeno odpojeno Probíhají změny
Account#	Zobrazuje číslo přidělené aktuálnímu účtu
MAC adress	Zobrazuje MAC adresu nebo jedinečné ID přihlášeného modulu Paradox
Security profile	Zobrazuje nastavený bezpečnostní profil
Last poll time	Zobrazuje datum a čas posledního hlášení přítomnosti modulu
Last IP adress	Zobrazuje IP adresu, ze které přišlo poslední hlášení modulu
IP device	Zobrazuje internetový modul na straně ústředny
Panel	Zobrazuje typ ústředny
Registered on	Datum registrace

Tab.1 Zobrazovací funkce

Číslo objektu se při registraci pevně sváže s MAC adresou komunikačního modulu PARADOX. Pokud dojde k výměně tohoto modulu, je nutné smazat v přijímači IPR1024 stávající objekt (a to i z koše) a potom provést novou registraci.

4.5.3 Bezpečnostní profily

V menu bezpečnostní profily lze nadefinovat až 32 profilů pro dohled nad moduly. Profily určují intervaly pro sledování ústředen. Pokud se v nastavené době přijímač nepřihlásí, přijímač vyhlásí jeho ztrátu. V následující tabulce jsou čtyři výchozí bezpečnostní profily.

ID	Název	Interval dohledu	Čas prodlevy
00	Bez dohledu	24h	Ne
01	Vysoká bezpečnost	2m	5m
02	Střední	10m	30m
03	Nízká	20m	1h

Tab. 2 Bezpečnostní profily

4.5.4 Log soubor

Přístupové web-rozhraní vytváří systémový log soubor, který sleduje systémové události a potíže, které se vyskytli v systému. Jedná se o XML dokument, kde je uloženo posledních 150 událostí.

4.5.5 Zálohování systému

Na paměťové kartě v přijímači IPR1024 může být uloženo až 10 záloh. Záloha se provádí automaticky vždy deset minut po jakékoliv změně v databázi, nebo ručně pomocí menu na displeji. Uložené data obsahují nastavení systému a všechny informace o účtech. Toto umožňuje při výpadku přijímače rychlý a snadný přenos dat do jiného přijímače.

5 ZABEZPEČENÍ PŘENOSU POPLACHOVÝCH ZPRÁV MEZI I&HAS A DPPC

Kapitola pojednává o zabezpečení komunikace a o možnostech znemožnit komunikaci mezi DPPC a prvky I&HAS v zastřežené budově a předává informace o zavedených bezpečnostních standardech z hlediska zabezpečení přenosu poplachových zpráv.

5.1 Obecné faktory

Reálná hrozba pro zabezpečený objekt v zastřeženém stavu nastává v těchto případech i za předpokladu správné funkčnosti instalovaného systému:

- průběh sabotáže nezpůsobí okamžité vyvolání poplachu na DPPC,
- zastřežený objekt nestihne odeslat poplachovou zprávu na DPPC ještě před cíleným přerušením komunikace pachatelem,
- absence sekundárních přenosových cest v případě selhání primárního přenosu,
- pravidelný interval kontroly spojení mezi ústřednou a DPPC je natolik dlouhý, že poskytne pachateli po úspěšné sabotáži dostatek času páchat trestnou činnost a opustit objekt než DPPC klasifikuje situaci jako poplach.

Faktory, které ovlivňují pravděpodobnost úspěšnosti sabotáže:

- zabezpečení poplachové zprávy proti přečtení a změně dat,
- délka intervalu pravidelné kontroly spojení,
- rozmístění I&HAS komponentů a kabelů z hlediska dostupnosti pro pachatele,
- zařízení pro detekci sabotáže komponentů a ústředen (tamper, antimasking),
- alternativní- záložní přenosové cesty.

Většinu zmíněných faktorů upravuje platná norma **ČSN EN 50131-1 ed. 2**, která obsahuje i kategorizaci odolnosti zabezpečení právě proti sabotážím, záměně zprávy a detektorům pokusů o manipulaci s ústřednou a rozvodovými skříněmi. Obecné zásady umisťování komponent I&HAS a vedených kabelů se uvádí v odborné literatuře.

5.2 Maximální přípustný interval od přijetí posledního signálu

Norma udává maximální přípustný interval od přijetí poslední zprávy I&HAS. Po uplynutí doby musí být vygenerována zpráva sabotáže nebo poruchy zařízení nebo jednoho z komponentů.

	Stupeň1	Stupeň 2	Stupeň 3	Stupeň 4
Maximální přípustný interval od přijetí posledního signálu nebo zprávy	60 min	20 min	60 s	10 s

Tab. 3 Maximální interval od přijetí signálu nebo zprávy

5.3 Zabezpečení proti záměně zprávy

Opatření proti neoprávněné záměně komunikátoru obdobným zařízením zmiňovaná norma rozlišuje na základě parametrů dle následující tabulky:

S0	Žádné zabezpečení
S1	Prostředky pro detekci záměny přidáním identifikátoru nebo adresy ke všem poplachovým zprávám
S2	Využití šifrování identifikátoru nebo adresy, přidání neopakovatelného kódu pro každý komunikátor

Tab. 4 Zabezpečení proti záměně zprávy

Identifikace vždy vyžaduje dostatečný počet kódů tak, aby každý komunikátor měl jedinečný kód. Minimální rozsah jedinečných adres parametru S2 je 250.

5.4 Zabezpečení informace

Zabezpečení informace kategorizuje platná norma **ČSN EN 50131-1 ed. 2.** dle následující tabulky:

I0	Žádné opatření
I1	Opatření zamezující neoprávněnému přečtení informace
I2	Opatření zamezující neoprávněné modifikaci přenášené informace
I3	Opatření zamezující neoprávněnému přečtení a modifikaci informace

Tab. 5 Zabezpečení informace

Výše uvedené opatření se využívá šifrování a metody kryptografické autentizace. U šifrování synchronních poplachových přenosových systémů musí být dodrženo pravidlo algoritmu, že v datové posloupnosti se po sobě následujících 100 bitů nebude opakovat v 10 000 000 po sobě následujících bitech. U asynchronních poplachových přenosových systémů se nesmí po sobě následujících 100 bajtů opakovat v 1 000 000 po sobě následujících bajtech.[8]

6 MOŽNOSTI SABOTÁŽÍ PŘENOSU POPLACHOVÉ ZPRÁVY Z I&HAS NA DPPC

Následující kapitoly pojednávají o možnostech sabotáží v takovém smyslu, kdy si pachatel zprostředkuje možnost nedetekovatelně vstoupit do zabezpečeného objektu nebo zóny. Důležité aspekty v definovaném smyslu jsou četnost kontrol spojení ústředen s DPPC a vyhodnocení dispečera změny stavu. Situace, kdy je i úspěšná sabotáž přenosu detekovatelná na straně DPPC, nemá pro potencionálního pachatele smysl a nedává mu ani dostatečný čas páchat v objektu trestnou činnost. Primární měřítko je stupeň zabezpečení dle platné normy, do kterého daný zabezpečovací systém spadá.

6.1 Telefonní linka

Přenos pomocí telefonní linky je v České republice hojně zastoupen i přes svá rizika související s pokusy o napadení nebo přerušení přenosové trasy a nedostatkům, které spočívají v těchto faktorech:

- v případě snadné dostupnosti je pachateli umožněna manipulace s rozvodovou skříní nebo přerušení kabelu,
- pomalému přenosu zprávy na DPPC,
- kontrola spojení pouze jednou za 24 hodin,
- nízká spolehlivost přenosové trasy oproti ostatním typům připojení z hlediska poruch na telefonní lince.

6.2 Radiové připojení

Radiové připojení je udáváno jako nejbezpečnější a nejspolehlivější varianta připojení. Mezi výhody rádiového připojení patří:

- kontrola spojení s DPPC opakující se v řádech desítek vteřin,
- přenos zpráv mezi DPPC a I&HAS v reálném čase bez zpoždění,
- minimální riziko možného sabotování radiového přenosu.

Z toho vyplývá, že jakákoli i úspěšná manipulace pachatele s přenosovým zařízením nebo pokusem zarušit přenos poplachového signálu, bude v řádech desítek vteřin zaznamenána dispečerem DPPC.

6.3 Přenos pomocí IP standardu

Následující tvrzení plyne z rozhovoru s jednatelem bezpečnostní agentury SG'3 s.r.o. panem Michalem Cíchou. Přenos pomocí IP standardu využívá vlastní IP adresy, která je odlišná od adresy sítě objektu. Jakékoli pokusy hackingu prováděné na adresu sítě neovlivní komunikaci ústředny s DPPC. Spolehlivost zabezpečení garantuje četnost kontroly spojení, která je v natolik krátkých intervalech, že potencionálnímu pachateli neposkytuje dostatek času v objektu pro loupež a páchání trestné činnosti.

Pokud se nejedná o GPRS, které poskytuje telefonní operátor, je toto propojení spolehlivé. Kategorie GPRS v této práci bude dále klasifikována spolu s GSM připojením, jelikož je také poskytována mobilním operátorem.

6.4 GSM ústředny

Jak již bylo zmíněno, GSM ústředny využívají pro přenos na DPPC mobilní operátory. V České republice mají mobilní operátoři přidělena tato frekvenční pásma:

- E-GSM (975-1023 MHz)
- P-GSM (GSM 900)
- DCS (GSM 1800) včetně nově přidělených pásem v prosinci 2013[12]

Zabezpečení GSM je uskutečněno pomocí A5 šifrovacího algoritmu. Verzí A5 bylo od roku 1987 vyrobeno několik, ale většina z nich byla prolomena. S dostupnou technikou již byla provedena veřejná demonstrace odposlechu hovoru v reálném čase a byly zaznamenány po celém světě další případy odposlechů mobilních telefonů. Odposlech mobilních telefonů je dnes každodenní policejní praktika i v České republice.[13]

Z toho vyplývá, že samotný GSM systém vzhledem k jeho aktuální úrovni zabezpečení nemusí být bez dalších úprav v blízké budoucnosti dostačující jak pro běžné hovory, tak pro přenos poplachových zpráv.

Mezi další nebezpečí pro GSM přenos představuje využití rušení signálu pomocí rušičky.

6.4.1 Rušička GSM signálu

Princip rušičky GSM signálu je zahlcení celého frekvenčního pásma rušivým signálem. Zařízení v dosahu rušičky ztratí signál s mobilním operátorem, a tím je znemožněna veškerá komunikace. Použití zařízení pro rušení signálu sítí mobilních operátorů je

v České republice protizákonné. Výjimku mohou od Českého telekomunikačního úřadu dostat pouze některé státní orgány a instituce, například Ministerstvo obrany nebo Ministerstvo vnitra.[14]

V dnešní době je rušička snadno dostupná ke koupi. Česká obchodní inspekce (ČOI) upozorňuje prodejce, spotřebitele a případné majitele, že již samotný prodej, výroba nebo dovoz těchto zařízení je nelegální, a to v rámci celé Evropské unie. Žádná rušička nesplňuje ani nemůže splnit požadavky příslušných právních předpisů, proto tyto výrobky nelze vůbec uvádět na trh, a tudíž ani nabízet a prodávat. V případě rušiček se řada prodejců mylně domnívá, že zákonem stanovené povinnosti splní, když zákazníka upozorní na zákaz použití daného výrobku v ČR.

Reálné využití rušičky pro narušení přenosu poplachových zpráv představují rušičky od 10 000 Kč, které mají dosah v okruhu větším než deset metrů. Zahltí celé GSM pásmo a UMTS ,a tak znemožní hovorový přenos i přenos SMS zpráv na DPPC.

6.4.2 Reakce DPPC při zarušení GSM komunikátoru rušičkou

Dle normy **ČSN EN 50131-1 ed. 2.** je sice definována tabulka, podle které může zařízení spadat do stupně zabezpečení dle testů prostředků pro detekci, zpoždění, modifikaci a ztrátě signálu, ale u GSM komunikátorů, které využívají mobilní síť operátorů pro přenos poplachové zprávy na DPPC, je neřešitelný problém nedostupnost operátora. Občasné vypadnutí signálu ústředny totiž dispečink klasifikuje pouze jako dočasný výpadek signálu mobilního operátora a nereaguje na něj jako na poplach. DPPC si sice samo hlídá frekvenci spojení, ale ta je mnohem delší než například u rádiového spojení, takže pokud se GSM ústředna sama neozve, DPPC oznámí, že je problém se spojením, ale to může nastat po deseti minutách, po hodinovém intervalu, v horším případě po daleko delší době.

Z toho vyplývá, že dispečer DPPC nedokáže okamžitě rozpoznat, zda pouze vypadl signál operátora nebo je zastřežený objekt pod útokem. Další negativní faktor pro tuto skutečnost, který přidává potencionálnímu pachateli minuty navíc, je povinná reakce dispečera, po kterém je v případě nedostupnosti signálu vyžadováno pouze informování provozovatele systému o vypadnutí signálu nebo poruše a čekání na jeho další pokyny.[15]

6.4.3 Ohrožená skupina vlastníků GSM komunikátoru

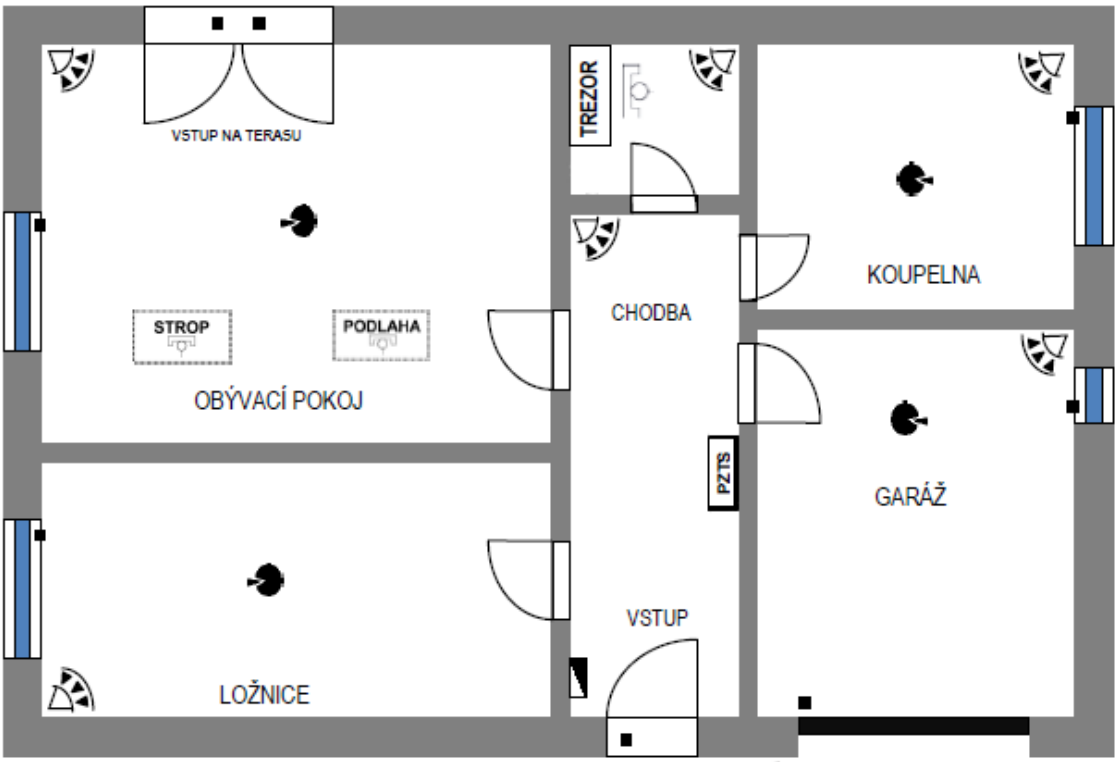
Cílová skupina, které hrozí nejvyšší riziko napadení rušičkou, je sféra malých podniků, kanceláří a bytů, které se spoléhají z různých důvodů na cenově dostupné jedno-komunikační GSM alarmy. Na základě získání důležitých informací o takto zabezpečeném objektu například osobní návštěvou nebo spoluprácí s některým ze zaměstnanců, se pachateli otevírá cesta vloupat se s vysokou pravděpodobností úspěchu do objektu a to nezaznamenatelně.

K tomuto tématu přispěl i Vladimír Vrba, bývalý vedoucí oddělení technické ochrany na Policii ČR v Ústí nad Labem., nyní působící v oblasti poskytování bezpečnostních služeb. Pro Černou kroniku 15. května 2013 k tématu rušiček uvedl, že největší hrozbou jsou nekvalitní levné dostupné GSM alarmy z Číny, a proto pro pachatele je zakoupení dražší rušičky v řádech deseti tisíc pouhá investice do budoucna.

Příkladným scénářem byla situace s bezdrátovým Evolveo Sonix GSM alarmem napojeným na DPPC, kdy se pachatel v červnu roku 2011 přes tento zabezpečovací systém vloupal naprosto nezaznamenán v zastřeženém stavu do firemní kanceláře, vykradl ji a samotný Evolveo Sonix s příslušnými komponenty odcizil. Na základě této kauzy a dalších technických problémů byl produkt stažen z prodeje.[16]

6.4.4 Předpokládaný postup pachatele s rušičkou signálu při pokusu o vloupání do střeženého objektu GSM ústřednou

Prvním krokem při postupu pachatele s patřičným vybavením je zapnutí rušivého signálu již před vstupem do střeženého objektu. S pravděpodobným předpokladem předešlého zkoumání objektu pachatel zná rozmístění detektorů, ale hlavně ústředny, na kterou jsou veškeré prvky napojeny. V tomto případě je pro pachatele prolomitelné zabezpečení jakéhokoli objektu, který má ústřednu v takovém okruhu dosahu vstupních dveří popřípadě oken v přízemních patrech, že ji zasáhne rušivý signál ještě před samotným zahajujícím pokusem o překonání mechanických zábranných prvků. V momentě zarušení komunikace ústředny s DPPC se pachateli otevírá cesta nezaznamenatelně se pohybovat ve střeženém prostoru a páchat trestnou činnost. Reakce dohledového centra na takto vzniklou situaci byla popsána v předchozích částech praktické části bakalářské práce. Příkladnou situaci nevhodného umístění ústředny v blízkosti vstupních dveří vykresluje následující obrázek.



Obr. 8 Nevhodné umístění ústředny PZTS[8]

6.4.5 Zařízení pro detekci rušení signálu

Pro detekci rušivého signálu existuje výrobek od výrobce Manufacturer. Lze připojit k ústředně I&HAS a při detekci rušivého signálu stihne odeslat varovnou SMS zprávu na DPPC popřípadě mobilní telefon ještě před tím, než dojde k výpadku signálu. Produkt byl primárně vyroben pro policejní a bezpečnostní složky pro minimalizaci rizik spojených s pokusy o napadení vozidel přepravujících finanční hotovost. Cena produktu se udává od 24 000 Kč. Produkt není dlouho na trhu, proto lze očekávat do budoucna snížení jeho pořizovací ceny na uživatelsky dostupnou hodnotu.[17]

Obr. 9 Detektor rušení signálu[17]

6.4.6 Pokyny pro minimalizaci rizik spojených s pokusy nasazení rušičky GSM signálu ve střeženém prostoru

Jak již bylo uvedeno, nedetekovatelné zarušení GSM ústředny lze zařadit mezi rizikový faktor. Kromě obecných zásad umisťování komponentů I&HAS a ústředen, které jsou dostupné v odborné literatuře, doporučuji dbát následujících pokynů, které obsahují doporučení a zásady, jak minimalizovat pravděpodobnost úspěšně nedetekovaného zarušení komunikace GSM ústředny s DPPC pomocí rušičky GSM signálu:

- vzhledem k omezenému dosahu rušičky na desítky metrů, ale schopností rušivého signálu proniknout přes průměrně tlustou zeď, sklo a jiný materiál, umístit GSM ústřednu co nejdále od vchodových dveří, prostorů a výplní, kde mohou hrozit pokusy o nasazení rušičky a brát v potaz koordinaci více pachatelů (zapnutí rušivého signálu v blízkosti oken v nižších patrech, balkónů, vstupů na terasu, apod.),
- dovybavení ústředny GSM o detektor rušivého signálu,
- zkrácení obvyklého intervalu kontroly spojení s DPPC vzhledem k průlomové odolnosti instalovaných mechanických zábranných systémů,
- omezení detailů ohledně instalovaného zabezpečení zaměstnancům v daném objektu, zejména interval kontroly spojení, vlastnosti ústředny.

ZÁVĚR

Bakalářské práce přibližuje čtenáři problematiku zabezpečení komunikačních kanálů mezi dozorovým a poplachovým přijímacím centrem DPPC a zabezpečovacím systémem I&HAS. Na základě osobních pohovorů, dostupné literatury a platných norem jsem pojednal o zabezpečení a bezpečnostních nedostatcích u konkrétních rozhraní.

V teoretické části jsem se zaměřil na historii, vývoj a legislativu dozorového a poplachového přijímacího centra. Pojednal jsem o problematice požadavků a pokynů dispečera a uvedl výhody napojení objektů na dohledové centrum. Dále byl připomenut odborné veřejnosti pojem I&HAS a v návaznosti na oba produkty jsem uvedl způsoby propojení DPPC a I&HAS.

V praktické části jsem vypracoval postup při připojení na dohledové centrum s přijímačem IPR1024 Variant plus na základě poskytnutého manuálu výrobcem. Pojednal jsem o zabezpečení komunikace mezi dohledovým centrem a I&HAS prvky a možnostech sabotáže. Uvedl jsem jednak některé způsoby zabezpečení, které jsou dány platnou normou, a způsoby zabezpečení, kterými disponuje samotný signál přenosu v podobě pravidel šifrování. Neméně důležitá část praktické části se zabývá zabezpečením GSM komunikátoru a jeho nedostatky v bezpečnosti, následným názorným imaginárním postupem při pokusu provést vloupání s patřičným vybavením za účelem nezaznamenatelně proniknout do zastřežené zóny.

Hlavním přínosem bakalářské práce je shledání GSM ústředen jako velmi rizikové řešení zabezpečení objektu. Za uvedených podmínek lze zařízení úspěšně a hlavně nedetekovatelně odříznout od komunikace s DPPC pomocí rušičky. Takto vzniklá situace není jednoznačně a okamžitě klasifikována dohledovým centrem jako poplach a vzniká tak prostor pro potencionálního pachatele realizovat v zabezpečeném objektu trestnou činnost. Dílčím produktem mé práce je vypracovaný seznam pokynů a pravidel pro umístění GSM ústředny vzhledem k možným hrozbám plynoucím právě z pokusů o sabotáž komunikace s DPPC.

ZÁVĚR V ANGLIČTINĚ

The bachelor thesis brings the reader issues of a security communication channel between supervisory and Monitoring and alarm receiving centre MARC and security system I& HAS. Based on personal interviews, literature and applicable standards, I discussed the security and security insufficiencies of the specific interfaces.

In the theoretical part I focused on the history, development and legislation of Monitoring and alarm receiving centre. I described the problematic of the requirements and instructions of a dispatcher and I stated the benefits of connected objects to Monitoring and alarm receiving centre. Then for professional public it was also reminded I&HAS and in relation to both products I mentioned the ways of linking MARC and I & HAS.

In the practical part I have developed a procedure of connection MARC with receiver IPR1024 Variant plus based on the manual provided by the manufacturer and possibility of sabotage. I mentioned firstly some security methods, which are given by the applicable standards and secondly security methods, which has a transmission signal itself in the form of encryption rules. Equally important part of the practical part deals with the security of GSM communicator and its safety deficiencies, followed by the vivid imaginary procedure when attempting to burglary with proper equipment in the order to penetrate unnoticeably to the armed zone.

The sectional product of this bachelor thesis is the reunion of GSM panels as high-risk solution of objects securing. Under these conditions, the device can be successfully and mostly undetectable cut off from the communication with the MARC with using jammers. The resulting situation is not clearly and immediately classified as in the MARC and it is creating a space for a potential perpetrator to realize a crime in a secure object. The important product of my work is the elaborated list of guidelines and rules for GSM panels which are regarded to possible threats, ensued from the attempts to sabotage communication with MARC.

SEZNAM POUŽITÉ LITERATURY

[1] ČERVÍČEK, Martin. Interview. In: *Otázky Václava Moravce*. TV, ČT 1. 15. prosince 2013. 12:00

[2] POPARDOWSKI, Ivo. *Bezpečnostní zpravodaj*. [online]. [cit. 2014-04-25]. Dostupné z: http://www.bezpecnostni-zpravodaj.cz/poplachove zabezpecovaci-a-tisnove-systemy-pco-dppc-pts-pzts-historie-legislativa-normativni-zasady-provozu/

[3] DRGA, Rudolf a Vladimír LAUCKÝ. *Speciální technologie komerční bezpečnosti*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012, 224 s. ISBN 978-80-7454-146-9.

[4] VLÁDA ČESKÉ REPUBLIKY: *Návrh zákona o soukromé bezpečnostní činnosti a soukromé bezpečnostní službě a o změně souvisejících zákonů*. [online]. [cit. 2013-12-12]. Dostupné z:: http://www.vlada.cz/cz/ppov/lrv/ria/databaze/mv-navrh-zakona-o-soukrome-bezpecnostni-cinnosti-a-soukrome-bezpecnostni-sluzbe-a-o-zmene-souvisejicich-zakonu-109036/.

[5] KAMENÍK, Jiří a František BRABEC. *Komerční bezpečnost: Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*. Vyd. 1. Praha: ASPI, 2007, s. 78-79. ISBN 9788073573096.

[6] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I*. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. ISBN 978-80-7318-889-4.

[7] Pojištění domácnosti. *ČSOB pojišťovna* [online]. s. 20 [cit. 2014-02-10]. Dostupné z: http://www.csobpoj.cz/cs/produkty/pojisteni-majetku-a-odpovednosti/Documents/VPP_PMO.pdf

[8] VALOUCH, Jan. *Projektování bezpečnostních systémů*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2011. ISBN 978-80-7454-230-5

[9] Dálková ostraha pultem centralizované ochrany, PCO. *H1 security services* [online]. [cit. 2014-02-14]. Dostupné z: http://www.pcosecurityh1.cz/pult_centralizovane_ochrany_pco.html

[10] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Vyd. 2. S.I.: Cricetus, 2003, 351 s. ISBN 80-902-9382-4

[11] Quad-Band. *Phonescoop.com* [online]. [cit. 2014-02-15]. Dostupné z: http://www.phonescoop.com/glossary/term.php?gid=139

[12] Frekvenční příděl na pásmech GSM, DCS, UMTS a LTE v České republice. *Gsmweb.cz* [online]. [cit. 2014-05-25]. Dostupné z: http://www.gsmweb.cz/clanky/freq2.htm

[13] Využití proudových šifer v současnosti. *Access server* [online]. [cit. 2014-05-25]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2009080001

[14] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management III*. 1.vyd. Zlín: VeRBuM, 2013, 456 s. ISBN 978-80-87500-35-4

[15] Pravidla provozování PCO u HZS Karlovarského kraje. In: *Sbírka interních aktů řízení ředitele HZS Karlovarského kraje* [online]. 2010 [cit. 2014-04-27]. Dostupné z: www.hzscr.cz/soubor/pco-doc.aspx

[16] Evolveo Sonix bezdrátový GSM alarm. *Czc.cz* [online]. [cit. 2014-04-25]. Dostupné z: http://www.czc.cz/evolveo-sonix-bezdratovy-gsm-alarm_2/79781/produkt

[17] Detektor GSM Rušenia. *Market SK: Centrum elektronickeho obchodovania na Slovensku* [online]. [cit. 2014-05-28]. Dostupné z: http://www.market.sk/obchod/detektory-vf-plostic/455/detektor-gsm-rusenia-detail.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

DPCC Dozorová a poplachová přijímací centra

MARC Monitoring and Alarm Recieving Centre

ARC Alarm Recieving Centre

PCO Pult centrální ochrany

RVHP Rada vzájemné hospodářské pomoci

ČSSR Československá socialistická republika

ČR Česká republika

NBÚ Národní bezpečnostní úřad

ID Schopnostní stupeň invalidního důchodu

SBS Soukromé bezpečnostní služby

PC Osobní počítač

CCTV Uzavřený televizní okruh

I&HAS Intrusion and Hold-up Alarm System

PZTS Poplachové zabezpečovací a tísňové systémy

GSM Globální Systém pro Mobilní komunikaci

GPS Globální polohovací systém

UPS Nepřerušitelný zdroj energie

SELV Bezpečné malé napětí

ELV Velmi nízké napětí

VPS Virtuální privátní síť

LAN Lokální počítačová síť

WAN Rozlehlá počítačová síť

IP Internetový protokol

SIM Účastnická identifikační karta

SMS Krátká textová zpráva

AES	Standard pokročilého šifrování
MLR	Typ binárního formátu
LCD	Displej z tekutých krystalů
LED	Dioda emitující světlo
COM	Rozhraní sériového portu
AC	Napájecí vstup elektrického proudu
MAC	Identifikátor síťového zařízení. Fyzická adresa
GPRS	General Packet Radio Service
ČOI	Česká obchodní inspekce
XML	Standardní formát pro výměnu informací
UTMS	Standard třetí generace mobilních sítí
ČSOB	Československá obchodní banka, a. s.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: VÝTAH ZE ZÁVĚREČNÉ ZPRÁVY Z HODNOCENÍ DOPADŮ REGULACE

Důvodová zpráva

Obecná část

A/ Závěrečná zpráva z hodnocení dopadů regulace

Současná právní úprava, ale i faktická situace na trhu soukromých bezpečnostních služeb neřeší a ani není schopna vyřešit základní bezpečnostní rizika spojená s poskytováním soukromé bezpečnostní služby. Zde se má na mysli situace, kdy provozovatel soukromé bezpečnostní služby poskytuje tuto zároveň ve prospěch objednatele a zároveň i v jeho neprospěch, na základě objednávky jiné osoby.

Nezřídka se rovněž stává, že soukromá bezpečnostní služba poskytuje objednateli nějakou dobu např. ostrahu majetku. Bezprostředně po ukončení předchozí objednávky se na tuto soukromou bezpečnostní službu obrátí např. konkurenční firma se žádostí o výkon jiné bezpečnostní činnosti v neprospěch původního objednatele. Vzhledem k tomu, že oslovená soukromá bezpečnostní služba je dobře obeznámena s prostředím původního objednatele (znalost jeho silných i slabých stránek), je realizace nové zakázky víceméně bezproblémová z pohledu soukromé bezpečnostní služby, nicméně z pohledu objektu zájmu soukromé bezpečnostní služby může způsobit původnímu objednateli nedozírné škody různého charakteru. Tím vzniká zcela nepřehledné podnikatelské prostředí, které oprávněně vyvolává nedůvěru veřejnosti v objektivitu poskytovaných služeb, vnáší řevnivost mezi samotné poskytovatele soukromých bezpečnostních služeb a celkově výrazně negativně ovlivňuje celkové klima v této oblasti.

Stávající právní úprava neumožňuje vyloučení střetu zájmů po skončení smluvního stavu nebo v jeho průběhu a smluvní regulace je velmi problematická, neboť neexistuje žádný kontrolní mechanismus, který by tento aspekt mohl kontrolovat a při zjištění pochybení z této skutečnosti vyvodit patřičné závěry. Nová právní úprava při takovém pochybení zakládá i možnost ztráty licence.

Dále je nutno uvést, že soukromé bezpečnostní služby mohou představovat, díky svému personálnímu a materiálně technickému vybavení výrazné bezpečnostní riziko. I když profesionální přístup a etické zásady řady provozovatelů takové selhání snižuje, soukromé bezpečnostní služby se mohou stát a stávají se nástrojem nekalého konkurenčního boje podnikatelských, politických a dalších subjektů.

PŘÍLOHA P2: VÝTAH ZE STANOVISKA KOMISE PRO HODNOCENÍ DOPADU REGULACE

Komise pro hodnocení dopadů regulace
Legislativní rada vlády České republiky

V Praze dne 4. února 2013
Č.j.: 36/13

Stanovisko
komise pro hodnocení dopadů regulace

k návrhu
zákona o soukromé bezpečnostní činnosti a soukromé bezpečnostní službě a o změně souvisejících zákonů

Návrh zákona doprovází "závěrečná zpráva z hodnocení dopadů regulace" (dále jen "**Zpráva RIA**"), která by měla vysvětlovat důvody vedoucí k zavedení této nové regulace, resp., k razantnímu zpřísnění stávající regulace. Na tyto požadavky ovšem Zpráva RIA zcela rezignuje, přičemž níže jsou uvedeny zásadní výhrady ke Zprávě RIA.

Chybí identifikace problému a vysvětlení, z čeho "*jednoznačně vyplývá nedostatečnost [] právní úpravy*" (str. 51 návrhu). Zpráva RIA by měla obsahovat popis jednotlivých konkrétních problematických oblastí (např. kriminálních činností, který se účastní podniky provozující SBS, nedostatků pozorovaných v činnostech SBS, odkaz na mediální kauzy, zjištění policie ČR, závěry konzultací, atd.) a až na tomto základě hodnotit dostatečnost stávající regulace. Zpráva RIA odkazuje na právní úpravu v zahraničí, avšak právě z jediné zmínky o faktické situaci (str. 87, odkaz na Velkou Británii) vyplývá, že regulace SBS se přijímá v reakci na konkrétní problém (např. jejich zneužívání k výběru "výpalného" na Slovensku).

Popis provedených konzultací je zcela nedostatečný, neobsahuje žádné konkrétní detaily, odkazy na výstupy jednotlivých setkání, identifikaci zúčastněných profesních sdružení. Spolu s četnými odkazy na zdůvodnění jednotlivých opatření odkazem na konzultace s profesními sdruženími (bez dalších důvodů) však návrh vyvolává otázku, zda nemůže jeho nezamýšleným, či dokonce zamýšleným, účinkem být omezení konkurence na trhu SBS. Takovou pochybnost musí Zpráva RIA rozptýlit nade vše.

Předložená zpráva RIA zcela nevyhovuje požadavkům na tvorbu legislativy na základě hodnocení jejích očekávaných dopadů. Doporučujeme její přepracování v souladu s obecnými zásadami pro hodnocení dopadů regulace schválených Vládou ČR a doprovodnými metodikami procesu RIA zveřejněnými na webu pracovní komise RIA (http://ria.vlada.cz). Výše uvedené výtky představují pouze implementaci zmíněných materiálu na předložený materiál.

Vypracoval: **Mgr. Juraj Alexander, LL.M.**

Prof. Ing. Michal Mejstřík, CSc.
předseda komise

Příloha P3: SOUHLAS S POUŽITÍM MATERIÁLU FIRMY VARIANT SPOL. S R.O.

Souhlas s použitím firemního materiálu

Společnost Variant plus spol. s r.o. uděluje souhlas s použitím firemního materiálu :

Instalační manuál IPR1024 FW verze 2.21 a vyšší

studentu Univerzity Tomáše Bati ve Zlíně Michalu Přikrylovi, nar. 27. 12.1988. Materiál je povolen ke zpracování v domluveném rozsahu pro účely Bakalářské práce.

Datum 28. 2. 2014

Razítko: VARIANT plus, spol. s r.o. U Obůrky 5, 674 01 TŘEBÍČ DIČ:CZ46997108

VARIANT plus

VARIANT plus, spol. s r.o.
U Obůrky 5, 674 01 TŘEBÍČ
Tel/Fax: **565659681**
rh@variant.cz, www.variant.cz

Objednávky obchod@variant.cz, 565 659 600

Servis servis@variant.cz, 565 659 680

Podpis