

# Řešení přenosových tras a protokolů dohledového a poplachového přijímacího centra

Tomáš Krejčí

---

Bakalářská práce  
2018



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Tomáš Krejčí**  
Osobní číslo: **A15754**  
Studijní program: **B3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**  
Forma studia: **kombinovaná**

Téma práce: **Řešení přenosových tras a protokolů dohledového a poplachového přijímacího centra**

Téma anglicky: **Resolving Transmission Routes and Protocols in a Surveillance and Alarm Receiving Centre**

Zásady pro vypracování:

1. Vypracujte literární rešerši zaměřenou na technickou část přenosových tras signálů z PZTS do DPPC.
2. Zdokumentujte technické řešení přenosových tras DPPC firmy XY.
3. Zdokumentujte stávající překladové tabulky v administraci systému DPPC.
4. Vytvořte a zimplementujte novou překladovou tabulku SIA IP do DPPC.
5. Vytvořte manuál instalačního technika PZTS a správce DPPC v oblasti připojování střežených objektů na DPPC firmy XY.

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **IVANKA, Ján, 2014. Systemizace bezpečnostního průmyslu I. Vyd. 5. Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN 978-80-7454-410-1.**
2. **LAUCKÝ, Vladimír, 2010. Technologie komerční bezpečnosti I. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN 978-80-7318-889-4.**
3. **DRGA, Rudolf a LAUCKÝ, Vladimír, 2012. Speciální technologie komerční bezpečnosti. Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN 978-80-7454-146-9.**
4. **TNI 33 4592, Poplachové systémy a EPS – Požadavky na přenos zpráv ze střežených objektů pomocí internet protokolu, 2014. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.**
5. **ANSI/SIA DC-09-2013. SIA Digital Communication Standard Internet Protocol Event Reporting, Silver Spring: The Security Industry Association.**
6. **Radom, s.r.o., 2016. Systém RADOMNET II pro RADOM SECURITY a RADOM SECURITY FIRE: uživatelský manuál. 4. Pardubice: Radom, s.r.o.**
7. **Tyco Security Products, 2017. Zabezpečovací ústředna série Power Neo instalační manuál v 1.3. Hradec Králové: KELCOM International, spol. s r.o.**
8. **Tyco Security Products, 2016. Sur-Gard System II instalační manuál v 2.0. Hradec Králové: KELCOM International, spol. s r.o.**

Vedoucí bakalářské práce:

**Ing. Ján Ivanka**

Ústav bezpečnostního inženýrství


Datum zadání bakalářské práce:

**8. prosince 2017**

Termín odevzdání bakalářské práce:

**24. května 2018**

Ve Zlíně dne 12. prosince 2017



doc. Mgr. Milan Adámek, Ph.D.  
*děkan*



Ing. Jan Valouch, Ph.D.  
*ředitel ústavu*


### **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 diplomové/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 – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- 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, dne 23.5.2018

  
.....  
podpis diplomanta

## **ABSTRAKT**

Cílem bakalářské práce je stručně přiblížit problematiku přenosu událostí z poplachových zabezpečovacích a tísňových systémů PZTS do dohledových a poplachových přijímacích center DPPC.

V úvodu teoretické části jsou vyjmenovány základní technické normy, kterými se řídí montáž, servis a provoz zabezpečovacích systémů. Všeobecně o problematice přenosových tras, přenosových formátů a překladových tabulek pojednává část zaměřená na koncová zařízení dohledových center.

Za účelem zpřesnění a pochopení, instalačními techniky PZTS a správci DPPC, přenosu zpráv je zdokumentována a zpracována přenosová soustava dohledového centra firmy XY, kterou bakalářská práce končí.

**Klíčová slova:** dohledové a poplachové přijímací centrum (DPPC), poplachový zabezpečovací a tísňový systém (PZTS), přenosová trasa, přenosový formát

## **ABSTRACT**

The aim of the bachelor thesis is to briefly approach the issue of transmitting events from Intrusion and hold-up alarm systems (further in the work only referred to as "PZTS") into Monitoring and alarm receiving centres (further in the work only referred to as "DPPC").

At the beginning of the theoretical part the basic technical standards, which regulate the installation, maintaining and operation of alarm systems, are listed. The issue of transmission routes, transmission formats and translation tables are in general mentioned in a section focused on the endpoints of monitoring centers.

For the purpose of specification and understanding concerning transmission of messages, by installers of PZTS and administrators of DPPC, a transmission system of the monitoring centre of the XY company is documented and processed at the end of the bachelor thesis.

**Key words:** Monitoring and alarm receiving centre (DPPC), Intrusion and hold-up alarm system (PZTS), transmission route, transmission format

Na tomto místě bych rád poděkoval vedoucímu práce panu Ing. Jánů Ivankovi za veškeré rady, připomínky a předané vědomosti poskytnuté během vypracování této bakalářské práce. Zvláště pak za nekonečnou trpělivost a shovívavost.

Dále bych chtěl poděkovat mé rodině a zaměstnavateli za podporu po celou dobu studia.



# OBSAH

<b>ÚVOD</b> .....	<b>8</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>10</b>
<b>1 POPLACHOVÉ ZABEZPEČOVACÍ A TÍŠŇOVÉ SYSTÉMY</b> .....	<b>11</b>
1.1 NORMY PZTS .....	11
1.2 STUPNĚ ZABEZPEČENÍ .....	13
1.3 TŘÍDY PROSTŘEDÍ.....	14
1.4 VSTUPY A FUNKČNÍ POŽADAVKY PZTS .....	14
<b>2 DOHLEDOVÉ A POPLACHOVÉ PŘIJÍMACÍ CENTRUM</b> .....	<b>16</b>
2.1 PŘENOSOVÉ TRASY.....	17
2.1.1 Přenos po telefonní lince .....	18
2.1.2 Přenos po rádiové síti .....	19
2.1.3 Přenos po GSM – SMS .....	20
2.1.4 Přenos po GSM 3G/GPRS .....	20
2.1.5 Přenos po Internetu .....	21
2.2 PŘENOSOVÉ FORMÁTY .....	22
2.2.1 Pulsní formát .....	22
2.2.2 Tónový formát.....	23
2.2.3 Digitální (modemový) formát .....	25
2.3 PŘEKLADOVÉ TABULKY .....	26
2.3.1 Tabulka formátu 4+2.....	26
2.3.2 Tabulka formátu CID .....	27
2.3.3 Tabulka formátu SIA.....	28
<b>II PRAKTICKÁ ČÁST</b> .....	<b>30</b>
<b>3 DPPC FIMY XY</b> .....	<b>31</b>
3.1 HARDWAROVÉ VYBAVENÍ PŘENOSOVÝCH TRAS .....	32
3.1.1 Příjem zpráv po telefonní lince .....	33
3.1.2 Příjem zpráv po rádiové síti .....	36
3.1.3 Příjem zpráv po GSM – SMS.....	39
3.1.4 Příjem zpráv po Internetu, 3G/GPRS.....	41
3.1.4.1 Komunikátory RADOM .....	41
3.1.4.2 Komunikátory SATEL.....	43
3.1.4.3 Zařízení s přímým přístupem TCP, UDP.....	47
3.2 PŘEKLADOVÉ TABULKY V PPC .....	49
3.2.1 Tabulka Tel42 .....	49
3.2.2 Tabulka CID .....	50
3.2.3 Tabulka SIA IP .....	51
<b>ZÁVĚR</b> .....	<b>53</b>
<b>SEZNAM POUŽITÉ LITERATURY</b> .....	<b>55</b>
<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK</b> .....	<b>57</b>
<b>SEZNAM OBRÁZKŮ</b> .....	<b>59</b>
<b>SEZNAM TABULEK</b> .....	<b>60</b>
<b>SEZNAM PŘÍLOH</b> .....	<b>61</b>

## ÚVOD

Dnešní doba sebou přináší postupné zvyšování hodnoty majetku a tím roste potřeba jedinců i firem svůj těžce nabitý majetek náležitě chránit. Zároveň dochází k technologickým pokrokům a bezpečnostní systémy jsou čím dál více sofistikovanější. Poptávka po službách bezpečnostního průmyslu neutichá, naopak se objevuje zvýšený zájem zákazníků svoje bezpečnostní systémy modernizovat a vylepšovat. Známe rčení platí i v tomto odvětví a můžeme konstatovat, že je vsutku pravdivé: „bezpečnostní systém je tak dobrý, jak dobrý je jeho nejslabší článek“.

Celý bezpečnostní systém je pak složen ze všech možných periférií a jeho výběr by měl předcházet dokonale kompletní analýze rizik a dokonalemu bezpečnostnímu projektu, ve kterém se nemůžeme specializovat pouze na určitou část bezpečnostního opatření, musíme vzít v potaz všechny aspekty rizik a k tomu odpovídající protiopatření.

Snahou bakalářské práce je čtenářům přiblížit pouze část o bezpečnostních systémech s problematikou přenosových tras, formátů a překladových tabulek z poplachových zabezpečovacích a tísňových systémů na dohledová a poplachová přijímací centra. Jaké události se budou přenášet z PZTS a jaký mají význam práce neřeší, ale předpokládá, již určitou znalost o bezpečnostních systémech čtenáře.

Poplachové zabezpečovací a tísňové systémy (dále jen PZTS) komunikují s dohledovými a poplachovými přijímacími centry (dále jen DPPC) po mnoha komunikačních kanálech. K přenosu využívají také různé přenosové formáty. Moderní trendy přenosů, za využití Internetu a datových služeb mobilních operátorů, umožňují přenášet mnohem více informací, než bylo doposud běžné. Připojení PZTS po pevné telefonní lince se jeví jako dávnou minulostí. Většina výrobců PZTS implementuje jako primární, v některých případech i ojedinělý, formát komunikace protokol SIA IP.

V úvodní části, se bakalářská práce věnuje všeobecným požadavkům na poplachové zabezpečovací a tísňové systémy, s důrazem na přehled používaných norem v aktuálním znění. Cílem úvodu práce je čtenáři, respektive instalačním technikům, vyjmenovat a přiblížit zásadní normované požadavky, kterými by se měli řídit při montáži a servisu zabezpečovací techniky PZTS.

V části následující se čtenáři mohou dočíst, jaké komunikační kanály jsou v ČR k dispozici, jaké jsou jejich výhody, nebo naopak nevýhody. Mohou se seznámit s řešením, jak se



informace z krabičky na zdi, dostane na monitory operátorů bezpečnostních center. V posloupnosti je vyjádřen i vývoj bezpečnosti přenosu, respektive kódování událostí do přenášených zpráv, včetně závislosti na velikosti a objemu dat. Teoretickou část zakončují vztahy pro kódování a zpětný překlad přenášené zprávy v PZTS a v DPPC pomocí překladových tabulek.

Závěrem bakalářské práce, v části praktické, je zdokumentována přenosová soustava firmy XY provozující dohledové centrum a měla by sloužit instalačním technikům PZTS a správci DPPC jako manuál pro připojování objektů ke střežení.

Ve zveřejněné práci bylo použito fiktivních parametrů a nastavení, pro dokumentaci aktuálního stavu přenosových tras.

## **I. TEORETICKÁ ČÁST**

## 1 POPLACHOVÉ ZABEZPEČOVACÍ A TÍSŇOVÉ SYSTÉMY

Poplachové zabezpečovací a tísňové systémy můžeme definovat jako soubor ústředěn (řídících jednotek), detektorů, tísňových zařízení, výstražných zařízení, komunikátorů – přenosových zařízení a napájecích zdrojů, jejichž prostřednictvím je signalizováno na určeném místě, tzv. příjemce poplachu, narušení, napadení střeženého objektu nebo prostoru. V normách popisujících problematiku PZTS je také využíváno anglické označení I&HAS (Intrusion and hold-up alarm systém), což sdružuje systémy IAS (Intruder alarm systém) a HAS (Hold-up alarm systém).

Účelem PZTS je zvýšit bezpečnost střežených prostor a osob.



*Obr. 1: Vybrané prvky PZTS [11]*

### 1.1 Normy PZTS

Výroba, montáž, servis a revize se řídí řadou specifických norem a předpisů. Pro obor PZTS jsou v platném znění především normy řady ČSN EN 50131-X. Aktuální znění všech norem je dostupné na [www: < https://csnonline.unmz.cz >](https://csnonline.unmz.cz), jedná se o placenou službu. V *Tab. 1* je výčet platných norem k V.2018.

Tab. 1: Základní přehled platných norem PZTS

Označení	Zkrácený název normy	Datum akt.
ČSN EN 50130-4 ed. 2	Pop.sys. - Část 4: Elektromagnetická kompatibilita - Norma skupiny výrobků: Požadavky na odolnost komponentů požárních systémů, poplachových zabezpečovacích a tísňových systémů a systémů CCTV, kontroly vstupu a přivolání pomoci	IV.15
ČSN EN 50130-5 ed. 2	Pop.sys. - Část 5: Metody zkoušek vlivu prostředí	V.12
ČSN EN 50136-1	Pop.sys. - Pop. přenosové sys. a zař. - Část 1: Obecné požadavky na poplachové přenosové systémy	X.12
ČSN EN 50136-2	Pop.sys. - Pop. přenosové sys. a zař. - Část 2: Požadavky na komunikátor ve střeženém prostoru (SPT)	VII.14
ČSN CLC/TS 50136-7	Pop.sys. - Pop. přenosové sys. a zař. - Část 7: Pokyny pro aplikace	XII.17
ČSN CLC/TS 50136-9	Pop.sys. - Pop. přenosové sys. a zař. - Část 9: Požadavky na obecný protokol pro přenos poplachu s využitím Internetového protokolu	XII.17
ČSN EN 50131-1 ed. 2	Pop.sys. - PZTS - Část 1: Systémové požadavky	XI.17
ČSN CLC/TS 50131-2-10	Pop.sys. - PZTS - Část 2-10: Detektory narušení - Detektory stavu otevření (magnetické kontakty)	X.14
ČSN EN 50131-2-2 ed. 2	Pop.sys. - PZTS - Část 2-2: Detektory narušení - Pasivní infračervené detektory	VI.18
ČSN EN 50131-2-3	Pop.sys. - PZTS - Část 2-3: Požadavky na mikrovlnné detektory	IX.14
ČSN EN 50131-2-4	Pop.sys. - PZTS - Část 2-4: Požadavky na kombinované pasivní infračervené a mikrovlnné detektory	IX.14
ČSN EN 50131-2-5	Pop.sys. - PZTS - Část 2-5: Požadavky na kombinované pasivní infračervené a ultrazvukové detektory	IX.14
ČSN EN 50131-2-6	Pop.sys. - PZTS - Část 2-6: Detektory otevření (magnetické kontakty)	IX.14
ČSN EN 50131-2-7-1	Pop.sys. - PZTS - Část 2-7-1: Detektory narušení - Detektory rozbíjení skla (akustické)	XI.16
ČSN EN 50131-2-7-2	Pop.sys. - PZTS - Část 2-7-2: Detektory narušení - Detektory rozbíjení skla (pasivní)	XI.16
ČSN EN 50131-2-7-3	Pop.sys. - PZTS - Část 2-7-3: Detektory narušení - Detektory rozbíjení skla (aktivní)	XI.16
ČSN CLC/TS 50131-2-8	Pop.sys. - PZTS - Část 2-8: Detektory narušení - Otřesové detektory	IX.14
ČSN EN 50131-3	Pop.sys. - PZTS - Část 3: Ústředny	I.10
ČSN EN 50131-4	Pop.sys. - PZTS - Část 4: Výstražná zařízení	III.10
ČSN EN 50131-5-3 ed. 2	Pop.sys. - Elektrické zabezpečovací systémy - Část 5-3: Požadavky na zařízení využívající bezdrátové propojení	IX.17
ČSN CLC/TS 50131-5-4	Pop.sys. - PZTS - Část 5-4: Zkoušky systémové kompatibility I&HAS zařízení nacházejících se ve střežených prostorech	IV.13

ČSN EN 50131-6 ed. 3	Pop.sys. - PZTS - Část 6: Napájecí zdroje	III.18
ČSN CLC/TS 50131-7	Pop.sys. - PZTS - Část 7: Pokyny pro aplikace	IV.11
ČSN EN 50131-8	Pop.sys. - PZTS - Část 8: Zamlžovací bezpečnostní zařízení/systémy	III.10
ČSN CLC/TS 50131-9	Pop.sys. - PZTS - Část 9: Verifikace poplachu - Metody a principy	VII.15
ČSN EN 50131-10	Pop.sys. - PZTS - Část 10: Aplikace specifických požadavků na komunikátor ve střeženém prostoru (SPT)	II.15
ČSN CLC/TS 50131-11	Pop.sys. - PZTS - Část 11: Tísňová zařízení	IX.14
ČSN CLC/TS 50131-12	Pop.sys. - PZTS - Část 12: Metody a požadavky pro nastavování stavu střežení a klidu poplachových zabezpečovacích systémů (IAS)	I.17

## 1.2 Stupně zabezpečení

Norma ČSN EN 50131-1 ed.2/A1/A2/Z2 odst.6 nám definuje jednotlivé stupně zabezpečení prvků PZTS. Celý systém PZTS pak odpovídá nejnižší hodnotě stupně zabezpečení použité komponenty. Jednotlivé stupně nám určují míru rizika překonání systému a jako vodítko pro stanovení rizika slouží případná znalost a vybavenost lupiče nebo „vetřelce“ (termín vetřelec zahrnuje všechny typy ohrožení, např. loupežné přepadení, pohružky fyzickým násilím apod.). Rozlišujeme čtyři stupně zabezpečení, přičemž nejnižší je stupeň 1 a nejvyšší stupeň 4.

Tab. 2: Stupně zabezpečení [12]

<b>Stupeň 1: Nízké riziko</b>	Předpokládá se, že vetřelec nebo lupič mají malou znalost I&HAS a mají k dispozici omezený sortiment snadno dostupných nástrojů.
<b>Stupeň 2: Nízké až střední riziko</b>	Předpokládá se, že vetřelec nebo lupič mají omezené znalosti I&HAS a používání běžného nářadí a přenosných přístrojů (např. multimetr).
<b>Stupeň 3: Střední až vysoké riziko</b>	Předpokládá se, že vetřelec nebo lupič jsou obeznámeni s I&HAS a mají rozsáhlý sortiment nástrojů a přenosných elektronických zařízení.
<b>Stupeň 4: Vysoké riziko</b>	Používá se tehdy, má-li zabezpečení prioritu před všemi ostatními hledisky. Předpokládá se, že vetřelec nebo lupič jsou schopní nebo mají možnost vypracovat podrobný plán vniknutí a mají kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících komponentů I&HAS.

### 1.3 Třídy prostředí

Při výběru jednotlivých komponent systémů PZTS je nutné brát v potaz vliv prostředí, do kterého bude každý jednotlivý prvek instalován. Komponenty musí správně pracovat, jsou-li vystaveny působení vlivu prostředí až do třídy, dle definice normy ČSN EN 50131-1/A1/A2/Z2 odst.7, do které jsou přiřazeny.

Tab. 3: Třídy prostředí [12]

<b>Třída prostředí 1 - vnitřní</b>
<p>Vlivy prostředí vyskytující se obvykle ve vnitřních prostorách při stálé teplotě (například obytných nebo obchodních objektech).</p> <p>Poznámka – předpokládají se změny teploty v rozmezí +5°C až +40°C při střední relativní vlhkosti přibližně 75% bez kondenzace.</p>
<b>Třída prostředí 2 - vnitřní - všeobecné</b>
<p>Vlivy prostředí vyskytující se obvykle ve vnitřních prostorách, kde není stálá teplota (například na chodbách, v halách nebo na schodištích a tam, kde může docházet ke kondenzaci na oknech a v nevytápěných skladových prostorách nebo schodištích v nichž vytápění není trvalé.</p> <p>Poznámka – předpokládají se změny teplot v rozmezí -10°C až +40°C při střední relativní vlhkosti přibližně 75% bez kondenzace.</p>
<b>Třída prostředí 3 - venkovní - chráněné nebo extrémní vnitřní podmínky</b>
<p>Vlivy prostředí vyskytující se obvykle vně budov, přičemž komponenty I&amp;HAS nejsou plně vystavené povětrnostním vlivům.</p> <p>Poznámka – předpokládají se změny teplot v rozmezí -25°C až +50°C při střední relativní vlhkosti přibližně 75% bez kondenzace. Po dobu 30 dní v průběhu roku se mohou změny relativní vlhkosti pohybovat v rozmezí 85% až 95% bez kondenzace.</p>
<b>Třída prostředí 4 - venkovní - všeobecné</b>
<p>Vlivy prostředí vyskytující se obvykle vně budov, přičemž komponenty I&amp;HAS jsou plně vystavené povětrnostním vlivům.</p> <p>Poznámka – předpokládají se změny teplot v rozmezí -25°C až +60°C při střední relativní vlhkosti přibližně 75% bez kondenzace. Po dobu 30 dní v průběhu roku se mohou změny relativní vlhkosti pohybovat v rozmezí 85% až 95% bez kondenzace.</p>

### 1.4 Vstupy a funkční požadavky PZTS

Systémy PZTS musí v závislosti na požadavku stupně bezpečnosti přijímat a vyhodnocovat různé nahodilé stavy vzniklých situací. Norma ČSN EN 50131-3 nám definuje základní

funkční požadavky na ústředny a jejich vstupy (stavy od detektorů). Systémy musí umět detekovat, zaznamenat, vyhodnotit a předat zejména stavy:

- narušení,
- tísňové,
- sabotážní,
- poruchové,
- vstup/výstup uživatelů,
- zakrytí, maskování,
- snížení rozsahu pokrytí detektoru,
- nepoplachové (technické) vstupy.



## 2 DOHLEDOVÉ A POPLACHOVÉ PŘIJÍMACÍ CENTRUM

Dohledové a poplachové přijímací centrum (DPPC, dříve označováno PCO) si lze představit jako dispečerské pracoviště s nepřetržitým provozem, sloužící ke sběru aktuálních stavů a informací ze střežených objektů. Aktuální stavy jsou přenášeny na DPPC pomocí speciálních kódovaných zpráv z bezpečnostních systémů, např. PZTS, EPS nebo CCTV.



*Obr. 2: DPPC Jablotron [13]*

Úkolem DPPC je obdržené informace kvalifikovaně vyhodnotit a učinit všechna možná opatření na vzniklou situaci. Scénáře postupů si většinou určuje zákazník (v koordinaci s bezpečnostní agenturou) a operátor dohledového centra postupuje přesně dle pokynů k jednotlivým objektům. Většina DPPC v ČR disponuje vlastní zásahovou skupinou, a tak jsou bezpečnostní agentury schopny zajistit vyšší bezpečnost střežených objektů a osob. Úkolem operátora je tak i veškerá koordinace prováděných zásahů, případné předání události k došetření Policii ČR

K přenosu zpráv z objektů (bezpečnostních ústředí) slouží přenosové systémy a zařízení. Požadavky na přenos definuje řada norem ČSN EN 50136.

Tab. 4: Výčet norem pro přenosové trasy

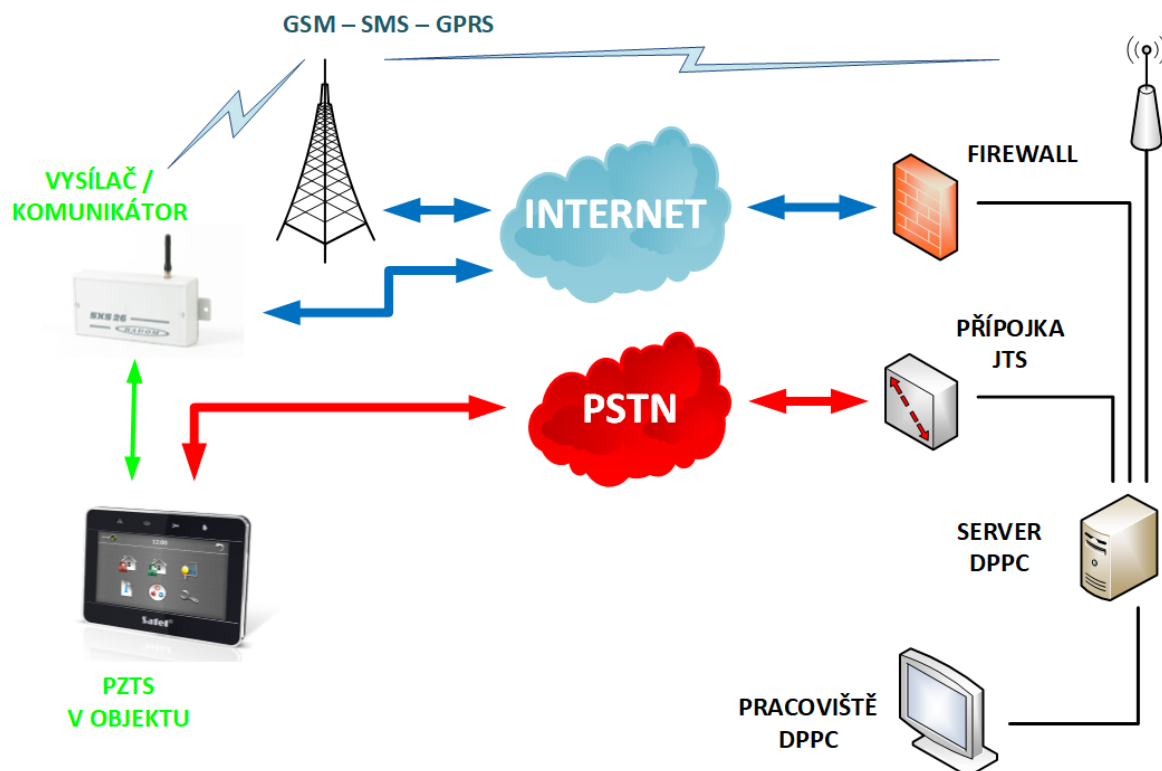
Označení	Zkrácený název normy	Datum akt.
ČSN EN 50136-1	Pop.sys. - Pop. přenosové sys. a zař. - Část 1: Obecné požadavky na poplachové přenosové systémy	X.12
ČSN EN 50136-2	Pop.sys. - Pop. přenosové sys. a zař. - Část 2: Požadavky na komunikátor ve střeženém prostoru (SPT)	VII.14
ČSN EN 50136-3	Pop.sys. - Pop. přenosové sys. a zař. - Část 3: Požadavky na komunikátor přijímacího centra (RCT)	VII.14
ČSN CLC/TS 50136-4	Pop.sys. - Pop. přenosové sys. a zař. - Část 4: Indikační a ovládací zařízení používaná v poplachových přijímacích centrech	XI.05
ČSN CLC/TS 50136-7	Pop.sys. - Pop. přenosové sys. a zař. - Část 7: Pokyny pro aplikace	XII.17
ČSN CLC/TS 50136-9	Pop.sys. - Pop. přenosové sys. a zař. - Část 9: Požadavky na obecný protokol pro přenos poplachu s využitím Internetového protokolu	XII.17

## 2.1 Přenosové trasy

Mezi bezpečnostními ústřednami PZTS a dohledovými centry DPPC, respektive poplachovými přijímacími centry (dále jen PPC), probíhá výměna informací pomocí přenosových zařízení (komunikátorů) s využitím různých přenosových tras. Komunikace může být jednosměrná nebo obousměrná, v závislosti na použití komponent přenosového systému. Každá přenosová trasa má svá specifika spolehlivosti, odolnosti nebo finanční náročnosti. Zároveň však každý zabezpečený objekt má jinou hodnotu a jiné nároky na stupeň zabezpečení. U objektů vyšších stupňů zabezpečení je požadováno využití dvou nezávislých komunikačních kanálů.

Výběr komunikačních tras musí bezpodmínečně vzejít z doporučení bezpečnostní agentury a bezpečnostního technika s přihlédnutím na střežený majetek a finanční možnosti zákazníka. Správná volba komunikačního kanálu je důležitým aspektem celého bezpečnostního systému a důležitým faktorem na poskytovanou službu.

*Obr. 3* graficky znázorňuje možný výběr komunikačních tras. Schematicky je naznačeno propojení jednotlivých základních komponent systému.



Obr. 3: Zjednodušené schéma komunikačních tras, vlastní zdroj.

### 2.1.1 Přenos po telefonní lince

V minulosti nejčastěji používané připojení zabezpečovacích ústředen k dohledovým centřům DPPC (dříve označováno PCO). Výrobci ústředen PZTS (dříve označováno EZS) implementovali telefonní komunikátory přímo na desky ústředen, právě pro širokou přístupnost a relativně i cenovou dostupnost.

Pro přenos informací slouží hovorové pásmo jednotné telefonní sítě (JTS). Ústředny PZTS navazují spojení s PPC vytvořením telefonního čísla nebo čísel navázaných na hardware dohledového centra. Po předání informací a příjmu potvrzení ze strany PPC ústředna komunikaci ukončí zavěšením linky.

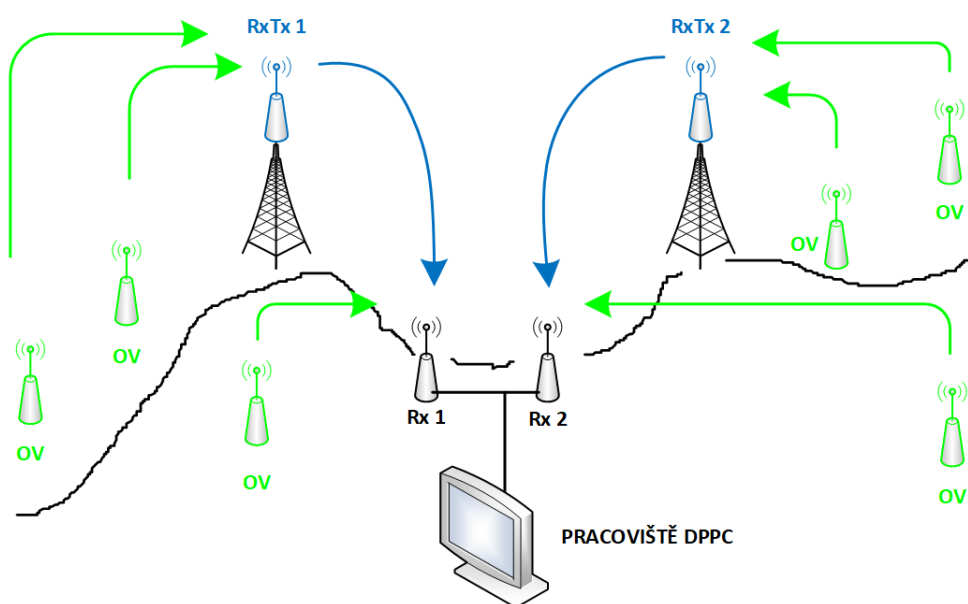
Toto připojení není v dnešní době doporučováno vzhledem k velké časové odezvě přenosu a také vzhledem k bezpečnostnímu riziku přerušování telefonního připojení pachatelem. Testy spojení jsou obvykle nastaveny pouze na jeden testovací přenos za 12 nebo 24 hodin.

### 2.1.2 Přenos po rádiové síti

Mezi nejspolehlivější způsoby komunikace PZTS a PPC můžeme určitě zařadit přenosy po vyhrazené rádiové síti. Bezpečnostní agentury provozující dohledová centra mají pro tyto přenosy vyhrazený vlastní frekvenční rozsah, mají vybudovanou vlastní rádiovou síť a pro komunikaci slouží speciální rádiové vysílače. Pro vykrytí většího území příjmu signálu jsou bezpečnostní agentury nuceni zřizovat retranslační stanice.

Na *Obr. 4* vidíme princip předávání událostí po vytvořené rádiové síti s využitím:

- OV – objektových vysílačů,
- RxTx – retranslačních stanic,
- Rx – koncových přijímacích stanic PPC.



*Obr. 4: Blokové schéma rádiové sítě DPPC, vlastní zdroj*

Správu rádiového spektra v ČR zastřešuje Český telekomunikační úřad (dále jen ČTÚ), který uděluje (odebírá) oprávnění k využití přiděleného komunikačního rozsahu (frekvence). V současnosti je využívána pro přenos signálů bezpečnostních systémů frekvence 400 MHz. Dosah radiovysílačů je omezen na maximální vzdálenost 20 km. Komunikace probíhá v režimu vysílač – přijímač a je jednosměrná. V principu vysílač vysílá určitý počet telegramů za určitý čas, v případě neobdržení stanoveného počtu telegramů vyhlásí PPC ztrátu spojení s objektem.

Velikou nevýhodou této přenosové soustavy je bohužel její finanční náročnost jak na provozatele DPPC, tak pro jejich zákazníky (koncové uživatele).

### 2.1.3 Přenos po GSM – SMS

S rozvojem mobilních sítí a nabídkou operátorů na jejich služby se samozřejmě začaly objevovat komunikátory pro přenos informací po síti GSM (Globální Systém Mobilní komunikace).

Zpočátku se využívalo pro přenos zpráv z ústředí PZTS hovorového pásma, obdobně jako při využití telefonní linky. Výhodou tohoto připojení je prioritizace mobilních operátorů na právě hovorové pásmo svého přiděleného kmitočtu. Nevýhodou jsou pak provozní náklady na mobilní vytáčené připojení a tím uskutečňované placené hovory. V posledních letech však operátoři nabízejí různé balíčky, nebo neomezené volání za paušální ceny.

Alternativou je využití služeb, kdy komunikátor zakóduje přenášené informace z ústředny do krátké textové zprávy (dále jen SMS) a odešle do přijímače PPC. Toto opticky jednoduché řešení má však jednu obrovskou nevýhodu. Omezené frekvenční pásmo mobilních operátorů tento kanál v případě zatížení ostatních kanálů zařadí na kanál s nejnižší prioritou přenosu. V praxi je zcela běžné, že doručení SMS zprávy může trvat až 72 hodin.

V dnešní době jsou oba přenosy GSM i SMS doporučovány pouze jako záložní, pro jinou primární přenosovou trasu.

### 2.1.4 Přenos po GSM 3G/GPRS

Sítě GSM disponují také datovým pásmem a službou GPRS (General Packet Radio Service), která využívá pro přenos dat technologie přepojování paketů a volných časových slotů. Kvalitu připojení zajišťuje pokrytí signálem operátor mobilních služeb. V současnosti operátoři nabízejí zvýhodněné sazby pro technologická zařízení (označují je M2M – Machine to Machine) s nízkým měsíčním přenosem dat, a tak se tato cesta stala jednou z neekonomičtějších na provoz. Datové přenosy obvykle nepřekročí 50 MB objemu dat za měsíc.

Velikou výhodou datového připojení je možnost plynulé obousměrné komunikace mezi systémem PZTS a dohledovým centrem PPC, popř. lze navázat i uživatelské funkce systému. Moderní systémy PZTS disponují také celou řadou podpůrných technologických prvků (např. k ovládání vytápění, ovládání rolet nebo dalšími různými ovládacími prvky). S ústřednami PZTS a datovým připojením jsou dodavatelé systémů téměř neomezeni na různorodé

aplikace a požadavky zákazníků. Prioritou však zůstává (oproti systémům „chytré domácnosti“) bezpečnost střeženého prostoru, resp. osob.

Přenosové trasy GPRS jsou monitorovány DPPC téměř nepřetržitě. Při ztrátě několika málo paketů ze střeženého objektu systémy PPC vyhlásí ztrátu spojení s objektem a pokusí se o opětovné navázání spojení. V případě neúspěchu upozorní operátora o dlouhodobé neúspěšné komunikaci s objektem. Ten dle pokynů z karty objektu učiní patřičná opatření.

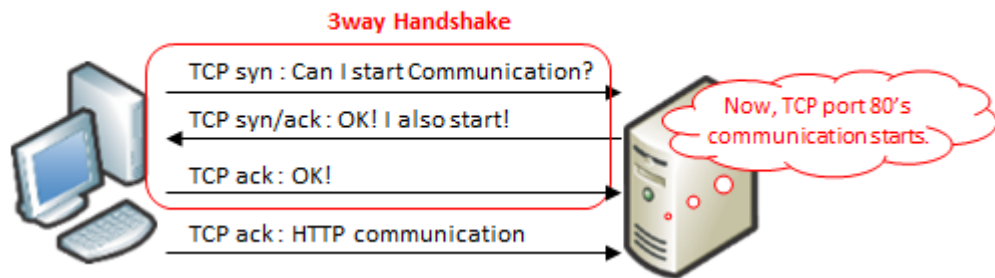
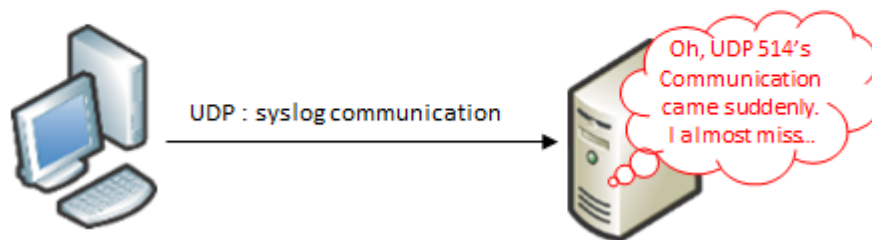
Žádný systém není však nenapadnutelný, a tak i tato přenosová trasa v sobě nese riziko zarušení. Pachatelům jsou bohužel dobře dostupné tzv. rušičky signálů, které se při napadení objektů nezdráhají použít. Dobré bezpečnostní agentury doporučují svým zákazníkům tyto trasy zálohovat jinou nezávislou přenosovou cestou.

### 2.1.5 Přenos po Internetu

Internet se stal součástí téměř každé domácnosti nebo podniku. Právě pro jeho dostupnost je přenosová trasa jedna z nejpoužívanějších dnešní doby. Instalace internetového komunikátoru PZTS bývá velmi snadná a montážní technici připojují komunikátor jako každé další zařízení do lokálních sítí LAN (Local Area Network) v zabezpečeném objektu.

Komunikace je stejně jako u přenosů GPRS obousměrná a běží v reálném čase. Ztráty spojení jsou vyhodnocovány okamžitě a operátoři dohledových center DPPC mají plnou kontrolu nad stavy připojených objektů. Velkou podporu při vyhodnocování informací z poplachových zařízení může poskytnout kamerový systém instalovaný v zabezpečených objektech.

Pro transport informací od PZTS do PPC jsou využívány protokoly TCP a UDP. Pro jednoduchost můžeme říci, že TCP protokol je spolehlivější, ověřovaný s obousměrnou komunikací. UDP je oproti tomu jednodušší, ale bez ověření přenášené informace. Výhodou UDP je však jeho menší zatížení datového přenosu a především větší rychlost předané zprávy. Volba protokolu může být závislá na zvolené technologii, nebo nastavením komunikace instalačním technikem.

How to start TCP communicationHow to start UDP communication

Obr. 5: Navázání spojení při TCP a UDP [14]

Kvalita a spolehlivost internetového připojení je především závislá na volbě providera ISP (Internet service provider). Je zřejmé, že připojení pomocí optické sítě, nebo metalicky bude mnohonásobně spolehlivější než připojení pomocí Wi-Fi.

I k tomuto typu přenosové trasy musí být bezpečnostní agenturou doporučena záložní komunikační cesta.

## 2.2 Přenosové formáty

Na rozdíl od komunikačních tras je volba na přenosové formáty plně v kompetenci bezpečnostní agentury provozující DPPC, resp. na použitém hardwaru. Jen bezpečnostní technik PZTS (DPPC) je schopen určit, které informace budou přenášeny a v jakém formátu. Správná volba formátu ovlivňuje bezpečné předávání mezi ústřednou PZTS a přijímači DPPC.

V principu jde o to, jakým způsobem budou zakódované zprávy předávány mezi komunikátorem PZTS a přijímačem PPC po zvolené přenosové trase.

### 2.2.1 Pulsní formát

Pulsní formáty byly využívány především v dobách přenosu po pevných telefonních linkách. Požadavek byl na co nejrychlejší předání informace a tím pádem nebylo moc prostoru na



přenášení mnoha informací. Zpráva musela být co nejmenší a nejjednodušší. V dnešní době se tento přenosový formát využívá jen zřídka.

Pro přenos pulsních formátů jsou využívány analogové telefonní linky. Informace a přenášené zprávy jsou kódovány do určitého počtu pulsů za určitý čas. Rychlost přenosu určuje použitý hardware bezpečnostního systému PZTS i PPC. Pracuje se o rychlostech 1200, 2400 nebo 4600 bit/s. Kontrola přenosu informace nebo zprávy vyžaduje zopakování celého balíku přenášených dat.

Tab. 5: Protokoly pro pulsní přenos [15]

Název protokolu	Handshake	Kiss off	Protokol	Formát
<b>Ademco Slow</b>	1400Hz	1400Hz	10bps	4/2
<b>Silent Knight fast</b>	1400Hz	1400Hz	14bps	4/2
<b>Franklin</b>	2300Hz	2300Hz	20bps	4/2
<b>Radionics</b>	2300Hz	2300Hz	40bps	4/2
<b>Sur-Gard</b>	2300Hz	2300Hz	DTMF	4/3

Nejčastěji používaným formátem je však 4+2. První čtyři číslice označují číslo objektu a zbylé dvě udávají kód události.

Klíč kódování je velice jednoduchý a to tak, že počet pulsů se rovná danému číslu v HEX soustavě, tzn. zároveň i maximální počet definovaných zpráv na 256. Např. tři pulsy jsou rovny číslici 3, deset pulsů odpovídá písmenu A. 0 se u tohoto formátu vynechává, resp. není definována a v čísle objektu se používá právě písmeno A.

Každá bezpečnostní agentura provozující DPPC používá vlastní překladovou tabulku pro kódování a dekódování zpráv přenášených formátem 4+2,

### 2.2.2 Tónový formát

Modernější způsob komunikace v hovorových pásmech přenosových tras spočívá v přenosu tónů. Číslice jsou kódovány do dvojice tónů o různých frekvencích. Tím se rapidně zkrátila doba potřebná pro přenos a odpočítávání pulsů, zároveň také došlo ke zmenšení chybovosti a přeslechu přenášených informací. Kontrola přenosu již spočívá pouze v kontrolním součtu.

Standard tónového přenosu (DTMF) je 50 ms tónu a 50 ms ticha. Při využití větších frekvencí (rychlejší komunikace) mohou nastat problémy se synchronizací a časováním. Odchylka frekvencí může mít maximální hodnotu  $\pm 1,5\%$ .

Tab. 6: DTMF tabulka frekvencí

HEX	Spodní tón (Hz)	Horní tón (Hz)	DEC
<b>1</b>	697	1209	1
<b>2</b>	697	1336	2
<b>3</b>	697	1477	3
<b>4</b>	770	1209	4
<b>5</b>	770	1336	5
<b>6</b>	770	1477	6
<b>7</b>	852	1209	7
<b>8</b>	852	1336	8
<b>9</b>	852	1447	9
<b>A=0</b>	941	1336	10
<b>B</b>	941	1209	11
<b>C</b>	941	1477	12
<b>D</b>	697	1633	13
<b>E</b>	770	1633	14
<b>F</b>	852	1633	15

V přenosu s tónovou volbou se otevřela možnost přenášet více informací za stejný čas. Výrobci ústředěn sjednotili kódovací protokoly (překladové tabulky) a tím instalačním technikům systémů PZTS odpadla nutnost vyžadovat překladové tabulky od provozovatelů DPPP.

V ústřednách však i nadále zůstává možnost volby informací a zpráv, které budou přenášeny na monitory operátorů DPPC.

Tab. 7: Protokoly pro tónový přenos [15]

Název protokolu	Handshake	Kiss off	Protokol	Formát
<b>Sur-Gard</b>	Dual tone	1400Hz	DTMF	4/3
<b>Ademco fast DTMF</b>	Dual tone	1400Hz	DTMF	4/9
<b>Ademco expres</b>	Dual tone	1400Hz	DTMF	4ID/2
<b>Contact ID DSC</b>	Dual tone	1400Hz	DTMF	4ID/4
<b>Contact ID</b>	Dual tone	1400Hz	DTMF	CID

Nejvýznamnějším zástupcem tónového formátu je pak Ademco CID (Contact ID).

### 2.2.3 Digitální (modemový) formát

Poslední a nejmodernější přenosový formát je pak již formát digitální. Přenášeny jsou pak datové pakety zakódovány dle překladových tabulek a zároveň se také zavádí šifrování dat. Pro kryptování je pak použita šifra AES (128, 192 nebo 256 bitů). Digitální formát umožňuje i určitou kontrolu přenášených událostí, jednoznačnou a ověřenou identifikaci zabezpečeného objektu, ať ze strany ID objektu, IP nebo MAC adresy.

Komunikace jsou již plně duplexní a umožňují systémům DPPC také částečné ovládání PZTS. Pro velkou datovou propustnost přenosovým kanálem je přenášeno mnohem více informací než v předešlých případech. Pokud HW a SW vybavení DPPC dovolí, jsou přenášeny i např. názvy bloků, zón nebo jména obsluh systému PZTS instalovaného v zabezpečeném objektu.

Výrobci moderních zařízení PPC již plně implementovali do svých výrobků datovou komunikaci s protokolem IP (TCP i UDP) a bezpečnostní agentury provozující DPPC nasazují, dotvářejí do svých softwarů překladovou tabulku SIA IP.

## 2.3 Překladové tabulky

Aby bylo možné zasílané zprávy z ústředny PZTS bezchybně zobrazovat na monitoru stanice DPPC, musí zasílaná data být správně kódována na straně PZTS a správně rozkódována na straně PPC (poplachové přijímací centrum). Musí být zabezpečen soulad v programování komunikátoru ústředny a nastavením karty objektu na straně PPC. Tento soulad nám zajistí překladové tabulky a správně nastavená komunikační trasa. Jak bylo již výše zmíněno, jsou tabulky, které jsou plně v kompetenci správců systémů PPC a naopak tabulky, které jsou normované. Instalační technik se musí bezpodmínečně informovat a seznámit s komunikačními formáty a překladovými tabulkami dohledového centra bezpečnostní agentury, ke kterému zabezpečovaný objekt připojuje.

### 2.3.1 Tabulka formátu 4+2

Jak již bylo zmíněno tabulku „pomaleho“ formátu 4+2 si vytváří administrátoři PPC sami, je pouze na nich společně s instalačními technikami, jaké události z PZTS se budou přenášet na dispečerské pracoviště DPPC. Samozřejmě tím nesmí být dotčeny požadavky a přání zákazníka.

Tato tabulka se používá především při přenosu po pevných telefonních linkách s pulsním formátem. Nové instalace zabezpečovacích systémů již tímto způsobem s největší pravděpodobností připojené nebudou, ale stále se setkáváme s instalacemi, které tento přenos a kódování využívají.

Formát zprávy na PPC je pak znázorněn v *Tab. 8*

*Tab. 8: Formát 4/2*

ABCD YZ	
ABCD	Identifikační číslo objektu (1-F)
YZ	Kód události

Základ tohoto překladu spočíval v jednoduchém klíči a to tak, že **X** (první číslice kódu události) prezentovalo typ události a **Y** (druhá číslice) znamenala konkrétní smyčku, nebo uživatele. Záleží však na požadavku na přenášené události a na omezení překladové tabulky na maximálně 256 pozic. Např. kód 9876 11 by se mohl překládat jako **Poplach zóny 1** na objektu s **identifikačním číslem 9876**.

### 2.3.2 Tabulka formátu CID

Nejvýznamnějším zástupcem překladu přenosu přes tónový formát je tabulka Ademco Contact ID (dále jen CID). Řada systémů komunikujících moderním datovým přenosem však tuto tabulku využívá také. Tato tabulka je svou strukturou velmi jednoduchá, ale hlavně byla standardizovaná, a výrobci zabezpečovacích systému, až na výjimky, implementují normovanou tabulku CID do svých výrobků. Řetězec Q XYZ pak příkládají do instalačních manuálů ústředny.

Tab. 9: Struktura tabulky CID

<b>ACCT MT QXYZ GG CCC</b>	
<b>ACCT</b> (account)	4 čísla pro <b>identifikaci objektu</b> (1 – F)
<b>MT</b> (message type)	<b>Formát zprávy.</b>  Toto dvoumístné číslo definuje PPC, že zpráva je ve formátu Contact ID, a zároveň i jeho verzi. Pro toto určení je použita standardně hodnota 18 nebo hodnota 98.
<b>Q</b> (event qualifer)	Definuje <b>druh události</b> :  1 – Vznik nové událost nebo odemčeno 3 – Obnova události nebo zavřeno 6 – Potvrzení dříve přenesené události
<b>XYZ</b> (event code)	3 čísla určující <b>událost</b> (1 – F)
<b>GG</b> (group)	<b>Čísla podsystému nebo skupiny</b> (1 – F)
<b>CCC</b> (zone number)	<b>Číslo zóny, uživatele</b> , (1 – F)  Pokud není u události další určení (uživatel, zóna) je posláno číslo AAA (000).
<b>S</b> (checksum)	<b>Kontrolní součet</b>  Součet všech čísel + S musí být dělitelný 15 beze zbytku. (součet všech čísel + S) MOD 15= 0  Pokud je číslo přímo dělitelné 15 a není potřeba přičítat, je na tuto pozici poslána hodnota F.

Při přenosu jsou použity HEXA čísla 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Přenos A(hex) značí v čísle objektu 0. V nastaveních PPC se často objevuje volba překladu A-0, nebo 0-A. Rozdíly jsou způsobeny v druhu přenosového kanálu a použití různých ústředen. Je potřeba si uvědomit, zda 0 nebo A je použito v ID objektu nebo kódu události.

### 2.3.3 Tabulka formátu SIA

Prozatím poslední a nejmodernější přenos signálů je po datových kanálech, prostřednictvím digitálních komunikátorů a sítí. V současnosti se pro překlad událostí využívá standardu dle ANSI/SIA DC-09-2013 (Approved American National Standard/Security Industry Association). Dokument SIA Digital Communication Standard – Internet protokol Event Reporting (2013) podrobně vysvětluje jaké kódy protokol SIA používá, jaké přenosové kanály a s jakým protokolem pracuje.

SIA formáty slibují jednotnou obousměrnou komunikaci „většiny“ renomovaných výrobců bezpečnostní techniky. Ovšem to jsme si již slibovali i od formátů CID.

Velkou výsadou je pak zavedení časových razítek přímo v přenášené zprávě (timestamp), jednoznačná identifikace a verifikace původce (IP nebo MAC adresa) zprávy a v neposlední řadě zavedení kryptovacího mechanismu. Je využíváno symetrického šifrování AES, počet bitů a systém nasazení je pak odvislý od výrobce komunikačních prvků přenosových tras.

Výrobci zařízení PPC však tento celý protokol filtrují a při tvorbě tabulek administrátorům „zjednodušují“ jejich práci na nezbytné minimum. Při tvorbě překladových tabulek bohužel musíme vzít v úvahu verzi protokolu SIA, kterou do svých zařízení implementoval výrobce bezpečnostního systému PZTS. I když výrobci „slibovali“ přistoupení na jednotnost, najdeme v datasheetech ústředen od různých výrobců rozdíly. Provozovatelé dohledových center budou muset vytvořit překladové tabulky dle výrobců, pravdou ale je, že princip zůstává stejný.

Předpis zprávy vychází z následujícího vzorce *Tab. 10*:

Tab. 10: Předpis překladové tabulky SIA [16]

<LF><CRC><0LLL> <“id“><seq><Rcvr><Lpref><#acct>[<pad>  ...data... ] [x...data ]<timestamp> <CR>	
<b>LF</b>	ASCII znak 0x0A hex
<b>CRC</b>	započítávají se první platný znak ID až poslední znak před CR
<b>0LLL</b>	délka zprávy, započítávají se stejné znaky jako u CRC
<b>„id“</b>	toto pole obsahuje informaci (příznak) o použitém formátu datového pole ve zprávě, typu zprávy a informaci, zda je či není použito kryptování
<b>seq</b>	vysílací zařízení přiřadí číslo každé generované zprávě. PPC vysílá toto číslo zpět v potvrzovací zprávě. Pokud zpráva není potvrzena, číslo se nezvyšuje. Rozsah čísel zpráv je 0001–9999
<b>Rcvr</b>	číslo příjemce slouží k dalšímu rozšíření identifikačního čísla, jako jeho prefix. Hodnoty jsou ASCII „R1-R6“. Vysílání tohoto parametru je nepovinné
<b>Lpref</b>	Account prefix) rozšíření ID o další čísla ... L+1-6 hex čísel. Pokud toto nechceme využít vysíláme L0. Parametr je podobný jako linka příjemce
<b>#acct</b>	ID objektu naprogramované v objektovém zařízení
<b>pad a data</b>	výplň datového pole na sudý násobek 16 pro kódování
<b>x.data</b>	přidává k datům další rozšiřující informace např. MAC Adresu
<b>timestamp</b>	(časové razítko) <_HH:MM:SS,MM-DD-YYYY> čas je GMT povolená diference pro platnost zprávy je +20/-40 sec
<b>CR</b>	ASCII znak 0x0D hex



## **II. PRAKTICKÁ ČÁST**

### 3 DPPC FIMY XY

Dohledové a poplachové přijímací centrum společnosti XY využívá k příjmu a vyhodnocení událostí z bezpečnostních systémů softwarový nástroj RADOMNET II od společnosti RADOM Pardubice. Systém RADOMNET pracuje na architektuře server – klient, kde příjem, překlad, zpracování a archivaci obstarává serverová aplikace RADOMNET SERVER instalovaná na serveru a vyhodnocení příchozích událostí operátorovi dohledového centra zprostředkuje aplikace RADOMNET CLIENT. Pracovních stanic může být v systému desítky.

As vzniklu	Objekt (Filt)	Text	Data	Medium	Čas zařízení	Událost
05.2018 12:37:12	1203	Periodický test ústředny	0x16 A2 AA AA A	TelefonSmet : 1		Informační událost bez upozornění
05.2018 12:35:56	1277					Operátor odbavil událost
05.2018 12:35:42	1230	Operátor vyhodnotil událost jako planou				Operátor odbavil událost
05.2018 12:35:26	1230	obnova narušení zóny 33	0x31 33 A8 A3 3	TelefonSmet : 1		Deaktivace poplachu
05.2018 12:35:19	1230	Odbavení zvukové signalizace				Vypnutí zvukové signalizace dispečerem
05.2018 12:35:18	1230	Poplach 24 hod zóny 33 v bloku 8	0x11 33 A8 A3 3	TelefonSmet : 1		Aktivace poplachu
05.2018 12:34:38	1212	Periodický test ústředny	0x16 A2 A1 AA A	TelefonSmet : 1		Informační událost bez upozornění
05.2018 12:33:52	1238	Periodický test ústředny	0x16 A2 A1 AA A	TelefonSmet : 1		Informační událost bez upozornění
05.2018 12:33:52	1238	Periodický test ústředny	0x16 A2 A1 AA A	TelefonSmet : 1		Informační událost bez upozornění
05.2018 12:31:23	1912	Periodický test ústředny	0x52 50 00 00 00	TCP : 1		Informační událost bez upozornění
05.2018 12:28:15	1212	Odemčení bloku 2 uživatelem 1	0x14 A1 A2 AA 1	TelefonSmet : 1		Odemčeno
05.2018 12:26:23	1237	Zamčení bloku 2 uživatelem 2	0x34 A1 A1 AA 2	INET : 1		Zamčeno
05.2018 12:25:55	1230	Periodický test ústředny	0x16 A2 A1 AA A	TelefonSmet : 1		Informační událost bez upozornění
05.2018 12:22:36	1202	SMS na číslo +420602842603 odeslána				GSM modem odeslal SMS na statický objekt
05.2018 12:22:30	1202	SMS na číslo +420602842603: Zamčeno1 Česká Olešná				Odesláni automatické SMS
05.2018 12:22:29	1202	Zamčení bloku 1 uživatelem 1	0x34 A1 A1 AA 1	TelefonSmet : 1		Zamčeno
05.2018 12:21:23	1912	Periodický test ústředny	0x52 50 00 00 00	TCP : 1		Informační událost bez upozornění
05.2018 12:19:46	1277	Obnova spojení INET		INET : 1		INET - obnova spojení
05.2018 12:17:15	1277	SW reset		INET : 1		SW reset
05.2018 12:16:16	1288	Periodický test ústředny	0x16 A2 A1 AA A	INET : 1		Informační událost bez upozornění
05.2018 12:15:54	1272	odemčeno kodem 2	0x36	Telefon : 2		Odemčeno
05.2018 12:11:23	1912	Periodický test ústředny	0x52 50 00 00 00	TCP : 1		Informační událost bez upozornění
05.2018 12:09:35	1237	Odemčení bloku 1 uživatelem 2	0x14 A1 A1 AA 2	INET : 1		Odemčeno
05.2018 12:03:51	1231	Periodický test ústředny	0x16 A2 AA AA A	INET : 1		Informační událost bez upozornění
05.2018 12:03:43	1278	Periodický test ústředny	0x16 A2 A1 AA A	Telefon SMET : 1		Informační událost bez upozornění
05.2018 12:03:30	1298	Periodický test ústředny	0x16 A2 AA AA A	INET : 1		Informační událost bez upozornění
05.2018 12:02:40	1285	Zamčení bloku 1 uživatelem 40	0x34 A1 A1 AA 4	INET : 1		Zamčeno
05.2018 12:01:48	1261	Zamčení bloku 1 uživatelem 3	0x34 A1 A1 AA 3	TelefonSmet : 1		Zamčeno
05.2018 12:01:22	1912	Periodický test ústředny	0x52 50 00 00 00	TCP : 1		Informační událost bez upozornění
05.2018 12:00:40	1271	Periodický test ústředny	0x16 A2 AA AA A	INET : 1		Informační událost bez upozornění
05.2018 12:00:14	1270	Periodický test ústředny	0x16 A2 AA AA A	TelefonSmet : 1		Informační událost bez upozornění

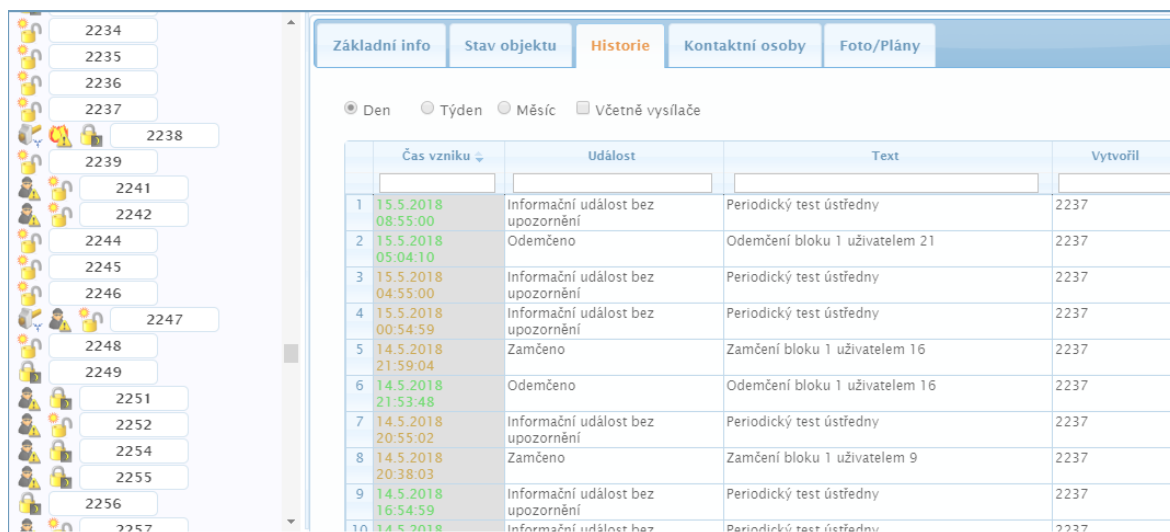
Obr. 6: Náhled prostředí RADOMNET klient [7]

V současnosti jsou na dohledovém centru použiti 3 klienti:

- operátor,
- supervizor,
- administrátor.

Servisní technici společnosti mají k dispozici připojení do PPC pomocí webového rozhraní, což jim velmi usnadní práci při připojování, opravách nebo revizích zabezpečovacích systémů u zákazníka. Supervizor a administrátor nastavují v klientské administraci systému práva přístupu uživatelů ke kartám a historii událostí střežených objektů.

Adresa pro webové rozhraní je: <http://dppc.spolecnost.biz:85000>



The screenshot shows a web interface for RADOMNET WEB. On the left is a sidebar with a list of icons and numbers (2234 to 2257). The main area has a navigation bar with tabs: 'Základní info', 'Stav objektu', 'Historie', 'Kontaktní osoby', and 'Foto/Plány'. Below the navigation bar are radio buttons for 'Den', 'Týden', 'Měsíc', and a checkbox for 'Včetně vysílače'. The main content is a table with the following data:

	Čas vzniku	Událost	Text	Vytvořil
1	15.5.2018 08:55:00	Informační událost bez upozornění	Periodický test ústředny	2237
2	15.5.2018 05:04:10	Odemčeno	Odemčení bloku 1 uživatelem 21	2237
3	15.5.2018 04:55:00	Informační událost bez upozornění	Periodický test ústředny	2237
4	15.5.2018 00:54:59	Informační událost bez upozornění	Periodický test ústředny	2237
5	14.5.2018 21:59:04	Zamčeno	Zamčení bloku 1 uživatelem 16	2237
6	14.5.2018 21:53:48	Odemčeno	Odemčení bloku 1 uživatelem 16	2237
7	14.5.2018 20:55:02	Informační událost bez upozornění	Periodický test ústředny	2237
8	14.5.2018 20:38:03	Zamčeno	Zamčení bloku 1 uživatelem 9	2237
9	14.5.2018 16:54:59	Informační událost bez upozornění	Periodický test ústředny	2237
10	14.5.2018	Informační událost bez upozornění	Periodický test ústředny	2237

Obr. 7: Výřez obrazovky webového rozhraní RADOMNET WEB [7]

Server a jeho redundance, na hardwaru DELL, jsou umístěny v rackové skříni v serverovně DPPC. Napájení pro vybraná zařízení DPPC je zálohováno centrálním online záložním zdrojem UPS. V případě dlouhodobých výpadků napájecí soustavy je dodávka energie řešena pomocí benzínového agregátu.

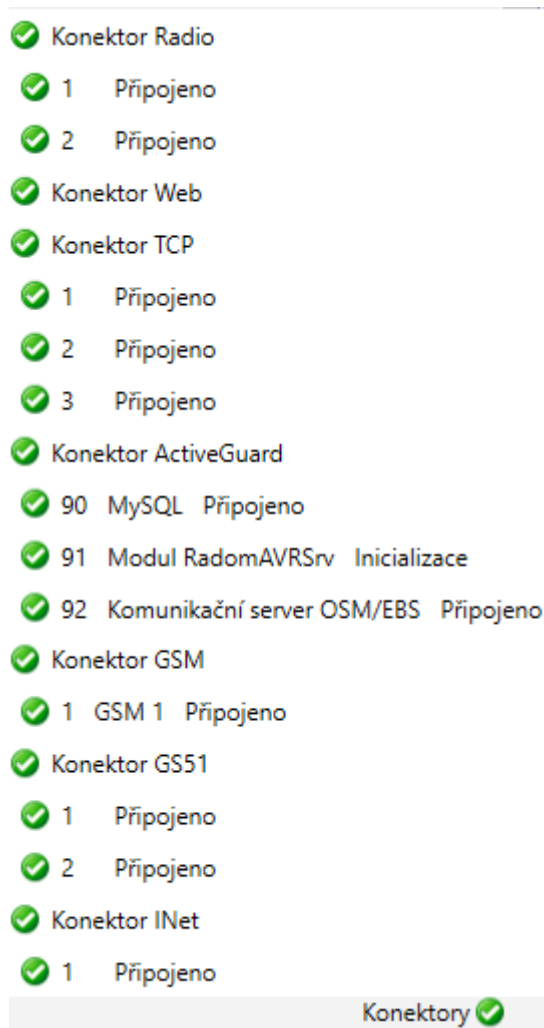
Software RADOMNET II jako celek využívá ke své činnosti databáze SQL, které jsou součástí instalace serverové aplikace.

Zprostředkovatelem komunikace mezi přijímačem událostí po přenosových trasách a řídicím softwarem systému RADOMNET je výrobcem nazýván softwarový konektor. Každá přijímaná přenosová trasa musí mít přiřazen svůj vlastní konektor, který je pak odpovědný za správné předávání událostí do vyhodnocovacího softwaru a zároveň udržuje a hlídá aktuální stav přenosové trasy, resp. stav hardwarového přijímače. Operátorům a správcům systému se pak při poruše odpovídající trasy konektor nahlásí poruchovým stavem.

### 3.1 Hardwarové vybavení přenosových tras

Kvalitní technické výrobky a jejich pravidelná údržba zajistí bezproblémový a bezporuchový provoz každého systému. Pro systémy dohledových center to platí dvojnásob, při výběru komponent PPC nesmíme také zapomenout na kompatibilitu systémů. Každý výrobce prezentuje svoje výrobky jako nejlepší, ale plně funkční je většinou pouze s omezeným počtem dalších výrobků. Na trhu je nepřehledné množství bezpečnostních systémů, ale některé

jsou schopny komunikovat s PPC pouze prostřednictvím svých přijímačů. Bezpečnostní agentury provozující DPPC ale musí připojovat většinu bezpečnostních systému, tak i ve společnosti XY dochází k pořizování a implementacím nových přijímacích zařízení. Starší zařízení nelze odpojovat, pokud jsou na přenosových trasách připojené střežené objekty.



Obr. 8: Konektory - připojené komunikační kanály v PPC [7]

### 3.1.1 Příjem zpráv po telefonní lince

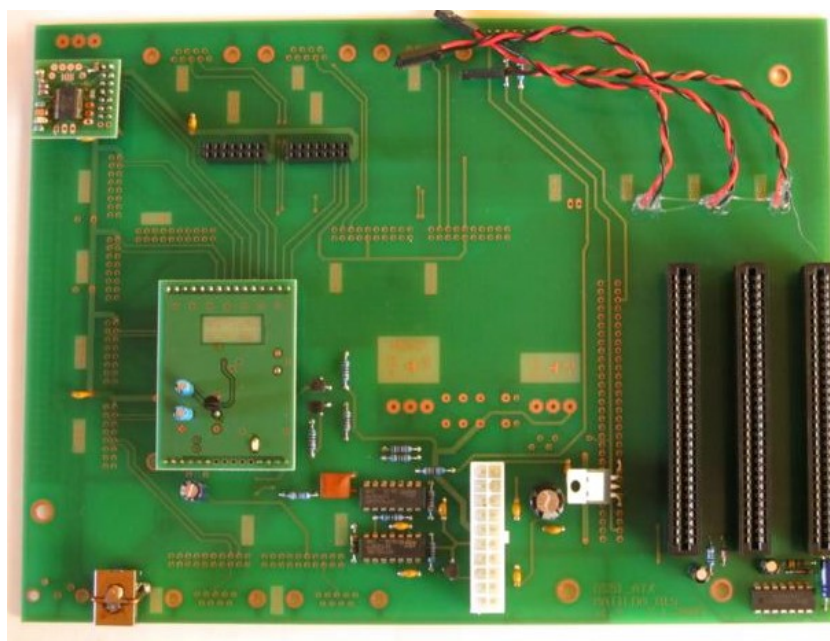
Firma na svém PPC využívá pro příjem událostí **telefonní kartu GS51** od společnosti Matilda. Dle parametrů prodejce RADOM [4] karta GS51 umožňuje současný příjem ze dvou nezávislých telefonních linek a zpracovává formát přenosu dat pulsní nebo tónový, v podobě DTMF. Karta je vybavena zvukovým modulem, který provádí patřičnou zvukovou

signalizaci vyvedenou přes nf zesilovač na reproduktor. Přes jednu telefonní kartu GS51 lze předávat do PPC zprávy až z 512 zabezpečovacích ústředen (objektů).



*Obr. 9 Telefonní karta GS51 [17]*

Konektivita se stanicí PPC je přes rozhraní ISA slotu. Toto rozhraní se však dnes ve stanicích počítačů nepoužívá, a proto je nutné karty umístit do specializovaných boxů, které mají vlastní napájení a jsou propojeny se serverem PPC přes USB port.



*Obr. 10: USB box pro GS51 [17]*

USB box má firma XY vybaven dvěma kartami GS51. Výbava umožňuje příjem z maximálně 4 telefonních linek. Zařízení je umístěno v serverovně dohledového centra v rackové skříni společně se serverem PPC. Zálohování napájení je řešeno centrální online UPS umístěnou v serverovně.

Privody telefonních linek jsou řešeny páteřně z rozvodné telefonní skříň ve sklepe, přímo na patchpanely do racku v serverovně PPC. Jsou zřízeny celkem 3 vyhrazená telefonní čísla pro přenosy událostí z objektových zařízení na PPC.

Nad všemi čísly je operátorem O2 zřízena sériová služba přepínání, tzn. že obsazené číslo je automaticky na ústřednách O2 přepojeno na linku čísla následujícího. V praxi tedy programujeme do ústředen PZTS pouze „hlavní“ telefonní číslo s pěti pokusy opakování přenosu. Záložní telefonní číslo není potřeba programovat, o tento krok se postará již zmíněná série telefonních čísel.

Obr. 11: Příklad nastavení telefonní komunikace [7]

Pro komunikaci je nutný telefonní komunikátor v ústředně PZTS a přípojka JTS.

Tab. 11: Telefonní čísla pro PPC a zapojení

Tel. číslo	Označení na patchpanelu	Vstup do PCO boxu
951 753 001 (primární)	T3.21	1/1
951 753 002	T3.22	1/2
951 753 003	T3.23	2/1
Jiné využití	Jiné využití	2/2

### 3.1.2 Příjem zpráv po rádiové síti

Rádiovou síť má bezpečnostní agentura vybudovanou na prvcích společnosti RADOM. Ve svém okolí provozuje dvě retranslační stanice **SRE40** a přijímá signály ze dvou přijímačů **SRX10/400**. Objektové vysílače používá s označením **STX23/400**.

Přidělené frekvenční pásmo má od ČTÚ na pozicích 4XX MHz a 4YY MHz vždy s fixací na 5 let. Administrátor PPC je povinen pravidelně aktualizovat seznam připojených zařízení a platit za správu licence poplatky.



Obr. 12: Rádiový přijímač SRX10/400, zdroj autor

**Přijímače SRX10/400** jsou umístěny v serverovně dohledového centra s označení R1 a R2. Antény jsou pak vytaženy a umístěny na stožár na střeše firemní budovy. Konektivitu do serveru zabezpečuje rozhraní RS232 (sériová linka) a převodníky Lantronix UDS-2100. Jedná se o dvouportové převodníky sériové linky na rozhraní ethernet. V serveru se pak zabezpečuje přenos pomocí virtuálního sériového portu do software PPC.

Nastavení převodníku je na IP adrese: **192.168.1.50** a komunikačním portu **10 001**. V software serveru PPC je nastavení virtuálních portů na:

- COM4 pro R1,
- COM5 pro R2.





Obr. 13: Převodník Lantronix UDS-2100, [18]

Napájení a zálohování technologických prvků je opět řešeno centrální UPS v serverovně.

**Retranslační stanice SRE40** jsou na pevných stanovištích na pozicích:

- RT1 – GPS:  $xx^{\circ}x'xx.xxx''N$ ,  $xx^{\circ}xx'xx.xxx''E$ ,
- RT2 – GPS:  $yy^{\circ}y'yy.yyy''N$ ,  $yy^{\circ}yy'y.yyy''E$ .

Zařízení jsou umístěna v buňkách a antény vyvedeny na stožáry vysílačů. Napájení je zálohováno vlastním akumulátorem přímo v retranslační stanici.

Všechny aktuální stavy retranslačních stanic jsou také přenášeny online na pracoviště DPPC, tak má operátor naprostý přehled, že daná komunikační trasa je nebo není v pořádku.





*Obr. 14: Retranslační stanice, vlastní zdroj*

Instalace, propojení ústředen a objektových **vysílačů STX23/400** se řídí pokyny výrobců. Přenosová zařízení (objektové vysílače) mají vlastní systém zálohování napájení pomocí vlastních akumulátorů instalovaných do boxu společně s vysílačem. Antény vysílačů se doporučuje umisťovat vně objektu.

Pro správnou komunikaci přes rádiovou síť je vyžadováno do ústředen programovat objektové číslo 9999. Číslo vysílače a rádiovou síť sdělí technikovi PZTS administrátor PPC. Použití vnitřních, resp. venkovních antén musí naopak instalační technik PZTS sdělit administrátorovi PPC pro správné nastavení objektové karty.

Obr. 15: Příklad nastavení rádiové komunikace [7]

Administrátor i operátor DPPC mají v softwaru k dispozici diagnostický nástroj pro sledování aktuálního stavu objektových vysílačů. Jen správně nastavené zařízení může vykazovat bezproblémový provoz. Proto je při instalacích vysílačů nutná spolupráce technika PZTS a administrátora PPC.

Popis	Medium (rá)	Hlavní	Čas příjmu	%	Přijato	Min	Act	Max
4214	Rádio	<input type="checkbox"/>	14.05.2018 12:48:48	38	6	59	76	82
1115	Rádio	<input checked="" type="checkbox"/>	14.05.2018 12:48:48	62	10	64	70	83
1544	Rádio	<input checked="" type="checkbox"/>	14.05.2018 12:48:13	31	5	41	91	99
1621	Rádio	<input checked="" type="checkbox"/>	14.05.2018 12:48:49	81	13	79	100	110
1610	Rádio	<input checked="" type="checkbox"/>	14.05.2018 12:48:24	44	7	56	88	97
1116	Rádio	<input checked="" type="checkbox"/>	14.05.2018 11:36:12	0	0	52	65	68
stodola	Rádio	<input checked="" type="checkbox"/>	14.05.2018 12:48:01	106	17	85	89	92
	Rádio1-naREL	<input checked="" type="checkbox"/>	14.05.2018 12:48:36	150	24	41	97	99
	Rádio2-přímo	<input checked="" type="checkbox"/>	14.05.2018 12:48:25			41	73	99
1308	Rádio	<input checked="" type="checkbox"/>	14.05.2018 12:47:48	69	11	54	88	93
1605	Rádio	<input checked="" type="checkbox"/>	14.05.2018 12:48:48	56	9	63	83	94
2269	Rádio	<input checked="" type="checkbox"/>	14.05.2018 12:48:00	50	8	41	79	88
3202	Rádio	<input checked="" type="checkbox"/>	14.05.2018 12:48:49	62	10	41	71	87
1407	Rádio	<input checked="" type="checkbox"/>	14.05.2018 12:48:24	62	10	41	78	89
1618	Rádio	<input checked="" type="checkbox"/>	14.05.2018 12:48:48	94	15	72	86	93

Obr. 16: Ukázka diagnostiky rádiové sítě z prostředí PPC [7]

### 3.1.3 Příjem zpráv po GSM – SMS

Je zřejmé, že při použití softwaru by měla být zabezpečena stoprocentní funkčnost s technologickými prvky stejného výrobce, v našem případě máme SW PPC od společnosti RADOM. Platí to i v případě přijímače pro přenosovou trasu po síti GSM, respektive po SMS kanálu. GSM přijímač **SRX10G**, který je také instalován v serverovně DPPC, dokáže

nejen přijímat a vyvolávat telefonní hovory, ale je schopen komunikovat na bázi datových SMS zpráv.



*Obr. 17: Přijímač SRX10G, vlastní zdroj*

Propojení se serverem PPC je realizováno pomocí sériového kanálu RS232 a sériového kabelu. PPC pak využívá toto zařízení na portu **COM1** přímo, bez dalších převodníků.

Telefonní číslo GSM přijímače a zároveň vysílače je: **606 606 606**

Vzhledem k umístění v serverovně je zálohování napájení opět pomocí centrální UPS.

Toto zařízení bylo primárně zřizováno za účelem příjmu SMS zpráv z objektů, viz. kapitola SMS přenos. Ovšem daleko větší využití dnes nachází při zasílání automatických SMS zpráv majitelům a obsluhám PZTS v jejich objektech. Zároveň je také komunikátor používán při odchozím volání přímo ze softwaru PPC. Tím je zabezpečeno, že veškerá komunikace se zákazníkem se zároveň zaznamenává do objektové historie.

Na objektech je možné použít dvojici vysílačů společnosti Radom:

- SXS24 - GSM – přenos pouze po SMS,
- SXS26/GPRS – umožňuje přenášet zprávy po:
  - GSM – SMS,
  - GPRS.

Jméno	Typ události	Smyčka/osoba	Text zprávy
2	Deaktivace poruchy akumulátoru ústředny		Akumulátor obnoven
1	Aktivace poruchy akumulátoru ústředny		Porucha akumulátoru
1	Aktivace poruchy napájení ústředny		Porucha napájení EZS
2	Aktivace poplachu		Poplach v objektu{0}
1	Zamčeno		Zamčeno{0}
2	Aktivace poruchy napájení ústředny		Porucha napájení EZS
2	Zamčeno		Zamčeno{0}
1	Deaktivace poruchy akumulátoru ústředny		Akumulátor obnoven
2	Deaktivace poruchy napájení ústředny		Napájení obnoveno
2	Odemčeno		Odemčeno{0}
2	Aktivace poruchy akumulátoru ústředny		Porucha akumulátoru
1	Aktivace poplachu		Poplach v objektu{0}
1	Deaktivace poruchy napájení ústředny		Napájení obnoveno
1	Odemčeno		Odemčeno{0}

Obr. 18: Ukázka nastavení automatických SMS zpráv [7]

### 3.1.4 Příjem zpráv po Internetu, 3G/GPRS

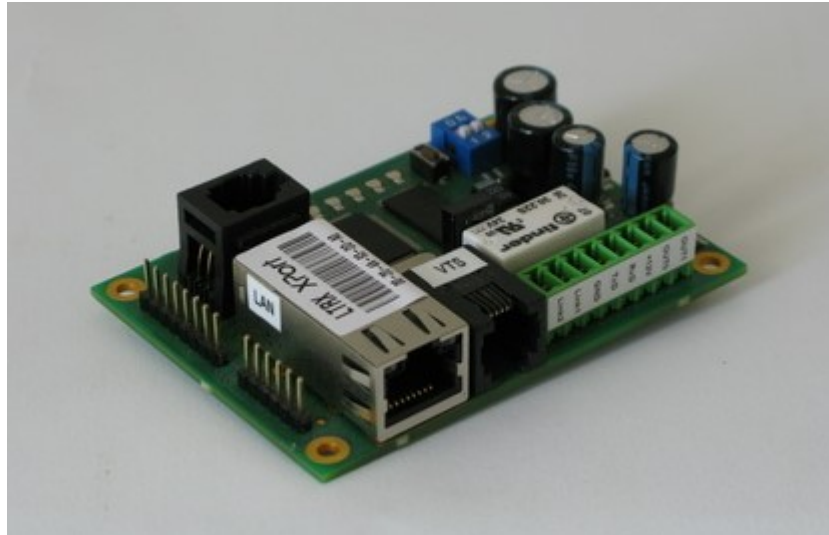
U datových přenosů je situace na trhu v začátcích, i když řada výrobců PPC a zabezpečovacích technik již společnou řeč našla. V první fázi vývoje a uvolnění komunikační techniky vedla výrobce snaha držet svoje řady a prodávat především své výrobky. Proto bylo nutné nasadit na datové trasy PPC řadu přijímačů od různých výrobců. Situace se ale postupně zlepšuje a již nyní je možné připojovat objekty pomocí internetových cest přímo přes konektivitu internetu.

#### 3.1.4.1 Komunikátory RADOM

Mezi prvními zástupci datové komunikace s PPC firmy XY byl dokončený vývoj komunikátoru od společnosti RADOM. **INET – telefonní internetový komunikátor** se připojuje na výstup telefonního komunikátoru zabezpečovací ústředny ve střeženém objektu. Ústředna se programuje obdobným způsobem jako u rádiového přenosu. Rozdílné je pouze programování cílové IP adresy a průchozího portu.

Dle specifikace výrobce [21] „je určen k přenosu zpráv ve formátu ADEMCO CONTACT ID získaných z telefonního výstupu elektronické zabezpečovací ústředny na vzdálený pult centralizované ochrany (PCO) RADOM SECURITY. S PCO probíhá komunikace

prostřednictvím UDP/IP paketů na rozhraní Ethernet“. Z uvedeného plyne i nastavení komunikačního formátu programování ústředny na CID.



Obr. 19: INET komunikátor [19]

Sofistikovanější a modernější je objektové přenosové zařízení SXS26/NET. Výrobek podporuje až tři přenosové trasy současně, primární a dvě záložní. Jmenovitě to jsou:

- Internet,
- GPRS,
- a SMS datové přenosy.



Obr. 20: Vysílač SXS26 [20]



Redundance přenosových tras s tímto zařízením však nelze chápat při požadavku vyšších tříd zabezpečení jako dvě plnohodnotné nezávislé přenosové trasy, protože v zařízení je použit pouze jeden napájecí zdroj.

Zálohování napájení vysílače INET i SXS26 je realizováno připojením na napájecí svorky zdroje ústředny, která je již zálohovaná akumulátorem. Musí být přihlédnuto na proudovou spotřebu  $80 \div 200$  mA, aby nedošlo ke snížení doby zálohovaného napájení při výpadku elektrické energie a tím nebyly porušeny zásady montáže zabezpečovacích systémů.

Veřejná IP adresa pro komunikaci s PPC je **10.10.10.10** a firewallem je nastaven průchozí **port** komunikace **UDP** na hodnotu **10 080**.

Testy spojení probíhají v zařízeních směrem k PPC téměř nepřetržitě a signalizaci ztráty spojení s objektem nastavujeme na 180 s.

Definované komunikační cesty objektu

Komunikace z objektu	Nahoru	Typ komunikace: INET	<input type="checkbox"/> Zakázaný příjem
INET (Hlavní)	Dolů	Název: INET	IP: 0.0.0.0
Komunikátor (Hlavní)		Formát zprávy: UDP šifrovaná	Port: 10080
GPRS	Nový	Konektor: Konektor INet	Číslo vysílače: 44
Typ ovládání		Index zařízení: 1	Typ vysílače: ...
nenastaveno		Signalizace ztráty spojení: Automaticky	00:02:30
		Prodleva ztráty spojení: INET krátký	00:00:20

Obr. 21: Příklad nastavení INET komunikace [7]

### 3.1.4.2 Komunikátory SATEL

Velmi rozšířeným výrobcem montovaných bezpečnostních systémů se v ČR poslední dobou stala firma SATEL z Polska. První výrobky se připojovaly pouze pomocí pevných linek. Brzy po zahájení expanze na český trh se firma zorientovala na českého zákazníka, začala dodavatelům naslouchat, a do svých zařízení implementovat komponenty dle jejich požadavků. Defacto současně s českým výrobcem RADOM vyvinula první komunikátory pro internetovou komunikaci. Její velkou výhodou však byla cena přenosového zařízení a tím pádem zákazníci upřednostňovali toto řešení.

Komunikátor nazvala **ETHM – universální komunikační modul**, který se připojuje na výstup telefonního komunikátoru ústředny PZTS. Přes tónový formát přenosu přijímá zprávy s protokoly: Ademco Slow, Silent Knight fast, Radionics 1400, Radionics 1400 s paritou, Ademco Express a Contact ID. Výčet protokolů definuje kompatibilitu se zabezpečovacími

ústřednami jiných výrobců. Výstup je přenášen pomocí připojení zákazníka do Internetu a směrován na bránu PPC.

Firma SATEL, jako jedna z mála, neustále sleduje potřeby zákazníků, své výrobky zdokonaluje a na trh uvádí další nové zařízení. První komunikátory byly zcela universální a kompatibilní s ostatními ústřednami, které měly telefonní komunikátor.

Další vývoj vlastních ústřednen donutil firmu rozdělit výrobu komunikátorů pro své ústředny a pro ústředny druhých stran.



Obr. 22: Komunikátor ETHM 1 Plus [21]

### **ETHM-2: Univerzální TCP/IP komunikační modul**

Je nástupcem první řady ETHM komunikátorů a výrobce slibuje kompatibilitu i s ústřednami bez telefonního komunikátoru. Dodavatel dále v technických parametrech uvádí [11]:

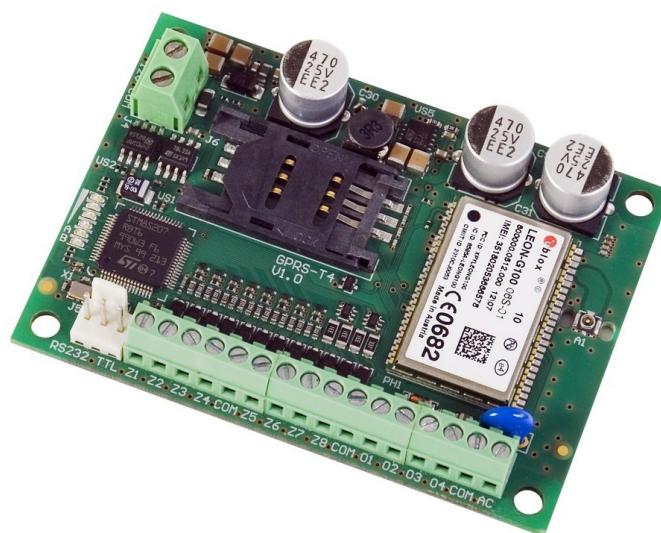
- simulace analogové telefonní linky,
- schopnost přijímat zprávy zaslané v telefonním přenosovém formátu a zasílat je na monitorovací stanici přes síť ethernet, prostřednictvím TCP/IP protokolu,
- 5 zón pro spuštění TCP/IP hlášení,
- zasílání e-mailů na osobní účty,
- vzdálená správa přes webové rozhraní,
- vzdálené ovládání přes webové rozhraní,
- potvrzení přijetí zprávy o vzniku události,

- paměť pro příjem 512 zpráv událostí,
- kódovaný přenos zpráv událostí,
- dálkový dohled stavu výstupů,
- napájecí výstup,
- monitoring stavu vstupů, výstupů, napájení, komunikace atd. prostřednictvím kódů zaslaných přes ethernetovou síť na dvě monitorovací stanice nebo e-mailem,
- konfigurace pomocí portu RS-232 programem ETHM-2 Soft, nebo webovým prohlížečem,
- kontrola připojení ethernetového kabelu,
- vestavěný spínaný napájecí zdroj 1,2A,
- obvod pro dobíjení a kontrolu záložního akumulátoru.

### ETHM-1 Plus: TCP/IP komunikační modul

Komunikátor je kompatibilní pouze s výrobky od SATELU, komunikace mezi ústřednou a přenosovým zařízením probíhá po vnitřní sběrnici systému PZTS a přes Internet (TCP i UDP) zasílá události na bránu PPC. Přenos je šifrován 192 bitovým AES symetrickým klíčem, který generuje přijímač na straně PPC při prvotní komunikaci.

Na rozdíl od univerzálních komunikátorů ETHM 1 Plus umožňuje uživatelům a servisním technikům přístup do ovládání a programování ústředny vzdáleně. SATEL vyvinul vlastní aplikace pro mobilní chytré telefony a uvolnil je pro běžné používání uživatelům.



Obr. 23: Modul GPRS T4 [22]



Řada digitálních modulů **GPRS-T 1 až 6 - CLIP/GPRS/SMS komunikátor** je posledním zástupcem od firmy SATEL, které jsou prezentovány v této práci. Oproti předchozím modulům, komunikátory GPRS komunikují s PPC prostřednictvím mobilních sítí operátorů. Jak název napovídá může být využito SMS i GPRS kanálu, a to jak v primárním přenosu, tak i záložním. V principu číslování modulů se jedná o vybavení a volbu funkcí zvoleného modulu.

Aby bylo možné přenášet zprávy od všech jmenovaných přenosových zařízení společnosti SATEL přenést do PPC po síti Internet, musel výrobce vymyslet cestu, jak události převést do formátu, které umělo PPC číst. V té době nebyl ještě implementován komunikační protokol TCP/UDP ve většině zařízení PPC.

Polští vývojáři našli zcela jednoduché řešení a vyvinuli vlastní zařízení, které přijímá datové zprávy po TCP/UDP a předává je v tónovém formátu po telefonní lince přijímači PPC. Pro provozovatele dohledových center to znamená obsazenou pozici telefonní karty, ale agentury zároveň dokázaly uspokojit zákazníka datovým přenosem.



Obr. 24: SMET-256 [23]

**SMET – 256 TCP/IP převodník protokolu Satel**

Dodavatel uvádí parametry [13]:

- konvertuje TCP/IP na formát přenosu po telefonní lince,
- kompatibilní se SATEL Ethernet a GPRS vysílači,
- simulace pro visonic RC4000 a SurGuard MLR2 přijímače,
- podpora až 256 uživatelů s individuálním dohledem spojení,
- podpora neomezeného množství uživatelů bez kontroly spojení,
- buffer událostí, dokud přijímač úspěšně nepřijme všechna hlášení,
- ethernetový dohled spojení,
- volitelné filtrování vybraných fyzických adres (MAC),
- konfigurace pomocí webového prohlížeče (TCP/IP připojení) nebo software (RS-232 připojení),
- podpora pro získání automatické IP adresy v DHCP síti.

V nastavení SMETka je použito následujících parametrů:

*Tab. 12: Nastavení SMET*

<b>Popis</b>	<b>Hodnota</b>
<b>IP adresa</b>	192.168.1.53
<b>Veřejná IP adresa</b>	10.10.10.10
<b>Port TCP</b>	10153
<b>ID</b>	SMET
<b>PASS</b>	256

Využití tohoto připojení na PPC firmy XY je v současnosti v maximální kapacitě. Není již možné další objekty tímto způsobem připojovat, pokud nedojde k odpojení jiného objektu.

### **3.1.4.3 Zařízení s přímým přístupem TCP, UDP**

Poslední, v této chvíli také nejčastěji používaná, přenosová trasa implementovaná do PPC je digitální cesta s přenosem po Internetu. Pro navázání spojení využívá oba protokoly, jak

TCP, tak UDP. Volba protokolu zůstává na technikovi PZTS a správci PPC. Kryptování přenášených dat je závislé na použitých komponentech systému a na nastavení komunikačních cest při instalaci systému.

Příchozí spojení zabezpečovacích systémů je filtrováno přes firewall PPC. Na serveru dohledového centra jsou instalovány tři softwarové konektory TCP a jeden UDP pro přímou komunikaci se zabezpečeným objektem po Internetu. V této komunikační trase není využito žádného hardwarového zprostředkovatele komunikace. Komunikátory PZTS předávají události „přímo“ na síťové rozhraní serveru PPC.

The screenshot shows a web-based configuration interface for defining communication paths for an object. The main section is titled "Definované komunikační cesty objektu". On the left, there is a list of communication paths, with "TCP (Hlavní)" selected. Below this list are buttons for "Nahoru" and "Dolu", and a "Nový" button. There are also dropdown menus for "GPRS" and "Typ ovládání" (set to "nenastaveno"). The main configuration area contains the following fields:

- Typ komunikace: TCP (with a checkbox for "Zakázaný příjem")
- Název: TCP
- Formát zpráv: SIA
- Konektor: Konektor TCP
- Index zařízení: 1
- Signalizace ztráty spojení: APS (with a time field of 00:03:00)
- Prodleva ztráty spojení: GPRS krátký (with a time field of 00:00:20)
- IP: 0.0.0.0
- Port: 0
- Perioda dotazů[s]: 10
- Heslo: (empty)
- Heslo2: (empty)
- Krypt. klíč: (filled with dots, with a checkmark in the adjacent box)
- Id ústředny: 0

Obr. 25: Příklad nastavení TCP komunikace [7]

TCP, UDP komunikace, jako jediná v DPPC firmy XY, využívá k překladu událostí tabulku SIA IP. Některé typy ústředí PZTS jsou tak schopny přenášet události, včetně programovaných popisů zón, bloků nebo uživatelů přímo z ústředny. V těchto případech není nutné již vypisovat názvy do karty objektu administrátorem PPC a operátorovi pak přichází události včetně aktuálního pojmenování. Alternativně lze použít tabulky CID, ovšem není možné využívat funkce automatických textů.

V současnosti je doporučeno primárně využívat TCP komunikaci. Testy spojení komunikátoru PZTS s PPC v maximální hodnotě tři krát 120 s. Ústředny a průchodnost celé přenosové soustavy testujeme maximálně po 4 hodinových cyklech.

Na straně zabezpečovacích systémů již většina výrobců dodává ethernetový port přímo na desce ústředny, nebo se IP komunikátor připojuje na vnitřní sběrnici systémů PZTS. DPPC firmy XY je připravena napřímo přijímat a vyhodnocovat události ze systémů výrobců:

- Satel,
- DSC,
- Galaxy,

- Paradox,
- nebo Siemens.

Podpora pro komunikaci dalších výrobců systémů PZTS bude implementována do softwarového vybavení PPC v dohledné době.

*Tab. 13 Nastavení TCP/UDP komunikace*

Popis	Hodnota
IP adresa	192.168.1.100
Veřejná IP adresa	10.10.10.10
Port TCP 1	10155
Port TCP 2	10156
Port TCP 3	10157
Port UDP	10158

## 3.2 Překladové tabulky v PPC

Základem správné interpretace přenášených událostí z PZTS na monitory operátorů DPPC jsou tzv. překladové tabulky. V systému Radomnet je zadávání a tvorba tabulek v plné kompetenci administrátora PPC, ten si musí uvědomit, vyhodnotit a správně přiřadit odpovídající tabulku připojovaným bezpečnostním systémům PZTS. Musí zkontrolovat překladové tabulky všech připojovaných ústředěn a správně je zanést do systému PPC. V příloze PI je pak uveden příklad a porovnání tabulek CID a SIA implementovaných do ústředěn řady NEO, výrobce DSC.

### 3.2.1 Tabulka Tel42

Překladová tabulka formátu 4/2 je zástupcem nejstarších používaných tabulek. Její tvorba spočívá v definici dvojice číslic v HEX soustavě. V Radomnet II je definován jako **Kód** (HEX) při **8 bitech** a přiřazené odpovídající **události**. Text události, popř. význam konkrétní smyčky (zóny) lze vytvořit dle požadavků zákazníků, operátorů nebo instalačních techniků PZTS. Příklad jedné z tabulek pro 4/2 je uveden na *Obr. 26*.

Kód [HEX]	Počet bitů kódu	Událost	Text události	Konkrétní smyčka	Událost vysílače
11	8	Aktivace sabotáže ústředny	poplach ochranné kontakty		<input type="checkbox"/>
12	8	Odemčeno	odemčeno kod 26-30		<input type="checkbox"/>
13	8	Zamčeno	zamčeno kod 31-40		<input type="checkbox"/>
14	8	Aktivace poplachu	poplach zona 1	1	<input type="checkbox"/>
15	8	Aktivace poplachu	poplach zona 5	5	<input type="checkbox"/>
16	8	Aktivace poplachu	poplach zona 10	10	<input type="checkbox"/>
17	8	Aktivace poplachu	poplach zona 16	16	<input type="checkbox"/>
18	8	Aktivace poplachu	zamčeno pod nátlakem	21	<input type="checkbox"/>
19	8	Odemčeno	odemčeno kodem 8	8	<input type="checkbox"/>
1A	8	Aktivace poplachu	poplach zona 57	57	<input type="checkbox"/>
1B	8	Aktivace poplachu	poplach zona 58	58	<input type="checkbox"/>
1C	8	Aktivace poplachu	poplach zona 59	59	<input type="checkbox"/>
1D	8	Aktivace poplachu	poplach zona 60	60	<input type="checkbox"/>
1E	8	Aktivace poplachu	poplach zona 56	56	<input type="checkbox"/>
1F	8	Odemčeno	odemčeno kod 31-40		<input type="checkbox"/>
21	8	Informační událost s upozorněním	porucha sirény		<input type="checkbox"/>
22	8	Zamčeno	zamčeno kod 41-50		<input type="checkbox"/>
23	8	Aktivace poplachu	poplach zona 2	2	<input type="checkbox"/>
24	8	Aktivace poplachu	poplach zona 6	6	<input type="checkbox"/>
25	8	Aktivace poplachu	poplach zona 11	11	<input type="checkbox"/>
27	8	Odemčeno	odemčeno kodem 1	1	<input type="checkbox"/>
28	8	Odemčeno	odemčeno kodem 9	9	<input type="checkbox"/>
29	8	Odemčeno	odemčeno po poplachu		<input type="checkbox"/>
2A	8	Aktivace poplachu	poplach zona 66	66	<input type="checkbox"/>
2B	8	Aktivace poplachu	poplach zona 67	67	<input type="checkbox"/>
2C	8	Aktivace poplachu	poplach zona 68	68	<input type="checkbox"/>
2D	8	Aktivace poplachu	poplach zona 69	69	<input type="checkbox"/>
2E	8	Aktivace poplachu	poplach zona 70	70	<input type="checkbox"/>
2F	8	Aktivace poplachu	poplach zona 71	71	<input type="checkbox"/>
31	8	Aktivace poplachu	tíseň	21	<input type="checkbox"/>
32	8	Aktivace poplachu	poplach zona 3	3	<input type="checkbox"/>
--	--	--	--	--	--

Obr. 26: Ukázka překladové tabulky Tel42 v DPPC [7]

### 3.2.2 Tabulka CID

V tabulkách CID je definován jako **Kód** (HEX) řetězec **Q XYZ** ze struktury formátu CID z *Tab. 9*. Odpovídajícímu kódu je přiřazena adekvátní událost z předdefinovaných událostí systému Radomnet II. Text události je, stejně jako u 4/2, definicí uživatelů, kde již můžeme pro jednotlivé události definovat masku překladu.

Při zadávání masky však musíme dbát na sestupnou posloupnost a masku definovat od největší proměnné, např. {2}, {1}, {0}. V následujícím kroku vybereme, zda se má překládat jméno smyčky (zóny), bloku nebo uživatele.

Proměnné textu události		Formát: Dec				
Index proměnné: 2	Vkládaná proměnná: Pouze hodnotu	Maska: Prvek	Posun: 0	Násobek: 1		
Index proměnné: 1	Vkládaná proměnná: Pouze hodnotu	Maska: Skupina	Posun: 0	Násobek: 0		
Index proměnné: 0	Vkládaná proměnná: Popis smyčky	Maska: Výsledek	Posun: 0	Násobek: 1		

Obr. 27: Definice masky tabulky CID [7]

Kód [HEX]	Událost	Text události	Konkrétní smyčka	Událost vysílače
1100	Aktivace poplachu	Poplach - žádost lékaře	21	<input type="checkbox"/>
1110	Aktivace požáru	Poplach požár zóny {0}	maska	<input type="checkbox"/>
1114	Aktivace požáru	Teplotní detektor {0} v bloku {1} [*{2}*]	maska	<input type="checkbox"/>
Proměnné textu událostí Formát: [Dec]				
Index proměnné: 2	Vkládaná proměnná:	Popis smyčky	Maska: Prvek	Posun: 0 Násobek: 1
Index proměnné: 0	Vkládaná proměnná:	Popis smyčky	Maska: Prvek	Posun: 0 Násobek: 1
Index proměnné: 1	Vkládaná proměnná:	Popis smyčky	Maska: Prvek	Posun: 0 Násobek: 1
1115	Aktivace požáru	Poplach požár tlačítka	20	<input type="checkbox"/>
1118	Aktivace požáru	tlačítka POŽÁR	23	<input type="checkbox"/>
1120	Aktivace poplachu	Tišňový poplach PANIKA (klávesnice)	22	<input type="checkbox"/>
1121	Aktivace poplachu	Tišňový poplach PŘEPADENÍ (tíseň uživatele {0})	maska	<input type="checkbox"/>
1122	Aktivace poplachu	Tišňový poplach PŘEPADENÍ tlačítka {0}	maska	<input type="checkbox"/>
1130	Aktivace poplachu	Poplach zóny {0} v bloku {1} [*{2}*]	maska	<input type="checkbox"/>
1131	Aktivace poplachu	Poplach perimetr zóny {0} v bloku {1} [*{2}*]	maska	<input type="checkbox"/>
1132	Aktivace poplachu	Poplach vnitřní zóny {0} v bloku {1} [*{2}*]	maska	<input type="checkbox"/>
1133	Aktivace poplachu	Poplach 24 hod zóny {0} v bloku {1} [*{2}*]	maska	<input type="checkbox"/>
1134	Aktivace poplachu	Poplach příchod/odchod zóny {0} bloku {1} [*{2}*]	maska	<input type="checkbox"/>
1135	Aktivace poplachu	Poplach den/noc zóny {0} v bloku {1} [*{2}*]	maska	<input type="checkbox"/>
1136	Aktivace poplachu	Poplach venkovní zóny {0} v bloku {1} [*{2}*]	maska	<input type="checkbox"/>
1137	Aktivace sabotáže ústředny	Poplach sabotážní zóny {0}	maska	<input type="checkbox"/>
1138	Aktivace poplachu	Nepotvrzený poplach zóny {0} v bloku {1} [*{2}*]	maska	<input type="checkbox"/>
1139	Aktivace poplachu	Potvrzený poplach - křížový alarm		<input type="checkbox"/>
1140	Aktivace poplachu	Celkový poplach zóny {0}	maska	<input type="checkbox"/>
1143	Aktivace sabotáže ústředny	Sabotáž/porucha modulu {0} v bloku {1} [*{2}*]	maska	<input type="checkbox"/>
1144	Aktivace sabotáže ústředny	Sabotáž zóny {0} v bloku {1} [*{2}*]	maska	<input type="checkbox"/>
1145	Aktivace sabotáže ústředny	Sabotáž rozšíř. modulu {0} v bloku {1} [*{2}*]	maska	<input type="checkbox"/>
1151	Aktivace poplachu	Únik plynu zóny {0} v bloku {1} [*{2}*]	maska	<input type="checkbox"/>
1154	Aktivace poplachu	Únik vody zóny {0} v bloku {1} [*{2}*]	maska	<input type="checkbox"/>
1200	Aktivace požáru	Požární únikový východ		<input type="checkbox"/>

Obr. 28: Ukázka překladové tabulky CID v DPPC [7]

### 3.2.3 Tabulka SIA IP

V této chvíli asi nejpoužívanější tabulkou nově instalovaných zařízení je SIA IP. Univerzální tabulka vychází z normy ANSI/SIA DC-09-2013 a je modifikována a kontrolována ústřednami řady DSC NEO a SATEL Integra. Samotná tabulka pak vychází ze 40 bitového **Kódu** (HEX) definovaného dle formátu v *Tab. 10* a sekci <data>.

Prvních 16 bitů definuje kód události ze seznamu předdefinovaných událostí systému Radomnet II. Následujících 8 bitů může značit číslo oblasti (bloku) nebo část systému PZTS a posledních 16 bitů pak znamená konkrétní smyčku, modul nebo osobu uživatele PZTS.

V instalačních manuálech ústředny (nebo i v přijímačích internetové komunikace) jsou události ve formátu SIA uváděny dle předpisu **N riB YZ ZZZZ**, kde:

- N – nová událost,
- riB – číslo bloku/oblasti
- YZ – kód události v ASCII (pro potřeby Radomnetu je nutné převést do HEX),
- ZZZZ – číslo zóny/smyčky/osoby.

Příklad převodu YZ a porovnání s CID je pak pochopitelné v příloze PI.

Masku je nutné definovat stejně jako u tabulky CID v sestupném indexu.

Kód [HEX]	Počet bitů kódu	Událost	Text události	Konkrétní smyčka	Subsystém	Událost vysílá
4152	16	Deaktivace poruchy napájení ústředny	Obnova AC napájení porucha - na ústředně			<input type="checkbox"/>
4154	16	Aktivace poruchy napájení ústředny	AC napájení porucha - na ústředně			<input type="checkbox"/>
4241	16	Aktivace poplachu	Poplach v bloku {2/2} zóna {1/1} {{0}}	maska		<input checked="" type="checkbox"/>

Proměnné textu události		Formát: Hex
Index proměnné: 0	Vkládaná proměnná: Popis smyčky	Posun: 0 Násobek: 1
Index proměnné: 1	Vkládaná proměnná: Pouze hodnotu	První bit masky: 25 Počet bitů masky: 16 Posun: 0 Násobek: 1
Index proměnné: 2	Vkládaná proměnná: Pouze hodnotu	První bit masky: 17 Počet bitů masky: 8 Posun: 0 Násobek: 0

4247	16	Informační událost bez upozornění	Alarm v bloku {0} nepotvrzen	maska		<input type="checkbox"/>
4248	16	Deaktivace poplachu	Obnova zóny {1} {{0}}	maska		<input type="checkbox"/>
424D	16	Informační událost bez upozornění	Poplach v bloku {0} potvrzen	maska		<input type="checkbox"/>
4256	16	Informační událost s upozorněním	Poplach v bloku {0} potvrzen	maska		<input type="checkbox"/>
4341	16	Zamčeno	Automatické zapnutí bloku {0/0}	maska		<input type="checkbox"/>
4347	16	Zamčeno	Částečné zamčení bloku {0}	maska		<input type="checkbox"/>
434C	16	Zamčeno	Zamčení bloku {2/2} uživatelem {0/0} {{1}}	maska		<input type="checkbox"/>
4352	16	Informační událost s upozorněním	Poplach při odchodu uživatel {1/1} {{0}}	maska		<input type="checkbox"/>
4541	16	Informační událost s upozorněním	Chyba při odchodu uživatele {1/1} {{0}}	maska		<input type="checkbox"/>
4545	16	Informační událost bez upozornění	Chyba při odchodu uživatele			<input type="checkbox"/>
454A	16	Deaktivace sabotáže ústředny	Obnova temperu modulu {0}	maska		<input type="checkbox"/>
4552	16	Informační událost bez upozornění	Obnova Porucha komunikace s modulem {0}	maska		<input type="checkbox"/>
4553	16	Aktivace sabotáže ústředny	Tamper modulu {0}	maska		<input type="checkbox"/>
4554	16	Informační událost s upozorněním	Porucha komunikace s modulem {0}	maska		<input type="checkbox"/>
4641	16	Aktivace požáru	POŽÁRNÍ poplach zóny {1} {{0}}	maska		<input type="checkbox"/>
4648	16	Deaktivace požáru	Obnova POŽÁRU			<input type="checkbox"/>
4652	16	Deaktivace požáru	Obnova požáru			<input type="checkbox"/>
4653	16	Aktivace požáru	POŽÁR s kontrolou hlásiče {1} {{0}}	maska		<input type="checkbox"/>
4656	16	Deaktivace požáru	obnova požáru hlásiče {1} {{0}}	maska		<input type="checkbox"/>
4841	16	Aktivace poplachu	PŘEPADENÍ {1} {{0}}	maska		<input type="checkbox"/>
4848	16	Deaktivace poplachu	Obnova přepadní {1} {{0}}	maska		<input type="checkbox"/>

Obr. 29: Ukázka překladové tabulky SIA v DPPC [7]

## ZÁVĚR

Bakalářská práce si klade za úkol jednoduše objasnit problém komunikačních cest v připojování objektových zařízení PZTS na dohledová centra bezpečnostních agentur. Práce je koncipovaná na nejčastější dotazy instalačních techniků, případně obchodních zástupců montážních firem nabízejících instalace systémů PZTS v oblasti připojení na DPPC. Administrátorům PPC práce stanovuje a určuje možnosti připojení objektů a usnadňuje orientaci v již provozovaných trasách, včetně jejich technické i kancelářsko-administrativní činnosti.

Součástí úvodní části jsou vyjmenovány aktuálně (k V.2018) platné normy týkající se instalace systémů PZTS, včetně požadavků na přenosové zařízení, resp. trasy. Vyjmenované a popsání jsou všechny přenosové kanály, které jsou v současné době na trhu k dispozici (respektive, všechny trasy, kterými disponuje dohledové centrum společnosti XY).

Telefonní linka se již při připojování nových objektů téměř nepoužívá (dovolím si tvrdit, že se nepoužívá vůbec), avšak stále zůstávají na DPPC připojeny „starší“ objekty, tím pádem je nutné i toto připojení zmínit, popsat a udržovat.

Rádiové sítě jsou definovány jako „nejbezpečnější“, ale bohužel pro jejich nepříznivou cenovou dostupnost koncovým uživatelům se připojují pouze objekty ve vyšším stupni zabezpečení. Udržování těchto přenosových cest je proto velice důležité a provozovatelům DPPC umožňuje připojovat velice zajímavé objekty.

Nejmodernější trendy přenosu nám nabízejí digitální formáty a digitální přenosové trasy, ať už na bázi internetu nebo mobilních datových sítí. V každém případě je nespornou výhodou obousměrná komunikace, množství přenášených dat a v neposlední řadě rychlost komunikace. Výrobci systémů bezpečnostních technologií jsou dnes již plně orientováni na tento typ komunikace, a právě pro jeho snadnou dostupnost a cenovou výhodnost jsou tyto přenosové kanály preferovány.

Nesmím zapomenout zmínit i přenos událostí pomocí SMS zpráv. Relativně jednoduché a levné řešení s sebou však přináší velké riziko zpoždění při přenosu události a tím i velké riziko při napadení objektu. Pachatel má daleko více času na páchaní trestné činnosti a tím samozřejmě může způsobit daleko větší škody. Tento přenosový kanál si dovolím nazvat jako absolutně nevhodný pro přenos poplachových událostí ze systémů PZTS.

Každá přenosová trasa má svoji specifickou schopnost přenést určité množství informací za určitý čas. Formáty přenosu jsou tak uzpůsobeny, aby přenesly co nejvíce dat za co nejkratší



možnou dobu. Překladové tabulky jsou právě prostředkem formátování a kódování přenášených událostí.

Během tvorby bakalářské práce jsem společně s dodavatelem systému Radomnet II implementoval do PPC přímou komunikační trasu po Internetu. Předpokladem správné funkčnosti byla plná tvorba překladové tabulky SIA IP. Plná integrace digitální cesty byla doprovázena ověřováním funkčnosti na ústřednách DSC NEO a SATEL Integra, které jsem testoval, programoval přímo na komunikačních trasách do PPC. Ověřena byla přímo každá odeslaná událost ze systému PZTS, až do uživatelského okna operátora. Mohu tvrdit, že při implementaci jsem 100 % ověřil pravost přenášených událostí.

Následně po uvolnění datové přenosové trasy došlo na DDPC firmy XY k připojení/přepojení cca 250 hlídaných objektů pomocí datových linek. Výrazně ubylo pláných výjezdů k objektům, které z nějakých důvodů vykazovaly ztráty spojení po svých předešlých trasách.

Velkou částí obměny tvořilo přepojení objektů komunikujících po pevných telefonních linkách. V následujících dnech dojde ke zrušení jedné telefonní linky pro její nadbytečnost a tím samozřejmě k finanční úspoře firmy XY. V dalších krocích inovace PPC by mělo následovat přepojování objektů přes komunikační zařízení SMET, které komunikuje prostřednictvím telefonní karty a tím dochází k prodloužení přenosu událostí, ale také k deformacím zpráv a častým neshodám s komunikačním formátem. Zařízení SMET poté bude od PPC odpojeno.

V praktické části jsou zmonitorovány a zdokumentovány veškeré komunikační kanály, včetně nastavení komunikačních cest.

Přínos bakalářské práce vidím především ve vylepšení, zrychlení a zvýšení spolehlivosti přenosu na DPPC firmy XY, včetně finančních úspor. Zároveň pro instalační techniky PZTS a správce PPC jsou v práci definovány a zdokumentovány použité komponenty a nastavení pro jednotlivé přenosové trasy i formáty.

**SEZNAM POUŽITÉ LITERATURY**

- [1] IVANKA, Ján. *Systemizace bezpečnostního průmyslu I*. Vyd. 5. Zlín: Univerzita Tomáše Bati ve Zlíně, 2014. ISBN 978-80-7454-410-1.
- [2] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I*. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. ISBN 978-80-7318-889-4.
- [3] DRGA, Rudolf a LAUCKÝ, Vladimír. *Speciální technologie komerční bezpečnosti*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. ISBN 978-80-7454-146-9.
- [4] TNI 33 4592, *Poplachové systémy a EPS - Požadavky na přenos zpráv ze střežených objektů pomocí internet protokolu*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.
- [5] AGA - ASOCIACE GREMIUM ALARM. *Ademco Contact ID protokol SIA DC - 05 -1999.09*. Praha, 2007.
- [6] ANSI/SIA DC-09-2013. *SIA Digital Communication Standard – Internet Protocol Event Reporting*, Silver Spring: The Security Industry Association, 2013.
- [7] Radom, s.r.o.. *Systém RADOMNET II pro RADOM SECURITY a RADOM SECURITY FIRE: uživatelský manuál. 4*. Pardubice: Radom, s.r.o, 2016.
- [8] Tyco Security Products. *Zabezpečovací ústředna série Power Neo – instalační manuál v 1.3*. Hradec Králové: KELCOM International, spol. s r.o., 2017.
- [9] Tyco Security Products. *Sur-Gard System II – instalační manuál v 2.0*. Hradec Králové: KELCOM International, spol. s r.o., 2016.
- [10] SIA DC-05-1999.09. *Digital Communication Standard -Ademco ® Contact ID Protocol -for Alarm Systém Communications*, Alexandria, VA: The Security Industry Association, 1999.
- [11] KELCOM. *PZTS*. [online]. 2010 [cit. 2017-26-04]. Dostupné z www: <http://www.kelcom.cz/elektronicke-zabezpecovaci-systemy/zabezpecovaci-ustredny/dsc-power-neo/>
- [12] ČSN EN 50131-1 ed. 2/A1/A2/Z2. *Poplachové systémy – Poplachové zabezpečovací a tísňové systémy. Část 1: Systémové požadavky*. Praha: Český normalizační institut, 2007.
- [13] JABLOTRON. *Bezpečnostní centrum* [online], 2018, [cit. 2018-05-13]. Dostupné z: <http://www.bezpecnostnicentrum.cz/cs/virtualni-prohlidka>

- [14] *TCP/UDP Overview* [online], 2018, [cit. 2018-05-13]. Dostupné z: <https://milestone-of-se.nesuke.com/en/nw-basic/tcp-udp/tcp-udp-summary/>
- [15] RADOM. *Telefonní karta GS51* [online], 2018, [cit. 2018-05-13]. Dostupné z: <http://www.radom.eu/produkty-a-sluzby/ochrana-majetku/pulty-centralizovane-ochrany-pco-/dispecerske-monitorovaci-pracoviste/zarizeni-pro-prijem-informaci-z-hlidanych-objektu/telefonni-karta-gs51.htm>
- [16] HRUŠKA, Ivan. *Dohledové a poplachové přijímací centrum a jeho specifika v sektoru soukromé bezpečnosti*. Univerzita Tomáše Bati ve Zlíně. Diplomová práce. 2014
- [17] MATILDA elektronika *Matilda PCO box*. [online], 2010, [cit. 2018-05-13]. Dostupné z: [http://www.matilda.unas.cz/\\_firma/pcobox.html](http://www.matilda.unas.cz/_firma/pcobox.html)
- [18] LANTRONIX. *UDS2100 External Device Server*. [online], 2018, [cit. 2018-05-13]. Dostupné z: <https://www.lantronix.com/products/uds2100/>
- [19] RADOM. *INET – telefonní internetový komunikátor*. [online], 2018, [cit. 2018-05-13]. Dostupné z: <http://www.radom.eu/produkty-a-sluzby/ochrana-majetku/pulty-centralizovane-ochrany-pco-/objektova-zarizeni/iv-prenos-informaci-po-datovych-sitich-lanwamn/telefonni-internetovy-komunikator-inet.htm>
- [20] RADOM. *SXS26/NET – objektové přenosové zařízení*. [online], 2018, [cit. 2018-05-13]. Dostupné z: <http://www.radom.eu/produkty-a-sluzby/ochrana-majetku/pulty-centralizovane-ochrany-pco-/objektova-zarizeni/iv-prenos-informaci-po-datovych-sitich-lanwamn/sxs26net---objektove-prenosove-zarizeni.htm>
- [21] EUROALARM. *ETHM 1 Plus* [online], 2015, [cit. 2018-05-13]. Dostupné z: <https://www.euroalarm.cz/eshop-zabezpecovaci-technika/zabezpeceni/komunikace/ethernet/ethm-1-plus>
- [22] EUROALARM. *GPRS – T4* [online], 2017, [cit. 2018-05-13]. Dostupné z: <https://www.euroalarm.cz/eshop-zabezpecovaci-technika/zabezpeceni/komunikace/gsm-gprs/gprs-t4>
- [23] EUROALARM. *Smet - 256* [online], 2014, [cit. 2018-05-13]. Dostupné z: <https://www.euroalarm.cz/eshop-zabezpecovaci-technika/zabezpeceni/komunikace/pulty-pco/smet-256>

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

AES	Advanced Encryption Standard
ANSI	Approved American National Standard
CCTV	Kamerový systém
CID	Contact ID protokol
ČR	Česká republika
ČSN	Česká státní norma
ČTÚ	Český telekomunikační úřad
DPPC	Dohledové a poplachové přijímací centrum.
DTMF	Dual tone multi frequency
EPS	Elektrická požární signalizace
EZS	Elektrické zabezpečovací systémy
GMT	Greenwich Mean Time
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Globální Systém Mobilní komunikace
HAS	Hold-up alarm systém
HW	Hardware
I&HAS	Intrusion and hold-up alarm systém
IAS	Intruder alarm systém
IP	Internet Protocol
ISA	Industry Standard Architecture
ISP	Internet service provider
JTS	Jednotná telefonní síť
LAN	Local Area Network

---

MAC	Media Access Control
PCO	Pult centralizované ochrany
PPC	Poplachové přijímací centrum
PSTN	Public Switched Telecommunication Networks
PZTS	Poplachový zabezpečovací a tísňový systém.
SIA	Security Industry Association
SMS	Short message service – krátká textová zpráva
SW	Software
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus

**SEZNAM OBRÁZKŮ**

Obr. 1: Vybrané prvky PZTS [11] .....	11
Obr. 2: DPPC Jablotron [13].....	16
Obr. 3: Zjednodušené schéma komunikačních tras, vlastní zdroj. ....	18
Obr. 4: Blokové schéma rádiové sítě DPPC, vlastní zdroj .....	19
Obr. 5: Navázání spojení při TCP a UDP [14] .....	22
Obr. 6: Náhled prostředí RADOMNET klient [7].....	31
Obr. 7: Výřez obrazovky webového rozhraní RADOMNET WEB [7] .....	32
Obr. 8: Konektory - připojené komunikační kanály v PPC [7] .....	33
Obr. 9 Telefonní karta GS51 [17] .....	34
Obr. 10: USB box pro GS51 [17] .....	34
Obr. 11: Příklad nastavení telefonní komunikace [7] .....	35
Obr. 12: Rádiový přijímač SRX10/400, zdroj autor .....	36
Obr. 13: Převodník Lantronix UDS-2100, [18].....	37
Obr. 14: Retranslační stanice, vlastní zdroj .....	38
Obr. 15: Příklad nastavení rádiové komunikace [7] .....	39
Obr. 16: Ukázka diagnostiky rádiové sítě z prostředí PPC [7].....	39
Obr. 17: Přijímač SRX10G, vlastní zdroj.....	40
Obr. 18: Ukázka nastavení automatických SMS zpráv [7].....	41
Obr. 19: INET komunikátor [19].....	42
Obr. 20: Vysílač SXS26 [20].....	42
Obr. 21: Příklad nastavení INET komunikace [7] .....	43
Obr. 22: Komunikátor ETHM 1 Plus [21].....	44
Obr. 23: Modul GPRS T4 [22] .....	45
Obr. 24: SMET-256 [23] .....	46
Obr. 25: Příklad nastavení TCP komunikace [7].....	48
Obr. 26: Ukázka překladové tabulky Tel42 v DPPC [7] .....	50
Obr. 27: Defínice masky tabulky CID [7] .....	50
Obr. 28: Ukázka překladové tabulky CID v DPPC [7].....	51
Obr. 29: Ukázka překladové tabulky SIA v DPPC [7].....	52

**SEZNAM TABULEK**

Tab. 1: Základní přehled platných norem PZTS.....	12
Tab. 2: Stupně zabezpečení [12].....	13
Tab. 3: Třídy prostředí [12] .....	14
Tab. 4: Výčet norem pro přenosové trasy.....	17
Tab. 5: Protokoly pro pulsní přenos [15].....	23
Tab. 6: DTMF tabulka frekvencí .....	24
Tab. 7: Protokoly pro tónový přenos [15].....	25
Tab. 8: Formát 4/2 .....	26
Tab. 9: Struktura tabulky CID .....	27
Tab. 10: Předpis překladové tabulky SIA [16] .....	29
Tab. 11: Telefonní čísla pro PPC a zapojení .....	35
Tab. 12: Nastavení SMET .....	47
Tab. 13 Nastavení TCP/UDP komunikace .....	49

## SEZNAM PŘÍLOH

P I: POROVNÁNÍ TABULEK CID A SIA PRO DSC NEO