

# Koncepce systému Kronos a porovnání s jinými systémy poplachových přijímacích center

The Kronos System Concept and its Comparison with Other  
Alarm Receiving Centers

Bc. Wojciech Bogdański

---

Diplomová práce  
2012



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2011/2012

## ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Wojciech BOGDANSKI**  
Osobní číslo: **A10951**  
Studijní program: **N 3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Koncepce systému Kronos a porovnání s jinými systémy poplachových přijímacích center**

Zásady pro vypracování:

1. Vysvětlete základní koncepci systému Kronos.
2. Zpracujte blokové schémata jednotlivých SW modulů.
3. Vysvětlete normy týkající se poplachových přijímacích center (PPC).
4. Porovnejte system Kronos s jinými systémy.
5. Vyhodnoťte přínosy Kronos systému a naznačte jejich další vývoj.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. ČSN EN 50136-1. Poplachové systémy - Elektrické zabezpečovací systémy Praha : Český normalizační institut, 2011.
2. NEXT! s.c., Bielsko-Biaza. Szawomir Piela, Bartzomiej Dryja - Software Product List KRONOS NET 2.x, 2011.
3. LUKÁŠ, L. et al. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011. ISBN 78-80-87500-05-7.
4. KINDL, J. Projektování bezpečnostních systémů I. 1. vyd. Univerzita Tomáše Bati ve Zlíně, Zlín 2004.
5. VYORÁLEK, R. Pulty centralizované ochrany. Zlín, 2005. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. Marek Čandík Ph.D.

Vedoucí diplomové práce:

**Ing. Rudolf Drga**

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

**24. února 2012**

Termín odevzdání diplomové práce:

**15. května 2012**

Ve Zlíně dne 24. února 2012



L.S.

prof. Ing. Vladimír Vašek, CSc.  
*děkan*

doc. RNDr. Vojtěch Křesálek, CSc.  
*ředitel ústavu*

## ABSTRAKT

Cílem diplomové práce je specifikace koncepce systému Kronos NET a jeho porovnání s jiným systémem poplachových přijímacích center. V první části je popsána historie, současný stav, vysvětlené normy týkající se poplachových přijímacích center. Důležitou součástí je naznačení jejich dalšího vývoje. Závěr práce tvoří vysvětlení základní koncepce systému Kronos NET, zpracování blokového schématu jednotlivých softwarových modulů popsaných systémů, porovnání systému Kronos NET s jiným systémem a vyhodnocení přínosu Kronos NET.

Klíčová slova:

Dohledové Poplachové Přijímací Centra (DPPC), Pult Centralizované Ochrany Objektů (PCO), Průmysl Komerční Bezpečnosti (PKB), Poplachový Zabezpečovací a Tísňový Systém (PTZS), Soukromá Bezpečnostní Služba (SBS),

## ABSTRACT

The aim of this thesis is a specification the Kronos NET system concept and its comparison with other alarm receiving centers. In the first part is described history, contemporary situation of alarm receiving centers and the standards for alarm receiving centers are explained. The important part of this thesis is to indicate their further development. In the conclusion an explanation of basic concepts of the Kronos NET, is a well processing a block diagrams of the software modules described systems as the comparison of the Kronos NET with another system and the evaluation of the benefits of the Kronos NET.

Keywords:

Alarm Receiving Centre (ARC), Commercial Security Business, Intruder and Hold – Up Alarm System (I&HAS), Private Agency of Security.

Rád bych poděkoval všem, kteří mi pomohli při zpracování mé diplomové práce. Především děkuji Ing. Rudolfu Drgovi za odborné vedení, konzultace a za poskytnuté připomínky ke zpracování a obsahu práce. Dále pak děkuji pracovníkům firmy MOBA s r.o. a Jablonet s.r.o.. za cenné rady.

**Prohlašuji, že**

- beru na vědomí, že odevzdáním diplomové/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 diplomová/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 diplomovou/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 s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/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 diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....  
podpis diplomanta

**OBSAH**

<b>ÚVOD</b> .....	<b>9</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>11</b>
<b>1 HISTORIE DPPC</b> .....	<b>12</b>
<b>2 CHARAKTERISTIKA DPPC</b> .....	<b>15</b>
2.1 OBECNÉ POŽADAVKY NA PROVOZ DPPC .....	15
2.2 SLUŽBY NA DPPC.....	18
2.3 SLOŽENÍ DPPC .....	20
2.3.1 SAMOSTATNÉ NEZÁVISLÉ ZAŘÍZENÍ – REKY .....	20
2.3.2 OSOBNÍ POČÍTAČE .....	21
2.3.3 KOMBINACE .....	21
2.3.4 TYPY PŘENOSŮ .....	22
2.3.5 ZPRÁVY NA DPPC.....	30
2.3.6 PŘENOSOVÉ FORMÁTY .....	31
<b>3 LEGISLATIVA</b> .....	<b>34</b>
3.1 ZÁKLADNÍ ZÁSADY PROVOZU DPPC .....	34
3.2 ČSN EN 50518 – 1 .....	35
3.3 ČSN EN 50518 – 2.....	36
3.4 ČSN EN 50518 – 3.....	37
<b>4 VYVOJ SYSTÉMŮ DPPC</b> .....	<b>39</b>
<b>II PRAKTICKÁ ČÁST</b> .....	<b>41</b>
<b>5 POROVNÁNÍ SOFTWARE</b> .....	<b>42</b>
5.1 NET – G .....	43
5.1.1 MODUL APPPCO.....	45
5.1.2 MODUL APPDRIVER.....	60
5.1.3 MODUL APPMAIL .....	61
5.1.4 KEYADMINISTRATOR .....	62
5.1.5 MODUL WATCHDOG.....	63
5.1.6 MODUL WATCHCONNECT TCP .....	64
5.1.7 MODUL STATISTIKA.....	65
5.1.8 MODUL APPSERVIS .....	66
5.1.9 SHRNUÍ – VÝHODY SYSTÉMU NET-G .....	69

5.2	KRONOS NET.....	70
5.2.1	MONITORING CONSOLE.....	75
5.2.2	DATA EDIT CONSOLE.....	80
5.2.3	SERVICE CONSOLE.....	85
5.2.4	BILLING CONSOLE.....	87
5.2.5	CONFIGURATION TOOLS.....	88
5.2.6	CLIENT CONSOLE.....	89
5.2.7	SHRnutí – VÝHODY SYSTÉMU KRONOS NET.....	90
5.3	OHODNOCENÍ SYSTÉMŮ – PŘÍNOSY.....	93
	<b>ZÁVĚR.....</b>	<b>97</b>
	<b>ZÁVĚR V ANGLIČTINĚ.....</b>	<b>99</b>
	<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>101</b>
	<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>102</b>
	<b>SEZNAM OBRÁZKŮ.....</b>	<b>104</b>
	<b>SEZNAM PŘÍLOH.....</b>	<b>105</b>



## ÚVOD

Ve své diplomové práci se budu zabývat koncepcí systému Kronos NET a porovnáím ho s jinými systémy poplachových přijímacích center. V teoretické části popíšu historii poplachových přijímacích center, jejich charakteristiku a legislativu týkající se poplachových přijímacích center. V praktické části vysvětlím základní koncepci systémů, zpracuji blokové schéma jednotlivých softwarových modulů, porovnáím systém NET-G od společnosti NAM se systémem Kronos NET od společnosti Next!, vyhodnotím přínosy obou systémů a pak se pokusím naznačit směr dalšího vývoje poplachových přijímacích center. Při psaní diplomové práce budu používat knihy, časopisy, normy a manuály, které jsou běžně pro studenty dostupné.

Při zpracování teoretické části diplomové práce pro mě bude mimo jiné velice užitečná publikace Lukáše L. et al. *Bezpečnostní Technologie, Systémy a Management I*, kde je obecně popsána historie a charakteristika poplachových přijímacích center. Dalšími zdroji, se kterými budu pracovat, jsou normy ČSN EN 50518 1-3 o dohledových a poplachových přijímacích centrech. Z těchto zdrojů získám nezbytné informace pro sepsání legislativní části práce. Při psaní praktické části budu používat dva zdroje, a to manuál od společnosti NAM, *Monitorovací software NET-G: Manuál správce*, a manuál od společnosti Next!, *Software Product List KRONOS NET 2*. Pomůžou mi zorientovat se při testování aplikací.

Abych téma diplomové práce zpracoval přehledně, stanovím si kapitoly, ve kterých jasně vysvětlím princip dohledových a poplachových přijímacích center. Začnu kapitolou Historie, ve které popíšu začátky provozu prvních poplachových center a jejich další vývoj do dnešní doby. Pak se pokusím o charakterizování poplachových přijímacích center (PPC). Popíšu obecné požadavky na provoz, služby PPC, přenosové formáty, trasy atd. Další kapitolou teoretické části bude Legislativa. V ní především s využitím normy ČSN EN 50518 popíšu právní prostředí v oblasti dohledových a poplachových přijímacích center. Teoretickou část uzavře kapitola, ve které pokusím se předpovědět směr, jakým se poplachová přijímací centra budou dále vyvíjet. V praktické části podrobně popíšu chování systémů Kronos NET a NET-G za provozu a pak vyhodnotím jejich přínosy a slabiny.

Při psaní práce budu používat knihy, skripta, časopisy z oboru bezpečnostních technologií, protože obsahují širokou škálu informací týkajících se poplachových přijímacích center. Díky nim budu moci pojmout teoretickou část diplomové práce. Využívat budu také manuály a programy, softwary NET-G a Kronos NET. Nejprve budu testovat software

NET-G a pak stejným způsobem otestuji konkurenční produkt Kronos NET. Díky tomu zjistím, jak se systémy chovají za provozu a budu mít dostatek informací, abych je mohl mezi sebou porovnat.

## **I. TEORETICKÁ ČÁST**

## 1 HISTORIE DPPC

Dohledová Přijímací Poplachová Centra (odtud zkratka DPPC) jsou součástí lidského života už desítky let. V České republice vznikla první DPPC u policie v polovině sedmdesátých let. Mnoho desetiletí předtím končily výstupy dálkových signalizací z významných objektů na policejních stanicích. V roce 1851 byl v Bostonu (Spojené státy americké) zahájen provoz prvního skutečného DPPC, integrujícího výstupy „volacích skříněk“, praotců dnešních hlásičů požáru. V polovině devatenáctého století založil Edwin T. Holmes v New Yorku první DPPC pro zabezpečovací systém. První evropskou variantou systémů DPPC byl systém veřejných požárních hlásičů v Německu (Hamburku) vybudovaný kolem roku 1890. [1]

Původní návod k použití tohoto požárního hlásiče, uvedeného do provozu v dubnu 1864 v San Francisku (Spojené Státy americké) bude dnešním uživatelům znít jako pohádka od babičky. V překladu do češtiny by zněl asi takto: *„Po zjištění požáru v blízkosti vaší volací skřínky pomalu a plynule zatočte klikou 25 až 30krát, potom chvíli vyčkejte, a pokud neuslyšíte tikání ze skřínky nebo požární zvonky, postup opakujte. Jestliže stále nezaznamenáte žádný poplach, přejděte k jiné skřínce a vyhlase poplach z ní. Nikdy neotvírejte skříňku a nedotýkejte se kliky, jedině v případě požáru. Nikdy neohlašujte požár, který vidíte z dálky. Před odchodem se ujistěte, že skříňka je uzamčena.“* [1]

Přijímací Poplachová Centra se během času vyvíjela. Nejdříve pomalu, a pak, s rozvojem telekomunikace, případně dálnopisu, a především po vzniku nových komunikačních prostředků a digitální techniky v uplynulých desetiletích, čím dál rychleji.

Přijímací Poplachová Centra se původně používala pouze u Policie ČR. Historie využívání takovéto prevence v kriminálním světě se datuje od roku 1976. Původní přijímací poplachová centra byla jen linková s přenosem signálu po telefonní síti. Všechna tato technika byla používána původně v zemích východního bloku, a to v Rusku a v Bulharsku. V r. 1989 používal policejní sbor cca 50 přijímacích poplachových center, na něž bylo napojeno cca 500 velmi důležitých objektů, u nichž bylo vysoké riziko napadení. Tato napojení byla prováděna jako nástrahová, na rozdíl od dnešní doby na nich nebylo zřetelně viditelné, zda pozorovaný objekt má dálkovou kontrolu, protože se počítalo se zadržením zločinců na místě. Od roku 1987 bylo přijímací poplachové centrum s hlídaným objektem spojeno prostřednictvím telefonních linek. Zájemce o zabezpečení si musel u společnosti poskytující telefonní služby zažádat o namontování speciálního prvku do telekomunikační

ústředny. Přenos informací se odehrával v nadhovorovém pásmu, a hlavním přínosem tohoto systému bylo, že zaznamenal i případné havárie nebo sabotáže telefonního vedení.

Po roce 1990 radikálně narostl počet objektů hlídaných soukromými službami, a to mělo za následek i výrazný nárůst počtu odhalení trestné činnosti ve vloupání pachatelů do objektů. v roce 1992 se usnesením vlády č. 584/1992 sjednotil typ DPPC provozovaných u Policie České republiky. Ministerstvo vnitra si jako nejlepší vybralo rádiolinkový DPPC systém FAUTOR II. Přechod všech poplachových center na tento jednotný systém byl dokončen na začátku roku 1996.

Po změně politického systému se na začátku roku 1990 začalo ve velkém rozvíjet soukromé podnikání. Zvýšený počet podniků, nárůst kriminality a zvýšená potřeba dbát o bezpečnost svého majetku otevřely trh pro agentury poskytující soukromé bezpečnostní služby. Ty hned pochopily, že v okolí vzniká velmi dobrý trh pro rozvoj soukromých bezpečnostních služeb, protože policie nemá dostatečný počet lidí ani technické vybavení na to, aby na svá přijímací poplachová centra připojila všechny zájemce o střežení objektů.

V této době začínají soukromé bezpečnostní služby využívat přijímací poplachová centra. Ze začátku se používala linková DPPC s přenosem po telekomunikační lince. Nejčastěji se používaly zejména produkty kanadského výrobce SUAQUARD SGDR1. Na těchto a podobných typech DPPC se přijímaly a vyhodnocovaly zprávy v binárních kódech. Při malém počtu zapojených objektů tento princip vyhovoval, ale s nárůstem pozorovaných objektů se zvyšovalo riziko špatného vyhodnocení zprávy. To bylo odstraněno až s příchodem nových DPPC vyvíjených a vyráběných v tuzemsku, které již využívali na vyhodnocení zprávy nadstavbový software. Linková DPPC byla na začátku 90. let dvacátého století závislá na možnostech telefonní sítě. Ta byla v té době analogová, velice nespolehlivá a plná míst, kde mohlo dojít ke vzniku problému. Vytvoření přenosové trasy pro poplachové zprávy trvalo i celé měsíce, protože čekací lhůty na zprovoznění telefonní linky byly velice dlouhé. Z tohoto důvodu začala vznikat a dále se vyvíjet rádiová DPPC českých výrobců. Nejznámějšími bezpečnostní systémy, které ovládly ve své době trh, byly RADOM nebo NAM. Zakládání rádiových sítí bylo pro provozovatele velice finančně náročné, protože společnost vytvářející DPPC musela na vlastní náklady – a ty byly obrovské – zřídit vlastní soukromou rádiovou síť. Pak se prostřednictvím tyto sítě přenášely informace. V hlídaném objektu byly umístěny: ústředna PZTS, rádiový vysílač a na straně DPPC byl přijímač, který s ním komunikoval. Rádiové pulty byly a dodnes stále jsou užívány pro svou spolehlivost, a to hlavně v „nevlňových“ nebo klimaticky

příhodných oblastech. To, že tento systém vznikl v českém prostředí, zapříčinil fakt, že na západě fungovala kvalitní telefonní síť, která umožňovala přenos informací pro DPPC, a tak nikdo nemusel vytvářet alternativní přenosové trasy.

Na začátku 90. let dvacátého století zaznamenala ČR prudký nárůst trestné činnosti. Na základě zákonů začala města zřizovat městské policie. Ne ve všech městech byly soukromé bezpečnostní služby dost ekonomicky silné na to, aby postavily DPPC, proto se touto problematikou začala zabývat městská policie. Po stránce technického vybavení kopírovala městská policie soukromé agentury a jejich dnešní DPPC se neliší od těch, které se používají v soukromých bezpečnostních službách. Na počátku rozvoje těchto služeb bylo jejich hlavním cílem ochrana městských objektů, jako jsou školy, divadla, radnice apod. Časem však u městské policie v České republice zvítězila komercializace a snaha o maximální využití DPPC, kterou MP využívá pro ochranu státního majetku, také při zabezpečení soukromého sektoru. V té době městské policie konkurují SBS ve službách DPPC. [2]

V roce 2011 byly zavedeny změny v legislativě PKB. Podle nové normy začalo platit nové pojmenování Pultu Centralizované Ochrany. Navrženo nový mezinárodní název pro PCO – Alarm Receiving Centre (ARC), který v překladu znamená Poplachová přijímací centra (PPC), někdy se používá také název Dohledová poplachová přijímací centra (DPPC).

## 2 CHARAKTERISTIKA DPPC

*„Přijímací Poplachové Centrum (PPC) je dispečerské zařízení, vybavené výpočetní technikou, která vyhodnocuje poplachové a informační stavy z PZTS instalovaného ve střeženém objektu. Zprávy jsou na toto zařízení přenášeny různými způsoby (telefonní linkou, mobilní sítí, rádiovou sítí atd.). DPPC tedy slouží k vyhodnocování údajů přenášených z střeženého objektu. Výstupy ze systému jsou zpracovány speciálním uživatelským programem, který umožňuje podrobný přehled o stavu střeženého objektu a nabízí i nejrůznější doplňkové služby pro snadnější práci a efektivní reakci na vznik dané události. Po vyhodnocení poplachového signálu se vyrozumí - dle smluvních podmínek: zákazník, oprávněná osoba, policie nebo havarijní služba, nebo se vydá pokyn zásahové jednotce k provedení předepsaných činností. Pokud dojde k narušení objektu, je tento prověřen výjezdovou skupinou. Elektronická forma ostrahy objektů je klienty preferována vzhledem ke snadné dostupnosti a relativně nízkým pořizovacím nákladům poplachových zábranných a tísňových systémů (PZTS).“ [3]*

### 2.1 Obecné požadavky na provoz DPPC

Základní funkcí DPPC je posílání vyhodnocených zpráv z bezpečnostních a jiných zařízení hlídané osoby na přijímací centrum bezpečnostní agentury. Dál postupují bezpečnostní pracovníci DPPC podle typu události tak, aby co nejrychleji a nejefektivněji vyřešili vzniklý problém v souladu s platnými směrniciemi a smlouvou mezi DPPC a klientem.

„Dálková“ ochrana přes poplachové přijímací centrum je v současné době jedním z nejlepších způsobů, jak ochránit majetek.

Kvalitu služeb, které poskytuje bezpečnostní agentura, můžeme měřit podle času, který potřebuje k tomu, aby vyřešila problém, podle profesionality bezpečnostních pracovníků a podle techniky přenosu informací. Dobře provedený zásah se snaží co nejvíc minimalizovat škody na chráněném objektu, a to jak ze strany pachatele, tak i ze strany zasahujících zaměstnanců. Důraz je kladen především na ochranu života a zdraví každého účastníka zásahu.

Rychlost, s kterou dojde k zásahu, je ovlivněna dojezdovým časem, tedy dobou, kterou potřebuje bezpečnostní automobil zásahové skupiny k přejezdu z místa sídla zásahové centrály do místa napadeného objektu. Dobu dojezdu po zjištění útoku na objekt ovlivňuje

několik faktorů. Většinu z nich není možné ovlivnit (dopravní zácpy na cestách, kvalita přístupové komunikace, počasí atd.). Kromě těchto vlivů je velmi důležitá také vzdálenost napadeného objektu od nejbližšího centra zásahové jednotky. Centra jsou rozmísťována tak, aby byla zákazníkům vždy co nejbližší.

Kvalita služeb je také závislá na správném zadávání a provádění rozkazů. Je důležité zkrátit na minimum čas od vzniku poplachu do výjezdu zásahové skupiny k objektu. Proto je nutné mít zpracované podrobné pokyny, které musí každý bezpečnostní zaměstnanec dokonale znát a dodržovat. Má-li být zásah co nejrychlejší a nejdokonalejší, nelze připustit, aby pracovníci improvizovali. V dnešní době jsou vytvářeny obecné a specifické modelové situace, které se neustále zdokonalují a propracovávají.

Profesionální zaměstnanci jsou tedy dalším článkem, který je pro dokonalou ochranu majetku zcela nezbytný. Všichni uchazeči o práci v zásahových jednotkách musí splňovat všechna následující kritéria:

- věk 21 let,
- trestní bezúhonnost,
- držitel zbrojního průkazu,
- držitel řidičského oprávnění minimálně kategorie B,
- minimálně dvouletá praxe atp.

Kromě toho se také zkoumají fyzické a psychické předpoklady k vykonávání práce v PKB. Zaměstnanci jsou pravidelně zkoušeni ze svých znalostí a schopností a také proškolení pro rozšíření dovedností potřebných k profesionalizaci.

Další důležitou podmínkou správného fungování PPC je volba vhodného způsobu přenosu informace z objektu na přijímací poplachové centrum. Přenos informací by měl co nejlépe splňovat tyto požadavky:

- kontrola přenosu dat,
- nejrychlejší přenos zprávy na DPPC,
- schopnost zařízení předávat informace o všech stavech v hlídaném objektu.



**Operační středisko musí mít:**

- homologované poplachové přijímací centrum včetně záložního zdroje,
- speciální linky pro přenos dat (signálů) z PZTS do DPPC,
- počítač s diskem pro archivaci dat DPPC s databází všech hlídaných objektů,
- zařízení pro komunikaci: mobilní telefony, vysílačky, CB rádio,
- archiv protokolů z každého výjezdu zásahové jednotky,
- aktuální archiv listů fyzické ochrany,
- dokumentaci: manuály, směrnice k objektům, metodické pokyny, atd.

**Personální podmínky:**

Z pohledu personálního obsazení pozic v sektoru práce na DPPC se dlouhodobě klade nárok na obsazování míst odborně vyškolenými odborníky. Zaměstnanci DPPC by měly splňovat následující podmínky:

- schopnost řešit mimořádné situace,
- schopnost pracovat ve stresu a pod tlakem,
- znalost DPPC po technické a manuální stránce,
- schopnost komunikace.

**Požadavky na pracovníky zásahových jednotek:**

- disciplinovanost,
- fyzická zdatnost,
- dobrá znalost zásahových metod,
- znalost topografie střežených objektů,
- schopnost ovládat zbraně a zkušenost s používáním zbraní a dalších donucovacích prostředků.[3]

## 2.2 Služby na DPPC

Služby na DPPC u soukromých provozovatelů stojí na komerčních základech. Majitelé DPPC poskytují bohatou nabídku služeb. Základní rozdíl, který mezi nabídkami je, spočívá v postupu dispečera při příjmu poplachové informace a v ceně. V sektoru samozřejmě vládne konkurence, a proto je žádoucí vytvořit každému zákazníkovi individuální nabídku.

Zde jsem uvedl příklady služeb, které nabízí bezpečnostní agentury. Služby se samozřejmě můžou kombinovat.

### Monitoring

Je to základní služba, kterou poskytují bezpečnostní agentury. Obsahuje monitoringový systém. Náplní této služby je sběr, vyhodnocení a archivace dat z objektů. Ve chvíli přijetí poplachové zprávy předává operátor DPPC zákazníkovi informace o vzniklé události na předem domluvená telefonní čísla. Zákazník pak sám dál rozhoduje, zda vzniklou situaci na objektu prověří on sám, nebo zda mají zasáhnout zásahové skupiny DPPC. Při telefonickém kontaktu se zákazníkem lze po domluvě využívat i předem domluvená hesla pro identifikaci osob, které rozhodují o způsobu prověření poplachu.

### Zásah

Klíčovou složkou zásahu je výjezdová skupina, která po obdržení poplachové zprávy vyráží na místo prověřit situaci, případně provést preventivní nebo represivní zásah v rámci zákona. Zásahovou skupinu vždy vede k cíli operátor DPPC. Operátor díky Monitoring Console neustále předává aktuální informace o stavu v objektu, na kterém vznikl poplach.

Provozovatelé DPPC svým zákazníkům obvykle nabízí dvě varianty platby tohoto typu služeb:

- Zákazník platí měsíční paušál, který zahrnuje všechny výjezdy k objektu.
- Zákazník platí provozovateli DPPC za každý výjezd.

## **Patrol**

Patrol je systém, který je považovaný za preventivní nástroj ochrany objektů. V podstatě slouží jako fyzická ostraha. Spravuje ho zásahová skupina DPPC. Jde o využití výjezdové jednotky v čase, kdy se řeší zákrok na základě poplachové zprávy.

Podstatou služby je provedení akce výjezdové skupiny v době plnění služby a provádění preventivní prověrky objektů a jejich okolí dle harmonogramu. Celá služba Patrol je preventivní a působí na podvědomí okolí (objekt není ponechán bez kontroly, je zabezpečen profesionální bezpečnostní skupinou).

## **Doplňkové služby**

Doplňkové služby nabízí agentury DPPC svým zákazníkům pro zlepšení komfortu nabízených bezpečnostních služeb. Patří mezi ně například:

- Vyrozumění odpovědného personálu pokud objekt nebyl v určitém čase zastřežen.
- Zasílání SMS o stavu objektů. Z DPPC konzoly je možné na dálku komunikovat s elektronickým zařízením (zastínění oken, spouštění klimatizace, zapnutí osvětlení, spouštění topení atd.).
- Informování zákazníka DPPC o výpadku dodávky elektrické energie, o poruchách telefonní linky apod.
- Měsíční nebo týdenní výpisy (záleží na nabídce) z historie objektu, posílané poštou nebo v elektronické podobě.
- Správa odkódování a zakódování objektů pomocí dálkového ovládní ústředí PZTS.
- Dálkový dohled zákazníků nad objekty pomocí kamerového systému CCTV.

## **Servis**

Jestliže je společnost DPPC i dodavatelem bezpečnostních systémů, může svým zákazníkům za zvýšený poplatek nabízet i servis bezpečnostního zařízení provozovaný 24 hodin denně.

## Ostraha

Ostraha se využívá v případě zvýšeného rizika napadení chráněného objektu. Zásahová skupina provede opatření a v době zaznamenání napadení chráněné oblasti ihned informuje majitele objektu, ve vážných případech také Policii ČR.

Společnost DPPC by měla mít dostatek pracovníků fyzické ostrahy, kteří dokážou zajistit bezpečnost prostorů chráněné oblasti do příjezdu správce objektu, popřípadě do začátku pracovní doby zaměstnanců v objektu.

Větší část provozovatelů DPPC v oblasti komerčního zabezpečení poskytuje kompletní služby od zajišťování fyzické ochrany, přes transport hotovosti a cenin, až po technickou oblast (montáže PZTS, CCTV, EPS). Zákazník se pouze rozhoduje, kterou ze široké nabídky služeb využije pro ochranu svého majetku. [3]

## 2.3 Složení DPPC

Dohledová a poplachová přijímací centra jsou většinou provozovány jedním z následujících dvou způsobů.

- Jako autonomní systém, který je provozován samostatně.
- Jako systém provozovaný pomocí počítače.

### 2.3.1 Samostatné nezávislé zařízení – Reky

Reky jsou samostatná zařízení, která obsahují záložní zdroj a jsou schopna samostatného provozu po určitou dobu) např. 12 hodin i bez napájení 230V. Rek většinou obsahuje sloty pro různé moduly – telefonní linková karta, ISDN karta, rádio-karta, karta pro tiskárnu. Jednotlivé karty mají svoji vnitřní paměť až na 2000 událostí, pro případ výpadku, nebo servisního zásahu ne REKU. Tím že nevyužívají žádný operační systém, jsou velmi spolehlivé a málo náchylné k „padání“ systému. Na čelní straně takového reku většinou najdeme ovládací a programovací klávesnici a display klávesnici. Zprávy jsou zobrazovány na displeji a při příchodu rovněž tisknuty on-line na tiskárně protože displeje reků jsou max. dvouřádkové a zprávy by se ztrácely. Nevýhodou reků je, že zobrazují zprávy v číselném formátu, chybí jim textový překlad, proto jsou méně adresné a rozklíčování číselného kódu zabere čas. Obsluha při příchodu zprávy musí podle pomocné

dokumentace zjistit, o jaký objekt se jedná, jaký typ zprávy je signalizován a případně z které zóny je hlášen poplach. Provoz takového typu DPPC omezuje používání libovolných překladových tabulek pro bezpečnostní ústředny. Měl by být dodržen postup, že například kódy začínající 3 jsou vyhrazeny pro poplach (u všech objektů) tak, aby bylo pro obsluhu hned jasné, jaký typ zprávy zpracovává. Složitější to je ovšem u velkokapacitních ústreden, které mají například 256 zón. Potom nastává problém jak jednoduše vytvořit programovací tabulku pro přenosové zprávy. [2]

### 2.3.2 Osobní počítače

Jsou v podstatě PC stanice (osobní počítače) se všemi svými výhodami a nevýhodami. PC pracují s operačním systémem (DOS nebo Windows). V poslední době je možno systémy DPPC v PC provozovatele jako součást počítače, tj. telefonní, rádiová, GSM nebo ISDN karta je zasunuta na základní desce PC, nebo jsou tyto karty mimo PC v krabici a s počítačem komunikují přes USB připojení nebo sériové rozhraní (port COM). Jednotlivé karty mohou mít svoji vnitřní paměť až na 2000 událostí, pro případ výpadku, nebo servisního zásahu na PC. Takovéto zařízení je vlastně Hardware DPPC.

Další nezbytnou součástí DPPC v PC je Software. Je to vyhodnocovací a řídicí program, který zajišťuje komunikaci HW DPPC s SW PC a pracuje s daty z HW DPPC.

DPPC provozované na PC musí mít funkční obě části SW i HW. Jeden bez druhého jsou v podstatě zbytečné. Nevýhodou takovýchto zařízení je finančně náročná záloha napájení v případě výpadku proudu. Běžné UPS záložní zdroje vydrží cca ½ hodiny, což je velmi málo. Dále je to problém se stabilitou systému a HW počítače. Je potřeba si uvědomit, že DPPC potažmo PC je zapnutý neustále, 24 hodin denně, 365 dní v roce. To sebou nese zvýšené požadavky na odolnost celého systému.[2]

### 2.3.3 Kombinace

V současné době nejvhodnější architektura systémů DPPC. Jedná se o dvě oddělené části DPPC. Jde o ReK (popsaný výše) schopný samostatné práce i při výpadku DPPC, lehce zálohovatelný v případě výpadku 230V. Celé toto zřízení je navíc zastřešeno SW nadstavbou DPPC, která běží pod operačním systémem na PC (viz výše). Zprávy jsou přijímány a vyhodnocovány na ReKu a duplicitně jsou tyto zprávy zpracovávány ještě v PC

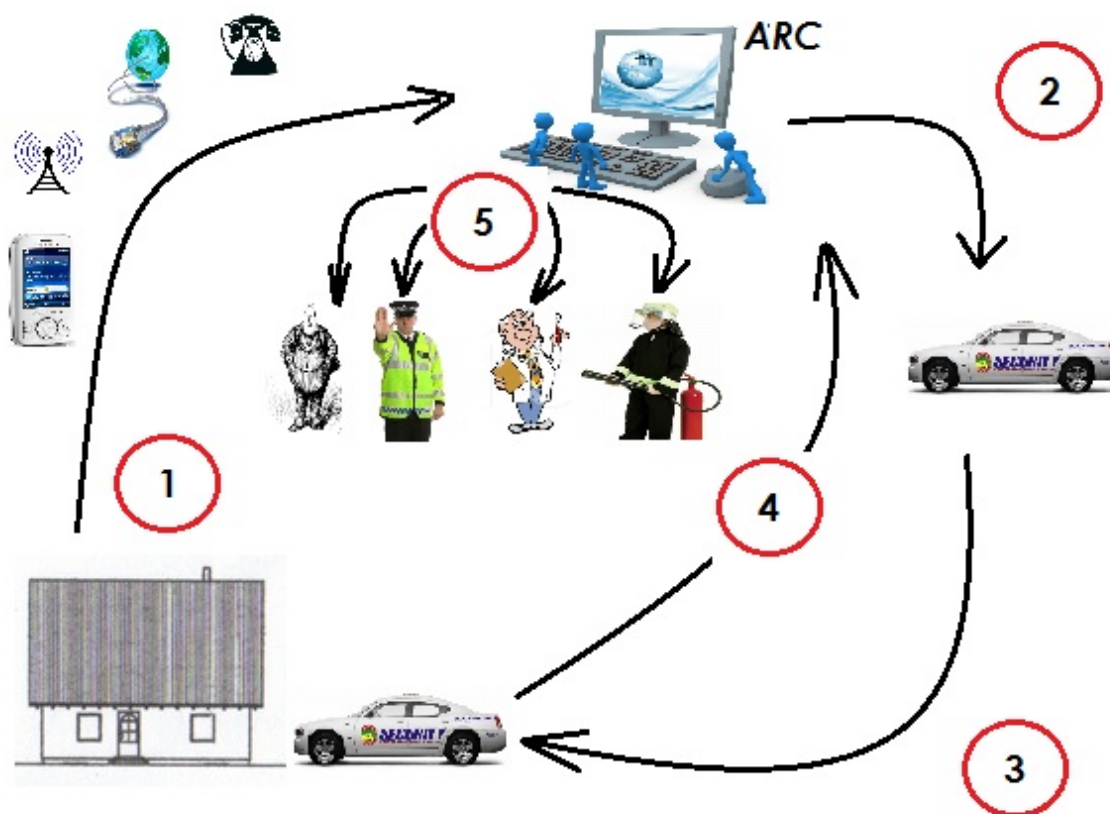
pro větší uživatelský komfort. Reky jsou k PC připojeny přes USB nebo sériové rozhraní. Nadstavbové SW DPPC umožňují provozovat několik systémů DPPC od různých výrobců. To je s výhodou využíváno, pokud se slučují některé firmy využívající jiné typy DPPC nebo, když provozovatel využívá rádiovou část od specializované firmy např. Radom a telefonní část např. od firmy NAM.

Jistým možným využitím kombinovaného DPPC je GSM karta která jednak umožňuje přijímat zprávy ve tvaru SMS do DPPC a odesílat vybrané typy z práv z vybraných nebo všech objektů jako SMS informaci. v podstatě zkopíruje textovou podobu zprávy přijaté a vygenerované na DPPC jako SMS na dané mobilní tel číslo. Službu lze nabízet zákazníkům, kteří mimo připojení na DPPC jsou rovněž on-line informováni o změnách stavů na bezpečnostním zařízení. S výhodou je této možnosti využíváno k tzv. bezobslužnému provozu DPPC. Poplachové zprávy se naprogramují jako SMS vyrozumění na mobilní číslo zásahové jednotky. Ta je potom informována přímo v terénu o poplachu přijatém DPPC automaticky pomocí SMS, aniž by musela být u DPPC obsluha. [2]

#### 2.3.4 Typy přenosů

Přenos poplachových informací ze střeženého objektu na DPPC je prioritní funkcí dobře navrhnutého bezpečnostního systému. Typy přenosů dat se liší v několika bodech: první z nich je náročnost na instalace, druhou je spolehlivost systému a třetí pořizovací a provozní náklady. V současnosti je stále kladen důraz na všeobecné zvyšování rychlosti přenosových cest. Nejčastěji používané komunikační přenosové trasy jsou:

- Telefonní (JTS)
  - Hovorové, nadhovorové pásmo, ISDN,
- GSM
  - Hovorový kanál, SMS, GPRS,
- Rádiová
  - Jednosměrná, obousměrná, jedno-frekvenční, vice-frekvenční,
- Internet.



Obr. 1 Schéma přenosu a vazeb u DPPC

Obrázek představuje přenosovou trasu a vazbu na DPPC. V prvním kroku posílá ústředna PZTS signál o napadení objektu pomocí telefonní, radiové, GSM/GPRS nebo internetové sítě na DPPC. Operátor DPPC po přijetí informace z objektu v druhém kroku vysílá zásahovou skupinu k objektu, od kterého přišel poplachový signál. V třetím kroku zásahová jednotka provede stanovené zákroky na místě. Ve čtvrtém kroku zásahová jednotka posílá zpětnou informaci operátorovi DPPC o stavu objektu. V pátém kroku operátor DPPC informuje klienta, případně složky IZS o stavu objektu.

#### 2.3.4.1 Telefonní linka (JTS)

Při vzniku DPPC byly telefonní linky jediným způsobem přenosu zpráv ze vzdálených objektů. I v dnešní době je telefonní linka stále velmi používanou přenosovou trasou. Rozvoj technologií radiových sítí, GSM sítí, internetu a neustálý úbytek telefonních přípojek zapříčiňuje odklon od používání této trasy.

JTS lze pro přenosy zpráv na DPPC rovněž využít na několika způsoby:

- hovorové pásmo
- ISDN
- nadhovorové pásmo

#### 2.3.4.1.1.1 Hovorové pásmo

Jedna z nejpoužívanějších přenosových tras v oblasti zabezpečení. Telefonní linka se připojí do ústředny PZTS a následně se s ústředny PZTS vytvoří připojení pro koncové zařízení. Takovéto připojení je vždy nutno dodržet, aby byla splněna podmínka priority vysílání informací ústřednou na PZTS. Tam, kde je použita pobočková telefonní ústředna, musí být signál veden nejprve do PZTS a následně teprve do telefonní ústředny. Tímto řešením je umožněno běžné užívání telefonní linky pro hovory. V případě, že dojde na ústředně PZTS k události, tato zajistí přerušování stávajícího hovoru, uvolní si linku na dobu nezbytně nutnou pro předání zprávy na PZTS a znovu linku uvolní pro další použití.

Na straně PZTS jsou linky zapojené do tzv. telefonních karet.



Obr. 2 Telefonní karta GS51 od firmy Matylda [3]

Na straně DPPC by se měly využívat minimálně dvě linky, počet záložních linek je závislý na počtu smyček připojených objektů a použitém přenosovém formátu.

Nastavení se většinou provádí tak, že do ústředny PZTS se naprogramují dvě čísla a v případě obsazené linky A začne ústředna vytáčet linku B. Pokud je obsazená i linka B, pak se celý postup opakuje až do vyhlášení chybné komunikace. Tento proces je poměrně časově náročný. Využívá se tedy služba provozovatele JTS, který za poplatek nabízí tzv. sériovou linku. Ústředna potom vždy vytáčí jen první telefonní číslo PZTS a pokud je toto obsazeno, pak je hovor automaticky přeměrován na druhou linku telefonní karty.



Provozovatele PZTS by měli zajistit utajení telefonního čísla zapojeného PZTS tak, aby zamezili zlomyslnému volání a tím blokování linek PZTS.

V poslední době provozovatelé mohou využívat tzv. sériové linky ve formátu 842 xxx xxx, které umožňují softwarovým nastavením vytvářet směrování na straně poskytovatele telefonních služeb. To znamená, že při dovolání na první telefonní číslo dojde, v případě jeho obsazení, ve zlomku sekundy k překlopení na druhé telefonní číslo.

Hlavní výhodou přenosu v hovorném pásmu telefonních linek jsou nízké pořizovací náklady, protože většina ústředn PZTS má implementován telefonní komunikátor. Mezi nevýhody patří zejména snadné přerušení, snadné vyřazení trasy obsazením linky, zpoplatnění každého přenosu zprávy, nevhodná tarifkace. Periodické testy se provádějí zpravidla jednou denně. [12]

#### 2.3.4.1.1.2 *Telefonní linka v nad-hovorovém pásmu*

Jedna se o přenosovou trasu, které se již prakticky v ČR nevyužívá. Poplachové informace jsou při tomto způsobu přenosu přeměněny na signál o kmitočtu nad hovorným pásmem 20 000 Hz. Výhodou je okamžitá indikace přerušení trasy, nevýhodou byla nutnost přemostění ve všech telefonních ústřednách na trase objekt – PZTS. [12]

#### 2.3.4.1.2 ISDN – Digital

ISDN je zkratka anglického termínu Integrated Services Digital Network, český název pro tuto síť je Digitální síť integrovaných služeb.

Dnešní telefonní sítě jsou založeny na digitálních telefonních ústřednách a přenosové cesty mezi ústřednami jsou také plně digitalizovány. Poslední analogovou částí sítě tak zůstává účastnická přípojka. Tedy poslední část od ústředny k telefonnímu přístroji (modemu, faxu atd.) účastníka. ISDN nabízí plně digitální přenos až k účastníkovi (A/D a D/A převod signálu se odehrává přímo v koncovém přístroji).

ISDN dále nabízí možnost komunikovat pomocí jedné digitální účastnické přípojky prostřednictvím hlasu, textu a obrazu. Obecně pak mluvíme o multimediální komunikaci. ISDN přípojku lze pomocí takzvaného terminálového adaptéru, samozřejmě použít také pro připojení do sítě Internet. V Evropě bylo po počátečních problémech s kompatibilitou zavedeno tzv. EURO-ISDN, které zaručuje shodnou implementaci ISDN po celé Evropě. V Evropě se tedy pod pojmem ISDN myslí vždy EURO-ISDN.

ISDN nabízí dva typy přípojek:

- **BRI** – Basic Rate Interface, je účastnická přípojka na kterou lze připojit až 8 koncových zařízení (telefon, fax, modem, ...). Označuje se 2B + D.
- **PRI** – Primary Rate Interface, tento typ přípojky je určený pro připojení pobočkových ústředen, nelze ji využívat pro připojení koncových účastnických zařízení. V Evropě a Austrálii se označuje 30B + D. V Severní Americe a Japonsku má jiné parametry a najde se ji pod označením 23B + D.

Přípojka 2B + D (základní přístup) znamená tedy dva nezávislé B kanály o rychlosti 64 kbit/s určené pro přenos hlasu, faxu, obrazu, dat atd. a jednoho D kanálu o rychlosti 16 kbit/s určeného pro přenos signalizace.

Přípojka 30B + D (primární přístup) znamená třicet nezávislých B kanálů o rychlosti 64 kbit/s a jeden D kanál také o rychlosti 64 kbit/s určený pro přenos signalizace.[9]

Výhodou ISDN je posílání dat mezi objekty. DPPC je stále hlídáno, při jakémkoliv přerušení posílané zprávy je ihned oznámena porucha v konzole softwaru.

Nevýhodou ISDN přenosu je nutnost vlastnit ISDN karty pro tento typ přenosů dat. Na straně objektu musí být nainstalovaná linka, která bude schopna posílat stejné typy dat. V České republice se tento typ přenosu příliš neujal, hlavně kvůli vysokým cenám za ISDN karty pro DPPC a také proto, že v době upgradu ISDN byl v ČR kladen větší důraz na rozvoj mobilních sítí, které ISDN plně předběhly.[3]

#### **2.3.4.2 Sítě mobilních operátorů GSM**

Pro posílání poplachových informací z objektů na DPPC se dá využít síť GSM – mobilních operátorů (Global System for Mobile Communications). Připojení GSM je používáno hlavně v objektech bez telefonní linky a tam, kde využití rádiového přenosu není vhodné. Systém přenosu dat se vyvinul hlavně pro provoz sítí GSM. Mobilní síť druhé generace tvoří soustava stanic provozovaných na frekvenci 0,9/1,8 GHz.

Nevýhodou je dost vysoká cena za kontrolu spojení, protože mobilní operátoři si stanovují vysoké tarifní ceny, a tudíž nedochází k tak častým kontrolním spojení, jak by bylo zapotřebí. Cenově výhodnější je posílání dat s využitím systému GPRS, kde je už za menší měsíční paušál možné poslat libovolný objem informací.

GPRS je mobilní datová služba dostupná pro uživatele GSM sítě. GSM komunikátor má za úkol odesílat na DPPC jakékoliv změny na vstupu a také pravidelné zprávy ke kontrole.

Tento typ přenosu dat je perspektivní, protože nabízí zákazníkům vysokou kvalitu pokrytí a nízké provozní náklady v souladu s ceníkem hlasových přenosů. Výhodou je také dvousměrná komunikace mezi stanovištěm poplachových přijímacích center a modulem GPRS instalovaným v objektu, který má více než 99% pokrytí na území EU.

GPRS je paketově přepínané, což znamená, že více uživatelů sdílí stejný přenosový kanál a data se přenášejí, pouze když jsou odeslána. Celková kapacita linky může být okamžitě vyhrazena těm uživatelům, kteří zrovna posílají data, což poskytuje vyšší prostupnost tam, kde uživatelé posílají nebo přijímají data periodicky, např. prohlížení webových stránek, okamžité přijímání e-mailů, chatování. To jsou příklady, kde se využívá občasný přenos dat, což prospívá sdílení dostupné kapacity.

GPRS specifikace zahrnuje podporu protokolů IP, PPP, OSPIH a X.25. Poslední z nich se používá pro aplikace jako například bezdrátové platební terminály a bankomaty, ačkoliv byl odebrán z důvodů požadavků standardu. X.25 je stále podporován přes PPP nebo přes IP, což má ovšem za následek nutnosti používání routerů nebo zapouzdření přímo do koncového terminálu. V praxi podporují operátoři na GPRS pouze IP a někdy také PPP.

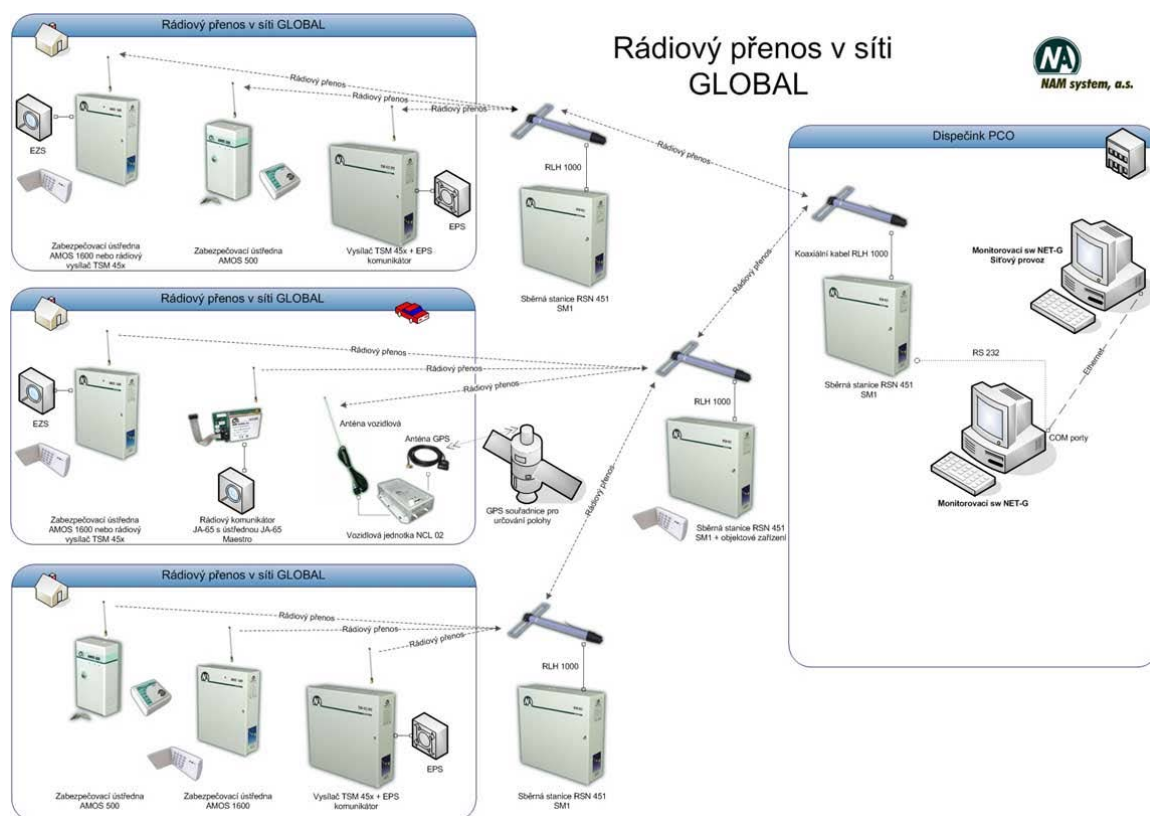
V době poruchy přenosu informace přes GPRS se modul automaticky přepne ze zajištěné přenosové trasy na náhradní a pošle zprávu o výpadku GPRS přenosu.

Na straně DPPC je nainstalován GSM přijímač, který přijímá zprávy ze sítě GPRS. Přijímač může ihned po příchodu SMS z objektu odeslat zprávu na telefonní číslo zadané v systému. Takové řešení umožňuje shrnutí všech informací o stavu bezpečnostního systému v objektu.[13]

### **2.3.4.3 Rádiový přenos**

Jedná se o další přenosovou trasu pro přenos poplachových zpráv z ústředí PZTS na DPPC. Ke zřízení této přenosové trasy je nutné mít povolení od Českého telekomunikačního úřadu, který povoluje zřízení a vybudování vlastní rádiové sítě a provoz na určených frekvencích. Vybudování vlastní rádiové sítě klade nároky jak na čas, tak na finance. Aby se mohl objekt připojit prostřednictvím rádiové sítě, měří se v objektu rádiový signál, který zajišťuje spolehlivý přenos dat. Nejlepší podmínky pro provoz sítě jsou při umístění vysílače v rovinném prostředí, s náročnějším terénem rostou náklady na postavení kvalitní síťové stanice a celkové náklady na provoz rádiové sítě. U zákazníka se

montuje vysílač nastavený na frekvenci provozovanou společností DPPC. Výhodou pro zákazníky je, že provoz sítě a přenos dat na DPPC je zdarma. Výhodou je také kontrola spojení s objektem, která se provádí jedenkrát za minutu. Takové řešení je vhodné pro objekty, které vlastní telefonní linku buď vůbec nemají, nebo je hodně poruchová. Rádiové sítě používají duplexní přenos a vysílače v objektech mají funkci retranslační stanice v případě nutnosti delšího dosahu pokrytí od základny.



Obr. 3 Schéma rádiové sítě GLOBAL od fy. NAM [8]

Nevýhodou je riziko výskytu rádiových rušičů. Provozovateli DPPC je signalizována okamžitá ztráta rádiového spojení vysílače s obslužným centrem, ale neví, zda je objekt ohrožen napadením. Při velkém počtu napojených objektů to pak působí obrovské problémy a každá poplachová zpráva se musí složitě kontrolovat. [2]

#### 2.3.4.4 Datový spoj – internet

Do bezpečnostních systémů a všeobecně do společnosti přinesl internet nové možnosti. Umožňuje například posílání dat do systémů DPPC včetně obrazové a hlasové kontroly stavu objektů. V DPPC díky internetu vznikla možnost vzdálené kontroly objektů.

Společnost tím ušetří obrovské náklady spojené s nepotřebnými výjezdy bezpečnostní jednotky.

Internet využívá dva základní typy transportních protokolů:

**TCP** - (Transmission Control Protocol) je jedním ze základních protokolů, konkrétně představuje transportní vrstvu. Použitím TCP mohou aplikace na počítačích propojených do sítě vytvořit mezi sebou spojení, přes které mohou přenášet data. Protokol garantuje spolehlivé doručování a doručování ve správném pořadí. TCP také rozlišuje data pro vícenásobné, současně běžící aplikace (například webový server a emailový server) běžící na stejném počítači.

**UDP** – (User Datagram Protocol) je jedním ze sady protokolů internetu. O protokolu UDP říkáme, že nedává záruky na datagramy, které přenáší mezi počítači v síti. Někdy je označován jako nespolehlivý, ale to je velmi zavádějící označení. Na rozdíl od protokolu TCP totiž nezaručuje, zda se přenášený datagram neztratí, zda se nezmění pořadí doručených datagramů nebo zda se některý datagram nedoručí vícekrát.

Protokol UDP je vhodný pro nasazení, které vyžaduje jednoduchost nebo pro aplikace pracující systémem otázka-odpověď (např. DNS, sdílení souborů v LAN). Jeho bezstavovost je užitečná pro servery, které obsluhují mnoho klientů nebo pro nasazení, kde se počítá se ztrátami datagramů a není vhodné, aby se ztrácel čas novým odesláním (starých) nedoručených zpráv.

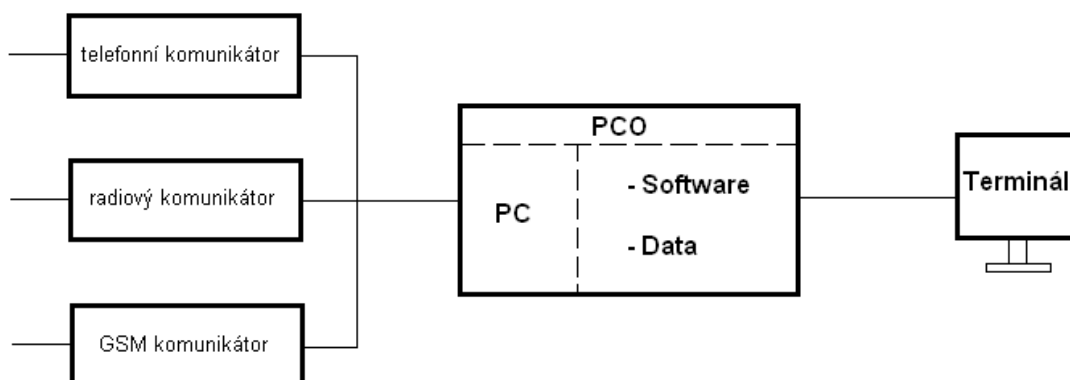
#### **2.3.4.5 Kombinovaný přenos**

Pro bezpečnější přenos dat se používá kombinace dvou druhů přenosů, které jsem výše představil. Ve většině případů se využívá varianta JTS a rádiový spoj, nebo JTS a GSM komunikace. Primární je například přenos zpráv po rádiové síti a paralelně nebo záložně po JTS. V době nedostupnosti kontrolní zprávy z objektů např. po uplynutí pěti minut, nebo pokud ústředna PZTS v objektu přijme potvrzení o zaregistrování vyslané zprávy, je použita náhradní přenosová trasa například prostřednictvím GSM. Toto opatření má ukázat, zda pachatel nevyřadil přenosovou cestu, aby zabránil odchodu zpráv na DPPC. Narušení dvou přenosových cest současně je velice nepravděpodobné. Pokud pachatel dokoná sabotáž (přestřihne nebo zruší telefonické vedení) ústředny PZTS tento zákrok zaznamenají a zašlou poplachovou informací na DPPC. V případě porušení rádiové cesty

vygeneruje DPPC informaci o odmítnutí přijetí kontrolní zprávy a v době napadení objektu je možné předat zprávu náhradním kanálem (JTS).

U všech objektů je důležité rozhodnout o vhodném typu přenosu přímo na místě v závislosti na technické i finanční situaci zákazníka. Instalaci a provozu zařízení včetně zvolení způsobu přenosu poplachových zpráv je třeba věnovat mimořádnou pozornost. Zákazník si dnes již může vybrat, který způsob přenosu poplachových informací využije pro svůj objekt. Důležitá je také vzdálenost objektu od DPPC. Pro vyšší spolehlivost a splnění pojistných podmínek se instalují dva typy přenosů pro případ přerušení trasy jednoho z nich.

Systémy se budují tak, aby informace o poplachu byla v co nejkratším čase přenesena, zpracována a správně vyhodnocena.



Obr. 4 Blokové schéma DPPC [3]

Zařízení DPPC je zobrazeno na obr. č. 4. Poplachové zprávy přicházejí z komunikátorů do DPPC, kde jsou zpracovány a zobrazeny na terminálu pro obsluhu. [3]

### 2.3.5 Zprávy na DPPC

Jedná se o zprávy, které jsou vysílány bezpečnostním systémem, instalovaným ve vzdáleném objektu. Vhodným programováním se definují typy a adresy zpráv, které budou vysílány z objektu a následně přijímány na DPPC.

1. Poplachové zprávy: jsou nejdůležitější informace přenášené z bezpečnostního systému a jsou z hlediska přenosu prioritní. Uživatelský software na DPPC

okamžitě zobrazí napadené místo a umístění detektoru, který hlásí poplach. Součástí poplachových zpráv je tzv. panik poplach (ohrožení zdraví nebo života). Dalšími typy jsou poplachu: sabotážní, požární, pohybový, otřesový.

2. Poruchové zprávy: jsou druhé nejdůležitější přenášené informace. Informují pracovníka DPPC o poruchách bezpečnostního systému. Jedná se zejména o tyto poruchy: porucha napájení, záložního zdroje, porucha sirény, výpadek telefonní linky. Operátor po přijetí těchto zpráv informuje obsluhu bezpečnostního systému případně servisního technika.
3. Testovací zprávy: bezpečnostní systém informuje v předem určených časových intervalech DPPC zprávou „Automatický test“, která oznamuje, že přenosová trasa je funkční.
4. Ostatní zprávy: Mají informační charakter, některé SBS je nepoužívají. Jedná se zejména o tyto zprávy: aktivace/deaktivace bezpečnostního systému, odemčení/uzamčení dveří, práce technika atd.

Uživatelský software odděluje typy zpráv barevným zobrazením a akustickou signalizací. Navíc ukládá a hlídá zprávy, kterými dispečer na přijetí poplachu reaguje. Tyto zprávy se nazývají „operátorské“ a jsou to například: voláno do objektu, vyslána zásahová jednotka, volána PČR, prohlídka objektu bez závad, příčina poplachu nezjištěna atd. [4]

### 2.3.6 Přenosové formáty

Přenosové formáty jsou programovány v ústřednách nebo komunikátorech PZTS. Jedná se vlastně o „kódovanou“ zprávu (informaci), kterou bezpečnostní systém předává po přenosové trase do DPPC. Na straně DPPC je zpráva přeložena (dekódována) a následně zobrazena na monitoru operátora. DPPC potvrdí bezpečnostnímu systému přijetí této informace.

Základní dělení přenosových formátů:

- Pulsní formáty:

Formát 3+1,3+1 – rozšířený, 3+2, 4+1, 4+1 – rozšířený, 4+2, 4+2 – rozšířený, 4+3, formáty z paritou.

- Tónové formáty:
  - Contact ID
  - DTMF
- Modemové formáty – SIA

Pulzní formáty se označují takové formáty, které pro přenos jednotlivých zpráv využívají určitého počtu pulsů v určitém čase. V České republice je jedním z nejrozšířenějších formátů 4+2 (první čtyři čísla znamenají číslo objektu + další dvě čísla jsou kód zprávy). Jde o tzv. pulzní formát vysílaný po analogové lince. Mezi analogové formáty patří např. 4+2,4+3,4+1 Ademco expres, Radionics. Všechny tyto formáty využívají přenosové rychlosti 1200,2400, 4600 bit/s a záleží jen na typu DPPC, se kterým formátem a rychlostí dokáže pracovat. Dalším druhem formátů jsou tzv. tónové, mezi které patří Contact ID, DTMF. Každá číslice má svou přiřazenou dvojici tónů určité frekvence. Těchto dvojic tónů je maximálně 16. Díky tomu se podstatně zkrátila doba vytáčení a spojení s volanou stanicí. Modemové formáty SIA to třetí typ přenosových formátů. Hlavní výhodou SIA formátu je časově krátký přenos více informací najednou. Z ústředny PZTS je většinou potřeba přenést jen jednu, zato důležitou zprávu. U SIA se požívá tzv. full – duplex přenos, data se přenášejí oběma směry (tj. i z PPC do PZTS), komunikace (až na přenosovou rychlost) velmi připomíná běžné modemy pro telefonní linky (28 800 bit/s). Data se přenášejí pomocí 1 a 0 (velmi připomíná starší způsob připojení na internet pomocí modemu). [12]

DPPC odpovídá ústředně dvěma signály, které jsou nazvány Handshake a Kissoff

### **2.3.6.1 Handshake**

Handshake generuje DPPC po zvednutí linky a potvrzuje ústředně připravenost přijmout data a průchodnost přenosové cesty. Handshake musí přesně časově a frekvenčně odpovídat následujícímu předpisu, jinak ústředna nezačne posílat data.[2]



Signál	Vyzvánění	Pauza	HANDSHAKE			Pauza	data
Linka vyzvednuta							
Linka položena							
	1	2	3	4	5	6	7
1	Vyzvánění na telefonní lince						
2	Prodleva před posláním handshake minimálně 0,5 sec maximálně 2 sec. Tato prodleva slouží pro ustálení telefonní linky po zvednutí						
3	Signál 1400Hz +/- 3% s trváním 100msec +/- 5%						
4	Pauza 100 msec +/- 5%						
5	Signál 2300 Hz +/- 3% s trváním 100 msec +/- 5%						
6	Pauza před posláním dat 250 msec – max 300 msec po doznění handshake nebo kissoff						
7	Posílání dat						

Obr. 5 Princip handshake [8]

### 2.3.6.2 *Kissoff*

Signál Kissoff oznamuje ústředně, že DPPC přijal zprávu bez chyb. Kissoff je tón v Hz (např. 1400 Hz) +/- 3 % s dobou trvání minimálně 750 msec – max. 1 sec. Ústředna musí detekovat minimálně 400 msec signálu Kissoff, aby byl signál vyhodnocen jako „platný“. Ústředna akceptuje odchylku frekvence +/- 5% pro zpětnou kompatibilitu.

Pokud ústředna nevyhodnotí Kissoff musí zprávu poslat minimálně 4x a teprve potom může telefonní linku položit a vytáčet znovu. Čítač posílání zpráv je pro každou zprávu samostatný a je resetován vždy po zachycení signálu Kissoff.

Bezpečnostní ústředny využívají hexadecimálního (šestnáctkového) kódování. [2]

### 2.3.6.3 *Počet pokusů*

Pokud ústředna nevyhodnotí Kissoff musí zprávu poslat minimálně 4 krát a teprve potom může telefonní linku položit a vytáčet znovu. Čítač posílání zpráv je pro každou zprávu samostatný a je resetován vždy po zachycení signálu Kissoff. [2]

### 3 LEGISLATIVA

#### Dohledové a poplachové přijímací centrum

Obecně vžitá termíny:

- Poplachové Přijímací Centrum (PPC)
- Multimediální Dohledové Centrum (MDC)

Mezinárodní zkratka

- ARC (Alarm Receiving Centre)

#### 3.1 Základní zásady provozu DPPC

Základní zásady provozu DPPC jsou:

- Přenosová cesta musí být kontrolována nejméně jednou za 24 hodin (u zařízení stupňů zabezpečení 3 a 4 musí být ztráta spojení signalizovaná na DPPC i na objektovém zařízení).
- U PZTS stupňů 3 a 4 nesmí být, v případě ztráty spojení, možné uvést systém do stavu střežení.
- Při napojení zařízení stupňů 1 a 2 na telefonní linky nebo po síti GSM se připouští kontrola spojení jednou za 24 hodin, povinné je však trvalé hlídání napájecího napětí na lince nebo trvalá kontrola přítomnosti GSM signálu.
- U systémů sloužících pro přenos poplachových zpráv z objektu stupně 3 a 4 je dále předepsaná náhradní přenosová cesta, která musí být stejně spolehlivá jako cesta hlavní.
- Je-li pro přenos na DPPC použit rádiový signál, musí být spojení kontrolováno nejméně 1krát za 5 minut.
- Je-li pro přenos na DPPC používaná telefonní linka, musí být jej stav trvale hlídán a výsledek musí být signalizován jako poruchový stav nejdéle do dvou minut. Pro přívod má být použit zemní kabel vstupující do objektu pod zemí a v objektu by měl procházet skrytě (pod omítkou), případně musí být veden zabezpečenými prostory.

- Skříně telefonního rozvodu musí být opatřeny sabotážními kontakty napojenými na PZS na 24 hodinové smyčce.

Kromě požadavku normy ČSN EN 50-131-1 a její národní přílohy na přenos signálů na DPPC a provoz DPPC upraven normami řady ČSN EN 50 136, např. ČSN EN 50 136-2-2 a ČSN EN 50 136 1-4. [4]

DPPC je centrum s trvalou obsluhou, do nějž jsou podávány informace týkající se stavu jednoho nebo více poplachových systémů. (EN 50136-1:200X, 4.1.2) s účinností od 1. 1. 2011 je v České republice fungování DPPC upraveno normou ČSN EN 50518, kterou připravila technická komise CENELEC (evropský výbor pro normalizaci v elektrotechnice).

Norma se skládá z 3 částí:

- ČSN EN 50518 – 1 Umístění a konstrukční požadavky (prosinec 2010)
- ČSN EN 50518 – 2 Požadavky na technické řešení (srpen 2011)
- ČSN EN 50518 – 3 Pracovní postupy a požadavky na provoz (leden 2012)

### 3.2 ČSN EN 50518 – 1

V této části normy EN 50518 se stanovují minimální požadavky na návrh, konstrukci a funkční zařízení pro budovy, v nichž se uskutečňuje monitorování, příjem a zpracování (poplachových) signálů generovaných poplachovými systémy jako integrální část celkového procesu zajištění bezpečí a zabezpečení. Požadavky se vztahují jak na případy dálkové konfigurace, v nichž více systémů přenáší informace do jednoho nebo více poplachových přijímacích center (PPC), tak na případy jednoho centra určeného pro monitorování a zpracování poplachů generovaných jedním nebo více poplachovými systémy, nalézajícími se v témže perimetru příslušného místa.

Podle normy musí být DPPC situován v místě s nízkým rizikem požáru, výbuchu, zaplavení, vandalismu a nebezpečí hrozícího z jiných míst. V případě, že DPPC není jediným uživatelem objektu, v němž je umístěno, musí být od zbytku budovy odděleno fyzickou bariérou, sestávající ze stěn, podlah, stropů a nezbytných otvorů.

Při volbě místa pro umístění DPPC se posuzují rizika, pak se může uvnitř objektu instalovat systém v místě dostupném pro provozního pracovníka DPPC. Norma obsahuje

kapitolu 5, ve které je stanoveno přesné stavební řešení. Podkapitoly obsahují informace o konstrukci, odolnosti a ochraně DPPC, o tom, jaké příslušenství se má v takových centrech nacházet, jaké mají být hranice otvorů v místnostech a jejich technologická pokročilost. Norma popisuje vstupní předsíň do DPPC, ale i to, jak má být vybavena, jaké má mít zabezpečení dveří, jaké zamykací mechanismy se mají použít, kde má být umístěn nouzový východ, jakou odolnost mají mít zasklené plochy a přesně stanovují možnost použití ventilace v objektech. V části poplachových systémů DPPC se dozvíme, že elektronická detekce pro všechny základní části DPPC musí postihovat následující události: útok zvenčí, požár, vchod a východ, plyn, komunikace, tiseň, monitorování bezpečnosti personálu, signalizaci elektronických ochranných systémů, CCTV. Veškeré systémy uvedené v kapitole poplachových systémů DPPC musí být udržovány podle požadavků příslušných norem. V případech, kdy normy neexistují, se musí údržba provádět podle směrnic výrobce tak, aby byla zaručena trvalá spolehlivost. Norma v poslední kapitole stanovuje napájení DPPC elektrickým proudem. V první kapitole omezuje a upřesňuje použití síťového napájení a v následující kapitole se zmiňuje o záložních zdrojích napájení. Tak se dozvíme, že síťové napájení musí být dostatečně chráněné před požárem, mechanickým poškozením a dimenzováno tak, aby byl zajištěn stálý dostatečný příkon pro všechna zařízení DPPC. [5]

### 3.3 ČSN EN 50518 – 2

ČSN EN 50518 – 2 je evropská norma, která se vztahuje na veškerá dohledová a poplachová přijímací centra, která monitorují a/nebo přijímají a/nebo zpracovávají signály vyžadující okamžitou reakci.

Druhá část normy ČSN EN 50518 stanovuje technické požadavky týkající se DPPC. Dále zahrnuje funkční kritéria a ověřování výkonnosti. V normě se píše, že poplachové přijímací zařízení a zdroje musí zajišťovat následující výkonnost:

Čas mezi časem přijetí výstupního signálu z komunikátoru přijímacího centra do indikačního zařízení a časem počátku události musí splňovat následující výkonnostní kritéria:

- v případě tísňových poplachů: 30 s u 80 % přijatých signálů a 60 s u 98,5 % přijatých signálů,

- v případě všech ostatních poplachů: 90 s u 80 % přijatých signálů a 180 s u 98,5 % přijatých signálů,

Souladu s výše uvedenými kritérii musí být dosaženo v průběhu dvanácti po sobě jdoucích měsíců.

V požadavcích na komunikaci se klade důraz na to, aby DPPC disponovala zařízením, které zálohuje data posílané do DPPC po dobu min. 3 měsíců. Stanovuje také obsah příchozích signálů a popis práce dispečera při přijímání informací zasílaných na DPPC. Norma dále nařizuje testování zařízení potřebných při provozu DPPC a zálohování dokumentace o provedených testech. Zařízení musí být synchronizované se světovým časem (UTC) a kontrola synchronizace se musí provádět minimálně jednou za 24 hodin. V normě se věnuje pozornost evropské směrnici o ochraně osobních údajů. Její dodržování je povinné v následujících oblastech:

- údaje o zákazníkovi,
- údaje o vnější komunikaci DPPC,
- záznamy o zákrocích dispečera.

Výše uvedené údaje jsou uschovávány po dobu odpovídající požadavkům v normě: údaje o klientovi a o zákrocích dispečera po dobu 2 let, informace o komunikaci DPPC po dobu 3 let.

Poslední kapitola normy stanovuje, že v případě vyřazení DPPC z činnosti musí být připravený vypracovaný nouzový plán pro vypořádání se s následky. [6]

### 3.4 ČSN EN 50518 – 3

ČSN EN 50518 – 3 se vztahuje na všechna dohledová a poplachová přijímací centra, která monitorují a/nebo přijímají a/nebo zpracovávají signály vyžadující okamžitou reakci. Tato část normy EN 50518 stanovuje minimální postupy a požadavky na provoz DPPC. Přijímací poplachová centra musí být trvale obsazena nejméně dvěma dispečery. Pokud je DPPC provozovno současně s jiným DPPC a provozní postupy zajišťují stejný efekt jako u DPPC obsazeného dvěma dispečery, je tento požadavek splněn. Norma stanovuje, jaké vzdělání musí mít člověk, aby mohl pracovat v prostředí DPPC. V každém centru se musí nacházet provozní dokumentace, která obsahuje předpisy pro provozní postupy.

Taková dokumentace musí být dostupná všem bezpečnostním pracovníkům a obsahovat postup pro testování, vstup do DPPC a odchod z DPPC, správu databází, provozní kontinuitu a nouzové stavy, evakuační postupy, zpracování signálů.

Pro soubor EN 50518 musí být proveden audit. Audit podle norem musí být proveden každoročně akreditačním orgánem podle EN 45011 nebo EN-ISO/IEC 17020. Za případné odchylky od normy pak odpovídá vedoucí DPPC, který je zodpovědný také za odstranění zjištěných chyb. Vedoucí je zodpovědný také za normu na vypracování postupu pro zacházení, údržbu, ukládání, likvidaci a vedení zákaznických údajů. Při elektronické archivaci údajů musí být všechny údaje bezpečně ukládány a musí být zavedeny zálohovací postupy. [7]

## 4 VÝVOJ SYSTÉMŮ DPPC

S přihlédnutím k okolnostem dalšího možného vývoje lze očekávat, že provozovatelé DPPC budou v rámci snižování provozních nákladů stále častěji tíhnout ke komplexním softwarovým řešením, jakým je např. Kronos NET. Je dost dobře možné, že se dočkáme vzniku celostátních DPPC, které se budou snažit provádět akvizice, a jejich podíl na trhu se bude zvětšovat. U klasických regionálních provozovatelů DPPC bude stálá poptávka po výjezdových silách a výnos z nich bude tvořit významnou část celkového obrátu.

Pro získání nových zákazníků se budou stále více využívat moderní marketingové nástroje, které známe z trhu se spotřebním zbožím (prodej zařízení na splátky, zapůjčení zařízení na dobu trvání smlouvy apod.). V úvahu připadají také doplňkové služby, o které zákazník bude mít zájem a které bude možné obchodně realizovat (střežení vozidel, internet providing, časově omezené střežení objektu, řízení ovládání spotřebičů v objektech apod.).

V oblasti komunikací dochází ke stálému rozšiřování možností prostřednictvím rozvíjejícího se internetu. Tato síť nabízí obrovské možnosti přenosu dat, a proto je stále více využívána i v PKB. Proto lze v přenosových cestách mezi střeženými objekty a DPPC očekávat patrný a stále větší odklon od analogových linek na úkor radia, GPRS, internetu a dalších novějších technologií. Výrobci se budou snažit vylepšit technologie tak, aby správa přenosových tras byla pro provozovatele co nejjednodušší a počet výpadků co nejnižší (automatická konfigurace sítě, redundantní provoz, automatické testování atd.). Nelze přesně odhadnout, kam se bude internet dále odvíjet, má však on určitou nevýhodu, a to je možnost napadení virovými a jinými škodlivými aplikacemi. Ale díky novým technologiím se počítá se vznikem provozu bezpečného a cenově přijatelného systému.

Co se týká současného stavu monitorovacích softwaru moderních DPPC, tak ten je nadčasový a mnozí provozovatele nevyužívají veškeré jeho možnosti ani z poloviny. Očekává se, že další vývoj bude stále víc směřovat do oblastí internetu. S rostoucím množstvím zpracovávaných informací je třeba využívat programy s databázovým jádrem, grafickými podklady a možností dálkového ovládání jednotlivých technologií. Díky rozdílným přístupům společností se prostředí DPPC přizpůsobuje těm technologiím, které daná firma přímo vyvíjí a aplikuje do objektů. Výrobci DPPC většinou propagují vlastní software navrhnutý pro zpracování signálů svých výrobků. Tyto programy se budou neustále rozšiřovat, jelikož se postupem času bude zpracovávat více informací a stavových

hlášení. Protože v nových tzv. inteligentních budovách jsou technologie nejrůznějších značek a výrobců, pro komunikaci bude tedy nutné, aby byl uživatelský software dostatečně kompatibilní, využíval příslušné standardy, přenosové formáty a dokázal tak všechny tyto technologie monitorovat a ovládat. Proto se předpokládá, že monitorovací software budou umožňovat přístup koncových uživatelů služeb k záznamům o provozu na jejich zařízeních (sestavám události, logům apod.). Správu u upgradu softwaru bude v rámci outsourcingu provádět specializovaná firma a provozovatele DPPC budou v budoucnu moci stále častěji přistupovat ke svým datům vzdáleně. [4]

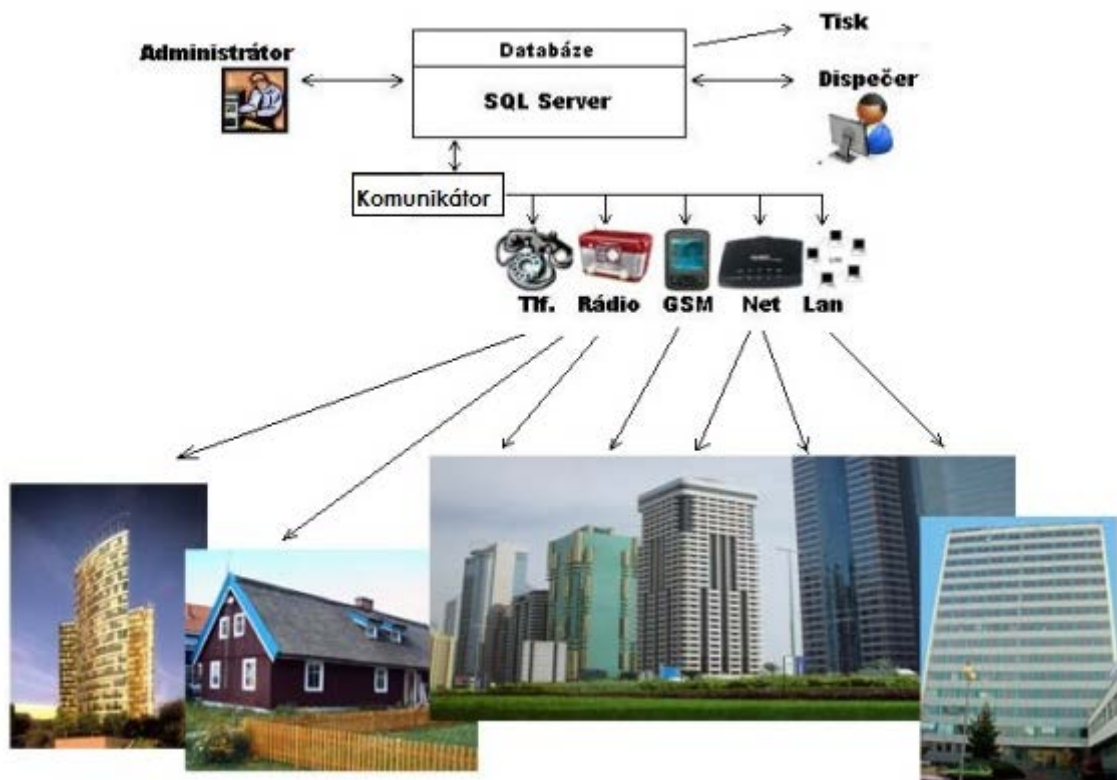


## **II. PRAKTICKÁ ČÁST**

## 5 POROVNÁNÍ SOFTWARE

Uživatelský software vznikl s potřebou rychle a bezpečně zpracovávat větší množství přijatých informací na DPPC. Jeho úkolem je jasně a přehledně zobrazovat přijaté zprávy tak, aby byl operátor schopen co nejrychleji reagovat na vzniklou událost. Důležitou vlastností je přehlednost a názornost zobrazované zprávy, zvukový doprovod, barevné odlišení dle důležitosti atd. Bývá doplněn o celou škálu dalších užitečných funkcí pro efektivnější práci. v současné době se do těchto aplikací promítá velké množství grafických prvků, jako jsou schémata, mapy, modely a fotografie pro přehlednější práci. Jádrem systému je databázová aplikace, která dokáže zpracovávat a bezpečně uchovat velké množství informací. Díky své spolehlivosti je často využíván Microsoft SQL Server.

Uživatelský software je stejně jako většina aplikací složen z několika modulů, které představují určité ovládací a funkční vlastnosti. Jednotlivé moduly lze do programu doinstalovat a rozšířit funkce celého systému. Každý tento modul zastává danou operaci (např. modul pro příjem zpráv, modul zastávající automatické funkce, modul dálkové komunikace, modul pro hromadné zpracování výpisů atd.).



Obr. 6 Schéma funkce střežení

Zprávy ze střeženého objektu jsou daným komunikačním kanálem přijaty ke zpracování příslušným modulem systému (modemem) a pomocí SQL Serveru uloženy do databáze. Zde jsou pod přihlášením uloženy tak, aby nedošlo k jejich neoprávněnému užívání.

Uživatelský software se v pravidelném časovém intervalu dotazuje databáze na aktuální stav. Jestliže je v databázi nový údaj, zobrazí se na monitoru obsluhujícího pracovníka.[3]

## 5.1 NET – G

Software NET-G pro monitorování se zrodil hlavně z narůstajících požadavků Policie České republiky a soukromých bezpečnostních služeb zpracovávat data z DPPC rychle a bezpečně, používat síťový provoz dispečinků, z potřeby skloubit dohromady hlídání objektů v metropoli se střežením a monitorováním umístění zásahových jednotek nebo s monitorováním technologických stavů atd.

Software NET-G je postaven na Inter-base SQL databázi, která je poměrně bezpečná, o čemž svědčí i její používání ve zdravotnictví a armádě USA. Tato SQL databáze umožňuje kdykoliv za plného provozu provést zálohování nebo využít možnosti provádět aktivní kopii databáze na jiný disk.

Podporován a zároveň doporučován je vzdálený přístup k systému přes modem, což umožňuje správci systému pracovat se softwarem při napojování objektů u zákazníka, nebo řediteli firmy přímo z bydlíště ze svého notebooku. Zároveň je společnost NAM, schopna servisně podporovat tento systém. [8]

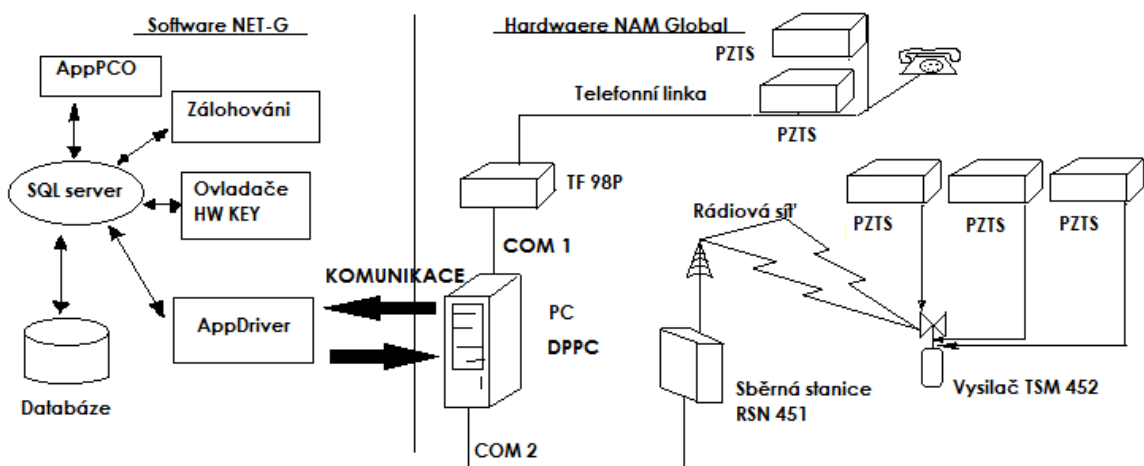
Software NET-G se skládá z několika modulů. Některé z nich jsou součástí hlavní instalace, některé jsou zvlášť samostatně placené. Kterýkoliv z těchto modulů lze kdykoliv doinstalovat a rozšířit tak možnosti celého systému. Základní moduly potřebné ke spuštění a ovládání softwaru NET-G jsou:

- **Modul AppPCO**
- **Modul AppDriver**

Přehled všech modulů:

- **Modul AppPCO** – hlavní dispečerský modul sloužící k obsluze, zadávání objektů, výpisům historie apod.
- **Modul AppDriver** – modul zabezpečující zpracování dat přijatých ze zařízení

- **Manuál NET–G** – kompletní manuál ve formátu HTML
- **Modul AppMail** – modul sloužící k hromadnému zpracování výpisů mailem, faxem, tiskem
- **Modul KeyAdministrator** – modul sloužící k dálkové konfiguraci HW klíče
- **Modul WatchDog** – modul sloužící k hlídání běhu všech zvolených programových součástí na jednom PC nebo na všech PC v síti
- **Modul ClientSiren** – modul slouží k záloze zvukové karty a reproduktorů. Krom houkání přes zvukovou kartu, houká tento modul pomocí interního reproduktoru PC.
- **Modul WatchDogTCP** – modul sloužící ke kontrole propustnosti PC sítě mezi jednotlivými počítači i s moduly NET–G.
- **Modul Statistika** – tento modul lze využít pro tvorbu statistických údajů z událostí. Modul vytváří tabulky a přehledné grafy v MS Excel.
- **Modul AppServis** – modul samostatně nepoužitelný, sloužící k distribuci dat pro následující servisy:
  - **Servis Print** – modul vznikl na základě požadavků ČSN. Pomocí tohoto modulu lze tisknout v režimu ON–LINE Vámi definované události.
  - **Servis Sound** – modul sloužící k přehrávání definovaných wav souborů a zároveň využívá COM port PC k zakličování rádiostanice, přes kterou se potom přenáší přehrávané zvuky. Používá se u tzv. bezobslužných DPPC.
  - **Servis SMS** – díky tomuto modulu se může automaticky při příchodu definované události na definovaný objekt odeslat Vámi připravená SMS na přednastavená telefonní čísla.
  - **Servis SMS+** – modul sloužící k hlídání bdělosti operátora a k hlídání času potvrzení důležité zprávy + tísňové volání operátora.
  - **Servis COM** – tento servis zajišťuje odeslání jakéhokoliv příkazu ve formátu RS 232 do sériového portu počítače. Vyvinut byl pro spolupráci softwaru NET–G s kamerovými systémy.

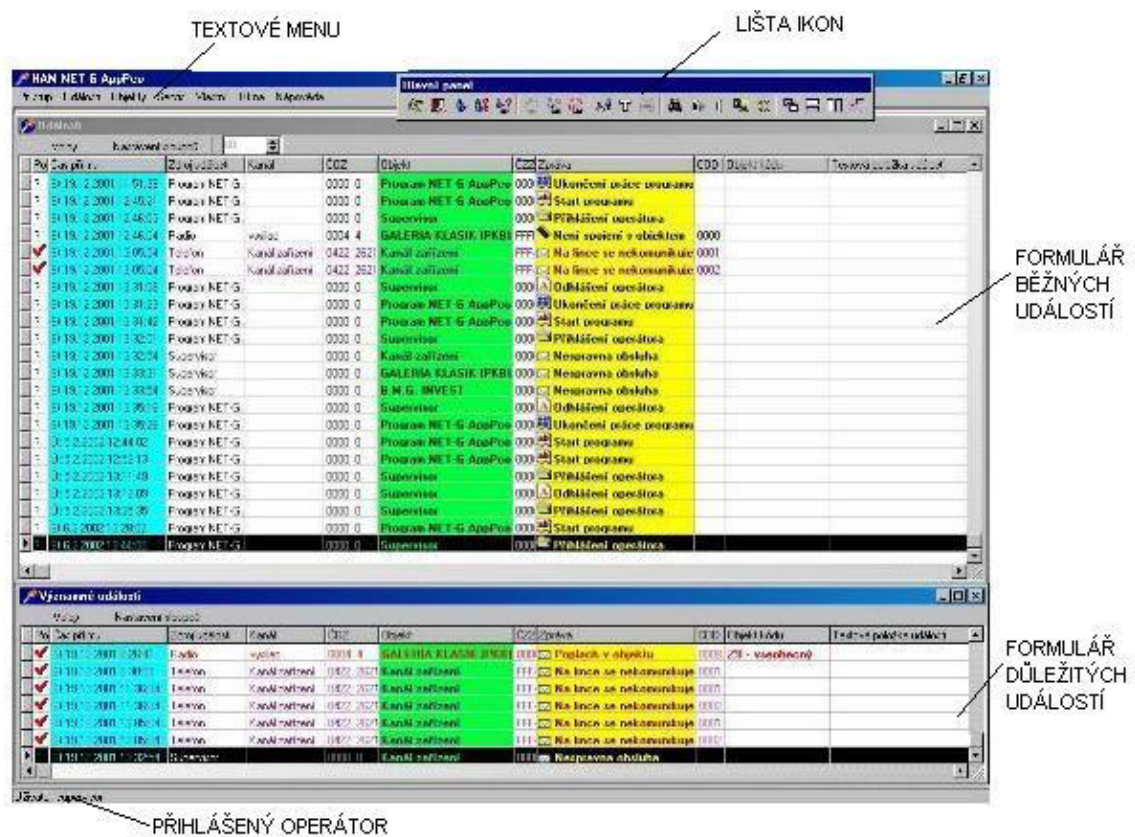


Obr. 7 Schéma architektury modulu NET-G a hardwaru NAM GLOBAL

Na schématu je znázorněna komunikační trasa od vzniku zprávy až po její zobrazení operátorovi. Zprávu generuje zabezpečovací ústředna PZTS a následně je přenesena buď pomocí integrovaného komunikátoru ústředny PZTS po telefonních linkách na kartu TF 98P nebo pomocí připojeného vysílače TSM 452 na sběrnou stanici RSN 451. Výstup z telefonní karty nebo sběrné stanice je připojen na COM port počítače s nainstalovaným NET-G. O vyčítání zpráv z připojených zařízení se stará modul AppDriver, který zprávu vyčte a pomocí SQL serveru ji uloží do databáze. Program AppPCO slouží jako zobrazovací software a umožňuje veškerou práci dispečera. AppPCO se neustále dotazuje pomocí SQL serveru do databáze. V případě, že je v databázi zapsaná nová zpráva, okamžitě ji zobrazí. Služeb SQL serveru využívá rovněž zálohovací program NET-G Backup, který umožňuje zálohovat databázi za chodu programů. Ovladač pro HW klíč, je ochranou proti neoprávněnému využití aplikace.

### 5.1.1 Modul AppPCO

Modul AppPCO slouží k monitorování přicházejících událostí, posouzení údajů posílaných ze střežených objektů. Po přihlášení uživatele se zobrazí výchozí obrazovka se dvěma okny a lištou ikon.



Obr. 8 Systémové okno [8]

Toto je základní obrazovka, ve které se operátoři pohybují po většinu času. Kliknutím na jednotlivé části se zobrazí příslušné informace.

### 5.1.1.1 Hlavní okna aplikace

#### Okno běžných událostí

V okně jsou zobrazovány příchozí události, které mají být zpracovávány na daném pracovišti. V ukázce je vidět průběžný stav událostí, které jsou operátorovi zobrazovány v tomto okně. Jsou v řádku barevně odlišeny podle důležitosti jednotlivých událostí. Můžou zde nastat tři stavy:

- černá barva – běžné události (odchody, příchody, periodické testy apod.)
- červená barva – POPLACHY, kromě optického odlišení tyto zprávy navíc aktivují zvuk sirény a vyžadují odbavení operátorem

- fialová barva – důležité události (výpadek sítě, porucha AKU apod.), kromě optického odlišení tyto zprávy navíc aktivují zvuk sirény a vyžadují odbavení operátorem

Při příchodu nové události je generován zvuk podle výchozího nastavení zvuku.

PO	Čas příjmu	Zdroj události	Kanál	ČOZ	Objekt	ČZ	Zpráva	CDD	Objekt kódu	Textová položka události
?	Si 19.12.2001 11:51:39	Program NET-G.		0000 0	Program NET-G AppPco	000	Ukončení práce programu			
?	Si 19.12.2001 12:45:21	Program NET-G.		0000 0	Program NET-G AppPco	000	Start programu			
?	Si 19.12.2001 12:46:03	Program NET-G.		0000 0	Supervisor	000	Přihlášení operátora			
?	Si 19.12.2001 12:46:04	Radio	vysílač	0004 4	GALERIA KLASIK (PKB)	FFF	Není spojení s objektem	0000		
✓	Si 19.12.2001 13:05:04	Telefon	Kanál zařízení	0422 2621	Kanál zařízení	FFF	Na lince se nekomunikuje	0001		
✓	Si 19.12.2001 13:05:04	Telefon	Kanál zařízení	0422 2621	Kanál zařízení	FFF	Na lince se nekomunikuje	0002		
?	Si 19.12.2001 13:31:06	Program NET-G.		0000 0	Supervisor	000	Odhlášení operátora			
?	Si 19.12.2001 13:31:23	Program NET-G.		0000 0	Program NET-G AppPco	000	Ukončení práce programu			
?	Si 19.12.2001 13:31:42	Program NET-G.		0000 0	Program NET-G AppPco	000	Start programu			
?	Si 19.12.2001 13:32:01	Program NET-G.		0000 0	Supervisor	000	Přihlášení operátora			
?	Si 19.12.2001 13:32:54	Supervisor		0000 0	Kanál zařízení	000	Nespravná obsluha			
?	Si 19.12.2001 13:33:31	Supervisor		0000 0	GALERIA KLASIK (PKB)	000	Nespravná obsluha			
?	Si 19.12.2001 13:33:54	Supervisor		0000 0	B.M.G. INVEST	000	Nespravná obsluha			
?	Si 19.12.2001 13:35:16	Program NET-G.		0000 0	Supervisor	000	Odhlášení operátora			
?	Si 19.12.2001 13:35:26	Program NET-G.		0000 0	Program NET-G AppPco	000	Ukončení práce programu			
?	Uř 5.2.2002 12:44:02	Program NET-G.		0000 0	Program NET-G AppPco	000	Start programu			
?	Uř 5.2.2002 12:52:13	Program NET-G.		0000 0	Program NET-G AppPco	000	Start programu			
?	Uř 5.2.2002 13:11:43	Program NET-G.		0000 0	Supervisor	000	Přihlášení operátora			
?	Uř 5.2.2002 13:12:09	Program NET-G.		0000 0	Supervisor	000	Odhlášení operátora			
?	Uř 5.2.2002 13:25:35	Program NET-G.		0000 0	Supervisor	000	Přihlášení operátora			
?	Si 6.2.2002 13:28:02	Program NET-G.		0000 0	Program NET-G AppPco	000	Start programu			
?	Si 6.2.2002 13:44:00	Program NET-G.		0000 0	Supervisor	000	Přihlášení operátora			

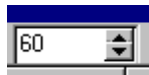
Obr. 9 Okno běžných událostí [8]


Na obrázku vidíme klasické znázornění se sloupci nastavenými pro optimální rozlišení. Význam jednotlivých sloupců je následující:

- PO (potvrzení) – u zpráv, které jsou důležité nebo poplachové se zobrazí zaškrtnutý znak jako informace o potvrzení události operátorem.
- Čas příjmu – zde se vypisuje skutečný čas příchodu dané události.
- Zdroj události – jedná se o to, jak byla zpráva přijata (rádiovou cestou, telefonní kartou, nebo zda byla zpráva vygenerována softwarem).
- Kanál – je upřesňující informace o příjmu událostí (u telefonní karty např. Linka 1 nebo Linka 2)
- ČOZ (číslo objektu na zařízení) – zde se objeví číslo objektu tak, jak bylo přijato. V levém sloupci ve formátu HEXa a v pravém ve formátu DEC.
- Objekt – textový překlad čísla objektu. Tento text je dispečerem definovatelný při definování objektu do NET-G.

- ČZZ (číslo zprávy ze zařízení) – jedná se o přijatý přenosový kód. v levém sloupci ve formátu HEXa a v pravém ve formátu DEC.
- Zpráva – opět textový překlad přenosového kódu. Překlad je závislý na použité převodní tabulce zpráv.
- COD – kód sloužící k dalšímu zpracování pro upřesnění příchozí informace. U formátu 4+1, 4+2, 4+3 tvořený kopírováním přenosového kódu, u formátu ContactID jde o skutečné upřesnění zprávy.
- Objekt kódu – upřesňující informace vztahující se ke zprávě. Např. při zprávě „ODCHOD z OBJEKTU“ se zde může objevit „UŽIVATEL Č. 1“.
- Textová položka události – operátoři mohou vkládat vlastní doplňující informace k příchozím událostem. Ty se potom zobrazují v tomto sloupci.

Každý tento sloupec lze upravit podle svých představ. Klepnutím levým tlačítkem myši na název sloupce se zobrazí okno umožňující nastavit vlastnosti sloupce.



Další pole, které je vidět na obrazovce, je . Toto pole zobrazuje, kolik událostí zpět se má uchovávat v okně běžných událostí. Pokud potřebujete z jakéhokoliv důvodu zachovat vyšší počet událostí, stačí jen přepsat toto číslo a provést obnovu dat. Nedoporučuje se ale tuto hodnotu přílišně zvětšovat, neboť při každé aktualizaci tohoto okna by docházelo k načítání velkého počtu zpráv, a tím i ke zpomalování systému.

**Nastavení sloupců** – po stisku tohoto tlačítka se zobrazí seznam všech sloupců, které lze v okně běžných událostí zobrazit. Pokud jsme si při nastavování vlastností jednotlivých sloupců omylem zrušili jeho viditelnost, můžeme jej zde opět zobrazit. Poslední volbou v tomto okně je „**Převzít nastavení z okna událostí/důl. událostí**“. Pomocí tohoto tlačítka můžeme provést překopírování nastavení sloupců z jednoho okna do druhého. Cílem kopírování je vždy okno, z kterého tuto volbu voláme.

**Volby** – po stisku se zobrazí následující nabídka:

- obnova dat – ruční aktualizace zobrazených dat. Doporučují se provést po změně hodnoty udávající počet zobrazených událostí.
- zachovat nalistovanou – pokud budeme v tomto okně vyhledávat nějakou starší zprávu a budeme rolovat v okně, tak při každé nově příchozí zprávě se kurzor automaticky nastaví na tuto novou zprávu. Zaškrtneme-li tuto volbu, kurzor nám bude stále stát na vámi vybrané zprávě.



- všechny události – některé události mohou být správcem systému nastaveny jako skryté, proto že nemají výraznější význam pro operátora. Jsou to například „poloha GPS“ apod. Vybráním této volby způsobíte jejich zobrazování v okně běžných událostí.

Pro zjednodušení práce operátora a pro zrychlení reakcí na jednotlivé podněty je možnost použití odkazů z událostí. Tuto možnost vyvoláme stiskem pravého tlačítka myši na zvolené události. Pro jednotlivé volby lze použít „rychlé klávesy“. Přehled těchto kláves je napravo od jednotlivých voleb.

	Pá 4.12.1998 6:55:36	Pracoviště PC01	Pult PC0
			CC01 Pult PC0
			CC01 Pult PC0
			CC01 Pult PC0
			CC01 Pult PC0
			CC01 Pult PC0
			CC01 Karta Ma
			CC01 Supervis
	Pá 4.12.1998 7:15:20	Pracoviště PC01	Program I
	Pá 4.12.1998 7:15:20	Pracoviště PC01	Program I
	Pá 4.12.1998 7:22:54	Pracoviště PC01	Program I

Obr. 10 Odkazů z událostí [8]

**ukaž pracoviště** – zobrazí podrobné informace a konfiguraci pracoviště, na kterém byla tato událost přijata a zpracována.

**ukaž zdroj** – zobrazí podrobné informace a konfiguraci zařízení, kterým byla tato událost přijata a zpracována.

**ukaž objekt** – rychlý skok na objekt, ze kterého byla událost přijata.

**objekt kódu** – rychlý skok na smyčku nebo na osobu, která byla identifikována jako zdroj události.

**vložení vlastní události** – tato volba umožňuje vložení vlastní informace operátora k události. Lze předdefinovat libovolný počet zpráv, které může operátor vložit, může si vybrat, zda chce událost přiřadit objektu, ze kterého tuto možnost zavolal, nebo k jinému objektu definovanému v systému. Dále lze doplnit vlastní operátorův text do třiceti znaků nebo v poli „vlastní rozsáhlý text“ bez omezení počtu znaků.

**informace o události** – zobrazí informace o čase potvrzení události a o operátorovi, který událost potvrdil.

### Okno významných událostí

V okně jsou zobrazovány příchozí události, které mají být zpracovávány na daném pracovišti, a které mají nastavenou úroveň jako Důležité nebo Poplach. V ukázce je vidět průběžný stav událostí, které jsou operátorovi zobrazovány v tomto okně.

Významné události						
Volby		Nastavení sloupců				
PRI	Po	Čas příjmu	Objekt	Zpráva	Objekt kódu	Čas zápisu
A	?	Po 11.02.2002 05:29:29	18 MŠ Moravská	☑ Poplach v objektu		11.02.2002 05:29:29
A	?	Po 11.02.2002 05:59:03	188 ZŠ Frýdecká	☑ Poplach v objektu		11.02.2002 05:59:03
A	?	Po 11.02.2002 06:35:36	172 MŠ Frýdecká	☑ Poplach v objektu		11.02.2002 06:35:36
A	?	Po 11.02.2002 06:37:01	172 MŠ Frýdecká	☑ Poplach v objektu		11.02.2002 06:37:01
G	?	Po 11.02.2002 07:06:50	SV HAV 3 Gymnázium	☒ Není spojení s objektem		11.02.2002 07:06:50
G	?	Po 11.02.2002 07:52:17	SV HAV 3 Gymnázium	☒ Není spojení s objektem		11.02.2002 07:52:17
G	?	Po 11.02.2002 08:41:08	SV HAV 3 Gymnázium	☒ Není spojení s objektem		11.02.2002 08:41:08
A	?	Po 11.02.2002 08:46:44	170 SMP Havířov komisariát 2	☑ Poplach v objektu		11.02.2002 08:46:44

Obr. 11 Okno významných událostí [8]

Při příchodu nové události je generován zvuk podle výchozího nastavení zvuku a zároveň je spuštěna siréna.

Na obrázku výše vidíme klasické znázornění, sloupce nastavenými pro optimální rozlišení. Význam jednotlivých sloupců je následující:

- PO (potvrzení) – u zpráv, které jsou důležité nebo poplachové se zobrazí zaškrťovací znak jako informace o potvrzení události operátorem.
- Čas příjmu – zde se vypisuje skutečný čas příchodu dané události.
- Zdroj události – jedná se o to, jak byla zpráva přijata (rádiovou cestou, telefonní kartou, nebo zda byla zpráva vygenerována softwarem).
- Kanál – je upřesňující informace o příjmu události (u telefonní karty např. Linka 1 nebo Linka 2)
- ČOZ (číslo objektu na zařízení) – zde se objeví číslo objektu tak, jak bylo přijato. v levém sloupci ve formátu HEXa a v pravém ve formátu DEC.
- Objekt – textový překlad čísla objektu. Tento text je dispečerem definovatelný při definování objektu do NET-G.
- ČZZ (číslo zprávy ze zařízení) – jedná se o přijatý přenosový kód. v levém sloupci ve formátu HEXa a v pravém ve formátu DEC.

- Zpráva – opět textový překlad přenosového kódu. Překlad je závislý na použité převodní tabulce zpráv.
- COD – kód sloužící k dalšímu zpracování pro upřesnění příchozí informace. U formátu 4+1, 4+2, 4+3 tvořený kopírováním přenosového kódu, u formátu ContactID jde o skutečné upřesnění zprávy.
- Objekt kódu – upřesňující informace vztahující se ke zprávě, např. Při zprávě „ODCHOD z OBJEKTU“ se zde může objevit „UŽIVATEL Č. 1“.
- Textová položka události – operátoři mohou vkládat vlastní doplňující informace k příchozím událostem. Ty se potom zobrazují v tomto sloupci.


Každý tento sloupec lze upravit podle uživatelských představ. Klepnutím levým tlačítkem myši na název sloupce se zobrazí okno umožňující nastavit vlastnosti sloupce.

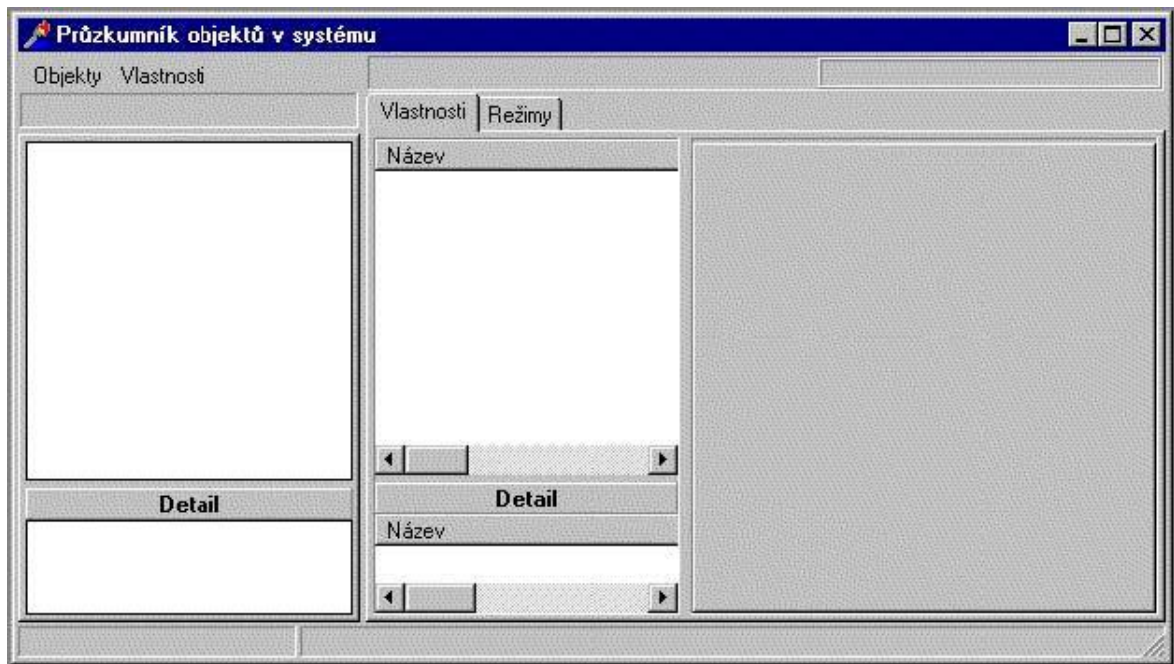
Následující možnosti takové jako „Nastavení sloupců“, „Volby“ a „Rychlé klávesy“ se používají stejně jako v předcházejícím okně běžných událostí.

### **Okno průzkumníka objektů**

Okno průzkumníka objektů je spolu s oknem událostí a oknem důležitých událostí nejdůležitějším oknem v aplikaci. Zvládnutí práce s tímto oknem a pochopení principů, podle kterých se v okně pracuje, je základním předpokladem zvládnutí ovládnání celé aplikace. Toto okno má hlavně organizační funkci, to znamená, že pomáhá udržovat objekty – přidávat, upravovat, sledovat aktuální stav jejich vlastností, apod.

Nejprve je nutné si uvědomit, že pojmem objekt není myšlen pouze hlídaný objekt, ale objekt obecně, tzn. například počítač, operátor, čidlo i hlídaný objekt. Jak je patrné, tyto objekty jsou různého typu a mají přiřazeny různé vlastnosti různých typů – s typy se pracuje prostřednictvím okna průzkumníka typů. Okno průzkumníka objektů lze otevřít

klepnutím na ikonu na liště ikon  nebo klávesou F4.



Obr. 12 Okno průzkumníka objektů[8]

Pro práci s objekty je potřeba načíst celou strukturu do okna. Toto lze provést pomocí menu **Objekty|Načti strom...**

**Menu vlastnosti** – kliknutím se zobrazí nabídka:

- načti vlastnosti objektu – znovunačtení vlastností objektu na kterém stojíme
- najdi vlastnost typu – slouží pro vyhledání určitého typu vlastnosti u objektu
- bez formulářových – u každého objektu jsou určité vlastnosti, které jsou obsahem formuláře objektu. Standardně nejsou běžně vidět jako jednotlivé položky, ale pouze jejich obsahy. Zrušením tohoto zaškrtnutí zobrazí tyto vlastnosti.
- bez status – touto volbou lze vypnout zobrazování informačního řádku, který zobrazuje název, typ a číslo vlastnosti v systému.

**Menu objekty** – po kliknutí se rozbolí volba:

- načti strom objektů – tuto volbu je nutno provést vždy při prvním otevření „okna průzkumníka objektů“. Pomocí tohoto menu provedete načtení objektů, jejich vlastností a obsahů.

Tímto úkonem se vyplní strom objektů, který znázorní strom objektů. Okno průzkumníka objektů je rozděleno na tři části:

- Okno objektů

- Okno vlastností
- Okno obsahu vlastností

### **Okno objektů**

Při návrhu aplikace se vycházelo z toho, že počet objektů není omezený a že mohou být jeho počty různé. Proto bylo nutné navrhnout vhodnou strukturu, která jednoduchým a přehledným způsobem zorganizuje velké množství objektů. Byla přijatá stromová struktura, která je aplikována i v jiných oknech aplikace.

Každému uživateli se zobrazí ve stromu pouze objekty, které má přístupné – na které má přiděleno právo. Pouze supervizor má implicitně vždy zobrazeny všechny objekty definované v systému, nicméně i ostatní uživatelé mohou mít zobrazeny všechny objekty v případě, že mají takové práva.

Pokud má se na to právo, může se měnit strukturu stromu objektů, tzn. přidat, opravit nebo zrušit objekt. K těmto akcím se dostane přes menu, které se objeví, pokud se stiskne pravé tlačítko (Oprav objekt..., Přidej objekt..., Vymaž objekt...). Veškeré tyto akce se pak provádějí prostřednictvím průvodce. v celém programu se díky stromové architektuře lze setkat s výrazy „Nadřazený objekt“, „Objekt na stejné úrovni“, „Podřazený objekt“. Je to dáno zařazením objektu do stromové struktury.

### **Okno vlastností**

Každý objekt má určitý počet různých druhů vlastností. Seznam jednotlivých vlastností se zobrazí po kliknutí na vybraný objekt v prostředním sloupci „okna průzkumníka objektů“. I zde se zobrazí pouze ty vlastnosti, ke kterým má daný operátor právo přístupu a viditelnosti. Pokud má se právo, může se provádět úpravy v tomto seznamu, tzn. akce Oprav vlastnost..., Přidej vlastnost..., Vymaž vlastnost... Tyto operace jsou opět přístupné prostřednictvím menu, které se objeví po stisku pravého tlačítka myši nad tímto panelem. Veškeré akce se provádějí prostřednictvím příslušného průvodce.

Jak dá se zjistit, mají některé typy vlastností částečně upraven vzhled stránek svých průvodců (jedná se především o „odkazové“ typy, kdy se jako přípustné hodnoty vlastnosti nabízí pouze objekty typově odpovídající těmto vlastnostem). Na druhé straně existuje také

velká skupina typu vlastností, která používá průvodce univerzálního. Významy jednotlivých vlastností budou popisovány dále v manuálu.

### **Okno obsahu vlastností**

Většina vlastností má své hodnoty, kterými blíže charakterizuje daný objekt. Jejich zobrazení se liší závislosti na typu dané vlastnosti a některé typy vlastnosti ani svoji hodnotu nezobrazují.

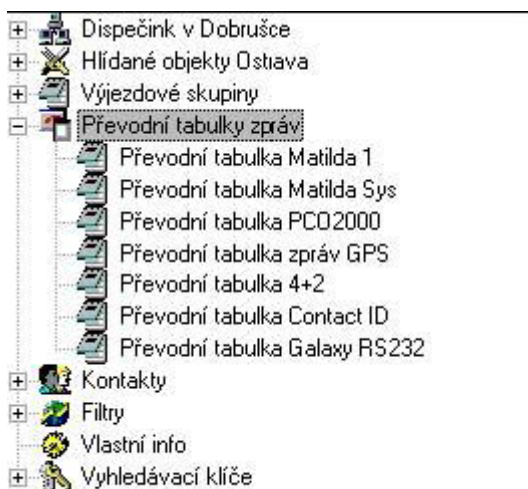
Pokud nemá vlastnost definované rozhraní, je o tom informován příslušným textem.

Vybráním jiné vlastnosti dojde k zápisu změny provedené na předchozí vlastnosti. Představení rozhraní všech typů vlastností by bylo zdlouhavé a navíc stále není a asi nikdy nebude konečný jejich počet (bude se podle potřeb doplňovat). Plyne to z principu, který charakterizuje celou aplikaci, kdy se snažilo zachovat maximálně možné otevřenou cestu a neklást zbytečná omezení.

#### **5.1.1.2 Převodní tabulky**

##### **Definice převodních tabulek**

Převodní tabulky zpráv tvoří speciální větev v hierarchii objektů – jsou uspořádány pod objektem typu Převodní tabulky zpráv. Příkladem takového uspořádání může být například následující hierarchie:



Obr. 13 Převodní tabulka[8]

Lze vytvořit neomezený počet převodních tabulek – objektů typu Převodní tabulka zpráv. Princip převodní tabulky je zřejmý: převádí číslo zprávy, která přijde na nějaké zařízení na číslo zprávy, která je definovaná v systému NET-G AppPCO.

Například: ke každému zařízení by měla existovat právě jedna převodní tabulka. K objektu typu Převodní tabulka zpráv je nutné pro každou zprávu definovat vlastnost typu Převod čísla zprávy, jejímiž hodnotami jsou číslo příchozí zprávy a číslo zprávy v systému.

Pomocí množiny převodních tabulek zpráv lze pak jednoduše sjednotit zprávy přicházející pod různými čísly na různých zařízeních na jednotné číslo zprávy, které je definováno v systému – viz průzkumník číselníku zpráv.

To znamená, že chceme-li v převodní tabulce převést nějakou zprávu, musíme ji nejprve mít nadefinovanou v číselníku zpráv.

S tabulkami můžeme manipulovat a to přes:

- Tvorbu převodní tabulky zpráv rozšířenou editací,
- Export a import převodních tabulek,
- Spojení 2 tabulek.

### **5.1.1.3 Defínování hlídaného objektu**

Systém NET-G je určen pro monitoring a zpracování událostí v napojených hlídaných objektech zákazníků bezpečnostní agentury.

#### **Větev hlídaných objektů**

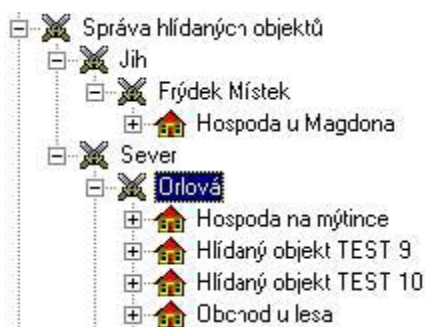
Nejprve musíme si uvědomit, podle jakých pravidel jsou v průzkumníku objektů vytvářeny objekty ve větvi hlídaných objektů.

#### **Typy objektů**

Větev hlídaných objektů lze definovat podle schématu předdefinovaných typů ve větvi hlídaných objektů. Tyto typy určují vazební poměry při definování jednotlivých položek v této větvi.

#### **Definované objekty**

Na obrázku č.15 je vidět příklad definované větve hlídaných objektů tak, jak ho lze nadefinovat v Průzkumníku objektů v systému.



Obr. 14 větve hlídaných objektů [8]

V hierarchii je v tomto případě na vrcholu objekt Správa hlídaných objektů stejnojmenného typu. Podřízené objekty typu Oblast hlídaných objektů jsou vytvořeny dva s názvy Jih a Sever. Pod těmito oblastmi jsou objekty typu Skupina hlídaných objektů s názvy Frýdek Místek a Orlová. Pod nimi jsou vytvořeny již konečně objekty typu Hlídaný objekt s názvy Hospoda u Magdona nebo Hospoda na mýtince a další.

### **Přidání objektu**

Objekty je možno definovat dvěma způsoby podobně jako Převodní tabulky zpráv:

- Ručním vkládáním vlastností a objektů
- Rozšířenou editací

### **Přidání objektu do stromové architektury**

Postup přidání hlídaného objektu je obdobný jako přidání jakéhokoliv objektu ve stromové struktuře systému. Pomocí pravého tlačítka myši vyvoláme na nadřizovém nebo typově stejném objektu menu a volbou Přidej objekt... vyvoláme průvodce.

V průvodci zvolíme Přidání podřízeného. Automaticky se zobrazí možné typy k přidání. Vybereme daný typ: např. Hlídaný objekt, a se přesuneme na další stránku průvodce, kde opravíme název objektu. Na další stránce pak už jen potvrdíme přidání objektu.

Ve struktuře větve se objeví uživatelem nově nadefinovaný objekt typu Hlídaný objekt. Je vytvořen automaticky se všemi vlastnostmi a pod objekty, které jsou v typech definovány jako automatické. Automaticky se tedy vytvoří všechny formulářové vlastnosti a vlastnost formulář, do něhož můžeme ihned zadávat údaje.



Editací můžeme rozšířit a to tak, že ve stromě objektů se klikne na hlídaný objekt pravým tlačítkem myši a z nabídky vyberte Rozšířená editace. Otevře se nám okno, ve kterém se může nastavit například: název objektu, zakláni vlastnosti objektu.

Rozšířená editace obsahuje záložku „Připojení“ umožňuje ona editace jednotlivých připojení objektu na kanály. V levé části je výběr jednotlivých připojení a vpravo pak parametry těchto připojení. Jednotlivá připojení je možno přidávat nebo rušit pomocí menu nad výběrem připojení. Každému připojení vybereme z nabídky „Kanál zařízení“ jeden komunikační kanál.

Program NET – G provádí hlídání doby kontroly a to dvěma způsoby:

1. reakce na každou přijatou zprávu – program kontroluje příchod libovolné zprávy z objektu. Pokud taková to zpráva je přijata, program začíná znovu odpočítávat nastavenou dobu kontroly od ní.
2. reakce na zvolenou zprávu – program kontroluje jen příchod uživatelem nadefinované zprávy, ostatní ignoruje. Pokud je zvolená zpráva přijata, program začíná znovu odpočítávat nastavenou dobu kontroly od ní.

Okno také obsahuje záložku:

- Smyčky – umožňuje editovat smyčky a jim příslušející čidla.
- Sekce – umožňuje editaci Sekcí objektu. Každá sekce objektu vlastní určité smyčky. Zavření nebo otevření sekce pak nastavuje stav těchto smyček.
- Kontakty – umožňuje editovat odkazy na kontaktní osoby. Podmínkou je, že všechny kontakty jsou nadefinovány ve větvi Kontakty.
- Převody kódů – Převody kódů se skládají ze tří částí, a to z Převodu kódu na Smyčky, Sekce a Osoby.
  - Převody na smyčky – Převod se provádí pro zprávy typu POPLACH nebo OBNOVENÍSMYČKY. Převod určuje, které smyčky jsou nastavovány tímto kódem do stavu poplachu nebo obnovení a zároveň se operátorovi daná smyčka vypisuje v řádku události.
  - Převody na sekce – Převod se provádí také pro zprávy typu ODCHOD nebo PŘÍCHOD. Převod určuje, které sekce daného objektu jsou otevírány nebo zavírány daným kódem.
  - Převod na osoby – Převod se provádí pro zprávy typu ODCHOD nebo PŘÍCHOD. Kód je převeden na odkazovanou osobu, která je zobrazována

operátorovi v řádku události. Tím je známa operátorovi osoba, která provedla odchod. Osoby, na které chceme odkazovat, musí být nadefinovány ve větvi kontaktů.

### Nastavení automatického hlídání uzavření objektů

Program NET – G umožňuje nastavení u každé hlídané sekce, či u každého objektu jinou provozní dobu. Funkce REŽIMY potom nejen že v daný čas zkontroluje, zda je daná sekce uzavřena (zakódována), ale i jestli v době od konce do začátku pracovní doby někdo hlídáný objekt nevypnul, byť platným přístupovým kódem. Doba kontroly uzavření objektu je omezena na CELÉ HODINY.

**Průvodce manipulace s objektem**

Stav objektu  
 objekt není vypnutý  
 objekt je vypnutý

Přístup  
 Objekt povolen  
 Objekt zakázán

**Týdenní režim**

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Pondělí	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█
Úterý	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█
Středa	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█
Čtvrtek	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█
Pátek	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█
Sobota	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█
Neděle	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█

**Měsíční režim**

1 5 10 15 20 25 30

**Roční režim**

1 2 3 4 5 6 7 8 9 10 11 12

Výpis všech akcí

OK Storno

Obr. 15 Nastavené automatické hlídání uzavřeného objektu [8]

#### 5.1.1.4 Filtry neboli výpisy

Filtr znamená určitý dotaz na data uložená v databázi. Výsledkem provedení filtru je tabulka dat odpovídající danému dotazu.

Sestava znamená určitou grafickou předlohu, podle níž lze výsledek filtru zobrazovat nebo tisknout.

Tyto filtry a předlohy sestav si může správce systému NET – G jakkoliv upravovat nebo definovat své vlastní nové. Společnost NAM dále publikuje nové texty dotazů na svých věbových stránkách, odkud si správci systémů budou moci stáhnout nové texty filtrů i předlohy sestav. Lze vytvářet sestavy ze všech tabulek přítomných v databázi.

První dvě vlastnosti Filtr SQL a Předloha sestavy nemají vlastní zobrazení. Pokud pracujeme s filtrem, se používá třetí vlastnost – Test sestavy. Tato vlastnost má definováno zobrazení, ve kterém se dá definovat jednotlivé vlastnosti filtru.

Zobrazení má tři záložky:

- **Dotaz** je první z nich. Je to výsledná tabulka provedeného filtru.
- Záložka **Sestava** umožňuje zobrazení výsledku filtru podle předdefinované grafické předlohy.
- **Parametry** je to záložka, ve které se nadefinuje typ objektu, u kterých se bude filtr zobrazovat.

### 5.1.1.5 Kontakty

U každého objektu mělo by se definovat kontaktní osoby, které budou kontaktovány na základě situace objektu. Dále mělo by se definovat kontaktní osoby, které mohou manipulovat se zařízením PZTS na definovaném objektu.

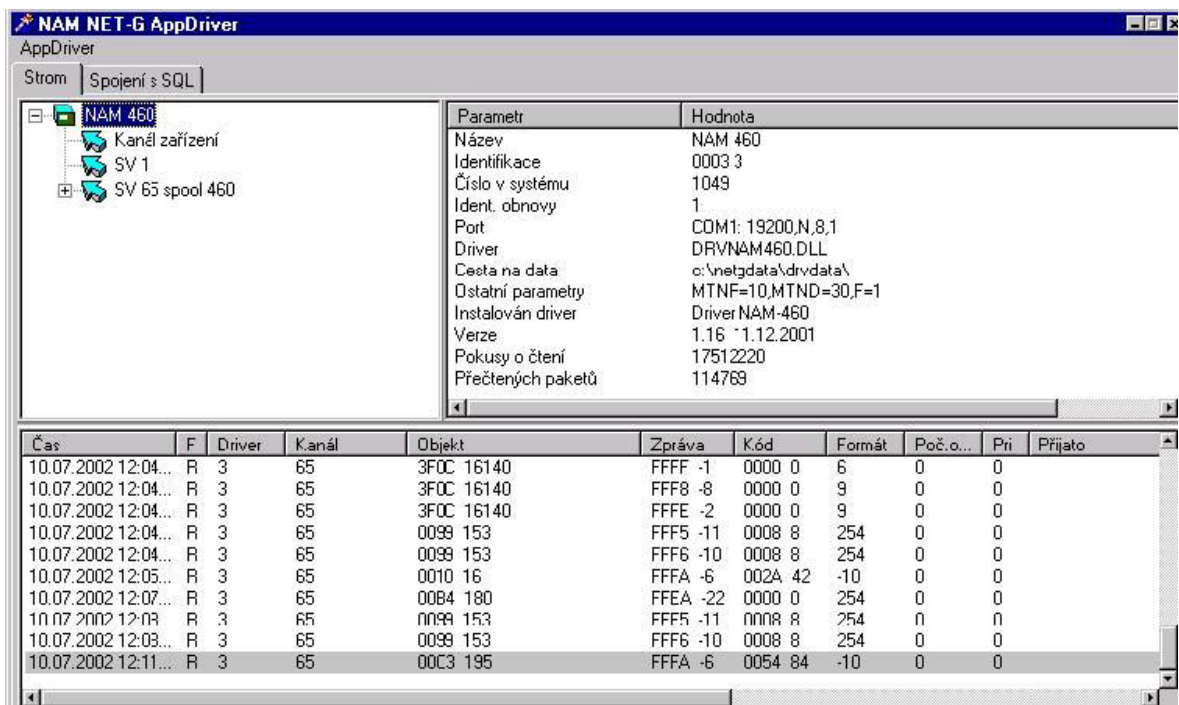
The image shows a screenshot of a software application. On the left is a tree view with various system components. The main area on the right displays a form titled 'Formulář zákazníka' (Customer Form). The form includes several input fields: 'IČO' (Company ID), 'DIČ' (VAT ID), 'Adresa' (Address) with sub-fields for 'Ulice' (Street), 'Město' (City), 'Tel' (Telephone), 'Fax', and 'Mobil' (Mobile); 'Bankovní spojení' (Bank account); 'ČP' (Postal code); 'PSČ' (Postal code); and 'Poštovní adresa' (Postal address).

Obr. 16 Formulář zákazníka [8]

### 5.1.2 MODUL AppDriver

Modul AppDriver slouží ke zpracování přijatých dat ze zařízení, k obsluze připojených zařízení a obsluze portů na PC. Proto pokud máme spuštěný modul NET-G, je nutno mít vždy spuštěný modul AppDriver, jinak operátor DPPC nebude přijímat žádná data ze zařízení.

Modul je tvořen jedním základním oknem, které má multifunkční přepínání stránek pomocí záložek. Záložka „Strom“ zobrazuje nakonfigurované ovladače a jejich základní hodnoty nastavení, jejich kanály a na nich připojené objekty. Ve spodní části okna je možno sledovat 50 posledních událostí přijatých driveru.



Obr. 17 Základní okno modulu AppDriver [8]

Aplikace je tvořena pouze jedním hlavním oknem, které má multifunkční přepínání stránek pomocí záložek. Záložka „Strom“ zobrazuje nakonfigurované ovladače a jejich základní hodnoty nastavení, jejich kanály a na nich připojené objekty. Ve spodní části okna je možno sledovat 50 posledních událostí, přijatých driveru (obr17).

Druhou záložkou je „Spojení s SQL“, informuje ona o stavu spojení se serverem SQL. AppDriver jako správce ovladačů se také stará o ukládání dat předaných od jednotlivých zařízení, do databáze SQL serveru. V listu je možné sledovat poslední odeslané události na server SQL.

NAM NET-G AppDriver

AppDriver

Strom   Spojení s SQL

Pracoviště: 3  
Již přečteno: 100 / 0

Čas	F	Driver	Kanál	Objekt	Zpráva	Kód	Formát	Poč.o...	Pri	Přijato
5.12.1998 8:29:08	P	2	1	6	2	0	0	0	0	
5.12.1998 8:35:34	P	2	1	5	2	0	0	0	0	
5.12.1998 9:55:26	P	2	2	260	130	1	0	0	0	
5.12.1998 9:55:46	P	2	2	260	18	225	0	0	0	
5.12.1998 9:57:10	P	2	2	260	129	1	0	0	0	
5.12.1998 9:57:32	P	2	2	260	18	225	0	0	0	
5.12.1998 10:02:10	P	2	1	14	2	0	0	0	0	
5.12.1998 10:33:54	P	2	1	14	3	0	0	0	0	
5.12.1998 10:38:28	P	2	1	13	2	0	0	0	0	
5.12.1998 10:57:30	P	2	1	13	3	0	0	0	0	
5.12.1998 12:00:00	P	2	2	258	9	0	0	0	0	
5.12.1998 12:04:00	P	2	1	1	3	0	0	0	0	
5.12.1998 12:05:26	P	2	2	257	129	2	0	0	0	
5.12.1998 12:19:22	P	2	1	61	3	0	0	0	0	
5.12.1998 12:49:22	P	2	1	6	3	0	0	0	0	
5.12.1998 12:57:00	P	2	1	11	3	0	0	0	0	
5.12.1998 13:14:04	P	2	1	19	3	0	0	0	0	
5.12.1998 13:36:02	P	2	1	2	3	0	0	0	0	

Obr. 18 Okno Spojení s SQL [8]

Ta složka obsahují dvě pozice:

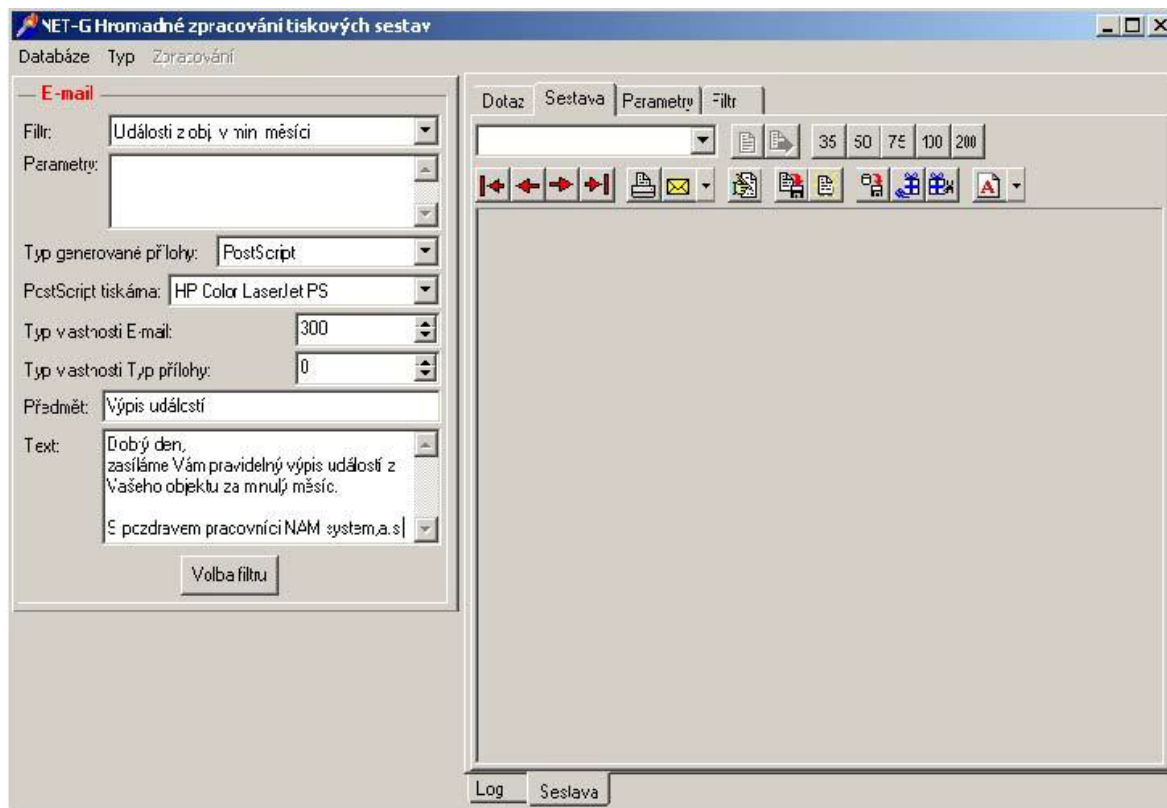
- Pracoviště – Identifikátor pracoviště, pod kterým je přihlašován AppDriver k SQL serveru
- Již přečteno – Počet paketů odeslaných od startu aplikace / počet opakování při chybě zápisu

AppDriver jak i větší část modulů Net-G má schopnost konfigurace v okně AppDriveru.

### 5.1.3 MODUL AppMail

Modul byl vyvinut pro hromadné pracování výstupních sestav. Tento modul umožňuje odesílání výstupních sestav vybraných objektů pomocí elektronické pošty, tisknout na tiskárně nebo odesílat faxem. Jednotlivý tisk nebo odeslání e-mailem je možné i v AppPCO. Zatížení operátora DPPC těmito operacemi je však značné a s velkým počtem

objektů je již prakticky tato činnost nemožná v souběhu s prací nad DPPC. Modul NET-G AppMail umožňuje nakonfigurovat podmínky pro hromadný výstup, jednotlivě otestovat a poté také spustit hromadný výstup sestav.

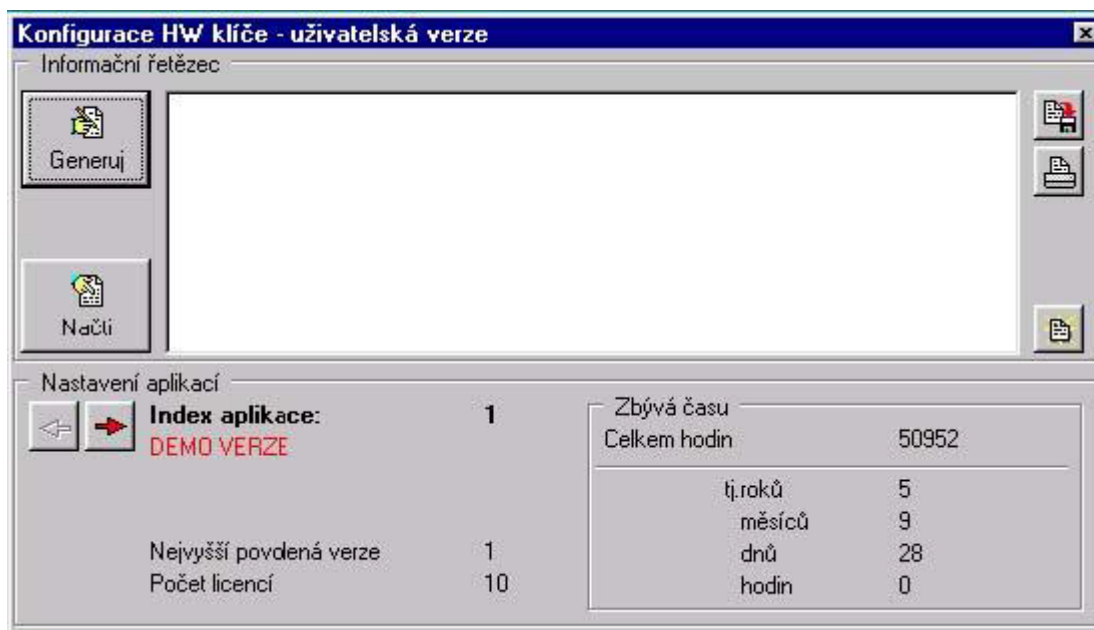


Obr. 19 Hromadné zpracování tiskových sestav[8]

Pro svou činnost vyžaduje operační systém Microsoft Windows 2000/XP/7. Modul NET-G AppMail je licencován. Pro správný chod modulu je nutné, aby byl povolen v licenčním HW klíč i NET-G.

#### 5.1.4 KeyAdministrator

Tento programový modul je určen pro správu HW klíče, který je součástí dodávky systému NET-G. Použitím tohoto modulu již nadále není nutné posílat klíč pro rekonfiguraci, nýbrž stačí pouze poslat příslušný textový soubor nebo případně fax s informačním řetězcem. Toto řešení je daleko rychlejší a také levnější než předchozí.

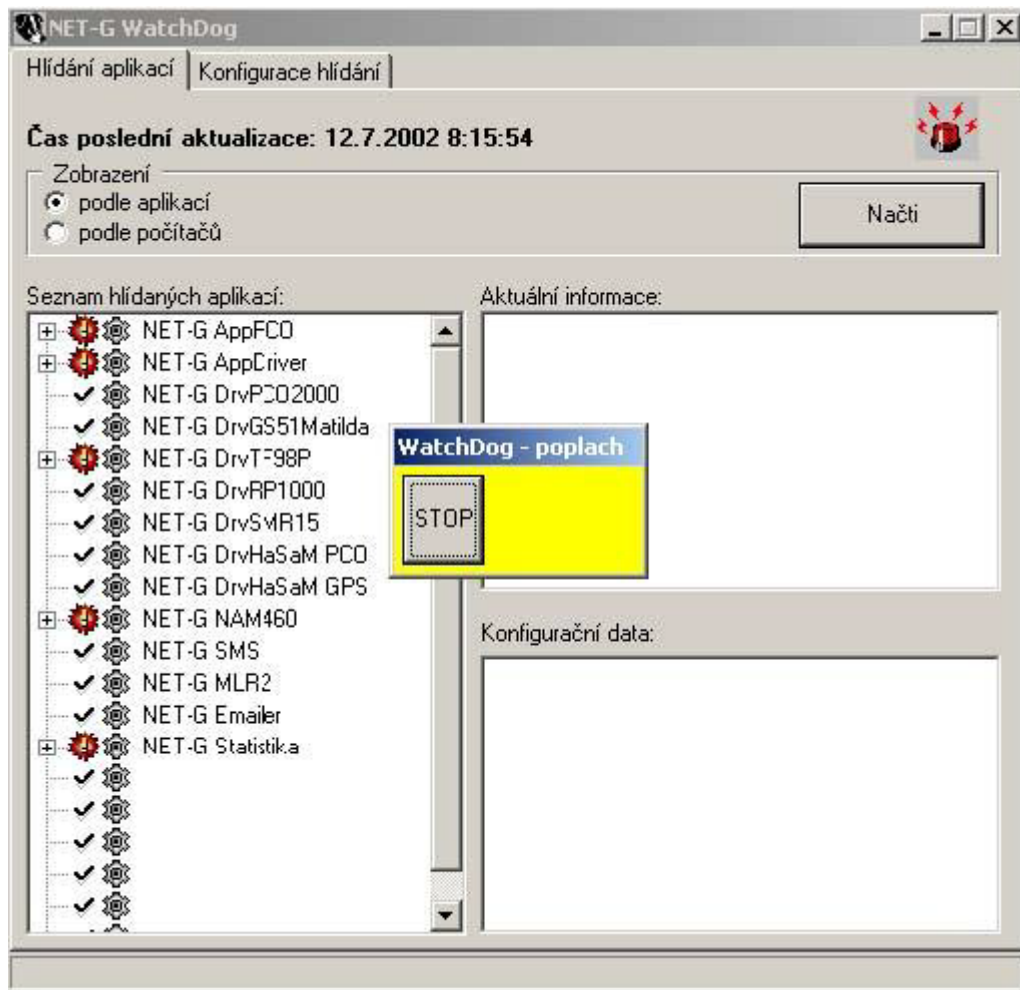


Obr. 20 Konfigurace HW klíče [8]

Pomocí modulu KeyAdministrátor se může dálkově měnit konfiguraci HW klíče. Pomocí tohoto modulu vygenerujeme zakódovaný řetězec nesoucí informace o klíči. Ten se pošle mailem na oddělení technické podpory společnosti NAM system, a.s. Tam se on upraví podle potřeby a zašlou ho zpět. Nový klíč si uživatel nahraje pomocí modulu KeyAdministrátor do klíče a ten má ihned změněny parametry.

### 5.1.5 MODUL WatchDog

Modul WatchDog (strážný pes) je doplňkovým modulem dodávky systému NET-G. Jeho funkcí je monitorovat a hlídat běh dalších modulů systému NET-G v závislosti na konkrétní konfiguraci HW klíče (určující typy a počty povolených aplikací) a konfiguraci hlídání v rámci modulu WatchDog. Tato aplikace může běžet na libovolném počítači, který však musí být připojen k serverovému PC (tzn. počítači, na kterém běží SQL server). Podmínkou správného chodu této aplikace je shoda systémového času na příslušných počítačích.



Obr. 21 Modul WatchDog [8]

Tento modul je součástí standardní instalace a měl by sloužit k zajištění kvalitnějšího a bezpečnějšího provozu celého systému NET-G na uživatelském dispečinku.

### 5.1.6 MODUL WatchConnect TCP

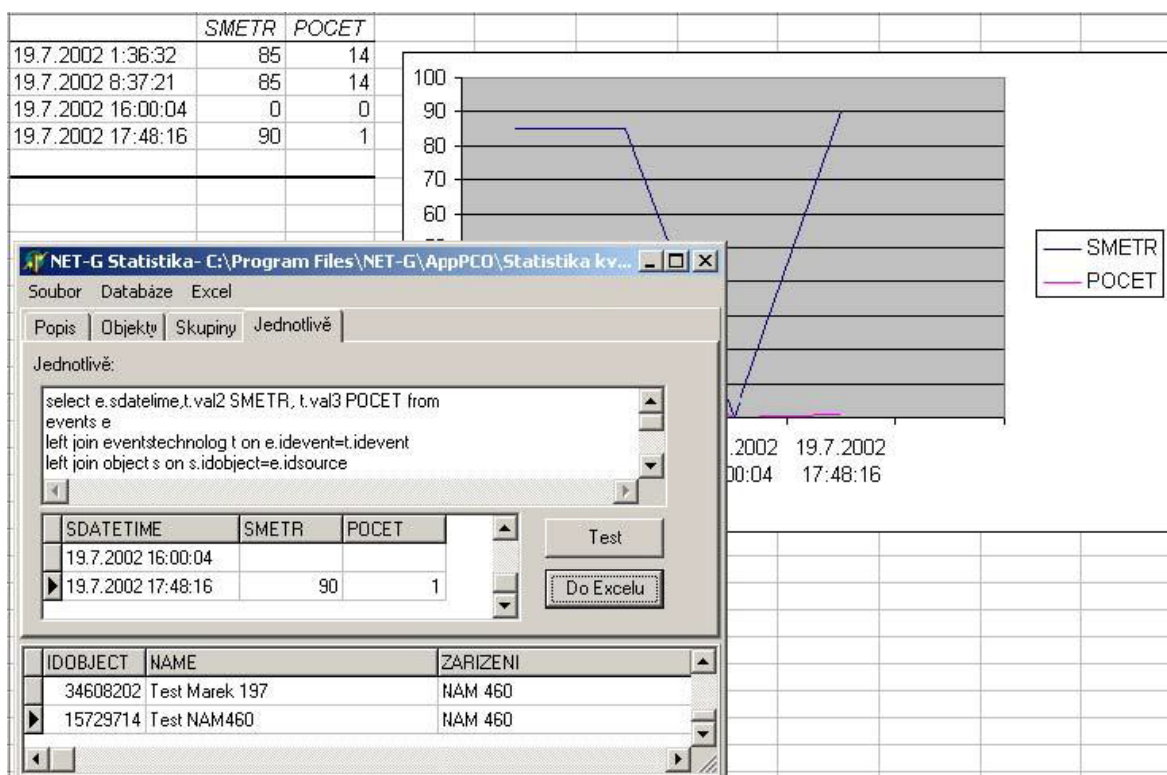
Modul slouží pro nastavení a kontrolu spojení klientského počítače se serverem NET-G. Program pro kontrolu spojení se jmenuje WatchConnectTCP a je nutné jej spouštět na klientském PC nejlépe po startu PC.



### 5.1.7 MODUL Statistika

Společnost NAM vyvinula pro statistické zpracování položek v databázi událostí NET-G nový modul NET-G Statistika. Tento modul umožňuje definovat a používat SQL dotazy pro výběry dat, tyto odesílat do programu MS Excel a automaticky z nich tvořit grafy. Z událostí pro statistické zpracování jsou vhodné např. kvalita signálu objektů, výpadky spojení, poplachové události, kvalita pozadí atd.

Použitá technologie Microsoft OLE, implementovaná v operačních systémech Windows, umožnila komunikaci s programem MS Excel a využít tohoto programu jako cílového pro uložení a presentaci dat z modulu NET-G Statistika. Požadovaný operační systém je tedy Microsoft Windows 2000/XP/7.



Obr. 22 Modul Net-G Statistika [8]

Modul NET-G Statistika je licencován. Pro správný chod modulu je nutné, aby byl povolen v licenčním HW klíči NET-G. Licenci je možné povolit vzdáleně pomocí modulu NET-G KeyAdministrator.

### 5.1.8 Modul AppServis

Pro efektivní práci dalších vyvíjených modulů NET-G, které reagují na vzniklou událost, bylo nutné vyvinout spolehlivý systém distribuce událostí k těmto klientským modulům. Dalším hlediskem, které při vývoji událostního serveru NET-G bylo zohledněno, je požadavek běhu jednotlivých modulů jako služeb systému, tedy startovaných společně se startem operačního systému a prací tzv. na pozadí i bez přihlášení k operačnímu systému.

Událostní systém je napojen na centrální databázi NET-G pomocí UDF (User Defined Function), která je volána při změnách v databázi. Je tedy patrné, že je nutno instalovat příslušné DLL a také provést vložení úprav do databáze pomocí příslušného SP (Servis Pack) NET-G databáze. K dispozici je deaktivační a aktivační SP, které slouží k deaktivaci nebo aktivaci spolupráce databáze s událostním systémem.

#### 5.1.8.1 Servis *PRINT*

Pomocí tohoto modulu lze tisknout v režimu ON-LINE uživatelem definované události. Služba NET-G Print Service je dalším komerčním modulem v událostním systému NET-G. Skládá se ze služby Print Service a konfiguračního programu Print Config.

#### **Print Service**

COM Service Server NET-G Print je server zpracovávající události NET-G a provádějící jejich on-line tisk na tiskárnu. On-line print je vyžadován normou pro DPPC zařízení ČSN EN 50131-Z1. Událost je tedy ihned po jejím zpracování systémem DPPC (NET-G) vytištěna. Server je instalován jako služba systému NT, spouští a zastavuje se ve správci služeb. Může běžet na více počítačích současně. Instalace tohoto modulu je samostatná.

#### **Print Config**

Konfigurační modul serveru NET-G Print umožňuje správci lokální i vzdálené (síťové) připojení k Print serveru, jeho konfiguraci a testování výstupu tisku. Modul je instalován jako Windows aplikace a je možné ho takto spouštět.

#### 5.1.8.2 Servis *SOUND*

Služba NET-modul sloužící k přehrávání definovaných .wav souborů a zároveň využívá COM port PC k zaklíčování radiostanice, přes kterou se potom přenáší přehrávané zvuky. Používá se u tzv. bezobslužných DPPC. Sound Service je prvním komerčním modulem

v událostním systému NET-G. Skládá se ze služby Sound Service a konfiguračního programu Sound Config.

### **Sound Service**

COM Service Server NET-G Sound je server zpracovávající události NET-G a provádějící zvukovou prezentaci těchto událostí dle konfigurací příslušných spustitelných objektů a jejich vlastností. Server je instalován jako služba systému NT, spouští a zastavuje se ve správci služeb. Může běžet na více počítačích současně. Instalace tohoto modulu je samostatná.

### **Sound Config**

Konfigurační modul serveru NET-G Sound umožňuje správci lokální i vzdálené (síťové) připojení k Sound serveru, jeho konfiguraci, testování zvukového výstupu a klíčování. Modul je instalován jako Windows aplikace a je možné ho takto spouštět.

#### **5.1.8.3 Servis SMS**

Díky tomuto modulu se může automaticky při příchodu definované události na definovaný objekt odeslat Vámi připravená SMS na přednastavená telefonní čísla. Služba NET-G Servis SMS je komerčním modulem v událostním systému NET-G. Skládá se ze služby SMS Service a konfiguračního programu SMS Config.

### **SMS Service**

COM Service Server NET-G SMS je server zpracovávající události NET-G a provádějící odesílání těchto událostí jako krátké textové zprávy (SMS) do sítě GSM dle konfigurací příslušných spustitelných objektů a jejich vlastností. Server je instalován jako služba systému NT, spouští a zastavuje se ve správci služeb. Může běžet na více počítačích současně. Instalace tohoto modulu je samostatná.

### **SMS Config**

Konfigurační modul NET-G SMS Config umožňuje správci lokální i vzdálené (síťové) připojení k SMS serveru, jeho konfiguraci, testování spojení s GSM telefonem, odesílání testovací SMS a další možnosti. Modul je instalován jako Windows aplikace a je možné ho takto spouštět.

#### 5.1.8.4 Servis SMS+

Modul sloužící k hlídání bdělosti operátora a k hlídání času potvrzení důležité zprávy tísňové volání operátora. Tento modul doplňuje NET-G. Služba NET-G Servis SMS + je komerčním modulem v systému NET-G. Skládá se ze služby AppServerAddEvent.exe a AppWatchOperator.exe.

#### Umístění

Oba moduly, včetně jejich INI souborů, se nacházejí ve složce \Program Files\NET-G\NET-G SMS Service\

#### AppServerAddEvent

Jedná se o modul, v němž se konfiguruje, které funkce budou aktivní, jakými časy se budou jednotlivé funkce řídit a jaké události v NET-G budou generovány. Modul se instaluje automaticky s NET-G.

#### AppWatchOperator

Tento modul umožňuje konfiguraci klávesových zkratk pro jednotlivé funkce a otestování funkčnosti jednotlivých funkcí a adaptérů připojených na COM port. Modul se instaluje automaticky s NET-G.

#### 5.1.8.5 Servis COM

Tento servis zajišťuje odeslání jakéhokoliv příkazu ve formátu RS 232 do sériového portu počítače. Vyvinut byl pro spolupráci softwaru NET-G s kamerovými systémy. Služba NET-G Servis COM je komerčním modulem v událostním systému NET-G. Skládá se ze služby COM Service a konfiguračního programu COM Config.

#### COM Service

COM Service Server NET-G COM je server zpracovávající události NET-G a provádějící odesílání těchto událostí formou volitelných paketů přes sériové rozhraní PC dle konfigurací příslušných spustitelných objektů a jejich vlastností. Server je instalován jako služba systému NT, spouští a zastavuje se ve správci služeb. Může běžet na více počítačích současně. Instalace tohoto modulu je samostatná.

## COM Config

Konfigurační modul NET-G COM Config umožňuje správci lokální i vzdálené (síťové) připojení ke COM serveru, jeho konfiguraci, odesílání testovacího paketu a další možnosti. Modul je instalován jako Windows aplikace a je možné ho takto spouštět.

### 5.1.9 Shrnutí – výhody systému NET-G

Akciová společnost NAM se zabývá vlastním vývojem rádio-telefonních DPPC již od roku 1992 a dnes se řadí k významným výrobcům DPPC v ČR. Na základě mnohaletých zkušeností z vývoje, výroby a provozu DPPC vznikl rádiotelefonní pult s označením NAM GLOBAL.

Základem DPPC NAM GLOBAL je vždy počítač s monitorovacím softwarem NET-G, který je navržen jako otevřený systém. Monitorovací software NET-G je to profesionální systém, který uspokojuje potřeby bezpečnostních agentur při vzdáleném monitoringu stavu objektů. Umožňuje rychle a bezpečně zpracovávat data z různých přijímacích poplachových center.

Uložená data jsou dobře chráněna použitou klient/server architekturou. Základ tvoří InterBase SQL server. Data lze kdykoliv za plného provozu systému zálohovat a také lze využít tzv. stínování databáze na jiné diskové zařízení. V programu je vysoce propracovaná strategie práv přístupu k informacím všem uživatelům.

S operačním systémem Windows lze NET-G využít jak pro provoz na lokálním PC, tak pro práci v síti. v síti lze vzájemně propojit několik pracovišť a bezpečně využít předností síťového provozu.

Vzdálený přístup k systému je podporován přes modem. Toto umožňuje pracovat se systémem servisnímu technikovi při napojování nového objektu u zákazníka nebo řediteli firmy přímo z bydliště, ze svého notebooku. Zároveň je společnost NAM schopna vzdáleně servisně přistupovat k tomuto systému.

Základem software NET-G jsou dva moduly: monitorovací modul AppPCO a modul ovladačů AppDriver. Příslušné ovladače jsou pak dodány v závislosti na tom, jaká zařízení DPPC zákazník používá. Dalším modulem v NET-G je modul AppServis, který obhospodařuje různé druhy servisů. Např. servis zabezpečující přehrání zvuku, servis umožňující odesílání událostí jako SMS na mobilní telefon apod.

Téměř, co lze v systému NET-G definovat, většinou není omezeno. V softwaru NET-G lze definovat více než 65 000 objektů. Objektem může být hlídaný objekt, střežený automobil, kontaktní osoba, firma nebo pracoviště dispečinku. Ke každému připojenému DPPC jde definovat „neomezené“ množství převodních tabulek zpráv, objektů atd. Tyto převodní tabulky umožňují sloučit např. rádiové a telefonní objekty definované v DPPC do jednoho objektu v systému NET-G. Jediná věc, která omezuje software NET-G je kapacita disku serveru a počet definovatelných adresáři zařízení komunikující s DPPC v objektu. Počet objektů lze pro zákazníka nastavit a vždy rozšířit, podle individuálních potřeb konkrétního DPPC.

Každý z definovaných objektů je zařazen a má své místo v tzv. stromové struktuře, podobné té, jakou známe z běžných operačních systémů. Tuto strukturu lze měnit, upravovat, rozšiřovat o další objekty, zpřehledňovat ji vytvářením skupin a podskupin.

Ke každému objektu jde přiřadit libovolný počet vlastností různého typu, jako jsou texty, grafika, převodní tabulky, unifikované typy adres nebo skladových karet atd. Tato data lze sdružovat do formulářů a tak je zpřehlednit. Rovněž formuláře jdou přiřadit ke kterémukoliv objektu.

## 5.2 Kronos NET

KronosNET je systém, jehož hlavním úkolem je podporovat řízení v poplachových přijímacích centrech.

Skládá se ze tří bloků zahrnujících:

- vedení monitorovací služeb DPPC,
- údržbu monitorovacího zařízení,
- zúčtování.

Důraz je kladen na stabilitu, ergonomii a efektivitu, které v průběhu vývoje produktu umožňují sledování víc než 100 tisíc objektů na jediné monitorovací stanici a zpracování mnohem více než 100 signálů za sekundu při zachování plné analýzy signálu. Navíc díky flexibilitě programu toto množství může být snadno rozšířeno.

Monitorovací modul slouží k integraci dohledu budov, vozidel, lidí, kamer, životního prostředí (měření teploty, vlhkosti, atd.), prodejních automatů, bezpečnostních strážců a

řízení přístupů a časů práce. Rozsah služeb, které aplikace zahrnuje, se den za dnem zvětšuje.

Společnost Next! spolupracuje s výrobcí zařízení zahrnujících přímo 50 stanic bazových a objektových vysílačů. Komunikace s nimi se koná přes rádiovou síť, telefonní linku, GSM/GPRS nebo informační síť. Vysoký stupeň automatizace aplikace umožňuje zbavit provozovatele povinnosti plnit mnoho úkolů, zejména těch, které souvisejí s různými způsoby oznamování zákazníkům, zaměstnancům a subdodavatelům.

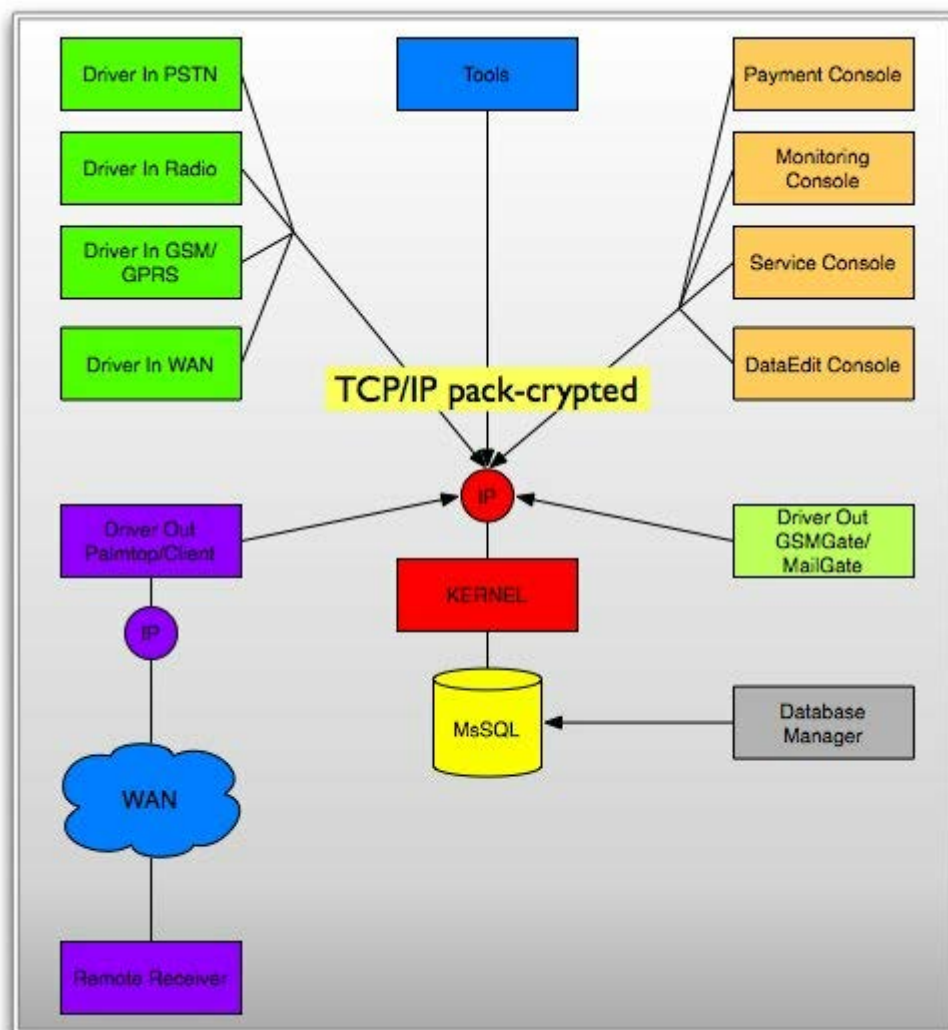
Servisní modul organizuje v jednom prostředí celou práci servisního oddělení počínaje servisem, údržbou, instalací, modernizací a konče demontáží měřicích a poplachových systémů. Tento modul umožňuje stálou kontrolu nad servisním týmem a jejich následným vypořádáním se, se zadanými úkoly. Prostřednictvím úzké integrace s Monitorovacím modulem mají oprávněné osoby možnost nahlédnout do provozu zařízení nainstalovaných v budovách, a to i z mobilních zařízení typu PDA.

Zúčtovací modul umožňuje shromažďování všech událostí spojených se zúčtováním služeb poskytnutých zákazníkovi na jednom místě a následné vygenerování faktur na základě těchto informací. Tyto faktury lze tisknout přímo z programu, nebo exportovat do externích finančních a účetních systému. Celek je založen na extrémně flexibilním mechanismu nízkých cen a kalendáře se slevami.[10]

### **Architektura systému**

Kronos NET je plně síťovým řešením založeným na mnohvrstvé modulární architektuře. Tato struktura zajišťuje:

- možnost disperze ve velké oblasti,
- zabezpečení dat,
- zaměření funkčnosti systému na skutečné potřeby,
- spolehlivost systému.



Obr. 23 Schéma architektury modulu KronosNET [10]

**Moduly a jejich funkce:**

**Kernel** – centrální modul systému odpovídá za zpracování signálu, sdílení dat z databáze a kontrolu práce ostatních modulů.

**MSSQL** – vysoce výkonný databázový server od společnosti Microsoft v bezplatné či komerční verzi.

**Monitoring Console** – terminál provozovatele určený pro zpracování alarmů a provádění monitorovacích služeb.

**Data Edit Console** – terminál pro správce dat používaný pro správu dat zákazníků a objektů.



**Billing Console** – terminál pro finanční oddělení, který se používá k provádění vypořádání se s klienty.

**Service Console** – terminál pro správce servisu, který umožňuje kontrolovat aktuální stav realizované služby, údržby, montáže, modernizace a demontáže v objektu.

**Driver In PSTN** – ovladače přijímající signály z telefonního kanálu.

**Driver In Radio** – ovladače přijímající signály z rádiového kanálu.

**Driver In GSM / GPRS** – ovladače přijímající signály z kanálů sítí GSM.

**Driver In WAN** – ovladače přijímající signály ze sítě WAN.

**Driver Out Palmtop/Clinet** – ovladače poskytující data pro PDA zařízení a pro aplikace externích zákazníků jako například hasičský záchranný sbor, policie, jednotlivý zákazník.

**Driver Out GSMGate/MailGate** – ovladač posílající na základě poplachové události nebo otázky od uživatele informace přes SMS a e-mail. Umožňuje také zasilání vyjádření bezpečnostních služeb v určitém čase.

**Remote Receiver** – odborné terminály navržené pro hasičský záchranný sbor, policii nebo jednotlivé zákazníky.

**Configuration Tools** – program nástrojů pro dálkovou diagnostiku systému a konfigurace.

**Database Manager** – software pro správu databází.

### **Bezpečnost**

Architektura systému je jednou z nejbezpečnějších na trhu, a to jak z hlediska ochrany před neoprávněným přístupem zvenku, tak z hlediska stability systému. Výrobce vynaložil veškeré úsilí, aby databáze obsahující údaje o zákaznících nebyla ihned k dispozici, dokonce ani v místní síti. Tuto zvýšenou bezpečnost umožnilo použití třívrstvé architektury. Jediný modul, který má právo přistupovat k databázi, s výjimkou servisních nástrojů, je Kernel. On sám vyžaduje autorizaci od každého modulu a přistupujícího uživatele, opakovaně kontroluje oprávnění a neustále monitoruje činnost uživatele. Navíc se celá transmise odehrává za pomoci zvláštního autorizačního produktu používajícího šifrování VMPC, balení rámců a také re-transmise vypojení změn.

Otázka stability by sama vydala na samostatnou kapitolu. Modulární struktura systému a rozptýlení programu na více počítačích nabízí výjimečnou odolnost, a to i v případě havárií

hardwaru. Poškození jednoho z počítačů odpojí jen část funkce systému, navíc díky automatickému řízení rezervních modulů lze okamžitě spustit bezobslužné zálohování.

Pozornost si zaslouží také fakt, že díky unikátní technologii diskové vyrovnávací paměti, systém udržuje jeho současný stav, a to nejen na nezávislé (krátkodobé) paměti, ale i na datovém disku. Vypnutí počítače proto nezpůsobí ztrátu dat.

### **Rezervní centra**

Systém umožňuje tvorbu rezervních center, které se v případě poruchy spustí automaticky. Existují dvě možnosti přípravy rezervních center:

- v případě poruchy hlavního rezervního centra se spustí dodatečné centrum,
- v případě poruchy hlavního centra se instalace rozptýlí.

První řešení spočívá v přípravě datového serveru a modulu Kernel pracujících v odlišných místech, kde se v případě absence spojení s hlavním centrem automaticky přepnou moduly. To je nejčastější řešení. Vyžaduje síťové propojení mezi hlavním a záložním centrem.

Druhé řešení je inovační a umožňuje vytvořit několik bezobslužných místních stanic přenášejících data do hlavního centra. V případě komunikačních problémů následuje rozptýlení a přestup bezobslužných stanic do manuálního režimu.

### **Retransmise a spolupráce**

Unikátní vlastností tohoto programu je mimořádná schopnost přenosu alarmů a signálů. Příjemcem mohou být buď další informační systémy, nebo konkrétní osoby, nebo dokonce spolupracující bezpečnostní agentury.

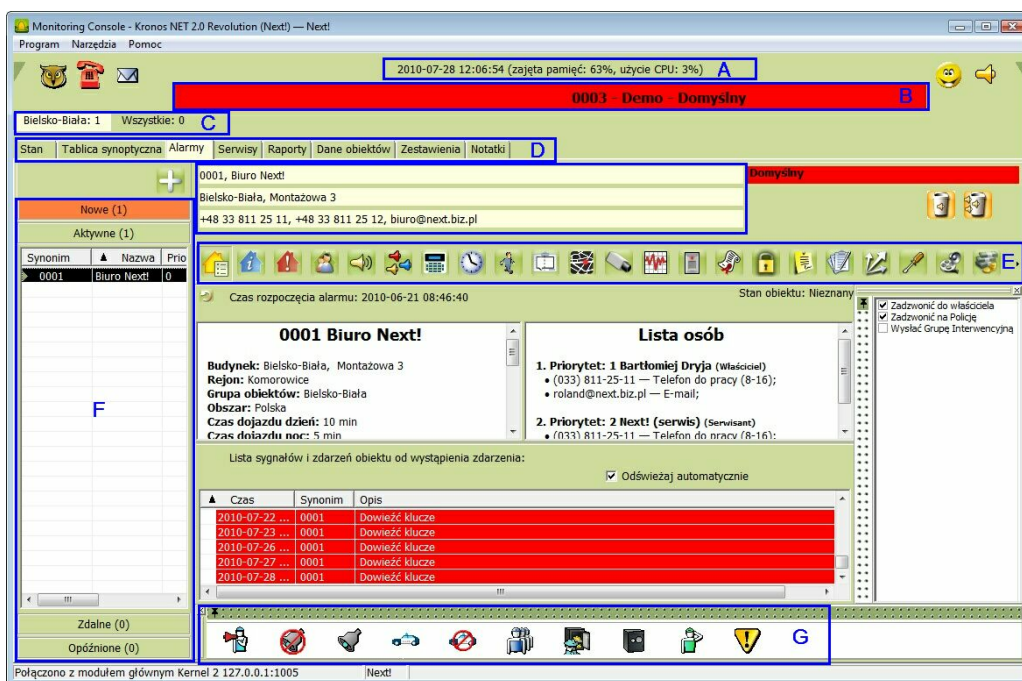
Platforma Kronos NET umožňuje spojení mezi systémy různých firem a zajišťuje předání alarmů z chráněných objektů. Veškeré údaje o těchto objektech jsou pak k dispozici po dobu obsluhy poplachu. Zároveň se získávají informace o prováděných opatřeních. Příjemcem signálů bývá subdodavatel programu Kronos LT, taková komunikace je pouze jednostranná. Navíc je připraven zjednodušený terminál, který může být nainstalován u hasičů nebo policie. Tento terminál nepoužívá lokální databáze, a proto nevyžaduje žádnou údržbu a může být dálkově ovládán. Takový terminál přijímá poplachové události a informace o objektech z hlavního systému přes informační síť.

## Zabezpečení hardwaru

Program je zabezpečen proti nelegálnímu kopírování a používání pomocí speciálního klíče HASP značky Alladin. Jsou to klíče dodávané speciálně od výrobce softwaru a nemůžou být nahrazené jinými. Klíč je požadován pro snadnou práci programu a musí být připojen k počítači, na kterém je nainstalován modul Kernel. Je také možné využít ovladač RemoteHASP, který bude posílat do modulu Kernel data z licence, z klíče HASP, připojeného přes USB port do jiného počítače. [10]

### 5.2.1 Monitoring Console

Modul byl zkonstruován za účelem usnadnění obsluhy poplachů, kontroly dat a generování zúčtování. Je to základní modul, který používá operátor DPPC. Monitorovací konzola vypadá takto:



Obr. 24 Hlavní obrazovka Monitoring Console – složka Alarmů. [10]

Písmenka v obrázku označují nejdůležitější funkce a ukazatele:

A - Systémové hodiny a ukazatel procentuální náročnosti systému na procesor a paměť RAM.

B - Proužek novinek.

C - Skupiny objektů zařazených do Monitoring Console.

D - Záložky pro přístup do jednotlivých funkčních bloků.

E - Možnosti zpracování alarmů.

F - Seznam aktuálních alarmů v systému.

G - Aktivity v zacházení s alarmy.

a ikony:

- **koperty** – komunikace mezi konzolami v systému Kronos NET,
- **sova** - Knowledge Base – Znalostní Báze,
- **smiley ikona** – kliknutím na ikonu se zobrazí seznam posledních chyb,
- **telefon** – umožňuje volbu připojení přes zkonfigurovaný modem připojený k počítači, přes digitální telefon nebo přes záznamové zařízení,
- **reproduktor** – vypíná akustický alarm až do příchodu dalšího poplachové události.

Po stlačení a kliknutí na levý horní roh se nám otevře okno Vedení intervenčních skupin.

Po stlačení a kliknutí na pravý horní roh se nám otevře okno Systémové Informace.

#### **5.2.1.1 Záložka Stav**

Záložka třídí data týkající se současného a minulého stavu systému Kronos NET. Na jednotlivých panelech se zobrazuje nastavení signálů, které přišly do systému, činností vykonaných na objektu a událostí, které se vyskytly v systému:

- Signály,
- událostí objektu,
- systémové událostí.

#### **5.2.1.2 Synoptická tabulka**

Synoptická tabulka ukazuje grafické stavy všech objektů zobrazené v jednom místě.

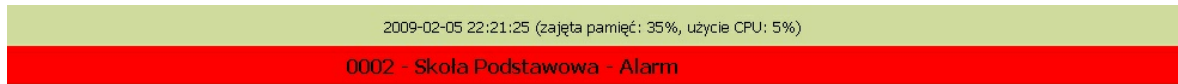
Objekty jsou označeny barvami a navíc ikonami, které podrobněji popisují jejich stav.

- červená barva znamená, že na objektu je poplach,
- modrá barva znamená, že na objektu právě probíhá servis.

#### **5.2.1.3 Poplachy**

Záložka na obsluhu poplachů je základní záložka pro práci v programu.

Pokud v seznamu se poplachů ukáže nová pozice, a my se nacházíme na jiné záložce, tak záložka poplachu začne blikat oranžovou barvou a pod hodinkami se ukáže novinkový proužek informující o názvu objektu a druhu poplachu, který vyskytnul se v systému.



Obr. 25 Přicházející poplach[10]

Když se nacházíme v složce Poplarchy, bliká paprsek Nové, kde se nacházejí ještě neobsloužené poplarchy. Systém rovněž informuje operátora o vzniku nového poplachu zvukovým signálem.

Na levé straně záložky se nacházejí čtyři pásy obsahující aktuální poplarchy v systému. Kliknutím pravým tlačítkem myši na konkrétní poplach otevřeme kontextové menu, obsahující následující možnosti:

- Výzvědní (uvolní z aktivní) – (*Przejmij (Zwolnij w Aktywnych)*)
- Přejdi ke
- Přenes k servisu – (*Przenieś do serwisu*)
- Odložit
- Odstranit
- Výzvědní vše (uvolní z aktivní) – (*Przejmij wszystkie (Zwolnij w Aktywnych)*)
- Odstranit vše
- Výzvědní vybraný typ (uvolní z aktivní) – (*Przejmij wybranego typu (Zwolnij w Aktywnych)*),
- Odstranit vybraný typ (Ukaž okna poplachů k odstranění) – (*Usuń wybranego typu (Wyświetli okno z typami alarmów do usunięcia)*)

Všechny poplarchy jsou tříděné tak, aby několik událostí stejného typu a stejného objektu nevyvolávalo víc poplachů vyžadujících osobní obsluhu. Poplach může být provozován pouze na jedné stanici. Tyto funkce zajišťuje systém, který spravuje přidělování poplachů ke stanovištím. Zastaví-li se kurzor nad poplachem, ukáže se zkrácená informace vztahující se k danému poplachu. V programu je možné samostatné přidání poplachů. Velmi důležitá funkce programu je třídění poplachů, které usnadňuje práci v případě, že vznikne větší množství poplachů naráz. Alarmy se třídí na nové, aktivní, dálkové a opožděné. Práce s obsluhou poplachů je snadnější, a tak se minimalizuje riziko nezjištění

vzniku poplachu v objektu. Po přijetí zprávy a nastavení poplachu jako aktivní poplach, se v horní části záložky ukáže informace týkající se objektu a druhu poplachu. V centrální části se nachází pracovní pole ukazující vybraná data objektu. V době obsluhy poplachu je možné registrovat následující činnosti: Oznámit osobu, Zrušení poplachu, Soukromé zásahové skupiny, Zrušení zásahové skupiny, Příjezd zásahové skupiny, poplach, planý poplach, Konec provozu poplachu, Jiné. Operátor se může pohybovat mezi skupinami informací po celou dobu obsluhy poplachu. Seznam dostupných operací záleží na nastavení konfigurací systému. Po vzniku poplachu má operátor k dispozici informace o stavu, názvu, obci, oblasti, kontaktech objektu a také předpokládanou dobu dojezdu, datum spuštění poplachu, poznámky a seznam osob přiřazených k objektu. Operátor v okně modulu uvidí plný rozsah informací a manuálních možností potřebných k správnému zabezpečení objektu.

#### **5.2.1.4 Servisy**

Záložka Servisy umožňuje obsluhu servisu objektů. V servisním režimu poplachové signály nevzbuzují poplach. Výjimku stanoví situace, kdy je daný poplach definován jako neblokovaný poplach přes servis. Obsluha servisu je analogická s obsluhou poplachů. Rozdílem je jeden nástroj navíc (vyžadované signály), který umožňuje porovnávat seznam signálů, které přišly, se signály, jejichž přítomnost je nutná k tomu, aby servis byl zaznamenán jako kompletní z hlediska přenosové účinnosti.

#### **5.2.1.5 Raporty**

V záložce raporty se nacházejí poplachové, informační a denní servisní raporty, které čekají na zpracování operátorem. Do dokladů se zapisují v databázi z konce obsluhy servisu, poplachu nebo konce služby.

#### **5.2.1.6 Údaje z objektů**

Tato volba dovoluje nahlédnout do dat došlých z objektů, která se nenacházejí v poplachovém či servisním režimu. Po zvolení objektu jsou všechny dostupné volby analogické jako v případě obsluhy poplachu, jen s tím rozdílem, že všechny tyto volby související s archivními daty požadují ruční zvolení období. Tato nabídka umožňuje také několik možností tisku, exportu a posílání některých dat mailem.

### 5.2.1.7 Výkazy

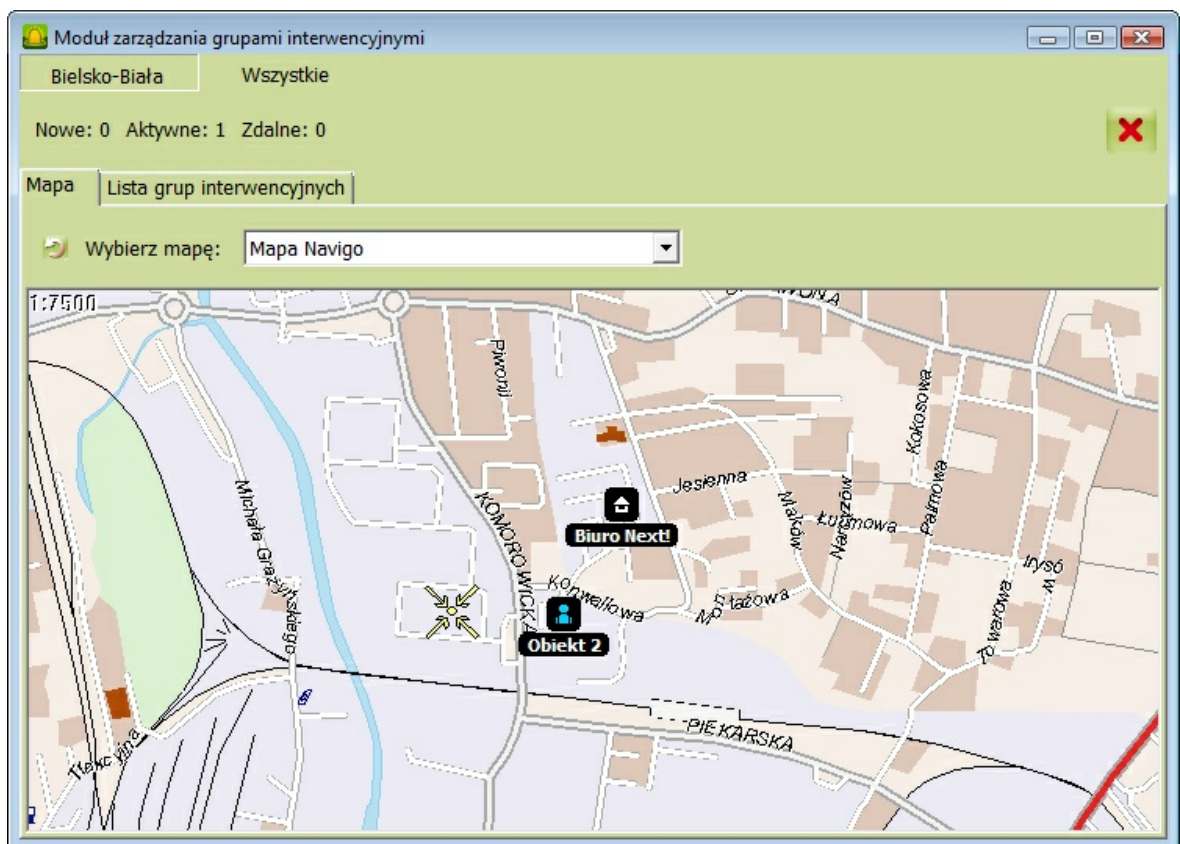
Záložka Výkazy umožňuje prohlížet souhrnné údaje týkající se všech objektů, nebo celého systému. Výkazy jsou vysílány v paketech tak, že uživatel nemusí čekat na výsledky do konce doby sběru všech dat. Tyto a další mechanismy umožňují přípravu výkazů, a to i z období za několik měsíců.

### 5.2.1.8 Poznámky

Záložka prezentuje poznámky týkající se všech uživatelů a slouží jako úřední deska.

### 5.2.1.9 Řízení skupin

Jedná se o okno s mapou a s označenými položkami intervenčních skupin a objektů, které jsou ve stavu obsluhovaných poplachů v dané konzole, a kterým byla dříve zadána zeměpisná poloha pro zobrazení mapy. Mapy se zobrazují v menu Konzola editace – kapitola Mapy, pozice objekty. Mapy, které jsou v nabídce, pocházejí z databáze Google, nebo Navigo.

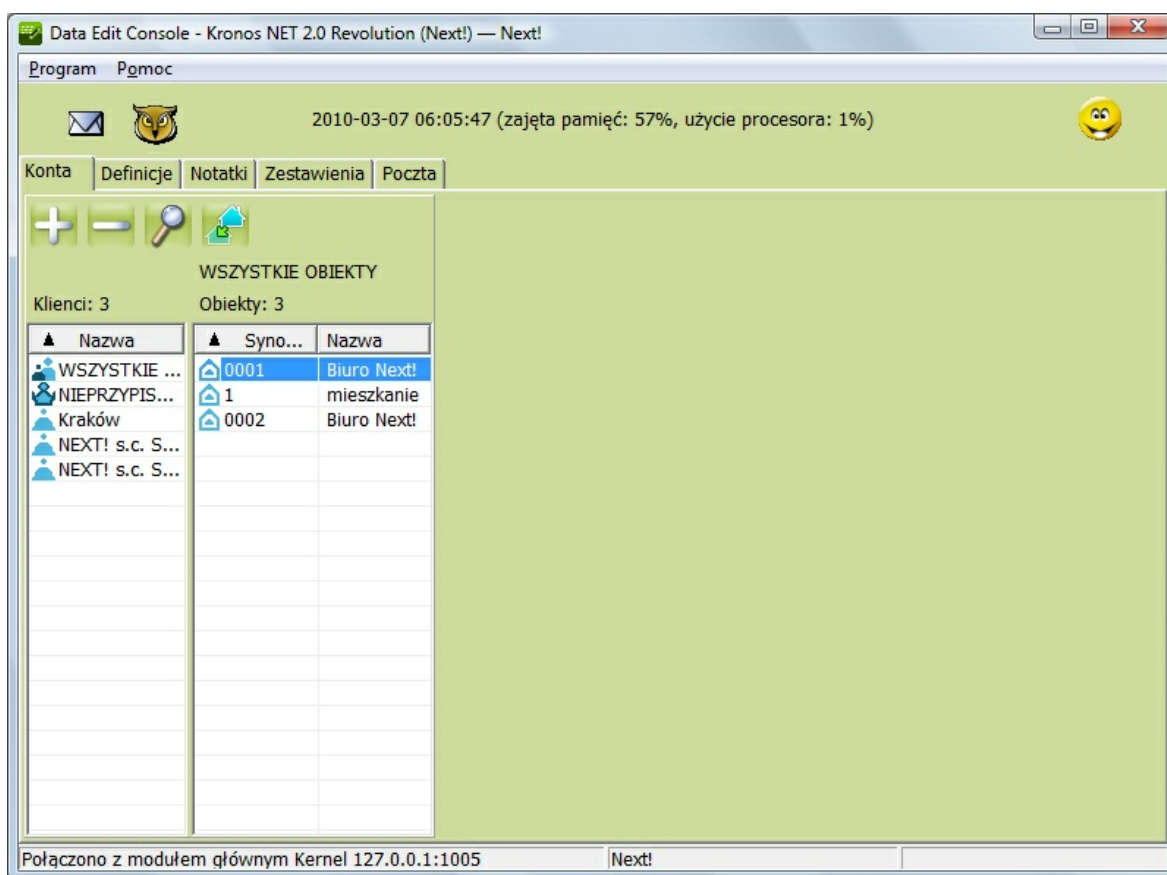


Obr. 26 Mapa objektu Navigo [10]

Na záložce Seznam Intervenčních Skupin může operátor DPPC řídit intervenční skupiny, dodatečné funkce jsou k dispozici, pokud je skupina vybavena Mobilní Konzolou Intervenčních Skupin. [10]

### 5.2.2 Data Edit Console

Tento modul slouží pro zadávání dat objektů, zákazníků a nezbytných definic k obsluze objektů v monitorovacím systému. Umožňuje kontrolu parametrů monitoringu, servisu, výpočtu a řízení smluv zákazníka. Pro potřeby kontroly údajů, nabízí konzola celou řadu souborů zohledňujících více průřezových kritérií.



Obr. 27 Data Edit Console [10]

Okno Konzola editace se skládá z pěti základních záložek:

- Definice – definice vzorů a šablon používaných v systému,
- Účty – přidávání, editace a také odstranění účtu zákazníků a objektů,
- Poznámky – obsahují poznámky zadané uživatele,
- Výkazy – seznam výkazů,



- Pošta – vnitřní poštovní systém od Kronos NET, umožňující kontakt se zákazníkem.

### 5.2.2.1 Záložka definice

Ze záložky definice máme přístup do seznamů, šablon, vzorů a slovníků týkajících se všech objektů. Data o nich je vhodné zadat do systému před přidáním samotných objektů. V záložce Seznam osob je možné přidávat, upravovat nebo odstraňovat informace o všech osobách, které mají něco společného s objektem v monitorovacím systému.

V šabloně zařízení tvoříme definice zařízení a interpretujeme signály a funkce, jejichž nastavení a závislosti na objektech zůstávají stejné bez ohledu na importy a aktualizace šablon. Tato možnost zrychluje přidávání nových objektů a usnadňuje uživatelům původně náročnou práci související s definováním zařízení na objektech. Na záložce Globální Poplarchy jsou vypočítané poplarchy, které systém může vygenerovat, různým poplachům je přidělena priorita (čím nižší tím důležitější) a také barva poplachu. V definicích upozornění zadáváme vzorce upozornění, které mohou být následně přiřazeny k objektům. Při přidávání nových typů upozornění je třeba je definovat a zadat jejich název a popis.

K definování procesů a obsluze poplachů se používají Vzory Procesů, které je následně možné přiřadit k objektu.

Šablony Smluv se využívají, když je třeba přiřadit smlouvy k objektům. Je možné v nich podle potřeby vyplnit libovolné pole, měnit obsah smlouvy, přidávat na základě dohody různé slevy apod.

Další záložkou je záložka Expresní Systém. Je to informační databáze dostupná ze všech konzol. Dají se do ní umístit pomůcky, manuály nebo doplňkové informace dostupné pro všechny uživatele systému. Pomůcky mohou být umístěné v databázi jak ve formě textu, tak i jako předem připravené obrázky ve formátu JPG.

V Kalendáři Svátků se definuje datum svátků na celý rok. Tato funkce má význam při nastavování režimu úkolů, stavů, změn stavů. Systém pak vyhodnocuje poplarchy v závislosti na této informaci.

Objekty mohou být definované v Monitoring Console na předem připravených mapách. K zobrazení terénu se mohou využívat vlastní mapové podklady (bitmapové mapy ve formátu JPG) nebo, po zakoupení licence, mapy společností Google či NavigoX. Pokud je k dispozici více map, nastaví se priority jejich užívání v Monitoring Console.


### 5.2.2.2 Záložka Účty: správa zákazníků a objektů

Záložka Účty se dělí na následující články:

- Seznam zákazníků – obsahuje seznam zákazníků, které systém obsluhuje.
- Seznam objektů – obsahuje seznam objektů roztříděný podle zákazníků.
- Všechny objekty – obsahuje seznam všech objektů, které jsou zavedeny v systému.
- Nepřipsané objekty – seznam objektů, které nejsou přiřazené k žádnému zákazníkovi.
- Pracovní Prostor – prostor, v kterém je možné upravovat údaje o vybraných zákaznících nebo objektech.

V této konzole na první pohled upoutá ještě Počítadlo nad seznamem objektů, které ukazuje aktuální počet aktivních objektů v systému a maximální počet aktivních objektů.



Přidání nového objektu do systému je velice snadné. Stačí stlačit ikonu  a program nás provede vkládáním všech údajů potřebných k tomu, aby operátoři dokázali správně zareagovat v případě vzniku poplachu v objektu. Nejprve se systém ptá na jméno objektu/osoby. Pak vyžaduje doplnění všech základních údajů o chráněném objektu/osobě (adresa, číslo bankovních účtů atd.). Pokud osoba vlastní více objektů, je možné pro usnadnění práce se správou faktur propojit informace o všech těchto objektech.

Zápisy, které v systému o osobách/objektech máme, můžeme kdykoli upravovat. Stačí



stisknout tlačítko  a otevře se editační okno:

Obr. 28 Úprava dat objekt/osoba [10]

V tomto okně můžeme doplňovat nejen základní informace o objektech či osobách, ale také přidávat údaje například o dojezdových časech k objektu ve dne nebo v noci, informace o osobách, které se v objektu pohybují, spojení na osoby, které je třeba kontaktovat v případě vzniku poplachu, polohu objektu (zeměpisná šířka a délka), překážky, které mohou blokovat příjem příchozích signálů přes Kernel, systémy PZTS, EPS, CCTV atd., které se nacházejí ve sledovaném objektu, způsob obsluhování objektu (přístup přes SMS, přes web, servis, finance, monitoring atd.).

Výše jsem popsal základní údaje, které se do systému zadávají. V systému je též možné přidat detailní informace. Těto možnosti se využívá, pokud chceme k objektu přidat nového majitele, nový kontakt, dobu platnosti spojení osob s objektem, fotky strážných, pokyny pro strážné v objektu, upozornění pro zásahové skupiny při kontrole vzniklých poplachů.

Konzola umožňuje zadání režimu zálohování systému. Zadává se tam, kdo a kdy bude zodpovědný za servis zálohování systému na objektu.

Na záložce zařízení přidáváme, prohlížíme a upravujeme zařízení už přidaná do objektu, můžeme také konfigurovat kontrolu zkoušek, parametry zařízení a výstupné převody pro zařízení v objektu. Je možné nastavit čas, kdy má strážný na objektu vykonat obchůzku, a následně ho sledovat nebo zkontrolovat zda strážný byl v určenou dobu na zadaném místě.

Úprava dat týkajících se monitoringu objektu je možná po zvolení objektu a kliknutí na ikonu Monitoring. Tam lze nastavit přeposílání, které se používá ke konfiguraci, přeposílání poplachů, změně skupin signálů nebo servisního režimu do vnitřních modulů, které mohou posílat poplachu, skupiny signálů nebo servisní režim.

Na záložce poplachu se dají přidat pravidla týkající se obecných poplachů na daném objektu (tichý, zpožděný, ignoruj servis, ignoruj blokádu).

Záložka Funkce se používá pro automatické generování poplachu pro objekt v závislosti na čase. Funkce úkolů umožňuje generování zvoleného poplachu v konkrétním objektu v určitém čase nebo v určité době. Umožňuje to automatické zabezpečení přes definované způsoby zabezpečení objektů v daném čase.

Na záložce smlouvy je třeba přidat údaje o smlouvách, které se týkají daného objektu. Totéž okno slouží k editaci smluv, které byly do systému zadány dříve. Pokud dojde ke vzniku událostí specifikovaných ve smlouvě, vygeneruje se podle ceníku položka, která má být zaplacená. Ceník událostí může obsahovat zároveň jednorázové události (např. poplach, posílání SMS) i pravidelné položky (např. měsíční poplatek za služby).

Poslední volbou systému v Úprava Dat je Historie Změn Objektů. Tam se ukládají všechny změny dat týkající se daného objektu, datum zadaných změn a také informace o uživateli, který tyto změny provedl.

### **5.2.2.3 Poznámky**

V záložce Poznámky se zadávají všeobecné poznámky, které se přímo nevztahují ke konkrétním objektům. Tato záložka plní funkci nástěnky či informační tabule, přístup na ni je možný ze všech konzol.

### **5.2.2.4 Výkazy**

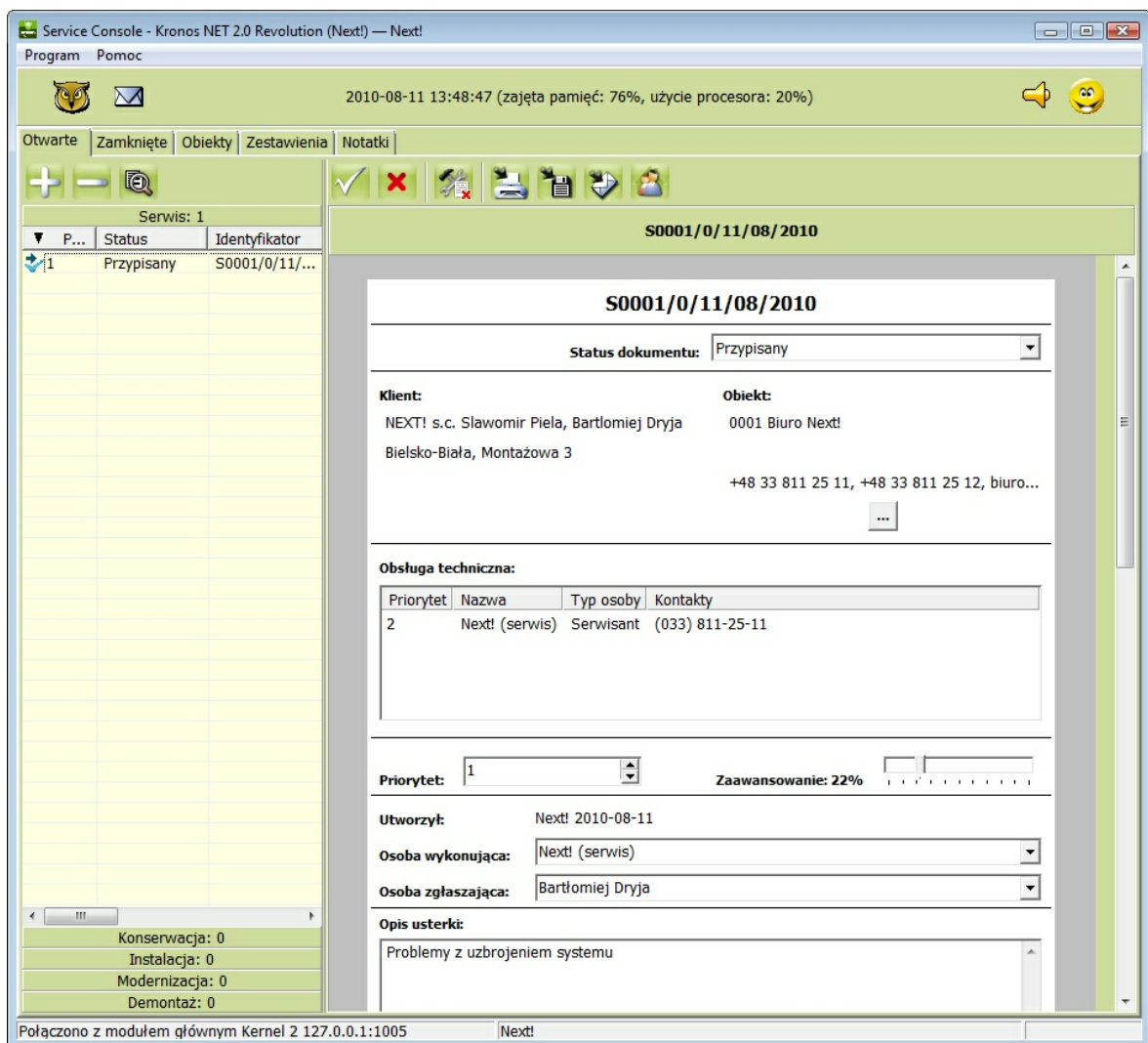
Na záložce Výkazy se tvoří různé výkazy a výpisy dat podle zadaných kritérií. Výkazy je možné seřadit podle vybraného sloupce. Vybráním výkazu ze seznamu se uživateli zobrazí požadovaná data.

### 5.2.2.5 Pošta

Prostřednictvím záložky Pošta se posílají zprávy všem uživatelům konzoly Zákazník, kteří jsou definováni v systému jako uživatelé s dálkovým přístupem. Pošta umožňuje posílání jak textových, tak obrázkových zpráv (např. scan dokladu). Podle toho, o jaký druh zprávy jde, se přizpůsobuje i prostředí okna. [10]

### 5.2.3 Service Console

Servisní konzola umožňuje jednak vydávání dokladů o servisních objednávkách, údržbě, instalacích, modernizaci a demontáži, jednak prohlížení archivovaných dokumentů. Dají se v ní prohlížet vybraná data objektů, generovat platby za objekt a také vytvářet výkazy různého druhu.



Obr. 29 Service Console [10]

### 5.2.3.1 Otevřené

V záložce Otevřené je možné přidávat, editovat a také odstraňovat následující objednávky pro objekty:

- Servis – servisní objednávky vytvořené v Service Console nebo v Monitoring Console (Výkaz vydaných servisních objednávek).
- Údržba – objednávky údržeb se vytvářejí v Service Console, nebo automaticky přes systém podle rozvrhu (Objednávky Údržeb).
- Instalace – objednávky instalací.
- Modernizace – objednávky modernizace.
- Demontáž – objednávky demontáží.

### 5.2.3.2 Uzavřené

Na záložce Uzavřené, máme přístup k archivním objednávkám příslušejícím ke zvolenému dnu. Pole není možné editovat, ani odstraňovat již uzavřené doklady. Tato funkce je užitečná pro uživatele, kteří provozují větší počet objektů, k rychlému vyhledávání zpráv.

### 5.2.3.3 Objekty

Z této záložce máme přístup k informacím, které se týkají objektů či zákazníků, nemáme zde však možnost tyto údaje měnit. V záložce se dají generovat dodatečné platby, které má zákazník uhradit. Na záložce se nacházejí tato pole:

- Seznam zákazníků – seznam zákazníků v systému,
- Seznam objektů – zobrazuje objekty patřící k určitému zákazníkovi. Dále při volbě:
  - Všechny objekty – zobrazuje všechny objekty zadané do systému
  - Nepřiřazené objekty – zobrazí seznam objektů, které nejsou přiřazeny žádnému zákazníkovi
- Pracovní oblast – oblast, kde máme přístup k údajům o zákaznicích nebo objektech.

### 5.2.3.4 Výkazy

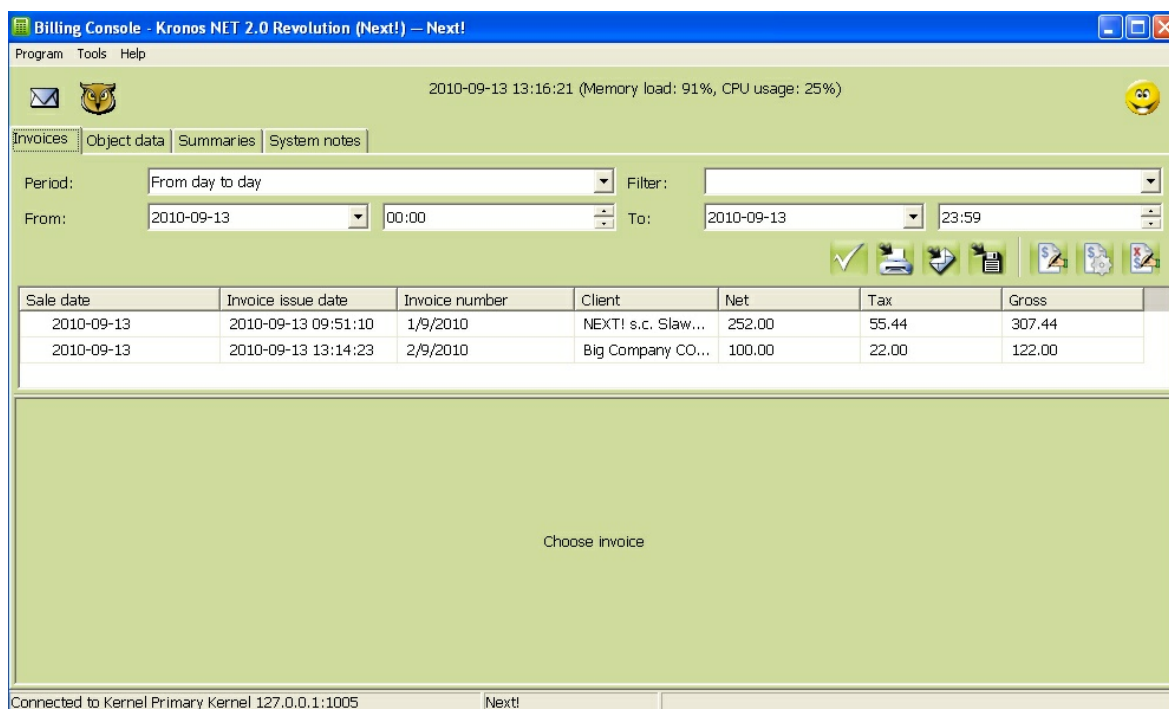
Záložka obsahuje výkazy provedených úkonů (servis, zálohování, montáž, modernizace, demontáž, další akce). Výkazový doklad je možné vytisknout, exportovat do souboru HTML nebo CSV, případně poslat mailem.

### 5.2.3.5 Poznámky

V záložce Poznámky jsou dříve zadané obecné poznámky, které se nevztahují k žádnému konkrétnímu objektu. Záložka slouží hlavně jako informační nástěnka pro zaměstnance. Poznámky je možné editovat nebo odstraňovat ze všech konzol. [10]

### 5.2.4 Billing Console

Konzola se používá pro fakturaci zákazníkům, provádí se na ní ruční i automatické přípravy faktur a také jejich kontrola na základě údajů získaných z jiných modulů. Umožňuje také spolupráci s externími systémy prostřednictvím mechanismu exportu faktur a importu pohledávek.



Obr. 30 Billing Console [10]

Konzola se skládá z následujících záložek:

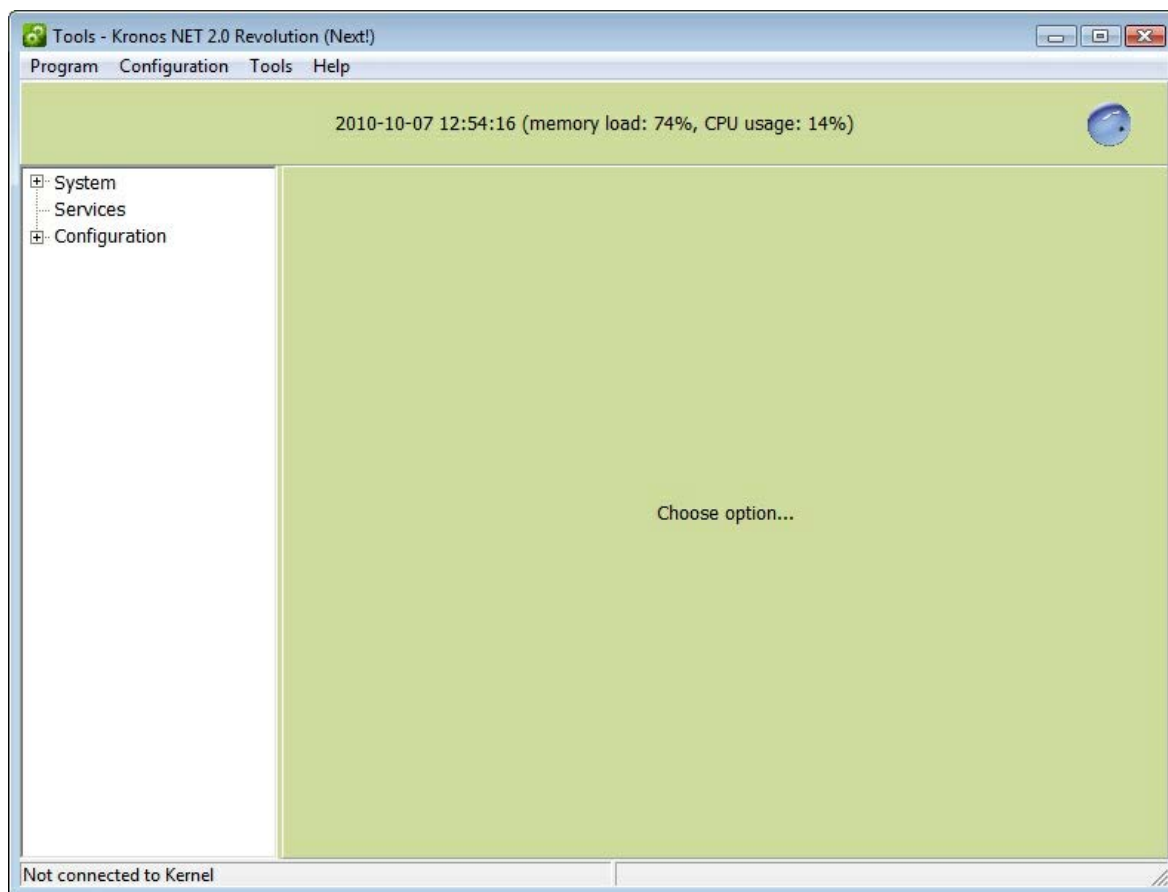
- Faktury – umožňuje prohlížet, upravovat a ručně nebo automaticky vytvářet či opravovat faktury.
- Data Objektů – umožňuje zobrazení dat zákazníků a předmětů týkajících se fakturace. Tato záložka obsahuje údaje:
  - Seznam zákazníků – zobrazuje seznam zákazníků v systému.

- Seznam objektů – po zvolení jména zákazníka vypíše systém seznam objektů, které jsou k této osobě přiřazené. Pokud zvolíme možnost:
  - Všechny objekty – zobrazí se všechny objekty zadané v systému.
  - Nepřiřazené objekty – zobrazí se seznam objektů, které nejsou přiřazeny žádnému zákazníkovi.
- Výkazy – náhled na výkazy spojené s vyúčtováním zákazníků např.:
  - výkaz nezaplacených faktur,
  - seznam zákazníků, kteří neplatí včas,
  - souhrn údajů o prodeji,
  - výkaz příjmů,
  - souhrn vytvořených faktur.
- Systémové Poznámky - poznámky vložené uživatelem systému. V záložce se zadávají obecné poznámky, které nejsou spojeny s žádným objektem. Mají funkci informační tabule. Poznámky je možné editovat nebo odstraňovat ze všech konzol.  
[10]

### 5.2.5 Configuration Tools

Distribuční balík Kronos NET obsahuje program Configuration Tools. Je to program, který slouží k diagnostice, řízení systému a konfiguraci jednotlivých modulů. Konfigurace se vždy vztahuje na moduly nainstalované na počítači, na kterém byl program Tools spuštěn.



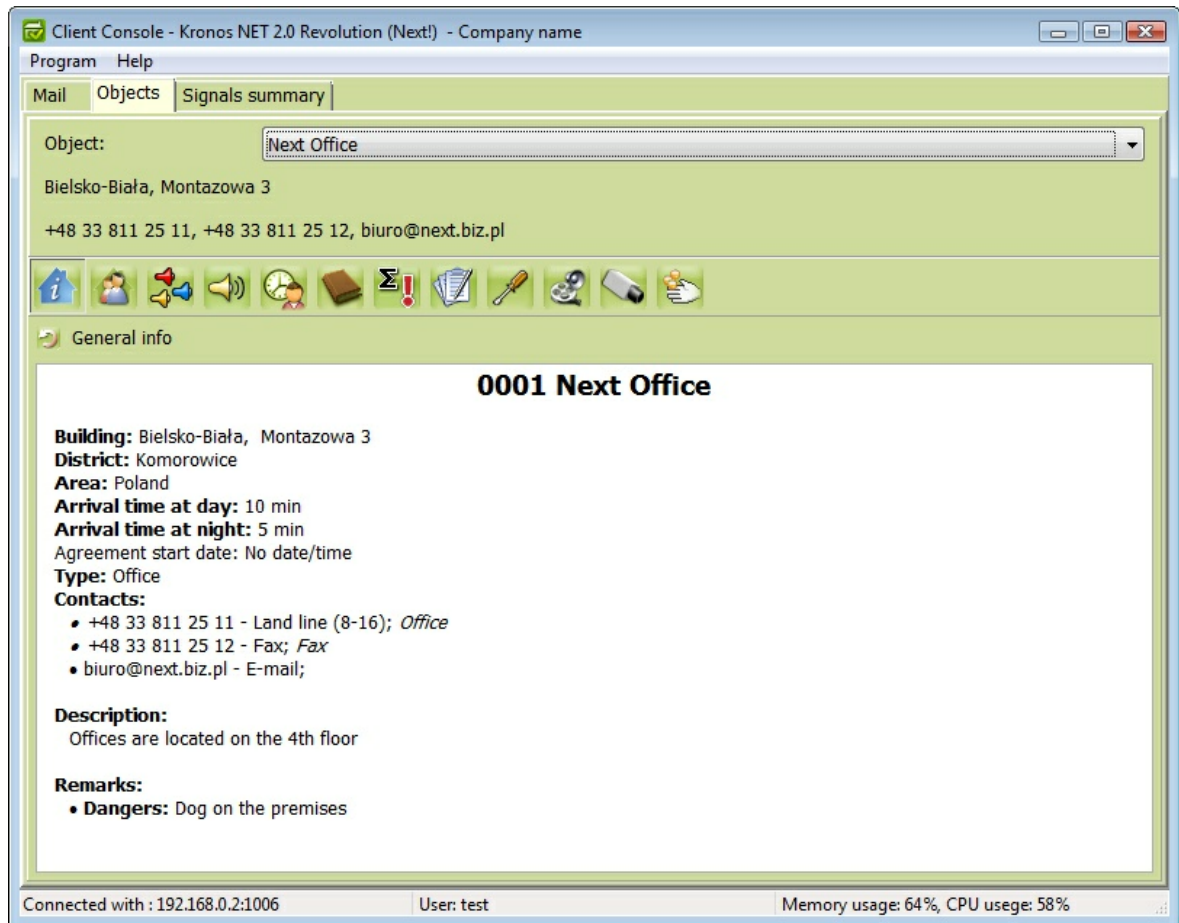


Obr. 31 Configuration Tools [10]

Tato konzola je klíčovým nástrojem pro IT oddělení, poskytuje kompletní přehled o aktuálním stavu práce systému, o průběhu událostí, provozuje rezervní centra. Veškerá aktivita může probíhat na vzdálený přístup prostřednictvím internetu. Tento modul by měl být k dispozici pouze pro zkušené uživatele, protože jeho nesprávné použití může způsobit poruchy systému a nevratné ztráty. [10]

### 5.2.6 Client Console

Konzola umožňuje náhled do dat objektů přiřazených k uživatelům, kteří se identifikují uživatelským jménem a heslem. To umožňuje výměnu zpráv mezi Konzolou editace a uživatelem. Při prvním spuštění této konzoly se zobrazí okno pro nastavení konzoly Zákazník, ve kterém je nutné nastavit přístupová data do ovladače konzoly Zákazník.



Obr. 32 Client Console [10]

Okno konzoly Zákazník obsahuje záložky:

- Pošta – vnitřní poštovní systém Kronos NET, používá se k výměně zpráv mezi konzolami Editace a Zákazník. Umožňuje odesílat textové a obrázkové zprávy, prohlížet je a odpovídat na ně.
- Objekty – data objektů zaregistrovaného zákazníka. Ze záložky objekty se může uživatel vzdáleně podívat na data vybraného objektu, ke kterému má přístup.
- Výkaz signálů – obsahuje zprávy o průběhu signálů ze zákaznickových objektů. Signály se dají vygenerovat buď za určitý časový úsek, nebo vyfiltrovat podle zadaných kritérií. [10]

### 5.2.7 Shrnutí – výhody systému Kronos NET

Síťové, softwarové řešení pro monitorovací a dohledová centra od společnosti Next! nabízí moderní platformu pro komplexní zpracování a správu přijímaných stavů z elektronických systémů, kterou lze s úspěchem použít všude tam, kde vzniká potřeba flexibility práce pod

vysokým zatížením systému, ale také všude tam, kde jsou jednotlivé prvky systému distribuovány napříč značně rozsáhlou oblastí.

System umožňuje současnou existenci až 100 000 a víc objektů na jedné instalační centrále systému a zároveň umožňuje další dělení na libovolný počet instalací v rámci jedné společnosti.

Podle mého názoru je instalace tohoto systému vhodná zejména pro střední a velké bezpečnostní agentury.

Kronos NET je jako celek zaměřen na automatizaci procesů spojených s řízením a rozhodováním při událostech v systému. Jeho hlavním cílem je usnadnit práci manažerům, dispečerům a účetním.

Poskytuje možnost vzdálené správy, raport informací o chybách, dynamické přepínání mezi záložními centry a samostatnou práci jednotlivých složek systému. Přitom nevyžaduje, aby se v paměti udržovaly zbytečné informace, a automaticky upozorňuje na důležité skutečnosti.

Jeho hlavní přínos by se dal shrnout do slov otevřenost a modularita. Na základě zákaznickových požadavků a potřeb je možné připojení a přenos různými přenosovými cestami.

System Kronos NET ve svých základních funkcích poskytuje také např. komplexní zařízení. Nezáleží na tom, zda je třeba zjistit polohu odcizeného vozidla, reagovat na příliš nízkou teplotu v chladírenském skladu, přijmout signál z mobilního tísňového hlásiče nebo sledovat obraz v systému CCTV, to vše lze provést pomocí jednoho standardizovaného rozhraní. Spojení funkcí monitoring objektů, vozidel, osob a pochůzek s kontrolou vykonávání servisů, revizí, montáží a také fakturace představuje systém mnohostranného použití. Jestliže platí, že Kronos NET dokáže na jednom stanovišti zpracovat až 100 000 a víc poplachů, pak lze jeho kapacitu v podmínkách českých a slovenských DPPC charakterizovat jako téměř „neomezenou“. S rostoucími nároky uživatelů přímo úměrně roste nárok na vývoj monitorovacích softwarů a na pracovníky DPPC, což následně zvyšuje náklady. Automatické odesílání zpráv pomocí SMS, e-mailů nebo jednoduché manipulace s konzolou tak pomáhá zkrátit čas školení nových pracovníků, čímž se naopak tyto náklady snižují. Díky modulární architektuře systému a mechanismu trvalé kontroly lze snadno vytvořit záložní DPPC, který slouží jako nouzový DPPC. Správce DPPC je vždy upozorněn přes systém pomocí zpráv SMS o všech problémech a díky

implementovaným nástrojům může okamžitě provést veškeré opravy. Systém dokáže automaticky nebo ručně přeposílat poplachy na další pracoviště DPPC, případně může vytvářet lokální monitorovací stanice pro potřeby hasičů nebo jiných zákazníků. Kronos NET je aplikace, která je otevřená všem dodavatelům různých zařízení – telefonních karet, rádiových a GSM/GPRS vysílačů, GPS jednotek a obchůzkových systémů. Uživatelé systému Kronos NET proto nejsou závislí na jednom dodavateli, díky tomu se významně snižují nákupní ceny těchto zařízení.

S ohledem na základní vlastnosti uvedené ve shrnutí může systém Kronos NET pomoci také podstatně snížit provozní náklady spjaté s chodem celé firmy, neboť není nutno dokupovat části DPPC a samostatné aplikace jako podklady pro fakturaci, řízení smluv, připomínkování, servisní protokoly, protože jsou již implementovány přímo v softwaru ve formě rozšiřujících modulů.

Takzvané Správcovské moduly mají možnost zadávání objektů do DPPC pomocí šablon zařízení a vzorových objektů, výpisů statistik a raportů klientům o prováděných službách, podrobných výpisů o změnách na objektech, řízení smluv, připomínkování, reklamace, atd.

V dispečerských modulech je možnost video-verifikace poplachů, také zadávání objektů do DPPC pomocí šablon, automatické reporty klientům, podrobné výpisy o změnách na objektech a činnostech operátorů. Jako po prve na světě v monitorovacích stanicích vzniklá možnost integrované kontroly obchůzky při využití čipů RFID.

Klientské moduly obsahují automatické vyřizování SMS dotazů, automatické výpisy v nastavených intervalech, internetový přístup a možnost odložení doby kontroly uzavření objektu, či řízení jednorázových nebo dočasných přístupů do objektu.

Servisní moduly mají možnost řízení servisních a montážních prací, automatické generování požadavků na revize dle uzavřené smlouvy, zadávání požadavků dispečerem přímo z DPPC, sledování průběhů prací, termínů a nákladů, tisk servisních listů.

Poslední dva moduly v rozšířené nabídce umožňují kontrolu stavu objektů přímo ve vozidle a účtování poplatků dle smlouvy, s možností připsání slevy, vyúčtování jednorázových úkonů.

### 5.3 Ohodnocení systémů – přínosy

Kronos NET od společnosti Next! a Net-G od NAM jsou vedoucími produkty na trhu PKB. Po důkladném seznámení se s těmito systémy mám dostatek informací na to, abych je mohl posoudit a vzájemně porovnat.

Nejprve bych se chtěl zmínit o typu činnosti a o politice, kterou vedou společnosti, které vyrábějí produkty popsané v mé diplomové práci. Společnost Next!, tvůrce programu Kronos NET je typická společnost orientující se na tvorbu a prodej softwaru. Naopak firma NAM se zabývá prodejem jak softwaru, tak i hardwaru svého výrobku. Obchodní politika společnosti NAM stála původně na prodeji systému NET-G, jehož funkčnost byla z větší části omezena na spolupráci s hardwarem vyráběným společností NAM. Politiku prodeje ale musela společnost změnit, když se na trh dostaly konkurenční softwary jako například Kronos NET, a musela rozšířit možnosti spolupráce programu NET-G s hardwarem konkurenčních společností.

Program Kronos NET je nástrojem integrujícím dohledové systémy, mimo jiné umí spolupracovat s každým komunikátorem. Vlastní bohatou databázi ovladačů k většině známých, populárních, nejčastěji používaných výrobků, které figurují na trhu. Kronos NET má tzv. „otevřené prostředí“. V praxi to znamená, že pokud by se našlo zařízení, se kterým by Kronos NET neuměl komunikovat, pošle operátor DPPC informace o zařízení na servisní oddělení spravující Kronos NET. Pracovníci servisního oddělení sdělí údaje o zařízení programátorům společnosti Next!. Programátoři problémové drivery zpracují a přidají je do databáze systému Kronos NET. Takové řešení software NET-G nenabízí.

Ve společnosti Next! stejně jako v NAM funguje nepřetržitě centrum péče o zákazníky. Kronos NET má jedinou výjimku, že má pro servis vytvořenou speciální Servis Conzole, která umožňuje přímou komunikaci operátora s technicko-programátorským oddělením společnosti. Díky tomu může operátor kdykoli požádat servis např. o:

- vytvoření nových driverů,
- objednání zakázky na servis,
- upgrade systému (pokud vyšla nová verze),
- dohled nad prací techniků při dálkových servisech.

Navíc správce DPPC dostává pomocí mailů, SMS informace o ukončení servisních prací na DPPC. Servis Kronos NET má spuštěný program, který umožňuje rychle zareagovat na vzniklou poruchu systému u operátora DPPC. Program hodnotí chování ze všech modulů u

operátora a při vzniku jakékoliv havárie (přeplnění disku, výpadek služby) program pošle informace o poruše na servis a oni to okamžitě opraví.

Nevýhodou implementace tohoto typu řešení je, že servisní pracovníci podpory softwarů mají přístup k počítačům a ke všem datům svých zákazníků (DPPC), kteří vedou zabezpečení objektů připojených na DPPC. Ohrožení spočívá v možnosti výskytu nepovoleného přístupu do systému DPPC, kde se můžou vyskytovat utajované informace o zabezpečených objektech. Proto by SW systémy měly poskytovat svým zákazníkům výběr úrovně zabezpečení přístupu servisních pracovníků podpory. Vzdálený přístup pomocí modulů se u NET-G provádí v „uzavřeném prostoru“. Data DPPC zákazníka jsou u NET-G zálohované v databázi. Díky tomu má společnost NAM plný přístup k datům DPPC zákazníka. Kdyby správce DPPC chtěl zabránit vzdálenému připojení společností NAM, zůstal by bez objektů. Řešený problém v systému Kronos NET je podobný. Rozdíl oproti NET-G je v tom, že vzdálený přístup společnosti Next! se dá v libovolné chvíli zablokovat a hlídání objektů lze provozovat bez nutnosti poskytování informací o objektech pro servisní oddělení Kronos NET.

Společnost NAM původně prodávala na software NET-G licence, které umožňovaly provoz systému na vlastním počítači. Taková investice do programu představovala pro osobu začínající podnikat v oboru PKB obrovské náklady. Kronos NET tuto cenovou politiku změnil, když zavedl měsíční licenční poplatky za provoz softwaru. Cena softwaru Kronos NET se odvíjí od počtu spravovaných objektů. V poslední době NAM zavedla podobný cenový systém. I když od společností Next! dostáváme za základní cenu kompletní systém Kronos NET se všemi konzolami. NET-G nabízí v základním řešení jen dvě základní konzoly: monitorovací a driverů. Za další moduly si musí správce DPPC připlatit.

Další změnou, kterou program Kronos NET vynutil svým jednáním na konkurenci, je systém spravování poplachů. U NET-G to dříve bylo tak, že když na monitorovací konzolu došel poplach, byl zpracován jako „Událost“. Vypadalo to tak, že ve chvíli, kdy přicházelo větší množství poplachů, vznikala na DPPC zmatek. Program vydával hlasité zvuky až do doby, než se začaly řešit všechny poplachu na jednou. To operátorovi DPPC znemožňovalo správnou práci. Situace se změnila poté, co Kronos NET zavedl systém zpracování poplachu jako „Akce“. Princip je ten, že v době, kdy dojde poplach na Monitorovací konzolu, může ho operátor v klidu zpracovávat a při vzniku dalších poplachů z jiných objektů, je o dalším poplachu jen informován. Na operátorovi pak záleží, jak bude

poplarchy dále řešit. Operátor může poplarchy předat jiným operátorům, nebo pracovat se všemi najednou. Velkou výhodou systému Kronos NET je samostatné zpracování poplachu. Smyslem tohoto systému je, aby operátor DPPC co nejrychleji zpracoval přicházející poplach. Systém upozorňuje pouze na ty poplarchy, které má příslušná osoba řešit, ukazuje operátorovi jen skutečně ty nejdůležitější informace o poplachu na objektu.

Každý operátor DPPC se musí umět při práci vyrovnávat se stresem. Není to jednoduché, ale od operátora se požaduje solidní, zodpovědná, efektivní práce a rychlá reakce na vzniklá nebezpečí. Úspěch akce záleží z velké části na operátorovi DPPC. Proto by měl pracovat s co nejcitlivější monitorovací konzolou, kde je všechno uspořádané a snadno dostupné. V malých a středních společnostech PKB si operátoři DPPC zvyknou na práci s prostředím všech konzol během několika dní. Ve velkých společnostech, které zaměstnávají několik set pracovníků, není čas na dlouhá školení a zaučování nových pracovníků. Podle mého názoru má Kronos NET oproti NET-G přehlednější, jednodušší konzolu, která umožňuje rychlou adaptaci nového pracovníka v novém prostředí a zároveň pomáhá zaměstnavatelům ušetřit peníze a čas za školení.

Velmi podstatnou schopností softwaru v prostředí DPPC je možnost filtrovat informace. Je to funkce operátory DPPC často využívaná. V NET-G je třeba filtry předem nastavit, což je velmi náročné, vyžaduje to od operátora znalosti a schopnosti, které většinou nemá a musí je nejprve získat. Kronos NET problém filtrů vyřešil pomocí naprogramování funkce podobné vyhledávači Google. Informace se po zadání klíčových slov filtrují (znaky nemusí stoprocentně odpovídat hledané informaci, filtr vyhledá data, která se zadaným slovům nejvíce podobají). Navíc Kronos NET, na rozdíl od NET-G, ukládá do své databáze všechny a ne jen vybrané systémové údaje. Díky tomu se správce DPPC může kdykoliv pomocí filtru podívat do archivu a zjistit např. kdo ze zaměstnanců kdy co udělal při práci se systémem Kronos NET.

Další věcí, která v nabídce systému NET-G evidentně chybí, je Fakturační modul. Kronos NET tento modul zákazníkům nabízí. Modul obsahuje širokou škálu možností umožňujících jednoduché a čitelné zúčtování DPPC zákazníků.

Je vidět, že Kronos NET byl vytvořen nejen pro správce DPPC, ale také s ohledem na zákazníky DPPC. Nabízí jim speciální konzoly, díky kterým může zákazník kdykoli zkontrolovat stav svého hlídaného objektu. Tvůrci Kronos NET mysleli na to, aby bylo možné posílat zákazníkům veškeré informace, které si jen budou přát (poplach, zpožděný poplach, vyslání zásahu) pomocí SMS, e-mailů. Kronos NET nemá žádná omezení týkající

se tohoto typu posílaných zpráv. I když v NET-G je také možnost poslání SMS, je jejich počet i typ informací omezen a je nutné si za tuto službu extra připlatit.

Společnost NEXT! v poslední době publikovala novou verzi programu Kronos NET 2.1, která obsahuje hodně funkcí ulehčujících používání a provoz systému, např.:

- Videokonzola – navržena pro provádění videodohledů, tvoření vlastních náhledů z vlastních IP kamer (pro denní i noční změny).
- Tutch Monitoring Console – dotekové operační prostředí bez používání klávesnic.
- Konzola Zákazník – nové řešení, možnost přístupu na konzolu pomocí prohlížeče a rozšíření pravomoci klienta (výpisy zpráv, editování kontaktů při potvrzení editace přes operátora DPPC).
- Možnost kontrolování polohy vozidel v oblastech.

Po přezkoumání softwarů a politik firem jsem mohl vytvořit tabulku (příloha č.1), která obsahuje řadu kritérií, které umožňují porovnání jakýkoli softwarů DPPC. Kritéria, které se nacházejí v tabulce jsou funkce jaké by měl každý software DPPC obsahovat. Tyto funkce jsou rozděleny na méně a více významné s pohledu správců, uživatelů, provozovatelů softwarů DPPC. Porovnání softwarů proběhlo tak, že každé funkci jsem přidělil body, které po sčítání dali koncový výsledek. Hodnotu bodů jsem stanovil ve stupnici hodnocení (příloha č.2).

Výše prezentované porovnání a provedené tabulkové sestavení (příloha č.1) směřuje k jednoznačnému závěru, že jednoznačným vítězem srovnání je Kronos NET. Má modernější, bohatší škálu možností než konkurenční systém. Politika prodeje i používání je pro zákazníka, operátora i samotného správce DPPC uživatelsky příjemnější. Tento závěr potvrzuje i fakt, že produkt Kronos NET je nejčastěji implementovanou dohledovou platformou v největších polských společnostech, od kterých dostává nejvyšší hodnocení za provoz v referenčních správách.



## ZÁVĚR

Po zpracování teoretické a praktické části mé diplomové práce jsem dospěl k následujícím závěrům.

V teoretické části začínám kapitolou Historie DPPC. Již v roce 1853 byly Edwinem Holmesem vytvořeny první DPPC v New Yorku, v Československu došlo k první použití zabezpečovací techniky v roce 1933. V době druhé světové války byla tvorba a instalace bezpečnostních systémů plně v kompetenci Ministerstva vnitra, pak převzal oprávnění nad ochranou osob a majetku Sbor Národní Bezpečnosti. V osmdesátých letech to pak byla jeho složka veřejná bezpečnost. Komerčním dodavatelem byla společnost TESLA. Největšího rozmachu dosáhly DPPC hlavně v 50. – 60. letech. V roce 1970 se přidala i skupina zahraničních výrobců. Pak došlo k obohacení Českého trhu. Vývoj vedl ke změnám systémů a zařízení. Na začátku roku 1990 došlo k nárůstu podnikajících subjektů, a tím pádem také ke vzniku SBS. To umožnilo rozvoj DPPC na trhu PKB také po stránce legislativní. Normy, které platí v České republice od roku 2011, nařizují změnu dřívější zkratky PCO na DPPC, případně PPC podle přesného překladu anglické zkratky ARC.

Zjistil jsem, že dnešní poplachová přijímací centra v PKB nabízejí velký počet služeb pro své zákazníky. Bezpečnostní agentury se časem stávají komplexními a do svých služeb zahrnují nejen provozování DPPC, ale také tvorbu návrhů, instalace systémů PZTS, přístupových, CCTV, EPS systémů, převozů cenin atd. Pro přenos poplachových signálů na DPPC se pořád využívá telefonní linka, rádiový přenos, GSM/GPRS systém. Největší poptávka je v dnešní době po rádiových sítích. Z hlediska vybavení DPPC je systém po stránce hardwarové i softwarové na dosud nejvyšší technické úrovni. Provozovatelé DPPC se snaží poskytovat svým zákazníkům vysokou kvalitu služeb za co nejatraktivnější cenu. Proto se společnosti, které tvoří softwarové a hardwarové systémy, předstihují ve vydávání nových aktualizací ke svým systémům. Díky tomu se zvyšuje bezpečí a kvalita poskytovaných služeb.

Aby kvalita nabízených služeb v celém prostředí PKB neklesla pod určitou úroveň, jsou stanoveny normy, jako např.: ČSN EN 50131, ČSN EN 50518 1-3. Díky tomu mají provozovatelé DPPC kompletní přehled např.: o projektových požadavcích, technických řešeních a také o požadavcích týkajících se podnikání v oblasti DPPC.

V poslední teoretické kapitole diplomové práce se soustředím na zjištění směru vývoje DPPC. Po pečlivé analýze prostředí PKB jsem zjistil, že úroveň technického pokroku hardwaru i softwaru je na vysoké úrovni, což přispívá k úspoře lidí ve společnostech DPPC. Prostředí DPPC využívá prověřené bezpečnostní metody provozu založené na stanovených normách. Politika společností DPPC měla často vliv na kvalitu poskytovaných služeb nabízených zákazníkům. Díky vznikající konkurenci na trhu se kvalita služeb DPPC bude stále zlepšovat a to bude mít vliv na naše bezpečí. Společnosti budou díky zvyšující se komplexnosti vnitřních struktur nabízet svým zákazníkům stále větší a větší rozsah služeb.

Po zpracování teoretické části jsem přistoupil k části praktické, ve které jsem se zabýval testováním dvou na první pohled podobných systémů, a to NET-G a Kronos NET. Poté, co jsem provedl komplexní analýzu, kontrolu všech systémových modulů a analýzu prodejní politiky obou společností, které softwary vyrábějí, vyvodil jsem závěry a porovnávací tabulku a graf (příloha č. 1, 2). Z mého výzkumu vyplývá, že Kronos NET je lepší systémový software pro DPPC než NET-G. Kronos NET je podle mého názoru díky své průhlednosti, jednoduchému ovládní, komplexnosti, rozsáhlé systémové architektuře a dodatečným službám v rámci servisu softwaru, úspory finančních nákladů a lidí jedním z nejlepších systémů pro správce DPPC nabízených na trhu. K závěru jsem dospěl po dlouhé práci a důkladné analýze obou systémů. Díky spolupráci se zástupci společností, které systémy dlouhodobě používají, jsem získal i pohled ze strany dlouhodobých provozovatelů DPPC. Jako velice užitečné hodnotím také konzultace se servisními techniky, kteří na systému pracují. Jejich zkušeností byly pro mě velmi užitečné při vytváření vlastního názoru na téma praktické funkcionality jednotlivých systémů.

## ZÁVĚR V ANGLIČTINĚ

After processing of theoretical and practical part of my dissertation I came to the following conclusions.

In theoretical part I start with chapter History of ARC. Edwin Holmes created first ARC in New York in 1853, the first implication of security of technology in Czechoslovakia was used in 1933. Creation and installation of I&HAS was fully in competence of Home Office during the WWII, then Sbor Národní Bezpečnosti (SNB) took the permission of protection people and property. In 80's it was its component Veřejná bezpečnost (VB). TESLA was a commercial supplier. The biggest rise of ARC was in 50's – 60's. A group of foreign producers joined in 1970. Czech market was enriched after that. The evolution led to changes of systems. In the beginning of 1990 business entities was increasing, and thus to formation of SBS. That enabled ARC to expand in the market of PKB from the legislative point of view. Standards which are valid in the Czech Republic since 2011 order to change previous abbreviation from PCO to DPPC, alternatively to ARC according to the right translation from English.

I found out that contemporary Alarms Receiving Centers in PKB offers amount of services for its customers. Safety agencies become complex and they include not only running of ARC as their service but also creation of proposals, installation of I&HAS, EPS systems, transportation of fee stamps etc. ARC uses telephone line, radio transfer, GSM/GPRS system for its transfer of alarm signals. Nowadays, the biggest demand is a radio net. According to ARC equipment is system in terms of hardware and software on the highest technical level. ARC operators try to offer high quality service to their customers. That is the reason why companies creating software and hardware systems are passing in releasing new updates to their systems. Thanks to this the safety and quality of providing services is increasing.

To make quality of providing services in PKB stable there are standards, e. g. ČSN EN 50131, ČSN EN 50518 1-3. Thanks to this ARC operators have complete awareness about project requests, technical solutions and requests about business in ARC.

In the last theoretical chapter of my dissertation I focus on developing determination of ARC. After careful analysis of environment in PKB I found out that level of technical progress of hardware and software is on high level which contributes to saving people in ARC companies. Environment in ARC takes advantage of checked safety methods

established on given standards. I remarked that policy of ARC influenced quality of services offered to customers. Thanks to emerging competition is quality of ARC going to be improved and that will influence our security. Companies will offer bigger and bigger amount of services because of growing complexity of inner structure.

After processing theoretical part I proceeded to practical part which is occupying with testing of two at first sight same systems. These are NET-G and Kronos NET. I tested these systems on the computer and I helped myself with their manuals. After that I made a complex analysis, checked system modules and analysis of selling policy of both companies that produce software I made a conclusion. The result is that Kronos NET is better system software for ARC than NET-G. In my opinion Kronos NET is thanks to its transparency, simple control, complexity, extensive system architecture and added services one of the best system for ARC admin offered in the market that I know. These are conclusions resulting of long work and precise analysis of both systems. Meeting representatives of companies where the usage of software systems is long-term I have gain a perspective from the side of retentive ARC operators. A consultation with service technician working on those systems was beneficial. Their experience was very useful for me in creating of my own opinion on topic of practical functionality of each system.

**SEZNAM POUŽITÉ LITERATURY**

- [1] *Naše téma: Monitorování objektů*. Magazín SECURITY, květen/červen 2003, roč. X, č. 3/2003, s. 7-27. ISSN 1210-8723
- [2] VYORÁLEK, Radim. *Pulty centralizované ochrany*. Univerzita Tomáše Bati ve Zlíně, 2005. UTB Zlín. Bakalářská práce.
- [3] ZAPLETAL, Pavel. *Perspektiva PPC*. Univerzita Tomáše Bati ve Zlíně, 2009. UTB Zlín. Diplomová práce.
- [4] LUKÁŠ, L. et al. *Bezpečnostní technologie, systémy a management I*. 1. vyd. Zlín: VerBuM, 2011. ISBN 78-80-87500-05-7.
- [5] ČSN EN 50518-1. *Dohledová a poplachova přijímací centra – Část 1: Umístění a konstrukční požadavky*. Praha: Český normalizační institut, 2010.
- [6] ČSN EN 50518-2. *Dohledová a poplachova přijímací centra – Část 2: Technické požadavky*. Praha: Český normalizační institut, 2011.
- [7] ČSN EN 50518-3. *Dohledová a poplachova přijímací centra – Část 3: Pracovní postupy a požadavky na provoz*. Praha: Český normalizační institut, 2012.
- [8] NAM systém, a.s., Orlová. *Monitorovací software NET-G: Manuál správce*. 1.22. vyd. Orlová, 2012.
- [9] ISDN. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2012, 26-02-2012 [cit. 2012-02-29]. Dostupné z: <http://cs.wikipedia.org/wiki/ISDN>
- [10] NEXT! s.c., Bielsko-Biala. Sławomir Piela, Bartłomiej Dryja - *Software Product List KRONOS NET 2*, 2011.
- [11] KINDL, J. *Projektování bezpečnostních systémů I*. 1. vyd. Univerzita Tomáše Bati ve Zlíně, Zlín 2004.
- [12] NAM systém, a.s. *Pult Centrální Ochrany NAM GLOBAL: Výuková Skripta*. Orlová.
- [13] GPRS. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-2012, 20-03-2012 [cit. 2012-03-29]. Dostupné z: [//pl.wikipedia.org/wiki/GPRS](http://pl.wikipedia.org/wiki/GPRS)

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

ARC	Alarm Receiving Centre (Dohledové Poplachové Přijímací Centrum).
BRI	Basic Rate Interface (Základní přípojka).
CCTV	Closed Circuit Television (Kamerový Systém).
CSV	Comma Separated Values (Hodnoty Oddělené Čárkami).
ČR	Česká Republika.
DNS	Domain Name Systém (Hierarchický Systém Doménových Jmen).
DPPC	Dohledové Poplachové Přijímací Centrum.
DTMF	Dual-tone multi-frequency (Tónová volba).
EPS	Elektrická Požární Signalizace.
GPS	Global Positioning System (Globální Pozemní Systém).
GPRS	General Packet Radio Service (Všeobecná Paketová Rádioová Služba).
GSM	Global System for Mobile Communication (Globální Systém pro Mobilní Komunikaci).
HW	Hardware.
IP	Internet Protocol (Komunikační Protokol).
IZTS	Integrated Services Digital Network (Digitální síť integrovaných služeb).
IZS	Integrovaný Záchranný Systém.
JTS	Jednotná Telefonní Síť.
MDC	Multimediální Dohledové Centrum
PCO	Pulty Centralizované Ochrany.
PKB	Průmysl Komerční Bezpečnosti.
PPC	Poplachové Přijímací Centrum.
PRI	Primary Rate Interface (Primární Přípojka).
PZTS/I&HAS	Poplachový Zabezpečovací a Tísňový Systém (Intruder and Hold up Alarm Systém).

---

RFID	Radio-Frequency Identification (Identifikace na Rádiové Frekvenci).
SBS	Soukromá Bezpečnostní Služba.
SW	Software.
TCP	Transmission Control Protocol (TCP protokol).
UPD	User Datagram Protocol (UPD protokol).
UTC	Coordinated Universal Time (Koordinovaný Světový Čas).

**SEZNAM OBRÁZKŮ**

Obr. 1 Schéma přenosu a vazeb u DPPC.....	23
Obr. 2 Telefonní karta GS51 od firmy Matylda .....	24
Obr. 3 Schéma rádiové sítě GLOBAL od fy. NAM .....	28
Obr. 4 Blokové schéma DPPC .....	30
Obr. 5 Princip handshake .....	33
Obr. 6 Schéma funkce střežení .....	42
Obr. 7 Schéma architektury modulu NET-G a hardwaru NAM GLOBAL.....	45
Obr. 8 Systémové okno .....	46
Obr. 9 Okno běžných událostí .....	47
Obr. 10 Odkazů z událostí .....	49
Obr. 11 Okno významných událostí .....	50
Obr. 12 Okno průzkumníka objektů .....	52
Obr. 13 Převodní tabulka .....	54
Obr. 14 Větev hlídaných objektů .....	56
Obr. 15 Nastavené automatické hlídání uzavřeného objektu .....	58
Obr. 16 Formulář zákazníka .....	59
Obr. 17 Základní okno modulu AppDriver .....	60
Obr. 18 Okno Spojení s SQL .....	61
Obr. 19 Hromadné zpracování tiskových sestav .....	62
Obr. 20 Konfigurace HW klíče .....	63
Obr. 21 Modul WatchDog .....	64
Obr. 22 Modul Net-G Statistika .....	65
Obr. 23 Schéma architektury modulu KronosNET .....	72
Obr. 24 Hlavní obrazovka Monitoring Console – složka Alarmů. ....	75
Obr. 25 Přicházející poplach.....	77
Obr. 26 Mapa objektu Navigo .....	79
Obr. 27 Data Edit Console .....	80
Obr. 28 Úprava dat objekt/osoba .....	83
Obr. 29 Service Console .....	85
Obr. 30 Billing Console .....	87
Obr. 31 Configuration Tools .....	89
Obr. 32 Client Console .....	90



## SEZNAM PŘÍLOH

- P.I Tabulka a Graf na porovnání softwarů pro DPPC.
- P.II Stupnice hodnocení softwarů.

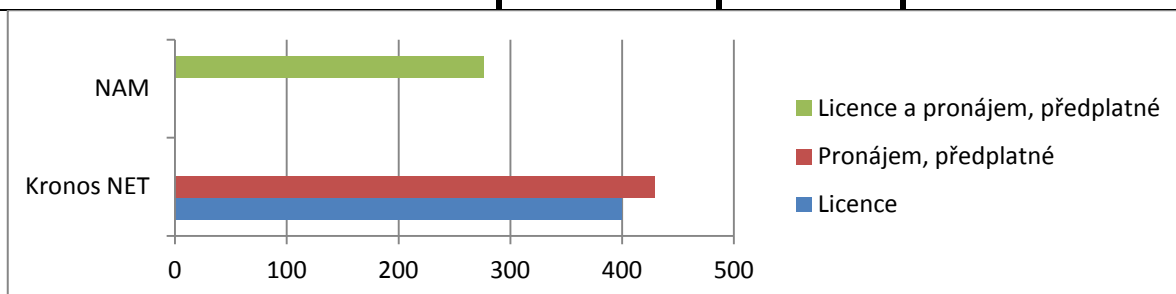
## PŘÍLOHA P I: TABULKA A GRAF NA POROVNÁNÍ SOFTWARE PRO DPPC

		KRONOS NET				NET-G	
Počet objektů	Od	500		5	1	5	
	Do	+100 000		5	+65 000	3	
Doporučení	Velkost firem	Střední až velké		3	Všechny typy	5	
Náklady – služby		Licence		Pronájem, předplatné		Licence	Pronájem, předplatné
	<i>Základní program</i>	<i>ANO – Všechny konzole</i>	<i>10</i>	<i>ANO – Všechny konzole</i>	<i>10</i>	<i>ANO – konzole monitoringu a driverů - zbytek dle potřeb zpoplatněný</i>	<i>5</i>
	<i>Servis</i>	<i>NE</i>	<i>0</i>	<i>ANO</i>	<i>10</i>	<i>ANO -6 měsíců zdarma</i>	<i>8</i>
	<i>Aktualizace programu</i>	<i>NE</i>	<i>0</i>	<i>ANO</i>	<i>10</i>	<i>ANO</i>	<i>10</i>
	<i>Možnost nahlášení vlastních modifikace</i>	<i>NE</i>	<i>0</i>	<i>ANO</i>	<i>10</i>	<i>NE</i>	<i>0</i>
Komunikační kanály	JTS	ANO		5	ANO	5	
	GSM/GPRS	ANO		5	ANO	5	
	Rádio	ANO		5	ANO	5	
	Internet	ANO		5	ANO	5	
Bezpečnost	<i>Možnost zablokování a odblokování vzdáleného přístupu na db. server. Bez ztráty dat o objektech</i>	ANO		10	NE	0	
	<i>Šifrovaně transmise</i>	ANO		10	ANO	8	
	<i>Ochrana disků před útratou paměti</i>	ANO		10	ANO	10	
	<i>Rezervní centra automaticky zapínané</i>	ANO		10	ANO	10	
	<i>Systém „stínování databáze“</i>	ANO		10	ANO	8	

Přístup		Místní		Dálkově		Místní		Dálkově	
		ANO	10	ANO	10	ANO	10	ANO	10
	<i>PC</i>	ANO	10	ANO	10	ANO	10	ANO	10
	<i>PDA</i>			ANO	8			NE	0
	<i>Dotykový displej</i>	ANO	10			NE	0		
<b>Výkon</b>	<i>Rychlost zpracování zpráv ze 100 000 objektů</i>	100 zpráv/s			10	n/a		8	
<b>Kompatibilita</b>	<i>Počet typů spolupracujících ústředěn PZTS (ovladače pro komunikaci)</i>	50+			10	13+		5	
	<i>Možnost přidávání nových driveru PZTS</i>	ANO			10	ANO		8	
<b>Monitoring</b>	<i>Budov</i>	ANO			10	ANO		8	
	<i>Vozidel</i>	ANO			10	ANO		10	
	<i>Strážných na objektech</i>	ANO			10	NE		0	
	<i>Prostředí (teploty, vlhkostí)</i>	ANO			10	ANO		8	
	<i>Verifikace poplachu pomocí IP kamer, fotek</i>	ANO			8	NE		0	
	<i>Prodejních automatů</i>	ANO			5	ANO		5	
	<i>Času práce</i>	ANO			8	ANO		8	
	<i>Automatické zasílání zpráv pomocí SMS, e-mail</i>	ANO – neomezeno			10	ANO – omezeny počet zpráv zdarma		5	
	<i>Možnost zálohování přichozích telefonických hovorů</i>	ANO			5	n/a		3	
	<i>Systém raportování o událostech na objektech</i>	ANO			5	ANO		5	
	<i>Bezobslužná činnost stanice monitoringu</i>	ANO			8	NE		0	
	<i>Jednoduchá konzola pro Policii, Hasiče</i>	ANO			3	NE		0	

<b>Servis</b>	Spolupráce pro	<i>Konservace – bezpečný, spolehlivý provoz</i>	ANO	10	ANO	8
		<i>Konsultace</i>	ANO	10	ANO	10
		<i>Modernizace</i>	ANO	10	ANO	8
		Pomoc při instalace a reinstalace poplachových systémů na objektech	ANO	3	NE	0
	<i>Vzdálený servis ARC</i>		ANO	10	ANO	10
	Výpisy servisní		ANO	5	n/a	3
<b>Účetnictví</b>	<i>Posílání faktur</i>	<i>Automatické</i>	ANO	8	NE	0
		<i>Manuální</i>	ANO	8	ANO	8
	Mechanismus tvoření ceníků a slev		ANO	5	NE	0
<b>Management</b>	<i>Dálkový přístup</i>	<i>Servis</i>	ANO	10	ANO	8
		<i>Zákazník ARC</i>	ANO	10	NE	0
		<i>Správce ARC</i>	ANO	10	ANO	8
	Informování o událostech pomocí SMS		ANO - bezplatné	5	ANO – jenom 10 sms-ek/měsíčně – bezplatné	3
	Indikátor výkonnosti		ANO	3	NE	0
<b>Architektura</b>	<i>Síťová</i>		ANO	10	ANO	8
	Samostatná činnost modulů		ANO	5	NE	0
	<i>Zabezpečená</i>		ANO	10	ANO	8
<b>Filtrace</b>	Manuální (Programování vlastních filtrů)		NE	0	ANO	3
	<i>Automatická (jako např. Google systém)</i>		ANO	10	NE	0

Softwarové požadavky	Operační systém	2000/2003/XP/Vista/7	ANO	3	ANO	3
	Databáze	MSDE, MS SQL expres 2000/2005/2008; MSDE, MS SQL 2000/2005/2008	ANO	3	ANO	3
	PDA	PDA Windows Mobile 5/6, Comact Net 2.0.	ANO	3	NE	0
<b>Celkový počet bodů</b>			<b>Licence</b>	<b>Pronájem, předplatné</b>	<b>Licence a pronájem, předplatné</b>	
			<b>399</b>	<b>429</b>	<b>276</b>	



## PŘÍLOHA P II: STUPNICE HODNOCENÍ SOFTWARE

Stupnice hodnocení softwarů		
		Body
<i>Významné funkce(modrá barva)</i>	<i>Výborně - (nejmodernější, technologická novinka, velmi spolehlivá, bezpečná práce, „neomezenost“)</i>	<i>10</i>
	<i>Dobře - (moderní, docela nová technologie, spolehlivá, bezpečná práce, n/a)</i>	<i>8</i>
	<i>Dostatečně- (klasická, stará technologie, málo spolehlivá, bezpečná práce)</i>	<i>5</i>
Méně významné funkce	Výborně - (nejmodernější, technologická novinka, velmi spolehlivá, bezpečná práce, „neomezenost“)	<b>5</b>
	Dobře - (moderní, docela nová technologie, spolehlivá, bezpečná práce, n/a)	<b>3</b>
	Dostatečně- (klasická, stará technologie, málo spolehlivá, bezpečná práce)	<b>1</b>