DICOM INFORM

DIGITÁLNÍ A KOMUNIKAČNÍ TECHNIKA - DIGITAL & COMMUNICATION TECHNOLOGY

ČÍSLO 10 (2/00)
ČERVEN 2000

V TOMTO ČÍSLE

OCHRANA INFORMACÍ V RÁDIOVÉ KOMUNIKACI 1

NOVINKY

Řídicí rozhraní CI 13 2

Utajovač EU 13 3

TEORETICKÁ ČÁST

Utajovače řeči pro taktické rádiové stanice 5

ZÁKAZNICKÁ RUBRIKA

Ovládání rádiové stanice z PC 7

REKLAMNÍ ČÁST, ADRESY

IDEE 2000, DSA 2000 8

OCHRANA INFORMACÍ V RÁDIOVÉ KOMUNIKACI

Snahu utajit přenášené informace je možné v dějinách sledovat již od antiky. Pravděpodobně se jí lidstvo zabývá od okamžiku objevení písma, které dovolilo přenášet zprávy na větší vzdálenost. Velmi brzy se ukázalo, že ochrana dat jednoduchými prostředky (např. výběr kurýrů a jejich fyzická ochrana) nepostačuje. Proto byly hledány způsoby, jak učinit dokument pro jinou osobu než určeného příjemce nečitelným. Základním způsobem se stalo šifrování, tedy převod otevřeného textu do utajené podoby pomocí klíče. Metody šifrování se po celou dobu vývoje zkvalitňovaly. Současně se také zkvalitňovaly metody jak zašifrovanou informaci zjistit. Tento dlouhodobý rozvoj přinesl vznik samostatného vědního oboru - kryptologie.

Na utajovací systémy je kladena řada požadavků. Základní z nich byly definovány v roce 1883. Dnes jsou podle autora označovány jako požadavky Kerckhoffovy:

1. Systém by měl být, když ne teoreticky neprolomitelný, neprolomitelný prakticky.
2. Prozrazení detailů systému by nemělo způsobit problémy korespondentům.
3. Klíč by měl být zapamatovatelný bez poznámek a snadno měnitelný.
4. Kryptogram by měl být přenositelný pomocí telegrafu.
5. Kryptovací přístroj by měl být přenosný a obsluhovatelný jednou osobou.
6. Systém by měl být snadný, nevyžadovat znalost velkého počtu pravidel ani nezpůsobovat duševní námahu obsluhy.

Až do minulého století byl problém omezen na utajení psaného textu. Příchodem telefonu a zejména rádiového spojení vznikl požadavek i na utajení informací přenášených těmito médii.

Další nové požadavky přineslo masivní zavedení výpočetní techniky do zpracování informací. Na těchto prostředcích se informace vyskytuje v určitých stádiích zpracování v otevřené formě. To si vynucuje činit opatření zabraňující využít elektromagnetického vyzařování z těchto prostředků k odposlechu a vyhodnocení obsahu. Tato opatření bývají rázu pasivního (stínění) i aktivního (vyzařování šumového spektra do okolí těchto prostředků). Reálné nebezpečí takového odposlechu je však dnes vesměs přeceňováno v důsledku reklamních aktivit firem, které se zabývají výrobou prostředků pro tuto oblast.

Výpočetní technika také zásadním způsobem ovlivnila jak možnosti šifrování, tak možnosti prolomení šifer, protože poskytla možnost realizovat systémy dešifrování „hrubou silou“, tj. zkoušením použití všech možných podob klíče. Právě odolnost proti prolomení šifry tímto způsobem je důležitým parametrem při hodnocení utajovacích algoritmů.

Vzhledem k charakteru výrobků společnosti DICOM je logické, že hlavní pozornost je věnována prostředkům pro utajení řečové korespondence v taktické radiokomunikaci. Zde jsou na utajovací zařízení kladeny další požadavky, o kterých se více zmiňuje tématický článek v tomto čísle.

Ing. Jiří Krča
technický ředitel, tel.: 0632/522502

ŘÍDICÍ ROZHRANÍ CI 13

Řídicí rozhraní CI 13 je určeno pro zprostředkování a řízení zpráv mezi osobním počítačem a rádiovou stanicí RF 13. Mechanicky se připojuje k rádiové stanici a z ní je také napájeno.

Při vyšší koncentraci různých přístrojů se zhoršuje možnost řídit individuálně každý přístroj. Snahou je soustředit řízení všech těchto zařízení do jednoho místa aby se zvýšila operativnost obsluhy. Ve většině případů se pro sběr dat a řízení více přístrojů používá osobní počítač.

Rádiová stanice RF 13 neobsahuje standardní komunikační rozhraní, která jsou běžnou součástí osobních počítačů, takže ji není možné připojit přímo k počítači. Aby mohla být rádiová stanice RF 13 připojena k počítači, musí být použito zařízení, které zprostředkuje přenos zpráv mezi počítačem a rádiovou stanicí.

Řídicí rozhraní CI 13 zprostředkovává přenos řídicích příkazů a stavových informací mezi osobním počítačem třídy PC a rádiovou stanicí RF 13. Umožňuje tak nastavovat základní parametry rádiové stanice jako jsou: kanál, frekvence, atributy kanálu, vysílací výkon a vysílání/příjem FLASH zprávy přímo z počítače.

Řídicí rozhraní CI 13 neobsahuje žádné řídicí ani indikační prvky. Po připojení k rádiové stanici se zapíná/vypíná současně s rádiovou stanicí. Je možné ho připojit ke kterémukoli ze dvou NF konektorů rádiové stanice. Kromě signálu DKON jsou všechny signály rádiové stanice bez změny přivedeny na konektor EXT. Na tento konektor je možné připojit jakékoli zařízení, které se normálně připojuje přímo k rádiové stanici RF 13. Funkce CI 13 jsou omezeny pouze po připojení datového zařízení (modem). Je-li datové zařízení připojeno na druhý NF konektor rádiové stanice, neovlivňuje činnost řídicího rozhraní. Přes CI 13 není možné nastavit rádiovou stanici plnicím zařízením PK 13.

Na konektor COM je připojen počítač přes sériové rozhraní RS232C (RS485). V CI 13 je implementováno jedno z uvedených rozhraní podle požadavků zákazníka. Rozhraní RS232C obsahuje signály RxD, TxD, RTS, CTS a má pevně nastavené parametry: rychlost 19 200, 8 bitů, bez parity, 1 stop bit. Pro řízení toku se využívá signálů RTS/CTS. Rozhraní RS485 využívá signály RS+, RS-.

Počítač vysílá/přijímá zprávy do/z řídicího rozhraní. Zprávy mají definovaný protokol. Vysílaná zpráva je vlastně řídicím příkazem, který je upraven v řídicím rozhraní a předán dále do rádiové stanice. Ve většině případů po vykonaném příkazu rádiová stanice vyšle zpět informaci o novém stavu.

Další sled událostí závisí na nastaveném režimu řídicího rozhraní. CI 13 má dva režimy. Pokud je CI 13 nastaveno v režimu **automatického generování zpráv o změně**, uloží v paměti nový stav rádiové stanice a předá informaci o změně dále do počítače. Pokud je nastaveno v režimu **generování zpráv na požádání**, pouze uloží informaci o novém stavu rádiové stanice do paměti. Režimy se nastavují řídicím příkazem z počítače. Po startu a resetu je nastaven režim generování zpráv na požádání.

Technické parametry

Rozsah napájecího napětí	(9 až 15) V
Odběr proudu při napájecím napětí 12 V	max. 50 mA
Konektor pro připojení rádiové stanice a externího zařízení parametry signálů, viz RF 13	
Konektor pro připojení počítače	RS232C nebo RS485
Parametry rozhraní RS232C	
Přenosová rychlost	19,2 kbt/s
Parita	žádná
Datové bity	8
Stop bit	1
Režim provozu	duplex
Řízení přenosu	RTS/CTS
Provozní teploty	-20 °C až +60 °C
Hmotnost	800 g
Rozměry	183 mm x 128 mm x 44 mm

Ing. Jiří Blaha
KON, tel.: 0632/522841

UTAJOVAČE EU 13 pro rádiové stanice řady RF 13

Pro utajení řečové komunikace v rádiové síti RF 13/RF 1301 je určen nový utajovač EU 13. Utajovač využívá digitální přenos VKV kanálem s rychlostí 16 kb/s. Utajovač pracuje na principu proudového šifrování v reálném čase.

Při návrhu utajovače byly na základě zkušeností s provozem maskovače v RF 13 stanoveny následující základní požadavky:

- zvýšení kryptologické hodnoty oproti stávajícímu maskovači v RF 13;
- zlepšení srozumitelnosti při slabých signálech oproti maskovači;
- provozní kompatibilita s RF 13 a RF 1301 ve všech druzích provozu;
- záměnnost s modulem maskovače v RF 13 bez jakýchkoliv úprav stávajících radiostanic;
- možnost externího provedení vestavěného do mikrotelefonu, schopného provozu s kteroukoliv rádiovou stanicí RF 13 a RF 1301;

Obr. 1 Externí verze utajovače EU 13

PRINCIP ŠIFROVÁNÍ

Pro šifrování je použit generátor pseudonáhodné posloupnosti. Generátor je tvořen několika posuvnými registry s různou délkou bitů. Všechny použité registry generují posloupnost maximální délky. Pokud tyto posloupnosti nemají společného dělitele, je celková perioda: $P=(2^x-1)*(2^y-1)*....*(2^z-1)$. Pro použitou délku jednotlivých registrů a při rychlosti datového toku 16 kb/s je doba opakování přibližně $2,45*10^{15}$ let.

Při kódování je datový bit operací XOR s výstupy všech posuvných registrů zakódován. Poté se registry posunou a kóduje se další bit.

Operace dekódování je opačná - výsledkem operace XOR zakódovaného bitu s výstupy všech posuvných registrů je původní datový bit. Přirozeně jen za podmínky, že posuvné registry jsou ve stejném stavu jako při kódování. Proto na vysílací a přijímací straně musí být zabezpečen stejný počáteční stav registrů a registry se musí posunovat synchronně.

Počáteční stav generátoru pseudonáhodné posloupnosti je dán klíčem. Klíč je rozdělen na několik částí a jeho plnění do registrů není spojité. Jedna z jeho částí je generována generátorem náhodných čísel a posílá se v hlavičce zprávy. Další části klíče jsou zadávány speciálním zařízením pro plnění klíče.

Verifikace šifrovací metody

Pro jednotlivé generátory byly pomocí počítače navrženy zpětné vazby tak, aby generovaly posloupnost maximální délky a následně byla tato vlastnost ověřena vygenerováním celé posloupnosti programem v dostatečně rychlém počítači.

Dále bylo počítačem ověřeno, že posloupnosti jednotlivých generátorů nemají společné dělitele – jsou nesoudělné.

Kustomizace utajovače

Kustomizací se rozumí možnost individuálního nastavení vnitřní struktury šifrovacího bloku pro danou skupinu uživatelů (např. armáda jednoho státu).

Kustomizace je možná změnou v zapojení pseudonáhodného generátoru.

A to:

- jiným zapojením zpětných vazeb pro jednotlivé posuvné registry (registr bude samozřejmě vždy generovat posloupnost maximální délky),
- jinou délkou jednotlivých posuvných registrů v generátoru.

Tyto změny jsou změnami v software řídicího procesoru a bez znalosti obsahu paměti programu v řídicím procesoru nejsou přímo zjistitelné.

Konkrétní zapojení generátoru musí výrobce znát (aby vyloučil možnost duplikace při prodeji dalším zákazníkům). Tyto informace jsou však předmětem interního utajení.

Bezpečnost použité šifry

Protože použitý algoritmus není veřejný, není veřejně k dispozici ani detailní popis šifrovacího bloku. Protože šifrovací blok je realizován programově a program je zabezpečen proti čtení, je zamezeno rozluštění struktury šifrovacího bloku neautorizovanou osobou.

Pokud neautorizovaná osoba získá fyzický kus utajovače, je důležité, zda tato jednotka obsahuje platný klíč. Proto je utajovač vybaven tlačítkem pro smazání klíče. Po výmazu klíče je šifrovací blok vyřazen a nelze tedy zjistit ani jeho strukturu porovnáváním vstupního a výstupního proudu dat.

Pokud utajovač bude obsahovat klíč, může neautorizovaná osoba dekódovat přenos, dokud je klíč platný. Této situaci nelze technicky zamezit, je nutno zajistit, aby v tomto případě byl v rádiové síti klíč urychleně změněn.

Zjištění neznámého klíče z odposlechnutého signálu je prakticky nemožné, protože není nikdy k dispozici vstupní signál, který vstupoval do šifrovacího bloku vysílače. Tento vstupní signál navíc neobsahuje žádné periodicky se opakující sekvence, na jejichž základě by bylo možno zpětně analyzovat šifrovací algoritmus a získat klíč.

OBVODOVÁ REALIZACE

Utajovač digitalizuje analogový hovorový signál adaptivní modulací delta (CVSD). Digitalizovaný signál je zašifrován a pomocí GMSK modulátoru je připraven pro vysílání rádiovým kanálem v síti s kanálovou roztečí 25 kHz. Na přijímací straně je v utajovači přijatý analogový signál převeden na číslicový GMSK demodulátorem, odšifrován a CVSD dekodérem převeden zpět na analogový hovor.

Řízení činnosti utajovače je realizováno jednočipovým mikropočítačem.

Samotná šifrovací jednotka je konstruována tak, aby byla co nejvíce ztížena možnost zjištění klíče a zapojení generátoru pseudonáhodné posloupnosti. Proto je tento generátor realizován programově v jednočipovém mikropočítači. Jeho vnitřní strukturu je možno v určitých mezích měnit podle přání zákazníka změnou programu (kustomizace). Tento program je v paměti, která je zabezpečena proti čtení. Část klíče, která se zadává z plnicího zařízení, se uchovává ve vnitřní paměti (EEPROM) mikropočítače. Taktéž tato paměť je zabezpečena proti čtení.

Utajovač je konstruován v externím i interním provedení. Externí provedení je schopné pracovat s rádiovými stanicemi RF 13, nebo RF 1301. Interní provedení je konstruováno jako výměnný modul do RF 13, který nahrazuje modul maskovače v RF 13.

GENEROVÁNÍ KLÍČE

Klíč utajovače je rozdělen na dvě části.

Plovoucí část je vytvořena generátorem náhodných čísel a je přenášena na začátku každé relace.

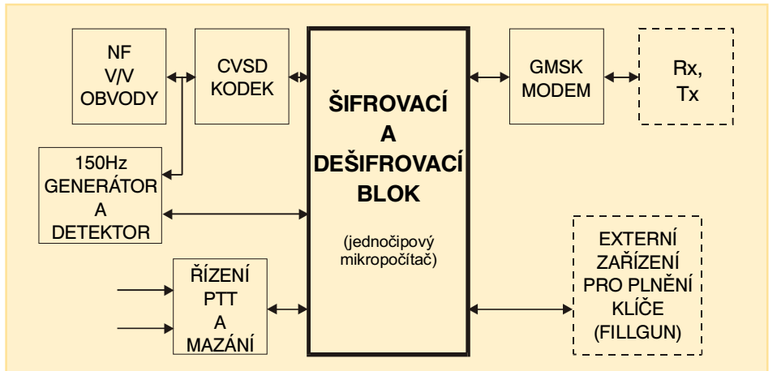
Pevná část klíče se do utajovače plní pomocí externího plnicího zařízení FG 13. Tato část klíče je vytvořena pomocí software v PC, potom je přenesena do plnicího zařízení a je k dispozici pro plnění do utajovače.

Plnicí zařízení také umožňuje vygenerovat náhodný klíč, pokud není k dispozici PC s programem.

SHRNUTÍ VLASTNOSTÍ

Použití šifrování na principu generátoru pseudonáhodné posloupnosti s neznámým vnitřním zapojením a rozděleným klíčem s plovoucí částí zvyšuje řádově kryptologickou hodnotu proti původnímu maskovači v RF 13.

Protože šifrovací algoritmus je realizován programově a program i klíč je zabezpečen proti čtení, je značně ztížena možnost zlomení šifry metodou „zpětného inženýrství".



Obr. 2 Blokové schema EU 13

Je zde také možnost jednoduché softwareové implementace algoritmu maskovače a přepínání mezi režimy nový utajovač-maskovač.

Utajovač je k dispozici ve dvou provedeních – jako výměnný modul do rádiové stanice RF 13, nebo jako externí doplněk k rádiovým stanicím RF 13 a RF 1301.

Ing. Pavel Joch
KON, tel.: 0632/522511

Utajovače řeči pro taktické rádiové stanice

Na utajovače řeči pro použití v rádiovém kanále jsou kromě požadavků kryptologického charakteru kladeny ještě další specifické požadavky:

- **schopnost činnosti prakticky v reálném čase, aby byl zachován charakter interaktivního rozhovoru;**
- **schopnost činnosti v rádiovém kanále se šumem a rušením;**
- **nenápadná podoba signálu (neprozrazující použití konkrétního typu utajovače) při příjmu běžnou rádiovou stanicí.**

Vzhledem k různorodosti uvedených požadavků je nutné při jejich plnění volit kompromis přiměřený praktickému používání zařízení. Některými způsoby se zabývá následující článek.

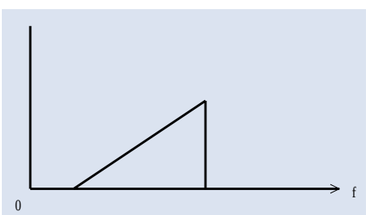
Používané způsoby utajení hlasové komunikace

Přístroje pro utajení hlasové komunikace můžeme dělit podle různých kritérií. Jedním z nich může být například požadavek na vlastnosti přenosového kanálu. Podle tohoto kritéria pak utajovače roztřídíme na takové, které ke své činnosti potřebují tzv. standardní telefonní kanál a na ostatní, které pracují v kanále proprietárním (zpravidla širším - ale ne vždy).

Zdálo by se, že utajovače ve standardním telefonním kanále jsou výhodnější, protože by mělo být možné je bez úprav použít s prakticky libovolnou technikou. Ve skutečnosti zde narážíme na specifické problémy. Prvním z nich je, že signál nesoucí utajenou řeč má jiné spektrální rozložení než řeč otevřená. To způsobí problémy paradoxně zejména u moderní techniky, jejíž přenosové kanály jsou optimalizovány právě pro přenos otevřené řeči. Druhým problémem je u složitějších systémů doba potřebná k synchronizaci. Ta bývá u těchto systémů nepříjemně dlouhá. Pro přehled je dále uvedeno několik postupů používaných při přenosu utajené řeči telefonním kanálem. Tyto přístroje jsou zahrnuty pod společný název analogové skramblery.

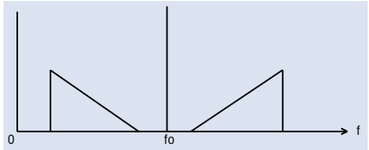
Analogové skramblery a utajovače

Nejnižším stupněm utajení hlasové komunikace je jednoduchá modifikace nízkofrekvenčního spektra. Je známo, že pro srozumitelný přenos řeči postačuje kmitočtové pásmo 300 Hz až 2 700 Hz. Pro přenos tohoto kmitočtového pásma jsou také dimenzovány hovorové kanály běžných rádiových stanic. Nejjednodušším způsobem utajení komunikace je obrácení kmitočtového spektra. Tento způsob je používán již několik desítek let. Na vysílací straně se obrácení kmitočtového spektra dosahuje například postupem schematicky naznačeným na obrázcích 1, 2 a 3.



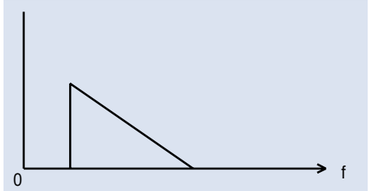
Obr. 1 Schéma spektra řeči

Řečovým signálem (spektrum na obr. 1) je amplitudově modulován pomocný kmitočet f_O (přibližně 3 kHz). Na výstupu modulátoru je spektrum zobrazené na obrázku 2.



Obr. 2 Pomocný kmitočet modulovaný spektrem řeči

Dolní propustí je z tohoto spektra odfiltrována pouze část padající do intervalu 300 Hz až 2 700 Hz (obr. 3).



Obr. 3 Obrácené spektrum řeči

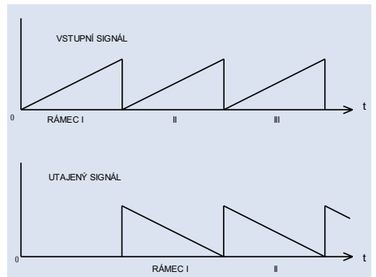
Na straně přijímací je postup získání původního řečového signálu obdobný.

Nevýhodou této metody je její poměrně snadná identifikace pouhým poslechem a tím možnost rychlého prozrazení.

Proto byl uvedený způsob průběžně zdokonalován. Prvním krokem bylo rozdělení nízkofrekvenčního pásma do dvou, případně více podpásem, jejichž spektrum je pak obraceno nezávisle.

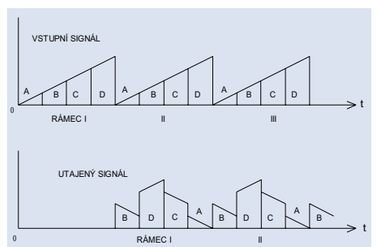
Dalšího zdokonalení bylo dosaženo tím, že výše uvedená podpásma se dynamicky mění v průběhu komunikace. Tímto způsobem lze již dosáhnout významného stupně utajení. Obvodová složitost takového zařízení je však vysoká. Její podstatnou část tvoří synchronizační obvody, které je nutno realizovat pomocí číslicové techniky. Rozvoj číslicové techniky však vedl k tomu, že dnes jsou analogové skramblery v uvedené podobě opouštěny a je využíváno stále více utajovacích zařízení číslicových.

Číslicová technika totiž dovoluje modifikovat signál nejen v doméně kmitočtové, ale i v doméně časové. V utajovačích se postupuje tak, že přicházející signál rozdělíme časově na tzv. rámce. Délku rámce můžeme volit libovolně, zpravidla ji zvolíme tak,



Obr. 4 Časové obrácení rámců

aby zpoždění způsobené délkou rámce nepůsobilo rušivě při interaktivní hlasové korespondenci. Tento rámec pak je možné vysílat např. pozpátku (obr. 4). Při praktické realizaci se používá ještě rozdělení rámce na segmenty, které jsou vysílány ve změněném pořadí, případně některé pozpátku (obr. 5).



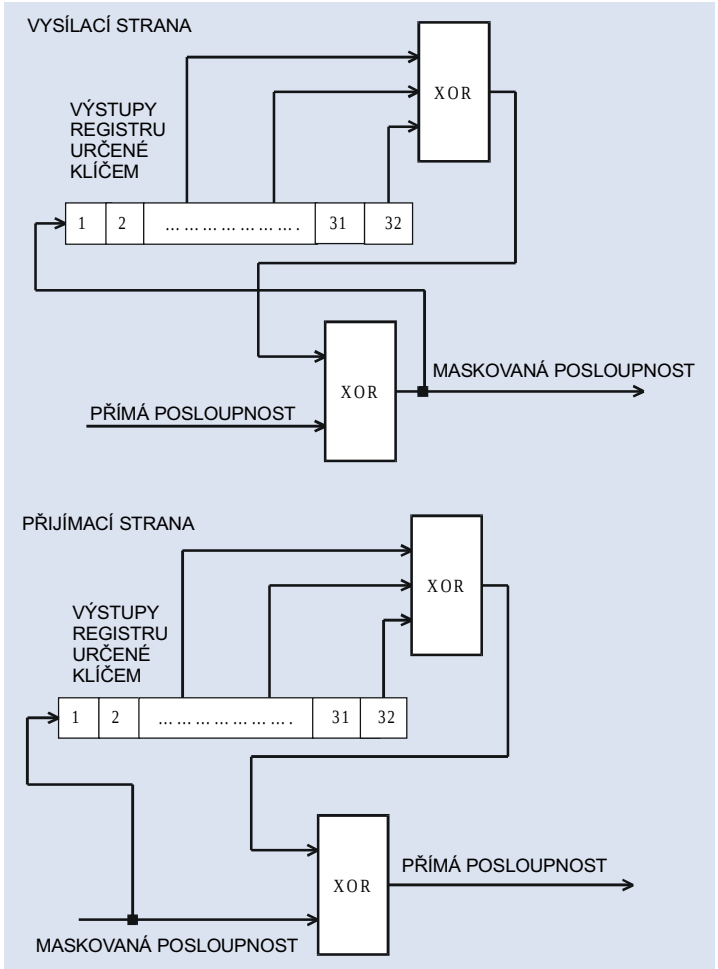
Obr. 5 Přeskládání segmentů v rámcích

Číslicové skramblery a utajovače

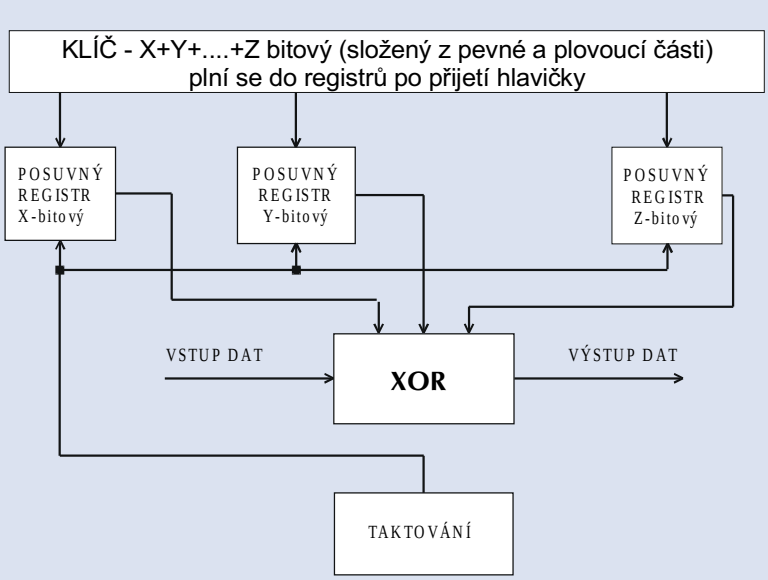
Do další kategorie utajovačů patří zařízení, která používají pro přenos po rádiové cestě jiného než telefonního kanálu. Nejčastěji bývá v tomto případě u taktických vojenských rádiových stanic pro VKV pásmo používán digitální přenos rychlostí 16 kb/s. Nabízí se tedy možnost nasadit utajovač na tento datový tok. Jedná se tedy o utajovač digitální. Nejjednodušším řešením je v tomto případě číslicový skrambler. Tohoto řešení je také použito ve standardní radiové stanici RF 13. Blokové schéma je uvedeno na obr. 6. Klíč v tomto případě je realizován 32bitovým slovem, jehož jednotlivé bity určují připojení výstupů buněk posuvného registru ke sčítačce modulo 2 (XOR).

Nevýhodou uvedeného řešení je skutečnost, že u něj dochází k tzv. násobení chyb. Tento jev se projevuje zhoršením kvality přenosu v okamžiku, kdy použitý rádiový kanál pracuje s reálnou chybovostí. Z důvodu násobení chyb není vhodné prodlužování posuvného registru ani jeho složitější konstrukce. To sebou přináší omezenou kryptologickou hodnotu.

Proto se pro náročnější aplikace používá složitějších a účinnějších metod. Pro utajení toku dat se nejčastěji používá buď proudového nebo blokového šifrování. Při proudovém šifrování jsou jednotlivé bity posloupnosti nesoucí informaci násobeny bity klíče. Při blokovém šifrování jsou bity posloupnosti nesoucí informaci nejdříve uloženy do bloků určité délky (64, 128 … bitů) a tyto bloky jsou pak zašifrovány. Výsledky dosažitelné oběma metodami jsou srovnatelné. Pro utajení typické fónické komunikace však vychází řešení s proudovým šifrováním méně nákladné.



Obr. 6 Číslicový skrambler (RF 13)



Obr. 7 Šifrovací a dešifrovací blok EU 13

Vernamova šifra a šifrování založené na pseudonáhodných posloupnostech

Princip Vernamovy šifry je jednoduchý. Jednotlivé bity zprávy jsou sčítány s bity řetězce náhodně generovaného klíče. Pokud je klíč opravdu náhodný a zpráva dostatečně dlouhá, je šifra nerozluštitelná, ale je zde problém distribuce klíče k příjemci, přičemž klíč má stejnou délku jako zpráva.

Proto se místo náhodného generátoru klíče používá generátor pseudonáhodný. Jeho perioda opakování musí být co největší, aby nedocházelo k opakování klíče během vysílání. Pokud například při datovém toku 16 000 bitů za vteřinu použijeme 64bitový posuvný registr jako generátor pseudonáhodné posloupnosti, jeho perioda opakování bude $(2^{64} - 1)/(16\ 000*3600*24*365)$=35,6 milionu let, což je dostatečné. Blokové schema generátoru pseudonáhodné posloupnosti je na obr. 7.

Pokud generátory pseudonáhodných posloupností na přijímací i vysílací straně jsou synchronní (ve stejný okamžik generují stejné číslo), není nutno přenášet k příjemci celý klíč.

Je zřejmé, že tento způsob šifrování je vhodný pro proudové šifrování a z jeho principu se vychází i při návrhu nového utajovače pro rádiové stanice RF 13, který je popsán v samostatném článku.

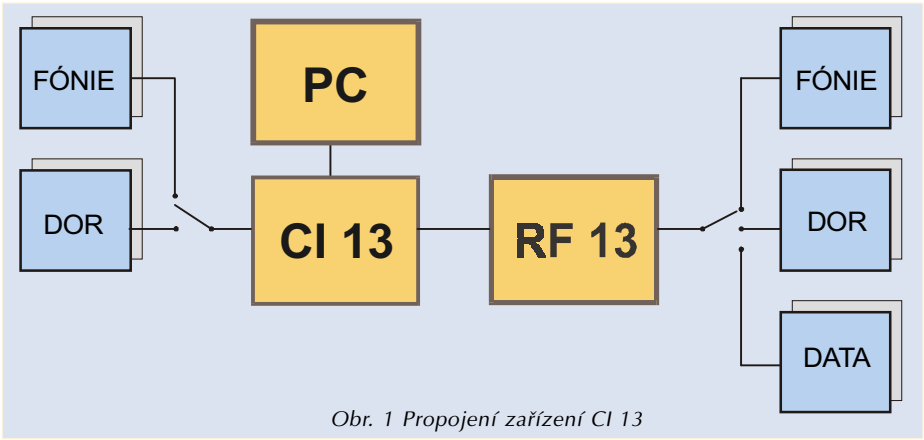
Ing. Jiří Krča, Ing. Pavel Joch
KON, tel.: 0632/522502, 522511

Ovládání rádiové stanice RF 13 z PC

Rádiové stanice řady RF 13 jsou od svého vzniku vybaveny sériovou komunikací, která je původně určena ke komunikaci s připojeným příslušenstvím. Příkladem je ovládání rádiové stanice z mikrotelefonu, zobrazení údajů na displeji mikrotelefonu, ovládání filtru AF 13, čtení dat z plnicího zařízení a podobně.

Tomuto určení byly přizpůsobeny vlastnosti sériové komunikace – je to nestandardní sériová komunikace v úrovni TTL, u které je řídicím prvkem, i z hlediska časování, rádiová stanice RF 13. V průběhu vývoje byla komunikace doplněna o další příkazy, které umožňují automatizované měření rádiových stanic v průběhu výroby. Jedná se především o ovládání, programování a nastavování parametrů „bez dotyku" na rádiovou stanici. Touto komunikací jsou vybaveny všechny stanice RF 13 od počátku sériové výroby.

V průběhu používání rádiových stanic RF 13 pro „speciální případy" je v několika systémech využívána tato komunikace pro ovládání rádiové stanice, ale vždy zařízením „ušitým na míru" pro daný případ. V poslední době vyvstaly požadavky některých zákazníků na ovládání rádiové stanice RF 13 z počítače. Vzhledem k charakteru sériového rozhraní rádiové stanice RF 13 nelze vytvořit ovládací program pro přímé připojení RF 13 k počítači řady PC, který by pracoval pod libovolným operačním systémem. Problémy jsou především u operačních systémů řady Windows. Proto byl v DICOM vyvinut pro ovládání stanice RF 13 z PC nový přístroj, nazvaný Řídicí rozhraní CI 13. Ten je popsán v části Novinky.



Obr. 1 Propojení zařízení CI 13

Propojení zařízení je patrné z obrázku 1. Funkce, které lze ovládat u rádiových stanic prostřednictvím CI 13, lze rozdělit do těchto skupin.

a) Povely shodné s ovládáním rádiové stanice mikrotelefonem

- přepnutí na předvolený kanál nahoru;
- přepnutí na předvolený kanál dolů;
- start skanování;
- ukončení módu skanování.

b) Další povely

- přepnutí na libovolný předvolený kanál;
- nastavení kmitočtu simplexního kanálu;
- nastavení kmitočtů semiduplexní ho kanálu;
- nastavení atributů rádiového kanálu (UT, SEL, SQ 150);
- nastavení vysílacího výkonu;
- naprogramování všech údajů rádiového kanálu;
- vyslání zprávy FLASH;
- posun kmitočtu o 25 kHz nahoru;
- posun kmitočtu o 25 kHz dolů;
- posun kmitočtu o 1 MHz nahoru;
- posun kmitočtu o 1 MHz dolů.

c) Informace o RF 13

- vyslání informace o stavu rádiové stanice na dotaz;
- vyslání informace o stavu rádiové stanice při každé změně;
- informace o připojeném zařízení;
- přijatá zpráva FLASH;
- chybové hlášení.

Předpokládáme, že potřeba ovládání rádiových stanic z PC poroste. Proto podáváme našim zákazníkům a uživatelům rádiových stanic RF 13 informaci této možnosti. Pro podrobnější informace se můžete obrátit na oddělení vývoje a konstrukce naší společnosti.

Ing. Zdeněk Pícha
vedoucí KON, tel.: 0632/522834

DSA 2000
7TH DEFENCE SERVICES ASIA
EXHIBITION & CONFERENCE

Ve dnech 11. až 14. 4. 2000 se uskutečnila v hlavním městě Malajsie, Kuala Lumpur, výstava obranné techniky Defence Services Asia 2000.

Jedná se o nejvýznamnější výstavu vojenské techniky v oblasti jihovýchodní Asie a podle některých i druhou nejvýznamnější výstavu tohoto druhu na světě. Mezi 420 vystavujícími firmami ze 40 zemí se zúčastnily v rámci české expozice také čtyři firmy z České republiky - DICOM spol. s r. o. Uherské Hradiště, ERA a.s. Pardubice, Sellier & Bellot a.s. Vlašim a Omnipol a.s. Praha.

Ing. Přemysl Večeřa
vedoucí OBO, tel.: 0632/522233

IDEE 2000

Ziskem Zlatého IDEE pro Rádiový datový terminál DT13, za nejlepší exponát v oboru elektrotechnika, se DICOM stal nejúspěšnější zahraniční firmou v rámci výstavy obranné techniky IDEE 2000, konané od 3. do 6. 5. 2000 v Trenčíně.

Ing. Přemysl Večeřa
vedoucí OBO, tel.: 0632/522233

DICOM INFORM - čtvrtletník společnosti DICOM. Vydavatel: DICOM, spol. s r.o. Toto číslo vychází 5. 6. 2000 v nákladu 150 ks. Redakce, grafické zpracování a tisk - oddělení DIN společnosti DICOM

DICOM, spol. s r.o., Sokolovská 573, P.O.Box 129, 686 01 Uherské Hradiště,Tel.: 0632/522603, Fax: 0632/522836, E-mail: dicom@pvtnet.cz, http://www.dicom.cz