MLS v podmínkách taktických komunikačních systémů

Prezentuje Pavel Kotyk

ROHDE&SCHWARZ

Prostředí taktických komunikací

- **Požadavky na:**
  - Integritu dat (tedy na odolnost proti rušení)- TRANSEC
    - Není součástí tématu
  - Dostupnost dat (problematika dosahů a konfigurací)
    - Není součástí tématu
  - Utajení dat
    - Na jaké úrovni- kruciální problém s přechodem mezi doménami
- **Požadavky na interoperabilitu a sdílení dat v rámci aliance/ mise**
  - Off line
  - On-line
  - On-Line/ On-air

Prostředí taktických komunikací

- **Požadavky na utajení dat:**
  - Jaká data, jak dlouho na jaké úrovni utajení
  - Vertikální řetezec při hiearchickém velení
    - Úroveň generální štáb
    - …
    - Jednotlivec v poli
  - Fragmentace dat a integrace dat a stím souvisejíc deklasifikace dat
  - Prostupy mezi doménami
    - Stacionární systémy typu polní velitelské stanoviště (IDG)
    - Mobilní platformy (typicky vozidla)

Prostředí taktických komunikací

- **Požadavky na interoperabilitu a sdílení dat alianční/ mise**

  - Off line
    - Otázka spíše administrativní („vzduchová kapsa“ a přenos dat na médiích typicky na štábní úrovni
    - GW pro propojení sítí
  - On-line
    - Otázka bezpečnostních filtrů
    - SW řešení
    - Fragmentace a integrace dat
  - On air
    - Velmi specifický případ
    - Konfigurace a sdílení klíčového hospodářství

Standard COMSEC v NATO

- **Základním standardem pro COMSEC spojení v NATO je řada zařízení:**
  - VINSON (KY57/58, KY 100)
  - KG84A/C
  - ANDVT- family/ KY100
  - KIV7
- **Detaily k algoritmům jsou klasifikovanou informací**
- **Jedná se o třídu algoritmů typu NSA Type 1**
- **Všechna tato zařízení se postupně nahrazují univerzálním prostředkem ELCRODAT 4-2**
- **ELCRODAT 4-2 je připraven pro implementace případného nového algoritmu cestou doplnění HW modulu**
- **Pro ČR existují pravidla pro instalaci ED4-2 do mobilních zástaveb**

NSA Type…. ?

- **NSA Type 1 = algoritmus certifikovaný NSA pro ochranu informací spadajících do oblasti utajovaných skutečností stanovených vládou USA**
- **NSA Type 2 = algoritmus , který je doporučen NSA pro ochranu informací na úrovni národní bezpečnosti, přenášeným veřejnými telekomunikačními sítěmi**
- **NSA Type 3 = algoritmus uznaný FIPS pro ochranu citlivých informací, které však nemají charakter informací podstatných pro národní bezpečnost**
- **NSA Type 4 = registrovaný algoritmus, který nesmí být použit pro ochranu utajovaných skutečností. Délka klíčů maximálně 40bitů.**

R&S SDTR

Reálná SW definovaná radiostanice nové generace

- Kompaktní radiostanice s co-site filtrem (antény od 1m od sebe)
- **30 – 512 MHz , 50 W**
- Minimalizované rozměry
- Otevřená platforma **SCA v2.2.2**
- **Síťové možnosti** (IPv4, IPv6, VoIP)
- **Red/black oddělení** na HW úrovní
- Speciální šifrovací modul s HW klíčem
- **Kompletní klíčové hospodářství**

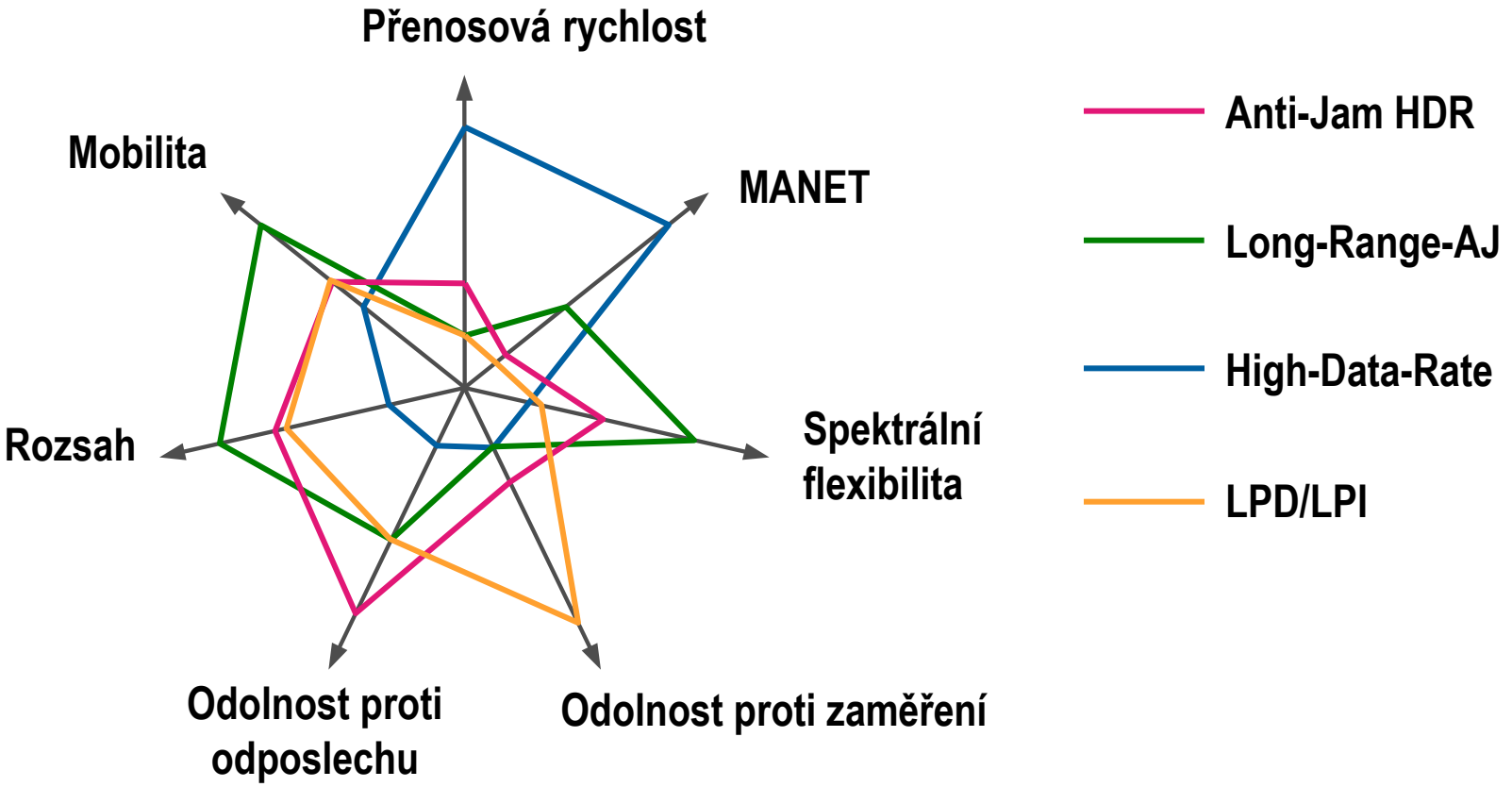
R&S SDTR

Reálná SW definovaná radiostanice nové generace

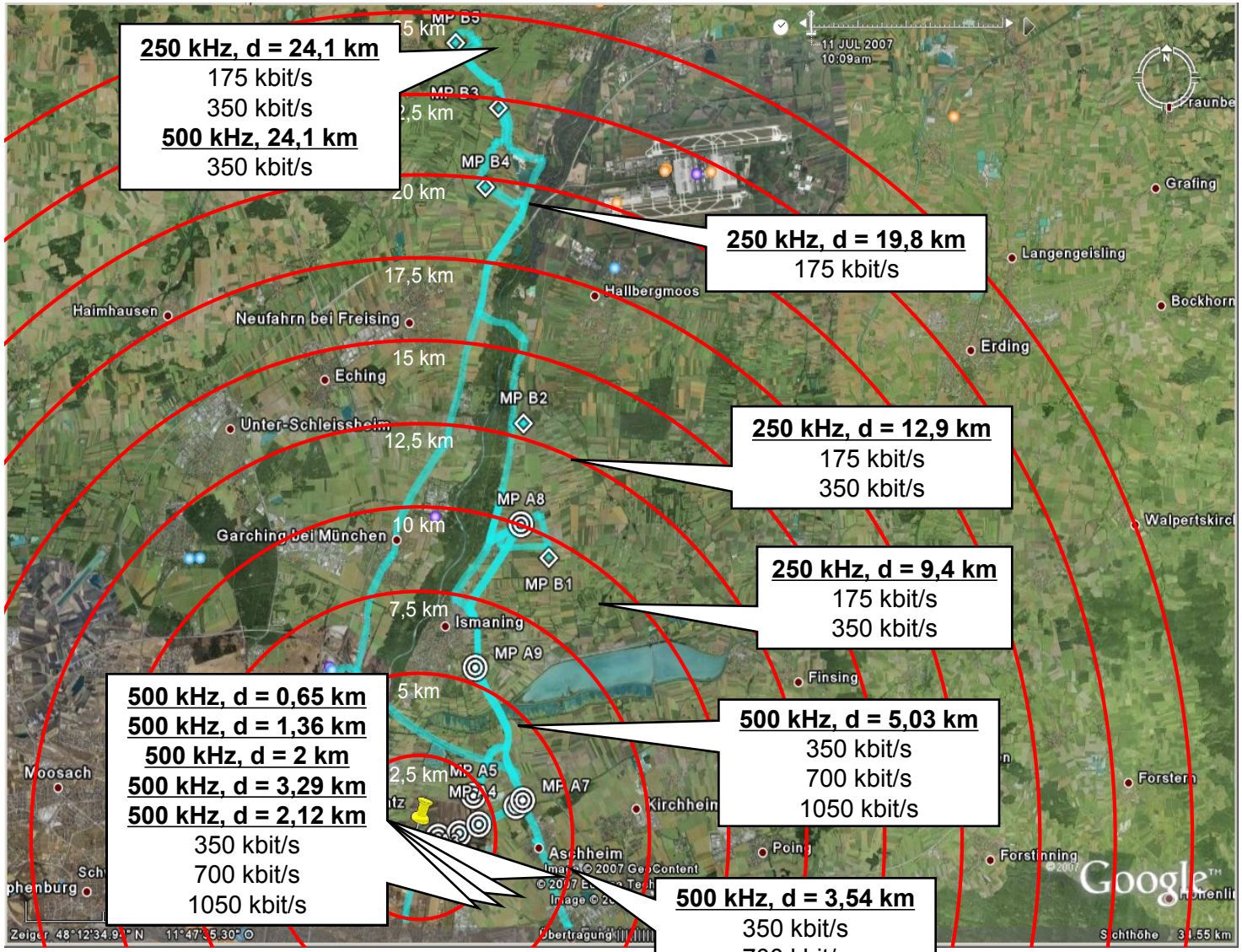
- Datové přenosy až 10 Mbps
- **Ortogonální sítě typu MANET**
- **TDMA: 2x hlas 1x data (VKV) 2x hlas 6x data (UKV)**
- Řada ECCM vlnových forem HDR
  - AJ-NB pásmo 25kHz data až 110kbit/s
  - AJ-WB pásmo 250kHz data až 621kbit/s
  - WB pásmo 500kHz data až 2Mbit/s
- Možnost integrace vlastních přenosových protokolů (WF)

Vlnové formy

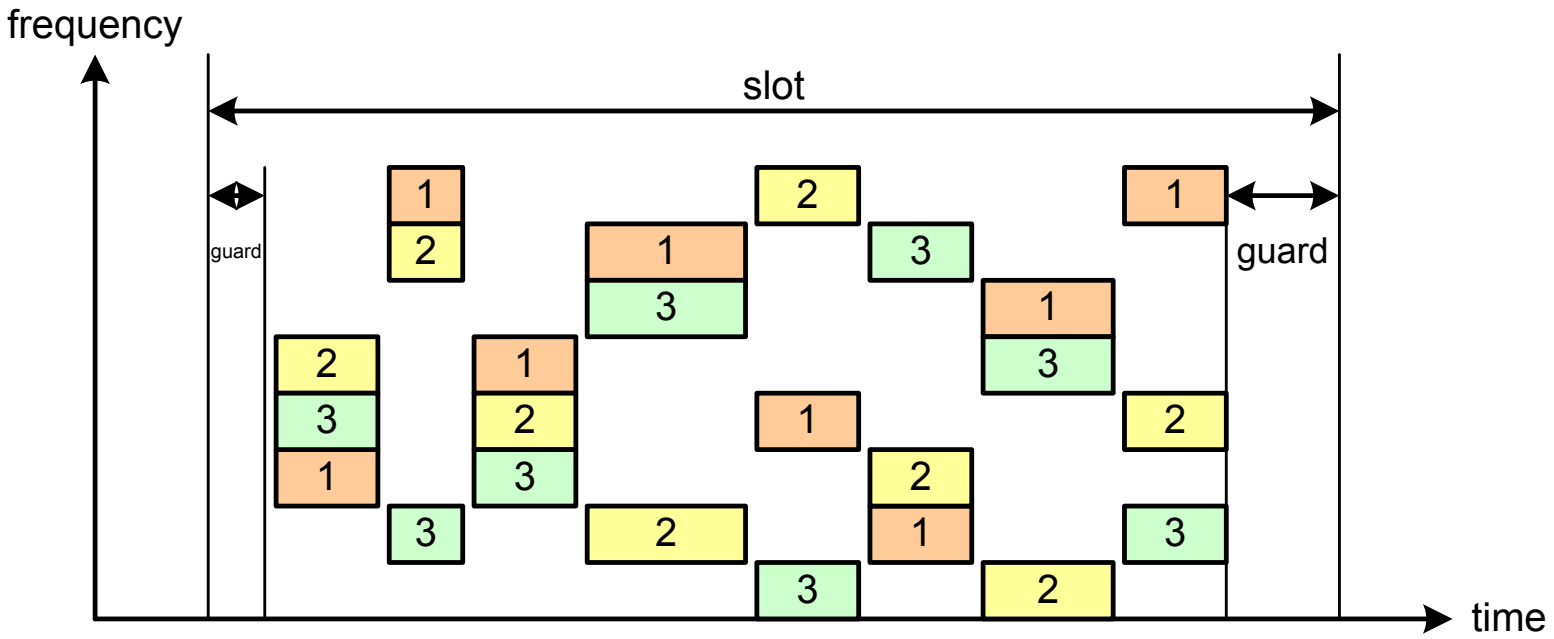
Waveform (vlnová forma) je komplexní termín pro přenos signálu/ dat/ hlasu a to ve smyslu použité modulace, kmitočtového skákání a způsobu šifrování

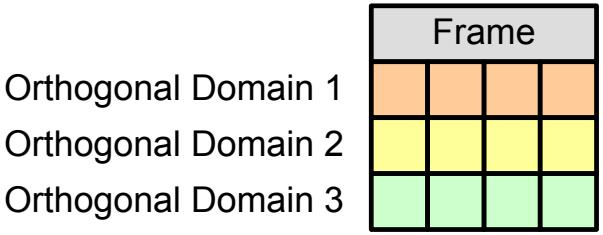


Polní testy Johanneskirchen



TRANSEC – ortogonální hopping





Systém automaticky zabezpečí, aby nedošlo ke vzájemnému rušení komunikace

Řešení do vozidel

1 x řídící jednotka

N x SDTR

- UHF/VHF 50W
- HDR-WB
- HDR-AJ (NB and WB)
- SECOM-P- DICOM
- SECOS, HQI/II

K x VK3150C (M3TR)

- HF 150W
- ALE 3G
- ST4538 IP xDL
- xDL = LDL, HDL, HDL+

IP

J x MR3000P

- DICOM

- SECOM-P

R&S®SDTR Příslušentství

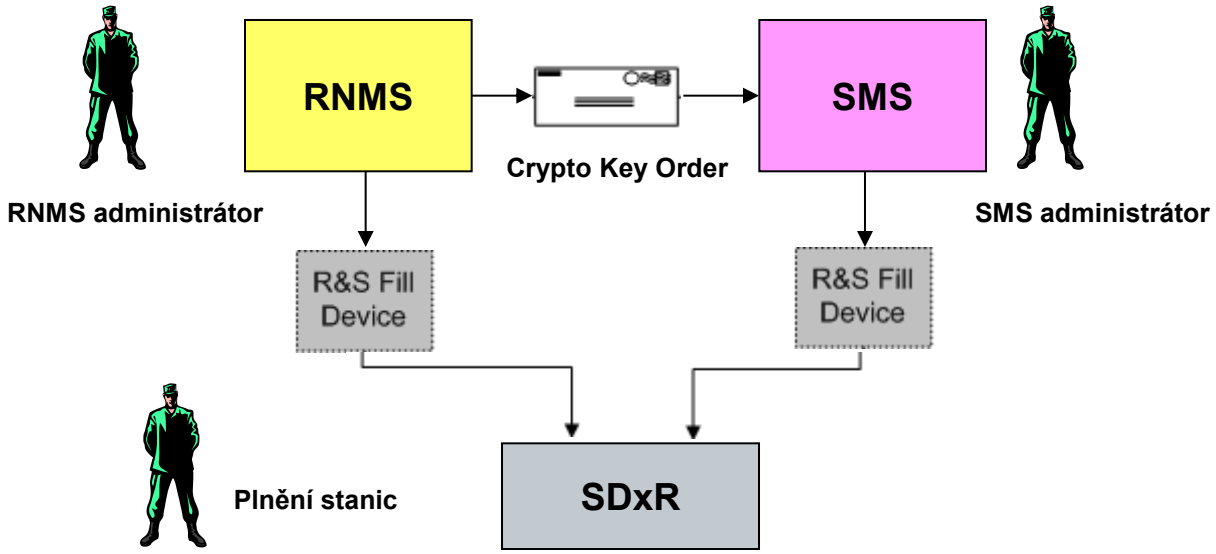
- **HW klíč (CIK)**
  - Umožňuje deklasifikaci zařízení
  - Provoz bez CIKu je rovněž možný

- **Řídící jednotka**
  - Pro ovládání 2xSDTR a 1xM3TR
  - Aplikace

Průběh konfigurace sítí

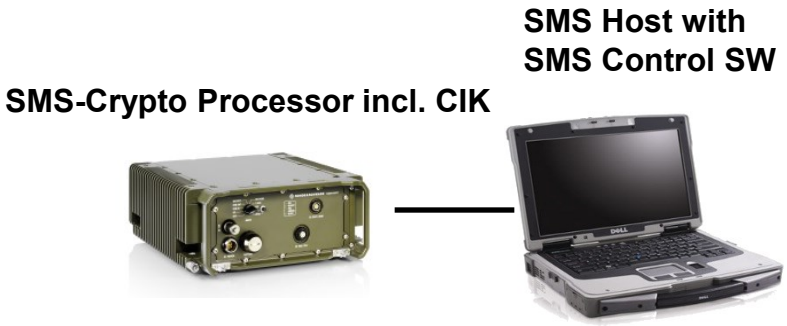
Plánování nové operace

1. Naplánování akce/ mise -RNMS
2. Distribuce konfiguračních dat do jednotlivých stanic
3. Požadavek na vygenerování klíčů RNMS na SMS
4. Vygenerování klíčů
5. Distribuce klíčů



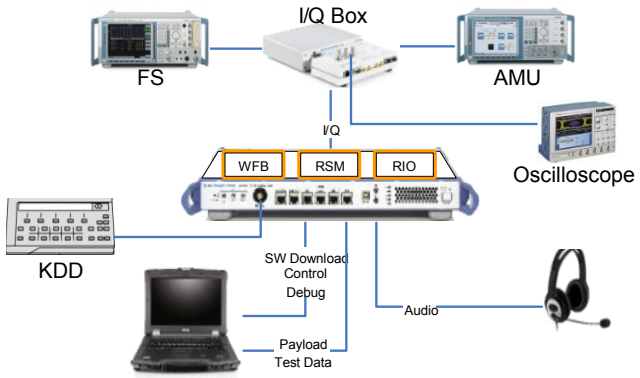
Jaké jsou funkcionality zařízení SMS?

- **Dvě základní funkcionality:**
  1. Generování černých klíčů pro ECCM komunikace
  2. Digitální podpis šifrování modifikované vlnové formy
- **Základní přístup: jeden produkt ve dvou variantách**
  - SMS: generování pracovních klíčů
  - SES: signing & encryption of software



Modifikace šifrovacího algoritmu zákazníkem

Krok 1:
Modifikace krypta



Krok 2:
digitální podpis
nového SW

Krok3:
Download SW SDxR
dešifrování a kontrola podpisu

Krok 0 :
Generování transportních a uživatelských klíčů

Shrnutí

- **Technické aspekty**
  - Moderní platforma schopná implementace provozů v řádu:
    - Tisíce skoků za sekundu
    - Jednotek Mbit/s
    - Šifra typu AES 256
  - Moderní ECCM provozy s TDMA charakteristikou
  - Radiostanice určená k certifikace na „SECRET“ úroveň
- **Ochrana investic**
  - Implementace provozů SECOM-P (DICOM HW20)
  - Implementace RF40 WF zahájena
  - Připravena na implementaci aliančních standardů typu COALWNW
  - Kapacitně schopná implementace provozů typu SINCGARS/ ANW2 (podmíněna dohodami vláda- vláda)

Shrnutí

- **Bezpečnostní aspekt**
  - Potenciál na certifikace „národní TAJNÉ“
  - Implementace jakéhokoliv WF (koncept WFDE)
  - Modifikace AES algoritmu cestou národní autority
  - Kompletní kryptografické zařízení součástí dodávky (SMS, SES)

pavel.kotyk@rohde-schwarz.com