

Integrált vezeték nélküli alkalmazások

Integrated Wireless Applications

BMEVIHIMA03



BME Hálózati Rendszerek és Szolgáltatások Tanszék 1



A tantárgy adatai

- Tárgyfelelős: Dr. Imre Sándor, Hálózati Rendszerek és Szolgáltatások Tanszék
- Oktatók: Dr. Imre Sándor és Schulcz Róbert, Hálózati Rendszerek és Szolgáltatások Tanszék
- A tantárgy célkitűzése: a mobil és vezeték nélküli szolgáltatások felépítése, a szükséges rendszerek integrációjának bemutatása mind a horizontális, mind a vertikális integrációra kitérve
- A tantárgyi adatlap:
<https://portal.vik.bme.hu/kepzes/targyak/VIHIMA03>
- A tantárgy honlapja:
<http://www.hit.bme.hu/~schulcz/BMEVIHIMA03/>



A félév beosztása

- A tárgy keretein belül előadások és gyakorlatok
- Az előadásokon hetente egy újabb téma elméleti háttere
- A gyakorlatokon az előadásokhoz kapcsolódó feladatok megoldása csoportos munkaként



Követelmények

- A szorgalmi időszakban egy nagy ZH
 - Az aláírás feltétele a legalább elégséges eredmény
- A vizsgaidőszakban szóbeli vizsga (elővizsga lehetséges)
- A félévvégi érdemjegyet a ZH pontszáma 25%-os, a vizsga eredménye 75%-os súllyal határozza meg
- Pótlási lehetőségek:
 - A szorgalmi időszakban pótló ZH
 - A pótlási időszakban pótló-pótló ZH



Motiváció

- Összetett vezeték nélküli rendszereket használunk a mindennapokban
- A vezeték nélküli szélessávú hozzáférések elterjedtsége meredeken növekszik



Forrás: <http://www.oecd.org/sti/broadband/oecdbroadbandportal.htm>

A félév során megismert technológiák

Vezeték nélküli technológiák a tárgy tematikájában



Mobil hálózati ismeretek

- Korábban tanultak felelevenítése
- Szolgáltatások integrációja
- A logikai és fizikai architektúrák különbségei
- Mobilitásmenedzsment kérdések
- Felhasználói mobilitás különböző technológiájú hálózatok között



Kliens-szerver kommunikáció mobil környezetben

- A jól ismert szolgáltatásarchitektúrák mobilalkalmazások körében való alkalmazása
- SOAP, REST stb.
- Felhasználói élményt befolyásoló tényezők a kliens-szerver kommunikációban
 - Például aszinkron eljárás hívások



Otthonautomatizálás, távfelügyelet, gépjármű távfelügyelet

- Otthoni vezérlések (vezetékes is), ezek távirányítása
- Gépjármű távfelügyeleti rendszerek
- Adatok a CAN-busz interfésztől a távfelügyeleti központig
- Riasztórendszerek megoldásai
- Interneten keresztül vezérelhető rendszerek



Car2car kommunikáció

- Forgalomszervezési problémák megoldása vezeték nélküli kommunikációval
- A gépjárművek között megosztott adatok, azok felhasználása
 - Baleset-megelőzés
 - Fogyasztáscsökkentés
 - Forgalomirányítás hatékonyabbá tétele
- A legújabb technológiák, ajánlások



Jármű fedélzeti kommunikáció

- A fedélzeti számítógépek fejlődése a diagnosztikai célú feladatoktól (például fogyasztásmérés) az integrált szórakoztatóközpontokig
- Kamerarendszerek az autóban
- CAN-busz, FlexRay
- D2B, MOST
- Egyéb járműipari kommunikációs technológiák

BME Hálózati Rendszerek és Szolgáltatások Tanszék 11

CAN – Controller Area Network

FlexRay

- drágább, megbízhatóbb, gyorsabb fedélzeti kommunikáció, mint a CAN,
- 10 Mbps, csillag- és busztopológia, kettőzéssel hibatűrő,
- jobb real-time garanciák, mint a CAN busszal
- FlexRay Consortium (Freescale Semiconductors, Robert Bosch GmbH, NXP Semiconductors, BMW AG, Volkswagen AG, Daimler AG, General Motors)
[<http://en.wikipedia.org/wiki/FlexRay>]
- Első alkalmazás: 2007 BMW X5 [<http://ae-plus.com/milestones/milestones-flexray>]

D2B – Domestic Digital Bus, Mercedes-Benz, száloptikás, 12 Mbps, multimédia, gyűrű

MOST – Media Oriented Systems Transport – gyűrű topológia, különböző változatok eltérő adatátviteli sebességekkel, optikai vagy réz alapú adatátvitel



Forgalomfüggő navigáció

- Az útvonaltervezés alapjai
- Forgalmi szituációk értelmezése navigációs rendszerekben
- TMC vevővel kiegészített GPS alapú navigáció
- Internet alapú forgalomfüggő navigáció
 - Nagyobb szolgáltatók által biztosított rendszerek
 - Közösségi alapon szerveződő forgalomfüggő navigációs megoldások



E-útdíj rendszerek

- HU-GO rendszer
- EU-GO rendszer
- A megoldások összehasonlítása
- Fedélzeti egységek működése
- Díjszámítás, útvonalváltozások kezelése különböző útdíjfizetési rendszerekben.



Online pénztárgépek

- A kasszák ellenőrzésének okai, indokai
- A kasszák ellenőrzésére korábban használt megoldások rövid áttekintése
- A pénztárgépek bekötésére vonatkozó szabályok
- Az online pénztárgépek kommunikációs megoldásai
- A magyar implementáció sajátosságai a külföldi megvalósításokhoz képest



Raktári alkalmazások, RFID

- A vezeték nélküli technológiák használata a logisztikában
- WLAN-alapú helymeghatározó rendszerek
- Cikkek, termékek RFID azonosítása
- Vezeték nélküli kommunikáció felhasználása a raktárgazdálkodási folyamatokban



Smart metering, távleolvasás

- Szenzorhálózatok, mérőeszközök
- Mérőeszközök kommunikációs megoldásai
- Real-time adatokat szolgáltató megoldások és naplózó rendszerek



Mobil fizetési megoldások

- A ma elterjedt megoldások ismertetése, műszaki háttere
- A tranzakciók mögötti pénzügyi folyamatok áttekintése
- A jogi szabályozás releváns részei
- A mobil fizetési megoldások költségei



Igénybevétel alapú tömegközlekedés

- RFID- és NFC- alapú tömegközlekedési jegyek használatának feltételei
- Megoldások a világ nagyvárosaiban
- Biztonsági problémák a tömegközlekedési jegyek használata során
- Online, offline megoldások összevetése



Kitekintés a jövőbe

- A jövő lehetséges vezeték nélküli kommunikációs megoldásai
- IoT koncepció
- Szabadtéri, fény alapú kommunikáció
- Kvantumkommunikáció

Mobil hálózati alapismeretek



A rádiós kommunikáció története

- Hertz 1888-ban „A levegőben való elektrodinamikus hullámokról és visszaverődésükről” című tanulmányában igazolja az elektromágneses hullámok létezését, megméri hullámhosszukat, sebességüket
- Marconi 1899-ben a La Manche csatornán, 1901-ben az Atlanti-óceánon keresztül táviratozott rádióhullámokkal



A rádiós kommunikáció története

- 1947-ben a Bell Labs mérnökei fogalmazzák meg a cellás elvet autós mobiltelefonokhoz
- 1968-ban részletesebb rendszerterv szintén a Bell Labs mérnökeitől:
 - Frekvencia újrafelhasználás
 - Handoff
- 1979-ben indul az AMPS (Advanced Mobile Phone System) rendszer
- 1989-ig analóg rendszerek uralják a piacot (NMT, TACS)

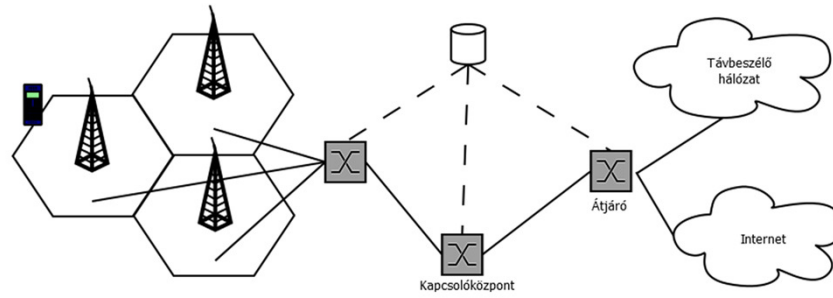


Digitális mobiltelefon-hálózatok

- A GSM szabvány (1989) forradalmasította a mobil távközlést
- 1999 UMTS
- 2001 HSDPA



Cellás hálózatok felépítése





Cellák formája

- Az elvi modellekben hatszög alakúak
- Elméletben körsugárzó antenna esetén kör alakúak, a valóságban a domborzat miatt bármilyen lehet ilyen antennával is
- Elterjedt a szektorantennák használata
- Sűrű forgalmú területeken előfordulnak egymásba ágyazott cellák
- A szomszédos cellák különböző frekvenciákat használnak (analóg rendszerek és GSM esetén)

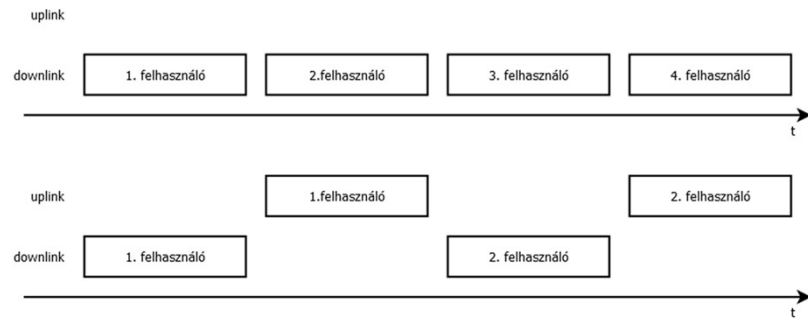


Multiplexálás vezeték nélküli rendszerekben

- Közös hozzáférés az átviteli közeghez
- Megoldandó:
 - A downstream, upstream irány elválasztása
 - Az egyes előfizetők forgalmának elkülönítése
- Elkülöníthetők a forgalmak:
 - Időben
 - Frekvenciában
 - Térben
 - Kódban



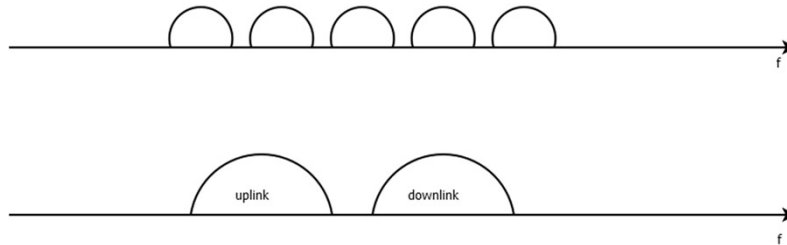
Multiplexálás – TDM/TDD



- A különböző csatornák elválasztása időben történik
- Pl.: TDM: GSM, TDD: WiMAX



Multiplexálás – FDM



- Az egyes felhasználók forgalmának vagy az uplink/downlink iránynak az elválasztása a frekvenciatartományban történik
- Pl.: FDD – GSM



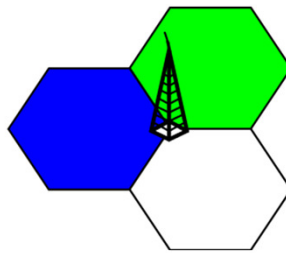
Multiplexálás – CDM

- Kódokkal történik az egyes felhasználók, illetve bázisállomások elkülönítése
- Hasonló jelerősséget igényel az egyes felhasználóktól a vételi oldalon
 - → CDD nincs
- Példa: UMTS
- Miért jó?
 - A TDMA az időréseket, az FDMA a spektrumot pazarolja, ha nem teljes a kihasználtság. A CDMA kihasználja a teljes rendelkezésre álló spektrumot időben folyamatosan.



Multiplexálás – SDM

- Az egyes forgalmak elkülönítése térben történik, ilyennek tekinthető a cellás felépítés esetén a frekvencia-újrafelhasználás
- Például szektorantennák alkalmazása esetén:





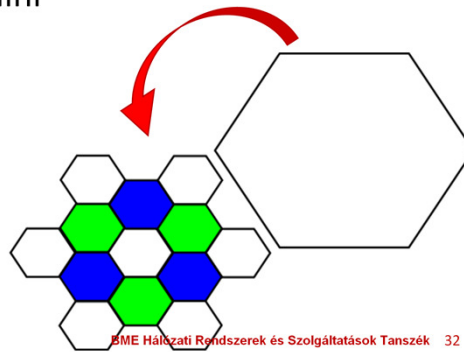
Frekvenciagazdálkodás GSM hálózatokban

- GSM 900
 - Uplink: 890-915 MHz
 - Downlink: 935-960 MHz
 - 200 kHz-es vivők → 124 vivő
 - Vivőnként 8/16 db időrés
 - Magyarországon jellemzően szolgáltatóként tízféle frekvencia-kiosztású cella, kb. 40 vivő / szolgáltató
 - Kb. 4 vivő / szolgáltató / cella → 32/64 beszédcsatorna / szolgáltató / cella
 - Városokban, nagy forgalmú területeken kisebb cellák kellenek!



Frekvenciagazdálkodás GSM hálózatokban

- A frekvenciatartományt részekre osztja a szolgáltató
- Szomszédos cellákban eltérő frekvenciákat használ
- A cellák kapacitása véges, nagyobb forgalom esetén kisebb cellákat kell használni
 - Előnye:
 - Kisebb adóteljesítmény
 - Nagy forgalom
 - Hátránya:
 - Sok bázisállomás szükséges



BME Hálózati Rendszerek és Szolgáltatások Tanszék 32



Cellák mérete

- Makrocella:
 - Nagy területeket fed le
 - Nagy adóteljesítmény szükséges
 - Ritkán lakott területeken, gyorsan mozgó felhasználók esetén előnyös
 - GSM esetén akár 35 km sugár (speciális hálózati eszközökkel akár 70 km)
- Mikrocella:
 - Kis terület lefedésére való
 - Sűrűn lakott területeken előnyös (nagyobb kapacitás egységnyi területre vetítve)
 - Kis teljesítmény
- Pikocella:
 - Beltéri lefedettséghez, vagy nagyon nagy forgalmú területekhez
 - Kis teljesítmény
- Femtocella:
 - Szélessávú vezetékcsatlakozás a szolgáltató infrastruktúrájához
 - Kevés vezeték nélküli eszközt támogatnak kis cellában
 - 10 méter körüli cellaméret



Cellák közötti mozgás – handover vagy handoff

- Ha a mobil eszköz egy másik cellába átmegy, nem szakadhat meg a kapcsolat, handover vagy handoff történik
 - Történhet a mobil eszköz vezérlésével
 - Pl.: DECT
 - Történhet a hálózat vezérlésével
 - Pl.: GSM, UMTS
 - Kommunikációs overheadet jelent
 - Forgalmuszervezési szempontból előnyösebb
 - Pl.: terhelt cellába nem lép be a végberendezés, esernyőcella esetén nincs folyamatos ide-oda lépkedés



Áramkörkapcsolás - csomagkapcsolás

- Áramkörkapcsolt átvitel:
 - Az erőforrásokat a hálózat a két kommunikáló végpont között lefoglalja
 - Akkor is foglalt az erőforrás, ha éppen nincs rajta forgalom
 - Nagyon jó QoS, viszont rossz kihasználtság
 - Drága
 - Beszédhez ideális
 - Az adatátvitel tipikusan nem ilyen, burstös, a folyamatosan lefoglalt csatorna nagyrészt kihasználatlan



Csomagkapcsolt átvitel

- Nincs folyamatos erőforrás-foglalás
- De lehet QoS, nem feltétlenül statisztikus multiplexálás!



GSM/UMTS/LTE hálózati architektúrák

- Az európai rendszerek evolúciója a GSM használatának kezdeteitől napjainkig
- Lényegesen változott:
 - A felhasználók száma
 - A felhasználói igények: beszéd → adat
 - A forgalom összetétele
 - A hálózati architektúra
 - A jogszabályi környezet



GSM a kezdetekben

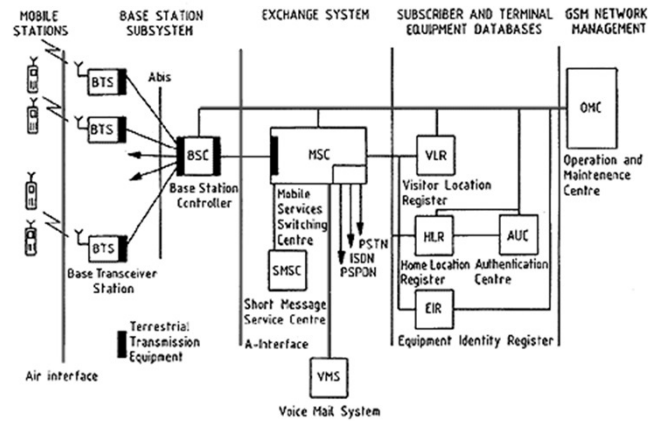
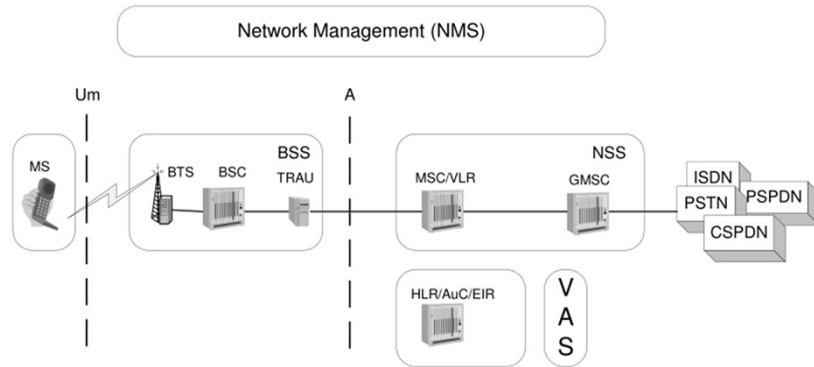


Fig. 1. GSM network architecture

Forrás: Nokia



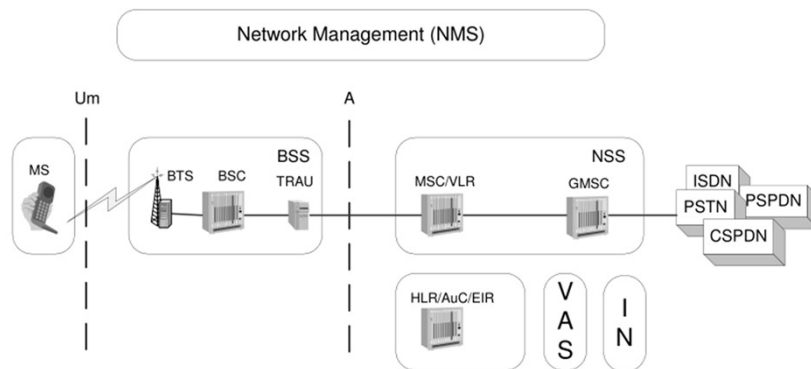
GSM értéknövelt szolgáltatásokkal



VAS: Value Added Service platform: SMS, hangposta stb.



GSM + IN (intelligent network)



IN: például előre fizetett, „kártyás” szolgáltatásokhoz

Forrás: Aalto University

BME Hálózati Rendszerek és Szolgáltatások Tanszék 40

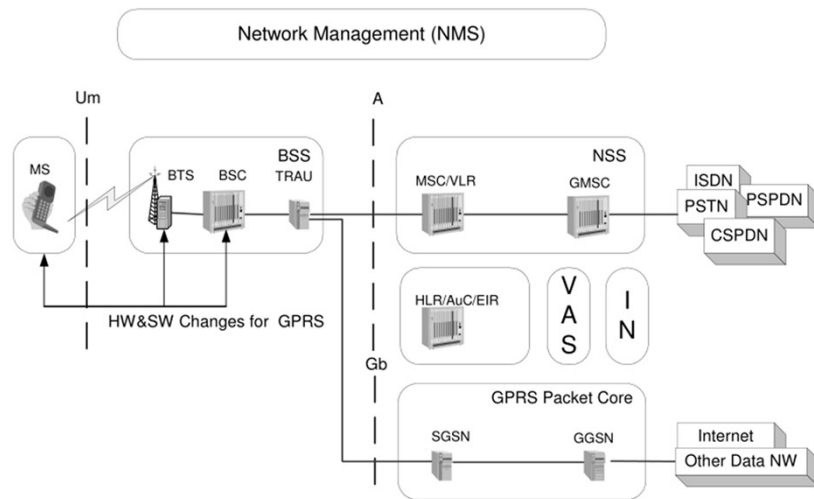


GSM + HSCSD

- A HSCSD (High-Speed Circuit Switched Data) megjelenése az architektúrán nem változtat
- Módosított rendszerelemek:
 - UE – User Equipment
 - BTS, BSC, MSC is változik
- Más csatornakódolás (14 kb/s adatátviteli sebesség)
- Több áramkörkapcsolt átviteli csatorna közösen kezelhető

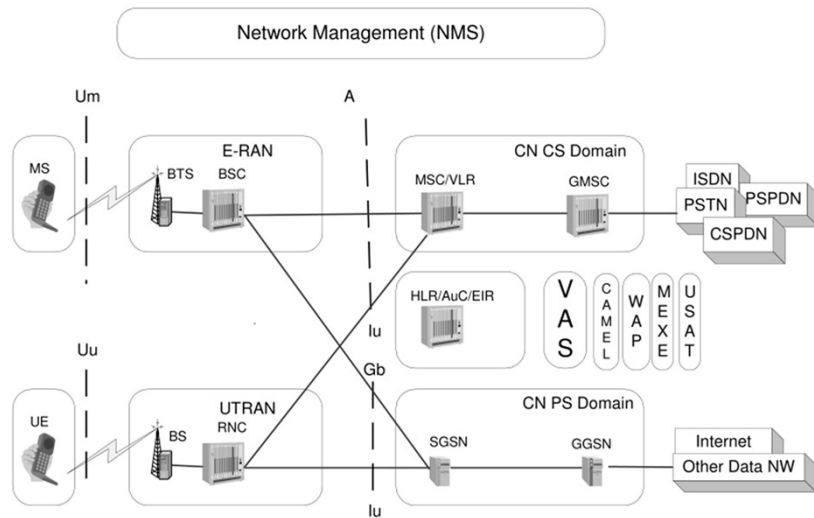


GSM + GPRS



Forrás: Aalto University

BME Hálózati Rendszerek és Szolgáltatások Tanszék 42

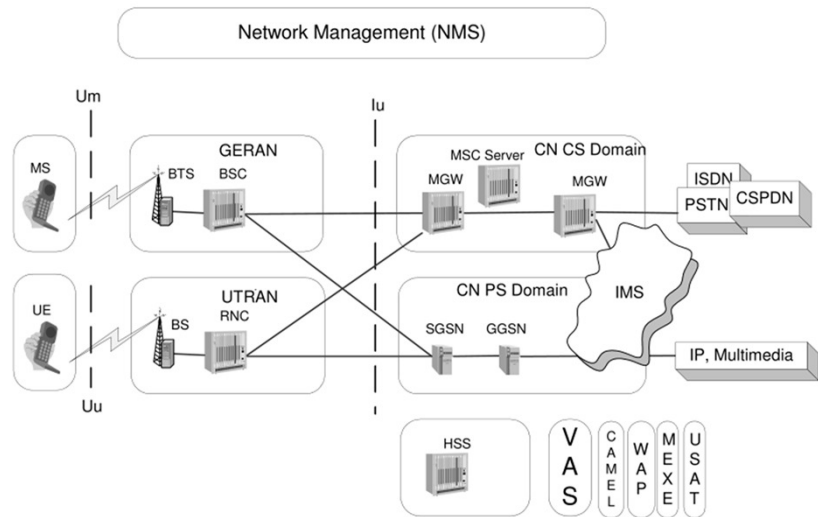


Forrás: Aalto University

BME Hálózati Rendszerek és Szolgáltatások Tanszék 43



3G R4

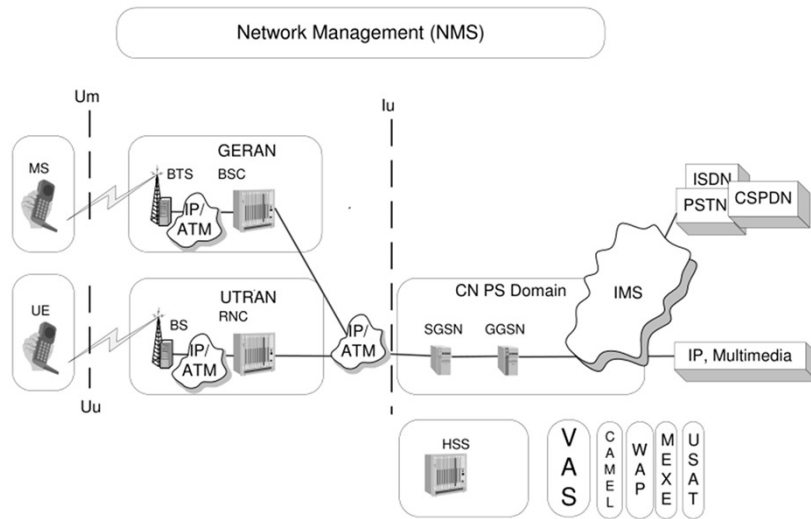


Forrás: Aalto University

BME Hálózati Rendszerek és Szolgáltatások Tanszék 44



3G R5

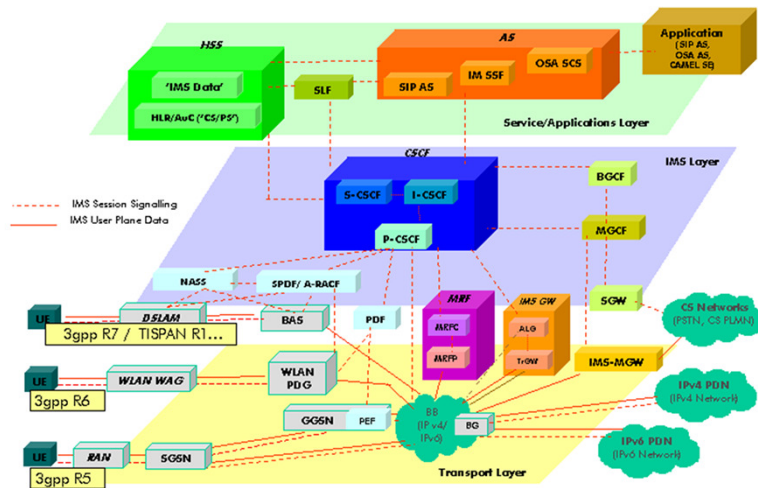


Forrás: Aalto University

BME Hálózati Rendszerek és Szolgáltatások Tanszék 45



IMS architektúra, 3GPP R6-R7

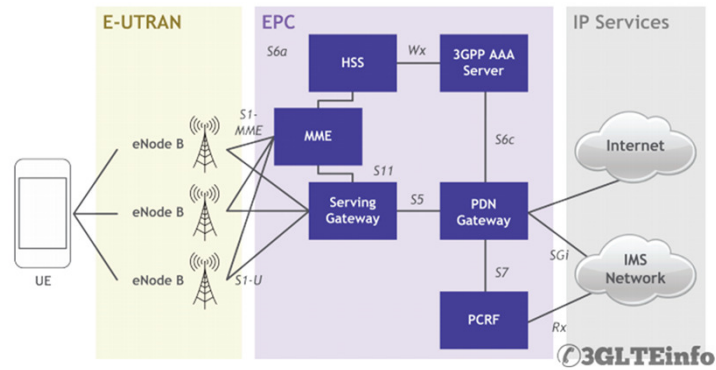


Forrás: Wikipedia, Bluezy

BME Hálózati Rendszerek és Szolgáltatások Tanszék 46



LTE – long term evolution

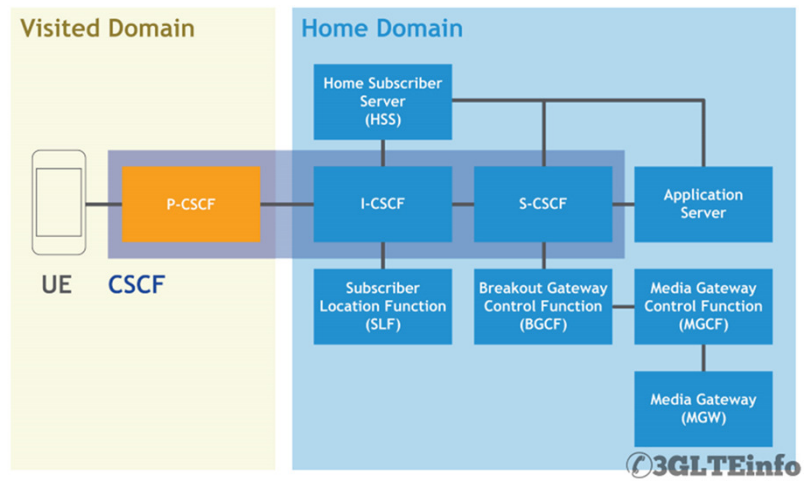


Forrás: www.3glteinfo.com

BME Hálózati Rendszerek és Szolgáltatások Tanszék 47



IMS Core



Forrás: www.3glteinfo.com

BME Hálózati Rendszerek és Szolgáltatások Tanszék 48



LTE és 2G/3G rendszerek együttműködése, LTE evolúció

- Kezdetben az LTE csak adatra
 - SVLTE – Simultaneous Voice and LTE
 - Két rádió, két kapcsolat: egy áramkörkapcsolt kapcsolat hanghívásra és SMS-re, egy LTE kapcsolat adatátvitelre
 - CSFB – Circuit Switched FallBack
 - Egy rádió elég. Adatátvitelre LTE, híváskor automatikus handover 2G/3G hálózatra
- VoLTE – Voice over LTE
 - Nem teljes LTE lefedettség esetén megoldandó az LTE → 2G/3G handover: SRVCC – Single Radio Voice Call Continuity
 - Rendkívül bonyolult
 - IMS-ben bonyolódó (SIP) hívás átadása 2G/3G MSC/MSS alá

Forrás: Qualcomm – VoLTE with SRVCC: The second phase of voice evolution for mobile LTE devices

BME Hálózati Rendszerek és Szolgáltatások Tanszék 49



SRVCC – Single Radio Voice Call Continuity

3GPP Rel-8

- PS → CS handover

3GPP Rel-9

- Kiegészítő szolgáltatások (supplementary services) támogatása az SRVCC folyamatban
- Segélyhívások átadása

3GPP Rel-10

- Alerting fázisú hívások átadása (aSRVCC)
- Tartott és konferenciahívások átadása (eSRVCC)

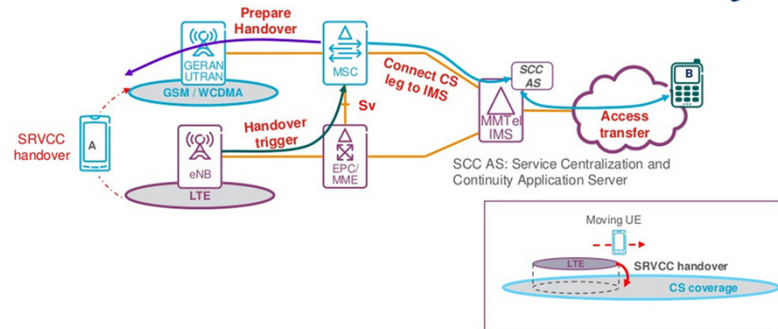
3GPP Rel-11

- Videóhívás (vSRVCC)
- CS → PS handover (rSRVCC)



SRVCC architektúra

Single Radio Voice Call Continuity (SRVCC)



Via: The 3G4G Blog - blog.3g4g.co.uk

Forrás: 3G4G Blog – <http://blog.3g4g.co.uk>

BME Hálózati Rendszerek és Szolgáltatások Tanszék 51



LTE és 2G/3G rendszerek együttműködése, LTE evolúció

- A jövő
 - LTE roaming
 - Csomagkapcsolt hanghívás és adatátvitel megszakítás nélkül LTE, HSPA, 3G és WiFi hálózatokon
 - Nem IMS-alapú szolgáltatásokkal való teljes együttműködés

Forrás: Qualcomm – VoLTE with SRVCC: The second phase of voice evolution for mobile LTE devices

BME Hálózati Rendszerek és Szolgáltatások Tanszék 52



Kliens-szerver kommunikáció ML



Témakörök

- Milyen alkalmazásoknál lehet erre szükség?
- Rossz megoldások (közvetlen adatbázis kapcsolat, statikus tartalmak)
- XML
- Web services
- SOAP, WSDL
- RSS
- REST
- JSON
- AJAX
- RPC
- Push notification



Mikor? Milyen alkalmazásnál



- Ha távoli adatokat kell elérjünk:
 - 1. Példa: egy hírportálhoz készült mobil alkalmazás:
 - El kell érni a hírek listáját a webes formázások nélkül
 - Keresni, rendezni, szűrni kell tudjunk
 - 2. Példa: egy ingatlan közvetítő alkalmazás:
 - Komplex keresési feladatok, találatok betöltése, lapozás a találatok között
 - Kapcsolatfelvétel, üzenet küldés
 - Titkos információk védelme (az ingatlan pontos címe, tulajdonos adatai)
- Ha adatokat szeretnénk eltárolni úgy, hogy azt más készüléken is elérhessük:
 - Felhő megoldások, biztonsági másolatok
- Üzenetküldés:
 - Ha két felhasználó akar egymással üzenetet váltani, egymásnak üzenetet küldeni.



Rossz megoldások

- Közvetlen kapcsolat az adatbázis szerverhez:
 - A kapcsolódási adatokat az alkalmazásba kellene "beégetni", ami könnyen kinyerhető mások számára
 - A hozzáférési adatok birtokában más adatokhoz is hozzáférhetünk
- HTML tartalmak parse-olása:
 - Nem kell külön adatforrás, majd a weblap adatait feldolgozzuk, átstrukturáljuk
 - egy apróbb design módosítás is működésképtelenné teheti az alkalmazást

BME Hálózati Rendszerek és Szolgáltatások Tanszék 56

Az adatbázis szerverek lehetőséget biztosítanak arra, hogy távolról is kapcsolódjunk hozzájuk, a jogosultságokat pedig le lehet korlátozni, hogy az adott felhasználó milyen tartalmakhoz férjen hozzá. Ezen jogosultságok beállítása azonban igen körülményes és sok feladatnál lehetetlen. Pl. egy felhasználók autentikációs adatait tartalmazó tartalmazó tábla esetén az adatbázis felhasználónak az egész táblát kell látni, hogy minden felhasználót tudjon azonosítani. Ha a programkódból kinyerjük az eltárolt adatokat, akkor könnyen olyan adatokhoz férhetünk hozzá, amihez amúgy nem lenne jogosultságunk.

Sokszor előfordul, hogy két rendszer között úgy kell adatokat átvinni, hogy az egyik oldal üzemeltetője nem akar/nem tud erre egy interfészt biztosítani, hanem a meglévő rendszert kell felhasználni, pl. egy weboldal. Ezen megoldások a jövőben rengeteg problémához vezetnek. Ilyen esetben reguláris kifejezésekkel próbáljuk kinyerni a szükséges adatokat, de mivel a weboldal tartalma, struktúrája változhat és a legtöbb esetben változik is, ezért a feldolgozó modul is folyamatos változtatást, karbantartást igényel.



Stateful vs. stateless

- Stateful: egy munkamenet azonosítóval azonosítja a klienst a szerver
 - Előnye: nem kell minden kérésben minden adatot elküldeni (pl. bejelentkezési adatok, keresési, szűrési feltételek)
 - Hátránya: a munkamenet inaktivitás után lejár, a munkamenet azonosító megszerzésével megismerhetjük a felhasználót.
 - Mobil alkalmazásoknál ritkán használjuk



Stateful vs. stateless

- Stateless: a szerver nem tárol el a korábbi tranzakcióinkból semmilyen adatot, minden tranzakcióban minden adatot meg kell adni.
 - Előnye: nem kell külön erőforrást fordítani a munkamenet kezelésére, életben tartására
 - Hátránya: Minden üzenetben meg kell adnunk minden adatot (pl. bejelentkezési adatok), ez növeli az üzenetek méretét

XML

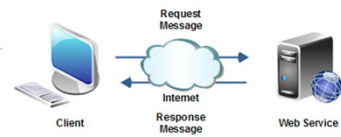
- EXtensible Markup Language
- Számos adatsere formátum közös jellemzője, hogy XML struktúrát használ
- Miért szeretjük az XML-t?
 - Szöveges állomány, ember számára is olvasható, értelmezhető
 - Gyakorlatilag minden platformon van támogatás a feldolgozásukra, generálásukra
 - Fejlett validálási megoldások (DTD, XSD)

```
<?xml version="1.0"?>
<quiz>
  <qanda seq="1">
    <question>
      Who was the forty-second
      president of the U.S.A.?
    </question>
    <answer>
      William Jefferson Clinton
    </answer>
  </qanda>
  <!-- Note: We need to add
  more questions later.-->
</quiz>
```





Web services



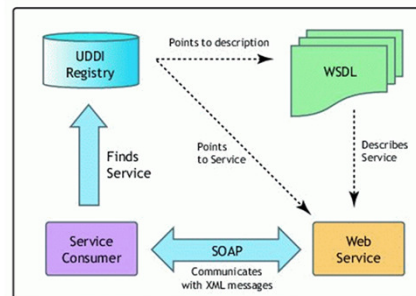
- Alkalmazások közötti adatcsere szabványok és protokollok gyűjteménye weben.
- Jellemzői:
 - Platformfüggetlen: nyílt szabványokra épül, amelyek széles körben elérhetőek (XML, HTTP)
 - Self-contained: Kliens oldalon nincs szükség külön szoftverre, elegendő egy programozási nyelv HTTP támogatással és XML feldolgozó képességgel.
 - Self-describing: az átvitt üzenet tartalmazza az adatstruktúra leírását is, nincs szükség külső metaadatokra (pl. XSD segítségével)
 - Moduláris: Több egyszerűbb web service egy komplex rendszerbe integrálható

XSD (Xml Schema definition): Az XML fájlok struktúráját és az egyes mezők tartalmát szabályozza. Megadható, hogy melyik mezőt kötelező kitölteni, hol milyen értéket várunk el.



Web services UDDI

- Universal Description, Discovery and Integration
- Egy platformfüggetlen megoldás web service szolgáltatásainak leírására, azok felderítésére és tárolására.
- SOAP protokollon történik a kommunikáció
- Manapság már nem használják széles körben



BME Hálózati Rendszerek és Szolgáltatások Tanszék 61

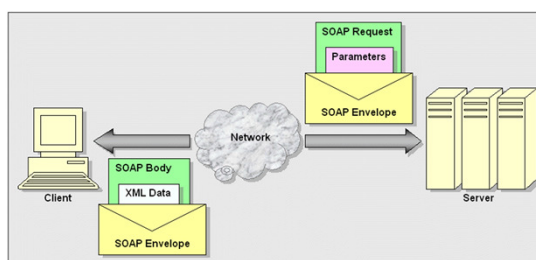
UDDI: a főbb szereplők közösen hozták létre (Dell, Fujitsu, HP, Hitachi, IBM, Intel, Microsoft, Oracle, SAP, and Sun és további 200 szereplő).

IBM, Microsoft és az SAP 2006-ben megszüntette az UDDI állomásait. A Microsoft 2010-ben pedig végleg kivezette a Windows Server operációs rendszereiből, helyette Biztalk-ot használnak.

SOAP (Simple Object Access Protocol): később részletesen lesz róla szó.

SOAP

- Simple Object Access Protocol
- Jellemzői:
 - Web service-ek eléréséhez kifejlesztett kommunikációs protokoll
 - XML alapú
 - Platform és programozási nyelv független
 - Egyszerű és bővíthető
 - Leggyakrabban HTTP-n működik, így a tűzfalak nem okoznak problémát.
 - 2003 óta W3C ajánlás





SOAP szintaxis

- Boríték elem (envelope), ami az XML dokumentumot azonosítja SOAP üzenetként
- Fejléc (header)
- Törzs (body)
- Státusz és hibakód (fault)
- Ezek pontos listája a SOAP névtérben vannak definiálva (ezen névterek használata kötelező):
<http://www.w3.org/2001/12/soap-envelope>
- A használható adattípusokat a SOAP encoding séma írja le:
<http://www.w3.org/2001/12/soap-encoding>



SOAP szintaxis

```
<?xml version="1.0"?>
<soap:Envelope
xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
soap:encodingStyle="http://www.w3.org/2001/12/soap-
encoding">

  <soap:Header>
    <m:Trans xmlns:m="http://www.w3schools.com/transaction/"
      soap:mustUnderstand="1">234
    </m:Trans>
  </soap:Header>

  <soap:Body>
    <m:GetPrice xmlns:m="http://www.w3schools.com/prices">
      <m:Item>Apples</m:Item>
    </m:GetPrice>
  </soap:Body>
</soap:Envelope>
```

BME Hálózati Rendszerek és Szolgáltatások Tanszék 64

Mindig a soap:Envelope elemnek kell lennie a gyökér elemnek!

A soap-envelope névtér használata kötelező!

A fejléc alkalmazás specifikus információkat tartalmazhat (nem kötelező), pl. hitelesítés, fizetési információ.

A mustUnderstand attribútum megadja, hogy a másik fél számára ennek a mezőnek a feldolgozása kötelező-e vagy sem.

A body részben szereplő példa a szerveren a GetPrice függvényt hívja meg, paraméterként pedig az Apples értéket adja át. Erre például ilyen választ kaphatunk:

```
<?xml version="1.0"?>
<soap:Envelope
xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
soap:encodingStyle="http://www.w3.org/2001/12/soap-encoding">

  <soap:Body>
    <m:GetPriceResponse xmlns:m="http://www.w3schools.com/prices">
      <m:Price>1.90</m:Price>
    </m:GetPriceResponse>
  </soap:Body>
</soap:Envelope>
```

</soap:Envelope>



SOAP HTTP felett

- Ha használni is szeretnénk a protokollt, akkor azt valahogy át kell vinnünk HTTP-n, erre a HTTP POST a megoldás:

Kérés:

```
POST /InStock HTTP/1.1
Host: www.example.org
Content-Type: application/soap+xml; charset=utf-8
Content-Length: nnn

<?xml version="1.0"?>
<soap:Envelope
  xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
  soap:encodingStyle="http://www.w3.org/2001/12/soap-encoding">
  <soap:Body xmlns:m="http://www.example.org/stock">
    <m:GetStockPrice>
      <m:StockName>IBM</m:StockName>
    </m:GetStockPrice>
  </soap:Body>
</soap:Envelope>

<soap:Fault>
</soap:Fault>
</soap:Body>
</soap:Envelope>
```




SOAP HTTP felett

Válasz:

HTTP/1.1 200 OK

Content-Type: application/soap+xml; charset=utf-8

Content-Length: nnn

```
<?xml version="1.0"?>
```

```
<soap:Envelope
```

```
  xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
```

```
  soap:encodingStyle="http://www.w3.org/2001/12/soap-encoding">
```

```
  <soap:Body xmlns:m="http://www.example.org/stock">
```

```
    <m:GetStockPriceResponse>
```

```
      <m:Price>34.5</m:Price>
```

```
    </m:GetStockPriceResponse>
```

```
  </soap:Body>
```

```
</soap:Envelope>
```



SOAP példa

- Az MNB SOAP szolgáltatásából akarjuk lekérni az adott napi HUF-EUF árfolyamot.

- Kliens oldalon PHP kódot használunk:

```
$client = new  
SoapClient('http://www.mnb.hu/arfolyamok.asmx?WSDL');  
$response_stdclass = $client->GetCurrentExchangeRates();  
$xml = $response_stdclass->GetCurrentExchangeRatesResult;  
$parser=xml_parser_create();  
xml_parse_into_struct($parser, $xml, $ertekek);
```



WSDL

- Web Services Description Language
- Web service-ek leírására használjuk, ebben definiálhatjuk, hogy milyen szolgáltatást tudunk elérni, milyen paraméterekkel.
- Az alábbi elemek definálhatóak:
 - Adattípusok
 - Üzenetek
 - Metódusok
 - Adatformátumok és protokollok

Pl. <http://www.mnb.hu/arfolyamok.asmx?WSDL>



WSDL példa

```
<message name="getTermRequest">
  <part name="term" type="xs:string"/>
</message>

<message name="getTermResponse">
  <part name="value" type="xs:string"/>
</message>

<portType name="glossaryTerms">
  <operation name="getTerm">
    <input message="getTermRequest"/>
    <output message="getTermResponse"/>
  </operation>
</portType>
```

BME Hálózati Rendszerek és Szolgáltatások Tanszék 69

Hagyományos programozási nyelvekkel összevetve a glossaryTerms egy függvénykönyvtárnak tekinthető, a getTerm pedig egy metódusnak ezen belül. A getTermRequest a metódus bemeneti paramtere, a getTermResponse pedig a visszatérési értéke.



SOAP mobil környezetben

- A protokoll tökéletesen alkalmas lenne mobil alkalmazásokhoz, de a natív SDK szinte egyik platform esetén sem támogatja.
- Léteznek 3rd party megoldások, de ezek nem működnek minden esetben hibátlanul, sok feladatra alkalmatlanok
- Új projekt esetén nem érdemes SOAP-ra építeni a rendszert
- Meglévő SOAP-os rendszerek esetén merülhet fel a használata

BME Hálózati Rendszerek és Szolgáltatások Tanszék 70

Az elérhető ingyenes SOAP implementációk annyira nem javasoltak, hogy sok esetben egyszerűbb egy proxy alkalmazást beiktatni a rendszerbe, ami SOAP-ról JSON-ra vagy REST-re fordít.



RSS

- Rich Site Summary / Really Simple Syndication
- Gyakran frissülő site-ok új tartalmainak rövid összefoglalójának terjesztésére fejlesztették ki.
- Wordpress és számos más ingyenes PHP rendszer tartalmazza alapértelmezetten ezt a funkciót
- Ez alkalmas lehet egy mobil hírolvasó alkalmazás vagy widget működéséhez.

Példa:

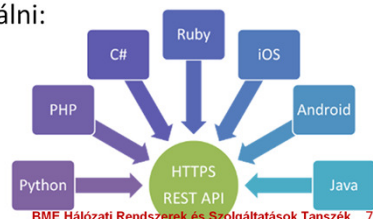
```
<item>
  <title>
    <![CDATA[
      Amikor még aranyból voltak a Földközi-tenger szigetei
    ]]>
  </title>
  <link>
    http://index.hu/mindekozben/poszt/2014/08/25/amikor\_meg\_aranybol\_voltak\_a\_foldkozi-tenger\_szigetei/
  </link>
</item>
```

A Wordpress rendszerekben a <http://sitenév/rss> címen érhető el alapértelmezésben az RSS feed. Gyakran előfordul, hogy más oldalakon (pl. www.hirkereso.hu) több oldal friss cikkeinek, híreinek listáját szeretnénk megjeleníteni. Ilyen célokra ideális az RSS.



REST

- Representational State Transfer: szoftverarchitektúra típus elosztott hipermédia rendszerek számára (pl. a világháló)
- A SOAP-pal ellentétben itt nincs hivatalos standard, mivel nem egy protokollról van szó, hanem egy szoftverarchitektúráról
- Kliensekből és szerverekből áll
- Eredetileg HTTP-re lett leírva, de megvalósítható más protokollon is.
- A kommunikáció menete megegyezik azzal, ahogy egy böngésző lekér egy weboldalt a kiszolgálóról, ezzel a HTTP protokoll számos előnyét ki tudja használni:
 - Proxy szerverek használata
 - Gyorsítótárazás
 - Autentikáció



BME Hálózati Rendszerek és Szolgáltatások Tanszék 72



REST megszorítások

- Egy API akkor lesz REST, ha teljesíti a következő megszorításokat:
 - Kliens-szerver architektúra
 - Állapotmentesség
 - Gyorsítótárazhatóság
 - Réteges felépítés (proxy szerverek támogatása)
 - Igényelt kód
 - Egységes interfész

BME Hálózati Rendszerek és Szolgáltatások Tanszék 73

Kliens-szerver architektúra: pl. böngésző-webszerver páros. A kliens nem foglalkozik adattárolással, a szerver pedig nem foglalkozik a felhasználói felülettel. Ezáltal skálázhatóbb és hordozhatóbb kódot kapunk.

Állapotmentesség: böngészőben lehetőség van a böngészési állapot tárolására egy munkamenet azonosító segítségével, REST API esetén ilyen megoldást nem alkalmazunk.

Gyorsítótárazhatóság: A válaszoknak tartalmaznia kell, hogy az gyorsítótárazható-e vagy sem.

Réteges felépítés: a szerver nem látja, hogy közvetlenül csatlakoztak-e hozzá vagy valamilyen közvetítő segítségével.

Igényelt kód: Opcionálisan kliens oldali programkódokat (javascript, java applet) is képes átadni a szerver a kliensnek.

Egységes interfész: nincsenek előre definiált tag-ek, opciók, paraméterek, az interfész szabadon alakítható ki a kliens és a szerver között, csupán néhány irányelvet kell betartani.



REST interfész irányelvek web service-ek esetén

- Erőforrások azonosítása: HTTP URI segítségével kell azonosítani az elérni kívánt erőforrást.
Pl.
https://api.twitter.com/1.1/users/show.json?user_id=BME_hu
- Formátum kiválasztása: általában JSON vagy XML, de lehet más MIME típus is.
- Standard HTTP metódusok használata (GET, POST, PUT, DELETE)
- Hiperlinkek használata a hivatkozásokhoz és az erőforrásokhoz

BME Hálózati Rendszerek és Szolgáltatások Tanszék 74

MIME: Multipurpose Internet Mail Extensions
(<http://en.wikipedia.org/wiki/MIME>)



REST példa

Erőforrás	GET	PUT	POST	DELETE
Lista URI, pl. http://api.example.com/v1/resources/	Listázza a tagokat, ez a lista URI-ket tartalmaz.	Cseréli a teljes listát egy újonnan feltöltöttre.	Új elem létrehozása a listában.	Teljes lista törlése .
Elem URI, pl. http://api.example.com/v1/resources/item17	A hivatkozott elem lekérése a listából	Cseréli a hivatkozott elemet a listából, ha nem létezik akkor létrehozza azt.	Ritkán használják, a hiathozott elemet egy listának tekinti és ezen belül hozz létre egy elemet. ¹	A hivatkozott elem törlése a listából.



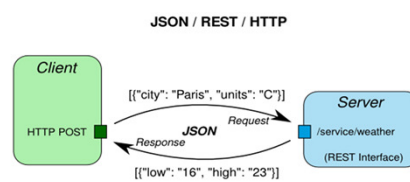
REST mobil alkalmazásoknál

- A legtöbb mobil operációs rendszer fejlesztőkörnyezete támogatja a REST API-t:
- Android
- iOS
- Windows Phone
- Blackberry 10



JSON

- JavaScript Object Notation
- Kis méretű, szöveges, ember által olvasható adatcsere formátum
- Az XML-nél tömörebb, kevesebb adatforgalmat igényel
- Támogatott adattípusok:
 - szám (double)
 - karakterlánc
 - bool
 - tömb
 - objektum
 - null





JSON példa

```
• {
  "vezetekNev": "Kovács",
  "cim" :
  {
    "utcaHazszam": "2. utca 21.",
    "varos"      : "New York",
  },
  "telefonSzam":
  [
    {
      "tipus" : "otthoni",
      "szam"  : "212 555-1234"
    },
    {
      "tipus" : "fax",
      "szam"  : "646 555-4567"
    }
  ]
}
```



JSON használata

- **Használata:**
 - Javascript AJAX
 - Mobil alkalmazások és webszerverek közötti adatcsere
- **Mobil alkalmazások:**
 - iOS, Android, Windows Phone SDK-ban egyszerűen feldolgozható és generálható JSON tartalom.
 - HTTP POST kérésben elküldjük a kérést a szerver felé
 - A válaszban visszakapjuk a kért eredményt



JSON mobil alkalmazás példa

Kérés:

```
{
  "message":
  {
    "action": "getTask",
    "request":
    {
      "params":
      {
        "taskID": "1234"
      }
    }
  }
}
```



JSON mobil alkalmazás példa

- Válasz:

```
{
  "message":
  {
    "action": "getTask",
    "response":
    {
      "resultCode": 0,
      "data":
      [
        {
          "filingNumber": "Iktatószám",
          "filingDate": "Iktatás dátuma",
          "documentLink": "Irátpéldány hivatkozások",
          "externalPartner": "Külső partnerek",
          "ownerOrganization": "Birtokló szervezet",
          "manager": "Ugyintéző",
          ...
        }
      ]
    }
  }
}
```




AJAX

- Asynchronous JavaScript and XML: interaktív webalkalmazások fejlesztésére szolgáló webfejlesztési technika. A Javascript a háttérben adatot cserél a kiszolgálóval a háttérben, így a lap újratöltése nélkül tudunk új tartalmat megjeleníteni.
- A következő technikák kombinációja:
 - XHTML vagy HTML és CSS
 - DOM (Dokumentum Objektum Modell)
 - XMLHttpRequest: objektum az aszinkron adatok kezelésére
 - XML: legtöbbször ezt a formátumot használják, de mostanában már JSON és más formátumok is használatosak.



AJAX példa jQuery segítségével

jQuery: egy nyílt forráskódú Javascript függvénykönyvtár, ami a egyszerűsíti a fejlesztést, elfedi a böngészők közötti különbséget.

```
$("#button").click(function(){  
    $.ajax({url: "demo_test.txt", success:  
function(result){  
    $("#div1").html(result);  
    }});  
});
```

BME Hálózati Rendszerek és Szolgáltatások Tanszék 83

Ez a mintakód jQuery nélkül nagyjából így néz ki:

```
var xmlhttp;  
if (window.XMLHttpRequest)  
    {  
        // code for IE7+, Firefox, Chrome, Opera, Safari  
        xmlhttp=new XMLHttpRequest();  
    }  
else  
    {  
        // code for IE6, IE5  
        xmlhttp=new ActiveXObject("Microsoft.XMLHTTP");  
    }  
xmlhttp.onreadystatechange=function()  
{  
    if (xmlhttp.readyState==4 && xmlhttp.status==200)  
    {  
        document.getElementById('A1').innerHTML=xmlhttp.status;  
        document.getElementById('A2').innerHTML=xmlhttp.statusText;  
        document.getElementById('A3').innerHTML=xmlhttp.responseText;  
    }  
}  
xmlhttp.open("GET","demo_test.txt",true);
```

```
xmlhttp.send();  
}
```



RPC

- Remote Procedure Call
- Processzek közötti kommunikáció adott programban
- A függvény vagy eljárás egy másik címtartományban vagy másik gépen fut
- A programozónak nem kell törődnie azzal, hogy helyi vagy távoli
- A kliens kezdeményezi a kapcsolódást az ismert szerverhez, hogy hajtson végre egy eljárást a megadott paraméterekkel
- A szerver szerver visszaküldi a választ a kliensnek és a program folytatja a munkáját

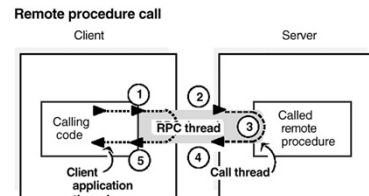
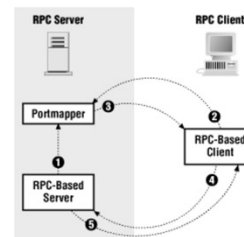


Figure 6-1 Execution Phases of an RPC Thread



ONC RPC implementáció

- Open Network Computing (ONC)
Remote Procedure Call (RPC)
- Sun RPC-ként is hivatkoznak rá, mert a 80-as években a Sun fejlesztette ki
- Unix rendszerekben széles körben elterjedt megoldás
- Az adatok serializálásához un. XDR payloadot állít elő
- TCP vagy UDP felett történhet a kommunikáció



External Data Representation (XDR):

http://en.wikipedia.org/wiki/External_Data_Representation



ONC RPC implementáció

- Az RPC kliens első lépésben egy Port mapper szolgáltatáshoz kapcsolódik
- Ez mindig a 111-es porton fut TCP vagy UDP felett
- A port mapper szolgáltatás mondja meg, hogy melyik RPC szolgáltatást milyen porton érhetünk el
- UNIX alapú rendszerknél az `rpcinfo -p` parancs segítségével tudjuk kilistázni az elérhető szolgáltatásokat
- A lista program szám, verzió szám párosokhoz tárolja el, hogy milyen porton és milyen protokollon (TCP/UDP) érhető el.
- A leggyakrabban használt ONC RPC-t használó szolgáltatás az NFS (Network File System)

BME Hálózati Rendszerek és Szolgáltatások Tanszék 86

Példa:

```
$ rpcinfo -p program vers proto port 100000 2 tcp 111 portmapper 100000 2 udp 111
portmapper 100003 2 udp 2049 nfs 100003 3 udp 2049 nfs 100003 4 udp 2049 nfs
100003 2 tcp 2049 nfs 100003 3 tcp 2049 nfs 100003 4 tcp 2049 nfs 100024 1 udp
32770 status 100021 1 udp 32770 nlockmgr 100021 3 udp 32770 nlockmgr 100021 4
udp 32770 nlockmgr 100024 1 tcp 32769 status 100021 1 tcp 32769 nlockmgr 100021 3
tcp 32769 nlockmgr 100021 4 tcp 32769 nlockmgr 100005 1 udp 644 mountd 100005 1
tcp 645 mountd 100005 2 udp 644 mountd 100005 2 tcp 645 mountd 100005 3 udp 644
mountd 100005 3 tcp 645 mountd
```

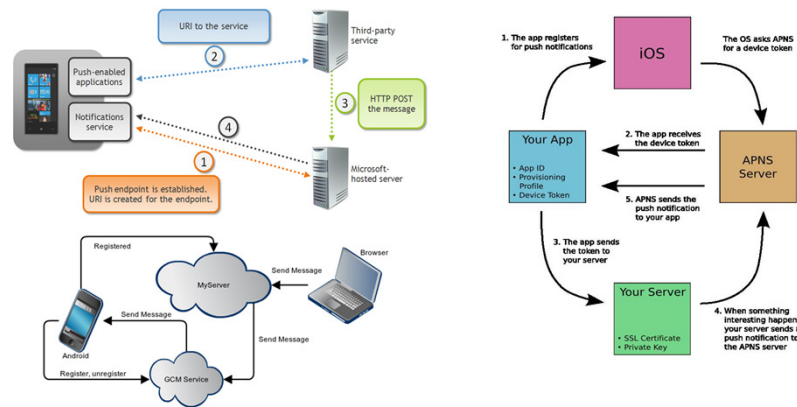


XML-RPC implementáció

- Az adatokat XML fájlalba kódolva juttatja el egymásnak a kliens és a szerver
- HTTP felett történik a kommunikáció
- HTTP basic authentication segítségével történhet a hitelesítés
- A REST-tel ellentétben itt a távoli eljárások hívása a lényeg, nem adatok lekérése, módosítása.
- A SOAP-nál egyszerűbb, mert:
 - Az adatok kódolására csak egy módszer van, ellenben a SOAP-nál több is.
 - Egyszerűbb biztonsági rendszer (HTTP basic authentication hitelesítés)
 - Nincs szükség WSDL szolgáltatás leíróra.
- Az utóbbi időkben elterjedt a JSON-RPC implementáció is, ez egyedül a használt formátumban különbözik az XML-RPC-től.



Push Notification





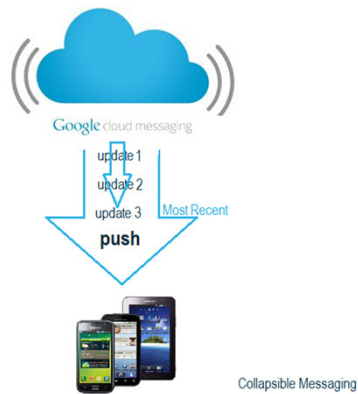
Push Notification

- A mobil készülék életben tart egy TCP kapcsolatot, amire a szerver értesítéseket tud küldeni.
- Android esetén Google Cloud Messaging (GCM) néven érhető el
- iOS esetén Apple Push Notification Service (APNs)
- Ha értesítést szeretnénk küldeni, akkor a Notification server felé kell elküldenünk az alkalmazás azonosítóját, a felhasználó azonosítóját és az üzenetet.
- A mobil készülék az alkalmazás azonosító alapján dönti el, hogy melyik alkalmazásnak szól és engedélyezett-e az értesítés.



Google Cloud Messaging (GCM)

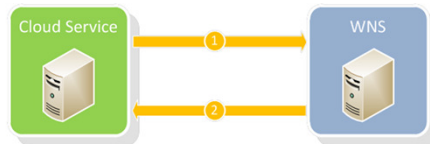
- Google ingyenes szolgáltatása, mellyel eredetileg Androidos eszközökre és Chrome alapú rendszerekre lehetett push üzeneteket küldeni
- A szolgáltatás mára már iOS alapú eszközökre is használható
- A protokoll leírása szabadon elérhető és számos ingyenesen elérhető implementációt is találhatunk





Windows Push Notification Services (WNS)

- Működését tekintve hasonló az Apple és a Google megoldásához
- Működése:
 - A mobil alkalmazás igényel egy ún. Notification channel-t a WNS szolgáltatástól
 - Ezt egy URI-ban adja vissza a mobil alkalmazásnak a WNS
 - Ezt az URI-t a mobil alkalmazás elküldi az alkalmazáshoz tartozó szervernek
 - Később ezzel az URI-val lehet azonosítani az eszközt.





Apple Push Notification Service (APN)

- iOS 3.0-tól kezdve támogatottak a push üzenetek
- OSX 10.7-től kezdve pedig az asztali operációs rendszerre is küldhető push üzenet
- iOS 8-nál korábbi verzióknál maximum 256 byte lehetett az üzenet mérete, ezt követően 2 kbyte-ra növekedett.





Biztonság

- Problémák azonosítása:
 - Átviteli anomáliák:
 - Forgalom lehallgatása
 - Forgalom megváltoztatása, manipulálása
 - Mentett forgalom visszajátzása
 - Cél szerver meghamisítása
 - Kliens oldali anomáliák:
 - Kliens alkalmazás visszafejtése, konstansként tárolt címek, adatokkal való visszaélés
 - Kliens alkalmazás adatbázisának, tárolt adatainak módosítása
- Az átvitt adatok bizalmasságának, fontosságának meghatározása
- A fontosság alapján az átviteli protokoll kiválasztása:
 - HTTP: bizalmas információt nem tartalmazó adatok esetén javasolt
 - HTTPS: a lehallgatás ellen megfelelő védelmet nyújt, a közbeékelődéses támadással szemben csak akkor nyújt védelmet, ha a kliens és a szerver is meg tud győződni a másik fél tanúsítványának valódiságáról.

4. Otthonautomatizálás, távfelügyelet, gépjármű felügyelet



Témakörök

- Otthonautomatizálás
 - Szabványos protokollok
 - Ipari megoldások
- Otthon és gépjármű felügyelet
 - Kamera rendszerek
 - Riasztó rendszerek
 - Távfelügyelet



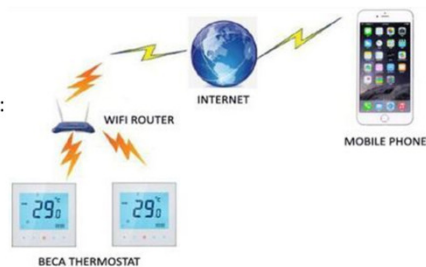
Otthonautomatizálás

- Célok
 - Kényelem növelése
 - Pl. motoros redőny, automata garázskapu
 - Energiatakarékosság
 - Pl. hűtés-fűtés, világítás, szellőztetés optimalizálása
 - Jobb életminőség
 - Pl. páratartalom szabályozás, hővisszanyerős szellőztetés



Otthonautomatizálás - fűtés

- Termosztát: egy beállított küszöbhőmérséklet elérése esetén elektromos érintkezést alkot. Ennek segítségével tudja a kazánt ki-be kapcsolni. Ez tekinthető az első fűtés automatizálási megoldásnak. Fejlettségtől függően különböző fajtákkal találkozhatunk:
 - Egyszerű analóg termosztát: egy potméter segítségével beállíthatjuk a kívánt hőmérsékletet (esetenként csak 1-5 közötti fokozatot)
 - Helyben programozható termosztát: lehetőség van napokra és azon belül napszakokra lebontva megadni az elvárt hőmérsékletet.
 - Időjárás követő termosztát: a külső hőmérséklet függvényében képes a kazán további paramétereit is szabályozni (pl. előremenő vízhőmérséklet)
 - Távolról programozható termosztát: régebben telefonos interfészen, az újabb modelleket wifin keresztül távolról is lehet programozni.



BME Hálózati Rendszerek és Szolgáltatások Tanszék 97

Példa egy Wifin keresztül programozható és vezérelhető termosztátra:
<http://www.aliexpress.com/item/FAN-COIL-WIFI-ROOM-THERMOSTAT/32313494728.html>



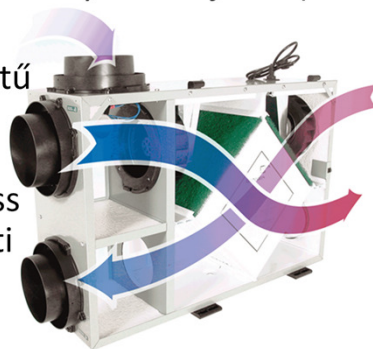
Otthonautomatizálás – hűtés, fűtés

- Hőszivattyús fűtés esetén fal, mennyezet és padlófűtés használata ajánlott, mivel ez a technológia csak alacsonyabb víz hőmérsékletet tud gazdaságosan előállítani
- Ez a hűtési-fűtési forma azonban összetettebb vezérlést tesz szükségessé:
 - A falak hűtésénél páralecsapódás és penész képződés jöhet létre ha hirtelen túlságosan lehűtjük a falat, ezért a vezérlésnek a harmatpont feletti értékre szabad csak hűteni a falakat.
 - Ezek a berendezések ún. Geo tarifa csomagban kapják az elektromos áramot. Itt az olcsóbb tarifáért cserébe csak napi 20 órán át garantált az elektromos áram ellátás. Ezekre a kimaradásokra fel kell készülnie a vezérlésnek.



Otthonautomatizálás – Szellőztetés

- Az ablakok kinyitása nem gazdaságos (télen kihűl a lakás, nyáron bemelegszik, sok szennyeződés jut be)
- Hővisszanyerős szellőzés:
az elhasznált, szobahőmérsékletű levegő és a friss levegőt egy hőcserélőben egymás mellett áramoltatják, így a beérkező friss levegő nem hűti le vagy melegíti fel a helyiséget.





Otthonautomatizálás – Szellőztetés

- A hőcserélőnél a kondenzvíz kicsapódik, így a páratartalom is szabályozható
- A beérkező levegő különböző szűrőkkel megtisztítható, így tisztább, kevesebb pollen tartalmú levegő jut be.
- A szellőztetés helyiségenként szabályozható



Otthonautomatizálás - világítás

- Lámpák különböző kombinációban történő fel-le kapcsolása, távvezérlés: hagyományos kapcsolókkal és alternatív bekötésű kapcsolókkal nagyon bonyolult, sok kapcsolóból álló rendszert kapunk, ilyen esetben már egy célszerű egy központi vezérlőt alkalmazni.
- A nagyobb gyártók (Schneider, Legrand): saját, zárt protokollon működő rendszereket fejlesztettek erre a célra. Programozásuk korlátozott, egyedi igényeket nem minden esetben tud kielégíteni.



Otthonautomatizálás – átfogó megoldások

- Olyan rendszerek, amelyekkel a legtöbb korábban ismertetett feladat egyben megoldható
- Szabványos protokollok:
 - KNX
 - X10
 - CAN
- Elterjedt megoldások
 - Loxone
 - Velbus



KNX

- ISO-OSI alapú hálózati kommunikációs protokoll
épület automatizálási feladatokra
- Szabványosított (EN 50090, ISO/IEC 14543)
- A KNX Association felügyeli a szabványt
- A szervezetnek több 100 gyártó és több 1000 ipari partner a tagja.
- Három korábbi szabványra épül:
 - EIB (European Installation Bus)
 - EHS (European Home Systems Protocol)
 - BatiBus



KNX fizikai réteg

- Az alábbi fizikai átviteli megoldások támogatottak:
 - Sodrott érpár (EIB és BatiBus szabványokból örökölt)
 - Vivőáramú átvitel (EIB és EHS szabványokból örökölt)
 - Rádiós (KNX-RF)
 - Infra
 - Ethernet (KNXnet/IP)



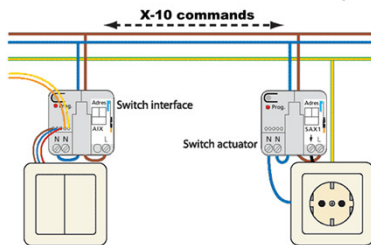
KNX rendszer

- Minden elem vezetékes vagy vezeték nélküli összeköttetésben állnak, hogy adatokat tudjanak cserélni.
- Szenzorok: pl. fénymérő, hőmérő, nyomógomb, mozgásérzékelő
- Végrehajtók: pl. fűtés szelepek, fényerő szabályzó.
- Az eszközöket egy 16 bites címmel lehet megcímezni => 65536 elemet tud kezelni a rendszer



X10 protokoll

- Ipari szabvány elektronikus eszközök közötti kommunikációra
- Eredetileg vivőáramon történő kommunikációra fejlesztették ki, később rádiós változatot is definiáltak
- A háztartási 110 / 230 voltos hálózaton működik.

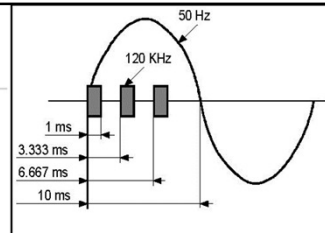


BME Hálózati Rendszerek és Szolgáltatások Tanszék 106

1975-ben fejlesztette ki egy Pico Electronics nevű cég otthoni eszközök távvezérlésére.



X10 protokoll



- Az átvitelt a váltóáram nullátmenet pontjához szinkronizáljuk, ahhoz minél közelebb.
- 120 kHz-es frekvencia
- 22 bites kódokat küld, ennek felépítése:
 - 4 bit Start code, minden esetben 1110
 - 8 bit House code
 - 10 bit Unit code: (pl. 00001- minden lámpa le, 000011- minden lámpa fel)

BME Hálózati Rendszerek és Szolgáltatások Tanszék 107

Protokoll részletes leírása: http://www.haibrain.com/informatie-domotica-x10-protocol-c-131_148_141.html?language=en



CAN busz

- Control Area network
- Multi master protokoll: nincs kiválasztott busz vezérlő, minden csomópont teljesen egyenrangú
- Üzenetközpontú: egyedi azonosító (identifier) alapján történik az üzenetek azonosítása, amit a hordozott információ fontossága szerint kapnak
- Nem-destruktív arbitrációs mechanizmus (non-destructive arbitration): CSMA/CD+CR technikát használ
- Broadcast: üzeneteket mindig minden csomópont megkapja

BME Hálózati Rendszerek és Szolgáltatások Tanszék 108

Az üzenetek azonosítása nem a küldő vagy a fogadó csomópont címe alapján történik (mint általában a többi buszrendszerénél), hanem egyedi azonosító (identifier) alapján, amit a hordozott információ fontossága szerint kapnak. Az üzenetazonosító határozza meg tehát az adott üzenet prioritását, valamint közvetlenül szerepet játszik a buszért való versengés eldöntésében is.

Az adatbuszt elérni kívánó csomópontok várnak a busz felszabadulásáig, majd megkezdik a kommunikációt a kezdő bit (start bit) átvitelével, amely szinkronizálja az összes kommunikációs partnert. Ezután történik az üzenetazonosító továbbítása. Több partner egyidejű adási szándéka esetén ebben a szakaszban történik az ütközés feloldása, bitszintű arbitrációval. Ezt a technikát nem-destruktív arbitrációs mechanizmusnak (non-destructive arbitration) nevezzük, mivel a „vesztes” csomópont úgy mond le buszigényéről, hogy amiatt az átvitt magasabb prioritású üzenet nem sérül. Ez annyit jelent, hogy mindennemű késleltetés nélkül a legmagasabb prioritású üzenet továbbítódik a buszon.

A buszon továbbított üzeneteket mindig minden csomópont megkapja (broadcast), és ellenőrzi. A csomópontok az üzenetek azonosítója alapján döntenek el, hogy pufferelek-e azt későbbi kiértékelés céljából vagy figyelmen kívül hagyják. Az üzenetszűrőt (message filtering) a felhasználói alkalmazás állítja be.



CAN busz

- Eseményvezérelt: amikor valamelyik csomópontnak van küldendő üzenete, akkor kezdi meg az adást, ellentétben az időosztásos rendszerekkel.
- Távoli válaszkérés: lehetőség van távoli válaszkérő üzenet küldésére, ha egy távoli csomóponttól van szükség információra.
- Flexibilis: dinamikusan rákapcsolhatunk ill. leválaszthatunk eszközöket a többi csomópont megzavarása nélkül
- Gyors: maximális sebessége 1000kbit/s (40m-es buszhossznál).

BME Hálózati Rendszerek és Szolgáltatások Tanszék 109

Az üzenetek rövidek, a késleltetési idő maximálva van, az arbitráció pedig gyors. Az utóbbi tulajdonságok alkalmassá teszik a CAN rendszert a valós idejű események (pl.: ABS, motorvezérlés) irányítására.



CAN busz

- Olcsó: elterjedt, széles körben használt. Sorozatgyártásban olcsón előállítható eszközök alkotják.
- Robosztus: hibadetektáló és hibakezelő mechanizmusokkal rendelkezik
 - 15 bites, 6-os Hamming-távolságú CRC
 - Üzenetek automatikus újraküldése
 - Vezetékhiba detektálás:
 - Szakadás
 - Testzárlat
 - Egyéb zárlat
 - Nyugtázás: az üzenetek globális nyugtázó mezővel rendelkeznek

BME Hálózati Rendszerek és Szolgáltatások Tanszék 110

Az üzenetek globális nyugtázó mezővel rendelkeznek, amely jelzi a küldő csomópontnak, hogy legalább egy kommunikációs partnerhez hibátlanul megérkezett az üzenet. Így a küldő információt kap arról, hogy még a buszhoz van-e csatlakoztatva, vagy sem. A broadcast-jellegű üzenettovábbítás következtében minden csomópont nyugtázó jellel válaszol, ha nem észleltek hibát



CAN alkalmazási területei

- Autóipar
- Ipari automatizálás
 - Orvosi elektronika
 - Háztartási eszközök
 - Épület automatizálás
 - Vasúti rendszerek
 - Hajózás
 - Mezőgazdasági rendszerek
 - Repülőgép elektronika
 - Robotvezérlés
 - Intelligens motorvezérlés
- Űrtechnológia



CAN protokoll felépítése

- ISO-OSI modell alapján épül fel.
- A fizikai és az adatkapcsolati réteget definiálja melyet magasabb szintű protokollok egészítenek ki
- Fizikai réteg:
 - Nincs kikötés a fizikai médiumra, de a csavart érpár a legelterjedtebb.
 - Feladatai:
 - A/D konverzió
 - Jeltovábbítás
 - Bitidőzítés és szinkron
 - Maximális sebesség: 1 Mbit/s

BME Hálózati Rendszerek és Szolgáltatások Tanszék 112

Ilyen magasabb rendű protokollok:

CANOpen, Device Net, Smart Distributed Systems (SDS), J1939, CAN Application Layer (CAL), CANKingdom, OSEK/VDX



CAN protokoll felépítése

- Adatkapcsolati réteg:
 - MAC és LLC alrétegekre bontható
 - LLC (Logical Link Control):
 - Busz felől kapott üzenetek szűrése
 - Túlcsoordulás jelzés
 - Hibaállapotok felismerése
 - MAC (Medium Access Control):
 - Keretek összeállítása
 - Vezérli az arbitrációt
 - Felismeri és jelzi a hibákat
 - Hiba elszigetelő (Fault Confinement) eljárás az állandó meghibásodások megkülönböztetése



SDR

- Short Range Devices (kis hatótávolságú eszközök)
- Gyűjtő kategória, minden olyan általános célú rádiós eszközre, amelyek kis távolságban, kis energiával kommunikálnak (távírányítók, szenzorok, stb)
- Főbb csoportjaik:
 - Általános (távérő, távirányító, riasztó, adatátviteli és hasonló célú) alkalmazások
 - Lavina vészjeladó és vészjelvevő alkalmazások
 - Szélessávú adatátviteli alkalmazások (vezeték nélküli egér, nyomtató)
 - Vasúti alkalmazások
 - Közúti közlekedési és forgalmi telematikai (RTTT) alkalmazások
 - Rádiómeghatározó alkalmazások (mozgásérzékelő, ajtónyitás-vezérlők, sebességmérő radarok)
 - Riasztó alkalmazások
 - Modellirányító alkalmazások
 - Induktív alkalmazások (immobilizerek, állatazonosítók)
 - Rádiómikrofon alkalmazások (zsinór nélküli mikrofonok)
 - Rádiófrekvenciás azonosító (RFID) alkalmazások
 - Aktív orvosi implantátumok és perifériáik
 - Vezetéknélküli hangfrekvenciás alkalmazások (pl. vezeték nélküli fejhallgatók)

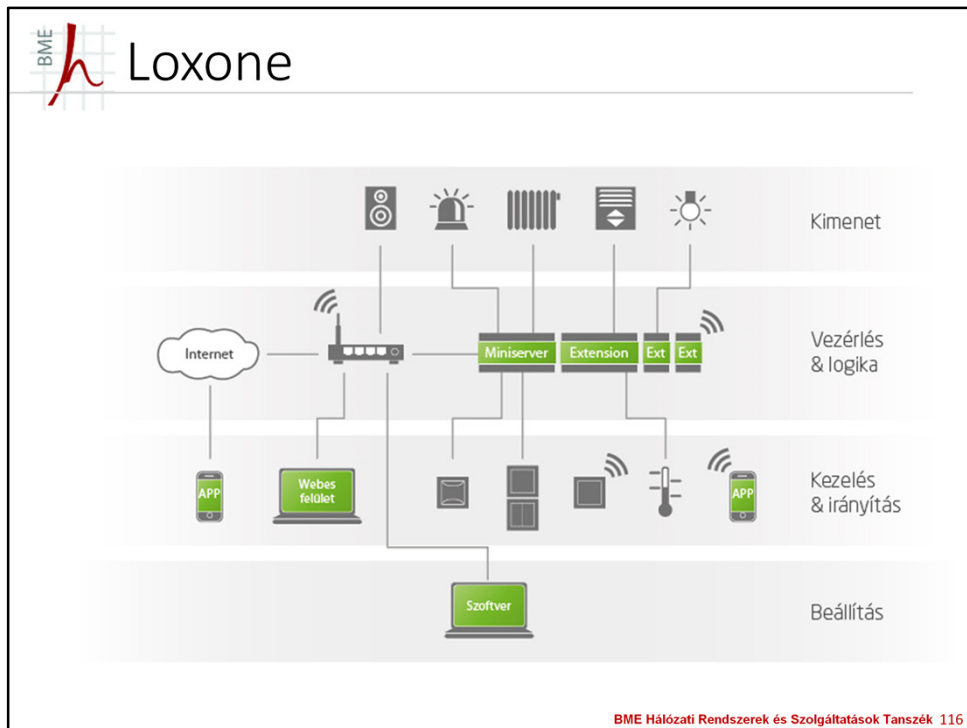
BME Hálózati Rendszerek és Szolgáltatások Tanszék 114

http://nmhh.hu/dokumentum/319/kis_hatotavolsagu_eszkozok_srdk.pdf



ZigBee

- Alacsony energia igényű, 10-100 méteres távolságokra kifejlesztett vezeték nélküli kommunikációs protokoll
- Titkosított átvitel
- 250 kb/s maximális sebesség
- ISM sávban működik (2.4GHz, 868MHz, ...)
- Gyakorlati alkalmazása széles körben nem terjedt el

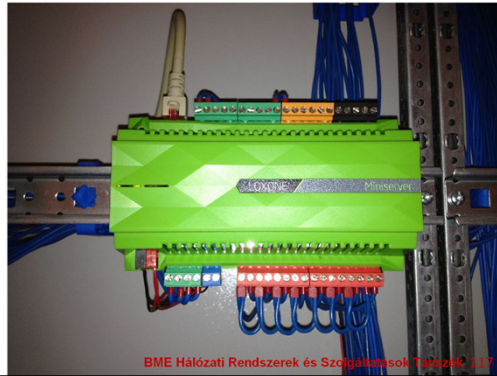


A miniserver nevű a rendszer központi eleme, erre köthetjük rá a vezérelni kívánt eszközöket vagy bővítő eszközöket.
Lehetőség van webes felületről, mobiltelefonról, táblagépről vagy hagyományos kapcsolóról is vezérelni az eszközöket.



Loxone miniserver

- Műszaki adatai:
 - 8 digitális bemenet
 - 4 analóg bemenet
 - 8 digitális kimenet
 - 4 analóg kimenet
 - LAN csatlakozó
 - Beépített webszerver
 - Konfigurációs szoftver
 - KNX rendszerrel való együttműködéshez külön eszköz is licensz szükséges



BME Hálózati Rendszerek és Szolgáltatások Tanszék 117



Velbus

- Moduláris rendszer, központi elem nélkül
- Az elemek között a kapcsolat egy négy vezetékes buszon történik
- A konfigurálás történhet manuálisan vagy PC-s szoftver segítségével.
- Modulok:
 - Bemeneti modulok: a nyomógomboktól, kapcsolóktól, érzékelőktől érkező információt átalakítják és továbbítják a buszon.
 - Kimeneti modulok: a buszon érkező információkat értelmezik még és vezérlik a szükséges egységeket (világítás, fűtés, légkondicionálás, stb)
- <http://www.velbus.eu/>



Otthon felügyeleti megoldások

- Cél:
 - Bűncselekmény elleni védelem:
 - Riasztó berendezés megszólalása elriassza az elkövetőt
 - Riasztás esetén az elkövetők tettenérése.
 - Képi bizonyítékok egy korábbi incidensről
 - Tűz és egyéb katasztrófák elleni védelem:
 - Tűzjelző, automata oltó berendezések
 - Fagyvédelem (pl. hőmérséklet monitorozása)
 - Gázszivárgás, CO szivárgás elleni védelem
 - Csőtörés, elárasztás elleni védelem



Kamera rendszerek

- Elemei:
 - Kamerák:
 - Analóg
 - SD (650-700 TV sor)
 - HD-SDI (1080 sor)
 - IP
 - DVR / NVR: Digital Video Recorder / Network Video Recorder



HD-SDI



BME Hálózati Rendszerek és Szolgáltatások Tanszék 120



Kamerák

- Analóg kamerák:
 - Koax kábel a DVR és a kamera között
 - Alacsony késleltetés az IP kamerákhoz képest
 - Külön kábel kell a kép, a hang és a táp átviteléhez
 - SD és a HD rendszerek azonos kábelezésen működnek
- IP kamerák
 - UTP kábelrel vagy Wifin működnek
 - PoE támogatás esetén elegendő 1 kábel
 - CMOS felbontástól az 5-6 megapixelig elérhető számos felbontásban
 - Nagyobb késleltetés



Kamerák kiválasztási szempontjai

- Kültéri / Beltéri
- Fali / Mennyezeti
- Látószög / távolság: az objektívek egy megadott tartományban állíthatóak illetve különböző objektívvel rendelhetőek
- Éjjeli infra üzemmód
- Kamera szenzor gyártója, típusa (teszt videó felvételek összehasonlítása)

BME Hálózati Rendszerek és Szolgáltatások Tanszék 122

Ezen az oldalon különböző szenzorú kamerák képeit lehet összehasonlítani:
<https://www.youtube.com/user/bigsecurity1/videos>



Kamera rögzítő eszköz

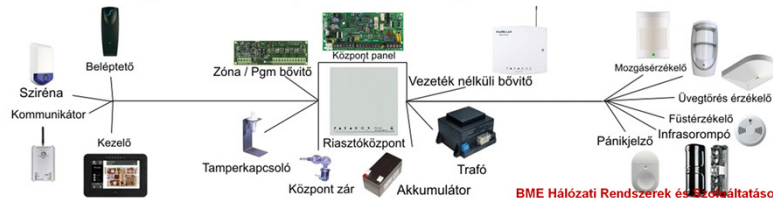
- DVR / NVR eszközök képesek több kamera egyidejű kezelésére (4, 8, 16, ...).
- Folyamatos képrögzítés vagy mozgásra / külső triggerre induló rögzítés merevlemezre vagy hálózati eszközre.
- Böngészőből, okostelefonról elérhető felület
- Helyhiány esetén a régi felvételek automatikus törlése
- E-mail értesítő, FTP-s feltöltés (modell függő)
- Létezik PC-s kártya az analóg kártyák kezelésére, de elterjedtebb a külön eszköz.



Riasztó berendezések

- Elemei:

- Riasztóközpont
- Kezelők
- Mozgásérzékelők
- Nyitásérzékelők
- Egyéb érzékelők (üvegtörés, füst, infrarompó)
- Hang és fényjelzők
- Akkumulátorok
- Távfelügyeleti modul (kommunikátor)





Riasztó berendezések

- Riasztóközpont:
 - Érzékelők kimenetének feldolgozása
 - Kezelők működésének kontrollálása
 - Jelzések továbbítása a kommunikátor és a szirénák felé
- Kezelő egység:
 - Riasztás, élesítés ki-be kapcsolása
 - A központ programozása
 - Rendszer üzenetek megtekintése



BME Hálózati Rendszerek és Szolgáltatások Tanszék 125



Riasztó berendezések - mozgásérzékelők

- Legtöbb esetben Passzív infra mozgásérzékelőt (PIR) használnak
- Három részből áll:
 - Érzékelőelem
 - Optikai rendszer
 - Jelfeldolgozó áramkör
- Terület infravörös tartományba eső sugárzását figyel (pl. testhő) és egy pontra fókuszálja az optikai rendszer
- A fókuszpontban egy piroelektromos elven működő érzékelőelem található
- A szenzor által előállított elektromos jeleket egy jelfeldolgozó áramkör értékeli ki

BME Hálózati Rendszerek és Szolgáltatások Tanszék 126

A piroelektromos szenzor feladata, hogy a védett területen mozgó ember által kiváltott infrasugárzás szintjének – a környezet alap jelszintjéhez viszonyított – megváltozását villamos jelváltozássá alakítsa.

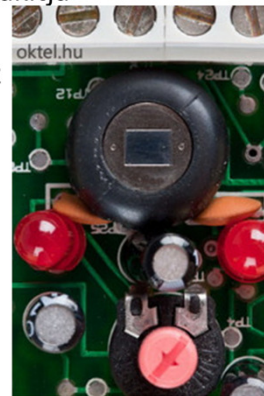
Forrás: <http://oktel.hu/szolgáltatatas/riasztoberendezesek/mozgaserzekelok/a-passziv-infra-es-felepitesi/>



Riasztó berendezések - mozgásérzékelők

- Érékelőelem

- A környezet sugárzásainak változását érzékeli és az infravörös sugárzást elektromos jelekké alakítja
- Piroelektromos elven működő tranzisztor
- 10 μm -es hullámhossznál a legnagyobb az érzékenysége (emberi testre jellemző)
- Fémtokban helyezkedik el, tetején egy infraszűrővel ellátott ablak van
- Úgy alakították ki, hogy a gyors hőmérsékletváltozásra reagáljon



BME Hálózati Rendszerek és Szolgáltatások Tanszék 127

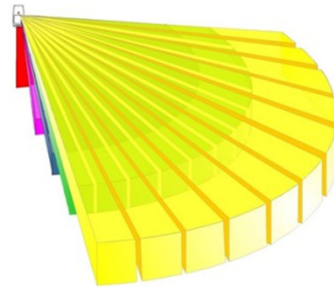
A képen egy piroszenzor látható.



Riasztó berendezések - mozgásérzékelők

- Optikai rendszer

- A környezet által kibocsátott és visszavert infravörös energiát az érzékelő elemre fókuszálja
- Tükrös vagy Fresnel-lencsés kialakítású lehet.
- Legyező szerű látótér
- Érzékeny és érzéketlen zónákat hoz létre
- A nyalábokat metszve felváltva lép érzékeny és érzéketlen zónákba



BME Hálózati Rendszerek és Szolgáltatások Tanszék 128

Lencsés érzékelők esetében egy lencsesorokból álló lencserendszer kerül az érzékelő elem elé, tükrös érzékelők esetében pedig az érzékelő elem mögé, és mindkét megoldás egy pontba gyűjti a hőszugárzást.

Az infraérzékelő látótere felülnézetből úgy néz ki, mintha több, egymás alá helyezett legyezőt fognánk össze ujjainkkal, ahol a lencserendszer fókuszpontja a legyezők töve, az érzékelőnyalábok pedig a legyező kiterjesztett részei lennének. A legyezőt alkotó gúlaszerű nyalábok olyan sávokat hoznak létre, amelyek a védett helyiséget érzékeny és érzéketlen zónákra bontják. Az érzékeny zónákban az infra érzékeli a hőmérsékletváltozást, az érzéketlen szektorokban viszont nem.

Amikor egy ember átmegy a védett helyiségen, merőlegesen metszve a nyalábokat, felváltva lép be érzékeny és érzéketlen zónákba. Az érzékeny zónában tartózkodás megemeli az érzékelt alaphőmérsékletet, az érzéketlen zónában tartózkodás változatlanul hagyja azt. Ez a hőmérséklet-változáson alapuló mozgásérzékelés alapja.

Fentiekből következik, hogy a PIR érzékenyebb a nyalábokra merőleges irányú mozgásra, mint a velük párhuzamos irányúra. Felvetődhet a kérdés, hogy ha a

betörő nem merőlegesen, hanem két nyaláb közti holt térben mozog, akkor észrevétlen maradhat-e? Nos, semmi esetre sem. A védett térbe belépő ember nem tudhatja, hogy a helyiség mely részein helyezkednek el az érzékeny és érzéketlen zónák. Persze teszteléssel ki lehet deríteni: sétatesztnek hívják a telepítők ellenőrzési módszerét, de ez betörés idején kivitelezhetetlen, hiszen egy rossz mozdulat már riasztást generál. Ráadásul a szűkülő nyalábok között nincs is akkora rés, hogy egy ember azon belül mozogni tudjon.



Riasztó berendezések - mozgásérzékelők

- Jelfeldolgozó áramkör
 - Folyamatosan figyeli a változásokat
 - Felerősíti és kiértékeli azokat a jeleket, amelyeket a szenzorok összegyűjtöttek
 - Emberi mozgás elkülönítése a melegvérű állatok mozgásától, a huzattól és számos más zavaró jeltől
 - Impulzusszámlálóval csökkenthető a téves riasztások száma
 - A legfejlettebb érzékelők a jelfeldolgozást ASIC áramkörökkel vagy mikroprocesszor alkalmazásával végzik el.

BME Hálózati Rendszerek és Szolgáltatások Tanszék 129

Az intelligens mozgásérzékelők nemcsak a piroszenzor által észlelt jel szintjét figyelik, hanem a jel amplitúdóját, szélességét, csúcsszintjét, felfutási idejét, energiáját, formáját, valamint az egymást követő jelek időkülönbségét is. Minden jelet összevetnek a memóriájukban sablonszerűen tárolt „mozgás” és „nem mozgás” jelmintákkal és ennek alapján döntenek el, hogy riasztási jelzést generálnak, vagy a jelzést tévesnek minősítik.



Riasztó berendezések – egyéb érzékelők

- Felületvédelem: az épület határoló felületeinek (ajtók, ablakok, falazat, tetőszerkezet) védelme
 - Nyitásérzékelők
 - Üvegtörés érzékelők
 - Falbontás érzékelők
 - Infrarompók
- Tárgyvédelem: nagyobb értékű eszközök vagy ezeket tartalmazó objektumok (páncélszekrény) védelme
 - Közelítésérzékelők
 - Testhang érzékelők
 - Elmozdítás érzékelők
 - Súlykapcsolók
- Személyvédelmi eszközök: veszélybe került emberek számára veszély jelzési lehetőség
 - Támadásjelzők (pánikkapcsoló)
 - Dőlésjelzők
 - Éberségjelzők

BME Hálózati Rendszerek és Szolgáltatások Tanszék 130

A dőlésjelzőt alapvetően védelmi feladatokat ellátó személyek, például börtönőrök, biztonsági őrök számára fejlesztették ki, mely esetleges megtámadásuk esetén az illető személy eldőlését képes jelezni. A **dőlésjelző** nem más, mint egy **gravitációs kapcsoló**, ami akkor hoz létre riasztást, ha a dőlésjelzőt viselő személy helyzete a függőleges alaphelyzettől valamilyen meghatározott szögben eltér. A dőlésjelző kiegészül egy rádióadóval is. Ennek segítségével lehet támadásjelzést küldeni az őrparancsnok vagy a szolgálatvezető felé.

Az **éberségjelzőt** kettős funkcióra fejlesztették ki: egyrészt ellenőrző, másrészt védelmi feladatot lát el. Egyrészt ellenőrzi a biztonsági őr, portás, diszpécser, stb. ébrenlétét, másrészt megvédi a támadásoktól esetleges elalvásának ideje alatt. Az éberségjelző működési elve egyszerű: az eszköz véletlenszerű időközönként egy fényjelzést produkál, melyet meghatározott módon kell nyugtázni. Ha ez nem történik meg, hangjelzéssel jelzi az elalvást. Ha ennek hatására sem érkezik nyugtázás, akkor riasztást küld a felügyeleti állomás felé, hiszen ebben az esetben megnő a valószínűsége annak, hogy az egyént támadás érte.



Riasztó berendezések – hang és fényjelzők

- Kültéri sziréna
 - Elemei:
 - nyomókamrás hangszóró
 - vezérlő elektronika
 - fényjelző
 - akkumulátor
 - szabotázs kapcsolók
 - a mechanikai védelmet biztosító burkolat
 - Környezeti hatásokkal szembeni ellenálló képesség (hőmérséklet, korrózió)
 - IP-védelem
 - Szabotázs védelem

BME Hálózati Rendszerek és Szolgáltatások Tanszék 131

IP védelem: Minden kültéri szirénára jellemző, hogy a gyártók meghatározzák a szilárd tárgyakkal és a vízzel szembeni védettségük mértékét. Ez az ún. IP védettségi fokozat, amely az IP jelölésből (Ingression Protection) és két számjegyből áll. Az első számjegyből, amelynek értéke 0-tól 6-ig terjedhet, az eszközök szilárd testek elleni védelméről kaphatunk információt. Ez takarhat védelem nélkülséget, az 1mm-től 50mm átmérőjű tárgyak behatolása elleni, valamint a por elleni különböző védelmi fokozatot. A második számjegy a folyadékok elleni védelem mértékét jelöli 0-tól 8-ig, ami szintén a védelem nélkülségtől indulva a csepegő, freccsenő víz hatásán keresztül a vízbemerítésig, és a tartós víz alatti működésig jelöli az adott sziréna védelmi szintjét. A legtöbb kültéri sziréna legalább IP34-es védettséggel rendelkezik. Ez 2,5 mm átmérőjű testek (pl. szerszámok) burkolat alá történő behatolása, valamint freccsenő víz elleni védettséget jelent.

A kültéri szirénákra vonatkozó szabvány előírása szerint a kültéri szirénáknak kettős házzal kell rendelkezniük. A külső ház általában műanyagból, a belső ház pedig acéllemezről vagy annak szilárdságával megegyező egyéb anyagból készül, de olyan típusok is vannak, amelyeknél mindkét ház fémből van. Azonban mindegyik esetben el kell érniük együttesen az 1,5 mm vastagságú acéllemez

szilárdságát. Mindkét háznak máshogy helyezkedik el a lamellázása, ezáltal a purhabbal való kifújással történő szabotálás elméletileg kivédhető. A fejlettebb eszközök rendelkeznek kifejezetten habkifújás és fúrásvédelemmel, illetve egyes különleges típusok már a sziréna burkolatának 10-15 cm-es megközelítésekor is képesek szabotázsjelzést kiváltani. A riasztóhoz csatlakozó vezetékeket, belső alkatrészeket úgy kell elhelyezni, hogy azok ne legyenek láthatóak és hozzáférhetőek. Komoly szakmai hibának tekintjük, ha a szirénát és a riasztóközpontot összekötő vezeték látható módon van felszerelve.



Riasztó berendezések – hang és fényjelzők

- Vezeték nélküli kültéri sziréna
 - A nagy energia igénye miatt eleinte csak a kommunikáció volt vezetékes, az utóbbi években jelentek meg az elemes, teljesen vezetékes nélküli megoldások
- Beltéri sziréna
 - A betörőre hatnak (ellenben a kültéri szirénára, ami a külvilágra)
 - Kisebbség az elvárások a kültéri szirénákhoz képest (környezeti hatások)
 - Nincs IP védelem
 - Általában nincs fényjelzés
 - Műanyag burkolat



BME Hálózati Rendszerek és Szolgáltatások Tanszék 132



Riasztó berendezések – vezeték nélküli megoldások

- Előnyei:
 - Egyszerűen és gyorsan telepíthető
 - Nem igényel vésést, kábelezést (utólagos beépítésnél jelentős szempont)
- Hátrányai:
 - Drágább
 - Elemek, akkumulátorok cseréje, töltése több karbantartást igényel
 - A rádiós közegből eredő problémák (zaj, interferencia)



Riasztó berendezések – vezeték nélküli megoldások

- Hibrid riasztó
 - Vezetékes riasztóközpont rádiós bővítő modullal
 - Vegyesen vannak vezetékes és vezeték nélküli zónák
 - Utólagos bővítésnél vagy nagy távolságoknál lehet előnyös
 - Bizonyos elemek csak vezetékesen kapcsolódhatnak a rendszerhez (kezelőegység, sziréna)



BME Hálózati Rendszerek és Szolgáltatások Tanszék 134



Riasztó berendezések – vezeték nélküli megoldások

- 20-50 méteres beltéri hatótáv (1-2 km nyílt terepen)
- Téves jelzéseket kiszűrő, zavarérzékeny, megbízható működés
- Életjelet küld a rendszer központja felé
- 3-5 éves akku élettartam
- Jelzi a telepek lemerülését
- A régebbi rendszerek 433 MHz-en működtek, a modernebb eszközök már 868 MHz-en

BME Hálózati Rendszerek és Szolgáltatások Tanszék 135

Néhány évvel ezelőtt a vezeték nélküli rendszerek működési frekvenciatartománya általában a 433 MHz-es sáv volt, és problémát jelentett, hogy ugyanezt a frekvenciát használja számos más rádiós eszköz, például a vezeték nélküli kapucsengők, az autóriasztók, az automata kapuk távirányítói, valamint a gyermekőrzők. Eleinte a kódvariációk is igen csekélyek voltak, mindössze 256 variációból álltak. A sok téves riasztás kiküszöbölése érdekében egyre több gyártó tért át a 868 MHz-es frekvenciájú eszközök alkalmazására. Ma már a rádiós jelátvitel kódolt, a kódvariációk elérik a több milliós nagyságrendet, melyek az ugrókódos algoritmusoknak köszönhetően sokkal jobban ellenállnak a külső zavarforrásoknak. Emellett az is említésre méltó, hogy a frekvenciatartomány növekedésével csökkent az eszközök mérete is, hiszen a magasabb frekvencia miatt sokkal kisebb méretű antenna akár a készülék belsejében is elhelyezkedhet.



Riasztó berendezések - kommunikátor

- Riasztási esemény és állapotjelentés küldése távoli rendszereknek
- Távoli programozás, élesítés
- Fajtai:
 - PSTN:
 - DTMF vezérlés
 - Modemes elérés
 - GSM
 - IP

BME Hálózati Rendszerek és Szolgáltatások Tanszék 136

<http://www.riasztorendszerbolt.hu/behatozasjelzok-biztonsagi-rendszerek-lakas-riasztok-riasztorendszerek/riasztorendszer-kozpontok-kiegeszitok-erzekelok-hangjelzok/gsm-gprs-ip-kommunikatorok-pstn-vonalpotlok-riasztorendszerekhez>



Gépjármű felügyelet

- Riasztó berendezések:
 - Nyitásérzékelő
 - Mozcásérzékelő
- Nyomkövető rendszerek:
 - Műholdas helymeghatározás
 - Mobil adatkapcsolaton keresztüli pozíció jelentés
- Online fedélzeti rendszerek:
 - Szoftver frissítések
 - Szerviz információk kicserélése a gyártóval



Nyomkövető rendszerek

- Lopás elleni védelem:
 - Aktuális pozíció jelentése mobil adatkapcsolaton keresztül
 - Zavaró eszközökkel blokkolható a működése!
 - A mobil adatforgalom folyamatos költséggel jár
- Flottakövetés:
 - Céges autóflotta felügyelete
 - Megtervezett útvonalról való letérés jelzése a központ felé
 - Üzemanyag szint folyamatos ellenőrzés és jelentése (a visszaélések kiküszöbölésére)
- Az adatforgalom mennyisége elég alacsony (a GPS koordináták néhány byte-on elküldhetők)
- Gondoskodni kell szükség esetén a külföldi adatroamingról is.

Car2car kommunikáció



Tartalom

- Célok
- V2V
- V2I
- ITS
 - DSRC
 - CALM
- Mobile ad hoc network
- IEEE 802.11p
- IEEE 1608
- SAE J2735
- Alkalmazási területek
 - Biztonság
 - Forgalom menedzsment
 - Vezetés támogató rendszerek
 - Rendőri támogató funkciók
 - Útdíj fizetési megoldások
 - Útvonal optimalizálás
 - Reklámok
 - Információs rendszerek
 - Önjáró autók



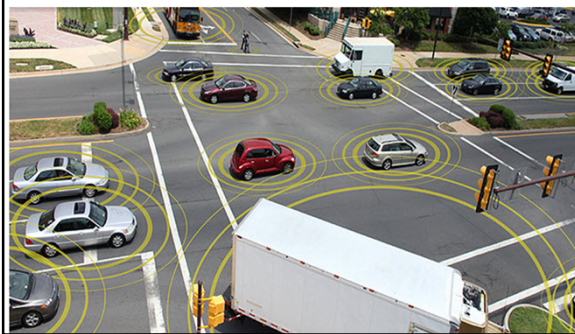
Célok

- Közúti közlekedés biztonságának növelése
- A baleseti károk költségeinek csökkentése
- 1.2M halálos közlekedési baleset évente és 50M sérülés (WHO)
- 300 milliárd dollár káresemény évente (American Automobile Association), a cél ennek a csökkentése
- A közlekedési balesetek közel fele kereszteződésekben történik, ezek jelentősen csökkenthetők lennének egy helyi figyelmeztető rendszer segítségével
- A sebességhatárok betartatási egyszerűbb lenne



Célok

- IEEE 802.11p (WAVE) protokoll használata a környező autókkal történő kommunikáció során
- Veszély, forgalmi és egyéb adatok kicserélése
- Összehangolt navigáció



BME Hálózati Rendszerek és Szolgáltatások Tanszék 142



V2V és V2I

- V2V (Vehicle to Vehicle): járművek közötti ad hoc kommunikáció
- V2I (Vehicle to Infrastructure): útmenti telepített eszközzel történő kommunikáció (jelzőlámpa, útdíj kapu, útkarbantartást jelző berendezés).
- Jelenleg kísérleti projektek zajlanak a technológia tesztelésére
- V2I feladatok:
 - Piros lámpán történő áthaladás észlelése
 - Sebesség túllépés észlelése
 - Stop táblánál történő megállás észlelése
 - Időjárás figyelmeztetés (szél, lefagyás, stb)
 - Vasúti fénysorompó tilos jelzés figyelmeztetés
 - Túlméretes jármű figyelmeztetés



V2V

- V2V megvalósítandó feladatok:
 - Megkülönböztető jelzésű járművek jelzése
 - Útkarbantartások jelzése
 - Gyalogos forgalom sűrűségének jelzése
 - Jelzőlámpák időzítésének jelzése
 - Vészjelzés: 37 típust definiáltak

BME Hálózati Rendszerek és Szolgáltatások Tanszék 144

<http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf>



V2V vészjelzés típusok

- Vehicle Failure
- Control Loss with Prior Vehicle Action
- Control Loss without Prior Vehicle Action
- Running Red Light
- Running Stop Sign
- Road Edge Departure with Prior Vehicle Maneuver
- Road Edge Departure without Prior Vehicle Maneuver
- Road Edge Departure While Backing Up
- Animal Crash with Prior Vehicle Maneuver
- Animal Crash without Prior Vehicle Maneuver
- Pedestrian Crash with Prior Vehicle Maneuver
- Pedestrian Crash without Prior Vehicle Maneuver
- Pedalcyclist Crash with Prior Vehicle Maneuver
- Pedalcyclist Crash without Prior Vehicle Maneuver
- Backing Up into Another Vehicle
- Vehicle(s) Turning – Same Direction
- Vehicle(s) Not Making a Maneuver – Opposite Direction
- Following Vehicle Making a Maneuver
- Lead Vehicle Accelerating
- Lead Vehicle Moving at Lower Constant Speed
- Lead Vehicle Decelerating
- Lead Vehicle Stopped
- Left Turn Across Path from Opposite Directions at Signalized Junctions
- Vehicle Turning Right at Signalized Junctions
- Left Turn Across Path from Opposite Directions at Non-Signalized Junctions
- Straight Crossing Paths at Non-Signalized Junctions
- Vehicle(s) Turning at Non-Signalized Junctions
- Vehicle(s) Parking – Same Direction
- Vehicle(s) Changing Lanes – Same Direction
- Vehicle(s) Drifting – Same Direction
- Vehicle(s) Making a Maneuver – Opposite Direction
- Evasive Action with Prior Vehicle Maneuver
- Evasive Action without Prior Vehicle Maneuver
- Non-Collision Incident
- Object Crash with Prior Vehicle Maneuver
- Object Crash without Prior Vehicle Maneuver
- Other

BME Hálózati Rendszerek és Szolgáltatások Tanszék 145



V2V szituációk

Scenario and warning type	Scenario example
Rear end collision scenarios	
Forward collision warning Approaching a vehicle that is decelerating or stopped.	
Emergency electronic brake light warning Approaching a vehicle stopped in roadway but not visible due to obstructions.	
Lane change scenarios	
Blind spot warning Beginning lane departure that could encroach on the travel lane of another vehicle traveling in the same direction; can detect vehicles not yet in blind spot.	
Do not pass warning Encroaching onto the travel lane of another vehicle traveling in opposite direction; can detect moving vehicles not yet in blind spot.	
Intersection scenario	
Blind intersection warning Encroaching onto the travel lane of another vehicle with whom driver is crossing paths at a blind intersection or an intersection without a traffic signal.	

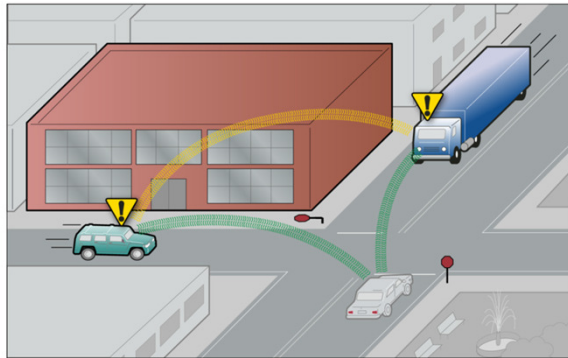
BME Hálózati Rendszerek és Szolgáltatások Tanszék 146

Frontális ütközésre figyelmeztetés: az előttünk lévő (vagy a sorban előrébb) a hirtelen fékezésről veszjelzést küld a környezetének.
A kommunikáció hatótávolsága 300 méter körül alakul.



V2V szituációk

- Kereszteződés áthajtás: STOP táblás kereszteződésnél figyelmezteti a vezetőt, ha jármű közeledik



Source: GAO.

BME Hálózati Rendszerek és Szolgáltatások Tanszék 147

A képen a STOP tábla kidőlt, ennek veszélyére figyelmeztetik egymást az autók.



V2V szituációk

- Balra kanyarodás: figyelmezteti a vezetőt, ha szemből érkezik egy gépjármű és ezért a balra kanyarodás ütközéssel járna
- Elektronikus féklámpa jelzés: egy nem közvetlenül előttünk lévő jármű hirtelen fékezéséről kapunk tájékoztatást. Rossz időjárás esetén lehet nagy jelentősége.



V2V szituációk

- Szenzorokra épülő szituációk: meglévő szenzoros rendszerek adatainak továbbítása más járművek számára:
 - FCW (Forward Collision Warning – Frontális ütközés Figyelmeztetés): Radaros és kamerás megoldással próbálja az előttünk álló autót/tárgyakat felismerni és figyelmeztetni. Ha ezt V2V kommunikációban egymás között meg tudják osztani az autók, akkor előbb értesülnek az esetről.
 - Holttér figyelés és sávváltás figyelmeztetés: sávváltáskor figyelmeztetést kapuk, ha a gépjármű holtterében egy másik gépjármű található vagy közeledik oda.



V2V üzenetek

- Basic safety message (BSM): egységesített formátum (SAE J2735), hogy mindenki el tudja olvasni. Tartalmazza többek között a gépjármű helyzetét, gyorsulását.
- Certificate exchange messages: PKI az üzenetek azonosítására. Lehetőség van aláírt és titkosított üzenetek küldésére is.

BME Hálózati Rendszerek és Szolgáltatások Tanszék 150

PKI: Public Key Infrastructure



V2V BSM formátum

- Kötelező elemek:
 - Position (Latitude, Longitude, Elevation, Positional accuracy)
 - Motion (Transmission state, Speed, Steering wheel angle, Heading (irány), Longitudinal acceleration, Vertical acceleration, Lateral acceleration, Yaw rate (farolás mértéke), Brake applied status, Traction control state, Stability control status, Auxiliary brake status, Brake status not available, Antilock brake status, Brake boost applied)
 - Vehicle size (Vehicle width, Vehicle length)



V2V BSM formátum

- Opcionális elemek:
 - Vehicle safety extension: flag-eket tartalmazhat, pl: viszvillogók bekapcsolva, ABS aktiválva, defekt, stb.
 - Path history
 - Transmission and speed
 - Path Prediction (Radius of curve, Confidence)
 - RTCM Package: GPS üzenetek szabványos formátuma, differenciális szolgáltatás támogatással
 - Full position vector
 - RTCM header

BME Hálózati Rendszerek és Szolgáltatások Tanszék 152

RTCM: Radio Technical Commission for Maritime Services

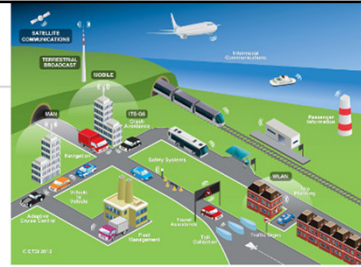


V2I

- Szereplők:
 - Vehicle On-Board Unit/Equipment (OBU vagy OBE)
 - Roadside Unit/Equipment (RSU vagy RSE)
 - Biztonságos kommunikációs csatorna
- Alkalmazási területek:
 - Biztonság
 - Hatékonyság növelése: torlódások jelzése, dinamikus forgalomirányítás, navigáció
 - Fizetés és információ: parkolás, behajtási díjak, autópálya díjfizetés

BME Hálózati Rendszerek és Szolgáltatások Tanszék 153

V2I: Vehicle to Infrastructure.



- Intelligent transportation systems
(Intelligens közlekedési rendszerek)
- Gyűjtő csoport, minden olyan rendszer ide tartozik, amelyben információs és kommunikációs technológiákat alkalmaznak a közúti közlekedés területén
- Az Európai Unió 2010-es irányelve (2010/40/EU) az ITS rendszerek közúti közlekedésben történő kiépítését határozza meg

2010/40/EU irányelv: <http://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32010L0040>



ITS kiemelt területei

- közúti, forgalmi és utazási adatok optimális felhasználása
- forgalom- és teherszállítási irányítási ITS-szolgáltatások folyamatossága
- közúti közlekedésbiztonsággal és óvintézkedésekkel kapcsolatos ITS-alkalmazások
- jármű összekapcsolása a közlekedési infrastruktúrával



- Vezeték nélküli kommunikáció
 - DSRC (Dedicated Short-Range Communications): egy vagy kétirányú, kis és közepes hatótávolságú kommunikációs csatornák, kifejezetten autóiipari célokra kialakítva
 - CALM (Continuous Air interface Long and Medium range).
Jellemzői:
 - Folyamatos kommunikáció három módon:
 - Gépjármű – gépjármű
 - Gépjármű – infrastruktúra
 - Infrastruktúra – infrastruktúra
 - Interoperabilitás és észrevétlen handover képesség
 - IP forgalomból csak IPv6 támogatott, de támogatott a nem-IP forgalom (pl. ütközés detektáló rendszereknél)
 - Platform független, több rádiós protokoll támogatása

Az alap CALM rendszer architektúrára (ISO 27217) 10 különböző hálózati protokollt támogat.



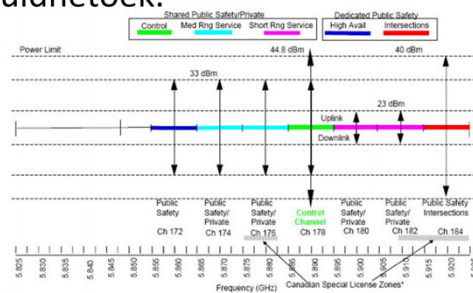
DSRC

- 1999-ben az FCC 75 MHz-es tartományt allokalált az 5.9GHz-es tartományban, kizárólagosan a vehicle to vehicle és vehicle to infrastructure kommunikáció számára
- Az IEEE 802.11p szabványosításnál ennek a tartománynak a használatát tűzték ki célul.
- Régióként eltérő, hogy milyen sávok használhatóak



DSRC – USA spektrum

- A DSRC spektrumot hét 10 MHz-es blokkra osztották
- A 178-as csatorna a vezérlő csatorna (control channel – CCH), ezen csak biztonsági üzenetek (safty communication) küldhetők.
- 182 és 184-es csatornák fenntartottak, a többi az un. Service channel (SCH)

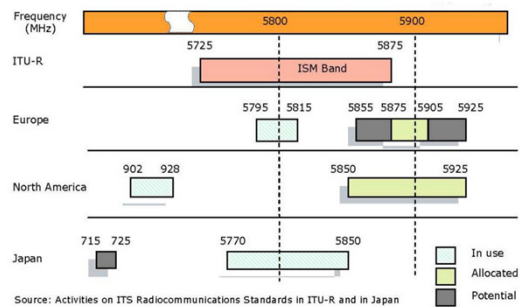


BME Hálózati Rendszerek és Szolgáltatások Tanszék 158



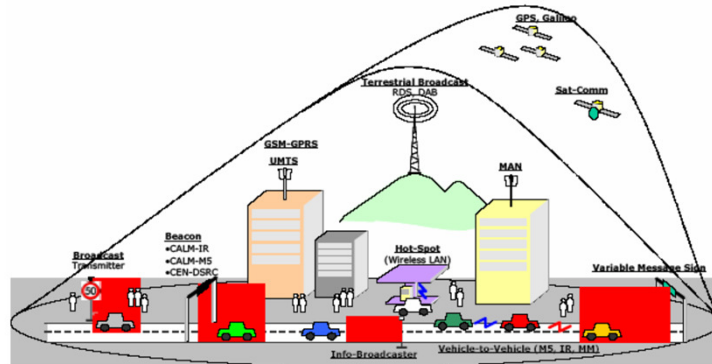
DSRC – EU spektrum

- 2008-ban az Európai Bizottság EU szinten egységes frekvencia blokkokat jelölt ki.
- 30 MHz-es spektrumot jelöltek ki az 5.9MHz-es tartományban
- A sávok nem teljesen egyeznek az FCC által kijelöltekkel, de azonos rádiós eszköz használható.





CALM környezet





CALM air interface protokollok

- 2G mobil rendszerek (GSM/GPRS)
- 3G mobil rendszerek (IMT-2000, W-CDMA, CDMA, EVDO)
- Infa
- Wireless LAN (802.11)
- Milliméteres hullám rendszerek (pl. radar)
- DSRC
- Wireless WAN (WiMax)
- Broadcast jelek (Digital Audio Broadcasting – DAB, GPS)
- PAN (Personal Area Networking) (pl. UWB, Bluetooth)

BME Hálózati Rendszerek és Szolgáltatások Tanszék 161

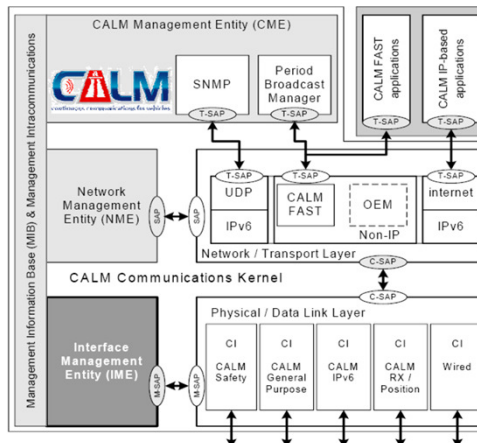
Millimeter wave: https://hu.wikipedia.org/wiki/Millim%C3%A9teres_hull%C3%A1m

UWB: <https://en.wikipedia.org/wiki/Ultra-wideband>



CALM jelen - jövő

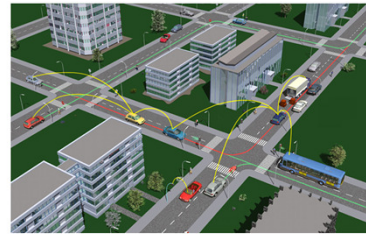
- Sok támogatott protokoll miatt komplex management stack
- Bevezetése bonyolult, csak bizonyos részeit tervezik implementálni
- A 2007-es szabványosítás óta nem terjedt el széles körben a mai napig sem.





Mobile Ad Hoc Network (MANET)

- Car 2 car kommunikációnál gyakori szituáció, hogy nincs a közelben egy telepített infrastruktúra sem, csak néhány autó
- Mobil ad hoc hálózatokban folyamatosan változik a hálózat összetétele, létszámának száma
- A csomópontok a kapott üzeneteket megismételhetik, hogy az további autóhoz is eljuthasson, növelve ezzel a hatótávolságot.



BME Hálózati Rendszerek és Szolgáltatások Tanszék 163

A mobil ad hoc hálózatok topológiája folyamatos változásban van, az egyik csomópont nem ugyanazokat az csomópontokat látja. Hogy a hatótávolságot növeljék, ezért a csomópontok üzenet ismétlőként is funkcionálnak egy megadott TTL értékig, ezzel növelve a hatótávolságot.



Mobile Ad Hoc Network (MANET)

- Forgalom típusok:
 - Peer to Peer: Két, egymást közvetlenül elérő eszköz között
 - Remote to Remote: a két eszköz közvetlenül nem látja egymást, csak közvetítőn keresztül tudnak kommunikálni, de a kapcsolat tartós, állandó útonalú (pl. egy kocsisor elején és végén lévő autók, akik egy irányba haladnak)
 - Dinamikus: Az eszközök eltérő úton mozognak, az útvonalat mindig újra fel kell építeni, csak rövid ideig él a kapcsolat



MANET Különleges tulajdonságok

- Autonóm terminál: az eszközök állomásként és routerként is működnek
- Elosztott működés: mivel nincs központi infrastruktúra, ezért a vezérlés és az irányítás elosztott. A csomópontok együttműködnek egymással, képesek ellátni biztonsági és átjáró funkciót is.
- Dinamikus hálózati topológia: A topológia gyorsan és kiszámíthatatlanul változik
- Multi-hop routing: A csomagokat 1 vagy több köztes csomóponton keresztül is továbbításra kerülnek a célállomáshoz
- Sáv szélesség korlátozott, ingadozó kapacitás mennyiség: a csatorna zajos, interferencia és fading léphet fel. Sok résztvevő esetén pedig az ütközés esélye is megnövekszik.
- Energia és számítási kapacitás korlát: A legtöbb esetben a mobil eszközök végzik a kommunikációt, kis memória és számítási kapacitással. Optimalizált algoritmusokra van szükség az erőforrások jó kihasználásához.
- Csökkentett biztonság: a vezeték nélküli kommunikáció több veszély forrást rejt magában, pl. lehallgatás, megszemélyesítéses támadás, túlterheléses támadás



MANET routing

- IP routing nem használható: folyamatosan változik a helyzete, a hálózati összetétele, az elérhető szomszédok
- Mobil IP protokoll sem megoldás: nincs egy központi infrastruktúra, ami nyilvántartaná, hogy melyik eszköz hol van, hogy érhető el
- Multicast routing: nem feltétlenül lesz minden célcím 1 hop távolságra, ez bonyolítja a kommunikációt
- AODV (Ad-Hoc On-Demand Distance Vector routing protocol)
- OLSR (Optimized Link State routing)
- ZRP (Zone Routing Protocol)

BME Hálózati Rendszerek és Szolgáltatások Tanszék 166

AODV: reaktív protokoll (RFC 3561)

OSLR: *proaktív protokoll* (RFC3626)

ZRP: http://www.olsr.org/docs/report_html/node18.html



IEEE 802.11p

- Wireless Access in Vehicular Environments (WAVE)
- DSRC frekvencia sávokat használja (5.9 GHz)
- EU és USA frekvenciát nem egyeznek (de van átfedés), azonos eszközök használhatóak, csak konfigurációs különbség lesz az engedélyezett csatornák terén.
- 802.11 szabvány kiterjesztése
MAC és fizikai réteg
specifikációval



BME Hálózati Rendszerek és Szolgáltatások Tanszék 167



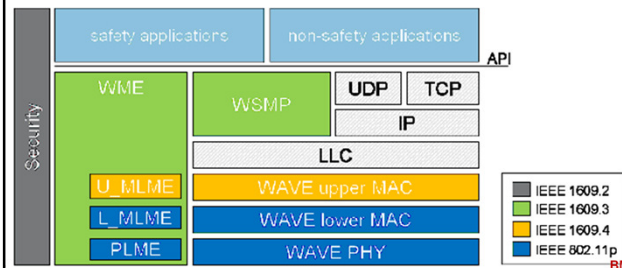
IEEE 802.11p

- On-board unit (OBU): gépjármű fedélzeti eszköz
- Roadside unit (RSU): WiFi access pointként viselkednek
- Public Safety OBU (PSOBU): olyan gépjárműn lévő eszköz, ami hasonló szolgáltatást tud nyújtani, mint egy RSU (rendőr, tűzoltó, mentők alkalmaznák a jövőben)
- Csatorna: több csatorna áll rendelkezésre, (országonként eltérhetnek). Két részre osztja a szabvány:
 - Control channel: broadcast kommunikáció és más csatornák forgalmának vezérlése
 - Service channel
- Nincs felcsatlakozás (association), mint a hagyományos 802.11-es megoldásoknál, az RSU beacon üzenetei segítségével történik a kommunikáció
- A szabvány jelenleg draft stádiumban van



IEEE 1609

- IEEE 1609 szabványcsalád foglalkozik V2V protokoll fel management és a biztonsági kérdéseivel:
 - IEEE 1609.1: erőforrás kezelés
 - IEEE 1609.2: biztonsági szolgáltatások
 - IEEE 1609.3: hálózati szolgáltatások
 - IEEE 1609.4: több csatornás kommunikáció



BME Hálózati Rendszerek és Szolgáltatások Tanszék 169



SAE J2735

- V2V üzeneteket (Message Set Dictionary) a SAE szervezet definiálta
- Egy V2V üzenet DF-ek és DE-ek halmaza
- 15 üzenet típus
- 72 DF
- 146 DE
- 11 Külső DE

BME Hálózati Rendszerek és Szolgáltatások Tanszék 170

SAE: Society of Automotive Engineers www.sae.org

DF (Data Frame) : üzenet mezők csoportja, pl. ablaktörlő

DE (Data Element): üzenet mező pl. első ablaktörlő



Alkalmazási területek - biztonság

- Kereszteződés figyelmeztetés: másik közeledő autóra figyelmeztetés, fejlettebb rendszerben akár az elsőbbség eldöntését is végezheti V2V rendszer
- Figyelmeztetés autópályára felhajtáskor
- Akadály felismerés: úton álló autó, idegen tárgy
- Figyelmeztetés hirtelen megállás esetén
- Balesetek jelentése
- Sáv váltáskor figyelmeztetés ha a sáv foglalt vagy hamarosan azzá válik



Alkalmazási területek – forgalom szabályozás

- A forgalom optimalizálását szolgálják:
- Változtatható sebességkorlátok
- Adaptív jelzőlámpák: forgalom függvényében változó programok
- Kereszteződés vezérlés: a V2V rendszerek egymás között egyeztetik, hogy melyik gépjármű haladhat át előbb
- Mentők, tűzoltók gyorsabb, hatékonyabb értesítése



Alkalmazási területek – vezető támogató rendszerek

- Út menti tárgyak, eszközök információt sugározhatnak az arra közlekedő járműveknek:
 - Parkolás: szabad parkolóhelyek mutatása
 - Tempomat: ha a sebességkorlátozást (pl. útfelújításnál) észleli a jármű, akkor a tempomatot automatikusan az új sebességhatárra tudja állítani
 - Sávtartás asszisztens
 - Útmenti tábla felismerés: a táblába épített V2I berendezés sugározza a tábla adatait.



Alkalmazási területek – szabállysértések felügyelete

- Megfigyelés: 802.11p control csatornán keresztül lehetőség van video streaming-re is, de a opott autók keresése is hatékonyabb lehet.
- Sebességhatár figyelmeztetés
- Sebesség lekérdezése (rendőr lekérdezi az elhaladó autót)
- Félreállítási parancs küldése
- Piroslámpás áthaladás jelzése

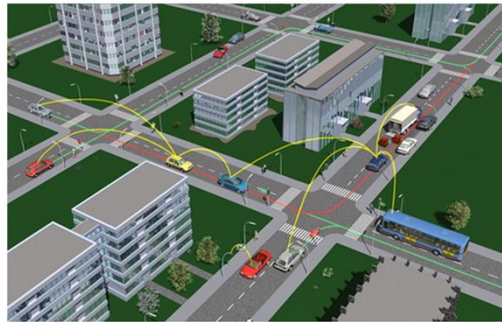
BME Hálózati Rendszerek és Szolgáltatások Tanszék 174

Live video streaming in IEEE 802.11p vehicular networks:
http://www2.hh.se/staff/magnusj/papers/2014_INFOCOM.pdf



CAR 2 CAR Communication Consortium

- Autógyártók, alkatrészgyártók és fejlesztő cégek alkotják
- Céljai:
 - Nyílt szabvány kifejlesztése az kooperatív ITS rendszerekre
 - Validálási eljárás a V2V rendszerekhez
 - Üzleti modell a piaci bevezetésre és annak ütemezése



BME Hálózati Rendszerek és Szolgáltatások Tanszék 175

Autógyártók: Audi, BMW, Daimler, Ford, Honda, Hyunday, Jaguar, Man, Opel, PSA, Renault, VW, Volvo, Yamaha



National Highway Traffic Safety Administration (USA)

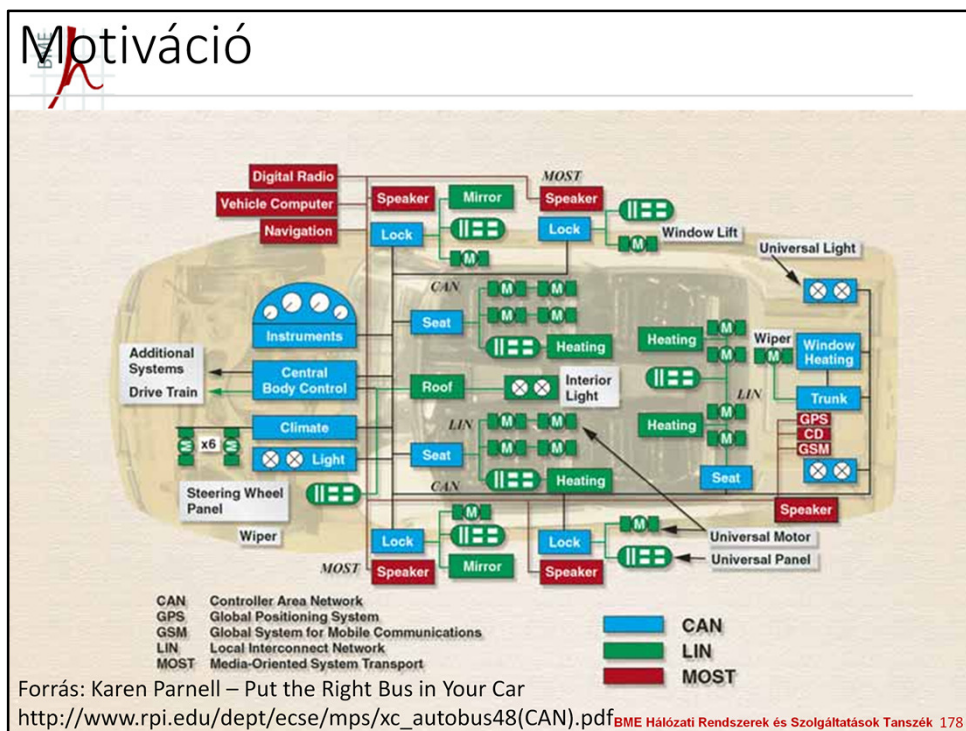
- Céljuk a közutak biztonságának növelése
- A V2V kommunikációs technológiától jelentős javulást remélnek
- Safetypilot néven indítottak egy projektet, 2800 autóval a V2V technológia élesben történő tesztelésére.
- A szervezet célkitűzése, hogy néhány éven belül az új gépjárművekbe kötelezően kerüljenek V2V eszközök.

BME Hálózati Rendszerek és Szolgáltatások Tanszék 176

<http://www.safercar.gov/v2v/index.html>

Jármű fedélzeti kommunikáció

Motiváció





OBD – On-board diagnostics

- Az Egyesült Államokban indult kezdeményezés, a károsanyag-kibocsátást ellenőrző fedélzeti rendszerek hibáinak ellenőrzését írták elő.
- Az OBD első változata, az OBD I az Egyesült Államokban 1988-tól kötelező.
- Hiba esetén a műszerfalon elhelyezett lámpa figyelmezteti a jármű vezetőjét a hibára. Közúti ellenőrzésnél a hatóság is ellenőrizhette.
 - MIL (Malfunction Indicator Light) vagy Check Engine
- A hibakódot (gyártótól függő) vagy a MIL villogja el, vagy diagnosztikai műszerrel olvasható ki (nincs szabvány)

Forrás: Dr. Lakatos István – OBD, EOBD (fedélzeti diagnosztika)
http://rs1.sze.hu/~lakatos/OBD_EOBD.pdf

BME Hálózati Rendszerek és Szolgáltatások Tanszék 179



OBD – On-board diagnostics

- OBD II 1996-től hatályos
- A lámpa már nem csak világít, villoghat is, a lámpa üzemmódjai, megjelenése (ISO 2575) szabványosak
 - Villogás – katalizátor veszélyben
 - Világít – kipufogógáz hiba
- A hiba bekövetkeztekor mért paraméterek rögzítése a hibakeresés megkönnyítése érdekében
- Szabványos hibakódok, csak diagnosztikai műszerrel olvasható ki
- Szabványos diagnosztikai csatlakozó
- Szabványosított ellenőrző rendszerek

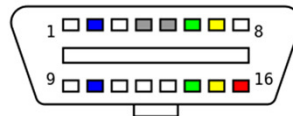
Forrás: Dr. Lakatos István – OBD, EOBD (fedélzeti diagnosztika)
http://rs1.sze.hu/~lakatos/OBD_EOBD.pdf

BME Hálózati Rendszerek és Szolgáltatások Tanszék 180



OBD II csatlakozó – SAE J1962

- 16-pólusú csatlakozó
- Többféle protokollt támogat, legfontosabbak:
 - SAE J1850 PWM
 - SAE J1850 VPW
 - ISO 9142-2
 - ISO 14230
 - ISO 15765 (CAN)



Kép forrása:
http://commons.wikimedia.org/wiki/File:OBD_connector_shape.svg

Forrás: Dr. Lakatos István – OBD, EOBD (fedélzeti diagnosztika)
http://rs1.sze.hu/~lakatos/OBD_EOBD.pdf

BME Hálózati Rendszerek és Szolgáltatások Tanszék 181



CAN (ISO 11898)

- CAN 2.0 – 1991 Robert Bosch GmbH
- A fejlesztés 1983-ban kezdődik, 1993-ban nemzetközi szabvány
- Buszrendszer (általában)
- Autóipari felhasználásra tervezve
- Több master a buszon
- Eseményvezérelt
- Üzenetközpontú (prioritásos üzenetek)
- Garantált késleltetés
- Hiba érzékelés
- CSMA/CD+CR – Carrier Sense Multiple Access, Collision Detection, Collision Resolution



CAN (ISO 11898)

- Sebesség:
 - High speed CAN: 0,125-1 Mb/s
 - Low speed CAN: 10-125 kb/s
- Maximális távolság: 40-500m
 - Adatsebesség és átviteli közeg függvénye
- Rövid keretek



CAN protokoll stack

Alkalmazás réteg

- A CAN nem specifikálja

Object réteg

- Üzenetek szűrése
- Üzenetek és állapotok kezelése

Átviteli (transfer) réteg

- Időzítések
- Busz arbitráció
- Keretszervezés
- Hibavédelem

Fizikai réteg

- Jelszintek és bitábrázolás
- Átviteli közeg

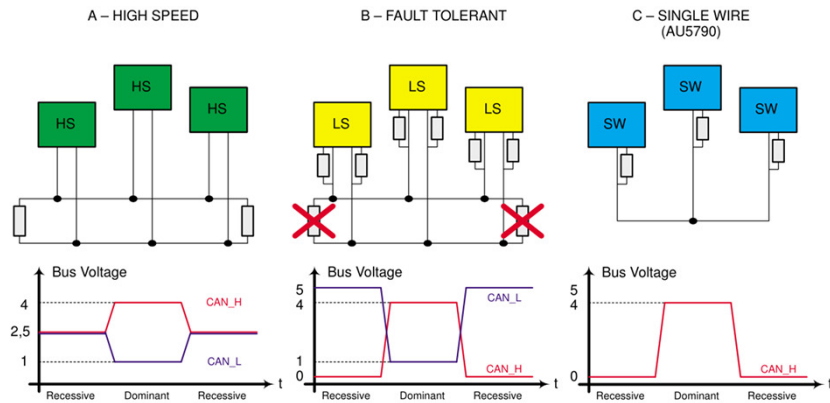


CAN fizikai réteg

- A CAN szabvány nem köti meg a fizikai médium típusát
- A legelterjedtebb megoldás: csavart érpár (ISO11898)
- Maximális bitráta: 1 Mb/s
- Differenciális átvitel
- Az érpár két vezetéke: CAN_H és CAN_L
- A busz végein lezáró ellenállások (120Ω)



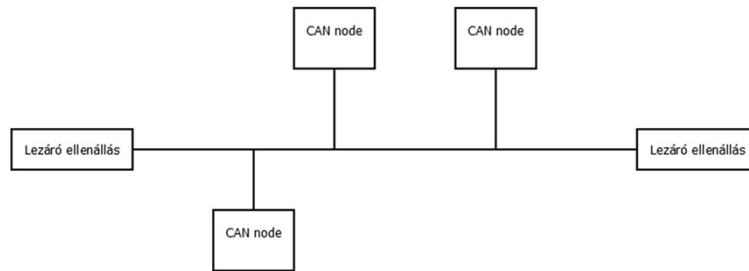
CAN fizikai réteg



Kép forrása: Philips AN2005 AU5790 Single wire CAN transceiver
http://www.nxp.com/documents/application_note/AN2005.pdf

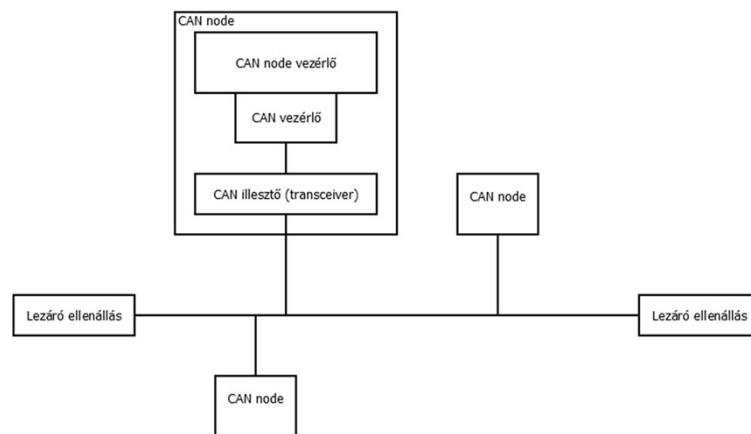


CAN busz fizikai csatlakozás



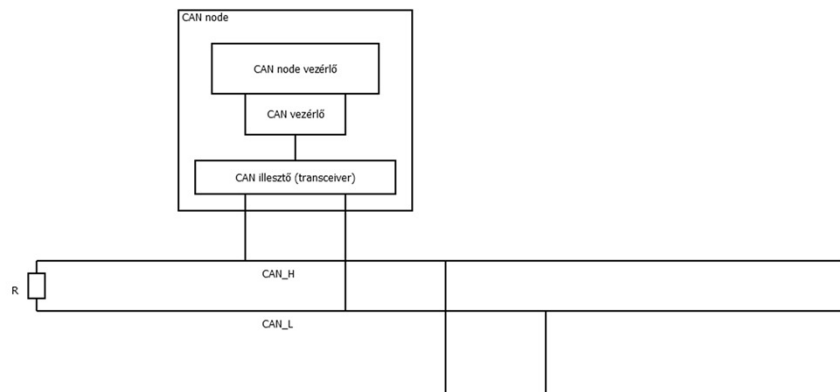


CAN busz fizikai csatlakozás





CAN fizikai csatlakozás

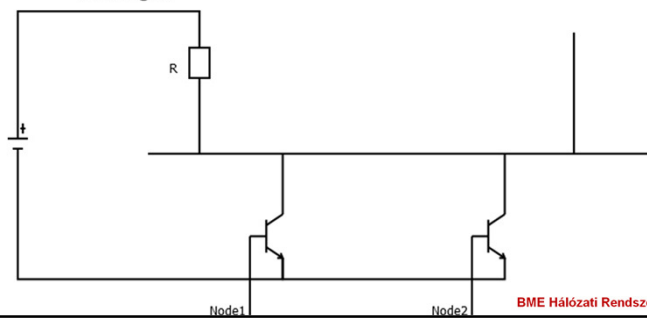




CAN illesztő működése

- A CAN busz logikai ÉS kapuként működik
- Akkor magas az átvitt logikai érték, ha minden csomópont magas értéket kíván a buszra küldeni, vagy nem visz át adatot

Analógia:

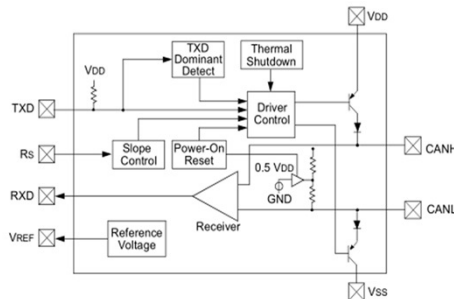


BME Hálózati Rendszerek és Szolgáltatások Tanszék 190



CAN illesztő működése

- A valóságban több, mint egy open collectoros meghajtás
- Példa: Microchip MCP2551 CAN transceiver



Kép forrása: Microchip MCP2551 High-Speed CAN Transceiver Datasheet
<http://ww1.microchip.com/downloads/en/DeviceDoc/21667f.pdf>

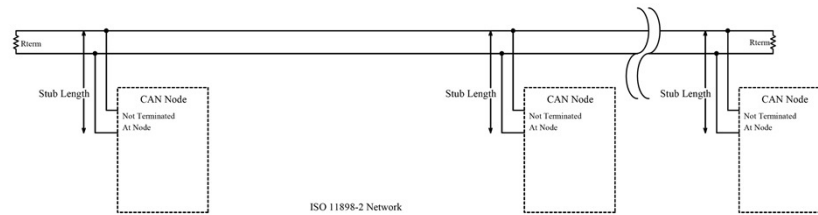
BME Hálózati Rendszerek és Szolgáltatások Tanszék 191



CAN architektúra

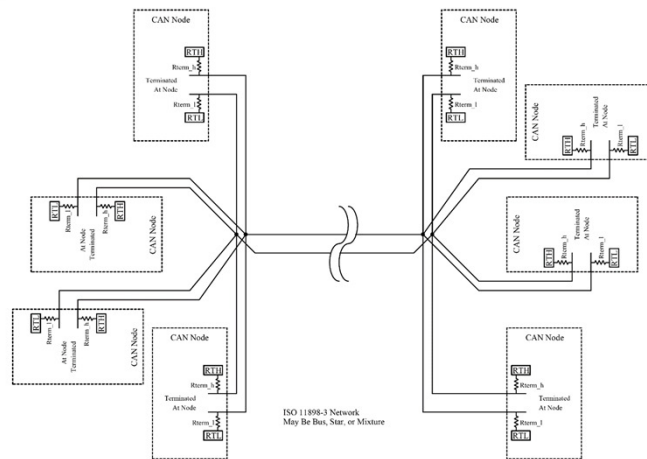
High speed CAN (ISO 11898-2)

- Busz, lezáró ellenállásokkal ($120\ \Omega$)



A kép forrása: EE JRW, Wikimedia Commons
http://en.wikipedia.org/wiki/File:CAN_ISO11898-2_Network.png

Low speed fault-tolerant CAN (ISO 11898-3)



A kép forrása: EE JRW, Wikimedia Commons

http://commons.wikimedia.org/wiki/File:CAN_ISO11898-3_Network.png

BME Hálózati Rendszerek és Szolgáltatások Tanszék 193



High speed CAN jelszintek

- A busz differenciális, a logikai jel a CAN_H és CAN_L vezetékek feszültségkülönbsége
- Ez az interferenciát csökkenti
- A logikai alacsony állapottal reprezentáljuk az 1 bitet
- A logikai alacsony állapot nagyimpedanciájú – recesszív
- A logikai magas állapot kisimpedanciájú – domináns
- Azaz, ha több node egyszerre ad, és legalább egy node 0 bitet (azaz logikai magas jelet) ad le, a buszról olvasható bit a 0 lesz → busz arbitráció alapja



CAN bit reprezentáció

- NRZ – non return to zero kódolás
- A szinkronizáció nehéz – azonos egymást követő bitek esetén ritka jelváltás
- Megoldás: bit stuffing
 - 5 egymást követő azonos bitet követően a CAN beszúr egy ellentétes bitet, amelyet a vevő csomópontok kötelesek figyelmen kívül hagyni
 - Szerepe a szinkronizáció fenntartása
- Válaszidő jittert okoz, tervezéskor foglalkozni kell vele!



CAN busz arbitráció

- Az alap séma CSMA/CA+CR
- A keretek arbitrációs mezője szolgál a közeghozzáférés vezérésére
- Egy állomás akkor kezdhet adni, ha a buszt nem használja senki (CSMA/CA)
- A CAN keret első bitje egy domináns bit (0), minden adni kívánó állomás az először adni kezdő állomás SOF (start of frame) bitjének élére szinkronizál
- Itt is van bit stuffing



CAN busz arbitráció

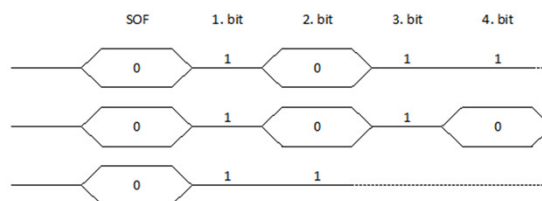
- Ismétlés: ha a buszon legalább egy csomópont domináns jelet (azaz 0 bitet) ad, a buszról a domináns jel olvasható ki
- Bitenkénti arbitráció
- Az busz arbitráció során a csomópontok elkezdik a keret sugárzását, közben figyelik, hogy mi olvasható a buszon. Ha a buszon nem az a jel olvasható, amit egy adott csomópont ad, akkor az a csomópont beszünteti az adást



CAN busz arbitráció – példa

- Tekintsünk három csomópontot, amelyek egy időben a következő három arbitrációs mezőt tartalmazó üzenetet szeretnék küldeni

- 10110101011
- 10100011011
- 11001010111



- Az üzenetet a második állomás tudja elküldeni, a harmadik állomás a második arbitrációs bit után, az első állomás a negyedik arbitrációs bit után állítja le a küldést



CAN üzenetek

- Négy üzenettípus:
 - Data frame – adat
 - Remote frame – adat kérés
 - Error frame – hibajelzés
 - Overload frame – csomópont túlterhelésének jelzése
- Két üzenetformátum
 - Standard formátum
 - 11 arbitrációs bit üzenetazonosítóként
 - Kiterjesztett (extended) formátum
 - 11 + 18 bites üzenetazonosító



CAN keretformátum

	START OF FRAME	ARBITRATION FIELD				CONTROL FIELD				DATA FIELD	CRC FIELD		ACK FIELD	END OF FRAME
Standard format	START 1 bit	IDENTIFIER 11 bit				RTR 1 bit	IDE 1 bit	r0 1 bit	DLC 4 bit	DATA 0..64 bit	CRC 15 bit	CRC DEL 1 bit	ACK 2 bit	EOF IF 10 bit
Extended format	START 1 bit	IDENTIFIER 11 bit	SRR 1 bit	IDE 1 bit	IDENTIFIER 18 bit	RTR 1 bit	r1 1 bit	r0 1 bit	DLC 4 bit	DATA 0..64 bit	CRC 15 bit	CRC DEL 1 bit	ACK 2 bit	EOF IF 10 bit

- Start of frame: domináns bit (0)
- Arbitration field: a busz arbitrációban vesz részt, illetve üzenet azonosítóként szolgál
 - Identifier: üzenet azonosító (egyben prioritás)
 - RTR bit: remote transmit request, remote frame-ekben recesszív
 - SRR bit: recesszív bit, az RTR bitet helyettesíti extended frame-ekben
 - IDE bit: ha a keret standard frame, domináns, ha extended frame, recesszív; az IDE bit offsetje megegyezik a két keretformátumban



CAN keretformátum

	START OF FRAME	ARBITRATION FIELD				CONTROL FIELD				DATA FIELD	CRC FIELD		ACK FIELD	END OF FRAME
Standard format	START 1 bit	IDENTIFIER 11 bit				RTR 1 bit	IDE 1 bit	r0 1 bit	DLC 4 bit	DATA 0..64 bit	CRC 15 bit	CRC DEL 1 bit	ACK 2 bit	EOF IF 10 bit
Extended format	START 1 bit	IDENTIFIER 11 bit	SRR 1 bit	IDE 1 bit	IDENTIFIER 18 bit	RTR 1 bit	r1 1 bit	r0 1 bit	DLC 4 bit	DATA 0..64 bit	CRC 15 bit	CRC DEL 1 bit	ACK 2 bit	EOF IF 10 bit

- Control field:
 - Standard frame-ek esetén itt szerepel az IDE bit
 - r1, r0 fenntartott bitek, dominánsként küldendő, de bármely értéket el kell fogadnia a vevő csomópontoknak
 - DLC: data length code, az adatmezőben lévő adat hosszát adja meg bájtokban, értéke 0..8
- Data field: a küldendő adat



CAN keretformátum

	START OF FRAME	ARBITRATION FIELD					CONTROL FIELD			DATA FIELD	CRC FIELD	ACK FIELD	END OF FRAME	
Standard format	START 1 bit	IDENTIFIER 11 bit				RTR 1 bit	IDE 1 bit	r0 1 bit	DLC 4 bit	DATA 0..64 bit	CRC 15 bit	CRC DEL 1 bit	ACK 2 bit	EOF IF 10 bit
Extended format	START 1 bit	IDENTIFIER 11 bit	SRR 1 bit	IDE 1 bit	IDENTIFIER 18 bit	RTR 1 bit	r1 1 bit	r0 1 bit	DLC 4 bit	DATA 0..64 bit	CRC 15 bit	CRC DEL 1 bit	ACK 2 bit	EOF IF 10 bit

- CRC field:
 - CRC: ellenőrző összeg a start of frame, arbitration, control és data field adataiból
 - $x^{15}+x^{14}+x^{10}+x^8+x^7+x^4+x^3+1$ generátorpolinom
 - CRC DEL: CRC delimiter, mindig recesszív
- ACK field:
 - Két bit: ACK slot és ACK delimiter, ACK slot: azonnali nyugtázás, az adó recesszív bitet ad, a vevő domináns; ACK delimiter mindig recesszív
- End of frame: 7 recesszív bit, 3 bit a minimum IFS



CAN keretformátum

- Hibakeretben (error frame) 6 egymást követő domináns/recesszív bit, majd 8 egymást követő recesszív bit
 - Domináns: error active mód
 - Recesszív: error passive mód
 - Például adás közbeni hiba esetén
 - A 6 egymást követő domináns/recesszív bit normális esetben nem fordulhatna elő (bit stuffing miatt)
- Overload keret: 6 domináns + 8 recesszív bit, maximum 2 küldhető



CAN alkalmazás réteg

- A CAN szabvány nem definiálja
- CiA (CAN in Automation)
 - Szabványosító testület
 - Részt vett a CAN FD (Flexible Data-Rate) protokoll tervezésében is
 - ~8 Mbps sebesség, 64-bites adatmezővel rendelkező CAN
- CANopen
 - Ipari automatizálás
- EnergyBus
 - Elektromos járművek, energiaellátó rendszerek



FlexRay

- Az autóban átvitt adatok köre folyamatosan nő az egyre fejlettebb elektronikus rendszerek miatt
- Megjelent a nagyobb adatátviteli sebesség igénye a CAN-hez hasonló megbízhatósággal
- A gépjárművekben több CAN-busz működik egyidőben



FlexRay

	Maximális sebesség	Költségek	Adatvezetékek
CAN	1 Mb/s	Közepes	2
LIN	40 kb/s	Alacsony	1
FlexRay	10 Mb/s	Magas	2 vagy 4

- Eltérő felhasználási területek

- CAN – blokkolásgátló, váltó, motor diagnosztika
- LIN – ülésállítás, tükörállítás, egyéb kiegészítő kényelmi felszerelések
- FlexRay – új technológiák, drive-by-wire, felfüggesztés, új biztonsági berendezések



FlexRay fizikai réteg

- Busz topológia lezáró ellenállásokkal ($80-110\Omega$)
- Árnyékolatlan csavart érpár
- Differenciális átvitel, mindkét bit domináns, nincs recesszív állapot
- Dual-channel működés lehetséges
 - Vagy a megbízhatóság növelésére
 - Vagy a sávszélesség növelésére
- 2,5; 5; 10 Mb/s adatátviteli sebesség
 - Minden sebességet támogatnia kell a hálózatnak



FlexRay topológia

- Busz
 - CAN, LIN buszhoz hasonló
- Csillagpontos hálózat
 - A csomópontok egy központi csomóponthoz (olyan, mint egy Ethernet HUB) csatlakoznak, ami jelismétléssel köti össze a többi
 - Hibatűrés érdekében
 - Rövidebb vezetékek miatt kevésbé zavarérzékeny
- A kettő kombinációja



FlexRay protokoll

- Időosztásos protokoll, akár mikroszekundumos pontosságú adatküldési időkkal
- CAN-szerű eseményvezérelt működést is támogat
- TDMA közeghozzáférés
- Minden FlexRay eszköz szinkronizált órajellel működik
- Determinisztikus átviteli idők
- Minden csomópontot előre be kell konfigurálni a hálózat paramétereivel



FlexRay protokoll

- Az időt ciklusokra bontjuk
- Egy ciklus részei:
 - Statikus szegmens: fix időszeltek real-time alkalmazásoknak, tervezési időben beosztva
 - Dinamikus szegmens: esemény alapú, részben futásidőben dől el a pontos beosztása
- A ciklusok párba szervezve
- A ciklus állhat kizárólag statikus szegmensből



FlexRay protokoll – statikus szegmens

- Mindkét csatornán azonos időzítés (az átvitt adat lehet különböző)
- A kereteket mindenképpen el kell küldeni
- Rögzített keretsorrend, rögzített időzítés
- A FlexRay hálózat tervezésekor rögzítik a paramétereket
- Nem igényalapú



FlexRay protokoll- dinamikus szegmens

- Igényalapú kerettovábbítás
- A két csatorna időzítése különbözhet (az átvitt adat is)
- Rugalmas az időzítés
- Nem garantált az átvitel az adott cikluson belül, elképzelhető, hogy bár egy csomópontnak lenne továbbítandó üzenete, az az aktuális ciklus dinamikus szegmensében már nem továbbítható



FlexRay első alkalmazás

- BMW X5 (2007)
 - <http://www.bmw.de/de/footer/publications-links/technology-guide/flex-ray.html>
- Az adaptív lengéscsillapítók vezérlését FlexRay buszon keresztül oldották meg
- Részletek:
http://www.eetimes.com/document.asp?doc_id=1272784&page_number=1



BME Hálózati Rendszerek és Szolgáltatások Tanszék 213



D2B és MOST busz

- D2B – Domestic Digital Bus
- MOST – Media Oriented Systems Transport
- Igény fejlett multimédiás alkalmazások támogatására
- Nagy sebességű adatátvitel
- A D2B az 1990-es évek elejétől fejlesztett technológia
 - Optical Chip Consortium: Philips, Matsushita stb.
 - Mercedes és Jaguar járművekben fordult elő
- MOST – a D2B utódjának tekinthető, 1998-tól fejlesztik:
 - Volkswagen, BMW, Daimler-Chrysler, Becker Automotive, Oasis Silicon



MOST busz

- Üvegszáloptikás vagy rézalapú hálózat
- Szinkron hálózat
- Eredetleg gyűrű topológiával (de elképzelhető más topológia is)
- Egy master, legfeljebb 64 slave
 - Slave-ek lehetnek például: vezérlőpanel, erősítő, kijelző, navigációs berendezés
- 25, 50 vagy 150 Mb/s adatátviteli sebesség érhető el
- A mai járművek többségében ezt a technológiát használják
- Nem csak a fizikai és adatkapcsolati réteget, hanem a teljes stack-et szabványosították



MOST busz

- Ethernet csatorna a buszon (150 Mb/s MOST)
- DTCP (Digital Transport Content Protection) támogatás
 - DVD
 - Blu-ray

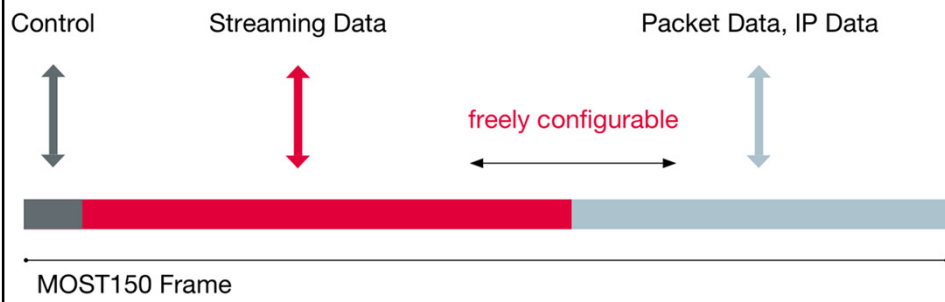


MOST busz

- 3 kommunikációs csatorna
 - Control channel
 - Eseményvezérelt
 - Kis sávszélesség
 - Asynchronous channel
 - Csomagalapú átvitel
 - Nagy sávszélesség
 - Nagy csomagok
 - Synchronous channel
 - Nagy sávszélesség-igényű folyamatos adatfolyamok számára



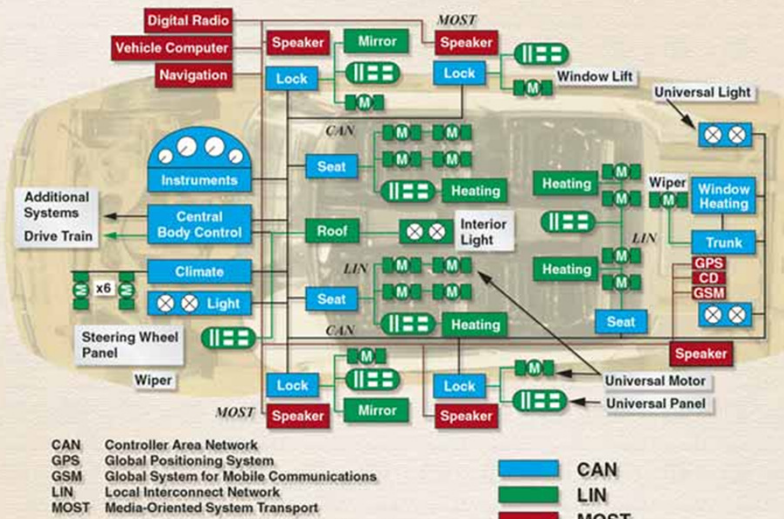
MOST keretformátum



Forrás: MOST Cooperation – MOST Informative April 2015 with MOST Forum Papers

BME Hálózati Rendszerek és Szolgáltatások Tanszék 218

Ismétlés



Forrás: Karen Parnell – Put the Right Bus in Your Car

[http://www.rpi.edu/dept/ecse/mps/xc_autobus48\(CAN\).pdf](http://www.rpi.edu/dept/ecse/mps/xc_autobus48(CAN).pdf) BME Hálózati Rendszerek és Szolgáltatások Tanszék 219

Forgalomfüggő navigáció



Tartalom

- Célok
- Optimális útvonal
- Előzmény sebesség információk
- Forgalmi statisztikák
- RDS-TMC
 - Helyszínek kódok
 - TMC-Pro
- Népszerű rendszerek:
 - iGO
 - Garmin
 - Sygic
- TPEG
- HD Radio
- Egyéb megoldások
- Online rendszerek
 - Google Maps
 - Waze



Célok

- Adott időpontban megtalálni az optimális útvonalat két pont között
- Az utazás közben bekövetkezett események hatására a navigáció módosítsa az útvonalunkat
- Egyéni preferenciák figyelembevétele (fogyasztás optimalizálása)
- Rendkívüli eseményekre időben reagálás (áttervezés, kerülőút):
 - Baleset
 - Teljes útzár
 - Útkarbantartás, munkavégzés
 - Jeges, csúszós út
 - Úton álló jármű
- Tervezhetőség: ha tudjuk, hogy mikorra érkezünk a célállomásra, akkor pontosabban meg tudjuk tervezni az utazásunk



Optimális útvonal

- Mindig a leggyorsabb útvonal a legjobb?
- A megtett távolság milyen súlyban számítsen?
- Az átlagfogyasztást vegyük-e figyelembe?
- Az alternatív útvonalaknál a szintkülönbséget figyelembe vegyük?
- Példa:
Kiindulás: Budapest Campona bevásárlóközpont
Uticél: Dunakeszi
Az autó városi fogyasztása: 8,3 l/100 km
Országúti fogyasztás: 5,2 l/100 km

BME Hálózati Rendszerek és Szolgáltatások Tanszék 223

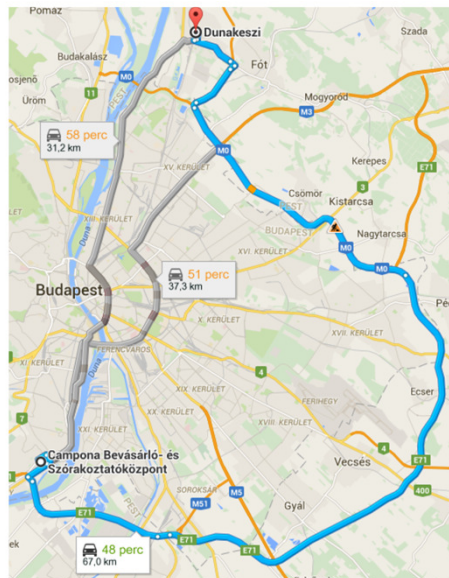
A Nav N Go iGO szoftverében lehetőség van un. Zöld útvonal tervezésére, ami a széndioxid kibocsátást is figyelembe veszi az útvonal tervezésénél, ezzel elérhetjük, hogy ha két pont között a legrövidebb út egy hegyen való átkeléssel érhető el, de kicsit hosszabb útvonalon meg lehet kerülni a hegyet, akkor az utóbbit részesítjük előnyben.



Optimális útvonal

1. útvonal	48 perc	57 km
2. útvonal	51 perc	37,3 km
3. útvonal	58 perc	31,2 km

- Melyik útvonalat válasszuk?
- Sietünk vagy spórolunk?



BME Hálózati Rendszerek és Szolgáltatások Tanszék 224



Optimális útvonal

- Néhány perc nyereség megér 30 km különbséget?
- Eltérő átlagfogyasztás városban és országúton.
57 km-es út: 3,5 l benzin
31,2 km-es út: 2,6 l benzin
- A navigációs rendszerek általában nem tudják megtalálni az optimumot
(leggyorsabb vagy legrövidebb opció van csak)
- Nem látjuk a forgalom trendjét (pl. csúcsidő közeleg), változhat a forgalom közben



Előzmény sebesség információk

- Egyes útvonalak, útszakaszok múltbeli forgalmi statisztikái napra és napszakra bontva
- Előnyei:
 - Nincs szükség semmi plusz berendezésre, sem online kapcsolatra, a térképfrissítés részeként kerül az eszközre
 - Az útvonalak átlagos terheltsége a napszak függvényében elég jól modellezhető
- Hátrányai:
 - Rendszeresen frissíteni kell az adatokat, hogy a változásokat követni tudjuk
 - A rendkívüli helyzetekkel (balesetek, lezárások) nem tud mit kezdeni ez a megoldás
 - Az évszakok közötti eltérések jelentősek lehetnek (pl. nyár, ősz)



Forgalmi statisztikák

- A készülék korábbi útvonalaiból kinyert átlagsebességek alapján tanulja meg a rendszer az egyes útvonalak áteresztő képességét.
- Használható az előzmény sebesség információkkal együtt illetve önmagában is.
- Előnyei:
 - Itt sincs szükség külön vevő berendezésre, online kapcsolatra
 - Gyakori használat esetén naprakész adatok állnak rendelkezésünkre
- Hátrányai:
 - Ha először járunk egy útszakaszon, akkor arról nincsenek információink
 - 1-1 szélsőséges adat befolyásolhatja a statisztikát
 - A rendkívüli helyzetekkel ez a megoldás sem tud megbirkózni



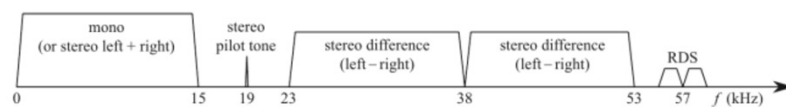
Szélessávú frekvenciamodulált átvitel

- +/- 100 kHz körüli lökettel rendelkeznek, tehát a 200 kHz-es csatornában elfér
- A hangja Hi-Fi minőségű sztereó zene átvitelére, így műsorszórásra kiválóan alkalmas
- Sztereó hang átvitele:
 - A szélessávú FM műsorszórás a kezdeti időkben mono volt, erre kellett kompatibilis, ugyanakkor sávtakarékos megoldással sztereó átvitelt varázsolni
 - A hangot 15 kHz-ig átvisszük, 19 kHz-en pedig referencia vivőt (pilot jelet) sugárzunk
 - A 19 kHz dupláját adó és vevőoldalon egyaránt előállítva a 38 +/- 15 kHz-es jelfrekvenciát a sztereó átvitelre úgy fogjuk felhasználni, hogy ide moduláljuk bele AM jelként a bal-jobb különbségi jelet
 - Tehát a 0..15 kHz szállítja a bal és jobb hangcsatorna átlagjelét, a 38 kHz +/- 15 kHz-es spektrumban pedig különbségi jelet szállítunk
- Az 57 kHz-en még egy pilotjelet elhelyeztek, aminek alapötletét az ARI-nak rövidített közlekedésinformációs rendszer adta. Itt digitális adat továbbítására adtak lehetőséget. Ezt Radio Data System-nek (RDS) nevezték, amit az 1980-as évek közepén szabványosítottak is.



RDS

- Az RDS a 57 kHz-es vivője a sztereó pilot 19 kHz-es vivőjével szinkronban, 0 fokban vagy 90 fokkal eltolva található meg
- Mono adás esetén ilyen megkötés nincs. Az RDS-t BPSK-ban modulálják, majd szinkronhelyesen felkeverik az 57 kHz-re
- Az adatsebesség 1187,5 b/s





RDS

- Az adat az adóban NRZ kódolva lesz, és ezután lesz egy differenciálás után a BPSK modulátorba vezetve
- Az adatcsomag felépítése:
 - Az adatcsomag 104 bitből áll, amit 4 darab 26 bites blokkra lehet szétosztani
 - A blokkon 16 bites információszót és egy 10 bites ellenőrzőszót tartalmaznak
 - Az első blokkban található a 16 bites programazonosító kód (PI)
 - Található benne programnév-kód (PS), ami alapján az állomásnév kerül kijelzésre
 - 5 bit műsorszám típus (PTY), amely a jelenleg sugárzott műsor kategóriáját jelzi
 - Közlekedési információs szolgáltatás jelző bit (TP), amely azt jelzi, hogy a műsor közlekedési információkat is tartalmazhat



RDS

- Adatcsomag felépítése (folyt.):
 - Alternatív frekvenciák listája (AF), amely megadja, hogy a vétel romlása esetén hol található meg még ugyanez a műsor
 - Közlekedési közlemény jelző (TA) bit, amelyet aktiválnak, ha közlekedési információt sugároznak
 - Zene/beszéd bit (M/S), amelyet arra lehet például használni, hogyha a zenét hangosabban akarjuk hallani a számok közötti beszédnél
 - Műsorszám azonosító (PIN), amivel egy konkrét műsorszám eleje és vége megjelölhető, például automatikus felvétel céljából
 - Rádiószöveg (RT), amivel folyamatosan megjeleníthető időjárás jelentést vagy zeneszám információ küldhető
 - Pontos idő és dátum (CT) is küldhető a vevőnek RDS üzenetben
 - TMC (Traffic Message Channel): A közutakon zajló forgalomról nyújt hasznos, valós idejű információkat



RDS-TMC

- A szabvány kidolgozását az EBU (European Broadcasting Union) a Bosch/Blaupunkt és a Philips cégekkel közösen még a 80-as évek közepén kezdte meg
- Az első hivatalos TMC-adás pedig 1997-ben indult el – ekkor azonban még csak az autórádió kijelzőjén, szöveges formában jelentek meg az üzenetek
- A TMC fejlődésének a navigációs készülékek elterjedése adott újabb lendületet, amelyek a GPS helymeghatározás révén már helyfüggően és grafikus formában tudják megjeleníteni a TMC-üzeneteket, sőt a torlódást elkerülő útvonalat is képesek tervezni
- Ma szinte minden nyugat-európai országban működik TMC szolgáltatás, míg az új Európai Unió tagállamok közül először a Cseh Köztársaságban, majd 2008 augusztusától Magyarországon és – 2009 júniusa óta – Szlovéniában érhető el



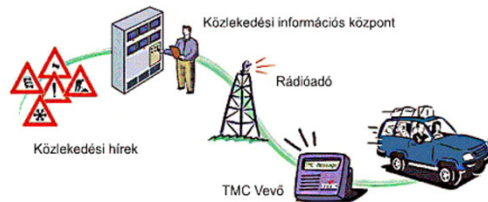
RDS-TMC

- A jelenleg forgalomban levő navigációs készülékek túlnyomó többsége vagy eleve rendelkezik beépített TMC-vevővel
- Vagy külső TMC vevővel (a köznyelvben TMC-antennával) kiegészítve alkalmas a TMC közlekedési hírek vételére
- A kis sávszélesség miatt a TMC-csatorna használatának döntő fontosságú feltétele, hogy minden szükséges helyszín, esemény és ajánlás kódolt formában álljon rendelkezésre



RDS-TMC

- A rendszer három nagy egységre bontható:
 - Szolgáltatói oldal: közlekedési események begyűjtése, kódolása
 - Adó oldal: kisugárzás, Magyarországon az MR2 Petőfi Rádió sugározza országosan
 - Vevő oldal: vevő egység, navigációs rendszer integráció, felhasználói felület





RDS-TMC szolgáltatói oldal feladatai

- ISO-szabványoknak, földrajzi lefedettségében a szakmai és felhasználói elvárásoknak megfelelő lokációs tábla elkészítése az adott országra
- Ez a tábla geokódolva és a megfelelő attribútumokkal ellátva tartalmazza az ország főbb közlekedési csomópontjait
- Minden, a táblában szereplő lokációs pontnak egyedi azonosítója van
- Magyarország lokációs tábláját a TrafficNav Kft. készítette el, amelyet 2007 őszén a TISA (Traveller Information Services Association) Fórum (korábbi nevén: TMC Fórum) tanúsított
- A TISA Fórum a TMC-szolgáltatások szabványait előkészítő és a szolgáltatásokat összehangoló nemzetközi szervezet
- A szolgáltatónak ezután fel kell vennie a kapcsolatot a digitális térképek gyártóival, hogy beépítsék ezt a táblát a térképbe
- Az események is kódolva vannak, ezt a szoftvernek kell feloldania
- Az eseménylista több nyelven tartalmazza az esemény leírását és kódját

BME Hálózati Rendszerek és Szolgáltatások Tanszék 235

http://geogis.detek.unideb.hu/Konferencia2010/Kotet/Terinformatika_konferenciakotet_Debrecen_2010.pdf



RDS-TMC szolgáltatói oldal feladatai

- A szolgáltató legfőbb feladata a különböző forrásból származó közlekedési események gyűjtése, ellenőrzése és kódolása
- Ennek során az erre a célra kifejlesztett szoftver segítségével manuálisan és akár automatikusan is kódolt forgalmi üzeneteket lehet előállítani
- Az operátor a szoftver segítségével az RDS kis sávzélességéhez igazodva a helyet, az eseményt és az irányt néhány bit-értékű számsorral alakítja



RDS-TMC

- TMC együtt tud működni GPS-alapú navigációs szoftverrel
- Lehetővé teszi az útvonal újratervezését az esetleges forgalmi dugók, balesetek, torlódások, útlezárások, forgalomelterelések, határátkelőhelyi várakozási idők függvényében
- A TMC-vevő egy FM-rádióvevő, amely a rádiófrekvencián sugárzott RDS-információkból kiszűri a TMC-jeleket, majd továbbítja azokat a navigációs készüléknek



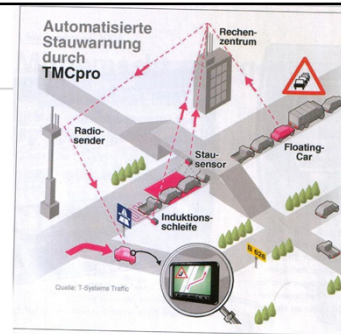
RDS-TMC üzenet felépítése

- RDS-adat bit-értéke 1187.5 bit másodpercenként, ez percenként 15 TMC üzenet kisugárzására ad lehetőséget. Egy TMC-üzenet 37 bitnyi értéket jelent:
 - 11 bit az esemény (esemény kód + időpont)
 - 16 bit kezdőpont
 - 1 bit irány
 - 3 bit végpont
 - 3 bit időtartam
 - 3 bit egyéb információk számára



TMC Pro

- RDS-TMC technológia
- Fizetős prémium szolgáltatás egyes országokban (pl. Németország)
- Az úttestbe épített indukciós érzékelők mellett nagyjából ötvenezer (50 000) autót felszereltek aktív jeladóval
- Ezek jeleit sugározták egy FM adó felé
- Az adó az összegyűjtött és értékelt jeleket továbbította a navigációs készülékek TMC vevői felé



- A magyar Nav N Go cég terméke
- Első verziója 2005-ben mutatkozott be Windows CE és Windows Mobile platformra
- Verziók:
 - iGO My Way 2006
 - iGO 8
 - iGO Amigo
 - iGO Primo
- TMC alapú forgalom alapú navigáció már a legelső verziótól elérhető
- Az iGO primo pedig már képes TMC adatok fogadására HTTP felett is.



- A cég termékei piacvezetőek az egész világon
- Számos autó gyári navigációját is a cég szoftverei látják el
- A Windows Mobile és CE verziókon kívül a szoftver elérhető iPhone és Android operációs rendszerekre is.
- A cég felvásárolta a TopMap Kft.-t, aki a Közép-Európai országok térképeit készítette

- Megfelelő licence és hardver esetén a szoftver automatikusan kezeli a TMC-t
- A szoftver automatikusan pásztázza az FM frekvenciákat, amíg elérhető szolgáltatást nem talál.
- A szolgáltatás igénybevételéhez országonként licence-t kell vásárolni.





Garmin

- Nem csak szoftvert, hanem komplett készülékeket értékesítenek
- A navigáció sokkal szélesebb palettájával foglalkoznak:
 - Hajózás
 - Repülés
 - Szabadtéri sport
 - Utcai navigáció (autó, kamion, motor)





Garmin forgalomi adatok

- TMC: az újabb készülékek támogatják a TMC szolgáltatást, egyes modellekhez külön kell megvásárolni a vevő berendezést.
- GTM: HD Radio adásokkal sugárzott forgalmi információk
- Online: a garmin készülékek nem rendelkeznek internet kapcsolattal, ezért egy okostelefonos alkalmazás (Smartphone Link) segítségével bluetooth-on jut el az élő forgalmi információ a készülékre



Sygyic

- 2004-ben alakított Szlovák cég
- A legtöbb mobil platformra kiadták navigációs szoftverüket, még az olyan platformokra is, mint:
 - Samsung Bada
 - Nokia Maemo
 - Symbian
 - Windows Mobile / CE





Sygic forgalmi információk

- Éves előfizetési díj ellenében online forgalmi információk
- A világ jelentős részén elérhető a szolgáltatás (Magyarországon is)



BME Hálózati Rendszerek és Szolgáltatások Tanszék 246

<http://www.sygic.com/gps-navigation/live-services>



TPEG

- Transport Protocol Experts Group
- A szabvány kidolgozását az EBU (European Broadcasting Union) 1997-ben kezdte meg
- Részben az RDS-TMC alapjaira épül, de ember által jobban értelmezhető és gépi feldolgozásra is alkalmas üzeneteket használ
- Nincs szükség előre definiált lokációs és esemény táblázatokra
- Két generáció van, jelenleg a TPEG2-t használják (ISO 21219)
- DAB (Digital Audio Broadcasting) rádióállomásokkal sugározzák:
 - egy csatorna 1500 kHz, amelyen 9-12 rádióállomást lehet párhuzamosan sugározni
 - DAB esetén MPEG-1 Audio Layer II (MP2) audió codec
 - DAB+ esetén AAC+ codec
- Nincs olyan szűk sávzélesség korlát, mint az RDS esetén
- Jelenleg az alábbi országokban használják: Németország, Norvégia, Belgium, Hollandia

BME Hálózati Rendszerek és Szolgáltatások Tanszék 247

<https://en.wikipedia.org/wiki/TPEG>



HD Radio

- USA-ban a digitális rádió sugárzás szabványa lett 2002-től
- Hivatalos neve: NRSC-5-C
- AM, FM támogatása
- A HD csak márkanév, nincs összefüggés a TV szabványnál használt High Definition rövidítéssel
- 300 kb/s sávszélesség jut egy csatornára
- MPEG-4 HE-AAC-en alapuló audio codec
- TPEG szolgáltatás támogatott a forgalmi információk továbbításához

BME Hálózati Rendszerek és Szolgáltatások Tanszék 248

https://en.wikipedia.org/wiki/HD_Radio



Egyéb megoldások

- Az FM-műsorszóráson kívül más adatátviteli lehetőségek is rendelkezésre állnak a közlekedési információk továbbítására
- Forgalmi információk SMS-ben: a navigációs szoftver hozzáfér a beérkezett SMS-ekhez és képes feldolgozni azokat. Nem terjedt el a megoldás.
- Interneten keresztüli letöltés:
pl. Nav N Go REST API:
<http://zippy.naviextras.com/services/index/rest/2/boot>



Online rendszerek

- A navigációs szoftver folyamatos online kapcsolatot tart fent a központi szerverrel
- A kommunikáció kétirányú:
 - A kliens letölti a térképet
 - A kliens elküldi a kiinduló helyet és az úticélt és a központi szerver fogja megtervezni az útvonalat
 - A kliens jelenti a pillanatnyi helyét, sebességét ezzel információt szolgáltatva az útvonalról a szerver számára.
 - A felhasználók maguk is küldhetnek jelentést a forgalmi szituációról



Online rendszerek

- **Előnyök:**
 - Nincs szükség térkép frissítésre, mindig a legfrissebb térképet kapjuk
 - Az úthálózat változásait gyorsan követi a rendszer
 - A forgalmi eseményekre gyorsan képes reagálni a rendszer
- **Hátrányok:**
 - Folyamatos adatkapcsolatot igényel (az adatforgalom ugyan nem jelentős)
 - A felhasználói jelentések sokszor körülményesek, elvonhatják a figyelmet a vezetésről
 - Csak akkor kapunk valós adatokat, ha a felhasználói bázis elég nagy. Ha bizonyos utak csak azért nem látszanak zsúfoltnak, mert arra nem járt még senki, akkor nem fogunk valós képet kapni.



Online útvonal tervezés

- Az útvonal tervező server:
 - A kezdő és célállomások között előállítja a lehetséges alternatív útvonalakat
 - Az egyes útvonalakat szakaszokra bontja
 - Szakaszonként meghatározza, hogy mennyi idő alatt tehető meg az adott forgalmi körülmények között
 - Kiválasztja a tervezési szempontnak legjobban megfelelő útvonalat
 - Egyes alkalmazásoknál lehetőségünk van az alternatív útvonalak között választani



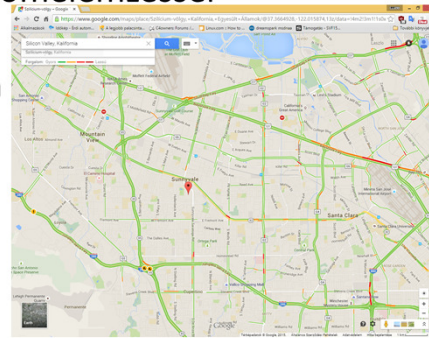
Online útvonal tervezés

- A tervezésnél figyelembe kell vennie a tervezésnél:
 - Nehéz forgalmi szituációk kerülése:
 - Visszafordulás
 - Többsávos főútvonal kereszteződése (vagy balra kanyarodás)
Jelzőlámpa nélküli kereszteződésben
 - Rövid időn belüli sávváltások
 - Földutak, rossz minőségű utak elkerülése
 - Díjköteles útszakaszokra figyelmeztetés vagy azok elkerülése



Google Maps

- A korai verziókban csak előzmény sebesség adatok alapján kalkulálták a várható érkezési időt
- 2004-ben a Google felvásárolta a ZipDash nevű céget, akik valós idejű forgalomelemzéssel foglalkoztak
- 2007-ben került integrálásra a valós idejű forgalmi információ a szoftverbe



BME Hálózati Rendszerek és Szolgáltatások Tanszék 254



Waze

- Waze Mobile Izraeli cég 2009-ben jelentette meg a szoftvert a főbb mobil platformokra
- Nyílt forráskódú, közösségi navigáció
- A felhasználók által elért átlagsebességek alapján tervezi az útvonalat és szolgáltat valós idejű forgalmi információkat
- A térkép adatait pedig a szolgáltatást használóktól gyűjti (térkép szerkesztő funkció)
- a felhasználók maguk is jelenthetnek a szoftver segítségével baleseteket, dugókat, fix traffipaxokat, rendőri ellenőrzéseket, sőt, szerkeszthetik az utakat, házszámokat, helyeket

BME Hálózati Rendszerek és Szolgáltatások Tanszék 255

Forráskód: https://wiki.waze.com/wiki/Source_code



Waze

- A Waze szabadon letölthető és használható bárhol a világon, de csak néhány ország rendelkezik teljes térképpel
- Gondoskodik a felhasználó pillanatnyi helyzetének és sebességének névtelen módon történő felhasználásáról az adatbázisának pontosítására
- A Waze szoftverét GNU General Public Licence v2 védi, ez nem terjed ki a térképadatokra
- 2013-ban a Google megvásárolta a céget 1,3 milliárd dollárért
- A 3-as verziótól a nyílt forráskódú licence megszűnt és az alkalmazás zárt forráskódúvá vált
- A felvásárlás után a Waze alkalmazás megmaradt külön alkalmazás, de a forgalmi adatokat és jelentéseket a Google térképe is átveszi és megjeleníti

BME Hálózati Rendszerek és Szolgáltatások Tanszék 256

Jelenleg a következő országok rendelkeznek teljes térképpel a Waze-ban: Magyarország, Amerikai Egyesült Államok, Kanada, Franciaország, Németország, Olaszország, Hollandia, Belgium, Egyesült Királyság, Spanyolország, Izrael (valószínűleg a legteljesebb térképpel^[1]), Ecuador, Argentína egyes részei, és Panama.



Waze

- A szoftver közösségi funkciókat is megvalósít:
 - Útvonal és az érkezés várható idejének megosztása ismerősökkel
 - A felhasználók a megtett kilométerek és a jelentések után pontokat kapnak, a pontok alapján pedig rangok szerezhetőek
 - Minél magasabb rangja van a felhasználónak, annál nagyobb súllyal veszik figyelembe a jelentését.
 - Üzemanyag töltő állomások árainak beküldése, megjelenítése



BME Hálózati Rendszerek és Szolgáltatások Tanszék 257

E-útdíj rendszerek



Tartalom

- Célok
- Komponensek
- EETS
- Magyar megoldás
 - Eseti felhasználás
 - Rendszerek felhasználás
- Európai és külföldi megoldások
 - Fizető kapuk
 - Rendszámfelismerő rendszerek
 - DSRC
 - GNSS
 - RFID
 - Tachográf alapú rendszerek
- Környező országok megoldásai



Célok

- Megtett úttal arányos fizetés
- Egyszerű, nagy áteresztő képességű rendszer
- Díjszedés a forgalom zavarása nélkül
- Sebességtől független kapcsolat
- Minden forgalmi körülmény esetén elérhető (oszlopban haladás, előzés, torlódás, stb.)
- Ellenőrzési és szankciós lehetőség a helyszínen
- A rendszer alkalmazható legyen a teljes hálózaton
- Manipulálhatatlan legyen



Célok

- Zavarhatatlan legyen
- Minden előforduló környezeti feltételnek megfeleljen
- Távfelügyelhető legyen
- Ellenálljon a rongálási kísérleteknek
- Elfogadható költség-haszon arány



Komponensek

- Járművön belüli (fedélzeti) eszközök
 - Elektronikus matrica (Tag)
 - Egy előre programozott kódot tárol
 - Központi adatfeldolgozást és adattárolást igényel
 - Korlátozott áthaladási sebesség
 - Fedélzeti berendezés (On-board Unit)
 - Adatfeldolgozási és –tárolási képesség
 - Chip-kártyás változata biztonságosabb, járművön kívül is használható és feltölthető (pre-paid)
 - Akár útmenti infrastruktúra nélkül is, pl. GPS-el

BME Hálózati Rendszerek és Szolgáltatások Tanszék 262

http://www.uvt.bme.hu/targyak/int_kozl/ea_2005/intelligens_ea_4.pdf



Komponensek

- Útmenti infrastruktúra
 - Fix telepítésű, matrica-olvasó berendezések
 - Kommunikálnak a fedélzeti berendezéssel (DSRC)
 - Képesek adatfeldolgozásra
 - Kommunikálnak a központi berendezéssel
 - Fedélzeti berendezést kiszolgáló infrastruktúra
 - Helymeghatározás: pl. markerekkel
 - GSM hálózat
 - „Virtuális” útdíjgyűjtő helyek



EETS

- European Electronic Toll Service - Európai Elektronikus Útdíjszedési Szolgáltatás
- Az EETS a díjköteles közlekedést szolgálja ki azzal, hogy elektronikus módon biztosít fizetési lehetőséget és pénzmozgást az útdíjszedés résztvevői között
- Segítségével a felhasználó képes egyszerű és zökkenőmentes módon képes fizetni az útdíjszedőnek
- A szolgáltatás lehetővé teszi, hogy a fedélzeti eszköz (OBU) közreműködésével és egyetlen szolgáltatóval történő szerződéskötéssel az úthasználó könnyedén eleget tudjon tenni díjfizetési kötelezettségének az Unió területén belül bárhol



BME Hálózati Rendszerek és Szolgáltatások Tanszék 264



EETS

- Az EETS miatt visszaszorult a fizetőkapus készpénzfizetési megoldás
- Megfelelő szolgáltatóval leszerződve és a fedélzeti eszköz segítségével a fuvarozó képes országokon átívelő útvonalát előre megtervezni
- Az EETS ötlete 2004-ben került bele az Európai Unió Bizottságának egyik direktívájába, a Bizottság 2009-ben pedig elfogadta azt
- A határozat foglalja pontokba az útdíjbeszedők, a szolgáltatók, valamint az úthasználók jogait és kötelezettségeit is



Magyar megoldás – eseti felhasználók

- Viszonylati jegy váltása az értékesítési pontokon:
 - egy útvonal tervező segítségével megtervezi, hogy honnan hova szeretne eljutni
 - A kikalkulált útvonalra tudja megváltani a jegyet a felhasználó
 - A viszonylati jegy adott rendszámra, egy utazásra, egy irányba érvényes
- Az ellenőrzés a matricás rendszerénél is használatos kamerás rendszerrel és eseti ellenőrzéssel valósítható meg



Magyar megoldás – fedélzeti eszköz

- A szerződött logisztikai szolgáltatók által már korábban a járművekbe beszerelt, vagy újonnan, a felhasználó által az értékesítési pontokon vásárolt GPS alapú nyomkövető eszköz
- A fedélzeti eszköz a flottakövető rendszeren keresztül automatikusan viszonylati jegyet vált a gépjárműre.
- Az útdíj köteles útszakaszokon haladva szakaszonként, maximum 26 km-enként automatikus jegytépést jelző sípjelet ad a készülék

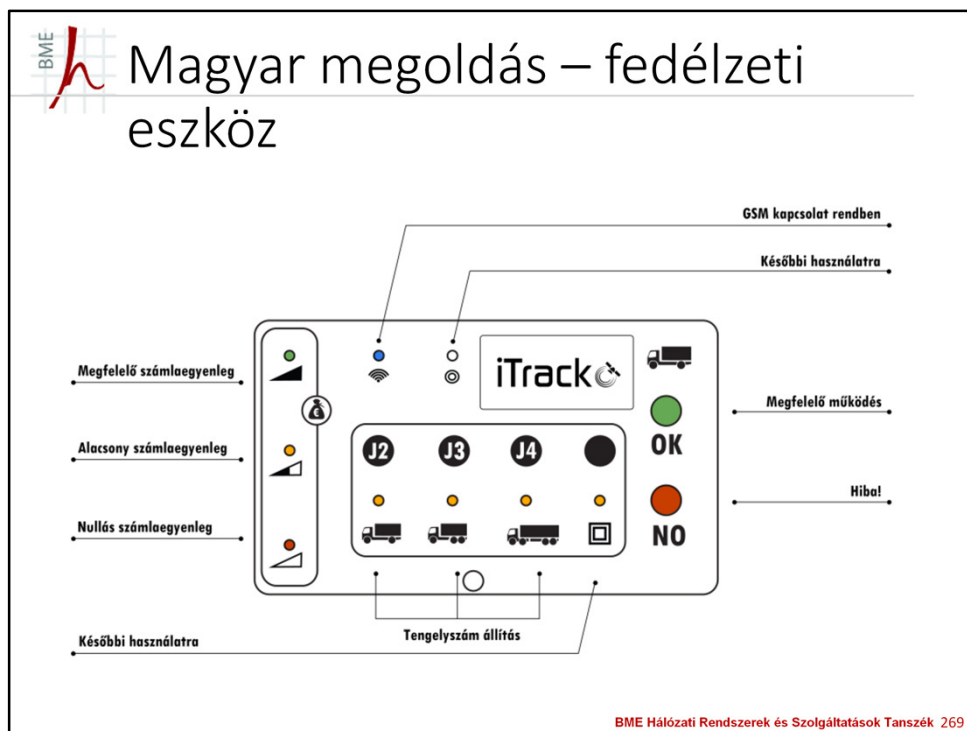


Magyar megoldás – fedélzeti eszköz

- A szakaszhatárok jellemzően a kereszteződéseknel vannak, ami újabb jegytépést kell generáljon, amit a sápolás jelez
- A fuvarozónak számlával kell rendelkeznie a szolgáltatónál és előre feltöltött egyenlege terhére tudja igénybe venni a szolgáltatást



BME Hálózati Rendszerek és Szolgáltatások Tanszék 268



A fedélzeti egység a vezetőnek egyszerű beállítási lehetőségeket nyújt a tengelyszám állításra, visszajelzést kap a helyes működésről és a számlaegyenlegről



Magyar megoldás – fedélzeti eszköz

- A szolgáltatást csak olyan flottakövető cég rendszerével lehet igénybe venni, akik auditált bevallási közreműködők
- A használat előtt a fedélzeti eszközt regisztrálni kell a szolgáltatónál
- A regisztrációt követően járműhez és folyószámlához kell azt rendelni



Magyar megoldás – fedélzeti eszköz

Gépjármű

Gépjármű létrehozása

Ország*	Magyarország
Rendszám*	Jármű rendszámán feltüntetett felsőjelzés
Euró-kód*	Válasszon Euró-kódot!
Kategória*	Válasszon kategóriát!
Folyószámlához rendelés*	Válasszon folyószámlát!
OBU id	pl. 940123654987
OBU PIN	PIN használata OBU szolgáltatónként eltérhet
Járműkategória beállítása*	Web

Bevallási Közreműködő igénybevétele esetén:
Amennyiben a Bevallási Közreműködő kód tengelyszám kategóriát, akkor annak alapján történik az utóji beállítása.
Természetesen abban az esetben, ha a Bevallási Közreműködő nem küld ilyen értéket, szintén a HU-GO oldalon, a jármű adatai között megadott tengelyszám alapján történik az utóji beállítása.

HU-GO portálon esetén: Minden esetben a HU-GO oldalon, a jármű adatai között megadott tengelyszám (JOB-) kategória érték alapján történik az utóji beállítása.

Súly		t
Tengelyterhelés		t
Szélesség		m
Magasság		m
Hossz		m

BME Hálózati Rendszerek és Szolgáltatások Tanszék 271

A fedélzeti eszközt egy OBU id és OBU pin segítségével lehet regisztrálni



Európai megoldások

- Autópálya matrica / kuponok
 - Átalánydíjas
 - Alacsony üzemeltetési költségek
 - Ellenőrzésre kevés lehetőség
 - Forgalomszámlálásra nem használható
 - Hamisítási lehetőségek felmerülése

MATRICA
VIGNETTE



BME Hálózati Rendszerek és Szolgáltatások Tanszék 272



Európai megoldások - Kamerás rendszerek (rendszámazonosítás)

- A fizető felhasználók a rendszám alapján azonosíthatóak
- Adatvédelmi kérdések
- Magyarországon ellenőrzésre ezt a rendsert használják
- Előnyök:
 - Jól bevált technológia behajtási díjas rendszereknél
 - Nincs szükség külön eszközre a gépjárműben
 - Hatékony üzemeltetés és egyszerű bírságolás
 - Más technológiákkal kombinálva növelhető a hatékonysága
 - Nincs sebesség megkötés a gépjárműre nézve



BME Hálózati Rendszerek és Szolgáltatások Tanszék 273



Európai megoldások - Kamerás rendszerek (rendszámaazonosítás)

- Hátrányok:
 - Jó minőségű rendszámok szükségesek
 - Erős időjárásfüggőség (vizuális megfigyelés miatt)
 - Naprakész jármű adatbázis elérése szükséges
 - Sikertelenség esetén a kézi felismerés plusz költséggel járhat
 - Precíz kamera beállításra van szükség a megfelelő működéshez
 - Nehéz komplex díjszabásokra alkalmazni
 - A rendszámtáblák nem szabványosítottak, országonként eltérő



Európai megoldások - Díjfizető kapuk

- Közvetlen fizetési lehetőség az elkülönített útvonalakon
- Jelentős üzemeltetési költségek
- Szűk keresztmetszetet okoz
- Felhasználók elégedetlenek
- Speciális infrastruktúraelemekhez kötött használat (alagutak, hidak, stb.)
- Jelenleg ilyen megoldással találkozhatunk:
 - Horvátország
 - Olaszország
 - Franciaország



BME Hálózati Rendszerek és Szolgáltatások Tanszék 275

http://www.kkk.gov.hu/remos_downloads/Tolling_systems_in_Europe.186.pdf

-



Külföldi megoldások - RFID

- Előnye a DSRC technológiához képest, hogy olcsóbb a fedélzeti eszköz (DSRC ~ 10 EUR, RFID ~ 1 EUR)
- UHF 868-956 MHz frekvencia tartományban működnek
- Az antennák egyszerre több tag-et is tudnak olvasni
- A legmodernebb megoldások esetén lassítás nélkül is lehetőség van a leolvasásra



BME Hálózati Rendszerek és Szolgáltatások Tanszék 277



Külföldi megoldások - RFID

- Aktív rendszer: azonosításra 0-100 km/h-ig (Kalifornia FASTTRACK)
- Passzív rendszer: azonosítás 240 km/h-ig (Argentína)
- Kis hatótáv
- Elsősorban Amerikában és Kanadában használják
- A 902-956 MHz nem kompatibilis az uniós szabványokkal



BME Hálózati Rendszerek és Szolgáltatások Tanszék 278



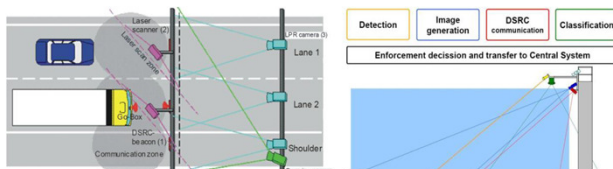
Európai megoldások - DSRC

- Dedikált rövid hatótávú kommunikáció 5,8 GHz
 - Kétirányú rövid és közepes távolságú kommunikáció
 - Közúti közlekedés számára kifejlesztett protokollok
 - Több mint 20 országban használják útdíj gyűjtéshez
 - V2I és V2V rendszereket is támogatja
 - Könnyű ellenőrzési lehetőségek
 - Elterjedt megoldás
 - Alacsony kommunikációs költségek
 - Forgalomszámlálásra is használhatóak
 - Felhasználóbarát
 - A szükséges kommunikációs infrastruktúra miatt alacsony flexibilitás és bővítési lehetőségek



Európai megoldások - DSRC

- Alkalmazott megoldások:
 - Fizetőkapu sorompóval: a gépjármű korlátozott sebességgel kell hogy megközelítse a kaput, sikeres tranzakció esetén a sorompó automatikusan nyílik. Áteresztő képesség: 6-700 autó / sáv / óra
 - Szabad haladásos rendszerek (multi-lane free flow tolling - MLFF): az úttest feletti portálokra helyezik a DSRC eszközöket, a járműveket a haladásban nem akadályozza. Áteresztő képesség: 3000 autó / sáv / óra



BME Hálózati Rendszerek és Szolgáltatások Tanszék 280



Európai megoldások - DSRC

- Előnyök:
 - Széles körben használt, egyszerű és kiforrott technológia
 - EETS által javasolt technológia
 - Megbízható, nagy teljesítményű, kis interferencia
 - Olcsó OBU és alacsony üzemeltetési OBU költségek
 - Számos ilyen rendszer üzemel Európában
 - Földalatti létesítményekben is használható
 - Könnyebb együttműködési lehetőség a különböző országok rendszerei között



Európai megoldások - DSRC

- Hátrányok:
 - Az úthálózat mentén ki kell építeni a rendszert (olvasókat telepíteni)
 - Nagy beruházási és fenntartási költségek
 - Nehéz a hálózat módosítása, bővítése
 - Sok kereszteződés, fel-lehajtó esetén nagyon költséges
 - Az olvasóknak nehéz helyet találni (az út fölötti állványokra, portálokra kell szerelni, hogy rálátása legyen a fedélzeti egységre). Nem autópályán ennek sokkal nehezebb helyet találni.
 - Alacsony forgalmú útszakaszokon a megtérülés és a profit kérdéses



Európai megoldások - GNSS

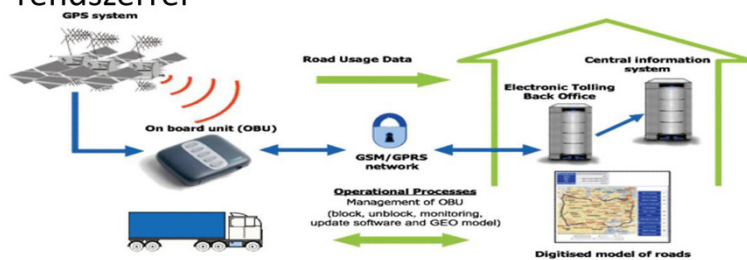
- A fedélzeti berendezés (OBU) automatikusan rögzíti a jármű pozícióját
- Virtuális fizetőkapuk
- Teljes területet lefedő rendszer
- Lehetőség van a különböző szakaszokon eltérő útdíj meghatározására
- Magas kommunikációs költségek (GPRS)
- Pontossága függ a műholdas helymeghatározás pontosságától
- Ellenőrzési nehézségek
- Korlátozott forgalmi adatok a magas költségekért cserébe

BME Hálózati Rendszerek és Szolgáltatások Tanszék 283

GNSS: Global Navigation Satellite System, GPS, GLONASS, Galileo, Beidou műholdas rendszerek együttesét értjük alatta

A magyar HO GO is GNSS alapú megoldás.

- Az ellenőrzéshez más technológiákkal kombinálják:
 - DSRC-t is építenek a fedélzeti egységbe
 - Rendszámfelismerő kamerákat alkalmaznak.
- A fedélzeti egység folyamatos kétirányú kommunikációt folytat a központi feldolgozó rendszerrel





Európai megoldások - GNSS

- **Előnyök**
 - A fizetős úthálózat gyorsan és könnyen bővíthető, változtatható.
 - Kevés útmenti infrastruktúra építés szükséges
 - Alacsony üzemeltetési költség
 - Egyszerűen tudunk további értéknövelt szolgáltatást hozzáadni az online kapcsolat révén (pl. forgalmi információk)
- **Hátrányok**
 - Önmagában a GPS koordináták egy bíróságon még nem elég bizonyító erejűek, ezért fényképes bizonyítékról is gondoskodni kell
 - A fedélzeti egység drágább a többi megoldáshoz képest, megfelelőségi tesztelése összetettebb
 - A műholdas és a mobiltelefonos lefedettség nem minden pontján biztosított a fizetős útszakasznak (pl. alagutak), ez problémát okozhat az elszámolásnál
 - Újabb, kevésbé kiforrott megoldás, mint a DSRC
 - Az adatforgalom költségekkel jár
 - Sok információt gyűjt be a járműről a rendszer, adatvédelmi kérdések merülhetnek fel (pl. mikor hol járt, hol állt meg, stb)

BME Hálózati Rendszerek és Szolgáltatások Tanszék 285

Német autópálya alagutaknál olyan megoldással próbálkoznak, hogy földi sugárzású GPS jeleket sugároznak. A térrő kimaradásokat pedig buffereléssel és ismételt újraküldéssel lehet orvosolni.

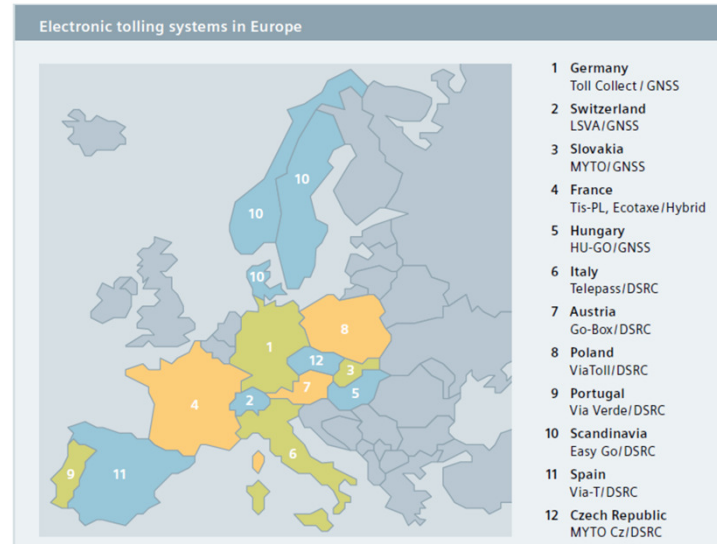


Európai megoldások - Tachográf alapú díjfizetés

- Minden busz és tehergépjármű kötelező tartozéka
- Svájcban használják a külföldi gépjárművek esetén
- Pontos adatok állnak rendelkezésre az útvonalról
- A kiolvasás és fizetés lassú, nagy forgalmi torlódást okoz



BME Hálózati Rendszerek és Szolgáltatások Tanszék 286





Ausztria

- A 3,5 tonna fölötti összsúllyal rendelkező gépjárművekbe kötelező beszerezni az úgynevezett GO-Boxot.
- DSRC alapú
- Amikor egy díjszedő kapun áthalad, akkor egy hangjelzés szólal meg a hangjelzőn keresztül (1 x csipogás = tranzakció rendben)
- Ha az útdíj nem lett kiegyenlítve: Erre 5 órán és legkésőbb 100 kilométeren belül van lehetősége egy GO értékesítő helyen a vezetőnek



Ausztria

- A készülék lítium elemeket tartalmaz, amelyek élettartama kb. 5 év
- 472 fizetőkapu - 2100 km-es hálózat
- Rendszerbe bevontak néhány alagutat is, ott hagyományos fizetőkapuk találhatóak
- Lehetőség van internetes (elektronikus) fizetésre is



Németország

- GNNS/GPRS alapú, minden OBU tartalmaz DSRC-t az ellenőrzéshez
- 12 tonna feletti tehergépjárművekre
- 12.000 km-nyi autópályára van kiterjesztve a rendszer, 300 ellenőrző állomás + 300 mobil állomás
- Az úthasználati díj a jármű tengelyszámától és a környezetvédelmi besorolásától függ



Svájc

- LSVA (Leistungabhängige Schwerverkehrsabgabe)
- 2001. január elsejétől a teljes úthálózaton működik
- 3,5 tonna összsúly felett
- Díjszámítás a közforgalmú utakon megtett kilométer és a károsanyag-kibocsátás alapján
- Turistabuszok, traktorok, lakóautók, stb. átalányt fizetnek



Svájc

- A kötelező fedélzeti berendezés (belföldi gépjárművekre) funkciói:
 - a megtett kilométerek rögzítése
 - automatikus aktiválás és deaktiválás az országhatáron
 - GPS segítségével a tachográf és a határátlépés ellenőrzése
 - pótkocsi felismerése szenzor segítségével
- a tulajdonos az adatokat havonta kiolvassa a chip-kártyáról, és megküldi az adóhivatalnak



- Külföldi gépjárművek:
 - Nem írható el ő kötelező OBU
 - OBU nélkül azonosító chip-kártya (ID-card)
 - az összes paramétert (megengedett tömeg, stb.) rögzítik
 - automatikus aktiválás és deaktiválás az országhatáron egy önkiszolgáló berendezéssel
 - be- és kilépéskor automatikus km-leolvasás
 - a díj kilépéskor fizetendő egy automatánál
- Ellenőrzés:
 - Belföldi jármű esetén útközben, DSRC állomásokon
 - Külföldi jármű esetén az országhatáron tachográf-ellenőrzés



Csehország

- Bevezetés éve: 2007
- Technológia: DSRC
- A rendszer és a fedélzeti készülék neve: PREMID
- 3,5 t fölött kötelező
- Differenciálás:
 - tengelyszám szerint
 - károsanyag-kibocsátás szerint
 - naptári napok szerint



Lengyelország

- Bevezetés éve: 2011
- Technológia: DSRC
- A rendszer és a fedélzeti készülék neve: VIA-BOX
- 3,5 t fölött vagy 9 személyes járműtől
- Differenciálás:
 - össztömeg szerint
 - károsanyag-kibocsátás szerint



Szlovákia

- Bevezetés éve: 2010
- Technológia: vegyes (DSRC és GPS)
- A rendszer és a fedélzeti készülék neve: EMYTO
- 3,5 t fölött vagy 9 személyes járműtől
- Differenciálás:
 - tengelyszám szerint
 - károsanyag-kibocsátás szerint

Online pénztárgépek



Tartalom

- Célok
- Magyar rendszer
 - Adóügyi ellenőrző egység
 - PC alapú kasszák
 - 20-50 gépes nagyáruházak
 - Adatkapcsolat
 - Architektúra
 - Revízió
 - Szoftverfrissítés menete
- Külföldi rendszerek



Célok

- Nyugtaadási kötelezettség betartatása
- Hatósági ellenőrzések megkönnyítése
- Forgalom alakulásának követése a hatóság részéről
- Kiugró forgalmi adatokra gyors reagálás



Online pénztárgép szükségessége

- A korábbi rendszer számos visszaélésre adott lehetőséget:
 - CANCEL gombot nyomtak mielőtt a nyugtát kinyomtatnák
 - Oktató módban használták a készüléket
 - RAM törlés napi zárás előtt, majd óra vissza, és a tényleges forgalom harmadáig új bizonylatok

BME Hálózati Rendszerek és Szolgáltatások Tanszék 300

Un. Gyűjtőkosaras pénztárgépnél csak akkor került nyomtatásra a nyugta, a az összes tétel után lezárták a nyugtát. A régi gépek ezt a kosarat nem tárolták el az adómemóriában, így ha törölték, akkor nincs nyoma sehol.



Magyar megoldás

- 3/2013. (II. 15.) NGM rendelet fogalmazza meg a pénztárgépek és taxaméterek műszaki követelményeit
- A rendelet követelményeinek nem megfelelő pénztárgépeket kell cserélni
- A pénztárgép online funkcióit az Adóügyi Ellenőrző Egység látja el

BME Hálózati Rendszerek és Szolgáltatások Tanszék 301

http://www.nav.gov.hu/data/cms291645/OPG_kozlemenyn.pdf



Magyar megoldás - AEE

- AEE: Adóügyi Ellenőrző egység
- A pénztárgépben keletkezett adatokat UTF-8-as kódlap szerinti karakterkódolású, XML típusú naplóállományokban kell tárolnia
- A NAV szerver utasítására el kell küldenie a tárolt adatokat az adóhatóság részére
- Élettartama során az AEE memóriaegysége folyamatosan tárol, sohasem töröl. Ennek megfelelően min. egymillió kiadott bizonylat adatainak eltárolására alkalmasnak kell lennie (min. 16 Gb tárhelykapacitással kell rendelkeznie)
- A megtelt vagy meghibásodott AEE-t csak cserélni lehet, törölni és újrafelhasználni nem



Magyar megoldás - AEE

- Az AEE a NAV szerverével titkosított kapcsolatot alakít ki, amelynek privát kulcsát a NAV szolgáltatja
- A titkosított kapcsolat kialakításához szükséges privát kulcs rendelkezésre bocsátásának rendjét a NAV hivatalos honlapján közleményben teszi közzé
- Az AEE gyártóknak az alábbi adatokat kell a NAV felé eljuttatni:
 - AEE-be épített GSM egység IMEI szám
 - AEE-be épített SIM kártya IMSI szám
 - Gyártó megnevezés
 - AEE gyártói típusnév
 - AEE hardver verzió
 - AEE egyedi gyártási szám
 - AEE szoftver megnevezés
 - AEE szoftver verziója



Magyar megoldás - AEE

- Az AEE modulban használt X.509 aláíró tanúsítványt AEE gyártónként egy ROOT CA-val kell kibocsátani
- AEE-k, a NAV szerverével, HTTP protokoll szerinti, POST metódusú, üzenetekkel kommunikálnak
- Az AEE-t fizikailag a pénztárgép burkolatán belül kell elhelyezni.
- Az AEE a számítógép alapú pénztárgépnél elhelyezhető a nyomtatóban is, ekkor a nyomtatónak is plombálnak kell lennie
- Az AEE-t úgy kell kivitelezni, hogy kizárólag a burkolat roncsolásával legyen nyitható
- Az AEE-be a gyártónak ipari beágyazású, magyarországi mobilhálózaton csomagkapcsolt adatátvitelre alkalmas GSM modult kell beépítenie, multislot class 12 besorolással



Magyar megoldás - AEE

- Az AEE-nek képesnek kell lennie minden magyar mobilszolgáltató hálózatra felkapcsolódni.
- Az AEE-nek nem lehet érvényes, nyilvános hálózaton való azonosítást lehetővé tevő IP- címe. Az AEE nem folytathat kommunikációt más AEE-kkel
- Az AEE-vel kapcsolatos egyéb műszaki követelmények:
 - Device Certificate alkalmazhatósága
 - SSL titkosítási eljárás támogatása
 - User Authentiction /Managed PKI-Service támogatása
 - Az adatkapcsolat kiszolgálására a meglévő mobilkommunikációs nyilvános hálózatokon keresztül
 - IT Biztonsági szabályozás és megoldások alkalmazása szükséges a rendelkezésre állás, bizalmasság, adatok sértetlensége területén
 - Valós idejű, ütemezett illetve folyamatos adatgyűjtésre, TCP/IP protokollt alkalmazza az AEE szabványos kommunikációhoz

BME Hálózati Rendszerek és Szolgáltatások Tanszék 305

A Nav természetesen eléri az eszközöket ebben a belső ip hálózaton. Ha az eszköz offline lenne, akkor SMS-ben küldhet ébresztést a NAV.

A magyar szolgáltatóknak nem sikerült megállapodniuk egy olyan belföldi roaming megoldásról, hogy 1 hazai sim kártyával mindhárom szolgáltató hálózatra fel lehessen jelentkezni, ezért jelenleg külföldi roaming partnerrel működik a szolgáltatás.

http://www.szintezis.hu/upload/3_2013.-ii.-15.-ngm-rendelet.pdf



Magyar megoldás - AEE

- Az adatkommunikációs folyamatban szereplő eszközök informatikai védelme érdekében
 - Az elektronikus hitelesítés PKI – X.509 Registration Authority (RA) szerinti legyen
 - A Certificate authority SAS 70 Type II auditált legyen
 - Az RSA aszimmetrikus kulcs mérete legalább 2048 bit legyen
 - az Alkalmazott memóriamodul legalább 16GB kapacitású SDHC class 6 vagy annál magasabb besorolású legyen
 - Biztosítani kell az illetéktelen módosításokkal, hálózat alapú támadásokkal (vírusok, programférgék, szándékos hacker tevékenység stb.) szembeni védelmet
 - Az AEE beágyazott GSM moduljával szembeni követelmények:
 - Az AEE-nek képesnek kell lennie GPRS technológiával, valamint az EDGE, HSDPA, UMTS technológiák egyikével történő adattovábbításra
 - A SIM feleljen meg az ETSI M2M UICC standard (TS 102.671) szabványban foglaltaknak
 - Az AEE-nek alkalmasnak kell lennie a benne működő üzemeltető program (továbbiakban: AEE szoftver) távoli frissítésére a NAV szerveréről
 - Az AEE-nek képesnek kell lennie a kezelő figyelmeztetésére, ha az AEE szoftver frissítése a kezelővel kapcsolatban bármilyen követelményt támaszt vagy támaszthat



Magyar megoldás - AEE

- Egyes területekre a törvény külön követelményeket fogalmaz meg:
 - Üzemanyagkút-kezelő pénztárgép
 - Hordozható pénztárgépek
 - Mobil menetjegykiadó pénztárgépek
 - Éttermi pénztárgépek
 - Gyógyszertári pénztárgépek
 - Önkiszolgáló pénztárgépek



Magyar megoldás - AEE

- Tárolt bizonylati adatok tartalmára és szerkezetére vonatkozó előírások:
 - Az eszköz üzembe helyezésétől, illetve a legutóbbi adatszolgáltatástól az aktuális pillanatig terjedő idő- szakra vonatkozóan ANSI 1250-es kódlap szerinti karakterkódolású szöveges állományokban kell tárolnia
 - Az AEE-nek adattovábbításkor a legutóbbi bejegyzéssel érintett szöveges állományt le kell zárnia, és azt a NAV szerverei felé el kell küldenie
 - Az AEE-nek minden adattovábbítás megkezdését követően új szöveges állományt kell nyitnia, és abban kell folytatnia a bejegyzések rögzítését
 - Az AEE-nek a szöveges állományt annak megnyitását követő 24 óra elteltével akkor is le kell zárnia és újat kell nyitnia, ha ezen idő alatt nem történt adattovábbítás a NAV szervere felé
 - Az AEE-nek az elküldött állományt az elküldés megkezdésének időpontja szerinti AAAAAAAAAA_ééééhhnnóóppmm_s.txt néven kell eltarolnia

BME Hálózati Rendszerek és Szolgáltatások Tanszék 308

AAAAAAAAA: A pénztárgép AP száma 9 karakteren

éééé: az év száma négy számjegyen,

hh: a hónap sorszámát két számjegyen,

nn: a nap sorszáma két számjegyen,

óó: az óra száma két számjegyen,

pp: a perc száma két számjegyen,

mm: a másodperc száma két számjegyen

s: a fájl 1-től kezdődően, kihagyás és ismétlés nélkül képzett sorszáma az AEE élettartama során



Magyar megoldás – PC alapú kasszák

- A teljes rendszer cseréje hatalmas költség lenne
- A nyomtatóba építhető az AEE, ekkor adóügyi nyomtatónak nevezzük
- Elegendő csak a nyomtatót kicserélni
- Tilos:
 - Pénztárgép alaplapra integrált nyomtató-vezérlés
 - HUB vagy router a három fő egység között (PG, AEE, printer)



BME Hálózati Rendszerek és Szolgáltatások Tanszék 309

<http://konferenciak.advalorem.hu/uploads/files/Integr%C3%A1ci%C3%B3%20%C3%A9s%20korszakunk%20online%20pe%20CC%81nzt%C3%A1rg%C3%A9pek%20m%C3%B6g%C3%B6tt%20van.pdf>
<https://www.youtube.com/watch?v=T42iiHy7ogY>



Magyar megoldás – 20-50 gépes áruházz

- Az AEE rögzítő/naplózó és kommunikációs egysége fizikailag elkülönülten kerül kiépítésre több rögzítő/naplózó egység egy központi kommunikációs egységgel történő kiszolgálásával
- Az AEE-k ezzel az egységgel kommunikálnak
- A Központi kommunikációs egység kommunikál a NAV rendszerével
- Speciális engedélyezési eljárás:
 - Első körben elvi forgalmazási engedély
 - Második körben az üzembe helyezést megelőzően, az üzembe helyezés helyszínén ellenőrzi a központi kommunikációs egységet és az alkalmazott hálózati eszközöket.



Magyar megoldás - Adatkapcsolat

- Miért GSM?
 - védettebb, mint a nyílt internet
 - nincs nyilvános IP cím
- Miért SIM chip?
 - a chipen nehezen másolható azonosító van: az IMSI
- Miért roaming?
 - A szolgáltatók lefedettsége nem egyforma
 - A cél, hogy minél több helyen működjön a szolgáltatás
 - Az egyik szolgáltató esetleges műszaki hibája esetén a másik szolgáltatókon is működik a szolgáltatás



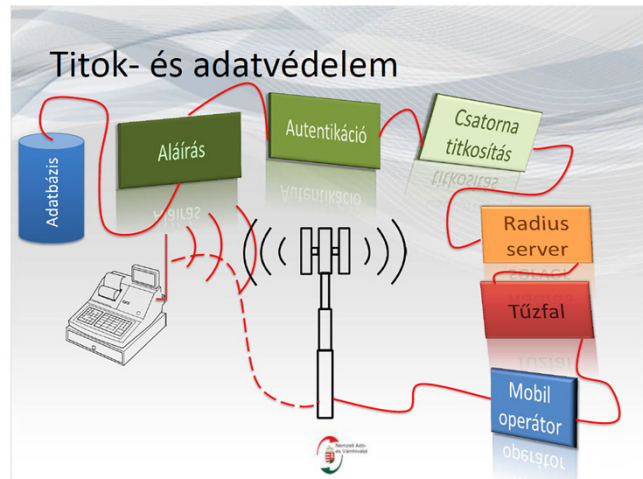
Magyar megoldás - Adatkapcsolat

- És ha nincs lefedettség?
 - Időnként
 - biztonságos helyi tárolás
 - Állandóan
 - off line jelentés (<100 felmentési kérelem)
 - Nincs térrő: NMHH szakvéleményre, 1 év felmentés
 - Ilyenkor havi adatszolgáltatás, revízió



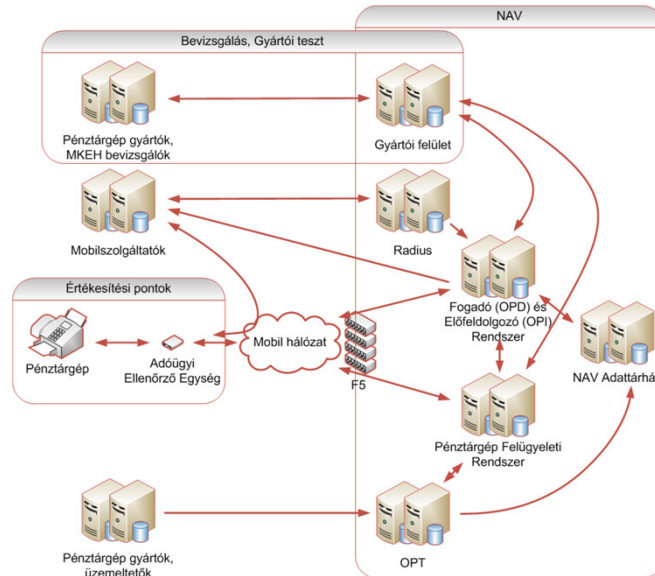
Magyar megoldás - Biztonság

- Boltok közötti mozgatás kiküszöbölése:
 - Cellainformációk küldése
 - Térerő, hőmérséklet, gyorsulás adatok küldése
 - A PG kikapcsolt állapotában is minimum 48 óráig működik az AEE, 46 óra után is képes 2 óra folyamatos kommunikációra
 - Adatbányászat a petabájtos tárolóban (szakmánkénti séma-illesztés, hazai és EU-s áfa adatokkal és vámadatokkal összevetés, kereskedelmi láncok,
 - „deviáns” géptípusok kiszűrése, szoftvereik auditálása



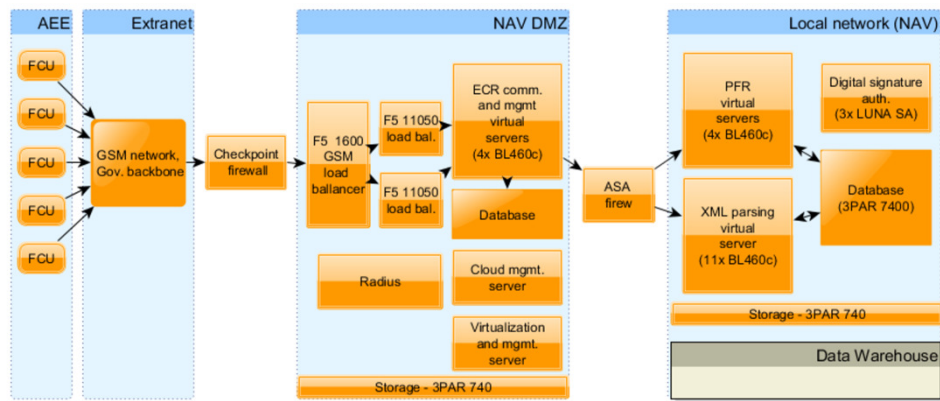


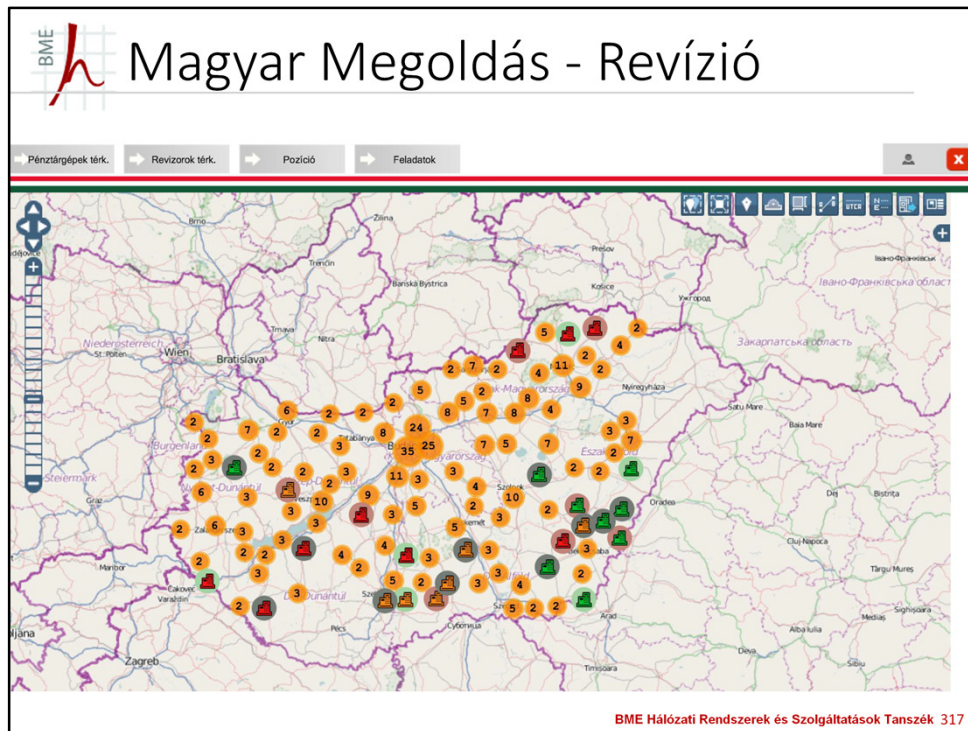
Magyar megoldás - Architektúra





Magyar megoldás - Architektúra





Térképen kereshetők az online pénztárgépek és a revizorok is.
Színkódokkal van jelölve, hogy melyik pénztárgép milyen aktivitást mutat.





esemény, küldendő üzenet leírása	üzenet tartalom	URL ahová az üzenet küldendő	NAV	AEE
30 perces jelzés	TRMRDY-XXXXXXXXXX-S-N-T	https://opg.nav.gov.hu/msg		
Firmware update fogadásra felszólítás	FRWUPD-ééééhnnóópmm-HHHHHHHHHH			
Firmware update fogadásra kész (YY:05)	ANS-XXXXXXXX-YY-HHHHHHHHHH	https://opg.nav.gov.hu/swu		
szoftver update	UPDDL-NN-CCCC			
szoftver update darabok	UPDREQ-NN-XXXXXXXXXX	https://opg.nav.gov.hu/swu		
Firmware részlet update küldése	firmware fáj darab			
Firmware update letöltve (YY:06)	ANS-XXXXXXXX-YY-HHHHHHHHHH	https://opg.nav.gov.hu/swu		
nyugta (YY:04)	ACK-YY-HHHHHHHHHH			
Firmware update végrehajtva (YY:07)	ANS-XXXXXXXX-YY-HHHHHHHHHH	https://opg.nav.gov.hu/swu		
nyugta (YY:04)	ACK-YY-HHHHHHHHHH			

BME Hálózati Rendszerek és Szolgáltatások Tanszék 320

Biztonsági okokból a firmware frissítés is csak a NAV rendszerén keresztül történik, mivel harmadik fél által történő frissítés esetén előfordulhatna, hogy módosított szoftver kerül fel a készülékre



Pénztárgép szoftver frissítés folyamata

- Az UPDDTL~NN~CCCC : üzenetben az „~NN” a küldendő összes üzenet száma
- Ezt követi a „~CCCC” ami a firmware-fájl minden szeletére számított CRC értékek sorozata
- Végül a teljes firmware SHA256 algoritmussal készített ellenőrző kódja 64 karakteren
- Az AEE egység a szeletek számának ismeretében folyamatosan elkéri a NAV szerverétől a UPDREQ üzenettel a soron következő szoftverszelet darabot
- Az utolsó szelet megérkezését követően ANS (YY:06) választ küldi a NAV szerverének a sikeres fogadást követően
- A frissítésre átadott firmware fájl csak egy fájlból állhat. A firmware fájl nevének az alábbiak szerint kell összeállnia. A999_T9_V9999.BIN ahol, A999 megegyezik a pénztárgép AP számának első négy karakterével.
- T9 a firmware típusa ami jelen szabályok szerint, csak egy lehet így T1, a V9999 a firmware szigorúan növekvő verziószáma
- Pl. A001_T1_V0001.BIN
- A NAV a AEE irányába küldött firmware szeleteket A001_T1_V0001.BIN_S01-től A001_T1_V0001.BIN_S99-ig azonosítja

BME Hálózati Rendszerek és Szolgáltatások Tanszék 321

Az AP szám az adóügyi ellenőrző egység egyedi azonosító száma



Pénztárgép üzembehelyezési folyamata

esemény, küldendő üzenet leírása	üzenet tartalom	URL ahová az üzenet küldendő	NAV	AEE
Regisztrációs fájl küldése (nem autentikálva)	(fájlnév benne üzembehelyezési kód)	https://opgreg.nav.gov.hu/reg	←	
válasz elutasítás esetén (YY: értékét lásd táblázat alatt)	ACK-YY-#####		→	
válaszok befogadás esetében: 1. adózi törzsadatok (P1n, n=1)	DEFUPD-XXXXXXXX-P1n-P2n-P3n-P4n-P5n-P6n-P7n-P8n-#####		→	
Adózi törzsadatok frissítése (YY:08)	ANS-XXXXXXXX-YY-#####	https://opgreg.nav.gov.hu/msg	←	
válaszok befogadás esetében: 2. üzemeletési telephely adatok (P1n, n=3)	DEFUPD-XXXXXXXX-P1n-P2n-P3n-P4n-P5n-P6n-P7n-P8n-#####		→	
Adózi törzsadatok frissítése (YY:08)	ANS-XXXXXXXX-YY-#####	https://opgreg.nav.gov.hu/msg	←	
autentikációs tanúsítvány letöltése	privát kulcs (priv fájl)		→	
Tanúsítványok frissítése (YY:09)	ANS-XXXXXXXX-YY-#####	https://opgreg.nav.gov.hu/msg	←	
autentikációs tanúsítvány letöltése	tanúsítvány (cer fájl)		→	
Tanúsítványok frissítése (YY:09)	ANS-XXXXXXXX-YY-#####	https://opgreg.nav.gov.hu/msg	←	
válaszok befogadás esetében: 4. kévváltoztató adózi törzsadatok (P1n, n=2)	DEFUPD-XXXXXXXX-P1n-P2n-P3n-P4n-P5n-P6n-P7n-P8n-#####		→	
Adózi törzsadatok frissítése (YY:08)	ANS-XXXXXXXX-YY-#####	https://opgreg.nav.gov.hu/msg	←	
3. vagy 4. küldés ANS válasz után nyugta (YY:04)	ACK-YY-#####		→	
Visszajelentkezés már autentikálva	TRMRDY-XXXXXXXX-S-N-T	https://opg.nav.gov.hu/msg	←	
Nyugta	(AQX-YY-#####)		→	

BME Hálózati Rendszerek és Szolgáltatások Tanszék 322



Pénztárgép üzembehelyezési folyamata

- 3. lépésben a NAV elküldi a az AEE autentikációs tanúsítványát két külön fájlban, melyből az első a privátkulcsot, a második a tanúsítványt fogja magába foglalni. Az AEE-nek külön mindkettőt ANS-09-es üzenettel kell nyugtáznia
- Az AEE egységneknek lévő kriptográfiai chipnek FIPS 140-2 szabvány szerinti EAL3 értékeléssel kell rendelkeznie: célja a privát kulcs védelme, exportálhatatlansága
- Az eszköz élettartama alatt a tanúsítványok nem fognak lejárni

BME Hálózati Rendszerek és Szolgáltatások Tanszék 323

Az AEE eszközzel szemben elvárás, hogy a kriptográfiai funkciók (rejtjelezés, hitelesítés, kulcstárolás) megvalósításában legalább olyan biztonsági modulra támaszkodjon, amelynek áramköri (chip) szinten FIPS 140-2 szabvány szerint kétszintű vagy commoncriteria EAL3 szintű értékeléssel rendelkezik



FIPS 140-2

- Federal Information Processing Standard (FIPS) Publication 140-2
- USA kormányzati biztonsági szabvány kriptografikus modulok akkreditálására
- Szoftveres és hardveres követelményeket is tartalmaz
- 4 szintet definiál





FIPS 140-2 szintek

- 1. szint: hardveres követelményt nem tartalmaz, csupán egy jóváhagyott algoritmus használatát írja elő. Az 1-es szintnek egy PC is megfelel
- 2. szint: fizikai védelmet is előír, a privát kulcsokhoz csak fizikai sérülés okozásával lehet hozzáférni (pl. plomba, zárható tok, ház)
- 3. szint: további hardveres védelmet ír elő annak érdekében, hogy a támadó ne férhessen hozzá a privát kulcsokhoz. Ezen védelmek lényege, hogy a hozzáférési kísérletet nagy eséllyel észleljék és arra reagáljanak (pl. semmisítsék meg az érzékeny adatokat)
- 4. szint: a legmagasabb biztonsági szint, minden kulcs hozzáférési kísérlet esetén azonnal meg kell azokat semmisíteni



Technológiák

- ECR: Electronic Cash Register
- EFP: Electronic Fiscal Printer
- ESD: Electronic Signature/Sales Device
- SCD/SCU/SCM: Sales Control {Device | Unit | Module}



ECR

- Elektronikus pénztárgép (általában PC alapú)
- Csatlakoztatható hozzá
 - Mérleg
 - Vonalkód olvasó
 - POS terminál
- Adóhatóság felé történő online kommunikációt nem valósít meg



ETR

- Az ECR-hez képest ez tartalmaz egy nem törölhető tárolót az adóügyi adatok tárolására
- A tárolt adatokhoz csak az illetékesek (pl. adóhatóság) férhet hozzá.
- Offline változat: helyben tárolja az adatokat és csak a helyszínen lehet letölteni az adóügyi adatokat
- Online változat: a napló állományokat távolról is le lehet kérdezni illetve rendszeresen elküldeni a hatóságnak.



EFP

- Nagyobb áruházláncok által használt PC-s kasszák esetén a nyomtatóba építik az adóügyi rögzítő egységet
- Egy drága rendszer esetén olcsóbb megoldás, hogy csak a nyomtatót kell cserélni



ESD

- Egy olyan eszköz, ami egyedi aláírást szolgáltat egy nyugtához.
- Az aláírás a nyugta tartalmától függ, abban bármi változás más aláírást eredményez
- Az aláírás egy hexadecimális hash érték
- Az ESD általában hálózaton kapcsolódik a rendszerhez
- Az aláírást a gépen is tárolják, így később ellenőrizhető.

123456789 123456789 123456789 123456789

ELADÓ CÉG NEVE	
ELADÓ CÉG SZÉKHELYE	
ÜZLET NEVE	
ÜZLET CÍME	
ELADÓ CÉG ADÓSZÁMA	
----- NYUGTA -----	
UTIKÖNYV	1 115
A00	
SZÁLLÁSI	1 234
C00	
1,234 kg * 1000 Ft/kg	

ÖSSZESEN:	2 349 Ft
KÉSZPÉNZ:	2 500 Ft
VISSZAJÁRÓ:	150 Ft
KEREKÍTÉS:	1 Ft
KÖSZÖNJÜK, HOGY NÁLUNK VÁSÁROLT!	
NYUGTASZÁM:	1234-00001
2011.01.15.	11:15
NAV Ellenőrző kód: ABC09	
Van NAV	AP XXXXXXXX
Ellenőrző kód	Van AP szám

BME Hálózati Rendszerek és Szolgáltatások Tanszék 330



SCD/SCU/SCM

- Nagy áruházak sok pénztárgépből álló rendszere esetén egy központi egység, amihez több pénztárgép kapcsolódik
- A magyar Központi kommunikációs egység ezt a funkciót látja el



Külföldi megoldások

- A világon még nem terjedt el széles körben, de találunk számos példát a környező országokban.
- Először Görögországban vezették be 1988-ban, de csak a kereskedelem egy szűk körére.
- Európa
 - Görögország, Románia, Bulgária, Koszovó, Montenegro, Moldova, Svédország, Horvátország
- Egyéb: Dél-Korea, Mexikó, Dominika, Panama, Argentína, Brazília, Chile, Paraguay, Kenya, Tanzánia, Ruanda

BME Hálózati Rendszerek és Szolgáltatások Tanszék 332

<http://www.imf.org/external/pubs/ft/wp/2015/wp1573.pdf>



Külföldi megoldások - Horvátország

- 2013-ban került bevezetésre
- Minden tranzakciós az adóhatóság szerverének kell jóváhagyni, csak ezt követően nyomtatható ki
- Internet kapcsolat szükséges, de nincs kikötve, hogy vezetékes vagy mobil
- Egy pénztárgép 5 évre kap tanúsítványt, ezt követően meg kell újítani
- A vásárlóknak lehetősége van a számla sorszáma alapján ellenőrizni annak valóságát, ezért a vásárlók jutalmakat kaphatnak (sorsolás útján)
- Kapcsolódási problémák esetére kidolgoztak egy megoldást:
 - A számla az adóhatóság jóváhagyó kódja (JIR) nélkül kerül kinyomtatásra, de tartalmaznia kell egy erre a célra rendszeresített biztonsági kódot.
 - Két napos határidő van ilyenkor a nyugta utólagos jóváhagyására

BME Hálózati Rendszerek és Szolgáltatások Tanszék 333

<http://www.fiscalization.hr/en/questions-and-answers>

Raktári alkalmazások, RFID rendszerek



Azonosítási módszerek

Tudás

- Jelszó
- PIN- kód

Birtok

- Kulcs
- Vonalkód
- Mágneskártya
- Chipkártya
- Smart card
- **RFID**

Biometria

- Hang
- Ujjlenyomat
- Arc
- Írisz
- Retina



Történeti áttekintés – a kezdetek

- Hadiipari alkalmazással kezdődött
 - A II. világháborúban a britek kifejlesztették a radart
 - Sir Robert Alexander Wattson-Watt
 - A radar kiegészítése azonosítással
 - IFF – Identification Friend or Foe
- Harry Stockman, "Communication by Means of Reflected Power" (visszavert hullámokon alapuló kommunikáció) 1948



Történeti áttekintés – kereskedelmi alkalmazások

- Kereskedelmi alkalmazások
- Sensormatic → EAS – Electronic Article Surveillance
 - 1 bites tag (olcsó és könnyen használható)
 - Nehezen terjedt el
 - Megalapozta az RFID elterjedését
- *Matt Lezin és Tom Wilson* üvegkapszulába ágyazott RFID-t „épít be” szarvasmarhába az 1970-es években



BME Hálózati Rendszerek és Szolgáltatások Tanszék 337

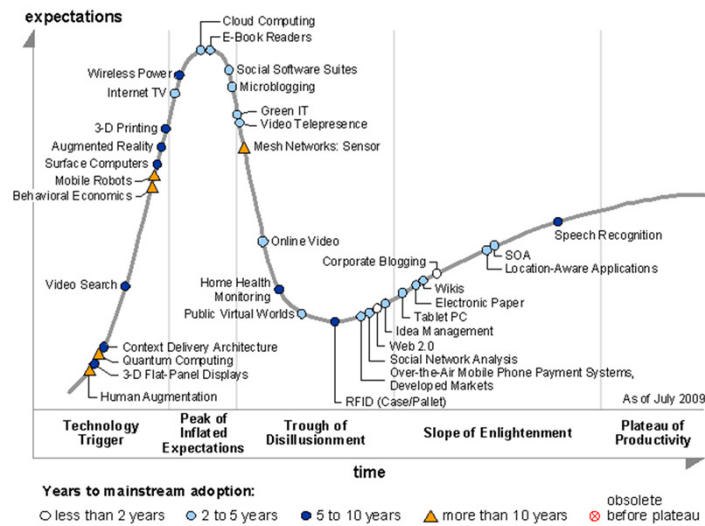


Történeti áttekintés – kereskedelmi alkalmazások

- Logisztika
- Útdíj (mikrohullámú és induktív csatolású)
- Beléptetés
- Texas (TIRIS)
- Walmart
- UHF RFID lendülete: Auto-ID
 - Uniform Code Council, az EAN International, a Procter & Gamble és a Gillette
 - Csak egy szám a tag-ben (olcsóbb)
- EPC számozási eljárás: Uniform Code Council + EAN International → EPCglobal



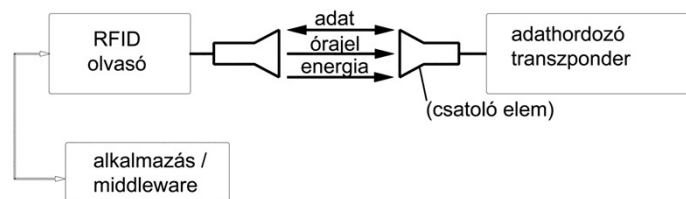
Történeti áttekintés





RFID rendszer felépítése

- Transzponder, mely az azonosítani kívánt objektumon helyezkedik el
- Olvasó, mely olvasni és/vagy írni is képes a transzpondert
- Háttér infrastruktúra





RFID rendszerek osztályozása



LF rendszerek (<135 kHz)

- induktív csatolás, kis távolság
- Legelterjedtebbek (technológia kiforrott)
- Legkevésbé nyelődik folyadékokban, illetve fémekben

HF rendszerek (13,56 MHz)

- induktív csatolást és kapacitív csatolást használók is
- kicsi, vagy közepes olvasási távolság
- Jól áthatolnak a fémes anyagokon és folyadékokon
- Smart card

UHF rendszerek (EU: 868 MHz, USA 915 MHz)

- Kapacitív csatolás
- nagy olvasási távolsággal és gyors adatátviteli-sebességgel rendelkeznek
- sok tag olvasása esetén is megfelelő megoldás
- az IC technológia fejlődése révén az LF és HF tag-eknél olcsóbbak

Mikrohullámú rendszerek (2,45 GHz; 5,8 GHz)

- hasonló olvasási tulajdonságokkal rendelkeznek, mint az UHF
- még gyorsabb adatátviteli-sebesség
- fém és folyadékok közelében ezek olvasási sebessége csökken leginkább



RFID rendszerek osztályozása

Frekvencia	Előnyök	Hátrányok	Alkalmazási területek
Alacsony (9-135 kHz)	Legelterjedtebb változat Fémes környezetben is működőképes	1,5 méternél kisebb olvasási távolság Nem EPC szabványos	Allatazonosítás Könyvtári nyilvántartás
Magas (13,56 MHz)	Jelenleg is elterjedt Nedves környezetben is működik		Raklapazonosítás Betegazonosítás Reptéri alkalmazások
Ultra magas (300-1200 MHz)	1,5 méternél nagyobb olvasási távolság Nedves környezetben is működőképes Növekvő elterjedés	Elnyelődés veszélye Japánban nem használható	Jármű nyomonkövetés
Mikrohullám (2,45, vagy 5,8 GHz)	1,5 méternél nagyobb olvasási távolság		Járműbeléptetés

BME Hálózati Rendszerek és Szolgáltatások Tanszék 342

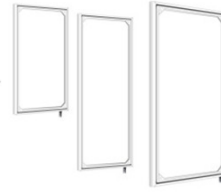


Fizikai környezet hatásai

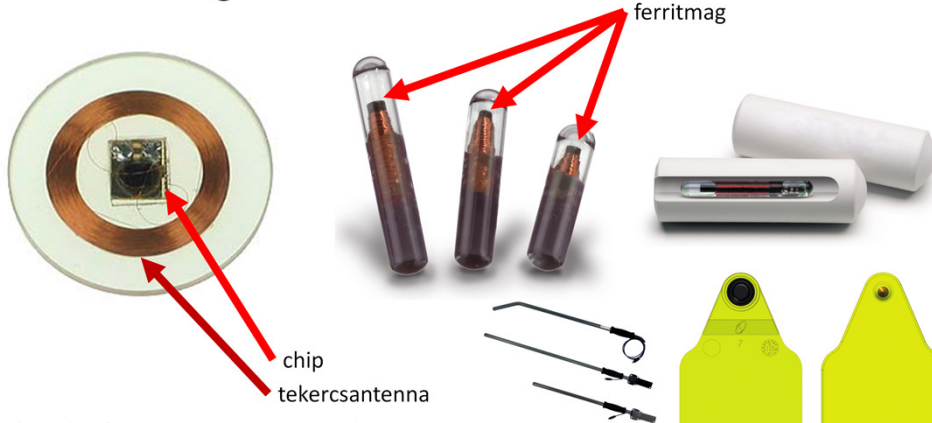
Anyag \ Frekv.	LF	HF	UHF	Mikrohullám
Ruházat	Áthatol rajta	Áthatol rajta	Áthatol rajta	Áthatol rajta
Száraz fa	Áthatol rajta	Áthatol rajta	Áthatol rajta	Elnyelődik
Grafit	Áthatol rajta	Áthatol rajta	Visszaverődik	Visszaverődik
Folyadékok (ált.)	Áthatol rajta	Áthatol rajta	Elnyelődik	Elnyelődik
Fémek (fólia)	Áthatol rajta	Áthatolhat	Visszaverődik	Visszaverődik
Motorolaj	Áthatol rajta	Áthatol rajta	Áthatol rajta	Áthatol rajta
Papír termékek	Áthatol rajta	Áthatol rajta	Áthatol rajta	Áthatol rajta
Műanyagok (ált.)	Áthatol rajta	Áthatol rajta	Áthatol rajta	Áthatol rajta
Sámpón	Áthatol rajta	Áthatol rajta	Elnyelődik	Elnyelődik
Víz	Áthatol rajta	Áthatol rajta	Elnyelődik	Elnyelődik
Nedves fa	Áthatol rajta	Áthatol rajta	Elnyelődik	Elnyelődik



LF tagek és antennák



- A tagekben lévő antenna jellemzően lég- vagy ferritmagra tekercselt rézvezeték



Képek forrása: Datamars, Futurlec, rfidcanada

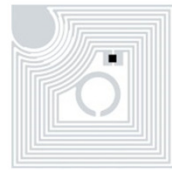
BME Hálózati Rendszerek és Szolgáltatások Tanszék - 344



HF tagek és antennák



- Kisebbs menetszámú tekercsek
- Jellemzően légmaggal



Képek forrása: rfidcanada

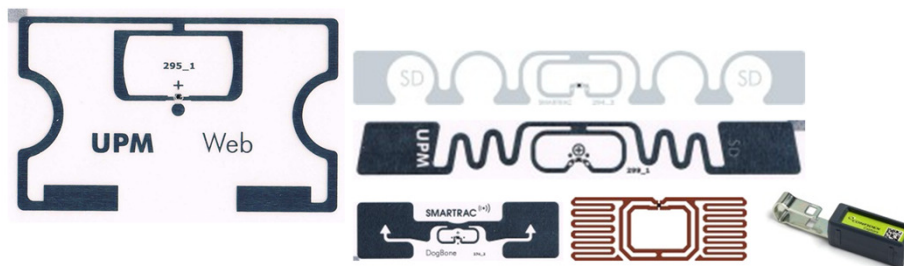
BME Hálózati Rendszerek és Szolgáltatások Tanszék 345



UHF tagek és antennák



- Patch és dipól antennák
- Lehet tekercs, egy menetes tekercs:
 - Near-field olvasáshoz



Képek forrása: rfidcanada

BME Hálózati Rendszerek és Szolgáltatások Tanszék 346



RFID működési módok

- Aktív – önálló energiaellátás (például telep)
- Félpaszív – önálló energiaellátás, de a kommunikáció a passzív rendszereknél megszokott
- Passzív – a működéséhez szükséges energiát az olvasótól kapja



Kitérő: NFC

- Near Field Communication
- HF (13,56 MHz) rádiós kommunikáció
- Körülbelül maximum 10 cm távolság
- ISO 18000-3 RFID szabvány
- 106 – 424 kb/s adatátviteli sebesség
- Két működési mód
 - Aktív
 - Mindkét résztvevő fél áramforrással kell, hogy rendelkezzen
 - Felváltva adás
 - Passzív



Kitérő: NFC

- Fizetési rendszerek
 - Google Wallet
- Egyszerűbb konfiguráció
 - Bluetooth, WLAN
- RFID- tól örökölt lehetőségek
- NDEF – NFC Data Exchange Format
 - URI-k, MIME-type-pal rendelkező adatok átvitele



RFID a logisztikában

- Nagy tömegű áru mozgásának követése
- Helymeghatározás
- Áru eredetiségének ellenőrzése
- Az árut a szállítás során ért hatások rögzítése



Kép forrása: CAEN RFID S.r.l.

BME Hálózati Rendszerek és Szolgáltatások Tanszék 350



RFID és vonalkód

Vonalkód

- Optikai rálátást igényel
- Egyszerre egy vonalkód olvasható le
- Általában termékcsoportot jelöl a kód
- Viszonylag kis mennyiségű adatot tárol (kivéve pl. QR-kód)
- Olcsó címke
- Érzéketlen a hordozó felület anyagi minőségére (általában)
- Egymáshoz közeli leolvasók nem zavarják egymást
- Egyszer írhatók



RFID

- Nem szükséges optikai rálátás
- „Egyszerre” több RFID is leolvasható
- A kód konkrét példányt jelöl
- Nagy mennyiségű adat tárolása is lehetséges
- Egy címke költsége magasabb, mint a vonalkód
- Különböző felületekre különböző címke alkalmas
- Egymáshoz közeli leolvasók zavarhatják egymást
- Újraírhatók lehetnek



BME Hálózati Rendszerek és Szolgáltatások Tanszék 351

A vonalkód jelentéssel bír; szövege: aki a felévben először megfejt, ZH + 5%



RFID a logisztikában – tétel szintű azonosítás

- Nagy mennyiségű RFID címke leolvasása szükséges az azonosítási pontokon
- A címkék jellemzően nem használhatók újra
- A nagy mennyiség miatt UHF technológia használata lehetséges
 - Olcsó címkék
 - Gyors adatátvitel, fejlett többes leolvasási protokoll
- Jól kezelhető, ha az azonosítandó termékek hasonlóak és csekély a víz-, illetve fémtartalmuk



RFID a logisztikában – raklap szintű azonosítás

- Egy-egy címke egy szállítási egységet jelöl
- A címke újrafelhasználható
- Nagyobb tolerancia a címkeárral kapcsolatban
- HF, UHF vagy WLAN megoldások is szóba jöhetnek

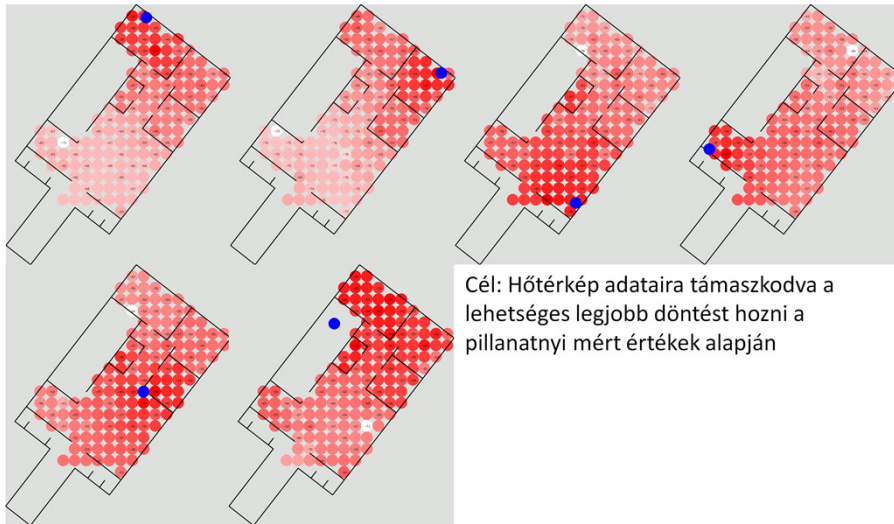


RFID a logisztikában – helymeghatározás

- Helymeghatározás szektorszinten
 - UHF – kapukkal
 - WLAN – jelerősség alapján
 - Sűrűbben elhelyezett AP-k, mint egy csupán adatátvitelre használt WLAN hálózat esetén
- Helymeghatározás valós időben
 - WLAN – jelerősség alapján
 - WLAN – TDoA (Time difference of arrival) elven
 - UWB (ultra-wideband) eszközökkel
 - Akár néhány centiméteres pontosság



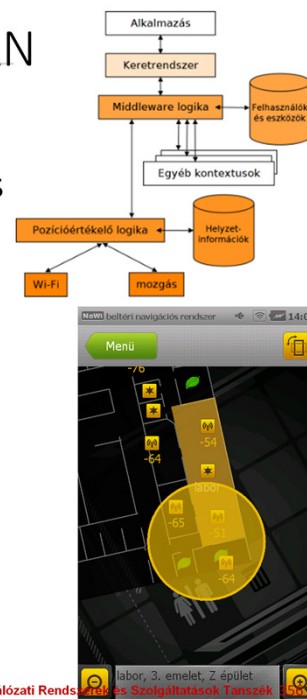
RFID a logisztikában – WLAN helymeghatározás



Cél: Hő térkép adataira támaszkodva a lehetséges legjobb döntést hozni a pillanatnyi mért értékek alapján

RFID a logisztikában – WLAN helymeghatározás – NaWi

- Beltéri WiFi helymeghatározás és navigációs keretrendszer
 - Felhasználók, eszközök
 - POIk, útvonalak
- Saját algoritmus
 - Előzetes felmérés
 - Hullámterjedés
 - Fizikai jellemzők
 - Mozgási jellemzők
- Szerver
 - Oracle, PHP, SOAP
- Kliens
 - Android 2.1, Windows Mobile 5.0
- BME MIK fejlesztés





RFID a logisztikában – könyvtár

- Speciális terület
- A jelölt termékek
 - Hasonlóak
 - Nem kerülnek ki tartósan a tulajdonos ellenőrzése alól
 - Rádiófrekvenciás szempontból általában könnyen kezelhetők
 - Vannak kivételek: audio-gyűjtemények, fémes borítójú könyvek
- Áruvédelmi igények is fellépnek



RFID a logisztikában – könyvtár

- A korábbi telepítésű rendszerek jellemzően HF-ek
 - Dán adatmodell
 - Példányok adatai a könyvekbe ragasztott címkéken
 - Szabványos megoldások
- Újabban UHF-re történő áttérés
 - Olcsóbb címke
 - Kevesebb adat a címkén, jellemzően csak egy kód
 - Áruvédelemre alkalmasabb
 - Rendkívül fiatal szabvány, a korábbi megoldások jellemzően egyediek, sokszor fontosabb az azokkal való kompatibilitás, mint a szabványnak való megfelelés



RFID a logisztikában – könyvtár

HF

- Az egész világon elterjedt
- Korán szabványosították
 - ISO15693, ISO28560-1/2/3
- Kis leolvasási távolság
- A vizes közeg (pl.: emberi test) kevésbé zavarja
- Drágább címkék

UHF

- Az egész világon elterjedt
- Viszonylag új szabvány
 - ISO18000-6C, ISO28560-4 (2014)
- Nagyobb leolvasási távolság
- A közeli tagek egymást árnyékoló hatása kevésbé jellemző
- Gyorsabb többes leolvasás
- A vizes közeg jobban zavarja

Forrás: Udvardy-Nagy István – Library – RFID

BME Hálózati Rendszerek és Szolgáltatások Tanszék 359



RFID a logisztikában – könyvtár

A bevezetés problémái

- Nagy mennyiségű címkézendő példány
- Nagy eltérések a forgási sebességekben
 - Pl.: egyetemi könyvtárban régi diplomatervek, szakdolgozatok és tantárgyhoz kapcsolódó kötetek
- Címkék elhelyezése a könyvekben
- Címkék tartalma:
 - Korábban is meglévő azonosító
 - Teljesen új, független azonosító



Képek forrása: Udvardy-Nagy István – Library – RFID

BME Hálózati Rendszerek és Szolgáltatások Tanszék 360



RFID a logisztikában – könyvtár

A bevezetés problémái

Címkézés meglévő azonosító használatával

- A meglévő azonosító a címkére írása
 - A helyszínen vagy előre gyártva
- Az RFID inlay a példányba ragasztása



Címkézés új azonosító használatával

- Az RFID inlay a példányba ragasztása
 - Előre gyártva
- A meglévő azonosító és az új azonosító összerendelése
 - A helyszínen
- Az összerendelés mentése az adatbázisba

Képek forrása: NordiClD

BME Hálózati Rendszerek és Szolgáltatások Tanszék 361



RFID a logisztikában – könyvtár Felhasználási lehetőségek

- Könyvek, folyóiratok azonosítása
- Automatikus azonosítás
 - Önkiszolgáló kölcsönzés
 - Önkiszolgáló visszavétel
- Keresés kézi RFID eszközzel



Képek forrása: Udvardy-Nagy István – Library – RFID

BME Hálózati Rendszerek és Szolgáltatások Tanszék 362



RFID a logisztikában – könyvtár

Bővítési lehetőségek

- Áruvédelem
- Könyvtárfelhasználók azonosítása RFID technológiával
 - RF smart card
 - NFC
- Automatikus szortírozás
- Olvasótermi statisztika



Képek forrása: Udvardy-Nagy István – Library – RFID

Smart metering, távleolvasás



A körülmények

- Közműszolgáltatások számlázása igénybevétel alapján
 - Víz és csatornadíj,
 - Villamosenergia-díj,
 - Gázdíj
 - Stb.
- A mérőórák bizonyos esetekben csak az ingatlanon belül helyezhetők el
- A leolvasás ebben az esetben körülményes, az ingatlan birtokosának hozzájárulását igényli



Motivációk

- Az elektromos energia tárolása nagy mennyiségben rövid távon sem megoldott
- Növekvő fogyasztás
- Növekvő árak
- Elektromos járművek megjelenése
 - Plug-in hybrid
- Egyre kiegyensúlyozatlanabb fogyasztás



Motiváció – példa

- Kovács úr villanyautójával reggel elmegy a munkahelyére
- Este ugyanezzel a járművel hazatér, majd az autót a hálózatra csatlakoztatja
- Este Kovács úron kívül még 500 000 dolgozó csatlakoztatja az autóját
- Az elektromos autók töltési ideje viszonylag magas, legalább egy-két óra, de potenciálisan rövidebb idő, mint ami rendelkezésre áll a következő indulásig
- Megoldható-e az, hogy a nagy számú fogyasztó egyenletes terhelést jelentsen a hálózatra?

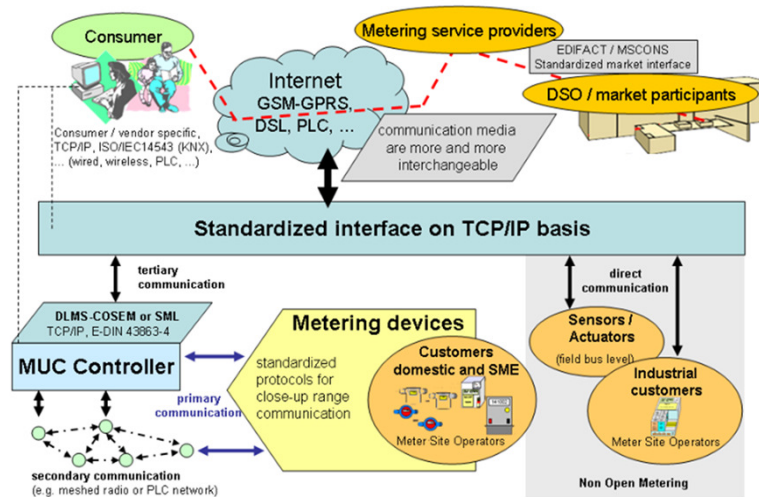


Smart metering eszközök

- Automatikus leolvasás
- Periodikus adatküldés a szolgáltatók felé
- Előnyök:
 - Rendszeres fogyasztásalapú számlázás
 - Adatküldési gyakoriságtól függően jól követhető fogyasztás
 - A leolvasáshoz nem szükséges személyes jelenlét a szolgáltató részéről
 - A leolvasáshoz nem szükséges együttműködés a felhasználó részéről



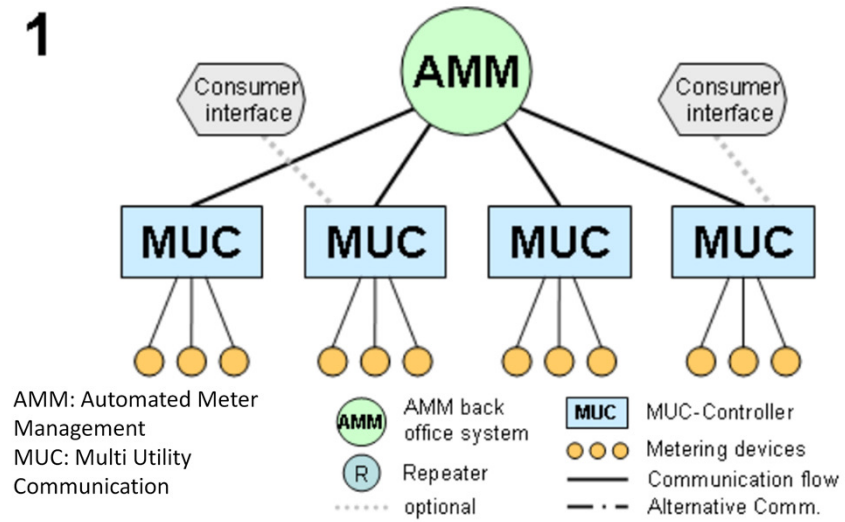
OMS – Open Metering System



Forrás: OMS Specification Volume 1 General Part v1.4.0

BME Hálózati Rendszerek és Szolgáltatások Tanszék 369

1



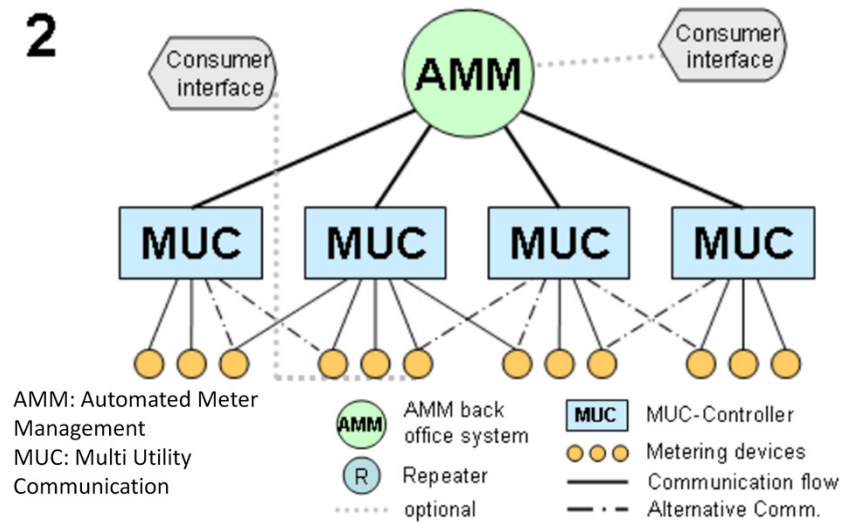
Forrás: OMS Specification Volume 1 General Part v1.4.0

BME Hálózati Rendszerek és Szolgáltatások Tanszék 370



OMS architektúra

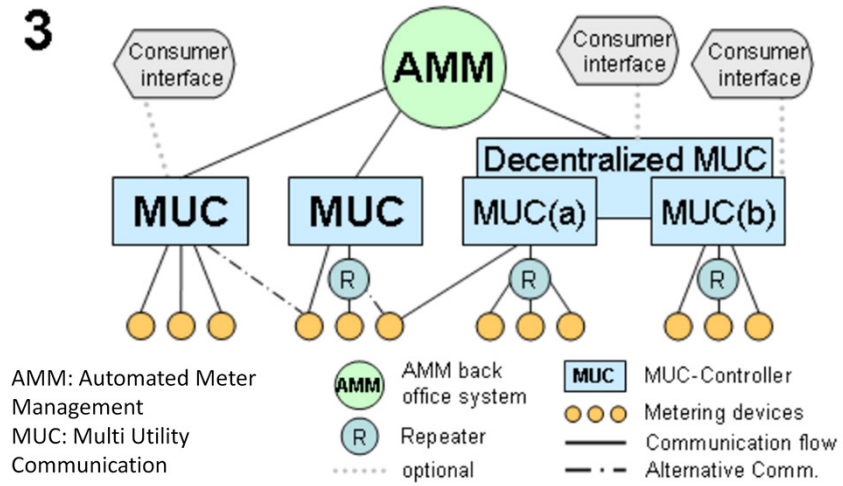
2



Forrás: OMS Specification Volume 1 General Part v1.4.0

BME Hálózati Rendszerek és Szolgáltatások Tanszék 371

3



Forrás: OMS Specification Volume 1 General Part v1.4.0

BME Hálózati Rendszerek és Szolgáltatások Tanszék 372



OMS AMM és MUC controller

- A MUC controller feladata az architektúrában a mérőeszközöktől származó fogyasztási adatok feldolgozása és az AMM felé történő továbbítása
- Az AMM vagy AMM BO (back-office) a mérési szolgáltatónál elhelyezett a mérési adatokat aggregáló, illetve az üzleti rendszerek felé továbbító rendszerek



OMS evolúció

- 1. generáció
 - Egyirányú kommunikáció mérőeszközök számára
- 2. generáció
 - Kétirányú kommunikáció támogatása
 - Repeater eszközök támogatása
 - A holland szabályozással történő harmonizáció
- 3. generáció
 - Szinkron adatküldés támogatása
- 4. generáció
 - Adatbiztonsági fejlesztések a német szabályozásoknak való megfelelés érdekében

Forrás: metering4all Issue 2

<http://oms-group.org/en/metering4all/oms-metering4all/>

BME Hálózati Rendszerek és Szolgáltatások Tanszék 374



OMS mérőeszközök

- A specifikáció szerint ezek kommunikálnak közvetlenül a MUC egységekkel az elsődleges interfészeken (primary interface) keresztül
- Szenzorok és aktuátorok
- A szenzorok mérőeszközök, amik legalább a mért számlálóérték közlésére képesek
- Az aktuátorok megszakítók vagy terhelést szabályozó egységek



OMS mérőeszközök

- Egyszerű mérő (basic meter)
 - A pillanatnyilag érvényes mérést vagy kérésre, vagy automatikusan, rendszeres időközönként elküldi
 - A küldött adat a helyi kijelzőn láthatóval megegyező
 - Hitelesítést nem igényel a hozzáférés (mivel csak olvasás történik)



OMS mérőeszközök

- Kifinomult mérő (sophisticated meter)
 - Egyszerű mérők plusz funkciókkal
 - Pl. a mért értékek mellett időbélyeget is tárolnak,
 - Beépített órával rendelkeznek
 - Egyszerű statisztikákra képesek
 - Mindig kétirányú a kommunikációjuk
 - A mérőállás kiolvasásán kívül a funkciók hitelesítést igényelnek
 - A mérőállást a kiolvasáskor az eszköz aláírja (ECC – elliptic curve cryptography)

Forrás: OMS Specification Volume 1 General Part v1.4.0

BME Hálózati Rendszerek és Szolgáltatások Tanszék 377



OMS mérőeszközök

- Aktuátor (actuator)
 - Valójában nem mérőeszköz
 - Fogyasztás korlátozását teszi lehetővé
 - Megszakítók, kapcsolók, szelepek stb.
 - Kétirányú kommunikációra képesek



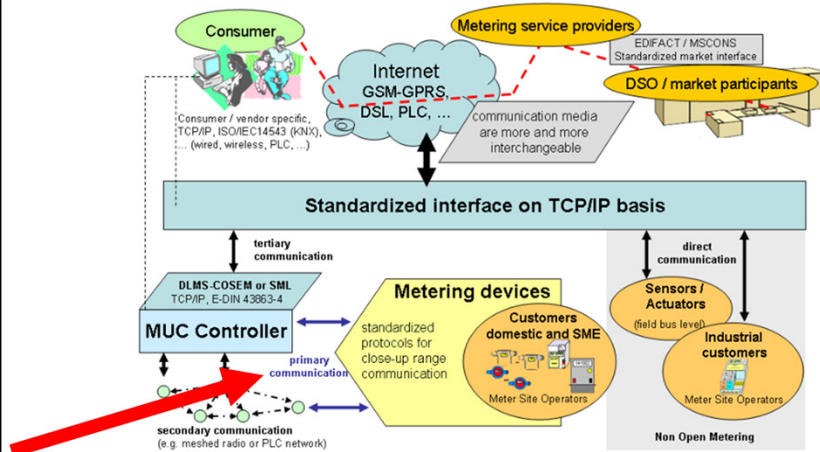
OMS mérőeszközök

- Repeater (repeater)
 - Valójában nem mérőeszköz
 - A kommunikációs csatorna hatótávját kiterjesztő eszköz
 - Lehetnek egyirányú kommunikációt támogató vagy kétirányú kommunikációt támogató repeaterek



OVS primary communication

- A mérőóra és a MUC közötti kapcsolat



Forrás: OVS Specification Volume 2 Primary Communication Part v3.0.1

BME Hálózati Rendszerek és Szolgáltatások Tanszék 380



OMS primary communication

- A fizikai réteg lehet kétvezetékes M-Bus vagy titkosított vezeték nélküli M-Bus (wM-Bus), a jövőben PLC (power line communication)
- M-Bus: Meter-Bus
 - Specifikusan a mérőeszközök kommunikációjára kidolgozott buszrendszer

The M-Bus logo is displayed in a large, bold, blue font. The 'M' is stylized with a thick, blocky appearance, and the 'Bus' is in a standard sans-serif font. A horizontal line underlines the 'Bus' part of the text.

Forrás: OMS Specification Volume 2 Primary Communication Part v3.0.1

Kép forrása: <http://www.mbus.com>

BME Hálózati Rendszerek és Szolgáltatások Tanszék 381



OMS primary communication – M-Bus

- EN13757-2 szabvány szerint
- Kétvezetékes rendszer
- Opcionálisan áramellátás is lehetséges
- A buszra köthető egységek számát a MUC gyártója határozza meg
- A minimális követelmények e tekintetben az M-Bus szabványban (EN13757-2) leírt mini master által teljesítendő
- A vezetékek tetszőlegesen felcserélhetők a slave-eknél
- A slave-ekben soros védőellenállás ($430\Omega \pm 10\Omega$) egy esetleges rövidzár esetén az áram korlátozása érdekében

Forrás: OMS Specification Volume 2 Primary Communication Part v3.0.1

BME Hálózati Rendszerek és Szolgáltatások Tanszék 382



OMS primary communication wM-Bus

- EN13757-4 szabvány szerint
- Egyszeri ismétlés repeater eszköz segítségével a hatótávolság kiterjesztése érdekében
- Multi-hop ismétlés nem engedélyezett
- 868-870 MHz-es ISM sávban
- 169,4 MHz-es ETSI 300 220-1 V2.4.1-ben definiált sávban
- wM-Bus S1, S2, T1 és T2 üzemmódok használhatók OMS rendszerekben

Forrás: OMS Specification Volume 2 Primary Communication Part v3.0.1

BME Hálózati Rendszerek és Szolgáltatások Tanszék 383



OMS primary communication wM-Bus

- S1 és T1 üzemmódok egyirányú adatátviteli szabványok
 - Egyszerű (basic) mérő igényeihez elegendő
 - Az S1 üzemmód esetén a 868MHz-es sáv használata esetén az EN13757-4 szabvány előírja, hogy a csatorna kitöltöttsége egy node-ra 0,02% lehet, azaz egy slave egy órában összesen 720 ms ideig küldhet

Forrás: OMS Specification Volume 2 Primary Communication Part v3.0.1

BME Hálózati Rendszerek és Szolgáltatások Tanszék 384



OMS primary communication wM-Bus

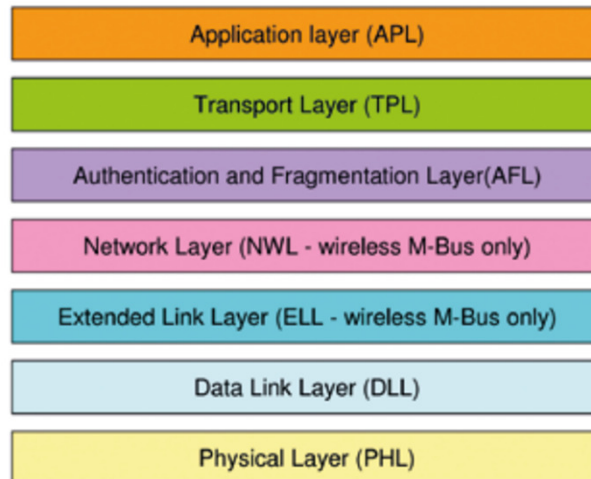
- Az S2 és T2 üzemmódok az S1 és T1 üzemmódok kiterjesztései kétirányú kommunikációhoz
 - Lehetséges a MUC → mérő irányú kommunikáció
 - Az S2 üzemmód esetén csak a long preamble támogatott
- Az egy keretben el nem férő üzenetek darabolása és összeillesztése alkalmazásrétegbeli feladat
- A telep kímélése érdekében gyakori megoldás, hogy a MUC → slave kommunikáció csak egy slave → MUC átvitelt követő rövid időablakban lehetséges, ez után a slave a rádiós modulját teljesen kikapcsolja

Forrás: OMS Specification Volume 2 Primary Communication Part v3.0.1

BME Hálózati Rendszerek és Szolgáltatások Tanszék 385



OMS protokoll stack



Forrás: metering4all Issue 3

<http://oms-group.org/en/metering4all/oms-metering4all/>

BME Hálózati Rendszerek és Szolgáltatások Tanszék 386



OMS szabványok

- EN 13757-1:2003: Communication system for meters and remote reading of meters - Part 1: Data exchange
- EN 13757-2:2004: Communication systems for and remote reading of meters - Part 2: Physical and link layer
- EN 13757-3:2004: Communication systems for and remote reading of meters - Part 3: Dedicated application layer
- EN 13757-3:2013: Communication systems for and remote reading of meters - Part 3: Dedicated application layer
- EN 13757-4:2005: Communication systems for meters and remote reading of meters - Part 4: Wireless meter readout (Radio meter reading for operation in the 868 MHz to 870 MHz SRD band)
- EN 13757-4:2013: Communication systems for meters and remote reading of meters - Part 4: Wireless meter readout (Radio meter reading for operation in SRD bands)
- EN 13757-5:2008: Communication systems for meters and remote reading of meters - Part 5: Wireless relaying
- EN 13757-6:2008: Communication systems for meters and remote reading of meters - Part 6: Local Bus

Forrás: <http://oms-group.org/en/standard-sources/>

BME Hálózati Rendszerek és Szolgáltatások Tanszék 387



Pillanatnyi helyzet Európában

- Az EU célkitűzése
 - 2020-ra a villamos fogyasztók legalább 80%-a okos mérővel legyen ellátva (2009/72/EC), ha a vonatkozó költség-haszon elemzés ezt indokolja
- Svédország (100%) és Olaszország (95%) jár élen az okos áramfogyasztás-mérők bevezetésében
- A bevezetés folyamatban Ausztriában, Dániában, Észtországban, Finnországban, Spanyolországban
- Az okos gázórák bevezetése folyamatban Olaszországban

Forrás: Council of European Energy Regulators – Status Review of Regulatory Aspects of Smart Metering

BME Hálózati Rendszerek és Szolgáltatások Tanszék 388

CBA államok szintjén – 2013 közepére nem mindenki adott le CBA-, a leadók kb. kétharmada adott le ilyen dokumentumot pozitív eredménnyel az elektromos áram vonatkozásában, kb. egyharmada a gázórák cseréjével kapcsolatban



Okos méréshez okos tarifák

- A megtakarítás érdekében ösztönözni kell az okos mérőkből származó adatokat felhasználva a fogyasztókat a tudatos energiafelhasználásra
- Példa:
 - Ingyenes villamosenergia-szolgáltatás hétvégén magasabb hétköznapi tarifával kombinálva mindenkinek megérheti
 - A fogyasztó a nagy áramfelvételű berendezések üzemeltetését hétvégére időzíti (mosógép, mosogatógép, vasaló stb.), ingyenes áramból üzemeltet
 - A termelőnél az erőművek optimális közeli terhelés mellett üzemelhetnek, egyenletesebb a terhelés a hálózaton



Okos méréshez okos tarifák

- Üresjáratok kihasználása
- Vezérelt módon
- Nem vezérelt, időzített módon
- Akár óránkénti felbontással



Együttműködés otthonautomatizálási rendszerekkel

- Az energiahatékonyságot növelni lehet, ha a szolgáltató tudja jelezni a háztartások felé, hogy mikor fogyasszanak
- Mai megoldás: vezérelt tarifa („éjszakai áram”), pl. bojlerekhez, hőtároló kályhákhoz

Mobil fizetési megoldások



Tartalom

- Emeltdíjas szolgáltatások
- Szolgáltatók saját megoldásai
- Mobil tárca
- NFC
- Mobilbank
- PayPal Here
- Jogi szabályozás



Emeltdíjas szolgáltatások

- Legnagyobb múltra visszatekintő megoldás
- Jelenleg még mindig a legelterjedtebb megoldás
- Típusai:
 - Emeltdíjas telefonhívás
 - Idő alapú
 - Kapcsolás alapú
 - SMS
 - MO SMS
 - MT SMS



Emeltdíjas telefonhívás

- Már vezetékes telefonoknál is működő fizetési módszer
- A havi telefonszámlából vagy a prepaid egyenlegből kerül levonásra a fizetendő összeg
- A telefon szolgáltató a jutalék (jellemzően 10-20%) levonása után fizeti ki a fizetett összeget.
- Az szolgáltatást kínáló általában nem a szolgáltatóval állnak közvetlen szerződésben, hanem közvetítő fizetési szolgáltatóval szerződnek



Emeltdíjas telefonhívás – idő alapú hívás

- Az adott emeltdíjas telefonszámnak van egy fix percdíja
- A számlázás másodperc alapon történik
- Ha pontos összeget akarunk beszélni, akkor nem ez a megfelelő megoldás
- Főbb alkalmazási területek:
 - Élő jós, horoszkóp szolgáltatás
 - Adományvonal
 - Tudakozó
 - Műszaki támogató vonal
 - Társkereső
 - Egyéb

BME Hálózati Rendszerek és Szolgáltatások Tanszék 396

Egyéb: pl. felnőtt tartalmak
https://www.telenor.hu/edsz_lista/



Emeltdíjas telefonhívás – kapcsolás alapú hívás

- Amint felvették a hívott oldalon a készüléket megtörténik az összeg levonása
- Nagyobb összegek gyors beszédésére alkalmas
- Az emeltdíjas SMS elterjedésével háttérbe szorult



Emeltdíjas SMS

- Jelenleg a legnépszerűbb fizetési mód kis összegű fizetésekre
- Típusai:
 - Mobile Originated
 - Mobile Terminated
 - SMS Chat
- A szolgáltatók magas részesedést kérnek a szolgáltatásért:
 - Az emeltdíjas szolgáltatást nyújtó csak az SMS értékének 50-65%-át (forgalom és díjsáv függően) kapja meg
 - A válasz SMS költségét és az emeltdíjas SMS fogadás (csak Vodafone) költsége is a szolgáltatást nyújtót terheli



Emeltdíjas SMS

- A szolgáltatást nyújtó az elküldött SMS-t általában HTTP GET üzenetben kapja meg
- A szolgáltató megkapja:
 - A küldő telefonszámát
 - Szolgáltatóját
 - Emeltdíjas számot, ahova az SMS-t küldte
 - SMS szövegét
 - Üzenet egyedi azonosítóját
- A válasz SMS szövegét erre a HTTP kérésre kell válaszként visszaadni.



Emeltdíjas SMS – Mobile Originated

- Ez a „hagyományos” emeltdíjas SMS
- Az elküldött SMS után vonódik le az ellenérték a számláról vagy az egyenlegről
- Az emeltdíjas szolgáltatónak 1 percen belül válasz SMS-t kell küldenie a felhasználónak
- 80 Ft-tól 4000 Ft-ig léteznek díjsávok
- Telefonszámok:
 - 06-90-XXX-XXX
 - 06-91-XXX-XXX (felnőtt tartalmak ki vannak zárva)
 - 17XX, 17XXX, 16XXX, 16XXXX

BME Hálózati Rendszerek és Szolgáltatások Tanszék 400

Ha a szolgáltató nem küld válasz SMS-t, akkor egyes szolgáltatók nem is vonják le a felhasználótól az összeget.



Emeltdíjas SMS – Mobile Terminated

- A fogadott SMS után kell fizetni
- A sok korábbi visszaélés miatt az alábbi szigorú szabályok alapján lehet igénybe venni:
 - Az ügyfél egy normál díjas SMS-ben elküldi a szolgáltatás kulcsszavát (és esetleg további paramétereket).
 - Üdvözlő SMS-t 3 percen belül vissza kell küldeni az ügyfélnek
 - A feliratkozás ugyanis csak abban az esetben történik meg, ha ez az üdvözlő SMS 3 percen belül megérkezik az ügyfél telefonjára
 - Az üdvözlő SMS-nek tartalmaznia kell:
 - Milyen gyakran fognak emeltdíjas SMS-t küldeni (napi, heti, havi)
 - Az SMS díja
 - Lemondási lehetőség (STOP szó elküldésével)
 - Az üdvözlő SMS nem tartalmazhat a szolgáltatással kapcsolatos tényleges tartalmat, illetve hirdetést, de a szolgáltatásra vagy annak jellegére való utalást igen.
 - Az üzenetből egyértelműnek kell lennie az ügyfél számára, hogy milyen szolgáltatásra regisztrált, hogy tévedés esetén azonnal lemondhassa azt
 - A feliratkozást követően 2 percig még nem küldhető emeltdíjas SMS



Emeltdíjas SMS – SMSChat

- A MO SMS szabályain lazítottak, nem kell 1 percen belül válasz üzenetnek érkeznie az elküldött SMS-re, elég azt 10 percen belül elküldeni.
- Ezzel a könnyítéssel alkalmassá válik a rendszer pl. társkereső szolgáltatóknak arra, hogy ezen keresztül tudjanak a felhasználóik egymással kommunikálni
- Pl. user1 és user2 felhasználói az adott társkereső oldalnak. User1 szeretne user2-vel csevegni:
 - User1 elküld egy emeltdíjas SMS-t a társkereső szolgáltató számára olyan formában, hogy az üzenet első szava (prefix) tartalmazza, hogy minek szeretné az üzenetet küldeni:
user2 Szia!
 - A szolgáltató megkapja a „user2 Szia!” SMS-t, amit egy alapidíjas SMS-ben (feladónak az emeltdíjas szám fog szerepelni) elküld user2 telefonjára.
 - User2 elküldi a válaszát hasonló módon, amit user1 fog megkapni



Emeltdíjas SMS – SMSChat

- A példa második lépésében user2-nek egy olyan alapidíjas SMS-t küldünk, aminek a feladója egy emeltdíjas szám
- Ezzel korábban többen visszaéltek, ezért szigorítottak az emeltdíjas feladóval kiküldött SMS-ek szabályán:
 - Ha az elmúlt 48 órában nem érkezett SMS az adott telefonszámról, akkor csak egy ún. Feliratkozás után küldhető neki SMS
 - A feliratkozás azt jelenti, hogy pl. egy weboldalon bekéri a felhasználó nevét, telefonszámát és mobil szolgáltatóját.

BME Hálózati Rendszerek és Szolgáltatások Tanszék 403

Egyes szolgáltatók ezt a feliratkozási rendszert sem fogadják el, náluk nem küldhető úgy SMS a felhasználónak, hogy előtte nem jött tőle 48 órán belül SMS.



Szolgáltatók saját megoldásai

- A szolgáltató az előfizető számlája/egyenlege egyszerűen meg tudja terhelni
- Nincs szükség közvetítő szolgáltatóra, nincs igazán költsége sem a tranzakciónak
- Jellemző szolgáltatások:
 - Mobil parkolás
 - Autópálya matrica
 - Lottó, totó
 - Újság előfizetés
 - Buszjegy, vasúti menetjegy
 - Színház és rendezvényjegy

BME Hálózati Rendszerek és Szolgáltatások Tanszék 404

<http://www.telekom.hu/mobil/lakossagi/tarifak/szolgáltatások/mobilvasarlas/mobilvasarlas>



Szolgáltatók saját megoldásai

- A fizetés indítása történhet alapdíjas SMS küldésével vagy USSD kódok segítségével
- Mivel csak a szolgáltató nyújtja ezen szolgáltatásokat, ezért azok köre limitált
- Nincs lehetőség harmadik fél bevonására kedvező jutalék mellett
- A felhasználót terheli az elküldött alapdíjas SMS költsége (ha nem USSD kódon keresztül történik a szolgáltatás igénybevétele)

BME Hálózati Rendszerek és Szolgáltatások Tanszék 405

Az emeldíjas SMS tulajdonképpen a harmadik fél bevonására egy megoldás, de a magas jutalékok miatt csak kis összegű fizetésre használható



Mobil tárca

- Egy virtuális számlán keresztül történik a fizetés
- Ez a számla lehet:
 - Egy hozzárendelt bankkártya
 - Átutalással, egyéb befizetéssel előre feltöltött számla
- A fizetés egy mobil alkalmazásban történik
- Általában egy QR kódot kell beolvasunk a telefon kamerájával, majd a mobil tárca alkalmazásban azt jóváhagyni
- A fizetés történhet alapidíjas SMS elküldésével



Mobil Tárca - Népszerű szolgáltatások



BME Hálózati Rendszerek és Szolgáltatások Tanszék 407



Mobil Tárca - PayU

- Bankkártya alapú fizetés mobil alkalmazás segítségével
- Az alkalmazás segítségével bármely bankkártyájának felhasználásával teljesítheti elektronikus kifizetését
- Dijnet.hu közüzemi számlák kifizetési QR kód segítségével



BME Hálózati Rendszerek és Szolgáltatások Tanszék 408



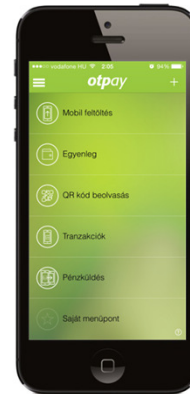
Nemzeti Mobilfizetési Zrt.

- Parkolás, autópálya matrica, HU-GO útdíj fizetése
- Prepaid rendszerben előre fel kell tölteni az egyenlegünket (pl. átutalás)
- SMS üzenettel indítható és állítható le a parkolás illetve vásárolható az autópálya matrica
- A vásárlás a feltöltött egyenleg terhére történik
- A mobil alkalmazás segít az SMS elküldésében (GPS alapján meghatározza a parkolási zónát és a hozzá tartozó telefonszámot)



OTPay

- Az OTPay a magyarországi bankok által kiadott MasterCard, VISA és American Express bank- és hitelkártyákkal használható alkalmazás
- Eltárolja legalább egy bankkártyája adatait, és utána a telefon segítségével a kártyához tartozó számláról tud tranzakciókat indítani
- Használható:
 - Mobilegyenleg feltöltésre
 - Pénz küldés másoknak (csak OTP ügyfelek között)
 - Fizetés webáruházakban, egyes éttermekben



BME Hálózati Rendszerek és Szolgáltatások Tanszék 410



Mastercard Mobile

- MasterCard, a Cellum Csoport, a T-Mobile, a Telenor és az FHB Bank együttműködésével valósult meg
- QR-kód lefotózásával fizethetjük ki közüzemi és telekommunikációs számláinkat, rendezhetjük a taxiszámlát, és alapítványoknak küldhetünk adományt
- Feltölthetjük mobiltelefon- vagy fesztiválkártyáinkat
- Egyes webáruházakban is fizethetünk



BME Hálózati Rendszerek és Szolgáltatások Tanszék 411



NFC

- Near Field Communication
- Ugyanúgy tudunk kommunikálni egy Javacard alkalmazással, mint egy chipes bankkártya esetén
- Megvalósítható vele többek között fizetés is.
- Számos felső és középkategóriás telefon rendelkezik már NFS chip-pel
- Sajnos nem minden operációs rendszeren van API az NFC-hez (iOS-nél nincs)



NFC komponensek

- Javacard: A ma használt sim kártyák és chipes bankkártyák mind javacard-ok, java-ban lehet alkalmazásokat fejleszteni.
- Secure element: a telefon sim kártyája rendelkezik egy olyan interfésszel, aminek segítségével egy mobil alkalmazás meg tud hívni egy, a sim kártyán tárolt alkalmazást
- Javacard alkalmazás: ennek az alkalmazásnak kell a mobil fizetést lebonyolítani.

BME Hálózati Rendszerek és Szolgáltatások Tanszék 413

https://en.wikipedia.org/wiki/Java_Card_OpenPlatform

A kártyák egyrészt besorolhatóak annak függvényében, hogy a JCOP (JavaCard Open Platform) melyik verzióját támogatják (3.1 jelenleg a legújabb).

Másrészt a Global Platform szervezet API-ból melyik verziót támogatják.

Ezen felül is még számos paramétere eltérő lehet a kártyáknak (pl. hány bites RSA kulcsot támogat).



NFC fizetési rendszer - JavaCard alkalmazás

- Minden JavaCard alkalmazás rendelkezik egy azonosítóval (AID)
- Az olvasó a JavaCard-dal un. APDU üzenetekkel kommunikál
- Vannak előre definiált utasítások (alkalmazás kiválasztása, fájl műveletek, stb), az előre nem definiált utasításokat az alkalmazásban tudjuk kezelni.
- A SIM kártyára csak a szolgáltató tud JavaCard alkalmazást telepíteni (szükségesek a hitelesítő kulcsok a telepítéshez):
 - Távolról OTA megoldás segítségével
 - Kártyaolvasóval

BME Hálózati Rendszerek és Szolgáltatások Tanszék 414

A telepítéshez szükség van a kártya MAC, ENC és KEK kulcsaira
APDU: Application Protocol Data Unit



NFC fizetési rendszer - JavaCard alkalmazás

- Telepítést követően be kell állítani, hogy az alkalmazás elérhető legyen NFC interfészen is
- A legtöbb NFS-s telefonnak van beépített Secure Element-je is, a sim kártyától függetlenül.
- Ide viszont csak a gyártó tud telepíteni
- Léteznek olyan SD kártyák, amikben van Secure Element

BME Hálózati Rendszerek és Szolgáltatások Tanszék 415

Az SD kártyás Secure Element egy harmadik félnek az egyetlen esélye, hogy saját javacard alkalmazást tudjon egy felhasználó készülékére rakni. Ennek szintén sok problémája van:

- 1 telefon 1 sd kártya, több szolgáltató már nem tud ezzel a módszerrel élni
- Nem minden telefon támogatja az SD kártyás Secure Elementet
- Van olyan telefon, amiben nincs SD kártya hely (iPhone)



NFC fizetési rendszer - JavaCard alkalmazás

- Fizetési alkalmazásnál az alkalmazás feladata, hogy azonosítsa magát a fizetési szolgáltató felé. A biztonság érdekében ezt nyilvános kulcsú titkosítással teszi, a telepítéskor felrakott privát kulcsa segítségével.
- A secure element-nek biztosítani kell, hogy a privát kulcs ne legyen exportálható, kinyerhető



NFC fizetési rendszer - JavaCard alkalmazás

- A MasterCard lehetőséget biztosít arra, hogy a szolgáltatók saját PayPass alkalmazást készítsenek.
- Ennek azonban nagyon szigorú követelményei vannak:
 - A telefon itt úgy viselkedik, mint egy PayPass-os bankkártya, ezért banki háttérre is szükség van
 - A mobil alkalmazásnál meg van szabva, hogy hogy nézhet ki, milyen elemeket kell tartalmaznia
 - Az alkalmazást a MasterCard-nak kell auditálnia.



NFC fizetési rendszer - JavaCard alkalmazás

- Az okostelefonos alkalmazás csak egy segédprogram, maga a fizetés a Sim kártyán lévő alkalmazás és az NFC terminál (és ezen keresztül a bank) között zajlik
- Sok telefon esetén az NFC a telefon kikapcsolását követően is működik.



NFC fizetési rendszer – Secure Element

- Védett platform, ami megakadályozza a benne lévő adatok kinyerését (fizikai és szoftveres védelem is)
- Itt tárolódnak a titkos kulcsok és egyéb bizalmas adatok
- Az adatokhoz csak a kártyán futó alkalmazások férnek hozzá
- Az alkalmazás hibája következtében kinyerhetőek lehetnek ezek az adatok



NFC biztonság

- Man in The Middle: a titkosításnak köszönhetően a kommunikációt módosítani nem tudja, csak lehallgatni.
- Relay attack: az áldozat NFC-s telefonja mellé rakjuk a leolvasókat/telefonunkat, majd egy másik eszköz felé interneten/wifin keresztül továbbítjuk az adatokat, amivel fizetünk.
- A Relay attack ellen az alábbi módszerekkel tudunk csak védekezni:
 - Kikapcsoljuk az NFC-t, ha nincs rá szükség
 - Olyan tokot használunk, ami árnyékolja az NFC kommunikációt
 - Vásárláskor PIN kód kérése



BME Hálózati Rendszerek és Szolgáltatások Tanszék 420



Telekom Mobiltárca

- Az OTP bankkal közösen hozták létre
- A használat feltétele egy OTP-s folyószámla és OTP MasterCard Mobil PayPass kártya
- Csak Androidon 4.2-es vagy újabb készülékeken működik
- Elérhető szolgáltatások:
 - PayPass fizetés
 - SuperShop hűségpont gyűjtése
 - Színház és koncertjegy érvényesítés

BME Hálózati Rendszerek és Szolgáltatások Tanszék 421

A MasterCard Mobil PayPass kártya tulajdonképpen a Javacard alkalmazás a sim kártyánkra

<http://www.telekom.hu/mobil/lakossagi/tarifak/szolgaltatasok/mobilvasarlas/mobiltarca>



Mobilbank

- Mobiltelefon segítségével az ügyfelek minden rendelkezésükre álló banki szolgáltatást is elérhetnek
- Számos megoldás létezik:
 - WAP (mára már teljesen kiszorult)
 - Mobiltelefonra optimalizált weboldal
 - Mobil alkalmazás

BME Hálózati Rendszerek és Szolgáltatások Tanszék 422

http://www.mnb.hu/Root/Dokumentumtar/MNB/Kiadvanyok/mnbhu_mnbtanulmanyok/mnbhu_mt_85/mt_85.pdf



PayPal Here



BME Hálózati Rendszerek és Szolgáltatások Tanszék 423



PayPal Here

- A mobil telefonunkat egy POS terminállá alakíthatjuk
- Kártyás vásárlásokat tudunk bonyolítani a Paypal számlánkra
- A Paypal számláról átutalhatjuk a folyószámlánkra a befolyt összeget
- Az olvasót egyszeri díj ellenében kell megvásárolni, utána nincs havidíja a szolgáltatásnak

BME Hálózati Rendszerek és Szolgáltatások Tanszék 424

<https://www.paypal.com/webapps/mpp/credit-card-reader>



PayPal Here

- Az első generációs olvasók:
 - Csak mágnes csík olvasását tették lehetővé (chipet nem)
 - Audio bemeneten csatlakoztatható a telefonhoz az olvasó
 - Mivel nem minden készüléknél egyforma a headset csatlakozás, ezért kompatibilitási problémák fordultak elő
 - Pin kód megadására nem volt lehetőség
- A legújabb olvasó:
 - Bluetooth-on párosítható
 - Chipes kártyákat is kezel
 - Pin kódot is kér vásárláskor



PayPal Here

- A szolgáltatás indulásakor USA, Kanada, Ausztrália és Hong Kong országokban volt elérhető a szolgáltatás
- 2013-ban került bevezetésre a szolgáltatás az Egyesült Királyságban
- A cég ígérete szerint hamarosan további európai országokban is elérhető lesz a szolgáltatás.



Jogi szabályozás

- Általában a szabályozás követő jellegű
- Fizetési szolgáltató vagy banki szolgáltatás?
- Fizikai letelepedésre és fizikai jelenlét mellett végzett tevékenységek szabályozására alkotott 10-20 éves jogszabályok sokszor nem egyértelműen alkalmazhatók a távollévők közötti, határon átnyúló tranzakciókra
- Az elektronikus pénz definíciója bekerült az Európai szabályozásba: 2009/110/EK irányelv (ELMI direktíva)

BME Hálózati Rendszerek és Szolgáltatások Tanszék 427

Általában a szabályozás követő jellegű és csak az innovatív konstrukciók megjelenése után kerül sor a jogi szabályozására. vagyis az innovatív konstrukció szüli a szabályozást (szükség esetén) és nem fordítva.

Jogi szempontból nagy különbség van abban, hogy a szolgáltató tárolja-e az ügyfelek pénzét egy későbbi vásárláshoz vagy csak egy közvetítő szolgáltatóként viselkedik. Az előbbi esetben már felmerül a banki szolgáltatás lehetősége, melyek szigorúbb szabályozás alá tartoznak.

vegyük például azt az egyszerű esetet, amikor egy internetes fizetési szolgáltatást (pl. PayPal) vesz valaki igénybe magyarországról. Ekkor a jog kétféleképpen ítélheti meg a konstrukciót:

- a jogi helyzet olyan, mintha a magyar ügyfél „utazott” volna ki a fizetési megoldás szolgáltatójának székhelyére és ott vette volna igénybe a szolgáltatást az ottani nemzeti jog szabályai szerint. Ebben az esetben a hazai szabályok szigorúsága és a kemény felügyelet mit sem ér, hiszen valójában nagyon könnyű kívülről szolgáltatni, az internetes szolgáltató letelepedés és szolgáltatásnyújtás helyéül azt a tagállamot fogja választani, amelyekben a szabályozás számára legkevésbé korlátozó.
- b) a jogi helyzet olyan, mintha a fizetési megoldás szolgáltatója „határon átnyúló szolgáltatásként, de Magyarországon nyújtaná a szolgáltatást. Ekkor a magyar szabályok

vonatkoznak a fizetési megoldás szolgáltatójának tevékenységére, ezeknek azonban érdemben érvényt szerezni a hazai hatóságok (akár a felügyelet, akár egyéb fogyasztóvédelemben érintett hazai hatóságok vagy szervezetek) csak akkor tudnak, ha intenzív közreműködésre számíthatnak a szolgáltató letelepedési országának hatóságai részéről.

A két eset önmagában is kihívások elé állítja a hatóságokat és szabályozókat, de ami a problémát súlyosbítja, hogy sok esetben objektív szempontok alapján egyszerűen nem lehet eldönteni, hogy a kettő közül melyik alkalmazandó a jog szempontjából.

Pénzforgalmi szempontból ez két okból is problémás lehet:

- egyrészt a szolgáltatást nyújtó intézmény „prudenciális felügyelete” szempontjából, vagyis, hogy ki felügyel arra, hogy az intézmény felelős gazdálkodást folytatva vissza tudja fizetni az ügyfél rábízott pénzét;
- másrészt az ügyfelek jogai, a szolgáltató kötelezettségei (pl. kártérítési szabályok, ügyfél-tájékoztatásra vonatkozó szabályok) betartásának szempontjából, vagyis milyen kártérítési, milyen ügyfél-tájékoztatási szabályok érvényesek.

További szabályozási dilemmát jelent a hasonló szolgáltatások eltérő szabályozása. az egyes szolgáltatások számos eltérő technológiát, megoldást alkalmazva is megvalósíthatóak hasonló módon, miközben a rájuk vonatkozó szabályozások akár teljesen eltérőek is lehetnek. Erre az egyik legjobb példa a már említett, és a 7.2.2.1. pontban részletesen kifejtett bankszámla és a szerveralapú elektronikus pénz párosa, amelyek a gyakorlatban meglehetősen hasonlóan viselkednek.

http://www.mnb.hu/Root/Dokumentumtar/MNB/Kiadvanyok/mnbhu_mnbtanulmanyok/mnbhu_mt_85/mt_85.pdf

Igénybevétel alapú tömegközlekedés



Társadalmi igény

- Igazságosabb díjfizetés
- Időalapú, utazásalapú jegyek problémái
 - Ugyanannyit kell fizetni egy megállónyi és végállomástól végállomásig tartó utazásokkor
 - Forgalmi dugó esetén az egy jeggyel megtehető távolság drasztikusan csökkenhet
- Távolságalapú jegyek problémái
 - Nehezen adminisztrálható (fel- és leszállásnál is regisztrálni kell a helyszínt)
- Ismeretlen számú utazás, nem optimális üzleti konstrukciók választásához vezethet
 - Nem tudjuk feltétlenül, hogy mire van szükségünk? Vonaljegy, napijegy, heti bérlet?



Szolgáltatói igények

- Pontosabb kép a felhasználók utazási szokásairól, a járművek terheltségéről
- Beléptetőkapukkal munkaerő-költség megtakarítás (BKV)
- Nem fizető utasok hatékonyabb kiszűrése
- Értéknövelt szolgáltatások
 - Internetes egyenlegfeltöltés, jegyvásárlás
 - SMS egyenlegfeltöltés, jegyvásárlás
 - Automatikus tarifaváltás kedvezőbb konstrukcióra



Megvalósítási lehetőségek

- Mágneskártyás rendszerek
 - Olcsó
 - Könnyebben hamisítható
 - Mozgó alkatrészek vannak a leolvasóban (legalább a kártya mozog)
- Smart kártyás rendszerek
 - Drágább a kártya
 - Nehezen hamisítható vagy jelenlegi ismereteink szerint nem hamisítható
 - Nincsenek mozgó alkatrészek



Smart kártyás rendszerek a tömegközlekedésben

- NXP MIFARE termékcsalád
 - MIFARE Classic 1k és 4k
 - MIFARE DESFire
 - MIFARE DESFire EV1
 - MIFARE Plus S/2k/X
 - MIFARE Ultralight
 - MIFARE SmartMX



MIFARE

- ISO 14443 A kommunikáció
- 13,56 MHz frekvencia
- Tekercsantenna
- Olvasási távolság: ~ 3-6 cm



MIFARE Classic 1k/4k

- Vezeték nélkül elérhető memória
 - 1k – 1024 bit; 16 szektor
 - 4k – 4096 bit; 40 szektor ($32 \times 64 \text{ bit} + 8 \times 256 \text{ bit}$)
- Biztonsági funkciók
 - Szektoronként két darab hatbites kulcs
 - Nem nyújt valódi biztonságot, feltörték (lásd: következő dia)
- Díjfizetéshez kapcsolódó funkciók
 - Számlálók alkalmazásának lehetősége a memóriában
 - Beállítható, hogy a két kulcs közül az egyik csak decrement műveletre legyen használható

BME Hálózati Rendszerek és Szolgáltatások Tanszék 434

Mifare Classic mini: 320 bájt 5 szektorban



MIFARE Classic 1k/4k

- **Crypto-1 algoritmus**
 - Körülbelül 400 NAND kapus megvalósítás lehetséges
 - Egy 48-bites kulcsokkal üzemelő folyamkódoló
 - Az algoritmust és a megvalósítást is titokban próbálta tartani a gyártó NXP
 - Feltörték:
 - 2007 decemberében publikálták az első eredményeket (a chipet 1994-ben mutatták be)
 - gnireenigne esreverR
 - Bővebben: K. Nohl, D. Evans, Starbug, H. Plötz – Reverse-Engineering a Cryptographic RFID Tag

BME Hálózati Rendszerek és Szolgáltatások Tanszék 435

Reverse engineering: mikroszkóp + fényképezőgép + known-plaintext attack
Algoritmus kiderült + a 16-bites RNG hiányosságai is kiderültek
2007-ben még speciális hardvert használtak a feltöréshez, 2008-ban K. Nohl bemutatta,
hogy egy átlagos PC-n is másodpercek alatt törhető a Crypto-1 titkosítás



MIFARE DESFire/DESFire EV1/EV2

- DES, 3-DES algoritmusok, EV1 változat esetén AES is elérhető
- Fájrendszer a kártyán
 - →több alkalmazást is támogat egy adott kártya
- Distance bounding protokoll támogatás (EV2)
 - MIFARE Proximity check
 - Relay attack típusú támadás megakadályozása céljából



MIFARE Ultralight

- 512-bites memória (16 page × 4 byte)
- Nincs kriptográfiai funkció
- Biztonsági funkciók:
 - Írásvédelem
 - OTP bitek
- Olcsó
 - Eldobható jegyeként használható
- Ultralight EV1:
 - 384-/1024-bites változatok
 - Számlálók
 - 32-bites jelszavas védelem
 - Eredetiség-vizsgálat (nem NXP által gyártott chippek szűrése)
- Ultralight C:
 - 1536-bites memória
 - 3DES



MIFARE Plus S/X

- 2k/4k memória
- UID
- AES-128 titkosítás
- A migrációt elősegítő funkciók MIFARE Classic-ról
- Plus S: Slim: könnyű migráció Classic-ról
- Plus X: eXpert: több elérhető parancs, proximity check

BME Hálózati Rendszerek és Szolgáltatások Tanszék 438

X: eXpert



MIFARE SmartMX

- Kártya kettős interfésszel
 - ISO7816 kontaktusos interfész
 - ISO14443A vezeték nélküli interfész
- MIFARE Classic, Plus és DESFire emuláció a vezeték nélküli interfészen



Online és offline rendszerek

- Offline ellenőrzés lehetséges
- Az online ellenőrzés sok esetben (például MIFARE Classic kártyák használata esetén) biztonságosabb lehet
- Jellemzőbb az offline-online hibrid rendszerek használata
 - Offline tranzakciókra képes
 - A tranzakciók adatait nagyobb csomagokban küldik a központi adatbázisba
- Online rendszerek előnyei lehetnek:
 - Bankkártya elfogadásának lehetősége



Kitérő: biztonsági problémák, támadási lehetőségek

- Pénzről szól...
- Anyagi előny érdekében, szabotázs jelleggel, egyszerűen technikai kihívásként értelmezve a feladatot támadásoknak vannak kitéve a tömegközlekedési rendszerek
- Erőforráskorlátos rendszerek
 - Különböző bonyolultságú titkosító hardverek
 - Párszáz kaputól bonyolult processzoros rendszerekig
 - DE: probléma: olcsó eldobható jegyek



Kitérő: biztonsági problémák, mi van a háttérben?

- Egyszerű hardver
- Olcsó hardver
- Képzetlen felhasználók
 - A rádiós kommunikáció működését nem ismerik
- Kompromisszumos megoldások az ár és a bonyolultság tekintetében
 - Megkötések: pl.: nem elvihető kártyák



Kitérő: támadások típusai

- Man-in-the-middle támadás
 - Speciális eset: relay attack
- A kriptográfiai algoritmusok támadása matematikai módszerekkel
- Side-channel támadások
 - Az implementációt támadják, nem az algoritmust
- Lehallgatás
- Visszajátszásos támadás
- Kártya klónozás, hamisítás
- DoS, Denial of Service támadás
 - Pl.: jamming, tag tönkretétele nagyfeszültségű impulzussal
- Támadások az üzleti rendszerek ellen

Forrás: A. Mitrokovska, M.R. Rieback, A.S. Tanenbaum – Classification of RFID attacks

BME Hálózati Rendszerek és Szolgáltatások Tanszék 443



Kitérő: támadások elleni védekezési lehetőségek

- Man-in-the-middle: általában algoritmikus védelem
- Kriptográfiai algoritmusok elleni támadások: jobb algoritmusok
- Side-channel támadások: mérnöki megoldások
- Denial of Service: nincs megoldás
- Lehallgatás: fejlett algoritmusok
- Visszajátszásos támadás: algoritmikus védelem
- Kártya klónozás, hamisítás: algoritmikus védelem



Kitérő: relay attack, distance bounding protokoll

- Relay attack:
 - Átjátszásos támadás
 - Lényege: a kártya jelenlétét szimuláljuk a kártyától távoli helyen a kártya és az olvasó közötti kommunikációba történő beékelődéssel
 - Az átvitt adatok megfelelő titkosítási algoritmusok és kulcsok esetén nem ismerhetők meg, csupán a kártya helyét „hamisítja” ez a támadás





Kitérő: relay attack, distance bounding protokoll

- Relay attack kivitelezhető
 - Fizikai rétegben
 - Felsőbb rétegekben
 - Több rétegben (pl.: NFC telefon secure element elleni támadás)
- Egyetlen változás: megnövekedett késleltetés
 - Ha keverők segítségével történik a támadás, a növekedés $1\ \mu\text{s}$ alatt maradhat
 - [P. Thevenon, O. Savry, S. Tedjini, R. Malherbi-Martins – Attacks on the HF Physical Layer of Contactless and RFID Systems]
 - $20\ \mu\text{s}$ körüli késleltetésnövekedés érhető el DSP technológiával
 - [Gerhard Hancke – A Practical Relay Attack on ISO 14443 Proximity Cards]
 - APDU hosszal arányos késleltetésnövekedés tapasztalható a felsőbb rétegekben
 - [M. Weiss - Performing Relay Attacks on ISO14443 Contactless Smart Cards using NFC Mobil Equipment]



Kitérő: relay attack, distance bounding protokoll

- A tag-olvasó távolság felső korlátjának becslését szolgálja
- Kihívás- válasz alapú kommunikáció
- Nagyon gyors válaszidővel
 - Rendszerint több szakaszból állnak ennek biztosítására:
 - Inicializáló szakasz
 - Gyors kérdés-válasz szakasz
 - Kiértékelés szakasz
- Pontos időmérés szükséges
- Saját oszcillátor vagy aszinkron logika kell, a vivőfrekvencia órajelként történő felhasználása ebben az esetben nem biztonságos
- Bővebben: *G.P. Hancke – Design of a secure distance-bounding channel for RFID*



Támadások módjának változása

- Kezdetben analitikus támadások
 - A titkosítási algoritmusok ellen
 - Egyedi, gyártóspecifikus algoritmusok
 - Security by obscurity
- A gyártók reagáltak
 - Nyilvános, kipróbált algoritmusok
 - Megfelelő kulcsméret
 - Gondosan megvalósított RNG
- A támadások jellemzően immár SCA (side-channel attack) típusúak: nem az algoritmust, az implementációt támadják



Külföldi rendszerek – Hong Kong – Octopus card

- 1997 szeptemberében vezették be
- Előd: mágneskártyás rendszer 1979-től az MTR-en (Mass Transit Railway), 1989-től a buszokon is
- Sony FeliCa technológiát használ: 1-64 kB kapacitás
- Store and forward működés: a tranzakció offline, de a tranzakciók adatait egy központi rendszerbe küldik az olvasók



Külföldi rendszerek – London – Oyster card

- 2003 júliusától működik
- 2010 januárig Mifare Classic 1k kártya
- 2010-től Mifare DESFire EV1
- Bérletet vagy feltöltött pénzeszeget tárol
- Store and forward működés az Octopus cardhoz hasonlóan
- A metróban be- és kilépéskor, a felszíni közlekedés esetén az utazás megkezdésekor kell a kártyát az olvasóhoz érinteni

https://en.wikipedia.org/wiki/Oyster_card

BME Hálózati Rendszerek és Szolgáltatások Tanszék 450



A budapesti tervek

- Többször változott, az aktuális állapot:
 - Forgóvillás beléptetés a metróban
 - Érintőterminálok a felszíni tömegközlekedésben
 - Névre szóló és anonim bérletek
 - Érintés nélküli azonosítás
 - A bérletet a felszíni járatokon nem kötelező leolvastatni, a jegyeket igen
 - A tervek szerint a rendszer támogatni fogja a vezeték nélküli bankkártyákat (PayPass, PayWave)
 - Bevezetés 2017-re

Forrás:

<http://www.bkk.hu/fejleszteseink/elektronikus-jegyrendszer/> BME Hálózati Rendszerek és Szolgáltatások Tanszék 451



A budapesti tervek

- **Problémák:**
 - Kártyák logisztikája
 - A jegykezelő készülékek cseréje
 - A járművek elektromos hálózatának átalakítását is igényelheti, a mechanikus lyukasztókhoz jelenleg nincs elektromos áram, adatkapcsolat kivezetve
 - Az ellenőrzés módja változik
 - Banki szolgáltatások kialakítása jelentős feladat
 - A vegyes üzem problémái

Kitekintés a jövőbe – kvantumkommunikáció