



## TOTALCRYPT

*Megkezdődött a CableWorld Kft. fizető tv rendszerének gyártása*

A tartalomból:

- IP TV a valóságban  
*a CableWorld telephelyén megtekinthető Magyarország első IP TV mérőállomása*
- A kódolt adások vétele, a CAM Analyzer bemutatása  
*a Quad család demodulátorai már Common Interfészes változatban is kaphatók*
- CW-4873 QAM Demodulator Quad  
*Négy DVB-C vevő egy vázban 4×2 ASI kimenettel és CI-vel is*
- A CableWorld termékek vezérlése interneten keresztül  
*A CW-Net használata a távoli asztal funkcióval*
- A TotalCrypt kódolási rendszer bemutatása  
*Pay Tv rendszer építés CableWorld termékekkel*
- Ajándékok a CW-Net használói részére  
*Szabad MAC cím állítási lehetőség az SW-4891 szoftverrel*  
*A transport stream folyamatos rögzítése, fájlba írása*  
*Teszteljük és fejlesztjük együtt a TS analízátor szoftverét*

# CableWorld

## hírek

A CableWorld Kft. technikai magazinja  
2006. június

Számunk fő témája:

**A műsorok kódolása és dekódolása**

**32.**



## IP TV szolgáltatás a valóságban

Ami tegnap még csak álom volt, mára valósággá vált!

Minden korábbi előrejelzést felülmúló tempóban épülnek az IP TV rendszerek Magyarországon. Az építők a következő két kérdésre szeretnének választ kapni:

- Milyen a hazai távközlési hálózatok valós állapota, mire képesek akkor, amikor a szélessávú átvitelt nem csak a játék szintjén kell biztosítani?
- Ki és mekkora piaci részesedést tud magának megszerezni, milyen a nyerő üzlet- és reklám politika?

E kemény küzdelemben természetesen minden titkos: valamennyi cikk, reklámfilm stb. gondosan megtervezett időpontban stratégiai lépésként kerül ki. Talán senkinek az érdekeit nem sérti, ha eláruljuk, hogy 2006-ban legalább 5-6 szolgáltató szándékozik megjelenni ezen a piacon.

Újságunk olvasóinak elmondjuk, hogy az IP TV szolgáltatásnak többféle változata van. Az Interneten keresztül ma is számos televízióműsor érhető el, de itt az alkalmazott alacsony adatsebesség (100-300 kbit/s) miatt e szolgáltatások minősége sokkal gyengébb, mint amelyet a jelenlegi analóg műsorszórásban megszoktunk. Az adatsebesség növelésével a minőség olyan mértékben javítható, hogy 3-4 Mbit/s felett már az analógénál jobb minőséget kapunk, és további adatsebesség növeléssel a HDTV területére is beléphetünk.



### Beugrató kérdés 1.:

Hogy lehet a nehezen kigyötört 3-4 Mbit/s adatsebességgel 10-20 vagy még több tv-műsort átvinni?

#### Megoldás:

Az IP TV esetében nem áll „feleslegesen” egyidejűleg rendelkezésre a fali aljzaton az összes csatorna, a rendszer mindössze a kiválasztott egyetlen programot küldi el az előfizetőnek, ehhez pedig ez az adatsebesség megfelelő.

Az új szolgáltatások megvalósításához minden eszköz rendelkezésre áll, mindössze azt kell tisztázni, hogy távközlési hálózataink mennyiben képesek megszákítás nélkül, folyamatosan biztosítani ezt a nagyobb adatsebességet.

Fontos tudni, hogy 3-4 Mbit/s környékén a szolgáltatás minősége azonossá válik a DVB-S, DVB-C és DVB-T átvitel minőségével és az IP TV negyedikként igen versenyképesen kér helyet magának ebben a sorban.

A hazai IP TV szolgáltatások kiépíthetőségének tesztelésére a TVnet és a CableWorld Kft. közös mintarendszert épített, amelyben a CableWorld IP TV fejállomása szolgáltatja a jelet, a TVnet pedig biztosítja a jel eljuttatását a fejállomásról az előfizetőkhöz.

### Beugrató kérdés 2.:

Melyik kódolás (scrambling) fajtát célszerű használni az IP TV átvitelnél?

#### Megoldás:

Az IP TV esetében nincs szükség semmiféle kódolásra, hiszen a szolgáltató szervere csak azt a műsort küldi el az előfizetőnek, amelyet az előfizető a set-top boxán végzett beállítással „lehívott”. Így a műsor csak az előfizető tv-jén jelenik meg, a szolgáltató pedig bájtt pontos-sággal tud minden kiküldött adatot.

E kísérleti összeállításban a jel szolgáltatása a TVnet észak-pesti telephelyéről történik, és Budapest számos helyén már kérhető a vétel kiépítése. A CableWorld telephelyén (XI. ker.) kialakította Magyarország első IP TV mérőállomását, ahol az érdeklődőknek a működés megtekintésén kívül mérések és tesztek elvégzésére is lehetőségük nyílik. A kísérleti fázisban csökkentett csatornaszámmal, FTA műsorokkal folynak a vizsgálatok, de a nagy csatornaszámú végleges rendszer kialakításához sem kell több, mint néhány nap. A CableWorld Kft. telephelyén felépített IP TV mérőállomás cikkünk fényképén látható.



A hagyományos tv műsorszolgáltatás tesztelésével párhuzamosan több platformon is folyik Video On Demand (VOD - Előfizetői kérésre történő műsor küldés) szolgáltatás konfigurálása és tesztelése. Ezek egyikén

sikeresen vizsgázott a Kasenna cég Serveréből és a CableWorld IP TV Serveriből épített hibrid VOD rendszer, bizonyítva a Kasenna és a CableWorld termékek kompatibilitását.

Szerkesztők

## A Quad család CI modullal

Teljeskörű Common Interface megvalósítás saját fejlesztésű célintegrált áramkörökkel

*Az évek során számos hasznos (és gyakran meglepő) tapasztalatot gyűjtöttünk a CW-4142 QPSK DEMODULATOR és a CW-4144 ASI DESCRAMBLER készülékekben felépített Common Interface (CI) áramkör működése során. Ezen tapasztalatok felhasználásával készült el az új CI egység, amely a QUAD család minden tagjába (műholdas, földi, kábeles, valamint ASI bemenetű) beépítésre kerül.*

*A fejlesztés a korábbiakhoz képest több területen lényeges változást hozott:*

- Az IC gyártóktól való függést megszüntetendő a speciális CI controller chipet saját fejlesztésű változatra cseréltük.
- A Conditional Access Module (CAM) programozásának lehetőségei lényegesen bővültek.
- A modul saját menüjében történő navigálás, a kívánt paraméterek beállítása a készülékhez csatlakoztatott számítógép segítségével egyszerűen elvégezhető.
- A modul és a készülék (illetve a CI működését vezérlő host processor) közötti kommunikáció, valamint a kommunikációs szoftver egyes rétegeiben zajló folyamatok működés közben történő nyomon követése teljesen új lehetőségeket kínál a felhasználó számára.

### 1. A Common Interface felépítése és működése

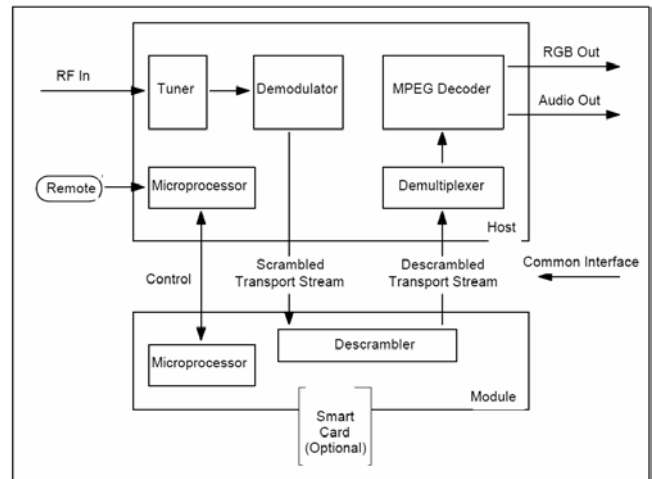
A set top boxok gyártóinak egyik törekvése, hogy a készülék minél többféle Conditional Access System, azaz kódolási rendszerhez illeszthető legyen. (Kódolás alatt a továbbiakban „titkosítást”, a fizető TV kialakításához szükséges hozzáférés vezérlést kell érteni.) Az egyik lehetőség, hogy többféle, a készülékbe épített Security module kerül alkalmazásra. Ennek azonban a vevő fizikai mérete, illetve gazdaságossági szempontok is határt szabnak.

A másik megoldás, hogy a descrambling (az adatok kódolása), illetve a hozzá kapcsolódó egyéb funkciók egy külső áramköri egységben, a Conditional Access Module-ban (CAM) kerülnek megvalósításra. A vevőkészülék (host) és a modul között egy szabványos kommunikációs felületet definiáltak, ez a Common Interface. Ennek az univerzális csatlakozási felületnek a részletes leírását az EN 50221: 1997 jelű szabvány tartalmazza.

Számunkra a digitális fejállomásban csak ez utóbbi megvalósítás jöhetett szóba. Egyrészt azért, mert készülékeinknek az összes létező kódolási rendszerhez illeszkedni kell, (már amennyiben létezik hozzá CA

modul is), másrészt a beépített Security module alkalmazásához különféle titoktartási szerződések és jogdíjak társulnak, amelyek számunkra nem elfogadhatóak.

A Common Interface alkalmazásának alapesetét az 1. ábra szemlélteti. A felső nagy téglalapban láthatjuk a vevőkészülék főbb szerkezeti egységeit. Az alsó téglalap szemlélteti a modult. A modul a gyakorlatban speciális, 68 pólusú csatlakozón keresztül kapcsolódik a hosthoz.



1. ábra

A modul csatlakoztatásakor alacsony szintre húzza a csatlakozó egyik pontját. A host érzékelve ezt, egy inicializálási folyamatot indít el, amelynek során kiolvassa a modul megfelelő memória területéről az úgynevezett kártya információs struktúrát (Card Information Structure, CIS). Ez egy adatbázis, amely fontos konfigurációs és egyéb információkat (pl. írási és olvasási címek, stb.) hordoz a modulról. A CIS ismeretében a host a konfigurációs paraméterek segítségével beállítja a modul megfelelő üzemmódját. Ezután a host a demodulátorból a kódolt transport streamet a modul descrambler áramkörébe küldi. Innen a TS, amely már egy, vagy esetleg több dekódolt (nem titkosított) programot tartalmaz, visszakerül a host demultiplexerébe, majd innen az MPEG2 dekódolóba. A csatlakozási felület tehát a modul és a host között a Common Interface. Egy hosthoz több modul is csatlakoztatható, ilyenkor a TS minden modulon áthalad.

Amint az ábrán is látszik, a CI alapvetően két részből áll. Az egyik a Transport Stream Interface, a másik a Command Interface:

- A TS Interface a titkosított programokat tartalmazó transport stream továbbítására szolgál.
- A Command Interface a host és a modul kommunikációját biztosítja.



A CI teljes megvalósítása szoftveres és hardveres elemek együtteséből áll. A CI szoftver a kommunikációs rendszerekben általános layer szervezésű, a különböző feladatokat layerekbe (réteg) csoportosítja. A TS Interface layerai közül a CI csak a fizikai és a link réteget definiálja, a többi az MPEG2 szabvány része.

A Command Interface a szabvány szerint öt layerből áll, ezek logikai sorrendben a következők: physical, link, transport, session, application. Az egyes rétegek szabványos, az adott rétegre jellemző adategységekkel (LPD: Link Protokoll Data Unit, TPDU: Transport Protokoll Data Unit stb.) kommunikálnak a szomszédos rétegekkel. Az adategységekbe van „becsomagolva” a modul illetve a host által a másiknak küldött információ. Az application és session rétegeket teljes mértékben lefedi a szabvány. A transport és link rétegek kismértékben függenek a fizikai rétegtől. A fizikai réteg viszont az adott implementációnak megfelelően sokféle lehet. Például a mi esetünkben a fizikai réteg megvalósítása teljesen eltérő a CW-4142-ben és a QUAD családban.

A modul műszaki specifikációját a PCMCIA (Personal Computer Memory Card International Association) szervezet által kiadott PC Card Standard rögzíti. A Conditional Access modul tulajdonképpen egy II. típusú, 16 bites, speciális alkalmazásra kifejlesztett PC kártya. A PC kártya szabvány külön fejezetben (Metaformat Specification) foglalkozik vele.

## 2. CA Module Controller and Analyzer szoftver

A Conditional Access Module Analyzer and Programmer szoftver (SW-4872) a QUAD család CI-vel felszerelt változatainak (CW-4872, CW-4874, CW-4876, CW-4878) közös vezérlő és programozó szoftvere.

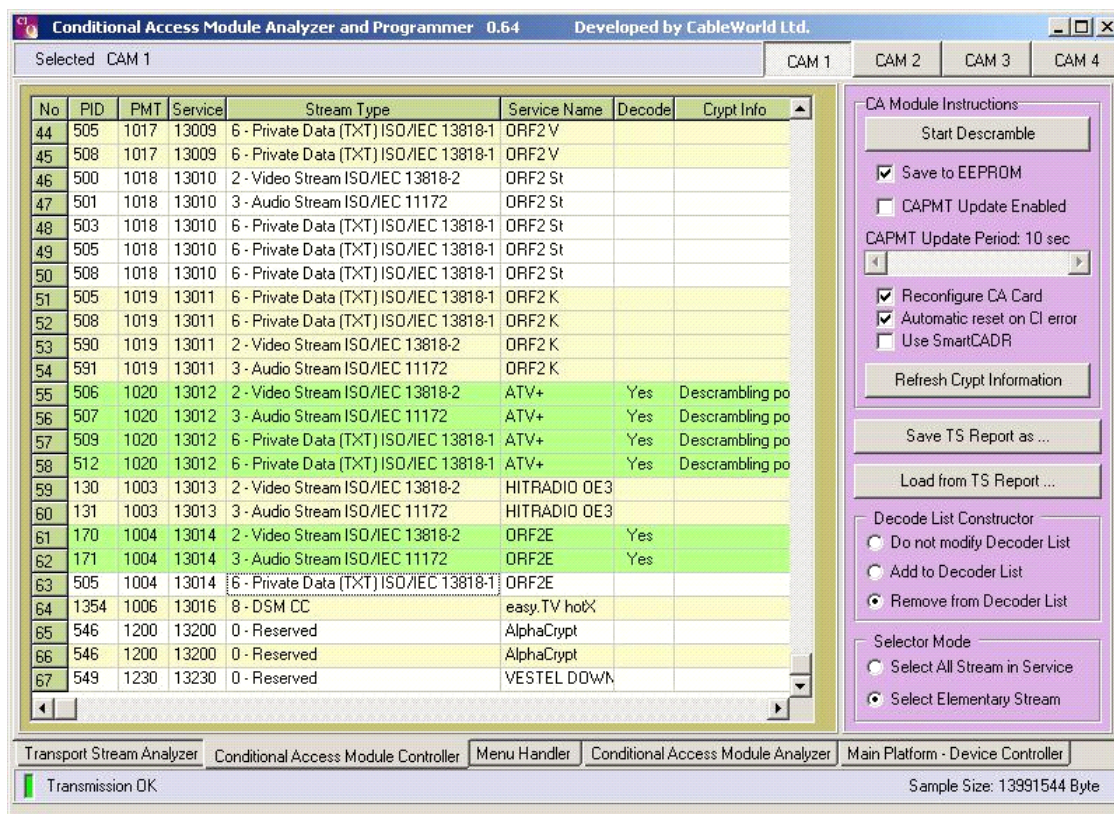
A program alkalmas a bemeneti transport stream analizálására, majd a stream összetevőiből egy adatbázis (CA-PMT) összeállítására, amelynek segítségével a csatlakoztatott max. 4 db CA modult egyenként a kívánt program, vagy programok dekódolására konfigurálhatjuk.

A szoftver a különféle tevékenységeket platformokba csoportosítva tartalmazza, amelyek külön-külön ablakokban jelennek meg.

A CA modulba küldendő üzeneteket, és a modulból érkező információkat a befogadó berendezés vezérlő processzora (host processor) a CW-Net adatátviteli- és készülék vezérlő rendszer segítségével juttatja el a felhasználó számítógépére.

A CW-Net egy 100 Mbit/s sebességű Ethernet hálózat, amelyet az alkalmazott utasítások formátuma miatt nevezünk így. A számítógép és a készülék Internet Protocol alatt, UDP/IP csomagokban kommunikál egymással.

A kívánt paraméterek beállítása és tárolása után a készülék a számítógép nélkül is önálló, folyamatos üzemre alkalmas.



2. ábra

Az SW-4872 CAM Analyzer and Programmer szoftver kezelőfelülete a dekódolásra történő stream kijelölés folyamatában

A szoftver elindítását követően a "Main Platform-Device Controller" fülre kattintva teremthetünk kapcsolatot a készülékkel. A CW-Net kapcsolat kiépítését és a készülék IP címének beállítását követően nyomjuk meg a Query gombot. (A CW-Net címzési tartományának használatához előzetesen jelöljük be a „Use CW-Net” négyzetet.) A "Query" gomb megnyomásának hatására a szoftver kapcsolatot létesít a kiválasztott készülékkel, kiírja annak nevét, típusát és gyártási számát. Használat közben a négy darab CA modulból a kommunikációra kiválasztott sorszámról a fejléc bal szélén, a transport stream átviteléről a lábléc bal szélén kapunk tájékoztatást.

### 3. Transport Stream Analyzer platform

A kiválasztott modulba érkező transport stream-ből mintát véve, a szoftver analizálja azt, és a kapott eredmény alapján tudjuk a Conditional Access Module Controller platformon elvégezni a kívánt elementary streamek dekódolásra történő kiválasztását, engedélyezését és tiltását.

A mintavétel a Get Sample gombra kattintással történik. A beépített analyzer a minta alapján egy jelentést készít, amely szükség szerint fájlba is menthető. A mintavétel eredménye a lap bal oldalán jelenik meg könnyen áttekinthető formában. Az egyes szervizekre (műsor szolgáltatásokra) kattintva az összetevők legfontosabb jellemzőit láthatjuk.

### 4. Conditional Access Module Controller platform

Itt történik a CA modul konfigurálásához szükséges CA-PMT üzenetek összeállítása és a modulba küldése a felhasználó által kiválasztott programösszetevők alapján (2. ábra). Minden vízszintes sor egy -az analizáláskor talált- programösszetevőt jelöl. A képernyőn zöld sorok jelentik a dekódolásra kiválasztott összetevőket.

A kiválasztott programok dekódolása a host processor által a modulba küldött CA-PMT tábla alapján történik. A CA-PMT táblát a szoftver automatikusan állítja elő a mintavétel során talált (de természetesen csak az általunk dekódolni kívánt programokhoz tartozó) PMT táblákból a felesleges descriptorok (leírók) törlésével. Mivel fejlécekben egy CA modullal egyidejűleg általában több program dekódolása célszerű, ilyenkor minden egyes dekódolandó program CA-PMT tábláját el kell küldeni a modul számára. A táblákat a modul megvizsgálja, és programonként választ küld, hogy a dekódolás lehetséges-e (2. ábra Crypt Info oszlopa).

**Fontos tudni: a CA modulok dekódolási kapacitása a dekódolható elementary streamek (ES) számában van meghatározva.** Ez a modul típusától, hardver változatától (gyári számtól), szoftverének verzió számától, stb. függően erősen változik, általában 8 és 24 között van. Tehát, ha feltesszük, hogy modulunk 8 ES egyidejű dekódolására képes, ez 4 program dekódolhatóságát jelenti, (programonként egy video- és egy audio

streammel számolva). Bizonyos típusú modulok egyáltalán nem támogatják több program egyidejű dekódolását. Ezért a modulok beszerzése előtt mindenképpen előzetes tájékozódást javasunk.

**Az említett ES feldolgozási korlátok túllépése egyes streamek vagy teljes programok dekódolásának véletlenszerű leállását eredményezi!**

A tapasztalat szerint a CA modulok megbízhatósága nem mindig megfelelő, gyakoriak a leállások. A szoftver különféle kapcsolók segítségével sokféle lehetőséget kínál ezek kivédésére. Például általunk választott gyakorisággal újraküldhetjük a CA-PMT táblákat, a táblák újraküldése előtt inicializálhatjuk a modult, stb. (Részletes ismertetés a szoftver helpjében található.) Ezzel a leállások ugyan nem küszöbölhetők ki, de biztosított a modul újraindítása, és így -néhány másodperc kieséstől eltekintve- a folyamatos üzem.

### 5. Menu Handler platform

Minden CA modulnak saját menürendszere van, amelyben számos információ található, illetve bizonyos paraméterek itt állíthatók be. Ilyenek, pl. az előfizetői kártya azonosítói, a jogosultságra vonatkozó információk (mely programok vételére alkalmas a kártya, mikor van vége az adott jogosultsági periódusnak, stb.). Az „Enter Menu” gombbal utasíthatjuk a CA modult, hogy küldje el a menü-rendszerét leíró üzenetet. A menü felépítése, az egyes menüpontok a baloldali mezőben láthatók. A menü szerkezete a modul szoftverétől függ és modultípusonként erősen változó. A menüstruktúra alapvetően a televízió képernyőjén történő megjelenítéshez készült. Ezért legfelül mindig találunk egy címsort (Title), alatta az alcímet (SubTitle), ezután következnek modulonként változó számban a különféle menüpontok és ezt követően a képernyő aljára szánt üzenet (Bottom). A kiválasztott menüpontból a hozzátartozó almenübe a megfelelő sorban lévő „Select” gombra kattintva jutunk. A menüpontok között gyakran találhatunk az illetéktelenek hozzáférését megakadályozó PIN kódok beállítására szolgáló, vagy a modul szoftverének frissítését indító parancsot, stb.

### 6. Conditional Access Module Analyzer platform

Ez a programrész a modul belső működéséről, - a felhasználó számára egyébként rejtett - paramétereiről tájékoztat. Nyomon követhetjük az egyes rétegek működését az aktuális dekódolási állapotot, belenézhetünk a CIS-be, stb. Az analízis eredménye fájlba menthető, így jegyzőkönyvként is használható. Az egyes fogalmak megértéséhez a Common Interface szabvány ad útmutatót. A felmerült kérdések megválaszolásában szívesen állunk partnereink rendelkezésére.

Veres Péter

## A CW-4873 QAM Demodulator Quad

Négy független QAM demodulátor ASI kimenettel, CW-Net vezérléssel



Befejeződött a QAM demodulátor Quad fejlesztése, így teljessé vált a digitális televíziórendszerek számára fejlesztett Quad család, amelynek tagjai:

- CW-4871 QPSK Demodulator FTA változat
- CW-4872 QPSK Demodulator CI változat
- CW-4873 QAM Demodulator FTA változat
- CW-4874 QAM Demodulator CI változat
- CW-4875 OFDM Demodulator FTA változat
- CW-4876 OFDM Demodulator CI változat
- CW-4878 ASI Descrambler CI változat

Társaihoz hasonlóan a QAM Demodulator Quad is négy egymástól független demodulátort tartalmaz, CW-Net vezérléssel rendelkezik és a ma beszerezhető legkorszerűbb áramkörkészletre épül.

### 1. CW-4873, -74 QAM Demodulator Quad

A készülék felépítése, részegységei:

- 4 db QAM demodulátor
- 4x2 db ASI kimenet
- Ethernet kontroller
- Kapcsolóüzemű tápegység
- Előlapi üzemmód kijelzők

A CW-4873 és CW-4874 típusú új készülékben a korábban használt Philips demodulátor IC továbbfejlesztett változata került felhasználásra a Philips cég által gyártott tunerbe építve. Az új tuner mérete sokat csökkent az előző típushoz képest, ugyanakkor sok új, a CableWorld rendszerében jól kihasználható újdotást tartalmaz.

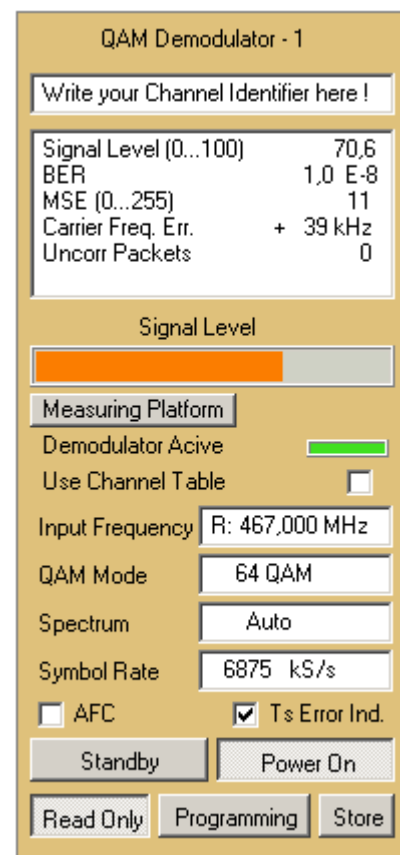
Ez a tuner igen széles körben alkalmazható set top boxtól a professzionális mérővevőig, mivel kiváló műszaki tulajdonságai mellett támogatja a profi felhasználók által elvárt mérési funkciókat is. A többi Quad modellhez hasonlóan a bemenet mellett egy továbbfűzött,  $\pm 0.5$  dB erősítésű kimeneti csatlakozót is találunk, ami nagyban megkönnyíti a jel szétosztását, több demodulátor felfűzését egy jelre.

A tuner vezérlését általunk fejlesztett PIC mikrovezérlő látja el, amelynek a CW-Net Ethernet Controller egység továbbítja a számítógépből érkező üzeneteket és kéréseket. A számítógép csak a kívánt vételi paraméterek beállítására, illetve a felügyeleti funkciók ellátására szolgál. A készülék természetesen számítógép nélküli önálló üzemre is képes.

### 2. A készülék kezelése

A paraméterek beállítása és a működési adatok kijelzése egy könnyen áttekinthető grafikus kezelőfelületen történik. Az általános üzemmódokat tartalmazó mezők mellett a vételi paramétereket négy egyforma mező tartalmazza. Egy ilyen mezőt mutat az 1. ábra.

A felső szerkesztő ablakba a csatorna azonosítására alkalmas szöveg írható, ami a későbbiekben megkönnyíti a munkát. Ez alatt a vétel minőségét leíró mérési eredményeket találjuk. Az első sorban a beérkező jel szintjét látjuk 0-tól 100-as értéktartományban. A legideálisabb paramétereket a jelszint 75-ös értéke környékén mérhetjük.



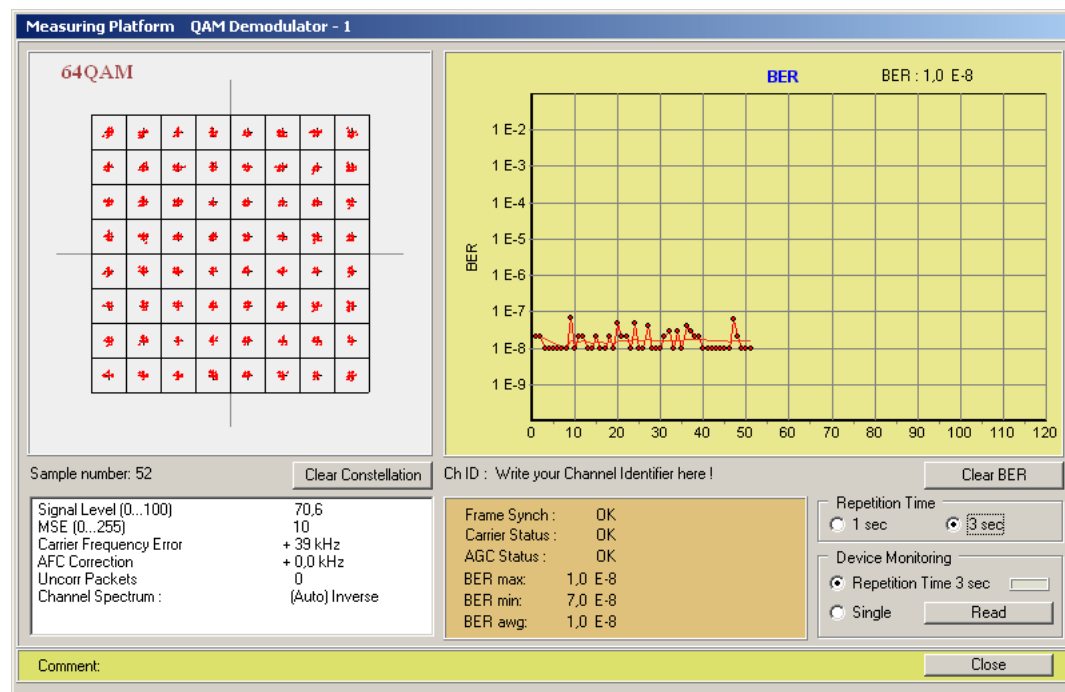
1. ábra. A QAM demodulátor modul kezelőfelülete

Az átvitel minőségét legjobban leíró mérési érték a BER (Bit Error Rate), amely az átvitelben keletkezett hibás bitek és az összesen átvitt bitek arányát adja meg. A BER értékét a tuner önállóan méri.

A következő sorban az MSE (Mean Square Error) értékét láthatjuk. Ez az érték a konstelláció torzulásairól tájékoztat. Értéke 20 alatti értéknél ideális. Láthatjuk még a beállított frekvencia eltérését a névleges értékhez képest. Nagyobb eltérés esetén 62,5 kHz-es raszterben korrigálhatunk. Végül az esetleges javíthatatlan paketek számát olvashatjuk. Ennek nullától eltérő értéke esetén számíthatunk a kép kockásodására, akadására.



A vételi paraméterek (frekvencia, moduláció, spektrum, szimbólumsebesség) helyes beállítása, majd a beállítások programozása után a készülék előlapján található zöld led világítani kezd, ami a lockolási folyamat befejezését jelenti.



### 3. Measuring platform

A measuring platform gomb megnyomása után egy új ablak jelenik meg a képernyőn. Ezen az oldalon részletesen tájékozódhatunk a vétel minőségéről. A bal sarokban láthatjuk a konstellációs ábrát, amit kellő mennyiségű mintavétel után elemezhetünk. A konstellációs ábráról fontos információkat tudhatunk meg az esetleges torzításokról, túlvezérlésekről, jelminőségről.

A konstelláció mellett találjuk a BER mérőt, ami az idő függvényében ábrázolja a BER értékét. Az ábra valamely pontjára kattintva az egér jobb gombjával eltolhatjuk, a ballal nagyíthatjuk az ábrát. A grafikonon két görbét láthatunk, az egyik az aktuális BER értéket mutatja, a másik az átlagos értéket. A grafikon jobb felső sarkában az éppen aktuális értéket olvashatjuk. A mérés  $10^8$ -os tartományban folyik, ami azt jelenti, hogy  $10^8$  bit lefutása után kapjuk meg a korrekt értéket. Ezért két olvasás között el kell telnie annyi időnek, ami alatt lefut az adott mennyiségű adat. Nagyon alacsony adatsebesség mellett ez több másodpercet is igénybe vehet, ezért ilyenkor célszerű a „single” módban mintavételezni (ld. jobb alsó sarokban).

### 4. Az AFC funkció

Az AFC funkciót MMDS rendszerek megbízható vételére fejlesztettük ki. A parabola fókuszpontjában elhelyezkedő fejre a venni kívánt nagyfrekvenciás jel mellett a napsugarak is koncentrálnak. Ez jelentősen

megnövelheti az LNB hőmérsékletét. Az így létrejövő éjszakai és nappali nagy hőmérséklet-ingadozás az LNB oszcillátorára is kellemetlen hatással van, tehát a konvertált csatornák középfrekvenciája ingadozni fog. Az elmászott frekvencia miatt a vétel minősége jelen-

tősen romolhat, esetleg a vétel meg is szűnhet. Ennek elkerülése érdekében készült az AFC funkció. A szolgáltatás bekapcsolása után a készülék a beállított frekvencia mellett  $\pm 3,5$  MHz távolságban képes a jelre ráfogni. A benntartási tartomány  $\pm 4$  MHz-ig terjed. A sáv letapogatása miatt a végleges lockolási folyamat 15 - 20 másodpercig is eltarthat, a szimbólumsebesség és az elhangolódástól függően. A jel megtalálása után a készülék másodpercenként egyszer ellenőrzi a frek-

kvencia-eltérést, és ha 50 kHz-nél nagyobb hibát mér, azonnal korrigálja azt. A demodulátor a frekvencia változása mellett a szimbólumsebesség esetleges változásait is képes követni. Jó minőségű és nagy adatsebességű jel esetén a képen nem tapasztalunk akadást az áthangolás alatt sem.

### Főbb műszaki adatok

#### RF bemenet

Bemeneti frekvenciasáv	51...858 MHz
Bemeneti jelszint	44...84dB $\mu$ V
RF bemeneti impedancia	75 ohm
RF bemeneti csatlakozó	F aljzat
RF kimeneti csatlakozó	F aljzat
Átmeneti csillaapítás	$\pm 5$ dB, tipikusan 0 dB

#### Jelfeldolgozás

Moduláció	QPSK, 16QAM, 32QAM 64QAM, 128QAM, 256QAM
Szimbólumsebesség	1 ... 7 MS/s
AFC üzemmód adatai	6875 kS/s esetén
Frekvencia befogási tartomány	$\pm 3.5$ MHz
Frekvencia benntartási tartomány	$\pm 4.0$ MHz
Vezérlő szoftver	SW-4873

Uhrin Csaba

## Készülékeink távvezérlése interneten illetve helyi hálózaton keresztül

Ingyenes megoldás a készülékek ethernet hálózatokon keresztül történő beállításához és ellenőrzéséhez a CW-Net alkalmazói részére

### 1. Távvezérlés, távfelügyelet

A digitális televíziótechnika a készülékvezérlés és a rendszerépítés területén is számos újdonságot kínál. A kábeltelevízió üzemeltetők és a hasonló szolgáltatást biztosító cégek álma valósul meg akkor, amikor az IP technológia lehetővé teszi, hogy a helyszínrre történő kiszállás nélkül, akár otthoni dolgozószobájából ellenőrizhesse az Önre bízott rendszer működését, és ha szükségessé válik, a készülékek konfigurálásával vagy a jelek átkapcsolásával stb. beavatkozzon annak működésébe.

A CableWorld Kft. CW-4000 digitális rendszerében a készülékvezérlés Internet Protocol felhasználásával központi számítógépről történik. Az egyik fontos jellemzője a rendszernek, hogy a számítógépet csak a készülékek konfigurálásához és a működés ellenőrzéséhez kell alkalmazni, azaz a PC a folyamatos üzemhez nem szükséges. A készülékek a 100 Mbit/s sebességű CW-Net rendszeren keresztül kapcsolódnak a számítógéphez, így feldolgozás vagy ellenőrzés céljából akár a teljes transport stream átvihető a számítógépbe. A másik fontos rendszerjellemző, hogy mivel valamennyi bemenet és kimenet jele a PC-be vihető, így akár a két készülék közötti ASI kábel egyik és másik végén lévő jel is vizsgálható, azaz a kábelek hibája is kimutatható. A felsorolt szolgáltatások árban foglaltak, így a felügyeleti rendszer kiépítése plusz költséget nem jelent.

A CW-Net rendszer switchen, vagy hasonló eszközön keresztül gyakorlatilag korlátlan számú készülék összekapcsolását lehetővé teszi. Az összekapcsolt készülékek mindegyike a közös vezérlő gépről programozható, a működésük folyamatosan ellenőrizhető.

A távfelügyeleti rendszerek nagy hiányossága, hogy nem teszik lehetővé nagyobb mennyiségű adat nagyobb távolságra történő eljuttatását, így csak az egyszerűbb paraméterek ellenőrzésére nyújtanak lehetőséget. A CW-Net rendszer e hiányosságot úgy számolja fel, hogy távfelügyeleti ellenőrző számítógép-ként a beállításához használt gépet veszi igénybe, és a szoftverek is azonosak. Távolról történő elérés esetén a nagy adatsebességet igénylő bonyolult szoftverek a vezérlő gépen futnak, és csak az eredményeket szemléltető képernyő információi kerülnek átvitelre egy távoli pontba. Mint látni lehet, a képernyő átvitele már nem a CableWorld megoldása, ezt mi csak felhasználjuk. Ez a szolgáltatás az Ön számítógépén is telepítve van, mi csak megmutatjuk használatát.

### 2. A távoli asztal használata

A Windows operációs rendszernek része a távoli asztal szolgáltatás, amely lehetővé teszi, hogy az interneten, illetve helyi számítógép hálózaton keresztül lássa egy távoli számítógép képernyőjét. A gyakorlatban ez azt jelenti, hogy az asztalán lévő monitoron ugyanazt a képet látja, mint ami az interneten keresztül hozzá kapcsolt másik számítógép monitorán látható, miközben az egeret mozgatva vagy a billentyűzetet használva, a távolban ugyanúgy hajtódnak végre az utasítások, mintha ott lenne. Már közepes adatsebességű összeköttetés esetén is alig észrevehető a létrejövő késleltetés.

Természetesen a távoli asztal használata esetén mind a két gépnek bekapcsolt állapotban kell lennie. Kábeltelevízió fejállomások és hasonló rendszerek esetében a folyamatosan működő felügyeleti számítógépeknél célszerű ennek az alkalmazásnak a használata. A távoli asztal segítségével a képernyő mellett az összes alkalmazás, fájl, hálózati erőforrás ugyanúgy elérhető, mintha ott ülnénk. A távoli asztal használata automatikusan lezárja a számítógépet, így kollégája vagy más személyek ezen idő alatt nem férhetnek hozzá. A lezárás a CTRL+ALT+DEL billentyűkombináció lenyomásával oldható fel. A távoli asztal segítségével egy számítógépen több felhasználónak is lehet aktív munkamenete, de e cikkben a több felhasználós esettel nem foglalkozunk.

### 3. A megvalósításhoz szükséges eszközök

A távoli asztal kapcsolat kiépítéséhez és használatához a következők szükségesek:

- a CW-Net rendszert működtető számítógép, amely CW-4890 Data Boss, vagy hasonló, Windows XP Professional operációs rendszerrel és internet csatlakozással rendelkezik
- az Ön számítógépe, amelyről vezérelni akarja a távolban lévő rendszert, internet csatlakozással és „távoli asztal kapcsolat” programmal
- a felhasználói fiókok és engedélyek kialakítása a távoli gépen. Ezek minden esetben jelszóval védettek legyenek!

Router használata esetén a távoli számítógép környezetében 3389-es port forward használatának engedélyezése is szükséges.



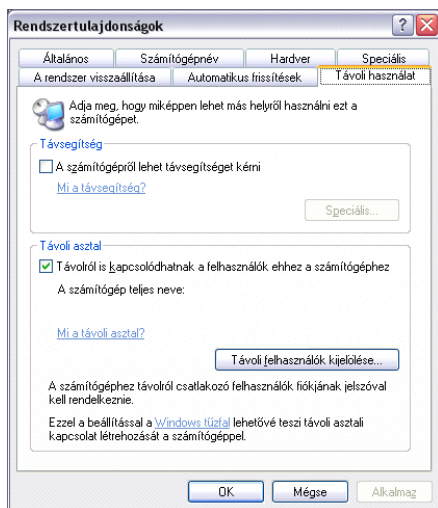
#### 4. A távoli számítógép beállítása

A szolgáltatás használatához a távoli számítógépet a következők szerint kell beállítani:

- nyissa meg a Vezérlőpultról a Rendszertulajdonságok párbeszédpanelét
- jelölje be a Távoli használat lap, Távolról is kapcsolódhatnak a felhasználók ehhez a számítógéphez jelölőnégyzetet, majd kattintson az OK gombra (2. ábra)
- ellenőrizze, hogy rendelkezik-e a csatlakozáshoz szükséges engedélyekkel, majd kattintson az OK gombra

Megjegyzés:

A Távoli asztal szolgáltatás engedélyezéséhez rendszergazdaként, vagy a Rendszergazdák csoport tagjaként kell bejelentkezni.



2. ábra

A rendszertulajdonságok beállítása

#### 5. Kapcsolódás a távoli számítógéphez

- nyissa meg a Távoli asztal kapcsolat ablakot
- a számítógép mezőbe írja be a számítógép nevét vagy IP címét (3. ábra). A számítógép lehet terminál kiszolgáló, vagy egy olyan számítógép, amelyen a Windows Professional vagy Server fut, és engedélyezve van rajta a távoli asztal kapcsolat
- kattintson a Csatlakozás gombra
- megjelenik a Bejelentkezés a Windows rendszerbe párbeszédpanel
- a Bejelentkezés a Windows rendszerbe párbeszédpanelen írja be a felhasználó nevét, jelszavát és (ha szükséges) a tartományt, majd kattintson az OK gombra



3. ábra

A távoli asztal kapcsolat megjelenő ablaka

#### 6. A kapcsolat bontása a munka befejezése nélkül

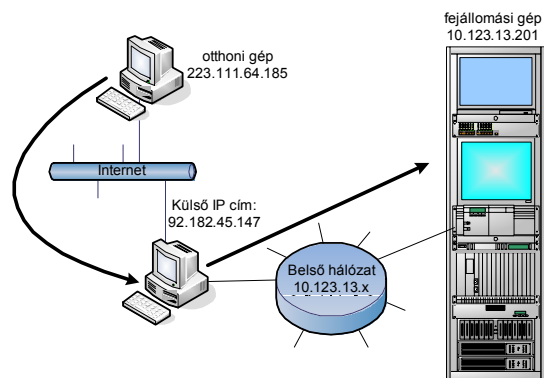
Abban az esetben, ha rövidebb időre szeretné bontani a kapcsolatot, vagy szeretné, ha a kapcsolat bontása után elindított program még futna a távoli számítógépen, a következők szerint járjon el:

- a Távoli asztal kapcsolat ablakában kattintson a Start gombra, majd a Kapcsolat bontása parancsra
- a Biztosan megszakítja a kapcsolatot? ablakban kattintson a Kapcsolat megszakítása gombra
- ezután egy figyelmeztető ablak jelenik meg a távoli asztal levált felirattal, itt kattintson az OK gombra

#### 7. Egy érdekes lehetőség

Érdekesség, hogy a távoli asztal segítségével úgy mond „láncba” lehet kapcsolni a gépeket. Tegyük fel, hogy egy olyan rendszert szeretnénk, ahol a fejállomásban található gép nem csatlakozik közvetlenül az internethez, azonban a belső ethernet hálózaton, található egy gép, amely igen, és mi otthonról, az interneten keresztül szeretnénk elérni a fejállomás PC-jét.

Ezt úgy valósíthatjuk meg otthonról, hogy távoli asztal eléréssel ahhoz a géphez kapcsolódunk, amelyik rendelkezik internetes kapcsolattal, ezután ezen a számítógépen keresztül a fejállomásban található géppel létesítünk távoli asztal kapcsolatot. Ennek a kapcsolódási lehetőségnek a blokkvázlatát ábrázolja a 4. ábra.



4. ábra

A távoli asztal kapcsolat egy másik számítógépen keresztül.

Majernik Zoltán

# TOTALCRYPT

Előfizetéses tv rendszer kábeltelevízió hálózatok, MMDS és hasonló rendszerek számára max. 500.000 előfizetőig

*Előfizetéses televízió műsorszolgáltatásról akkor beszélünk, ha a műsorhoz való hozzáférést csak azok számára tesszük lehetővé, akik az esedékes díjakat megfizették. Már az analóg technikában is nagy volt az igény a fizetős rendszerek iránt, de a megvalósításhoz a digitális technika sokkal kedvezőbb.*

*2005 végén olyan mértékben megnövekedett az érdeklődés a CableWorld kódoló (scrambler) rendszerének fejlesztése iránt, hogy fejlesztő kapacitásainkat megduplázva, felgyorsított ütemben kellett folytatnunk munkánkat. A fejlesztés végéhez érve, most indítjuk a felhasználói teszteket és igyekszünk egyre szélesebb körben bemutatni rendszerünket.*

## 1. Miért nagy az érdeklődés a TotalCrypt iránt?

A megnövekedett érdeklődés döntően a következő két okra vezethető vissza:

♣ A „nagyok” által kidolgozott titkosítási eljárások (Cryptoworks, Nagra, Irdeto stb.) globális rendszerekben (pl. műholdas műsorszórás) kerültek alkalmazásra. Mivel feltörhetetlen megoldást nem lehet készíteni, ezeket rendszeresen feltörik és a kulcsokat az interneten keresztül azonnal széleskörben elterjesztik.

*E feltörés ellen a legjobb védekezés olyan rendszer használata, amelyet csak szűk körben alkalmaznak, s így annak feltörése nem földünk teljes lakosságának érdeke. A CableWorld megoldása nem az említett globális rendszerek igényei alapján készült, ezért a hatalmas előfizetői számú műholdas műsorszórásban nem is lehet használni.*

♣ Az üzemeltetők mellett a kódolási rendszerek gyártói is látják, hogy az előfizetős rendszerekben nagy pénz van, ezért berendezéseiket és szolgáltatásikat igen magas áron kínálják, azaz ők is részesedni kívánnak ebből a nagy profitból.

*A CableWorld ismerve partnerei helyzetét és e piaci igényt, igen mérsékelt határozta meg árait. Kiemelkedő előny, hogy a TotalCrypt rendszer használóinak sem egyszeri felhasználói díjat, sem a bevétellel arányos havi díjat nem kell fizetniük.*

## 2. Mi a TotalCrypt rendszer lényege?

A kódolás, amit itt célszerűbb „scramblerezésnek” nevezni, a programozható CW-4861 Pay Tv Scrambler segítségével történik. A készülék egy transport streamen belül max. 64 db különböző PID-ű elementary stream kódolására alkalmas és a címzett előfizetői set-top boxok vezérléséhez szükséges információkat is a transport streambe ülteti. A készülék fényképe az 1. ábrán látható.



1. ábra

CW-4861 Pay TV Scrambler

Kódoló egy transport streamre, azon belül 64 összetevőre

A fejlesztés során fontos célkitűzés volt, hogy a rendszerek üzemeltetői mind-mind más kódolású rendszert kapjanak, így a rendszerek között az előfizetők ne tudjanak egyikből a másikba átjárni, ügyeskedni. Ennek érdekében a TotalCrypt üzemeltetői saját azonosítót kapnak, és a rendszer csak saját dekódereivel működik. Az azonosító számot – az egyébként univerzális kialakítású CW-4861-be – a felhasználónak üzembe helyezéskor kell beprogramoznia.

Az azonosító mellett az üzemeltetőnek kell beprogramoznia a kódolandó streamek PID értékét és a kódolás módját. A kódolás módját 8 különböző típusú kulcs állítja és a felhasználó programozással határozza meg, hogy az ő rendszerében mely kulcsállásokkal történjen a titkosítás. A kulcsok időben bármikor átállíthatók, esetleges feltörés esetén sincs szükség a rendszer lecserélésére, a kódolási eljárást az üzemeltető maga is bármikor meg tudja változtatni. A kulcsok időben változó mozgásra is programozhatók.

Fontos tudni, hogy egy hálózaton belül tetszőleges számú csatorna adatfolyamának kódolására van lehetőségünk, mivel a dekóderek 10, 20 vagy 50 Pay Tv Scrambler-rel is képesek egyidejűleg működni.

## 3. Hogyan történik az előfizető azonosítása?

A TotalCrypt rendszer dekódere a set-top box (majd nemsokára a digitális tv-vevőkészülék) Common Interface (CI) csatlakozóján keresztül lép a rendszerbe. A 2. ábrán látható TCM-061 Descrambler Modul egyedi azonosító számmal rendelkezik és csatlakoztatása után önállóan kommunikál a set-top boxszal. A kommunikáció végén kikéri a transport streamet a set-top box-ból, megkeresi benne a neki címzett utasításokat, és ennek megfelelően elvégzi a szükséges dekódolási lépéseket. A számára előírt dekódolást követően az átalakított transport streamet adja vissza a set-top boxnak.

A Scrambler azonosítójuk alapján kezeli a modulokat. A modulok száma egy hálózaton belül nem lehet több, mint 500 000. A modul csak akkor működik, ha a TS-ben érkező Provider Identifier Key és a Station Identifier Key megegyezik a modulban tárolt értékkel.

2. ábra

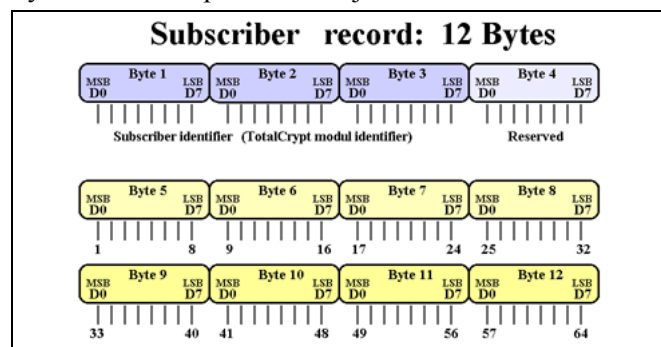
A CI adapterbe helyezendő  
TCM-061 típusú  
Descrambler Module fényképe



A röviden PI Key és SI Key-nek nevezett két azonosító a korábban említett üzemeltetői azonosító, amely azt biztosítja, hogy az egyik hálózathoz ne lehessen a másikba átvinni a modulokat. A tervezés során úgy találtuk megfelelőnek, ha a kódoló legalább másodpercenként kommunikál a modullal azért, hogy a bekapcsolást vagy a csatornaváltást követően a feléledési idő ne legyen több, mint 1 másodperc.

#### 4. Hogyan történik a vétel engedélyezése?

A TotalCrypt rendszer az előfizetői adatokat fájlba rendezve várja. A fájl felépítése nagyon egyszerű, 12 bájtos recordokból áll. Az első 4 bájt tartalmazza az előfizető azonosítóját, pontosabban a Descrambler modul címét, a további 8 bájt minden egyes bitje külön-külön vezérli a 64 tagú descrambler működését. 0 esetén a működés letiltva, 1 esetén engedélyezve. Egy ilyen record felépítését mutatja a 3. ábra.



3. ábra

A record szerkezete az előfizetői fájlban

Az SW-4861 Pay TV Scrambler Controller szoftver tetszőleges méretű fájlt tud fogadni, így a rendszer akár egy előfizetővel is működtethető. A szoftver két exe-vel rendelkezik, az egyik az üzemeltető (szakember), a másik a kezelő személyzet számára készült. Az üzemeltető programját futtatva a teljes rendszer konfigurálható és tesztelhető, a teszteléshez előfizetői engedélyező fájl is készíthető, illetve segítségével nagyobb fájlokba is betekintést nyerhetünk. A kezelő személyzet programját futtatva mindössze az előfizetői adatbázis betöltésére van lehetőség. Élesben működő hálózatoknál az előfizetői adatokat a számlázó szoftvertől várja a rendszer. Számos felhasználónk kérésére alakítottuk úgy az előfizetők kezelését, hogy ügyesebb felhasználóink maguk is kézbe vehessék ennek irányítását. Nagyobb rendszerek működtetéséhez az ECO-Soft céggel vagyunk kapcsolatban az előfizetők számlázó programból történő kezelésére.

A CW-4861 két memóriával rendelkezik, így az előfizetői adatok a folyamatos működés zavarása nélkül, üzem közben is bármikor módosíthatók.

#### 5. Hogyan lehet feltörni a rendszert?

A hozzáférést korlátozó rendszerek két legfontosabb jellemzője a minőség és a feltörhetőség. A minőségről a digitális technikában nincs mit beszélni, ha működik a rendszer, akkor a minőségnek azonosnak kell lennie a stúdióminőséggel. A feltörhetőséget a kódolás megfejthetősége és a hamisítás oldaláról kell megvizsgálni.

- Megfejthetetlen kódolás nem létezik, minden megfejtés csak eszköz és idő kérdése. A hackerek a legkritikábban próbálkoznak ezzel a módszerrel, mivel könnyebb és olcsóbb a fejlesztői környezetből megszerezni az információkat, mint a tényleges kódolást megfejteni. A TotalCrypt ez irányból is erőteljesen védett, a kódolást csak néhányan ismerik.
- A feltörés leggyakoribb módja a hamisítás, azaz megkísérlik a dekódoló modult lemásolni, sokszorosítani. A TCM-061 Descrambler Modulban a ma létező legkorszerűbb (hi-tech) FPGA került alkalmazásra, amelyet direkt ilyen célokra fejlesztettek ki úgy, hogy a benne tárolt adatokat ne lehessen kiolvasni. A tervezetthez képest azért csúszunk néhány hónapot a fejlesztéssel, mert csúszott ezen IC-k amerikai fejlesztése. Jelenleg is e típus ES (Engineering Sampling) mintáival dolgozunk és egy nagyobb kapacitású változatot használunk, mert a kisebb testvér nincs még készen. A hamisíthatatlanságot itt az alkalmazott különleges flash technológia biztosítja.

#### 6. Hány streamet dekódol egyszerre a modul?

A TCM-061-es modul 64 dekódoló egységgel készül, így egyidejűleg akár mind a 64 kódolt stream dekódolva jelenik meg a kimenetén. Különleges, professzionális alkalmazásoknál ez a tulajdonsága kiemelkedő előny lehet.

#### 7. Hogyan alakul a TotalCrypt ára?

A TotalCrypt rendszer kedvező ára lehetővé teszi, hogy egészen kis rendszerek is alkalmazzák. A fejjel-omási kódoló, amely a 8 MHz-es sávban lévő 8-10 programot kódolja 950.000 Ft+ÁFA. A dekódoló modul ára a tesztekhez 39,90 EUR. A modul jellemzően három importált alkatrészből áll, ezért az áráról csak Európában lehet beszélni. Jelenleg 1000 db gyártása van folyamatban, amelynek célja a felhasználói tesztek igényeinek biztosítása. A további ár a gyártási darabszám függvénye lesz.

Több csatorna kódolása esetén csak a fejállomás egységek számát kell növelni, a modulok gyakorlatilag korlátlan csatornaszámig használhatók.

Zigó József



## Újdonságok, ajándék a CW-Net használóinak

Folyamatosan bővül a CW-Net felhasználói köre

*Korábbi ígéretiünknek megfelelően folyamatosan gondoskodunk arról, hogy a CW-Net használói újságunk valamennyi számában találjanak néhány újdonságot, érdekességet. Ezúttal a profi felhasználókat lepjük meg néhány új megoldással.*

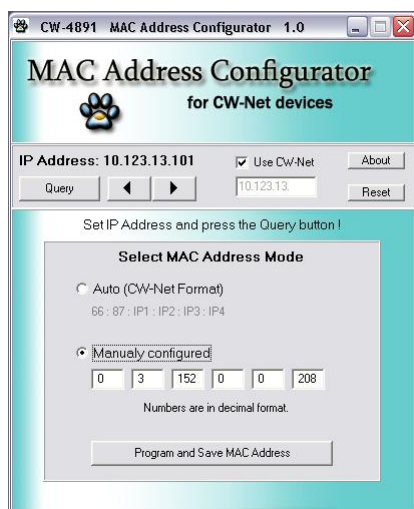
### 1. A MAC cím programozhatóságának lehetősége

A számítógép hálózatokban nem lehet két készüléknek azonos MAC címe. A hálókártya gyártói ezt úgy biztosítják, hogy központi helyen regisztráltatják magukat és a részükre fenntartott tartományból minden kártyába egyedi címet íratnak.

A másik lehetőség – ezt választotta a CableWorld is – a felhasználó által definiált MAC cím használata, de ezt a rendszergazdának komolyan kézben kell tartania. A CableWorld úgy vette le e komplikált feladatot a felhasználók válláról, hogy a MAC cím első két bájtyába h42, h57 értéket írt és az egyediséget a következő négy bájtbá épített IP címmel oldotta meg.

Most, hogy Európa egyre több országában, egyre nagyobb cégek, egyre nagyobb rendszerekben használják a CW-Net vezérlést, többen kérték a részükre lefoglalt MAC cím tartományának használhatóságát. A CW-Net Controller 1.50 szoftver változatától kezdődően lehetősége van a felhasználónak bármilyen MAC cím beállítására. A MAC beállítása a honlapunkról letölthető SW-4891 szoftverrel végezhető el. A szoftver kezelőfelülete az 1. ábrán látható.

A kezdő felhasználókat arra kérjük, hogy csak abban a esetben merészkedjenek e területre, ha pontosan



tudják, hogy mit csinálnak. A profik is vegyék figyelembe, hogy a MAC megváltoztatása után a switchek stb. a MAC tábla frissítéséig nem látják a készüléket.

1. ábra  
Az SW-4891 MAC Configurator kezelőfelülete

### 2. A TS folyamatos rögzítése fájlba

Az SW-4811 Transport Stream Analyzer szoftver továbbfejlesztése az első változat megjelenése óta folyamatos. Az elmúlt hetekben számos felhasználónk kérésére elkészült a transport stream folyamatos rögzítését biztosító modul, amelynek használatához adunk rövid előzetest.

Bevezetésként le kell szögezni, hogy a transport stream általában egy 40-50 Mbit/s sebességű adatfolyam, amelynek fájlba írása némi figyelmet igényel. A nagy adatsebesség miatt az első lépés annak a fájlnek a létrehozása, amelybe az adatfolyamot bele kívánjuk tenni. Szoftverünk a fájl elején egy 256 bájtos azonosítót helyez el, amelybe a project neve és a felvétel időpontja is belekerül. Ezt követően indulhat a beérkező adatfolyam folyamatos fájlba írása. A nagy adatsebesség miatt a fájl mérete igen gyorsan nő és hamar elérheti a GBájtos nagyságrendet így akár a HD teljes szabad kapacitását is elfoglalhatja. A figyelmetlenségekből adódó hibák elkerülésére egy biztonsági kapcsolót is beépítettünk, amellyel a fájl mérete 10 MB és 100 GB közé korlátozható.

Az ilyen óriás méretű fájlok analízálása nehézkes, ezért a szoftver egy vágót is tartalmaz, amellyel a fájl tetszőleges helyéről kivágható egy kisebb minta, amely a vágást követően azonnal bekerül az analízátorba, de önálló fájlként is menthető.

### 3. TS Analyzer szoftver újabb változata

Az elmúlt év tapasztalata azt mutatja, hogy például a TS Analyzer szoftver fejlesztése soha sem fejezhető be, mivel hetente jelentkeznek az újabb és újabb felhasználói igények. Annak érdekében, hogy felhasználóink még aktívabban bekapcsolódhassanak e fejlesztésekbe és már a részeredményeket is használni tudják, májusban azzal a felhívással tesszük honlapunkra az új változatot, hogy

**teszteljük és fejlesszük közösen!**

Valamennyi teszt eredményt és javaslatot szeretettel várunk, a jó ötleteket igyekszünk mielőbb beépíteni és közzétenni. A gyártó részéről új, eddig nem említett modulként a real time sebesség analízátort adjuk ajándékként, amelynek megismerése és használata kellems időtöltés lehet.

Zigó József

**CableWorld Kft.**

H-1116 Budapest  
Kondorfa utca 6/B  
Hungary

Tel.: +36 1 371 2595

Fax: +36 1 204 7839

✉ 1519 Budapest, Pf. 418, Hungary

E-mail: cableworld@cableworld.hu

Internet: www.cableworld.hu