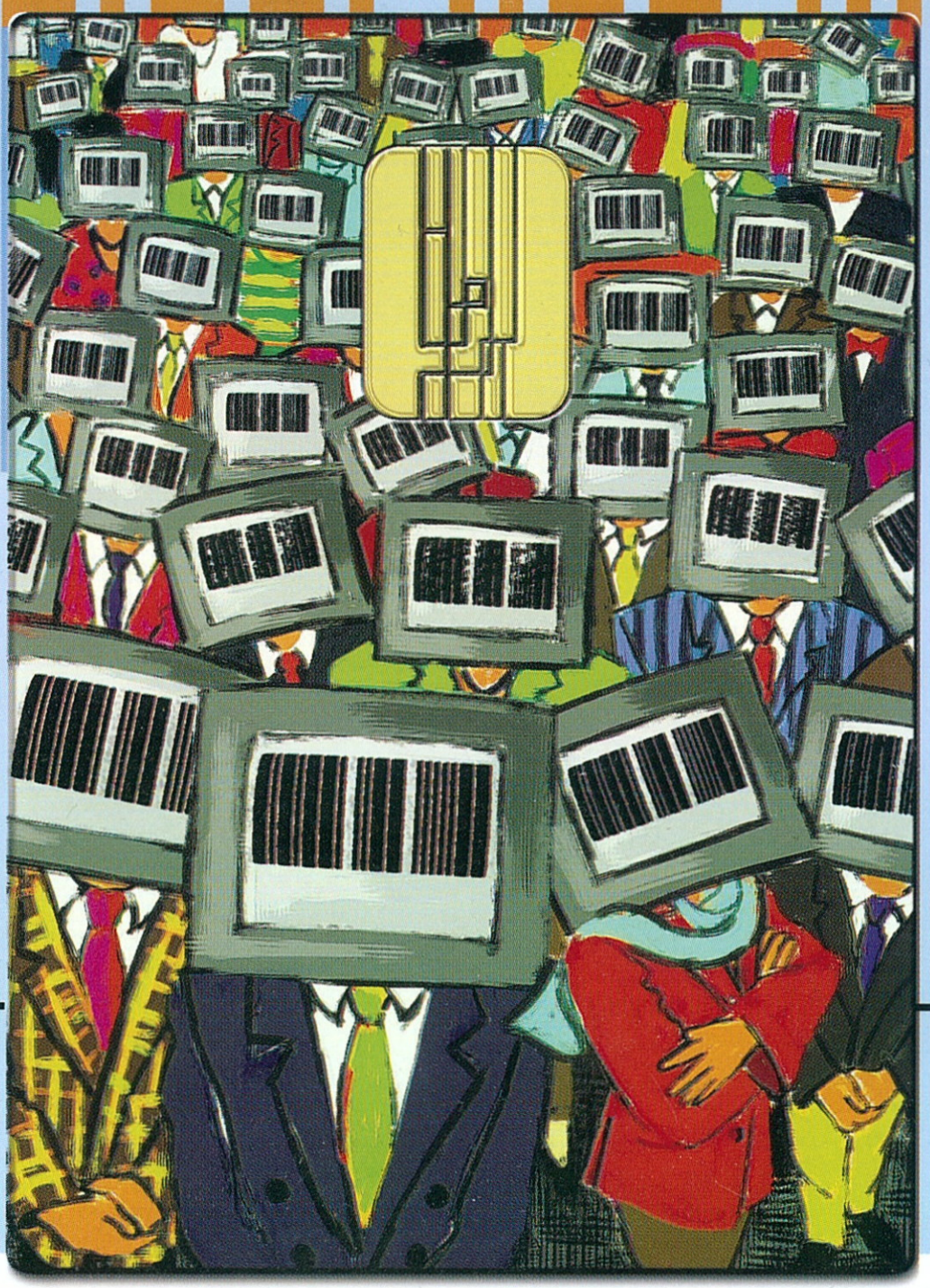
Allaga Gyula, Avar Gábor, Jancsó Tamás, Melis György, Sárkány Márta

A vonalkódtól a chipkártyáig

AUTOMATIKUS AZONOSÍTÁS ELMÉLETBEN ÉS GYAKORLATBAN



- **36 00**
- **45 000 liter**
- **5 kamion elemesbut**
- **45 000 naposcsibe,**
- **60 000 méter rézhuzal,**
- **2000 doboz parfüm,**
- **3 konténer színes ceruza:**
  – 26 000 zöld,
  – 14 000…

Cikksz. 00-4567-00-56
-4567-5678
00-4567456
ksz. NGT-02678-8
Cikksz. G-3567
Cikksz. 009-00063-DOP
Cikksz. AAA-AA-45
Cikksz. VTK-356
Cikksz. ?
Cikksz. 00-4567-00-56
Cikksz. 689-3567
Cikksz. 10-4555-09-26
Cikksz. 10-4555-09-26-A

Ki győzi követni?

A nagy tömegű áru gyors továbbítása a modern logisztika feladata. A rádiófrekvenciás azonosítás gyorsítja, és biztonságosabbá teszi a szállítási láncban az áru útját.

Miért előnyös az RFID az Ön cége számára?

- Hatékonyabb, mint az optikai (vonalkódos) rendszerek,
- több információ tárolására és továbbítására alkalmas,
- az adatok nagyobb távolságból is leolvashatók,
- strapabíró, tehát mind alacsony, mind magas hőmérsékleten képes működni,
- egy időben több címke is leolvasható, mégis kisebb a hibalehetőség.

Felkeltettük az érdeklődését?

Tudjon meg többet az Állami Nyomda RFID megodásairól az interneten: **www.allaminyomda.hu/rfid**

ÁLLAMI NYOMDA RT.

RFID
ÁLLAMI NYOMDA

1102 Budapest, Halom u. 5. Telefon: 431 1200

3. kötet

A vonalkódtól a chipkártyáig

A VONALKÓDTÓL A CHIPKÁRTYÁIG

ISBN 963 04 5800 4 ö
ISBN 963 00 6865 6

Kiadja az Adverticum Rt.
Felelős kiadó: Szabó Hedvig Mária vezérigazgató
Tipográfia és nyomdai előkészítés: Adverticum Rt.

Nyomdai munka:
RO-LA Valkó
Felelős vezető:
Rózsavölgyi Sándor ügyvezető igazgató
Tel.: 28/483-118
www.rola.hu
E-mail: ro-la@rola.hu

Allaga Gyula – Avar Gábor – Jancsó Tamás –
Melis György – Sárkány Márta

A vonalkódtól a chipkártyáig

5. változatlan kiadás

adverticum rt.

Budapest, 2007

A szerzőkről

Sárkány Márta
közgazdász-tanár

Cégét 1994-ben alapította, több sikeres vállalkozás fejlesztési és stratégiai tanácsadója. 1994-ben Tokióban menedzserdiplomát kap, majd Angliában és az USA-ban több ízben ösztöndíjasként tanulmányozza az automatikus azonosítási piacot. Az utóbbi években az informatikai rendszerek és a szervezet fejlesztése témájában végez kutatásokat. A Vonalkódtechnika és a Kártyás rendszerek című könyv társszerzője.

Allaga Gyula
villamosmérnök

A Sárkány Rt. résztulajdonosa és elnöke. Több mint 10 éve foglalkozik automatikus azonosítási problémákkal. A vonalkód és a chipkártya nyomtatásának specialistája, szervezési szakértő. A Vonalkódtechnika és a Kártyás rendszerek című könyv társszerzője.

Avar Gábor
okl. gépészmérnök, szervező szakmérnök

A Videoton Számítástechnikai Gyárában a minőségbiztosítási osztályon dolgozik, majd számítógéplicencek átvételében és honosításában vesz részt. A Bull Magyarországnál az indirekt eladási csatorna felépítésének aktív szervezője, majd az egészségügyi alkalmazások koordinálója. A Vonalkódtechnika és a Kártyás rendszerek című könyv társszerzője.

Melis Zoltán
villamosmérnök, mérnök-közgazdász

A BCS Hungary Kft. tulajdonos-ügyvezetője, három idegen nyelven beszél. Programozóként indul a pályán. Saját vállalkozását 1992-ben indítja, elsősorban az angliai szakmai képzéseken és külföldi munkahelyeken szerzett tapasztalatok alapján. A Vonalkódtechnika és a Kártyás rendszerek című könyv társszerzője.

Jancsó Tamás
aerofotogeodéta mérnök

A Sárkány Rt. koordinációs igazgatója, több idegen nyelven beszél. Fejlesztési projektek szervezésében és az ehhez szükséges partnerkapcsolatok kialakításában vesz részt. Jelenleg is több kutatási projekt témavezetője és koordinátora, az automatikus alakfelismerés specialistája.

A könyv szakmai fejezeteinek megírásáért köszönetet mondunk:
Dr. Balogh Pálnak (LiB Kft.)
Magyar Bélának (EAN Consulting)
Dr. Nádor Györgynek
A Login Kft. munkatársainak
A Gábor Dénes Informatikai Főiskola hallgatóinak

Tartalomjegyzék

Alkalmazási riportok

Előszó

Az automatikus azonosítás ma már átszövi mindazon területek tevékenységét, ahol nagy tömegű információt kell a számítógépes rendszerbe integrálni. Az utóbbi években az internetes technológia, az adat- és információcsere fejlődési üteme annyira felgyorsult, hogy kulcskérdéssé vált az azonosíthatóság. Külön iparág fejlődött ki az automatikus azonosítási feladatok megoldására. A sort a vonalkódtechnika nyitotta meg, és napjainkban az azonosítási módszerek sora tovább bővül. A különféle azonosítási technikáknál, az újabb és újabb módszereknél nem az a fő jellemző, hogy melyik a fejlettebb, hanem az, hogy ezek különféle funkciókat képesek ellátni, és ma már árnyaltabban, hatékonyabban választhatjuk ki az adott probléma megoldásának legjobban megfelelő azonosítási technikát. Így a legfontosabb elem, amit a rendszerek tervezésénél figyelembe kell venni, az, hogy mindegyik típusú azonosítástechnika más-más területen jelent hatékony megoldást az automatikus azonosítási megoldások közül.

Magyarországon több mint tíz éve jelentek meg a vonalkódos szakcégek, s fejlesztenek, telepítenek rendszereket a legkülönbözőbb felhasználási területeken: a kereskedelemben, a könyvtárakban, a gyógyszertárakban, a benzinkutaknál, a legkülönbözőbb profilú iparvállalatoknál vagy sporteseményeken. A nagy tömegű információ feldolgozásánál ma már nálunk is szinte minden esetben alkalmaznak vonalkódtechnikát.

A vonalkódos rendszerek fejlesztésére fordított összegek évről évre dinamikusan növekednek világszerte.

Ahol az adatbevitelnél fontos szerepet játszik az egyértelmű és biztonságos azonosítás, az egyéb automatikus azonosítási technikák használata jelenti a megoldást a felhasználóknak. Az idő és a távolság elhanyagolható tényezővé válik, hiszen az árumozgásnál, személyek, eszközök és alkatrészek azonosításánál, pénzügyi tranzakciónál az azonosítás egyértelműen és gyorsan elvégezhető vonalkód, chipkártya, ujjlenyomat-scanner stb. segítségével. Az ilyen rendszerek pontos és percrekész adatszolgáltatási lehetősége jobban szolgálja és gyorsítja a vezetői döntések meghozatalát. Azt, hogy milyen azonosítási technikát válasszunk, mindig

a célnak és a stratégiának kell meghatároznia. A vonalkód alacsonyabb biztonsági szintet nyújt, mint a chipkártyás azonosítás, viszont mindkét típusú felhasználás gazdaságosan és célszerűen alkalmazható. Az e-business terjedésével ma már a biometrikus és a chipkártyás technikák kerültek előtérbe, de ez nem csökkentette a vonalkód iránti keresletet.

Több éve működő, egymáshoz hasonló kereskedelmi rendszerek hosszú távú gazdasági elemzésénél megállapították (nem hazai adat), hogy a vonalkód bevezetése a költségeket egyrészről 2%-kal növelte, másrészről 6%-kal csökkentette. A magyar sajátosságok ennél a 4%-nál nagyobb profitot is eredményezhetnek. Nem egy olyan hazai alkalmazási példát ismerünk, ahol a vonalkódos rendszer 1,5-2 hónap alatt megtérült.

Az automatikus azonosítás piacán a nemzetközi összehasonlítások szerint Magyarország továbbra is az élvonalban van. Hazai szakembereink megszerzik mindazt a tudást, amely Nyugat-Európában hozzáférhető. Az újabb keletű – pl. a chipkártyás és egyes biometrikus – azonosítási technikákat egyre több hazai cég kínálatában találhatjuk meg. A magyar szakcégek nemzetközi színvonalú referenciákkal rendelkeznek, amiről az általuk írt alkalmazási riportokból is megbizonyosodhatunk. A regiszterben a legjelentősebb hazai vállalkozások listája található, tőlük szerezhetők be konkrét ajánlatok egy-egy problémára.

Egyre több felsőoktatási intézmény és oktatási központ ismeri fel azt a tényt, hogy az automatikus azonosítás mint önálló tantárgy érdemes arra, hogy szervesen beépüljön a tantervbe.

Összegezve: egy informatikai rendszer alapkérdéseként fogalmazódik meg az adatbevitel, az azonosítás, az információk automatikus felismerése – s ehhez szolgáltat háttéranyagot A vonalkódtól a chipkártyáig című könyv.

Ajánljuk ezt a kötetet mindazoknak, akik az automatikus azonosítás alkalmazói, vagy most ismerkednek az ilyen rendszerek lehetőségeivel.

Köszönetet mondunk mindenkinek, akik munkánkat segítették.

A SZERZŐK

Vonalkódtechnika

A vonalkód

A vonalkódtechnikáról általánosságban

A vonalkódtechnika az automatikus azonosítás leggyakrabban használt eszközeinek egyike. Automatikus azonosítás alatt azokat az eljárásokat és technikákat értjük, amelyek lehetővé teszik, hogy emberi beavatkozás nélkül egy objektumról adatokat nyerjünk, és azokat további feldolgozásra alkalmas formára átalakítsuk.

A legfontosabb automatikus azonosítások közé tartozik a vonalkódtechnikán kívül a rádiófrekvenciás azonosítás (RF), az optikai karakterfelismerés (OCR), a mágneskártya-azonosítás, a hangazonosítás, az alakfelismerés, a biometrikus azonosítás és a smart cardok.

Már az 50-es évek végén megjelentek az első, gyakorlatilag is alkalmazható vonalkódolvasók, de az igazi áttörés a 70-es évek elején kezdődött, és a fejlődés napjainkban is tapasztalható.

Az első kereskedelmi alkalmazás 1973-ban történt, az USA-ban, ahol a kiskereskedelemben kezdték el használni az UPC-ről elnevezett vonalkódtípust. Ezt eleinte kizárólag fogyasztási cikkek körében használták, de 1980-tól már ajánlást tettek valamilyen vonalkód alkalmazására gyűjtő- és szállítási csomagolásokon is.

Európában az UPC mintájára alakult meg az EAN Nemzetközi Termékszámozási Társaság 1977-ben, 12 európai ország részvételével, brüsszeli székhellyel; célkitűzése egy egységes termékazonosítási rendszer világméretű bevezetése, amely a vonalkódra épül. Magyarország 1984-ben csatlakozott a társasághoz, a képviseletet a Csomagolási és Anyagmozgatási Országos Szövetség látja el. Többek között az EAN dolgozta ki az elektronikus adatcserére vonatkozó EANCOM szabványt az ENSZ EDIFACT rendszerével összhangban.

A fogyasztási csomagolásokon szereplő EAN kódok műszaki előírásait az MSZ 20451 számú szabvány határozza meg.

A vonalkódtechnikában rejlő lehetőségek

Előnyei:

- egységes, szabvány által meghatározott azonosítók,
- alacsony költség,
- könnyű előállíthatóság,
- nagy sebességű olvasás lehetősége,
- viszonylag nagy távolságról is pontosan olvasható,
- sokrétű alkalmazás.

Hátrányai:

- korlátozott információtartalom,
- nem dinamikus,
- speciális környezetben nem alkalmazható (szélsőséges környezeti körülmények),
- hamisítás lehetősége.

Hatásai:

- termelékenység növekedése,
- költségek csökkenése,
- akár 40%-os raktárkészlet-csökkenés,
- selejtmentes gyártás,
- just-in-time technológia,
- disztribúció és szállítási feladatok akár 1/7 idő alatt történő elvégzése,
- a termelés bármilyen szállítási egység szintjén követhető (például raklap, sor, karton stb.),
- logisztikai kapcsolat anyagfolyam és termékfolyam között,
- minőségi előírások betarthatósága és regisztrálhatósága.

A vonalkód kialakulásának története

A vonalkód ősének sokan a Morse-kódot tekintik, amelyben az angol ábécé betűi és a számjegyek szerepelnek különböző hosszúságú jelek és a köztük lévő szünetek formájában. Például az

A betű formája: jel–szünet–jel–jel, ugyanez számjegyekkel: 1011; vagy a

B betű formája: jel–jel–szünet–jel–szünet–jel–szünet–jel, amely számjegyekkel: 11010101.

A többi betű is hasonló, eltérő számú és váltakozó elhelyezkedésű jel sorozatából áll, amelyeket a megkülönböztetésükhöz szükséges szünet választ el egymástól. Az említett „jel" az elemi információ, egy bit, vonalkódos nevén: modul.

A vonalkód két lényeges pontban tér el a Morse-kódtól. Egyrészt a modulok közti szünet nem egyszerűen a jel elválasztására szolgál, hanem maga is jelértékű információ lehet, tehát a vonalkód sötét és világos modulok sorozatából áll. Másrészt egy kódolandó karakter mindig rögzített számú modulból áll, s azon belül a sötét és világos jelpárok száma is rögzített.

Nézzünk egy példát a könnyebb érthetőség kedvéért. Az egyik vonalkódtípus mindegyik karaktere hét modulból és azon belül két jelpárból áll, azaz:

1 számjegy kódja:	0	0	1	1	0	0	1	
	1	2	3	4	5	6	7	a modulok sorszáma
	1	1	1	1	2	2	2	a jelpárok sorszáma
2 számjegy kódja:	0	0	1	0	0	1	1	
	1	2	3	4	5	6	7	a modulok sorszáma
	1	1	1	2	2	2	2	a jelpárok sorszáma

(A kódban az 1 a sötét, a 0 a világos modult jelenti.)

A kódolás paramétereinek rögzítése egyben meghatározza a kódolható karakterek számát is, hiszen meghatározott számú modulból meghatározott számú elempárt csak véges és könnyen kiszámítható módon tudunk kiválasztani.

Az alábbi táblázatban néhány vonalkódtípust hasonlítunk össze kódolási méreteik szerint.

Kódtípus	Modulméret	Jelpárok száma	Kódolható karakterek száma	Felhasználható karakterek száma	Biztonsági faktor
EAN/UPC	7	2	20	10	2,0
CODE128	11	3	252	106	2,4
PDF417	17	4	10480	2787	3,8

A biztonságos olvasás érdekében nem használják ki a teljes kódolható karaktermennyiséget, hanem úgy választják ki a felhasznált karaktereket,

hogy azok kódja a lehető legjobban eltérjen egymástól. Így az apró nyomtatási hibák és az olvasás bizonytalanságai a legkisebb valószínűséggel eredményeznek hibás adatfelismerést.

A vonalkód felépítése

- nyugalmi zóna,
- start karakter (nem minden vonalkódtípusnál),
- kódolt adatok (a lényeges információt tartalmazzák),
- ellenőrző karakter (nem minden vonalkódtípusnál),
- stop karakter,
- nyugalmi zóna,
- értelmező sor.

A kereskedelemben leginkább az EAN kódok használatosak, általában az EAN-13 az elterjedt. E kód 13 karakterből áll, az első kettő-három tartalmazza az ország azonosítóját (Magyarországé 599). A következő négy-öt karakter a gyártó azonosítója, amelyet a Magyar Gazdasági Kamara Csomagolási és Anyagmozgatási Országos Szövetség ETK/EAN Irodájánál igényelhetnek a gyártók. Újabb négy-öt karakter adja meg a termék azonosító karaktereit. Az utolsón az ellenőrzőszám szerepel. Az EAN-8 az EAN-13 rövidített formája. Rögzített hossza 8 karakter. A kettő közötti lényeges eltérés az ellenőrzőszám képzésében van.

A főbb vonalkódtípusok

A hagyományos vonalkódok felépítése azonos: egymással párhuzamos fekete és fehér vonalak alkotják. Egy előre meghatározott szabály szerint a vonalak és közök szélességének változása hordozza az információt.

Az egyes vonalkódok abban különböznek, hogy egy adott karakternek milyen fekete és fehér vonalakból álló struktúrát feleltethetünk meg. Legegyszerűbb, ha a Morse-ábécére gondolunk, ahol az átvitt hangjelzések hosszának megfeleltethetünk egy arányos szélességű vonalat.

Minden vonalkódtípus egy általános szabályrendszer szerint épül fel, ugyanakkor szinte mindegyik megsérti az általános elvek legalább egyikét. Valamennyi vonalkód felépítése az alábbi struktúrán alapul: a vonalkód elején egy nyugalmi zóna található, ezt követi a start karakter, egy vagy több adatkarakter, opcionálisan egy vagy több ellenőrző karakter, majd a stop karakter, végül a hátsó nyugalmi zóna.

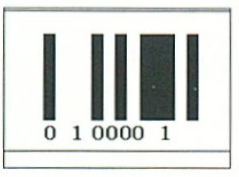
Egy vonalkód karakterkészlete azt adja meg, hogy az adott kódrendszer segítségével milyen karakterek kódolhatók (numerikus, alfanumerikus, kis- és nagybetűk, vezérlő karakterek). A vonalkód modulmérete (X méret) a vonalkódot alkotó legkeskenyebb vonal fizikai szélességét határozza meg, és általában a hüvelyk ezredrészében adják meg (mil).

A vonalkódok lehetnek fix vagy tetszőleges hosszúságúak. (Ebben az esetben csak az olvasás gyakorlati követelményei szabnak határt.) Önellenőrző a kód akkor, ha egy egyszerű nyomtatási hiba hatására nem kapunk vissza más karaktert olvasáskor, azaz nem történik úgynevezett helyettesítési hiba. Önszinkronizáló a vonalkód, ha az olvasó a kód struktúrájából tud következtetni a vonalak és vonalközök relatív szélességére.

Vonalkódok csoportosítása fizikai felépítésük szerint

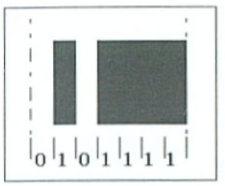
Bináris és deltakódok

A vonalkódok egyik csoportját alkotják a bináris kódok. Közös jellemzőjük, hogy a széles vonalakhoz és vonalközökhöz egy bináris 1-est rendelünk, míg a keskeny vonalakhoz, illetve vonalközökhöz 0-t.



A keskeny és széles vonalak aránya rögzített, általában 1:2 és 1:3 között mozog. A vastag elemek rögzített száma biztosítja az egy karakter kódolásához szükséges hely szélességének állandóságát és az önszinkronizáló tulajdonságot.

Az úgynevezett (n,k) kódok közé sorolják a többi vonalkódot (delta-kódok). Ezek közös jellemzője, hogy a fekete vonalakhoz a szélességüknek megfelelő darabszámú 1-est rendelünk, míg a vonalközökhöz hasonló szempontok alapján 0-kat.



Az (n,k) típusú kódok rögzített számú vonal- és vonalközpárból állnak (k), melyek kiterjedése ugyancsak rögzített számú modulból áll (n), azért, hogy az önszinkronizáló tulajdonság biztosítva legyen. Az EAN kód egy (7,2) típusú (n,k) kód.

Diszkrét és folytonos kódok

Ez a vonalkódtípusok egy másik osztályozását jelenti. Diszkrétek azok a kódok, ahol a karaktereket elválasztó vonalközök nem hordoznak információt. A megoldás a Morse-kód alapjait követi (Diszkrét 2of5, Kód39).

Az úgynevezett folytonos kódok esetében a karakterek közötti szünetek is részei a kódnak, így információt hordoznak (Interleave 2of5, UPC/EAN, Kód128, PDF417).

Egy- és többjelentésű kódok

További osztályozási lehetőség annak vizsgálata, hogy az adott vonal/vonalköz egyértelműen meghatároz-e egy adott karaktert, vagy sem. A vonalkódok többsége egyjelentésű, azaz egyértelműen hozzárendelhető egy karakter egy vonalakból álló mintázathoz (Kód39, Interleave 2of5, UPC/EAN).

A többjelentésű kódok több karakterkészletet kódolnak, amelyek között vezérlő kódokkal választhatunk. Az elv hasonló a számítógép billentyűzetén található Shift és Alt billentyűk funkciójához (Kód128, PDF417).

Hagyományos vonalkódok

A hagyományosnak titulált vonalkódok közös jellemzője, hogy szerkezetük egymással párhuzamos vonalak sokaságával jellemezhető. Felépítésüknél fogva nagyfokú redundanciát tartalmaznak, azaz az információtartalom a vonalak magasságában többszörösen ismétlődik.

UPC

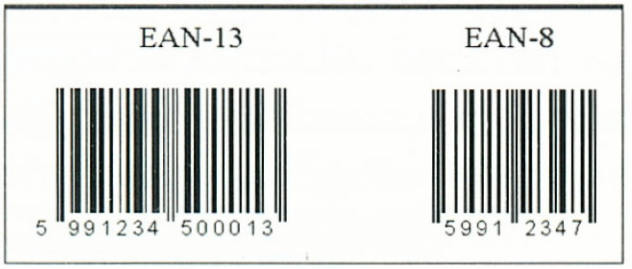
Az UPC kód egy vonalkódtípust és egy termékazonosítási rendszert takar egyidejűleg. Az adattartalom meghatározása nem önkényes, meg kell felelnie az egyedi termékazonosító kiadásáért felelős szerv előírásainak.

A kódot tipikusan kereskedelmi alkalmazásokra fejlesztették ki kb. 20 évvel ezelőtt az USA-ban. Rögzített hosszúságú (12, illetve 6 karakter), numerikus, (7,2) típusú kód. Önellenőrző, folytonos, moduló 10-es ellenőrző algoritmust használ.

EAN

Az EAN ötvözi az UPC kódot, így az első világméretű termékazonosító rendszer és kódtípus. Az adattartalomnak az UPC-hez hasonlóan meg kell felelnie az egyedi termékazonosító kiadásáért felelős szerv előírásainak.

Az EAN-13 felépítése az alábbi szabályokat követi: az első 2 vagy 3 karakter az országazonosító, például Magyarország 599. A rákövetkező négy-öt a gyártó azonosítója. A további karakterhelyeken, egészen a 12.-ig a termékazonosító karaktert találjuk, amelynek meghatározása a gyártó feladata. Az utolsó karakteren szerepel az ellenőrző szám. Az EAN-8 az EAN-13 rövidített formája, egyszerű helytakarékossági okokból.



Rögzített hosszúságú (13, illetve 8 karakter), numerikus, (7,2) típusú kód. Önellenőrző, folytonos, ellenőrző jeggyel a végén.

Az UPC és EAN kódok elláthatók egy kiegészítő kóddal, amely 2 vagy 5 karakter hosszúságú lehet. Funkciója a termékváltozatok egyedi jelölése, így például azonos tartalmú könyv különböző kötésben történő megjelenése vagy képeslapok egyedi változatainak megjelölése.

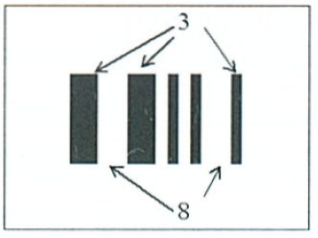
A UPC és EAN kódok nyomtatását a négyféle vonalvastagság, valamint a teljesen nyílt rendszerű felhasználás miatt körültekintően kell elvégezni. A szabvány ajánlásában megtalálhatók a mérettől függő tűrések is.

Interleave 2of5

Az Interleave 2of5 kód a „kettő az ötből" kódcsalád legismertebb tagja. Az átfedéses kettő az ötből kód az eredeti diszkrét kettő az ötből kód továbbfejlesztett változata. Egyszerű felépítésű, ugyanakkor tömör numerikus kódtípus.

Elnevezését onnan kapta, hogy egy karakter öt modulból áll, amelyből kettő széles, három pedig keskeny, s vagy csak fekete, vagy csak fehér vonalak alkotják.

Ez csak úgy lehetséges, hogy az egyik karakter sötét moduljait a másik karakter világos moduljai választják el egymástól, mintegy átszőve az egyiket a másikkal.



Fő alkalmazási területe a gyűjtőcsomagolások vonalkódos jelölése. Alkalmazása során körültekintően kell eljárni, mivel a kód részhalmaza is értelmes lehet az olvasás folyamatán. Ezt a hibalehetőséget a kód köré nyomtatott kerettel és ellenőrző összeg beépítésével lehet kivédeni.

További felhasználási területe: zárt ipari rendszerek (alkatrészek, fődarabok jelölése), egészségügyi alkalmazások (tb-kártya), okmány- és dokumentációs alkalmazások (APEH-nyomtatványok, receptek) stb.

A diszkrét kettő az ötből kód a gyakorlatban alig fordul elő, hiszen nagyon kis információsűrűséget képes biztosítani. Létezik néhány egyedi változata, amely speciális alkalmazásokban előfordulhat, így az ipari 2of5, amely egyedi start és stop karakterekkel van ellátva, valamint a Kód11, amely a - karaktert tartalmazza ráadásként.

Kód39

A Kód39 volt az első alfanumerikus kód, és zárt alkalmazásokban talán még ma is a legelterjedtebb. Ezt áttekinthető, egyszerű felépítésének köszönheti. Amikor alfanumerikus kódot kell választanunk, ez az első, amely szóba jön.

Diszkrét, önellenőrző, tetszőleges hosszúságú, amely a legkülönfélébb nyomtatási eljárásokkal előállítható. Egy karakter öt vonalból és négy vonalközből áll (5+4=9), melyből három széles (3).

A karakterkészlet 43 karakter kódolását teszi lehetővé (nagybetűk, számjegyek és néhány egyéb karakter), ellenőrző összeg moduló 43 algoritmussal képezhető.

Létezik a kódnak egy altípusa, a Kód39 teljes ASCII, amely az eredeti egyfajta kiterjesztésének tekinthető. Lehetővé teszi a teljes ASCII-karakterkészlet kódolását. A már említett módon, Shift-karakterek alkalmazásával alakították ki ezt a többjelentésű kódváltozatot. Az altípus hátránya a bonyolult felépítés és a kis információsűrűség, úgyhogy a gyakorlatban helyette szinte kizárólag a Kód128-at érdemes használni. A Kód32 elnevezésű kód ugyancsak a Kód39 egy altípusa, ahol a numerikus számjegyeket először a 32-s számrendszerbe átírva érhető el jóval nagyobb információsűrűség.

Kód128

A legszélesebb felhasználási területen megtalálható e vonalkód. Sikerének oka a nagy sűrűség melletti nagy megbízhatóság a bőséges és többféleképpen variálható karakterkészlettel.

Elnevezése az első 128 ASCII-karakter kódolhatóságából származik; (11,4) típusú, önellenőrző, folytonos kód. Hossza szabadon választható, moduló 103 algoritmussal számolható az ellenőrző összeg, amelyet a kód biztonságos olvashatósága érdekében a legtöbb esetben alkalmaznak.

A három, A, B és C jelzéssel megkülönböztetett típuskészlet közül a B jelű az alapvető, a másik kettőben csak számjegyeket kódolhatunk. A kód magába épít egy ellenőrző karaktert, amelyről a felhasználó nem szerez tudomást. Az ellenőrző karakter képzéséhez itt már a kódolandó karakternek a karaktersorban elfoglalt sorszámát is figyelembe kell venni.

A Kód128 változatait megtaláljuk más rendszerekben is, így a vérkészítmények jelölésére az ISBT128 változatot, míg a palettacímkék jelölésére az EAN-128 kódváltozatot használják.

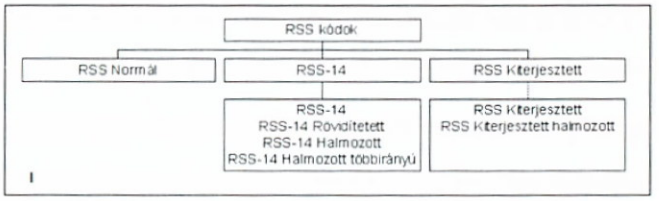
RSS

Az RSS az elmúlt két évtized egyetlen igazán új kódrendszere, amelyet kereskedelmi-logisztikai alkalmazásokra fejlesztettek ki. Az új kód-

rendszert az alábbi igények hívták életre: kisméretű és változó súlyú tárgyak jelölése és kiegészítő, másodlagos információ kódolása. A kódrendszer az EAN/UCC által kifejlesztett, a kereskedelmi folyamatokra optimalizált megoldás.

Az RSS kód önállóan is használható, vagy kétdimenziós kóddal kiegészítve, úgynevezett összetett (kompozit) kódban szerepelhet. Az RSS nem helyettesíti az EAN/UPC kódokat, viszont komplex felépítésének és különféle változatainak köszönhetően univerzálisabb jelöléstechnikát kínál.

A kód nagyméretű kódszavakból áll, amelyek legalább négy, maximum hét vonalból és vonalközből állnak. A kódszavakat alkotó vonalak egy–nyolc egység szélesek lehetnek. Valamennyi RSS kód felépítéséből következően alkalmas több irányból történő, illetve teljesen irányfüggetlen olvasásra. Ezt a kódban elhelyezett vezérlő karakterek biztosítják, amelyek mintegy irányítják az olvasót, hogy a kódnak éppen melyik részét pásztázza. Az alábbi ábrán az RSS különböző változatait foglaltuk össze.



Az RSS normál a legkisebb méretű tagja a családnak, két kódszóból és egy ellenőrző karakterből áll. A két kódszóban egy 14 hosszú EAN/UCC azonosítót és egy kapcsolómezőt helyezhetünk el, amely a 2D-kódrészre mutat. Az RSS-14 és annak négy különböző változata négy kódszóból és egy ellenőrző karakterből áll.

Az RSS kiterjesztett változata 4–22 kódszóban 74 számjegyet vagy kb. 40 alfanumerikus karaktert képes kódolni. Az irányfüggetlen olvasás és a nagy információkapacitás miatt egyedülálló tulajdonságokkal rendelkezik. Halmozott változata tulajdonképpen egy 2D-kódként is felfogható.

Egyéb vonalkódtípusok

Az ismertetett típusok mellett még számos más, kisebb-nagyobb mértékben használt vonalkód létezik, mint például a Codabar, a Matrix 2of5, az Ages, a Kód93, a Fujitsu, a Delta Distance A, a Norand, az RTC, az Ames, a Logmars, a Plessey, az AS-6, az AS-10, a Postnet, az MSI és a Nixdorf kód, amelyeket itt nem részletezünk.

A kétdimenziós (2D) vonalkódok

Mióta az EAN/UPC kódok a kereskedelmi-logisztikai folyamatok szabványos adathordozóivá váltak, a vonalkód nélkülözhetetlenné vált a gyors és pontos adatgyűjtésben. A vonalakkal ábrázolt adatformátum olcsó és megbízható, emellett az olvasást végző eszközök is nagy olvasási sebességet, megbízhatóságot és könnyű használatot szavatolnak.

A felhasználók részéről egyre több alkalommal felmerült az igény, hogy egyrészről szeretnének több információt elhelyezni a kódban, másrészről kisméretű kódban szeretnék elhelyezni ezt a növekvő mértékű információt. Mivel a korábban ismertetett hagyományos kódoknak olyan kitételeknek kell megfelelniük, mint a minimális vonalszélesség, a nyugalmi zónák, a start/stop karakterek, sokszor csak a rendelkezésre álló helynél nagyobb méretben állíthatók elő.

Ezekre a kihívásokra válaszul alakultak ki a kétdimenziós vonalkódnak elnevezett rendszerek. Felépítésük szerint két csoportba sorolhatók: egy részük úgynevezett halmozott szerkezetű kód, másik részük pedig mátrixkód.

Halmozott kódok

A halmozott kétdimenziós kódok a hagyományos vonalkódok szerkezetére jellemző vonalak és vonalközök változó szélességű sokaságából állnak. Abban különböznek a hagyományos kódoktól, hogy több, vékony szeletre hasított vonalkód kerül egymás tetejére. A legismertebb a Codablock, a Kód16k, a Kód49 és a PDF417. Valamennyi képes nagyobb mennyiségű információ kódolására, ám ugyanakkor nem jelent megoldást a kis helyigényből fakadó problémára, mivel minimális mérete megegyezik egydimenziós társaiéval,

és az olvasás iránya is kötött. Az alábbiakban röviden ismertetjük az említett típusokat.

Kód49

A kód 2–8 sorból állhat. Minden sor 4 kódszót tartalmaz a start és stop karakteren kívül, és hetven modulból épül fel. Egy kódszó 16 modulból áll, ami 4 sötét és világos modulpárt tartalmaz, s két karakter kódolását teszi lehetővé. Minden sor tartalmaz ellenőrző karaktert, és a sorok számától függően a teljes kódra vonatkozó további ellenőrző karakterek is beépítésre kerülnek, ezért maximum 49 alfanumerikus karakter vagy 81 számjegy kódolását végezhetjük el vele.

Kód16k

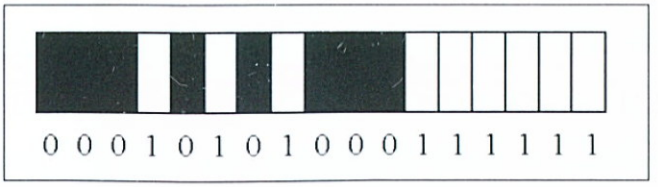
Fizikai megjelenésében nagyon hasonlít a Kód49-re. A sorok száma 2 és 16 között változhat, és minden sor egyedi start és stop karakterrel rendelkezik. Soronként szintén hetven modulból áll, amely öt karaktert tartalmaz. A sorokat egymástól és a nyugalmi zónától külön elválasztó vonal védi. A karakterek kódolása a Kód128 inverzeként történik. Több ellenőrző karaktert tartalmaz, de soronkéntit nem. A vonalkód maximum 77 ASCII-karaktert vagy 154 számjegyet tartalmazhat.

Codablock

A Kód39 struktúrárjáa épül, de elvileg létezik Kód128 és 2of5 változata is. Minden sor tartalmaz a start és stop karakterek mellett sorazonosító jeleket is. Egy sorba maximum 22 karakter helyezhető el, és a sorok száma nem lehet több, mint 62, ami összesen 1360 karakter kinyomtatására ad lehetőséget, figyelemmel a több egymásra épülő ellenőrző számra. Fizikai méretét adott korlátok mellett szabadon alakíthatjuk ki.

PDF417

A PDF417 kódrendszerben az alapvető adategység – azaz értelmezhető információt tartalmazó legkisebb elem – elnevezése a kódszó. A szimbólumot alkotó valamennyi kódszó fizikai hossza azonos, és mindet 17 egyenlő szélességű modulra lehet bontani.



Minden kódszó felépítésében 4 fekete és 4 fehér építőelem vesz részt. Ezek minimális szélessége 1, a maximális pedig 6 modulnyi. Minden esetben a 4 fekete és 4 fehér vonal teljes modulszélessége 17. Vagyis a PDF417 elnevezés (Portable Data File 4-17) a kódrendszer felépítéséből származik.

Matematikai kifejezésekkel élve az ilyen struktúrájú kódot (n,k,m) kódnak nevezik, ahol n a kódszót alkotó modulszám, k a vonalak és szóközök száma, míg m a vonalak és szóközök maximális modulszélességét definiálja.

Elsőre azt feltételezhetnénk, hogy minden kódszó egy számjegyet, egy ASCII-karaktert vagy valamilyen hasonló adategységet tartalmaz, amely vonal és szóközök formájában van kódolva. De ez nem igaz. A PDF417 kódrendszer 929 különböző kódszót definiál. Így a PDF417 „ábécéje" vagy karakterkészlete 929 elemet tartalmaz, amelyek mindegyikét egy adott vonalakból és szünetekből álló, 17 modulszélességű alakzat reprezentálja, s 0-tól 928-ig vesz fel értékeket. A PDF417 összesen tizenkét különböző üzemmódot támogat, amelyből az első három kötött, a többi pedig szabadon felhasználható.

	1.Mód	2.Mód	3.Mód	12.Mód
0. Kódszó	AA	NULL	"000"	???
1. Kódszó	AB	SOH	"001"	???
2. Kódszó	AC	STX	"002"	???
3. Kódszó	AD	ETX	"003"	???
4. Kódszó	AE	EOT	"004"	???
928. Kódszó				

Mivel a kód leolvasása alkalmával először csak az egyes kódszavak kerülnek felismerésre, dekódolásra, ezért ezt az első fázist alacsony szintű dekódolásnak hívják. A kódszó jelentésének meghatározása csak egy második fázisban történik, ezt hívják magas szintű dekódolásnak. Ebben a lépésben a kódszó jelentésének meghatározása a pillanatnyi üzemmód alapján történik, ami elméletileg egy 929 sorból és 12 oszlopból álló táblázat megfelelő cellájának kikeresését jelenti.

A PDF417-ben kilenc biztonsági vagy hibajavítási szint található. Minél magasabb biztonsági szintre ugrunk, annál nagyobb része semmisülhet meg a szimbólumnak úgy, hogy az eredeti információtartalom 100%-ban visszaállítható. A PDF417 felkínálja a felhasználónak, hogy válasszon a biztonsági szintek közül, így lehetővé teszi a hozzáadandó hibajavító kódszavak mennyiségének megválasztását.

Mikro PDF417

Ez a kód a normál PDF417 helytakarékos változata, amely az eredeti PDF417-tel kompatibilis.

Mikro PDF417

A Mikro PDF417-specifikáció néhány megszorítást tartalmaz a kód méretére, a kódolható karakterek számára és a hibajavítási képességre nézve. Az univerzális tulajdonságok korlátozása fejében egy nagyon helytakarékos kódot kapunk, amely őrzi az eredeti kódrendszer legfontosabb tulajdonságait, ugyanakkor a hagyományos méreteknél sokkal kisebb helyet igényel.

Mátrixkódok

A mátrixkódok meglehetősen kevéssé emlékeztetnek bennünket a hagyományos vonalkódokra. Ahelyett, hogy vonalakat használnának a kódoláshoz, világos és sötét cellákból építkeznek, amelyek elrendezése mátrixszerű alakzatot követ.

Ez az alternatív technológia sokkal előnyösebb, amikor nagy távolságtartományban gyorsan mozgó objektumokat kell azonosítani. Például egy csomagelosztó központban a futószalagon mozgó dobozok orientációja, távolsága az olvasófejtől véletlenszerűen változik egy adott intervallumban. A technika másik előnye, hogy nagyon kis helyen lehet kódolni nagyobb mennyiségű adatot. A hibajavítás a többi kétdimenziós kódhoz hasonlóan úgy történik, hogy a hibajavító kódszavak átszövik a kódot fizikai kiterjedésében.

Maxicode

Rögzített méretű és kapacitású kód, melynek a struktúrája is állandó. Helyzetét a központi koncentrikus körök azonosítják. Hárombites, 60°-os irányítású kódolási elrendezésre épül. Többfokozatú hibavédettséggel rendelkezik.

Data Matrix

Négyzetes elrendezésű, nagy sűrűségű kódrendszer. Elsődleges felhasználási területe az elektronikai alkatrészek jelölése. Változó kapacitású kód, helyzetét a négyzetet alkotó keretvonalak határozzák meg. Többfokozatú hibavédettséggel rendelkezik.

Napjainkban a Data Matrix elsődleges felhasználási területe az elektronikus alkatrészek azonosítása olyan direkt jelölési technikákkal, mint pl. a lézergravírozás. A kódot olyan alkalmazásban célszerű használni, ahol lényeges szempont a terület gazdaságossága, pl. kisméretű tárgyak jelölésénél, a nagy sebességű rögzített leolvasás és a kompatibilitás direkt jelölőtechnikákkal.

Data Matrix

QR

A kód Japánban terjedt el, nagy kapacitású, mátrixstruktúrájú. Helyzetét a négyzetes struktúra három sarkában található ábrák segítenek meghatározni a kameraolvasók számára.

Halmozott RSS

A halmozott RSS egy viszonylag egyszerű felépítésű 2D-kód, az egydimenziós RSS két sorba tördelt változata. Elsődleges alkalmazási területe az UCC/EAN által szabványosított, a kereskedelmi ellátási lánc felada-

Halmozott RSS

taira kifejlesztett kódrendszer. A halmozott RSS kód a pénztárgépek körüli irányfüggetlen olvasásra optimalizált, és a kompozit kódok egydimenziós összetevőjeként szerepelhet.

A kompozit vagy összetett kód

A kompozit kód egy olyan új típusú kódrendszer, amelyben egy hagyományos és egy kétdimenziós kód kombinációja található. A 2D-komponens önmagában nem értelmezhető, az adattartalom az alatta elhelyezkedő 1D-vonalkóddal együtt érvényes. A 2D-rész mintegy kiegészíti az alapinformációt rögzítő 1D-kód tartalmát. Az alábbi ábrán egy úgynevezett CC-A kompozitkód-variációt látunk a felépítés szemléltetése céljából. A CC-A, CC-B és CC-C változatok főleg a 2D-rész kódtípusában és a kódolható információ mennyiségében különböznek egymástól.

A hagyományos 1D-komponens a CC-A és CC-B változatban lehet az EAN és az UPC kód normál vagy rövidített változata, lehet UCC/EAN-128, RSS, RSS-14 és az RSS kiterjesztett változata, míg a CC-C változatban csak az UCC/EAN-128 szerepelhet. A 2D-kódrész a CC-A és CC-B változatban Mikro PDF417, a CC-C változatban pedig PDF417 lehet. Az 1D-kód a legtöbb esetben egy úgynevezett kapcsolómezőt tartalmaz, utalva a 2D-kódrész tartalmára és típusára.

Egyéb 2D-vonalkódtípusok

Az ismertetett típusok mellett még számos más, kisebb mértékben használt 2D-vonalkód létezik, mint például a Code One, a DotCode, a Snowflake, az Ultracode és az USD-5, amelyeket itt nem részletezünk.

Melyik kétdimenziós kódot válasszuk?

A kétdimenziós (2D) kódok alkalmazási területei és felhasználási előnyei mára teljesen egyértelművé váltak. Az installált rendszerek száma

már most is jelentős, és gyorsan növekszik az új felhasználási területek száma. Napjainkban a 2D-kódok megtalálhatók a jogosítványokon, személyi igazolványokon, katonai azonosító kártyákon, csomagolásokon, félvezetőkön, szállítmányozási papírokon, gyógyászati termékeken, termelési ellenőrzőlapokon és számos más felhasználásban.

A 2D-kódok gyors elterjedése nem meglepő, hiszen a hagyományos egydimenziós vonalkódok lehetőségein túlmutató megoldásokra világszerte igény van. Az új technológiát elfogadott és bevezetett ipari szabványok támogatják.

Minden egyes alkalmazási terület sajátosságokat mutat a vonalkód nyomtatását, olvasását és rendszerintegrációját illetően. Sem a hagyományos 1D-, sem pedig a 2D-technológiában nem létezik mindenki számára megfelelő, általános megoldás. Ezért érdemes áttekinteni azokat a szempontokat, amelyek tekintetbe vétele minden 2D-alkalmazás feltérképezéséhez szükséges.

Főbb kérdések a megfelelő 2D-rendszer kiválasztásakor

Egy optimális 2D-rendszer kiválasztása a feladat alapos kiértékelésével kezdődik, hogy meghatározhassuk az alkalmazásspecifikus igényeket. Az általánosan felmerülő kérdések:

Milyen és mennyi információt szeretnék elhelyezni a 2D-vonalkódban?

Milyen hordozó segítségével lehet ezt az információt a leghatékonyabban továbbítani (papír, címke, közvetlen alkatrészjelölés stb.)?

Milyen helykorlátokkal kell számolni a vonalkód nyomtatásánál?

Új rendszer kialakításáról van szó, vagy a már meglévő rendszer továbbfejlesztéséről?

A felhasználó által felügyelt zárt rendszerről van szó, vagy pedig egy nyílt rendszerről, ahol a szállítókkal és az ügyfelekkel folyamatos a kommunikáció, és bárki előállíthat vagy olvashat 2D típusú információt?

Mi a 2D-vonalkód olvasásának kívánatos módja (rögzített, kézi stb.)?

Milyen visszamenőleges kompatibilitás szükséges a már meglévő vonalkódos rendszerekkel?

A különböző szabványügyi hivatalok kiértékelésének eredménye található a következő táblázatban.

Szervezet	Alkalmazási szabványok	Javaslat
ANSI MH10.8 Unit, Szállítmányozás, Címkék	Szállítási címke és EDI, nagy sebességű szortírozás	PDF417, MaxiCode
Motorgépjárművek Nyilvántartásának Adminisztrátori Szervezete (AAMVA)	Észak-amerikai gépjármű-nyilvántartás	PDF417
US Védelmi Minisztérium	Logisztika	PDF417
US Energiaügyi Minisztérium	Veszélyesanyag-megjelölés	PDF417
Gépjárműipari Szövetség	Gyártásellenőrzés, szállítmányozás, EDI és MEO – alkatrészgyártás, szortírozás	PDF417, Data Matrix, MaxiCode
Elektronikai Ipari Szövetség	Alkatrészgyártás	Data Matrix
EAN/UCC	Termékjelölés, kereskedelmi és ipari ellátási lánc	Kompozit kód, Mikro PDF417 és RSS
SEMI	Egészségügyi termékjelölés	Kompozit kód, PDF417 és Mikro PDF417
HIBC	Ostyagyártás	Data Matrix

Mint ahogy a táblázatból is kitűnik, a PDF417 kódot ezen ágazatok mindegyike kiválasztotta olyan alkalmazási területekre, mint a címkézés, a dokumentumjelölés és az azonosító kártyák. A Data Matrixot az alkatrészek közvetlen megjelöléséhez választották, míg a MaxiCode-ot a szortírozáshoz és nyomkövetéshez. A halmozott RSS kód elsődleges felhasználása az ellátási láncban várható, kiegészítő információk jelölésére. A táblázatból látható, hogy gyakorlatilag négy olyan 2D-kódrendszer van, amely komoly megfontolás tárgya lehet egy adott feladatra történő kiválasztás során. A következő táblázat mintegy útmutatóul szolgál a megfelelő kódrendszer kiválasztásához.

Kódrendszer	PDF417 és Mikro PDF	MaxiCode	Data Matrix	2D RSS
Alkalmazás	Hajózási és egyéb okmányok, rakodási számla, rakomány-jegyzék, papír-EDI, közbiztonság, tárgyi-eszköz-jelölés, személyi azonosító kártyák, jogosítványok, eszközkalibráció, ellátási láncban kompozit kódok	Nagy sebességű csomagszortírozás és -azonosítás	Alkatrészjelölés	Ellátási láncban kiegészítő információk jelölése, változó súly
Adatmennyiség (tipikus)	50–2500 karakter	100 karakter	< 60 karakter	< 25..100 karakter
Olvasás (elsődleges módszerek)	Kézi olvasók, kézi terminálok, rögzített szkennerek, lézer, CCD és kamera	Nagy sebességű CCD kamerák	Rögzített CCD kamerák	Kézi olvasó, lézer, CCD és kamera
Nyomtatás (elsődleges módszerek)	Címkék, okmányok, kártyák	Címkék	Direkt gravírozás, tinta, lézer	Címke
Referencia (ügyfelek/ vásárlók)	RPS, Thomson, Ericsson, Volvo, Arizona DOT, Florida DOT, Corning, Boehringer Mannheim PX, TNT	UPS	Motorola, Intel, HP	Bevezetése 2000-től

Az EAN/UCC rendszer

A főbb vonalkódtípusokkal foglalkozó fejezetben már röviden érintettük az EAN/UCC rendszert. Nézzük most meg részletesebben is az ebbe a csoportba tartozó kódokat, hiszen a vonalkódok legnagyobb felhasználási területe még ma is a kereskedelem és a raktározás.

Bevezetés

Az üzleti élet dinamikája gyorsabban változott az utóbbi években, mint a második világháborút követő teljes időszakban. A gyors fejlődés az értéklánccban, az elosztás új csatornái, a változó igények és növekvő szolgáltatási elvárások váltak az üzleti élet információtechnológiájának kritikus fontosságú tényezőivé.

Az EAN/UCC szabványok a minden elosztási láncban működő, kereskedelmi partnerek közötti nemzeti és nemzetközi kommunikáció eszközeivé váltak, beleértve az alapanyag-szállítókat, a gyártókat, a nagykereskedőket, a disztribútorokat, a kiskereskedőket, a kórházakat és a végső ügyfeleket vagy fogyasztókat.

Sok cég kiterjeszti elosztási csatornáit más iparágak olyan piacaira és ügyfeleire, amelyek nála nem hagyományosak. Annak a cégnek, amely iparág-specifikus szabványt választ, szembe kell néznie a két vagy több rendszer párhuzamos fenntartásának potenciálisan magas költségeivel, amennyiben termékeit, szolgáltatásait értékesíteni akarja, vagy egyszerűen csak kommunikálna „zárt körén" kívül.

A kereskedelem hatékonysága és az ellátási lánc optimalizálása függ a forgalmazott termékek, igénybe vett szolgáltatások és/vagy helyek pontos azonosításától.

Az EAN/UCC rendszer szabványok készlete, amelyek lehetővé teszik a globális, iparágak közötti ellátási lánc hatékony vezetését a termékek, szállítási egységek, tárgyi eszközök, helyek és szolgáltatások egyedi azonosítása révén. Segíti az elektronikus kereskedelmet, beleértve a teljes követhetőséget.

Az azonosító számok vonalkódjelképekkel jeleníthetők meg, lehetővé téve az elektronikus olvasást a bolti pénztáraknál, a raktári átvételnél és minden egyéb helyen, amely az üzleti folyamatokban szükséges. A rend-

szert úgy tervezték, hogy legyőzze a cég-, szervezet- vagy iparág-specifikus kódolási rendszerek korlátjait, a kereskedelmet sokkal hatékonyabbá és az ügyfelekre kedvezően reagálóvá tegye.

Ezek az azonosító számok használhatók továbbá az elektronikus adatcsere (EDI) üzeneteiben a kereskedelem gyorsaságának és pontosságának növelésére. Az egyedi azonosítás biztosításán kívül a rendszer lehetővé teszi kiegészítő információk (pl. minőségmegőrzési idő, gyártási és tételszám) megjelenítését vonalkódos formában.

Az EAN/UCC rendszer alapelveinek és felépítésének követése lehetővé teszi a felhasználóknak, hogy az EAN/UCC adatok automatikus kezelését végző alkalmazásokat tervezzenek. A rendszer logikája garantálja, hogy a vonalkódokból nyert adatokból összetéveszthetetlen elektronikus üzenetek legyenek készíthetők, és azok feldolgozása teljesen előre programozható legyen.

A rendszer minden iparágban, kereskedelmi vagy közszolgáltatásban való használatra alkalmas, és változásai nem zavarják a meglévő felhasználókat.

A különböző EAN/UCC szabványok alkalmazása a logisztikai tevékenységek jelentős javítását, a papírmunka költségeinek csökkenését, rövidebb rendelési és szállítási határidőket, a teljes ellátási lánc nagyobb pontosságát és jobb vezetését eredményezi. Naponta rendkívüli költségmegtakarítást érnek el az EAN/UCC rendszer használói, mert ugyanazokat a kommunikációs megoldásokat használják összes kereskedelmi partnerükkel, ugyanakkor saját belátásuk szerint szabadon használhatják saját belső alkalmazásaikat. Az összes EAN/UCC jelkép és adattartalom-azonosító (AI) megfelel az ISO és CEN szabványoknak.

Az EAN/UCC rendszer alapjai és alapelvei

Az alkalmazás területei

Az EAN/UCC rendszer különböző alkalmazási területeket fed le. Ez tartalmaz kereskedelmi és logisztikai egységeket, tárgyi eszközöket és helyeket.

Ezek az alkalmazások szabványos számozásirendszer-struktúrán alapulnak, amelyekkel minden érintett egység és annak valamennyi adata

azonosítható. A számok jelentik a kulcsot az adatbázisokhoz való hozzáféréshez és a tranzakciók összes üzenetében kezelt egységek téveszthetetlen azonosításához. Minden információ, amely leír egy terméket vagy szolgáltatást és annak jellemzőit, adatbázisokban található. Ezeket először a szállító közli a felhasználóval, az első – szabványos üzenettel vagy elektronikus katalógussal lebonyolított – tranzakció előtt.

A számokat vonalkódok jelenítik meg, lehetővé téve az automatikus adatgyűjtést minden ponton, ahol egy egység elhagy egy helyszínt, vagy megérkezik egy helyszínre.

A vonalkódolás rendszerint beépül a gyártási folyamatba a gyártó oldalán: más információkkal együtt a csomagolásra nyomtatják, vagy a gyártási folyamatban címkére nyomtatva rögzítik az egységre.

Azonos számokat használnak az EDI-üzenetekben is, biztosítva, hogy az egység azonosítási tranzakciójának minden információja eljusson a megfelelő partnerekhez. A szabványos számozási struktúrák teszik lehetővé a világviszonylatban garantált összetéveszthetetlen azonosítást a megfelelő alkalmazási körben.

A számozási rendszer és a vonalkód-jelképrendszer

Globális Kereskedelmi Egység (azonosító) Szám (GTIN)

A GTIN kereskedelmi egységek világviszonylatú egyedi azonosítására szolgál.

Kereskedelmi egység minden egység (termék vagy szolgáltatás), amelynél igény a rá vonatkozó, előre meghatározott információk visszanyerése és ezen információknak az elosztási folyamat bármely pontján árazás, megrendelés vagy számlázás céljából történő felhasználása.

A kereskedelmi egységek azonosítása és vonalkódos jelölése lehetővé teszi a kiskereskedelmi pénztári munka, a termékérkeztetés, a leltárirányítás, az újrarendelés, a forgalomanalízis és számos további üzleti alkalmazás automatizálását.

Példa: egy kanna végfelhasználói eladásra szánt festék, egy 6 kanna festéket tartalmazó doboz, 24 doboz 1 kg-os gyeptrágyát tartalmazó gyűjtőcsomagolás, 1 hajsampont és 1 kondicionálót tartalmazó csoportcsomagolás.

Szállítási Egység Sorszámos (azonosító) Kódja (SSCC)

Az SSCC szabványos azonosító szám, amelyet logisztikai (szállítási és/vagy tárolási) egységek egyedi azonosítására használnak.

Logisztikai egység egy bármely összeállítású egység, amelyet szállítás és/vagy raktározás céljára alakítottak ki, és az ellátási lánc tárgyát képezi.

A logisztikai egységen vonalkóddal jelölt SSCC leolvasása lehetővé teszi az egység fizikai mozgásának egyedi követését az egység fizikai mozgása és a csatlakozó információáramlás közötti kapcsolat létrehozásával. Ez megnyitja számos további alkalmazás fejlesztésének lehetőségét, úgymint átrakás, szállítási útvonalak, automatizált érkeztetés stb.

Példa: egy láda, amely 12 különböző méretű és színű szoknyát, valamint 20 különböző méretű és színű kabátot tartalmaz, logisztikai egységnek tekintendő. Az egyenként 12 festékes kannát tartalmazó, 40 dobozból képzett rakodólapos egységrakomány szintén logisztikai egység.

Globális Hely (azonosító) Szám (GLN)

A GLN egy cég vagy szervezet – mint jogi személy – azonosítására szolgál. A GLN-ek használhatók továbbá cégen belüli fizikai vagy funkcionális helyek azonosítására.

A helyazonosító szám egy azonosító szám, amely fizikai, funkcionális vagy jogi helyekre utal.

Vonalkód-jelképrendszerek

Az EAN/UCC rendszer három különböző vonalkód-jelképrendszert hagyott jóvá. A kiskereskedelmi pénztári leolvasás céljára csak az EAN/UPC vonalkódok használhatók. Más alkalmazásokban, raktári érkeztetésben vagy a raktárakban három különböző vonalkód-jelképrendszer használható: EAN/UPC, ITF-14 vagy UCC/EAN-128.

Kereskedelmi egységek azonosítása és számozási struktúrája

Kereskedelemi egység minden egység (termék vagy szolgáltatás), amelynél igény a rá vonatkozó, előre meghatározott információk visszanyerése és ezen információknak az elosztási folyamat bármely pontján árazás, megrendelés vagy számlázás céljából történő felhasználása. Ez a meghatározás a nyersanyagoktól a fogyasztási készárukig mindent le-

fed, és vonatkozik minden olyan szolgáltatásra, amelynek előre meghatározott jellemzői vannak.

A kereskedelmi egységek GTIN-nel vannak számozva, amihez négyféle számozási struktúrát használnak: EAN/UCC-8, UCC-12, EAN/UCC-13 és EAN/UCC-14. Amennyiben adatállományban vannak, akkor mindegyik egy 14 jegyű mezőt foglal el. A számozási struktúrák közötti választást az egység természete és a felhasználói alkalmazás célja befolyásolja.

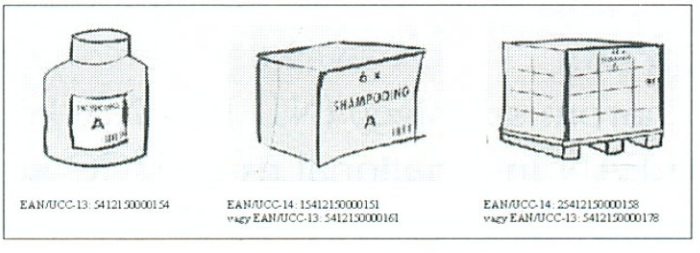
Az EAN/UCC rendszer egyik fő alkalmazási területe az egységek bolti pénztárnál leolvasással történő azonosítása, amelyeket általában fogyasztói egységeknek neveznek. Ezeket EAN/UCC-13 számmal (vagy UCC-12-vel, ha Észak-Amerikában értékesítik) azonosítják. Nagyon kis méretű egységekhez EAN/UCC-8 (vagy nulla elhagyású UCC-12) használandó.

Bár 2005. január 1-jei határidővel be fog következni az EAN/UCC-13 világviszonylatú elfogadása, az UPC-A vagy UPC-E jelképpel megjelenített UCC-12 szabványos számozási struktúra még szükséges az USA-ban és Kanadában a kiskereskedelemben értékesített egységekhez. Ez azért lényeges, mert több észak-amerikai használó még nem tudja számítógépes állományában az EAN/UCC-13 azonosító számokat kezelni.

A kiskereskedelmi boltokban nem értékesített kereskedelmi egységek fizikai formája nagyon különböző lehet: kartondoboz, burkolt vagy pántolt egységrakomány, műanyag fóliával burkolt tálca, rekesz palackokkal stb. Ilyen egységek azonosítása végezhető:

- külön EAN/UCC-13 szám adásával vagy
- egy EAN/UCC-14 szám képzésével alkotott szám adásával. Ennek képzése a számozott egység által tartalmazott fogyasztói csomagolás száma elé helyezett „indikátorral" történik, amelynek értéke 1-től 8-ig terjedhet. Ez a megoldás csak standard kereskedelmi egységek homogén csoportjánál használható, ahol minden egység tartalma azonos.

A két eljárás vegyesen is használható, akár egy cégen belül.



Ez a példa mindkét számozási megoldást mutatja

A számozási struktúra

Az alábbiakban négy számozási struktúrát ismertetünk. Először egy struktúrát kell választani egy egységhez, majd számot kell adni neki. Nem engedélyezett azonos egységnek másik számot adni vagy más számozási struktúrát használni.

Indikátor	A tartalmazott (fogyasztói) egység azonosító száma (ellenőrzőszám nélkül)	Ellenőrzőszám
I	N_1 N_2 N_3 N_4 N_5 N_6 N_7 N_8 N_9 N_{10} N_{11} N_{12}	C

EAN/UCC-14 struktúra

EAN/UCC cégprefix és termékszám	Ellenőrzőszám
N_1 N_2 N_3 N_4 N_5 N_6 N_7 N_8 N_9 N_{10} N_{11} N_{12}	C

EAN/UCC-13 struktúra

UCC cégprefix és termékszám	Ellenőrzőszám
N_1 N_2 N_3 N_4 N_5 N_6 N_7 N_8 N_9 N_{10} N_{11} N_{12}	C

UCC-12 struktúra

EAN/UCC cégprefix és termékszám	Ellenőrzőszám
N_1 N_2 N_3 N_4 N_5 N_6 N_7	C

EAN/UCC-8 struktúra

Az indikátor

Csak az EAN/UCC-14 számban használható. Ez 1 és 8 közötti értékeket vehet fel állandó mennyiségű kereskedelmi egységeknél, változó mennyiségű egységeknél az értéke 9. A legegyszerűbb eljárás e szám kiadására a sorszám (1, 2, 3...) a kereskedelmi egységek eltérő összeállításaira.

EAN/UCC cégprefix

Az első két vagy három számjegy (N1, N2, N3) képezi az EAN/UCC prefixet, amelyet az EAN International és az UCC közösen állapít meg. Ez nem jelenti azt, hogy az egység abban az országban készült, amelyben kódolták.

Az ezt követő EAN/UCC cégazonosító számot a nemzeti számozó szervezet adja.

Az EAN/UCC elő- és cégazonosító száma képezi az EAN/UCC cégprefixet, amelyet a rendszer minden használója a nemzeti számozó szervezettől vagy az UCC-től kap meg. Általában 6-tól 10-ig terjedő számjegyet tartalmaz, a cég igénye szerint.

A termékszám

A termékszám jellemzően 1–6 karakter hosszúságú, amely nem „beszélő" szám. Ez azt jelenti, hogy a szám egyes számjegyei nem tartalmaznak osztályozást vagy egyéb különleges információt.

A legegyszerűbb út a termékszámok kiadására a sorszámozás (001, 002, 003 stb.).

Ellenőrzőszám

Az ellenőrzőszám a GTIN utolsó (jobb oldali szélső) számjegye. A szám összes többi jegyéből számolandó, és annak biztosítására használatos, hogy a vonalkód olvasása helyesen történt, és a szám helyesen van felépítve.

Figyelem!

A számot mindig egészként kell használni. Az adatfeldolgozás sohasem alapulhat a GTIN valamelyik részén.

Kereskedelmi egységek jelképjelölése

Vonalkódok jellemzői

Egy vonalkód egységre történő felvitelére számos eljárás létezik, így többek között:

- a vonalkód beépítése a csomagolásgrafikába,
- közvetlen, online nyomtatás a csomagolásra,
- előre nyomtatott címke felhelyezése.

Méretek

A vonalkódok különböző méretekben nyomtathatók ki. A méretet a nyomtatási feltételek függvényében kell megválasztani. Kisméretű vonal-

kód csak jó minőségű nyomtatónak jó minőségű nyomathordozóval történő párosítása esetén használható.

Nem lehetséges a vonalkódméret önkényes kiválasztása, hogy az a csomagolás előre meghatározott méretű felületébe illeszkedjék.

A méret minden vonalkódtípus esetében egy legkisebb és egy legnagyobb érték között helyezkedhet el. Közvetlen nyomtatás esetén a méretet a kísérletek után a nyomda állapítja meg.

A vonalkódot képelemekből (pixelekből) vagy pontokból felépítő eljárások nem képesek az összes lehetséges méretű vonalkód előállítására.

Világos mezők

Minden vonalkódtípusnál szükséges egy világos mező az első vonal előtt és az utolsó után. Ez rendkívül fontos. A világos mező mérete függ a vonalkód típusától és méretétől. A benne lévő bármely nyomat megakadályozhatja a vonalkódjelkép olvasását.

Színek és kontraszt

A vonalkódolvasók (szkennerek) a fényvisszaverés (reflexió) mérésével dolgoznak. Jelentős kontrasztnak kell lenni a sötét vonalak és a világos színek között. Ehhez elegendő sűrűségű festék szükséges, hogy a vonalak ne legyenek foltosak. Összetett színek nem igazán alkalmasak a vonalkódok nyomtatásához, homogén színek használata jobb eredményt ad.

Az olvasók vörös fényű fénysugárral dolgoznak. Az emberi szem által érzékelt kontraszt nem elegendő a vonalkódolvasónak.

A vonalkódok különböző színekkel nyomtathatók: alapelv, hogy vöröset és rózsaszínt tartalmazó világos színek alkalmasak a világos közökhöz és világos mezőkhöz. Sötét színek – mint a fekete, a kék és a zöld – használhatók a vonalakhoz. Fényes nyomathordozók megváltoztathatják a fényvisszaverődést, ezért nyomtatás előtt kísérleteket kell végezni. Átlátszó burkolás szintén csökkenti a kontrasztot, ezért a teljes csomagolással végzett próbák szükségesek, ha burkolást használnak.

Nyomtatási minőség

A nyomtatási feltételeket rendszeresen ellenőrizni kell a nyomtatás folyamán annak biztosítására, hogy azok nem romlottak a kezdeti helyzet-

hez képest. Több eljárás létezik a vonalkód minőségének becslésére. Használhatók egyszerű vizuális eljárások, például meghatározott méretű H alakú jelek nyomtatása a kereten belül, az ITF-14 vonalkódnál.

Elhelyezés

A vonalkód-leolvasás hatékonysága és pontossága lényegesen növelhető a vonalkód ajánlott elhelyezésével. Minden olvasási környezetben a vonalkódok elhelyezésének következetessége eredményezi a legnagyobb termelékenységet.

Az EAN/UCC rendszerben használt vonalkódok

EAN/UPC jelképek

A kiskereskedelmi boltokban értékesített egységeket a következő EAN/UCC vonalkódjelképek egyikével kell jelölni: EAN-13, UPC-A, EAN-8 vagy UPC-E.

Ezek a jelképek használhatók nem kiskereskedelemben értékesített kereskedelmi egységeken is.

Vonalkódos címkéket kell használni, amennyiben a nyomtatási feltételek és/vagy a nyomathordozók nem megfelelőek.

A következő vonalkódok itt alapméretben láthatók (nagyítási tényező: 100%) a világos mezővel együtt. Minden vonalkódtípushoz adott a legkisebb és legnagyobb méret.

EAN-8 jelkép
Legkisebb méret: 21,38x17,05 mm
Legnagyobb méret: 53,46x42,62 mm

EAN-13 jelkép
Legkisebb méret: 29,83x20,73 mm
Legnagyobb méret: 74,58x51,82 mm

UPC-A jelkép
Legkisebb méret: 29,83x20,73 mm
Legnagyobb méret: 74,58x51,82 mm

UPC-E jelkép
Legkisebb méret: 17,69x20,73 mm
Legnagyobb méret: 44,22x51,82 mm

Az EAN/UPC jelképek 80% és 200% közötti nagyítási tényezőjű méretben nyomtathatók. A minden környezetben – beleértve a szállítópályán történő olvasást is – biztonságos olvasás érdekében 150%-os legkisebb nagyítási tényező használandó.

A jelképet omnidirekcionális olvasásra tervezték.

A jelkép magasságának csökkentése megszünteti az omnidirekcionális tulajdonságot, ezért a magasságcsökkentés a legutolsó lehetőség, ha a rendelkezésre álló hely csak alacsonyabb jelkép elhelyezésére elegendő.

Világosmező-jelző – amely a > jel hegyével jelöli a világos mező határait – használata határozottan ajánlott.

ITF-14 jelkép

Azon cégek részére, amelyek kartonra vagy hullámpapír lemezre közvetlenül akarnak vonalkódot nyomtatni, az ITF-14 jelkép sokkal célszerűbb. A nyomtatási tűrések kevésbé szigorúak. Előre nyomtatás, közvetett hőnyomtatás (termo-transfer) vagy tintasugaras (ink-jet) felvitel is lehetséges.

Az alábbi méretek tartalmazzák a keretet is:
Legkisebb méret: 44,725x22,30 mm
Legnagyobb méret: 152,40x41,40 mm

Kétféle szélességű világos és sötét vonal használatos: széles és keskeny. Arányuk 2,5:1. Az ITF-14 jelkép 25 és 100% közötti nagyítási tényezőjű méretben nyomtatható. A minden környezetben – beleértve a szállítópályán történő olvasást is – biztonságos olvasás érdekében 50%-os legkisebb nagyítási tényező használandó.

UCC/EAN-128 jelkép

Az UCC/EAN-128 változó hosszúságú, függően a kódolt karakterek számától, típusától és a nyomtatás minőségétől. Adott adathosszúsághoz a jelkép hossza meghatározott szélső értékek között változhat, hogy alkalmazkodjon a különböző nyomtatási eljárások minőségéhez. A jel-

képet beépített vagy mozgatható olvasókkal végzett kétirányú olvasásra tervezték.

Az UCC/EAN-128 jelképek 25 és 100% közötti nagyítási tényezőjű méretben nyomtathatók. A minden környezetben – beleértve a szállítópályán történő olvasást is – biztonságos olvasás érdekében 50%-os legkisebb nagyítási tényező használandó.

Az UCC/EAN-128 jelképrendszer rendkívül rugalmas. Lehetővé teszi különböző hosszúságú információk megjelenítését és több információ egyetlen vonalkódjelképben történő ábrázolását. Ezt nevezik láncolásnak.

Az AI-k olyan kódok, amelyek egyértelműen meghatározzák az őket követő információ jelentését és hosszát.

Az AI-t követő információ tartalmazhat numerikus és/vagy alfanumerikus jeleket 30 karakterig terjedő hosszúságban. Az adatmezők az AI-tól függően lehetnek kötött vagy változó hosszúságúak.

A jellemzők mint adatok egy kereskedelmi vagy szállítási egységre vonatkoznak, de önmagukban nincs értelmük. A jellegzetességek AI-k használatával és UCC/EAN-128 jelképpel jeleníthetők meg. Rendelkezésre áll számos AI a kereskedelmi egységek méreteire vonatkozóan, ezek tömeg esetén a nettó tömeget fejezik ki. Ugyanígy a szállítási egységek ún. logisztikai mértékeire is léteznek AI-k, ezek tömeg esetén a bruttó tömeget fejezik ki.

A következő táblázat a teljes AI-lista kivonata.

Adattartalom azonosító "AI"	Teljes cím	Formátum
0	Szállítási Egységek Sorszám Kódja (SSCC)	n2+n18
1	Globális Kereskedelmi Egység Szám (GTIN)	n2+n14
2	Logisztikai egység tartalmának GTIN-je	n2+n14
10	Gyártási tételszám	n2+an...20
11	Gyártás napja (ÉÉHHNN)	n2+n6
15	Minőségmegőrzési határidő (ÉÉHHNN)	n2+n6
17	Fogyaszthatósági határidő (ÉÉHHNN)	n2+n6
21	Gyártási szám	n2+an...20
310X	Nettó tömeg (kg)	n4+n6
37	Logisztikai egységben lévő kereskedelmi egységek száma (db)	n2+n...8
401	Küldeménykód	n3+an...30
420	Belföldi szállítási cím postai irányítószámmal	n3+an...30

A példa szerinti EAN/UCC-128 vonalkód GTIN-t, minőségmegőrzési határidőt és gyártási tételszámot ábrázol

Megfontolások a jelképrendszerek használatánál

Egyedül az UCC/EAN-128 jelképrendszer jöhet szóba, amennyiben az azonosítás mellett kiegészítő jellemzők is szükségesek. Az UCC/EAN-128 használható (01-es) adattartalom-azonosítóval UCC-12, EAN/UCC-13 vagy EAN/UCC-14 számok kódolására.

Amennyiben bármely okból szükséges az azonosítás mellett kiegészítő információkat (gyártási szám stb.) is nyomtatni, és a kereskedelmi egység EAN-13 vagy ITF-14 jelképpel van jelölve, akkor lehetséges:

- a kiegészítő információkat UCC/EAN-128 jelképpel ábrázolt címke felhelyezésével megjeleníteni a korábban felvitt EAN-13 vagy ITF-14 kiegészítéseként. Az összes jelképet vízszintesen kell elhelyezni. Ez a megoldás akkor használandó, ha az ügyfél még nem képes az UCC/EAN-128 jelkép olvasására;
- címkén ábrázolni a meglévő jelképet is. Az eredeti jelképben ábrázolt azonosító számot a címkére kell nyomtatni a többi választott jellemzővel együtt, lehetőleg UCC/EAN-128-cal.

Logisztikai egységek

Logisztikai egység egy bármely összeállítású egység, amelyet szállítás és/vagy raktározás céljára alakítottak ki, és az ellátási lánc tárgyát képezi.

Az EAN/UCC rendszer egyik fontos alkalmazása a logisztikai egységek követése az ellátási láncon keresztül. Erre a célra egy szabványosított EAN azonosító szám, a Szállítási Egység Sorszám (azonosító) Kódja (angolul Serial Shipping Container Code, általánosan elterjedt rövidítéssel SSCC) azonosítja a logisztikai egységet.

Ez a szám minden logisztikai egységre vonatkozólag egyedi, s az összes logisztikai egységre és elvileg minden logisztikai alkalmazásra használható.

Ha a kereskedelmi partnerek – beleértve a szállítókat és a harmadik partnert – mindegyike leolvassa az SSCC-t, és EDI-üzeneteket cserél, amelyek a logisztikai egység teljes leírását adják, és a megfelelő adatállomány, amellyel ez az információ elérhető, online módon rendelkezésre áll, akkor az SSCC-n kívül semmi mást nem szükséges feltüntetni.

Ám ezek a feltételek még ritkán valósulnak meg, ezért jól használható az SSCC-hez kapcsolódó jellemzők vonalkódos ábrázolása a logisztikai egységen.

Mivel minden logisztikai egységet el kell látni saját, egyedülálló SSCC-vel, az ezt tartalmazó vonalkód előre nyomtatása a csomagolóanyagra nem praktikus. Címkét kell készíteni, amelyet a szállítási egység (pl. egységrakomány) keletkezésekor rögzítenek azon.

Továbbá a logisztikai egység kereskedelmi egység is lehet, ennélfogva a kereskedelmi egységekre vonatkozó EAN/UCC specifikációknak is tárgya. Amennyiben ez a helyzet, akkor logikus egyetlen címkét készíteni, amely tartalmazza az összes szükséges vonalkódolt információt.

Az EAN International és az UCC – együttműködve a gyártók, kiskereskedők és szállítók képviselőivel, valamint az EAN Nemzeti Számozó Szervezetekkel – kidolgozott egy önkéntesen alkalmazható szabványt: az EAN/UCC logisztikai címkét. Ennek központjában az SSCC és annak a logisztikai egységen történő alkalmazása áll.

Az SSCC

Adat-tartalom azonosító		Serial Shipping Container Code (SSCC) Szállítási Egység Sorszám (azonosító) Kódja		
	Kiterjesztő szám	EAN/UCC cégprefix	Egységsorszám	Ellenőrző szám
00	N1	N2 N3 N4 N5 N6 N7 N8 N9 N10 N11 N12 N13 N14 N15 N16 N17		N18

A kiterjesztőszám az SSCC számkapacitásának növelésére szolgál. Az SSCC-t képező cég adja ki.

Az EAN cégprefixet a nemzeti számozó szervezet adja ki a rendszer használójának, amely rendszerint a logisztikai egység összeállítója. Ez világviszonylatban egyedivé teszi a számot, de nem azonosítja annak eredetét.

Az egységsorszám egy egyszerű sorszám, amellyel a cégprefix birtokosa egészíti ki a cégprefixet N17-ig. A legegyszerűbb megoldás a sorszám képzésére az egymás után következő számok kiadása: 000, 001, 002, 003...

Az SSCC az a szám, amely minden logisztikai egységet azonosít, függetlenül attól, hogy standard vagy sem, homogén vagy kevert tartalmú.

Ha egy cég meg akarja különböztetni gyártó üzemeit az SSCC-ben, megteheti, hogy az egyes üzemeknek SSCC-blokkokat ad ki.

Az SSCC-t deklarálják a szállítási értesítésben, a szállítólevélben és minden szállítási üzenetben.

A logisztikai címke

A logisztikai címke felépítése támogatja az ellátási lánc folyamatát az információk három logikai csoportba rendezésével: feladó-, ügyfél- és szállítócímkeként. Mind a három címkerész eltérő időben kerül felvitelre, amikor a megfelelő információk rendelkezésre állnak. Mindegyik címkerészben elkülönülnek egymástól a szöveges és vonalkódos információk, lehetővé téve azok eltérő gépi, illetve kézi feldolgozását.

A címkéző – az a szervezet, amely felelős a címke nyomtatásáért és felhelyezéséért – határozza meg a címke tartalmát, formáját és méretét. Az SSCC az egyetlen kötelező elem minden EAN/UCC logisztikai címkén. Az egyéb információknak, ha szükségesek, ki kell elégíteniük az általános és az adattartalom-azonosító rendszer előírásait.

Egy címkerész az információknak olyan csoportja, amely adott időben általában rendelkezésre áll. Három címkerész áll rendelkezésre, amelynek mindegyike egy információs csoportot reprezentál. Alapvetően a sorrend fentről lefelé: szállító, ügyfél és feladó. Ez a sorrend változhat a logisztikai egység mérete és a kiszolgált üzleti folyamat függvényében.

Feladórész

Az ebbe a csoportba tartozó információk általában a feladónál történő csomagoláskor ismertek. A kötelező SSCC-t itt adják meg, amely az azonosító. A kereskedelmiegység-azonosítást (GTIN) – amennyiben használják – itt adják meg.

Egyéb – elsősorban a feladó számára fontos, de az ügyfél és a szállító által is használható – információk szintén itt helyezhetők el. Ezek a termeléssel összefüggő adatok, úgymint termékváltozat, gyártási, csomagolási, minőségmegőrzési és fogyaszthatósági idő, gyártási szám és gyártási tételszám.

Ügyfélrész

Az ebbe a csoportba tartozó információk általában a feladónál a megrendelés, illetve a megrendelésfeldolgozás idején válnak ismertté. Jellem-

ző információk: szállítási cím helyazonosítóval, megrendelési szám, valamint ügyfélspecifikus útvonal és kezelési információk.

Szállítórész

Az ebbe a csoportba tartozó információk általában a feladás idején válnak ismertté, és jellemzően a szállítással kapcsolatosak. Jellemző információk: szállítási cím postai irányítószámmal, szállítmányszám, valamint szállítóspecifikus útvonal és kezelési információk.

Címke feladó-, ügyfél- és szállítórésszel

Helyazonosító számozás

Az EAN/UCC Globális Hely(azonosító) Szám (Global Location Number, GLN) lehetővé teszi fizikai vagy funkcionális helyek, valamint jogi személyek egyedi és összetéveszthetetlen azonosítását.

Egy kereskedelmi kapcsolat számos céget érint: a szállítót, az ügyfelet, a logisztikai szolgáltatót stb. Mindegyik cégnél több részleg is érdekelt lehet.

A kereskedelmi partnerek részére szükséges a kapcsolatukra jellemző helyek és funkciók pontos azonosítása a megfelelő állományban.

Az EAN/UCC-13 standard számozási struktúra használható erre a célra.

Minden cég vagy szervezet, amely rendelkezik GLN-számképzéshez EAN/UCC cégazonosító prefixszel, adhat EAN GLN-eket saját különböző helyeinek. Minden megkülönböztetést igénylő címnek, minden funkciónak külön számot kell adni.

A GLN-eket használó cég felelőssége, hogy üzleti partnereit informálja az összes kiadott számról és azok részleteiről.

EDI-kommunikációban a GLN-t az összes érintett fizikai hely azonosítására használják.

A GLN-ek használhatók vonalkódos formában is: több adattartalom-azonosító van erre a célra, mint „Szállítási cím...” (AI=410), „Számlatovábbítás...” (AI=411) vagy „Feladó...” (AI=412), ahol a helyekre az EAN/UCC helyazonosító vonatkozik.

Az egyetlen vonalkód-jelképrendszer, amellyel a GLN kódolható, az UCC/EAN-128.

EDI

Az üzleti élet naponta egyre több papírdokumentumot állít elő. Ezek a papírok – a megrendelésektől és számláktól a termékkatalógusokig, értékesítési beszámolókig – biztosítják az élő információkat, amelyek a kereskedelmi tranzakciókban a fizikai folyamatokat megelőzik, azokhoz csatlakoznak, vagy azokat követik.

Az utóbbi években óriási erőforrásokat vontak be a fizikai termelési és disztribúciós folyamatok áramvonalasításába. Ugyanakkor kevesebb figyelmet kapott a szervezetek közötti információáramlás fejlesztése.

Az információk áramlását – mind a belső, mind a külső adatcsere területén – racionalizálni kell. Az EDI (Electrinoc Data Interchange, azaz Elektronikus Adatcsere) a kereskedelmi partnerek részére hatékony üzleti eszközt biztosít az adatoknak az egyik számítógépből közvetlenül egy másikba való továbbítására.

Az EDI a strukturált adatok továbbítását jelenti, üzenetszabványok használatával, elektronikus úton egy számítógépes alkalmazásból egy másikba, minimális emberi közreműködéssel. Ez a csere magában foglal kereskedelmi tranzakciókat, illetve azok kereskedelmi, logisztikai és pénzügyi vonzatait. Az EDI eredményes bevezetése minden szervezet esetében több szakágat érintő projekt, amely magas fokú elkötelezettséget kíván meg mind a felső vezetéstől, mind a különböző tevékenységekért felelős funkcionális vezetők széles körétől. Testületi célkitűzések és eljárások szükségesek annak vizsgálatára, hogy változtatni kell-e a jelenlegi funkcionális eljárásokat, s új üzleti kapcsolatokat kell-e kiépíteni és ápolni. A rendszer központjában az információk jobb használata, a belső és az üzleti partnerek közötti jobb megosztása áll,

úgy, hogy a kapcsolatok megbízhatóbbak legyenek, a felek pedig tájékozottabbak.

Az EANCOM részletezett bevezetési irányelv az UN/EDIFACT szabványos üzeneteihez. 45 üzenetet tartalmaz az adatmezők használatára vonatkozó világos meghatározásokkal és értelmezésekkel, lehetővé téve a kereskedelmi partnerek egyszerű, pontos és olcsó adatcseréjét.

Rendelkezésre állnak minden kereskedelmi igényt kielégítő, különböző üzenettípusok a különböző kereskedelmi partneri kapcsolatokhoz.

- A törzsadatüzenetek leírják az érdekelt partnereket és termékeket.
- A kereskedelmi tranzakciók megrendeléssel kezdődnek, és többféle terhelési üzenettel végződnek, a kereskedelmi tevékenység logikai ciklusát követve.
- A beszámoló- és tervezőüzeneteket a kereskedelmi partnerek informálására, a kereskedelmi tevékenység vagy a jövőbeli igények megtervezésére használják, ami lehetővé teszi az ellátási lánc modernizálását.
- A logisztikai szolgáltatóknak vagy szállítóknak szóló instrukciók és beszámolók lehetővé teszik az ellátási lánc minden fokának automatizálását.

Az EANCOM több mint szabványosított üzenetek készlete, amely az EAN/UCC nemzetközi számokon alapul, és nem a kereskedelmi partnerek kétoldalú megállapodásain. Az EAN-számok használata természetesen megkönnyíti a bevezetést a későbbi kereskedelmi partnerekkel kapcsolatban.

A GTIN ebben a kézikönyvben kereskedelmi egységek (termékek, szolgáltatások) azonosítását írja le az egyetlen nemzetközi és ágazatközi számozási rendszerben, amely egyedi, összetéveszthetetlen azonosító számot biztosít az egységeknek és azok változatainak, származási helytől és célállomástól függetlenül. Az EANCOM-üzenetek különösen fontosak nyitott környezetben. A cégeknek nem kell kereszthivatkozásokat fenntartaniuk minden kereskedelmi partner belső számaira vonatkozólag. A GLN nyújtja a leghatékonyabb kommunikációs eszközt helyek és cégek azonosítására. Ugyanúgy, ahogy az EANCOM-üzenetekben használható, alkalmas hálózatokban az EDI-üzeneteknek a megnevezett postaládába, munkahelyre vagy alkalmazáshoz történő címzésére. Az EANCOM-üzeneteket arra tervezték, hogy a csatlakozó szabványok (termék-

és helyazonosítás, vonalkódolás) összes előnyét bontakoztassák ki, a használó élvezze a legnagyobb hatékonyságot és hasznot. Használatuk az egész világon fejlődik.

Az EDI-nek számos világos költsége és előnye van; elsősorban az üzlet lebonyolításának egyik útja, legfontosabb előnyei stratégiaiak. A stratégiai előnyök között jellemző az ügyfelek nagyobb elégedettsége, a javuló szállítói kapcsolatok. Egyéb stratégiai előny lehet a piaci szegmensben fenntartható fejlődés és a kompetitív előnyök, a dolgozók növekvő termelékenysége és morálja.

A vonalkódok nyomtatása

Miután kiválasztottuk a vonalkódtípusokat, a következő lépés azok megjelenítése, kinyomtatása. Azért nem beszélhetünk kizárólag nyomtatásról, mert néhány speciális esetben alkalmaznak például fémbe mart vagy domborított kódokat. A felhasználások döntő többségében azonban a nyomtatók használata dominál.

Ma már az informatikai rendszerekhez kínált nyomtatók szinte mindegyik típusa alkalmas a vonalkód nyomtatására grafikus vezérlési lehetőségén keresztül, illetve számos nyomtató nyelvi szinten vagy opcionálisan kínálja néhány vonalkódtípus megjelenítését. A hagyományos nyomtatók mellett a speciálisan vonalkódnyomtatásra kifejlesztett berendezések széles skálájából is választhatunk, hozzátéve, hogy ezek kiválóan alkalmasak egyéb, nemcsak vonalkód-nyomtatási feladatok ellátásra. Természetesen nem feledkezhetünk el a legáltalánosabb, a nyomdai úton történő előállításról sem.

Felmerül tehát a kérdés: mivel nyomtassunk vonalkódot?

Mint láttuk, sokféleképpen nyomtathatunk vonalkódot, de a nyomtatás technikájának megválasztásánál az egész rendszert át kell látnunk, és figyelembe kell vegyük az érvényes nemzeti és nemzetközi szabvány előírásokat.

Számos kérdésre kell választ adni a helyes nyomtatóválasztáshoz:

- Milyen adatokat kell kezelnie?
- Mekkora méretben?
- Milyen alapanyagra?
- Milyen sebességgel?
- Milyen rendszerben (on-line, off-line)?
- Mekkora költséggel?
- Milyen körülmények között?
- Milyen felhasználási időtartamra?
- Milyen gyakran fogy ki, és milyen gyorsan cserélhető a kellékanyag?

A kérdést tehát így kell átfogalmaznunk: mivel célszerű vonalkódot nyomtatnunk?

Ezt, sajnos, gyakran csak egyoldalú gazdasági megfontolások (pl. költségtakarékosság) döntik el. Egyáltalán nem biztos, hogy az ilyen, a vo-

nalkódtechnika ismerete nélküli döntések akár rövid, akár hosszú távon ténylegesen olcsóbb megoldást eredményeznek.

Az a szempont, hogy valami alkalmas egy feladat megoldására, még nem szükségszerűen jelenti azt, hogy használni is érdemes arra. Az űrrepülőgép is képes teherszállításra, mégis viszonylag kevesen járnak bevásárolni vele.

Érdemes elgondolkodni a következő tényen. A világ egyik legnagyobb lézernyomtató-gyártója, amely maga is ajánl vonalkód-nyomtatási opciót berendezéseihez, gyártmányai azonosítását vonalkódnyomtatóval készült címkével végzi el. A felhasználást pedig nem a „megteheti", hanem a „meg kell tennie" kulcsszó indokolta.

A nyomdai úton történő vonalkód-előállítás

A nyomdai előállítás alapja a mesterfilm, amelyet szintén célszerű szakcégekkel elkészíttetni, mert csak ezek rendelkeznek a külön erre a feladatra kifejlesztett, nagy értékű célberendezéssel. A mesterfilmkészítő gépek a nyomatot a szabványok, a tűrések, a kontrasztosság és számos más lényeges szempont ellenőrzésével készítik el.

Mesterfilm

A számítógépes kiadványszerkesztő rendszerek és az azokhoz kapcsolt nagy felbontású lézernyomtatók elterjedésével is elfogadható minőségű vonalkód kerülhet közvetlenül a csomagolási tervbe. Ehhez sokan kínálnak olyan kis – és viszonylag olcsó – célprogramokat, amelyek

a vonalkódot ismert grafikus állományokba (PCX, BMP stb.) képzik le, így válik felhasználhatóvá a kiadványszerkesztő rendszerek számára.

A kereskedelmi áruk csomagolásán egyre gyakrabban találjuk meg a vonalkódot. Egyes országokban meghaladja a 80%-ot, de már nálunk is 50% felett van a vonalkóddal megjelölt termékek aránya. Sajnos egy részük használhatatlan, bár a csomagolástervezéssel foglalkozók egyre inkább figyelembe veszik a vonalkódolvasás specialitásait.

A hiba származhat a vonalkód helytelen, nem szakszerű generálásából (például francia edényeken találtunk vonalkódszerű csíkokat, vagy néhány sajnálatos hazai példát is említhetnénk). Másik ok lehet a nyomtatási minőség hibája, ami többnyire az olcsó csomagolásokon fordul elő, vagy azok a mesterfilmek okozzák, amelyeket nem az erre kifejlesztett célberendezéseken, hanem lézer- vagy vonalkódnyomtatókon állítanak elő.

A leggyakoribb ok azonban a vonalkódismeret hiánya és a figyelmetlenség. Egy-két éve még találkozhattunk olyan vonalkóddal, amelyet a kocka alakú margarin élére terveztek, így azt csak derékszögben meghajlított olvasóval lehetett volna leolvasni (amelynek kifejlesztése sajnos még várat magára). Gyakori hiba a nyugalmi zóna elhagyása, az olvasók által nem látható helyre kerülés vagy a nem eléggé kontrasztos színválasztás. Ide tartozhat még a gyártók által (figyelmetlenségből?) elkövetett hiba, amikor különböző típusú termékeiket ugyanazzal a kóddal azonosítják.

A mai helyzetre tehát az a jellemző, hogy a nyomdák felkészültek a feladatra, a csomagolástervezők szakcéget bevonva képesek szakmailag is megfelelő vonalkódos csomagolást tervezni, a mesterfilm megvásárolható a szakcégeknél, és ez a lehető legolcsóbb vonalkód-készítési megoldás.

A gyártók rákényszerültek a vonalkódos csomagolás előállítására, mert a kereskedő, az exportőr előírja, és vonalkód nélkül nem veszi át a terméket. Viszonylag kevés még azoknak az alkalmazásoknak a száma, ahol a vonalkód lehetőségeit már a gyártó is kihasználja (termeléskövetés, minőségbiztosítás, raktárkezelés stb.), pedig ez számára is költségcsökkenést és a rendelkezésekkel (pl. fogyasztóvédelem) szembeni jobb megfelelést eredményezhet, vagy nagymértékben elősegítheti az ISO minőségi követelményeinek teljesítését.

Nyomtatás az informatikában általánosan használt nyomtatókon

Mátrix-, lézer- vagy tintasugaras nyomtató szinte biztosan előfordul a számítógépes környezetben. Az említettek mellett léteznek más elvű és más teljesítménykategóriába tartozó típusok is, de kisebb elterjedtségük miatt ezekkel most nem foglalkozunk.

A mátrixnyomtatók nagyon jók többpéldányos nyomtatási feladatok megoldására (pl. számlakészítés), a lézer- és tintasugaras nyomtatók kiváló minőségben nyomtatnak szöveget, grafikus ábrákat.

A vonalkódolvasók „szemével" azonban egyikük sem megfelelő a vonalkód nyomtatására. A már ismertetett szempontok mellett az olvasók számára rendkívül fontos a vonalegyenesség és a fedettség.

Különböző nyomtatótípusokon készült vonalkódok összehasonlítása

Az ábrán látható, az emberi szem számára alig érzékelhető eltérések oka, hogy a lézer- és mátrixnyomtatás pontokból építkezik, a professzionális vonalkódnyomtatók viszont négyszögletes elemi egységekkel dolgoznak. A gyors, megbízható olvasáshoz tehát jó minőségű nyomtatási képre van szükség – különösen igaz ez a tömörített vagy a kétdimenziós kódok esetében, amelyek egyre inkább teret nyerhetnek a jövőben.

További hátrányt jelent a mátrix- és a lézerprintereknél az üzemeltetési veszteség a vonalkód nyomtatása közben. A megfelelő méretre vágás, az egyenletes színhatás biztosítása kétszer annyiba kerülhet a lézeres és mátrixtechnikával. Szemben az itt alkalmazható pusztán tucatnyi címketípussal, a professzionális vonalkódnyomtatók több száz tesztelt címke-, ragasztó- és festékszalag-kombinációval dolgozhatnak.

Egy amerikai cég üzemeltetési tapasztalati alapján készített táblázatot adunk közre. Az adatok különböző professzionális nyomtatótípusokról szerzett többéves tapasztalatok alapján keletkeztek, amelyeket évi egymillió darab címke nyomtatása során nyertek. A berendezések amortizációját 5 évre számolták ki. A táblázatot, mivel jórészt közismert kifejezéseket tartalmaz, eredeti formájában közöljük.

Z-140 Thermal Transfer	
Printer Amortization ($5,895/ years)	$ 4.72
Thermal Transfer Ribbons (368 @ $33.66)	$ 49.50
Thermal Printhead (2 @ $1,267)	$ 10.14
Cost/4,000 Labels	***$64.36***

Laser Printer					
Percent of Toner Coverage:	5%	10%	15%	20%	25%
Printer Amortization ($7,995/ years)	$ 6.40	$ 6.40	$ 6.40	$ 6.40	$ 6.40
Toner (31 1/4 kits per 5% density @ $115)	$14.38	$ 28.76	$ 43.14	$ 57.52	$71.90
Developer (2.5 units @ $280)	$ 2.80	$ 2.80	$ 2.80	$ 2.80	$ 2.80
OPC cartridges (12.5 units @ $203)	$10.15	$10.15	$10.15	$10.15	$10.15
Fusers (0.41 @ $540)	$ .89	$ .89	$ .89	$ .89	$ .89
Cost/4,000 labels (1,000 sheets)	$34.62	$49.00	$63.38	$77.76	$92.14

Speciális alkalmazásoknál a vonalkód tintasugaras nyomtatóval történő előállítása is elképzelhető. Itt a festék közvetlenül a termékre vagy a csomagolóanyagra kerül, ezért ennél a technikánál a hordozó felület megválasztása a legfontosabb. Ez a típusú nyomtatás gyors, számottevő az elérhető anyagmegtakarítás, ugyanakkor rendszerbe integrálása elég speciális, és korlátozott azon anyagok köre, amelyekre ilyen módon kerülhet fel a vonalkód.

Amennyiben a kódolt információ hosszú távú eltarthatósága is szempont (pl. leltári szám, könyvtári azonosítás, tartós raktározás, garanciális időtartam követése stb.), vagy más speciális minőségi követelménynek kell megfelelni (pl. víz- vagy dörzsölésállóság), ezeket a hagyományos nyomtatók nyújtotta lehetőségekkel sokkal nehezebb és költségesebb megoldani, ha egyáltalán lehetséges.

Ahol a nyomtatási igény alacsony – napi néhány száz darabos tétel –, és zárt technológia biztosítja az adattévesztés lehetőségének kizárását, célszerű lehet külső szakcéggel legyártatni a vonalkódot. Többezres darabszám felett már saját nyomtatást javasolunk. Ha úgy döntünk, hogy mátrix-, illetve lézernyomtatón állítjuk elő a kódot, ehhez rendelkezésre állnak a magyar piacon a megfelelő szoftverek, de minden esetben győződjünk meg az olvashatóság biztonságáról.

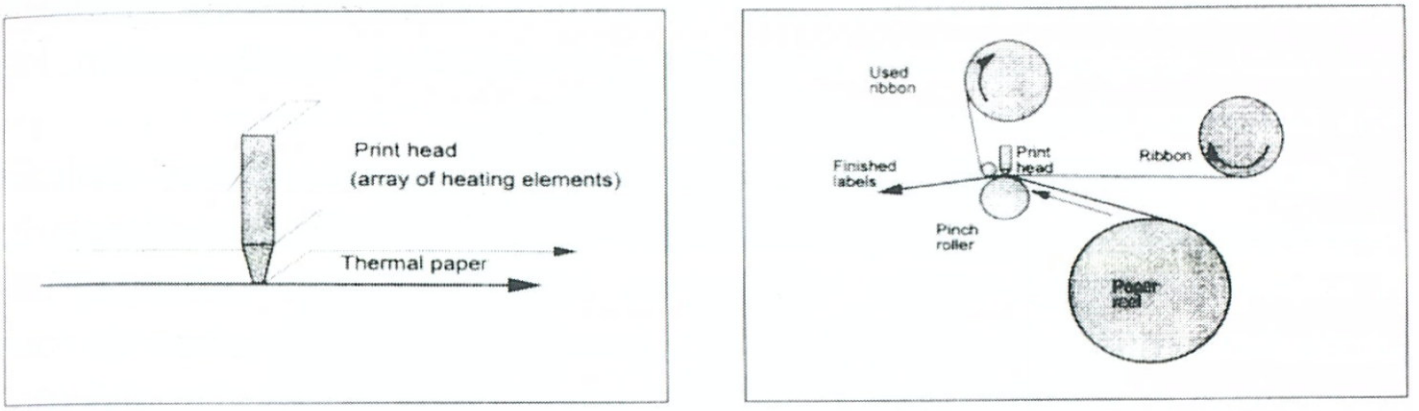
Az alábbi táblázatban néhány fontosabb szempont szerint hasonlítjuk össze a különböző nyomtatókat.

Szempont	Direct thermal	Termo-transzfer	Lézer	Mátrix (pont)	Tinta-sugaras
Nyomtatási felbontás	közepes-jó	közepes-jó	közepes-jó	közepes	megfelelő-közepes
Vonal-egyenesség	nagyon jó	nagyon jó	jó	megfelelő	megfelelő
Kontraszt	jó	nagyon jó	nagyon jó	jó*	nagyon jó
Infravörös olvashatóság	nem	igen	igen	igen	igen
Dörzsölés-állóság	jó	megfelelő-kiváló	jó	jó	jó
Vonalkód magassága	szabadon állítható	szabadon állítható	szabadon állítható	szabadon állítható	korlátozott
Címke élettartama	rövid	hosszú-speciális	hosszú	hosszú	hosszú
Nyomtatás minősége	nagyon jó	nagyon jó	nagyon jó	jó*	közepes-jó
Ár/ teljesítmény	jó	közepes	közepes	jó	közepes

(A * jelölés oka, hogy a jelzett minősítés erősen függ a festékszalag használtságától.)

A professzionális vonalkódnyomtatók

A professzionális vonalkódnyomtatóknak két alaptípusa van: a csak hőérzékeny papírra (direct thermal) és a festékszalag felhasználásával (termo-transzfer) dolgozó nyomtató. Természetesen több más szempont szerint is csoportosíthatnánk őket, pl. hordozható–rögzített, ipari–kereskedelmi, on-line–off-line stb.



Vonalkódnyomtatók működési sémái

Az előbb alkalmazott festékszalag elnevezés ugyan nem felel meg a valóságnak, hiszen itt egy nagyon vékony hordozó fóliára vékony rétegben felvitt hőérzékeny anyagot égetünk át a címke alapanyagába, de felhasználási szempontból tekinthetjük úgy, mint egy egyszer felhasználható festékszalagot, ezért a továbbiakban ezt az elnevezést használjuk.

Mindkettőben a legdrágább és a kopás veszélyének leginkább kitett alkatrész a nyomtatófej, amely az égetési hőmérsékletet szabályozza. Működési tartományuk gyártónként eltérő lehet, ezért is szokták garanciájukat a gyártók által specifikált anyagok felhasználásához kötni. Többségük elemi négyzetekből álló vonal, amelynek hossza adja meg a nyomtatási szélességet. A rögzített fej előtt elhaladó anyag helyzetétől függően, a nyomtatási terv alapján, a fejvezérlő elektronika szolgáltatta impulzusok melegítik fel az elemi egységeket. A legújabb nyomtatófejek folyamatosan mérik minden elemi egység hőmérsékletét, és a névleges értéktől történő eltérés esetén módosítják a vezérlést. Ezzel a módszerrel a fejek élettartama a korábbi 3–6 hónapról akár öt évre is megnőhet, de ehhez egyéb karbantartási előírásokat is be kell tartani.

A direkt nyomtatás olcsóbb, hiszen nem kell hozzá festékszalag, ugyanakkor az előállított címke érzékeny a fényre, a hőmérsékletre, és gyorsabban öregszik, vagyis nem annyira időtálló (gondoljunk itt eltűnő vagy elsötétedő telefaxüzeneteinkre). Tipikus felhasználási területe a vonalkódos kereskedelmi rendszerekben a belső vonalkódok és pótlások nyomtatása, hiszen itt az áruk viszonylag gyorsan elhagyják az értékesítési pontokat, és megsemmisülnek. Megtalálhatjuk még hűtőipari alkalmazásokban, illetve a hordozható nyomtatók döntő többsége is direkt nyomtató, amelyeket főként kiegészítő nyomtatóként, sérülés esetén, hiány pótlására alkalmaznak.

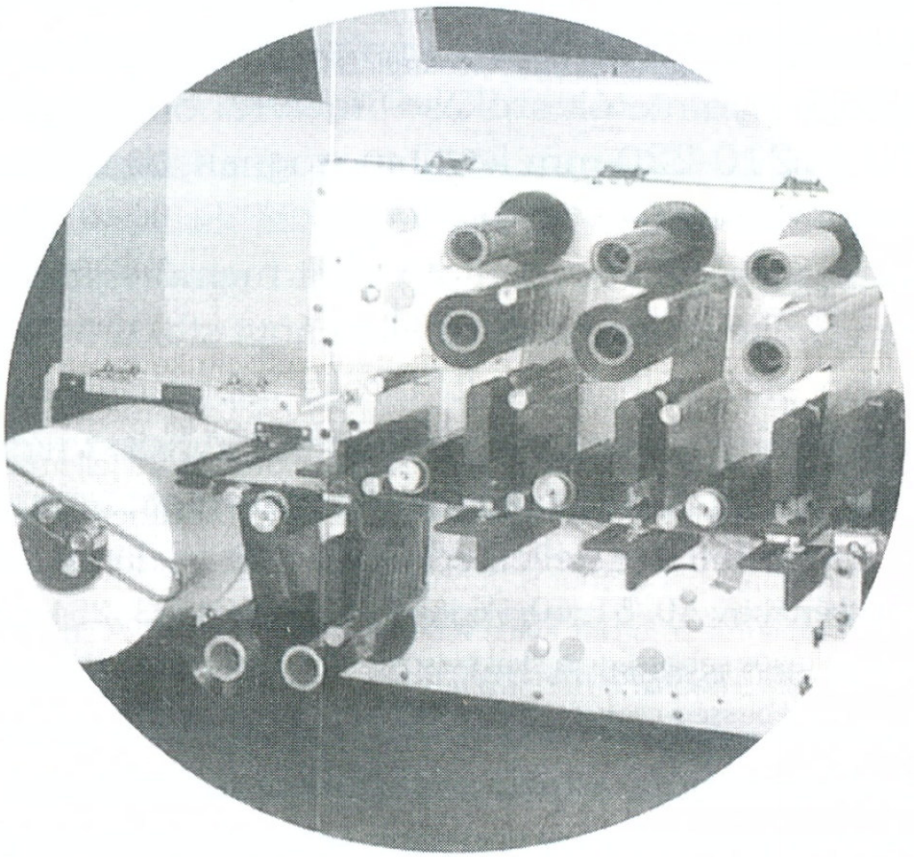
Termo-transzfer elven szinte minden anyagra nyomtathatunk, csak az alapanyaghoz illeszkedő festékszalagot kell megfelelően kiválasztani. A normál papírtól kezdve a kartonokon, különböző papír–műanyag keverékeken, műanyagokon, textileken, fémmel kevert papírokon és műanyagokon át a szélsőséges környezeti követelményeknek ellenálló matériákig számtalan anyag nyomtatására találunk példákat. Ipari alkalmazásokra csak ilyet javasolunk.

Mindkét típusú nyomtatóval gyorsan, megbízható minőségben lehet előállítani vonalkódcímkét nagy mennyiségben, amit számtalan érzékelő szenzor, több léptető motor és egyszerű, de rendkívül megbízható mechanikai kialakítások tesznek lehetővé.

Természetesen a címkére nemcsak vonalkód kerülhet. A vonalkódnyomtató a memóriájában pontról pontra megtervezett címketervet tárol (bittérkép), így különböző szöveges és tetszőleges grafikus információk kinyomtatására képes. Nyelvi szinten számos, állítható méretű betűkészletet és egyéb grafikus lehetőséget is tartalmaz. A piacon megtalálható professzionális vonalkódnyomtatókhoz ma már a legkorszerűbb szoftvereket kínálják (akár magyar nyelven), Windows-platformon is, amelyekkel a legkülönlegesebb igényeket is ki lehet elégíteni, közel a kiadványszerkesztő programok színvonalához. Az informatikában általánosan elterjedt tervezőszoftverek nem tartalmazzák a vonalkódnyomtatók meghajtóit, ezért sok gyártó konvertáló programot is mellékel berendezéseihez.

Az alapkészülékek mellett találhatunk speciális, színes vagy műanyagkártya-nyomtatást is lehetővé tévő vonalkódprintert, habár ezek ma még

igen drágák. Az informatikában általánosan használt eszközök ára dinamikusan csökken, míg a vonalkód-technikai eszközöké kevésbé, így ezek árszintje magasabb. Az eltérések oka egyrészt a tömegszerűségben rejlik (a számítástechnikai berendezések két-három nagyságrenddel nagyobb darabszámban készülnek), másrészt a látszólag hasonló berendezések (lézernyomtató–vonalkódnyomtató, grafikus scanner–vonalkódszkenner) a műszaki tartalom tekintetében jelentősen eltérnek egymástól, összehasonlításuk helytelen.



Egy színes nyomtató belső kialakítása

A vonalkódnyomtatók közötti különbségek

Az egyes gyártók termékcsaládokat kínálnak aszerint, hogy a nyomtatók milyen alkalmazási feladatot láthatnak el. Más nyomtatót alkalmazhatnak a kiskereskedelmi cégek és az iparvállalatok, a kórházak és a raktárak. Melyek az eltérések a műszaki paraméterekben?

A nyomtatófej felbontása. A felbontást az elemi négyszög mérete adja, amit az egy méretegységben lévő pontok számával szokás meghatá-

rozni. Általánosan 4–12 pont/mm (100–300 dpi), a gyakoribb érték a 6–8 pont/mm. A kereskedelmi kódok szabványos modulméretértékét a 12,6 pont/mm felbontással, az ipari kódokét inkább a 8 pont/mm felbontással lehet jól megközelíteni. A 4 pont/mm és az a körüli, valamint a nem négyzet alakú kialakítás viszonylag ritka.

A nyomtatási szélesség. Ez az adat már a nyomtatók típusjelzésében is szerepelni szokott. Egyes esetekben nem a fej-, hanem a maximális anyagszélességre utal, ami rendszerint eltér egymástól; az utóbbi a nagyobb. Kialakult néhány általánosan használt mérettartomány. A 30-40 mm inkább a hordozható, az 50-60 mm pedig a direkt nyomtatókra jellemző. A nagyobb nyomtatók szokásos méretei 80-90, 104-110, 127-140, 160-170 és 210-220 mm körül mozognak, de nem minden gyártó alkalmazkodik ezekhez.

A memória nagysága. A nyomtató saját memóriájában tárolhat számos különböző címketervet, grafikus állományt stb. amelyet munka közben dinamikusan aktivizálhatunk. Itt tárolja a pontonként megtervezett címketervet is, ebből következően a nyomtatható hosszméret is a memórianagyság függvénye. A 32, 64 kilobyte méretű memória inkább csak a hordozható nyomtatókra jellemző, a szokásos alapérték 256, 512 kilobyte, ami többnyire 1-2 megabyte-ig bővíthető.

A nyomtatás sebessége. A beépített léptető motor(ok) sebességétől függően az ismert értékek: 40, 51, 60, 76, 102, 127, 152, 203, 254 és 305 mm/sec. A nyomtatás szokásos sebessége a skála első kétharmadán található értékek valamelyike. A nagyobb sebesség csak ott érhető el, ahol a nyomtatófej vezérlése is képes követni a változásokat, de a hatására keletkező minőségromlást a fejnyomás és a hőmérséklet növelésével próbálják kompenzálni. Ez még jobban felgyorsítja a rongálódási folyamatot.

A peel-off opció. Elsősorban on-line rendszerekbe ajánlott megoldás, amikor is a címke első kétharmada leválasztható a hordozóról, így a felhasználó egyetlen mozdulattal felragaszthatja a címkét, illetve lehetőséget ad az automatizálásra is. A hordozó visszacsévélésre kerül, tehát a hulladék kezelése megoldott. A nyomtató addig nem hajt végre új nyomtatást, míg a legutolsó leválasztott címkét el nem távolították.

A vágófej opció. A nyomtatóba szerelhető lehetőség, amely a felhasználó által megszabott helyen méretre vágja a címkét. Használata lassítja

a nyomtató működését, de olcsóbb kellékanyag felhasználását teszi lehetővé, mert stancolás nélküli, folyamatos anyagot alkalmazhatunk.

A slitter opció. Lehetővé teszi az anyag hosszirányú felvágását (pl. többpályás etikettek szétválasztása). Értelemszerűen csak a nyomtatás elvégzése utáni, külső szerelésű lehetőség.

A vezérlés. A 8 és 16 bites technológia már szinte alig található meg. A legkorszerűbb nyomtatókban két darab 32 bites processzor végzi felváltva a vezérlést.

A kommunikáció lehet soros (RS-232) vagy paralel (Centronics), illetve számos típuson mindkettőt megtalálhatjuk. Az általános felhasználhatóság érdekében opcionálisan RS-422, twinax, koax (IBM) kommunikációs interfész is választható.

A nyomtatók képesek állapotuk (státus) visszajelzésére. Ez aktivizálódik szoftverkérdésre vagy hibák (pl. kellékanyag-kifogyás, túlmelegedés stb.) hatására is. Hiba esetén az aktuális állapot és az éppen nyomtatott címketerv mentésre kerül.

A kellékanyag-továbbítás. A többnyire tekercsben előkészített alapanyag gumi (műanyag) hengerek között, dörzshajtással kerül továbbításra. A papír mérete 50-60 és 200-250 g között változhat. A festékszalagot egy feltekerő cséve húzza, amelynek a tartó cséve ellenfeszít, hogy a lehető legsimábban haladjon el a nyomtatófej előtt. A fejet ritkábban a saját súlya tartja az anyagon, és egy mechanikus retesz gátolja meg az elmozdulását, gyakrabban a reteszre szerelt rugós feszítés segítségével állítható be a fejnyomás.

Etikettek esetén a nyomtatók képesek a címke hosszának mérésére. Az optikai szenzor vagy a címkehatárt figyeli, amihez szükséges egy minimális címketávolság meghagyása, vagy a címkék hátulján lévő előnyomott jelzést vizsgálja.

Az alkalmazott festékszalagot egy másik optikai szenzor ellenőrzi.

A fontkészlet. A nyomtatók több, méretben állítható karaktertípust használnak, egy vagy több ismert nyomdai betűtípusban. Gyakran megtalálhatjuk köztük az OCR-A és OCR-B szabványokat is, így egyéb felhasználások számára szintén hasznosak lehetnek. Léteznek olyan nyomtatók, amelyek alkalmasak tetszőleges betűtípus kezelésére fontkártyákon keresztül, így igényes nyomdai feladatok ellátására is alkalmasak.

A felsorolt funkciók beállítása történhet kézzel, a nyomtató frontoldalán található vezérlő gombokkal, az értékeket egy kis kijelzőn megjelenítve, vagy szoftveres úton, vezérlő utasításokkal, amelyek képesek a kézi beállítást felülbírálni.

A helyes beállítás a nyomat minősége mellett a nyomtató élettartamát is befolyásolja. Akkor állítottuk be jól a nyomtatónkat, ha a megkívánt sebesség és jó nyomatminőség mellett a lehető legkisebb fejnyomást és -hőmérsékletet sikerült elérni, amihez más szempontokat (pl. festékszalag-feszítés) is figyelembe vettünk. A nyomtatók a jobb beállítás elérése érdekében többféle tesztcímke nyomtatását is lehetővé teszik.

A megfelelő címke és festékszalag kiválasztása

A kiválasztást segítő szakember várhatóan a következő kérdéseket teszi majd fel, ezért célszerű ezek megválaszolására előre felkészülni. Ez a témakör természetesen erősen összefügg a nyomtatóválasztással.

- Milyen alkalmazásról van szó? Más és más vonalkódcímke szükséges egy autó összeszerelésénél a főalkatrészekre, egy porszívó gyártás közbeni nyomon követésére, egy könyvtár olvasóinak kártyáira, a vérkészítmények speciális műanyag zsákjára vagy a tb-kártyákra.
- Milyen mennyiségben kell előállítani a vonalkódcímkét? Jó mérőszám lehet a napi szükséglet meghatározása nagyságrendi szinten.
- Mikor van szükség a vonalkódcímke előállítására? Előre elkészíthetjük, és azután tároljuk, adagoljuk, vagy pedig a termék létrejöttével, módosulásával együtt kell keletkeznie.
- Hogyan kerül fel az adott termékre, csomagolásra? Kézzel felragasztva vagy automatikusan felhelyezve, tasakba téve vagy függő címkeként felkötözve, bevarrva vagy műanyag tokba olvasztva (laminálva) – sokféle változat elképzelhető. A ragasztandó típusoknál fontos a felület minőségének ismerete.
- Milyenek az olvasási körülmények? A nagyon közeli vagy nagy távolságú olvasási igények, illetve az egyéb külső körülmények (pl. tűző napsütés) is befolyásoló tényezők.
- Mennyi ideig van szükség a címkére? Egy gyorsan forgó élelmi-

szerről van szó, amelynél elegendő egy termo-papírcímke direkt nyomtatással, vagy egy eladott motorkerékpár több évig ellenőrizendő garanciajegyére kerül a kód? Ennél a kérdésnél nyilván az is meghatározó, hogy milyen környezetben tárolják az árut. Fedett raktárban, szabad téren, napfénynek, esőnek, hónak kitéve vagy hűtőházban?

Milyen igénybevételek érhetik a címkét? Számos környezeti hatásnak – szennyeződés, olaj, zsír, alkohol, karcolás, magas hőmérséklet – ellenálló típus létezik. Sportversenyeken a tépés- és vízálló rajtszámot igénylik.

Milyen legyen a ragasztó? Az élelmiszerek, az egészségügyi alkalmazások speciális minőséget követelnek meg, míg a felhasználók egyik fele a könnyen eltávolítható, másik csoportja az eltávolíthatatlan típust igényli, illetve szélsőséges hőmérsékleti és páraviszonyok is előfordulhatnak.

Milyen a címke információs igénye? A feleslegesen nagy címke pazarlás, a túlzottan kicsi használhatatlan lehet. A méretet az információszükséglet és az ergonómia együttesen befolyásolja.

Milyenek a biztonsági követelmények? A biztonsági címkék eltávolítás után gyűrődnek, vagy eltávolítás közben szétszakadnak, így újrafelhasználásuk lehetetlen. Létezik olyan típus, amely leszedése esetén is hagy maga után lenyomatot. Másik biztonsági terület a másolás elleni védelem, a hamisíthatatlanság, amire szintén léteznek megoldások (pl. infrafényű takarások).

A felsoroltakból látható, hogy sokrétű és gondos tervezőmunkát igényel a vonalkódcímke alapanyagainak kiválasztása, annál is inkább, mert a rossz minőségű kellékanyag lerövidíti a nyomtató élettartamát, és rongálja a legdrágább alkatrészt, a fejet. Minden esetben forduljunk tehát szakcéghez már a tervezési szakaszban. Egy általános elvet mindenképpen be kell tartani. Termo-transzfer nyomtatásnál a festékszalagnak szélesebbnek kell lennie az alapanyagnál, különben a fej az anyag szélénél erőteljesen kopni kezd.

A nyomtatók üzemeltetése, karbantartása és szervizelése

A vonalkódrendszer alapja a jó minőségben nyomtatott vonalkódcímke. Gyakran hibáztatják a vonalkódolvasót vagy annak kezelőjét, ha

a vonalkód nem olvasható, pedig az ok sokszor a rossz minőségű címkében keresendő.

Néhány gyakori hibaok:

- a vonalkódcímke vagy festékszalag elöregedett,
- a színes címke rosszul tervezett, a vonalkód nehezen olvasható,
- a címketervező program nem megfelelően kezeli a szabványokat,
- az anyag reflexiója nem megfelelő.

Egy rendszer beüzemelésénél elvégezzük az optimális nyomtatóbeállítást, de ez nem jelenti azt, hogy az idők végezetéig változatlanul hagyható.

Minden új vonalkódcímke-széria előtt javasoljuk a tesztcímkegyártást, illetve a folyamatos gyártás során is célszerű az ellenőrzésére szolgáló speciális berendezés használata.

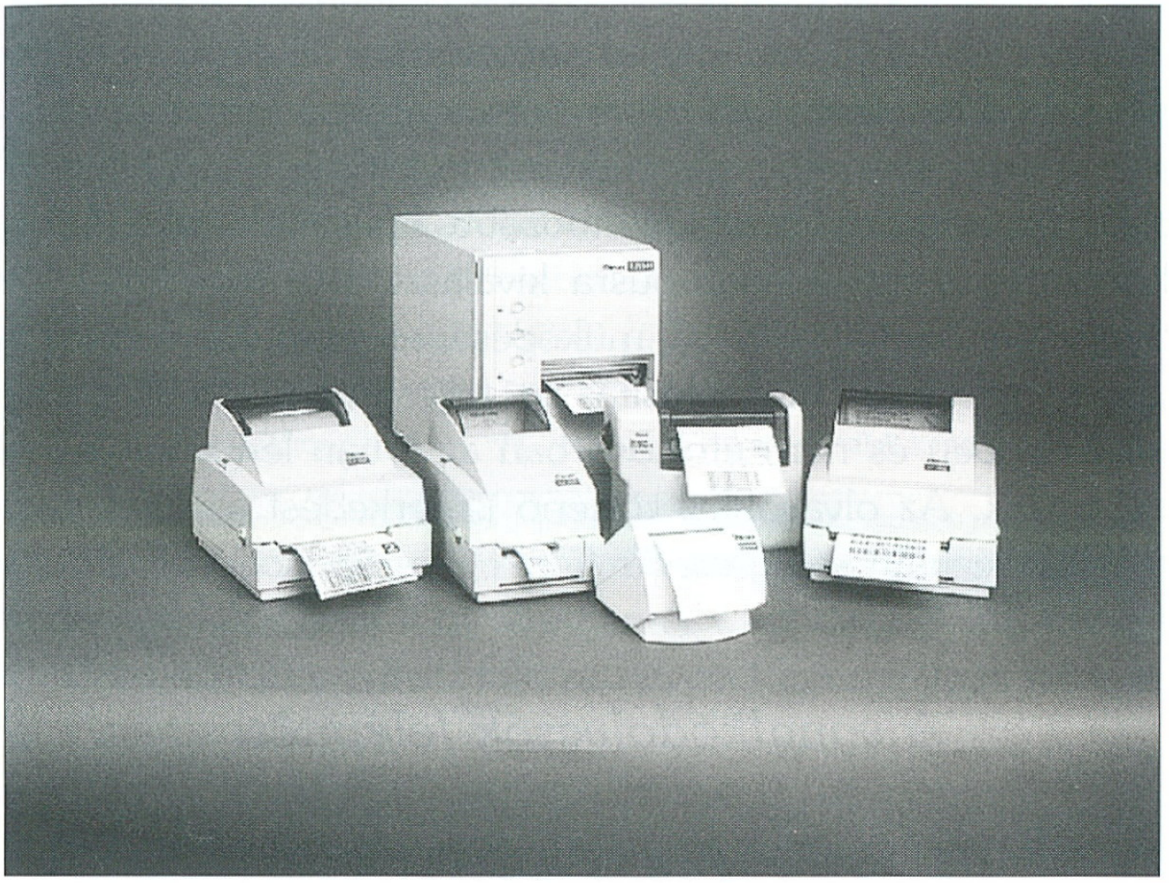
A működtetés során természetes a mozgó alkatrészek kilazulása és kopása. Ezt időszakos karbantartással tudjuk kiküszöbölni. A kopott alkatrészek cseréjét érdemes már kis mértéknél is elvégezni, mert nemcsak a nyomtatási minőségben jelentkezhetnek, de elősegíthetik más, esetleg értékesebb részek roncsolódását is.

A rendszeres tisztítás ugyancsak hozzásegít a nyomtatók biztonságos működéséhez. Különösen fontos a nyomtatófej takarítása, mert a környezeti szennyeződéseken kívül a címkék ragasztóanyaga is könnyen rákerülhet. Ez az eleinte csak alig észrevehető ragasztómennyiség megtapadása esetén rohamosan növekedni kezd, és a fej melegedésétől szét is kenődik. Eltávolítása történhet a nyomtatókhoz mellékelt tisztítókészlettel vagy fejtisztító alkohollal, puha anyag felhasználásával. A nyomtatófejek gyors tönkremeneteléhez vezet, ha a szennyeződést nem távolítják el; a hatására keletkező nyomtatásminőség-romlást a fejnyomás és a hőmérséklet növelésével próbálják kompenzálni, ami még jobban felgyorsítja a rongálódási folyamatot.

A vonalkódnyomtatók telepítésével együtt a szakcégek betanítják az üzemeltetőket a címketervezésre, a megfelelő üzemeltetési és karbantartási szabályokra. A nyomtatók szerelését gyakran nem tudjuk elvégezni hagyományos szerszámokkal. Ne barkácsoljunk, inkább vásároljunk hozzájuk illő szerszámkészletet, vagy bízzuk a javítást a szakcégekre.

Az optimális vonalkódnyomtató kiválasztását tehát a lehetséges típusok és azok kellékeinek részletes elemzése után tudjuk megvalósítani,

ami nem egyszerű, nem kevés munkát igénylő feladat, viszont a költségeket és a vonalkódos rendszer alapjait meghatározó kérdés.



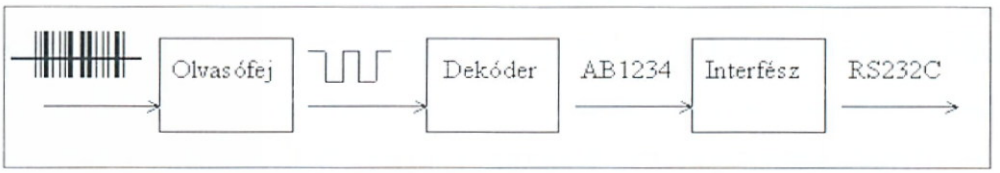
A vonalkódolvasók

A különféle vonalkódolvasó berendezések ugyanazt a feladatot látják el, a különböző szélességű, egymással párhuzamos fekete és fehér vonalak formájában kódolt információ gyors és biztonságos felismerését, majd az adatok valamilyen számítógépes rendszer felé történő továbbítását.

Napjainkra az olvasók legkülönbözőbb típusait kínálják a gyártók. Nem könnyű egy-egy feladattípusra kiválasztani a legmegfelelőbb eszközt. Szinte valamennyi olvasó működésének alapelve azonos, ugyanakkor az eltérő fizikai megvalósítás és teljesítmény miatt a méretben, a kezelhetőségben és nem utolsósorban az árban lényeges különbséget tapasztalhatunk. Az olvasókkal történő ismerkedést az általános felépítéstől kezdjük, ezután végighaladunk az egyes típusokon.

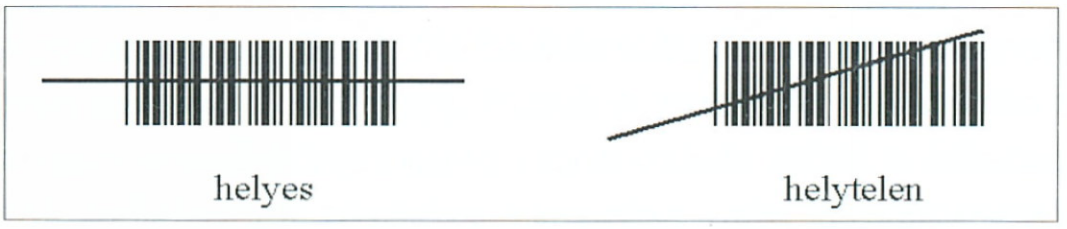
A vonalkódolvasók felépítése

Az olvasók működésének alapelve, vagyis az olvasás és a kódfelismerés (dekódolás) folyamata jól nyomon követhető, három fázisra bontható, mint azt az alábbi ábra mutatja.

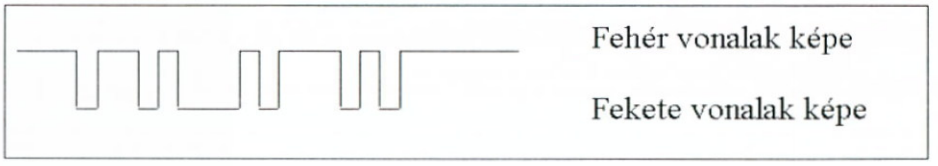


Az olvasófej

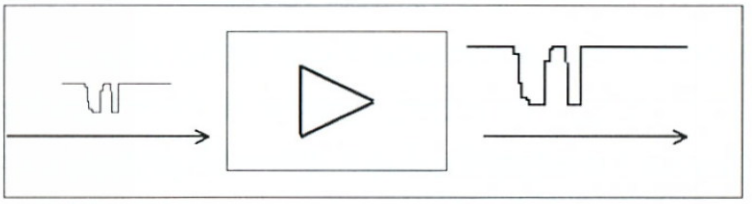
Az olvasás első fázisa az egymással párhuzamos vonalakra merőleges irányban történő letapogatás. A merőlegesség ugyan nem feltétele az olvasásnak, de egy-két kódtípustól eltekintve az már igen, hogy a pásztázó nyaláb valamennyi vonalat folyamatosan keresztezze.



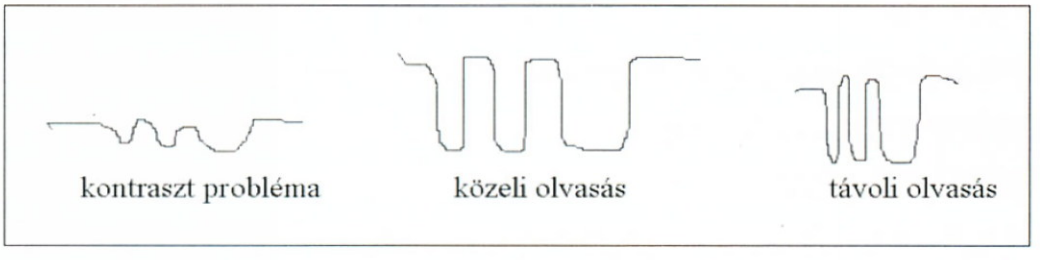
A fekete és fehér vonalak megvilágítása egy fókuszált LED (színes, általában piros fényt kibocsátó elem) vagy félvezető lézer alapú fényforrással történik. A fényforrás mozgatása történhet a felhasználó kézmozdulataival vagy valamilyen, az olvasóba beépített elektromechanikus tükörrendszerrel. A vonalkódról visszaverődő fényerősség változása mintegy kirajzolja a kód képét elektronikus formában. A módszer azon alapul, hogy a sötét vonalak jóval kevesebb fényt vernek vissza, mint a világos színűek.



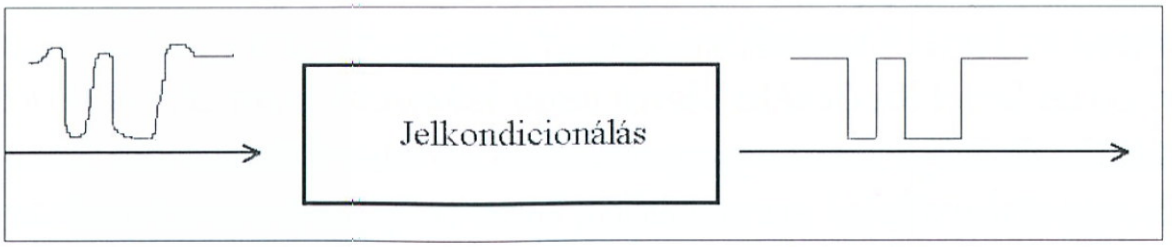
A visszaverődő fény egy fényérzékelő áramköri elemre kerül, ahol a leolvasandó kód képmását kapjuk egy nagyon piciny elektronikus jel formájában. Ezt a jelet egy erősítőfokozatra vezetik, amelynek kimenetén az alábbi jelet mérhetjük:



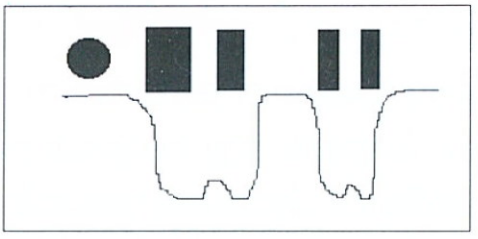
Gondoljunk bele, hogy minőségétől, a kód méretétől és színétől, illetve az olvasás távolságától függően mennyire eltérő eredményt kaphatunk egy-egy ilyen letapogatási folyamatban.



A visszaverődő fénysugár által szolgáltatott elektromos jelet valamilyen előre meghatározott értékűre célszerű alakítani, hogy a felismerési folyamatot megelőző mintavételezés kezdetét vehesse. Ezt a fázist jelkondicionálásnak hívják.

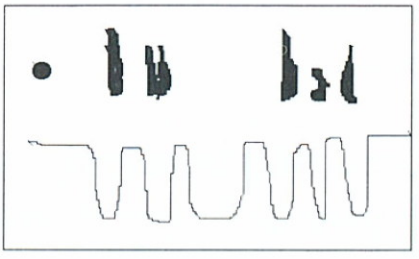


A vonalkódot alkotó vonalak minimális szélességének (ez az úgynevezett modulméret) és a letapogatást végző fénypont átmérőjének illeszkednie kell egymáshoz. A túlságosan nagy méretű fényforrással történő letapogatás (kicsiny kód vagy távoli olvasás esetén) az ábrán látható eredményt adja.



Mivel a letapogató pont átmérője jóval nagyobb a modulméretnél, ezért a vékony vonalak letapogatása nem lehetséges. Az olvasó nem tudja leolvasni a kódot, vagy rosszabb esetben hibásan teszi. (Ezt a megfelelő kódtípus és hossz kiválasztásával elkerülhetjük.)

A túlságosan kis méretű fénypont viszont a kevésbé jó minőségű vonalkód olvasásánál okozhat problémát, mégpedig a nyomtatási hibák esetén, amikor esetleg a festékpöttyöket is vonalaknak látja.



A probléma a lézeres és a CCD-elven működő olvasóknál egyaránt fennáll. A gyártók igyekeznek a fenti problémákat úgy kezelni, hogy kismérétű fénypontot építenek be az olvasóba, ugyanakkor a fénysugarat függőleges irányban megnyújtják, így a nyomtatási hibák nagyobbik része kiküszöbölhető. Ez a technika leginkább a mátrixnyomtatóval készített kódok olvasásánál használatos.

A vonalkódolvasók adatlapjában szinte kivétel nélkül megadják az olvasható kódméreteket. A garantáltan olvasható kódok modulméretét – így az olvasók felbontását – az inch ezredrészében (mil) szokták megadni (10 mil = 0,254 mm). Tipikus mérettartomány az 5–55 mil.

Az olvasók fontos paramétere az úgynevezett olvasási távolságtartomány (DOF), amely azt írja le, hogy egy adott méretű kód a fejtől számítva milyen távolságból olvasható.

A dekóder

A vonalkód-olvasási folyamat második lépcsője az első fázisban előállított jel feldolgozása, amely egy úgynevezett mintavételezési eljárással kezdődik. Ez nem más, mint a visszavert és kondicionált jel nagyságának nagyon gyors, egymás utáni vizsgálata. A mintavételi értékekből számítással elvégezhető a leolvasott fekete és fehér vonalak távolságának és szélességének becslése. (Pontosabb, ha fekete és fehér vonalak helyett „jól visszaverő" és „rosszul visszaverő" területekről beszélünk.)

A vonalkód felismerése a kódot határoló nyugalmi zónákkal, illetve a start és stop karakterekkel kezdődik. Maga a kódtartalom felismerése ezután következik: így először a lehetséges kódtípusok közötti automatikus szelektálás, majd a tényleges kódtartalom meghatározása. A dekódolás egy meglehetősen bonyolult és többlépcsős folyamat, amely ráadásul a másodperc töredéke alatt lefut, ezért nem csodálkozhatunk azon, ha a gyártók a részletes algoritmust hétpecsétes titokként őrzik. A felismerő algoritmusok a korszerű jelfeldolgozási ismeretek teljes matematikai apparátusát használják. A leolvasott kódot alkotó vonalszélességek becslése alapján megtörténik a detektált kód felismerése, és a dekódoló egység kimenetén megjelenik a visszanyert adat karakteres formában tárolva.

A dekódolás ideje azért lehet mindössze a másodperc töredéke, mivel a túl hosszú késleltetés a kódolvasást végző személy számára ergonómiailag elfogadhatatlan. A berendezések értékének nagy hányadát a jelfeldolgozó és kiértékelő algoritmus testesíti meg, amelynek alapján érezhető különbségek vannak egy-egy olvasó között.

Az olvasófejek és dekóderek együttes olvasási képességét az úgynevezett első olvasási arány (FRR) mutatójával mérik, amely 100 alkalomból a sikeres olvasások várható értékét adja meg, adott környezeti feltételek és nyomtatási minőség mellett.

Egy másik paraméter méri az olvasó- és dekóderegység döntési és felismerési képességét. Ez a mérőszám az úgynevezett helyettesítési hibaarány (SER), amely százalékos formában azt adja meg, milyen gyakran fordul elő olyan dekódolási folyamat, amelynek hibás a végeredménye (például 12345 helyett 12344 olvasása helyettesítési hibának számít, de 1234 úgyszintén). A mérőszám értéke azonos nyomtatási és környezeti feltételek esetén vonalkódfajtánként eltérő értéket ad.

A dekódolást végző programok a berendezések belsejében, csak olvasható memóriamodulban (PROM, EPROM) találhatók. Léteznek eszközök, amelyek programja a szakszervizben viszonylag egyszerű eljárással frissíthető. Így az olvasó alkalmassá tehető például újfajta vonalkód felismerésére és olvasására.

A dekódolási folyamat legtöbbször nem ér véget a kód felismerésével, a felhasználó igényelheti például lezáró karakter hozzáadását (enter) a kód végéhez, vagy akár ennél összetettebb utófeldolgozás is szóba jöhet. Az előírt formátumú adat ezután kerülhet az interfészegységen keresztül a külvilágba, amely legtöbbször fizikailag egybe van építve a dekódoló résszel.

Milyen torzító hatások érhetnek egy vonalkód-olvasási műveletet? A legelső a vonalkódolvasó ceruzák esetében előforduló pásztázásisebesség-ingadozás, aminek hatására a vonalak az olvasó számára megvastagodnak, illetve elvékonyodnak. Torzulást okoz a görbült felületre helyezett vonalkód, amelynek csak egy síkra vetített felületét látja a CCD vagy lézerolvasó. Nehezebben korrigálható torzulások jelentkeznek gyűrött címkék, illetve a pásztázási sebességhez képest gyorsan mozgó kód esetén. A csomagolóanyag reflexiós tulajdonságai, a nyomtatási technológia és a színezés tovább nehezítheti a felismerést. A vonalkódok felépítése nem szimmetrikus abban az értelemben, hogy egy olvasónak meg kell állapítania, jobbról balra vagy balról jobbra pásztázza végig az adott kódot.

Az olvasók tévedhetnek, de egy jó minőségű készülék inkább nem olvas, mint hogy rossz információt továbbítson a felhasználó rendszerébe.

(Itt kell megjegyeznünk, hogy létezik olyan helyettesítési hiba, amelyért még a legjobb olvasó sem hibáztatható. Egyes kódok ugyanis olyan felépítésűek – az I 2of5 ilyen –, hogy egyes esetekben a belső részük is értelmes, szabályos kódot alkot, ennélfogva a valóságostól eltérő adat kerülhet leolvasásra.)

A megoldás erre és az ehhez hasonló problémákra a körültekintő rendszertervezésben rejlik. Egy zárt rendszerben legtöbbször előre lehet tudni az alkalmazandó kódfajtákat és azok előforduló hosszértékeit, amely gyakran egy vagy két állandó érték. Az olvasókat pedig be lehet programozni arra, hogy egy-két kódtípust ismerjenek fel, és ezen belül is megadható a megengedett hosszértékek halmaza.

A legtöbb dekóder automatikusan megkülönbözteti a fényceruzát a lézerolvasótól. A fizikailag több bemeneti csatlakozási ponttal ellátott eszközök egyszerre több olvasót is tudnak kezelni, gondoskodva arról, hogy az adatok egymástól megkülönböztetve, de szigorúan egymás után kerüljenek továbbításra a háttérrendszer felé. Természetesen az egyes bemenetek egymástól függetlenül, külön-külön programozhatók.

A dekóderek között nagy különbség van a többletszolgáltatások terén is. Felkínálhatnak olyan lehetőségeket, mint a bemenettől és a kódtípustól függő adatformázás, például karakterek törlése, beszúrása, ismétlése. A legtöbb esetben állítható a kereskedelmi UPC/EAN kód olvasásának biztonsági szintje, így egy adott alkalmazásban össze lehet hangolni az olvasás sebességét és a dekódolás biztonságát. Gyakran adott a lehetőség a kereskedelmi kódok (EAN-8, EAN-13, UPC-A, UPC-E) közötti konverzióra is.

Sok esetben – például futószalag mellett történő olvasáskor – szükség lehet arra, hogy a dekóder jelezze a sikertelen olvasás eredményét, ami történhet hangjelzéssel vagy egyedi adat elküldésével.

Az interfész

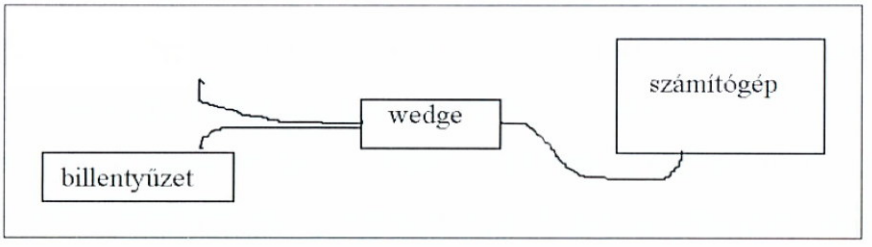
Az interfész az olvasók harmadik és egyben utolsó egysége, amelyet legtöbbször fizikailag egybeépítenek a dekóderrésszel. Funkciója azért fontos, mert a kimenetén előálló adatfolyamot lehet fizikailag továbbítani a külvilág felé.

Gyakran találkozhatunk úgynevezett többszörös interfészegységgel, amely a programozástól függően más és más fizikai jel kibocsátására ké-

pes. Így például a billentyűzet és az RS232 soros jeleit gyakran ugyanaz az interfész támogatja, a kettő közötti váltás egy vezérlő vonalkód beolvasásával elvégezhető.

A számítógépeken a soros RS232 port vagy a billentyűzet jelenti a legismertebb bemenetet. Míg a soros vonal egységesnek mondható – eltekintve a csatlakozó típusától és vezetékeinek számától –, addig a billentyűzetbemenet fizikailag (hardverszempontból) és programozástechnikailag (szoftverszempontból) szinte minden terminháltípus esetén más és más. A billentyűzethez történő illesztés programozástechnikailag ugyanakkor könnyebb, hiszen a billentyűzetet kezelő program minden gépen eleve rendelkezésre áll. A soros vonali adatok kezelése viszont a legtöbb esetben kisebb-nagyobb programírással jár együtt.

A számítógépek billentyűzetével párhuzamosan kötött interfészt (wedge) az alábbi ábrán láthatjuk, az olvasó mintegy beékelődik a billentyűzet és a számítógép közé.



A számítógép nem tudja megkülönböztetni a valóságos billentyűleütéseket az olvasó által szolgáltatott adatoktól. A nem szokványos terminálok billentyűzetéhez történő illesztésnél érdemes szakember tanácsát kikérni, mivel szükség lehet karakterkésleltetések beállítására. Néha olyan árnyalatnyi finomságok döntenek egy berendezés mellett, hogy meg tudja-e különböztetni mondjuk a 102 gombos billentyűzet két home billentyűjét.

Vonalkódolvasókat nem csak számítógépekhez, hanem a legnagyobb számban számítógép alapú pénztárgépekhez használnak. A pénztárgépek a legkülönfélébb bemenetekkel rendelkeznek, mivel a gyártók szeretnek saját, általában más gyártókétól különböző interfészt definiálni.

Sajátos megoldás az úgynevezett intelligens kábel, amely az olvasóból kijövő általános interfészjelet átalakítja a kívánt típusúra. Nagy-nagy elő-

nye, hogy a pénztárgép cseréje esetén sem kell az olvasót leváltani, elegendő a kábeldarabot változtatni.

A CCD-olvasók és a lézerszkennerek kimenete lehet wandemuláció, ami azt jelenti, hogy az olvasók olyan kimenetet állítanak elő, mintha az egy fényceruza felől érkezett volna. Így egy fényceruza könnyen kiváltható nagyobb teljesítményű olvasóval anélkül, hogy a rendszerelemeken bármilyen változtatást kellene végrehajtani. Tipikusan erre van szükség hordozható adatgyűjtők olvasóinak cseréjekor.

A korszerű számítógépeken megtalálható az úgynevezett USB-bemenet, amely a hagyományos billentyűzet- és a soros-párhuzamos bemeneteket egységes interfészbe tömöríti. Egy gépre több USB-eszközt, így több olvasót is köthetünk, amelynek jeleit legtöbbször maga az operációs rendszer kezeli. Az alábbi táblázat röviden összefoglalja a legismertebb interfészeket.

Wand	Fényceruzát emuláló kimenet
Lézer	Lézerolvasót emuláló kimenet
RS232C	Aszinkron soros-vonali kimenet
Duál RS232C	Kettős aszinkron soros-vonali kimenet
IBM POS	IBM pénztárgépekhez kimenet
OCIA	Optikailag csatolt soros interfész
Wedge	Terminál billentyűzet emuláció
OCR	Optikai karkater felismerő emuláció
USB	Univerzális soros busz

A vonalkódolvasók fajtái

Az alábbi összefoglaló táblázat segít az egyes olvasók közötti eligazodásban.

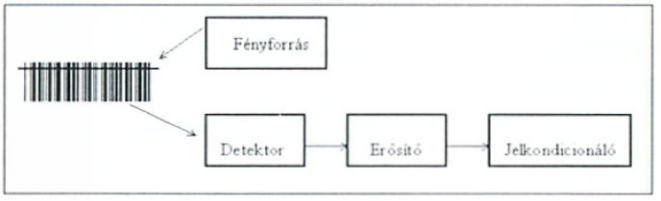
Tipus	Kézi vagy fix	Tipikus felbontás	Olvasási tartomány	Sebesség	Árfekvés
Fényceruza	Kézi	10 mil - 25 mil	0 cm	közepes	Alacsony
CCD olvasó	Kézi és fix	5 mil - 40 mil	0 - 5 cm	jó	Alacsony
Lézer olvasó	Kézi és fix	5 mil - 100 mil	0 - 100 cm	kiváló	Közepes
Lézer 2D	Kézi és fix	5 mil - 40 mil	0 - 30 cm	kiváló	Magas
Képalkotó	Kézi és fix	5 mil - 40 mil	0 - 50 cm	jó	Magas

A fényceruza

A vonalkódolvasó ceruza (fényceruza vagy wand) az olvasók közismert, klasszikus megoldása. Népszerűségét kis méretének, hordozható-

ságának és viszonylag alacsony árának köszönheti. Használata során a felhasználónak egy mozdulattal – lehetőleg állandó sebességgel – a vonalakra merőlegesen kell végighúznia az olvasó hegyét. Az olvasás kiindulópontjának a vonalkódot körülvevő nyugalmi zónán kívülre kell esnie. Az olvasófejet általában úgy alakítják ki, hogy azt egy írószerszámhoz hasonlóan kényelmesen, kis szögben lehessen tartani.

A ceruzák optikájának fizikai kialakítása többféle lehet, de az elv minden berendezésben azonos. Fényforrásként látható fényű vagy infravörös LED szolgál, amelynek fényét üvegszállal vagy valamilyen lencserendszer segítségével fókuszálják. Ahogy a felhasználó végighúzza az olvasó hegyét a vonalkód teljes tartományán, a visszavert fény egy lencserendszeren keresztül összegyűlik, majd egy fényérzékelő detektorra vetül. A detektor a visszavert fény intenzitásával arányos piciny kimeneti áramot állít elő, amely erősítés és kondicionálás után kerül a dekódoregység bemenetére.



A ceruzák fix lencserendszere a lézerolvasóknál megszokott vonalkódfelbontás jóval kisebb tartományát fogja át. Ez azt jelenti, hogy egy átlagos tulajdonságú fényceruza a 10–25 mil modulméretű vonalkódokat tudja biztonsággal olvasni.

Ha a leolvasandó kódok között nagy számban fordul elő 10 mil-nél kisebb, akkor más fókuszú lencserendszerrel ellátott olvasóra van szükség (a lencserendszer fókuszálási tulajdonságait szokták apertúrának is nevezni). Nem megfelelő lencserendszer esetén az első olvasási arány értéke nagyon alacsonnyá válhat, ami a berendezést nehezen használhatóvá teszi. A gyártók részletesen specifikálják adatlapjaikban, hogy egy adott vonalkód modulméretéhez milyen apertúrájú olvasó illeszkedik a legjobban.

A fényceruzák használata rövid betanulási időt igényel. A ceruza végét lehetőleg állandó sebességgel, adott szögben tartva kell végighúzni a kódon. Ügyelni kell arra, hogy az olvasás ne az első vonalnál, hanem a vo-

nalakat körülvevő nyugalmi zónán kívül kezdődjön. A mozgatás sebessége általában 10 és 150 cm/sec között változhat.

A ceruza végének érintenie kell a kódot, de az olvasás akkor is sikeres, ha a nyomtatott kódot 0,5 mm-nél vékonyabb, átlátszó fóliaréteg borítja. (A vonalkódot érintő olvasáshoz olyan címke ajánlott, amelynek nyomtatási technológiája védelmet nyújt az olvasó fejének koptató hatása ellen. Így a termocímkék megfelelőek, de a termo-transzfer típusúak közül csak a kaparásálló festékszalaggal nyomtatottak jók, egyébként laminálni kell őket.)

A ceruzák első olvasási aránya már elfogadható, ha meghaladja a 90%-ot. (Ez az érték lézer- vagy CCD-olvasóknál elfogadhatatlanul alacsony!) Az olvasók tápellátása az interfész felől történik, amely általában külön egységet képez. A működési feszültség értéke tipikusan 5, illetve 12 V, a ceruza áramfelvétele néhány mA körüli, dekóderrel együtt 50–80 mA szokott lenni.

A látható fényű ceruzák általában olvassák a különféle technológiával nyomtatott kódokat, természetesen a színes vonalkódok vagy a kiugróan rossz minőségű felületek esetén nem árt óvatosnak lenni, és a vásárlás előtt gyakorlati tesztet végezni. Az infravörös (IR) tartományban működő eszközök karbon alapú festékkel nyomtatott kódok olvasására használhatók, ennek megfelelően a közönséges termocímke ezen olvasók számára láthatatlan.

A vonalkódolvasó ceruza kiválasztásakor az alábbi szempontokat érdemes figyelembe venni:

- apertúraméret (a vonalkód modulszélességének függvénye),
- a fényforrásként használt LED hullámhossza (infravörös vagy normál),
- nyomtatási technológia (dörzsölés- és kaparásállóság),
- áramfelvétel,
- a rendelkezésre álló interfész,
- mechanikai ellenálló képesség és élettartam,
- ár.

A CCD-olvasók

Ha egy felhasználót megkérdezünk, melyik olvasó jut eszébe a vonalkódolvasó szó hallatán, majdnem biztos, hogy a CCD-olvasóra gondol. Ez az egyik legelterjedtebb vonalkódos eszköz.

A vonalkód megvilágítása egy piros színű LED-sorral történik – a fényforrások száma 5 és 10 közé esik –, amely fókuszálás nélkül világítja be a leolvasandó területet. A megvilágított vonalkód képe egy lencserendszeren halad át, és egy fényérzékelő detektorokból álló cellasorra vetül (CCD). Egy ilyen tömb 1024, 2048 vagy 4096 képpontot tartalmaz, azaz ilyen finomságú lesz a kép felbontása.

A működés alapelve az, hogy a félvezető alapú detektorpontokban elektromos töltés halmozódik fel, mégpedig a visszavert fényintenzitással arányosan. Az így keletkezett képet másodpercenként több százszor kiolvasva megkapjuk az olvasandó kód „elektronikus képmását". Ez az elektronikus kép a ceruzához hasonlóan kondicionálás után dekóderre kerül, amely előállítja a kódban tárolt információt.

Hagyományos CCD-olvasók

A hagyományos olvasók fogalmába tartoznak a klasszikus CCD-eszközök. Közepes árfekvésüknek, egyszerű felépítésüknek, ugyanakkor nagy megbízhatóságuknak – hiszen nem tartalmaznak elektromechanikus elemet – köszönhetik népszerűségüket. A másodpercenkénti több százszoros letapogatási sebesség kielégítő olvasási teljesítményt és magas első olvasási arányt garantál elvétve előforduló helyettesítési hibák mellett. A mechanikus igénybevételt csökkentendő a szkenner fejét általában gumipánttal veszik körbe.

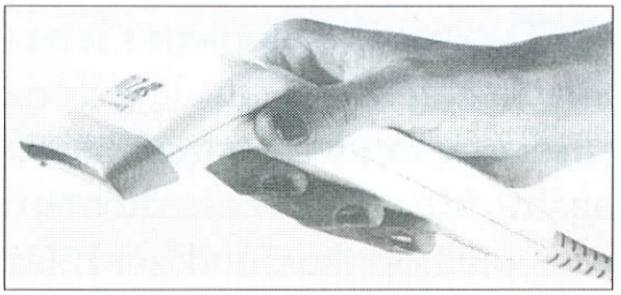
A megfelelő olvasó kiválasztásánál figyelembe kell venni a fej szélességét. Mivel az olvasási tartomány néhány centiméteren belül van, a leolvasandó kódnál szélesebb fejű olvasó ajánlott. A könnyű kezelhetőség érdekében célszerű a legnagyobb kód méreténél 20-30%-kal nagyobb fejméretet választani.

Mivel ezeket a készülékeket elsősorban kereskedelmi alkalmazásokra fejlesztették ki, ahol a leolvasandó kódok mérete kevés kivételtől eltekintve a 25–50 mm-es tartományba esik, így a 60, illetve 80 mm-es fejméret a leggyakoribb, de van 40 és 100 mm-es fejjel szerelt olvasó is.

Az olvasás szélességét látszólag növelhetjük az UPC/EAN kódoknál megvalósítható technikával: a kód leolvasását két részletben végezzük, s az egyik felének sikeres olvasását külön sípszó jelzi.

A dekóder és az interfész legtöbbször az olvasófejjel egy házba kerül, és a szokásos billentyűzet- és RS232 soros kimenettel csatlakozik a külvilág felé. A CCD-olvasókat szokták úgynevezett fényceruza- vagy lézerszkenner-emulátor (ceruza- vagy lézerkimenet tökéletes utánzása) kimenettel szerelni, ami a felhasználó számára azzal az előnnyel jár, hogy a korábban használt olvasóit egy mozdulattal CCD-olvasóra cserélheti az interfészegység és a programok bárminemű változtatása nélkül.

A legtöbb berendezés el van látva kézi nyomógombbal, amely az olvasás indítására szolgál. Ha átkapcsolunk automatikus olvasásra, a készülék folyamatosan pásztáz leolvasandó kód után.



A CCD-olvasók a tápellátást általában a háttérrendszer felől, ritkább esetben tápegységről kapják. A ceruzákhoz hasonlóan állandó – általában +5 V – tápfeszültséget igényelnek, áramfelvételük interfésztől függően 80 és 120 mA közé esik.

Az olvasók felbontását, azaz a legkisebb olvasható kód modulméretét a fotodióda-cellák sűrűsége határozza meg. Ajánlott, hogy legalább kettő, de inkább négy cella vastag legyen a legfinomabb felbontású kód vonalvastagsága. Ez a gyakorlatban 5-6 mil modulméretű kódok olvasását teszi lehetővé.

Az olvasók túlnyomó többsége kézi kivitelű, de létezik fix telepítésű CCD-olvasó is, amely futószalag melletti alkalmazásokra ajánlott. Egy részük a videokamerákra emlékeztet, olvasási távolságtartományuk jellemzően 10 és 20 cm között mozog.

A megfelelő olvasó kiválasztásánál az alábbi szempontokat érdemes figyelembe venni:

- az olvasó fejmérete,
- az olvasó felbontása,
- a letapogatás sebessége,

- olvasási tartomány és szög,
- olvasható kódtípusok,
- interfész-lehetőségek,
- áramfelvétel,
- ár.

Különleges CCD-olvasók

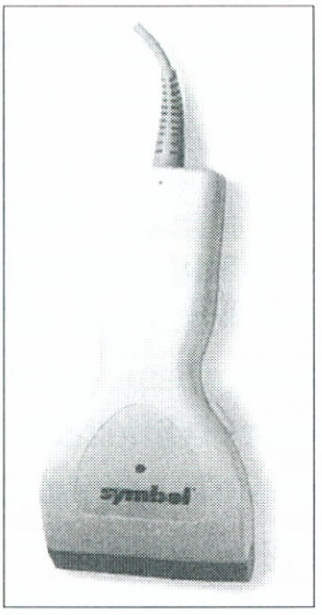
A CCD-olvasók fejlesztésének irányát egyrészt az olvasási tartomány növelése, másrészt a kétdimenziós (2D) vonalkódok olvasása jelenti. Mind a kézi, mind a fix telepítésű kivitelben megjelentek ilyen tudású eszközök.

A nagy távolságú CCD-olvasók különleges lencserendszert, fókuszált megvilágítást és egy nagy érzékenységű detektorsort tartalmaznak. Az olvasási távolság egy nagyságrenddel nagyobb, mint hagyományos társaiknál, és elérheti az 50-60 cm-t. Az eszközök nagyfokú elterjedése magasabb áruk és a bonyolult optikai rendszer miatt nem várható. A nagyobb távolságról történő olvasásra inkább lézerolvasót célszerű használni.

A kétdimenziós CCD-olvasók jellemző tulajdonsága, hogy az olvasási távolság változatlanul hagyása mellett sebességüket megnövelik, és a kétdimenziós kódok olvasására alkalmas felismerő programokkal látják el. (A kétdimenziós kódok olvasása a nagy adatmennyiség és az összetett hibadetektáló és -javító algoritmusok miatt egy nagyságrenddel gyorsabb dekóderprogramot követel meg.)

Mivel a kétdimenziós kódok nem csak szélességükben, hanem magasságukban is hordoznak információt – ezért hívják ezeket kétdimenziósnak –, a 2D-olvasókat nem elegendő a kód fölé helyezni, hanem merőleges irányban végig is kell rajta húzni. A CCD-olvasók között találunk olyan, „kenyérpirítóelven" működő eszközt, amelybe egy hagyományos vagy 2D-kódot tartalmazó kártyát kell behelyezni, és ezután azt lenyomni. A kézi raszterezés műveletét maga az olvasó végzi a kártya függőleges irányú emelésével és kidobásával.

Természetesen a 2D-olvasók a hagyományos olvasókkal kompatibilisek, valamennyi egydimenziós kódot is olvassák. Áruk kicsit magasabb, mint egydimenziós változataiké.



Lézerolvasók

A lézerolvasók a vonalkódolvasás legnagyobb teljesítményű eszközei. Ez megmutatkozik a berendezések viszonylag magasabb árfekvésében.

Az első lézerolvasók He-Ne lézert tartalmaztak. A kibocsátott fény frekvenciája a 633 nm közelébe esett, ami nagyon jól látható színű sugárzást jelentett. A ma alkalmazott félvezető lézerek frekvenciatartománya 650 és 675 nm közötti, ami az emberi szem számára kevésbé intenzíven érzékelhető, azaz halványabbnak látszik egyforma fizikai teljesítmény esetén. A félvezető-technológia fejlődésével várható a kibocsátott fény frekvenciájának további csökkenése.

A kibocsátott lézerfény frekvenciája egy adott érték köré összpontosul, azaz monokróm, egyszínű. Mindemellett koherens is, azaz a kibocsátott fény hullámai azonos fázisban rezegnek. A lézer kis térrészbe koncentrálva terjed, és ez a tulajdonsága teszi lehetővé, hogy az olvasók nagy távolságról (ez ma már a 10 métert is meghaladja) képesek vonalkódolvasásra.

A többi olvasóval ellentétben itt nem a visszavert, hanem a kilépő fénysugár fókuszált. A félvezető lézerből kilépő keskeny nyaláb bizonyos terelés és fókuszálás után egy rezgő vagy forgó tükörrendszerre vetül. A rezgés frekvenciája kézi olvasó esetén 40/sec körüli, így az emberi szem számára csak egy keskeny fénycsík látható. A normál lézerolvasók pontmérete úgy van beállítva, hogy jó minőségű kódok esetén az alábbi – modulszélességtől függő – olvasási távolságtartomány garantált:

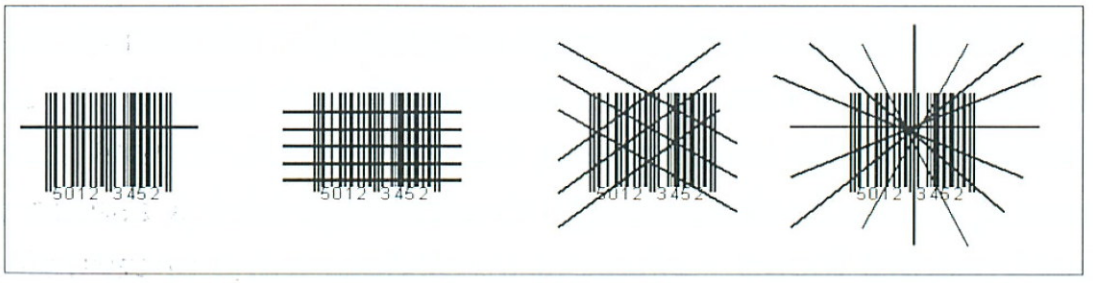
Modulméret	Olvasási zóna
5 mil (0.13mm)	1 - 10 cm
7.5 mil (0.20mm)	0 - 20 cm
10 mil (0.26mm)	0 - 30 cm
20 mil (0.51mm)	5 - 50 cm
40 mil (1.02mm)	10 - 80 cm
55 mil (1.43mm)	15 - 100 cm

A keskeny lézernyaláb a kódról diffúz módon verődik vissza, azaz a tér minden irányába szétszóródik. Az olvasóban egy polarizációs és egy, a megvilágító fény frekvenciájára hangolt szűrő található. Ezeknek köszönhető, hogy egy lézerolvasó távolról, erős környezeti fény ellenére képes akár rossz minőségű kódok olvasására is. A nagyon gyenge visszavert jelből ki tudja szűrni a lényeges információt hordozó részt.

Minél kisebb a kód modulszélessége (azaz minél vékonyabb vonalakból áll), annál kisebb az olvasási távolság. A bonyolult matematikai modellek helyett érdemes egy-egy gyártó adatlapját elővenni az olvasási tartomány vizsgálatához. Vigyázzunk arra, hogy a megadott értékek átlagosan, adott hőmérsékleten és csak kiváló minőségű kódok esetén érvényesek.

A pásztázó mozgást létrehozó tükörrendszert egy motor vagy mágnes rezegteti, illetve forgatja. A tükör ideális esetben saját rezonanciafrekvenciáján rezeg, egy hangvillához hasonlóan. Ekkor egészen kis áramfelvétel mellett már egy piciny mágneses tekercs is elegendő a rezgés elindításához és folyamatos fenntartásához.

A leggyakoribbak az egy vonalban pásztázó szkennerek, de vannak úgynevezett raszterszkennerek – főleg kétdimenziós kódok olvasására –, amelyek sok párhuzamos vonallal pásztáznak, és vannak több irányból pásztázó (omnidirekcionális) szkennerek, amelyek az adott térrészt különböző irányú vonalak sokaságával tapogatják le.



A lézerek által kibocsátott fény természeténél fogva nagy fényenergiát jelent kis térrészbe koncentrálva, ennélfogva felhasználására szigorú előírások vonatkoznak.

A kimenő teljesítmény alapján a lézereket különböző osztályokba sorolják. Az osztályba sorolás meglehetősen összetett előírások alapján elvégzett mérésekkel történik, és a gyártók kötelezettsége. Egy berendezés osztályba sorolása alapvetően a teljesítménytől függ, de a besorolásnál figyelembe kell venni a kibocsátott fény frekvenciáját, impulzusüzem esetén a fénykibocsátás idejének a teljes időtartamra vetített arányát, az úgynevezett kitöltési tényezőt, valamint a besugárzás időtartamát.

Általánosan elmondható, hogy a lézeres olvasókból kilépő fénysugárba tilos belenézni, mert az erős fény kárt tehet az emberi szemben. A forgalomban lévő lézeres vonalkódolvasók túlnyomó többsége az 1-es és 2-es osztályba tartozik, de van 3A osztályba tartozó olvasó is.

1-es osztályú lézergyártmány: ebbe az osztályba sorolják azokat a berendezéseket, amelyek véletlen vagy szándékos belenézés esetén sem jelentenek veszélyt a szemre. A megengedett értékek az amerikai és az európai szabványokban kissé eltérnek, sőt még az európai előírások sem egységesek. A kereskedelemben elsősorban az 1-es osztályú olvasókat lehet forgalomba hozni, a magasabb osztályba soroltak kereskedelemben történő alkalmazásának szigorú előírásai vannak. (Ennek oka az, hogy egy pénztárgép mellett bárki belenézhet a lézersugárba, hiszen egy kiskorú vásárlótól nem várható el, hogy a lézersugár veszélyességét ismerje.)

Az eszközből kilépő lézerteljesítményt két módon lehet korlátozni az 1-es osztályba sorolt berendezéseknél. Vagy kellően nagy térrészbe – sok különálló vonalat előállítva – vetítik a pásztázó nyalábot (pl. pultszkenner esetén), vagy pedig korlátozzák adott időtartamra a lézerfény kibocsátási idejét. Ezzel elérhető, hogy a felületegységre eső állandó fényteljesítmény értéke kisebb legyen a megengedettnél. Utóbbi inkább kézi olvasók estén elterjedt megoldás, ahol az egy vonalban történő pásztázásnak köszönhetően a felületegységre eső fényenergia viszonylag nagy.

2-es osztályú lézergyártmány: a legtöbb lézerolvasó ebbe az osztályba tartozik. Ezek a lézerek már nem veszélytelenek, de véletlen belenézés-

kor nem okozhatnak szemsérülést, mert a veszélyben lévő retinát a kikerülési reakciók – pislogás, illetve a fej vagy a tekintet elfordítása – megvédik. A kilépő lézersugárba szándékosan belenézni viszont egyáltalán nem ajánlott, sőt veszélyes lehet! A 2-es osztályú olvasók kimenő fényteljesítménye maximálisan 1 mW lehet folyamatosan, impulzusüzemben pedig táblázatból kikereshető érték.

3A osztályú lézergyártmány: ide sorolandó valamennyi lézerolvasó, amely a 2-es osztályú lézerekre megadott kisugárzási határérték ötszörösét meg nem haladó fényteljesítményt (5 mW) bocsát ki. A nagy távolságú és a nagy fényerejű olvasók ebbe az osztályba tartoznak, fényteljesítményük azonban általában nem haladja meg a 2,5 mW-ot. A 3A osztályú lézergyártmány fénysugarába szabad szemmel vagy optikai eszközön keresztül belenézni veszélyes, így tilos! A szemet a kikerülési reakciók (pupillareflex) ennek ellenére általában megvédik.

A 3B és 4-es osztályú lézerek ismertetésétől itt eltekintünk, mivel vonalkódolvasó készülék ilyen nagy teljesítményű kategóriába nem eshet. Ezek a lézerek egészségügyi és ipari alkalmazásokban lelhetők fel.

A lézerolvasók felhasználási területe nemcsak a nagy távolságú olvasásra szorítkozik. A lézerszkenner könnyen olvas műanyag fólián, üvegen keresztül, és a gyűrött vagy görbült felületre helyezett címke sem jelent nehézséget. Nagyfokú kényelmet jelent, hogy a címke síkjától 40-50 fokos szögben elfordítva is jól használható.

Normál lézerolvasók

A legismertebb és a legnagyobb darabszámban használt olvasófajta. Közös jellemzője, hogy az eszköz egy vonalban másodpercenként körülbelül negyvenet pásztáz. Az olvasók csoportosítása nem könnyű, többféle szempont szerint is osztályozhatók.

Leginkább az alkalmazás típusa (közeli vagy távoli olvasás, kézi vagy fix telepítés, kábeles vagy kábel nélküli, nyomógombos vagy fotocellás indítás stb.), az olvasási teljesítmény (kis, közepes vagy nagy átbocsátóképesség), valamint a környezeti behatásokkal szembeni ellenállás (kereskedelem, ipar, különleges körülmények) alapján határozzák meg a kívánt típust. Leggyakrabban a dekóderrel és az interfésszel egy tokba vannak szerelve, de létezik dekóder nélküli változat is.

A kereskedelmi alkalmazásokra ajánlott olvasók közepes fizikai igénybevételre készülnek, teljesítményük a közepestől a nagy átbocsátóképességig terjed.

Olvasási képességük kiváló, ezek az eszközök birkóznak meg a legkönnyebben a kereskedelemben előforduló anomáliákkal, amikor a nagyvonalúan elintézett nyomtatás következtében a vonalkódok jóval a megengedett határértéken kívülre esnek. A kereskedelmi olvasók – igen kifinomult felismerő algoritmusaiknak és az eszközökbe rejtett különleges áramköri megoldásoknak köszönhetően – rendkívül tapasztaltak a vonalkódok „betegségeit" illetően, képesek a hibás kódokhoz történő alkalmazkodásra (például nyomtatási vagy kontrasztprobléma), illetve egyes kódok részekben történő leolvasására. Könnyedén veszik a legtöbb akadályt, amellyel nap mint nap szembesülnek. A gyűrött, különleges színű, hiányos vagy torzult kódok sem tudják zavarba hozni őket. (A zártabb ipari rendszerekben a nyomtatás folyamata sokkal egységesebb képet mutat, ott az olvasókra ilyen jellegű kihívás nem vár.)

Az olvasási távolság tipikusan az 5–50 cm-es távolságtartományba esik, fix olvasó esetén kicsit közelebb, kézi olvasó esetén pedig kissé távolabb van. A legújabb típusok érintő olvasásra is képesek. A hagyományos készülékeket állványra helyezve a felhasználó mindkét keze szabaddá válik. Az intelligens olvasók észreveszik, ha állványra helyezik őket, és automatikus pásztázásra váltanak. Állványos használat esetén ügyelni kell az olvasó alá helyezett kód megfelelő irányba történő állítására, ami csökkenti az átbocsátóképességet.

A lézerolvasóknak van egy úgynevezett holtzónájuk, amely egy néhány fokos szögtartomány. Amikor az olvasót a merőlegeshez közeli szögben tartjuk, a visszaverődő fény az olvasóba jutva azt mintegy „elvakítja". Ezért a lézerszkennerek használatánál ügyelni kell arra, hogy lehetőleg a merőlegestől eltérő szögben „lőjünk rá" a kódra. (A raszterolvasók holtzónája kb. 10 fokos, a több irányban pásztázóké pedig a gyakorlatban érzékelhetetlen, mivel az egyik pásztázó vonal azonnal kisegíti a másikat.)

Ahogy a CCD-olvasók körében egyes típusok a lézerszkennerek irányába fejlődnek, úgy a lézeres olvasók között is van olyan, amely ránézésre CCD-olvasónak tűnik. Közelebbről szemügyre véve azonnal látható, hogy fényforrásként lézert használ, de ez majdnem fókuszálás nélkül lép ki a szkennerablakon, ennélfogva olvasási tartománya tipikusan a 0–10 cm-es tartományba esik.

A gyártók általában egy ár–teljesítmény grafikonon ábrázolják az egyes típusokat. A kis teljesítményű berendezések a rossz minőségű kódokkal nehezen boldogulnak, általában közeli olvasásra alkalmasak, vevőnként néhány cikkre tervezték őket. Ahogy növekszik a teljesítmény, úgy nő az olvasási tartomány és az olvasás sebessége, javul a rossz minőségű kódok olvasási képessége, és természetesen emelkedik az ár is.

A legjobb minőségű olvasók lézere adaptív logikájú, azaz képes alkalmazkodni a vonalkód rossz tulajdonságaihoz: kiküszöböli a kontrasztproblémákat vagy a vonalak torzulását. A kábelt sokszor rádiófrekvenciás kapcsolat helyettesíti, ekkor az egész napi működést egy nagy kapacitású akkumulátor biztosítja. A csúcsmodellek áruvédelmi rendszerekben való működésre is fel vannak készítve (EAS), tökéletes ergonómiával rendelkeznek, ellenállnak a mechanikai hatásoknak, ütődéseknek, az erős környezeti fénynek, és olvasási távolságuk könnyen meghaladhatja az 1 métert, amit aranybevonatú, elliptikus felületű tükörrendszer garantál. Az olvasó nyelében többfunkciós interfész kap helyet, gyakorlatilag bármilyen eszközhöz illeszthető.

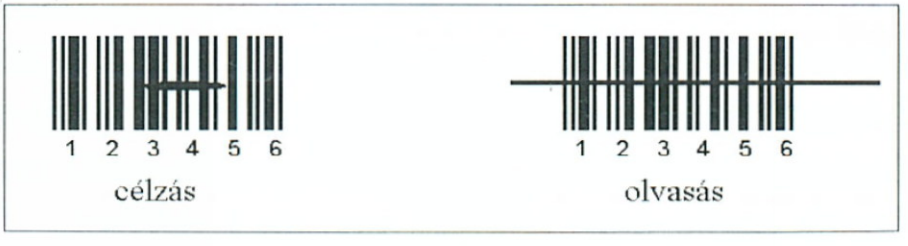
A hagyományos olvasók másik nagy csoportját az ipari alkalmazásokra orientált eszközök alkotják, ahol a fő követelmény a biztonságos és gyors olvasás mellett a mechanikai, valamint a környezeti (nedvesség, por, fény, hő) hatásokkal szembeni ellenálló képesség.

Az ipari kivitelű szkennerek külső burkolata szinte törhetetlen. A bur-

kolóelemeket gumitömítésekkel olyan szorosan illesztik, hogy a nedvesség se hatolhasson be a szkenner belsejébe. Így biztosítható a meglehetősen érzékeny elektromechanikus részegységek védelme. A legkorszerűbb készülékek maradandó károsodás nélkül kibírják az 1,5-2 méter magasról történő leejtést, akár kemény felületre is.

Az ipari olvasókat a legkülönfélébb optikával szerelik. A normál olvasók a kereskedelemben használatosakhoz hasonló tartományban olvasnak, léteznek azonban olyan nagy távolságú eszközök, amelyek olvasási tartománya elérheti a 10 métert. Ügyelni kell arra, hogy ezek az eszközök legtöbbször nem alkalmasak a közeli olvasásra, és a finom felbontású kódokat sem látják, mivel a kibocsátott sugárnyaláb keskeny, és közelre nem fókuszál. Az olvasási tartomány sokszor 1-1,5 méternél kezdődik, és a címke reflexiós tulajdonságaitól függően 5-15 méternél végződik. Természetesen itt is van kivétel, ha elég mélyen nyúlunk a pénztárcánkba, találunk kettős optikával szerelt olvasókat is, amelyek közelről és távolról úgyszintén kitűnően működnek, kis- és nagyméretű kód esetében egyaránt.

Az ipari olvasók optikája azonban nemcsak az olvasás távolságában különbözik. Vannak nagyon kicsiny vonalkódok olvasására kifejlesztett készülékek, amelyek 2-3 mil felbontású kódot olvasnak, viszonylag közeli tartományban, és vannak úgynevezett nagy fényerejű olvasók, amelyek közvetlen napfénynek kitett vagy rossz fényáteresztő felület (sötétített ablaküveg, elektronikus eszközök védőfóliája stb.) alatti kódok leolvasására alkalmasak. Az utóbbiak pásztázási vonalát nem lehet erős napsütésben látni, így a célzás megkönnyítése érdekében a nyomógomb első állásában egy pontba vetíti a lézersugarat. Ugyanígy kétállapotú a nagy távolságú olvasók indítógombja, amelynek kismértékű lenyomása esetén egy keskeny célzó sugarat kapunk, amely a gomb erősebb megnyomása esetén szélesedik ki, és kezd el olvasni a szkenner.



Az ipari olvasók fejlődésének iránya az egyre ütésállóbb kivitel és a környezeti hatásokkal szembeni ellenálló képesség fokozása. Működési hőmérséklettartományuk tipikusan mínusz 20 és plusz 50 Celsius-fok közé esik, de előfordul mínusz 30 és plusz 55 Celsius-fok között működő olvasó is.

Az ipari olvasók egy csoportja különleges, mesterséges intelligencia alapú felismerő áramkört rejt magában. Az úgynevezett Fuzzy Logic eszközök nemcsak fekete-fehér minták alapján próbálják megfejteni a kód tartalmát, hanem az emberi szemhez hasonlóan a szürke árnyalatait is megkülönböztetik. Ezt felhasználva a nem várt nyomtatási hibák ellenére is felismerik a kódot, és kiolvassák az információtartalmat. A hagyományos, igen–nem logikájú olvasók erre nem alkalmasak.

Ipari olvasókat használnak olyan különleges körülmények között, amikor mínusz 25 fokos hidegből hirtelen plusz 30 fokos melegbe kerül az eszköz, illetve fordítva. A különleges hőmérsékletváltozás következménye, hogy az olvasó ablakán lecsapódik a pára, egy időre lehetetlenné téve az olvasást. A megoldást a fűtött belsejű olvasó jelenti, amelyben egy parányi fűtőszál által felmelegített levegő kering, megakadályozva a páralecsapódást.

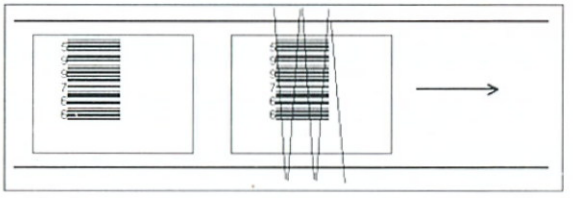
Az ipari és a kereskedelmi olvasók közötti átmenet a gyakorlatban folytonos, léteznek külsőleg ipari kivitelű berendezések, amelyek belső optikáját és felismerő logikáját a kereskedelmi körülményekhez optimalizálták. Sok nagykereskedelmi egység erős mechanikai igénybevételnek teszi ki az olvasókat, ugyanakkor szükség van az olvasási teljesítmény kereskedelmi környezetre történő áthangolására.

Szintén az ipari olvasók közé sorolhatók azok a speciális, ujjnyi méretű olvasók, amelyek felszabadítják a felhasználó mindkét kezét. Az olvasó általában az övre csíptetett adatgyűjtővel van összekötve, kábellel vagy anélkül.

Az ipari olvasók között is található „cordless" kivitelű, azaz vezeték nélküli. A fejlődés új iránya: a sokszor zavaró kábel kiküszöbölése rádiófrekvenciás módszerrel. Ezek a kis teljesítményű, kábel nélküli olvasók egy- vagy kétutas rádiós kapcsolattal a 418 MHz-es vagy a 2,4 GHz-es frekvenciatartományban működnek, hatósugaruk 3–30 méter, kisugárzott teljesítményük pedig nem haladja meg az 1 mW-ot.

A hagyományos olvasók között találunk kifejezetten fix telepítésre készített változatokat. Ezek elsősorban ipari körülmények közé készülnek, házuk különleges bevonatú. A pásztázó lézerfénynek a vonalkódot teljes egészében le kell pásztáznia. Amennyiben a vonalkód az olvasó előtt úgy halad el, hogy a pásztázási irány párhuzamos a haladással, akkor a mozgással azonos irányban történő pásztázás esetén a vonalkód a szkenner számára „megvastagodik", és megnő az olvasási tartomány. Előfordulhat azonban, hogy a kód kilóg a nyaláb nyílásszöge által meghatározott tartományból. A mozgással ellentétes irányban történő pásztázás esetén viszont a kód „soványabb" lesz, és emiatt az olvasási távolságtartomány leszűkül.

Amennyiben a pásztázás merőleges a kód haladási irányára, akkor csak azt kell biztosítani, hogy a lézer legalább kettő-öt alkalommal metssze az előtte elhaladó kódot, a tapasztalat szerint ugyanis minimálisan ennyi szükséges a biztonságos dekódoláshoz. Ez a feltétel a futószalag sebességének és a kód magasságának összehangolásával biztosítható.



Az olvasó kiválasztásánál a fő szempont a pásztázási sebesség és a nyílásszög, amelyet a futószalag mozgási sebességével kell összhangba hozni.

Elterjedőben vannak a miniatürizált, ennélfogva más berendezésbe is könnyen beépíthető, dekóderrel szerelt szkennermodulok, amelyek egy kisméretű mechanikus rezonátorra szerelt lézerdiódából és egy egykártyás, felületszerelt dekóderből állnak. Mint az ipari olvasók általában, ezek is normál lézerkimenettel, illetve RS232 interfésszel rendelkeznek.

A normál lézerolvasók tápfeszültségigénye tipikusan a 4,5–14 V-os tartományba esik, áramfelvételük interfésztől, RF- és lézerteljesítménytől függően 180 és 300 mA között mozog. Itt említjük meg, hogy létezik egy, a berendezések meghibásodásának várható átlagos idejét előrejelző paraméter (MTBF), amelynek szokásos értéke néhány ezer vagy tízezer óra. Értékét ritkán tüntetik fel az adatlapokon, ha mégis, az támpontot adhat a kellő számú tartalékeszköz meghatározásában.

A megfelelő berendezés kiválasztásánál az alábbi szempontokat érdemes figyelembe venni:

- alkalmazási környezet és használat módja (ipar, kereskedelem, kézi, fix, ergonómia),
- mekkora a leolvasandó kódok modulmérete és szélessége,
- mekkora az olvasási távolság,
- milyen minőségű kódok olvasására kell felkészülni,
- mekkora olvasási teljesítményre van szükség,
- épületen kívül és/vagy belül akarjuk-e használni,
- a kábeles vagy a kábel nélküli olvasás az előnyös,
- milyen rendszerbe kell az olvasót illeszteni (interfész),
- a környezeti hatásokkal szembeni követelmények (hőmérséklet, ütésállóság, pára),
- megbízhatóság (MTBF),
- áramfelvétel,
- akkumulátorkapacitás,
- ár.

Raszteres lézerolvasók

Az olvasók egy különleges csoportját alkotják az elsősorban kétdimenziós kódok olvasására kifejlesztett raszteres lézerolvasók. Az úgynevezett halmozott 2D-kódokat (PDF417, RSS, Kód49) lehet ezekkel könnyen leolvasni. Alapelvük hasonló, csak a korábbi pásztázási sebesség egy nagyságrenddel nagyobb (500/mp), és a lézersugarat merőleges irányban is rezgetik 25-50-szer másodpercenként. Egy kétdimenziós kód felülete így egy gombnyomással végigpásztázható.

Létezik kézi és fix telepítésű változat, valamint hordozható eszközbe szerelhető modul. A fix olvasók legtöbbször beépített fotocellát tartal-

maznak. Az intelligensebbek rasztere a kód méretétől függően nyílik, így a felhasználónak nem kell mozgatnia az eszközt.

A hagyományos és a raszteres olvasók között foglal helyet az úgynevezett kézi raszteres szkenner, amely tulajdonképpen egy nagy sebességgel, de csak 1 dimenzióban pásztázó olvasót takar. Ez a költségtakarékos megoldás azok számára előnyös, akik általában egydimenziós kódot olvasnak, ám alkalmanként szükség lehet kétdimenziós kód felismerésére is. A 2D-kódot az eszköz kézi mozgatásával lehet leolvasni. Létezik lézeres és CCD alapú változat.

Több irányból pásztázó (omnidirekcionális) olvasók

A kereskedelmi alkalmazások olvasási teljesítményének és megbízhatóságának igénye folyamatosan növekszik. Ráadásul a kétdimenziós és az összetett kódok is kezdenek elterjedni a gyakorlatban, ezért a gyártók olyan lézerolvasók kifejlesztésébe kezdtek, ahol a lézerdióda fényét egy gyorsan forgó tükörrendszerre vetítik. A különféle tükörelrendezésekkel más és más geometria alakítható ki. Ezzel a módszerrel a vonalkód pásztázása nagy sebességgel történik, másodpercenként akár több ezerszer, ugyanakkor a leolvasást végző vonalak a sík tetszőleges irányában állhatnak.

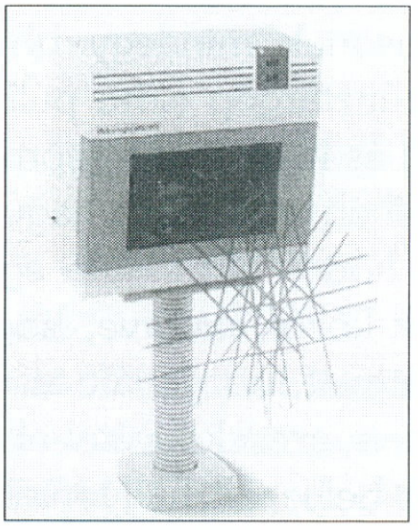
Rendkívül nagy előnyük az iránytól független olvasás, a kódot csak „meg kell mutatni" az olvasónak, mindegy, hogy milyen irányban tartjuk. Klasszikus alkalmazás a pénztárgép előtti pultba épített olvasó, ma már azonban létezik kisméretű és különleges geometriával rendelkező eszköz is – kézi vagy asztali kivitelben –, amely a hagyományos kódok mellett az összetett és kétdimenziós kódok olvasására egyaránt fel van készítve.

A fix telepítésű olvasók közös ismérve, hogy magát a vonalkódot, illetve az azt tartalmazó tárgyat mozgatják az olvasó előtt. A kereskedelemben használt ilyen berendezések kivétel nélkül több irányból pásztáznak – kivéve az állványra helyezett hagyományos olvasókat, amelyeket korábban tárgyaltunk. Mivel ezek az eszközök a kódot több részletben, különböző irányú vonalakkal pásztázzák, és a kód egyes részeit összeillesztik, a sikeres olvasásnak nem feltétele, hogy az olvasó a vonal teljes egészében metssze a kódot.

A kereskedelemben használt pultszkennerrel szemben általános elvárás a nagy átbocsátóképesség, az egyértelmű és a vonalkódtól független,

agresszív olvasás folyamatos üzemben. A többirányú pásztázás igénye abból fakad, hogy a gyors kiszolgálás érdekében a pénztárosnak nincs ideje az egyes termékeken elhelyezkedő kódok irányba történő forgatására. Ez meglehetősen kényelmetlen is lehet nagyméretű tárgyak esetén. (Itt utalunk a kereskedelemben használt egységes UPC/EAN kódok magasságára vonatkozó szabvány előírásaira, ugyanis korábban csak így volt biztosítható az irányfüggetlen olvasás egyenes vonalakkal pásztázó szkennerek esetében. A sugárnak legalább a kód egyik felét „be kellett fognia", s később a jobb és bal oldali részt össze kellett illesztenie. Ez ma már nem követelmény, mert a mai olvasók sok pici részből is képesek összeilleszteni egy nagyobb méretű kódot.)

A pultolvasók felépítésére jellemző, hogy általában 15–20 vonallal tapogatják le az olvasó fölötti vagy előtti térrészt. A vonalak legalább három, sokszor négy-öt különböző irányban pásztáznak. A kialakult fényrács felépítése az árucikkek feltételezett mozgási irányában optimalizált, így nem szimmetrikus a tér minden irányában. Sőt egy-egy készülékcsalád csak egy irányban történő rögzítésre és az ennek megfelelő olvasásra lett kialakítva. A szupermarketekben nagy számban látható pultszkennert mutat a következő ábra.



A szkenner síkjától mért olvasási távolság jellemzően 0 és 25 cm között változik (a legtöbb berendezés esetében ez a programban állítható). Érdemes megvizsgálni a pásztázott terület méretét és alakját az olvasási távolság függvényében. Előfordulhatnak ugyanis holtzónák, amikor az olvasási képesség egy kisebb térrészben leromlik.

Ezekről az olvasókról elmondható, hogy kódfelismerő programjukat az UPC/EAN kódokra optimalizálták. A legújabb fejlesztések eredményeként olyan kifinomult programokkal ellátott olvasók kerültek a piacra, amelyek képesek a kód egészen kicsiny darabjaiból is rekonstruálni az eredetit, vagy képesek a nagyon rossz minőségű kód adattartalmának megfejtésére is. Mivel ez a technikai megoldás a dekódolási sebesség csökkenésével jár együtt, a felhasználó az üzletben megjelenő vonalkódok minőségének függvényében kénytelen beállítani olvasóját.

Az olvasót általában kímélni kell a mechanikai behatásoktól, noha az annak felületére ejtett tárgyak tömegére és az ejtés magasságára a gyártók teszteredményeket szoktak közreadni. Az olvasók külső felületén végighúzott kemény tárgyak összekarcolják a közönséges üveget, ami zavaró reflexiót okozhat, és nagymértékben rontja az olvasási teljesítményt. Ezt úgy lehet kiküszöbölni, hogy keményített, különféle anyagokkal megerősített üveget alkalmazunk, mely bevonatok közül a legkeményebb, gyakorlatilag karcolhatatlan megoldás a zafír.

Mivel az olvasók egyik legkényesebb része a lézerdióda, ezért ennek élettartamát az eszközök tervezői úgy igyekeznek meghosszabbítani, hogy a vonalkódolvasás adott ideig történő szüneteltetése után a berendezés automatikusan valamilyen kímélő üzemmódba kapcsol (pulzáló üzemmód, kisebb fényteljesítmény). Az olvasó automatikusan érzékeli, ha egy tárgyat mozgatunk előtte, s a másodperc tört része alatt visszaáll normál üzemmódba. Az élettartamot csökkentő veszélyforrás a túlságosan magas hőmérséklet, így a gyártók igyekeznek minimalizálni a szkennerek teljesítményfelvételét, és gondoskodnak a különleges hőelvezetésről.

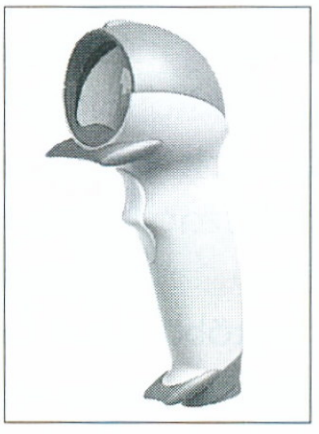
Az olvasók egy részét úgy alakították ki, hogy csak egy irányban legyen rögzíthető, míg más olvasók vízszintesen vagy akár az oldalukra fordítva is működtethetők. Sokszor felmerülő igény a pultszkenner és a kézi olvasó egyidejű használata, ami a nagyméretű vagy súlyos tárgyak leolvasását könnyíti meg. A legtöbb típus beépített kézi olvasó és mágneskártya bemenetével is rendelkezik.

Vannak mérleggel egybeépített olvasók, és léteznek olyan, árellenőrzésre kialakított eszközök, amelyek az árucikkek adatbázisához történő hozzáféréssel azonnal megmutatják kijelzőjükön a kért árucikk aktuális árát. A központi számítógéppel felépített kapcsolat lehet kábeles vagy rádiófrekvenciás.

Pultszkenner kiválasztásakor az alábbi szempontokat érdemes megfontolni:

- az olvasó mérete, pultba építhetősége,
- a lézerdióda és a mechanikusan forgó tükörrendszer élettartama,
- a dekóder és az interfész tulajdonságai,
- melyik kódtípusra optimalizált, és milyen hibajavító képességgel rendelkezik,
- a csatlakoztatható berendezések lehetősége,
- karcolásmentes ablakok,
- nedvesség- és porállóság,
- teljesítményfelvétel (nem csupán a villanyszámla miatt),
- pásztázási sebesség,
- szervizelhetőség,
- ár.

Az omnidirekcionális olvasók között egyre nagyobb számban találunk kisméretű kézi vagy asztali szkennereket. A pásztázási geometria különféle lehet, egy szkenner esetén is változtatható. A kézi változat átbocsátóképessége és olvasási teljesítménye a pultszkennerével egyenértékű, sőt egyes felhasználók szerint felül is múlja azokét. A következő ábrán látható olvasó beprogramozható olyan üzemmódra, amikor gombnyomásra csak egy vonalban pásztáz. Ez nagy segítség lehet széles és alacsony kódok esetében.



A felhasználóknak néhány évvel ezelőtt még be kellett érniük egy-két típussal. Manapság már a legtöbb gyártó kínál ilyen olvasót, van olyan is, amelyik több különböző típust. A választás nem könnyű ebben az

esetben sem, a legfontosabb szempontok az alábbiak lehetnek: Kézi vagy fix telepítésű olvasóra van szükség? Esetleg felváltva mindkét üzemmódra? Mekkora a hely az olvasó számára, és mekkora teljesítményt várunk el tőle (hány olvasásra számítunk percenként, milyen minőségűek a kódok)? Elegendő a hagyományos kódolvasásra felkészülni, vagy kétdimenziót is olvasnunk kell? Milyen az illesztési lehetőség? Milyen a szervizelhetőség, és mennyibe kerül?

Míg a pultszkennerek kifejezetten a pénztárgép melletti EAN/UPC kódok olvasására optimalizáltak, addig a többi olvasó általánosabb felhasználásra készült. Természetesen ezeknek is van áruvédelmi rendszerekre felkészített változata, de kódfelismerő képességük általánosabb, és nem teszik lehetővé külső perifériák csatlakoztatását, önálló működésre lettek felkészítve. Az alábbi ábrán látható készülék például a hagyományosak mellett a kétdimenziós és az összetett kódokat is olvassa.

Az ipari olvasók körében más teljesítményű és felépítésű berendezéseket találunk. Ezek tipikusan valamilyen futószalag mellé vagy fölé kerülnek, és a feladat a sokszor nagy sebességgel mozgó vonalkód leolvasása.

Ezekben a rendszerekben legtöbbször automatikusan és nagy biztonsággal kell leolvasni az olvasó előtt elhaladó kódot változó, a megszokottnál jóval nagyobb távolságból. Ráadásul még a leolvasandó kódok iránya is véletlenszerű. Az olvasók közös jellemzője, hogy nagy sebességű, omnidirekcionális (többirányú) vonalak sokaságával pásztáznak nagyméretű felületeket. Olvasási távolságtartományuk 1-től 2 méterig terjedhet. Ezek a professzionális, nagy teljesítményű olvasók több vonallal s meglehetősen nagy sebességgel pásztázzák az adott felületet,

s kifinomult felismerő algoritmusuk azt is lehetővé teszi, hogy a részletekben leolvasott kódot „fejben" később összeállítsák a másodperc töredéke alatt. Kimenetként jellemző az RS232-, RS422-, illetve RS485-csatlakozás.

A gyakorlatban előfordul az is, hogy előre meghatározott helyen, de egymás fölött elhelyezkedő vonalkódokat kell leolvasni egyidejűleg, és az adatokat ráadásul meghatározott sorrendben kell a háttérrendszer felé továbbítani. Erre a megoldás az, hogy a felismerő logikának kell megkülönböztetnie – a pásztázási sebesség megtartása mellett – a különböző időpontokban felismert és leolvasott kódokat. Mivel a dekódolt vonalkódok sorrendje az olvasások során véletlenszerűen változik, ezért arról is gondoskodni kell, hogy a háttérrendszer felé az adatok – vagy a sikertelen olvasások – a megfelelő sorrendben kerüljenek továbbításra.

A holografikus olvasókban ezt a technikát fejlesztették tovább, mégpedig úgy, hogy a fókuszált pásztázó vonalak az olvasó síkjától számítva 4-6-szor ismétlődnek különböző távolságokban, így az olvasás a harmadik, függőeges dimenzióban is jóval messzebbre kiterjed a megszokottnál, és növekszik a felbontás. Ezek az olvasók 0 és 250 cm között a nagy sebességgel és véletlenszerű távolságban elhaladó piciny, egy- és kétdimenziós kódokat is egyaránt nagy biztonsággal olvassák.

Az ilyen ipari olvasók általában 2-es osztályú berendezések. Legtöbbször nem folyamatosan pásztáznak, így a leolvasandó kód közeledését és az olvasás megkezdését valamilyen módon közölni kell az olvasóval, noha az igazán nagy sebességű rendszerekben ez a funkció nem megengedett. A távoli vezérlés történhet fotocellával vagy a háttérrendszer felől pl. soros vonalon érkező, programból vezérelt parancssorral.

Képrögzítő kamera

A képrögzítő kamera egy olyan digitális fényképezőgéphez hasonlít, amely egy teljes ábrát vagy képet rögzít a memóriájában, s a benne lévő egy- vagy kétdimenziós vonalkódot ennek alapján felismeri és dekódolja (digitális fénykép). A jelenlegi képrögzítési technológia CCD vagy CMOS technológiát alkalmazó 2D-s szenzorsorok köré épül, hasonlóan a videokamerákhoz. Az olvasógyártók olyan szenzorokat alkalmaznak, amelyek elrendezése akár 760x580 képpont (pixel) is lehet. Nagyobb méretű CCD-szenzorokat is kifejlesztettek már, de ezek előreláthatólag túl drágák lesznek az olyan rendszerekben, mint a kézi vonalkódolvasók.

A 2D-kód olvasásához a kamera egy vagy több pillanatfelvételt készít a kódról, amelynek pontosan az eszköz látómezejébe kell illeszkednie. Az így készült kép tényleges felbontása a CCD pixelszámától, a vonalkód sűrűségétől, valamint a rögzítendő felület és a rögzítő közötti távolságtól függ. Ahogy az olvasó távolodik a kódtól, annak elemei a CCD-szenzorok egy kisebb területére kerülnek, és ennek eredményeként a pillanatnyi felbontás – vagyis a képfelismerési képesség – csökken.

Gyakorlatilag tehát egy kézi készülékkel általában nem lehetséges mind a 760 vízszintes képpontot felhasználni 2D-szimbólumok vagy nagyméretű, széles 1D-kódok olvasásához. A kód mindkét oldalán lennie kell egy bizonyos margónak, amely biztosítja, hogy a vonalkód a rögzítő látóterén belül legyen. A pontatlan kezelői „célzás" következtében e „biztonsági sáv" nélkül a jel bizonyos százaléka majdnem biztosan kiesik az eszköz látóteréből. A gyakorlatban ez a sáv kb. 20%-kal csökkenti a hasznos képpontok számát.

A képfeldolgozó és dekódoló program a vonalkód legkisebb elemeinek azonosításához legalább 2 pixelt igényel. Ez korlátozza a 2D-szimbólumot alkotó elemek darabszámát, így ezen keresztül a vonalkód maximális méretét és információkapacitását. Ráadásul a nagyobb 2D- vagy szélesebb 1D-szimbólumok olvasása nehézkessé válik, mivel az olvasónak egyrészt

a) elég közel kell lennie a kódhoz, hogy megfelelő felbontást kapjunk, ugyanakkor

b) elég távol kell lennie ahhoz, hogy az egész képet befogja.

Nagyméretű 2D-kódok esetén az „elég közel, ugyanakkor elég távol" követelménye igen csekély olvasási távolságtartományt eredményez, ami jelentősen korlátozza a kényelmes használatot.

A 760 vízszintes képpont mint korlát akkor is nyilvánvalóvá válik, amikor a 2D-s „képrögzítő" olvasókat hasonlítjuk össze a hagyományos, lineáris CCD-olvasókkal, amelyek 2048 elemes egysoros tömböt használnak – ez majdnem háromszor nagyobb felbontást jelent.

A MaxiCode, a kisebb méretű PDF417 vagy a Data Matrix esetében, amelyet kisebb felbontással nyomtattak, a 2D-s képrögzítő olvasók viszonylag magas első leolvasási rátát produkálnak, megfelelő olvasási mélységgel. Ahol követelményként jelenik meg a széles lineáris vagy nagyobb méretű PDF417-olvasás, ott az olvasási tartomány (az a távolságtartomány, amelyen belül a jel olvasható) meglehetősen gyorsan csökken. Ez nehezíti az olvasó használatát.

Mindazonáltal fontos megjegyezni, hogy a MaxiCode kis méretének és alacsony írássűrűségének köszönhetően hatékonyan olvasható kézi képrögzítési technológiával. Mivel kevesebb mint 100 karaktert tartalmaz, így egy 25x20 mm méretű kód 35 mil nyomtatási felbontás mellett általában 7–22 cm távolságból jól olvasható.

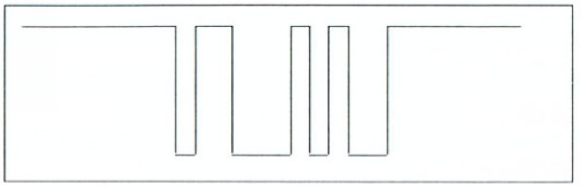
Vonalkód-ellenőrzés

A vonalkódos szabványok nem csupán a kód felépítését írják elő, hanem a nyomtatásnál elkövethető hiba mértékére is útmutatást adnak. Előírják például a vonalak szélességének megengedett maximális eltérését, ami a kódtípusoktól és a modulmérettől függően változik.

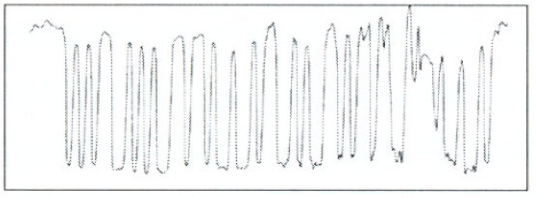
A vonalkódszkennerek működésekor meghatározható egy olyan tűréshatár, amely a biztonságos olvasáshoz szükséges. Amennyiben túllépjük a megengedett értékeket, a kód még felismerhető, ám az első olvasási arány nagymértékben csökken, és megnőhet a helyettesítési hibák előfordulási gyakorisága.

A vonalkód ellenőrzésének kulcsszerepe van a nyomtatási folyamatban. A megoldás az előállított kód analizálása úgynevezett vonalkód-ellenőrző berendezéssel. Számos gyártó kínál eszközt erre a célra; felbontásuk, érzékenységük többszörösen fölülmúlja a normál olvasókét.

Egy vonalkód leolvasása elméletileg úgy történik, hogy a tökéletesen kinyomtatott kódot végigpásztázzuk egy végtelenül kicsiny fényponttal, amely a fehér területeken visszaverődik, a fekete vonalakon pedig teljesen elnyelődik. Egy ilyen ideális olvasó az alábbi kimeneti jelet szolgáltatja:

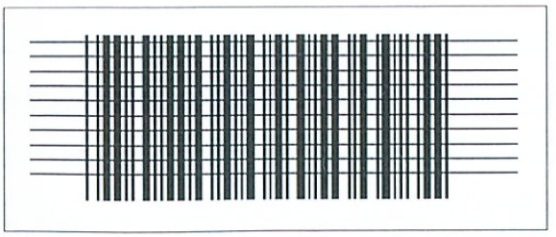


A vonalkód nyomtatása nem tökéletes, felülete pedig előre ki nem számítható módon nyeli el a rávetülő fénysugarat. A megvilágításra használt fényforrás nem pontszerű, és az elektronikus részegységek sem ideálisak. A hordozó felület egyenetlen, és a nyomat, valamint a festékterülés nem tökéletes. A felsorolt okok miatt az olvasók által szolgáltatott jelalak az alábbi formájú lesz:



A vonalkódok olvashatóságára egy ötfokozatú skálát használnak. Ezzel előre lehet jelezni az egyes tartományokba kerülő kódok későbbi olvashatóságát. Vajon miért nem létezik egy matematikai képlet a vonalkód „jóságának" megállapítására, amelybe csak be kell helyettesíteni néhány értéket? Azért, mert az olvashatóságot olyan nehezen számszerűsíthető tényezők befolyásolják, mint a vonalvastagságok megkülönböztethetőségének vagy a nyomtatási egyenetlenségnek az értéke. Ennek ellenére az egyes faktorok többé-kevésbé számszerűsíthetők, és együttes figyelembevételük eredményeként a vizsgált kód besorolható az A, B, C, D és F betűvel azonosított öt osztály valamelyikébe. Az A kategóriába kerülnek a legjobb minősítésű kódok, az F-be a legrosszabbak.

Melyek azok a tényezők, amelyek mindegyikét meg kell vizsgálni ellenőrzéskor? Először is 10 pásztázást kell végrehajtani a kód magasságában, egyenletesen elosztva.



Ezután megvizsgálandó, hogy a kód egy átlagos viszonyítási alapul szolgáló algoritmus segítségével egyáltalán olvasható-e, és megvan-e az előírt minimális különbség a fekete és a fehér vonalak fényvisszaverő tulajdonsága között (kontraszt). A kód rögtön az F kategóriába kerül besorolásra, ha bármelyik feltételnek nem tesz eleget. Ezután kerül sor az alábbi lépésekből álló analízisre:

- a vonalkód kontrasztértékének pontos meghatározása (SC),
- az élkontraszt (mennyire jól kivehető a vonalak határa) kiszámítása (EC),
- a moduláció meghatározása (MOD),
- a nyomtatási hibák mérőszámának meghatározása (ERN),
- a dekódolhatóság mérőszámának meghatározása.

Az analízis valamennyi lépésében a kódot be kell sorolni az A, B, C, D és F kategóriák valamelyikébe. Mivel a kód olvashatóságáért együttesen mind az öt mérési érték felelős, és egyik sem tudja javítani a másik hibáját, ezért a mérőszámok által meghatározott kategóriák közül a leggyengébb minősítésű fogja jellemezni a kódot. A 10 vonalas minta alapján kalkulált kategóriaértékeket átlagolni kell, hiszen ez mutatja valósághűen a későbbi olvasások várható értékeit.

Végül milyen következtetést vonhatunk le abból, ha a mérésen átesett kódot besoroltuk egy adott kategóriába? Ezt mutatja az alábbi táblázat.

A	A legjobb minőségű vonalkódok kerülnek ebbe a csoportba. Ha az olvasó csak egyszer pásztázza le a kódot, akkor az ebbe a csoportba kell kerüljön az ellenőrzés során, hogy az első olvasási arány elfogadható legyen.
B	A csoportba sorolt vonalkódok jó minőségűek, de egyszeres pásztázás esetén előfordulhat, hogy újra kell próbálkozni az olvasással. Azokban a rendszerekben elfogadható a minősége, ahol a ritkán előforduló újraolvasás nem okoz gondot.
C	A csoportba sorolt vonalkódok minősége közepes, s csak olyan alkalmazásokban nyújtanak elfogadható teljesítményt, ahol többszörös pásztázással történik egy-egy olvasás. (pultszkenner, CCD, lézerszkenner)
D	A csoportba sorolt vonalkódok minősége meglehetősen gyenge, és valószínűleg egyes olvasók nem, vagy csak nagyon nehezen fognak megbírkózni az olvasással. A rendszer tervezésekor biztosítani kell alternatív adatbeviteli lehetőséget (pl. manuális bevitel).
E	Az elfogadhatatlan minőségű kódok kerülnek ebbe a csoportba. Olvasásuk nagy valószínűséggel a legtöbb szkenner számára gondot okoz.

Vonalkódos adatgyűjtők

Memóriás olvasók

A memóriás olvasók a kézi olvasókkal állnak a legközelebbi rokonságban. Azért kerülnek külön fejezetben ismertetésre, mert már rendelkeznek az adatgyűjtők alaptulajdonságaival, azaz programozhatók, és képesek az összegyűjtött adatok tárolására, illetve áttöltésére.

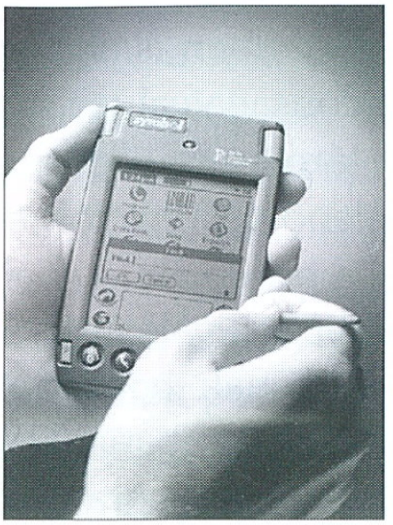
A használat során megjelenő új funkciók és a felhasználási lehetőségek korlátozottsága vezet el a hordozható adatgyűjtőkhöz mint univerzális megoldásokhoz. Az adatgyűjtők valójában hordozható számítógépek, amelyek vonalkódolvasóval vannak egybeépítve, és programozhatók. A memóriás olvasók viszont elsősorban olvasók, amelyek memóriával rendelkeznek, és eltérő mértékben programozhatók.

A vonalkódolvasók közös jellemzője, hogy állandó összeköttetésben állnak az adatfogadásra felkészített háttérrendszerrel – az összeköttetés lehet kábeles vagy rádiófrekvenciás. Az állandó összeköttetés biztosítja, hogy a leolvasott információ azonnal eljusson a vevőoldalra, amely ezután elvégzi a kívánt adatfeldolgozási műveletet (például számlakészítés egy pénztárgéppel). Észrevehetjük, hogy az adatáramlás gyakorlatilag egyirányú, és a gépi olvasáson kívül más funkciója nincs, eltekintve az egyszerűbb adatformázástól, mint amilyen például a sorlezáró karakterek hozzáfűzése. A korábban tárgyalt olvasók alapvetően erre a feladatra készülnek, eltérések az ergonómiában, az olvasás sebességében és távolságában, valamint a méretbeli különbségekben vannak.

Az alkalmazások egy része azonban másként működik, mégpedig éppen a mobilitási igényből fakadóan a háttérrendszerrel való folyamatos kapcsolattartás lehetősége eleve kizárt. Gondoljunk egy nagyméretű raktárhelyiségre, egy disztribúciós vagy egy szállítmányozási folyamatra, amely egymástól nagyobb fizikai távolságra lévő helyeken zajlik. Ilyen típusú feladatok megoldására olyan berendezés szükséges, amelynek legfőbb jellemzője az, hogy önálló tápforrással rendelkezik, képes vonalkódolvasásra és az adatok átmeneti, ugyanakkor biztonságos tárolására.

A háttérrendszerrel történő összeköttetés kialakítása és az összegyűjtött adatok biztonságos áttöltése általában felhasználói utasítás és közre-

működés alapján történik. Az adatgyűjtők rádiófrekvenciás változataitól egyelőre tekintsünk el. A rádiós eszközök a fenti tulajdonságokon felül folyamatos kapcsolattartásra is képesek, részletes ismertetésük külön fejezetben található.



Visszatérve a memóriás olvasókhoz, a legegyszerűbb típusok között a 32–128 kB kapacitással rendelkező, úgynevezett memóriás ceruzákat találjuk. A memóriás lézerszkennerek kapacitása valamivel nagyobb, úgy 128 kB és 1 MB közé tehető. Általában kisméretű kijelzővel, néhány gombos billentyűzettel rendelkeznek. Közös jellemzőjük, hogy belső tápforrásként tölthető akkumulátor szolgál, amely típustól függően 6–12 óra üzemidőszakot garantál. A háttérrendszerrel folyamatos kapcsolatban nem álló adatgyűjtőket off-line vagy batch típusúaknak nevezzük. Az adatgyűjtés folyamata a beolvasott információk egymás utáni tárolásából, majd áttöltéséből áll, ami magában foglalja az adatok szerkesztését és kívánság szerinti törlését is. Az áttöltésnél a soros vonal az elterjedt adatátviteli eljárás, ami elterjedtségének és sebességének köszönhető. A billentyűzeten keresztüli adatbevitel lassú, az átmeneti tároló kapacitása néhányszor tíz vagy száz karakter, és nem teszi lehetővé az adatátviteli folyamat szabályozását (a sérült adatok ismétlését, a puffer telítettségének jelzését), ami nemkívánatos adatvesztéssel járhat.

A memóriás olvasók között egyrészt azok típusában van különbség, másrészt az adatgyűjtési folyamat során nyújtott szolgáltatásokban, így például a memóriatartalom kijelzése, az olvasás időpontjának regisztrálá-

sa, illetve az intelligensebb változatoknál a programozhatóság kérdésében, valamint a billentyűzet és a kijelző méretében.

A berendezések általában lehetőséget adnak a mennyiségi adatoknak a leolvasott kódhoz történő hozzárendelésére. A billentyűs változatoknál ez egyszerűbb feladat, a többi olvasónál erre egy vonalkódos menüt tartalmazó „papírbillentyűzet" szolgál, amely helyettesíti a billentyűzetet. Használata akkor javasolt, ha ilyen manuális adatbevitelre csak ritkán van szükség.

A memóriás olvasók között találunk olyan eszközöket, amelyek alapesetben kábellel vagy rádiófrekvenciás úton csatlakoznak a háttérrendszerhez, azonban ha lecsatoljuk a kábelt, vagy kilépünk a lefedett tartományból, rögtön egy billentyűzettel és kijelzővel ellátott, programozható adatgyűjtőt kapunk. Ez a memóriás szkennerek legfejlettebb típusa, kiválóan használható ott, ahol sűrűn váltogatva olvasóra és adatgyűjtőre egyaránt szükség van.

A megfelelő berendezés kiválasztásánál érdemes figyelembe venni a memórianagyságot, a fizikai méretet és az ergonómiát, a súlyt, a környezeti ellenálló képességet (IP-fokozat). Fontos szempont az akkumulátorok kapacitása, a töltési sebesség és a programozhatóság, valamint a háttérrendszerhez történő illesztés és integrálás lehetősége.

Vonalkódos adatgyűjtők

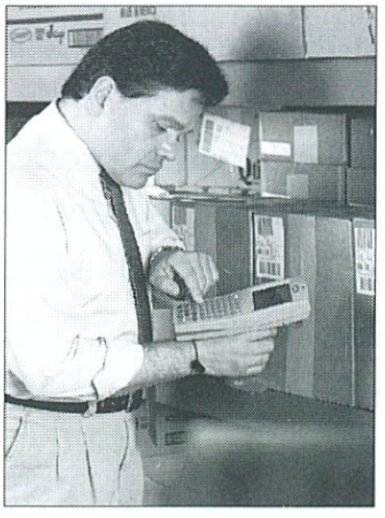
A vonalkódos adatgyűjtők meglehetősen összetett felépítésű és funkcionalitású eszközök. Gyakorlatilag magukban foglalják mindazt, ami egy vonalkódos mobil alkalmazásban szóba jöhet: olvasót, hordozható számítógépet, néha nyomtatót, rádiófrekvenciás és infravörös kommunikációt.

Az adatgyűjtőket nem lehet elválasztani a mögöttük álló számítógépes rendszertől, hiszen a feladat legtöbbször a már létező és jól bevált, de helyhez kötött feladat mobil eszközön történő elvégzése.

A mobilszámítógépek, vonalkódolvasók és rádiós egységek integrálása olyan berendezések piacra kerülését eredményezte, amelyek egy kisméretű, hordozható eszközben egyesítik mind az olvasók, mind a mikroszámítógépek, mind a rádiófrekvenciás kommunikáció legújabb eredményeit.

A mobil adatgyűjtők vizsgálatakor mindig szembe találjuk magunkat egy paradoxonnal. Arról van szó, hogy a mobil eszközzel szembeni elvárásokat – nagy számítási teljesítmény és memória, nagy teljesítményű akkumulátor, ugyanakkor kis méret és súly, GSM- és LAN-interfész, egy- és kétdimenziós lézerolvasó, robusztus felépítés, széles hőmérséklettartomány, nagy kijelző, könnyen kezelhető billentyűzet, nedvesség- és porállóság, nagy teljesítményű operációs rendszer, könnyű programozhatóság, valamint alacsony ár, hogy csak a legfontosabbakat említsük – egyszerre nem lehet teljesíteni. Amint egyes jellemzőkön javítunk, mások minősége csökkenni fog. Az egyes típusok abban különböznek egymástól, hogy a tulajdonságok mely csoportjára vannak optimalizálva. Például kis teljesítmény és memória, robusztus kivitel, rádió nélkül, kis kijelzővel, alacsony áron.

Az adatgyűjtők egyrészt feloldják a memóriás olvasók merev programozhatóságának korlátjait, másrészt lehetővé teszik, hogy a háttérrendszer adatfeldolgozó, tároló és megjelenítő képességét mobilizálva magunkkal vigyük a szükséges feladatrészeket az adatgyűjtés helyére.



A vonalkódos adatgyűjtők legtöbbször beépítve tartalmazzák a lézeres, illetve a CCD-vonalkódolvasót. A piacon kapható berendezéseknek temérdek típusa és változata létezik, még egy-egy gyártó termékskáláján belül is. Csoportosításukat elvégezhetjük az adatgyűjtők belső architektúrája, számítási teljesítménye, perifériacsatlakoztatási lehetőségei, programozhatósága és fizikai paraméterei alapján.

Klasszikus adatgyűjtők

A 8 bites architektúrájú eszközök ma már nagyon ritkák, felhasználási területük az egyszerű és árérzékeny adatgyűjtési feladatok elvégzése. Kivitelük egyszerű, kisméretű billentyűzettel, néhány soros kijelzővel vannak ellátva, és külső olvasó vagy integrált lézerszkenner csatlakoztatására alkalmasak. Az adatátvitel modemen vagy soros vonalon keresztül történik.

A nagyobb darabszámban elterjedt, klasszikus vonalkódos adatgyűjtők 16 vagy 32 bites architektúrájúak. Memóriaméretük tipikusan 512 kB és néhány MB közé tehető. A berendezések operációs rendszere gyárilag kerül beégetésre, a 16 bites eszközök legtöbbször egyedi operációs rendszert futtatnak, vagy a DOS egyes változatait. A PC-re kifejlesztett programok többsége változtatás nélkül nem futtatható ezeken az eszközökön, mivel a DOS-nál alacsonyabb szintű hívások eszközönként mások.

A 32 bites eszközök többsége már csaknem teljesen PC-kompatibilis, általában az MS-DOS teljes változata kerül gyárilag beégetésre. Ezeken A PC-s programok minimális változtatással futtathatók. Amit az adaptáláskor figyelembe kell venni, az a különleges kijelző és videomemória, az egyedi billentyűzet és az egyedi perifériák, mint például az integrált lézerolvasó. A gyártók az eszköz mellé adják azokat a kiegészítő programokat, amelyek annak specifikus fejlesztéséhez szükségesek.

A programok általában nem felejtő Flash memóriába kerülnek. A futtatásukra és az adattárolásra használt memóriaterület (RAM) mérete a néhány száz kB-tól a néhány vagy néhányszor tíz MB-ig terjed.

A klasszikus adatgyűjtők karakterorientált működésűek, LCD-kijelzőjük mérete 2–16 soros, soronként körülbelül 16-20 karakterrel. A ki-

jelzők legtöbbször grafikus üzemmódban is használhatók, kisebb méretű ábrák megjelenítésére. A billentyűzet általában eszközspecifikus, mérettől függően néhány vagy akár ötven-hatvan gombos is lehet, egy részüknél megfelelő kombinációkkal a teljes, 101 gombos klaviatúra emulálható.

Tipikus integrált periféria a CCD-szkenner, a lézerolvasó, az optikai RS232 interfész (a gyakori adatáttöltés igénybe veszi a mechanikus csatlakozókat), a beépített belső modem, az esetleges második soros vonal. Nem ritka, hogy az eszközök szabad PCMCIA-kártyahellyel rendelkeznek, elsősorban memóriabővítési feladatokra. Az olvasófej (ceruza, CCD, lézerolvasó) egy belső dekóderegységre csatlakozik, amelynek dekódoló, azaz vonalkód-felismerő képességét az operációs rendszerbe illeszkedő meghajtóprogram biztosítja. A beolvasott adat logikailag a billentyűzeten bevitt információval egyenértékű.

A berendezések további csoportosítása aszerint történhet, hogy azokat kereskedelmi vagy inkább nagyobb igénybevételű, ipari környezetre tervezték-e. Ezek a tulajdonságok a termék adatlapján ellenőrizhetők, legtöbbször annak színe is utal a különleges kivitelre. Az ipari felhasználásra szánt eszközöket szélsőséges mechanikai és hőmérsékleti igénybevételre tervezik, tipikusan 1,5-2 méterről leejthetők kemény felületre, a működési hőmérséklettartomány pedig –25-30 és +50-60 Celsius-fok közöttire tehető. Az IP-osztályba sorolás a porral és nedvességgel szembeni ellenállást mutatja. Egyes eszközök (IP66) folyamatosan működtethetők, miközben erős vízsugárral mossák a felületüket. Az adatgyűjtők egy különleges csoportját képezik a robbanásveszélyes környezetre tervezett eszközök.

Érintőképernyős terminálok

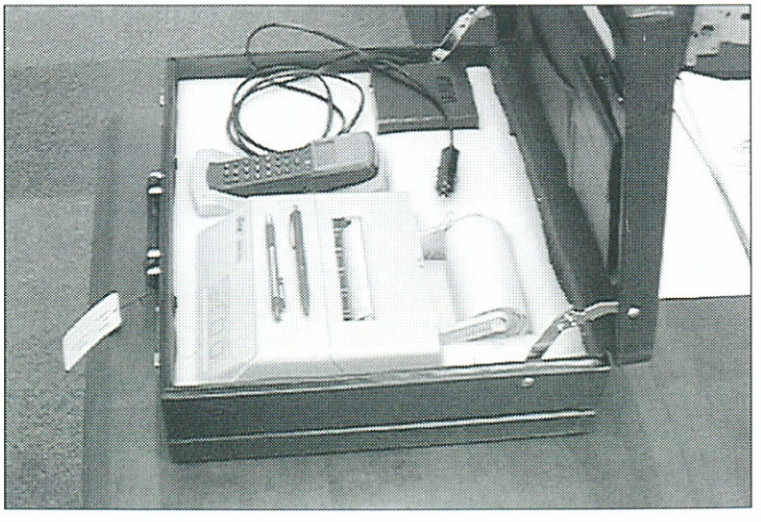
Az adatgyűjtők új generációját jelentik a nagyméretű érintőképernyővel szerelt, legtöbbször billentyűzet nélküli terminálok. A felhasználó az operációs rendszer által biztosított grafikus felületen keresztül dolgozik az eszközzel. Az asztali gépeknél szokásos egér helyett piciny műanyag pálcikával lehet a menüpontok között választani vagy a képernyőre „írni". A legtöbb eszközben alakfelismerő és nyelvi programok segítik a kézzel írt információ gépi formára történő alakítását és tárolását.

Természetesen az érintőképernyős eszközökben is van beépített szkenner, infravörös és RS232 kommunikációs port, illetve rádiófrekvenciás vagy GSM-es bővítési lehetőség.

Általánosan elmondható, hogy az érintőképernyők mérete az 1 és a teljes VGA (640x480) közé esik, alapértelmezésben fekete-fehér kijelzővel, míg a színes képernyő felárért rendelhető. A tipikus memóriaméret operációs rendszertől függően néhány MB-tól néhányszor 10 MB-ig terjed. A központi egység 16 vagy 32 bites, és legtöbbször egy lapkára integráltan tartalmazza a fontosabb elemeket. Az operációs rendszerek közül a kis erőforrás-igényű, stabil és gyors Palm OS, valamint a nagy teljesítményű, de erőforrás-igényesebb Windows CE a legelterjedtebb.

A fejlődés az egyre több funkciót megtestesítő eszközök felé halad, melyek a színes képernyő mellett egyszerre tartalmazhatnak 2D-s olvasót, lokális RF-interfészt, GSM- vagy GPRS-kártyát. Egy ilyen eszközzel az interneten történő böngészés és a lokális, nagy sebességű fájltranszfer mellett egyidejűleg még akár telefonálni is lehet.

A különleges felépítésű eszközök között léteznek hordozható nyomtatóval vagy kameraolvasóval egybeépített terminálok egészen speciális alkalmazásokra.



A kisméretű, hordozható adatgyűjtőkbe jelenleg nem építenek 486-osnál gyorsabb processzorokat, mivel a mobil alkalmazások számítási és adatfeldolgozási igényét ezek az eszközök bőven kielégítik, az operációs rendszer választásának teljes szabadságával. Nem szabad elfelejtenünk, hogy ezeket a berendezéseket nem arra tervezték, mint az asztali, illetve a hordozható gépeket, ennélfogva használati értékük meghatározásánál a sebességparaméterek kisebb súllyal szerepelnek, és inkább az összetett funkcionalitás, a kis méret és súly, valamint az ütésálló kivitel kerül előtérbe.

Külön fejezet foglalkozik a rádiófrekvenciás adatgyűjtőkkel, amelyek a hordozhatóság mellett biztosítják a folyamatos kapcsolatot a háttérrendszerrel. A felhasználó egy mobil, a háttérrendszer meghosszabbításaként felfogható eszközhöz jut. A jelenleg használt szórt spektrumú frekvenciatartomány 2,4-2,5 GHz, amely modulációtól függően 2 és 11 Mbps közötti sebességet biztosít. Kidolgozás alatt vannak már az új, 5,4 GHz-es tartományban működő eszközök, amelyek néhányszor 10 Mbps adatátviteli sebességet fognak produkálni.

A nagyobb frekvencia és a kisebb adóteljesítmény miatt a berendezések hatótávolsága csökken, ám egyúttal megnő a rendelkezésre álló sávszélesség, azaz a hordozható eszközön nemsokára lehetővé válik valós idejű videó átvitele.

Kártyás azonosítás

Mágneskártyás rendszerek

Az automatizált azonosítás iránti igény a gépek megjelenése óta megvan az emberekben. Joggal merült fel hát az is, hogy ne csak a fizikai erőkifejtéssel járó munkát gépesítsék, hanem a hozzá kapcsolódó tájékoztatási, adatgyűjtési, információfeldolgozási tevékenységeket is. Ez ugyanis olyan lehetőségeket biztosít a vezetés számára, hogy időben avatkozhasson be bármilyen folyamatba, illetve a humán faktort mint bizonytalansági tényezőt semlegesítse, megvalósítva az ember nélküli folyamatok lehetőségét, amelyek iránt az igényt először – népszerű formában – Jules Verne fogalmazta meg.

A második világháború után a mágneses jelrögzítés nagy fejlődésnek indult. A sikeres és tömegszerűvé tett hangrögzítők működésének mintájára a műszakiak – bár térben és időben elkülönülve – hozzáláttak az emberi környezetből származó információk mágneses úton való rögzítésének fejlesztéséhez. A témán belül a továbbiakban az adatok rögzítésével foglalkozunk.

Adatok rögzítése és olvasása

Az első kérdés az, hogy miképpen rögzítsük a keletkező adatokat, amelyek számok, betűk formájában jelentkeznek. Az addigi gyakorlatban (1950-et írunk) komplex információt, pl. hangot, zenét rögzítettek, mégpedig egy mikrofon segítségével, amely az akusztikus jelet elektromos információvá alakította át. Az így nyert folyamatos jelet rögzítették a mágnesszalagon (hangszalagon). Esetünkben azonban önálló, diszkrét jelek állnak rendelkezésre, amelyekben valamennyi szokásos írásjel szerepel; ezeket alacsony és magas jelek (nevezzük az alacsonyt 0, a magasat 1 értékűnek), azaz 0-k és 1-esek kombinációjaként írták le.

Az írásjelek megjelenítése önálló, diszkrét jelszintekkel, azaz 0-kkal és 1-esekkel, lehetővé tette, hogy egymás után alacsony és magas jelszinteket rögzítsünk a mágneses szalagon. Az ilyen adatokkal ellátott mágnescsík olvasása során az egymást követő alacsony és magas jelszinteket 0-ként és 1-ként értékelve s az így kialakuló számsort a következő táblázat (1. ábra) alapján dekódolva megkapjuk az eredeti, emberi szem által olvasható adatokat.

Adatbitek			Paritás		Karakter	Funkció
b1	b2	b3	b4	b5		
1	1	0	1	0	;	Startjel
0	0	0	0	1	0	Adat
1	0	0	0	0	1	Adat
0	1	0	0	0	2	Adat
1	1	0	0	1	3	Adat
0	0	1	0	0	4	Adat
1	0	1	0	1	5	Adat
0	1	1	0	1	6	Adat
1	1	1	0	0	7	Adat
0	0	0	1	0	8	Adat
1	0	0	1	1	9	Adat
1	0	1	1	0	=	Mezőelv.
0	1	0	1	1	>	Vezérlő jel
0	0	1	1	1	<	Vezérlő jel
0	1	1	1	0	>	Vezérlő jel
1	1	1	1	1	?	Stopjel

A 16 karakteres, 5 bites jelkészlet
10 numerikus adatkarakter
3 szerkesztő/mezőkarakter
3 vezérlő karakter

1. ábra. ANSI/ISO BCD Data Format

A fejlődés során a nemzetközi szabványosító szervezet, az ISO két kódoló/dekódoló formátumot alakított ki, szabványosított:

- az NASI/ISO BCD Data Formatot, amely számokat és néhány vezérlő jelet tartalmaz (1. ábra), valamint
- az ANSI/ISO ALPHA Data Formatot, amely összesen 64 karaktert, köztük 43 betűt és számot foglal magában (2. ábra).

Anélkül, hogy a mágneses jelrögzítés eljárását ismertetnénk, megállapíthatjuk, hogy lehetővé vált az 50-es évek technikai felszereltségével adatokat rögzíteni, majd olvasni mágnesszalag, mágnescsík segítségével.

A feliratozott, adatokkal ellátott mágnescsík olvasása során részben ugyanazokkal a problémákkal kell szembenézni, mint az írás során, részben pedig új gondokkal kell megküzdeni.

A fejlesztők elképzelése a mágnescsík használatáról az volt, hogy adott központi helyen történik az adatok mágnescsíkokra való felírása, majd azokat különböző helyeken olvassák le. Ennek megfelelően az író eszköz nagy pontosságú, költséges és bonyolult lehet, míg az olvasók olcsók és egyszerűek.

Adatbitek						Paritás	Karakter	Funkció
b1	b2	b3	b4	b5	b6	b7		
1	0	1	0	0	0	1	0%	Startjel
1	0	0	0	0	1	1	A	Adat
0	1	0	0	0	1	1	B	Adat
1	1	0	0	0	1	0	C	Adat
-	-	-	-	-	-	-	-	D-Z Adat
0	0	0	0	1	0	0	0	Adat
1	0	0	0	1	0	1	1	Adat
0	1	0	0	1	0	1	2	Adat
-	-	-	-	-	-	-	3-9	Adat
0	1	1	1	1	1	0	^	Mezőelv.
1	1	1	1	1	0	0	?	Stopjel

A 64 karakteres, 7 bites jelkészlet
43 numerikus adatkarakter
3 szerkesztő/mezőkarakter
18 vezérlő/speciális karakter

2. ábra. ANSI/ISO ALPHA Data Format

Ez az elképzelés részben abból a felismerésből fakadhatott, hogy a feliratozásnál minél kevesebb elektromos pontatlanságnak és hibának szabad a mágnesszalagon lévő adatokba kerülnie, az olvasás viszont egyszerűbb folyamat, amely egyszerűsített feltételek mellett, néhány paramétert betartva történhet meg. A fentiek a következő főbb fizikai-műszaki problémákban öltenek testet:

- a mágnescsíkon lévő elektromos jel nagysága,
- a jelnagyság folyamatossága,
- kódolási hiba,
- a mágnescsík haladási sebessége, gyorsulása,
- a továbbítás során fellépő erő és tehetetlenségi nyomaték,
- jelszinkronizációs, kódolási, gyorsulási, illetve fázishiba stb.

Ezen – és más egyéb – problémák leküzdésén évtizedeken át fáradoztak, míg megszülettek a manapság használatos eszközök.

Amikor a mágnescsík feliratozását és olvasását többé-kevésbé már kézben tartották a műszakiak, jött a következő megoldandó kérdés: annak elhelyezése, használata, kezelése.

A hangrögzítésre használt mágnesszalag esetében senki sem kérdőjelezi meg a szalag kezelésének módját, azaz hogy azt feltekercselik. Az adatrögzítés tekintetében azonban sok esetben egyáltalán nincs szükség ilyen mennyiségű, hosszúságú mágnescsíkra. Kézenfekvő volt, hogy

a mágnesszalagot kisebb darabokra kell vágni, és úgy felhasználni. Ezek a kisebb szalagdarabok, mágnescsíkok felragaszthatók különböző hordozókra, például papír-, karton- vagy műanyag lapokra. Ez a felismerés azonban új korlátokat is jelentett, nevezetesen, hogy a mágnescsík hossza befolyásolja a rögzíthető adatmennyiséget.

Az elmúlt időkben sokféle formai megoldás alakult ki:

- kártyák,
- bizonylatok,
- kartonok, űrlapok,
- jegyek,
- okiratok.

E megoldások a mágnescsík sajátosságait tekintve azonosak, különbség a megjelenés formájában van. A formát alapvetően nem a mágnescsík paraméterei határozzák meg, hanem a felhasználási, kezelési módok.

A formai kialakításokból következik, hogy valamennyi megoldás önálló tárgyként jelenik meg. Az eszközök „elvesztés" elleni védelme a tárolás, őrzés módja miatt megoldott. Olyan esetekben, ahol a mágnescsíkos hordozó nem személyhez van rendelve, hanem egy tárgyhoz, gondot jelent a kapcsolat biztosítása. A mágnescsíkokat ugyanis nem lehet a vonalkódcímkékhez hasonlóan felragasztani. Legjobb esetben is csak „függőcímkeként" helyezhető el egy másnescsíkos kártya vagy bizonylat. A függőcímke típusú elhelyezés az azonosítani kívánt tárgy kialakítását befolyásolja, ugyanakkor gondot jelent a kártya olvasása is, hiszen le kell venni a tárgyról, majd újra visszafűzni. Ez újabb gépesítési problémát okoz.

Az adatok biztonsága, (hamisítás elleni) védelme

Általában adatbiztonság alatt azt értik, hogy az információ ne vesszen el, illetve illetéktelenek ne férhessenek hozzá. A mágnescsík esetében, különösen, ha általános felhasználásról van szó, az adatvédelem kiterjed a mágnescsík védelmére is. Szennyeződése, sérülése esetén ugyanis a mágnescsík nem lesz olvasható, így az adat „elvész".

A mágnescsíkot védenünk kell:

- mechanikus sérülésektől (törés, kopás, hordozótól való elválás),
- portól,

- gőzök lecsapódásától,
- elektromos károsodástól (mágneses erőterektől),
- szennyeződésektől.

Minderre azért van szükség, mert használata alapvetően a mágnescsík és az író/olvasó fej közötti kapcsolaton, kontaktuson múlik. Ha ugyanis a mágnescsík megtört, vagy olyan szennyeződés került rá, amelynek hatására az írás/olvasás során az eltávolodik a fejtől, akkor a fejben indukált áram – az eltávolodás függvényében – nagymértékben csökken, akár olvashatatlanságot is eredményezhet. A kódolási és formátumszabvány sajátosságai miatt adathiba esetén az egész mágnescsík, illetve a rajta lévő adat nem értelmezhető.

Elektromos hatások, elektromágneses erőterek közelsége esetén felléphet a demagnetizálódás (lemágneseződés, a feliratozáskor történő felmágnesezés ellentéte), ami a kártya mágneses jellemzőinek sérülését jelenti. Ez a mechanikus károsodáshoz hasonlóan – bár nem látható módön – szintén tönkreteheti mágnescsíkos eszközünket, kártyánkat.

A demagnetizálódás többnyire a mágneskártya-tulajdonosok otthonában, munkahelyén vagy közlekedés közben történik meg, mágneses erőtérrel való érintkezés közben, pl. nagy teljesítményű villamos motorok, transzformátorok közelében. Bankkártyák esetében ez nem valós probléma, mivel a legtöbben védett helyen, levéltárcában tartják kártyájukat, ahol az ilyen közvetlen kapcsolat módfelett valószínűtlen. A személyi azonosító kártyákkal vagy beléptetőkártyákkal viszont az emberek már nem bánnak olyan óvatosan, mint „pénzes" kártyájukkal. Ezért a szokásosan használt 300 oerstedes (Oe), alacsony koercivitású mágnescsík helyett magas koercivitású, 4000 Oe-s mágnescsíkokat használnak. A magas koercivitású mágneskártyák a külső elektromágneses térrel szemben ellenállóbbak.

Az ilyen kártyákat elsősorban a biztonsági rendszereket gyártó cégek és az azokat alkalmazók vásárolják.

A gyakorlatban az alacsony koercivitású kártyákat LoCo vagy Low Energy (alacsony energiájú), míg a magas koercivitásúakat HiCo vagy High Energy (magas energiájú) kártyáknak is nevezik. Ez utóbbi meghatározás, amely az energiaszintre utal, félrevezető, mivel a koercivitás értékét félremagyarázzák olyan értelemben, miszerint a magas energiájú

mágnescsíkot alkalmazva az olvasófej kimenő jele magasabb. Ez helytelen, mivel a kimenő jel nagysága az alkalmazott anyag remanenciájától, azaz a visszamaradó mágnesességtől függ, nem pedig a koercivitástól, azaz a külső mágneses tér megkívánt erejétől, amely a mágnest előállítja, a mágnesezettséget megváltoztatja.

Az illetéktelenekkel szembeni adatvédelem területéhez tartozik még a mágnescsíkon lévő adatok másolása, illetve a kártyák hamisítása. A mágneskártyákat gyakran használják személyazonosítóként is. Ezért annak érdekében, hogy a kártyát más ne használhassa, alkalmazzák az úgynevezett PIN (Personal Identity Number) kódot, amelynek egyeznie kell a mágnescsíkon is rögzített személyi kóddal. A hamisítások elkerülésére első szinten az adattartalmat speciálisan kódolják, második szinten a PIN kódot használják, illetve harmadik biztonsági szintként 2 rétegben (egymásra) viszik fel a mágnescsíkokat, az alsó réteg magas koercivitású (4000 Oe), míg a felső – az általában használt – réteg alacsony koercivitású (300 Oe).

Aktív–passzív kártyák

Mint az a korábbiakból kiderült, ha adott számú mágnescsíkot (mágneskártyát) veszünk, valamint író és olvasó eszközöket, úgy felállíthatunk egy olyan rendszert, amelyben az adatokat, illetve azok változásait felírjuk a kártyákra, majd adott állomásokon, munkahelyeken leolvassuk az információkat, amelyek alapján eldönthetjük, hogy mit kell tenni az adott munkadarabokkal.

Természetesen számos más problémával kell még megküzdenünk, pl. a kártya elhelyezése, de elvileg egy működőképes rendszer állítható fel.

A mágnescsík, illetve a mágneskártya rendelkezik egy olyan előnnyel, amellyel egyetlen más eddigi automatikus azonosítási eszköz sem, mégpedig azzal a tulajdonsággal, hogy az azonosítási rendszerben aktív elemként funkcionál, szemben az OCR-rel vagy a vonalkóddal, amelyek passzív elemek, azaz előállításuk után nem változtathatók.

A feliratozott mágnescsík demagnetizálható, így az idejétmúlt adatokat átírhatjuk. Eklatáns példa erre az iskolai vagy könyvtári fénymásoló. Az adott összeg befizetése után a kapott mágneskártyával másolhatunk. A fénymásolóval egybeépített író/olvasó eszköz érzékeli, hány egysé-

günk van a kártyán. A másolást elvégezve újraírja a kártyánkat, mégpedig a kiinduló összeget csökkenti a másolás értékével, s az így kialakult záró egyenleg kerül vissza. Ha elfogytak az egységeink, úgy bizonyos összeg befizetése után feltöltik a kártyánkat. Ilyen jellegű használat esetén aktív mágneskártyáról beszélünk.

E rövid példa alapján elképzelhető, hány területen lehetne zárt vagy nyitott rendszerben használni a mágneskártyát, nemcsak mint azonosító eszközt, hanem mint a folyamatok irányításának aktív résztvevőjét. A szállodai szobakulcsként működő kártya fizetőeszköz lehet a szállodai vagy a kapcsolódó üdülőhelyi szolgáltatások igénybevételekor, benzinkútnál fizethetünk vele. Természetesen nyílt rendszerekben igen összehangolt tervezésre és kiépítésre van szükség, hogy elektronikus pénzként működhessen tetszőleges kibocsátó bankokkal szerződésben lévő üzletekben.

Sajnálatos módon ezek a lehetőségek, bár több mint 30 éve adottak, mégsem éltek velük oly módon, hogy az aktív (mágnes)kártya szerte a világon elterjedjen. Ennek oka elsősorban a műszaki háttér, hiszen csak az utóbbi 10 évben nyílt rá lehetőség, hogy az adott azonosítási pontokon, pl. pénztáraknál, elektronikus úton összegyűjthessék a keletkezett adatokat. A „mini" méretű számítógépek, a PC-k, illetve azok „mini" árai tették az utóbbi években lehetővé, hogy a keletkező adatokat azon a helyen, abban az időben gyűjtsék össze, amikor keletkeztek.

Valójában az utóbbi évek mikroelektronikai fejlődése biztosíthatja a hátteret a mágneskártya aktív módon való használatához. Az aktív mágneskártyás rendszereket korábban csak kisebb, zárt rendszerekben használták, illetve használják ma is. Különösen jó példa erre a már említett könyvtári másológép, ahol a „kicsi és zárt rendszer" egyetlen berendezésre korlátozódik.

A mágnescsíkon tárolható adatmennyiség

A mágnescsík kártyán való felhasználásával kapcsolatban elsőként az IATA (International Air Transport Association) definiált alkalmazási igényeket, így a mágneskártyán lévő első sávot IATA-sávnak nevezik. A második sávot ABA-nak nevezték el, mégpedig az American Banking Associationról. A harmadik neve THRIFT, ez a „gazdasági" sáv.

A mágneskártyán tehát a szabványok szerint 3 sáv található:

- IATA, amely ALPHA formátumban, 210 bpi (bit per inch) sűrűséggel feliratozható,
- ABA, amely BCD formátumban, 75 bpi sűrűséggel írható, olvasható,
- THRIFT, amely BCD formátumban, 210 bpi sűrűséggel írható, olvasható.

Tekintettel a kártyán lévő mágnescsík hosszára, illetve a szükséges vezérlő karakterekre, az egyes sávok adattartalma a következő:

- alfanumerikus jelek – 79 karakter,
- numerikus jelek – 40 karakter,
- numerikus jelek – 107 karakter.

Az egyes sávok természetesen külön-külön is használhatók. A javasolt adattartalom a következő:

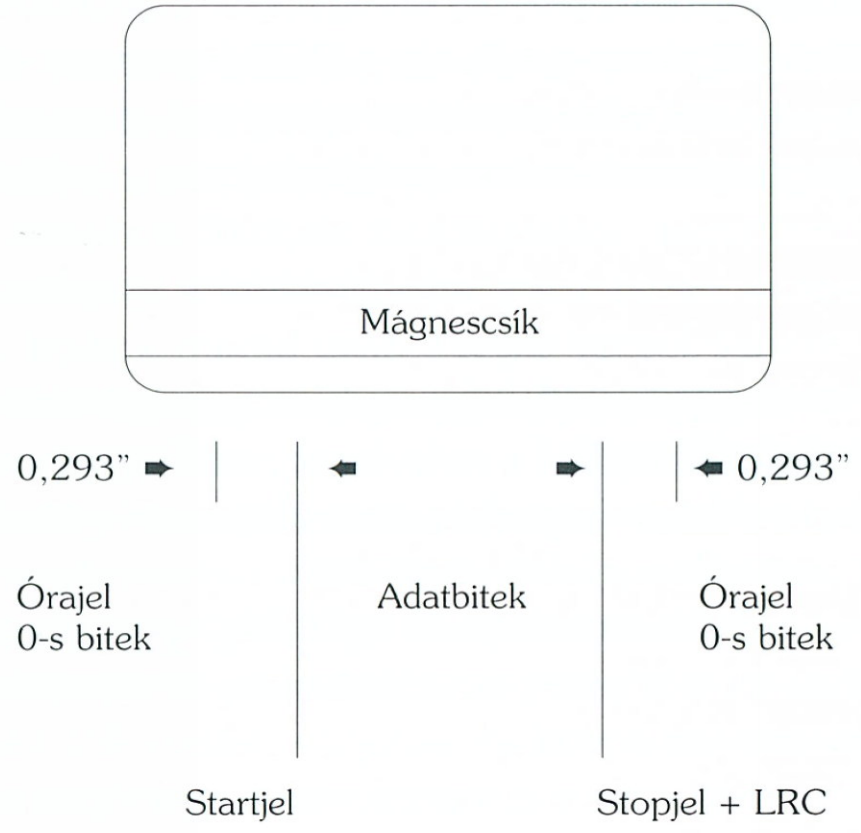
- kártyatulajdonos neve és számlaszáma,
- kártyatulajdonos számlaszáma, illetve biztonsági adatok,
- kártyatulajdonos számlaszáma, valamint egyéb tranzakciós információk.

A harmadik sávot olyan esetben javasolják, amikor újrakódoló sorra is szükség lehet, például amikor valamilyen készpénzes tranzakcióhoz használják.

Bár az ismertetett ANSI/ISO szabvány szerint a sávok használata bármilyen feladatra megfelelhet, nyomatékosan hangsúlyozni kell, hogy a mágnescsík kártyán való elhelyezése, illetve a sávok fizikai elhelyezkedése egyáltalán nem szigorúan korlátozott. Bármilyen kódolási sűrűséget, bármilyen adatformátumot bármilyen sávelrendezésben lehet használni. Az eddigi gyakorlat azt mutatja, hogy számos nem ANSI/ISO kombinációt használnak. Az ANSI/ISO specifikációt csak a pénzügyekkel kapcsolatos mágneskártyáknál követelik meg, amelyek arra hivatottak, hogy a nemzetközi kereskedelemben, bankhálózatban alkalmazzák.

A nem szabványos megoldásokat főleg biztosítási, valamint azonosító kártyák, szolgálati azonosítók, beléptetőkártyák, illetve más, zárt rendszerekben használatos kártyák esetében alkalmazzák. Ugyanakkor hangsúlyozni kell, hogy míg a kódolási sűrűség és az adatformátum módosítása a feliratozó/olvasó egység programjának (elektronikájának) módosítását igényli, addig a sávok fizikai elrendezésének változtatása

az író/olvasó egységek fizikai megváltoztatását is megköveteli. Ez utóbbi megoldás lényegesen bonyolultabb és költségesebb, mint az előzőekben leírt módosítás.



A jelsorozat kezdete és vége 0-s bitekkel.
Az utolsó karakter LRC paritás-ellenőrző jel.
A protokoll független a formátumtól, a sűrűségtől és a sávok számától.
A protokoll független a mágnescsík hosszától.

3. ábra. ANSI/ISO kódolási protokoll

Ennek tudható be, hogy a nem szabványos megoldások többnyire megtartják az ANSI/ISO szerinti sávelrendezést, ezzel az író/olvasókat is, változtatást az adatformátumban, a kódolási sűrűségben hajtanak végre. Mindezek függvényében csak a banki mágneskártya adattartalmáról, illetve az általa hordozott adatmennyiségről nyilatkozhatunk.

Más esetben a mágnescsík hossza, a formátum és a kódolási sűrűség ismeretében számítható ki a lehetséges adattartalom.

A mágnescsíkos rendszerek használata

Az eddigiek ismeretében már tudjuk, milyen műszaki paramétereket kell figyelembe vennünk, és milyen környezeti hatásokat kell kiküszöböl-

ni ahhoz, hogy az általunk alkalmazni kívánt mágneskártyás rendszer működhessen:

- Ha betűket, számokat egyaránt rögzíteni akarunk, úgy az ALPHA formátumot kell választani.
- Ha csak sávok rögzítése a cél, úgy a BCD formátum választása szükséges, mivel így egyúttal több karakter helyezhető el egységnyi hosszon.
- A tárolandó karakterek száma meghatározza a szükséges mágnescsík hosszát.
- Amennyiben a lehetőségek által biztosított mágnescsíkhossz nem elegendő, alkalmazzunk több sávot.
- A költséghatékonyság érdekében célszerű megtartani az ANSI/ISO szerinti 3 sáv fizikai méreteit.
- Amennyiben több sáv esetében sem elegendő a rendelkezésre álló hely, úgy csak numerikus jeleket rögzítsünk.
- Ha a 3 sáv, a BCD formátum és a 210 bpi sűrűség sem elegendő, úgy próbálkozhatunk a sűrűség növelésével is, ami azonban az olvasási biztonság romlásával jár együtt.
- Ha még mindezek után is gondunk van a szükséges adatok elhelyezésével, akkor meg kell vizsgálnunk más automatikus azonosítási eljárás alkalmazhatóságát.

A fentiek végiggondolásával első közelítésben kialakult mágneskártyás rendszerünk egyik fő eleme, a mágneskártya.

Második lépésben az író/olvasó terminálok telepítésével kell foglalkoznunk. Minden olyan esetben, amikor a mágnescsíkra új adatok kerülnek, tehát feliratozás történik, csak és kizárólag motoros kártyamozgatású író/olvasó készülék jöhet szóba. Az írás folyamán ugyanis eredendően biztosítani kell azt – számos más tényező mellett –, hogy egyenletes sebesség lépjen fel a mágnesszalag és az író fej között.

A későbbiekben ugyanis egy kézi olvasóval már az olvasó elektronikája kompenzálja a fellépő hibákat.

Ebből következik, hogy ha a kártya alkalmazása során változnak az adatok, úgy minden olyan munkahelyre, ahol az új adatokkal a régieket kiegészíteni vagy módosítani kell, mindenképpen motorizált író/olvasó eszköz telepítése szükséges. Az esetek többségében a kártya feliratozása

egyszer történik meg, és a rögzített adatok véglegesek maradnak részint a mágneskártya élettartamának végéig, részint a feladat megszűnéséig, amelynek érdekében a kártyán adatokat rögzítettek.

Ilyen rendszereknél a feleslegessé vált mágneskártyákat nem érdemes újra feliratozni, mivel a mágnescsík élettartama 2000-5000 leolvasás, azaz a leolvasás során ennyiszer történő mechanikus koptatás.

Harmadik lépésként ki kell alakítanunk azt az adatgyűjtő és -feldolgozó hálózatot, amely a kártyák leolvasásakor jelentkező információkat gyűjti, majd továbbítja a feldolgozó program, a számítógép felé.

A negyedik lépésre marad talán a legnehezebb feladat – mert a többi csak pénz kérdése –, hogy miként rögzítsük a mágneskártyákat azokhoz az emberekhez, tárgyakhoz, amelyeket a kártya azonosít. Az ember esetében ez viszonylag könnyű, mivel valamilyen tudati szempont kapcsolódik a kártya megőrzéséhez felhasználásának érdekében. Egyértelmű ez a tétel a biztonsági vagy pénzügyi kártyák esetében. Amennyiben azonban a mágneskártya tárgyakat azonosít, úgy jóval nehezebb a helyzetünk. Megfelelő felfogatási, rögzítési helyek kialakítására van szükség, amelyek biztosítják, hogy a kártya nem vész el, nem válik olvashatatlanná különféle sérülések, szennyeződések miatt. Minden egyes folyamat estében külön megoldásokat kell kitalálni.

Az elmúlt évtizedek gyakorlati kísérletei azt mutatták, hogy bármennyire törték is a fejüket a fejlesztők, nem sikerült általános megoldást találniuk. Ha eljutottunk az első négy probléma megoldásáig, még mindig nem dőlhetünk hátra kényelmes karosszékünkben.

Az ötödik próba az, hogy miként tudjuk az akár az emberekhez, akár a tárgyakhoz kötődő mágneskártyák írását/olvasását automatikus módon megoldani.

Esetünkben első közelítésben azt várjuk az automatikus megoldástól, hogy annak végrehajtása ember közreműködése nélkül valósuljon meg. De rá kell jönnünk, hogy a mágnescsík használata során, bármilyen hordozóra is helyezzük azt fel, az ember közreműködése elengedhetetlen. Gondoljunk csak vissza, hol is terjedt el tömegesen a mágnescsík:

- bankkártya,
- beléptető rendszerek,
- személyi azonosítás,

- útlevél,
- bank/takarékbetétkönyv,
- repülőjegy/beszállókártya,
- közlekedési (pl. metró-) jegy stb.

Mindegyiknél látjuk, hogy a mágnescsík leolvasásához biztosítva van az ember, aki egyúttal a kártya hordozója is. Az automatizált – esetleg ember nélküli – folyamatok alapvető igénye, hogy ne legyen szükség emberi, fizikai közreműködésre. A mai igényeket tekintve lehet, hogy a mágnescsíkos megoldás, a mágneskártya nem is azonosít automatikusan?

Mágneskártyás rendszerek eszközei

Fentebb már hangsúlyoztuk a rendkívüli fontosságát annak, hogy a mágnesfejet megfelelő kapcsolatban kell tartani a mágnescsíkkal a kódolási és az olvasási folyamat során. Nyilvánvalóan lényeges követelmény, hogy a mágnescsík precízen igazodjon a fejréshez az említett két műveletnél.

E két követelménynek, amely a mechanikai kialakítást lényegesen befolyásolja, fontos gyakorlati jelentősége van az olvasó, illetve az író/olvasó berendezés tervezésénél. A 4. ábra tartalmazza a legfontosabb paramétereket.

A fejrész–mágnescsík kapcsolat megfelelő fenntartása azt követeli meg, hogy a fej szabadon mozogjon annak érdekében, hogy követni tudja a kártya mozgását. Ugyanakkor a mozgás során egy megfelelően biztos kapcsolatnak kell létrejönnie, miközben a fej hozzányomódik a mágnescsíkhoz.

Mivel a gyakorlatban a mágnescsíkok mindig piszkosak, a fej nyomásának elég nagynak kell lennie ahhoz, hogy szó szerint eltávolítsa a szennyeződéseket róla, hogy a kódolási, illetve az olvasási hibákat elkerülhessük.

Az a követelmény tehát, hogy a hibák alacsony szinten való tartása miatt a fej erősen rányomódjon a mágnescsíkra, úgy a fejlesztők, mint a felhasználók által mind a mai napig sokat emlegetett probléma.

A mágnescsík egyrészt csiszoló-koptató hatást fejt ki, másrészt törékeny.

A csík jelentős kopást idéz elő a lágy anyagból készült fejen, ugyanakkor ha kemény anyagból készült fejet alkalmazunk, a mágnescsík törékenysége miatt könnyen károsodhat.

A gyakorlati kompromisszumot szem előtt tartva azt javasolják a szakemberek, hogy lágy fejanyagot használjunk, amelynek koptató hatása nem befolyásolja a mágnescsík hatékonyságát, ugyanakkor a fejet úgy kell megtervezni, hogy jelentős kopást elviseljen teljesítőképessége csökkenése nélkül.

Meg kell jegyezni, hogy tulajdonképpen a fej teremti meg a kapcsolatot a mágnescsík-technológiában a kártya és az egyéb berendezések között. Éppen ezért a rendszer minőségét, teljesítményét nem lehet kompenzálni más rendszerelemekkel.

Egyértelmű, hogy ha e kritikus pont kialakítása nem megfelelő színvonalú, úgy a rendszer működésétől sem szabad túlzott eredményeket elvárni.

Egy további mechanikai paraméter a mágnescsík sávjainak kijelölését, felírását biztosító megoldás. A kártyát vezető mechanizmusnak kell biztosítania, hogy a sávok párhuzamosan haladjanak, illetve a fejrés és a mágnescsík sávjai között ne jöjjön létre szöghiba. A nem párhuzamosság miatt kialakuló teljesítménycsökkenést azimut hibának nevezzük.

Mindezek mellett a kártyát vezető mechanizmusnak lehetővé kell tennie a kártya szabad mozgását annak érdekében, hogy elkerülhessünk más hibaforrást, amit egyébként stick-slipnek nevezünk.

A mágnesfej szerelése
- a fej kövesse a mágnescsík mozgását

A mágnesfej nyomó ereje
- biztos kapcsolatot kell fenntartani a fej és a mágnescsík között

A mágnesfej anyaga
- a fejnél és a mágnescsíknál elfogadható kopási érték

A mágneskártya mechanikus vezetése
- a mozgás során a fej és a sáv egymáshoz igazítása

4. ábra. Alapvető mechanikai paraméterek

Író/olvasó eszközök típusai

A mágnescsíkot alkalmazó kártyák írására/olvasására alapvetően 4 különböző típust alkalmaznak (5. ábra). Mindegyik rendelkezik sajátos

előnyökkel és hátrányokkal. Egyik típusról sem mondható el, hogy valamennyi alkalmazási lehetőség esetén egyformán hatékony lenne.

Manuális működtetésű résolvasó
- különböző kártyaméretek
- könnyű kezelés

Manuális működtetésű insert olvasó
- egyedi kártyaméretek
- könnyű üzembe helyezés

Motorizált működtetésű résolvasó
- álló kártya – mozgó fej
- a kezelõ vezérli a kártyát

Motorizált működtetésű insert olvasó
- álló fej – mozgó kártya
- a berendezés vezérli a kártyát

5. ábra. Író/olvasó eszközök típusai

A manuális „áthúzós" résolvasó előnye abban áll, hogy különböző szélességű és hosszúságú kártyák olvasására képes, és általában a legcélszerűbb manuális eszköz egy hibátlanul dolgozó szakember számára. Ugyanakkor ez az egység méretét tekintve nehezebben helyezhető üzembe, és nem tartja meg a kártyát az olvasás, illetve dekódolás közben.

A manuális „bedugós" insert olvasó általában kisebb, és könnyebben installálható. Ez a típus megtartja a kártyát a folyamat során. Hátránya, hogy csak bizonyos méretű kártyát fogad, és bonyolultabb a kezelése, mivel nehéz a kártyát úgy mozgatni, hogy az egyenletes sebességgel haladjon. Ez viszont hibákat von maga után. Mindkét manuális típus általában véve olcsó, és kevesebb karbantartást igényel, mint motorizált változatai.

A motorizált résolvasót néha „sidewinder"-nek is nevezik, mivel a kártya az olvasás során álló helyzetben marad, és a fej mozog a mágnescsík mentén.

Mint minden motorizált berendezés, azzal az előnnyel rendelkezik, hogy működése teljesen automatizált. Az ilyen eszközöknél az emberi tényezőt mint hibaforrást messzemenően kikapcsolják az írási/olvasási folyamatból. Ez a típus lehetővé teszi, hogy a kártya tulajdonosa ellenőrizze a folyamatot mechanikus hibák esetén.

A motorizált insert típusú eszköz átveszi a kártya mozgásának ellenőrzését a kezelőtől. Mindkét automatikus berendezés hátránya: nagyobb méret, magasabb költség, nagyobb karbantartásigény, valamint a mechanikus mozgás során fellépő hibák.

A gyakorlati alkalmazás során a mágnescsíkot író/olvasó eszköz megválasztásánál gondosan kell mérlegelni az említett jellemzőket, mégpedig az emberi tényezővel összefüggésben, hiszen az ember szintén része a mágneskártyás rendszernek.

Egy – már üzemelő – rendszer esetén nem ajánlatos, és sokszor nem is lehet az említett 4 típus bármelyikét valamelyik másikkal helyettesíteni. Ha mégis helyettesítésre van szükség, akkor azt csak nagyon ritkán lehet elvégezni áttervezés nélkül. Ez egyrészt azért fordulhat elő, mert a mágnescsíkos író/olvasó eszközökre nem fejlesztettek ki szabványokat, másrészt pedig azért, mert ezek könnyen átalakíthatók más, speciális felhasználásra alkalmas berendezésekké.

Ezen a területen sajnos az egyes eszközök nem cserészabatosak.

Ugyanakkor a piac a berendezések nagy választékát kínálja, minden felhasználónak külön-külön meg kell találnia az „igazit" a maga számára. Ha ez mégsem sikerülne, akkor a gyártó cégek általában elvégzik a felhasználói igények szerinti átalakításokat saját sorozatgyártású termékeiken.

Intelligens kártyarendszerek

Előzmények

Az aktív memóriakártyák a hetvenes évek közepén-végén kerültek az érdeklődés előterébe. A francia eredetű találmány a memóriakártya (carte á mémoire), az angol nyelvterületen az okos kártya (smart card), a németeknél a chipkarte nevet kapta. Nálunk eleinte az aktív memóriakártya volt használatos, majd a szakemberek az intelligens kártya névben egyeztek ki, azonban kapcsolataiknak megfelelően gyakrabban használják az idegen neveket.

Roland Moreno francia mérnök, újságíró 1972-ben jelentette be szabadalmi védelemre az aktív memóriakártyát. Akkor valószínűleg maga sem látta még pontosan, melyek a kártya alkalmazásának területei, illetve korlátjai. Ezt teljes körűen a mai napig sem tudjuk felmérni.

A mikroelektronikai technológia mostani fejlettségi szintje lehetővé tette – és egyre több alkalmazás igényelte – e kártyák megjelenését. A hitelkártya-méretű intelligens kártya ugyanis felhasználható mint jogosultságot bizonyító hozzáférési kulcs, elektronikus fizetési eszköz, hordozható adattároló.

Az említett eszközök jellemzője az aktív intelligencia, ami abból adódik, hogy a kártyában nem csak tároló, de feldolgozó áramkör (processzor) is lehet. A hitelkártya tárolási kapacitása 1-2 kilobyte, de esetenként elérheti, sőt meghaladhatja a 64 kilobyte-os értéket.

A processzornak köszönhetően a kártya a külvilággal intelligens párbeszédet folytathat, amelynek része az adatvédelmi és biztonsági célú ellenőrzések elvégzése, döntések meghozatala is. Az adatvédelem és biztonság céljára a kártyába írt szabályok kártyánként, illetve kártyakibocsátónként változhatnak. A kártya összes meglévő és lehetséges alkalmazása elsősorban a tárolási és döntéshozatali képességből adódik.

A kezdetben pénzkímélő, új fizetési eszköznek szánt intelligens kártyáról hamar kiderült, hogy alkalmazási lehetőségeinek köre ennél sokkal szélesebb. Egyrészt azért, mert minden korábbi, hasonló célú eszköznél nagyságrendekkel megbízhatóbb, nagy a tárolási kapacitása, valamint a beépített mikroprocesszor olyan új alkalmazásokat kínál, amelyeknek

nincsenek előzményei, másrészt mert a kártya off-line eszköz, ami további felhasználási dimenziókat nyújt. El kell fogadnunk a lehetőségek exponenciális bővülését hirdető tanokat, ha arra gondolunk, hogy a mikroelektronika fejlődésével újabb és újabb rekorderedmények születnek a kártyák tárolási kapacitása és feldolgozási tulajdonságai terén.

Mi a mikroáramkörös kártya, és melyek a funkciói?

A mikroáramkörös kártya szabványos hitelkártya-méretű műanyag lapba ágyazott, 8 érintkezős, általában egyetlen mikroáramkört tartalmazó eszköz. Csak programozható EPROM vagy újraprogramozható EEPROM típusú, nem felejtő tárolót, továbbá RAM-okat tartalmaz, amelyekhez – felhasználási céltól függően – az egyszerű huzalozott kapuhálózattól a bonyolult mikroprocesszoros vezérlésig terjedő logikai rendszer útján lehet hozzáférni.

A logikai rendszer egyrészt a külvilággal tartja a kapcsolatot, másrészt a kártyában tárolt adatokat védi.

A logikai rendszer funkciói:

- adatcsere-protokoll,
- memóriakezelés,
- belső funkciók biztonságos, hozzáférhetetlen kezelése.

A kisméretű kártya a benne tárolható viszonylag sok adat miatt hordozható adattárolóként is szolgálhat. A legfejlettebb technológiára épülő, nagy biztonságú belső logikája visszaélésmentes személyazonosításra teszi alkalmassá.

Önállóan képes számítógépi funkciók ellátására, így a legjobb hordozható eszköz hozzáférhető adatbankként, felhatalmazó kártyaként.

A hagyományos eszközökkel (mágneskártyák, belépők, jegyek, zsetonok, érmék, papírbizonylatok stb.) nem kielégítően megoldott problémákra okos, könnyen kezelhető, gyors és biztos eljárást kínál.

Az intelligens kártya szabványai

Az intelligens kártya fizikai méretei megegyeznek a szabványos hitelkártya méreteivel, amelyeket az ISO 7816 szabvány ír le. Ennek részei:

ISO 7816-1: fizikai paraméterek (pl. szélesség: 85,72 mm/3,375 inch, magasság: 54,03 mm/2,125 inch, vastagság: 0,76 mm [π0,08]/0,03 inch);

ISO 7816-2: a kapcsolódási pontok leírása (kártyaolvasók részére);

ISO 7816-3: az elektronikus jelek és az átviteli protokoll leírása;

ISO 7816-4: belső utasítások;

ISO 7816-5: alkalmazások kezelésének leírása;

ISO 7816-6: adatelemek leírása;

ISO 7816-7: SCQL (Structured Card Query Language) parancsok leírása.

Az utóbbi időben a szabvány újabb alpontokkal bővült (8–11), melyek közül kettő a biztonsági követelményeket határozza meg. Az intelligens kártyák területén – az internethálózathoz vagy a honi telefonkártya-rendszerhez hasonlóan – eleinte csupán a működés volt a fontos, de terjedésével a biztonságos működésre helyeződik át a hangsúly.

A kontaktusok funkciói

A kártya a külvilággal érintkezőkön keresztül tartja fenn a kapcsolatot.

Kapcsolódási pont alatt a kártya nyolc lábát értjük, amely az alábbi funkciókkal rendelkezik:

GND	GND, 0 V-os láb
+ 5 V	Vcc (tápfeszültség)
+ 25 V	Vpp (programozáshoz szükséges feszültség részére)
Órajel	Clock
Törlőjel	Reset
Adatjel	Data I/O, amelyen az adatjelek közlekednek
2 tartalék láb jövőbeni alkalmazások részére szabadon hagyva	

Meg kell említenünk a szabadon hagyott lábakkal kapcsolatban, hogy létezik olyan intelligens kártya, amely használja e lábak egyikét. Ilyen az SGS-Thomson által gyártott ST19-es kártyacsalád is, amely ma az egyik legsokoldalúbb és legbiztonságosabb a piacon.

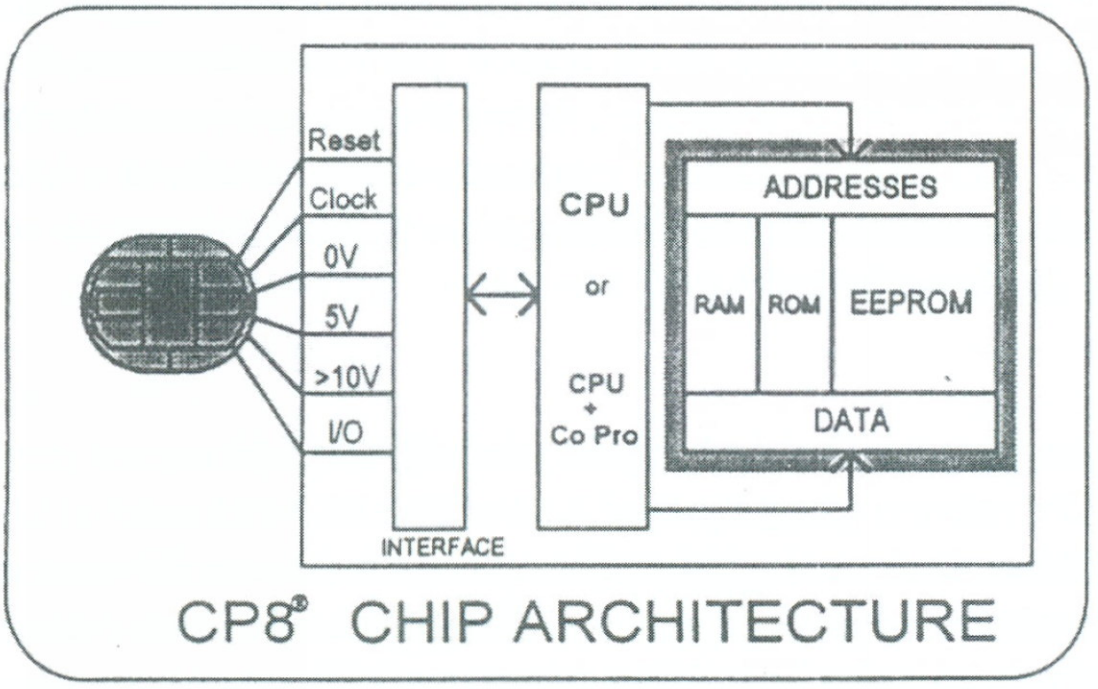
A kártya felületén elhelyezhető információhordozók

A chipen kívül a kártya felületén a már megszokott vagy új technológiájú információhordozók helyezhetők el, a szabványokban rögzített módon:

- ISO szabvány szerinti mágnescsík (az érintkezőkkel ellentétes oldalon, tehát a kártya hátoldalán),
- TRANSAC mágnescsík,
- a kártyába nyomtatott karaktersor (dombornyomás),
- vonalkódok,
- lézergravírozás,
- hologram,
- fénykép, aláírás,
- optikai diszkek által olvasható felület.

Ezekkel az információkkal összetett, mixed kártya alakítható ki. Különösen fontos ez azért, mert a banki hagyományokkal rendelkező országokban lehetővé teszi a folyamatos átmenetet a korábbi, elfogadott kártyarendszerekről az intelligens rendszerekre.

A kártya felépítése



1. ábra

A kártyában ROM (csak olvasható), RAM (olvasható, írható), EPROM (elektromosan programozható ROM) és esetleg EEPROM (elektromosan törölhető és programozható ROM) tárolóelemeket alkalmaznak. 1996-ban pedig megjelent a ferroelektromos RAM (FeRAM), amely lehetővé tette a kártyák rádiófrekvenciás kezelését.

A kártyában tárolt információ tartalma és felosztása az alkalmazástól függően nagyon sokféle lehet (lásd 2. ábra!):

- kívülről hozzáférhetetlen tartomány,
- a kártyában lévő mikroprogram vezérléstől függően írás/olvasás céljából hozzáférhető tartománya,
- szabadon, minden vizsgálat nélkül elérhető tartomány.

Az első tartomány csak a kártyán belül felhasználható információkat tárolja, úgymint a kártya kiadójának kódját, a tulajdonos PIN azonosítóját (PIN = Personal Identificafion Number), a kártya jogosító kódját és a szükséges mikroprogramok kódjait. A második tartomány jogosító és tranzakciós rekordokat tartalmaz, és kialakítása olyan, hogy a jogosításra vonatkozó információkat csak a kiadó változtathatja meg, de kizárólag a tulajdonos használhatja. E tartalom elérése függhet továbbá az érvényességi dátumtól, a korábbi felhasználásoktól vagy bármely más feltételtől, amely egy rövid program alakjában leírható.

A kártyában lévő processzor több feladatot is ellát. Így az adatfeldolgozás mellett a kártyában tárolt adatok párhuzamos–soros átalakítását a kártya tartalmának olvasásakor, illetve a soros–párhuzamos átalakítást a kártyába való íráskor. Ezzel a minimumra csökkenthető a kártya konfliktusainak száma, amikor a külvilággal tartja fenn a kapcsolatot, hiszen az átvitel sorosan történik.

A kártyaáramkörök fajtái

Kártyákba alkalmas lapkákat Európában a francia Thomson, a holland Philips, a német Siemens, az USA-ban a Motorola, Japánban az NEC, a Toshiba és a Casio gyárt, illetve más cégek.

Huzalozott logikájú kártyaáramkör (szinkron protokoll)

1. típus

Ilyenek pl. az előre fizetett telefonkártyák, a felépítésük szerint olcsó, 256 bites, egyszer programozható EPROM-os kártyák. A lapka a megbízható tömeggyártásnál kipróbált, n-csatornás, SI-kapus (MOS) technológiával készül. Sorosan hozzáférhető (bit by bit) és alacsony logikai jellel címezhető.

Zónák típusai	Olvasható	Írható	Törölhető	
Titkos zóna	N	N	N	Azonosítási információk
Access tracking zóna	Védett	N	N	Hozzáférések naplózása
Bizalmas zóna	Védett	N	N	Perszonalizálási adatok
Munka zónák	Definiálható			Perszonalizáláskor definiálják tulajdonságait
Szabadon olvasható zóna	I	N	N	Perszonalizálás publikus adatai
Gyártói zóna	I	N	N	Gyártási információk

2. ábra

Jól alkalmazható:

- viszonylag kis memóriakapacitásra,
- személyazonosításra,
- zsetonkártyaként automatákhoz,
- kis digitális rendszer kalibrálására,
- olyan rendszereknél, ahol sok kicsi eltérő változat van,
- kevés paraméter könnyű beállítását igénylő rendszereknél.

2. típus

Fejlettebb kártyachip, amelyben címdekóderrel és logikai egységgel rendelkező 9216 bites EPROM található. A logikai egység minden I/O vonalon jövő adatot dekódol, és tárol a memóriában, vagy kiolvas a memóriából. Az IC olyan olcsó memóriakártyában van, amelyet adat-hozzáférési célra személyazonosító számmal (PIN) terveztek. A PIN-t a logikai egység ismeri fel, jogosulatlan hozzáférés esetén detektál, három egymást követő hamis szám után reteszel, stb. Reteszelt kártya csak a kibocsátónál éleszthető újra.

Legfontosabb jellemzői:

- olvadó biztosítékkal védett azonosító terület,
- feszültségkomparátorral ellenőrzött Vpp,
- statikus órajelet nem igényel,
- memóriascrambling.

3. típus

A 3. típusú chip nem felejtő, 5 V-tal újraprogramozható, soros hozzáférésű memória, amely 22 em-es CMOS EEPROM-technológiával készül. 128 byte-os (128*8 bit) szervezésű, és a D/I (Data Input) érintkezőn hozzáférhető. Minden beírás-kiolvasás-törlés a D/I-ra történik, szinkronizálva az SC (Shift Clock) órajellel.

Jellemzői:

- nagy megbízhatóság (CMOS lebegőkapus technológia),
- egyetlen 5 V-os tápfeszültség,
- önidőzítő programozási ciklus,
- törölhető szó és bit,
- 10 000 törlési/beírási ciklus,
- tízévi adatmegőrzés.

Ez a chip ugyanazzal az alaparchitektúrával rendelkezik, mint a népszerű 1 kilobites standard EEPROM.

4. típus

A következő kártyachip nem felejtő, 5 V-tal újraprogramozható (EEPROM), memória-hozzáférésű biztonsági áramkörrel, vezérlőegységgel integrált memória. Főbb műszaki jellemzői azonosak az előzőével, de soros memóriaszervezése 24*16 bit.

A biztonsági áramkör:

- megvizsgálja a személyazonosító számot,
- számolja a hibás kódképzést,
- regisztrálja a beírás/törlés ciklusok számát,
- adott feltételek mellett képes a PIN egyszeri megváltoztatására.

Jellegzetes alkalmazásai:

- előre fizetett zsetonkártya /elektronikus pénztárca,
- azonosító kártya,
- elektronikus kulcs,
- telefonkártya.

Az összes típus kapható lapka, szelet, mikromodul és TAB formájában.

Mikroprocesszorral vezérelt memóriakártya-IC (aszinkron protokoll)

1. típus

Az első típus egylapkás NMOS mikroszámítógép-egység, beépített ROM-mal és EPROM-mal; speciálisan műanyag kányába tervezték, úgy, hogy megfeleljen a legmagasabb szoftvervédelmi követelményeknek is. Az IC 8 bites felépítésű. A cím- és adatbuszt azonban – biztonsági okból – a lapkában alakították ki. A külső kommunikáció egy interfészen keresztül történik, a CPU teljes ellenőrzése alatt, azaz a belső memória nem érhető el a normál interfész felhasználása mellett.

Ez a típus önprogramozó képességgel rendelkezik, ami azt jelenti, hogy saját maga képes a belső programmemória tartalmának kiolvasására és módosítására, külső beavatkozás nélkül csupán az előző állapotok (azaz egy, az alkalmazás folyamán előforduló esemény) figyelembevételével.

A szilíciumos EPROM technológia védelmet nyújt a szelektív törlés és újraírás útján való csaló felhasználással szemben.

Az EPROM-programozófeszültségnek a lapkán lévő referenciával való rendszeres összehasonlítása meggátolja, hogy a programozás elégtelen energiával menjen végbe, ami a helyes adatrögzítést kétségessé tenné.

Mivel kifejezetten a belső memóriába való illetéktelen beavatkozás elkerülésére tervezték, a személyi adatok biztonságára különösen érzékeny alkalmazásoknál ideálisan megfelel programok és adatok védelmére. Emellett a tervezésnél a bit- és byte-kezelés megkönnyítésére is gondoltak. N-csatornás, Si-kapus XMOS technológiával készül.

2. típus

A második típus az előző bővített memóriakapacitású változata RAM, ROM és EPROM tekintetében. Belső felépítése hasonló az előzőéhez, attól az alábbiakban különbözik:

- 76 byte-os RAM adatmemória,
- 3 kilobyte-os ROM,
- 4 kilobyte-os EPROM,
- 1 kilobyte adat vagy program (önprogramozó); 3 kilobyte csak adattárolásra.

3. típus

Az előzőhöz hasonló tulajdonságokkal rendelkezik, de az 1,5 æµm-es CMOS technológiának köszönhetően megnövelt memóriakapacitással és kisebb programozófeszültséggel.

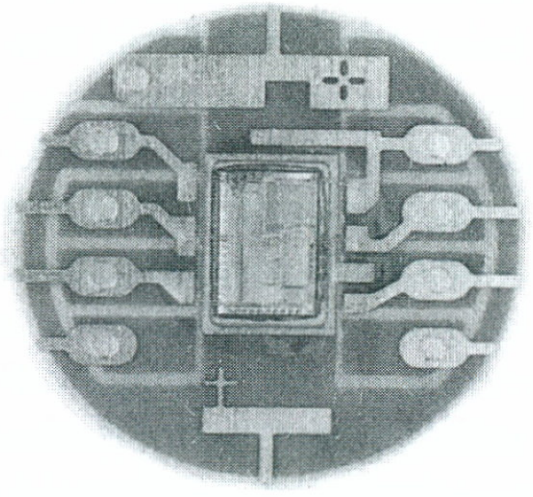
Az előzőektől eltérő főbb műszaki jellemzői:

- 256 byte-os RAM adattároló,
- 4 kilobyte-os ROM programtároló,
- 8 kilobyte-os EPROM önprogramozó lehetőséggel; 12,5 V-os EPROM-programozófeszültség.

4. típus

Egylapkás mikroszámítógép, amely az előzőekhez hasonló tulajdonságokkal, de eltérő memóriakapacitásokkal rendelkezik. A fő különbség azonban az, hogy 2,2 æµm-es CMOS EEPROM technológiával készül, adattárolója 2 kilobyte-os, elektromosan törölhető, illetve újraprogramozható, és önprogramozó képességgel is rendelkezik.

Valamennyi termék kapható lapka, szelet, mikromodul és TAB formájában.



3. ábra. Egy intelligens memóriachip nagyított képe

Alkalmazási területek: bankkártya, belépőkártya, VIDEOTEX fizetőkártya, elektromos csekkfüzet.

Valamennyi standard termék készülhet a megrendelő igényei szerinti EPROM-, EEPROM-, illetve ROM-elemekkel, megfelelően nagy darab-

számú alkalmazásokhoz, ami minimálisan 10 ezer kártyát jelent. A standard logikai hálózatok ugyancsak helyettesíthetők a megrendelő igényei szerinti specifikációjúakkal, és a standard mikroprocesszorok is kiegészíthetők további vagy alternatív utasításokkal.

A fejlesztés a jelenleg használatos technológiák tökéletesítésével a memóriakapacitás több megabitre való bővítésére irányul. Elkészült, de áttörő piaci kereslet még nem mutatkozott az 1 megabites kapacitású és a bonyolultabb adatkezelésre alkalmas, 16 bites mikroprocesszorú változat iránt.

Az európai fejlesztői konzorcium a 32 bites RISC architecktúrájú processzor használatát tűzte ki célul.

A memóriakártyát tervező mérnöknek összetett feladatot kellett megoldania; azt már tudjuk, hogy az intelligens kártya a kivezetések számának csökkentése érdekében soros átviteli vonalon kommunikál a külvilággal, de kérdés volt, hol legyen az érintkezőket magában foglaló „pogácsa" helye. A már alkalmazásban lévő kártyatípusok és azok olvasóberendezéseinek kialakítása, a dombornyomás és a mágnescsík elhelyezkedése miatt az áramkörök a kártyán a bal felső sarokban helyezkednek el.

A kártyában a tároló- és a processzoráramkörök két különálló vagy egyetlen lapkán helyezkednek el. A nagy igénybevételnek kitett kártyánál sem a félvezető lapok, sem az azokat egymással és a külső kontaktusokkal összekötő vezetékek nem károsodhatnak a használat közben. A mechanikai tervezés során az igényes kártyákkal szembeni elvárás tízéves időtartam és egymillió írás/olvasás.

A kártya tervezésekor nemcsak a külső, mechanikus igénybevételekre kell figyelemmel lenni, hanem gondolni kell a félvezető lapkák védelmére, elektromos és mágneses árnyékolására is. Hiszen az intelligens kártyákat a legkülönbözőbb környezetekben használhatják, pl. röntgensugárzásnak kitett orvosi laboratóriumban vagy benzinkútnál, ahol az autók gyújtórendszerében keletkező szikrák okozhatnak gondokat.

A kártyába épített lapkának kb. 30%-kal kell vékonyabbnak lennie, mint a tokozott integrált áramkörökben használatosnak. A mechanikus igénybevétel káros hatásainak elkerülése érdekében a lapkának minél kisebbnek kell lennie, következésképpen az elemsűrűséget az ésszerű maximumig kell fokozni. Egy-egy áramkör 100 ezer (sőt több) tranzisztornak megfelelő mennyiségű kapcsolási elemből is állhat. A tervezőnek kis

teljesítményfelvételű technológiát célszerű alkalmaznia, s persze gondolnia kell a gyártási költségek minimalizálására is. A sebesség általában nem elsőrendű szempont, hiszen az alkalmazások zömében a kártya legtöbb művelete a felhasználóval folytatott párbeszéd keretében zajlik, s az emberi kéz billentyűnyomogatásának sebessége jóval kisebb, mint egy viszonylag lassú processzor működése.

Az intelligenskártya-processzorok előállítására a legalkalmasabb a CMOS technológia, ennek teljesítményfelvétele kb. tizede az MOS áramkörökének, és zajérzékenysége is kedvező.

Kártyagyártás

Plasztikkártya gyártása

Laminált kártyák: a jó minőségű, finom grafikát átlátszó réteg fedi. A hő és a nyomás a felületek egymáshoz ragasztására szolgál. A chip helyét a plasztiklapba befúrják. Anyaga általában PVC.

Fröccsöntött kártyák: 250 Celsius-fokon olvadó műanyag gyöngyökből készülnek, és egy lépésben a kívánt formát érik el. E kártyák olcsóbbak az előzőeknél, azonban nem dombornyomhatók, és nem lehet rájuk mágnescsíkot elhelyezni.

Plasztik nyomtatása, tesztelése: a fröccsöntött kártyákat annyiszor nyomtatják, ahány szín szerepel rajtuk, majd mindkét típust vagy szemmel, vagy számítógéppel vezérelten ellenőrzik.

Chipgyártás: a chip, amely a szokásos IC-gyártási technológia terméke, a szeletke feldarabolása után az aranyérintkezőhöz huzalozásra kerül, majd az így kialakuló modult gyantával „kapszulázzák". Ez a gyártási fázis a legérzékenyebb, különösen a szennyeződésre, sztatikus feltöltődésre, ezért csak laboratóriumi tisztaságú üzemben végezhető el.

Chip és érintkezők beültetése: a fentiek szerint előálló modulokat a plasztikkártyák előre kialakított mélyedésébe ragasztják. E ragasztás minősége van talán a legnagyobb hatással a kártya későbbi megbízhatóságára. Eredetileg folyékony ragasztóval rögzítették a modulokat, azonban ez nem volt elegendően erős a két anyag (fém és plasztik) között. A használat során pedig a chip sokszor tört el a kemény kötés miatt,

amely a chip hátoldala és a plasztiklap között jött létre. E hátrányok kiküszöbölésére újabban a szalagos ragasztást használják, amikor is egy mindkét oldalán ragadó szalagra kerül a chipmodul, melynek hátoldala megbízhatóan ragad a fémréteghez. A chip hátoldala mögött levegő marad, így a használat közbeni mozgások nem bántják, miáltal élettartama meghosszabbodik. E száraz technológia jobb pozicionálási lehetőséget is nyújt.

A kártyákat a beültetett elemekkel a ragasztó ráolvasztása céljából hőkezelik, majd elvégzik a mechanikus és elektromos ellenőrzést.

A perszonalizálás során kerül a kártyára a generáló anyag, a PIN és a kriptográfiai biztonsági kulcs.

Preperszonalizálás: elektromos tesztelésből, a kezdeti fájlstruktúra és a kártyafüggetlen adatok, továbbá a szállítási kulcs felviteléből áll.

Perszonalizálás: ennek alkalmával az egyedi kártyaazonosítók egyrészt a chipbe, másrészt a plasztikhordozóra kerülnek. Leggyakoribb a felület hőnyomtatása vagy lézergravírozása.

Utóperszonalizálás: gyakorlatilag a személyes adatokkal való feltöltést jelenti.

Kereskedelmi forgalomban megjelenő terméktípusok

A fentebb ismertetett termékek az alábbi formákban állnak a további feldolgozók, illetve az alkalmazók rendelkezésére.

Lapkák

Szeletek formájában, ezek lehetnek darabolatlanok vagy daraboltak, szabványos gyűrűkre szerelve, ezek a legtöbb elembeültető berendezéssel való szerelésre alkalmasak.

Mikromodulokba szerelve. A mikromodul a műanyag kártyába való könnyű beillesztés céljára kifejlesztett különleges, filmhordozós (Tape Automated Building – TAB) tokozás. A mikromodulok filmszalagtekercsre szerelve kerülnek szállításra.

A modulokat maszkokkal fedik le, amelyeknek különböző típusai különböző alkalmazásokat hoznak létre.

Maszk típusa	Funkciója
M 4	Banki alkalmazásoknál általánosan használt maszk. Lehetővé teszi az EPROM tároló felosztását védelmi, adat- és gyártási információs területekre. A területek hozzáférhetősége tartalmuk titkossági fokától függ.
M 8	Hasonló az M 4 maszk funkcióihoz, csak a jogtalan hozzáférési szándék kezelésének eljárásában van eltérés.
M 9	A nagyobb kapacitású kártyáknál használják, funkciói hasonlóak az M 8 maszkéhoz (az egyre nagyobb kapacitású kártyák esetében az alkalmazási programok felfelé való kompatibilitását garantálja).
PC 1	A francia postai hatóságok igénye szerint kialakított, különböző postai szolgáltatások használatára jogosító maszk.
MP	A sokcélú (multi-purpose) kártyákhoz készült maszk. Ebben az esetben egy kártya több, egymástól teljesen független célra használható.

Bull CP8 intelligens kártyák főbb jellemzői

Méretek az ISO 7810 szabvány szerint	
vastagság	0,76 mm
magasság	53,98 mm
szélesség	85,60 mm
Környezeti hőmérséklet	0–50 C°
Relatív légnedvesség	max. 80%
Megengedett legnagyobb	
röntgensugárzás	0,1 grad
külső erő	1,5 newton
elektromágneses tér	1000 oersted
Max. statikus feszültség	1500 V
Az IC max. disszipációja	max. 0,8 W
Adatátviteli protokoll	aszinkron, félduplex
	9600 bit/sec

Fehér kártyák

Ez esetben a plasztiklapra elhelyezett chip kerül szállításra, és a perszonalizálás során a vásárló, esetleg a végfelhasználó igényeinek megfelelő minta és adattartalom kerül a kártyára. Általában kis sorozatoknál (5 ezer kártya alatt) használják. Előnye az egyediség, hátránya, hogy a chip közvetlen környezetében nem lehet mintát felvinni, mert a nyomtató esetleg megsérülne. Az így nyomtatott kártyák felületén elhelyezett minták tartóssága függ az alkalmazott nyomtatóeljárás minőségétől.

Előnyomott kártyák

Nagyobb sorozatban előállított vagy értékesebb kártyák esetében – pl. üzemanyag-, illetve bankkártya – a megrendelés alapján a plasztik felületének mintázása már a gyárban a teljes sorozatra megtörténik.

A kártyaolvasó terminál

A kártya és a külvilág között a kártyaolvasó terminálon keresztül áramlik az információ, vagyis az teremt kapcsolatot a külvilággal, és a terminál feladata a kártya feszültségellátása is.

Az intelligens kártyákhoz háromféle terminháltípust dolgoztak ki. Ezek általában 8 bites (többnyire 8085-ös vagy 6502-es) mikroprocesszorral épülnek fel. Legegyszerűbb közülük az úgynevezett ellenőrző terminál, amelybe a kártyát behelyezve egy kis, számjegyes billentyűzeten a titkos kód begépelhető. Ezt a kártyára a kibocsátáskor felírt kóddal összehasonlítja, és egyezés esetén a pozitív nyugtázás a folyadékkristályos megjelenítőn látható.

A következő típusba tartoznak a tranzakció lebonyolítására alkalmas terminálok, amelyek önállóan vagy hálózatba kapcsolva működtethetők. Ezeken keresztül már a tranzakciók is felírhatók a kártyákra. Ilyeneket használnak például eladói, POS (Point of Sale) terminálok gyanánt a kereskedelemben.

A terjedőben lévő elektronikus pénztárcák egyenlegének lekérdezése egyszerű kulcskarikára akasztható olvasóval is megoldható.

A fizetőkártyát kibocsátó bankok, illetve pénzintézetek feladata az új kártyák felhasználóhoz, személyhez rendelése, azaz perszonalizációja. Ez nagyszámítógépet, pontosabban nagy háttértárral összekötött, speciális terminálokat igényel, hiszen a kártyára felvitt minden – a perszonalizáció után megváltoztathatatlanná tett – adat a kibocsátó bank adatbázisának is részévé kell, hogy váljon.

A hitelkártya-olvasó terminálok felépítésének első feladata a nyolc kontaktust biztosító, a kártyára kapcsolódó és onnan oldható tűsor megvalósítása. A tűsor kártyára kapcsolódását egy mechanizmus segítségével a kártya nyílásba helyezésének, illetve eltolásának kell elvégeznie.

A mechanikus kontaktusok kialakítása előtt az elektromos feszültségszintek nem aktiválhatók.

A szolgáltatást nyújtó rendszerben egy számítógép nélkülözhetetlen, mivel vagy az nyújtja a szolgáltatást (pl. a nyilvános adatbázis elérését), vagy az vezérli a szolgáltatást nyújtó egységeket (pl. a kezelő nélküli benzinkutat). A szolgáltatási tranzakció végül is a számítógép és az igénybe vevő személy között zajlik le.

A kívánt szolgáltatás kiválasztásakor a szolgáltatást nyújtó számítógép és az igénybe vevő személy közötti tranzakcióhoz általában szükség van egy beviteli eszközre (pl. billentyűzetre) és egy kijelzőre. Ahol azonban a szolgáltatás egyszerű, és használata egyértelmű, ott ez a két eszköz ki is maradhat: pl. az automata benzinkútnál az adagolócső elvétele egyértelműen jelzi, hogy milyen benzint akarunk venni. A nyilvános telefonkészüléknél hasonlóan egyértelmű a helyzet, azonban a francia nyilvános videotex-adatbázis szolgáltatásaiból a felhasználó már egy Minitel-terminálon keresztül válogathat.

Intelligenskártya-alkalmazói szoftver

Az intelligens kártya számítástechnikai szempontból kettős szerepet játszik. Egyrészt információt tárol, másrészt olyan programot tartalmaz, amely szabályozza a kártya és a vele kapcsolatot teremtő berendezések közötti információcserét. Ez teszi lehetővé, hogy a tárolt adatokat nagy biztonsággal lehessen védeni az illetéktelen hozzáféréstől, és meg lehessen akadályozni a kártya jogtalan használatát. Az intelligenskártya-rendszer e tulajdonsága miatt válhat pénzforgalmat kiváltó eszközzé, illetve alkalmazható minden olyan helyen, ahol az adatok beírása, módosítása, illetve kiolvasása szigorú illetékességhez van kötve.

Az intelligens kártyákkal kapcsolatban az alábbi területeken merülnek fel szoftverfeladatok.

A kártya részéről:

- a kártyák és a kapcsolódó készülékek közötti adatbeviteli rendszer,
- belső író- és olvasórutinok,
- biztonsági rutinok önellenőrzés és hozzáférés-ellenőrzés céljából,
- az adatok ábrázolási módja, a memóriafelhasználás kérdései,
- alkalmazói programok.

A perifériák (kártyaolvasó) részéről:

- átvételi eljárások,
- érvényesség-ellenőrzés,
- ügyintézői és kártyatulajdonosi kezelőfelület: adatbevitel, kijelzés módja, engedélyezés, ellenőrzés,
- kártyaprogramozás.

Felhasználói vonatkozások:

- kibocsátási, kezdeti feltöltési eljárás,
- érvénytelenítési lehetőségek,
- tranzakciós műveletek,
- titkosság,
- adatbázissal való kapcsolat.

Fejlesztési feladatok:

- modellezés, szimuláció, emuláció,
- alkalmazási kapcsolatok analízise,
- szolgáltatásbővítési lehetőségek vizsgálata.

A szoftverfeladatok közül a kártyák belső programjai kívánnak meg különösen gondos előkészítést. Itt nagy sorozatban előállított termékről van szó, amelynél a megbízható működésről kell gondoskodni, ugyanakkor a kevés memóriahelyet jól ki kell használni. Noha a kártya előállítási költségét lehetőség szerint le kell szorítani, a cél elérése érdekében a kártyák programfejlesztésére mégis nagyobb ráfordítás szükséges.

Az intelligens kártya lehetőséget ad arra, hogy a tranzakciókat végső fokon feldolgozó adatbankrendszerrel való on-line kapcsolaton kívül a kiszolgáló készülék off-line módban üzemelhessen az adatbázissal való szakaszos kapcsolattal, ami mágneskazetta vagy mágneslemez cseréjével történhet.

Az intelligens kártya elterjedésével, illetve elterjesztésével kapcsolatban számolni kell a hagyományos pénzbedobós automaták mellett a kártyavezérlésű készülékekkel is (pl. nyilvános, szállodai vagy akár egyéni telefonkészülékek, automata üzemanyagtöltő állomások, jegyváltó-automaták stb.). Ilyenkor igazodni kell a meglévő rendszer adottságaihoz, illetve azt lehetőleg csupán kismértékben módosító változtatásokat kell végrehajtani.

Míg az elmúlt években a számítástechnika más területeihez képest a smart kártyák hardverfejlesztése szinte stagnált, addig az alkalmazások száma robbanásszerűen nőtt.

Az alábbiakban a legfontosabb területeket és azok egy-egy igen fontos projektjét említjük meg, a teljesség igénye nélkül.

Hűség (loyalty) rendszerek

A vásárlók márkahűségének kialakításához és fenntartásához kiváló eszköz a pontgyűjtésre szolgáló intelligens kártya. A vásárlók kedvezményeiket folyamatosan összegyűjthetik, ami sajátos szórakozási és játéklehetőséget kínál számukra. Először az üzemanyag- és utazásértékesítés területén jöttek létre, jelenleg pedig már a kombinált rendszerek kerülnek kialakításra. Így pl. a Shell kártyák millióit adta ki először az Egyesült Királyságban, majd nálunk is, s éppen Magyarországon valósította meg a McDonald's hálózatával a közös elfogadás kiépítését. A rendszerek egyik fő célja a fogyasztói szokások jobb megismerése és az azokhoz való alkalmazkodás.

Pénzügyi alkalmazások

Az e területen használt kártyák többsége ma még mágnescsíkos kártya, azonban az összes kártyahálózat tervezi az átállást a mikroprocesszoros intelligens kártyákra. A szállítók rövidesen csak az EMV (Europay, MasterCard, Visa) szabványt támogató kártyacsaládjaikkal vehetnek majd részt a bankkártyák ezen új generációjának létrejöttében.

E-Purse – elektronikus pénztárca: célja a kis értékű fizetések költségeinek csökkentése. A kártyán kvázi készpénz van nyilvántartva, amelylyel off-line módon lehet fizetni. Bár a Visa az 1996-os atlantai olimpián és New Yorkban bevezette Visa Cash néven, e rendszer mégis először Dániában és a Benelux államokban került nagyobb tömegű alkalmazásra.

Debit/credit kártyák: általában a bankok mágnescsíkkal is ellátott hibrid kártyáiként látnak napvilágot, és elsődleges céljuk a kártyabiztonság és a kártyával nyújtható szolgáltatások növelése. Az ipar bízik abban, hogy nincs messze az idő, amikor a PC-ket már chipkártyaolvasóval szál-

lítják, és a bankkártyát biztonságosan lehet használni az interneten. Franciaországban a GIE Carte Bancaire, Németországban a ZKA, az USA-ban pedig az AMEX adott ki chip/mágnescsík kombinációjú kártyát.

Az elektronikus kereskedelem (e-commerce) magában foglalja az egymástól fizikailag távol tartózkodó felek közötti kereskedelmi jellegű tevékenységek teljes körét, kis és nagy méretekben, a fogyasztói és szervezeti piacokon egyaránt. Az internet elterjedése biztosítja, hogy az elektronikus kereskedelem infrastruktúrája javarészt kiépül, így nem a kereskedőé, szolgáltatóé vagy termelőé az összes költség – következésképpen várható ezen alkalmazások gyors elterjedése.

Információtechnológiai alkalmazások

- NC-, netkomputerek
- PC standard tartozéka
- PC/SC munkacsoport

Kormányzati alkalmazások

Egészségügyi alkalmazások

- Betegbiztosítási kártyák
- Health passportok
- Ápolási kártyák
- Orvoskártyák

Kommunikáció

A GSM-mobiltelefonokban használt SIM kártyák is intelligens kártyák, amelyek egyik fő előnye, hogy információk tárolhatók rajtuk.

A kódolt műholdas csatornák vételéhez már ma használják az előfizetői kártyákat. A kártyák adott időszakra érvényesíthetők, illetve a megnézett programok értéke folyamatosan le is vonható a kártyán lévő összegből (Pay Per View rendszer).

Tömegközlekedés

Elsőként a loyalty jellegű rendszerek jelentek meg, amelyeknél a jegyvásárlások bizonyos gazdasági vagy kényelmi előnyökhöz voltak kötöt-

tek. Ezek a projektek a repülőtársaságok loyalty rendszereit próbálták utánozni a tömegközlekedésben, elsősorban a vonatközlekedésnél. A második generáció prepaid kártyákat használt, és már meglévő kapukkal vagy jegyeladó terminálokkal felszerelt rendszerekben vették használatba (metró, elővárosi vasutak stb.).

Ezt követően jelent meg és vált tömegméretekben használhatóvá a rádiófrekvenciás kártya. Ezek az érintkezésmentes kártyák kiválthatják a jegyeket és bérleteket, segítségükkel növelhető a csomópontok átbocsátóképessége, továbbá többször is biztonságosan és rugalmasan érvényesíthetők, ami számottevő költségmegtakarítást eredményez. További előnyük, hogy pénzügyi tranzakciókra és más szolgáltatókkal való együttműködésre is felhasználhatók.

Azonosítás

A smart kártyák a piacon való megjelenésük óta folyamatosan felhasználásra kerülnek a tulajdonosukat azonosító kártyákként. Eleinte pusztán azt a tulajdonságukat használták ki, hogy a tulajdonos meg tudta változtatni a jelszavát – a kártya ezzel növelte elfogadottságát.

Jelenleg egyrészt a tulajdonos fiziológiai/biológiai azonosítóinak kártyán való elhelyezésén dolgoznak a fejlesztők, ami a jelszó (password) kiküszöbölésével növeli a rendszer biztonságát. Másrészt a mögöttes rendszerek (adatbázisok, átviteli és hitelesítő rendszerek) kártyával való védhetőségén, hitelesíthetőségén munkálkodnak. 2000 nyarának legjelentősebb vívmánya, hogy június 30-án az Egyesült Államok elnöke, Bill Clinton egy smart kártya és annak jelszava használatával írta alá és iktatta törvénybe az elektronikus aláírás elfogadásáról szóló törvényt.

Chipkártyák adatbiztonsága

A fejezetben tárgyalásra kerülő kulcsszavak:

- a smart kártyás rendszerekhez kapcsolódó szoftverek,
- adatvédelem,
- adatbiztonság,
- kriptográfiai szabályok (digitális aláírás, multifunkciós kártyák, perszonalizáció, adatbiztonság).

A chipkártya mint varázseszköz

Mint a továbbiakban látni fogjuk, a chipkártyák megfelelő használat esetén sokat segítenek a megerősített biztonságú rendszerek létrehozásában, üzemeltetésében. Itt, a bevezetőben viszont ki kell emelni, hogy számos gyakorlati alkalmazásban megfigyelhetjük a kártyák helytelen használatát, nagyon sokféle szempontból.

A chipkártya egyes rendszerkialakítók szemében valamiféle varázsszó. „A chipkártya természetesen biztonságosabb, mint a tetszőlegesen választott alternatív eszköz" – halljuk, de az indoklás elmarad, sőt a részletesebb kérdések nyomán kiderül, hogy az illetőnek elemi fogalma sincs arról, hogy a kártya hogyan illeszkedik a rendszerbe, melyek a konkrét előnyei, és főleg melyek azok a gyenge pontok, ahol támadási felületet nyújt. Azt pedig ezek után végképp nem várhatjuk, hogy a számtalan, alapjaiban eltérő funkciójú kártya közül az alkalmazásnak valóban megfelelőt használják.

Ezt a fejezetet nem betörési útmutatónak szánjuk, hanem gondolatébresztőnek. A köd, a homályba burkolódzás csak azokat szolgálja, akik ellen – mondjuk éppen a chipkártya alkalmazásával – védekezni szeretnénk. Aki nem tudja, hogy miként lehet egy rendszerbe behatolni, nem lesz képes azt megvédeni sem.

A chipkártya használata mellett leggyakrabban elhangzó érv, hogy azt nem lehet lemásolni. Ezt valóban elfogadhatjuk alapnak. De egy rendszer szempontjából nem biztos, hogy a lemásolhatóság a legfontosabb szempont. Az a fontos tény is el szokott sikkadni a másolhatatlanság

mellett, hogy bizonyos esetekben a másolás felesleges lehet, ha a csatolófelületet a kártyához fizikailag alig hasonló eszközzel megtéveszthetjük.

A homály eloszlatásában sajnos a kártyák gyártói és forgalmazói sem mindig jeleskednek. A kártyával együtt forgalmazott, esetleg demoszintű szoftver bemutatásán túl a konkrétumokat magunknak kell kiválogatnunk több száz oldalnyi pelyva közül, rengeteg fontos körülmény pedig egyáltalán nem kerül megemlítésre. További problémákat jelenthet, hogy esetleg hiányos leírást kapunk a kártya eléréséről – nem beszélve arról, ha egyáltalán nem kapunk, s a kártyagyártó által szolgáltatott meghajtószoftverre kell hagyatkoznunk. Márpedig egy forrásban nem meglévő, nem bevizsgálható szoftverelem bevitele egy biztonsági rendszerbe igencsak meggondolandó, lehet, hogy ezzel nagyobb kockázatot vállalunk, mintha a kártya helyett valamilyen önmagában kevésbé biztonságos, de jobban specifikált eszközt alkalmaznánk.

A következő fejezetben összefoglaljuk azokat a területeket, ahol chipkártyát lehet alkalmazni. Igyekszünk minél több lehetséges problémát bemutatni, amelyre egy tényleges rendszer tervezésénél tekintettel kell lenni. Természetesen nem állíthatjuk, hogy a kapcsolódó problémák mindegyikéről szót ejtünk, de a biztonsági rendszerek sokfélesége ezt nem is teszi lehetővé. Egy konkrét helyzet specifikus problémáit mindig külön fel kell deríteni.

A tárgyalt anyagot két részre osztottuk. Előbb a kártya mint hardvereszköz használatáról lesz szó, és azokról a műveletekről, amelyekre használni szoktuk. A másik részben a számítógép felőli oldalt tekintjük át, a szoftver oldaláról megfogalmazható problémákat. A leírtak sok helyütt a korábbi fejezetekre építenek, így az anyag csupán az egészet átolvasva lesz értelmes. Aki csak a téma egy-egy vetületére kíváncsi, az is olvassa végig, különben alapvető szempontokat hagyhat figyelmen kívül, amelyeket korábban említettünk, de nem ismételtünk meg minden egyes bekezdésben.

Ez a kis összefoglaló természetesen nem törekedhet teljességre, hiszen egy-egy összefoglaló, inkább csak referenciákat felsoroló, kriptográfiával foglalkozó mű is terjedelmében az 1000 nagy alakú oldalt közelíti meg. Ahhoz viszont talán hozzásegít, hogy a chipkártyára már ne varázsszerként tekintsünk, hanem ismert tulajdonságokkal – erősségekkel és gyengeségekkel – rendelkező eszközként, amelyet jól átgondolt céljaink szolgálatába állíthatunk.

A chipkártyát az adatvédelem szolgálatában az alábbi főbb területeken használják:

- hozzáférés-védelem,
- rejtjelezés,
- hitelesítés.

Természetesen egy-egy gyakorlati alkalmazás a fentiek közül egyszerre több feladatot is elláthat, és több esetben ezek a funkciók annyira összefonódnak, hogy nem is lehet őket szétválasztani. A biztonsággal kapcsolatos számos probléma hasonlóan vetődik fel a különböző területeken, de ezeket a későbbiekben nem ismételjük meg. Ezért az első fejezetben írottak elolvasása akkor is szükséges, ha valaki nem érdekelt az egyszerű azonosításon alapuló hozzáférés-védelmi rendszerben, hanem azt egy rejtjelező-hitelesítő rendszer részeként alakítja ki.

Az egyszerű hozzáférés-védelem

Az egyszerű hozzáférés-védelem azt jelenti, hogy a számítógép használatához szükség van a kártyára. A gép bekapcsolásakor, tehát még mielőtt az operációs rendszer elindul, annak login funkciójában ellenőrzik, hogy az operátor rendelkezik-e a rendszerben regisztrált kártyával. Ha nem, akkor nem is képes erről a pontról továbbjutni, maximum kikapcsolhatja a gépet.

Ha a kártyáját a rendszer elfogadta, akkor dolgozhat, mint egy nyílt rendszeren.

Ugyanezen védelem egy kicsit bonyolultabb változatában az operációs rendszer folyamatosan vagy beállított időközönként figyeli a kártya jelenlétét, és amennyiben azt kihúzzák az olvasóból, blokkolja a gépet, míg az vissza nem kerül.

A kártya mint hozzáférés-védelmi azonosító

Ilyen alkalmazáshoz elméletileg egyedi sorszámmal rendelkező dumb kártya is elég lehet, mivel a gép nem vár el a kártyán tárolt adatot vagy pláne intelligens működést. A gépen található adatbázis tartalmazza a jo-

gosult kártyák sorszámát, a beolvasásnál elég összevetni, hogy a prezentált kártya száma szerepel-e a listán.

Arra, hogy egy ilyen rendszerbe behatoljunk, sokféle lehetőségünk van. Egy triviális verzió, hogy magát a hozzáférést korlátozó szoftverelemet eltávolítjuk vagy kikerüljük. PC esetében tipikus probléma, hogy floppyról indítjuk a rendszert, és így a DOS (Win95, NT stb.) olyan változatát indíthatjuk el, amelyben nincs installálva a védelem, és nyíltan hozzáférhetünk a fájlrendszerhez, benne a védeni kívánt programokhoz, adatokhoz. Önmagában az sem mindig elegendő, hogy nincs a gépben olyan cserélhető eszköz (floppy, CD, Zip-drive), amelyről az operációs rendszer indítható, ha a támadó szétszedheti a gépet. Hiszen akkor kiegészítheti a szükséges komponensekkel, vagy egyszerűen elviheti belőle az adathordozót otthoni leolvasásra.

Ha a gépet az előbbiek ellen védettnek tekintjük, a következő támadási felület a kártya csatolója. Ez sok esetben szabványos RS-232 bemenethez illeszkedik. Ezt a kapcsolatot könnyűszerrel le lehet hallgatni (ha történetesen nincs kémkábelünk, elég egy laptop két soros porttal, amelyet közbeiktatunk, és rajta egy pár soros, akár BASIC-ben megírható programmal, amely olvassa a két portot, a forgalmat fájlba írja, és továbbküldi). Ha a kártyáról statikus dolgot olvasunk le (olyasmit, mint a sorozatszám), az adatforgalom minden esetben azonos lesz. Ha ezt egyszer sikerült lehallgatni, az előző berendezéssel bármikor vissza is játszhatjuk a dolgot, a kártyaolvasót kiválthatjuk egy emulátorral, amelyet a gép nem fog tudni az igazi olvasótól megkülönböztetni. Védekezésképpen feltétlenül építsük az olvasót a gépbe, és a soros portra is közvetlenül a gépen belül csatlakoztassuk.

Védett olvasó esetén a támadó kénytelen magát a kártyát emulálni. Ne felejtsük el, hogy egy egyébként lemásolhatatlan smart kártya is csak néhány elektromos csatlakozón keresztül kommunikál az olvasóval, elméletileg hozzáférhető protokollt használva, így magát a kártyát is lehet emulálni. Például akinek régebb óta van dekóderes műholdvevője, jó eséllyel rendelkezik egyszerű kártyaemulátorral, melynek elkészítése mindössze néhány ezer forintba kerül. Ennek egyik végén kártyacsatlakozó található, a másikat egy PC soros portjára kell kötni, és persze megfelelő programmal kell a kártyát emulálni. A PC-k mellett zömmel fellelhető kártyaolva-

sók sajnos lehetővé teszik az emulátorkártya használatát. Komolyabb kártyafelhasználó rendszereknél ez ellen úgy védekeznek, hogy a kártyát nem közvetlenül az érintkezőhöz kell dugni, hanem azt a készülék „lenyeli", és egy speciális mechanika juttatja az olvasóhoz. Így ténylegesen csak egy plasztikkártyát használhatunk, drótok nélkül. Ha ráadásul az ilyen olvasó nem is adja vissza a nem megfelelőnek talált kártyákat, a speciálisan kémlelésre létrehozott smart kártyák ellen is védekezhetünk.

Ha nincs az előbbieknek megfelelő olvasónk, akkor dumb kártyát nem célszerű alkalmazni. Smart kártyából olyat kell választanunk, amely képes rejtve kiadni a benne lévő információt. Mondjuk a kártya egy X számot őriz, amelynek értékét nem lehet közvetlenül kiolvasni. Az olvasó egy véletlenszerűen generált Y számot küld a kártyának. A kártya egy egyirányú függvényt hajt végre az X és Y számmal, s visszaadja az eredményt. A lekérdező szintén elvégzi ezt a függvényt a nála jogosultként szereplő X számra és az általa adott Y-ra. Ha valamelyiknél az eredmény egyezik, akkor a kártya jogosult. Ha a függvény ténylegesen egyirányú (az eredmény és Y ismeretében X nem kiszámítható), és X, Y, valamit az eredmény tartománya elég nagy ahhoz, hogy végig lehetne próbálni az összes lehetséges esetet, akkor sikerül kivédeni a visszajátszásos támadást. A lehallgató hiába kezdemnyezi a gép és a kártya közötti kommunikációt, azzal nem megy semmire, amíg az újabb lekérdezéseknél mindig más Y érték szerepel a rejtvényben.

Ez a rendszer már elég kikezdhetetlennek tűnik, de itt is figyelni kell további szempontokra. Rögtön az egyik, hogy a jogosult X értékeket a lekérdező szoftverben biztonságosan kell őrizni. A kártyáról mondtuk, hogy onnan az értéket nem lehet kiszedni, de ugyanez a követelmény áll az ellenőrző szoftverre is. Hiszen ha X értéke ismeretes, az emulátor elvégezheti ugyanazt a műveletet, mint a kártya. (Egy másik lehetőség az, hogy a függvény titkos, de ez ugyanúgy kiolvasható, izolálható a szoftverből, mint az X értékek, viszont sokkal nehezebben védhető, hisz vélhetően sok rendszer használja ugyanazt a függvényt.) Ezt a táblázatot az operációs rendszer olyan területén kell elhelyezni, amelyhez a felhasználónak nincs hozzáférése (a kártyával belépett, jogosult felhasználónak sem). Egy belépő különösen a többi jogosult használó titkos értékeihez nem férhet hozzá.

Egy érdekes további lehetőség a behatolásra, ha ugyanaz a kártya több gépen is jogosult. A közbeiktatott emulátor nemcsak a kártyát emulálhatja a gép felé, hanem a gépet is a kártya felé. Ekkor elképzelhető, hogy a felhasználó a valódi kártyával éppen belépett az A gépen, a támadó pedig kezdeményezi a belépést B-n. A gép megadja az aktuális rejtvény Y számát. Ezt az emulátor megüzeni az A gépen lévőnek, amelyben még ott a kártya. Az emulátor olyan beszélgetést kezdeményez, mintha egy gép lenne ezzel az Y számmal. A kapott megfejtést visszaüzeni a B gép emulátorának, ahol így sikeresen be lehet lépni.

Rejtjelezés

A rejtjelezés egy olyan művelet, amellyel adatainkat illetéktelenek számára hozzáférhetetlen formára alakítjuk. Az előzőekben ismertetett hozzáférés-védelmi rendszer legfőbb gyengéje, hogy könnyen kiiktatható. Lehet, hogy elég egy bootlemez, és adataink ott vannak bárkinek kiszolgáltatva.

Ha az adatokat eleve rejtjelezve tároljuk, akkor hiába oldotta meg a behatoló a fájlrendszerhez való hozzáférést. Ahhoz, hogy az adatokat ténylegesen elérje, szüksége van a titkosító kulcsra. Ez viszont (jó esetben) nem található meg sehol a rendszerben, kizárólag a külső eszközön, pl. a smart kártyán. Indításkor a rendszer kéri a kártyát, leolvassa róla a kulcsot, és a továbbiakban ezzel dolgozik. A konkrét alkalmazástól függően elképzelhető, hogy az indításkor minden adat megfejtésre kerül; a munka ezek után úgy folyik, mintha kriptográfia egyáltalán nem is szerepelne a rendszerben, a nap végeztével pedig az állományok újra titkosításra kerülnek. Egy másik módszer, hogy a titkosítás beleépül a fájlolvasó és -író műveletekbe, vagy esetleg az egész fájlrendszer diszken lévő reprezentációja mindenestül titkosított.

A titkosításhoz (persze az adaton kívül) két fontos dolog kell. Egyrészt egy eljárás, másrészt a kulcs. Az eljárás maga is lehet titkos, ami elvileg hozzájárulhat a biztonsághoz, de felvet egy kérdést is: ha nem tudjuk, hogy mi az eljárás, akkor nem is tudjuk megvizsgálni, hogy az jó-e. Meg kell bíznunk az eljárás szállítójában. Ez pedig nem biztos, hogy jó ötlet: miért viseljük mi annak a kockázatát, hogy esetleg mások elnéztek vala-

mit, vagy éppenséggel lehet, hogy szándékosan „kamut" adnak el, amelyet maguk (vagy a szállító cég területe szerint illetékes hatóságok) rutinszerűen olvasnak. A nyilvános eljárásokat használva bárki otthon is megpróbálkozhat az adataink megfejtésével, széles körű irodalmi támogatással, de ugyanez az anyag nekünk is rendelkezésünkre áll. Ha egy eljárásról évek, évtizedek alatt nem derült ki, hogy rutinszerűen megfejthető (vagy precízen becsülhető a feltörés költsége és időigénye), akkor ezt mérlegelhetjük a konkrét alkalmazás tekintetében. Ha az eljárás gyengeségei ismertek, azok kiküszöbölésére fel tudunk készülni. S ha a módszer tényleg jó, akkor annak ismerete a feltörésben nem jelent komoly segítséget a kulcs nélkül. Adataink biztonságát tehát a kulcs titkossága fogja biztosítani.

A titkosításokat a kulcshasználat alapján két fontos csoportra osztjuk: szimmetrikus (egykulcsos) és aszimmetrikus (kétkulcsos) rendszerekre.

A szimmetrikus rendszerben egyetlen titkos kulcs van, ez szolgál az adatok titkosítására és megfejtésére. Ha a titkosító és a megfejtő nem ugyanaz a személy, akkor mindkettőnek rendelkeznie kell ugyanazzal a kulccsal, és egy eleve biztonságos csatornán azt egyeztetniük kell. Egyes esetekben sok szereplőnek kell hozzáférnie ugyanazokhoz az adatokhoz, és ez sérülékennyé teheti a rendszert. Hiszen bármelyiküknél kompromittálódhat a kulcs, és akkor a támadó hozzáfér az egész titkosított adattömeghez. Ami még rosszabb, hogy mivel mindenki azonos kulcsot használ, nem is lehet tudni, ki a felelős a nyilvánosságra kerülés miatt.

Az aszimmetrikus rendszernél egyetlen kulcs helyett kulcspár készül. Az egyik kulccsal rejtjelezett anyagot a másikkal lehet megfejteni, és viszont. A kulcspár egyik tagja lesz a titkos kulcs, a másik a nyilvános. Az alkalmazás érdekes, irányfüggő rejtjelezést tesz lehetővé: a nyilvános kulcsot oda lehet adni minden egyes partnernek, aki ezt használja üzenetei titkosítására. A megfejtésre viszont csak a titkos kulcs birtokosa képes. Ezt célszerűen egyetlen félre lehet bízni, így kompromittálódni is csak az ő hibájából lehet. Sajnos a jelenleg ismert, megbízható aszimmetrikus eljárások igen lassúak, így nagy tömegű adat titkosítására nem alkalmasak. A probléma feloldására szimmetrikus eljárással kombinálhatók: a nagy mennyiségű adatot szimmetrikus eljárással titkosítják egy véletlenszerűen generált kulccsal. Ezek után ezt az eseti kulcsot (session key) titkosítják az aszimmetrikus eljárással. Ha több végpontnak kell képesnek lennie

a megfejtésre, akkor az eseti kulcsot mindegyikük nyilvános kulcsával rejtjelezik, és a titkosított üzenettörzzsel együtt elküldik ezeket a kulcsblokkokat. Aki rendelkezik a megfelelő titkos kulccsal, meg tudja fejteni a saját blokkját és utána az abban talált kulccsal az üzenetet. A tisztán szimmetrikus eljáráshoz képest itt előny az is, hogy minden üzenetet eltérő kulccsal titkosítanak, s ha egy támadó valamiképpen meg tudja fejteni egy üzenet kulcsát, a többi üzenet tartalmához továbbra sem jut hozzá.

Mivel az aszimmetrikus eljárásban használt titkos kulcsot egyetlen végpont őrzi, ez lehetőséget ad a hitelesítésre is. Ezzel az aspektussal egy későbbi fejezetben foglalkozunk. E fejezet további részében titkosítás alatt alapértelmezésben szimmetrikus eljárással végzett kódolást értünk.

A kártyás rendszerekhez visszatérve: ha titkosítva akarunk adatokat tárolni, két lehetőség adódik. Az egyik, hogy a kártyát használjuk kulcstároló eszközként, a másik, hogy a kártya végzi el az egész titkosítást/megfejtést.

A kártya mint kulcstároló eszköz

Ebben az alkalmazásban semmi mást nem várunk a kártyától, mint hogy biztonságosan megőrizzen néhány byte-nyi adatot. Maga a titkosítás a gépen történik, az egyetlen ehhez szükséges külső adat a titkosító kulcs. A titkosító eljárást tekintve abból indulhatunk ki, hogy az ismert, és ha valaki hozzájutott a titkosított adatokhoz, valamint sikerült a kártyán tárolt kulcsot is megszereznie, bármely másik gépen elvégezheti a megfejtést.

A fentiekből következik, hogy a gép és a kártya között itt biztonságos, lehallgatásmentes vonalat kell kialakítanunk. A korábbi fejezetben kifejtett rejtvény/felelet protokoll nem működik, mert itt a gépnek nem elég arról meggyőződnie, hogy a kártya ismeri a kulcsot, hanem azt ki is kell onnan csalogatnia. Méghozzá nyílt formában. Ha valaki eközben lehallgatja a gép és a kártya között zajló párbeszédet, ugyanúgy meg tudja fejteni az átadott adatokat.

Az előző állítás egy esetben nem igaz: ha a kártya és a program rendelkezik valamilyen speciális, közös ismerettel, amelyet olyan időben cserélt ki, amikor a lehallgató garantáltan nem lehetett jelen.

Az egyszerű PIN kódos kártya nem adja ki az adatokat egyszerű lekér-

dezésre. Ehhez ugyanis ismerni kell egy speciális kódot, amelyet a kártya adattal való feltöltésekor írtak fel, és csak a kártya jogos birtokosa ismer. A lekérdezés előtt a gépnek igazolnia kell, hogy ismeri azt. Az eljárás hasonló a hozzáférés-védelemnél tárgyalthoz, mindössze a két oldal felcserélődik, itt nem a kártya igazolja magát a gépnek, hanem fordítva. Ha a gép sikeresen válaszolt a kártya által feladott rejtvényre, akkor a kártya kiadja a titkos adatot. (A smart kártyák egy része csak nyíltan, lehallgatható módon képes a PIN vételére – a választásnál ne feledkezzünk meg erről!) A lehallgató nem lesz képes önállóan igazolni magát a kártya felé (vagyis más alkalommal kiolvasni a tartalmát), viszont megvárhatja, amíg azt a gép egyszer megteszi, és megjegyzi magát a titkolandó adatot, mihelyt azt a kártya kiadja.

Ahhoz, hogy a lehallgatást megakadályozzuk, a titkos adatokat a kártyának nem szabad nyíltan kiadnia. Mivel a gép és a kártya rendelkezik egy közös tudással, amely nem jelenik meg nyílt formában a kommunikációban, ezt használhatják szimmetrikus titkosító kulcsként. Ha a kártya ezzel rejtjelezi a kiadott adatot, a gép meg tudja fejteni, a lehallgató viszont nem, hiszen ő az eredeti azonosítóval soha nem találkozik, csak annak kiegészített és egy irányba konvertált változatával.

Természetesen a gépet is védeni kell az eljárás alatt (és után!), hiszen hiába fáradozunk a kártyával, ha a beolvasott kulcs egyszerű eljárással kinyerhető a gép memóriájából, vagy a tulajdonos által beütött azonosító leolvasható a billentyűzetről, illetve a képernyőről. Azt se feledjük el, hogy a kártyán tárolt kulcs hosszú távú, és a támadónak elég egyszer ellopnia, attól kezdve kedvére „kriptózhat" ki és be.

A kártya mint titkosító eszköz

A másik lehetőségünk, hogy a titkosítást szőröstül-bőröstül a kártya végzi el. A titkos kulcs és a titkosító eljárás egyaránt a kártyában foglal helyet (az utóbbi lehet akár nem nyilvános eljárás is), a gép csak a nyílt adatokat küldi a kártyára, ahonnan visszakapja a titkosított megfelelőt, vagy a tikosított anyagot küldi, s visszakapja a nyíltat.

Az eljárás nagy előnye, hogy gyakorlatilag nem utánozható. Ha a kártya nincs jelen, semmilyen lehetőség nincs kriptográfiai funkciók végzésére.

A kártya felélesztését természetesen célszerű itt is valamilyen ismerethez, PIN-hez kötni, amelyet a kártya irányába (jó esetben lehallgatásbiztosan) igazolni kell a működés elindításához.

A lehallgatással kapcsolatban viszont gond lehet, hogy a gép–kártya kommunikációban megjelennek maguk az elrejtendő adatok, nyílt formában.

Hitelesítés

Az adatok hitelesítése két dolgot takar. Az egyik, hogy maga az adatállomány nem változott. A másik, hogy igazolja a hitelesítést végző személyét.

Hitelesítéshez többnyire az aszimmetrikus titkosítást használjuk. Az eljárást nagy vonalakban a titkosításról szóló fejezetben ismertettük. Az ott elmondottak szerint a küldött anyag titkosítását a nyilvános kulccsal végezzük. Így a megfejtést a titkos kulccsal rendelkező egyetlen személy tudja majd végrehajtani. A dolog megfordításával eljutunk a hitelesítéshez: ha egy anyagot a titkos kulccsal titkosítanak, akkor azt a nyilvános kulccsal lehet megfejteni. Ha találunk egy anyagot, amely egy nyilvános kulccsal megfejtve előállít egy dokumentumot, biztosak lehetünk benne, hogy az anyag titkosítását csak egyvalaki végezhette el, aki rendelkezett a szükséges titkos kulccsal.

Mint említettük, az aszimmetrikus eljárással végzett rejtjelezés igen lassú. Ezért egy egész adatállomány ilyen módon való rejtjelezése nem megoldható. Szerencsére léteznek olyan eljárások, amelyekkel a dokumentumról megbízható „lenyomat", úgynevezett message digest készíthető. A digest egyirányú eljárással készül az adatállományból. A dokumentum megváltoztatása átalakítja annak digestjét is. Matematikailag tudjuk egy jó eljárásról, hogy értelmes idő alatt nem kalkulálható egy választott digesthez tartozó adatállomány, sem két olyan adatállomány, amelynek digestje megegyezik. Természetesen léteznek olyan különböző üzenetek, melyek azonos eredményre vezetnek, hisz a digest fix hosszúságú (tipikusan 128 vagy 160 bit), és az összes létező (végtelen számú) üzenet erre a 2n számú digestre van leképezve. De az ilyen párokat gyakorlatilag nem lehet megtalálni.

A hitelesítés az előbbiek figyelembevételével úgy történik, hogy elkészítjük egy dokumentum digestjét, és titkosítjuk a hitelesítő személy titkos kulcsával. (A gyakorlatban a digest mellé még más információkat is el szoktak helyezni, pl. az aláírás idejét, a szabad helyeket pedig megfelelően feltöltik.) Így kapunk egy elektronikus aláírást, amelyet a dokumentum mellett tárolunk. Ha ellenőrizni kell a hitelességet, akkor egyrészt a dokumentumból újra elkészítjük a digestet, másrészt a feltételezett aláíró nyilvános kulcsával megfejtjük az aláírást. Ha a megfejtett aláírásban szereplő digest megegyezik a frissen képzettel, az igazolja, hogy a dokumentum változatlan, és az aláírást a használt kulcs párjának tulajdonosa végezte.

Meg kell említeni, hogy az aszimmetrikus rendszerben külön problémát vet fel a nyilvános kulcsok hitelesítése. Ezeket nem kell titkosan kezelni, természetükből adódóan azokat minden résztvevőhöz el kell juttatni. Viszont gondosan ügyelni kell arra, hogy az adott kulcsok és a hozzájuk tartozó azonosítók ne változhassanak. Tegyük fel, hogy Anna talál egy üzenetet, amelyet Béla írt alá, és ellenőrzi. Az adatbázisában megtalálta Béla kulcsát, a fent írt eljárással minden stimmel. No de honnan lehet tudni, hogy Béla kulcsa az adatbázisban valóban Béla kulcsa? Esetleg Hugó, a hamisító generált magának egy kulcspárt, és elhelyezte azt az adatbázisban Béla neve alá. Ilyenkor a Hugó által készített aláírások bizonyulnak majd jónak, sőt a Bélának címzett üzeneteket Hugó fogja tudni megfejteni. És ha rendelkezik Béla eredeti kulcsával, akkor a megfejtett és elolvasott üzeneteket titkosíthatja, s továbbküldheti Bélának. A problémák megoldása végett a nyilvános kulcsokat tartalmazó adatbázist hitelesíteni kell saját kulcsunkkal vagy egy megbízható harmadik félével. E kulcsok ellenőrzést szolgáló nyilvános részét pedig valamilyen megbízható, módosíthatatlan médiára kell helyezni.

A kártya mint hitelesítő eszköz

Ha a chipkártyát hitelesítésre akarjuk használni, gyakorlatilag ugyanazok a problémák és megoldások vetődnek fel, mint amelyeket a titkosításnál tárgyaltunk. Ez, ugye, nem igazán meglepő, hisz valójában a hitelesítés is titkosítás, csak más kulccsal és algoritmussal.

Ha a kártya csupán tárolja a kulcsot, semmi eltérés nincs a titkosításhoz képest, mindössze a beolvasott kulcs mérete lesz nagyobb.

Ha olyan intelligens kártyánk van, amely maga végzi az aláírást, akkor már két eset lehetséges. Vagy az eredeti (dokumentumszintű) adatokat küldjük a kártyára, és az kiszámolja a digestet, összeállítja az aláírásblokkot, s elvégzi a konverziót a titkos kulccsal. A másik lehetőség, hogy a gépen magunk csináljuk a digestet és a blokk kitöltését, a kártya ezt kapja inputként, s csak a titkos kulccsal való titkosítást végzi.

Léteznek kombinált rejtjelező-hitelesítő kártyák, amelyek az adatokat egy menetben titkosítják a kártyán generált, onnan ki sem kerülő eseti kulccsal, közben pedig elkészítik hozzá az aláírást és a titkosított kulcsblokkokat.

A kártyák perszonalizálása

Mielőtt a kártyát odaadnánk a tulajdonosának, fel kell töltenünk a rendszerre és a személyre szabott adatokkal. Ezzel egy időben nyilvántartásba kell vennünk azokban az adatbázisokban, amelyek az elfogadható kártyákat lajstromozzák, és azokhoz személyes információkat, hozzáférésjogokat stb. rendelnek.

A perszonalizálásról általánosságban nehéz beszélni, hiszen ahány kártya, rendszer és funkció, annyiféleképpen történhet. Egyes kártyák csak egyszer írhatók. Másokon területeket lehet konfigurálni, amelyek különböző kódok megadása esetén (vagy éppen kód nélkül, szabadon) írhatók, olvashatók, törölhetők. A jelszóvédelemmel rendelkező kártyákon elérés-nyilvántartó (access tracking) zóna is szokott lenni, amelyből kiderül, hogy hányszor adtak meg jó és rossz jelszót. Ha ez a zóna nem íródik felül automatikusan, a méretével korlátozhatjuk a kártya használatát: minden hozzáférés egy bejegyzést jelent a táblázatban, és ha a hely elfogy, akkor a kártya (vagy valamely területe) a továbbiakban nem használható.

A perszonalizáláskor kerülnek feltöltésre a védelmet adó kódok is. Ezek lehetnek egy- vagy többszintűek, és közülük egyesek a kártya élettartama során megváltoztathatók, míg mások nem. Többszintű kódrendszer esetén a kibocsátó és a kártya tulajdonosa külön kóddal rendelkezik. A kártya területeinek elérése ezekhez kötött, mondjuk a kibocsátó kód-

jával az adatok újraírhatók, a tulajdonoséval pedig olvashatók. Ha a kártyára személyes titkos kulcsot írunk, célszerű lehet úgy konfigurálni, hogy csak a tulajdonos tudja azt kiolvasni, a kibocsátó nem. (Viszont ha a kibocsátó törölheti, újraírhatja a kártyát, akkor az visszavonás után újrahasznosítható lesz, kiadható más személynek.)

A kártyaperszonalizáló műhelyt – különösen ha az kulcsokat is generál – szigorúan kell védeni. Mit sem ér a kártyába írt titok, ha azt már a keletkezése pillanatában ellophatják! Általában javasolható, hogy erre a célra alkalmazzunk szóló, hálózatba nem kötött gépet, esetleg laptopot, amely két használat között páncélszekrénybe van zárva. A gép és annak perifériái közé csatolható kémlelő készülékekre, valamint a gépen futó szoftverekre különös gonddal kell ügyelni.

Többcélú kártyák

Ha egy cégen belül több különálló rendszer használ kártyát, és ezek használatában azonos személyek is részt vesznek, felmerülhet az igény, hogy egy operátornak minél kevesebb fizikai kártyája legyen. Ez nemcsak kényelmi szempont, bizonyos helyeken komoly üzemeltetési problémákat vethet fel. Számos kártya automatikusan letiltja magát, ha néhányszor, esetleg csak egyszer rossz kódot adnak meg. És ha az operátor több rendszerben sokféle kártyát kénytelen használni, komoly az esélye, hogy nem a megfelelő kártyát helyezi be, vagy meg van győződve róla, hogy az olvasóban éppen valamelyik kártya található.

Az érem másik oldala természetesen a biztonság. Hiszen nem szabad kényelmi szempontok miatt egyszerűsíteni, ha fennáll a veszély, hogy áthallás következhet be. Különösen akkor jelent ez gondot, ha az egyes rendszerek biztonsági szintje jelentősen eltér. A közös használattal esetleg egy lazább rendszeren keresztül lehet egy szigorúbb adatait elcsenni. Mindenképpen helytelen lenne, ha az összes rendszer adatát a kártya ugyanazon területén akarnánk tárolni, ugyanazzal a kóddal védve.

Léteznek olyan kártyák, amelyekben hierarchikus zónarendszert lehet konfigurálni. Ezt úgy képzelhetjük el, mint a DOS vagy a Unix könyvtár- és fájlstruktúráját. Az egyes könyvtárakhoz önálló kódok és elérési jogok

rendelhetők. Ha megfelelően konfiguráljuk, akkor ez a kártya olyan, mintha egy pakli kártya lenne, az egyes mezők egymástól teljesen elszigeteltek. Így ha megköveteljük a ténylegesen különböző kódok használatát, már csak a kártya fizikai jelenlétével kapcsolatos aggályok merülnek fel.

Azt a szempontot is mérlegelni kell, hogy minél több rendszerben használjuk ugyanazt a kártyát, az annál többet van „elöl", nagyobb esélyel tudja egy illetéktelen megszerezni. Különösen igaz ez, ha egyes rendszerek a kártya jelenlétét folyamatosan megkívánják. Ekkor könnyen előfordul, hogy az operátor bennhagyja az olvasóban, laza felügyelet mellett. Másvalaki észrevétlenül kiveheti, és beléphet vele egy másik rendszerbe. Ha külön kártyákat használunk, könnyebben megkövetelhető lehet, hogy használaton kívül a kártyát biztonságos helyen tárolják.

A kártyakezelés biztonságának szoftveroldala

Mielőtt ténylegesen rátérnének a kártyával kapcsolatos dolgokra, elengedhetetlen, hogy szót ejtsünk néhány általánosabb dologról.

A biztonság alapja

Ahogy házat sem építünk homokra, a biztonságot is szilárd alapra kell helyezni, amelyre támaszkodhat. A „trusted base" (a továbbiakban TB) tartalmazza mindazon eljárásokat, bevizsgált programokat, feltételezett körülményeket, amelyeket minden más biztonsági szempont értékelésénél adottnak tekintünk.

Példaként nagy vonalakban összefoglalva: egy C2 biztonsági minősítésű Unix-rendszer esetében a TB tartalmazza a programok közül a kernelt és a loginprogramot, a feltételezések között pedig azt, hogy az adott gép fizikailag sérthetetlen, azon kizárólag ez az operációs rendszer indítható, a rootjogokkal rendelkező személy megbízható, egy-egy felhasználó jelszavát csak ő ismeri, és betartja a belépési protokollt. Ha mindezek a feltételek teljesülnek, akkor megvalósul mindaz, amit a C2 szint ígér: az egyes felhasználók kizárólag a kiosztott jogaik szerint érhetik el a rendszeren található entitásokat, és a tevékenységük megbízhatóan

naplózásra kerül. A rendszeren belülről a felhasználó nem képes többletjogokat szerezni vagy elkerülni saját nyomkövetését. Hasonlóan a rendszeren belülről nem lehet észrevétlenül ellopni a felhasználó jelszavát sem. A belépéssel kapcsolatos procedúra tartalmazza a jelszavak megválasztásának korlátjait, azok maximális használhatósági időtartamát és a belépőtől megkívánt figyelmet, hogy ellenőrizze a belépés után kiírt utolsó sikeres és sikertelen belépés időpontját.

Lássuk, hogy mit jelent ez a gyakorlatban! Találok egy fentiek szerinti gépet, és szeretnék behatolni, elvinni mások adatait. A gépet szétszedni nem tudom, a bekapcsolás után az eredeti kernel és az eredeti loginprogram indul. Mielőtt bármi egyebet tehetnék, meg kell adnom egy érvényes felhasználónevet és egy jelszót. Ezek hiányában egyáltalán nem léphetek tovább. Menjünk tovább úgy, hogy jogosult használója vagyok a rendszernek, és próbálok idegen eszközökhöz hozzáférni. Ekkor továbbjutok a loginon, és immár programok széles körét indíthatom el. A login révén viszont azonosításra kerültem, és az azonosítómat minden általam indított folyamat viseli. A kernel pedig minden egyes entitásnál, amelyhez hozzáférést kérek, ellenőrzi, hogy az én azonosítómmal elérhető-e. Így ha ezzel próbálkozom, a rendszer megtagadja a kiszolgálást, és a naplóban rögzíti a kísérlet tényét. Amire egész biztosan ügyelni kell a rendszerben: a TB részeire felhasználói szinten nem lehetnek olyan jogosultságok, amelyek lehetővé teszik annak módosítását. Képzeljük el, mi történne, ha módosítani tudnám a loginprogramot vagy annak adatállományait: ezzel tetszőleges jogosultságokat rendelhetnék magamhoz. A kernel módosításával pedig kikapcsolhatnám az ellenőrzést.

Maradék lehetőségeim már igencsak korlátozottak: megpróbálhatok még csapdát állítani egy másik felhasználónak. Olyan programot futtatok, amely a loginprogramnak álcázza magát, persze amennyire teheti. Bekéri a nevet és a jelszót, ezt elmenti, majd megpróbálhatja a felhasználó által végzett tevékenységet utánozni – ez, mivel a program a kurrens jogaimat használja, aligha fog menni –, vagy kilép, mintha a jelszó rossz lenne, és elindítja az eredeti logint, ahol a felhasználó belép. A dolog ott fog kiderülni, hogy a normál login a belépés után kiírja az utolsó sikeres és sikertelen belépés időpontját, és a belépő kötelessége észrevenni, hogy az utolsó sikertelen belépés kiírt időpontja nem egyezik meg

a néhány pillanattal azelőtti idővel. Amit azonnal jelent a rendszergazdának vagy a biztonsági felelősnek. A támadónak eleve rövid idő áll rendelkezésre az ellopott jelszó használatára, amíg azt be nem fagyasztják, de ami fontosabb, a naplóból pontosan kiderül, hogy ki volt az, aki a jelszót ellopta.

Lényeges dolog az is, hogy a belépéshez szükséges titkos elemek nem jelennek meg a felhasználószintű memóriában. Ha pl. a jogosult operátor felügyelet nélkül hagyja a terminált, amelyen belépett, egy arra járó hozzáférhet az illető adataihoz (a pillanatnyi lehetőség korlátjai között), de nem szerezheti meg a jövőbeni belépéshez szükséges információt, amellyel a hozzáférési időt tetszés szerint kiterjeszthetné.

Összefoglalva: láthatjuk, hogy amíg a TB (amúgy elég drasztikus) feltételei teljesülnek, rendszerünk megvalósítja a megcélzott biztonságot. Ezzel szemben, ha nem definiálták a TB-t (sajnos meglepően sok rendszernél ez a helyzet), akkor a biztonság a levegőben lóg, ha úgy tetszik, semmiféle biztonságról nem beszélhetünk, függetlenül attól, hogy milyen drága vagy „biztonságosnak tekintett" eszközöket használunk. Az idézőjel persze önmagában is komikus, hiszen egy eszköz biztonsága magában soha nem értékelhető, csak a TB-vel való relációjában.

A chipkártya integrálása a rendszerbe

A legokosabb smart kártya is csak szoftveren keresztül használható. Így a kártya biztonsági vonatkozásait ki kell terjesztenünk a kártyával kapcsolatot tartó szoftverre, illetve annak a rendszer többi részével (különösen a TB-vel) való kapcsolatára.

Chipkártyakezelés a meglevő TB részeként

Ehhez a megvalósításhoz a meglevő TB valamely szoftverelemének módosítása szükséges, mondjuk a kártyakezelőt a kernelbe vagy a logint végző programba integráljuk. Pl. hozzáférés-védelemre használt kártya esetén a login nemcsak jelszót kér, hanem egy regisztrált kártya meglétét is ellenőrzi. Vagy ekkor olvassa be a titkosító kulcsokat.

Helyes megvalósítás esetén természetesen ez egy nagyon jó módszer. Sajnos beszélni róla sokkal egyszerűbb, mint megvalósítani. Ne felejtsük el, hogy amennyiben bármilyen apró módosítást végzünk a TB-n, az

egészet újra kell minősíteni. Ehhez a kombinált módszerhez olyan minősítőre van szükség, aki képes mind az eredeti rendszer, mind az újonnan beültetett részek vizsgálatára. Ha mellőzzük ezt az újraminősítést, akkor nemhogy megerősítenénk a rendszert, de aláássuk a TB-t és ezzel az egész rendszert.

Viszont ha sikerült ez a megvalósítás, akkor a kriptográfiai funkciók támaszkodhatnak a rendszer által nyújtott védelemre. A kártyákról szóló fejezetben számos gépben őrzött kódról mondtuk el, hogy az titkosan kezelendő: ennek megvalósítása nem jelent különösebb problémát, hisz a TB szintjén ugyanez a követelmény számos más elemre is áll. A nyilvánoskulcs-adatbázis is tárolható a rendszeren egyszerű, csak olvasható fájlként.

Chipkártyakezelés a meglevő TB kiegészítéseként

Itt az integrálást úgy próbáljuk elvégezni, hogy a meglévő biztonsági szoftvereket nem módosítjuk, csak köréjük egy újabb héj kerül, amely az új funkciókat végzi. A minősítést itt sokkal egyszerűbb véghezvinni, hiszen az elsősorban az új részekre terjed ki, az eredeti rendszer minősítőitől csak annyit várunk el, hogy értékeljék, az új kiegészítés nem használ-e tiltott dolgokat, amelyekkel alásható a régi biztonsága. (Például ha a program egy része kernelszinten fut, lehet benne olyan kívülről meghívható funkció, amely a kernelszintű memória tetszőleges részét beolvassa. Ez természetesen nem megengedhető.)

A kiegészítés persze csak akkor lehetséges, ha az eredeti rendszer biztosít erre megfelelő lehetőségeket. Például ha a felhasználói login konfigurálható úgy, hogy a sikeres belépés után a belépő által nem módosítható módon konfigurált program indul el (shell, loginscript stb.), akkor ebbe helyezhetünk olyan funkciókat, amelyek a további működést meghatározzák. Amennyiben ezen a ponton még nincs lehetőség tetszőleges programok indítására, ez a kiegészítés akár felhasználói szinten is futhat. (Vegyük észre, hogy ebben az esetben a meglevő TB teljes egészében érintetlen!) Mondjuk, hogy a loginscriptben történik a kártya lekérdezése, és ha sikertelen, az azonnali kilépést von maga után. Ne felejtsük el, hogy ilyen módon rezidensen működő dolgokat általában nem implementálhatunk, csak olyat, amely a sikeres bejövetel után eltűnik. Ha

a rendszerhasználat teljes idejében jelen kell lennie, akkor már nagy valószínűséggel a kernelhez közelebbi szinten kell futnia, amelynek memóriája a felhasználó által indított programokból nem hozzáférhető. Természetesen a kiegészítőknek a TB más szoftverrészeihez hasonlóan felhasználói szintről módosíthatatlannak (és célszerűen olvashatatlannak) kell lenniük.

Ezzel és az előző pontban körülírt módszerrel (hangsúlyozottan helyes megvalósítás esetén) többletbiztonságot érhetünk el az eredeti rendszerhez képest, az eredeti biztonsághoz a kiegészítések által nyújtottak hozzáadódnak.

Chipkártyakezelés a TB-től függetlenül

Az előbbiek tekintetében felmerül a kérdés, hogy mi értelme ennek a fejezetnek, hiszen már leírtuk: a TB-től függetlenül semmiféle biztonság nem értelmezhető. Ez így igaz, ám ennek ellenére a gyakorlatban számos ilyen alkalmazással találkozunk. Ezért most arra mutatunk be néhány példát, hogy itt miért csak látszólagos a többletbiztonság.

Vegyünk alapul egy olyan alkalmazást, amely Win95 alatt fut, és egy titkos adatbázist kezel. Az adatbázishoz való hozzáféréshez egy chipkártyát használ, amelyről egy titkosító kulcsot olvas be. Az adatbázisnak csak a képernyőn megjelenő részét fejti meg, a módosításokat pedig titkosítva írja vissza. A kártya kihúzását érzékeli, és azonnal kilép.

Az adatok látszólag biztonságban vannak: a diszken sohasem találkozunk velük nyílt formában, a megfejtés és módosítás pedig elképzelhetetlen a kártya nélkül. A probléma ezzel az állítással ott van, hogy feltételeztük az operációs rendszer és a futó program biztonságos voltát. Holott éppen ez hiányzik. A Win95 rendszerben (amely itt csak ad hoc példa, számos más rendszer is szerepelhetne helyette) mind a kernel állományai, mind a memória védtelen. A felhasználó számára észrevehetetlenül a rendszerrel egy időben elindulhatnak olyan kémprogramok, amelyek megjegyzik a memória változásait, a portforgalmat, a billentyűzetleütéseket vagy bármi egyebet. És a rendszerre installált szoftverkomponensek – beleértve az operációs rendszert és a példaként szerepeltetett biztonsági alkalmazást – szintén észrevehetetlenül módosíthatóak. Nem jelent különösen nagy gondot a program kulcsbeolvasó részének izolálása, és né-

hány byte-nyi módosítással a kulcsot kiírhatjuk egy rejtett fájlba, ahonnan utóbb begyűjtjük. Vagy ha a rejtjelezéshez magát a kártyát használjuk, akkor rögzíthető a program által a kártyán végzett kommunikáció. Vagy a kalózrész megvárja, amíg a jogos használó inicializálta a kártyát a jelszó megadásával, majd magához ragadja a kommunikációt, és a teljes adatbázist elküldi a kártyára megfejtésre. A program mellett be lehet költözni a Win95 memória- vagy fájlkezelő funkcióiba, illetve a sorosport-meghajtóba, amelyre a kártyát csatoltuk.

Így egy ehhez hasonlóan homokra épített alkalmazás csak azok ellen véd, akik nem kíváncsiak az elrejtett dolgokra. Őket viszont sokkal olcsóbb és egyszerűbb módszerrel is távol lehetne tartani, amely ráadásul a jogosult kezelők mindennapi munkát is kevésbé zavarná.

Az előző problémák ellen védekezésképpen kitalálhatnák, hogy a program, mielőtt elindul, ellenőrizze saját integritását. Ez sajnos olyan kísérlet, mint amikor Münchausen báró a saját hajánál fogva húzza ki magát a mocsárból: ha a támadó képes módosítani a programot, akkor az ellenőrző részt is képes módosítani, hogy az mindig jónak találja magát. Az ellenőrzést valamilyen korábbi pontra kell helyezni. Mivel említettük, hogy a kémdolgokat az operációs rendszer elemeibe is helyezhetjük, az ellenőrzőt valahová a Win95 betöltése elé kell tennünk. Ráadásul olyan helyre, amelyet utólag nem lehet felülírni. Mondjuk egy írásvédett floppy tartalmaz egy szoftvert, amely ellenőrzi a merevlemezen levő programokat, majd elindítja az operációs rendszert.

Vegyük észre, hogy ezzel tulajdonképpen bevezettük a trusted base fogalmát. Egészen megbízhatónak persze csupán a floppyn levő saját programunkat tekinthetjük, ha csak ezt volt módunk megvizsgálni, a betöltött Win95 esetében már mindössze arra a sejtésre hagyatkozhatunk, hogy a betöltött operációs rendszer önmagában helyesen működik, és nem tartalmaz beépített kémfunkciókat. (Kevesen gondolnak például a virtuális memóriakezelőre mint beépített kémre. Az operációs rendszer a memória bármely darabját számunkra láthatatlanul kiírhatja a swap fájlba a benne levő elrejtendő adatokkal, titkos kulccsal stb.!) További probléma, hogy a rendszeren ettől kezdve csak az ellenőrzött és biztonságosnak hitt programokat szabad elindítani. Ha csupán egyetlen nem megbízhatót elindítunk, akkor az a működés teljes további biztonságát

veszélyezteti, egészen az újraindításig. Ezek a korlátozások pedig nagyon nehezen tarthatóak be, ha pedig mégis, a rendszer felhasználóbarát voltát nagyon nagy mértékben csökkenthetik.

Összefoglalva megállapíthatjuk, hogy a TB hiányában alkalmazott biztonságerősítők nem növelik jelentősen a biztonságot, a legokosabb smart kártyák alkalmazása esetén sem.

A smart kártyák piacának vélhető trendjei 2000-től 2004-ig

Az elkövetkező években a kártyás innovációk hangsúlya a szolgáltatások, a rendszerek fejlesztésére tevődik át, mert a technológia fejlődése megelőzte az alkalmazásokét.

Piaci szegmens, alkalmazások

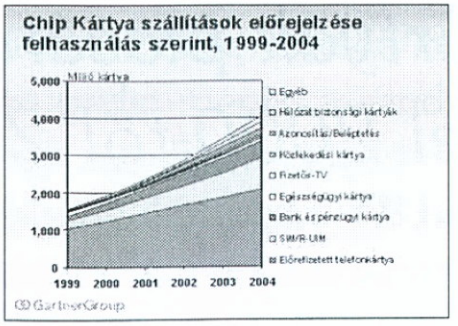
Az 1999-es 1,58 milliárdos chipkártyapiac a Gartner Group és a Dataquest elemzése szerint 2004-re mintegy háromszorosára, 4,12 milliárd egységre bővül. Ez évi 21%-os növekedést jelent. Az időszak alatt a telefon- és a SIM kártyák, valamint a pénzügyi alkalmazások kártyái maradnak a piacvezetők.

A SIM és a telefonkártyák piacának fejlődése lesz a legnagyobb hatással a technológiára. Már megfigyelhetők azok a tendenciák, amelyek e szegmens és más piaci igények konvergenciáját mutatják.

A pénzügyi szektor kártyarendszerei közül a legnagyobb hatású az EMV (Europay–MasterCard–Visa) nemzetközi méretű kredit/debit smart kártyáinak bevezetése lesz. E mellett jelentőségükben a második helyen maradnak a loyalty rendszerek. Várhatóan elkezdődnek, de még nem válnak átütő sikerűvé az elektronikuspénztárca-projektek.

Az Európai Bizottság által támogatott e-goverment projektek hozadéka lesz néhány nemzeti egészségbiztosítási, személyiigazolvány- és vezetőiengedély-projekt. Szerencsés esetben elkezdődik e pilotok interoperábilissá tétele.

A különböző földrészek fejlettségüktől függően különböző kártyarendszerek alkalmazásba vételét fogják előtérbe helyezni. Ázsiában és Közép-Amerikában elsődlegesen a telefóniához kapcsolódó rendszereket alkalmazzák majd, Európában, Japánban, Brazíliában és Mexikóban a pénzügyi kártyarendszerek fejlesztését várják. Az informatikai hálózatok biztonságát nyújtó kártyás rendszerek startja Észak-Amerikában várható, majd Európában folytatódik.



Alkalmazások konvergenciája

Az alkalmazások fejlesztőinek szóló legfontosabb üzenet a különböző szektorok konvergenciája, ami már nemcsak a kutatásban, hanem a technológiában és esetenként a tőke mozgásában is utolérhető.

Az előre fizetett telefonkártyák kombinálódnak egyéb szolgáltatói (pl. parkoló-) kártyákkal, mígnem ezeket felváltják vagy a kredit/debit, vagy a SIM kártyák, esetleg azok kombinációja.

A SIM kártyák a hálózatbiztonsági pénzügyi és loyalty rendszerekhez közelednek. E kombinációk erőteljes elterjedése várható.

A loyalty kártyák szívesen szuperpolálódnak a pénzügyi, illetve azonosítási kártyákra, és viszont. Itt a kártyaszám-növekedés motorja a pénzügyi szféra lesz.

A hálózati hozzáférést szabályozó kártyák elsődlegesen az azonosítási kártyákkal léptek frigyre, de az e-business növekedésével a pénzügyi szektor is belépett a kibocsátók körébe.

Chipek műszaki paraméterei és azok alkalmazási lehetőségei

Mint korábban említettük, a félvezető-technológia fejlődése elébe ment a piaci igényeknek. A gyártók funkcionalitásban és biztonsági szolgáltatásokban többet tudnak nyújtani a jelenlegi igényeknél.

Félvezetők műszaki paraméterei	Alkalmazások lehetőségei
32 bites processzor	Lehetővé teszi nagy teljesítményű operációs rendszerek és kriptográfia alkalmazását
Java kártyák, Multos, Windows for Smart Cards	Elválaszthatóvá teszi az alkalmazásokat a kártyától
Kriptográfiai funkciók, processzorok a kártyára való elhelyezése	Lehetővé teszi RSA kulcsok alkalmazását
64 KB-nél nagyobb EEPROM	A ROM-ban tárolt operációs rendszer használatával lehetővé teszi több alkalmazás dinamikus használatát
Dual interface (ISO7816és ISO14443)	A kártyák beléptető/azonosító vagy közlekedési rendszerekkel közös használata lehetséges
Memória menedzselhetőség	A kártyához kapcsolódó különböző alkalmazások „tűzfallal" való elválasztásához szükséges
Kódolt gyártási eljárás	„Reverse-engineering" ellenállóvá teszi a technológiákat
0.3 mikron alatti gyártási eljárás	Növeli a kihozatalt és további EEPROM integrálást teszi lehetővé

A táblázatban a kártyákban használt félvezetők műszaki paramétereinek jelenlegi szintjét és az abból kihozható alkalmazásfejlesztői igényeket párosítjuk.

Irók/olvasók, kapcsolat az e-businesshez

A kártyák használata láthatóan azokban az alkalmazásokban fog alapvetően növekedni, ahol azok valamilyen nagyobb csoport részeként szerepelnek. A kommunikációs társadalom is ezeket az alkalmazásokat fogja üzletileg honorálni.

A trendek erről az oldalról való megközelítése alapvető változást jelez.

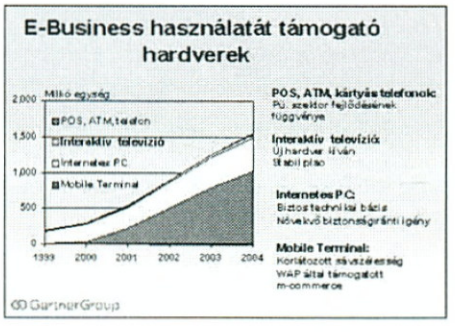
Ma a kártyák többségét bankjegykiadó (ATM), valamint fizetőhelyi (POS) terminálokban, PC-khez kapcsolt író/olvasó berendezésekben olvassák, illetve írják át tartalmukat. Ez a vizsgált időszak végére alapvetően meg fog változni.

Természetesen megmaradnak, ám volumenükben stagnálni fognak az ATM- és POS-eladások, hiszen ezek felső korlátja az eladóhelyek száma.

Az e-business, az e-banking, az internetes kereskedelem térhódításával és a professzionális felhasználók biztonsági igényeinek növekedésével megjelennek a PC-be integrált kártyaolvasók. Várhatóan az internetre kapcsolódó új PC-k mintegy fele ilyen módon kerül majd értékesítésre, ha ezt a szabványosodás követni fogja.

A fizetős tévék kártyahasználata az első lépcsője annak a fejlődésnek, amely a műholdas és kábeles interaktív média terjedését kíséri. E fejlődés alapja persze a PC és az analóg tévé konvergenciája, vagy az interaktivitást megvalósító hardver megjelenése, ahol azonban a PC-fejlesztés során létrejövő modulok egyszerűen beemelhetők lesznek.

A kártyaírók és -olvasók második legnagyobb piaca a mobiltelefonokhoz kötődik, mértékét tekintve 2004-re az összes installált kártyaolvasó kétharmada ezekben a készülékekben fog működni.



E fejlődésnek két fontos eleme van: egyrészt a harmadik generációs SIM kártyák megjelenésével színre lép az m-commerce (mobilkereskedelem), sőt már most piacon vannak több olvasóval rendelkező készülékek, másrészt kihordási fázisába került a Bluetooth- és a WAP-fejlesztés.

Árak

Rossz hír lehet a felhasználóknak, hogy a fenti sok jó tulajdonság ellenére bizonyos smart kártyák árának növekedése várható. Ennek fő oka, hogy míg korábban a kártyák eladási ára tartalmazta az alkalmazások ellenértékét is, addig a jövőbeni fejlesztések során a harmadik fél által készített operációs rendszerek kerülnek alkalmazásra, amelyek költsége a kártyák árát is növelni fogja. Ugyanakkor a törvényszerűség mindenképpen a kártya darabárának csökkentését jelenti.

Rádiófrekvenciás kommunikáció

Bevezetés a hálózatelméletbe

A rádiófrekvenciás lokális hálózatokkal történő ismerkedést az általános számítógép-hálózatokkal kezdjük. Mi is egy számítógép-hálózat? Egymással összekapcsolt, független berendezések összessége. Azért építünk hálózatot, mert

- információt szeretnénk másokkal megosztani,
- kommunikálni kívánunk másokkal,
- központi adatbázist használunk, vagy éppen
- mások számára is elérhetővé szeretnénk tenni információt vagy eszközöket.

Visszatekintve két évtizedes történetükre, azt találjuk, hogy a 70-es évek hálózata hierarchikus felépítésű volt, a számítási teljesítmény központosított, az állomások pedig egyszerű terminálok. A 80-as években megjelentek a PC alapú számítógép-hálózatok. A terminálok helyére egyre intelligensebb munkaállomások kerültek, ezek sokszor egyenrangú kapcsolatban álltak egymással. A helyi és a nagy távolságú rendszerek elkezdtek integrálódni a meglévő távközlési vonalak felhasználásával, és a 90-es években a legjelentősebb változás a különböző számítógép-hálózatok összekapcsolása.

Az új évezredben a számítógépeket nagy sebességű adatátviteli vonalak kötik össze, megsokszorozódott az adatátviteli sebesség és kapacitás. Az újdonság az, hogy az adat jellegű információ mellett ezek a rendszerek képesek valós idejű hang és videó átvitelére is. A különböző hálózatokat összekötő hálózatok közös nyelven, az internet nyelvén beszélnek. A legnagyobb kihívást manapság a sokféle hálózattípus összehangolása, valamint az adat- és hangátvitel integrálása jelenti. Ehhez számtalan kommunikációs eljárást szabványosítottak, amelyek közül néhányat részletesebben is áttekintünk.

Lokális és egyéb hálózatfajták

A számítógép-hálózatok egy jól elkülöníthető típusa a lokális hálózat (LAN). Azokat a rendszereket nevezzük lokálisnak, amelyekben egy kisméretű földrajzi területen független berendezések közvetlenül kommunikálnak egymással, közepes adatátviteli sebességgel. A tipikus sebesség a néhányszor tíz vagy száz Mbps-os tartományba esik, a fizikai méret pedig néhány

kilométerre tehető. Azt is mondhatjuk, hogy lokális hálózat az, amelyik nem vesz igénybe nyilvános hálózatot az adatforgalom lebonyolítására.

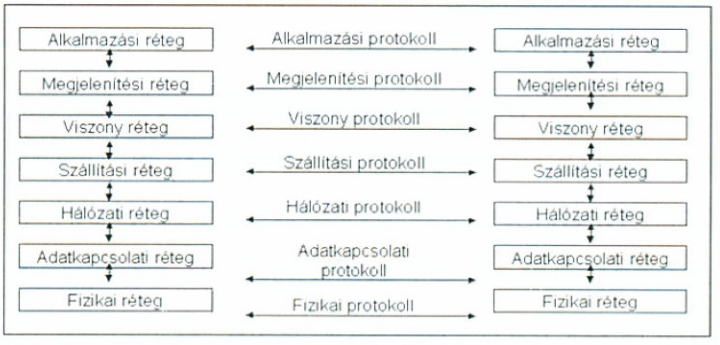
Egy hálózat alapvető eleme a fizikai kommunikációs csatorna. Ez lehet réz- vagy üvegszálas kábel, infravörös vagy rádiófrekvenciás csatorna, ekkor az elnevezése WLAN, azaz kábel nélküli LAN. Az összekötött állomások a hálózati illesztőkártyán és a kábelezésen keresztül létesítenek kapcsolatot.

A nagy távolságú hálózatok (WAN) fizikai kiterjedése jóval nagyobb (a városnyi méretű hálózatok elnevezése MAN), akár az egész Földet behálózó is lehet. Az adatátviteli sebesség egy-két nagyságrenddel kisebb a LAN-okénál. A kábel nélküli nagy távolságú hálózatok közül az elsősorban hangátvitelre használt GSM- és az adatátviteli célokra alkalmasabb GPRS-hálózatok ismertek, általános elnevezésük WWAN.

A lokális hálózatoknál jóval kisebb kiterjedésű a PAN, vagyis a személyes méretű hálózat. Az utóbbi évek technológiai fejlesztéseinek köszönhetően a mobiltelefon és a fülhallgató vagy a számítógép és az egér kábel nélküli kis hálózatba szervezhető rádiófrekvenciás kapcsolattal. A különféle gyártók eszközeinek együttműködéséhez ezt a hálózattípust is szabványosították.

OSI referenciamodell

A számítógép-hálózatok meglehetősen bonyolult kommunikációs rendszerek, ezek tervezését, az egyes hálózatok összekapcsolását szigorúan strukturált eszközökkel végzik. A hálózatok felépítésének vizsgálatakor egy szabványosított modellt (OSI) használunk. Ez a referenciamodell szemléletessé teszi az egyes hálózatok struktúráját. A modell hét réteget tartalmaz, amelyek egymásra épülnek. Az egyes rétegek jól definiált szolgáltatásokkal a fölöttük lévő elől eltakarják az alattuk lévő működésének részleteit.



Egy számítógépen belül az egyes rétegek fentről lefelé, illetve lentről fölfelé kommunikálnak, egy pontosan definiált interfészen keresztül. Két számítógép között viszont az egy szinten lévő rétegek kommunikációja a lényeges. Például két komputer hálózati rétege között a hálózati protokoll építi ki a logikai kapcsolatot. Azonos hálózati réteget tekintve az alattuk lévő fizikai és adatkapcsolati réteg közömbös, tetszőlegesen megválasztható.

Ez a felismerés segíteni fog bennünket annak megértésében, hogyan lehet összekapcsolni különböző számítógép-hálózatokat. A protokoll gyakorlatilag egy szabályhalmaz, amelynek betartásával két, egymással kommunikáló fél garantáltan meg fogja érteni egymást. Szokták a hálózati architektúrát egymásra pakolt rétegek sorozatának is nevezni.

Hálózatszabványosítás

A gyártók és a felhasználók hamar felismerték, hogy egyes hálózattípusokat célszerű előnyben részesíteni, szabványosítani, így a felhasználók olyan nyílt rendszerekkel dolgozhatnak, amelyek nem egy gyártó szeszélyességétől függnek. A lokális hálózatok szabványa természetesen a nagy gyártók által kifejlesztett hálózattípusokon alapul. Magában foglalja a topológiát, a hálózat közös csatornájához történő hozzáférés módszerét, az adatátviteli sebességet, az adatkeretek képzését, a forgalomvezérlést, valamint a hibakezelést.

A világon mindenütt elfogadott hálózatiszabvány-gyűjtemény az IEEE802, amely a fizikai réteg fölött elhelyezkedő adatkapcsolati réteget foglalja magában, különféle hálózattípusokra. A fizikai rétegek különböző szabványait itt nem tárgyaljuk.

Az IEEE802 szabvány

Az amerikai IEEE által megalkotott szabványgyűjtemény különféle nyílt, lokális hálózati architektúrákat definiál. Az IEEE802 tulajdonképpen azt specifikálja, hogy milyen legyen az a közös nyelv, amelynek segítségével az egyes állomások beszélgethetnek egymással. Az IEEE802 az alábbi szabványokat foglalja magában:

- 802.1 LAN-referenciamodell leírása
- 802.2 LLC (logikai kapcsolatvezérlés)

- 802.3 CSMA/CD (Ethernet)
- 802.4 Token Bus (vezérjeles sín)
- 802.5 Token Ring (vezérjeles gyűrű)
- 802.6 MAN (városi hálózatok)
- 802.10 Virtuális LAN
- 802.11 Kábel nélküli LAN (WLAN)
- 802.15 Kábel nélküli PAN (WPAN)

A 802.11 szabvány többek között azt írja elő, hogyan hagyja el egy adatcsomag az antennát elektromágneses sugárzás formájában úgy, hogy azt egy másik, 802.11-kompatibilis vevőberendezés venni és értelmezni tudja. A 802.3 szabvány egy konkrét megvalósítása a közismert Ethernet, míg a 802.5 a Token Ring-hálózatok teljes specifikációját tartalmazza.

Láthatjuk, hogy minden LAN-megoldás egy közösen hozzáférhető közegre épül, legyen az kábel vagy éppen az éter. Ennélfogva minden hálózat esetén gondoskodnunk kell egy alapvető dologról: mivel időben egyszerre több állomás akar kommunikálni ugyanazon a közegen, ezért definiálni kell egy protokollt (kommunikációs szabálygyűjteményt), amely koordinálja és vezérli ezt a kommunikációt. Az IEEE a különféle hálózattípusokhoz más és más közeghozzáférést vezérlő (MAC) protokollt definiál, ezek találhatók a 802.3 és 802.15 közötti szabványpontokban.

A hálózati protokollok

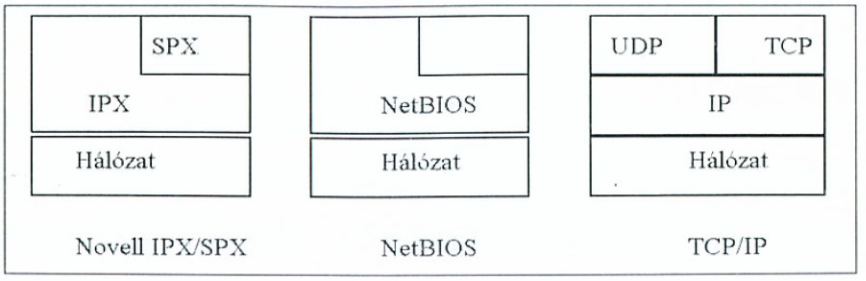
A hálózati és a szállítási réteg együttesen gondoskodik arról, hogy két tetszőleges, de külön hálózatban található gép között az adatáramlás hibátlanul folyjék.

A hálózatiréteg-protokoll feladata a rendelkezésre álló útvonalak közötti választás és egy csomagnak a címzetthez történő eljuttatása. A hálózati réteg nem sorrendtartó, tehát az egymás után indított csomagok tetszőleges sorrendben érkezhetnek a címzetthez, valamint nem gondoskodik az esetleg megsérült vagy elveszett csomagok újraküldéséről. Ilyen protokoll például az IP.

A szállítási réteg feladata teljes információs egységek mozgatása. Ha a hálózati rétegből egy hibás adatcsomag érkezik, ez a réteg javítja ki a hibát újraadással és nyugtázással. Az átvitel sorrendtartó és garantáltan hibamentes. Ilyen protokoll a TCP.

Szemléletessé téve a két protokollréteget, azt mondhatjuk, hogy a hálózati réteg leginkább egy feladott levélhez hasonlít, míg a transzportréteg egy folyamatos telefonbeszélgetéshez.

Az alábbi ábrán három ismert protokollvermet láthatunk.



A Novell-protokollt elsősorban Ethernet- és Token Ring-hálózatokhoz tervezték, nagyon hatékony, gyors és megbízható. Az IPX alkotja a hálózati réteget, az SPX pedig egy összeköttetés alapú transzportprotokoll. A szerver az általa kínált szolgáltatásokat egy SAP elnevezésű protokollal hirdeti meg a hálózati csomópontok számára.

A NetBIOS kiváló programozói interfésszel rendelkezik, ugyanakkor nem támogatja a hálózatok közötti forgalomirányítást.

A TCP/IP protokoll

A TCP/IP protokollt nonprofit szervezet alkotta meg abból a célból, hogy egy teljesen általános kommunikációs eljárást készítsen, amely két tetszőleges számítógép között működőképes. A TCP/IP hordozható, nyílt, szabványos architektúra. Az IP egy útvonalválasztó hálózati rétegbeli szolgáltatás, a TCP összeköttetés alapú szolgáltatást biztosít, míg az UDP összeköttetés-menteset.

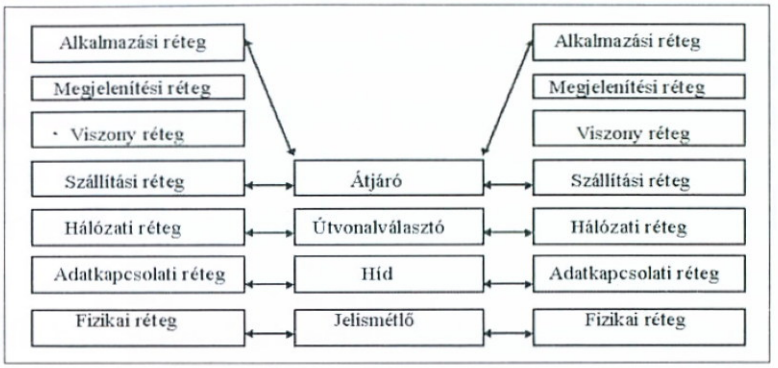
A TCP/IP egyik legfontosabb tulajdonsága, hogy teljesen közegfüggetlen. Hálózaton belüli kommunikáció esetén a hálózati állomásokat azonosító IP-címeket az alsóbb rétegek fizikai címeihez társítjuk. Így például Ethernet- és Token Ring-hálózaton az IP-címeket a hálózati kártyák által egyedileg meghatározott MAC-címekhez rendeljük hozzá, míg az ISDN- vagy X.25-ös nyilvános hálózaton az IP-címet a telefonszámmal kell összerendelni.

Egy TCP/IP hálózatban minden csomópont egyforma, azaz nincsenek hierarchikus kapcsolatok, így nincsenek a szerver által meghirdetett szolgáltatások sem. Ha egy hálózati állomás igénybe szeretne venni egy szolgáltatást, tudnia kell a szolgáltató IP-címét.

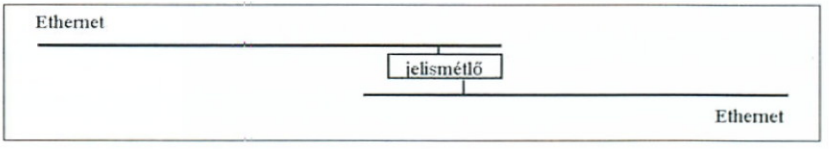
Hálózatok összekapcsolása

A 80-as, de főleg a 90-es évektől kezdődően a vállalatok elkezdték összekapcsolni helyi hálózataikat. Manapság már a legtöbb cég célja egy egységes, jól szervezett hálózatközi együttműködés, hálózati integráció kialakítása. A lokális hálózatok összekapcsolásának lehetőségeit jól szemléltethetjük az OSI modell egyes rétegein.

Minket elsősorban a lokális hálózatok közötti kapcsolatok érdekelnek, de érintőlegesen megemlítjük a városi, illetve a nagy távolságú hálózatokhoz történő kapcsolódás lehetőségeit is.

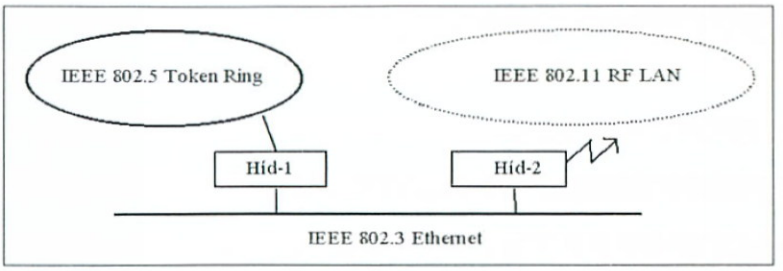


A legegyszerűbb összekötő elem a jelismétlő (repeater), amely a fizikai réteg szintjén a kábelszegmensek között végez elektronikus illesztést. Elsődleges feladata a hálózat fizikai kiterjesztése. A jelismétlő regenerálja és újraszinkronizálja a szegmensek közötti elektronikus adatjelet. Segítségével különböző fizikai kábeleket keverhetünk, vagy éppen meghibásodott hálózati részeket szigetelhetünk el egymástól. A jelismétlők speciális fajtája a csillagtopológiát biztosító hub, illetve a szegmensek közötti dinamikus kapcsolást végző switch.



Természetesen Token Ring-hálózatoknál is alkalmazhatunk jelismétlőt. Ahhoz viszont, hogy Ethernet- és Token Ring-hálózatot kössünk össze, más egységre van szükségünk. Emlékezzünk arra, hogy az Ethernet és a Token Ring teljesen eltérő MAC-protokollt használ, így az illesztőegységnek az adatkapcsolati rétegek közötti árjárhatóságot kell biztosítania. Azokat a berendezéseket, amelyek a különböző közeg-hozzáférési

protokollal rendelkező hálózatokat illesztik egymáshoz, hidaknak nevezzük (bridge).



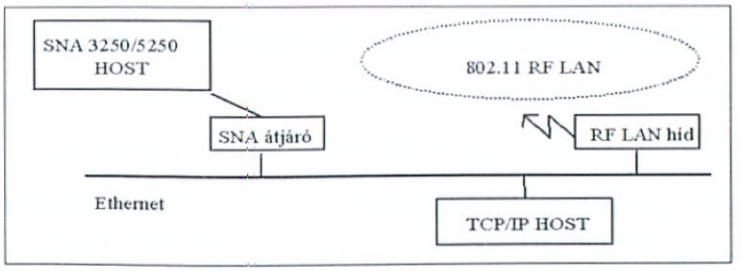
Vannak transzparens hidak, amelyek az illesztésen kívül egyéb funkciót nem látnak el, azaz válogatás nélkül továbbítják a hálózatok között az adatcsomagokat. Az intelligens hidak észreveszik, ha egy csomag címzettje a hálózaton belül van, és a forgalmat ennek megfelelően a hálózaton belül tartja. Az intelligens híd csak a másik hálózatnak szóló csomagot küldi tovább.

Nagyon fontos, hogy a hidak funkcióját megértsük, mivel a rádiófrekvenciás hálózatokat is egy hozzáférési pontnak nevezett hídon keresztül illeszthetjük a hagyományos hálózatokhoz. A hidak meglehetősen intelligens eszközök, hiszen nagyobb hálózatoknál olyan feladatokkal kell megbirkózniuk, mint a csomagduplikálás veszélye, ha egy hálózatból a másikba egynél több hídon keresztül is eljuthatunk, vagy hogy a hurkokat tartalmazó hálózati struktúrában a csomagok végtelen hosszú ideig keringenek.

Több lokális hálózat összekapcsolásakor meg kell oldani két számítógép között a megfelelő útvonal kiválasztását. A nagy hálózatokat általában a könnyebb kezelhetőség kedvéért alhálózatokra osztják. Az alhálózatok közötti tájékozódás a forgalomirányító csomópontok (routerek) feladata. Ezek munkáját az úgynevezett útvonalválasztó protokoll (RIP) segíti, amelynek segítségével lehetővé válik a hálózatok közötti információs táblák kicserélése. Ezek az egységek szolgálnak különböző protokollt használó hálózatok illesztésére is.

TCP/IP protokollt futtató hálózatokban minden állomás egyedi címmel rendelkezik, amely 32 bit hosszú, például 199.176.1.2 egy IP-csomópont címe lehet. Nemcsak az állomásoknak van címük, hanem a hálózatoknak is: nullára végződnek, és meghatározzák a hálózatba köthető csomópontok maximális számát.

Az átjárók végzik a legmagasabb szintű illesztést a számítógépes hálózatok között.



Hálózati operációs rendszerek

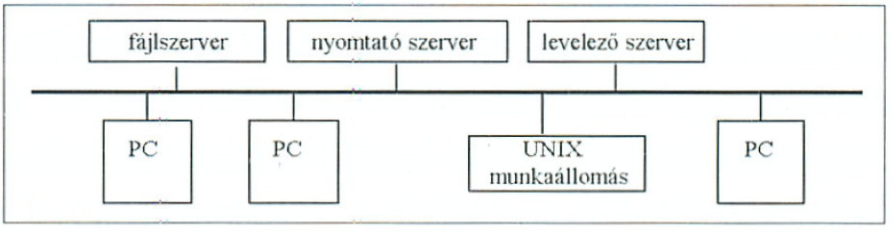
A hálózati operációs rendszer a hálózati egységek egymással történő összehangolt és megbízható működését garantálja. Az operációs rendszerek belső felépítése, kialakítása nagymértékben különbözik, ennek ellenére a nyújtott szolgáltatások és a támogatott hálózattípusok szempontjából felfedezhetünk sok közös tulajdonságot. A legelterjedtebb hálózati operációs rendszerek az alábbiak:

- Apple Talk,
- IBM LAN Server,
- Linux,
- Microsoft NT/2000,
- Novell Netware,
- Unix TCP/IP.

A legtöbb operációs rendszer támogatja a különféle MAC-protokollokat, némelyikük magasabb szintű hálózati funkciókat is megvalósít, például az útvonalválasztást. Valamennyi biztosít fájlszerverfunkciót, egy-egy eszközhöz történő párhuzamos hozzáférést, az írás alatt lévő rekordok kizárólagos használatát, hozzáférési jogokat, hálózatmenedzsmentet. A hálózati operációs rendszerek általában nagy memóriaigényűek, és képesek egyidejűleg több feladat párhuzamos végrehajtására.

Kliens–szerver modell

Az eddigiek folyamán kiépíthettünk magunknak egy képzeletbeli hálózatot; hogyan és mire is használhatjuk ezt a rendszert? Képzeljünk el egy modellt, amelyben a hálózat közös csatornájához kliensek és szerverek csatlakoznak.



Egy ilyen felépítésű rendszerben az alkalmazások a kliensgépek között kerülnek szétosztásra, amelyek előre definiált és jól meghatározott szolgáltatásokat vehetnek igénybe az egyes szerverektől. A szerverek szolgálják ki a kliensek kéréseit.

A modell lényege az, hogy fizikailag elkülönülő alkalmazások és szolgáltatók működnek együtt anélkül, hogy egy adott kliens tudná, hol található a szerver, vagy éppen milyen operációs rendszert futtat. A lokális hálózatokban a szerver egy logikai szolgáltatóközpont, amelyhez egyidejűleg több felhasználó férhet hozzá.

Hálózatmenedzsment

Mivel a számítógép-hálózatok meglehetősen összetett rendszerek, így felügyeletük, biztonságos működtetésük csak külön e célra kifejlesztett eszközökkel lehetséges. Terjedelmi okokból csupán azokat a funkciókat futjuk át, amelyeket a hálózatmenedzsmentnek biztosítania kell:

- konfigurálás,
- hibakezelés,
- teljesítményanalízis,
- hozzáférési jogok kiosztása, adatvédelem,
- hálózatfejlesztés.

A hagyományos hálózatokkal történő ismerkedést ezennel befejezzük. Ez a rövid bevezető azt a célt szolgálta, hogy a rádiófrekvenciás rendszerek megismerésének technikai alapjait megteremtse. Bármilyen hálózatot is szeretne a felhasználó, mindig kérje ki szakember véleményét, tanácsát. A fenti fogalmak alapos áttanulmányozásával a felhasználó birtokába jut annak a közös nyelvnek, amelyet a hálózati szakemberek használnak. A közös nyelv használata pedig elengedhetetlen az együttgondolkodáshoz.

RF-adatgyűjtés

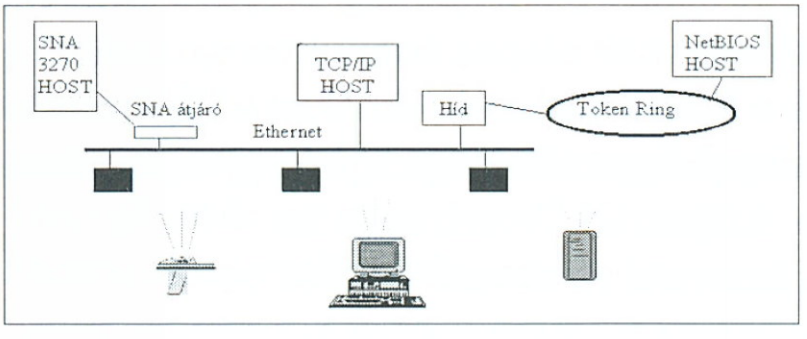
Bevezetés

A rádiófrekvenciás kommunikációt támogató rendszerek alkalmazói számtalan különböző megoldás közül választhatnak. A potenciális felhasználó nehezen tud eligazodni a kínált megoldások között. Azoknak szánjuk a következő fejezeteket, akik rádiófrekvenciás mobil adatgyűjtőkkel kívánják bővíteni jelenlegi rendszerüket. Szeretnénk átfogó képet adni a rendelkezésre álló megoldási lehetőségekről, a technológiai fejlődésről és a szabványosítási törekvésekről.

A továbbiakban a rádiófrekvenciás lokális hálózatok (WLAN) felépítésével, felhasználási lehetőségeivel foglalkozunk. Már a korábbi fejezetek is sugallták, hogy a felhasználó számára megnyugtató és hosszú távon kielégítő megoldást a szabványos, nyílt architektúra alkalmazása jelentheti. Éppen ezekről a szabványosítási törekvésekről és azok gyakorlati felhasználásáról lesz szó a következő fejezetekben.

Mi is az a rádiófrekvenciás hálózat (WLAN)?

A WLAN-t úgy kell tekinteni, mint a hagyományos vállalat létező számítógépes rendszerének kiterjesztését. Az alábbi ábrán egy mintahálózatot látunk, amely hagyományos és rádiófrekvenciás elemeket is tartalmaz.



Az ábrán látható fekete dobozok a rádiós hozzáférési pontok, amelyek feladata a rádiófrekvenciás hálózat illesztése a hagyományos hálózathoz. A rádiófrekvenciás illesztőkártyával ellátott PC-k, adatgyűjtők és nyomtatók ezek segítségével csatlakoznak a hálózatra.

A felhasználó tehát a rádiófrekvenciás illesztőegységek segítségével képes korábbi hálózatát kiterjeszteni az éterbe. A rádiós pontok által lefedett területen a mobil eszközök szabadon mozoghatnak. A cellás felépítésnek köszönhetően a hordozható egységek a rádiótelefonokhoz hasonló módon, észrevétlenül barangolnak a cellák között. Az adatátviteli sebesség a rádiós hálózat típusától függ, manapság tipikusan 2 és 11 Mbps közé esik.

A megfelelő RF-architektúra kiválasztásához érdemes szakember segítségét kérni, hiszen a feladatra optimalizált és a későbbi fejlesztési lehetőséget is magában hordozó megoldás kialakításához sok szempont egyidejű figyelembevétele szükséges, például:

- *Milyen a jelenleg használt LAN-környezet?*
- *Milyen a hálózati operációs rendszer?*
- *Milyen hostgépre kell csatlakozni?*
- *Milyen a hálózati forgalom a jelenlegi hálózaton?*
- *Mi a preferált hálózati kommunikációs protokoll?*
- *Milyen szintű hálózatmenedzsment szükséges?*
- *Mekkora területet kell besugározni?*
- *Milyen antennatípust használjunk?*
- *Hány mozgó egységet kell kiszolgálni egyidejűleg?*
- *Az adat mellett hang átvitele is szükséges-e a hálózaton?*

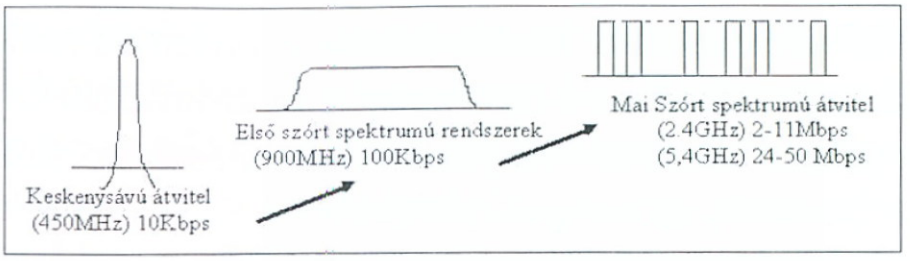
...és folytathatnánk a kérdéseket tovább. Ebben a rövid áttekintésben nem áll módunkban valamennyi kérdést részletesen megválaszolni, azonban néhány mintapéldán keresztül rávilágítunk azokra a szempontokra, amelyeket a felhasználónak és a rendszert kiépítőnek együtt kell végiggondolnia.

Technológiai fejlődés az RF-kommunikációban

A rádiófrekvenciás átvitel témaköre sok vaskos könyvet megtöltene. Itt mindössze azt a fejlődési irányt vázoljuk fel, amely az utóbbi évek technológiai fejlődésének terméke. A fejlődés irányát az egyre magasabb frekvenciák alkalmazása, az adatátviteli sebesség növekedése, valamint a szabványos architektúra kialakítása jelenti. A legkorszerűbb megoldások kerültek be az IEEE802.11 szabványba.

A rádiós rendszerek első generációjának működési frekvenciája 450 MHz, tipikus adatátviteli sebessége 10 kbps volt, 1-2 wattos adóteljesít-

mény mellett. Az alkalmazott keskeny sávú átviteltechnika alapelve az volt, hogy az átvinni kívánt információt egy előre meghatározott keskeny frekvenciatartományban sugározták. Az adott frekvenciát előre kellett kiválasztani, és gondoskodni kellett arról, hogy a közelben lehetőleg ne legyen másik eszköz, amelyik ugyanazt a sávot használja. A frekvencia kizárólagos használatáért folyamatosan díjat kellett fizetni.



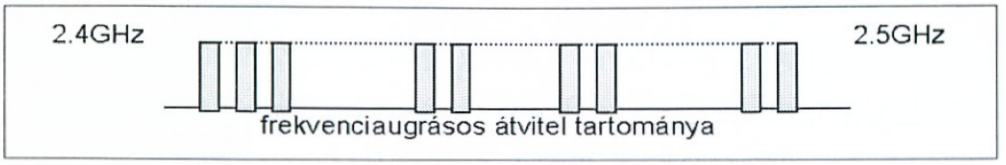
A technológiai fejlődés eredményeként a rendelkezésre álló frekvenciatartomány eltolódik a magasabb frekvenciák irányába. Ezzel egyidejűleg megnő az adatátvitelre felhasználható sávszélesség. Ezt felismerve dolgozták ki a zavarjelekre már kevésbé érzékeny, úgynevezett szórt spektrumú rendszereket. Az alapelv az, hogy úgy védekezünk a zavarjelek ellen, hogy az információt – egy széles frekvenciatartományban szétkenve – a szükségesnél többszörösen visszük át. Az átvitel során hozzáadódó zavarjelek ellenére nagy valószínűséggel épségben meg fog érkezni hozzánk az elküldött információ. Az alkalmazott frekvenciára korábban a 900 MHz volt a jellemző érték, újabban pedig a 2,4 GHz. Jelenleg már fejlesztik az 5,4 GHz-es tartományban működő, nagy sebességű rendszereket. Az adási teljesítmény a szórt spektrumú rendszerekben 1 W-nál kevesebb, a 2,4 GHz-es tartományban 100 és 500 mW közötti, 2–11 Mbps adatátviteli sebességgel. A jövő rendszereiben 1-2 W kimeneti teljesítmény mellett 24–100 Mbps-os sebesség várható, ami már eléri a hagyományos vezetékes Ethernet-hálózat sebességét.

A 2,4 GHz-es szórt spektrumú átvitel a korábbi keskeny sávú átvitelhez képest minőségi változást jelent. A nagyobb átviteli sebességet jobb zajtűrés jellemzi, és megnőtt az egy térrészben működtethető berendezések száma.

Egy rádiófrekvenciás rendszer átbocsátóképességét nagymértékben meghatározza, hogy a felhasznált frekvenciatartományt milyen hatékony-

sággal használják az eszközök. A technológia fejlődésének eredményeként két rádiós átviteli technika terjedt el, amely lényegében kiegészíti egymást.

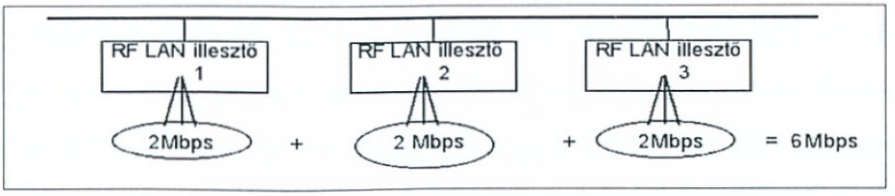
Az egyik az IEEE802.11-ben kidolgozott (1997) frekvenciaugrásos technika (FH), amely az alábbi módon működik: egy berendezés egyszerre csak egy keskeny sávú (1 MHz) tartományban ad, s az adási frekvencia másodpercenkénti többszöri változtatásával a zavarjelek hatása elkerülhető. Ezen az elven működnek a 802.15 szerinti WPAN-hálózati eszközök is, másodpercenként 100-szoros csatornaváltással.



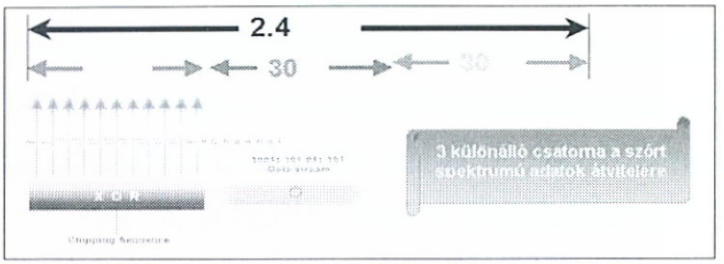
A csatornaváltás sorrendje az egy térrészben található eszközökre más és más, amit a 66, egymástól független ugrási táblázat határoz meg (pl. 5,43,36,17, illetve 23,43,2,9...). Ebből az következik, hogy az egymás közelében lévő berendezések – ha véletlenül ugyanazon a frekvencián kezdenek el adni – 78/79-ed valószínűséggel más frekvenciára fognak ugrani a csatornaváltás után. A frekvenciaugrásos technika nemcsak a rendszer belső zavarjeleitől véd meg, hanem a külső zavarjeleket is (pl. mikrohullámú sütő) könnyen kiszűri, mivel a minimális ugrás legalább 6 csatornaszélességnyi.

A tipikus adatátviteli sebesség 2 Mbps, az adóteljesítmény Európában 100 mW. A korábbi 450 MHz-es keskeny sávúakhoz képest valamennyi szórt spektrumú rendszer jellemzője a kisebb hatótávolság, ami azt jelenti, hogy ugyanakkora területen több adóvevőt kell elhelyezni. A tipikus áthidalható távolság épületen belül 25–75 m, épületen kívül pedig 50–150 m.

Felépítésénél fogva a frekvenciaugrásos átviteltechnika legnagyobb előnye abban rejlik, hogy a rádiófrekvenciás hálózatok illesztésére szolgáló úgynevezett hozzáférési pontok és mobil egységek nem zavarják egymást, így a hálózat újabb elemek hozzáadásával bármikor megnövelhető. Az új adóvevő egységek nemcsak a lefedett területet növelik, hanem az egész hálózat átbocsátóképességét. A hálózat remekül skálázható, és átbocsátóképessége lineárisan nő az alkalmazott berendezések darabszámával.



A másik, elterjedőben lévő szórt spektrumú technikát az IEEE802.11(b) szabványban specifikálták 1999-ben. Az adatátvitel úgy történik, hogy a rendelkezésre álló 2,4-2,5 GHz-es tartományt három egyenlő szélességű 30 MHz-es sávra bontja, és ebben a jóval szélesebb sávban történik az adatátvitel. A megoldás nagy előnye a megnövelt adatátviteli sebesség, amely maximum 11 Mbps lehet, és a zavaró jelek növekedése esetén automatikusan 5,5, illetve 2 Mbps-ra csökken.



A nagyobb sebesség kisebb hatótávolságot jelent, mégpedig a frekvenciaugrásos rendszer hatótávolságának a felét, vagyis egy térrészben négyszer annyi hozzáférési pont telepítése szükséges. Elsődleges felhasználási terület az irodai és egyéb mobil alkalmazások köre, ahol egy térrészben kevés eszköz található, ugyanakkor nagy adatátviteli sebességre van igény. (Itt kell megjegyezni, hogy a hozzáférési ponttól történő eltávolodáskor az átviteli sebesség szintén leesik 5,5, illetve 2 Mbps-ra, viszont az áthidalt távolság megközelíti a frekvenciaugrásosnál megszokottat.)

Az IEEE802.11 szabvány

Az IEEE802.11 a 802-es szabványcsalád legfiatalabbik tagja. Azért hívták életre, mert a rádiófrekvenciás hálózatok területén teljes káosz uralkodott. Valamennyi gyártó egyedi, a többivel nem kompatibilis rendszert alakított ki. A felhasználó számára ez azt jelentette, hogy teljesen ki volt szolgáltatva a rendszerelemek gyártójának.

Az IEEE802.11 WLAN-szabvány definiálja a közeg-hozzáférési (MAC) protokollt. A szabvány kialakításánál figyelembe vették, hogy különböző gyártók lokális hálózatai együtt tudjanak működni, valamint azt, hogy

a megoldás a fizikai rétegtől független legyen. (Infravörös és rádiófrekvenciás átvitelre egyaránt kiterjed.)

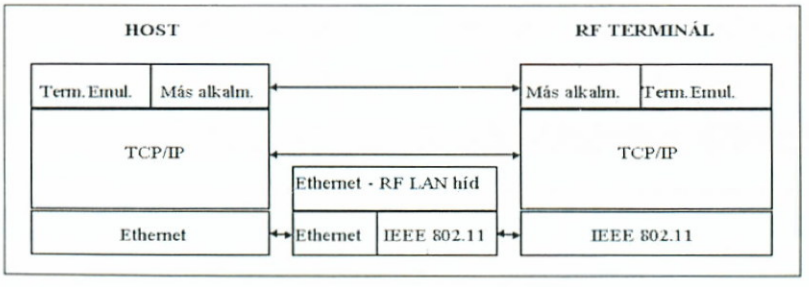
A szabvány célja egy egységes, épületen belüli, nagy sebességű lokális hálózati architektúra kialakítása, ahol az eszközök nem egy kábelen, hanem az „éterben" kommunikálnak. Az IEEE802.11 szabványt a legtöbb gyártó támogatja, így a Motorola, az Apple, a Xircom, az IBM, a Norand, az LXE, az AMD, a Proxim, az SMC és a Symbol.

A mozgó egységek folyamatosan aktív vagy teljesítménytakarékos üzemmódban működhetnek. A mozgó egységek és a hozzáférési pontok közötti adatátvitel teljesítménytakarékos. A mozgó terminálok úgy barangolhatnak a cellák között, hogy az átmenetek észrevehetetlenek. A többféle barangolási algoritmus lehetővé teszi a gyártók számára a termékdifferenciálást. Az adatátviteli sebesség a rádiófrekvenciás tartományban 1 és 2 Mbps, infravörös kommunikációnál 4 Mbps.

Az IEEE802.11(b) már a korábbi szabvány továbbfejlesztése a 11 Mbps-os sebesség irányába, és mondhatni teljes támogatást kap a világban, mivel valamennyi gyártó ugyanazt a chipsetet építi be eszközeibe (Cabletron, 3Com, Nokia, Ericsson, Compaq, Dell, Breezcom stb.). A 802.11(a) pedig az 5,4 GHz-es LAN-okat definiálja (HyperLAN).

Rádiófrekvenciás LAN-ok illesztése

A szabványosítási folyamat megindulása előtt valamennyi gyártó saját hálózati architektúrával rendelkezett, a kábeles háttérrendszerhez történő illesztéshez meglehetősen költséges átjárókra volt szükség, amelyekből más-más típus kellett a hosttól és a hálózati operációs rendszertől függően. Amennyiben nagyobb területet kellett lefedni, az átjárók számának növekedése nagyon költségessé tette a rendszert.



A nyílt, szabványos architektúra megkönnyíti az illesztést, ráadásul költséget takarít meg a felhasználónak, mivel a 802-kompatibilis hálóza-

tok között egy hídon keresztül közlekedhetünk. Az előző ábrán egy Ethernet-hálózathoz illesztett RF-LAN réteges felépítését láthatjuk. Az alkalmazás TCP/IP protokollon alapul.

Hang és adat integrálása RF-LAN-on

Míg a 90-es években az alapvetően beszédátvitelre használt vonalkapcsolt hálózatokat használták adatátvitelre is, addig az új évezred megfordította ezt a folyamatot. A nagy sebességű csomagkapcsolt hálózatokon az egyre gyorsabb útválasztóknak köszönhetően lehetővé vált a hang adatcsomagok formájában történő valós idejű átvitele. A megfelelő szabvány a H.323, a „hang az internet felett" (VoIP), amely elsősorban a gyártók berendezéseinek együttműködését hivatott biztosítani.

A rádiós LAN a hagyományos hálózattól csak a fizikai közegben különbözik, így a gyártók felismerték, hogy a kiépített rádiós hálózatot a szokványos adatátvitel mellett fel lehet használni hang vagy akár videó átvitelére. A működés alapelve megegyezik a kábeles világban megszokottal, a különbség mindössze az, hogy a telefonálásra használt eszköz a digitalizált beszédcsomagokat először a rádiós hozzáférési pont felé továbbítja, ahonnan azok már a megszokott vezetéken vagy másik mobil eszköz felé rádióhullámokon folytatják útjukat. A hívás pedig ingyenes. A számítógépes hálózat a klasszikus telefonhálózathoz átjáró segítségével illeszthető, ekkor persze a hívásért már fizetni kell a szolgáltatónak.

Szoftverillesztési kérdések RF-hálózaton

Ez a rész abból a célból íródott, hogy segítsen a felhasználóknak és a megoldásszállítóknak eligazodni abban, hogy adott környezetben és alkalmazási körülmények között milyen szoftveres megoldási lehetőségek állnak rendelkezésre RF-terminálok alkalmazása esetén. Azért, hogy

könnyebb legyen az eligazodás a rendelkezésre álló megoldások között, összegyűjtöttük valamennyit, és azzal a reménnyel tesszük közzé, hogy a szakemberek számára megfelelő eligazításul fog szolgálni.

Telnet-kliens (terminálemuláció)

A megoldási lehetőségek közül elsőként a klasszikus terminálemulációt vesszük sorra, amikor is a rádiós terminálon egy Telnet-kliensprogram fut. A megoldás egyszerű és gyors illesztést biztosít a legtöbb hostrendszerhez. Telnet esetén néhány követelménynek kell teljesülni, mielőtt a megoldást ajánlhatjuk.

Az informatikai háttérrendszernek lehetőleg hostcentrikusnak kell lennie, pl. IBM S/390, AS/400, Unix, Windows NT vagy bármilyen operációs rendszer (OS), amely támogatja a párhuzamos kiszolgálást és a több felhasználót. Személyi számítógépes (PC-s) hálózatok – mint a DOS-hálózat vagy a Windows 3.x/9x kliensek – nem javasoltak az ilyen kritikus felhasználásokra, habár elméletileg a működés lehetséges.

A gazdarendszernek futtatnia kell a TCP/IP protokollréteget.

Végül, de mind közül a legfontosabb az, hogy a gazdagépnek tudnia kell fogadni Telnet-kéréseket. Míg ez a Novell-, Unix- és IBM-rendszerek standard jellemzője, addig Windows NT-környezetben a felhasználónak külön kell megvásárolnia és telepítenie ezt a szerveroldali komponenst.

Mihelyt megvan minden fent említett építőelem, úgy a következő lépés egy-egy IP-cím megadása a mobil terminál, illetve az AP számára. Ezenkívül még az úgynevezett Subnet Mask, illetve több alhálózat esetén az alhálózatokat összekötő gateway/router címének megadása is szükséges. A mobil terminálon a Telnet-kliens elindítása után azonnal lehetőség van a host megadására és a bejelentkezésre. A felhasználó tetszőleges alkalmazása futtatható, jóllehet a képernyő csak részben, a mobil egység kijelzője által meghatározott méretben lesz látható. A Telnet-megoldás egyszerűsége és robusztussága fontos szempont, főleg akkor, ha a felhasználó szkeptikus az RF-alkalmazásokat illetően.

A megoldásban tehát az RF-terminál „buta" terminálként viselkedik, azaz olyan, mintha a felhasználó a hostgép egy konzoljánál ülne, a géphez közvetlenül csatlakoztatott billentyűzetet és kijelzőt használva. Az egyetlen különbség, hogy ez a konzol mobil, és mérete kisebb a megszokottnál.

A terminálemuláció előnyei

Csökken a fejlesztési idő. Az alkalmazások a hostgépen már rendelkezésre állnak, így csak a képernyőre írást kell módosítani, hogy az a kisebb kijelzőn is jól látható legyen.

Nincs betanulási idő, nem kell megismerni új fejlesztőeszközöket.

Az alkalmazásfejlesztés és a terminálemulációs programok karbantartásának centralizációja.

A hibaelhárítás és a támogatás sokkal könnyebb és gyorsabb ilyen szabványos eszköz használatával, így Telnet alkalmazásakor a felmerülő problémák reprodukálásának lehetősége bármilyen platformon rendelkezésre áll.

A nyílt és szabványos hálózati protokollok (Ethernet, TCP/IP, Telnet) használata azt jelenti, hogy a felhasználó nincs egy gyártó egyedi rendszeréhez kötve, és ez különösen fontos a beruházás jövőbeni értékállósága és továbbfejlesztése tekintetében.

A terminálemuláció hátrányai

Az RF-forgalom nagyobb és nem optimális – VT/HP emulációnál a mobil eszköz minden leütött karaktert átküld a hostnak, amelyet az a képernyőn megismétel –, habár ez egyre kevésbé okoz problémát a gyorsabb hálózatok és terminálok új generációinál.

Alapvető fontosságú, hogy a hostgép folyamatosan rendelkezésére álljon, és a rádiós lefedettség teljes legyen. Mihelyt a terminál kimozdul a lefedett területről egy adott időre, a hostkapcsolat lezárul, és egyes adatok elveszhetnek.

A mobil terminálóldali megjelenítést és az egyedi terminálfunkciókat (például hangeffektusok) nehezen lehet testre szabni, ennek lehetősége korlátozott.

Kliens–szerver megoldások

A Telnet-megoldás mellett találjuk a különféle kliens–szerver architektúrákat. Ezeket csoportosítani szokták aszerint, hogy a szerver és a kliensgép között milyen mértékű a munkamegosztás. A mobil eszközök a legtöbb esetben úgynevezett „vékony" kliensek, azaz kis számítási kapacitással és teljesítménnyel rendelkeznek, a rajtuk futó program minimális funkcionalitású. Mindent, amit le lehet szedni, eltávolítottak a kliensoldal-

ról, és a szerveroldalra pakolták. Ebben az értelemben az alkalmazás egy másik, erősebb gépen, az alkalmazásszerveren fut, és a terminál mint intelligens bemeneti-kimeneti eszköz szerepel. Ez a munkamegosztás biztosítja, hogy az olyan készülékek, amelyek nagyon kis feldolgozóképességgel és tárolókapacitással rendelkeznek, teljességgel együtt tudnak működni a korszerű operációs rendszerekkel és az azokon futó alkalmazásokkal. További előny, hogy a felhasználónak nem szükséges felújítania vagy lecserélnie mobil eszközeit minden alkalommal, amikor frissítést végez a hostrendszerben.

Miben is különböznek a kliens–szerver megoldások a Telnet alapú rendszerektől? Milyen esetekben érdemes ezeket a megoldásokat választani? A válasz a felhasználók által használt rendszerekben és a szoftverfejlesztési döntésekben keresendő.

Az asztali számítógépek kivételesen alacsony ára és az új, PC alapú hálózati operációs rendszerek térhódítása miatt a felhasználók túlnyomó többsége PC alapú hálózatot épít, vagy ilyennel egészíti ki nagygépes rendszerét. Ezeket a rendszereket korlátozottabb költségvetéssel lehet üzemeltetni, és a szoftverfejlesztések előtt szinte korlátlan lehetőségek nyílnak. Ezzel szemben a nagygépek esetében pusztán a rendszer üzemeltetéséhez is magasan képzett szakemberekre van szükség, hogy a fejlesztésről ne is beszéljünk. Ennélfogva egy olyan megoldás, amelynek nincs szüksége a host típusú architektúra minden követelményére – drága redundáns eszközök, menedzsment, szakértők, testre szabott alkalmazások stb. –, sokkal gyorsabban és olcsóbban kifejleszthető, telepíthető és üzemeltethető rendszert eredményez.

A Telnettől való legfőbb eltérés a helyi eszközképességek kihasználása, mint például adatok tárolása a helyi meghajtókon, korlátozott részfeladatok futtatása helyben és nem a szerveren, valamint a hostgéppel történő hatékonyabb kommunikáció biztosítása. Például az adatbeviteli mezők tartalmának és érvényességének ellenőrzése hatékonyabban történhet a helyi erőforrások kihasználásával, és a betáplált információ csak ellenőrzés után kerül fel a szerverre, csökkentve ezáltal az RF-forgalmat és a host igénybevételét.

A kliens–szerver megoldások egy érdekes változata az úgynevezett szerveroldali emuláció, amely a Telnet-megoldás, illetve a kliens–szerver

architektúra ötvözete, és heterogén hálózatok esetén előnyös. A működés alapelve az, hogy a különböző platformokon futó alkalmazások képernyőit egy szerver fogja össze – legtöbbször objektumorientált eszközökkel programozható módon –, és a mobil terminálok mint kliensek felé egy közös, úgynevezett szerveroldali emulációt biztosít. A megoldás a heterogén rendszerekben úgy teszi lehetővé a különböző platformokon működő számítógépek és programok elérését, hogy közben a kliensoldal egységes és jól kezelhető.

Előnyök

- Rövidebb betanulási szakasz, gyorsabb fejlesztési ciklus és integráció.
- Kisebb fejlesztési, telepítési és fenntartási költségek.
- Központi adminisztráció az alkalmazások és a terminálmenedzsment számára.
- Testre szabott alkalmazások a terminál egyedi tulajdonságainak figyelembevételével.
- Heterogén környezetben egyszerű és könnyen kezelhető megoldás.

Hátrányok

- Az alkalmazásszerver nélkül a rendszer működésképtelen.
- A kliensadatok nem körültekintő tárolása potenciálisan konfliktusokhoz és ellentmondásokhoz vezethet ugyanazon adatok kliens- és szerveroldali verziói között.
- Az alkalmazásszerver és a megfelelő operációs rendszer heterogénebbé teszi a hálózatot.

Alkalmazásgenerátorok

Az alkalmazásgenerátor-programok azoknak a felhasználóknak nyújtanak segítséget, akik nem akarnak elmélyedni a programozás részleteiben. A megoldás tulajdonképpen egy programgenerátor-program használata, amely legtöbbször Windows alapú, és grafikus felületen keresztül használható. Jóformán semmilyen programozói ismeretet nem kíván. Létrehoz egy nagyon kis méretű kódot, amelyet a terminálban található futtatóprogram értelmez utasításonként.

Az alkalmazásgenerátorok segítségével ugyanazt az alkalmazást lehet

hordozni hagyományos és RF-adatgyűjtők között néhány perces kiigazítással. A terminál egy időben több alkalmazást képes tárolni, és meg tud osztani ezek között közös adatokat, illetve állományokat, így csökkentve a különböző alkalmazások közötti adatcserével járó bonyodalmakat. Fő felhasználási területük a gyors demoalkalmazások és a kicsi–közepes méretű alkalmazások fejlesztése.

Előnyök

- Könnyen használható eszköz, programozói tudást nem igényel, alkalmazások létrehozása nagyon rövid idő alatt.
- A hagyományos adatgyűjtőkre írt alkalmazásokat könnyen lehet RF-környezetbe átvinni.
- A rádiós lefedettség hiánya esetén is működik az alkalmazás.

Hátrányok

- Korlátozott funkcionalitás, legtöbbször csak a beépített megoldásokkal lehet dolgozni.
- Létező rendszerekkel történő integrációra nem alkalmas, vagy nagyon korlátozottan használható.

Egyedi fejlesztések

Ha az előző megoldások egyike sem jelentene megoldást a felmerült problémára, akkor az RF-adatgyűjtők alacsony szintű, a hálózati kommunikációt is kezelő programozására van szükség. Ez legtöbbször C nyelvű programozást jelent, amelynek segítségével gyakorlatilag mindenre felkészíthetjük az eszközt, hiszen annak működése fölött teljes ellenőrzést gyakorolunk. A terminálemulációs programok és a kliens–szerver programok fejlesztése is ennek alapján történik.

Előnyök

- Teljes ellenőrzés az egész alkalmazás felett, anélkül, hogy támaszkodni kellene védjegyes fejlesztési eszközökre vagy könyvtárakra.
- Egyesíthetjük a különböző megoldások egyedi jellemzőit, mint például az adatok helyben történő tárolásának képessége vagy programok futtatásának lehetősége a host rendelkezésre állásától függetlenül stb.

• A standard szoftvermegoldásokban általában nem található meg a speciális funkciók kifejlesztésére alkalmas modulok vagy a különböző platformokra írt programok hordozása.

Hátrányok

• Az egész fejlesztés és mindenekfelett a tesztelési folyamat kizárólag a fejlesztő kezében van. A megbízhatóság és a hibatűrő képesség a fejlesztőn áll vagy bukik.

• A standard fejlesztési eszközöknek köszönhető rövidebb fejlesztési idő elvesztése növekvő árat jelent a felhasználó számára.

• A forráskód csak egy adott platformon lesz használható, amennyiben nem gondolnak a hordozhatóságra a fejlesztés szakaszában.

Egyéb azonosítási módok

Automatikus azonosítási módszerek

A kézi adatbevitel problémája

Ez jelenti az adatbevitel hagyományos módját, ahol az operátor egy billentyűzet segítségével begépeli a megfelelő karaktersorozatot. Megfigyelések azt mutatják, hogy ezzel a módszerrel átlagosan 300 karakterenként 1 karakter hibásan kerül be a rendszerbe. Ráadásul az adatbevitel sokszor már korábban összegyűjtött, papírra vetett információ begépelését jelenti.

Automatikus módszerek

A kézi adatbevitel hátrányainak kiküszöbölésére számos automatikus adatbeviteli módszer látott napvilágot. Ezek közös jellemzője, hogy valamilyen egyszerű indítójel hatására az információ automatikus, gépi beolvasása történik meg.

Optikai karakterfelismerés (OCR)

A hagyományos módszerek számokat és nagybetűket tartalmazó karakterkészletet használnak, a legismertebbek az OCR-A és OCR-B fontok.

OCR-A

ABCDE12345

Az információ leolvasása kamera jellegű olvasóval történik, amely az azt hordozó felületet pásztázza, leolvassa, majd visszaadja a kódolt információtartalmat.

Mágneses tintás karakterfelismerés (MICR)

Elsősorban banki alkalmazásokra kifejlesztett módszer, ahol a megfelelően kialakított betűkészlet mágneses tulajdonságokkal rendelkező tinta segítségével kerül fel az információhordozó anyagra. Ez legtöbbször banki felhasználású csekkeket jelent.

Mágnescsík

Viszonylag nagy mennyiségű információt lehet kódolni egy mágnescsík felületén, amire a bankkártyák jelentik a közismert gyakorlati pél-

dát. Az információ a számítógépekhez használt hajlékonylemezekhez hasonló módon írható, majd később visszaolvasható. A viszonylag szűk felhasználási kör annak a következménye, hogy a kódolás csak speciális eszközökkel végezhető, kicsi a környezeti hatásokkal szembeni ellenálló képesség, és a visszaolvasáshoz a felületen végig kell húzni a leolvasó egységet.

Beszédfelismerés

Ma már rendelkezésre állnak olyan berendezések, amelyek egy korábbi tanulási folyamatot felhasználva képesek az emberi beszéd felismerésére. A szóban forgó adatbeviteli eljárás nagy hátránya az operátortól, annak hangjától való függőség és a viszonylag bonyolult technikai megoldás. A számítógépen egy hosszabb szöveg begépelését segíti a beszédfelismerő program, amelynek csak „be kell diktálni" a mondanivalónkat, és az helyettünk „begépeli". Még a helyesírásellenőrzésre is ügyel.

Gépi alakfelismerés

Az előzőhöz kissé hasonló adatbeviteli módszer. Lényege, hogy egy nagy felbontású televíziókamera által szolgáltatott és később feldolgozott kép felismerése jelenti az adatbeviteli folyamat alapját. Meglehetősen bo-

nyolult a felhasznált alakfelismerő szoftver, s az alkalmazási kör igencsak testre szabott, így csupán egyedi rendszerekben terjedt el ez a technika. Közismert alkalmazás a szem íriszének vagy az ujjlenyomatnak a felismerése, amely minden embernél más, így egyértelmű és biztonságos felismerést tesz lehetővé.

Rádiófrekvenciás azonosítás

A rádiófrekvenciás azonosítást használó rendszerek olyan tárgyakat tudnak azonosítani, amelyek a rendszer számára optikailag láthatatlanok is lehetnek. Másik előnyük, hogy egy időben több tárgy azonosítása is megtörténhet. Működési elvük egyszerű. Egy adóberendezés rádiófrekvenciás jelet sugároz ki a térbe. A rádiós azonosító lapkán elhelyezett pi-

ciny áramkör ezt az energiát felhasználva működésbe lép, és visszasugároz például egy egyedi azonosítót. Az összetettebb lapkák arra is képesek, hogy adatot vegyenek és tároljanak, illetve küldjenek vissza. Tipikus alkalmazási terület az áruvédelem, amely tulajdonképpen ennek a technikának egy speciális, egybites változata, vagy a vasúti szállítóeszközök, háziállatok nyomon követése. Napjainkra az intelligens lapkák és az antennák mérete olyan kicsiny lett, hogy öntapadós címkékben is elhelyeznek ilyen rádiófrekvenciás azonosító chipeket, ezek programozása a címke kinyomtatása alkalmával automatikusan történik.

Chipkártya

A hitelkártyákhoz hasonló kivitelű eszközök, általában memóriachipet és valamilyen feldolgozó áramkört tartalmaznak integrálva. Előállításuk viszonylag költséges, ugyanakkor olvasásuk gyors és megbízható. Felhasználásuk napjainkban egyre jobban terjed: az elektronikus pontgyűjtés, a telefonkártya, az elektronikus pénztárca és számtalan más alkalmazás alapul ezen a technológián.

Gombmemória

Ez egy viszonylag új technológia, ahol kis memórialapkákat egy gombelem méretű és alakú acélperselybe erősítenek. A kis tokocska tökéletes szigetelést biztosít, ugyanakkor lehetőség van a kétirányú kommunikációra. Gyakorlatilag bármilyen tárgyhoz hozzáerősíthető, és ezek a kis memóriagombok több ezer karakternyi információ tárolására képesek. Általában mindegyik el van látva egy egyedi és megváltoztathatatlan azonosító kóddal. A tápellátást egy aprócska elem biztosítja. A memóriatartalom írható és olvasható egy megfelelő olvasófej hozzáérintésével.

Vonalkód

A vonalkód a felsorolásban az utolsó, ám elterjedtségét tekintve messzemenően az első helyen álló azonosítási technika. Statisztikai adatokra támaszkodva megállapítható, hogy a vonalkód az automatikus azonosítási ipar több mint 75%-át tudhatja magáénak.

Ezt köszönheti olcsó és viszonylag egyszerű előállíthatóságának, valamint könnyű és megbízható olvashatóságának. Az alábbi táblázat röviden összehasonlítja a felsorolt azonosítási technikák legfontosabb jellemzőit:

	20 kar beolv. idő	Cimke ktsg.	Olvasó ára	Helyett. hiba
Kézi adatbevitel	10 sec	Alacsony	Alacsony	Magas
OCR	4 sec	Alacsony	Közepes	Közepes
MICR	5 sec	Közepes	Magas	Közepes
Mágnescsík	3 sec	Közepes	Alacsony	Alacsony
Hangfelismerés	20 sec	Alacsony	Magas	Magas
Rádiófrekvencia	2 sec	Magas	Magas	Alacsony
Chip kártya	2 sec	Magas	Közepes	Alacsony
Vonalkód	1 sec	Alacsony	Alacsony	Alacsony

Miért a vonalkód jelenti a legelterjedtebb automatikus adatbeviteli technikát? A válasz a gyakorlati, gazdaságossági szempontok figyelembevételével egyszerűen megadható:

- a legolcsóbb technikák egyike,
- a legpontosabb és legmegbízhatóbb eljárások egyike,
- előállítása és nyomtatása széles körben hozzáférhető,
- kis és nagy információkapacitású kódok egyaránt rendelkezésre állnak.

A jelenleg használt vonalkódok között már nemcsak a hagyományos egydimenziós kódokkal találkozunk, hanem egyre több alkalmazásban jelenik meg a nagyságrendekkel nagyobb kapacitású kétdimenziós változat.

Az automatikus azonosítás azonban nemcsak az adatbeviteli technológia gazdaságossági szempontjából fontos, hanem szerepet kap a különféle logisztikai folyamatok technikai hátterének biztosításában. Az automatikus azonosítási módszerekkel a felhasználó a fizikai anyagáramlási folyamatokat pontosan követheti, ha biztosítani tudja az információ egyidejű gyűjtését és áramlását.

Az ipari és kereskedelmi szférában egyre növekvő volumenű termékáramlás tapasztalható. A határokon belüli és az országok közötti kereskedelem növekedési üteme jóval meghaladja az előállított termékek mennyiségének növekedési ütemét. Ennek fő oka a termelőegységek és az országok közötti növekvő munkamegosztás. Ez egyfelől együtt jár a hatékonyság és a termelékenység növekedésével, ugyanakkor nő az egymásrautaltság és a termék-, illetve anyagáramlási folyamatok mennyisége. Ezt az áramlási folyamatot kell kísérnie egy jól meghatározott és megbízható információáramlási folyamatnak.

Biometrikus azonosítás

Összefoglaló

Ez a fejezet széles áttekintést nyújt a biometria tárgyköréről, arról, hogy azt hogyan használják, hogyan mérik a teljesítőképességét, milyenek a tipikus rendszerek és a gyakorlati alkalmazások.

Mi a biometria, és miért kell vele foglalkoznunk?

A biometriát legjobban úgy határozhatjuk meg, mint olyan mérhető testi, illetve viselkedésbeli jellemvonások összességét, amelyek mérése alkalmas arra, hogy egy adott személy azonosságát ellenőrizni lehessen. Ezek a következőket foglalják magukban:

- ujjlenyomat-ellenőrzés,
- retina- és íriszletapogatás,
- kézgeometria-vizsgálat,
- hanganalízis,
- arcfelismerés,
- egyéb technikák.

Ezek minden olyan területen érdeklődésre tarthatnak számot, ahol lényeges az adott személyek azonosításának ellenőrzése. Kezdetben ezeket a technikákat elsődlegesen a különlegesen nagy biztonságú alkalmazásokban használták, de napjainkban már sokkal szélesebb körben találkozhatunk felhasználásukkal.

Mi a baj az azonosító kártyákkal és személyes azonosító számokkal?

A PIN (Personal Identification Number – személyes azonosító szám) volt az egyik első azonosító, amelyet automatikus felismerés céljára lehetett felhasználni. Azonban tudnunk kell, hogy ez a PIN felismerését jelenti, és nem azét a személyét, aki a PIN-t szolgáltatta. Ugyanez vonatkozik a kártyákra és egyéb jelekre, jelzésekre is. Egy jelet, jelzést könnyen fel lehet ismerni, de azt bárki adhatja. A biometrikus jellemző azonban nem vihető át egyik személyről a másikra (az igen bonyolult sebészeti és plasztikai műtétek taglalása nem tartozik ezen írás témájához). Ha az ellen-

őrzési folyamatot felhasználóbarát módon automatizálni lehet, akkor széles út nyílik a biometria integrálására a különböző eljárásokba.

Mit jelent ez a gyakorlatban?

Azt jelenti, hogy a személy azonosítása egyrészt sokkal korszerűbb módon végezhető el, másrészt az eljárás sokkal pontosabb, mivel a biometriai eszközöket nem lehet könnyen becsapni.

Az utazással és turizmussal kapcsolatosan a bevándorlás-ellenőrzésre, a beszállókapuknál történő személyazonosításra és egyéb, biztonsággal összefüggő funkciókra gondolunk. Ezenkívül azonban igen nagyszámú potenciális alkalmazásra van lehetőség olyan területen, mint a marketing, az utasok megkülönböztetett kiszolgálása, az on-line helyfoglalás, a kapcsolódó programok és így tovább, ahol a biometria igen hasznosan integrálható lehet egy meghatározott folyamat bizonyos lépésénél. Ezen túlmenően vannak vállalatokhoz, intézményekhez kapcsolódó alkalmazások, mint például a számítógépes munkahelyek védelme, a hálózati hozzáférés vezérlése, a fizikai beléptetés-ellenőrzés és egyéb potenciális alkalmazások.

Ez nem azt jelenti, hogy a biometria egy „minden betegségre alkalmas gyógyír" valamennyi, személyi azonosítással kapcsolatos tevékenységre – ettől távol állunk! De igen nagy érdeklődésre számot tartó új eszköz napjaink technológiai eszköztárában, amelyet jó, ha figyelembe veszünk, amikor az új évezred megoldásait dolgozzuk ki.

Mindez bizonyára tudományos fantasztikum, nem látjuk ezeket működés közben, a mindennapok gyakorlatában...

Több mint 10 éve ez egy gyakori és olykor jogos megjegyzés volt, mivel számos korai biometriai eszközt csak nehézkesen lehetett kezelni a gyakorlatban, és abba az árkategóriába tartozott, amely meggátolta széles körű felhasználását néhány, igen nagy biztonságú alkalmazás kivételével, ahol azt életképesnek vélték.

Napjainkra a helyzet alapvetően megváltozott, nemcsak az igen jelentékeny technikai fejlődés következtében, amely pontos, kifinomult termékeket szolgáltat, hanem abból eredően is, hogy a költségek olyan szintre csökkentek, ami lehetővé teszi az eszközök széles körben való elterjedését. Ezen túlmenően a felhasználásukra és alkalmazásokba törté-

nő integrálásukra vonatkozó ismeretek már nem tartoznak a „fekete mágia" körébe, amelyet annak néhány (ennek megfelelően díjazott) püspöke gyakorol, hanem a vonatkozó technológia mindennapos gyakorlatának részei, amelyekről egy átlagos hatéves gyermek nemsokára sok mindent el tud majd mondani nekünk.

Jelen fejezet hátralévő része erről részletesebben szól, és biztos hátteret nyújt ahhoz, hogy elmélyedhessünk ebben az érdekes és izgalmas technológiában.

A biometria kezdetei

Sokan úgy vélekednek a biometriáról, hogy az egy tudományos-fantasztikus, jövőbeli technológia, amelyet a napenergiával hajtott autókkal, élelmiszertablettákkal és egyéb ördögi eszközökkel együtt fogunk használni valamikor a közeli jövőben. Ez a kép azt sugallja, hogy ezek a huszonegyedik század cybercivilizációjának termékei.

Valójában azonban a biometriai ellenőrzés alapelveit jóval korábban ismerték meg, és tették a mindennapos gyakorlat részévé. Hogy pontosak legyünk, évezredekkel ezelőtt Nílus-völgyi eleink rutinszerűen alkalmaztak biometriai ellenőrzést számos mindennapi üzleti helyzetben. Jó néhány utalással rendelkezünk arra nézve, hogy egyéneket formálisan azonosítottak egyedi fizikai, fiziológiai paraméterek alapján, mint sebhelyek, mért fizikai jellemzőkkel, mint arcvonások, szem színe, magasság és így tovább. Ez előfordulhatott a mezőgazdaságban végrehajtott tranzakcióknál, ahol gabonát és egyéb élelmiszereket szolgáltattak be a központi tárolóhelyekre, valamint különböző jogi eljárásokkal kapcsolatosan. Természetesen elődeink (tudomásunk szerint) nem rendelkeztek automatizált elektronikus biometriai olvasókkal és számítógépes hálózatokkal, s nem olyan nagyszámú személlyel foglalkoztak, amire napjainkban nekünk számítanunk kell, de az alapelvek azonosak voltak.

Később, a XIX. században megnőtt az érdeklődés a terület iránt, a kriminológiai kutatások megpróbálták a fizikai jellegzetességeket összekapcsolni a bűnügyi irányzatokkal. Ennek érdekében különféle mérőeszkö-

zöket állítottak elő, és nagyszámú adatot gyűjtöttek össze. Az eredmények alapján nem lehetett végső következtetéseket levonni, de az egyén fizikai jellemvonásainak mérése gyakorlat maradt: az ujjlenyomat-ellenőrzés nemzetközi módszerré vált a rendőrhatóságoknál.

Gyakran vitatják az ujjlenyomatok abszolút egyediségét vagy különbözőségét. Az ujjlenyomatok ellenőrzésére használt kritériumok számos országban különböznek abban, hogy több vagy kevesebb minutiapont szükséges az azonosításhoz (a minutiapontokban az ujjlenyomat redői elágaznak vagy megszűnnek). Ennek ellenére annak idején ez volt a legjobb rendelkezésre álló módszer, és még ma is az elsődleges eljárás a rendőrhatóságok számára, bár napjainkban a fejlettebb országokban az ujjlenyomatok azonosítási eljárását már automatikus módszerekkel végzik.

Ezzel a háttérrel már egyáltalán nem meglepő, hogy az elektronika és a mikroprocesszorok teljesítményének kihasználásával a személyazonosítás automatizálására mind a katonai, mind a polgári szektorban számos elgondolás született. Különböző projekteket kezdeményeztek a biometria lehetőségeinek kutatására, és ezek közül az egyik végül egy nagy és meglehetősen ormótlan kézgeometria-olvasó előállításhoz vezetett. Nem volt túl szép, de működött, és tervezőit arra ösztönözte, hogy az eszközt tovább tökéletesítsék. Végül néhány specializálódott vállalat alakult, és egy sokkal kisebb és jóval többet tudó kézgeometriai olvasót fejlesztettek ki. Ez az eszköz jól működött, és kedvező fogadtatásra talált számos biometriai projektben szerte a világon.

Ezzel párhuzamosan az egyéb biometriai módszereket, például az ujjlenyomat-ellenőrzést addig javították, amíg megbízható, könnyen alkalmazható eszközöket kaptak. Az utóbbi években jelentős érdeklődést tapasztaltunk az íriszletapogatás és az arcfelismerési technikák iránt, amelyek az érintésmentes technológia lehetőségét nyújtják, bár további kérdések vetődnek fel velük kapcsolatban.

Az 1900-as évek utolsó évtizedében a biometrikus azonosító rendszerek ipara az egyetemek és a tudományos kutatóintézetek laboratóriumainak fellegváraiban működő, termékeinek eladásával küszködő, marginális ágazatból jelentékeny alkalmazások tekintélyes mennyiségű eszközét szállító, globális iparággá fejlődött.

Sok biometriai jellemzőre való hivatkozással találkozhatunk, ezek közül némelyek egyáltalán nem praktikusak, még akkor sem, ha technikailag érdekesek lehetnek. A gyakorlati használatra alkalmas, „népszerű" biometriai jellemzők, úgy tűnik, jelenleg a következő módszerek köré csoportosulnak:

Ujjlenyomat-azonosítás

Az ujjlenyomat-azonosításnak számos lehetséges megközelítése létezik. Egyes eljárások a minutiaazonosítás hagyományos rendőri módszerének emulációját használják, mások egyszerű alakzatazonosító eszközök, ismét mások sajátos, egyedi megközelítést alkalmaznak, határtartományokat és ultrahangos letapogatást foglalva magukban. Egyesek ezek közül felismerik, amikor élő ujjat tesznek a szenzorra, mások nem. Jelenleg a biometrikus eszközök közül legnagyobb számban az ujjlenyomat-vizsgáló eszközöket használják.

A megfelelő pontosságú (alacsony hibás elfogadási aránnyal rendelkező), potenciálisan elfogadható ujjlenyomat-olvasó használata során gyakrabban találkozhatunk használatbeli hibákkal a nem eléggé „fegyelmezett" felhasználók között. Az ujjlenyomat-ellenőrzés jó választás lehet házon belüli rendszerekre, ahol kielégítő tájékoztatás és oktatás biztosítható a felhasználók részére, és ahol a rendszereket ellenőrzött körülmények között használják.

Nem meglepő, hogy az az alkalmazási terület, ahol a cél a számítógépes munkahelyek hozzáférésének védelme, csaknem kizárólag ujjlenyomatokon alapszik, a viszonylag alacsony költségek, a kis méret és a könnyű integrálhatóság miatt.

Kézgeometria

Amint a név is sugallja, a kézgeometria a kéz és az ujjak fizikai karakterisztikáinak mérésével foglalkozik. Mint az egyik legjobban elterjedt módszer, a kézgeometria nemcsak gyors és pontos, hanem könnyen kezelhető is. Ez a módszer nagy felhasználói bázis esetén is alkalmazható, vagy olyan személyeknél, akik a rendszert ritkán használják, és ennél-

fogva kevésbé gyakorlottak a használatában. A felismerés pontossága igen nagy, eközben a rugalmas elfogadásiszint-szabályozás és konfigurálás a felhasználók igen tág körének igényeit elégíti ki. A kézgeometria-olvasók alkalmazási területe igen széles, beleértve a munkaidő-nyilvántartást is, ahol ezek az eszközök igen népszerűnek bizonyultak. A más rendszerekbe, illetve folyamatokba történő könnyű integrálhatóság és az egyszerű használat a kézgeometriát nyilvánvalóan számos biometriai projekt első lépcsőjévé teszi.

Hangazonosítás

Potenciálisan nagy érdeklődésre számot tartó technika – elég arra gondolnunk, hogy a hanggal folytatott kommunikáció mekkora teret foglal el mindennapi életünkben. Egyes alkalmazások falra szerelhető érzékelőket használnak, míg mások annak a lehetőségét dolgozták ki, hogy hogyan lehet beilleszteni a hangellenőrzést a konvencionális telefonkagylókba. Mialatt nagyszámú hangellenőrző termék került piaci bevezetésre, ezek közül nem egy jó néhány nehézséggel találkozik a gyakorlatban: az átalakítók és a helyi zajok következtében. Ezen túlmenően a regisztrálási eljárás gyakran sokkal bonyolultabb, mint más biometriai termékeknél, ami arra vezetett, hogy bizonyos körökben a hangellenőrzés használatát nem veszik szívesen. Ennek ellenére sok munkát végeztek a hangazonosítással kapcsolatosan, s ezek továbbra is folytatódnak, így érdeklődésre tarthat számot a fejlődés nyomon követése.

Retinaletapogatás

Bevezetett technológia, amelyben a retina egyedi alakzatát egy alacsony intenzitású fényforrás optikai sokszorozó felhasználásával letapogatja. A retinaletapogatás meglehetősen pontosnak bizonyult a használat során, de azt teszi szükségessé, hogy a felhasználó belenézzen egy érzékelőbe, és egy megadott pontra összpontosítsa tekintetét. Ez nem különösen kényelmes, ha valaki szemüveget visel, vagy ha nem szeretne kontaktusba kerülni az olvasóeszközzel. Fentiek miatt a retinaletapogatást a felhasználók nehezebben fogadják el, bár maga a technológia jól működhet. A vezető termékeket a kilencvenes évek közepén áttervezték, ami jobb felhasználói interfészt eredményezett, ám ennek ellenére –

a tömeges alkalmazásokkal összevetve – marginális biometriai technológiának tekinthetjük.

Íriszletapogatás

Az íriszletapogatás kétségtelenül a legkevésbé tolakodó módszer a szem jellegzetességein alapuló biometriában. Ehhez egy közönséges CCD-kamerát használnak, és nincs szükség közvetlen kontaktusra a felhasználó és az olvasó között. Ezenkívül az átlagosnál jobb azonosítási teljesítménnyel rendelkezik. A technológia felkeltette a fejlesztők figyelmét, és számíthatunk rá, hogy ennek eredményeképpen további termékek kerülnek kibocsátásra. Bebizonyosodott, hogy ezek a berendezések szemüveges felhasználóknál és különböző etnikai csoportok esetén is működnek. Az egyszerű felhasználás és az integrálhatóság nem erős oldaluk az íriszletapogató berendezéseknek, de új termékek bevezetése esetén ezeken a területeken fejlesztésekre számíthatunk.

Aláírás-ellenőrzés

Az aláírás-ellenőrzés egyéb alkalmazott technológiák melletti használata azok hatásosságát támogatja, igaz, ez elmondható mindenfajta biometrikus azonosításról. Az emberek megszokták, hogy a különféle tranzakcióknál az aláírásukat használják a személyazonosság hitelesítésére, és legtöbbször nem látnak semmi különöset abban, hogy ezt biometriai módszerrel egészítsék ki. Az aláírás-ellenőrző berendezések a gyakorlatban meglehetősen pontosnak bizonyulnak, és természetesen olyan alkalmazásokhoz ajánlhatók, ahol az aláírás elfogadott azonosító. Érdekes azonban, hogy más biometriai módszerekhez képest viszonylag kevés helyen alkalmazzák napjainkban.

Arcfelismerés

Ez a technika jelentős érdeklődést váltott ki, de lehetőségeit sokszor félreértelmezik. Gyakran merülnek fel kifogások olyan arcfelismerő berendezésekkel kapcsolatban, amelyek használatát a gyakorlatban nehéz megindokolni. Két statikus kép összehasonlítása (vannak olyan rendszerek, amelyek mindössze ezt végzik el, ezek egyáltalán nem tekinthetők biometrikus rendszereknek) nyilvánvalóan más feladat, mint egy személy

azonosítása egy adott csoporton belül. Az arcleolvasás elfogadottsága könnyen érthető a felhasználók szemszögéből, de realisztikusnak kell lennünk a technológiára vonatkozó elvárásainkban. Napjainkban az arcfelismerő rendszereknek korlátozott sikerük van a gyakorlati alkalmazásokban. Azonban a fejlődés folytatódik ebben az irányban is. Ha a technikai akadályokat le tudjuk győzni, az arcfelismerés elsődleges biometriai módszerré válhat.

Arcthermogram

Az arcthermogram olyan felvétel, amelyet infrakamerával készítenek, és az arc hőtérképét mutatja. A gép mintaazonosító algoritmust használva ellenőrzi a relatív hőmérsékletkülönbségeket az arcon, amelyek függetlenek a kortól, az egészségi állapottól és a test hőmérsékletétől is. A módszer kivételes pontosságú, 19 000 „adatpont" felvételével képes megkülönböztetni az egypetéjű ikreket – akár sötétben is. Ennek a technológiának a fejlesztése manapság a költségek csökkentésére irányul, annak érdekében, hogy minél szélesebb körben váljék alkalmazhatóvá az azonosítási és hitelesítési eljárásokban. Az arcthermogram a legígéretesebb módszer – a legpontosabb, leghatékonyabb és legbiztonságosabb eljárást kínálja, ha a technológiai költségek elfogadható szintre csökkennek.

Más biometriai módszerek is léteznek, beleértve a szag, a fülcimpa és egyéb paraméterek azonosítását. Ezek technikailag ugyan érdekesek lehetnek, de ma még nem tekinthetők megoldásnak napjaink alkalmazásaiban.

Alkalmazások – ami napjainkig történt

Napjaink biometriai alkalmazásainak többsége általában nem ismert a nagyközönség előtt. Ez annak a következménye, hogy a legtöbb alkalmazás olyan, viszonylag kis cég által kerül bevezetésre, amely ilyen jellegű rendszerekre specializálódott. Az ide tartozó alkalmazások közül lássunk néhány közérdeklődésre számot tartó példát!

• Büntetés-végrehajtó intézetek, ahol a fogva tartottakhoz érkező látogatókat azonosítják, hogy azok a látogatás ideje alatt a fogva tartottakkal ne cserélhessenek helyet – ami amúgy ismerős jelenség a börtönökben a világ minden pontján.

• Gépjárművezetői engedélyek kiadásánál, elkerülendő, hogy a gépjárművezetők (különösen a kamionsofőrök) több jogosítványt állíttassanak ki maguknak, vagy egymás között cserélgethessék azokat.

• Kedvezményes étkeztetési rendszerekben, például egyetemeken, ahol a hallgatók támogatásban részesülnek. Ilyen rendszerekben sok helyütt jelentős visszaélések tapasztalhatók.

• Pénzbeli támogatási rendszerek. Az USA-ban számos állam jelentős mennyiségű pénzt takarított meg biometriai ellenőrzési eljárások bevezetésével. Nem okozott meglepetést, hogy azoknak a személyeknek a száma, akik az eljárásban támogatásra tartanak igényt, drámaian csökkent, igazolva, hogy a biometrikus ellenőrzés hatékony eszköz lehet a jogtalan igénylők kiszűrésére.

• Határellenőrzés. Figyelemre méltó példa az amerikai INSPASS eljárás, melynek során az országba érkezőket olyan kártyával látták el, amely lehetővé tette számukra, hogy az elhelyezett biometrikus terminálokat használják, és elkerüljék a hosszadalmas sorbaállást a bevándorlási hivatalokban.

• Személyi igazolvány. Bruneiben mintegy 700 000 embert láttak el olyan chipkártya alapú személyi igazolvánnyal, amely tulajdonosának ujjlenyomatadatait is tartalmazza, így téve rendkívül egyszerűvé, gyorssá és biztonságossá annak alkalmazását.

• Szavazórendszerek, ahol a jogosult politikusok igazolják személyazonosságukat az eljárás során. Ennek segítségével megakadályozható a „helyettesek" által történő szavazás.

A felsoroltak csak kiragadott példák. Készülékek tízezreit telepítették már pénzügyi intézetektől, bankoktól, nagyvállalatoktól, fontos kormányzati és állami intézményektől kezdve katonai objektumokon, repülőtereken, laboratóriumokon át egészen a börtönökig. A könnyű használatnak és a nagy megbízhatóságnak köszönhetően a biometrikus módszer lett a mérce a belépési jogosultságot ellenőrző alkalmazások terén.

A biometrikus alkalmazások területeinek felsorolása olyan hosszú listát tenne ki, amely nemcsak jelen fejezet, de a könyv terjedelmét is bőven meghaladná.

Jövőbeni alkalmazások – néhány általános gondolat

Számos, biometriai alkalmazások használatára vonatkozó terv létezik. Íme, néhány példa:

Pénzkiadó automaták használata

A vezető bankok szinte kivétel nélkül kísérleteznek biometrikus elven működő rendszerekkel a pénzkiadó automaták használatával kapcsolatban, valamint hogy a biometriát általános eszközként használják a kártyákkal történő visszaélések ellen. Ám ezek a kísérletek ritkán tartalmaznak a teljes folyamatba integrált eszközöket, pedig ez könnyen elérhető lenne a biometria segítségével. Meggondolásra késztetik őket azok a – meg nem alapozott – vélemények, melyek szerint ilyen alkalmazásokkal potenciális ügyfeleket veszíthetnek. Mégis meglepő, hogy a bankok és pénzintézetek mind ez ideig nem alkalmazzák ezt a technológiát átfogó rendszerekben. Ennek okát valószínűleg nem az elméletekre vonatkozó kételyekben vagy technológiai, technikai hiányosságokban kell keresnünk, magyarázatot talán inkább a bankok minden vonatkozásban tapasztalható konzervativizmusa, újtól való idegenkedése adhat.

Személyi számítógépes munkahelyek és hálózati hozzáférések

Sokáig ez gyakran felvetődő, de ritkán megvalósított terület volt, mindaddig, amíg a legújabb fejlesztések hatására a biometriai eszközök ára drámaian zuhanni nem kezdett. Olyan általánosan ismert nevekkel együtt megjelenve a piacon, mint a Sony, a Compaq, a KeyTronics, a Samsung és mások, ezek az eszközök már csaknem standard számítógépes perifériának számítanak. Alkalmazásuk megteremti az átmenetet a tudomány és a fantasztikum világa, valamint a biometrikus eszközök mindennapos használata között.

Utazás és turizmus

Ebben az iparban sokan vannak, akik szeretnének egy sokcélú felhasználói kártyát előállítani az utazók számára. Ez a biometriai azonosítókat hordozó kártya lehetővé tenné, hogy segítségével az utazók a különböző, törzsutasok számára biztosított kedvezményeket igénybe vegyék, a határátlépést ellenőrző rendszerekben használják, valamint fizetési eszközként repülőjegyek vásárlásánál, szállodai költségek, bérautók díjainak kiegyenlítésénél stb. alkalmazzák – s mindezt kényelmesen, egyetlen kártyával.

Technikailag ez már ma lehetséges lenne, de politikai és kereskedelmi szempontból még számos kérdés vár megoldásra. Szerencsére ezek nem áthághatatlan akadályok. A legnagyobb kihívást itt egyébként az jelenti, hogy miként csomagoljuk be a kezdeményezést oly módon, hogy valóban vonzóvá tegyük a felhasználók számára.

Internetes tranzakciók

Itt általában mindenki a vonali tranzakciókra gondol, amely egy nyilvánvaló terület a biometria számára, bár néhány kérdés azért felmerül ezzel összefüggésben. Ha feltételezzük, hogy a költségek leszoríthatók olyan szintre, hogy a biometriai olvasó (és feltehetően a chipkártyaolvasó is) könnyen illeszthetővé váljon a számítógéphez, továbbra is fennáll a kétoldali hiteles regisztráció problémája. Természetesen, ha hitelkártyánk már hordozza biometriai adatainkat, az a dolgokat jelentősen leegyszerűsíti. Érdekes, hogy néhány biometrikus olvasót gyártó cég együttműködik titkosítási rendszerek fejlesztésével foglalkozó vállalatokkal, amelyek ily módon bővíthetik szolgáltatásaikat. Feltehetően érdekes fejleményekre számíthatunk ezen a téren a közeljövőben.

Telefonos tranzakciók

Számos távközlési központ vezetője nagy súlyt fektet a biometria alkalmazására. Azonban a hangazonosítás a biometria bonyolult területe, különösen akkor, ha nem áll rendelkezésre a közvetlen ellenőrzés lehetősége az átalakítók felett. A telefonkagylók, valamint a vonalak minősége és a felhasználói környezet sokszínűsége jelentős kihívás a hang-

ellenőrző technológia számára, s ehhez társul még a potenciális felhasználók körében tapasztalható igen változatos hozzáállás.

A technológia jól működhet ellenőrzött zárt rendszerek esetében, de megvalósítása igen bonyolulttá válik nagyobb léptékű terveknél. A felhasználóbarát hibajavítás és a hibakövetkezmények kiküszöbölési eljárásának megtervezése automatizált rendszerek esetén nem éppen gyenge idegrendszerűeknek való feladat.

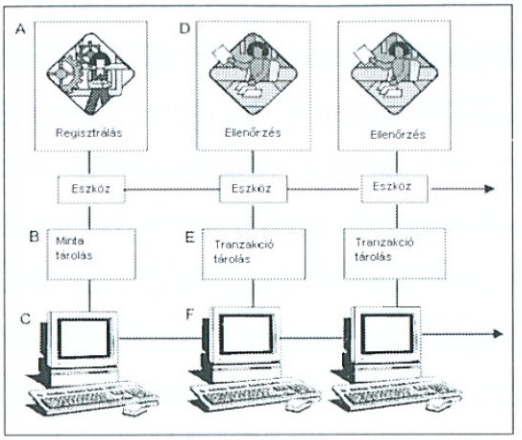
Ezzel együtt feltehetően ezen a téren is további fejlesztéseknek leszünk tanúi, mert nincs kétségünk afelől, hogy ebben a tekintetben is jelentős kutatómunka folyik.

Személyazonosító kártyák

A személyazonosító kártyán tárolt biometrikus adatok igen hasznosak lehetnének, ha egy ilyen kezdeményezés állami támogatást élvezne. Sajnos számos államban túl sokan vannak azok, akik határozottan nem akarják magukat azonosítani. Ez általában azzal jár együtt, hogy bármely erre vonatkozó javaslat hamarosan politikai csatározássá fajul. Ez a technológia egy ki nem használt lehetőséget képvisel. Érdekes, hogy Angliában egyes önkormányzatok biometrikus adatokat hordozó „polgárkártyákat" bocsátottak ki, amelyek tulajdonosai különböző előnyökben részesülhetnek: árkedvezmények a helyi üzletekben való vásárlás és bizonyos szolgáltatások igénybevétele esetén. Sajnos ez volumenében nem jelent túl nagy kihívást a biometriai ipar számára, bár ezek már ténylegesen személyazonosító kártyák. Van azonban olyan alkalmazási példa is, amely országos szinten használja ki a rendszerben rejlő lehetőségeket. Ez a Brunei szultánságban bevezetett, a világon a legmodernebbnek és legbiztonságosabbnak tartott személyi igazolvány, amely a hitelkártyaméretű intelligens chipkártyán a tulajdonos digitalizált ujjlenyomatának adatait is tartalmazza. A kártyát nemcsak a mintegy 300 000 helyi lakos számára készítették el, de hasonló – csak más-más színű – kártyát kapnak a tartózkodási engedéllyel rendelkezők, a vendégmunkások és a gyakori beutazók is. Ezzel a rendszer használóinak száma mintegy 700 000-re tehető. A hatóságok és a felhasználók a fő előnyök között általában a hamisíthatatlanságot, a gyorsaságot és a könnyű kezelhetőséget szokták kiemelni.

Hogyan működik? Tipikus eszköz/rendszer folyamatábra

Minden egyes biometriai eszköznek és rendszernek megvan a maga működési módszere, ám bizonyos általánosságok elmondhatók arra vonatkozóan, hogy tipikusan hogyan történik a biometrikus azonosítás. Ezeket az alábbiakban foglaljuk össze.



[A] Mielőtt valakinek biometrikusan akarjuk elvégezni az azonosítását, mintát kell vennünk a választott biometriai adatokból. Erre a mintára mint biometrikus maszkra fogunk hivatkozni a továbbiakban. Ez a minta szolgáltatja majd a referenciaadatokat az azonosítás és ellenőrzés során. A regisztráláskor általában több mintát vesznek (tipikusan hármat), azért, hogy átlagolás segítségével reprezentatív maszkot kaphassanak. Erre a maszkra történik aztán a hivatkozás egy azonosítón keresztül (amely tipikusan egy személyazonosító szám [PIN] vagy egy kártyaszám, ha ezt egy már létező ellenőrzési adathordozóval [kártyával] együtt használjuk) az élő mintával történő összehasonlításkor. A regisztrálási folyamat és az ennek eredményeképpen létrejött maszk minősége kritikus tényezője az adott biometriai alkalmazás sikerének. Egy rossz minőségű maszk gyakran okoz problémát a felhasználó számára, és ez a gyakorlatban a regisztrálás törléséhez vezethet.

[B] A maszk tárolása – különösen nagy, több ezer személyt kezelő alkalmazásoknál – igen sokrétű probléma. A lehetséges opciók a következők:

1) A maszk biometriai olvasóeszközön belül való tárolása.

2) A maszk központi tárolási helyen való tárolása, távol a biometriai olvasóeszköztől.

3) A maszk adathordozón, például chipkártyán való tárolása.

Az első opció, a maszk biometriai eszközön belül való tárolása éppúgy járhat előnyökkel, mint hátrányokkal, attól függően, hogy pontosan hogyan történt a kivitelezés. Előnye a gyors működés, mert egy viszonylag kisszámú maszkot hatékonyan tudunk tárolni magán az eszközön belül is. Ily módon a maszk elérése nem függ külső folyamatoktól. Egyes esetekben, ahol az azonosító egységek közvetlen hálózatban vannak összekötve, a maszkok a hálózaton belül megoszthatók.

A hátrány abból származhat, hogy a maszkok bizonyos mértékben sebezhetők, és attól függnek, hogy az azonosító eszköz jelen van, és kifogástalanul működik. Ha valami történik az azonosító eszközzel, lehet, hogy újra kell telepíteni a maszkadatbázist a felhasználói adatbázis újraregisztrálásával.

A második opció, a maszkok központi tárolási helyen való tárolása a rendszerprogramozók számára természetes. Ez jól működhet egy biztonságos hálózattal ellátott környezetben, ahol elégséges műveleti sebesség áll rendelkezésre a felhasználó számára láthatatlan maszkvisszakeresésre. Azt azonban figyelembe kell vennünk, hogy egyidejűleg működő nagyszámú olvasó esetén elég nagy adatforgalomra számíthatunk, különösen akkor, ha a felhasználók türelmetlenek, és egymás után többször is ellenőrzési kísérletet kezdeményeznek. A biometriai maszk mérete is hatással lehet a fenti jelenségre, a leggyakrabban használt módszereknél a méret 9 byte és 1,5 kilobyte között változik. Egy másik szempont, amelyet szintén figyelembe kell vennünk, a hálózatkiesés, mert ekkor a rendszer ténylegesen leáll, hacsak nem áll rendelkezésre egyfajta helyi tárolási kapacitás. Ez bizonyos eszközök esetében létrehozható. Ezek az azonosító eszközök a külső tárolót az új felhasználók azonosításához használják, és szükség esetén utasítják a rendszert, hogy keressen a központi tárolási helyen, ha a maszk lokálisan nem található meg.

A harmadik opció a maszk valamely adathordozón (kártyán) való tárolása. Ez két okból lehet vonzó. Egyrészt nem igényli a maszknak sem helyben, sem központi tárolóterületen történő tárolását (hacsak mi magunk nem akarjuk ezt), másrészt a felhasználók magukkal hordják maszkjukat, és bármelyik olvasóhelyen alkalmazhatják azt.

De itt figyelembe kell venni egyéb megfontolásokat is. A felhasználó abban bízik, hogy hatékonyan ellenőrizheti és birtokolhatja maszkját,

ezért nem tárolhatjuk azt valahol a rendszerben. Azonban ha a későbbiekben elveszti vagy megsérti az adathordozót (kártyát), amelyre a maszkot rögzítették, újra kell regisztráltatnia magát. Egy másik szempont lehet az egy egységre eső költség és a rendszer bonyolultsága, ha a chipkártya- és a biometriai olvasókat kombinálnunk kell minden egyes regisztrálásnál és azonosításnál.

Ha a felhasználók nem kifogásolják, megfontolandó a maszkok mind az adathordozón (kártyán), mind a központi helyen való tárolása (2. és 3. opció). Ez a kombinált módszer gyors működést biztosíthat akkor is, ha a kártyaolvasási eljárás valamilyen oknál fogva hibával végződik, vagy ha egy felhasználó elveszti az adathordozóját (kártyáját), és emellett megfelelő azonosítási információt tud szolgáltatni. A maszk tárolására vonatkozó választásunkat bizonyos mértékben a biometriai eszköz megválasztása is befolyásolhatja. Bizonyos eszközök nagyobb rugalmasságot nyújtanak ebben a tekintetben.

[C], [F] A hálózat témájában több változat is rendelkezésre állhat. Bizonyos eszközök integrált hálózati funkcióval rendelkeznek, gyakran RS485-ön vagy RS422-n keresztül, egy erre alkalmas protokollal. Ennek segítségével nagyszámú azonosítóeszközt köthetünk hálózatba, bármely további berendezés hozzáadása nélkül. Ugyanezt megtehetjük egy vezérlőfunkciót betöltő személyi számítógép segítségével is, amelyet a hálózat egyik végéhez kapcsolunk. Ebben az esetben azonban csaknem bizonyos, hogy alkalmazkodnunk kell a szoftver rendszertervéhez, protokolljához.

De megtervezhetjük saját magunk is a hálózatot, a protokollt és a monitorozási rendszert, kihasználva azt az előnyt, amelyet a legújabb generációs biometrikus API-k (Application Programming Interface) nyújtanak, így az olvasók funkcióit közvetlenül is elérhetjük. Ez abszolút rugalmasságot és ellenőrzést nyújt számunkra a rendszer tervezésénél, feltéve, hogy a kiválasztott azonosító eszköz ezt támogatja.

További lehetőség lehet, hogy a szállító által biztosított hálózatot saját felhasználói szoftverrel társítjuk az ellenőrzési pontoknál, amelyek kapcsolódhatnak a felügyeletünk alatt álló más rendszerekhez.

Bizonyos esetekben előfordulhat, hogy már van hálózatunk és ellenőrző interfészünk, amelybe a biometriai eszközök általános szabványon

(Wiegand vagy ABA) keresztül beilleszthetők. Ebben az esetben ezek mint további eszközök jelennek meg, bár külön meg kell vizsgálnunk a maszkok tárolásának és hozzáférésének lehetőségeit.

Az, hogy a hálózat hogyan kezeli a tranzakciókat, kritikus jelentőségű lehet bizonyos alkalmazásokban. Például lehetnek nagy területen megoszló, többszörös termináljaink, amelyek közül mindegyik egyidejű információmegjelenítést kér. Ez gyors és megbízható üzenettovábbítást tesz szükségessé, hiszen minden egyes terminálfelhasználó megkívánhatja, hogy egy megjelenített tranzakció „várakozik" állapotban maradjon mindaddig, amíg nincs válasz. Ehhez kell egy külön, helyi üzenetpuffer és valószínűleg egy priorizálási módszer is, annak biztosítására, hogy a kritikus jelentések azonnal feldolgozásra kerüljenek.

Szükség lehet a terminálszoftver változataira, felhasználók és alapfunkciók szerint. Mindezt biztonságosan és hatékonyan kell beilleszteni az általános hálózatba. Számos felmerülő kérdést kell figyelembe venni ezzel kapcsolatosan, és az általános rendszertervnek ezt tükröznie kell.

[D] Az ellenőrzési eljárás során a felhasználó igazolja azonosságát, vagy a PIN (személyi azonosító szám) megadásával, vagy egy adathordozó (kártya) bemutatásával, majd ennek megerősítésére biometriai adatot szolgáltat, amelyet össze kell vetni a referenciamaszkkal. Az azonosítás ennek megfelelően pozitív vagy negatív (az ezzel kapcsolatos paramétereket később, a teljesítményméréseknél tárgyaljuk). Erről a tranzakcióról feljegyzés készül, amelyet a rendszer elraktároz: vagy helyben, az azonosító eszközön belül, vagy hálózat esetében a központi számítógépen (vagy mindkét helyen).

Bizonyos eszközök esetében, ha nincs megegyezés a maszkok között, a felhasználónak több azonosítási kísérlet is megengedett az ellenőrzés során, mielőtt végleg visszautasításra kerül. Ennek a paraméternek a beállítása több szempontból is megfontolandó. Egyrészt, ugye, meg akarunk adni minden lehetőséget a regisztrált felhasználó számára (akinek nehézségei lehetnek a rendszer használata során), hogy sikeresen azonosítsa magát. Másrészt pedig nem kívánunk felesleges lehetőséget nyújtani a szélhámosoknak a kísérletezésre.

Bizonyos alkalmazások esetében a referenciamaszk automatikusan felújításra kerül minden egyes érvényes tranzakciónál. Ez azt a lehetősé-

get nyújtja a rendszer számára, hogy alkalmazkodjon a felhasználó maszkjának kisebb változásaihoz, amelyek életkori változások, helyi karcolások és egyebek következményei lehetnek. Ez különösen akkor hasznos, ha nagy felhasználói bázissal dolgozunk.

[E] A tranzakciók tárolása azért fontos terület, mert mindenki igényt tart biztonságos visszajelzésre a rendszer használatával kapcsolatban. Bizonyos eszközök csak korlátozott számú tranzakció tárolására képesek, amelyek közül a régebbiek új tranzakció esetén mindig felülírásra kerülnek. Ez addig működhet így, amíg biztosak vagyunk abban, hogy minden ilyen tranzakciót vissza tudunk nyerni, még mielőtt a puffer megtelik, és azok elvesznek. A gyakorlatban egyébként ennek előfordulása nem valószínű, hacsak komoly hálózati hiba nem lép fel. Egyes esetekben szükség lehet arra, hogy minden egyes biometrikus eszköz közvetlen kapcsolatban legyen egy helyi számítógéppel, amelyet periodikusan lekérdezünk (például éjszakánként) abból a célból, hogy a tranzakciókat egy központi helyre vonjuk össze. Mindkét esetben valószínűleg szükség lesz a hibák és rendkívüli események kezelésére, ezek pedig helyi üzenetváltást igényelnek. Ez lehet annyira egyszerű, mint egy áramkör zárása, ami abban az esetben, ha a tranzakció nem sikerül, egy jelzőt hoz működésbe.

Hogy mit tegyünk ezzel a tranzakcióadattal, az már más kérdés. Analizálhatjuk egy létező rendszerben (ha alkalmas formátumban jelenik meg), vagy írhatunk felhasználói alkalmazást a tranzakciók egyidejű jelentésével és egy központi adatbázisba történő felvételével.

A teljesítőképesség mérőszámai

Hibás elfogadások, hibás visszautasítások, azonos hibaarányok, regisztrációra és ellenőrzésre fordított idő – ezek a tipikus teljesítmény-mérőszámok, amelyekre az eszközök gyártói hivatkoznak (hogy ezeket hogyan határozták meg, az már egy másik kérdés). De mit jelentenek tulajdonképpen? Igazak-e ezek a teljesítménystatisztikák a megvalósított rendszerekre? Bizalommal fogadhatjuk-e ezeket az adatokat? Kutassunk tovább!

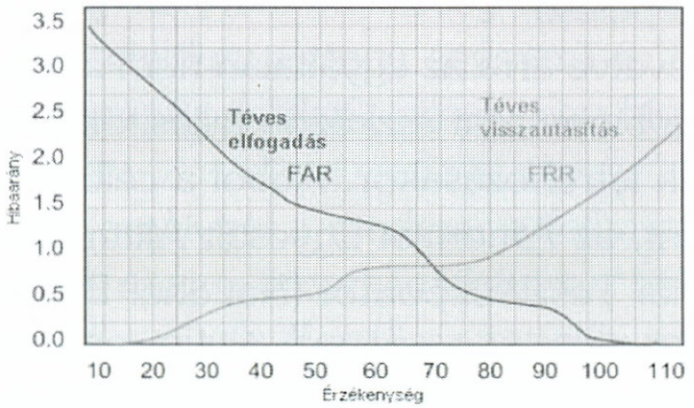
A hibás elfogadás aránya (FAR – False Accept Rates) annak a valószínűségét adja meg, hogy egy szélhámost a rendszer tévesen elfogad.

A hibás visszautasítás aránya (FRR – False Reject Rates) annak a valószínűségét jelenti, hogy egy regisztrált felhasználót visszautasít a rendszer.

Az a mérték, amellyel a rendszer a maszkokat azonosnak ítéli meg, gyakran beállítható egy küszöbérték megadásával, ezzel a rendszer ítélete az egyik vagy a másik irányba módosítható. Ezt az értéket érzékenységnek nevezzük, de nevezhetnénk küszöbértéknek is. Késztethetjük a rendszert nagyobb számú hamis elfogadásra, de kisebb számú hamis visszautasításra (felhasználóbarát) vagy nagyobb számú hamis visszautasításra, de kisebb számú hamis elfogadásra (felhasználóellenes), minthogy a két paraméter kölcsönösen kizárja egymást.

Valahol a szélső értékek között van az a pont, ahol a két görbe metszi egymást. Ez egy realisztikusabb teljesítménymérő szám, mint akár a hibás elfogadások, akár a hibás visszautasítások aránya külön-külön, egymástól függetlenül idézve.

Ezeket a mértékeket százalékokban (a hibatranzakciók százalékában) fejezik ki, egy 0,1% körüli azonos hibaaránnyal, amely tipikusnak mondható.



Azonban a fent említett százalékos hibaarány egy adott eszközre vonatkoztatva számos oknál fogva nem igaz a gyakorlatban. Ezek közé tartozik a felhasználói fegyelem, a felhasználói stressz, az eszköz pillanatnyi állapota, a felhasználói interfész, a válaszidő és egyéb változók. Hiszen a gyártók által közölt statisztikai adatok ellenőrzött laboratóriumi körülmények között végzett, korlátozott számú kísérleten alapulnak, amelyeket matematikai elméletekkel támogatnak. Ezeket mindig csak

vezérfonalaknak kell tekintenünk, és nem alapozhatunk rájuk az adott rendszerek teljesítményére vonatkozó elvárásainkban. Ennek természetesen nem az az oka, hogy a gyártók félre akarnak vezetni bennünket (a legtöbb esetben egyáltalán nem akarnak), hanem az, hogy csaknem lehetetlen pontos útmutatást adni arra vonatkozóan, hogyan fog működni egy eszköz a megvalósított alkalmazás konkrét feltételei között. Például a regisztrálásra fordítandó idő is a regisztrálási eljárás bizonyos paramétereitől függ. Részesültek a felhasználók előzetes oktatásban? Mennyire képzett az adminisztrátor, aki a regisztrálást végzi? Hány regisztrálási pont fog működni? Milyen egyéb folyamatok tartoznak a regisztráláshoz? És így tovább. A gyártók feltehetően nem képesek ezeket a változókat minden egyes rendszerre egyszerre modellezni, és olyan számokat idéznek, amelyek ellenőrzött körülmények között végrehajtott saját kísérleteiken alapulnak.

Az ellenőrzésre fordított időt gyakran félreértik, mert a gyártók általában a ténylegesen az ellenőrzési eljárásra fordított idő átlagát adják meg, ami nem foglalja magában azt a tartamot, amely az élő minta megadásához szükséges, vagy ahhoz, hogy egyéb folyamatokat is végrehajtsunk, mint például egy adathordozó (kártya) használata vagy a személyi azonosító szám (PIN) begépelése.

Mindezeket összevetve arra az egyáltalán nem meglepő következtetésre juthatunk, hogy a biometriai eszközök teljesítőképessége vitatottá válhat valós rendszerek létrehozásakor. Abból a célból, hogy független ítéletet lehessen alkotni, az Amerikai Egyesült Államokban megalapították a Nemzeti Biometriai Tesztközpontot (National Biometric Test Centre). A központ akadémiai intézménynek minősül, és rövid időn belül biztosan érdekes eredményekkel fog szolgálni. Azonban ez nem jelenti okvetlenül azt, hogy a gyártók az eredményekhez gyorsan igazodni fognak. Ezért egyelőre továbbra is úgy kell tekintenünk a gyártók által meghatározott specifikációkat, mint durva irányvonalakat, és csak a saját próbáinkban és megfigyeléseinkben bízhatunk, ha közelítő értékeket kívánunk szerezni az általános teljesítőképességről. Itt említjük meg a biometriai paraméterek (így az ujjlenyomatok, íriszek, kézformák és egyebek) egyediségének kérdését. A paraméterek hasonlósága egy felhasználói bázison belül befolyásolhatja a teljesítőképességet. Jelen írás keretein kívülre esik ennek

a szempontnak a vizsgálata, de az egész világon senkinek sincs megbízható adata erre vonatkozóan, ezért nem is állíthatjuk, hogy bármely biometriai adat valóban egyedi lenne. Ami biztos: annak a valószínűsége, hogy azonos ujjlenyomatokat, íriszeket, kézformákat és egyebeket találunk egy átlagos felhasználói adatbázison belül, elég kicsi ahhoz, hogy a kérdéses paramétert megbízható azonosítónak tekintsük. Szőrszálhasogatásnak tűnik, de jobb, ha tartózkodunk az abszolút egyediség kifejezéstől – néhány személy éppen eléggé hasonlít egymásra ahhoz, hogy az hibás elfogadásokat okozzon.

Ellenőrzés kontra azonosítás

Gyakran találkozunk a következő fogalmakkal: „ellenőrzés", „azonosítás". Ezeket néha összekeverik, amikor a biometriáról esik szó.

A rendelkezésre álló eszközök többsége ún. ellenőrző módban dolgozik. Ez azt jelenti, hogy azonosságot keresünk egy, a háttértárról (PIN beadásával vagy kártya alkalmazásával) lehívott, meghatározott maszk és egy összehasonlítás céljára bemutatott élő minta segítségével. Ennek eredménye azonosság vagy különbözőség lesz, az előre meghatározott paramétereknek megfelelően. Ez egy egyszerű és gyorsan végrehajtható, egy az egyhez történő „találat", amely egy bináris igen/nem eredményt hoz létre.

Néhány eszközről, amelynél a rendszer a felhasználó által bevitt minta azonosítását kísérli meg a maszkadatbázison belül, azt állítják, hogy biometrikus azonosítást nyújt. Egy összetettebb rendszer, nagy számú összehasonlítással, ebben az esetben akár többszörös eredményt is szolgáltathat, a tárolt maszkok számától és hasonlóságától függően.

Tételezzünk fel, hogy 750 000 maszkot tárolunk egy adatbázisban. A felhasználó megadja az élő mintát, az adatbázismotor pedig megkezdi a keresést. A keresés 10 000 valószínű azonosságot eredményez. Ilyenkor mi a teendő? Alkalmazhatunk bizonyos szűrőket a felhasználók neme, faji eredete, életkora és egyebek alapján a lista kezelhető szintig történő rövidítésére, ha megkapjuk ezeket az információkat a felhasználóktól. A végeredmény a potenciális azonosságok kezelhető méretű listá-

ja lesz. Természetesen egy kisebb adatbázisban nem biztos, hogy ez problémaként felmerül.

Mára bebizonyosodott tehát, hogy egyes eszközök jól működnek ily módon tízes nagyságrendű, kis felhasználói adatbázisok esetén, de a helyzet már néhány százat kitevő adatbázisok esetén is igen bonyolulttá válhat. Annak a matematikai valószínűsége, hogy „találatot" érjünk el egy ekkora sokaságban, enyhén szólva igen csekély. Egy nagy adatbázist, mint amilyen például az országhatárt átlépőké, csaknem lehetetlen ily módon kezelni a jelenlegi technológiával. S a kereséshez szükséges időt, ha egyszerre több felhasználó fordul a rendszerhez, a fentieknél még nem is vettük számításba.

Ez az azonosító működési mód napjainkban ritkán sikeres a gyakorlatban, kis léptékű, gondosan ellenőrzött helyzetek kivételével.

A felhasználó pszichológiája

Fenti tárgykörre ritkán találunk hivatkozást a biometria irodalmában. Ennek ellenére gondosan körbe kell járnunk a témát, hogyha sikeres rendszert akarunk tervezni és megvalósítani.

Ha egy felhasználó nem örül a biometriai eszköz alkalmazásának, valószínűleg nem is használja majd következetesen, és az átlagosnál nagyobb hibaszázalékot idéz elő. Ezzel ellentétben, ha egy felhasználó el van bűvölve az eszköz alkalmazásától, és lelkesedik érte, feltehetően rendeltetés szerint fogja azt használni, sokkal következetesebb lesz, és viszonylag alacsony hibaszázalékot fog elérni. A két szélsőség között pedig ott vannak azok, akiknek nincsenek különösebb előítéleteik, de idegesek, vagy épp ellenkezőleg, túlzottan magabiztosak: olyanok, akiknek fizikai nehézséget okoz az eszköz használata, akiket nem megfelelően készítettek fel, olyanok, akiknek a referenciamaszkja kevésbé sikerült, és olyanok, akik természetüknél fogva türelmetlenek és kevésbé megértők. A különösen tehetséges, megértő és felkészült felhasználók drámai hatással lehetnek a rendszerteljesítményre – éppúgy, mint a tehetségtelenek és felkészületlenek.

Nyilvánvalóan arra kell törekednünk, hogy (a rendszer szempontjából) jól képzett felhasználóink legyenek, akik jó minőségű referenciamaszkok-

kal rendelkeznek, és meg vannak elégedve az általános rendszertervvel, valamint átlátják annak előnyeit.

A leendő felhasználókat a rendszer használatára vonatkozó, megfelelő és részletes oktatásban kell részesítenünk, gondosan és sietség nélkül. A regisztrálási folyamat során meg kell adnunk nekik a lehetőséget, hogy a rendszerre vonatkozó általános kérdéseiket feltegyék. El kell látnunk őket olyan referenciadokumentációval, amely kellő részletességű információkat tartalmaz, és megfelelő utánakeresési lehetőségeket foglal magában. Mindennek a felhasználó számára kényelmes környezetben kell történnie, ahol kérdéseit felteheti. Ha nem vagyunk felkészülve rá, hogy mindezt mint minimumot megtegyük, soha ne gondoljunk ilyen rendszer bevezetésére.

Minél nagyobb a potenciális felhasználói bázis, annál nagyobb jelentőségűvé válik mindez, mert a szokatlan kívánalmak és/vagy félreértések lehetősége megnövekszik.

Bizonyos nyilvános alkalmazásokban, például börtönlátogató rendszerekben kézzelfogható és azonnali hasznot jelent a felhasználó számára a rendszer korrekt működése, és az adminisztratív hatóságok meg is követelik ezt. Ezért ezekben az esetekben számíthatunk a felhasználók együttműködésére, hiszen nekik is ez az érdekük.

Egy vállalati vagy magánalkalmazásban azonban törekednünk kell arra, hogy a rendszert érdekes és izgalmas kísérletté tegyük, ezzel párhuzamosan pedig minden felhasználó számára világosan meg kell fogalmaznunk annak hasznosságát. Ha a legkisebb kétség merül fel ezzel kapcsolatban, a rendszer valószínűleg nem lesz sikeres. Ezért a felhasználónak kell rendszertervünk középpontjában állnia, és nem a technológiának. Minden lépésénél a felhasználót kell előtérbe helyeznünk: gondosan át kell gondolnunk a felhasználói követelményeket. Ha ezt helyesen oldjuk meg, a technikai lehetőségekkel ráérünk bűvészkedni a későbbiek során.

Biometriai eredmények

A biometriai technológia tulajdonképpen már régóta jelen van, különösen a kiemelt információtechnológiai alkalmazásokban. Ezekben az automatizált azonosságvizsgálat hasznossága igazolja a beruházási költ-

ségeket. Gondoljunk csak például a szociális támogatások kifizetésére, a börtönlátogatási rendszerekre, a határellenőrzésekre. A vállalati szintű alkalmazások tekintetében gyakori az a vélemény, hogy még nem érkezett el az ideje, túl költséges, nem felhasználóbarát, vagy csak túl bonyolult.

Az információtechnológia világában kiemelt érdeklődésre tarthat számot a biometria egy lehetséges alkalmazása: a személyi számítógépek és helyi hálózatok hozzáférés-ellenőrzése. Számos új termék jelent meg ebben a vonatkozásban, a kártyaolvasókat magukban foglaló billentyűzetektől az egyszerű kártyaolvasókig és a különálló eszközökig. Ami nagyon fontos, hogy mára a költségek drámaian csökkentek. Ezelőtt pár évvel egy szabványos biometriai eszköz mintegy 1500 USA-dollárba került – amit gyakran 1500 angol fontra konvertáltak Angliában. Az árnak, úgy tűnik, kevés köze volt az eszközök számához vagy a gyártási minőséghez. Napjainkban azonban a dolgok már másképp állnak. Az eszközök széles skálája és az alacsony árak miatt – amelyek mintegy 150 USA-dollárnál kezdődnek – a helyi hálózatok adminisztrátorai már nagyobb kedvvel kísérleteznek a biometriai technológiákkal. A fizikai hozzáférés-ellenőrzés, idő- és jelenlét-ellenőrzés terén mára sokkal több eszköz áll rendelkezésre, s ezek közül sokhoz tartozik szoftverfejlesztői csomag, amely lehetővé teszi harmadik fél számára a testre szabott alkalmazásokba való integrálást, egyedi kívánságok szerint.

A biometria vállalati alkalmazásai

Pénzügy, pénzkezelés, kutatás, értékesítés, eladás. Kevés olyan vállalati osztály van, ahol ne tudnák értékelni a biztonságos személyazonosság-ellenőrzési módszer hasznosságát.

A mai gyakorlatban erősen támaszkodunk a jelszavakra. Vajon átlagosan hány jelszót használunk a munkánkkal kapcsolatosan? Milyen gyakran változnak ezek? Még egyikünk sem felejtett el soha egyetlen jelszót sem? Mi történik, ha ez bekövetkezik? Biztosak vagyunk abban, hogy ezeket a kérdéseket valamennyien megértjük. Ha végigmegyünk egy nagyobb vállalat munkatermén, vajon valamennyi személyi számítógép előtt ül egy alkalmazott? Lezárjuk-e komputerünket vagy számítógépes munkahelyünket, amikor távol vagyunk tőle, még néhány perc erejéig is? Némely esetben a hosszadalmas bejelentkezési procedúra el-

ijeszt ennek megtételétől. A biometrikus eljárás alkalmazása azonban a folyamatot jelentősen leegyszerűsíti és felgyorsítja, ugyanakkor pedig kiküszöböli, hogy jelszavakra és azok karbantartására támaszkodjunk. Létezik olyan vélemény, hogy bizonyos szervezetekben a jelszóval kapcsolatos problémák a segítségszolgáltatási időnek több mint 40%-át emésztik fel.

Első pillantásra tehát jó gondolatnak tűnik, hogy megfontoljuk a biometrikus bejelentkezési eljárás bevezetését. De csak akkor, ha a rendelkezésre álló eszközök megbízhatók, könnyen használhatók, áruk elérhető, és könnyen integrálhatók az általános információtechnológiai képbe. A legújabb fejlesztések arra engednek következni, hogy általában mindezek fennállnak. Igen jelentős munka folyik egy általános biometriai felhasználói programinterfész (API, Application Programming Interface) kifejlesztésére, azért, hogy megkönnyítsék harmadik személyek számára az alkalmazások kifejlesztését. A BioAPI konzorcium olyan vállalatokat foglal magában, mint a Microsoft, a Compaq, az IBM, a Novell és még sokan mások – mindezek a vállalatok világosan felismerték a biometrikus azonosítás jövőjét az információtechnológiában. Szoftveres rendszerprogramok már most rendelkezésre állnak OEM-használatra, ezek együttműködnek a Microsoft Windows 95/98/NT/2000 rendszerekkel bejelentkezésre, képernyővédő feloldására, fájlok és mappák titkosítására, illetve más funkciókra vonatkozóan. Számíthatunk rá, hogy ehhez hasonló más fejlesztésekre is sor kerül, és arra is, hogy a biometrikus ellenőrzést számos, az információtechnológia biztonságával kapcsolatos területre integrálni fogják. Úgy tűnik, a nehezén már túl vagyunk.

A biometria közelebbi meghatározása

A sikeres alkalmazásfejlesztési és üzembe állítási forgatókönyv a következőkben leírt folyamatot követheti:

1. Körvonalazzuk az üzleti és a működési követelményeket világosan, valamennyi aktuális problémával és azzal a hatással együtt, amelyet az adott helyzetre gyakorolnak.

2. Fejlesszünk ki és egyeztessünk egy alkalmas üzleti folyamatot, amely képes a technológia aktuális fejlettségétől függő adott helyzet lényeges javítására.

3. Fogalmazzuk meg számszerűen a működési elveket, úgymint a felhasználó személyek száma, időprofil, tranzakciók eloszlása, a belépési pontok típusa, céltranzakció-idő, környezeti meggondolások, rendszeroperátorok profilja, rendszeroperátorok rendelkezésre állása és így tovább.

4. Elemezzük a jelenleg fennálló helyzetet és folyamatokat abból a célból, hogy azonosítani tudjuk a jogosultságra vonatkozó követelményeket és a rendszer-együttműködést – lehet, hogy bizonyos létező eljárásokat meg kell tartanunk, vagy biztosítanunk kell a kompatibilitást.

5. Alakítsuk ki a rendszer felépítését, amely megfelel mindannak, amit az előbbiekben körvonalaztunk, de tartsuk meg a jövőbeni fejlesztések és módosítások lehetőségét.

6. Tervezzünk meg egy működési módszert és egy felhasználói interfészt, amely kielégíti a fenti követelményeket magától értetődő és vonzó módon.

7. Válasszuk ki a megfelelő front-end technológiát ennek megfelelően (azaz biometrikus eszközöket, biometrikus és chipkártyát stb.), bizonyosságot szerezve afelől, hogy a biometriai módszer a leginkább alkalmas erre az alkalmazásra.

8. Készítsük el a biometria és az adathordozó technológia kölcsönkapcsolatát a rendszerünkkel.

9. Minden részletre kiterjedően teszteljük le a rendszert, és dokumentáljuk is, mielőtt bemutatjuk azt az ügyfélnek, egyeztessünk és dokumentáljunk minden tervmódosítást.

10. Hozzunk létre és ütemezzünk be egy operátori kiképzőprogramot a rendszerkézikönyvekkel való ellátással együtt, amennyiben ez szükséges.

11. Telepítsük és állítsuk szolgálatba a rendszert, miután megtekintettük a helyet, feljegyeztük a lényeges feltételeket, és kellően figyelembe vettük a létező rendszereket.

12. Adjuk át a rendszert, miután meggyőződtünk arról, hogy az operátorok kellő mélységben megértették annak működését, s valamennyi, a működéshez szükséges adat megvan, és helyes.

A fenti példán megfigyelhettük, hogy a biometrikus azonosítás kiválasztása viszonylag késői pontja a folyamatnak. Ezt a paramétert csak akkor kell mérlegelnünk, ha már teljesen megértettük az üzleti igényeket és azt a potenciális hasznot, amelyet a biometrikus rendszer alkalmazása hozhat.

A rendszer kiválasztásánál a következőkre kell összpontosítanunk: a használat értékelhető egyszerűsége, elfogadható tranzakcióidő, hibaesetekre vonatkozó valószínűségi mértékszámok, hol kell tárolni a biometrikus maszkokat, regisztrálási folyamatok és az anyagi/technikai biztosítás folyamatai, általános összeférhetőség és kapcsolati vitapontok. Azt is meg kell gondolnunk, hogy hol tároljuk majd a biometrikus maszkokat. Lehet, hogy egy adathordozón, például egy chipkártyán, és azt a felhasználó viszi be a rendszerbe az ellenőrzés előtt. Ez nagy adatbázist tenne lehetővé, valamint bizonyos átjárhatóságot a rendszerek között, és a maszkok automatikus karbantartására szolgálhatna, ha szükség van rá. De dönthetünk úgy is, hogy a maszkokat egy központi adatbázisban tároljuk, és azokat összehasonlítás céljából mindig lehívjuk egy kártya áthúzásával vagy egy PIN bevitelével. Ennek a döntésnek természetesen hatása lesz a rendszerhardverre és a konfigurációra. Ha egy központi adatbázist tartunk karban, biztosabbak lehetünk nagyszámítógépes rendszerünkben és a nagyszámítógép, valamint a biometriai olvasók közötti kommunikációban, nem említve a szokásos adatbázis-karbantartást és a back-up igényeket.

Bizonyára észlelte a kedves olvasó, hogy már elég messzire jutottunk ebben a fejezetben anélkül, hogy előhozakodtunk volna a szokásos, biometrikus eszközökre vonatkozó kereskedelmi ígérgetésekkel. Ez szándékos: a teljes rendszer teljesítményére kell koncentrálnunk, nem az egyes komponensekére. A megvalósítás során az elméleti teljesítőképességet jelentős mértékben befolyásolhatják más, kevésbé számszerű paraméterek. Például egy rosszul elhelyezett olvasó, amelyet egyeseknek nehéz kényelmesen használni, minden bizonnyal több hibás visszautasítást fog eredményezni, még akkor is, ha a rendszer megfelelően működik. Hasonlóképpen, az oktatás/begyakorlás hiánya vagy az, hogy a rendszeradminisztrátorok és a szokásos felhasználók nem teljesen értik a rendszert, rontani fogja az általunk várt teljesítményt. A működési folyamatok

a felhasználói felfogóképességgel és hozzáállással párosulva sokkal jelentősebb teljesítménymeghatározók, mint a biometrikus hardverspecifikációk. Ezek az elemek az általános rendszertervvel és a komponensek teljesítőképességével együtt adják meg a rendszer összteljesítményét (TSP, Total System Performance), amit mindenekelőtt szem előtt kell tartanunk az egész projekt tervezése és megvalósítása során.

Eddig olyan dolgokat tárgyaltunk, amelyek mind megtalálhatók egy tipikus rendszerszállító–ügyfél szituációban. Néhány esetben a végfelhasználó (vagy értelemszerűen a rendszerház) OEM-terméket kíván, és azt akarja, hogy a saját felhasználói alkalmazását a pontos kívánalmaknak megfelelően maga fejlessze ki. A biometrikus alkalmazások kezdeti éveiben ez igen bonyolult lett volna, mert igen sok szabadalmaztatott termék állt rendelkezésre. Napjainkban az élet sokkal könnyebb az alkalmazói fejlesztőcsapat számára, mert több vezető gyártó cég vette a fáradságot a terméke használatához szoftverfejlesztői programcsomagok (SDK, Software Development Kit) kialakítására. Ezek rendszerint DLL-modulok formájában kaphatók, amelyeket a fejlesztő az alkalmazásából hívhat elő abból a célból, hogy az eszköz különböző funkcióit elérhesse. Ez lehetővé teszi a fejlesztő számára, hogy figyelmét a felhasználói interfészre és a program összefüggéseire összpontosítsa anélkül, hogy túlságosan bele kellene mélyednie az alacsony szintű kódolás részleteibe.

Ez egy lépés előre, és mint ilyen, üdvözlendő. Mindamellett egy kicsit eszközspecifikus abban az értelemben, hogy ha később egy másik front-end biometriai eszköz használata mellett döntünk, ennek megfelelően újra kell írnunk alkalmazásunkat. Bizonyos esetekben ez elfogadható lehet, de mi történik, ha egynél több típusú biometrikus eszközt kívánunk rendszerünkben használni? Ez nem is olyan ésszerűtlen. Megkívánhatjuk ugyanis kettős biometrikus azonosítás alkalmazását a fokozottabb biztonság érdekében, vagy különböző biometrikus eszközök alkalmazását különböző területeken, környezeti okokból. Ez egy kicsit bonyolíthatja a helyzetet. Talán jó lenne, ha volna egy egységesen elfogadott biometrikus alkalmazói programinterfész (API, Application Programming Interface), amelyet a felhasználók alkalmazhatnak a biometrikus módszerek keverésére egyetlen rendszeren belül. Igaz, jelentős munka folyt ebben az irányban, és amikor a kedves olvasó e sorokhoz ér, legalább egy ilyen

API-nak rendelkezésre kellene állnia. A kérdés az, hogy a biometrikus berendezéseket gyártó cégek örvendenének-e, hogy ennek eleget kell tenniük, és támogatnának-e egy ilyen kezdeményezést. Úgy gondoljuk, hajlani fognak erre, de egyúttal gyanítható, hogy időt fog igénybe venni, amíg beágyazódik a biometrikus kultúrába.

Na és a jövő? Nincs kétségünk afelől, hogy a biometrikus technológia már elég érett, és kiválóan használható különböző fejlett, személyazonossággal összefüggő alkalmazások széles körében. Mindazoknak, akik rendszerek összeállításával foglalkoznak, mind pedig a végfelhasználóknak szélesebb választék áll rendelkezésre front-end biometrikus komponensekből, mint bármikor ezelőtt, és ezeknek a komponenseknek testre szabott rendszerekbe való beillesztése könnyebb, mint valaha. Az egy egységre eső egyedi költség még viszonylag magas a biometrikus termékekre vonatkoztatva, de ez is változik, és számos cég, amely ilyen termékeket állít elő, éppen most dob piacra alacsonyabb költségű OEM-modulokat.

Röviden: ha valakinek olyan gyakorlati problémája van, amelyet a biometrikus azonosítás megoldhat, többé nincs oka kivárásos politikát folytatni egy pillanatig sem – a biometria él és virul, a legközelebbi disztribútornál a polcról leemelhetően rendelkezésre áll.

Alkalmazási riportok

Állóeszköz-nyilvántartás egy nagy részvénytársaságnál

(A Gábor Dénes Informatikai Főiskola hallgatójának esettanulmánya)

A probléma specifikációja

A 90-es évek Magyarországon a piacgazdaságra történő átállás során a hazai vállalatok-szervezetek szervezeti struktúrájában, felépítésében gyökeres változást kényszerítettek ki. Szinte mindennaposak voltak az átszervezések, osztályok szűntek meg, újak alakultak, vagy összevonták őket. Ezzel egyidejűleg a bútorok, munkaeszközök (például a személyi számítógépek, amelyek egyre nagyobb szerepet kaptak a cégek mindennapos feladatainak elvégzésében) is helyet változtattak használójukkal együtt.

Ebben a zavaros helyzetben nagyon fontos volt (és most is az), hogy a vállalat-szervezet pontos információkkal rendelkezzen vagyona helyzetéről, értékéről. Ennek alapja az állóeszköz-nyilvántartás, amely a rendszeres leltárkészítésre épül.

Ez volt a helyzet a cégi központjában is. Az állóeszköz-nyilvántartást már számítógépre vitték, de a leltározás nagyon körülményes volt. A leltári számokat kétféle módon rögzítették a tárgyakra, egy részük fém bilétákkal volt ellátva, más részük öntapadós matricára kézzel felírt leltári számot kapott.

Mind a két módszernek sok hátránya volt. A fémbiléták ugyan tartósak voltak, de könnyen leestek hordozójukról. A matricákkal még rosszabb volt a helyzet: könnyen lekoptak róluk a tollal rájuk írt számok, vagy elengedett a ragasztás. A kiadott leltári számokat fel kellett venni egy leltári ívre, valamint kézi kartonokat is kellett vezetni róluk. De a legnagyobb hátrányuk az volt, hogy a számokat csak vizuálisan lehetett leolvasni, illetve sok esetben körülményes volt hozzáférni, mert eldugott helyekre rögzítették, félve a megsemmisüléstől. Ez sok tévedéshez vezetett, és emiatt az állóeszközöket nehéz volt pontosan nyilvántartani, sok volt az eltérés a leltár és a nyilvántartás között.

Ezért döntött úgy a vállalat vezetése, hogy változtatni kell a leltározás módszerén, és a választás több lehetőség közül a vonalkódos rögzítésre esett.

A kidolgozott megoldás

Az osztályokat, főosztályokat költséghelyszinten különítették el egymástól, és az épületben lévő szobákat ezekbe a költséghelyekbe sorolták be. Minden szobát elláttak két vonalkód-azonosítóval, az egyik a költséghely, a másik a szobaszám kódját tartalmazta.

Végül a szobában található tárgyak is saját vonalkód-azonosítót kaptak, számkörönként elkülönítve a bútorokat, a gépeket stb., ezen belül pedig az értékkel és érték nélkül (pl. klaviatúra) nyilvántartottakat.

Költséghely-azonosító vonalkód

Szobaazonosító vonalkód

Eszközazonosító vonalkód

A vonalkódokat egy HP Laserjet II P típusú printeren nyomtatták ki QCP (Quattro Clean Technologie), speciális vonalkódnyomtatásra használatos, etikettfelépítésű, védőfelülettel ellátott, öntapadós papírra. Ennek nagy előnye, hogy a védőfelület miatt a rákerült vonalkód nagyon hosszú ideig sértetlen marad, és a papír jó tapadó tulajdonsága miatt nem eshet le hordozójáról.

A vonalkódok leolvasását egy Formula 500 típusú vonalkódolvasó fényceruzával végzik, amelynek fényforrása egy infravörös LED. Kapacitása 32 kB-nyi adat tárolására alkalmas, amellyel kb. 400 olvasás információit tudják egyszerre tárolni. Az összegyűjtött adatokat soros porton keresztül olvassák be a számítógépbe, és egy DBF-állományban tárolják.

Ezt az adatbázist egy saját fejlesztésű program dolgozza fel, megfeleltteti a beolvasott kódokat a tényleges állóeszközöknek, és igény szerinti listákat készít a vezetők számára, akik pl. így tudják figyelemmel kísérni a használatukban lévő számítógépek amortizációját. Ugyancsak ez az adatbázis az alapja az állóeszköz-nyilvántartó szoftvernek, amellyel a leltározás után ki lehet mutatni a leltáreltéréseket is.

Az újonnan beszerzett tárgyi eszközök is nyilvántartásba kerülnek, és ezzel egyidejűleg megkapják saját vonalkód-azonosítójukat.

Üzemeltetési tapasztalatok

Ennek a rendszernek – és a vonalkódnak – köszönhetően a cégnél megoldódott az állóeszközök pontos, naprakész nyilvántartása, lényegesen leegyszerűsödött a leltározás amúgy hosszadalmas és körülményes folyamata, s ez biztosítja a vezetők pontos információval való ellátását.

A vonalkódtechnika alkalmazása a nagyüzemi fotókidolgozásban

(A Gábor Dénes Informatikai Főiskola hallgatójának esettanulmánya)

A feladat specifikációja

Partner- és termékazonosítás az ország legnagyobb fotókereskedelmi hálózatában.

A cég a 80-as évek elején Magyarországon a legelső olyan vállalkozások között volt, amelyek a vonalkódtechnikát tevékenységük megkönnyítésére sikerrel alkalmazták. Ez az esettanulmány a nagyüzemi fotókidolgozással, a vonalkódtechnika e területen való alkalmazásával foglalkozik.

A cég hálózata rendkívül sokszínű, az egész országra kiterjed, és közel 400 üzletet foglal magában. Ezek közt vannak saját tulajdonban lévő üzletek, franchise- és egyéb partnerek is. Ezen üzletek tevékenységének nagy részét – a kereskedelmi áru forgalmazása mellett – az amatőr fotómunkák kidolgozásra való átvétele, majd a kész munka kiadása teszi ki.

A hálózat bármely üzletében felvett filmek a központi laboratóriumba futnak be. Ez a laboratórium Közép-Európa legnagyobb ilyen jellegű, ún. „fotofinishing" laboratóriuma.

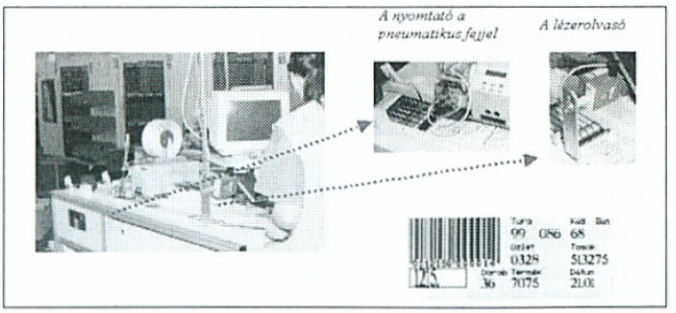
Ilyen méretű partnerhálózatnál és az e mellé társuló rendkívül széles termékválasztéknál (szinte csak a megrendelő fantáziája szab határt annak, hogy filmjéről milyen méretű, felületű képet szeretne, és milyen határidőre) nagyon fontos a partner- és termékazonosítás.

A kidolgozott megoldás

A partnerazonosítás eszköze – a munkavállalói tasak

A megrendelő által kidolgozásra átadott film az üzletben egy ún. munkavállalói tasakba kerül. Ez a tasak végig fogja kísérni a filmet, a megrendelő ebben fogja visszakapni az előhívott negatívot és az arról készült képeket. A tasak hátoldalán szerepel két, nyomdai úton előállított vonalkód, az egyik az üzlet azonosítószámát, a másik a tasak egye-

di azonosítóját tartalmazza. E kódoknak a laboratóriumi kidolgozás során lesz jelentőségük.



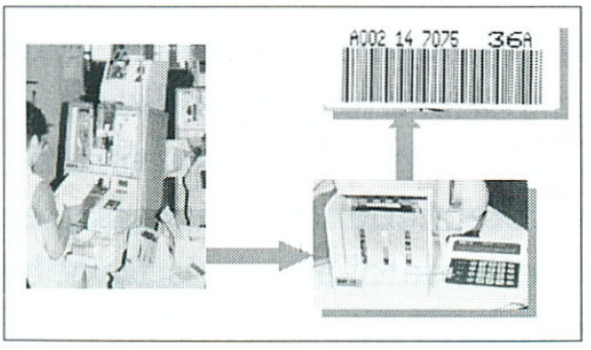
A munkavállalói tasak hátoldala a vonalkódokkal

A felvett fotómunkák a külön erre a célra szervezett közúti szállítási hálózat (ún. fotótúra) segítségével a központi laboratóriumba jutnak. Itt a megrendelések a technológiai folyamaton végighaladva, egy off-line rendszerű árazási szisztéma segítségével kiszállításra kész állapotba kerülnek.

Az off-line árazási rendszer

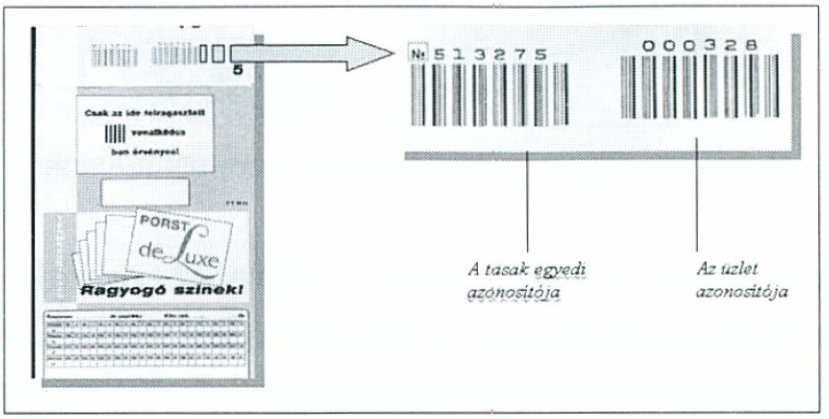
A kidolgozási folyamat utolsó szakaszában az előhívott filmek és a hozzájuk tartozó képek nagy tekercsekben fényképdaraboló automatákra, ún. vágógépekre kerülnek (ezekben a tekercsekben akár 90 db film is lehet, a hozzájuk tartozó papírtekercs pedig 350 m hosszú).

Minden vágógép on-line összeköttetésben van egy-egy direct thermal rendszerű, 150 dpi felbontású vonalkódnyomtatóval. A nyomtató 6x2 cm méretű hőérzékeny címkére nyomtatja a vonalkódot, amely tartalmazza a vágógép azonosító számát, a kiszolgáló személy kódját, a termékszámot és a képdarabszámot. A nyomtató a címkéket peel-off rendszerben adagolja, és a rendszert kiszolgáló személy azokat kézzel ragasztja fel a munkavállalói tasakok hátoldalára, miután a képeket is berakta oda.



A vágógép a vonalkódnyomtatóval és a vonalkód

Az immár 3 vonalkódot – és természetesen a kész képeket – tartalmazó tasak ilyen formában kész az árazórendszeren való áthaladásra. Az árazórendszer egy futószalagot, egy lézeres vonalkódolvasót, egy termocímkére dolgozó nyomtatót és az ezeket irányító számítógépes programot tartalmazza.



Az árazórendszer elemei és az árat tartalmazó vonalkód

A tasakokat kézzel, hátoldalukkal felfelé teszik a futószalagra. Azok elhaladnak az olvasó alatt, amely egy vonalban pásztázó, Datalogic LS 50 H (High Density) típusú lézerszkenner. Elméleti olvasási sebessége 500 scan/sec. Kimenő fényteljesítménye 0,95 mW, melynek alapján a 2-es osztályú lézergyártmányok közé sorolható. A leolvasott vonalkódokból a számítógép újabb vonalkódot és egyéb karakteres adatokat generál, melyeket a nyomtatóra továbbít. Ezt az EAN-13-as vonalkódot és az egyéb adatokat a nyomtató egy 3x8 cm-es hőérzékeny címkére nyomtatja, majd egy pneumatikus fej ezt a címkét az időközben a futószalagon odaérkezett tasakra nyomja, s ezzel egyidejűleg a tasakot le is zárja. A vonalkódot később, az üzletben kézi szkennerrel leolvassák, így a számlázás gyors és egyszerű lesz.

Ezután már csak a kész megrendelések manuális úton való szortírozása van hátra aszerint, hogy az ország mely részébe kell azokat szállítani. Ha ez is megtörtént, akkor a tételek kiszállításra készek.

Az árazórendszer fent leírt primer feladatán kívül eleget tesz még egy, nem kevésbé fontos követelménynek. Kapcsolatban áll egy központi számítógéppel, s a leolvasott adatokat oda is továbbítja. Ebben a központi számítógépben így az összes fontos termelési adat évekre visszamenőleg elérhető.

Üzemeltetési tapasztalatok, továbbfejlesztési lehetőségek

Nagy előrelépés lenne egy olyan on-line árazási rendszerre való áttérés, ahol minden egyes vágógép kapcsolatban állna a központi számítógéppel. Ez esetben természetesen a vágógépnél kell kialakítani a jelenlegi árazógép elvén működő rendszereket.

Elképzelhető egy automatizált végső szortírozási folyamat bevezetése is. Ez esetben a szortírozásra kész, végső vonalkóddal ellátott tasakok egy szállítószalag-rendszeren továbbhaladnak. A szállítószalag alatt mint „állomások" a különböző üzletek, esetleg üzletcsoportok tárolóhelyei (táskái) vannak. Az egyes táskák felett lévő billenő „ajtók" kinyílnak, amennyiben a táska fölé egy ahhoz az üzletcsoporthoz tartozó egység tasakja érkezik, így a tasak belepottyan a megfelelő táskába. A folyamat helyigényes, de rendkívül sok élőmunkát lehet vele megtakarítani. Szállítószalagot, vonalkódolvasót, az ajtókat működtető áramköröket és az egészet kézben tartó számítógépes támogatást igényel. Nyugat-európai laboratóriumokban alkalmaznak ilyen rendszert.

Időnként előfordul, hogy a vágógépet kezelő dolgozó a vonalkódcímkét ferdén ragasztja a tasakra. Az ebből a hibából eredő vonalkódolvasási problémák kiküszöbölhetők lennének egy omnidirekcionális vonalkódolvasó beépítésével az árazórendszerbe. Persze ennél olcsóbb megoldás a technológiai fegyelem betartása.

Az on-line árazási rendszer és az automatizált végszortírozás együttes alkalmazása látványos termelékenységjavulást hozhat. Ebben az esetben a vágógépektől a végső szortírozásig egy on-line folyamatként lehet felfogni az egész rendszert, tehát a vágógépektől emberi kéz érintése nélkül, kis túlzással futószalagon hagynák el a laboratóriumot a kész megrendelések. Nyugat-Európában ilyen rendszert is alkalmaznak.

Összegzésképpen elmondható, hogy egy jól szervezett és karbantartott automatikus azonosítási rendszer jött létre a nagyüzemi fotókidolgozás területén, referenciát teremtve ezzel a hasonló problémák megoldása előtt álló vállalkozásoknak.

Vonalkódok alkalmazása a termékek azonosításában

(A Gábor Dénes Informatikai Főiskola hallgatójának esettanulmánya)

A feladat specifikációja

A vonalkódtechnika bevezetésének előfeltételei

Az alkalmazási terület rövid leírása

Egy író-, illetve irodaszereket gyártó és forgalmazó részvénytársaságról van szó. Az általa forgalmazott termékek között megtalálhatók a legegyszerűbb golyóstollak és a magasabb igényeknek is megfelelő írószerek, valamint egyéb irodai termékek.

Széles körű árukínálatuk és nyilvántartási rendszerük következtében termékeik száma nem csekély. Áruikat szín, keménység (pl. radíroknál), csomagolási mód és egyéb tulajdonságok alapján is megkülönböztetett árukóddal tartják nyilván.

Első lépésként egy értékesítési területen, a pomázi üzletházukban szeretnék bevezetni a vonalkódolvasó használatát. Itt az értékesítés nem önkiszolgáló jellegű, részben a vevőkkel való személyes kapcsolattartás, részben pedig a helyi adottságok miatt. Az üzlethelyiség lényegében egy légterű, de négy szimbolikusan elkülönített részből áll, amelyek a következők:

- raktárhelyiség,
- eladótér, amely áruminták kiállítására alkalmas üzletberendezéssel van ellátva,
- számlázóhelyiség,
- pénztár.

Jelenleg a vásárlók kiszolgálása alapvetően kétféle módon történhet, attól függően, hogy a vevőnek van-e megrendelése. Amennyiben igen, a rendelés felvitele kézi rögzítéssel történik. A vevőt már előkészített áruval és pro forma számlával várják.

Abban az esetben, ha prompt vásárlásról van szó, a vevőt a munkatársak segítik az igényeinek leginkább megfelelő áruk kiválasztásában.

Azokat és a kért mennyiségeket felírják egy kiszedőlapra, majd ezt átadják a raktárnak. A raktáros összekészíti a vásárolni kívánt árukat, és a kiszedőlapra rávezeti az általa kiszedett termékek mennyiségeit. A kiszedőlapot ezután a számlázás kapja meg, ahol rögzítés után elkészítik a vevő számláját. A vevő készpénzes vásárlás esetén a számla és a pénztári nyugta felmutatásával, átutalásos fizetés esetén pedig a számla felmutatásával veheti át az árut.

A megoldás kidolgozásának folyamata

A társaságnál működő informatikai rendszer rövid leírása

Informatikai rendszerüket 1998-ban fejlesztették ki, amelynek bővítése, tökéletesítése a mai napig tart. Terveik között szerepel a vonalkódos azonosítási eljárással történő bevételezés, leltározás és a vevői rendelések felvitele prompt vevők kiszolgálása esetén.

A vonalkód alkalmazásának feltételei részben adottak, mivel saját előállítású termékeik teljes körűen, más vállalattól vásárolt termékeik pedig nagy számban rendelkeznek vonalkóddal. Informatikai rendszerük alkalmas a vonalkódok tárolására és az árukódhoz történő hozzárendelésére. Egy adott árukódhoz több vonalkód is rendelhető, attól függően, milyen kiszerelésekben történik az értékesítés.

Az árutörzshöz kapcsolódik a külső azonosítók törzse, amely a rendszerben előforduló külső azonosítók tárolására szolgáló nyilvántartás. Az azonosítók több forrásból származhatnak, ezek típuskóddal különíthetők el:

1 = gyári vonalkód: a szállítók hivatalos, a terméken szereplő vonalkódjai,

2 = belső vonalkód: a rendszer által generált, EAN szabvány szerinti belső vonalkód (2-vel kezdődik),

4 = szállítói árukód: a szállítók saját áruazonosítói,

5 = gyorskód: vonalkóddal nem ellátható, de nagy tömegben értékesített árukhoz egy rövid (maximum 2-3 jegyű), könnyen megjegyezhető kód.

Egy vonalkódhoz az alábbi adatokat kell kitölteni:

- külső kód fajtája (1 = gyári vonalkód),
- külső kód (maga a vonalkód),
- partnerkód (gyártó partnerkódja),
- gyűjtőkód (igen/nem),

- szorzó (termék darabszáma az adott csomagolásban),
- nyomtatható (igen/nem).

Kereskedelmi rendszerük rendelkezik egy úgynevezett Psion-kapcsolattal, amely az adatgyűjtő árutörzsének összegyűjtését, valamint a címkék nyomtatását teszi lehetővé.

Ezenkívül a számlázási modul képes adatokat beolvasni az adatgyűjtő által készített szöveges állományból, majd a szükséges ellenőrzések után előállítani egy pro forma számlát.

A vonalkód bevezetéséhez szükséges teendők

- Fel kell mérni az értékesített, de vonalkóddal nem rendelkező termékek körét.
- A beszállítóktól meg kell kérni a vonalkódokat, vagy amennyiben ez nem lehetséges, belső vonalkódokat kell generálni ezen termékekhez.
- Az ily módon megszerzett vagy generált vonalkódokat rögzíteni kell a külső azonosítók törzsébe.
- Ellenőrizni kell a külső azonosítók törzsének feltöltöttségét és tartalmának helyességét.
- Gondoskodni kell arról, hogy az árajánlatokban és egyéb kínálatokban minden terméknek a megfelelő vonalkódja szerepeljen. Ez nagyon pontos munkát igényel, mivel a vevők között találhatók olyan nagy üzlethálózatok, amelyek már teljesen automatikus termékazonosítással dolgoznak. Amikor ezeknek a vevőknek ajánlanak egy terméket adott vonalkóddal, azt rögtön felvezetik informatikai rendszerükbe, és vásárlás esetén nem fogadják el, ha ettől eltérő vonalkódot találnak a terméken vagy annak csomagolásán.
- Az üzletház árubemutató polcrendszerét át kell rendezni oly módon, hogy a termékeken lévő vonalkódok könnyen hozzáférhetők, szkennelhetők legyenek. A polcrendszer kézzel írott címkéit ki kell cserélni számítógépes, vonalkódot is tartalmazó címkékre.
- Ki kell szűrni azon termékeket, amelyek el vannak látva vonalkóddal, de a vonalkódolvasó mégsem tudja leolvasni azokat rossz minőségük vagy nem szabványos méretük miatt. Ezeket feltétlenül el kell látni termékcímkékkel.

• Mivel vannak olyan termékek, amelyeknek több vonalkódja is van, gondoskodni kell arról, hogy az adatgyűjtő árutörzse azokat az azonosítókat tartalmazza, amelyek a kiállított termékeken vagy azok címkéin szerepelnek.

A kiszolgálás tervezett menete

A vevők gyorsabb, pontosabb kiszolgálása és az emberi tévedések kiküszöbölése érdekében tervezik az adatgyűjtők alkalmazásának bevezetését. A rendelkezésükre álló eszköz egy Psion Workabout hordozható adatgyűjtő, amely 2 MB RAM-mal rendelkezik. Nincs állandó összeköttetésben a számítógéppel, az adatforgalmat egy dokkolóegységen keresztül tudja megvalósítani. Kezdetben kísérleti jelleggel csak egy darab adatgyűjtőt fognak használni, s amennyiben beváltja a hozzá fűzött reményeket, és gyorsítja, pontosabbá teszi a kiszolgálást, bővíteni szeretnék az adatgyűjtők számát és alkalmazási helyeit.

A továbbiakban sem szándékoznak eltérni attól a bevált kiszolgálási módszertől, amelyet eddig alkalmaztak. Munkatársuk személyesen kíséri végig a vásárlót az áruminták között, segítve őt a választékban való eligazodásban. A jövőben azonban nem kell kiszedőlapot vezetnie, mert az adatgyűjtő segítségével rögzíteni tudja a megrendelt termékek azonosítóit és a mennyiségeket. Az adatgyűjtőn lévő program négy fő funkciót lát el:

- PC-ről való letöltés,
- a megrendelés felvitele,
- leszedés,
- a rendelés PC-re töltése.

A Psion-törzs kialakítása

A munka megkezdése előtt gondoskodni kell arról, hogy az adatgyűjtő árutörzse naprakész állapotú legyen. Az informatikai kereskedelmi rendszer tartalmaz egy Psion-törzslegyűjtő alprogramot. Futtatásával a program összegyűjti az aktuális árutörzsből azoknak az árukódoknak az adatait, amelyeket értékesítenek, és amelyekből van készlet, valamint az ezekhez az árukhoz tartozó három legfontosabb belföldi eladási árat. Sajnos az adatgyűjtő memóriája kicsi ahhoz, hogy a raktári készleteket is be tudja olvasni.

Az adatokat elhelyezi az adott számítógép winchesterén, egy Laurel nevű alkönyvtárban.

Az adatgyűjtő és a számítógép közötti kapcsolat egy dokkolóegységen keresztül valósulhat meg, amelyet a számítógép COM1 vagy COM2 portjához lehet csatlakoztatni.

Az adatgyűjtőt be kell helyezni a dokkolóegységbe, és el kell indítani a PC-ről való letöltés programját. A PC-n szintén futtatni kell egy RCOM.EXE szoftvert, amely az árutörzset feltölti az adatgyűjtőre. Mivel az árutörzs viszonylag nagy, a folyamat kissé időigényes, kb. 20 percet vesz igénybe.

Az adatgyűjtő árutörzsének aktualitása érdekében azonban ajánlott ezt a folyamatot naponta legalább egyszer elvégezni.

Megrendelés felvitele

Meg kell adni egy tetszőleges vevőkódot, amellyel a rendelést azonosítani tudjuk. Ezen a néven, .txt kiterjesztéssel fog képezni egy szöveges állományt a PC-re töltés során.

Meg kell határozni a vevő árlistáját. Az adatgyűjtő három különböző árlistát tárol anyagtörzsében. Jellemzően három fő belföldi árlistájuk van:

- belföldi 1-es ár – nagykereskedők részére,
- belföldi 2-es ár – viszonteladók, kiskereskedők részére,
- belföldi 3-as ár – közületek, magánszemélyek részére.

Ezután következhet a megrendelés tételeinek felvitele. Alapvetően nincs más teendő, mint vagy a termékről, vagy a polcon elhelyezett címkéről beolvastatni a vonalkódot. A program elkezdi keresni a vonalkódhoz tartozó termék adatait.

Amikor az azonosítás megtörtént, a kijelzőn megjelenik a termék megnevezése, mennyiségi egysége, áfa-százaléka, egységára. A program vár a mennyiség beütésére.

Amennyiben az azonosítás sikertelen volt, adott a lehetőség a termék polcon elhelyezett címkéjéről rögzíteni az árukódot. Ez a probléma azonban csak abban az esetben fordulhat elő, ha valamelyik előkészítő folyamat pontatlan volt. Az azonosítási hibának több oka is lehet:

- az adatgyűjtő árutörzse elavult, régen lett feltöltve,
- a külső azonosítók törzsének feltöltése hibás,
- az adott termékből éppen nincs készletünk.

A rendelt mennyiséget be kell gépelni.

A tételek felvitelét addig folytatjuk, amíg van rendelt termék.

A rendelés felvitele közben a tab billentyű segítségével bármikor kérhetünk információt a felvett tételek nettó összegéről, ezzel tájékoztatva a vásárlót, hogy eddig milyen értékű a rendelése.

A program lehetőséget biztosít egy már rögzített tétel módosítására, illetve annak törlésére.

A rendelés tételeinek felvitelét, valamint karbantartását addig folytatjuk, míg el nem éri végleges formáját.

Leszedés

A megrendelés rögzítése után az adatgyűjtőt át kell adni a raktárosnak, aki a rendelkezésre álló árukészletből leszedi a rendelt árukat a raktári polcokról. Ha egy terméket már kikészített, rögzítenie kell a leszedett mennyiséget, amely nem lehet több, mint ami a rendelésben szerepel.

PC-re töltés

Az adatgyűjtő behelyezése az egységbe.

Az adatgyűjtőn a PC-re töltés menüpont elindítása.

A csatlakozó számítógépen el kell indítani az RCOM.EXE programot.

Ezzel a rendelés egy szöveges állomány formájában átkerül a PC-re, a Laurel alkönyvtárba. A fájl neve a rendelés felvitelének kezdetén megadott vevőazonosító, kiterjesztése pedig .txt.

Számlakészítés

A kereskedelmi rendszer számlázóprogramjában el kell készíteni az adott rendeléshez szükséges ideiglenes számla fejrészét, majd be kell lépni a tételek felvitelébe. Az adatgyűjtő nyomógombra kattintva megkérdezi, hogy mi a rendelésállomány neve, amit be akarunk olvasni. Ekkor kell megadni a szöveges állomány fájlnevét, kiterjesztéssel együtt.

Ennek hatására a számlázóprogram beolvassa a rendelés tételeit, ellenőrzi azokat, és amennyiben nem talál hibát, felveszi az ideiglenes szám-

la tételei közé. A hibásnak minősítettek megtekinthetők a fel nem vett tételek nyomógombjára kattintva. Itt nemcsak a hibás tételeket, hanem a hiba okát is láthatjuk.

A hiba oka lehet:

- nincs elég raktárkészlet,
- a legkisebb rendelhető mennyiségnél kevesebb szerepel a rendelésben.

Ha a számlázóprogram nem találja az általunk megadott állományt, akkor hibaüzenetet küld. Ebben az esetben valószínűleg mi tévedtünk, és elrontottuk az állomány nevét vagy kiterjesztését.

Ha a rendelés tételeinek beolvasása sikeres volt, akkor rendelkezésünkre áll egy pro forma számla, amelyen még tetszőleges változtatásokat végezhetünk, vagyis módosíthatjuk a mennyiségeket, vagy akár teljesen új tételekkel bővíthetjük számlánkat. Ekkor már nem alkalmazzuk az adatgyűjtőt, hanem hagyományos kézi rögzítéssel végezzük a korrigálást. Azért kell felkészülni az ideiglenes számla javítási lehetőségére, mert az alkalmazott vevőengedmények egy része a számlavégi összegtől függ. Annak érdekében, hogy a számla végösszege elérje ezt az értékhatárt, a vevő sok esetben úgy dönt, hogy vásárol még más termékeket is, vagy egy, a számlában már szereplő termék mennyiségét növeli.

Ha az ideiglenes számla karbantartása befejeződött, elindíthatjuk annak könyvelését. Ennek során történik meg a készletek csökkentése, a könyvelt számla elkészítése, kinyomtatása, valamint a vezetői információs állományok aktualizálása. A végleges számla módosítása már nem lehetséges, csak sztornózással vagy vevővisszáru készítésével.

A rendszer hardverigénye

A rendszer hardverigénye alapvetően két, jól elkülöníthető részből áll: az egyik a hálózat, a másik pedig a kézi adatgyűjtők oldala. Mivel a szóban forgó rt.-nél jól kiépített hálózat működik, ezért a rendszer hálózati oldalról nem igényel külön beruházást. Jelenleg öt számítógép-konfiguráció működik az üzletházban. Ezekből a PC-kből egy a pénztári feladatok ellátására szolgál, és a Novell Netware-kiszolgálóhoz kapcsolódik, négy pedig a Windows NT-szerverrel áll összeköttetésben, és a kereskedelmi rendszer használatára szolgál. Az üzletházon belüli elhelyezkedésük megfelelő, tehát a hálózat bővítése, illetve áthelyezése nem indokolt. Az

adatgyűjtővel történő rendelésfelvitel a használt számítógépek szempontjából nem igényel további beruházást. A jelenleg alkalmazott számítógépek megfelelnek a követelményeknek.

Ha az adatgyűjtő kísérleti alkalmazása beváltja a hozzá fűződő reményeket, vagyis gyorsítja, pontosabbá teszi a kiszolgálást, valamint a munkatársak munkaideje a rögzítés fáradságos tevékenysége helyett magasabb szintű feladatok ellátására lesz fordítható, akkor szándékukban áll további adatgyűjtők munkába állítása. Az üzletház napi forgalma igen változó, ezért a szükséges adatgyűjtők számának meghatározása nem könnyű feladat.

Az üzletház hardverigénye:

3 db Psion Workabout 64 kilobyte ROM-mal és 2 megabyte RAM-mal, elemről is működő kézi adatgyűjtő, 1 db Psion Workabout dokkolóegység.

Nyomtató vásárlását nem tartják feltétlenül szükségesnek, mivel a vállalatnál sok lézernyomtató és egy vonalkódnyomtató is üzemel, ezek bármelyikével le lehet bonyolítani a vonalkódos címkék nyomtatását.

A rendszer szoftverigénye

A rendszer szoftveroldalról is több részre bontható. Egyrészt szükség van az adatgyűjtőn futtatható leszedőrendszerre, másrészt az adatgyűjtő és a PC közötti adatátvitelt biztosító szoftverre. Ezenkívül az alkalmazott informatikai rendszernek képesnek kell lennie arra, hogy az adatgyűjtő által készített állományokat fogadni, konvertálni tudja.

Megtérülés és fejlesztési lehetőségek

A rendszer megtérülése ebben az esetben nem mutatható ki egészen pontosan, mivel nem egy teljesen új alkalmazásról van szó, ezért a költségek felmérése csak hozzávetőleges lehet. Például nem tudják megállapítani, hogy informatikai rendszerük árában milyen értéket képvisel az adatgyűjtővel való kapcsolódás.

Költségek

3 db Psion Workabout adatgyűjtő 2 megabyte memóriabővítéssel, leszedőrendszerrel ellátva	211 840 Ft/db	635 520 Ft
1 db dokkolóegység	61 840 Ft/db	61 840 Ft

Megtérülés

A diszkontáruházban reményeik szerint egy ember munkája kiváltható az alkalmazott technikával.

Tehát ha a befektetésük kb. 700 000 Ft, és az amortizációt nem számítjuk, valamint egy ember napi munkabérét a közterhekkel együtt 4000 Ft-ra kalkuláljuk, akkor ez havonta kb. 80 000 Ft-ot tesz ki. Tehát a ráfordítás kilenc hónap alatt megtérül.

A rendszer továbbfejlesztési lehetőségei

A közeljövőben szeretnék az adatgyűjtős vevőkiszolgálást más értékesítési területeken is bevezetni, mint például a Parker-értékesítésnél, a készáruraktárban és budapesti kirendeltségüknél.

Terveik között szerepel még a leltár adatgyűjtővel való lebonyolításának megvalósítása is. Az áruk vonalkódos azonosítással történő felismerése és a leltári készlet kézi adatgyűjtővel történő rögzítése jelentősen gyorsítaná a leltár folyamatát.

Továbbá tervezik a bevételezések kézi adatgyűjtővel való megvalósítását, ami egyrészt gyorsabbá, másrészt pontosabbá fogja tenni a készletvezetést. A bevételezés alatt a külső szállítótól érkező, valamint az üzemtől kapott áruk raktárra vételét kell érteni.

Összességében a vonalkódok alkalmazásával gyorsabb, biztonságosabb, korszerűbb árukezelést szeretnének elérni.

Magyarországon is hódít a chipkártya

(A Bull Magyarország Kft. referenciáiból)

A chipkártya – közismert nevén smart card – első ránézésre olyan, mint a hagyományos bankkártya, legtöbbször még a mágnescsík is megtalálható rajta. Azonban a figyelmes szemlélő már felfedezi az aranyozott érintkezőket, amelyeken keresztül a kártya kommunikál a külső eszközökkel.

A lényeg azonban nem látható. A smart card ugyanis attól különleges, hogy nem a könnyen hamisítható, sérülő mágnescsík tárolja az információkat, hanem a kártya belsejében lévő számítógép. Ez lényegében csak méretében különbözik a „nagyoktól", ugyanúgy van processzora, memóriája, programozható, és műveletek elvégzésére képes. Ezt kihasználva gyakorlatilag feltörhetetlen adattároló és hamisíthatatlan azonosító eszközként alkalmazható.

A smart card feltalálása a Bull nevéhez fűződik. A vállalat a kezdetektől fogva őrzi vezető helyét a kártyák és alkalmazások fejlesztésében, s a világ legnagyobb gyártói között van.

Korábban már több fórumon méltatták néhány sikeres alkalmazásukat, többek között:

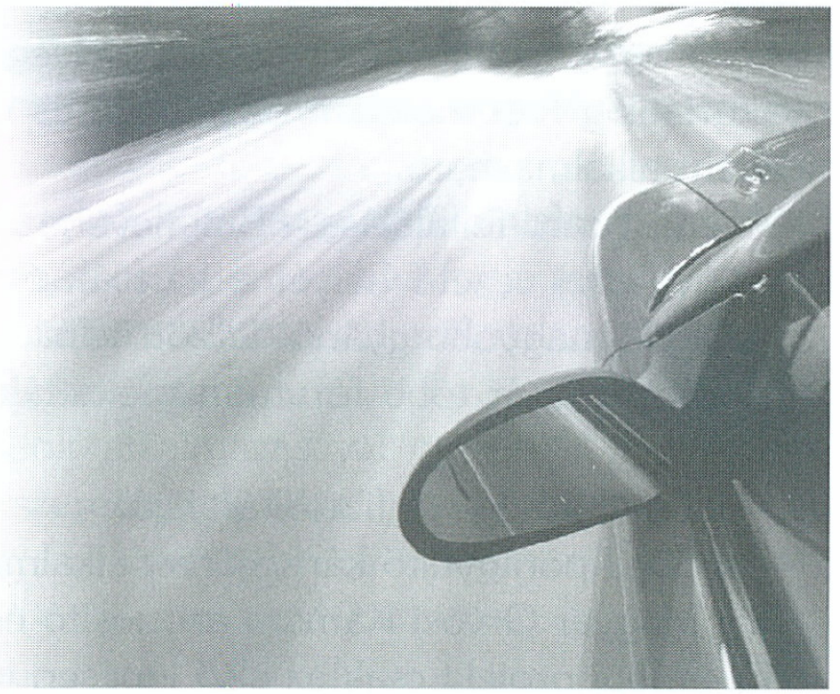
- a Total hűség- és fizetőkártyáját,
- a Shell pontgyűjtő kártyájának alkalmazásfejlesztését és
- a Magyar Orvosi Kamara azonosító és adattároló kártyáját.

Ez utóbbi projekt csak az első lépésen jutott túl. Jelenleg a fényképes kártya azonosítóként funkcionál, de már tesztelik a hamarosan betöltésre és aktivizálásra kerülő új alkalmazásokat, amelyek például nyilvántartják a kötelező továbbképzések eredményeit. A későbbiekben, ha a banki háttér elkészül, hitelkártyaként is használható lesz.

A Paksi Atomerőműnél az azonosítás biztonsága volt a legfontosabb, ezért választották a Bull chipkártyáját. Segítségével a tűzvédelmi rendszerhez való hozzáférés jogosultságát ellenőrzik. A biztonság fokozása érdekében nem elég a kártya használata, ismerni kell a hozzá tartozó PIN kódot is. A rendszer szoftverét az atomerőmű csapata fejlesztette, és a Bull Magyarország szállította a hardverelemeket.

A probléma specifikációja

A Bull Magyarország és a Sárkány Rt. egyik legújabb kártyás alkalmazása a Prímagáz megrendelésére készült. Közismert, hogy a gázzal hajtott autók olcsóbban üzemelnek, mint benzines társaik, és a környezetet is kevésbé szennyezik. Ezért elsősorban a sok autót üzemeltető szervezetek, vállalatok alakíttatják át gépkocsiparkjukat. Ez nem olcsó, sok szervezet nem is tudná saját erőből finanszírozni, ezért a Prímagáz speciális együttműködési konstrukcióval támogatja a gáztankolás bevezetését. A konstrukcióban hosszú távon, nagyon pontosan, autónként kell nyilvántartani a fogyasztást, és a keletkezett adatok alapján egy központból kell utólagosan és időszakosan a partnerekkel elszámolni. Ezért döntöttek úgy, hogy a gázautók chipkártyás fizetési rendszerrel tankolhatnak.



A kidolgozott megoldás

A rendszer minden elemében egyedi fejlesztésen alapszik. Az autókhoz smart card tartozik, a gázkutakhoz az elszámolást végző POS terminál, a Prímagáz központjához pedig egy szerver, amely naponta begyűjti a kutak adatait.

A kutaknál elhelyezett POS terminálon az arra jogosultsággal bíró személy állíthatja be a saját adatait és az aktuális gázárat.

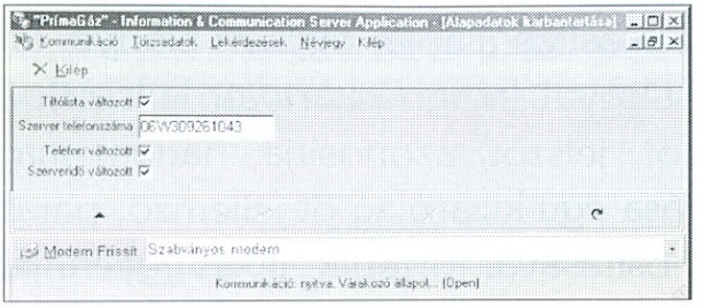
Tankolás után az autóhoz rendelt chipkártya segítségével „fizetnek", amikor is a tankolás helye, időpontja és mennyiségének rögzítése mellett

ellenőrzésre kerül a kártya jogosultsága és az autó napi és havi limitált fogyasztása is. A kártyák egyedi rendelés szerint készülnek, aminél megadásra kerülnek az autó- és a szervezeti adatok, illetve PIN kód használatának szükséglete is beállítható.

A kutak töltését végző szállítóautók is, saját azonosító kártyájukkal, ezen a rendszeren igazolják a kútnak átadott gázmennyiséget.

A nagy biztonságú megoldás miatt nincs szükség a tankolások központi ellenőrzésére, így a terminálok off-line módon működnek.

Minden éjjel, a terminál behívási időpontjában telefonkapcsolaton adják le napi adataikat a központi szervernek.



Ugyanekkor kapják vissza a kiszolgálógéptől a friss tiltólistát, illetve az olyan adatokat, amelyek megváltozása kihat működésükre (például behívószám és időpont). Amennyiben az adatforgalom nem sikeres, a terminál mindaddig nem fogad el újabb kártyát, amíg az adatfeladást el nem végeztetik vele.

A POS terminálok egy olyan, egyedi protokoll használatával kapcsolódnak a szerverre, amely belső hibajavító folyamataival az esetleges kapcsolati rendellenességeket kiszűri.

A szerveren keletkezett adatmennyiség tetszőleges időpontban, különböző szempontok szerint lekérdezhető, az adatok exportálhatók más, például a számlázást végző rendszerbe. Ezek alapján készülnek el az összesített tankolási számlák mellett a kutakkal történő elszámolások is.

Üzemeltetési tapasztalatok

A rendszer nyitott, azaz bárki csatlakozhat hozzá. A telepítés országosan már több mint hatvan gázkútnál megtörtént, és egyre nő a kártyahasználat száma is. Folyamatosan jelentkeznek mind a kártyaigények, mind a rendszerhez csatlakozni kívánó benzinkutak.

A biometrikus és chipkártyarendszer alkalmazási tapasztalatai

(A Folder Rt. referenciáiból)

A ID3D típusú biometrikus azonosítórendszer

A gazdaság különféle ágazataiban – így a számítástechnika, a haditechnika, az energiaszektor területén – jelentkező fokozott biztonságtechnikai elvárások vezettek a minden kétséget kizáró azonosítást célzó biometrikus eljárások kidolgozásához.

A biometrikus azonosítás alapja, egyben előnye, hogy nem a felhasználó által birtokolt tárgyat (mágneskártyát, kulcsot) vagy a megszerzett ismeretet (PIN kódot, jelszót) azonosítja, hanem magát a felhasználót. A személy azonosítása egy kizárólag őt jellemző, paraméterezhető biológiai sajátosság azonosításával történik. Ilyen egyéni jellegzetesség például az aláírás, a hang, az arckép, az ujjlenyomat vagy a kézfej.

A kérdéssel foglalkozó független intézetek az egyik legkedvezőbben minősített eszközként az ID3D típusú kézgeometria-azonosítót jelölik meg.

A berendezés a felhasználót kézfejének háromdimenziós képe alapján ismeri fel. A rendszerbe történő felvételezéskor a berendezésben elhelyezett kamera felvételeket készít a felhasználó kézfejéről, amelyek átlagolt adatai – mintánként 9 byte-on – kerülnek tárolásra. A felhasználó minden egyes azonosítása után az adatokat a berendezés a használatából nyert új adatok figyelembevételével módosítja, így követve a kéznek az idő múlásával bekövetkező változásait. Az ID3D rendelkezik a PIN kód bevitelére alkalmas billentyűzettel – amely egyben csendes riasztás kezdeményezésére is lehetőséget ad kényszerített alkalmazás esetén –, valamint opcionális kártyaolvasóval.

A berendezés működhet „stand alone" egységként vagy hálózatban; alkalmas például számítógépes hozzáférések szabályozására vagy beléptetőrendszerként közvetlenül ajtózár vezérlésére; önmagában vagy számítógéppel összekapcsolva statisztikai – munkaidő-nyilvántartási, mozgáskövetési – információk kezelésére.

Az ID3D azonosítórendszer előnyös tulajdonságait megbízhatósági, elfogadottsági, alkalmazhatósági mutatói bizonyítják.

Számos más eljárással összehasonlítva a hibás azonosítások aránya – a téves elfogadások és elutasítások száma – minimális, továbbá a mozgó alkatrészek nélküli berendezés működőképességét a fokozott igénybevétel nem befolyásolja.

A berendezés használata egyszerű, és kriminológiai képzettársításokkal nem jár; a kéz egy nyitott, átlátható területre helyezése nem kelt félelmet vagy bizalmatlanságot a felhasználóban.

Az ID3D alkalmazása a személyiségi jogok védelmét támogatja azzal, hogy a berendezés használatának néhány éves mellőzésével a felhasználó automatikusan kikerül a rendszer nyilvántartásából, mert az emberi kéz formája 4-5 év alatt – a berendezés számára felismerhetetlenné válva – átalakul.

Alkalmazási lehetőségek

A következőkben az ID3D néhány alkalmazási megoldását mutatjuk be.

• Az ID3D közvetlenül alkalmas ajtózár vezérlésére; önmagában vagy hálózatban – időzónák, hozzáférési és letiltási szintek felhasználók szerinti beállíthatóságával, a munkaidőre, mozgáskövetésre vonatkozó adatok nyilvántartásával – intelligens beléptető-, illetve mozgáskövető rendszerként működtethető.

• A pénzintézetnél telepített berendezés használatával gyorsan és teljes bizonyossággal megállapítható a pénzszállítást végző cégek – pénzszállításra előzetesen engedélyt kapott – munkatársainak személyazonossága.

• A banki ügyfelek azonosítását támogatja a CES (Confirmed Entrust System – Megerősített Meghatalmazási Rendszer). Az ID3D segítségével megvalósított CES rendszerben ellenőrizhető a fokozott számlavédelmi szolgáltatást megrendelő ügyfelek számlájáról tranzakciót kezdeményező személy jogosultsága. A teljes biztonságot kínáló komplett rendszerben az aláírók és állandó meghatalmazottak jogosultságát az ID3D vizsgálja.

• A berendezéssel szabályozható a számítógépes adatbázisok különböző szintű elérése az eltérő illetékességű felhasználók körében.

• A levelezőrendszerekbe, illetve a kihelyezett ügyfélterminálóknál integrált ID3D a digitális aláírásként szereplő kódok védelméről és/vagy megszemélyesítéséről gondoskodhat; e megoldás banki alkalmazását demonstráló példa a GIRO rendszerhez történő operátori hozzáférés ID3D-vel megvalósított kezelése.

A kidolgozott megoldás chipkártyára

MOK chipkártya

Az adatkezelés, így a biometrikus azonosítást célzó adatok védelmének biztonságát jelentősen növeli a kódok hardveren történő tárolása, aminek egyik lehetséges eszköze a chipkártya.

A chipkártya gyors népszerűsödését, elterjedését elsősorban az alábbiak indokolják:

• A chipkártya kis helyigény és nagyfokú mobilitás mellett képes betölteni a titkos kulcsokat tároló hardvereszköz szerepét.

• A chipkártya ára, kezelhetősége és az általa nyújtott biztonság kedvező arányt mutat, a biztonsági elvárások teljesítésére költségkímélő, felhasználóbarát megoldást kínál, így a felhasználók széles köre számára elérhető.

• A chipkártya multifunkcionalitását támogatja, hogy a chipben többféle alkalmazás elhelyezhető, amelynek igény szerinti aktivizálása a funkciók és szolgáltatások rugalmasan beállítható igénybevételét teszi lehetővé.

• A chipkártya szabványosítási folyamata, elfogadottságának terjedése mind nagyobb interoperabilitást eredményez.

A chipkártya már Magyarországon is hosszú ideje jelen van, például telefonkártyák, benzinkutas fizetőkártyák formájában.

Az első, fizetési funkcióra is alkalmas, chipes bankkártya a CIB Középeurópai Nemzetközi Bank Rt. és a Magyar Orvosi Kamara nevéhez fűződik.

A Magyar Orvosi Kamara – eleget téve törvényi kötelezettségének – a kamarai nyilvántartást és az orvosok működési igazolvánnyal történő ellátását chipkártya alapú rendszerrel valósította meg. Üzleti, műszaki és logisztikai megfontolásokból a chipkártya kibocsátását a CIB Bank vállalta.

A mindkét fél számára előnyös együttműködéssel létrejött kártya egyrészről az orvos személyes szakmai adatait rögzítő kamarai tagsági igazolványaként, másrészről lakossági banki szolgáltatásokat is kínáló nemzetközi bankkártyaként használható.

Az Affinity programot is magában foglaló kártya funkciói mindkét irányban bővíthetők:

- A tagságiigazolvány-funkció – a rendszer fejlesztési irányainak megfelelve – alkalmas egyéb információk regisztrálására, így továbbképzési vagy páciensadatok kezelésére.
- Bankkártyaként – a hazai és nemzetközi feltételek megteremtődésével – elektronikus pénztárcaként is működhet.

Üzemeltetési tapasztalatok

A rendszer beüzemelése folyamatban van, ezért részletes üzemeltetési tapasztalatokról még nem számolhatunk be.

EDI használata a kereskedelemben

(A Gábor Dénes Informatikai Főiskola hallgatójának esettanulmánya)

A kereskedelemben a vonalkódokat bolti szinten a pénztáraknál termékazonosítás céljából, vállalatoknál raktározáskor és az egymás közötti kereskedelem céljából alkalmazzák.

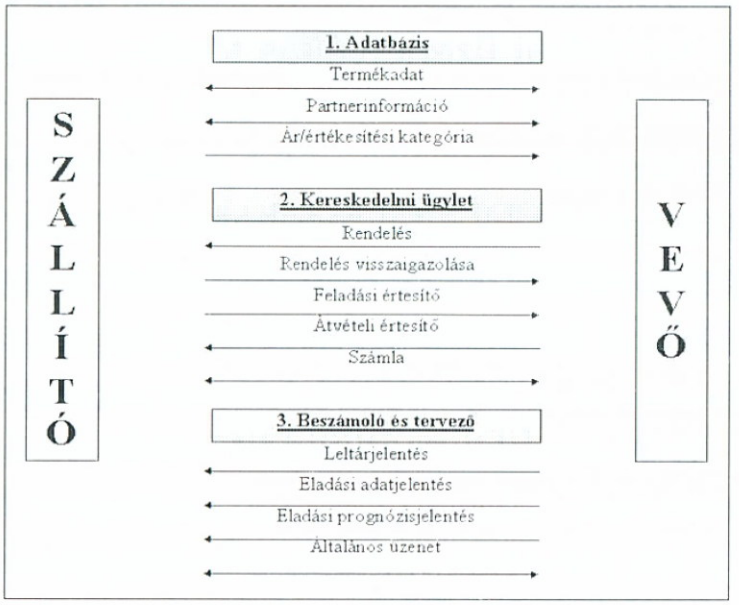
A Procter & Gamble esetében ez főként az EDI rendszerben van jelen.

Mi is az EDI?

Az EDI a partnerek közötti, vonalkód-azonosításra épülő információk és dokumentumok elektronikus úton történő cseréjére szolgál. Az információ cseréjére elektronikus módon, két komputer között kerül sor. Ennek alapfeltétele, hogy a két partner számítógépe kompatibilis legyen, s közös nyelvet beszéljen. Manapság ezt az értéknövelt hálózati szolgáltatások (VANS) segítségével érjük el, oly módon, hogy a beérkező információt fogadják, majd átkonfigurálják az adott komputer nyelvezetének megfelelően, vagy pedig későbbi felhasználás céljából tárolják. A VANS garantálja a gyors és biztonságos adatcserét. Az elektronikus úton történő kereskedelem igen jelentős költségcsökkenéssel jár, mivel feleslegessé válik a papírmunka, s rengeteg időt lehet megtakarítani. Az EDI segítségével az információ időeltolódástól és munkanaptól függetlenül elér a címzetthez. Használata nincs cégmérethez kötve, de a bevezetéshez szükséges beruházás miatt inkább a nagyobb vállalatok alkalmazzák. Talán a technikai háttér hiánya is lehet az egyik oka annak, hogy ma még csak kevesen élnek az EDI-szolgáltatók nyújtotta lehetőségekkel. A hazai felhasználók között kereskedelmi és termelővállalatok egyaránt megtalálhatók. Az EDI bevezetésének több kézzelfogható előnye is van. Az elektronikus úton elküldött üzenetet manuális beavatkozás nélkül, automatikusan be lehet tölteni a cég saját ügyviteli rendszerébe, nincs szükség a kézzel történő adatbevitelre, csökken a monoton manuális munka mennyisége és a hibák lehetősége, bizonyos feladatok egyszerűsödnek. A kereskedelemben az EDI rendkívül gyors módja annak, hogy az eladó a vevőket tájékoztassa a cég azon termékeiről, amelyekből rendelhetnek.

Sőt pontos adatszolgáltatás (például méret, súly, darabszám, karton stb.) közlésére is lehetőség van. Az EDI segítségével kiküszöbölhetők a nyelvi nehézségek, amelyek a nemzetközi kereskedelemben igen jelentősek. Erre a szabványosított EDI-üzenetek kiválóan alkalmasak lehetnek.

Az alapvető EDI-üzenet (EANCOM) felépítése



Az EDI az ECR (Efficient Consumer Response) alapja is, amit Magyarországon elsőként a Procter & Gamble kezdett el alkalmazni.

Az EDI-üzenetből a Metro és a Procter & Gamble között egyelőre csak a Rendelés (Order) rész működik.

A feladat specifikációja

Az EDI működtetése a Metro és a Procter & Gamble között.

A kidolgozott megoldás

A Metro és a Procter & Gamble közötti EDI-kapcsolat 1998-ban valósult meg, a két fél közös igénye alapján. A tervek szerint az EDI bevezetése mind a Procter & Gamble-nek, mind a Metrónak jelentős előnyökkel járt volna. Ezek közül a legfontosabbnak talán a rendelésekkel kapcsolatos időszükséglet csökkenése számít, de ezenkívül a pontosságnak és a megfelelő készletgazdálkodásnak is előnyére vált volna.

Ahhoz, hogy az EDI pontosan, hatékonyan és időben kezdjen működni, mindkét félnek meg kellett tennie a szükséges lépéseket. Miután

a Procter & Gamble munkatársai vázolták elképzeléseiket és az EDI-re vonatkozó tudnivalókat a vevő felé, s miután megtörtént a megegyezés, a vevőnek fel kellett készülnie az üzenet küldésére, az EDI rendszer üzembe állítására (ha eddig még nem rendelkezett volna ilyennel). Mikor ez megtörtént, a Procter & Gamble elküldte a termékek EAN kódjait tartalmazó listát, melyet a vevőnek be kellett vinnie saját rendszerébe. Ezután következett a tesztelés időszaka, ami körülbelül 1 hétig tartott. Ez idő alatt technikai üzenetváltás történt, amely azt a célt szolgálta, hogy ellenőrizzék, vajon minden termék és a rendelésben szereplő minden cég rendelkezik-e EAN kóddal, az helyes-e, és hogy a rendelési üzenet megfelel-e az EDI által meghatározott szabványnak. Amint megtörtént a tesztelés, indulhatott a párhuzamos futás, melynek során a vevő faxon és az EDI rendszeren keresztül egyaránt elküldte a rendelését a beszállítónak. A körülbelül 8 rendelést magában foglaló teszt alatt ellenőrizték, hogy az EDI-n átküldött rendelés egyezik-e a faxon leadottal. Természetesen akkor még az írásos rendelés számított mérvadónak. Ha a két rendelés minden alkalommal megegyezett, kezdődhetett a partnerek közötti EDI-rendeléses rendszer hivatalos működése.

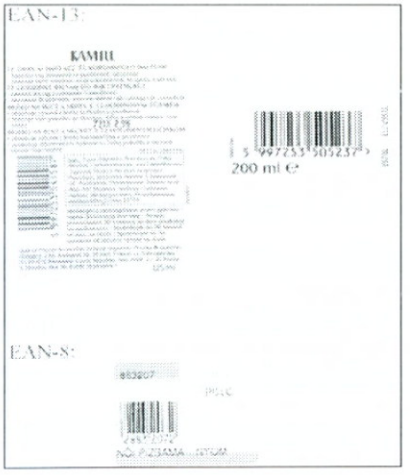
Az EDI működése és az ahhoz szükséges technikai eszközök a Metrónál

A Metro áruházban kétféle vonalkódot használnak:

- az EAN-13-at általában akkor, amikor a terméken már eleve szerepel a vonalkód,
- az EAN-8-at akkor, amikor a Metrónak saját magának kell kódolnia az adott terméket (a középső hat karakter általuk generált termékazonosító, tartalmaz egy ellenőrző és egy azonosító karaktert).

A vonalkódokat általában a felelős beszerző osztály viszi be a rendszerbe, amely egy Unix-szerveren futó Oracle-adatbázis. Az osztály feladata a vonalkódkészlet karbantartása is.

Ha a termék vonalkóddal együtt érkezik az áruház raktárába, akkor csak be kell vinni a rendszerbe, illetve ellenőrzik a kódot a Symbol LDT-vel (off-line rendszeren), így az új áru csak másnap jelenik meg a pénztárgépekben.



Ha a terméken nem szerepel vonalkód, akkor a Metrónak saját magának kell azt elkészítenie. Itt kétféle kódot alkalmaznak. Darabos terméknél vagy Metro-egységkiszerelésnél az EAN-8 használatos, míg a súlycikkek esetében (pl. hús, gyümölcs) az EAN-13 a meghatározó (ennél az első két kód tartalmazza a súlykódot – 28 –, a következő 4 a termékazonosító, a mellette lévő 5 karakter a súlyt írja le, míg az utolsó az ellenőrzőszám). A vonalkódokat UBI vonalkódnyomtatóval készítik, míg a súlykódokat a mérlegek nyomtatják, mivel beépített vonalkódnyomtatóval rendelkeznek. A mérlegből a termékre vonatkozó információk is lehívhatók, úgymint PLU szám (származtatott kód, amely a cikkszámmal van összerendelve), súly, ár, megnevezés stb.

Ha a termék bekerült a rendszerbe, a pénztárban kétféle módon azonosítható: kézi (UBI touch szkenner, PSC-lézerpisztoly, illetve Symbol 1850 lasertouch vonalkódolvasó) vagy asztali szkennerekkel (Spectro Physics). Mivel a termékek és a cégek azonosításához szükséges adatok megtalálhatók a pénztárgépekben – a központi rendszeren keresztül –, fizetéskor a számla rögtön bekerül az adatbázisba, és pár perc múlva akár készletellenőrzést, készletnyilvántartást és korrekciót is készíthetünk, ugyanis ez on-line rendszerben működik.

A felsoroltak közül egyedül a Symbol olvasók állnak off-line összeköttetésben a központi rendszerrel, ezért ezeket reggel töltik fel, és az előző esti adatot tartalmazzák (a nap folyamán a termék konfigurációján – EAN, kiszerelés stb. – változtatott adat csak másnap reggel kerül be az olvasókba).

A Metro a jövőben tervezi lecserélni rendszerét rádiófrekvenciás azonosításon működő on-line rendszerre. Olyan vásárlói ellenőrző display

kiépítését tervezik minden sorra, amelynek segítségével a vásárlók könnyen azonosíthatják a polcon található terméket a vonalkód alapján (pl. árinformációk). Ezen displayek alapjai online összeköttetésű vonalkódolvasók lennének.

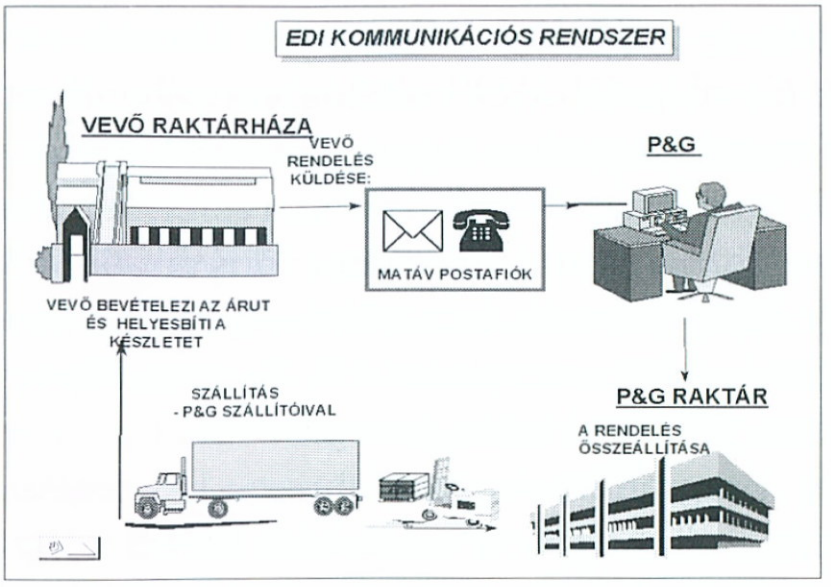
A Metro EDI-rendszerének működéséhez az adatbázisban egy új mező felvételére volt szükség, amely a rendelési vonalkódot tartalmazza (a cikkek azonosítására), és kizárólag rendeléskor használatos. Ezt a kódot a partnercég határozza meg, s lehet 8, 10, 12, 13, 14 karakter hosszúságú. Az esetleges változást az adott cégnek jeleznie kell a felelős beszerző felé, aki azt karbantartja. Mivel a Metro többféle kiszereléssel foglalkozik (kartonos, darabos stb.), ezért az ellenőrzőszám (check digit) segítségével határozzák meg, hogy mely Metro-egységről van szó (a P&G-nél a samponok esetében ez lehet kartonos, kétdarabos vagy darabos). A rendszer maga – mint a legtöbb cégnél – az Intercept Plus szoftvert használja (amely a Matáv rEDInet programja). A rendeléseket a rendszer reggel 7-kor automatikusan megpróbálja elküldeni; ha sikerül, akkor arról visszajelzés érkezik (mely nem azonos az EDI-s rendelés-visszaigazolással). Ha nem sikerül az átvitel, akkor a gép még kétszer megkísérli azonnal, majd délig félóránként próbálkozik. Ugyanakkor arra is van lehetőség, hogy a rendelést manuálisan küldjék el, amit sikertelenség esetén reggel 8-kor egy szakember egy program segítségével meg is tesz. A Metro tervezi, hogy a jövőben a megrendelésen az egységárakat is feltünteti, mellyel a nézeteltérések is elkerülhetők.

Mint már említettük, az adatbázisban vevőre vonatkozó adatok is szerepelnek, mivel a vevőket is vonalkóddal azonosítják, amely a vevőkártyán szerepel. Jelenleg – átmenetileg – kétféle kártyatípus van: papírkártya, melyet UBI nyomtatóval készítenek, illetve mágnescsíkos műanyag kártya, melyet Digicard kártyanyomtatóval hoznak létre, és mindkettőt helyben nyomtatják. A vevőazonosító szintén az EAN-13 kódon alapul. Az első két karakter: 20 (vevő), a következő kettő az áruházszám (ahol a vevőt regisztrálták), majd 6 karakter a vevőazonosító, az utolsó három pedig az ellenőrzőszám (az első kettőt a Metro generálja valamilyen algoritmus alapján, míg az utolsó az EAN ellenőrzőszám). Ezt is a központi rendszerbe töltik be, majd a kasszába kerül.

Az EDI felépítése, működése a Procter & Gamble-nél

A Procter & Gamble-nél 1998 első hónapjaiban kezdték el az EDI-t tudatosan alkalmazni Magyarországon. Az egész egy on-line kapcsolatú rendszerre épül, amely egy Novell 4-es szerveren fut. A szoftver szintén az Intercept Plus (konkrétan az Intercept Plus 5.04.16 verziója, melyet a közeljövőben szándékoznak lecserélni az 5.22-es verzióra, ez már 2000-kompatibilis). A kommunikáció US Robotics Sportster Flash 33,6 kbps-os modemen keresztül valósul meg.

Az EDIscript programnyelv mindennap 14 órakor ellenőrzi (egy batch fájl segítségével), hogy jött-e rendelés (mivel a P&G-nél is csak az EDI Order része él), és ha jött, arról értesíti az OSB osztályt (Ordering, Shipping, Billing). Az EDI rendszer a megrendelést egy ún. Flat File formátumra fordítja le, amelyben megadható az is, hogy a szerverben a fájlt hová tegye. Mivel az ügyviteli rendszer a Procter & Gamble-nél Platinum for Windows alatt fut, szükség van egy modulra (Premier EDI), amely a szövegfájlt fel tudja dolgozni, azaz az EAN kódokat egy adatbázis alapján megfelelteti a Platinumban szereplő kódoknak, majd az átkonvertálásról riportot készít. Így a megrendelés a tényleges Order Entrybe kerül a Platinumban. Ha bármely EAN kód nem szerepel a megrendelésen, az manuálisan ellenőrizhető és pótolható, ha termékről van szó. A partnercég vonalkódja elengedhetetlenül szükséges a megrendelésen, e nélkül a rendelés nem teljesíthető! Amint a rendelések bekerülnek a rendszerbe, a szállítási folyamat elindítható. Miután még egyszer ellenőrizték, a szállítási dátum alapján a Platinum szoftver kiválasztja, hogy mely rendeléseket küldjék ki a raktárba a következő napi szállításokhoz. Ezek után lefuttatnak egy programot, amelynek eredményeképpen elkészülnek az ún. szállítási összesítők (vállalatonként), amelyeket faxon ki is küldenek a szállítóknak. Ezzel egy időben kiküldik a Procter & Gamble raktárába a rendelési összesítőt a fent említett modemen keresztül (ebből ott másnapra elkészítik a rakodási összesítőt). A másnap délig összekészített szállítmányokat délután a raktárban felpakolják, ellenőrzik, majd szállítólevelet készítenek hozzá, amelyből egy példányt eljuttatnak a Procter & Gamble irodájába, egy a szállítónál marad, illetve kettőt a vevő kap meg (ebből egyet lepecsételve visszajuttat a Procter & Gamble-höz).



Üzemeltetési tapasztalatok és továbbfejlesztési lehetőségek

Mint fent már említettük, az EDI rendszer bevezetése jelentős költségcsökkenést, hatékony készletgazdálkodást eredményez, illetve nagymértékben elősegíti a just-in-time technológia alkalmazását. Emellett az ECR rendszernek is az egyik alapvető eleme.

Fejlesztésként mind a Metrónál, mind a Procter & Gamble-nél az EDI rendszer teljes mértékű kihasználását javasolnánk, amellyel még inkább csökkenthető a papírmunka, s a költségek, a hibalehetőségek, az emberi tévedések, illetve a szükséges munkaerő is.

Emellett a Metrónál egy hatékonyabb (on-line) rendszer kidolgozását javasolnánk, amellyel gyorsabb és pontosabb információáramlást tudnának megvalósítani. Erre tervezik a rádiófrekvenciás azonosítás bevezetését a jövőben.

BarVision termelésirányítási rendszer vonalkód és RFDC alkalmazásával

(A BCS Hungary Kft. referenciáiból)

A feladat specifikációja

A vonalkódos technológia mind szélesebb körű elterjedése új megoldandó feladatokat is jelent. A készletnyilvántartó rendszerek sokszínűsége, az ajánlások figyelmen kívül hagyása és a meghatározó külföldi partnerek elvárásainak való megfelelés kényszere komoly feladatok elé állítja a termelő vállalkozásokat. A Tiszai Vegyi Kombinát Rt. – BIAFOL Kft. 1999-ben üzembe helyezett új gyártósorának kapacitását túlnyomó részben az Európai Unió területén működő vállalatok kötik le. A magas minőségi követelmények mellett a termékek csomagolása és címkézése is kritikus tényező. A keletkező késztermékek egy-egy berendezésen párhuzamosan több rendelésre készülnek, melyekhez eltérő adattartalmú, megjelenésű és nyelvi változatú termékkísérő címkék tartoznak. A problémák megoldására beüzemelték a BCS Hungary által kifejlesztett BarVision termelésirányítási rendszert, amely egy rádiófrekvenciás hálózaton alapuló, vonalkódos üzemirányítási alkalmazáscsomag. A rendszer teljes integráltságot valósít meg a korszerű folyamatirányító berendezésekkel és az IBM AS400-as gépen futó BPCS információs alaprendszerrel.

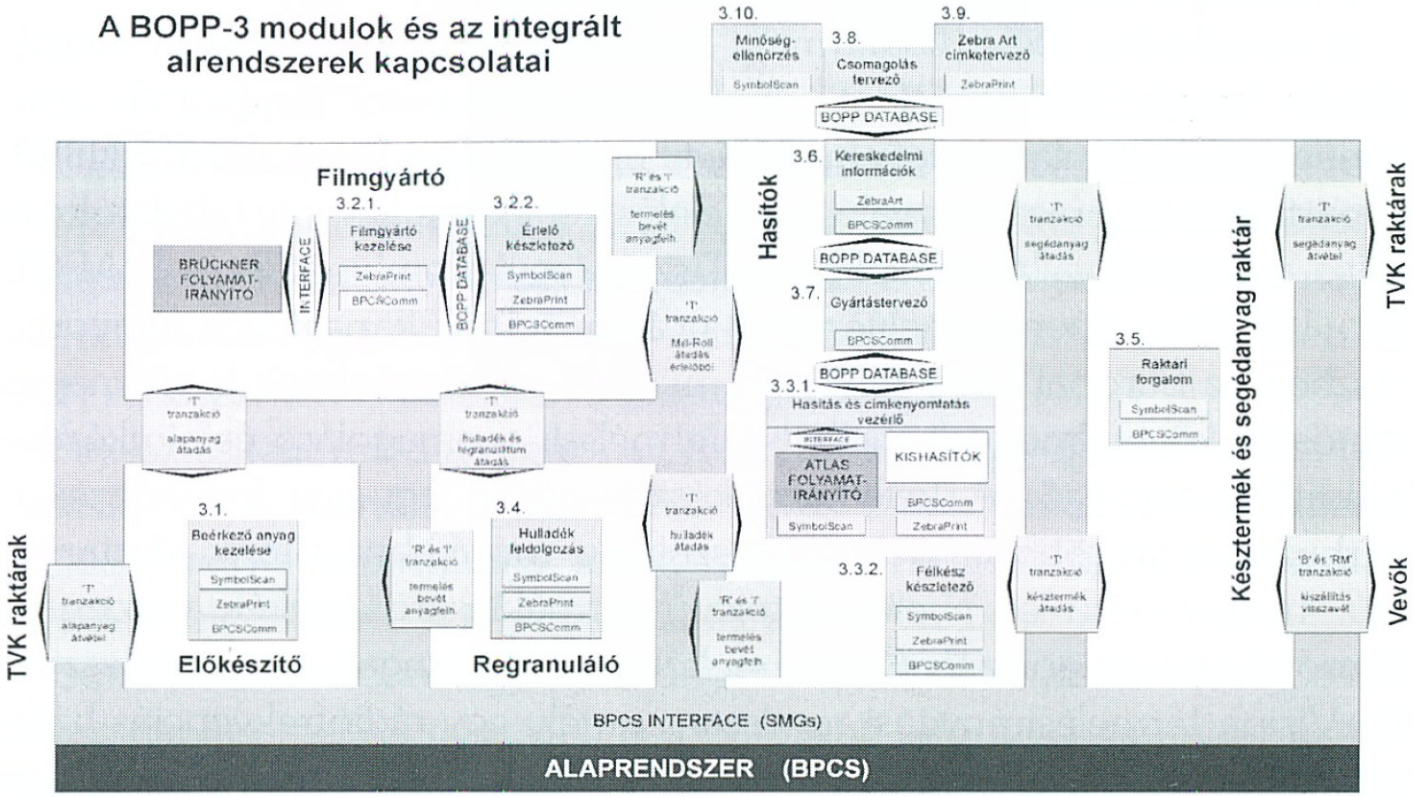
A fejlesztési célok

- Teljes IT-támogatás a BIAFOL Kft. termelési folyamatára.
- Az üzleti és a termelési folyamatok integrálása (Brückner, Atlas folyamatirányító rendszer).
- A kézi adatbevitel kiváltása.
- A vevők vonalkódos adatigényének rugalmas kiszolgálása.
- Automatikus adatátadás a BIAFOL Kft. információs alaprendszerének (BPCS).

A kidolgozott megoldás

Rendszeráttekintés

Az üzemirányítási rendszer két termelésifolyamat-irányító rendszerrel tart kapcsolatot. A Brückner filmgyártó sorától termelési és technológiai adatokat vesz át, az Atlas hasítóberendezésének beállítási utasításokat ad, és termelési információkat kap tőle. A rendszer a készletek mozgatási tranzakcióit rádiós hálózaton keresztül az adatgyűjtő terminálától kapja. A feldolgozott adatok a vállalatirányítási rendszerhez kerülnek.



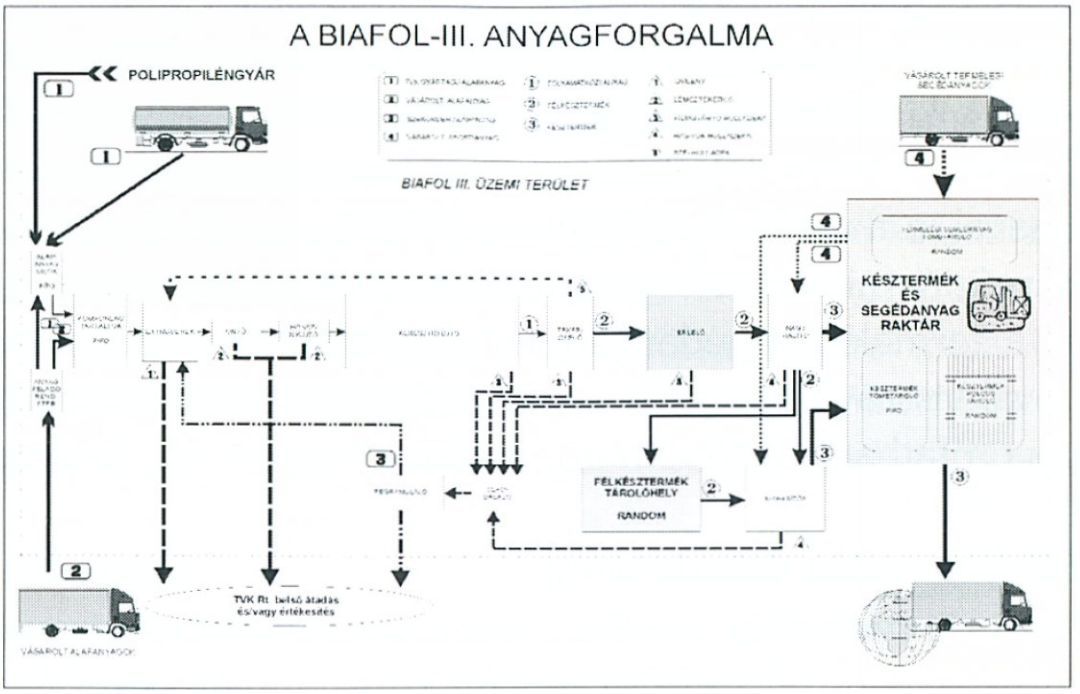
Kapcsolódó rendszerek

Az anyagforgalom ügyviteli támogatása

Alapanyag-ellátás

A külső beszállítóktól érkező anyagok beszerzését és bevételezését a TVK Rt. központi egységei végzik. Az anyagokat központi raktárakban tárolják, és az üzletág igényeinek megfelelő mennyiségben szállítják az üzemcsarnokba. A beérkező anyagokat a BPCS rendszerből lekérdezett azonosító, mennyiségi és minőségi adatokkal, rakományonként vonalkódos címkével látják el. Az alapanyagok az átmeneti tárolást követően pneumatikus anyagellátó rendszeren keresztül jutnak típusuknak megfelelően a komponenstartályokba. A feltöltött anyagok rakhelyváltási

tranzakcióit hordozható vonalkódos terminálon kell rögzíteni a BOPP adatbázisába és a BPCS rendszerbe.



Anyagforgalom

Termelésisegédanyag-ellátás

Az expediáló területére beérkező termelési segédanyagok átvételi ellenőrzése után cikkenként kinyomtathatók a megfelelő adattartalmú címkék, amelyek darabszáma attól függően határozható meg, hogy a tranzakcióban szereplő mennyiséget milyen tételekben szükséges azonosítani a későbbi felhasználáshoz. A címkék nyomtatása a raktáros irodájában történik. A beérkezett anyag átvétele a kinyomtatott címke felragasztásával és a rajta lévő vonalkód leolvasásával történik meg. Az így átvett mennyiségre a kezelői jóváhagyást követően rakhelyek közötti tranzakciót generál a rendszer.

Az expediálóból a gyártás szükségleteinek megfelelően, az átadásra kerülő anyagok vonalkódos címkéinek leolvasását követően, a rendszer rakhelyek közötti tranzakciót generál, és ezzel a feladott mennyiség átkerül az üzemcsarnok megfelelő rakhelyére.

Késztermék-raktározás

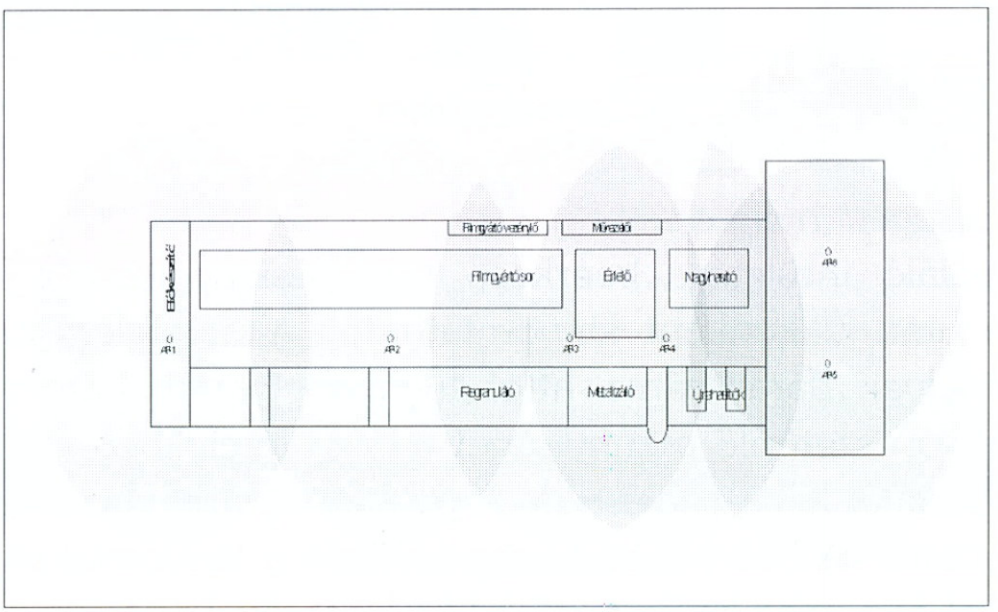
A késztermékek átvételét egy átadási terület közbeiktatásával oldják meg. Az üzemi területről átadandó rakományokat a hordozható terminál

segítségével logikailag kijelölik, a raktáros pedig a rakomány megérkezésekor a rajta lévő vonalkód leolvasásával és a tárolási rakhely megadásával veszi át. Az így beérkezett mennyiségre tranzakciót generál a rendszer.

A késztermék raktáron belüli áthelyezése, a szállítás előkészítése, a raktári területről a kültéri targoncáknak való átadás és az egységrakományok szállító járműre történő felrakásának megerősítése hordozható terminál alkalmazásával, a megfelelő BPCS-tranzakció generálásával történik.

A reklamáció miatt esetleg visszaérkezett rakományokat az átvételi rakhelyen a termelési segédanyagok mintájára kell a megfelelő BPCS-tranzakcióval visszavételezni. A segédanyagoknál leírtak szerint szükség esetén kinyomtatható a vonalkódos címke.

Rádiófrekvenciás lefedettség



Lefedettség

Az ábra a közel 300 méter hosszú üzemcsarnok rádiófrekvenciás lefedettségét szemlélteti. A termelési folyamat nagy adatforgalommal rendelkező helyeit biztonsági okokból többszörös lefedettséggel építették ki, így egy elérési pont estleges meghibásodása nem okoz észrevehető változást az adatforgalomban. A rendszerben 6 db AP-2412 Ethernet Access Point került telepítésre. Ezt az eszközmennyiséget kizárólag a nagyfokú biztonságra való törekvés indokolja. A mérések szerint az ábrán AP-1-ként jelölt elérési ponttal az AP-4-es körzetében is lehet kommunikálni.

A technológiai folyamat támogatása

A filmgyártó adatkezelése

A filmgyártó berendezést a Brückner folyamatirányító rendszere felügyeli és vezérli. A gyártósor technológiai paramétereit, az anyagfelhasználást és a sor végén keletkező ún. millroll tekercs paramétereit a rendszer automatikusan gyűjti.

A tekercs levételekor a BOPP-adatbázis és a BPCS számára termelésbevételezési és anyagfelhasználási tranzakciókat generál a rendszer. Szintén a tekercsváltáshoz kötődik az azonosításhoz szükséges vonalkódos címke előállítása két példányban, amely a leváltott tekercsre, illetve a tekercsből vett minőség-ellenőrzési mintára kerül.

Az érlelő tároló

A filmgyártóról levett tekercs min. 24 óra időtartamra az érlelő tárolóba kerül. A tekercsek további feldolgozása az ún. nagyhasító berendezésen történik. A keresés és a kiválasztás segítésére a millroll részletes paraméterei – a rakhelypozíciók és az érlelési idők feltüntetésével a grafikus raktártérképen – a tekercset szimbolizáló grafikus objektumra kattintva jeleníthetők meg. A rakhelyek közötti mozgatást az egér használatával, a szimbólum áthelyezésével lehet elvégezni, és a háttérben a változásról készlettranzakciót generál a rendszer.

A nagyhasító

Az érlelő tárolóból kikerülő tekercsek további feldolgozása az Atlas folyamatirányító rendszere által vezérelt nagyhasító berendezésen történik. A rendszer elektronikus úton fogadja a beállítási adatokat, és a hasítás megkezdése előtt kötelezően át kell adni a feldolgozandó tekercs azonosítóját, amelyet a kezelő a tekercscímkén lévő vonalkód leolvasásával ad meg. Az Atlas rendszer nyomon követi a keletkező tekercsek helyét, és az automata szállítópályába épített mérlegről lekerülő tekercsről elektronikus üzenetet küld a külső programok felé az elkészült tekercsek azonosító adatait és a mért tekercssúlyt illetően.

A keletkező tekercsek adatait egyenként, azonosítva és tekercssúllyal ellátva, üzenetként adja vissza az Atlas rendszere. Az átadott adatok és a rendeléshez rögzített címkeformátum alapján történik a vonalkódos

tekercs- és csévecímkék nyomtatása. A tekercsek adatait a rendszer folyamatosan rögzíti. A csomagolási előírás alapján a program automatikusan nyitja az új konténereket, és a megteltekre nyomtatja a konténereket azonosító címkéket. A teli rakományokon lévő tekercsek összesített mennyisége alapján termelésbevételi BPCS-tranzakciót generál a rendszer. A millrollfelhasználás BPCS-jelentése folyamatosan, a tekercsváltások alkalmával történik.

A nagyhasító berendezésen részben felhasznált millroll tekercsekre vonalkódos címkét nyomtat a rendszer, és generálja az érlelőbe való átadás BPCS-tranzakcióját.

Az újrahasítók

A nagyhasítón kötött és változó szélességű, félkészként gyártott tekercsek a félkészkészletezőbe kerülnek. A tárolás, a felhasználás megkezdésének jelzése az újrahasítóknál telepített számítógépen történik, a tekercseken lévő vonalkód leolvasásával. A keletkező tekercsekre a korábban elmondottak szerint készülnek a vonalkódos tekercs-, cséve- és rakománycímkék, valamint készlettranzakciók.

Címkék

Regranuláló

A filmgyártótól és a hasítóktól átkerülő hasznosítható hulladékok feldolgozása során keletkező szekunder alapanyagok termelésbevétel- és anyagfelhasználás-tranzakcióit generálja a program a kezelők által méréssel meghatározott mennyiségben. A konténerekbe vagy zsákokba fejtett szekunder anyagrakományokra azonosító címkét kell nyomtatni.

Mindennemű hulladék bálánként, illetve ketrecenként címkézendő, függetlenül attól, hogy a rakomány elhagyja-e az üzemet, vagy sem.

Üzemeltetési tapasztalatok, továbbfejlesztési lehetőségek

- Egyéb ügyviteli folyamatok támogatása
- A vevői igények feldolgozása
- Csomagolástervezés
- Gyártástervezés
- Változó adattartalmú címke tervezése
- Minőség-ellenőrzés

Fejlett megoldások

- „Drag and drop" technológia a felhasználói kommunikációban
- Szimulált fizikai készletmozgások a képernyőn
- Drag and drop on-line tranzakció-végrehajtás kézi adatbevitel nélkül

Az RF technológia előnyeinek kihasználásával

- A készlettranzakció az üzleti alkalmazásban hozható létre és paraméterezhető.
- Felhasználófüggő, a jogosultságnak megfelelő terminálképernyők és promptok.
- A terminálfunkciók az üzleti alkalmazásból szabályozhatók (C/S architektúra).
- Tetszőleges olvasási sorrend, prefixekkel ellátott vonalkódok („önazonosító" adatbevitel).
- Intelligens vonalkódos címkenyomtatás.
- Dinamikusan változó adatok az alkalmazásból.
- Felhasználó által definiált címkeformátum (nyelv és tartalom)

Rend, logisztikai támogatás az e-business korában

(A Psion Rendszerház Kft. referenciáiból)

A gazdasági események rögzítése, számbavétele már a sumérok óta hozzátartozik az „üzleti élethez". Kezdetben agyag, kő, fa, papirusz, majd papír volt az adathordozó. A gépi adatfeldolgozás, a számítástechnika korának beköszöntével a papírt (elsődleges bizonylatot) kellett a gépekhez vinni. A mobil informatikai eszközök ezt a folyamatot megfordították, hiszen ma már a kézigépeket lehet és kell a rögzítendő gazdasági eseményhez vinni. Ezzel a módszerrel azonnal elektronikusan tárolódik az adat, melynek segítségével könnyebb, gyorsabb és pontosabb lesz a nyilvántartásunk.

Az aktív keresők kb. 40-50%-a mobil (nem íróasztal melletti) tevékenységet végez, ezért az ilyen jellegű számítástechnikai feladatok tömege sem elhanyagolandó.

Az adatrögzítés gyorsítása és pontosítása érdekében egyre több és biztonságosabb technológiát, úgynevezett automatikus azonosítási eljárást fejlesztenek ki és vezetnek be a termelési, raktározási, kereskedelmi, sőt a banki tevékenységek megkönnyítéséhez; közismert azonosító módszer a vonalkód, a mágneskártya, a rádiófrekvenciás (passzív és aktív) chip, a tirismodul, a chipkártya (intelligens kártya), bonyolultabb eljárásoknál az ujjlenyomat, az íriszkép, a fotó stb.

Természetesen ahogy fejlődtek az azonosítók, úgy fejlődtek a jelleolvasó és -feldolgozó készülékek is. A felhasználók kényelmét szolgálja az a törekvés, hogy az ilyen azonosító eljárások minél könnyebben, akár on-line bekerüljenek a vállalati ügyviteli rendszerekbe (SAP, Scala, Libra, Infosys stb.).

Az elektronikus üzletvitel kora

Korábban egy vállalati tevékenység mértanilag zárt térben folyt le, például a cég telephelyén. Ma nem feltétlenül van így. Ez egyrészt fölértékelte a kommunikációt, amelynek mára legfontosabb médiuma az internet. Másrészt ebben a globalizációban, amikor is a vállalatok szemei és

karjai távol járnak a központtól, különösen feszesnek kell lennie az adatbázisokkal való kapcsolattartás rendjének, legyen az élő (on-line) vagy időről időre egyeztető jellegű (off-line). Ez a kitörés a behatárolt terekből továbbá azzal járt, hogy a vállalati tevékenységben megnövekedett annak a fontossága, miként lehet a megfelelő időben a megfelelő helyre szervezni a megfelelő erőforrásokat, munkatárgyakat, partnereket, ügyfeleket, termékeket az elérhető legkisebb költséggel. Tehát felértékelődött a logisztika szerepe.

Az elektronikus üzemvitel korának ipari-vállalati rendszereiben az egymással összefüggő tranzakciós körökben, a logisztikában a kommunikáció, az azonosítás (vonalkód, mágnescsík), az adatbevitel kulcsszerepet játszik. Ez a Psion termékeinek világa.

A feladat specifikációja

A Magyar Autóklubnak 300 ezer tagja van, és 80 segélyautó járja az országot. Ilyen körülmények között a kapcsolattartás és az adminisztráció alapvetően fontos.

A kidolgozott megoldás

Multifunkcionális mobil POS terminál

Ma korszerű rendszer egyszerűsít le és gyorsít fel minden feladatot, teljes információs apparátust nyújtva a hibajelentés regisztrálásától a munkalapok feldolgozásáig. Ennek feladata a központi adatfeldolgozó rendszerrel való dokkoló, diszpécseri, illetve távközléses adatkommunikációs kapcsolattartás is, az abban záródó tranzakciós körök (megbízások menedzselése, végső elszámolások, tagi adminisztrációk, a munkatársak tevékenységének követése-elszámolása) érdekében. Adatkommunikációt igényel a bankkártyás fizetés is (tiltott kártyák kiszűrése, authorizáció stb.).

A segélyautók fedélzeti ügyviteli rendszerének lelke egy beszerelt Psion Workabout adatgyűjtő ipari kéziszámítógép, amely szoftvere által POS terminál minőségű, összekapcsolva egy GSM SMS-rendszerrel (Ericsson SH 888), valamint egy mágneskártya-olvasóval egybeépített nyomtatóval (Huniprint MCR). Ezekkel a kézigép két soros vonalon kommunikál, egy harmadikat pedig a közeljövő GPS-rendszerével való kommunikációra szánnak.

A leggyakoribb működési mód a következő: telefonon segélyhívás érkezik valamelyik diszpécserközpontba. Itt a feladatot az adatokkal együtt kézzel számítógépre viszik. A gépkocsipark lehetőségei és a feladattömeg közötti kapcsolat működtetése a diszpécser feladata. A megbízás SMS formájában érkezik meg a segélykocsihoz. A Psion Workabout kijelzőjén jelentkező riasztást egyszerű esetben egy gombnyomással igazolják vissza, bonyolultabb, egyeztetést kívánó esetekben szóbeli vagy SMS-kapcsolat által. A folyamat köreinek fő összetevői visszacsatolt üzenetváltással: a feladat elvégzőjének kiválasztása (megkeresés – a segélykocsi helyzetének visszajelzése), a feladat elvállalása (kirovás – nyugtázás), a feladat teljesítése (kirovás – elvégzés visszaigazolása) és a fizetés (számlázás – fizetési visszaigazolás).

A legfontosabb ciklus maga a javítás–fizetés. Ennek az első fele a feladat visszaigazolásával kezdődik, és a szerelésről szóló jelentéssel végződik. A második fele a számlázással kezdődik, és a fizetés kivitelezésével végződik. Ez utóbbira több lehetőség is van, például rögzített, a Workaboutban tárolt árak mellett a bankkártyás fizetés, amely igényli a központtal és a bankkal való off-line vagy élő kapcsolatot. A mágneskártyaleolvasó a POS terminál szoftvere segítségével képes bankkártyát fogadni, az autóklubbal GSM útján kommunikál, ahonnan már a hagyományos modemes üzemmód révén tartják a kapcsolatot a bankszámla kezelőjével (K&H Bank).

Hogy a fedélzeti rendszer megbízhatóan el legyen látva minden szükséges adattal, továbbá a kiadott számlák információi a központi adatbázisba bekerüljenek, a kézigép adatait rendszeresen frissítik.

Üzemeltetési tapasztalatok

A segélyautók ügyvitelét forradalmasító technológia, illetve eszközpark megalapozta a Magyar Autóklub ISO 9002-es minőségbiztosítási dokumentációs módszertanát.

Természetesen az operatív munka támogatása mellett a korszerűsítésnek egyéb eredményei is vannak, pl. meghibásodási statisztikák, javítási munkák gazdaságossági vizsgálata, optimális hálózat kiépítése stb.

***

A feladat specifikációja

Vonalkóddal vezérelt operatív munkafolyamatok egy fémipari trösztnél.

A kidolgozott megoldás

Egy fémipari trösztnél működik a Kentaur becenevű, Windows NT-re és Psion Workaboutra épülő tmk-rendszer, amelynek egyik hatása éppen idevág. A PC-s rendszer adatbázisa a vonalkóddal azonosítható ellenőrzőpontokból, az azokon végrehajtandó karbantartó vagy más jellegű műveletekből és ezek lehetséges eredményeiből áll. Mindennap letöltik a bejárandó útvonalat az alkalmazott Workaboutjára, aki az ellenőrzőpontokat azonosítja a vonalkód leolvasásával (így mindenképpen végre kell hajtania a feladatot). A vonalkód leolvasása után a Workabout közli a teendőket, az esetleges megjegyzéseket. A dolgozó betáplálja a műveletek eredményeit a Workaboutba, és amennyiben az adatok nem felelnek meg az előzetesen megadott feltételeknek, egy kialakított riasztási lista alapján a rendszer értesíti a megadott személyeket. A nap végén a Workaboutról letöltik az adatokat

a központi adatbázisba, így pontos dokumentáció készíthető az üzemi rendszer állapotáról, ami a minőségbiztosításnak elengedhetetlen feltétele.

Üzemeltetési tapasztalatok

A leírt rendszer illeszkedik a fémipari tröszt minőségbiztosítási rendszeréhez.

***

A feladat specifikációja

Több mint 200 terítőautóval szállítja ki termékeit a forgalmazókhoz a Dréher Sörgyárak Rt. Az üzemvitelt-üzletvitelt a vállalat és feladatai nagyságrendjének megfelelően a legerőteljesebb kategóriába tartozó vállalatirányítási rendszer, az SAP R/3 támogatja. A feladat az értékesítés-áruterítés ügyvitelének hatékony megoldása volt.

A kidolgozott megoldás

SAP R/3 rendszerek Psion Workabouttal és vonalkóddal

A cég gazdasági életét döntően meghatározó értékesítés-áruterítés ügyvitelének számítógépesítését a Psion mobileszközeivel oldották meg hatékonyan. Az SAP megfelelő modulja a számlákat/szállítóleveleket nem nyomtatja papírra, hanem az aktuális számlák összes adatát a Psion Workaboutra töltik. A teherautó vezetője a rá vonatkozó túratervet is elektronikus formában kapja meg. A Workabout a tervnek megfelelően kínálja fel a soron következő szállítási címet. A tulajdonképpeni mobil eladás során a teherautóról átadott árukról, valamint visszavett göngyölegekről a helyszínen azonnal elkészül a számla és a szállítólevél. Az árukiszállítás-fizetés, a göngyöleg-visszavétel adatai azonnal a mobilszámítógépbe kerülnek, a vállalatirányítási rendszerrel kapcsolatot tartva. (A túrák – kiszállítások – végén a teherautó vezetőjétől átvett készülékek adatai az SAP rendszerbe kerülnek. Ezzel az eljárással gyorsan és gazdaságosan frissíthetők a napi forgalmi adatok. A fedélzeti egységek alapja ebben az esetben is a Psion Workabout kézigép, amelyhez Star DP8340-es nyomtató tartozik. Lehetőség van a jelenlegi konfiguráció bővítésére bankkártya-elfogadáshoz, GSM-, SMS-, GPS-technológiák alkalmazásához stb.).

Üzemeltetési tapasztalatok

Ez a terítőautós rendszer a vállalatirányítási nagyrendszer szeme és keze. A Psion kézigépei és a Psion Rendszerház partnereivel közösen köréjük épített mobil terminálok nagyban emelik a vállalatirányítási rendszer alkalmazhatóságát. Ennek referenciája minden olyan eset, amelyben Psion Workabouttal lehet hozzájuk csatlakozni, de az is, ha az adatbevitelt vonalkódolvasóval lehet támogatni – annál is inkább, mert vonalkódolvasóval a Psion Workabout is felszerelhető.

Általában az SAP kiterjesztése hiányzik, ezért a MÁV Informatika és a Psion Rendszerház Kft. együttműködési partnerként megállapodott, hogy különböző mobil alkalmazásokat fejleszt ki az SAP-hoz. Az első ilyen, referenciákkal rendelkező késztermék az AM modulhoz illesztett tárgyieszköz-leltározó alkalmazás. A Psion Workaboutok letölthetik az Eszköztörzs állományt, és a leltári adatok a törzshöz tartozó egyes cikkekről ugyancsak a Workabouton át jutnak vissza az AM modulhoz. Ezért a Workaboutokat vonalkódolvasóval egészítették ki. Az SAP beépített SapScript eszköze segítségével könnyedén készíthetők el a szükséges vonalkódok, vonalkódos nyomtatványok állományai. A rendszerházak az együttműködési megállapodásban rögzítették, hogy készek testre szabni, bevezetni bármilyen más intézménynél, vállalatnál is a vonalkódos nyilvántartásokat mint a logisztikát támogató korszerű eszközök egyik fajtáját.

Elektronikai alkatrészek kamerás minőség-ellenőrző rendszere

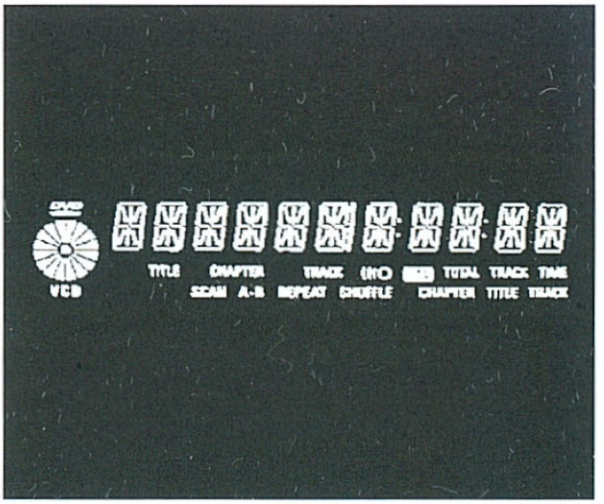
(A Vidikon Kft. és a Sárkány Rt. közös referenciáiból)

A probléma specifikációja

Az elektronikai iparban a beültetésre kerülő alkatrészek (tranzisztorok, kapcsolók, ellenállások stb.), digitális kijelzők (DVD-lejátszók és videomagnók kijelzői), komplett mechanikák (kazettás magnó, autórádió stb.) automatikus ellenőrzése kamerás azonosító rendszerrel, a digitális képfeldolgozási technikát alkalmazva hatékonyan megvalósítható.

Tekintsünk át egy megvalósult projektet! A feladat a következő volt:

A szórakoztatóelektronikában használt DVD-lejátszók kijelzőjének ellenőrzése. A kijelzőpanelen lévő szegmensek mindegyikének világítania kell az ellenőrzés során.



DVD-lejátszó kijelzőjének szegmensei

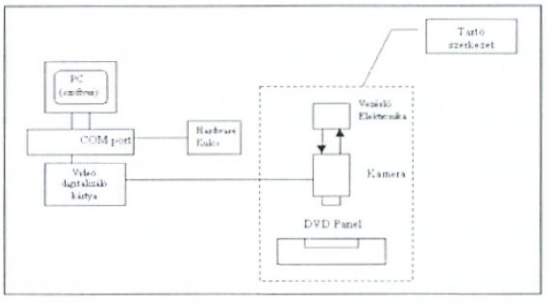
Az ellenőrzőprogramnak automatikusan el kell döntenie, hogy minden szegmens világít-e. A fenti képen látható DVD-kijelző esetében ez 199 db különálló szegmens vizsgálatát jelenti. Abban az esetben, ha talál hibás szegmenseket, akkor azt is ki kell jeleznie, hogy azok pontosan hol vannak. Az automatikus ellenőrzés időtartama maximum 3 mp lehet.

A kidolgozott megoldás

A feladat megoldásához egy célműszert kellett kifejleszteni, amely a következő részekből áll:

- kameratartó szerkezet,
- zoomos kamera, típusa Hitachi,
- mikrovezérlővel ellátott vezérlő elektronika a zoomos kamera vezérléséhez,
- mikrokontrolleres alapú hardverkulcs a termék védelméhez,
- PC (Pentium 233 MMX, 32 MB RAM),
- Bt848 videodigitalizáló kártya a zoomos kamera képének fogadásához,
- szoftveres alkalmazás Delphiben és Quick C-ben fejlesztve.

A rendszer elemeinek kapcsolódását a következő ábra szemlélteti:



Minőség-ellenőrző rendszer vázlata

A feladat az automatizált alakfelismerésre vezethető vissza. A felismerés mintaillesztéssel történik, ahol a (hibátlan) mintákat mint fotókat egy archívumban tároljuk az ellenőrzést megelőzően.

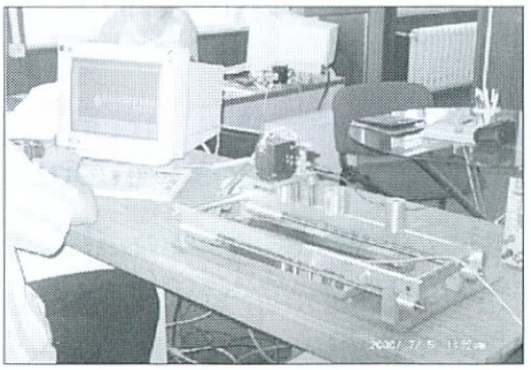
Amit meg kellett oldani:

- mintaarchívum kialakítása,
- a kamerákat tartó mechanika megtervezése,
- elektronikai fejlesztések a kamera automatizált működéséhez,
- szoftverfejlesztés az automatizált hibaellenőrzés megvalósítására, ami a kamera képét fogadó, a PC-ben lévő digitalizáló kártya programozását is jelenti.

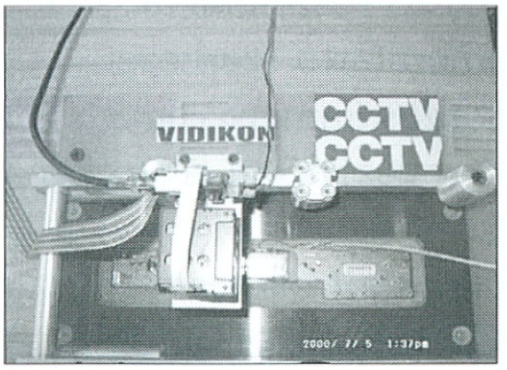
A kamerát vezérlő elektronika a következő feladatokat oldja meg:

Bekapcsoláskor a mikrovezérlőben tárolt algoritmus szerint automatikusan megvalósul a fókuszálás, és az optimális nagyítás is beállításra ke-

rül. A kijelző környezetében lévő háttér teljesen elsötétül, s az így kapott kép már alkalmas a képfeldolgozásra.



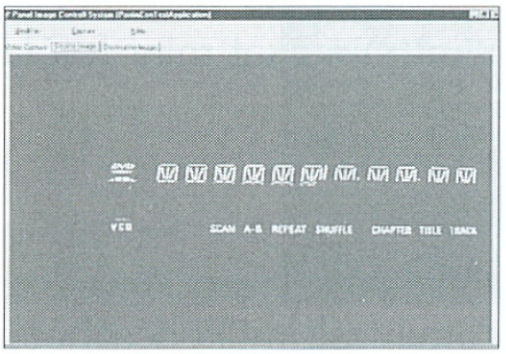
Az elkészült rendszer prototípusa



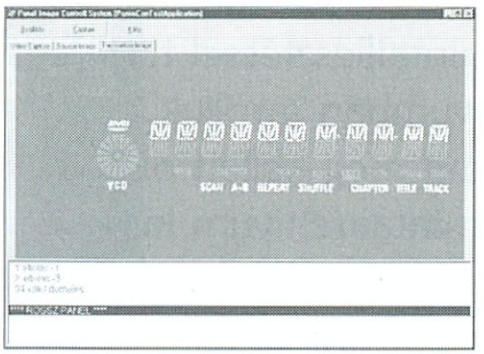
A kameratartó szerkezet és a DVD-panel

Üzemeltetési tapasztalatok

A szoftverfejlesztés során a mintaillesztés alapjául szolgáló etalonkép és a digitalizált kép illesztéséhez az X–Y irányú eltolásokat ki kellett küszöbölni. A program jelenleg +–8 pixel eltolást képes tolerálni és redukálni. A program akkor tekint hibásnak egy szegmenst, ha kevesebb mint 75%-a nem világít. A további fejlesztés során meg kellett valósítani azt is, hogy a forgatásból adódó hibákat szintén kiszűrje a program. Így a megbízhatóság jelenleg megközelíti a 100%-ot. A rendszer ipari tesztelése, beüzemelése megtörtént, és alkalmazást nyert a termelésben.



Hibás panel



Automatikusan felismert hibás szegmensek

Az adott módszerrel reményeink szerint nemcsak kijelzők, hanem egyéb elektronikai alkatrészek, mechanikák is vizsgálhatók és ellenőrizhetők lesznek. A feladat komplexitását növelheti az a tény, hogy háromdimenziós tárgyakat, felületeket kell majd vizsgálnunk. Ebben az esetben két lehetőség közül választhatunk.

A kamerapozíciókat úgy kell megválasztani, hogy csak a felület legjellemzőbb síkját lássuk, ekkor viszont egy tartószerkezeten több kamerát is kell rögzíteni a különböző alkatrészek megfigyelésére.

Ikerkamerákat kell alkalmazni sztereó felvételek készítéséhez, ebben az esetben különleges, háromdimenziós képfeldolgozásra lesz szükség, amivel a fotogrammetria tudománya foglalkozik.

Chipkártya a tömegközlekedésben

(A Bull Magyarország Kft. referenciáiból)

A tömegközlekedés világa

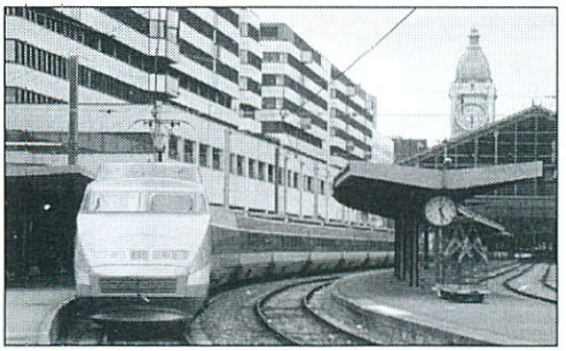
A tömegközlekedés világa jelentős fejlődésen megy keresztül. Napjainkban a tömegközlekedési szolgáltatások jövőbeni szereplőinek céljai az alábbi két feladat köré csoportosulnak:

- a mindennapi és a helyi közlekedés szervezése,
- a városok és régiók közötti utazóknak nyújtott szolgáltatások fejlesztése.

A különböző partnerek (busz, vonat stb.) között intermodalitás fejlesztésére irányuló szándék a közúti szállítással való versengés és a városközpontok helyzetének javítása céljából megvalósíthatónak tűnik, nemcsak az országos stratégiai tervezés, hanem a jelentős városi lakossággal rendelkező valamennyi ország szempontjából. Az ennek a témának szentelt kiállítások számának növekedése önmagában is elegendő lenne a fentiek igazolására.

Az intermodalitás fogalmát a személyszállítás tervezésénél figyelembe vett valamennyi közlekedési eszközt magában foglaló hálózat meghatározására és a háztól házig történő szállítás értelmében használjuk.

Például szolgáltatások koordinálása: autóparkoló + vonat + busz.



Az intermodalitás lehetőségei

A projektek a városrendezési és közlekedési szempontok egyeztetéséből születnek.

Jelenleg számos tájrendezési projekt van kialakulóban a városok körüli és a városokon belüli hálózatok, infrastruktúrák, valamint az átszállóhelyek fejlesztése céljából.

Már megvalósult hálózatok:

Valenciennes és az Észak-Pas-de-Calais projekt, Nancy, Lille és Vilaine, Chalons sur Saone, Strasbourg és Elzász.

Projektek:

Lyon, Marseille, Nizza, Cannes, Rennes, Bordeaux, la Rochelle, Montpellier és l'Herault, Strasbourg.

A fenti projektek meghatározása csak területi szempontok szerint történt, hiszen a potenciális utas a számára felkínált lehetőségek alapján választja ki az igénybe vett közlekedési eszközt. Ebből ered a viteldíjak, illetve a jegykiadó automaták jelentősége, másképpen fogalmazva az utasnak könnyítésként kínált, egyszerű tokban tartható egyetlen menetjegy lehetősége.

Fentiekből következik, hogy fejlesztési igénye miatt a közlekedési ágazat nagyon érdeklődik az intelligens kártyák iránt.

Milyen kártyát használjunk a közlekedésben?

A közlekedésben a jegyellenőrzésre és a jegykiadó automatákhoz tervezett kártyáknál az érintkezés nélküli technológiát alkalmazzák. Ebben az esetben kétféle módon lehet megvalósítani a közlekedés számára ajánlott megoldást:

- memóriával rendelkező kártyával,
- mikroprocesszoros kártyával.

Memóriával rendelkező kártyák

A memóriával rendelkező kártyákon lehet adatot tárolni (egyszerű memóriával rendelkezőkön 2 kB-nyit), de nem biztonságosak, használatuk pedig csak a közlekedésre korlátozódik. Legfőbb előnyük az olcsóságuk volt, ám a mikroprocesszoros kártyák árának jelentős csökkenését követően ez az előny megszűnt. A legleterjedtebb memóriával rendelkező kártyák a Mifare 1-es Philips-technológián alapulnak. A Bull nem szándékozik részt venni ezen a piacon.

Mikroprocesszoros kártyák

A mikroprocesszoros kártyák jelentős memóriakapacitással rendelkeznek, használatuk igen rugalmas, nagyon biztonságosak, és megfelelnek

az ISO szabvány előírásainak. Lehetőség van alkalmazásuk számának változtatására és felhasználási lehetőségeik bővítésére. Eddig legfőbb hátrányuk az árukban jelentkezett, amely jóval magasabb volt a többi kártyáénál. Az általuk kínált előnyök azonban igazolják a magasabb árat.

A Bull ajánlata a közlekedés számára 1998-ban

A Bull a CC Dou és újabban az ST Microelectronics technológiára alapuló TBHF1000 kártyákkal van jelen az érintkezés nélküli kártyák piacán.

TBHF1000

Mikroprocesszor:	Érintkezéses / érintkezés nélküli
Memória:	8 kB
Pénztárca:	Egyéni
Algoritmus:	DES
Szabvány:	ISO 7816

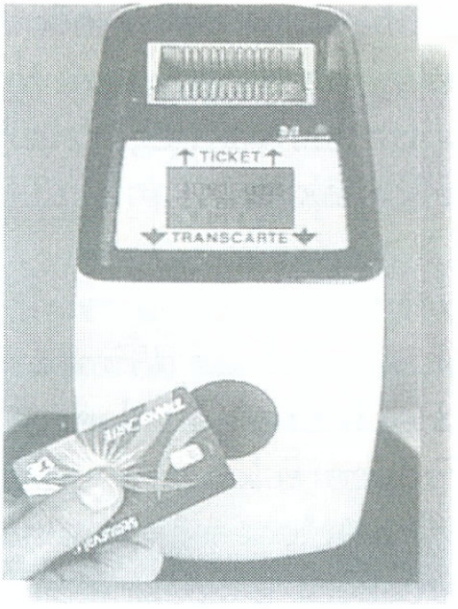
Ez a kártya számos alkalmazás tárolását teszi lehetővé, amelyhez a hozzáférés teljes mértékben paraméterezhető (szabad hozzáférés, olvasás- és/vagy írásvédelem). A fájlokhoz való hozzáférés az érintkezéses és az érintkezés nélküli részen keresztül is azonos biztonsági fokkal történik.

Az egyéni pénztárca csak előfizetési alkalmazásokhoz használható. A parancsok egyszerűek: betét, kivét, egyenlegközlés.

A biztonsági funkciók lehetővé teszik a kártyán lévő adatok kulcsokkal történő védelmét a leolvasás és/vagy írás ellen, a változtatható PIN kód kezelését, a bizonylati műveleteket stb. A DES algoritmus használatával szabványos, könnyen fejleszthető terméket kapunk.

A Semurval-projekt

A Semurval, a Valenciennes régió városi közlekedésirányítási vállalata 1997. december 1-jétől kezdte el használni az érintkezéses / érintkezés nélküli kártyát, a Transcarte-ot. Ez az első olyan kártya, amely a Bull operációs rendszerét tartalmazza, a Bull-kártyákra jellemzően nagyon biztonságos, és több funkcióra alkalmas mikroprocesszorát „érintkezés nélküli" kapacitások táplálják. Ez a bérletkártya feltölthető, így tehát a különböző egyéb kifizetésekre – közlekedésre vagy más szolgáltatásokra – szánt pénzt is lehet rajta tartani.



Ez a kártya kompatibilis az SNCF-fel, az Észak-Pas-de-Calais regionális hálózaton alkalmazott kártyával, amely a hagyományos érintkezéses chipkártyafunkcióval működik. Jelenlegi napi 100 000 buszjegy és napi 90 000 vidéki út árát fizetik ki ennek a kártyának a felhasználásával.

Az elkövetkező években a Transcarte egyre inkább el fog terjedni a fizető parkolókban, a megvalósításra kerülő valenciennes-i villamoson és bizonyos önkormányzati szolgáltatásoknál, mint pl. a közétkeztetésben, a könyvtárakban vagy az uszodákban.

Napjainkban világszerte a közlekedési ágazat jelenti az egyik legígéretesebb fejlesztési lehetőséget a mikroprocesszoros kártyák területén. Becslések szerint 2000-ben ez a piac több mint három és fél milliárd francia frankos bevételt jelenthet.

A Bull ajánlata 1999-ben

Az Uniprox leolvasó

A Bull bejelenti a piac első univerzális, technológiától független kártyaleolvasóját. A kártyák ellenőrzésére kifejlesztett Uniprox – közlekedés, épületek, nyilvános helyek, védett területek stb. – le tud olvasni minden érintkezés nélküli, akár más cégek által fejlesztett kártyát.

A piacon jelenleg található egyik legnagyobb teljesítményű RISC processzorral ellátott Uniprox néhány ezredmásodperc alatt az adatütköztetés kockázata nélkül felismeri és azonosítja a kártyát.

Az Uniprox bővíthető leolvasó, amely módosítás nélkül képes bármilyen új technológián alapuló, ma még ki sem fejlesztett kártyát elfogadni, az egyetlen feltétel, hogy a kártya megfeleljen az ISO szabványoknak (jelen esetben az ISO 14443-nak).

A Modeus-projekt

A Modeus céget bankok – a Caisses d'Empargne, a La Poste, a Société Générale, a Banques Populaires –, valamint közlekedési vállalatok – az RATP, az SNCF és a France Telecom – hozták létre. A projekt célja, hogy egyetlen intelligens kártyát lehessen használni menetjegyként (jegykiadó automaták), pénztárcaként (fizetési eszköz) és hozzáadott értékű szolgáltatások igénybevételére. Ugyanazzal a kártyával nemcsak a tömegközlekedési eszközökre lehet felszállni, hanem be lehet vásárolni, lehet telefonálni, valamint igénybe venni a város által nyújtott szolgáltatásokat, s törzsutasprogramokban részt venni.

Az érintkezés nélküli technológiának köszönhetően a Modeus kártya a leolvasótól néhány centiméterre tartva érvényesíthető, javítva ezzel a közlekedési feltételeket.

A Bull az ASK céggel közösen olyan elektronikus pénztárcát fejlesztett ki, amely megfelel a Banque de France biztonsági követelményeinek.

A Bull ajánlata 2000-ben

A TBHF1000 technológia fejlesztése a legújabb szabványok alapján történik, kriptoprocesszoros új egységek köré, amelyek felgyorsítják a DES-műveleteket.

Az elektronikus pénztárca, amelynek típusait a GIE Cartes Bancairesnek kell jóváhagynia, kiegészíti a közlekedésben és a városi szolgáltatásoknál használt alkalmazásokat.

Az új kártya kompatibilis lesz az 1999-ben meghatározásra kerülő 14443-1234 szabványokkal, valamint az ENV1545 közlekedési szabvánnyal.

Ily módon a kártya kielégíti a közlekedési eszközök üzemeltetőinek, a helyi és regionális önkormányzatok vezetőinek elvárásait, s meghódítja a mindennapi életet megkönnyítő, kevesebb időt igénylő megoldások elfogadására mindig kész kártyahasználókat.

A mikroprocesszor alapú kártyák előnyei

A közlekedési program számára a mikroprocesszoros kártyák számos döntő előnyt kínálnak. Vezérlőeszköz statisztikák összeállításához: értékesítés, forgalom, terméktípusok (bérletek, jegyek, gyűjtőjegyek, átalánydíjak stb.).

A menetjegy számítógépes leolvasásával történő hálózatirányítás statisztikák felállítását, valamint a közlekedési eszközöknek a forgalom nagyságához igazított közlekedtetését teszi lehetővé.

Ezenkívül ezek az adatok fontosak a beruházások irányításához, valamint a bevételeknek a multimodális láncba belépő, különböző szolgáltatócégek közötti elosztásához.

A távolról leolvasható TBHF1000 kártyával növelni lehet a jegyellenőrző automaták élettartamát. Az automaták nem függnek a leolvasó fejektől, amelyek a súrlódás miatt elkopnak. Ez pénzmegtakarítást jelent az üzemeltetőnek, mivel leolvasó fejekre nem kell költenie.

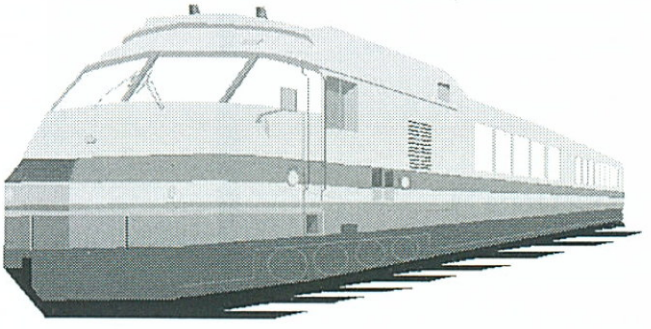
A kártya javítja a hamisítás elleni küzdelem esélyeit. Az első tapasztalatok alapján a hamisítások a felére csökkentek.

A kártya által kínált rugalmasságnak köszönhetően nagyon egyszerűen lehet paraméterezni vagy fejleszteni a közlekedési programot.

A kártya a törzsutasprogramokban való részvételt is lehetővé teszi.

Mivel a kártyán adatokat lehet tárolni, ezért a menetjegy megvételével egy időben pontokat lehet jóváírni az utasoknak, ami marketingszempontból jelentős előny a soros megoldásokhoz képest. Ezáltal az utasok elégedettebbek, és többen csatlakoznak a jegykiadó automaták programjához.

A felhasználók számára előny továbbá, hogy az intelligens kártyával gyorsabban kiérnek a vágányokhoz. Az „érintkezés nélküli" technológiának köszönhetően nincs szükség arra, hogy a jegyet behelyezzék a gépbe, ezáltal az utasok gyorsabban áthaladnak a jegykezelő pontokon.



A kártyával könnyebbé válik a menetjegyek megvétele.

A chipes kártya „érintkezéses" részét fel lehet tölteni a pénzkiadó automatáknál. Elektronikus pénztárcaként használható, a felhasználó tehát eldöntheti, hogy a kártyájával egy automatából, a pénztárnál vagy bizományosnál veszi-e meg a menetjegyét.

Az utas nyugodt, hiszen teljes biztonságban utazhat. A kártyája személyre szóló. Lopás vagy elvesztés esetén letilthatja, míg a név nélküli havijegy ellopása vagy elvesztése esetén semmit sem tehet.

PÉNZJEGYNYOMDA RÉSZVÉNYTÁRSASÁG

Távközlési kártyák (csipes és csip nélküli kártyák) • bankkártyák (MasterCard/VISA gyártási jogosultság) • kereskedelmi, törzsvásárlói kártyák csippel vagy anélkül • egészségügyi kártyák • közlekedési kártyák • csip nélküli I.D. okiratkártyák • csipes I.D. és e-aláíró kártyák • grafikai tervezés • kártyás alkalmazások, fejlesztések • megszemélyesítés

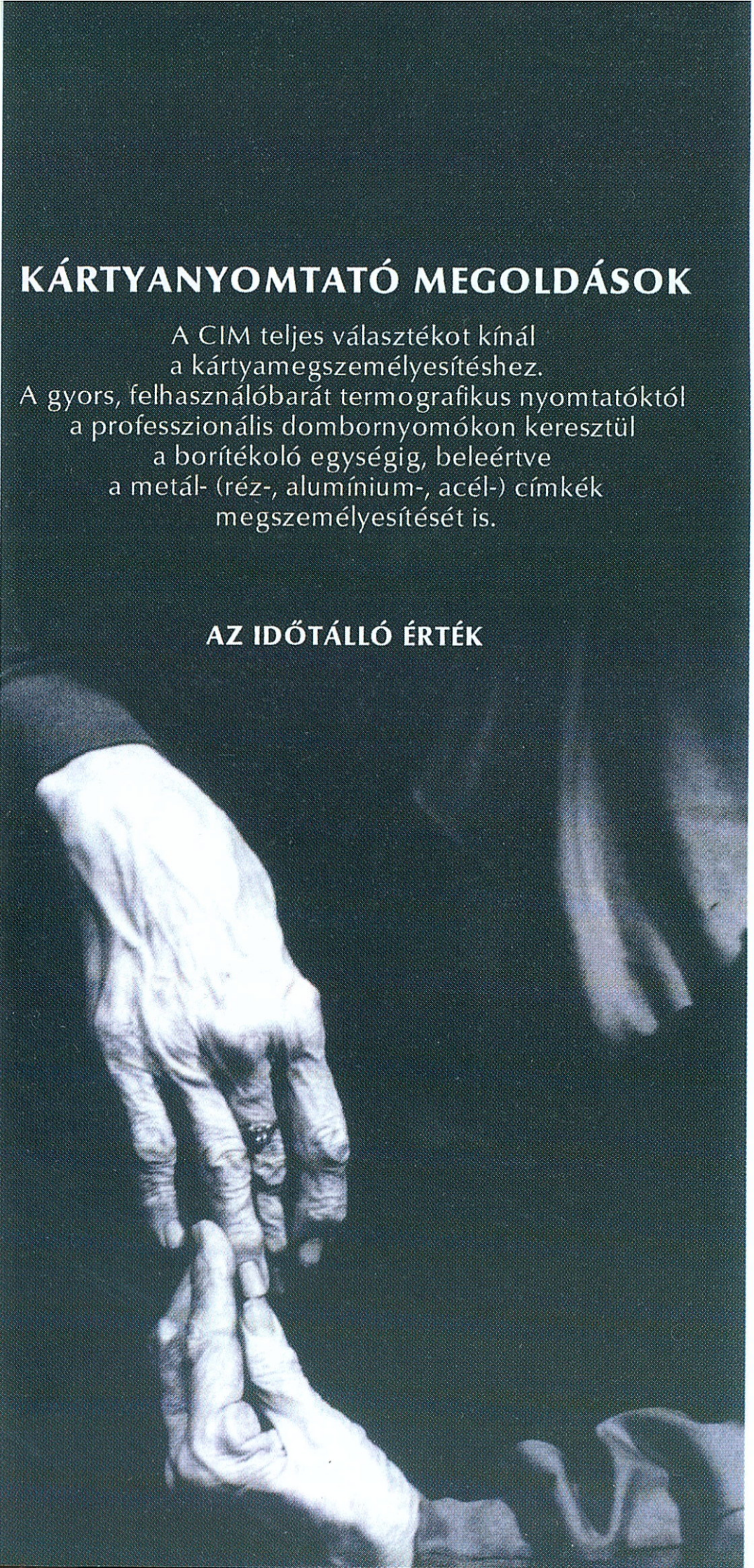
Gazdag hagyományok, biztonságos gyártási körülmények, teljes körű hamisítás elleni védelem.

Pénzjegynyomda Rt. • Kártya Üzletág • 1055 Budapest, Markó u. 13–17.
Telefon: (36-1) 269-2173, 269-5272 • Telefon/fax: (36-1) 332-0593
e-mail: mails@penzjegynyomda.hu

KÁRTYANYOMTATÓ MEGOLDÁSOK

A CIM teljes választékot kínál
a kártyamegszemélyesítéshez.
A gyors, felhasználóbarát termografikus nyomtatóktól
a professzionális dombornyomókon keresztül
a borítékoló egységig, beleértve
a metál- (réz-, alumínium-, acél-) címkék
megszemélyesítését is.

AZ IDŐTÁLLÓ ÉRTÉK



Hadsereg, motorgyár, logisztikai vállalatok, liftgyár, acélipar, autóipar

Kártyamegszemélyesítők
Klubkártyák
Hotelek
Bankok
Intézmények
Kaszinók
Gyorséttermek

CIM S.p.A. - Via O. Serra 2,
40012 Calderara di Reno BO, Italy
Tel.: +39 051.64.65.011
Fax: +39 051.64.65.012
info@cimitaly.it
www.cimitaly.it

CIM
THE PERSONALITY WRITER

A sikeres e-businesshez integrált szoftver-megoldás alkalmazása vezet.

	Oracle E-business Suite
Adatbázis-kezelés	✓
Marketing	✓
Értékesítés	✓
Támogatás	✓
Webáruházak	✓
Stratégiai beszerzés	✓
Termelésirányítás	✓
Ellátási lánc menedzsment	✓
Pénzügyi menedzsment	✓
Emberi erőforrás	✓

Egy teljes körű, integrált megoldás az Oracle-től,
vagy részmegoldások sokasága számos szállítótól.
A választás az Öné.

ORACLE®
SOFTWARE POWERS THE INTERNET™

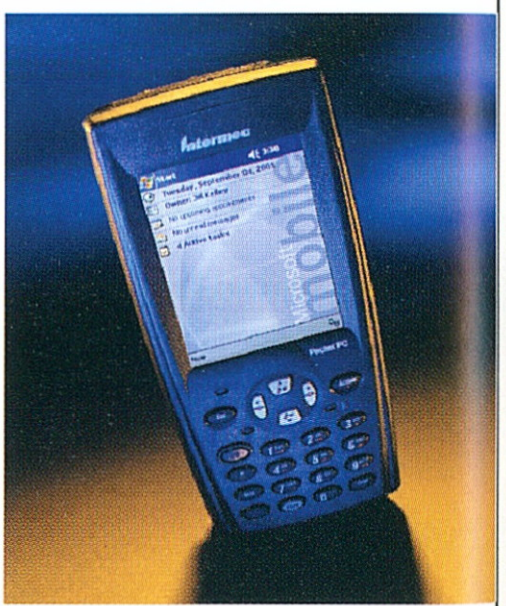
www.oracle.com/hu

MINŐSÉG A VONALKÓDTECHNIKÁBAN

A VIDEOTON Informatika Kft. ISO 9001 szerinti minőségbiztosítási rendszerrel, az INTERMEC Corp. magyarországi disztribútoraként világszínvonalú rendszerekkel, eszközökkel, kellékanyagokkal és szaktanácsadással áll a vonalkódtechnika alkalmazóinak rendelkezésére.

Intermec

- Vonalkód hálózatok
- RF hálózatok
- Vonalkódnyomtatók
- Olvasó eszközök
- Hordozható adatgyűjtők
- Szoftverek
- Kellékanyagok
- Beléptető, munkaidő-nyilvántartó rendszerek
- Kapcsolat integrált vállalat-irányítási sw-ekkel (SAP, MFG-PRO, SYMIX, PROMIX)



ISO 9001

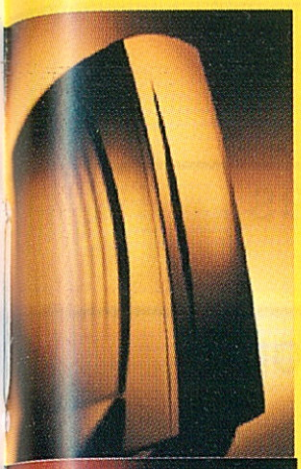
Deutscher Akkreditierungs Rat DAR

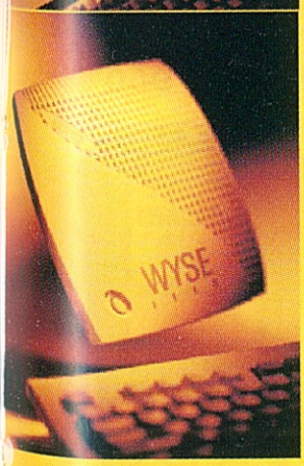
VIDEOTON INFORMATIKA

H-8002 Székesfehérvár, Berényi út 100.
Levélcím: 8002 Pf.:314 • E-mail: vonalkod@inform.videoton.hu
Telefon.: (22) 533-737 • Fax: (22) 533-739

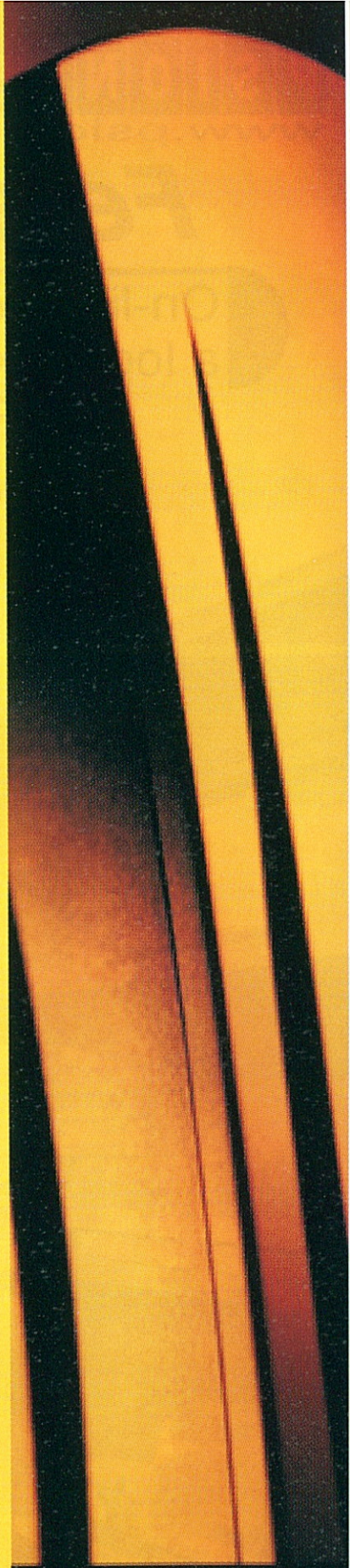
WYSE

Smarter. Easier. Thinner.
Innovative Thin Clients from Wyse.





A vékonykliens



Wyse®
Winterm

www.wyse.hu
www.wyse.com

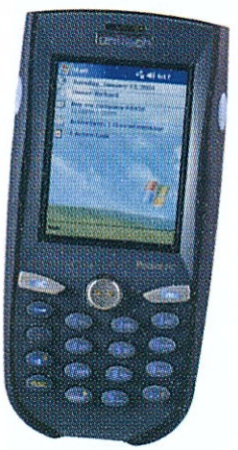
WYSE

PSION TEKLOGIX
www.psionteklogix.hu

Psion Rendszerház Kft.
1111 Budapest
Szt. Gellért tér 3.

Feladatra méretezve

- On-line adatforgalom a logisztikai folyamatokban
- Vezeték nélküli kommunikáció (WiFi, RF narrow-band, GPRS)
- Automatikus azonosítás (vonalkód, RFID)
- Költséghatékony megoldások



unitech
PA 950/960

PSION TEKLOGIX
WORKABOUT PRO

Minden, ami azonosítás...
Minden, ami adatgyűjtés...

Amit kínálunk:

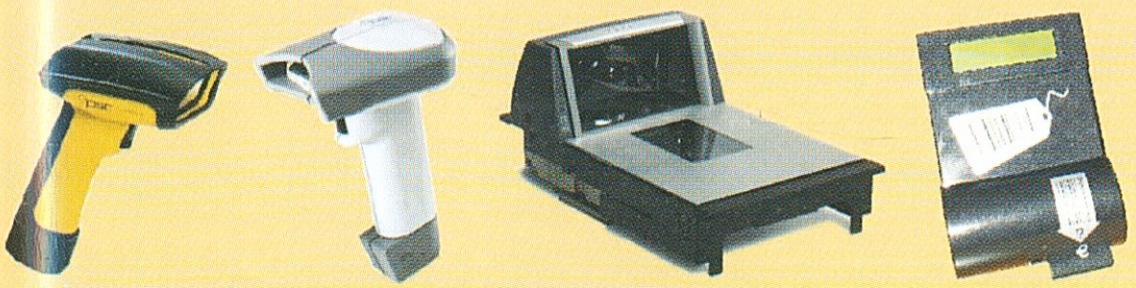
Vonalkódtechnikai eszközök forgalmazása
- kézi adatgyűjtők, adatgyűjtő szoftverek
- vezeték nélküli hálózati eszközök
- vonalkódolvasók
- etikett nyomtatók, nyomtató szoftverek
- öntapadós etikettek, kartonok és festékszalagok

Automatikus azonosítást alkalmazó rendszerek fejlesztése és telepítése
- raktári mozgások irányítása és követése
- ipari minőségbiztosításhoz termeléskövető rendszerek
- tárgyi eszköz leltár felvétel és nyilvántartás

Korszerű azonosítási technikák alkalmazása
- hang- és ujjlenyomat azonosítás
- RFID rádiós azonosító technikák

Szervizszolgáltatások
- komplett adatgyűjtő rendszerek karbantartása
- berendezések javítása, alkatrész-árusítás
- Intermec garanciális szervizközpont

Etikettszolgáltatások
- öntapadós, papír és műanyag alapú etikettek tervezése és kivitelezése
- nagy ragasztóanyag-, szín- és méretválaszték



Az INTERMEC kiemelt kereskedelmi és szervizpartnereként, garanciális szervizközpontként várjuk Önt!

A budapesti központ ISO 9001:2000 szabvány szerint működik.

VONALKÓD RENDSZERHÁZ VRH

Budapesti irodánk új címe:
1143 Budapest
Hungária körút 64.
Telefon: (1) 436 7575
E-mail: info@vonalkod.hu

Kirendeltségeink:
Debrecen, Cegléd u. 11.
Tel.: (52) 452 142
Szombathely, Selyemrét u. 5.
Tel.: (94) 510 657

VONALKÓD RENDSZERHÁZ

VONALKÓD VRH RENDSZERHÁZ

... minden, ami azonosítás!

www.vonalkod.hu

Intermec GLOBAL SERVICES PARTNER

Intermec

psc

ISO 9001 SGS Cert. Nr.: 90134-2