

Gianni Becattini

Raccolta delle dispense sui Sistemi di Bigliettazione Elettronica

- ***I Titoli Di Viaggio Elettronici***
- ***I Sistemi di Bordo***
- ***Tecniche e sistemi di comunicazione***



Titolo documento

File

Pagina/di

COVER

Gianni Becattini

Appunti sulla Bigliettazione Elettronica

I Titoli Di Viaggio Elettronici



AEP Advanced Engineering Projects s.r.l.
Via dei Colli, 240 - Signa (Firenze) - Italia
<http://www.aep-italia.it>



Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	1 / 39

1 Sommario

1	Sommario.....	2
2	Presentazione	4
3	Titoli Di Viaggio Tradizionali	5
3.1	Biglietti cartacei	5
4	Titoli Di Viaggio Elettronici.....	6
4.1	Generalità.....	6
4.2	Apparati di convalida	6
4.3	Sistemi di Bigliettazione Elettronica.....	6
5	Alcuni concetti.....	7
5.1	Il contratto di trasporto.....	7
5.2	Tariffazione flessibile.....	7
5.3	Configurazione.....	8
5.4	I profili	8
5.5	Qualche esempio	9
6	Biglietti con banda magnetica.....	11
6.1	Generalità.....	11
6.2	Principio di funzionamento.....	11
6.3	Standard di riferimento	11
6.4	Stampa di convalida	11
6.5	Vantaggi.....	12
6.6	Limitazioni	12
6.7	Sicurezza	12
6.8	Diffusione.....	12
7	Smart card.....	15
7.1	Carte senza chip	15
7.2	Le smart card.....	15
7.3	Vantaggi delle smart card.....	16
7.4	Classificazione	17
7.4.1	Smart card a memoria	17
7.4.2	Smart card a microprocessore.....	18
7.4.3	Classificazione per interfaccia	19
7.5	Le carte contact	20
7.6	Le carte contactless	21
7.7	Tipi complessi	22
7.8	Il supporto fisico	23
7.9	Sistemi a microprocessore.....	24
8	Gli standard per le smart card.....	25
8.1	Generalità.....	25
8.2	ISO 7816	25
8.3	ISO 14443	25
8.3.1	ISO 14443A e MIFARE	26
8.3.2	ISO 14443B	27
8.3.3	ISO 15693.....	28
8.3.4	ENV 1545	28

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	2/39

8.4	Calypso.....	29
8.5	Struttura dati di alcune carte	31
8.5.1	Carta MIFARE Classic	31
8.5.2	Carta GTML	31
9	Sicurezza e chiavi	35
9.1	Crittografia	35
9.2	I moduli SAM	36
9.3	Uso dei SAM come custodia per le chiavi	37
9.4	Altri impieghi dei moduli SAM	38
9.5	Chiavi differenziate	38
9.6	Titolarità degli elementi di sicurezza	39

2 Presentazione

Questa dispensa è stata originariamente presentata dall'autore all'Executive Master "SVILUPPO E GESTIONE DEI SISTEMI DI BIGLIETTAZIONE ELETTRONICA E DI PAGAMENTO DEI SERVIZI DI MOBILITÀ" organizzato da Clickutility e tenuto a Bologna dal settembre a dicembre 2007, con la collaborazione scientifica e il patrocinio di Club Italia ed il patrocinio dell'ANAV.

Essa appartiene ad una serie di tre volumetti orientati alla descrizione delle tecnologie di bordo:

- dispensa 1 - "Titoli Di Viaggio Elettronici (TDVE)" - descrive sommariamente i vari tipi di TDVE in un'ottica di funzionalità e di utilizzo con annotazioni anche di carattere commerciale;
- dispensa 2 - "Il Sistema Di Bordo (SDB)" - descrive principalmente le caratteristiche tecniche e di funzionamento dei terminali per l'utilizzo dei TDVE e di quelle parti accessorie che, installate a bordo del bus, costituiscono nel complesso il cosiddetto Sistema Di Bordo. In parallelo alla descrizione dei terminali vengono fornite informazioni più approfondite sui principi di funzionamento dei TDVE.
- dispensa 3 - "Tecniche e Sistemi di Comunicazione (COM)" - vengono descritte le principali tecniche di comunicazione usate all'interno ed all'esterno degli apparati di bordo, nonché i sistemi di terra che consentono lo scambio di dati con gli autobus.

Eventuali riferimenti al numero della dispensa sono via via riportati entro parentesi quadre (es. [1])

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	4/39

3 Titoli Di Viaggio Tradizionali

3.1 Biglietti cartacei

In Italia, il metodo ancora più usato per il pagamento dei servizi di mobilità urbani ed extraurbani rimane quello del classico biglietto cartaceo da obliterare in vettura o in stazione.



Questo sistema, assieme a qualche pregio, presenta vari inconvenienti:

- è poco pratico per l'utenza, poiché non sempre i punti di rivendita sono accessibili nel momento della necessità dell'acquisto;
- la distribuzione dei titoli di viaggio è problematica per l'elevato numero di biglietti diversi necessari o, in alternativa, per dover dotare le rivendite di macchine emettitrici da banco;
- non consente una flessibile politica tariffaria;
- non permette di "conoscere" facilmente l'utente né le sue abitudini;
- rende difficoltosa la condivisione del servizio su tratte comuni ad opera di diverse compagnie di trasporto e limita accordi che favorirebbero la fruibilità del servizio;
- è facilmente duplicabile in maniera abusiva, in seguito anche alla diffusione di scanner e di stampanti a colori di elevata qualità.

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	5/39

4 Titoli Di Viaggio Elettronici

4.1 Generalità

Per i motivi in precedenza indicati è oggi orientamento comune il ricorrere a Titoli Di Viaggio Elettronici (TDVE), che, oltre a non presentare gli inconvenienti sopra accennati, offrono molti vantaggi. L'epiteto "elettronici" non implica tanto una caratteristica intrinseca del titolo stesso quanto la possibilità di processare il medesimo attraverso apparati elettronici.

I TDVE più comuni sono i seguenti:

- i biglietti con banda magnetica;
- le *smart card* (ossia "carte intelligenti"), dette anche *carte chip* in quanto hanno un circuito integrato ("chip") a bordo o, ancora, *carte a microprocessore*.

Nei paragrafi successivi esamineremo più nel dettaglio queste due soluzioni.

4.2 Apparati di convalida

A seguito della introduzione dei TDVE anche gli apparati di convalida si sono evoluti ed hanno modificato il proprio nome. Oggi si parla di solito di

- **obliteratrici** - vecchi terminali per titoli di viaggio tradizionali;
- **validatrici** - nuovi terminali intelligenti per smart card e biglietti con banda magnetica;

anche se in pratica i due termini sono spesso usati indifferentemente.

4.3 Sistemi di Bigliettazione Elettronica

L'utilizzo dei titoli elettronici presuppone la predisposizione di un sistema articolato (Sistema di Bigliettazione Elettronica) che interessa tanto l'azienda quanto la rete di distribuzione e le stesse vetture adibite al servizio.

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	6/39

5 Alcuni concetti

5.1 Il contratto di trasporto

Il contratto di trasporto trova la sua definizione all'interno del codice civile all'art. 1678, in base al quale "il vettore si obbliga, verso corrispettivo, a trasferire persone o cose da un luogo ad un altro" e, nel frattempo, a custodirle. Il trasporto di persone si caratterizza per l'esistenza di un obbligo a carico del vettore che è quello di trasferire la persona ("passeggero") da un luogo ad un altro che per parte sua è vincolato alla effettuazione di un pagamento in denaro in cambio del servizio ricevuto.

Nel caso di un Sistemi di Bigliettazione Elettronica, i **contratti di servizio** sono le definizioni delle modalità di accesso al servizio stesso. Ad esempio la "carta valore per abbonati" oppure la "carta valore ordinaria".

5.2 Tariffazione flessibile

L'introduzione del Sistemi di Bigliettazione Elettronica permette di creare sistemi tariffari basati su logiche impossibili da implementare con la bigliettazione tradizionale. Si possono stabilire delle specifiche funzionali legate a nuove politiche di marketing o tra più compagnie.

Ad esempio, è possibile variare dinamicamente nella giornata le tariffe per incentivare l'uso del mezzo pubblico negli orari in cui gli autobus viaggiano con un modesto numero di passeggeri a bordo. Questo implica:

- che il passeggero abbia stipulato un opportuno contratto di trasporto, ossia, nel caso specifico, che sia munito di una carta a valore; la carta a valore, per sua natura deve essere di un tipo che risulti leggibile e riscrivibile a bordo;
- che i terminali a bordo siano in grado di leggere e scrivere le carte stesse e che conoscano l'ora del giorno e le tariffe da applicare in conseguenza;
- che sia previsto un qualche mezzo di trasmissione dati per informare i terminali a bordo di eventuali cambiamenti tariffari.

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	7/39

Estendendo l'esempio, potrebbe risultare auspicabile che una condizione di particolare favore dovesse essere aggiunta per i giorni festivi, magari in orari differenti.

5.3 Configurazione

Nel caso reale sono previsti normalmente vari tipi di contratti, diverse logiche tariffarie e/o la partecipazione di più operatori; diventa quindi indispensabile adeguare il funzionamento del Sistemi di Bigliettazione Elettronica ad una grande quantità di parametri. Ciò può essere ottenuto in due maniere diverse:

- scrivendo opportuni programmi applicativi per gli apparati componenti il SBE;
- utilizzando programmi applicativi parametrizzati che possano recepire le configurazioni funzionali prestabilite dalla Compagnia.

Si realizza così un sistema il cui comportamento molto flessibile e plasmabile in funzione delle necessità.

Questa flessibilità consente di introdurre logiche operative nuove, come ad esempio quella detta "check-in/check-out", di cui si parlerà nel seguito, impensabili con i modelli di bigliettazione tradizionale; altre ancora potranno essere introdotte in futuro sulla base delle esperienze fatte e della fantasia degli operatori.

5.4 I profili

In parallelo alla definizione dei contratti di trasporto e delle tariffe, è possibile anche tenere conto delle esigenze di particolari categorie di utenti, ancora una volta processabili con relativa facilità, malgrado la possibile complessità, grazie al Sistema di Bigliettazione Elettronica. I **profili** degli utenti possono essere quanto mai variegati e molteplici. E' ipotizzabile, ad esempio, che un singolo soggetto sia al tempo stesso studente, beneficiando quindi di alcune riduzioni orarie, e socio della squadra sportiva locale, con diritto di viaggiare gratuitamente in occasione di manifestazioni sportive. Sarà compito del SBE applicare correttamente le varie facilitazioni nelle varie circostanze.

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	8/39

Uno stesso TDVE può contenere una molteplicità contratti di trasporto e di profili utente e gestire correttamente, quando e come opportuno, le possibili relative combinazioni.

Questa flessibilità lascia pensare che sia possibile eliminare o ridurre significativamente l'impiego dei biglietti di corsa singola, potendo essere offerto a ciascun viaggiatore un prodotto tariffario personalizzato estremamente conveniente.

5.5 Qualche esempio

Si riporta qualche spunto sull'impiego di TDVE:

- **sconti dinamici** (ora del giorno, quantità, incentivazioni complesse ecc.);
- **sovrapprezzi dinamici** (servizi speciali, festivi, ore di punta ecc.);
- **abbonamenti** (settimanali, mensili, trimestrali, annuali ecc.), anche con tratta preferenziale;
- **carnet multicorsa;**
- **carnet del turista;**
- **carte a valore** - la carta contiene un valore, simile a denaro, che il cliente può spendere in varie maniere a bordo del bus, ad esempio per acquistare un biglietto singolo o rinnovare un abbonamento. La carta può essere ricaricata presso biglietterie, rivendite o macchine automatiche;
- **origine / destinazione** - il bus è dotato di opportuni sistemi per l'individuazione della fermata di salita. L'utente seleziona attraverso la tastiera della validatrice la località/zona di destinazione o la distanza, quando diversa dalla destinazione preferenziale prestabilita e registrata nella carta.
- **check-in/check-out** - L'utente deve convalidare sia all'entrata che all'uscita. Si paga esattamente in proporzione al servizio di cui fruisce ("pay per use"). Fornisce indicazioni molto precise sul flusso dei passeggeri.

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	9/39

Courtesy by AEP Ticketing Solutions

[Check-in/check-out]



6 Biglietti con banda magnetica

6.1 Generalità

I Titoli Di Viaggio Magnetici sono largamente usati e presentano una serie di vantaggi non trascurabili. Ritenuti superati fino a qualche anno addietro, sono oggi rivalutati come ideale complemento della tecnologia contactless.

6.2 Principio di funzionamento

Il loro principio di funzionamento è molto semplice. Su uno dei due lati viene applicata una "banda" magnetica, ossia qualcosa di molto simile ad un pezzetto di nastro magnetico, su cui è possibile registrare dati e rileggerli, in modo concettualmente molto simile a quello della registrazione audio. Ulteriori spiegazioni sono fornite in [1].

6.3 Standard di riferimento

I biglietti magnetici sono realizzati, nella maggior parte dei casi, in accordo allo standard ENV-753, con banda magnetica laterale o centrale. Questa ultima consente, per evidenti motivi di simmetria, l'introduzione del biglietto in due versi anche con una sola testina magnetica.

6.4 Stampa di convalida

I biglietti magnetici vengono di solito stampigliati in fase di validazione e la verifica può avvenire a vista; non sono richiesti apparati speciali per il personale di controllo e anche l'utente può facilmente verificarne il progressivo utilizzo.

Nella figura: un biglietto magnetico con stampa di convalida. Ben visibile la stripe centrale.



Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	11/39

6.5 Vantaggi

I loro vantaggi principali sono costituiti dal fatto che, ad un costo molto basso (0,01÷0,02€), offrono la possibilità di essere letti e scritti e quindi di implementare contratti di trasporto complessi. Possono inoltre essere tracciati e quindi permettono di raccogliere di una grande quantità di informazioni sul loro utilizzo.

Allo stato attuale dello sviluppo tecnologico, nessuna smart card offre la possibilità di realizzare biglietti di corsa singola o carnet multicorsa ad un costo così basso come quello del biglietto magnetico.

6.6 Limitazioni

Le limitazioni sono:

- **il numero di informazioni registrabili** - circa 25/50 byte contro le centinaia o le migliaia delle smart card;
- **il maggiore costo dei terminali** - per la maggiore complessità meccanica;
- **la minore praticità di impiego** - una smart card può essere validata anche senza estrarla dal portafogli o dalla borsetta.

6.7 Sicurezza

La sicurezza, grazie alla banda magnetica, ad una grafica adeguata e con il controllo a vista da parte degli ispettori, raggiunge livelli accettabili nella maggiore parte delle situazioni, anche se molto distanti da quelli conseguibili con le smart card.

6.8 Diffusione

Il rapporto costo/prestazioni resta tuttavia molto favorevole e tale da avere indotto numerose operatori del trasporto ad utilizzarli in parallelo alle carte elettroniche. Si citano ad esempio:

- **AIM** (Vicenza) - Maggiori informazioni su <http://www.aimvicenza.it/>
- **ACTT** (Treviso) - biglietti magnetici in formato ISO. Singoli, multipli, giornalieri, week-end e cumulativi. Maggiori informazioni su <http://www.actt.it> .

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	12/39

- **APM e Minimetrò** (Perugia) - biglietti magnetici in formato ISO con banda centrale. Moltissimi tipi di biglietti e abbonamenti urbani ed extraurbani. Maggiori informazioni su <http://www.apmperugia.it>.
- **ATAC** (Roma) - BIT Biglietto Integrato a Tempo (75 minuti), 5BIT MULTIBIT (5 x 75 minuti), BTI Biglietto Turistico Integrato (vale fino ore 24.00 del terzo giorno compreso quello della timbratura e per un numero illimitato di viaggi nel comune di Roma), BIG Biglietto Integrato Giornaliero, CIS Carta Integrata Settimanale (Per 7 giorni dalla data indicata dal cliente e per un numero illimitato di viaggi). Maggiori informazioni su <http://www.atac.roma.it>.
- **ATAM** (Arezzo) - maggiori informazioni su <http://www.atamarezzo.it/>.
- **ATC** (Terni) - biglietti magnetici in formato ISO con banda laterale. Biglietti e abbonamenti urbani ed extraurbani. Maggiori informazioni su <http://www.atcterni.it>.
- **ATCM** (Modena) - maggiori informazioni su <http://www.atcm.mo.it>.
- **ATM** (Milano) - il sistema di bigliettazione della capitale industriale d'Italia è uno dei più vasti ed articolati. Su biglietto magnetico, in formato ISO con banda laterale, prevede, in ambito urbano, oltre al classico biglietto ordinario singolo e al carnet da 10 viaggi, anche titoli innovativi quali il settimanale 2x6 e vari tipi di abbonamento (serale, giornaliero e bigiornaliero). Sono poi previsti un grande numero di titoli a validità extraurbana per le varie zone tariffarie in cui è divisa la metropoli ed il relativo hinterland. Maggiori informazioni su <http://www.atm-mi.it>.
- **Brescia Mobilità** (Brescia) - biglietti magnetici in formato ISO con banda laterale. Sono implementati titoli a tempo, carnet da 10 corse ed abbonamenti settimanali. Per maggiori informazioni www.bresciamobilita.it.
- **CTM** (Cagliari) - biglietti magnetici in formato ISO. Sono implementati titoli a tempo, carnet da 12 corse ed abbonamenti giornalieri. Per maggiori informazioni su <http://www.ctmcagliari.it>.
- **FTV** (Vicenza) - nuovo sistema in fase di implementazione basato anche su biglietti magnetici in formato ISO con banda centrale. Maggiori informazioni su <http://www.ftv.vi.it>.
- **GTT** (Torino) - biglietti magnetici in formato proprietario con banda laterale. Sono implementati biglietti ordinari, carnet da 15 corse, ab-

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	13/39

bonamento giornaliero, "Viaggiare insieme" per più persone, e "Shopping".

Per maggiori informazioni <http://www.comune.torino.it/gtt>.

- **Regione Sardegna** - ha bandito una gara per un Sistema di Bigliettazione Elettronica prevedendo biglietti magnetici e carte contactless.
- **Unico Campania** - ultimo in ordine alfabetico ma certo primo per importanza il sistema tariffario della regione Campania fa uso estensivo di titoli di viaggio su supporto magnetico ISO con banda centrale. Il sito <http://www.unicocampania.it> consente di scaricare il regolamento tariffario con tutte le informazioni relative.

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	14/39

7 Smart card

7.1 Carte senza chip

L'uso di carte in plastica per il riconoscimento e per transazioni finanziarie è iniziato negli anni '50, ma solo in seguito si è addivenuti ad un loro uso massiccio, nella forma delle cosiddette "carte di credito", universalmente diffuse.

La classica carta di credito "solo plastica" (ossia senza chip), tuttora in uso in Italia, ha il principale scopo di associare un numero al nome dell'intestatario; la banda magnetica contiene gli stessi dati riportati in rilievo, in forma leggibile con un apposito lettore.

Il livello di sicurezza delle carte di credito "solo plastica" è molto basso. Chiunque ne venga in possesso può utilizzarla; la richiesta del documento di identificazione è piuttosto rara. L'uso attraverso Internet risulta ancora più facile e l'impiego abusivo del titolo può continuare liberamente fino a che il proprietario legittimo non si accorga della perdita di possesso e non provveda ad bloccarlo.

La transazione basata sulla carta di credito avviene di regola previo collegamento dell'apposito apparato (POS) al centro servizi, sia per verificare che la carta non risulti bloccata che per assicurarsi dell'esistenza del credito (transazione "on line").

E' quindi evidente che la carta di credito presenta due gravi limitazioni:

- ha un livello di sicurezza pressoché nullo;
- richiede una connessione telefonica per l'esecuzione della transazione.

7.2 Le smart card

Ad entrambi questi inconvenienti pongono rimedio le "smart card", apparentemente simili a quelle "tutta plastica" ma con l'aggiunta di un circuito elettronico integrato ("chip") che può comunicare con gli appositi terminali tramite un connettore o, in alternativa alla connessione elettrica, tramite onde radio, come sarà meglio descritto nel seguito e nel modulo [2].

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	15/39



Una smart card reale

Nella memoria del chip possono essere registrate numerose informazioni, come i dati anagrafici e personali del proprietario, importi di credito, validità, agevolazioni, abbonamenti ecc.

Per il trasporto pubblico, le smart card rappresentano una evoluzione dei biglietti con banda magnetica.

7.3 Vantaggi delle smart card

Le smart card offrono molti vantaggi rispetto al biglietto magnetico, tra cui:

- **maggiore sicurezza** - le smart card offrono una sicurezza elevata, essendo intrinsecamente dotate di meccanismi di crittografia e di protezione; si prestano quindi ottimamente a conservare crediti di denaro o di trasporto. La falsificazione di una smart card, in particolare dei tipi più evoluti, o la sua ricarica abusiva risultano fuori della portata della maggior parte dei potenziali operatori criminali oltre a richiedere mezzi tali da risultare non conveniente nel contesto del Trasporto Pubblico Locale. Dalla maggiore sicurezza deriva inoltre la possibilità di effettuare transazioni fuori linea (off line).
- **maggiore capacità** di contenere dati; si parla di 500/16.000 byte contro i 25 di un biglietto magnetico e quindi possibilità di creare sistemi tariffari più articolati o di adibire la carta stessa anche ad altri servizi;

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	16/39

- **minor costo degli apparati di convalida** dovuto al fatto che gli apparati stessi non devono essere dotati di parti meccaniche come motori, cinghie, pulegge, cuscinetti ecc. Di conseguenza, anche la manutenzione risulta meno onerosa.
- **maggior durata**, nel caso di carte con supporto in plastica.

7.4 Classificazione

Le smart card attualmente in uso sono principalmente dei seguenti tipi:

- a memoria;
- a microprocessore.

Le prime sono più semplici ed hanno costi contenuti (1÷2 €); le seconde offrono una sicurezza superiore grazie alla presenza di un vero e proprio sistema di elaborazione all'interno del chip, a costi più elevati (3÷8 €).

Per la precisione, il titolo di "smart" non spetterebbe alle carte a memoria ma solo a quelle dotate di una qualche forma di intelligenza. L'uso corrente ha però decretato l'impiego del termine smart card nel senso più generale.

7.4.1 Smart card a memoria

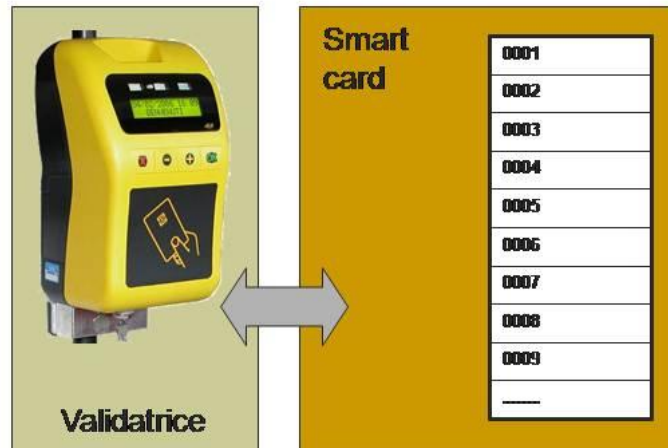
Nelle smart card a memoria è possibile la semplice scrittura e lettura di informazioni. Non sempre dotate di avanzati meccanismi di sicurezza hanno capacità che vanno da pochi byte a qualche migliaio di byte. Sono spesso relegate al semplice controllo accessi, anche se non mancano applicazioni di particolari tipi nel Trasporto Pubblico Locale.

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	17/39

Courtesy by AEP Ticketing Solutions

[Smart card a memoria]

- La smart card viene vista come sequenza di locazioni dove è possibile scrivere e leggere dati



7.4.2 Smart card a microprocessore

L'introduzione del microprocessore rende possibile non solo la scrittura e la lettura delle informazioni ma anche ma anche il loro processo. Ad esempio è possibile eseguire operazioni di crittografia anche a bordo della carta. Da questo consegue un livello di sicurezza molto elevato.

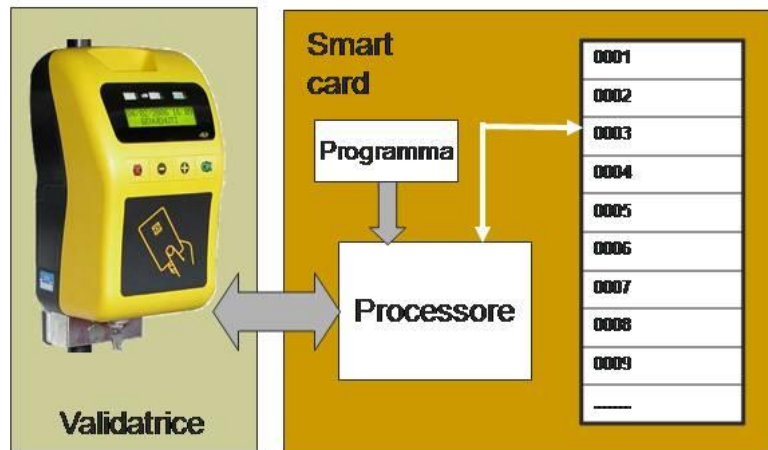
Si fabbricano modelli di carta a microprocessore anche con memoria molto estesa (32K o più).

Le smart card a microprocessore sono molto usate nel Trasporto Pubblico Locale.

Courtesy by AEP Ticketing Solutions

[Smart card a microprocessore]

- La smart card è vista come un computer con il quale dialogare.
- Il comportamento della SC è determinato da un **programma**.



7.4.3 Classificazione per interfaccia

Essendo le smart card passive, ossia non disponendo al proprio interno di una sorgente di alimentazione, per il loro interfacciamento al terminale (di emissione o di validazione) è necessario:

- fornire alla carta una tensione per l'alimentazione elettrica;
- prevedere la possibilità di inviare dati alla carta;
- prevedere la possibilità di ricevere dati dalla carta.

A questo fine si prevedono oggi due strade:

- **l'uso di contatti** - un opportuno connettore collega la carta ai circuiti interni del terminale.
- **l'uso di radio frequenza** - attraverso l'impiego di un campo elettromagnetico prodotto dal terminale che alimenta la carta e, per mezzo di una opportuna modulazione, trasferisce ad essa e da essa informazioni.

Nel primo caso si parla di carte a contatto ("contact"), nel secondo di carte senza contatto ("contactless") o a prossimità ("proximity"). L'impiego avviene semplicemente avvicinando la carta al terminale.

E' interessante notare che la differenza tra carte contact e contactless è solo tecnologica. Essa si limita al modo di accoppiare la carta al terminale. La prima classificazione esaminata (memoria/microprocessore) invece ha un carattere logico, e quindi, assai più profondo.

Non sussistono quindi diversità concettuali tra carte a contatto o senza contatto; esse possono, in linea di principio, essere assolutamente identiche. L'unica differenza è nel modo di utilizzo, che richiede l'introduzione in una fessura nel primo caso e la semplice "presentazione" nel secondo.

7.5 Le carte contact

Le carte contact, anche se meno frequentemente, sono utilizzate nel trasporto pubblico in quanto affiancano vari benefici all'inconveniente di una transazione più lunga dovuta al tempo di inserimento ed espulsione della carta. Vogliamo ricordare:

- la carta contact non presenta limiti alla complessità dell'elettronica conseguenti alla potenza di alimentazione, e quindi può fornire prestazioni elevate, in quanto alimentata direttamente dal terminale;
- i terminali per carte contact permettono all'utente di "prendere possesso" del terminale; questo è particolarmente utile ove sia prevista la possibilità che l'utente debba interagire col terminale stesso, per selezionare tariffe e/o richiedere altre operazioni, come il rinnovo dell'abbonamento. In questa circostanza, il poter "parcheggiare" offre una migliore l'utilizzabilità rispetto al sistema contactless.
- le carte bancarie, presto anche le normali carte di credito ed il Bancomat, la Carta Nazionale dei Servizi e la Carta di Identità Elettronica sono dotate di chip ed hanno oggi interfaccia a contatti. La prospettiva di impiego di queste carte richiede necessariamente, salvo evoluzioni delle stesse, una interfaccia di questo tipo.

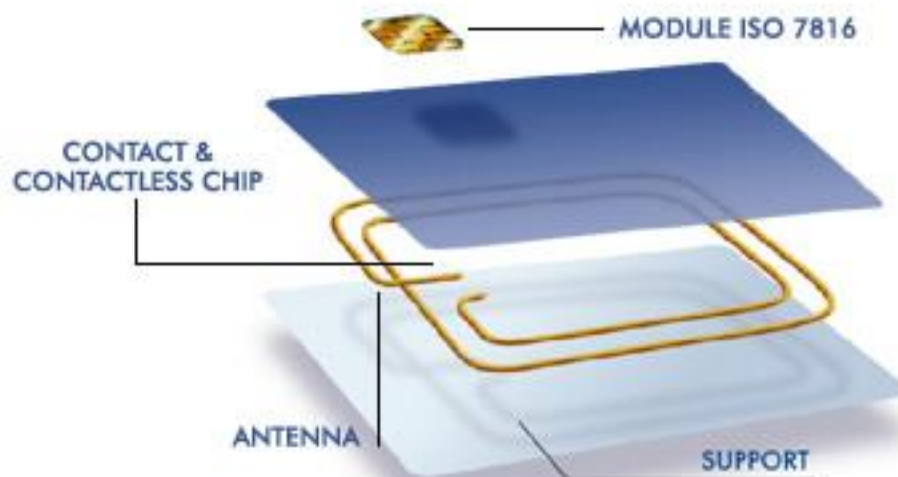
Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	20/39



Validazione a contatti

7.6 Le carte contactless

Le smart card contactless furono introdotte per la prima volta all'inizio degli anni 90; il loro impiego si sta velocemente diffondendo soprattutto nel mercato del trasporto di massa e del controllo degli accessi, anche per la loro estrema semplicità di impiego.



Come sarà meglio esaminato nel seguito, intervengono vari fattori tecnologici a limitare le prestazioni delle carte contactless. Ben si comprende, infatti, come il modesto trasferimento di energia consentito dal campo ma-

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	21/39

gnetico emesso dal terminale possa diventare un fattore limitante delle caratteristiche funzionali della carta stessa, anche in conseguenza della brevità del gesto dell'utilizzatore, che non consente di prevedere un tempo superiore a circa 500 millesimi di secondo per la transazione.

Nel caso del contatto, invece, la carta può impiegare tutta l'energia che serve così come non sussistono limiti di tempo, se quelli non imposti dalla pratica utilizzabilità.



Validazione contactless

7.7 Tipi complessi

Oltre ai tipi base sopra elencati esistono carte che combinano le due tecnologie contact/contactless, dette di tipo "dual interface", o "combi", in grado di comunicare con i terminali sia in modalità senza contatto che a contatto.

Queste carte possono essere costruite in due maniere:

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	22/39

- semplicemente riunendo due carte in una, ossia applicando un chip che opera in modo contact ed uno che opera in modo contactless nella stessa tessera; questa tecnica costruttiva è però obsoleta.
- creando un chip munito di doppia interfaccia (contact/contactless).

In questo ultimo caso, verrà utilizzata la modalità "senza contatto" per le transazioni di validazione a bordo autobus in modo da favorire un rapido incarrozzamento, mentre per le transazioni di ricarica, di controllo e/o di tipo finanziario sarà utilizzata la modalità "a contatto", che garantisce anche una maggiore praticità.

Le carte a doppia interfaccia hanno necessariamente costi più alti ma la loro diffusione crescente sta determinando la loro riduzione. Possono essere usate con i tradizionali lettori a contatto già installati nelle banche, nei POS ed in progetti di fidelizzazione della clientela, avendo in più tutti i vantaggi tipici delle contactless. Risultano quindi adatte ai trasporti, al controllo degli accessi ed in genere laddove sono richieste la facilità d'uso e la velocità della transazione. Le carte combi sono applicate anche per i sistemi di pagamento bancari o per alcuni tipi di transazioni via Internet.

7.8 Il supporto fisico

Con l'aumentare della diffusione delle smart card, i costruttori hanno esplorato nuove strade al fine di realizzare dei tipi di carta a costo estremamente ridotto, utilizzando un supporto fisico cartaceo anziché di plastica rigida.

Questi nuovi TDV hanno preso in nome di usa-e-getta ("disposable", in inglese) anche se, ancora, il loro costo non è poi così trascurabile (0,4÷0,5€). Per diluirne il costo, queste carte sono usate per creare dei carnet multicorsa; in certi casi, vengono anche ricaricate e quindi usate più volte.

Quest'ultima soluzione è implementata raramente, in quanto questo tipo di TDVE, per motivi di costo, presenta degli schemi di sicurezza semplificati che possono garantire contro le frodi solo attraverso un meccanismo di alterazione elettronica irreversibile di alcuni bit ("bruciatura").

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	23/39



L'uso di questa soluzione tecnica garantisce la sicurezza ma rende i biglietti non ricaricabili; viceversa scelte che consentano la ricarica non forniscono garanzia contro la ricarica abusiva.

7.9 Sistemi a microprocessore

Per comprendere meglio l'architettura ed il modo di funzionamento delle smart card è opportuno conoscere alcune nozioni circa l'architettura dei sistemi a microprocessore. Riferirsi a [2] per maggiori informazioni.

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	24/39

8 Gli standard per le smart card

8.1 Generalità

L' International Standards Organization (ISO) ha emesso una serie di standard per definire univocamente le smart card in termini di caratteristiche fisiche, elettriche e di comunicazione; si è creato così uno standard internazionale che dovrebbe garantire l'interoperabilità delle carte, ancorché prodotte da diversi produttori, nei vari circuiti di utilizzo.

Gli standard più significativi per le applicazioni di trasporto pubblico sono quelli descritti nei paragrafi seguenti.

8.2 ISO 7816

E' il più usato ed interessa tanto le carte a contatti che quelle contactless. E' composto da 10 parti, anche se solo le prime 4 sono quelle più conosciute:

- **ISO 7816 parte prima:** caratteristiche fisiche delle carte a contatti, resistenza a fenomeni fisici quali raggi UV e raggi X, campi elettromagnetici, elettrostatici ecc. Definisce inoltre le caratteristiche meccaniche e di resistenza allo stress.
- **ISO 7816 parte seconda:** definisce la posizione e la dimensione dei contatti;
- **ISO 7816 parte terza:** definisce segnali e protocolli di comunicazione;
- **ISO 7816 parte quarta:** contenuto dei messaggi, comandi e risposte trasmessi dal terminale alle carte e viceversa; struttura dati e file; modo di accesso ai dati ed ai file ecc.

8.3 ISO 14443

E' relativo solo alle carte contactless ed è composto dalle seguenti parti:

- **ISO 14443 parte prima:** dimensione delle carte contactless, qualità superficiale per la stampa, resistenza meccanica, resistenza agli UV ed ai raggi X, sensibilità ai campi elettromagnetici. Contiene informazioni molto limitate, rimandando ad altri standard come ad esempio l'ISO

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	25/39

7810 e 7816, stabilendo solo un certo numero di parametri aggiuntivi, come ad esempio i limiti di esposizione ai campi magnetici;

- **ISO 14443 parte seconda:** descrive le caratteristiche del trasferimento di potenza, basato su accoppiamento induttivo, e la comunicazione tra terminale e carta;
- **ISO 14443 parte terza:** descrive i meccanismi di inizializzazione e di anticollisione;
- **ISO 14443 parte quarta:** protocolli di trasmissione.

Come sarà indicato nel paragrafo successivo, lo standard ISO 14443 prevede due varianti, significativamente differenti, dette "tipo A" e "tipo B". Maggiori informazioni in [2].

8.3.1 ISO 14443A e MIFARE

Questo standard è quello previsto per la comunicazione a radio frequenza dalle carte contactless MIFARE.

MIFARE è la tecnologia contactless più diffusa, con centinaia di milioni di carte vendute. La tecnologia di queste carte, creata da Mikron, poi acquistata da Philips, è oggi di proprietà di NXP Semiconductors.

Le carte MIFARE classiche e MIFARE UltraLight sono fondamentalmente solo dispositivi di memoria; questa è suddivisa in segmenti e blocchi con semplici meccanismi di controllo degli accessi.

Basate su Application Specific Integrated Circuit (ASIC), hanno un limitato potere computazionale. Grazie al basso costo sono spesso usate per il controllo degli accessi o biglietti per manifestazioni sportive, mentre, per le limitate prestazioni, non trovano frequente applicazione in Italia nell'ambito del trasporto pubblico, probabilmente perché nella nostra nazione questo settore iniziato ad evolversi quando era ormai disponibile la più avanzata tecnologia B.

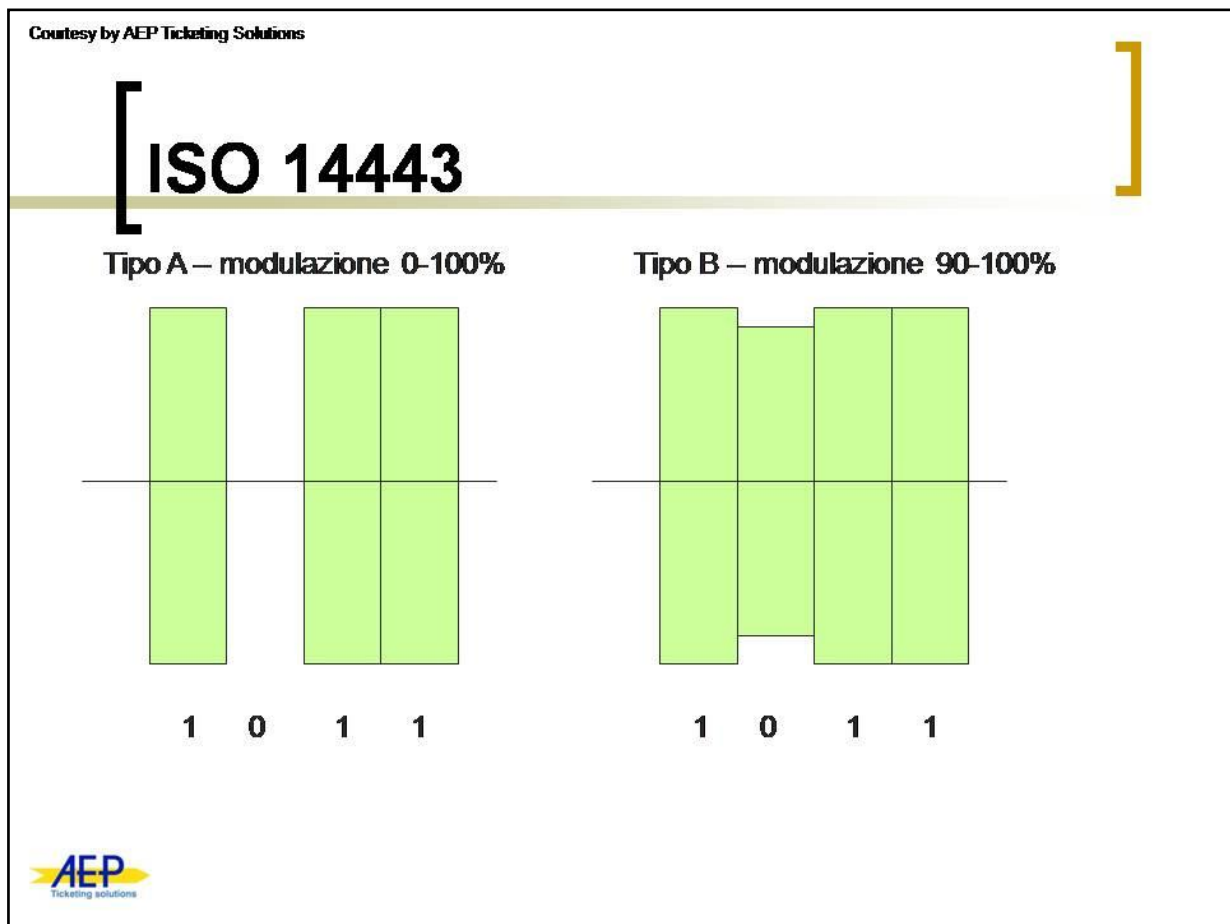
A causa del limitato grado di sicurezza e del fatto di operare solo in modalità senza contatto, le carte MIFARE non sono utilizzate in ambito bancario o per borsellini elettronici.

Si noti che la sola comunicazione in aderenza al 14443A non garantisce la compatibilità con le carte MIFARE. E' possibile cioè avere un terminale che processa carte di tipo A ma non carte MIFARE.

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	26/39

8.3.2 ISO 14443B

Si è detto che la comunicazione con le carte avviene con una tecnica in qualche modo simile al codice Morse. La modulazione della radio frequenza utilizzata nello standard di tipo A è di tipo 0/1, ossia si trasmette la portante per significare un "1" logico (linea Morse) e la si interrompe per lo "0" (punto Morse). Questo determina un trasferimento di energia ridotto: quando si trasmette uno "zero" il trasferimento di energia è nullo. L'energia media trasferita non risulta adeguata, in genere, al funzionamento delle carte a microprocessore. Per questo motivo è stato ideato lo standard del tipo B che ovvia a questo inconveniente.



Diversamente dallo standard 14443A, nato sulla base di prodotti già esistenti, la variante B non è derivata da alcun prodotto. La maggior parte delle carte contactless a microprocessore usano questo standard per la sua flessibilità nel consentire alti flussi di dati (fino a 847 Kbs) e il 100% di disponibilità durante la transazione del segnale di clock, che è critico per alcune CPU.

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	27/39

Va osservato che la tecnologia avanza a grandi passi e che allo stato attuale è possibile realizzare carte a microprocessore di tipo A. Resta comunque il fatto che, in parallelo, diviene possibile, con il tipo B, l'impiego di carte di tipo ancora più evoluto.

8.3.3 ISO 15693

Un ulteriore standard da citare è l'ISO 15693, il cosiddetto standard per le operazioni di "vicinità". Le carte aderenti a questo standard possono essere lette a distanza maggiore, fino a quasi un metro, usando antenne di grandi dimensioni, molto simili a quelle che si impiegano nei varchi di uscita dei supermercati con finalità antifurto.

Questo standard assicura però una bassa velocità di comunicazione, inadeguata alle esigenze di un Sistemi di Bigliettazione Elettronica. Anche l'affidabilità della transazione è imperfetta, per cui viene di solito relegato al rilevamento dei flussi di passeggeri.

Vengono costruite carte bi-standard (es. Picopass di Inside Technologies) capaci di operare anche in modo ISO 14443B per consentire il pagamento in modalità contactless e il rilevamento in modo vicinità.

8.3.4 ENV 1545

La norma ENV 1545 descrive la struttura dati raccomandata per le carte usate nelle applicazioni di trasporto pubblico. E' molto estesa e spesso ne viene usato solo un sotto assieme.

Non definisce il tracciato dati ma solo la modalità di codifica di numerosi possibili campi. Ad esempio la codifica suggerita da detta norma per un possibile campo "profilo utente" CustomerProfile. Esso viene definito come un intero a 6 bit (INTEGER(0 .. 63)) con la seguente codifica

--unspecified	0
--adult	1
--child	2
--student	3
--oldAgePensioner	4
--disabledNotfurtherspecifued	5
--disabledVisuallyImpaired	6
--disabledHearingImpari	7
--unemployed	8
--staff	9

--military	10
--resident	11
--industrialOwnedHaulage	12
--busTransportCompany	13
--farDistanceTransport	14
--localTransport	15
--commuter	16
--reservedForFutureCenUse	17..31
--contractProviderSpecific	32..63

8.4 Calypso

La società RATP di Parigi, che gestisce i trasporti pubblici della Ile de France (4000 bus, 420 stazioni di metropolitana), ha da molti anni effettuato cospicui investimenti per la definizione di una tecnologia per la bigliettazione elettronica.

La tecnologia Calypso, sviluppata per iniziativa da RATP, propone uno standard interoperabile di bigliettazione che è stato accettato anche in altre parti d'Europa e sta divenendo uno degli standard accettati per sistemi di pagamento con carte a microprocessore di tipo contactless.

La tecnologia Calypso, che è in continua evoluzione, è stata progettata congiuntamente agli operatori di trasporto di Bruxelles, Costanza, Lisbona, Parigi e Venezia ed è stata adottata dalle città di molti paesi incluse Parigi, Lisbona, Venezia, Lione, Skopje, Glasgow, Amiens, Avignone, Metz, Nizza.

Gli scopi di Calypso sono di definire delle specifiche di riferimento per le carte e per i terminali assicurare l'interoperabilità tra gli operatori.

Calypso è basato sugli standard internazionali già indicati (ISO 14443, ISO 7816, ENV1545), e in alcuni casi ha costituito la base stessa sulla quale è stato sviluppato lo standard e promuove la standardizzazione di altri elementi.

Al momento gli standard internazionali non sono abbastanza completi da garantire la reale interoperabilità dei prodotti di bigliettazione. Così Calypso, anticipando gli standard, propone specifiche, che cercano di definire completamente una comunicazione carta-terminale interoperabile per la bigliettazione.

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	29/39

La tabella indica le correnti relazioni tra gli standard internazionali e Calypso:

	Layer	Standard internazionali	Calypso
7	Gestione Sicurezza e architettura		Calypso Security Architecture
6	Software del terminale		Calypso API
5	Modello dati		Calypso Data Model
4	Meccanismi di sicurezza della carta e della SAM		Calypso Card Application
3	Struttura dati della carta	CEN ENV 1545	
2	S.o. della carta, comandi e struttura file	ISO 7816-4	
1	Interfaccia contact e contactless	ISO 7816 1-3 ISO 14443 B 1-4	

Le scelte Calypso sono le seguenti:

- ISO 7816 (parti da 1 a 4) per le applicazioni smart card. Questo è uno standard ben stabilito che è stato completato da Calypso per l'applicazione alla bigliettazione contactless (linea 4 nella tabella).
- ISO 14443B per il collegamento contactless.
- ENV 14445 per il dizionario dati della bigliettazione per il trasporto, che definisce i dati come supporto delle informazioni, eventi di pagamento ecc.

In aggiunta Calypso specifica con precisione i meccanismi di sicurezza per la carta e per il SAM (vedi nel seguito e [2]).

Inoltre, Calypso sta correntemente lavorando sulle linee guida che le altre parti del sistema di bigliettazione che non sono ancora state pubblicate.

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	30/39

I vantaggi promessi dalla tecnologia Calypso sono da ricercarsi fondamentalmente nella ricchezza di contenuti ben sperimentati e nella ricerca della standardizzazione delle carte e degli apparati.

Gli svantaggi della tecnologia Calypso sono nella sua complessità e nel maggior costo delle apparecchiature e delle carte. Pur basata su standard internazionali, richiede un premio di licenza per essere, anche se questi costi sono inferiori a quelli che si dovrebbero sostenere per sviluppare sistema di equivalenti caratteristiche. I costi delle licenze si applicano solo ai costruttori e non alle società di trasporto, ma è evidente che è comunque l'utente finale che, ancorché indirettamente, li sostiene nei fatti.

8.5 Struttura dati di alcune carte

8.5.1 Carta MIFARE Classic

Le MIFARE Standard offrono circa 768 byte per l'immagazzinamento dei dati, divisi in 16 "settori"; ogni settore è protetto da due diverse chiavi, chiamate A e B. Esse possono essere programmate per operazioni come lettura, scrittura, incremento del valore dei blocchi, ecc. Le MIFARE Standard 4k offrono 3 kB divisi in 64 settori.

Le MIFARE UltraLight hanno solo 512 bit di memoria (cioè 64 byte), senza sicurezza.

8.5.2 Carta GTML

La carta GTML è una delle più diffuse in Italia; anche se non più prodotta, è sostituita da altri modelli che sono però capaci di emularla. Si ritiene pertanto interessante descriverla nella sua veste originale.

La GTML è una carta nata specificamente per l'impiego in area trasporti, che segue in parte le indicazioni dello standard Calypso.

Poiché i diritti di trasporto rappresentano un valore economico, la carta è protetta per mezzo di algoritmi crittografici [2] per impedire a malintenzionati di produrre carte false o ricaricare la carta senza autorizzazioni.

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	31/39

Gli algoritmi crittografici sono basati su chiavi segrete, nascoste nella carta e nei relativi moduli SAM che per l'utilizzo delle stesse devono essere necessariamente presenti nella validatrice.

Dopo la fabbricazione nella carta vengono registrate le chiavi associate allo specifico cliente rendendo quindi la carta legata ad uno specifico Sistema di Bigliettazione Elettronica. Le chiavi devono essere le stesse registrate nei moduli SAM.

Le GTML sono carte con doppia interfaccia; possono quindi essere indifferentemente usate in modalità contactless o attraverso i contatti di cui la carta è dotata.

Esse aderiscono ai seguenti standard:

- ISO 7816;
- ISO 14443 (in parte);
- permettono di adottare strutture dati in aderenza alla norma ISO 1545.

La carta, dal punto di vista fisico, è aderente al disposto delle norme ISO 7810, ISO 7816-1 and ISO 14443-1.

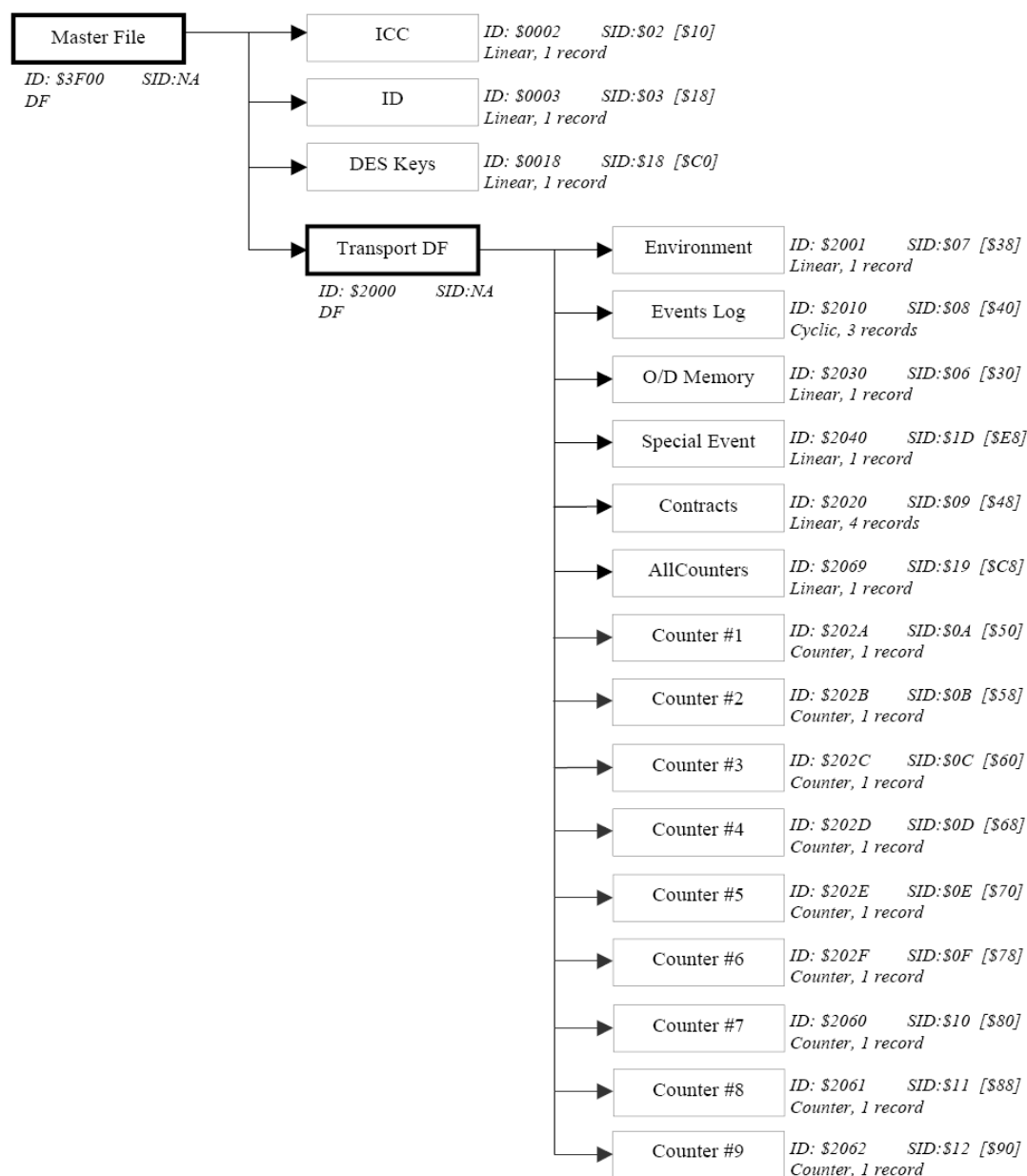
Nella modalità a contatti, aderisce allo standard ISO 7816-2/3/4.

In modalità contactless aderisce allo standard ISO 14443-2 (type B) - importante osservare che non rispetta né la parte 3 né la 4.

La struttura file della carta è fissa e prevista per il seguente uso:

- informazioni relative al titolare (protette da codice PIN),
- informazioni per l'applicazione (29 byte);
- 4 contratti (di 29 byte ciascuno);
- 9 contatori (da 0 a 16.777.215);
- log degli ultimi 3 eventi (di 29 byte ciascuno);
- altri dati applicativi (2 file di 29 byte ciascuno);
- informazioni di fabbricazione e chiavi segrete;
- crittografia DES con chiavi a 64 bit [vedi anche 2];

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	32/39



La struttura dati della carta GTML.

Nella carta ci sono due tipi di file:

- file dedicati (DF), direttori di file;
- file elementari EF, file contenenti dati.

I DF sono direttori che possono contenere file elementari ed altri DF.

La carta GTML ha due DF, il direttorio radice, chiamato Master File ed il DF trasporti contenente i dati relativi al trasporto.

Gli EF sono file contenenti dati: dati utenti organizzati in record lineari o ciclici, contatori, chiavi ecc. Essi sono gestiti internamente e non pos-

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	33/39

sono essere acceduti dall'esterno (per esempio, il file contenenti le chiavi).

Un file nella carta è identificato dal suo LID (Long Identifier). Alcuni file possono essere identificati anche con lo Short Identifier (SID).

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	34/39

9 Sicurezza e chiavi

9.1 Crittografia

Vedere anche [2].

La creazione di falsi documenti di viaggio, se sufficientemente semplice, è un'attività criminale potenzialmente lucrosa. E' indispensabile quindi prevedere adeguate contromisure. Molte possono essere le tecniche impiegabili per garantire la sicurezza della transazione di un TDVE.

La scienza della crittografia è antica e, negli ultimi decenni, ha fatto notevoli progressi, non solo per ragioni militari o strategiche ma anche perché indispensabile in ambito bancario.

Oggi si ritiene ormai accertato che non è opportuno basare la sicurezza sull'impiego di algoritmi segreti: essi prima o poi vengono conosciuti, esponendo il sistema a probabili effrazioni. Si tende invece ad utilizzare algoritmi crittografici pubblici, come ad esempio il DES e il triplo DES, basando



l'operazione di codifica su numeri segreti detti chiavi.

Attraverso un adeguato impiego di tecniche crittografiche è possibile assicurarsi contro l'impiego di carte non autorizzate o, viceversa, impedire che un terminale non legittimato possa sottrarre credito da carte autentiche. Diviene inoltre possibile essere certi che le transazioni inviate ad un centro servizi siano vere e non, ad esempio, create artificialmente allo scopo di alterare l'equa ripartizione del monte degli introiti.

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	35/39

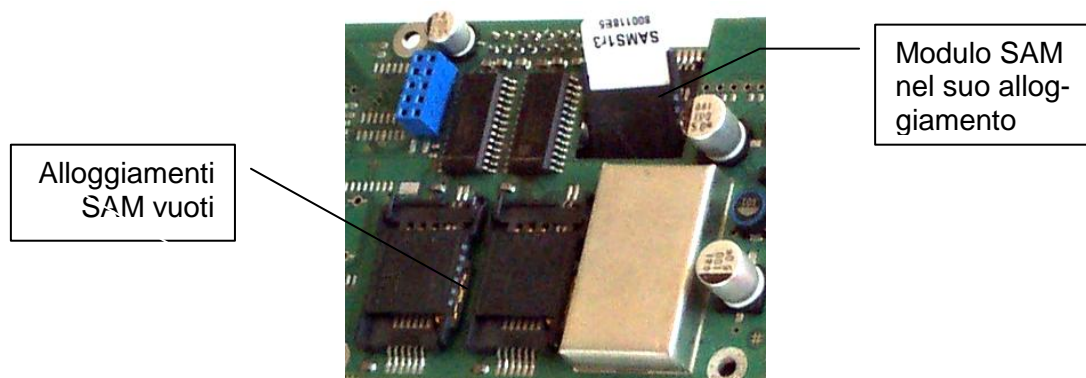
9.2 I moduli SAM

Una volta costruito un sistema basato sui principi ora esposti, il problema diventa quello di garantire la segretezza delle chiavi crittografiche.

Una soluzione, ormai di impiego generalizzato, è quella di utilizzare nei terminali una seconda smart card, detta SAM (Security Access Module). Essa viene, di solito, fisicamente "tagliata" per ridurne l'ingombro ed assume quindi l'aspetto esteriore delle classiche SIM impiegate per la telefonia cellulare.

Gli scopi del modulo SAM possono essere molteplici e differire a seconda dello schema di sicurezza adottato. Ad esempio, i moduli SAM possono essere usati per:

- contenere le chiavi crittografiche;
- eseguire operazioni di crittografia;
- conservare una copia delle transazioni effettuate;
- generare una firma elettronica che garantisca l'autenticità delle transazioni.



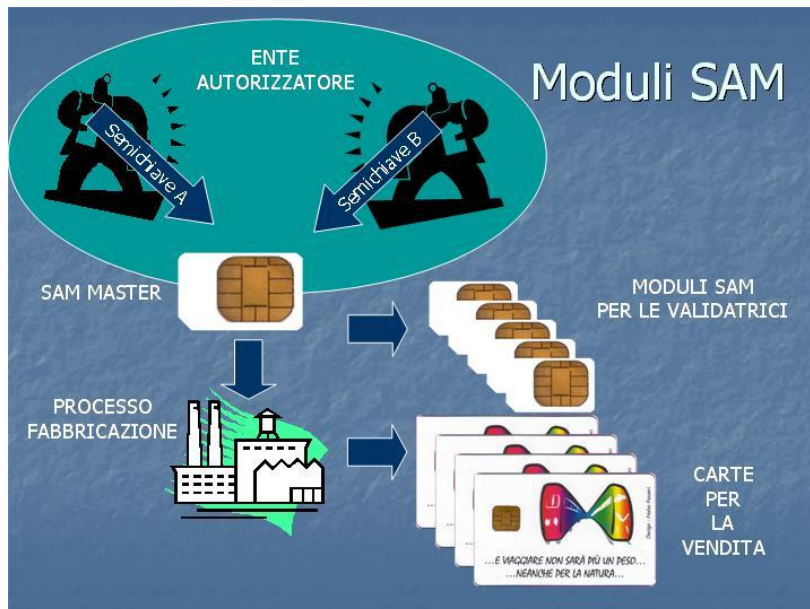
Grazie ai moduli SAM è possibile scindere la fornitura dei terminali, che può essere affidata virtualmente "a chiunque", dalla gestione della sicurezza e, al contempo, avere, nella stessa Comunità tariffaria, Compagnie servite da fornitori diversi, con apparati di marca e modello diversi.

I terminali, in questo caso, dovranno ovviamente risultare dotati di uno o più alloggiamenti ove inserire i moduli SAM stessi ed essere in grado di processarli.

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	36/39

9.3 Uso dei SAM come custodia per le chiavi

E' evidente che non è opportuno conservare le chiavi crittografiche nel software della validatrice, a portata di un qualunque addetto "infedele". E' anzi opportuno che nessuno le conosca nella loro interezza. Esse vengono invece generate, con una complessa e collaudata procedura, da due "semichiavi", in possesso di due persone diverse, ciascuna delle quali ignora l'altra semichiave. In base a questa procedura viene costruito un modulo, detto "SAM master" che è la "matrice" dalla quale possono essere generate, in modo automatico e sicuro, tanto le smart card di produzione, che saranno poi poste in vendita agli utenti, quanto i "moduli SAM", che hanno lo scopo di costituire il contenitore inviolabile in cui si trovano le chiavi all'interno delle validatrici e che risultano indispensabili per processare le carte prodotte con lo stesso insieme di chiavi.



Al momento della transazione, la validatrice, con un complesso procedimento, verifica, tra l'altro, che la smart card presentata dall'utente sia capace di eseguire le operazioni crittografiche previste; questo è possibile solo se la carta presentata è stata costruita con le stesse chiavi contenute nella SAM; viceversa fa la smart card, per controllare che la validatrice sia effettivamente in possesso della chiave corretta (mutua autenticazione).

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	37/39



Quindi se le chiavi con cui sono state costruite le carte non collimano con quelle contenute nel modulo SAM della validatrice, nessuna operazione da eseguirsi "in sicurezza" è possibile.

9.4 Altri impieghi dei moduli SAM

Alcuni moduli SAM possiedono una memoria riscrivibile sufficientemente grande da poter contenere un certo numero di transazioni. In caso di guasti al terminale, essi possono ancora essere impiegati per il recupero dei dati relativi alle operazioni effettuate.

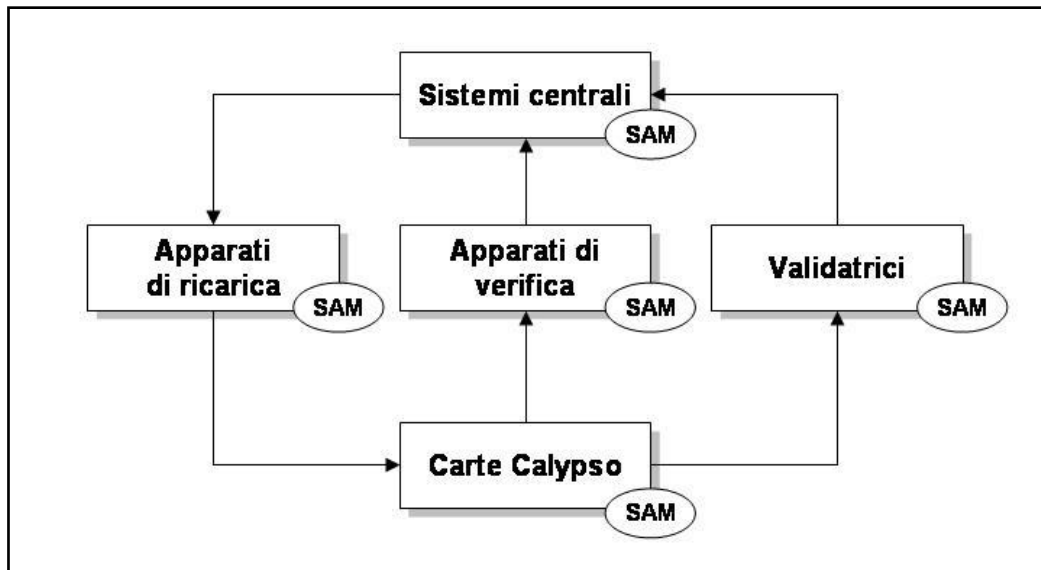
In certi casi è possibile utilizzare il modulo SAM anche per garantire la trasmissione dei dati verso il centro di controllo. Tramite il SAM viene generata una firma digitale da apporre in coda alla transazione. Il sistema centrale esegue una verifica e controlla che la firma sia corretta, permettendo così di individuare eventuali transazioni false.

9.5 Chiavi differenziate

Un modulo SAM può contenere o meno più chiavi per l'accesso a zone differenti della carta o per differenti operazioni. Ad esempio, si possono avere SAM con le sole chiavi per il solo "consumo" (transazione di fruizione) o contenenti anche le chiavi per eseguire la ricarica del credito.

Titolo documento	File	Pagina/di
I Titoli Di Viaggio Elettronici	701286.E00.IT DISPENSA TDVE.DOCX	38/39

Si osservi che, per evidenti ragioni di sicurezza, è opportuno controllare e limitare la diffusione di moduli SAM con chiavi che consentano solo le operazioni effettivamente necessarie.



9.6 Titolarità degli elementi di sicurezza

Le chiavi, i SAM master e tutti i diritti relativi ad essi sono normalmente di esclusiva proprietà dell'Ente regolatore, della Compagnia o della Comunità Tariffaria, cosicché non sussistano limitazioni alla "tiratura" delle carte e dei moduli SAM o all'introduzione nel sistema di apparati di marche differenti.

Gianni Becattini

Appunti sulla Bigliettazione Elettronica

Il sistema di bordo



AEP Advanced Engineering Projects s.r.l.
Via dei Colli, 240 - Signa (Firenze) - Italia
<http://www.aep-italia.it>



Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	1/67

1. Sommario

1.	Sommario.....	2
2.	Presentazione	5
3.	Introduzione	6
3.1	Il Sistema Di Bordo.....	6
3.2	Funzionalità.....	6
3.3	SBE ed AVM	7
4.	Architetture del Sistema Di Bordo.....	9
4.1	Le architetture di base	9
4.2	Componenti del Sistema Di Bordo	10
4.3	Esempi di Sistemi Di Bordo reali.....	11
4.3.1	Esempio 1 – CTP Napoli (TSF).....	11
4.3.2	Esempio 2 – APM Perugia (Siemens Italdata)	12
4.3.3	Esempio 3 – Città di Gaziantep, Turchia (Olivetti).....	12
4.3.4	Esempio 4 - Autobus Unico Campania/EAV (IPM, T&T ecc.)	12
5.	La validatrice	13
5.1	Generalità.....	13
5.2	Caratteristiche comuni	13
5.2.1	Interfaccia utente.....	14
5.2.2	Unità di processo	16
5.2.3	Periferiche di massa	16
5.2.4	Le interfacce	17
5.2.5	L'alimentatore e le batterie	17
5.2.6	Marcatura CE.....	18
5.2.7	Omologazioni.....	19
5.2.8	Organizzazione del software.....	19
5.2.9	La configurabilità.....	21
5.3	Riepilogo.....	22
6.	La validatrice per titoli tradizionali	23
7.	La validatrice magnetica	24
7.1	Principi della registrazione magnetica	24
7.2	Tecniche per la lettura	25
7.3	Normative internazionali.....	26
7.4	Codifica ed organizzazione dati	26
7.5	Codici di controllo.....	26
7.6	Architettura generale.....	27
7.7	Sequenza operativa.....	27
7.8	Posizione della banda magnetica sul biglietto e stampa di convalida.....	28
7.9	Sezione elettronica	28
7.10	Caratteristiche critiche delle validatrici magnetiche	29
7.11	Considerazioni sulla sicurezza	30
7.12	Caratteristiche per l'interoperabilità.....	31
8.	La validatrice per smart card a contatti.....	32
8.1	Le smart card.....	32
8.2	Sistemi a microprocessore.....	33

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	2/67

8.2.1	Il microprocessore.....	33
8.2.2	La memoria.....	35
8.2.3	Le unità di ingresso/uscita.....	36
8.3	La “maschera”.....	36
8.4	Funzioni della smart card.....	37
8.5	La sicurezza.....	38
8.6	Il principio di Kerckhoff.....	38
8.7	Uso della crittografia per garantire la sicurezza.....	38
8.8	Procedimenti crittografici.....	39
8.9	La mutua autenticazione.....	40
8.10	La sessione.....	41
8.11	La validatrice per smart card.....	41
8.12	Costruzione della validatrice per smart card a contatti.....	42
8.13	I contatti della carta.....	42
8.14	Gli scambi dati.....	42
8.15	I moduli SAM.....	43
9.	La validatrice contactless.....	45
9.1	Riconoscimento.....	45
9.2	Generalità.....	46
9.3	Trasferimento di energia.....	46
9.4	Comunicazione dal PCD alla PICC.....	48
9.4.1	Generalità.....	48
9.4.2	Tipo A e tipo B.....	48
9.4.3	Tipo A.....	48
9.4.4	Tipo B.....	49
9.5	Comunicazione dalla PICC al PCD.....	49
9.6	MIFARE ed altri standard.....	51
9.7	Altri standard.....	51
9.8	Il “coupler”.....	51
9.9	Normative e distanza di lettura.....	52
9.10	Tempo della transazione.....	53
9.11	Pregi delle validatrici contactless.....	54
10.	La console autista.....	55
10.1	Interfaccia utente (autista).....	55
10.1.1	Display.....	55
10.1.2	Avvisatore acustico.....	57
10.1.3	Tastiera.....	57
10.2	Interfaccia utente (passeggero).....	58
10.3	Unità di processo.....	58
10.4	Periferiche di massa.....	58
10.5	Le interfacce.....	58
10.6	L'alimentatore le batterie.....	58
10.7	Omologazioni.....	58
10.8	Organizzazione del software.....	59
10.9	Stampante di scontrini.....	59
10.9.1	Sezione di convalida contactless.....	60
11.	Apparati di comunicazione.....	61
11.1	Generalità.....	61
11.2	Comunicazione a breve raggio.....	61

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	3/67

11.3	Comunicazione a lungo raggio	61
12.	Sistemi di stazione	62
12.1	Generalità	62
12.2	Concentratore di stazione	62
12.3	Stazioni di metropolitana.....	63
12.4	Stazione medio/grandi	65
12.5	Stazioni non presidiate	66

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	4/67

2. Presentazione

Questa dispensa è stata originariamente presentata dall'autore all'Executive Master "SVILUPPO E GESTIONE DEI SISTEMI DI BIGLIETTAZIONE ELETTRONICA E DI PAGAMENTO DEI SERVIZI DI MOBILITÀ" organizzato da Clickutility e tenuto a Bologna dal settembre a dicembre 2007, con la collaborazione scientifica e il patrocinio di Club Italia ed il patrocinio dell'ANAV.

Essa appartiene ad una serie di tre volumetti orientati alla descrizione delle tecnologie di bordo:

- dispensa 1 - "Titoli Di Viaggio Elettronici (TDVE)" - descrive sommariamente i vari tipi di TDVE in un'ottica di funzionalità e di utilizzo con annotazioni anche di carattere commerciale;
- dispensa 2 - "Il Sistema Di Bordo (SDB)" - descrive principalmente le caratteristiche tecniche e di funzionamento dei terminali per l'utilizzo dei TDVE e di quelle parti accessorie che, installate a bordo del bus, costituiscono nel complesso il cosiddetto Sistema Di Bordo. In parallelo alla descrizione dei terminali vengono fornite informazioni più approfondite sui principi di funzionamento dei TDVE.
- dispensa 3 - "Tecniche e Sistemi di Comunicazione (COM)" - vengono descritte le principali tecniche di comunicazione usate all'interno ed all'esterno degli apparati di bordo, nonché i sistemi di terra che consentono lo scambio di dati con gli autobus.

Eventuali riferimenti al numero della dispensa sono via via riportati entro parentesi quadre (es. [1])

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	5/67

3. Introduzione

3.1 Il Sistema Di Bordo

In un Sistema di Bigliettazione Elettronica, viene di solito chiamato "Sistema Di Bordo" (SDB) l'insieme degli apparati che consentono la fruizione dei Titoli Di Viaggio Elettronici (TDVE).

Considerata la complessità di un Sistema di Bigliettazione Elettronica, infatti, la parte dedicata alla fruizione dei TDVE non si limita di solito alla validatrice, molti altri ancora essendo gli elementi indispensabili alla integrazione della stessa nel SBE.

Diverse possono essere le funzioni svolte dal Sistema Di Bordo, in aggiunta a quella primaria della convalida, in corrispondenza con l'impostazione generale del Sistema di Bigliettazione Elettronica. Ad esempio, il Sistema Di Bordo può prevedere o meno funzioni quali l'emissione a bordo di titoli di viaggio.

Un ulteriore livello di complessità viene aggiunto dalla eventuale presenza sul mezzo di un sistema di monitoraggio della flotta (AVM, Automatic Vehicle Monitoring), con cui il Sistema Di Bordo della bigliettazione può compenetrarsi o del quale può, con variabile convenienza, duplicare parte delle funzioni.

Nelle note successive sarà fatto riferimento quasi esclusivamente ai Sistemi Di Bordo installati su mezzi di superficie (autobus, tram ecc.) mentre sarà dedicato un paragrafo apposito ai sistemi per l'ambito ferroviario.

3.2 Funzionalità

Come ovvio, la funzione primaria del Sistema Di Bordo è quella di consentire la validazione dei TDV. A questo fine, il SDB deve poter quindi assolvere anche ad altre funzioni quali:

- **funzione di comunicazione** - le validatrici, per poter operare, devono ricevere dal sistema parametri di configurazione e vari tipi di liste e devono viceversa ad esso ritornare i file con le transazioni eseguite e gli storici contenenti le registrazioni degli eventi più signifi-

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	6/67

cativi del Sistema di Bigliettazione Elettronica (es. accensioni, spegnimenti, guasti ecc.).

- **funzione di localizzazione del mezzo** - finalizzata a determinare il numero della fermata o la zona per l'applicazione di tariffe dinamiche georiferite.
- **funzione di interfaccia con l'autista** - per consentire all'autista di controllare l'operatività della validatrice e di sospenderne la funzionalità durante le verifiche a bordo. Ove sia prevista la funzione di localizzazione è necessario un maggiore grado di interoperatività con il guidatore, sia per verificare il corretto rilevamento geografico, sia per l'introduzione di informazioni ausiliarie (linea, turno, corsa, ecc.).
- **funzione di vendita a bordo** - per consentire all'autista di emettere titoli di viaggio o di ricaricare carte a valore o abbonamenti.

3.3 SBE ed AVM

Si osservi che si è preferito ricorrere ad una definizione funzionale del Sistema Di Bordo in quanto, nella reale attuazione, si assiste alla messa in atto di una molteplicità di soluzioni tecniche diverse tra loro.

Le possibili combinazioni sono accresciute dalla già citata parziale sovrapposizione con l'eventuale sistema AVM. In particolare, le funzioni di:

- comunicazione,
- localizzazione,
- interfaccia con l'autista

sono di solito già assolute dal sistema AVM, ove presente.

In questa circostanza si pone l'interrogativo di procedere alla integrazione tra i due sistemi, con gli evidenti vantaggi di una migliore "pulizia" dovuta alla minimizzazione del numero dei componenti, o alla sovrapposizione dei medesimi, soluzione questa che consente una minore interdipendenza e quindi una maggiore flessibilità nella probabile ipotesi in cui siano richieste modifiche evolutive ad ambedue i sistemi.

La soluzione dell'integrazione implica che almeno uno dei due sistemi abbia un sufficiente grado di reale "apertura", ossia che disponga di tutte le

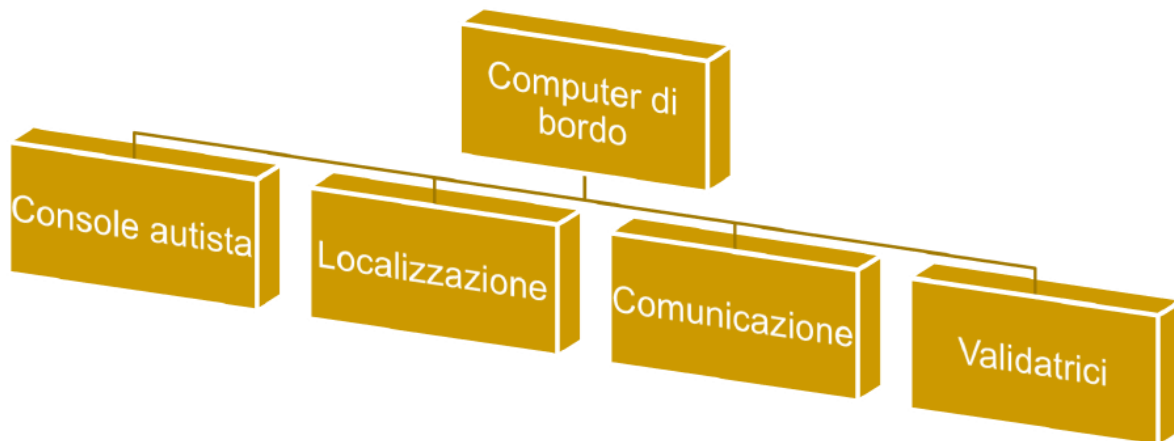
Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	7/67

necessarie informazioni o addirittura della possibilità di personalizzazione del relativo software, come sarà approfondito nel seguito.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	8/67

4. Architetture del Sistema Di Bordo

4.1 Le architetture di base



Per quanto possano differire le soluzioni proposte dai vari costruttori, si identificano di solito due tipi di architettura di base:

- con computer di bordo, detta anche ad "elaborazione concentrata" (fig. 1);
- senza computer di bordo, e quindi ad "elaborazione distribuita" (fig. 2).



Si osserva che anche in questa seconda ipotesi, talora, uno dei componenti del sistema distribuito finisce per assumere le funzioni di computer di bordo, mancando però una "black box" specificamente destinata alla sola funzione di processo.

Non sussistono, a priori, dei motivi per preferire una delle due soluzioni, anche se in linea di massima la riduzione del numero di componenti dovrebbe

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	9/67

implicare una riduzione dei costi di acquisto, di installazione e di manutenzione. E' quindi dovuta, in ogni caso, una valutazione complessiva della singola soluzione, stante anche un elevato livello di variabilità delle stesse, spesso conseguente alle notevoli possibilità oggi offerte dall'integrazione dell'elettronica digitale. Non è infrequente, infatti, che la sola elettronica di servizio di un sotto apparato potrebbe essere da sola potenzialmente sufficiente alla gestione di tutto il SDB.

4.2 Componenti del Sistema Di Bordo

Sono componenti del Sistema Di Bordo:

- una o più validatrici;
- la console autista eventualmente con funzioni di la vendita/ricarica a bordo;
- gli apparati di comunicazione;
- il computer di bordo;
- eventuali accessori.

Ad esclusione delle validatrici gli altri apparati possono essere o meno presenti. Solo in rari casi non sono presenti le validatrici ma solo l'unità per la vendita a bordo, cui vengono attribuite anche funzioni di convalida.

Gli apparati dovrebbero possedere le seguenti caratteristiche:

- **apertura** - una architettura aperta consente lo sviluppo e l'aggiornamento software anche a soggetti differenti dal costruttore;
- **interfacciabilità** - l'interfacciamento con altri apparati non necessariamente della stessa marca, deve essere possibile e non troppo difficoltoso;
- **evolubilità** - capaci di evolvere, anche in tempi successivi, verso le tecnologie più adeguate, grazie ad una struttura modulare.

Gli apparati sono descritti singolarmente nei capitoli successivi.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	10/67

4.3 Esempi di Sistemi Di Bordo reali

4.3.1 Esempio 1 – CTP Napoli (TSF)

Il primo esempio riporta un sistema di bordo piuttosto completo interamente dedicato alla applicazione nel Sistema di Bigliettazione Elettronica, ossia non integrato con un sistema AVM.

In esso si riconoscono tutti gli elementi fondamentali del Sistema Di Bordo, tranne quella del computer di bordo, non presente, le cui funzioni sono assolve dagli altri apparati in maniera distribuita.

In esso sono presenti le seguenti funzioni:

- **funzione di validazione** per titoli magnetici e contactless (Calypto);
- **funzione di comunicazione a breve raggio** ad alta velocità con l'utilizzo di un comunicatore senza fili ad alta velocità di tipo intelligente, in accordo allo standard IEEE 802.11 (WI-FI).
- **funzione di localizzazione del mezzo** con ricevitore GPS per il cambio zona automatico e riconoscimento della fermata.
- **funzione di interfaccia con l'autista** con l'impiego di una console autista di piccole dimensioni, di tipo intelligente e programmabile, con estesa memoria (256M byte), display alfanumerico e tastiera 12 tasti.

Il sistema è capace di gestire anche i turni macchina e le corse, in maniera del tutto automatica e, opzionalmente, di accumulare i dati dei passaggi alle fermate per l'analisi differita della regolarità del servizio.



Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	11/67

4.3.2 Esempio 2 – APM Perugia (Siemens Italdata)

Particolarità del caso presentato è la molteplicità di funzioni attribuite alla validatrice, che svolge anche le funzioni di localizzazione e di gestione della comunicazione GPRS, implementando i protocolli Internet TCP/IP, PPP ed FTP.

Sono quindi assolte le funzioni di validazione magnetica e contactless, di localizzazione e di comunicazione a lungo raggio, mentre è assente la funzione di interfaccia autista.

L'impostazione della linea avviene ad opera di una speciale smart card consegnata all'autista e presentata alla validatrice.

Anche in questo caso il computer di bordo è assente come elemento indipendente.

4.3.3 Esempio 3 – Città di Gaziantep, Turchia (Olivetti)

Anche in questo esempio, alla validatrice (magnetica + contactless MIFARE) sono attribuite funzioni inusuali; oltre alla gestione della comunicazione a lungo raggio GPRS, già vista nel caso precedente, la validatrice assolve la funzione di interfaccia con l'autista che può, attraverso la medesima, impostare la linea ed il verso di percorrenza, essendo la macchina ubicata in prossimità del posto di guida,.

Tra le particolarità, anche quella di poter ricevere messaggi dal Centro di Supervisione e Controllo.



4.3.4 Esempio 4 - Autobus Unico Campania/EAV (IPM, T&T ecc.)

Sistema utilizzato su molti nuovi autobus in consegna nella Regione Campania per il Sistema di Bigliettazione Elettronica Unico Campania. Il sistema, di tipo classico, prevede l'interfacciamento delle validatrici al sistema AVM installato a bordo.



Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	12/67

5. La validatrice

5.1 Generalità

In un Sistema di Bigliettazione Elettronica, le validatrici rappresentano certamente il "cuore" del Sistema Di Bordo e tutti gli altri componenti del medesimo sono in qualche modo finalizzati a consentire il loro regolare funzionamento.

Come evidente, le validatrici dovrebbero consentire il processo di tutti i titoli, presenti e futuri, del Sistema di Bigliettazione Elettronica, e, auspicabilmente, almeno nei periodi transitori, di quelli passati.

In termini pratici, questo si traduce in genere in:

- biglietti cartacei tradizionali;
- biglietti cartacei con banda magnetica;
- smart card di tipo contactless;
- smart card di tipo a contatti.

Difficilmente nello stesso Sistema di Bigliettazione Elettronica coesisteranno tutti questi tipi di TDV e quindi le caratteristiche della validatrice non risulteranno in pratica così ampie.

5.2 Caratteristiche comuni

La figura sottostante riporta lo schema a blocchi di una ipotetica validatrice elettronica nella quale siano presenti tutti i sotto sistemi di convalida in precedenza elencati, che, come affermato, raramente saranno contenuti nello stesso modello di validatrice.

Poiché in questi appunti ci si riferisce sempre a "validatrici" e non già a semplici obliterate cartacee, si descrivono qui di seguito le caratteristiche comuni ai vari tipi capaci di processare i titoli sopra elencati, elencando le differenze per le varie specializzazioni in paragrafi separati.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	13/67

5.2.1 Interfaccia utente

L'interfaccia utente delle validatrici è costituita dal display, le luci di segnalazione, l'avvisatore acustico e la tastiera, ove presente.

5.2.1.1 Display

Il display è di solito del tipo a carattere. La maggior parte delle macchine in commercio impiega il classico display LCD da 2 righe di 16 caratteri cadauna con illuminazione a LED che offre il vantaggio di una ottima visibilità in tutte le condizioni di illuminazione, sia per avere i caratteri di grandi dimensioni (8 mm), sia per la tecnologia costruttiva impiegata che lo rende ben visibile tanto al buio quanto in pieno sole. Su alcune macchine è invece installato un display grafico di piccole dimensioni (128x64 pixel) retroilluminato a LED. Non è comune un display grafico di dimensioni maggiori e tantomeno una interfaccia grafica (GUI) come ad esempio quella di Windows o di Linux.



Il display 2x16 utilizzato in molte validatrici sormontato da tre luci di segnalazione.

5.2.1.2 Luci di segnalazione

Le indicazioni del display sono sempre accompagnate da segnalazioni con luci luminose molto visibili, almeno una verde ed una rossa per segnalare l'esito positivo o negativo dell'operazione di convalida. In certi casi, di solito nelle validatrici magnetiche, può essere presente una terza luce di colore giallo per indicare che la transazione è in corso. Le luci sono sempre realizzate per mezzo di diodi LED colorati.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	14/67

5.2.1.3 Avvisatore acustico

L'esito della transazione è sempre segnalato anche da un segnale acustico, ottenuto in maniera piuttosto variegata. Il trasduttore elettroacustico più utilizzato è di tipo piezoelettrico, con emissione di suoni differenziati in tonalità o durata. Alcuni modelli dispongono invece di un altoparlante e, in qualche caso, anche di un generatore capace di riprodurre file sonori .wav o .mp3.

5.2.1.4 Tastiera

La tastiera per l'interazione con l'utente assume varie forme e dimensioni; è spesso opzionale in quanto di solito non facilmente accettata dall'utenza, in particolare su macchine di tipo contactless ove non è facile "prendere possesso" del terminale di convalida e quindi la digitazione eseguita corre il rischio di essere "rubata" da un altro viaggiatore.



Le filosofie in merito sono principalmente le seguenti:

- **nessuna tastiera** - ogni operazione prevista dal Sistema di Bigliettazione Elettronica avviene senza la necessità di compiere operazioni manuali da parte dell'utente.
- **tastiera monofunzionale** - una tastiera con pochi tasti (4 al massimo) ove a ciascun tasto è associato un significato prestabilito. Es. "Info" per la consultazione del titolo, "+Pers" per la convalida multipla per più persone ecc. Le indicazioni sono di solito riportate in forma di pittogramma per risultare comprensibili anche a viaggiatori di lingue diverse, per quanto sia difficile con una semplice icona trasmettere compiutamente il significato del tasto.
- **tastiera polifunzionale** - una tastiera con pochi tasti (4 al massimo) ove i tasti consentano di effettuare scelte tra varie opzioni di menu. I tasti possono avere il significato di "+", "-", "Annulla" e "Confer-

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	15/67

ma" e possono essere posti in prossimità del display per indicarne la funzione tramite il display stesso ("soft key").

- **tastiera funzionale e numerica** - si tratta di una completa tastiera numerica corredata da 12 o 16 tasti per digitazione di codici (es. identificativo della località di destinazione)

Nella foto precedente: una validatrice con tastiera polifunzionale e numerica.

5.2.2 Unità di processo

In assenza di una interfaccia grafica evoluta, si può affermare che ogni tipo di processore di recente generazione e con estesa capacità di indirizzamento (alcuni mega byte) è ampiamente adeguato ad assolvere tutte le funzioni richieste per il funzionamento della validatrice.

Le validatrici presenti sul mercato di solito usano nel proprio motore architetture di tipo "embedded" e quindi non un PC industriale. Questa soluzione presenta i seguenti vantaggi:

- rende assai più snella e producibile l'elettronica, per la quale è richiesta di solito la disponibilità di ricambi per almeno 10 anni; un periodo di tempo molto difficile da traguardare per le architetture di tipo PC in continua e mutevole evoluzione;
- rende assai più snella l'organizzazione del software, che può meglio sfruttare la piattaforma hardware a propria disposizione e conseguire una maggiore stabilità grazie anche alla minore dimensione del codice.

Di conseguenza all'architettura embedded, le memorie hanno dimensioni non particolarmente elevate: 2M byte di RAM e 512K/1024K di FLASH sono dimensioni tipiche. La modesta dimensione della RAM fa sì che sia possibile implementarla con tecnologia statica (SRAM) e mantenerla in costante alimentazione ad opera di una batteria tampone. E' quindi è più corretto definirla come NVSRAM (Non Volatile Static RAM).

5.2.3 Periferiche di massa

In qualunque architettura risulta particolarmente conveniente che la validatrice disponga di



Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	16/67

una estesa memoria riservata all'archiviazione, ove conservare i file di configurazione ricevuti dal Sistema di Bigliettazione Elettronica o quelli contenenti le transazioni di convalida ad esso destinati.

Questa è in certi casi assente o costituita da un modulo rimovibile appositamente progettato, ma la soluzione preferibile è certo l'adozione di un modulo di memoria da PC, a volte di tipo Compact FLASH, altre, preferibilmente, di tipo Secure Digital/Multi Media Card (vedi immagine), più attuali. Queste piccole schede, di ridotte dimensioni, sono largamente usate in molti dispositivi portatili (macchine fotografiche, navigatori, telefoni, riproduttori di musica ecc.) ed hanno costi ridotti e grandi capacità di memoria da (256M in su). Possono inoltre essere montate sui normali PC; molti portatili dispongono allo scopo di un appropriato connettore.

5.2.4 Le interfacce

Ogni validatrice dispone di un certo numero di interfacce per l'interconnessione della medesima con il Sistema Di Bordo o con eventuali accessori esterni.

Tra di esse si annoverano certamente le classiche seriali asincrone come la RS-232 e la RS-485, che resta tutt'oggi la "dorsale" più largamente usata sugli autobus. Più raramente viene usato il CAN bus, che pur tipico dell'ambiente "automotive", viene di solito riservato alle centraline elettroniche più tipiche del veicolo. Infrequente è l'uso di reti Ethernet, sia per la necessità di impiegare hub o switch per collegare tra loro i vari apparati, sia per i modesti volumi di dati solitamente scambiati.

In certi casi la validatrice può includere al proprio interno accessori che la mettono in grado di comunicare a distanza direttamente.

[per maggiori informazioni riferirsi al modulo del corso "Tecniche e sistemi di comunicazione"]

5.2.5 L'alimentatore e le batterie

L'alimentatore è quel circuito che, a partire dalla tensione di bordo del veicolo, genera le varie tensioni richieste per il funzionamento dei circuiti elettronici (ad esempio +5V, +3,3V ecc.).

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	17/67

In passato gli alimentatori erano di tipo dissipativo e la tensione in eccesso veniva smaltita sotto forma di calore. Oggi si usano di prevalenza circuiti a commutazione (switching) che aprono e chiudono, a frequenza elevata, un interruttore allo stato solido che afferrisce ad un condensatore, in modo da mantenere costante la tensione ai suoi estremi al valore desiderato. Gli alimentatori a commutazione risultano quindi assai più convenienti dal punto di vista energetico ed hanno una ridottissima emissione di calore.

Fa parte del circuito di alimentazione anche il "supervisore dell'alimentazione". Questo circuito ha lo scopo di monitorare continuamente la tensione in ingresso generando un segnale di allarme alla CPU qualora questa scenda al di sotto di un certo livello per poter predisporre le necessarie contromisure in caso di interruzione, eventualità comunque remota su di un autobus.

Sempre nell'alimentatore è presente la batteria tampone che provvede a mantenere l'alimentazione alla memoria NVSRAM e all'orologio calendario (detto anche RTC, Real Time Clock), di cui ogni validatrice è dotata.



Contrariamente a quanto si ritiene comunemente, l'impiego di batterie ricaricabili per questa funzione non è raccomandato, in quanto il permanente stato di ricarica provoca una riduzione della loro vita utile. Assai preferibile l'adozione delle più costose batterie al litio non ricaricabili (immagine a lato) che, nelle condizioni di normale utilizzo, possono raggiungere e superare la durata di dieci anni in servizio.

5.2.6 Marcatura CE

La marcatura CE è un contrassegno che deve essere apposto su determinate tipologie di prodotti per attestarne la rispondenza a tutte le direttive comunitarie ad esso applicabili. L'apposizione del marchio è



Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	18/67

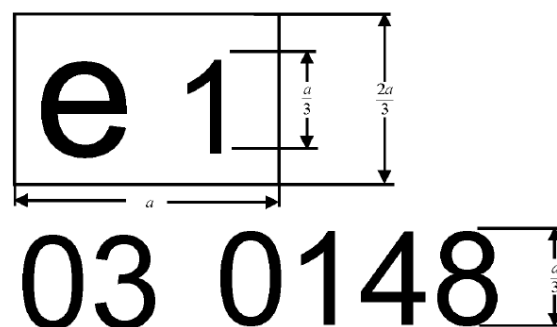
prescritta per legge per poter commercializzare il prodotto nei paesi aderenti allo Spazio Economico Europeo (SEE). La presenza del marchio CE garantisce ai consumatori che il prodotto abbia le necessarie caratteristiche di sicurezza d'uso.

Esempi di alcune direttive richieste per il marchio CE sono la direttiva bassa tensione, la direttiva macchine, la direttiva compatibilità elettromagnetica, ecc.

Il simbolo CE ufficialmente non è un'abbreviazione, anche se probabilmente ha origine dal francese Communauté Européenne o Conformité Européenne.

5.2.7 Omologazioni

Le norme inerenti agli apparati installati sui mezzi di trasporto sono piuttosto severe. Mentre per gli apparati di uso comune la conformità alle direttive di compatibilità elettromagnetica viene semplicemente dichiarata dal relativo costruttore, per gli altri apparati di bordo, è prevista l'omologazione in base alla



$a \geq 6 \text{ mm}$

normativa 2004/104/CE, eseguita ad opera di un organismo accreditato, come, ad esempio, il Ministero dei Trasporti che rilascia un numero di omologazione da apporre assieme al marchio previsto (figura). Per l'Italia il marchio è "e3".

La 2004/104/CE è relativa alla sola direttiva sulla compatibilità elettromagnetica; l'applicazione del marchio CE richiede quindi anche la conformità a tutte le altre direttive applicabili.

5.2.8 Organizzazione del software

Nella maggior parte dei moderni prodotti elettronici moderni, è compito dell'hardware, ossia della parte "fisica" dell'apparato, quello di rendere "possibili" le varie funzioni previste, di fatto poi attuate dal software, ossia dall'insieme dei programmi che controllano il funzionamento del pro-

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	19/67

cessore. Le validatrici non fanno eccezione a questa regola, e anche in questo caso il ruolo del software è preponderante, anche in considerazione della complessità dei moderni Sistema di Bigliettazione Elettronica.

La politica di sviluppo del software differisce sensibilmente da costruttore a costruttore; in certi casi (sistemi "chiusi") il processo di creazione dei programmi è riservato alla Casa che fornisce al Cliente solo gli applicativi già pronti ed è l'unica titolata ad eseguire modifiche o aggiunte.

In altri casi (sistemi "aperti") il Costruttore rende disponibile il cosiddetto "Software Developer Kit" (SDK), un insieme di elementi comprendenti non solo gli strumenti, quali compilatori di linguaggi ad alto livello, ma anche l'insieme delle informazioni e delle librerie che rendono possibile il completo controllo della macchina da parte di sviluppatori indipendenti. Questa soluzione, ove adottata, rende possibile, oltretutto, l'uso combinato, nello stesso sistema, di TDVE e di apparati di marche o di modelli diversi e al tempo stesso, la realizzazione da parte di System Integrator di procedure applicative gestionali relativamente indipendenti dall'hardware.

L'operazione di aggiornamento del software della validatrice è una operazione piuttosto critica, in considerazione del numero relativamente sempre elevato di unità e del fatto che spesso gli autobus si trovano in servizio per la maggior parte della giornata.

Vari modelli di validatrice prevedono una o più delle seguenti forme di aggiornamento del software:

- aggiornamento previa riprogrammazione del chip di memoria FLASH. L'operazione richiede lo smontaggio della macchina, l'estrazione del chip, il suo inserimento in una macchina apposita, la reinserzione ed il rimontaggio. Si tratta di una tecnica assolutamente obsoleta.
- aggiornamento previo collegamento alla validatrice di un PC o di un apposito apparato.
- aggiornamento automatico con inserzione di un modulo di memoria pre-programmato, ad esempio un modulo Multi Media Card.
- aggiornamento remoto attraverso la linea di comunicazione RS-485 e quindi ad opera del Sistema Di Bordo. Questo metodo consente l'aggiornamento remoto della flotta senza intervento manuale su ogni autobus.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	20/67

- disponibilità di un accessorio appositamente previsto (es. modem GPRS) per l'aggiornamento remoto della validatrice senza necessità di altri apparati intermediari.

5.2.9 La configurabilità

La scrittura di applicazioni personalizzate può costituire un impegno rilevante, sia per la necessità di disporre di personale adeguatamente preparato, sia perché è necessario apprendere e comprendere molti dettagli interni dell'apparato.

Alcuni costruttori offrono quindi soluzioni intermedie in cui, attraverso una serie di tabelle e di parametri, sia comunque possibile un buon livello di controllo dell'apparato.

E', ad esempio, da tempo partito un progetto denominato VCL, acronimo di *Validator Configuration Language*, il cui obiettivo è quello di definire un livello astratto di interfaccia tra i sistemi e gli apparati di validazione che semplifichi quanto possibile la realizzazione di sistemi misti e integrati.

I file di VCL sono scritti in formato testuale; essi possono quindi essere letti e modificati con un normale text editor (es. Notepad di Windows). Questo garantisce importanti vantaggi:

- gli sviluppatori dei sistemi possono facilmente verificare la funzionalità degli stessi semplicemente esaminando i file prodotti dalle procedure applicative che essi realizzano, prima di tentare il trasferimento agli apparati reali. Basta una semplice analisi per controllare gli elaborati;
- allo stesso modo, possono facilmente costruirsi file di attività "simulati" con le registrazioni delle transazioni, modificandoli di volta in volta per provare le varie possibili condizioni;
- i costruttori di apparati possono similmente provare gli stessi indipendentemente dai sistemi;
- in sistemi minori o nelle fasi transitorie, è possibile e semplice creare manualmente le configurazioni o correggere quelle esistenti per aggiungere nuovi titoli di viaggio o cambiare quelli già in uso.

Con VCL si possono ad esempio definire:

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	21/67

- mappe dati
- titoli di viaggio
- regole di processo per i titoli di viaggio
- regole per i trasbordi
- fasce orarie
- regole di stampa per i biglietti cartacei
- zone tariffarie ed insiemi di zone
- tracciati record per i file di attività
- parametri operativi
- ecc.

5.3 Riepilogo

In questo capitolo sono state fin qui analizzate le caratteristiche comuni ai vari tipi di validatrice, e quindi alle validatrici per:

- biglietti cartacei tradizionali;
- biglietti cartacei con banda magnetica;
- smart card di tipo a contatti;
- smart card di tipo contactless.

Nei paragrafi successivi saranno invece analizzate le caratteristiche specifiche di ciascuna di esse.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	22/67

6. La validatrice per titoli tradizionali

L'uso dei biglietti cartacei tradizionali è ancora molto diffuso in ambito nazionale anche in parallelo a TDV elettronici, per cui non mancano, nel panorama commerciale, modelli di validatrici elettroniche capaci di processare anche questo tipo di biglietto per mezzo della stampigliatura di data, ora e di qualche altra informazione.



In certi casi è previsto anche il taglio progressivo dell'angolo del biglietto, in modo da consentire la realizzazione di carnet multi corsa con la linea di stampa di convalida via via spostata dal bordo verso il centro del biglietto stesso.

Non mancano infine modelli di validatrice capaci di eseguire la lettura di un codice a barre dal biglietto prima di eseguire la stampa di convalida; questo consente di omettere la convalida qualora il biglietto non risulti per qualche motivo accettabile (es. fuori della zona ammessa) e di tenere traccia delle validazioni effettuate registrando i numeri di serie o le tipologie dei biglietti.

Nell'immagine precedente: una validatrice per titoli cartacei capace di evolvere al processo delle smart card a contatti e contactless.

Nell'immagine precedente: una validatrice per titoli cartacei capace di evolvere al processo delle smart card a contatti e contactless.

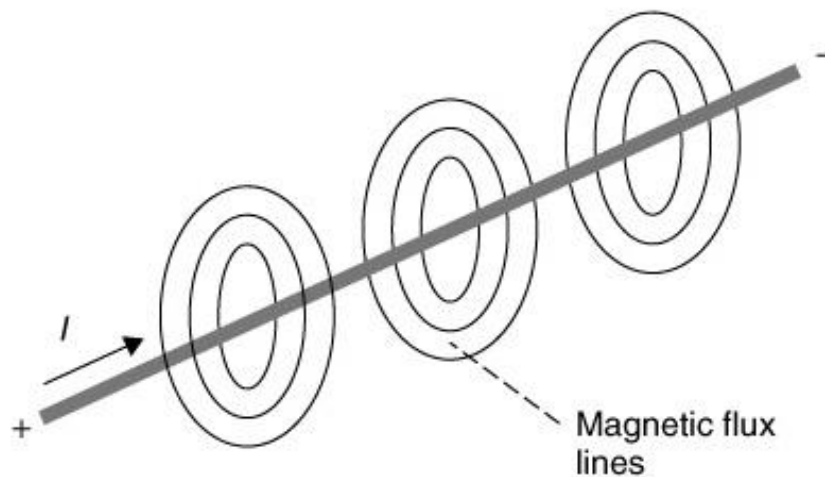
Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	23/67

7. La validatrice magnetica

7.1 Principi della registrazione magnetica

La registrazione magnetica è basata sulle leggi fisiche dell'elettromagnetismo scoperte dallo scienziato inglese Michael Faraday nella prima metà del 1800 (vedi nota nel par. 9.1).

Sul biglietto magnetico è riportata una striscia ("stripe") costruita con una vernice che contiene in sospensione particelle simili a minuscoli magneti permanenti (ossidi di ferro).



Un conduttore percorso da una corrente elettrica induce attorno a sé un campo magnetico che può essere impiegato per orientare in maniera concorde e stabile i poli Nord/Sud dei suddetti magneti.

Nel caso della validatrice, questo conduttore avvolto in più spire è racchiuso in un particolare dispositivo detto "testina magnetica" che opera in stretta prossimità con la *stripe*.

Invertendo la direzione della corrente e muovendo al contempo il biglietto è quindi possibile orientare sequenzialmente le particelle in direzione Nord/Sud o Sud/Nord e quindi, con opportune convenzioni, registrare degli "1" o degli "0" logici, detti "bit", da "binary digit".

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	24/67



Una testina magnetica

7.2 Tecniche per la lettura

Per la lettura si sfruttano ancora le leggi dell'elettromagnetismo che stabiliscono che variazioni temporali del flusso di un campo magnetico concatenato con un circuito elettrico generano un campo elettrico indotto in grado di dar vita ad una forza elettromotrice.

In pratica muovendo un magnete permanente in prossimità di una spira conduttrice, si induce in essa una tensione.

La lettura del biglietto magnetico avviene quindi usando una seconda testina magnetica (spesso fisicamente coincidente con la prima) e muovendo il biglietto magnetico dinnanzi ad essa. Il movimento dei minuscoli magneti provocherà l'induzione di una tensione nella testina e questa, amplificata e processata da opportuni circuiti, consentirà di eseguire la lettura delle informazioni in precedenza registrate.

Si osservi che un campo magnetico costante non dà origine al fenomeno dell'induzione, e quindi, per leggere i biglietti magnetici, è necessario comunque un movimento relativo tra testina e stripe. Questo implica che la validatrice magnetica deve prevedere un motore nonché i necessari cinematici che garantiscano la movimentazione del biglietto, con tutte le conseguenze del caso in termini di complessità costruttiva ed operativa.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	25/67

7.3 Normative internazionali

Le dimensioni dei biglietti, delle stripe e le altre caratteristiche cui deve sottostare la registrazione magnetica dei biglietti sono regolate da normative internazionali quali la ENV-753 cui si rimanda per dettagli ulteriori.

7.4 Codifica ed organizzazione dati

La registrazione avviene di solito con la tecnica F/2F, registrando una transizione per lo "0" e due per lo "1".

I dati registrati sono costituiti da una serie di bit, tipicamente circa 200 nella densità singola e 400 in quella doppia. Essi vengono organizzati in gruppi di 8 bit detti "byte" per un più facile utilizzo, anche se la loro suddivisione è talora non univoca, nel senso che validatrici di marche diverse o progetti diversi, ancorché utilizzanti le stesse validatrici, usano diversi criteri di raggruppamento.

Già con la codifica più comune in densità singola è possibile, in 25 byte, la implementazione di un buon numero di diversi tipi di TDV. Si osservi come sia possibile compensare la modesta capacità di memoria del biglietto con un maggiore sfruttamento delle caratteristiche di memoria della validatrice, ricorrendo a tabelle parametriche che forniscano al software una adeguata definizione del processo del titolo.

7.5 Codici di controllo

In coda alla traccia viene riservato lo spazio per la scrittura di un codice numerico di controllo, spesso di un solo byte, che può essere calcolato con criteri prestabiliti, alcuni semplici, altri più complessi, per assicurarsi circa la correttezza dei dati appena letti. Il più semplice è quello del cosiddetto "checksum" (somma di controllo), in cui il codice di controllo è costruito eseguendo la somma logica (XOR) di tutti gli altri byte, eventualmente a sommarsi con una costante prestabilita. In altri casi si ricorre ad esempio al Cyclic Redundancy Check (CRC), un algoritmo più complesso che offre però maggiore sicurezza.

Non sempre i codici di controllo garantiscono al 100% la correttezza dei dati, specie con l'uso del checksum, ma la probabilità di incorrere in er-

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	26/67

rori che si compensano è comunque molto bassa ed il metodo è universalmente ritenuto accettabile in relazione all'esigenza. Eventuali improbabili errori che superassero il controllo verrebbero poi facilmente bloccati dai successivi processi del software.

7.6 Architettura generale

Le validatrici per titoli magnetici prevedono di solito un canale abbastanza lungo (20-30 cm) per eseguire la movimentazione e la stampa di convalida. Per questo motivo esso viene di solito disposto verticalmente, con una unica bocchetta utilizzata tanto per l'introduzione che per la restituzione del biglietto. La bocchetta viene spesso posta dalla parte superiore della macchina per facilitare l'utenza, in particolare quella più svantaggiata, anche se non mancano esempi in cui la bocchetta si trova invece nella parte inferiore, per ridurre il rischio di introduzione di corpi estranei.

7.7 Sequenza operativa

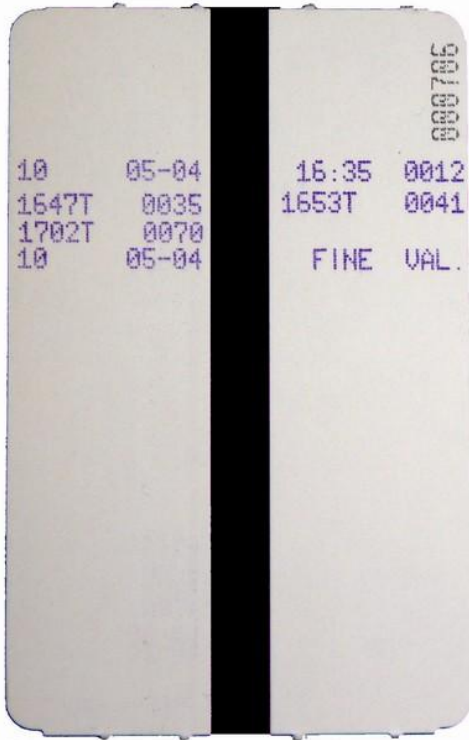
La sequenza delle operazioni di convalida è di solito la seguente:

- lettura della banda magnetica;
- controllo codice di sicurezza ed espulsione in caso di controllo negativo;
- controllo dati di viaggio ed espulsione in caso di controllo negativo;
- stampa di convalida, per consentire la verifica a vista da parte del viaggiatore e del personale di ispezione;
- scrittura dei dati aggiornati (es. con il numero di corse valide decrementato)
- rilettura dei dati scritti;
- espulsione.

In considerazione dell'elevato livello di affidabilità raggiunto dalle moderne validatrici, l'operazione di rilettura è di solito opzionale e non viene effettuata, anche perché rallenta alquanto la convalida.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	27/67

7.8 Posizione della banda magnetica sul biglietto e stampa di convalida



L'uso di biglietti a banda centrale è in genere da preferirsi, in quanto consente l'introduzione indifferente nei due versi (0° o 180°). I modelli più evoluti di validatrice provvedono automaticamente a ruotare la stampa e ad adattarne la posizione in modo che non siano rilevabili differenze nell'ordine delle convalide, ossia come se il biglietto fosse stato sempre inserito nello stesso verso.

Nel caso di biglietti con banda laterale, invece, il verso di inserzione risulta obbligato, a meno che non venga fatto uso di due testine, una per ciascun lato, con riconoscimento del verso di inserzione e selezione automatica.

Soluzioni "ogni verso", che richiederebbero 2 testine nel caso della banda centrale e addirittura 4 nel caso di quella laterale, non trovano casi noti di implementazione.

La stampa è di regola del tipo ad impatto di aghi, con nastro inchiostroato sostituibile. Più raramente di tipo termico, anche per il maggiore costo dei biglietti.

Nell'immagine precedente: biglietto magnetico con banda centrale e stampe di convalida.

7.9 Sezione elettronica

La parte elettronica della validatrice magnetica non presenta particolari caratteristiche rispetto ad una validatrice generica se non per la presenza di circuiti specializzati per il processo del biglietto magnetico.

In particolare sono presenti i seguenti circuiti:

- **lettura magnetica** - è richiesto un amplificatore differenziale per il segnale proveniente dalla testina, un circuito squadratore ed un deco-

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	28/67

dificatore in grado di separare i dati dal clock. La ricostruzione della stripe e la suddivisione in gruppi avviene ad opera della CPU.

- **scrittura magnetica** - eseguita di solito attraverso un ponte ad "H" che consente di invertire la corrente che percorre l'avvolgimento della bobina. La corrente può essere regolata in varie maniere, ad esempio attraverso una modulazione a periodo d'impulso (chopper).
- **controllo del motore** - il motore per il movimento del biglietto è di solito del tipo passo-passo che consente buone prestazioni con un consumo di corrente molto limitato. In alcuni modelli si ricorre invece a motori in corrente continua. I circuiti elettronici sono del tipo adeguato al modello del motore impiegato.
- **lettura sensori** - la presenza ed il movimento del biglietto magnetico vengono rilevati attraverso sensori, di solito di tipo fotoelettrico, costituiti da una sorgente di emissione, visibile od infrarossa, e da un fototransistore. E' importante che i sensori siano di ottima qualità; sensori scadenti sono pronti a sporcarsi o a fornire false letture.

7.10 Caratteristiche critiche delle validatrici magnetiche

Nella scelta di una validatrice magnetica è opportuno soffermarsi su alcune specifiche peculiarità oltre che su quelle più ovvie come la qualità costruttiva, la robustezza ecc.

La più importante è certamente la qualità della scrittura dei dati sulla traccia magnetica. Una qualità insufficiente o comunque disuniforme è alla base dei problemi di interoperabilità che possono verificarsi a volte anche tra macchine dello stesso modello; un biglietto scritto da una macchina non risulta leggibile da una altra o viceversa.

Una validatrice che scriva dati errati è fonte di gravi problemi in un Sistema di Bigliettazione Elettronica; essa infatti "guasterà" i biglietti rendendoli illeggibili, senza che neppure l'utente stesso ne abbia nozione fino alla convalida successiva, qualora non sia stato scelto di eseguire la rilettura di controllo. In questo modo si avrà l'effetto "serial killer" e non sarà affatto facile assicurare alla giustizia la validatrice "impazzita", che continuerà a registrare regolarmente le proprie transazioni apparendo del tutto normale agli occhi del sistema centrale.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	29/67

Per questo motivo potrebbe essere opportuno far eseguire delle validazioni di prova al personale di ispezione in occasione delle visite a bordo, che, se eseguite su biglietti dotati di una codifica particolare, potranno pure risultare utili per tenere traccia dell'attività degli ispettori.

Altra importante caratteristica di una validatrice magnetica è la capacità di espellere biglietti danneggiati. Le migliori validatrici possono processare positivamente anche biglietti molto stropicciati, ma ancor più importante è che questi titoli di viaggio vengano comunque espulsi e non costituiscono quindi motivo di messa fuori servizio della macchina, restando intrappolati all'interno della medesima.

In assenza di una specifica normativa, sono quindi opportune delle prove pratiche eseguite su base intuitiva.

7.11 Considerazioni sulla sicurezza

Il biglietto magnetico, per sua natura, non offre un livello di sicurezza particolarmente elevato ma tuttavia sufficiente nella maggior parte delle circostanze, anche perché usato esclusivamente per l'ambito del Trasporto Pubblico Locale e quindi con una limitata capacità di spesa, non comparabile con quello di una carta di credito (che, ove priva del chip, ne offre comunque uno ancor più basso).

Contribuiscono alla sicurezza del biglietto magnetico importanti elementi, quali:

- la veste grafica, eventualmente arricchita da elementi accessori quali ad esempio una banda olografica;
- il fatto che le convalide sono riportate a stampa e che la verifica avviene a vista da parte di personale specializzato;
- la presenza del numero di serie sulla banda magnetica che rende possibile al sistema centrale il rilevamento di una molteplicità di biglietti con lo stesso numero nel circuito di utilizzo e quindi il loro inserimento nella "lista nera" dei titoli proibiti.

Per questi motivi non viene di solito prestata particolare attenzione alla sicurezza della codifica magnetica, che generalmente non viene nemmeno crittografata, in quanto i dati, crittografati o meno, passerebbero comunque indenni attraverso un processo di semplice duplicazione.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	30/67

7.12 Caratteristiche per l'interoperabilità

Sulla base di quanto fin qui osservato, per rendere interoperabile un TDV magnetico è necessario conoscere:

- la tecnica utilizzata per la codifica;
- l'algoritmo per il calcolo del codice di controllo;
- l'algoritmo per il raggruppamento dei bit in numeri;
- la semantica dei vari campi (chiamata anche "data map") e le relative regole di processo, ossia le regole per la riscrittura dei campi modificati in seguito alla avvenuta transazione.

Nell'immagine a destra: una validatrice magnetica molto diffusa in Italia dotata anche di unità per il processo delle carte contactless.

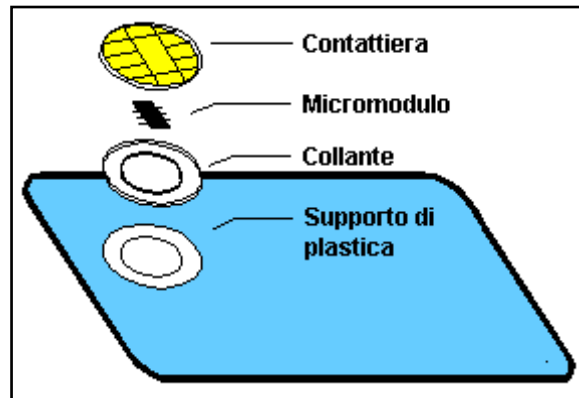


Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	31/67

8. La validatrice per smart card a contatti

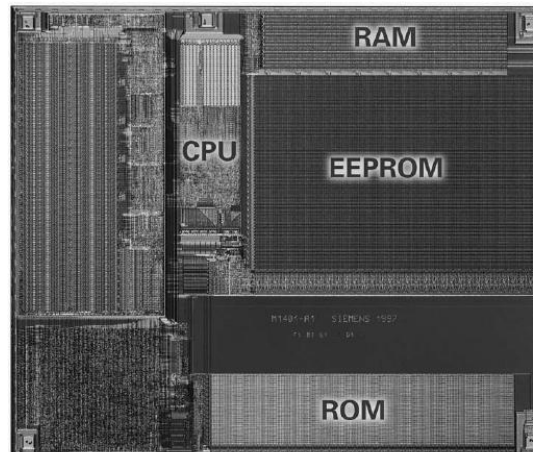
8.1 Le smart card

Le smart card sono già state sommariamente descritte in [1].

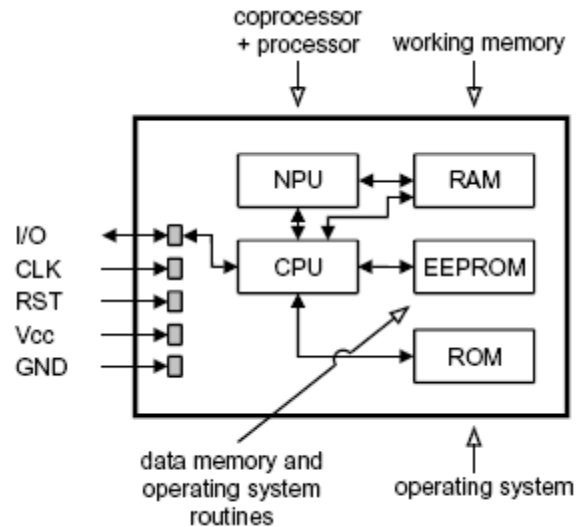


Struttura fisica della smart card

Le carte usate oggi nel trasporto pubblico sono di regola del tipo a micro-processore, ossia contengono al proprio interno un intero sistema di elaborazione, come quello illustrato, fortemente ingrandito, nella foto seguente.



Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	32/67



Schema a blocchi di una tipica carta a microprocessore

Negli ultimi anni le nuove tecniche di miniaturizzazione, mediante le quali è stato possibile produrre microchip sempre più piccoli a costi sempre più bassi, hanno consentito di realizzare smart card più potenti dotate di coprocessore crittografico e di buone capacità di memoria a costi accessibili. Tale disponibilità ha avviato una fase di notevole e sorprendente sviluppo che è partita dall'implementazione delle SIM card in ambito GSM fino ad arrivare alla realizzazione della Carta d'Identità Elettronica, delle carte di credito "intelligenti" e dei titoli di viaggio elettronici.

8.2 Sistemi a microprocessore

Per comprendere meglio l'architettura ed il modo di funzionamento delle smart card è necessario richiamare alcune nozioni circa l'architettura dei sistemi a microprocessore.

8.2.1 Il microprocessore

L'introduzione dei microprocessore, alla fine degli anni '70, ha avviato una rivoluzione nel campo dell'elettronica e delle sue applicazioni la cui "onda lunga" si estende fino ai nostri giorni.

Prima di esso, i circuiti elettronici venivano "costruiti" e "cablati" per adempiere a determinate funzioni. Ogni modifica funzionale richiedeva necessariamente la modifica fisica dei circuiti stessi.

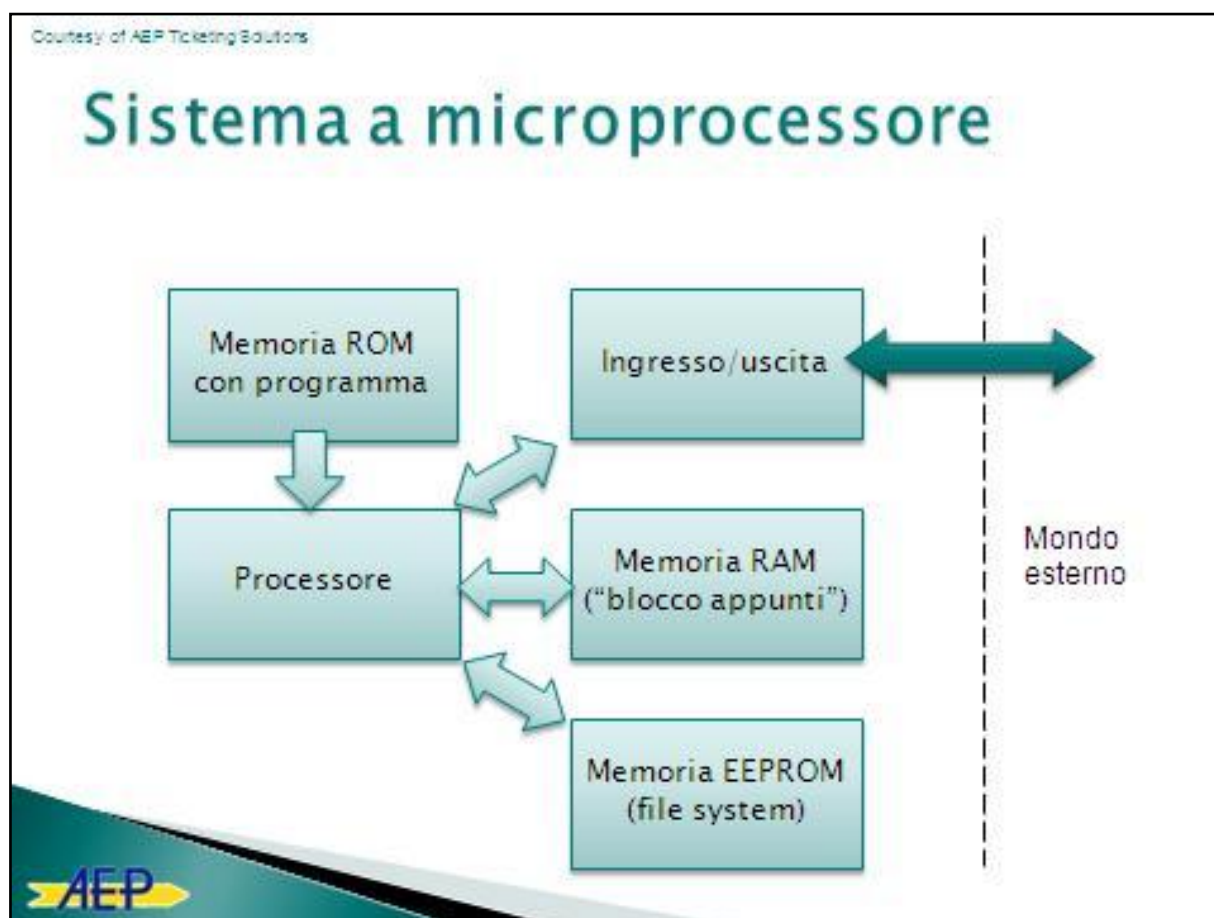
Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	33/67

Con il microprocessore tutto cambia: la logica di funzionamento del circuito non è più fornita dal circuito ma da una entità immateriale detta **programma**, ossia della codifica in istruzioni elementari di algoritmi astratti che descrivono il comportamento desiderato del sistema.

Questo ha una importante implicazione: il comportamento del sistema non è più vincolato alla complessità del circuito ma può diventare virtualmente sempre più evoluto semplicemente scrivendo programmi più complessi. Ed è da qui che parte quella impressionante evoluzione dei circuiti digitali alla quale ancora si stenta a fare abitudine.

Il microprocessore ha costituito, fra l'altro, la base ideale per la progettazione dei personal computer e del fenomeno evolutivo del software.

Le smart card a memoria sono ancora circuiti con "logica cablata"; le smart card a microprocessore sono invece, a tutti gli effetti, logicamente simili a dei computer ed il loro comportamento dipende in massima parte dal programma in esse contenuto.



La figura mostra lo schema a blocchi di un generico sistema a microprocessore. In esso sono riconoscibili:

- il microprocessore, ossia l'unità "intelligente" che decodifica ed esegue le istruzioni del programma, codificate in forma numerica. Esso è in grado di eseguire operazioni aritmetiche (es. $2+2$) o logiche (es. "se A è maggiore di B compi l'azione A1").
- la memoria contenente il programma;
- la memoria contenente dati temporanei (ad esempio i risultati parziali di certe elaborazioni);
- la memoria contenente i dati archiviati;
- i dispositivi di comunicazione o di generica interazione con il mondo esterno.

8.2.2 La memoria

In verità, quasi tutti i moderni microprocessori (ma non tutti) seguono il cosiddetto schema di Von Neumann in cui la memoria è concettualmente unica anche se contiene entità logicamente diverse come il programma ed i dati. Esistono però dei validi motivi per separare fisicamente le varie aree di memoria, in modo da poter usare per esse tecnologie differenti.

La memoria ideale dovrebbe presentare le seguenti caratteristiche:

- tempo di accesso bassissimo;
- consumo di energia minimo;
- dimensioni fisiche minime;
- ritenzione dei dati per un tempo infinito;
- costo minimo.

Purtroppo questo tipo di memoria non è ancora stato realizzato, per cui si utilizzano, a seconda delle necessità, più memorie costruite con tecnologia diversa. In particolare:

- **memoria RAM** - memoria in lettura/scrittura, veloce, riscrivibile un numero virtualmente illimitato di volte. Purtroppo è volatile: togliendo alimentazione, perde il suo contenuto e, alla accensione successiva presenta contenuti casuali. Nel caso in esame è buona per la conservazione dei dati temporanei.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	35/67

- **memoria ROM** - memoria in sola lettura, abbastanza veloce. Non potendo essere scritta se non in fase di fabbricazione torna utile per dati "fissi", ad esempio per la conservazione del programma.
- **memoria EEPROM** - memoria in lettura/scrittura, piuttosto lenta ma non volatile. E' l'ideale per ottenere un comportamento simile ad un hard disk. In essa si registrano i dati dell'utente, i contratti, i crediti, le ultime transazioni eseguite ecc.

E' opportuno valutare soltanto le specifiche funzionali e le dimensioni della memoria EEPROM della smart card. Processore, dimensioni di ROM e RAM sono ininfluenti ai fini delle performance, una volta definite le specifiche funzionali. E' consigliabile non inserirli nei criteri di scelta per non limitare inutilmente l'offerta di eventuali prodotti che siano capaci di centrare gli stessi obiettivi con tecniche più evolute.

8.2.3 Le unità di ingresso/uscita

Se un sistema a microprocessore disponesse solo di quanto fin qui esaminato sarebbe del tutto inutile, in quanto ancora privo della capacità di colloquiare o interagire con il mondo esterno. A questo scopo sono deputate le cosiddette "unità di ingresso/uscita" (I/O, ossia "input/output"). Nel caso generale, esse potrebbero essere costituite, ad esempio, da relè, ingressi per sensori ecc. Nel caso delle smart card, è presente una unica unità di I/O che viene usata per comunicare con il terminale attraverso il contatto o la radio frequenza. La comunicazione è di tipo seriale, una specie di "codice Morse", un bit dietro l'altro.

8.3 La "maschera"

Una carta, similmente ad un PC, non è in grado di compiere alcuna operazione utile finché non venga dotata di un programma.

Il produttore delle carte crea il programma che, risiedendo sulla carta, ne determina le caratteristiche funzionali. Una volta messo a punto, il programma viene passato al costruttore dei chip e trasformato in una maschera ottica per la fabbricazione della ROM. I chip, sulla base della stessa, verranno prodotti già con il programma all'interno, pronti per essere incorporati nella struttura plastica della scheda.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	36/67

Esistono oggi soluzioni alternative alla costruzione della ROM con il codice già all'interno; ad esempio esistono memorie dette OTP (One Time Programming) che consentono di inserire il programma dopo la fabbricazione del chip o addirittura della carta intera. Per motivi di abitudine, tuttavia, molti continuano a chiamare "maschera" il software della carta (il cui nome corretto sarebbe "firmware"). Da un altro punto di vista, il programma contenuto nel chip viene chiamato anche "sistema operativo".

Il termine "maschera" viene usato anche con un altro significato, ossia con quello di "tracciato dati", ossia della definizione delle modalità di registrazione delle informazioni operative all'interno della memoria o dei file.

Per evitare confusioni, è quindi opportuno evitare di usare detto termine preferendo quelli più appropriati di "firmware/sistema operativo" e "tracciato dati".

8.4 Funzioni della smart card

La smart card svolge due funzioni tra loro indipendenti, anche se collegate:

- consente di memorizzare informazioni;
- consente di assicurare che l'accesso (lettura e/o scrittura) a dette informazioni, o parte di esse, possa avvenire solo in determinate circostanze e ad opera dei soli soggetti autorizzati.

Nel caso del Trasporto Pubblico, questo significa che la carta può contenere informazioni pubbliche, ossia liberamente accessibili a chiunque (es. nome e cognome del titolare) ed altre riservate (sesso, indirizzo, credito residuo di un borsellino elettronico ecc.).

Nell'esempio, il credito del borsellino elettronico deve poter essere decrementato solo ad opera delle validatrici "autorizzate" ed incrementato solo presso le biglietterie o le rivendite tramite appositi apparati.

I meccanismi di sicurezza devono essere tali da rendere impossibile o, comunque molto difficile, l'accesso da parte di terzi alle informazioni riservate, nemmeno qualora questi siano dotati di particolari conoscenze tecniche o delle stesse apparecchiature, in marca e modello, usate dagli organi legittimamente preposti.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	37/67

8.5 La sicurezza

Queste esigenze di sicurezza vengono coperte con l'aiuto della crittografia, ossia della scienza di codificare dei messaggi in modo da renderli comprensibili solo a selezionati destinatari. Scopi della crittografia sono tra gli altri:

- **la confidenzialità**, ossia il fatto che solo i destinatari del messaggio possano leggerlo;
- **la integrità**, ossia il fatto che il messaggio crittografato venga trasmesso senza perdita di informazioni;
- **l'autenticità**, ossia il fatto che il destinatario sia in grado di verificare che il messaggio non è stato alterato nel corso della trasmissione.

A causa della sua importanza, sia in ambito militare che civile, la crittografia è una scienza particolarmente evoluta.

8.6 Il principio di Kerckhoff

E' opportuno innanzitutto sfatare un luogo comune; un sistema sicuro non deve essere basato sulla segretezza degli algoritmi usati per la codifica.

Il principio di Kerckhoff (1835-1903) stabilisce infatti che la sicurezza di un codifica crittografica debba essere basata su codici segreti detti "chiavi" e non sulla segretezza dell'algoritmo utilizzato.

8.7 Uso della crittografia per garantire la sicurezza

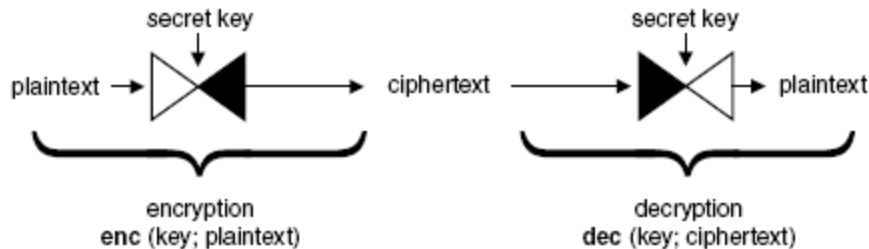
Tornando allo specifico, la transazione eseguita da una validatrice per smart card può essere protetta con tecniche crittografiche in varie fasi:

- consentendo la "mutua autenticazione", ossia il fatto che la validatrice sta "parlando" con una carta legittimata e che la carta sta "parlando" con una validatrice legittimata, ove con "legittimata" si intenda "effettivamente appartenente al Sistema di Bigliettazione Elettronica e operante nel rispetto delle sue regole";
- garantendo che lo scambio di dati avvenga in modo tale che essi, anche se intercettati, non risultino comprensibili;
- permettendo la generazione di "firme digitali" che possano garantire l'autenticità della transazione (si pensi al rischio che in un sistema

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	38/67

monetario elettronico ove uno degli operatori generasse false transazioni per crearsi crediti inesistenti).

8.8 Procedimenti crittografici



Il procedimento crittografico è usato per crittografare una serie di informazioni, dette semplicemente "testo", in un "testo cifrato" per mezzo di una "chiave".

Nei sistemi detti "simmetrici" una sola chiave è usata tanto per la codifica che per la decodifica, in quelli "asimmetrici" sono previste invece due chiavi per ciascuna di dette operazioni.

Il più noto algoritmo crittografico è il DES (Data Encryption Standard), introdotto nel 1977 da IBM assieme allo US National Bureau of Standards e definito dalla norma statunitense FIPS 46.

Esso è stato utilizzato per molti anni ma appare oggi limitato, soprattutto per la lunghezza della chiave a soli 56 bit, anche perché la grande evoluzione degli apparati per il calcolo elettronico lo ha reso pronò ad attacchi di tipo "brute force", ossia eseguiti con la prova successiva di ogni possibile chiave.

Per questo motivo si è evoluto nel triplo DES (3-DES) che, utilizzando due chiavi a 56 bit, moltiplicano il numero delle combinazioni. Lo XDES, da esso derivato, è sicuro quasi quanto il 3-DES ma più semplice da implementare.

Alla fine degli anni '90, al DES si è aggiunto l'AES Advanced Encryption Standard (AES), codificato nella norma FIPS 197, che, utilizzando chiavi a 128, 192 o 256 bit assume il nome di AES-128, AES-192 or AES-256.

La maggior parte delle carte oggi usate è in grado di compiere molti tipi di operazioni crittografiche. Spesso, risultando troppo lungo il tempo che sarebbe richiesto per eseguirle attraverso l'esecuzione del programma, esse

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	39/67

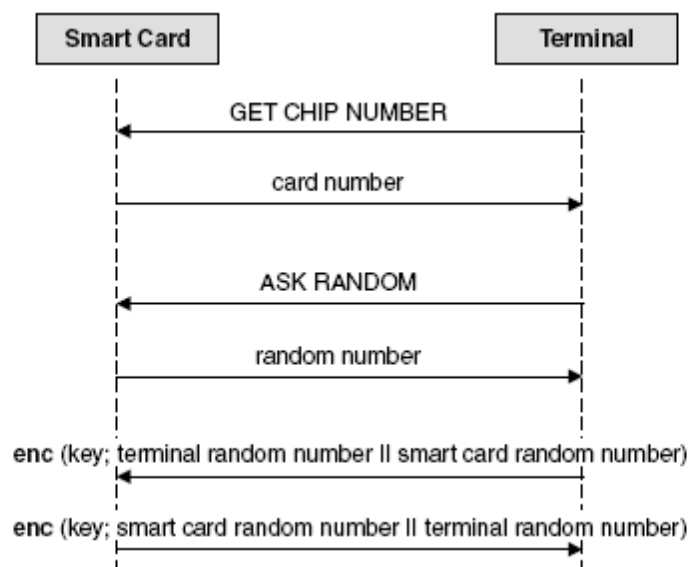
contengono al proprio interno anche un co-processore dedicato che consente di eseguirle in tempi molto rapidi.

8.9 La mutua autenticazione

E' molto importante che la validatrice e la smart card possano addivenire alla certezza che il dialogo avviene tra soggetti entrambi legittimati, ossia che dispongono delle stesse chiavi di crittografia, in entrambi inserite all'atto della costruzione.

Questo avviene tramite una operazione detta di "mutua autenticazione". Di solito (ISO 7816) questa avviene come segue:

- la validatrice richiede alla carta il suo numero seriale
- la carta lo invia
- il terminale richiede alla carta la generazione di un numero casuale;
- la carta genera un numero casuale e lo invia alla validatrice;
- la validatrice genera a sua volta un numero casuale, lo concatena con quello ottenuto dalla validatrice, lo crittografa e lo invia alla carta;
- la carta crittografa il numero ricevuto e lo ritorna alla validatrice che lo decripta, ottenendo così il numero casuale del terminale, lo ricodifica e lo invia;
- la validatrice decodifica e verifica i valori ritornati. In caso positivo la validatrice e la carta sono mutuamente autenticate.



8.10 La sessione

A parte la semplice identificazione (ad esempio, la verifica di un abbonamento), una transazione su smart card è di solito piuttosto complessa e per completarla sono necessarie spesso più operazioni di lettura e di scrittura. L'estrazione anticipata della carta prima del completamento della transazione può quindi portare al lasciare la carta in uno stato indefinito che può eventualmente pregiudicarne anche, nella peggiore ipotesi, la successiva affidabilità.

In generale questo non rappresenta un problema per la validatrice contact, in quanto la restituzione della carta è comandata dal software e l'utente non può estrarla quindi prima del completamento della transazione stesso.

Come si vedrà al capitolo successivo, nel caso di carte contactless è invece importante provvedere all'aggiornamento dei dati della carta solo alla chiusura della sessione.

8.11 La validatrice per smart card

Esistono oggi tre fondamentali motivi per decidere di adottare una validatrice per smart card:

- motivi storici, quando il Sistema di Bigliettazione Elettronica sia stato originariamente previsto per il processo di sole carte a contatti; in questi casi può risultare auspicabile che questa capacità possa essere congiunta alla convalida contactless per permettere l'evoluzione a TDV più moderni;
- motivi pratici, quando sia prevista una forte interazione tra utente e terminale di convalida, ad esempio per digitare il codice della stazione di destinazione. In questo caso il tempo complessivo della convalida è paragonabile all'operazione senza contatti ma si ha il vantaggio che la carta non deve essere tenuta dalla mano del passeggero e che la validatrice può trattenerla fino al completamento della transazione;
- motivi di promiscuità, quando debbano essere processate carte di tipo bancario per cui non è prevista una versione contactless; anche in questo caso la funzione di convalida a contatti potrebbe vantaggiosamente coesistere con quella a contactless.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	41/67

8.12 Costruzione della validatrice per smart card a contatti

Ovviamente la validatrice di smart card a contatti deve disporre di un opportuno connettore ove la carta stessa possa essere inserita.

Ai connettori con contatto a strisciamento, vengono di solito preferiti i connettori "a pinza" in cui i contatti mobili "atterranno" verticalmente su quelli della carta, per ridurre l'usura.

Nelle validatrici di questo tipo viene quasi esclusivamente utilizzato il sistema "a ritenuta"; la carta viene inserita nella fessura vincendo la resistenza di una molla a scatto. Un elettromagnete controllato dal software consente di restituire al viaggiatore la carta alla fine della transazione o qualora essa venga rifiutata.

8.13 I contatti della carta

La carta dispone di regola di 8 contatti; solo alcuni tipi più economici cercano un ulteriore risparmio riducendoli a 6.

Due contatti sono usati per l'alimentazione, uno per il RESET ed uno per lo scambio dati bidirezionale. Al contatto CLOCK deve invece essere fornita un'onda quadra a frequenza fissa come clock per la CPU della carta ed altre funzioni interne.

Un contatto (VPP) era utilizzato in passato per fornire la tensione necessaria alla scrittura nella EPROM. La tecnologia attuale consente di farne a meno, per cui è rimasto per compatibilità con le prime smart card.

Due contatti restano liberi per usi futuri (AUX1 ed AUX2).

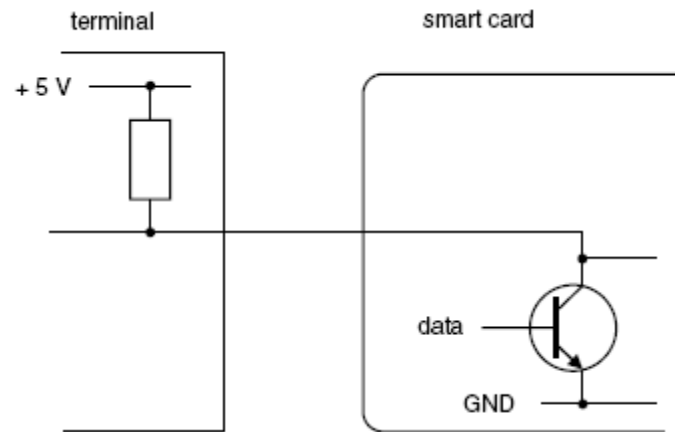
C1		C5
C2		C6
C3		C7
C4		C8

Vcc		GND
RST		Vpp
CLK		I/O
AUX1		AUX2

Vcc		GND
RST		Vpp
CLK		I/O

8.14 Gli scambi dati

Solo un contatto è usato per lo scambio dei dati; esso opera quindi in maniera bidirezionale e consente quindi solo trasmissioni in un senso o nell'altro alla volta (modo detto half duplex, vedi figura sottostante).



La comunicazione avviene in modalità seriale asincrona.

Riferirsi al modulo "Tecniche e sistemi di comunicazione" per informazioni ulteriori sulla comunicazione seriale.

8.15 I moduli SAM

La maggior parte delle validatrici per smart card prevedono la possibilità di ospitare al proprio interno uno o più "moduli SAM" (Security Access Module). Essi sono delle smart card, di solito private della parte plastica eccedente il connettore ed hanno quindi l'aspetto delle comuni SIM impiegate nella telefonia mobile.

Esse differiscono dalle carte normali soprattutto per il diverso firmware applicativo di cui sono dotate.

La validatrice "dialoga" con il modulo SAM esattamente come con la carta dell'utente; ove più moduli SAM sono previsti, uno soltanto alla volta viene utilizzato.

Il modulo SAM può essere logicamente visto come un "server" che fornisce, su richiesta, una serie di servizi, come ad esempio:

- la gestione delle chiavi crittografiche usate per garantire la sicurezza delle transazioni effettuate con le smart card;
- l'esecuzione di funzioni crittografiche come il DES, il DES-X, il triplo DES ecc.;
- generazione o verifica delle firme digitali.

L'utilizzo del SAM per l'esecuzione di queste funzioni presenta spesso il vantaggio di rendere più veloce l'operazione, potendo essere il SAM, ad e-

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	43/67

sempio, dotato di coprocessore per l'esecuzione della crittografia a livello hardware.

Ma ciò che è più importante, è che in questa organizzazione le chiavi crittografiche non sono mai direttamente accessibili da parte del software e non sono conosciute da alcuno, con enormi vantaggi dal punto di vista della sicurezza.

Un SAM può contenere più chiavi, ciascuna riservata ad un tipo di operazione; sono possibili cioè chiavi per accredito, per addebito ecc.

La maggior parte dei SAM prevedono la possibilità di aggiornare le chiavi in maniera remota, utilizzando ovviamente una procedura sicura che non consente la comprensione della nuova chiave anche nel caso in cui la comunicazione venisse intercettata.<

Ove il sistema tariffario preveda carte di circuiti diversi, è possibile utilizzare più moduli SAM in modo da garantire il completo isolamento degli elementi di sicurezza.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	44/67

9. La validatrice contactless

9.1 Riconoscimento

Michael Faraday nacque in Inghilterra nel 1791 da una famiglia molto modesta che riuscì a garantirgli soltanto la frequenza delle scuole elementari. A tredici anni cominciò a lavorare come apprendista in una legatoria e ciò gli permise di leggere moltissimi libri, soprattutto scientifici. Praticamente da autodidatta, riuscì a formarsi una notevole cultura, anche se la matematica rimase per lui sempre un grosso problema. Si appassionò alle ricerche di Humphry Davy, direttore della Royal Institution, seguì tutte le sue conferenze e raccolse in un libro gli appunti e le annotazioni prese. Regalò poi il suo libro allo stesso Davy, che poco dopo lo assunse come assistente nel centro che dirigeva. Questo permise a Faraday di dedicarsi alla sperimentazione, specialmente nel campo della chimica, dell'elettricità e del magnetismo. Scoprì così le leggi che regolano l'elettrolisi, l'effetto schermante delle gabbie metalliche e l'induzione elettromagnetica. I suoi successi nel campo scientifico lo resero famoso e nel 1825 fu nominato direttore della Royal Institution, nonché successore di Davy nella stessa cattedra universitaria. Anche se non conosceva a fondo il linguaggio matematico, lo scienziato riusciva lo stesso a descrivere e spiegare in maniera chiara ed efficace quanto andava scoprendo. Riusciva a farsi comprendere da tutti ed alle sue conferenze assisteva sempre un pubblico numeroso. Se avesse messo le sue scoperte a disposizione della nascente industria sarebbe diventato ricco, ma non pensò mai al denaro e morì, nel 1867, povero come era nato.



Anche la validatrice contactless, al pari di quella magnetica e per quanto meno evidente, è basata su leggi e principi scoperti dal grande scienziato Michael Faraday.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	45/67

9.2 Generalità

Le smart card utilizzate in ambito trasporti costituiscono una categoria ben precisa nell'ambito dei numerosi sistemi esistenti per l'identificazione a radio frequenza (RFID, Radio Frequency Identification) e ad esse saranno limitate le osservazioni che seguono.

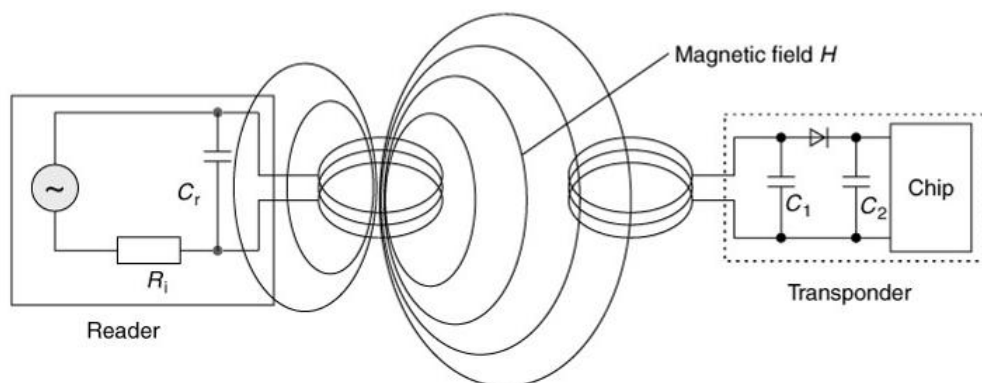
In ambito trasporti si utilizzano quasi solo esclusivamente smart card ad accoppiamento induttivo in accordo agli standard ISO 14443. Fare riferimento al modulo del corso "Titoli Di Viaggio Elettronici" per informazioni ulteriori.

In questo capitolo saranno descritti i principi che stanno alla base delle validatrici contactless (foto a lato).



9.3 Trasferimento di energia

Le smart card contactless sono concettualmente identiche a quelle del tipo a contatti ma presentano rispetto alle stesse l'ovvia differenza di dover operare in assenza di collegamento elettrico. L'energia necessaria al funzionamento della smart card, chiamata PICC negli standard di riferimento ("Proximity Inductive Chip Card"), deve essere quindi trasferita a carico del cosiddetto PCD ("Proximity Coupling Device"), ossia della validatrice.



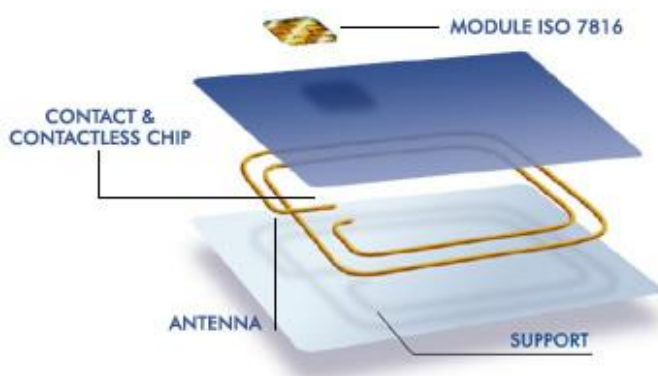
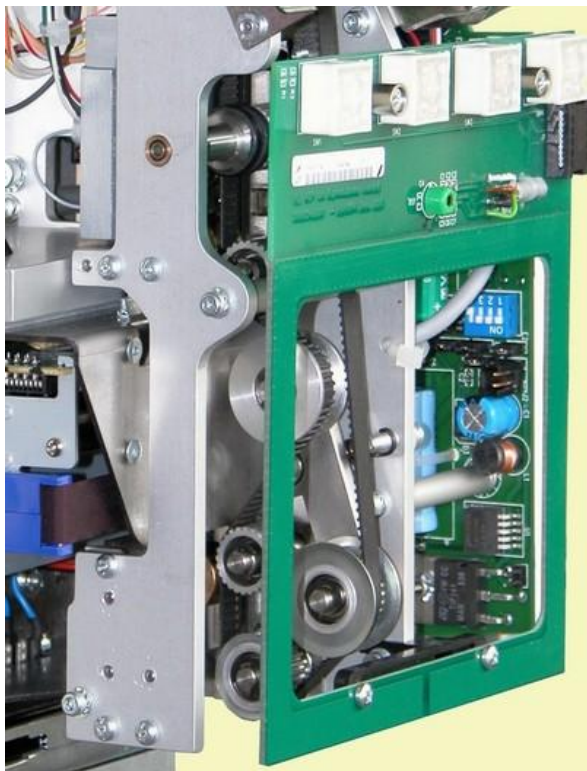
Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	46/67

A questo fine, il PCD genera un forte campo elettromagnetico alla frequenza di 13,56 MHz (onde corte) attraverso un induttore, ossia un avvolgimento di alcune spire di conduttore detto "antenna", che si accoppia con una corrispondente antenna ricavata nella smart card.

Poiché la lunghezza d'onda della frequenza usata ($13,56 \text{ MHz} = 22,1 \text{ m}$) è molte volte superiore alla distanza tra il PCD e la PICC, il campo elettromagnetico può essere considerato come un semplice campo magnetico alternato H che, come in un trasformatore elettrico, induce ai capi dell'antenna della smart card una tensione V , che a sua volta, raddrizzata e filtrata, provvede, alla alimentazione dei circuiti della carta stessa.

Per ottenere il trasferimento di energia, gli induttori (antenne) del PCD e del PICC devono risultare parte di circuiti risonanti e quindi portati all'accordo per mezzo di una opportuna capacità posta in parallelo a ciascuno di essi.

Il campo magnetico si misura in Ampere per metro (A/m). Lo standard ISO 14443 prevede che il campo magnetico per il funzionamento del PICC sia compreso tra 1,5 e 7,5 A/m rms.



Le antenne di una validatrice contactless e di una smart card

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	47/67

9.4 Comunicazione dal PCD alla PICC

9.4.1 Generalità

La modalità di comunicazione dal PCD alla PICC è facile da comprendere, a differenza di quella in senso inverso, più complessa, che sarà descritta nel paragrafo successivo.

Potendo il PCD stabilire di emettere o meno il campo magnetico verso la carta, esso dispone anche di una maniera di trasmettere alla stessa delle informazioni. Modulando il campo magnetico opportunamente, è infatti possibile inviare una sequenza di bit dalla validatrice alla smart card.

9.4.2 Tipo A e tipo B

Lo standard ISO 14443 parte seconda prevede che la trasmissione dal PCD alla PICC avvenga sempre utilizzando una modulazione di ampiezza della frequenza emessa, ma l'indice di modulazione differisce per i due tipi di comunicazione che lo standard stesso prevede: il "tipo A", storicamente preesistente, ed il "tipo B", nato successivamente come evoluzione dell'A.

L'indice di questa modulazione assume il valore del 100% nel caso del tipo A e del 10% nel caso del B.

9.4.3 Tipo A

Nel caso del tipo A, questo significa che all'invio dello stato logico "1" corrisponde l'emissione della portante a piena potenza mentre questa viene del tutto soppressa per la trasmissione dello "0".

Durante la trasmissione dello "0", quindi, la PICC non riceve energia e questa deve essere quindi prelevata a spese delle capacità di cui può essere dotata la carta internamente e/o del campo magnetico stesso.

Nel tipo A, il trasferimento di energia è quindi limitato e questo, per molto tempo, ha impedito di utilizzare nella PICC dei chip che non fossero delle semplici memorie o poco più, quindi con inferiori livelli di prestazioni, di capacità e di sicurezza.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	48/67

9.4.4 Tipo B

Nel tipo B la modulazione è solo del 10% e quindi, anche nella trasmissione dello "0" si ha ancora il trasferimento del 90% dell'energia.

Il tipo B ha potuto quindi utilizzare fin da subito circuiti più complessi che hanno consentito un considerevole salto qualitativo (microprocessore) rispetto alle prime carte di tipo A.

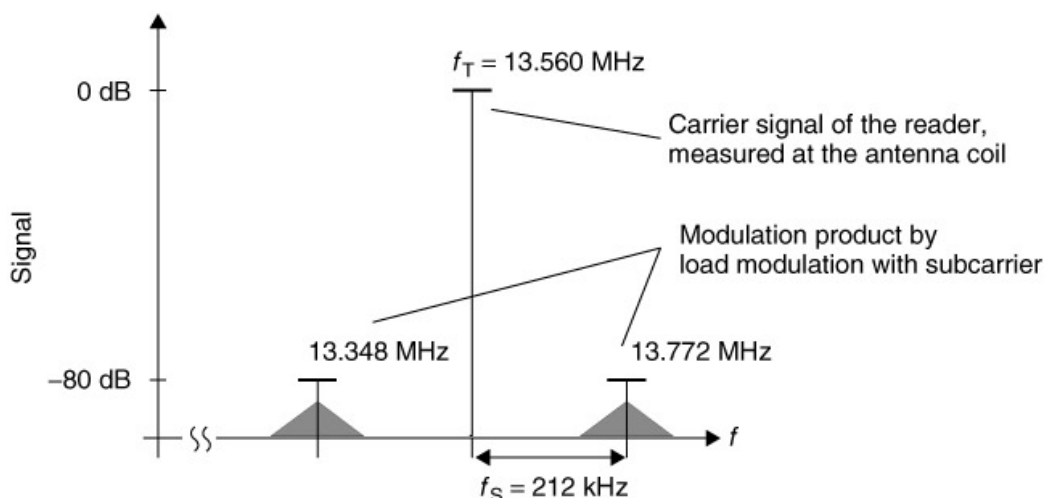
9.5 Comunicazione dalla PICC al PCD

Sono ancora le leggi di Faraday a consentire la comunicazione dalla PICC al PCD.

Si è detto che quando nel campo alternativo emesso dalla validatrice venga a trovarsi un circuito risonante, questo preleva energia dal campo stesso.

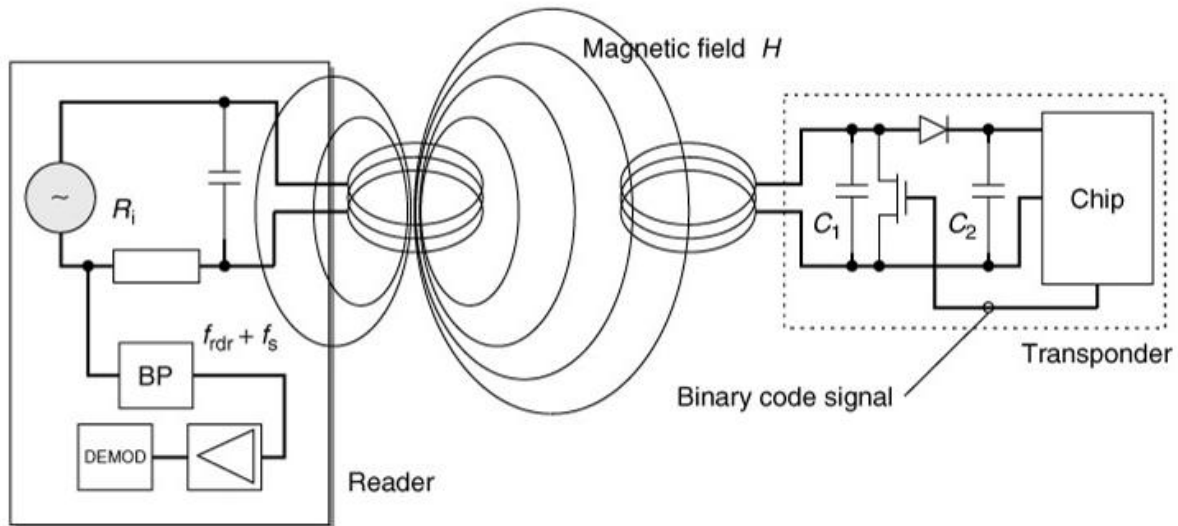
Il circuito generatore della validatrice "vede" una variazione di impedenza della propria antenna quando una carta è presente nel campo ed una variazione nel carico posto nel circuito risonante della carta, come in un trasformatore, si riflette in una variazione del carico visto dal generatore; pertanto in una variazione della tensione ai capi dell'antenna.

Variando a frequenza elevata (ma comunque a frequenza inferiore alla portante) il carico dell'antenna nella carta si vengono a creare due linee spettrali dette "sottoportanti" (vedi figura), simmetriche alla frequenza della portante che possono essere utilizzate, con opportuna modulazione, per trasferire dati dalla PICC al PCD.



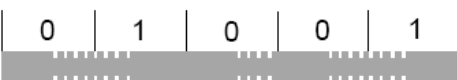
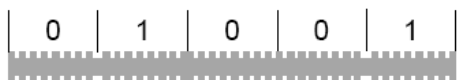


Questo tipo di modulazione è detto "modulazione di carico" ("load modulation").

La figura seguente illustra, nel principio, il circuito di modulazione di carico della PICC e di rilevazione da parte del PCD.



La sottostante figura illustra i vari parametri previsti dallo standard ISO 14443 per i tipi A e B. Si noti che edizioni successive della norma (2003) prevedono anche bit rate più elevati.

	Type A	Type B
PCD to PICC	ASK 100% Modified Miller, 106kbit/s 	ASK 10% NRZ, 106kbit/s 
PICC to PCD	Load Modulation Subcarrier $f_c/16$ OOK Manchester, 106kbit/s 	Load Modulation Subcarrier $f_c/16$ BPSK NRZ-L*, 106kbit/s 

9.6 MIFARE ed altri standard

La comunicazione delle classiche carte MIFARE, già descritto in [1] avviene in base allo standard ISO 14443 tipo A, impiegando però un protocollo proprietario invece di quello previsto da ISO 14443-4, con particolari procedure per autenticazione e la elaborazione.

Le carte MIFARE Ultralight impiegano lo stesso protocollo, ma senza lo standard di sicurezza.

Lo standard MIFARE è quindi uno standard chiuso e proprietario; la validatrice, per poterle processare, deve prevedere un apposito chip fornito dalla stessa NXP, che finisce per pesare sul costo del terminale come una royalty.

9.7 Altri standard

Tra gli altri standard utilizzati nel mondo dei trasporti, il FELICA di Sony (non impiegato in Italia) ed l'ISO 15693, per lettura a media distanza (anche 50 cm) .

9.8 Il "coupler"

Nella validatrice i circuiti che esplicano le funzioni di PCD sono generalmente due:

- il "coupler", ossia il circuito di interfaccia che emette la portante, trasmette e riceve i dati;
- l'antenna, ossia il circuito accordato contenente l'induttore cui si è fatto più volte riferimento in precedenza.

Il coupler, che può assumere varie connotazioni, è di solito un dispositivo complesso cui sono affidate anche le funzioni di interfaccia con il modulo SAM.

In certi casi il coupler è costituito da un modulo separato dotato di propria intelligenza, cioè di proprio processore, memoria, I/O ecc. In altri casi esso è incorporato nel circuito della validatrice e viene gestito dal processore principale.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	51/67



Un coupler intelligente reale – due moduli SAM sono visibili, altri due si trovano sul lato inferiore.
Può processare vari standard ISO ed anche altri proprietari, come il MIFARE.

9.9 Normative e distanza di lettura

Sulla base di quanto fin qui descritto, la validatrice contactless è a tutti gli effetti un trasmettitore radio, sia pure di modesta potenza. Per questo motivo deve sottostare alle severe norme europee ETSI EN 301-489 ed ETSI EN 300-330 per la compatibilità elettromagnetica.

Siamo quindi di fronte a due esigenze contrastanti, da un lato il desiderio di ottenere la più facile lettura alla maggiore distanza, dall'altro la necessità di limitare le emissioni per non eccedere i limiti previsti dalle norme sopraindicate nonché per rientrare nei limiti previsti per l'omologazione obbligatoria (vedere par. 5.2.7).

La distanza di lettura non è facilmente misurabile, in quanto varia anche in funzione della posizione della carta, del modello della stessa e della velocità e dell'angolo di avvicinamento.

Statisticamente si è osservato che pressoché tutti i viaggiatori avvicinano la carta fino al contatto con la zona sensibile, che viene sempre evidenziata con un opportuno pittogramma. La distanza di lettura non è quindi critica, se non per leggere la carta anche all'interno di un portafogli. E' quindi opportuno non eccedere nella distanza di lettura, essendo buona norma evitare sempre emissioni elettromagnetiche inutili, anche per il perico-

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	52/67

lo di interferenze con altre apparecchiature, in particolare con quelle elettromedicali (es. pace maker).

Gli apparati commerciali hanno di solito distanze di lettura variabili tra 30 e 80 mm - in nessun caso la carta deve essere letta ad una distanza maggiore di 100 mm.

9.10 Tempo della transazione

Il tempo della transazione dipende spesso dal numero di operazioni richieste e dal numero e dalla varietà degli standard delle carte utilizzate.

Il dialogo iniziale dal PCD alla PICC prevede la seguente sequenza:

- attivazione della PICC da parte del campo;
- la PICC resta in attesa silenziosa di comandi;
- trasmissione di un comando da parte del PCD;
- trasmissione di una risposta da parte della PICC.

La sequenza viene ripetuta alternativamente per ogni tipo di modulazione; se nel Sistema di Bigliettazione Elettronica sono utilizzate carte di tipo A e di tipo B, la sequenza verrà eseguita due volte.

Le carte più comuni operano ad un bit rate di 106 kbit/s e gli accessi richiedono sempre un certo numero di comandi, tanto maggiori quanti più sono i possibili contratti di trasporto e le operazioni previste.

Ai tempi necessari per le suddette operazioni si deve sommare il tempo necessario per il colloquio con il modulo SAM, ove questo sia previsto. Si comprende pertanto che sia difficile parlare in generale di tempo di transazione e che quest'ultimo dipenda spesso comunque in maniera incompressibile dal numero e dalla varietà delle operazioni richieste. Il tempo della transazione può quindi oscillare da un minimo di 120 ms ad un massimo di 500 ed oltre.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	53/67

9.11 Pregi delle validatrici contactless

La validatrice contactless, in virtù dei suoi principi di funzionamento in precedenza descritti, può assumere forme molto compatte e, se opportunamente costruita, può raggiungere elevati gradi di protezione in modo da risultare anche installabile all'aperto (es. stazioni).

L'utilizzo di soluzioni "totalmente contactless" non è però molto diffusa nel nostro paese, soprattutto per il fatto che non esiste ancora una soluzione ottimale di titolo di viaggio a prossimità per l'effettuazione di corse singole.

Per questo motivo la tecnologia contactless è frequentemente accoppiata, nella stessa macchina, con quella della banda magnetica o con l'obliterazione cartacea tradizionale (vedi figura).



Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	54/67

10. La console autista

Tra i componenti del Sistema Di Bordo, la console autista è probabilmente quella che presenta un maggior grado di variabilità nelle sue varie implementazioni. Si va infatti da un semplice terminale di tipo "non intelligente" capace solo di svolgere un numero assai limitato di funzioni, ad apparati basati su architettura PC, con display a colori di grandi dimensioni, eventualmente sensibili al tocco, interfaccia grafica, stampante e numerose interfacce tra cui quella contactless per il processo delle smart card. In certi casi sono presenti addirittura due interfacce utente, una per l'autista e l'altra per il passeggero.

10.1 Interfaccia utente (autista)

10.1.1 Display

Data la citata variabilità da un modello all'altro, si può affermare che sono disponibili sul mercato console autista con quasi ogni tipo di display, ad iniziare dal classico 2x16 a caratteri già descritto per le validatrici (par. 5.2.1.1) o addirittura da modelli di dimensioni minori.

Un buon compromesso tra dimensioni e leggibilità è rappresentato dai display grafici monocromatici della misura di 7,5 pollici, aventi di solito risoluzioni di "¼ di VGA", ossia di 320x240 pixel; dimensioni maggiori possono determinare qualche difficoltà nell'alloggiare l'apparato in prossimità dell'autista, mentre risoluzioni maggiori possono portare ad una dimensione del punto troppo ridotta, e quindi a difficoltà di lettura.

Esistono molte tecnologie per la realizzazione dei display di questo tipo, in costante evoluzione grazie al largo impiego fatto in ambito automobilistico per la realizzazione di navigatori.

Il display può usare una delle seguenti principali tecnologie:

- **trasmissiva** - l'illuminazione viene posizionata sul retro dello schermo e i cristalli liquidi agiscono da filtro facendo passare solo la componente cromatica desiderata. Si ottengono schermi molto luminosi anche se la fonte di luce spesso consuma più energia di quella richie-

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	55/67

sta dallo schermo in sé. La visibilità è migliore in condizioni di bassa illuminazione dall'ambiente, con l'ottimo in condizioni di completa oscurità;

- **riflessiva** - viene usata la luce presente nell'ambiente che viene riflessa da uno specchio posto dietro lo schermo. Questi tipi di schermo hanno un contrasto più basso rispetto a quelli di tipo trasmissivo, poiché la luce è costretta a passare due volte attraverso il filtro. La visibilità è migliore in condizioni di piena illuminazione dall'ambiente, anzi, maggiore è la luce esterna, meglio lo si vede. Un altro vantaggio di questa tecnologia è il bassissimo consumo, che però nel caso dell'autobus è irrilevante.
- **transflectiva** - gli schermi di questo tipo cercano di unire le caratteristiche migliori dei precedenti. Hanno un semi-specchio posto dietro il display, in grado di riflettere la luce frontale, ma di far passare la luce proveniente da un illuminatore posto nella parte posteriore. Questo tipo di display si va diffondendo rapidamente, soprattutto negli apparecchi mobili (telefoni cellulari e computer palmari), per la sua buona leggibilità in tutte le condizioni di luce.

I display sono sempre di tipo illuminato. Sono ancora molto usate le tradizionali lampade a scarica di gas, meno durevoli e più costose, anche a causa della necessità di montare un circuito survoltore per generare l'alta tensione da esse richieste per il funzionamento. Sempre più diffuse le illuminazioni con diodi LED di nuova generazione, che assicurano una luce bianca e molto intensa ed una durata assai maggiore.

I display a colori offrono immagini di qualità molto elevata, oltre a presentare un costo più elevato, non sempre risultano ben visibili in condizioni di forte illuminazione, ad esempio se esposti direttamente ai raggi solari.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	56/67



Una console autista con display grafico di tipo transreflectivo

In ogni caso è importante che sia prevista la possibilità di regolazione o di oscuramento del display per evitare fastidi durante la guida notturna.

10.1.2 Avvisatore acustico

I sistemi basati su architettura PC dispongono di regola di ampie capacità di sinterizzazione del suono e quindi della possibilità di riprodurre file .wav o .mp3. In altri casi è presente il beeper piezoelettrico come nelle validatrici.

10.1.3 Tastiera

Le interfacce "al tocco" ("touch screen") sono molto diffuse e molto comode da utilizzare e, grazie alla loro intuibilità, riducono in misura notevole la richiesta di formazione al personale.

Questa soluzione presenta anche il vantaggio di non richiedere nessuna tastiera; sono visualizzati solo i tasti che servono e quando servono. Ad esempio, per l'occasionale introduzione di stringhe alfanumeriche può essere visualizzata una adeguata tastiera, da far scomparire subito dopo. Maggiori sono anche le possibilità di cambiare lingua.

Ad un gradino subito inferiore dei touch screen, i "soft key", ossia tasti posti in prossimità dello schermo con funzioni variabili, descritte da etichette fatte comparire opportunamente.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	57/67

Modelli più semplici di console autista presentano solo una dozzina di tasti. In ogni caso è importante che siano retroilluminati.

10.2 Interfaccia utente (passeggero)

L'interfaccia verso il passeggero, ove presente, deve essere intesa in modo del tutto analogo al display, rivolto al cliente, presente nei registratori di cassa; essa ha infatti lo scopo di consentire la verifica in tempo reale dell'operazione di ricarica o di emissione eseguita dall'autista. Essa è quindi composta da un display, qualche tasto ed, eventualmente, dei LED in modo del tutto analogo a quanto presente nella validatrice (vedi par. 5.2.1).

10.3 Unità di processo

Anche in questo caso si ha una notevole variabilità; si passa da microcontrollori addirittura a soli 8 bit per le console autista più elementari a vere e proprie architetture da palmare o da PC, con tutti i gradi intermedi. Le architetture "maggiori" utilizzano di solito sistema operativo Windows o Linux.

Le dimensioni di memoria passano corrispondentemente da poche decine di byte a parecchi mega.

10.4 Periferiche di massa

Vale quanto già indicato per le validatrici nel par. 5.2.3.

10.5 Le interfacce

Vale quanto già indicato per le validatrici nel par. 5.2.4.

10.6 L'alimentatore le batterie

Vale quanto già indicato per le validatrici nel par. 5.2.5.

10.7 Omologazioni

Vale quanto già indicato per le validatrici nel par. 5.2.7.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	58/67

10.8 Organizzazione del software

Vale quanto già indicato per le validatrici nel par. 5.2.8.

10.9 Stampante di scontrini

Ove la console autista svolga anche la funzione di vendita/ricarica a bordo, è prevista una stampante di scontrini per l'emissione dei TDV o delle ricevute. Tutte le unità commerciali di questo tipo utilizzano una stampante di tipo termico, che, pur al prezzo di dover utilizzare carta speciale, offrono una ottima qualità di stampa ed una buona velocità.

La stampa termica avviene facendo passare la carta termosensibile sotto ad una riga di speciali transistori. Ogni transistore ha una bassa inerzia termica, può cioè riscaldarsi e raffreddarsi in tempi molto brevi. Comandando opportunamente questi elementi, accendendoli o meno, è possibile marcare una riga sulla carta termica, ove solo i punti accesi lasceranno una traccia visibile. Muovendo al contempo la carta si possono così stampare caratteri o elementi grafici.

Una buona stampante termica è in grado di fornire stampe molto contrastate, con un nero "pieno e marcato", anche se il biglietto prodotto risulta stabile solo per un tempo limitato (alcuni mesi) ed è piuttosto sensibile all'abrasione. In considerazione delle finalità, è comunque del tutto adeguato alla propria funzione.

Il distacco del biglietto avviene "a strappo"; essendo la console sempre manovrata dall'autista, non si reputa necessario aggiungere un costoso e pesante meccanismo di taglio automatico.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	59/67



Un biglietto emesso con stampante termica

10.9.1 Sezione di convalida contactless

Vale quanto già indicato per le validatrici nel cap. 9.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	60/67

11. Apparati di comunicazione

L'argomento è approfondito nel modulo "Tecniche e sistemi di comunicazione" [3] cui si rimanda per maggiori informazioni. In questo capitolo ci si limita ad una descrizione sommaria dei vari apparati utilizzati nei Sistemi Di Bordo.

11.1 Generalità

Il Sistema Di Bordo dispone di solito di uno dei seguenti sistemi di comunicazione o di entrambi:

- comunicazione a breve raggio, per il collegamento con il Concentratore Di Deposito nel tempo in cui il mezzo si trova parcheggiato;
- comunicazione a lungo raggio, riservata in particolare ai mezzi che non fanno abitualmente ritorno al deposito o che già ne dispongano per altra causa (es. per avere installato un sistema AVM).

11.2 Comunicazione a breve raggio

La comunicazione a breve raggio è di solito preferita in quanto avviene di regola a costo nullo ed anche perché spesso più prestante.

Le principali tecniche utilizzate sono le seguenti:

- apparati VHF/UHF di tipo proprietario;
- apparati basati su tecnologia Bluetooth;
- apparati basati su tecnologia IEEE 802.11 ("WI-FI");

11.3 Comunicazione a lungo raggio

La comunicazione a lungo raggio avviene in area pubblica; essa si è basata in passato su frequenze radio assegnate in concessione ma questo modello è stato del tutto reso obsoleto dagli apparati di telefonia mobile, oggi utilizzati per assolvere a questa funzione (GPRS/UMTS/EDGE ecc.).

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	61/67

12. Sistemi di stazione

12.1 Generalità

Si è fatto in precedenza costante riferimento al Sistema Di Bordo autobus.

Nelle stazioni ferroviarie è invece presente il Sistema Di Stazione (SDS) che si definisce in maniera analoga al Sistema Di Bordo, ossia come l'insieme degli apparati che consentono la fruizione dei Titoli Di Viaggio Elettronici (TDVE).

Anche in questo caso si assiste ad una grande varietà di soluzioni tecniche, diverse essendo le categorie di stazioni:

- stazioni di metropolitana;
- grandi e medie stazioni ferroviarie;
- piccole stazioni ferroviarie non presidiate.

Si descriveranno nel seguito le soluzioni tecniche più frequentemente adottate per ciascuna delle suddette tipologie.

12.2 Concentratore di stazione

Il concentratore di stazione, di solito un PC, ha lo scopo di interfacciare tutte le validatrici al Sistema di Bigliettazione Elettronica. Ove sia presente un certo numero di validatrici, è prevista una "dorsale" RS-485 comune a tutte le macchine o, più frequentemente, una connessione Ethernet a stella.

La posa dei cavi in ampi spazi aperti crea non pochi problemi a causa delle scariche elettrostatiche atmosferiche. E' quindi opportuno, in alcuni casi, provvedere adeguati scaricatori ad ambo gli estremi della linea.

Ove possibile, la soluzione Wireless LAN (WI-FI) può eliminare sia l'inconveniente citato che i non trascurabili costi di installazione e manutenzione delle linee in rame.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	62/67

12.3 Stazioni di metropolitana

Nelle stazioni della metropolitana sono universalmente impiegati varchi per il controllo degli accessi, ad ante o a tripode. L'apertura del passaggio è di regola controllata da una validatrice. Solo in un numero limitato di casi, e per motivi contingenti, si fa impiego di una normale validatrice montata su di un paletto. Di regola sono invece installati dei modelli specifici incorporati nel tornello, muniti di due bocchette per il biglietto, una di ingresso e l'altra di uscita, disposte in modo tale da accelerare il flusso dei passeggeri.

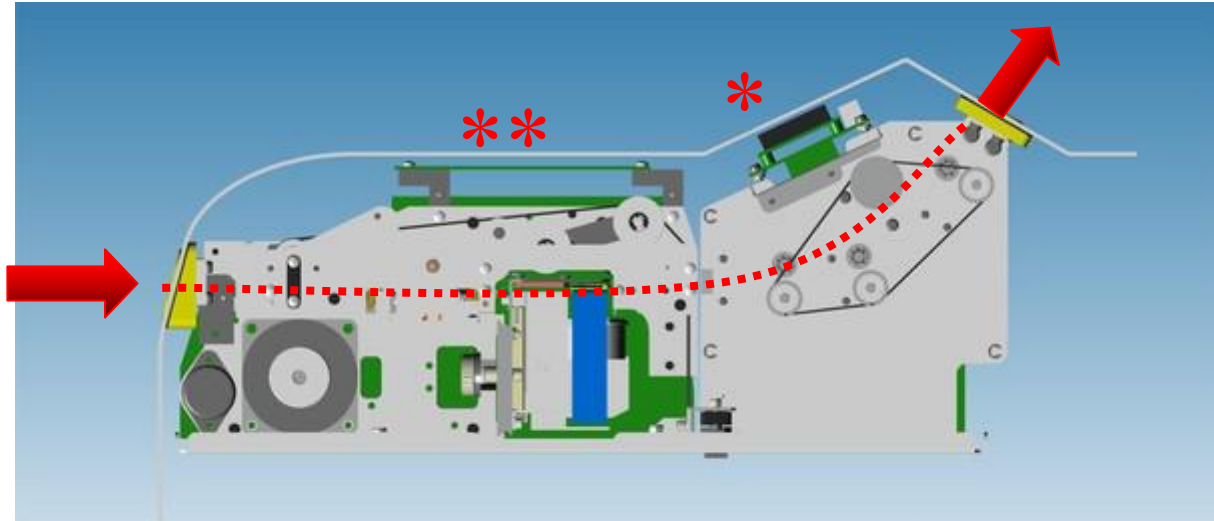


Normali validatrici interfacciate a tornelli di tipo tripode

La figura successiva mostra la bocchetta di entrata e quella di uscita nonché il percorso del biglietto.

In essa si osserva anche la sezione del profilo del tornello, all'interno del quale la validatrice si trova completamente protetta. Opportune finestre protette da laminati plastici consentono la visione del display (*) ed il passaggio del campo magnetico (***) utilizzato per la lettura della carta contactless.

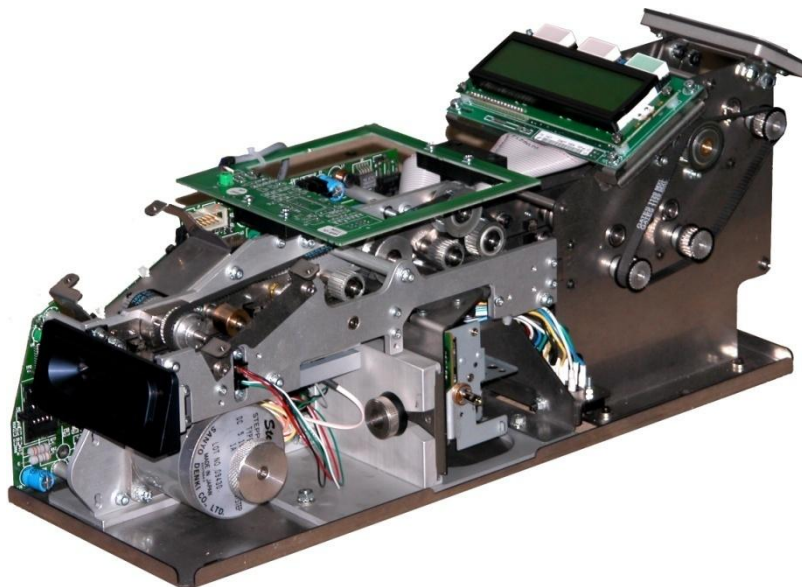
Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	63/67



La validatrice, per assolvere al compito del controllo del tornello, deve prevedere opportune interfacce. Sono possibili tanto interfacciamenti con contatti elettrici, nei due sensi, che una più evoluta comunicazione su canale seriale.

In molti casi la validatrice non si connette direttamente al concentratore del Sistema Di Stazione ma al tornello, che ha di solito una propria unità di elaborazione e comunicazione, che a sua volta è collegato al concentratore.

L'immagine ancora successiva mostra l'aspetto di una validatrice contactless + magnetica per tornello.



Nel tipo di stazione in esame, è sempre presente, in qualche forma, una linea di comunicazione che consente il collegamento del Sistema Di Stazione al Sistema di Bigliettazione Elettronica.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	64/67

La tensione di alimentazione alla validatrice viene fornita dal tornello.



Varchi di metropolitana in batteria - sullo sfondo, emettitrici di biglietti self service (Minimetrom, Perugia)

12.4 Stazione medio/grandi

Le stazioni di una certa dimensione sono costantemente presidiate e munite di pensiline per offrire protezione ai viaggiatori quando la stagione è inclemente.

In questo caso è possibile fare impiego di normali validatrici collegate al concentratore come indicato in precedenza e poste al riparo della pioggia.

Anche in queste stazioni, come nelle metropolitane, è sempre presente una linea di comunicazione per il collegamento al Sistema di Bigliettazione Elettronica.

L'alimentazione della validatrice avviene ad opera di un alimentatore da racchiudere in una scatola con sportello a chiave ove può essere alloggiato l'eventuale sistema di scaricatori.

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	65/67

12.5 Stazioni non presidiate

Il problema delle stazioni non presidiate richiede una soluzione diversa, in quanto:

- la validatrice non viene sorvegliata ed è quindi esposta ad azioni vandaliche;
- sono spesso assenti ripari dalla pioggia;
- non sono disponibili linee di comunicazione per collegare la validatrice al Sistema di Bigliettazione Elettronica.

Per questi motivi vengono utilizzate contromisure di vario tipo, come ad esempio la comunicazione GPRS e protezioni di varia forma.

Ove la validatrice disponga di adeguata potenza elaborativa e del necessario software, l'uso del collegamento telefonico permette di eliminare completamente il PC concentratore, con tutti i vantaggi del caso.

Sono presenti sul mercato validatrici in allestimenti speciali per l'impiego in stazioni ferroviarie non presidiate che possono ospitare al proprio interno anche l'alimentatore, il modulo e l'antenna GPRS, un condizionatore (riscaldatore / circolatore) ed un eventuale gruppo statico di continuità per far fronte alle interruzioni di tensione.

In questo caso la costruzione risulta particolarmente robusta e permette alla validatrice di essere esposta senza problemi alla pioggia battente.

L'immagine a lato riporta l'aspetto di una di queste validatrici; si osservi la zona sensibile per la lettura delle carte contactless nella parte superiore, seguita dal display e dalla bocchetta per il biglietto magnetico.



Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	66/67



Validatrici magnetiche per stazione

Titolo documento	File	Pagina/di
Il Sistema Di Bordo	701287.E00.IT DISPENSA SDB.DOCX	67/67

Gianni Becattini

Appunti sulla Bigliettazione Elettronica

Sistemi Di Comunicazione



AEP Advanced Engineering Projects s.r.l.
Via dei Colli, 240 - Signa (Firenze) - Italia
<http://www.aep-italia.it>



Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	1/48

1. Sommario

1.	Sommario.....	2
2.	Presentazione	4
3.	Introduzione	5
4.	Interfacce seriali.....	7
4.1	La codifica di dati alfanumerici	7
4.2	La telegrafia automatica.....	9
4.3	Il codice ASCII	13
4.4	Temporizzazioni.....	14
4.5	La parità	14
4.6	Numero dei bit.....	15
4.7	Controllo di flusso.....	15
4.7.1	Controllo di flusso per via hardware.....	15
4.7.2	Controllo di flusso per via software.....	16
4.8	Configurazione.....	16
4.9	L'UART	17
4.10	La bufferizzazione	18
4.11	Riepilogo	18
5.	Interfacce elettriche.....	19
5.1	Generalità	19
5.2	Loop di corrente	19
5.3	Codifica in tensione.....	20
5.4	EIA RS-232.....	21
5.4.1	Generalità.....	21
5.4.2	Storia.....	21
5.4.3	Livelli elettrici.....	22
5.4.4	Massima distanza.....	22
5.4.5	Circuito a 3 fili.....	23
5.4.6	Circuito con controllo di flusso	23
5.5	Interfaccia differenziale	24
5.6	Interfaccia EIA RS-422.....	26
5.7	Interfaccia EIA RS-485.....	26
5.8	Cablaggio di una linea differenziale	28
5.9	Riepilogo.....	29
6.	I protocolli.....	30
6.1	Generalità	30
6.2	Controllo degli errori.....	30
6.3	Regole di comportamento	31
6.4	I protocolli.....	32
6.5	Potenzialità del protocollo.....	32
6.6	Concordanza semantica.....	33
6.7	Complessità e variabilità	33
6.8	Kit di sviluppo.....	34
7.	Il CAN bus.....	35
7.1	Generalità.....	35

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	2/48

7.2	I livelli ISO-OSI.....	35
7.3	Standard.....	36
7.4	Caratteristiche del CAN.....	37
7.5	Utilizzo delle linee dell'autobus.....	37
8.	Comunicazione bordo/terra.....	38
8.1	Generalità.....	38
8.2	Comunicazione a breve e lungo raggio.....	38
8.3	Comunicazione a breve raggio.....	39
8.3.1	Raggi infrarossi.....	39
8.3.2	Comunicazioni radio a banda stretta.....	39
8.4	Comunicazioni radio spread spectrum (SS).....	40
8.4.1	La Wireless LAN.....	42
8.4.2	La sicurezza del WI-FI.....	42
8.4.3	Gli apparati di deposito.....	43
8.5	Gli apparecchi di bordo.....	44
8.5.1	Bluetooth.....	44
8.6	Comunicazione a lungo raggio.....	46
8.7	Caratteristiche della comunicazione GPRS.....	46
8.8	Il concentratore.....	47

2. Presentazione

Questa dispensa è stata originariamente presentata dall'autore all'Executive Master "SVILUPPO E GESTIONE DEI SISTEMI DI BIGLIETTAZIONE ELETTRONICA E DI PAGAMENTO DEI SERVIZI DI MOBILITÀ" organizzato da Clickutility e tenuto a Bologna dal settembre a dicembre 2007, con la collaborazione scientifica e il patrocinio di Club Italia ed il patrocinio dell'ANAV.

Essa appartiene ad una serie di tre volumetti orientati alla descrizione delle tecnologie di bordo:

- dispensa 1 - "Titoli Di Viaggio Elettronici (TDVE)" - descrive sommariamente i vari tipi di TDVE in un'ottica di funzionalità e di utilizzo con annotazioni anche di carattere commerciale;
- dispensa 2 - "Il Sistema Di Bordo (SDB)" - descrive principalmente le caratteristiche tecniche e di funzionamento dei terminali per l'utilizzo dei TDVE e di quelle parti accessorie che, installate a bordo del bus, costituiscono nel complesso il cosiddetto Sistema Di Bordo. In parallelo alla descrizione dei terminali vengono fornite informazioni più approfondite sui principi di funzionamento dei TDVE.
- dispensa 3 - "Tecniche e Sistemi di Comunicazione (COM)" - vengono descritte le principali tecniche di comunicazione usate all'interno ed all'esterno degli apparati di bordo, nonché i sistemi di terra che consentono lo scambio di dati con gli autobus.

Eventuali riferimenti al numero della dispensa sono via via riportati entro parentesi quadre (es. [1])

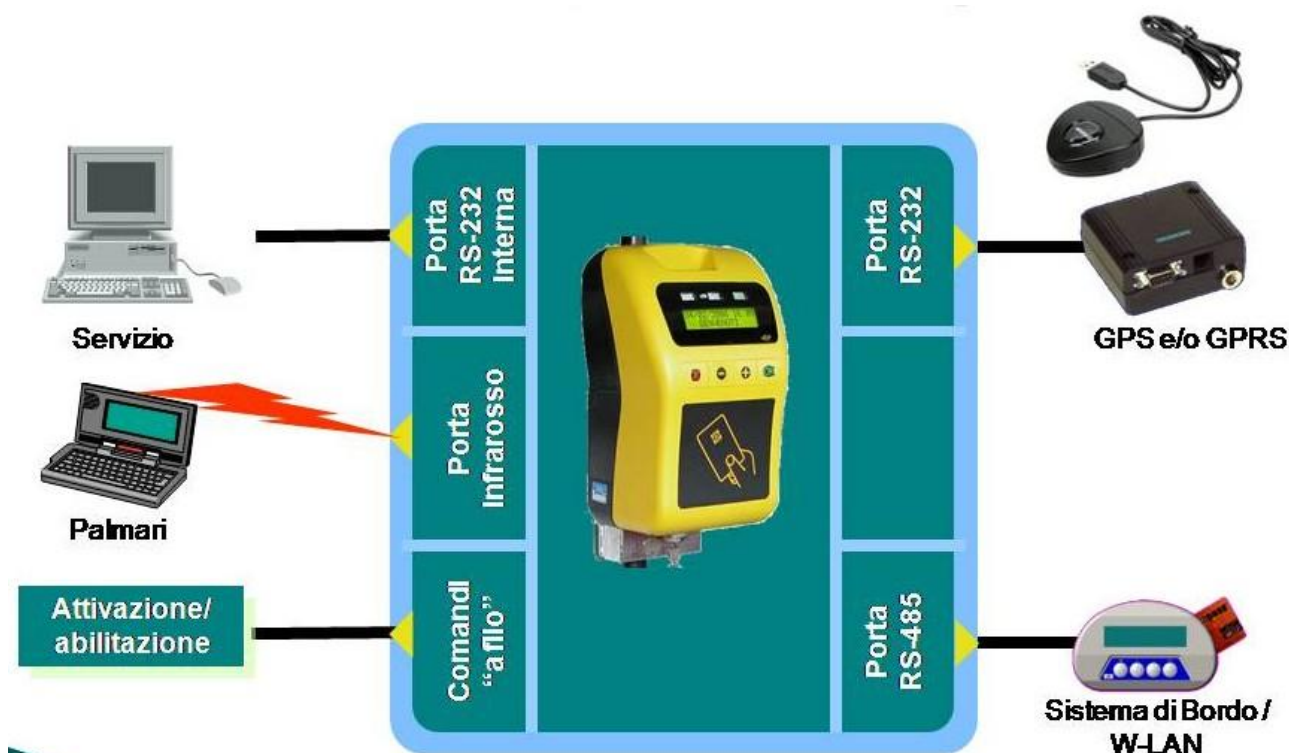
Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	4/48

3. Introduzione

In un Sistema di Bigliettazione Elettronica, gli apparati non operano mai singolarmente ma producono dati o necessitano di dati. Questi dati devono essere all'occorrenza opportunamente trasferiti.

Ogni apparato è quindi munito di **interfacce** che costituiscono le posizioni estreme del **canale di comunicazione** che lo unisce ad altri apparati.

L'**interfacciamento** è l'operazione con cui si collegano e si fanno interagire tra loro due o più apparati.



La figura precedente riporta un esempio di validatrice munita di varie interfacce, e precisamente:

- una porta RS-232 interna, accessibile solo al personale di manutenzione o agli sviluppatori;
- una porta ad infrarossi per il collegamento con un palmare per l'accesso ai dati senza connessione fisica;
- una porta RS-485 per l'interfacciamento con il Sistema Di Bordo;
- una porta RS-232 per eventuali accessori, come un modem GPRS od un ricevitore GPS;

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	5/48

alcune ingressi od uscite digitali, ad esempio per leggere un interruttore di abilitazione.

In queste note esamineremo nel seguito, sommariamente, i vari tipi di interfacce più comuni.

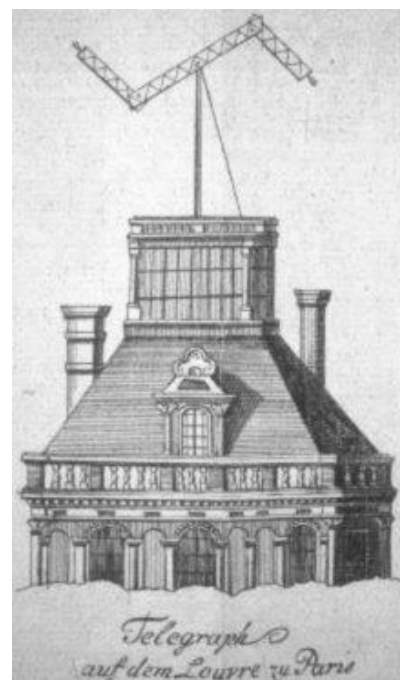
Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	6/48

4. Interfacce seriali

4.1 La codifica di dati alfanumerici

La necessità di comunicare è sempre stata presente in ogni civiltà ed in ogni epoca. Già gli antichi greci impiegavano falò per comunicare. Per la comunicazione diurna sono stati impiegati segnali sonori, sia di strumenti a fiato (corni) che percussioni (tamburi, tam-tam). Per distanze maggiori sono stati impiegati i segnali di fumo, comunemente associati agli Indiani d'America.

Verso la fine del diciottesimo secolo Claude Chappe e il fratello lavorarono allo sviluppo di un sistema telegrafico basato su una catena di segnalatori. Nel 1793 presentarono al pubblico il modello definitivo di telegrafo ad asta, così definito in quanto su una torre era installato un braccio rotante che portava alle estremità due bracci minori; il tutto era manovrabile per assumere configurazioni standardizzate corrispondenti a lettere, numeri e ordini di servizio. Da una postazione successiva, distante diversi chilometri, un addetto dotato di cannocchiale riceveva il messaggio e contemporaneamente lo ripeteva in modo che lo si vedesse dalla stazione successiva.



Senza voler qui ricostruirne la storia, la prima e più conosciuta forma di comunicazione per via elettrica di dati alfanumerici è costituita dal telegrafo Morse.

L'idea che Samuel Morse tradusse in pratica nel 1835 era abbastanza semplice: codificare ogni carattere in una sequenza univoca di "punti" e "linee" (marks) intervallati da spazi ("spaces") da trasmettersi con un tasto manipolatore e da riceversi con un apparecchio capace di scrivere i punti e le linee su di una striscia di carta.

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	7/48

INTERNATIONAL MORSE CODE

1. A dash is equal to three dots.
2. The space between parts of the same letter is equal to one dot.
3. The space between two letters is equal to three dots.
4. The space between two words is equal to five dots.

A	• —	U	• • —
B	— • • •	V	• • • —
C	— • — •	W	• — —
D	— • •	X	— • • —
E	•	Y	— • — —
F	• • — •	Z	— — • •
G	— — •		
H	• • • •		
I	• •		
J	• — — —		
K	— • —	1	• — — — —
L	• — • •	2	• • — — —
M	— —	3	• • • — —
N	— •	4	• • • • —
O	— — —	5	• • • • •
P	• — — •	6	— • • • •
Q	— — • —	7	— — • • •
R	• — • •	8	— — — • •
S	• • •	9	— — — — •
T	—	0	— — — — —

In realtà mr. Morse lavorò in due aree ben distinte:

l'idea di base nella sua forma generale, che condusse alla creazione della codifica Morse (tabella precedente);

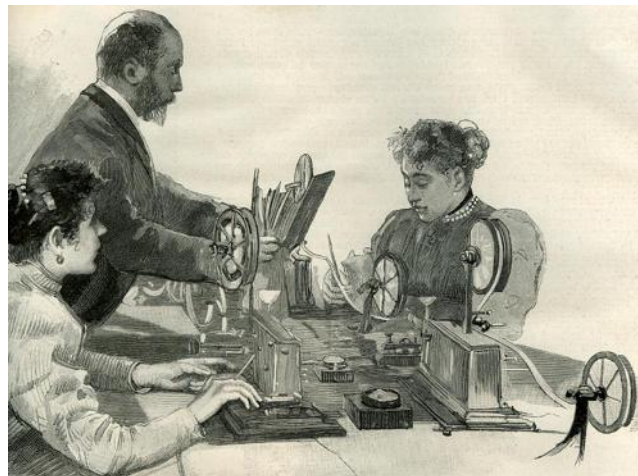
l'implementazione pratica del sistema telegrafico e dei relativi apparati.

L'idea di base, come si comprende, era del tutto svincolata dalla sua attuazione, tanto che il codice Morse è usato tuttora in trasmissioni effettuate per mezzo di quella radio che ai tempi del sig. Morse non era ancora stata inventata.



Un apparato telegrafico per codice Morse

4.2 La telegrafia automatica



Operatrici di telegrafo Morse

Se codice Morse rappresenta un importante traguardo nella evoluzione delle comunicazioni, esso non è tuttavia esente da difetti. Primo fra tutti quello di richiedere operatori addestrati che, per primi, costituivano il limite all'evoluzione di questo mezzo; un operatore molto bravo riesce a raggiungere solo i 100 caratteri al minuto.

A questi inconvenienti cercò di porre rimedio, circa 35 anni dopo, un certo sig. Emile Baudot.

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	9/48

Egli creò un codice simile al Morse ma passibile di essere generato ed interpretato per via meccanica, destinato a diventare, con qualche successiva evoluzione, la base delle più importanti tecniche moderne di comunicazione.

Nel codice Baudot tutti i caratteri hanno la stessa durata pari a cinque "unità", o "bit", come diciamo oggi. Ogni unità può essere "presente" o "assente" (tasto rilasciato, unità "vuota", stato logico "0").

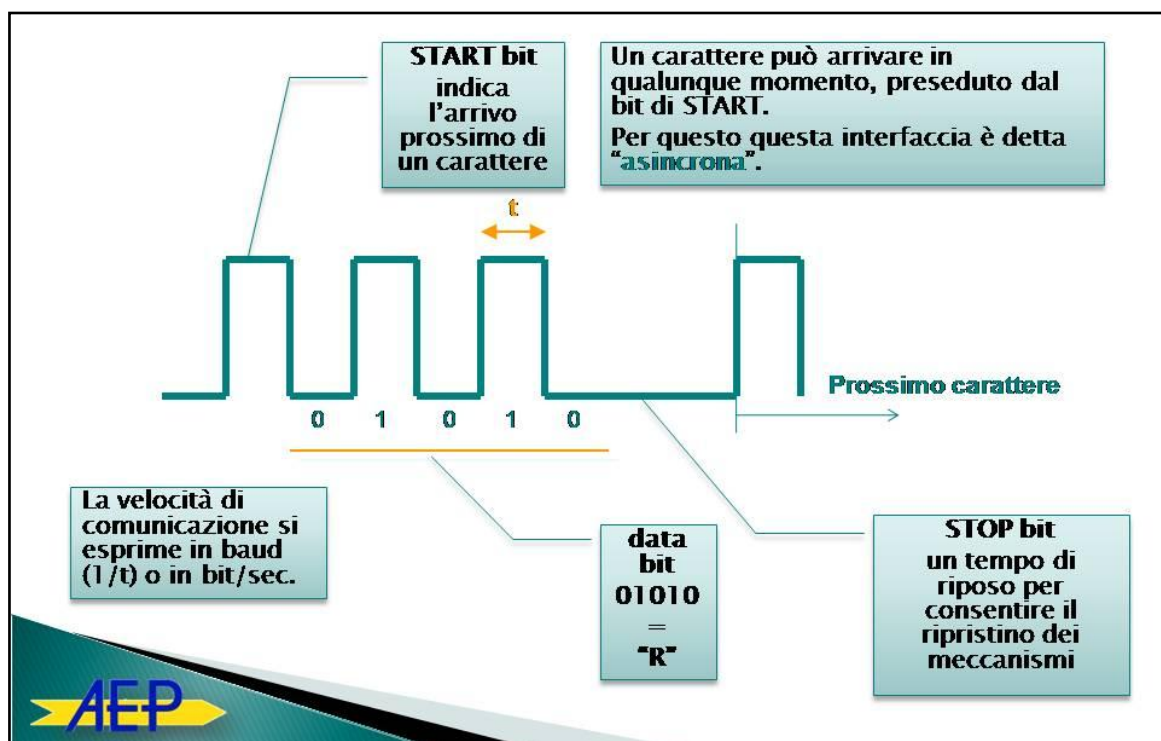
Allo stato "presente" o "assente" sono stati attribuiti vari nomi:

"mark" = tasto premuto, linea chiusa, ossia percorsa da corrente, stato logico "1";

"space" = tasto rilasciato, linea aperta, stato logico "0".

I termini "mark" e "space" sono i più usati, per analogia con la terminologia telegrafica:

Nella telegrafia Baudot un carattere può iniziare con un "mark" o con uno "space". E' quindi necessario anteporre alla trasmissione di ogni carattere uno "space" che anticipa il prossimo arrivo di un carattere. Questo bit aggiunto è chiamato "bit di start".



Trasmissione seriale in codice Baudot a 5 bit

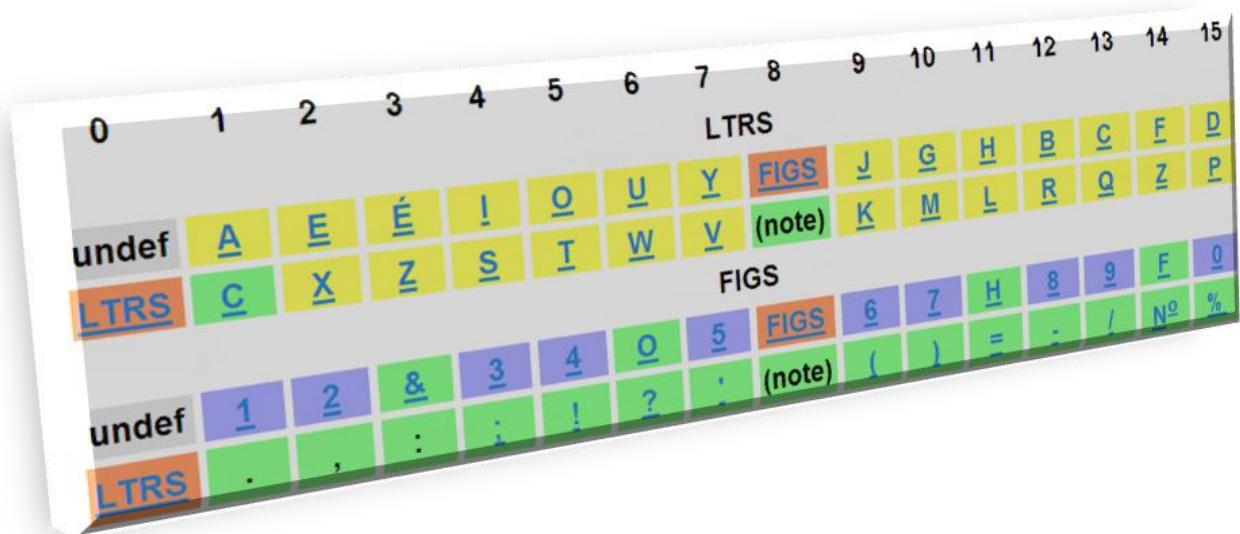
I meccanismi usati per la decodifica richiedono un tempo di ripristino per essere pronti ad accettare il carattere successivo. Per questo motivo fu

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	10/48

deciso di aggiungere in coda al carattere uno o più "bit di stop", che assumono sempre il valore "mark".

Essendo tutti i vari suddetti bit inviati uno dietro all'altro e in qualunque momento, questo tipo di comunicazione viene detto **"seriale asincrona"**.

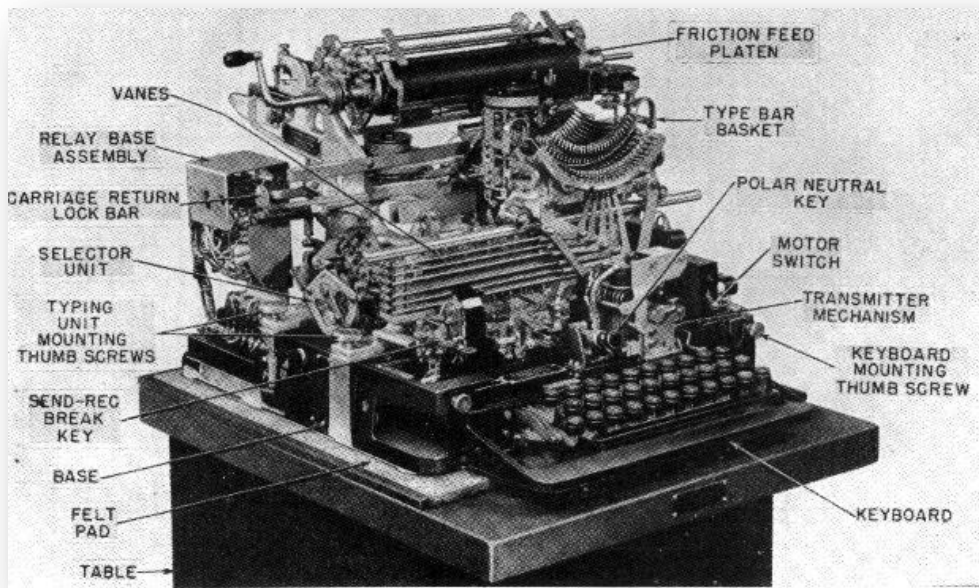
Poiché 5 bit si fanno solo 32 combinazioni, non sufficienti, quindi, per tutte le lettere, i numeri ed i segni di interpunzione, il sistema Baudot prevede un carattere speciale per passare da un set di caratteri (LTRS, lettere) ad un altro (FIGS, "figures", ossia cifre e segni).



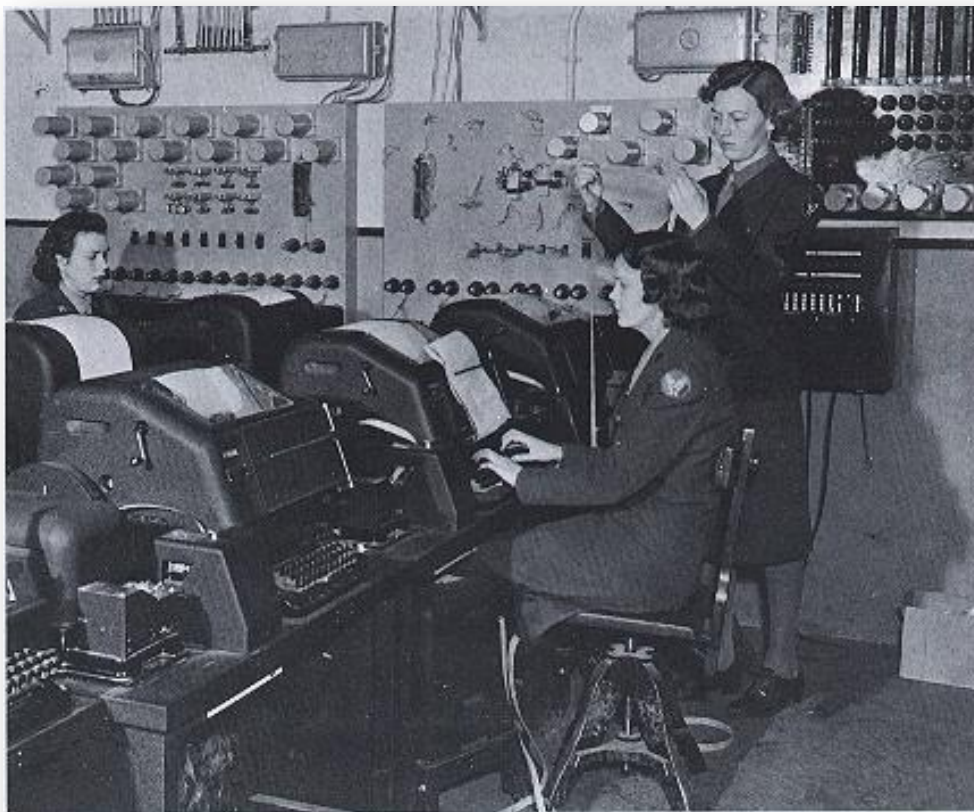
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
LTRS															
undef	A	E	É	I	O	U	Y	FIGS	J	G	H	B	C	F	D
LTRS	C	X	Z	S	T	W	V	(note)	K	M	L	R	Q	Z	P
FIGS															
undef	1	2	&	3	4	O	5	FIGS	6	7	H	8	9	F	0
LTRS	.	,	:	;	!	?	:	(note)	()	=	-	/	Nº	%

Il codice Baudot

Il codice Baudot conobbe ampissima diffusione; tutto il sistema Telex, in funzione fino a pochi anni fa, era basato su di esso e su macchine simili a quelle ideate da monsieur Baudot, così come le comunicazioni delle principali agenzie di stampa.



Telescrivente Teletype TG7 basata sul metodo Baudot



WACs assigned to the Eighth Air Force in England operate teletype machines. (DOD photograph)

Telescriventi TG7 utilizzate dagli alleati nella seconda guerra mondiale

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	12/48

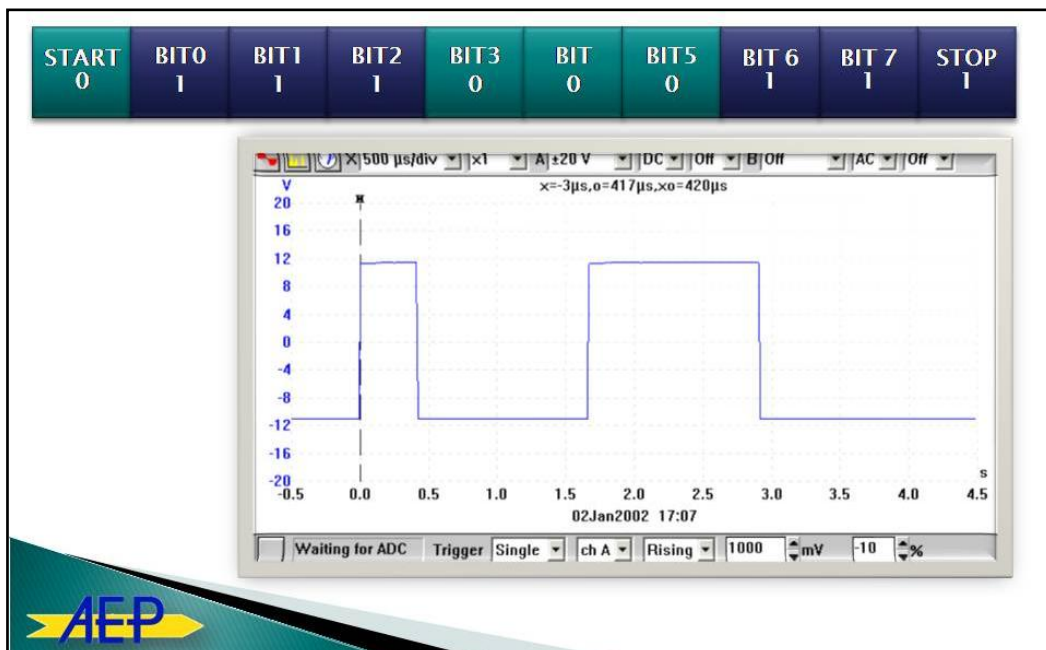
4.3 Il codice ASCII



Il codice ASCII a 7 bit

Può stupire che il codice ASCII (American Standard Code for Information Interchange - ISO 646), pubblicato nel 1967 ed utilizzato nelle moderne comunicazioni seriali differisca da quello originale di Emile Baudot solo per avere una differente codifica ed un maggiore numero di bit, 7 invece dei 5 originali, per evitare il meccanismo LETTERE/CIFRE.

Anche i 7 bit si dimostrarono però insufficienti (128 combinazioni), per cui si usa oggi il codice ASCII esteso, ad 8 bit (256 combinazioni).



La codifica ASCII del carattere "G" espressa in bit ed esaminata all'oscilloscopio.
Si osservi che la trasmissione inizia dal bit meno significativo.

4.4 Temporizzazioni

I limiti di velocità imposti dalla tecnologia elettromeccanica sono fortemente attenuati dall'impiego di circuiti elettronici.

La velocità di trasmissione, detta anche "**baud rate**", è espressa di solito in Baud, pari al reciproco della durata di un singolo bit. Ad esempio, a 9.600 baud corrisponde un tempo di bit di circa 104 us.

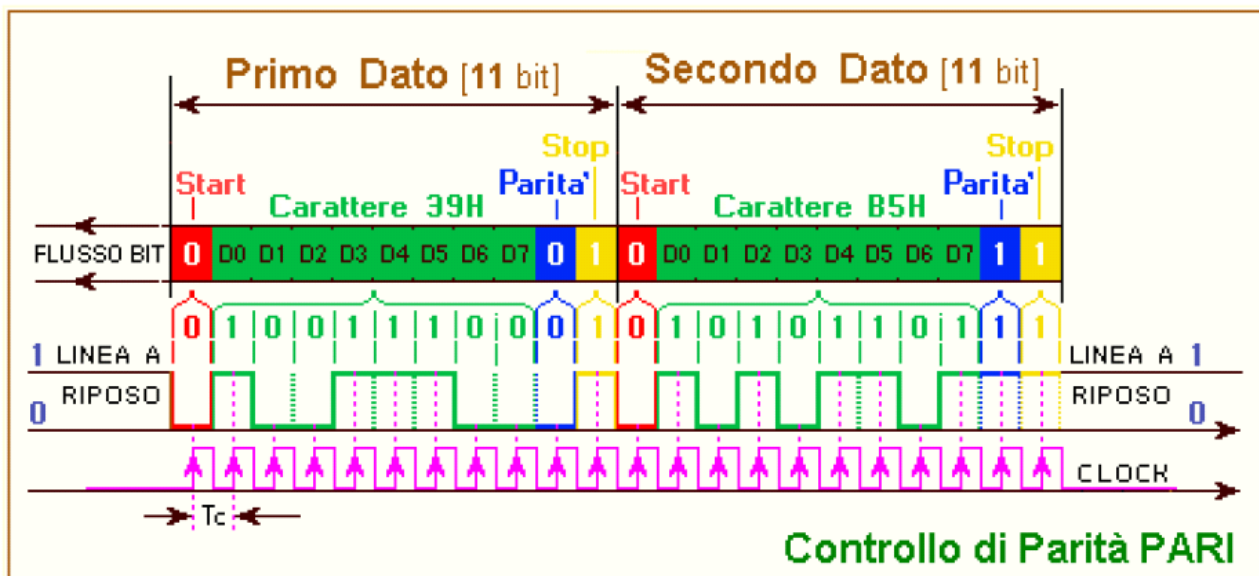
Per motivi storici si usano di solito i valori standard di 110, 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 e 115200 baud.

I bit di stop possono invece essere 1, 1 e $\frac{1}{2}$ o 2, anche se in pratica si usa solo il valore 1.

4.5 La parità

Per riconoscere eventuali errori dovuti ad interferenze o difetti dei meccanismi, fu pensato di aggiungere ad ogni carattere un bit ridondante, detto di "**parità**". Detto bit è posto a 1 nel caso in cui nel carattere i bit a 1 siano in numero dispari, mentre sarà posto a 0 nel caso in cui nel byte i bit a 1 siano in numero pari. Dovendo per esempio trasmettere la sequenza di bit 10011010, il bit di parità sarà uguale a 0.

Sono usate tanto la parità pari, quella ora descritta, che quella dispari, in logica negata (bit settato per fare gli "1" in numero dispari).



Controllo di parità

Questo sistema di controllo non è infallibile, infatti se nella trasmissione di un singolo carattere dovessero verificarsi contemporaneamente un numero pari di errori, il bit di parità non sarà in grado farli rilevare.

4.6 Numero dei bit

Il bit di parità viene aggiunto a quelli che compongono il carattere. Per definire compiutamente la trasmissione, oltre al baud rate, si devono quindi indicare:

- il numero dei bit che compongono il carattere (5, 6, 7 od 8);
- se si usa un ulteriore bit per parità;
- se la parità è pari o dispari o, in rari casi, fissa ad "1" o fissa a "0";
- quanti bit di stop devono essere aggiunti.

4.7 Controllo di flusso

In alcune circostanze è auspicabile poter sincronizzare due dispositivi, in modo tale che quello più lento possa bloccare la trasmissione da parte dell'altro quando non sia più in grado di seguire il flusso dei dati, per poi riattivarla non appena pronto.

Per questo motivo, in alcuni tipi di comunicazioni seriali, ad esempio quelle verso modem è prevista l'adozione del **controllo di flusso**, detto anche "handshaking" ("stretta di mano").

Il controllo di flusso può avvenire in due diverse maniere sostanzialmente diverse, come illustrato nei paragrafi successivi.

4.7.1 Controllo di flusso per via hardware

Il controllo di flusso per via hardware è ottenuto aggiungendo opportuni segnali all'interfaccia; ad esempio un uscita sull'apparato A che segnala che il ricevitore è pronto a ricevere dati ed un ingresso sull'apparato B che "legge" la condizione di "pronto" da parte del ricevitore. Quando il ricevitore non è più in grado di ricevere, esso "nega" l'uscita di "pronto". Questa condizione viene letta dall'apparato trasmettitore che sospende la trasmissione. Quando il ricevitore ha processato i dati in arrivo, asserisce l'uscita "pronto" invitando il corrispondente a riprendere l'invio.

In caso di trasmissione bidirezionale, ovviamente, questo meccanismo deve essere raddoppiato.

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	15/48

4.7.2 Controllo di flusso per via software

Il controllo di flusso per via software è ottenuto, in una trasmissione full duplex, inviando speciali caratteri di controllo che sicuramente non appartengono all'insieme dei caratteri utilizzabili per le normali comunicazioni con il significato di "arresta trasmissione" e di "invito a trasmettere". Nel codice ASCII questi caratteri sono di solito lo X-OFF e lo X-ON, rispettivamente.

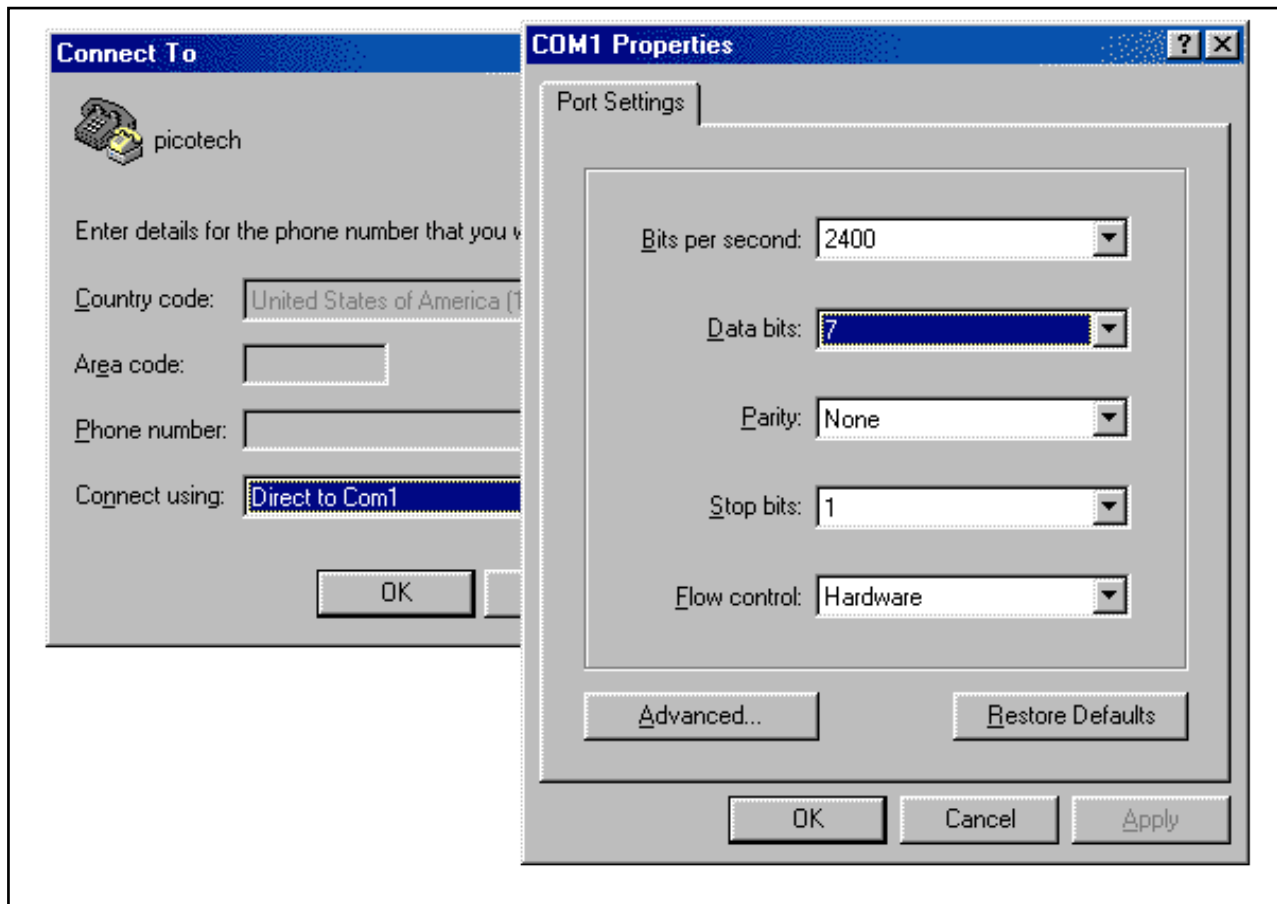
Se la comunicazione prevede l'invio di dati binari qualunque, questa tecnica non è utilizzabile, in quanto i dati stessi potrebbero casualmente contenere i caratteri di controllo, a meno che le regole di dialogo siano stabilite da un protocollo (vedere nel seguito).

Il controllo di flusso software è sempre meno indispensabile sugli apparati embedded, a causa delle maggiori prestazioni degli apparati stessi e della loro estesa memoria che consente comunque di ricevere grandi blocchi di informazioni. Quando necessario quello software è sempre preferito, ove possibile, su quello di tipo hardware a causa della minore complessità dei circuiti da collegare.

4.8 Configurazione

I numerosi parametri che caratterizzano la comunicazione seriale, questa deve essere di regola "configurata". Si vedano ad esempio, nella figura successiva, le finestre di configurazione del noto programma Windows "Hyperterminal". Si osservi, tra le altre, la casella della del "flow control" (controllo di flusso).

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	16/48



Vari parametri devono essere impostati per consentire il funzionamento della comunicazione seriale

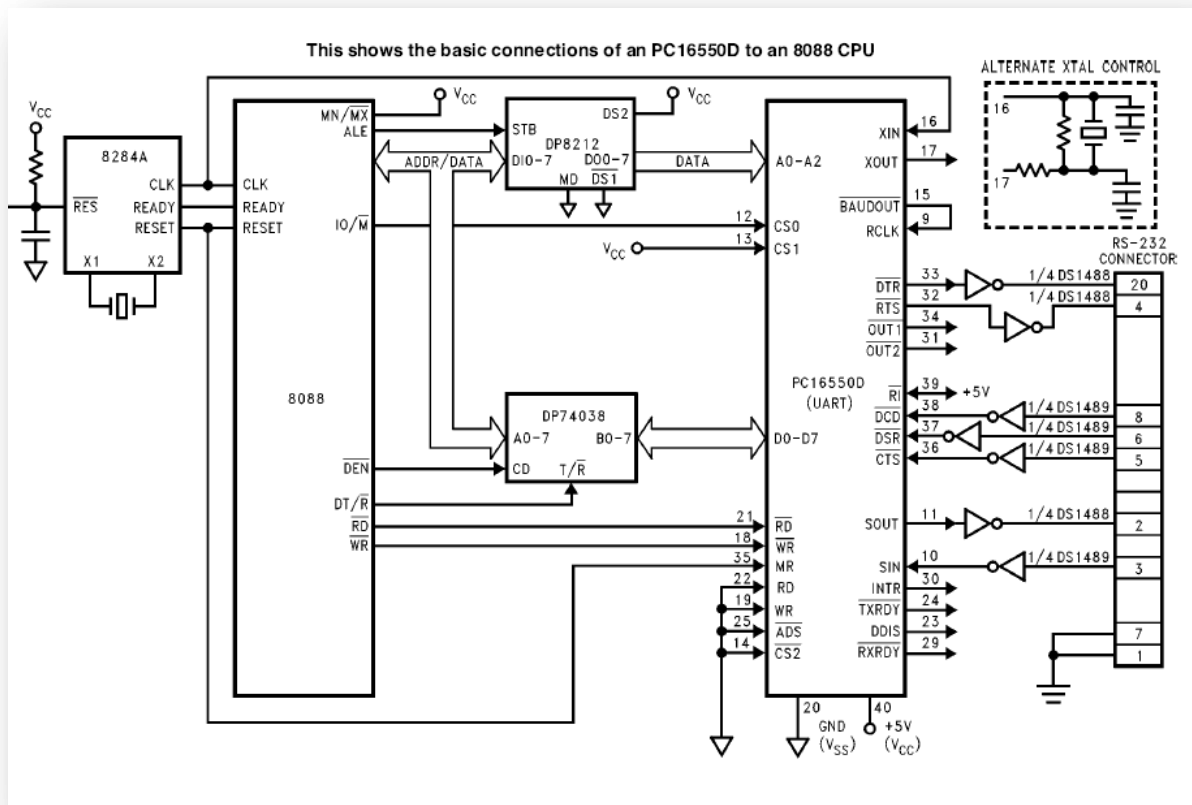
4.9 L'UART

Lo UART o Universal Asynchronous Receiver-Transmitter (ricevitore-trasmettitore asincrono universale) è l'implementazione allo stato solido dei meccanismi di ricezione e trasmissione della telescrivente Baudot.

Esso converte flussi di bit di dati dal formato parallelo al formato seriale asincrono o viceversa.

Tradizionalmente la UART è un componente ben individuato, anche se oggi una o più UART vengono integrate all'interno della CPU o di altri circuiti ad alta integrazione.

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	17/48



Interfacciamento tra CPU (8088) e UART (16550)

4.10 La bufferizzazione

Le UART prevedono delle opportune memorie ("buffer") per migliorare la capacità del circuito di ricevere e trasmettere dati velocemente. Il trasmettitore, ad esempio, consente di caricare il registro di uscita prima ancora che l'emissione del carattere precedente sia terminata, così come il ricevitore può prevedere una memoria FIFO (First In First Out) per immagazzinare i caratteri prima che il processore li abbia potuti leggere.

4.11 Riepilogo

Abbiamo visto in questo capitolo il funzionamento della comunicazione seriale asincrona per il trasferimento dati tra due apparati.

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	18/48

5. Interfacce elettriche

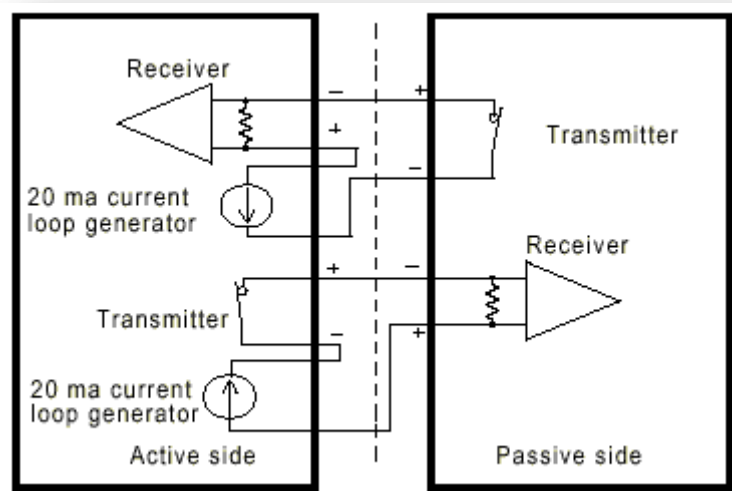
5.1 Generalità

Si è assunto, nel capitolo precedente, che sia possibile trasmettere tra due apparati un segnale elettrico digitale con due stati chiamati "0" (mark) e "1" (space), detto quindi binario.

Nel capitolo corrente si esamineranno le tecniche per la trasmissione di questo segnale.

5.2 Loop di corrente

La soluzione detta "a loop di corrente" è quella storica, largamente utilizzata nelle telescriventi ed oggi pressoché in disuso, tranne che su qualche sistema di bordo di precedente generazione.



Loop di corrente full duplex

Con riferimento alla figura precedente, si osservi come il contatto di manipolazione telegrafica sia posto in serie ad un circuito elettrico a corrente costante. Nelle telescriventi meccaniche l'organo ricevitore è costituito da una elettrocalamita che, disattivandosi, sgancia un ancorina mobile che avvia il ciclo di ricezione.

Gli stati possibili della linea sono:

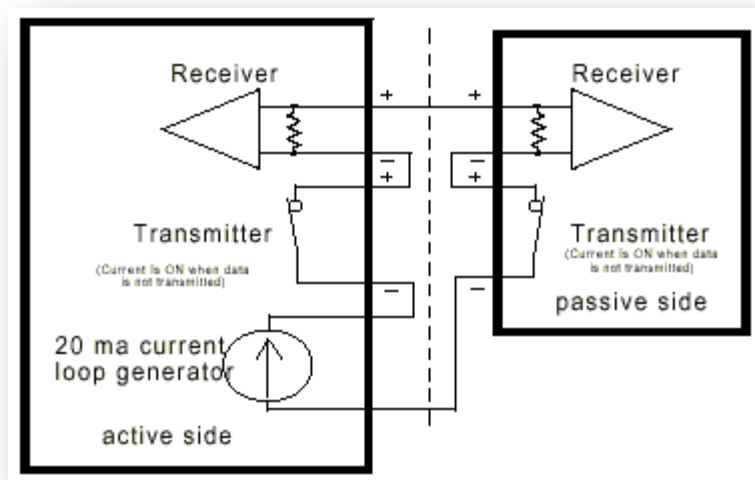
Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	19/48

mark - la linea è attraversata da corrente. Erano in uso standard a 20 o 60 mA;

space - la linea è aperta e quindi non è attraversata da corrente.

Il circuito è raddoppiato per consentire la comunicazione simultanea bidirezionale, detta "full duplex".

Nella figura successiva, invece, la configurazione "half duplex" che consente di ridurre il numero dei conduttori che compongono la linea, impedendo però la comunicazione simultanea nelle due direzioni.



Loop di corrente half duplex

Si osservi che i loop devono essere alimentati; il lato che fornisce l'alimentazione è detto "attivo".

Il metodo di trasmissione ora esaminato presenta limiti di velocità dovuti alla induttanza delle linee, che ritardano l'arrivo a regime della corrente o la sua interruzione. Si presta quindi solo a basse velocità di trasmissione.

5.3 Codifica in tensione

Un altro metodo per trasmettere lo stato "0/1" è costituito dalla codifica in tensione. In esso si associa ciascuno stato ad un valore di tensione. Poiché non è possibile garantire nelle varie condizioni l'esattezza dei valori di tensione, si definiscono di solito dei ranghi di valori ammessi. Ad esempio, è possibile utilizzare la seguente codifica:

zero: tra 0 e 2V

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	20/48

uno: tra 3,5 e 5V

Si osservi che è stata volutamente lasciata una zona "proibita" per ridurre le condizioni di indeterminazione.

La tecnica più utilizzata è quella definita dallo standard EIA RS-232, descritta al paragrafo successivo.

5.4 EIA RS-232

5.4.1 Generalità

Lo standard EIA RS-232 nacque nei primi anni '60 per opera della "Electronic Industries Association" ed era orientato alla comunicazione tra i mainframe e i terminali attraverso la linea telefonica, utilizzando un modem.

Le porte seriali EIA RS-232 erano presenti, fino a non molto tempo fa, in quasi tutti i PC ma sono oggi soppiantate dall'interfaccia USB. Esse sono invece tuttora molto utilizzate in moltissimi gli apparati per impiego industriale nonché in quelli che compongono il Sistema Di Bordo.

5.4.2 Storia

Lo RS-232 è uno standard costituito da una serie di protocolli meccanici, elettrici ed informatici che rendono possibile lo scambio di informazioni a bassa velocità tra dispositivi digitali. Esso include le caratteristiche elettriche dei segnali, la struttura e temporizzazioni dei dati seriali, la definizione dei segnali e dei protocolli per il controllo del flusso di dati seriali su un canale telefonico, il connettore e la disposizione dei suoi pin ed infine il tipo e la lunghezza massima dei possibili cavi di collegamento.

Nel corso di oltre 40 anni lo standard si è evoluto, pur mantenendosi in larga parte invariato. L'evoluzione è riconoscibile dalla sigla, leggendo l'ultima lettera; l'ultima revisione è del 1997 ed è indicata come EIA RS-232f. Probabilmente la versione più diffusa è la RS232c, del 1969, corrisponde alle specifiche europee CCITT raccomandazione V.24

Le informazioni riportate nel seguito sono relative principalmente al livello elettrico, sono state codificate inizialmente dallo standard EIA/TIA-232-E (sezione 2) e successivamente modificate in alcuni dettagli secondari dallo standard EIA/TIA-562.a

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	21/48

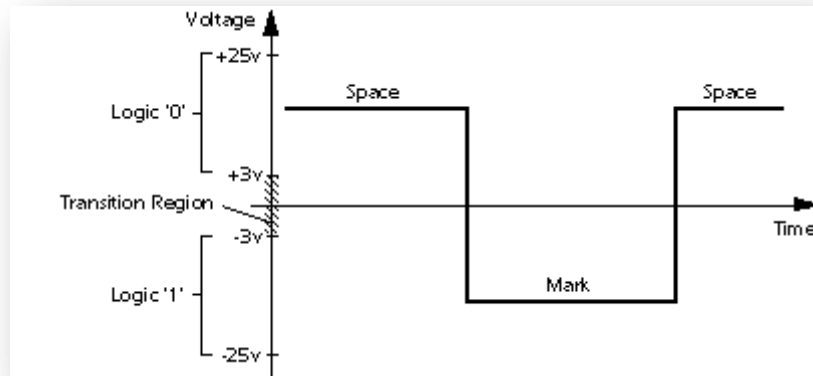
5.4.3 Livelli elettrici

I livelli elettrici previsti dallo standard sono tre:

mark: tensione compresa tra -3 e -25 V, di solito -12 V;

space: tensione compresa tra +3 e +25 V, di solito +12 V;

incertezza: tensione compresa tra -3 e +3 V.



La tensione di uscita ad un trasmettitore EIA RS-232 deve essere compresa in valore assoluto tra 5 V e 25 V (quest'ultimo valore ridotto a 13 V in alcune revisioni dello standard). A volte le tensioni in uscita sono intenzionalmente diminuite a +/- 6 V anziché 12 V per permettere minori emissioni elettromagnetiche, sempre critiche, e favorire maggiori velocità di trasmissione.

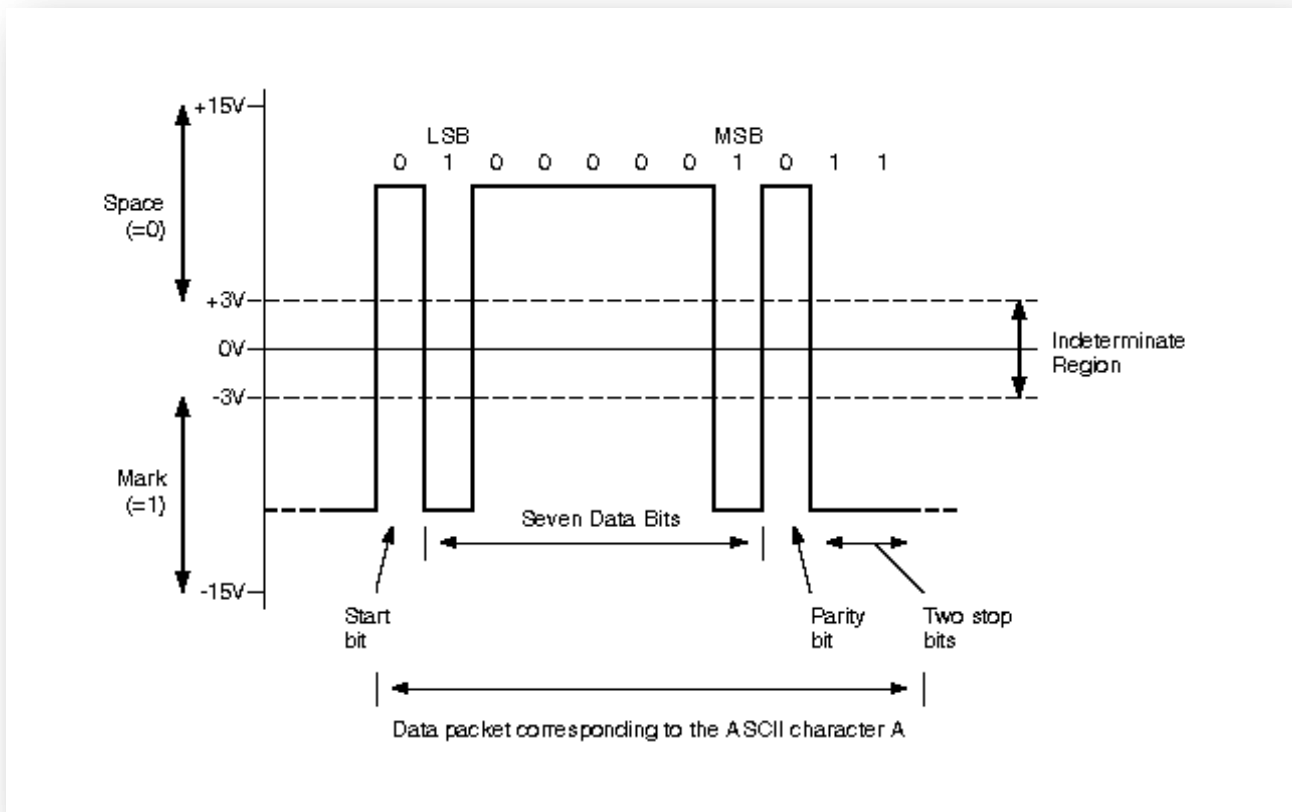
Il ricevitore deve funzionare correttamente con tensioni di ingresso comprese, sempre in modulo, tra i 3 V ed i 25 V. Molti ricevitori commerciali considerano semplicemente una tensione di soglia al valore di +2 V (sopra viene riconosciuto un segnale alto, sotto uno basso) anche se ciò non è pienamente aderente alla norme.

Lo slew-rate (cioè la pendenza del grafico del segnale nel passare da 1 a 0 o viceversa) deve essere minore di 30 V/us per evitare eccessive emissioni elettromagnetiche.

5.4.4 Massima distanza

Essendo la linea RS-232 di tipo non bilanciato (vedi nel seguito), essa è soggetta a raccogliere disturbi di natura elettrica; la massima distanza raccomandata per la connessione è inferiore ai 15 metri.

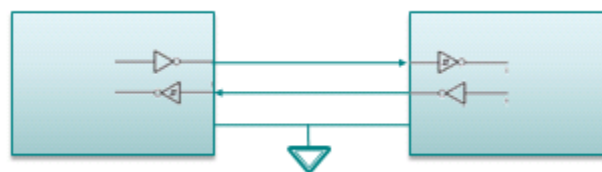
Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	22/48



Un esempio di trasmissione RS-232 del carattere 'A'

5.4.5 Circuito a 3 fili

Il collegamento più usato tra apparati muniti di interfaccia RS-232 è quello detto "a tre fili", appunto perché fa impiego di soli 3 conduttori, essendo la massa a comune.



RS-232 – circuito a 3 fili

Ove richiesto il controllo di flusso per via hardware (tipicamente nei modem), i conduttori utilizzati possono essere in numero maggiore, come mostrato nella seguente figura.

5.4.6 Circuito con controllo di flusso

Il circuito con controllo di flusso previsto originariamente dallo standard è molto complesso perché prevede l'impiego di un grande numero di segnali

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	23/48

(figura successiva). Nella realtà esso non è più utilizzato, in quanto per semplicità si preferisce ricorrere, anche ove indispensabile, al controllo di flusso software.

pin	lato DTE		Direzione	lato DCE	
	Descrizione			Descrizione	pin
1	Protective Ground	-	Protective Ground	1	
2	Transmitted Data	[DTE>DCE]	Received Data	2	
3	Received Data	[DCE>DTE]	Transmitted Data	3	
4	Request To Send	[DTE>DCE]	Clear To Send	4	
5	Clear To Send	[DCE>DTE]	Request To Send	5	
6	Data Set Ready	[DCE>DTE]	Data Set Ready	6	
7	Signal Ground	-	Signal Ground	7	
8	Data Carrier Detect	[DCE>DTE]	Data Carrier Detect	8	
9	Reserved	-	Reserved	9	
10	Reserved	-	Reserved	10	
11	Unassigned	-	Unassigned	11	
12	Secondary Data Carrier Detect	[DCE>DTE]	Secondary Data Carrier Detect	12	
13	Secondary Clear To Send	[DCE>DTE]	Secondary Request To Send	13	
14	Secondary Transmitted Data	[DTE>DCE]	Secondary Received Data	14	
15	Transmission Element Timing	[DCE>DTE]	Transmission Element Timing	15	
16	Secondary Received Data	[DCE>DTE]	Secondary Transmitted Data	16	
17	Receiver Element Timing	[DCE>DTE]	Receiver Element Timing	17	
18	Local Loopback	[DTE>DCE]	Local Loopback	18	
19	Secondary Request To Send	[DTE>DCE]	Secondary Clear To Send	19	
20	Data Terminal Ready	[DTE>DCE]	Data Terminal Ready	20	
21	Remote LoopBack	[DTE>DCE]	Remote LoopBack	21	
22	Ring Indicator	[DCE>DTE]	Ring Indicator	22	
23	Data Signal Rate Selector	[DTE>DCE]	Data Signal Rate Selector	23	
24	Transmitter Element Timing	[DTE>DCE]	Transmitter Element Timing	24	
25	Test Mode	[DCE>DTE]	Test Mode	25	

5.5 Interfaccia differenziale

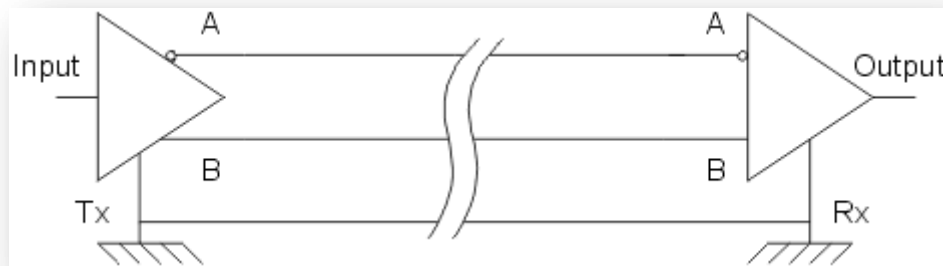
In generale quando 2 conduttori corrono paralleli tra loro (cosa normale per quelli racchiusi nel cavo seriale) il segnale di uno può interferire con quello dell'altro e viceversa, generando distorsioni e attenuazioni intollerabili.

Ancor più problematico è il fatto che un conduttore, tanto più è lungo, tanto più si comporta come un'antenna e tende quindi a raccogliere tutti i

disturbi di natura elettrica di cui l'etere è saturo, ad esempio anche le stesse trasmissioni radio.

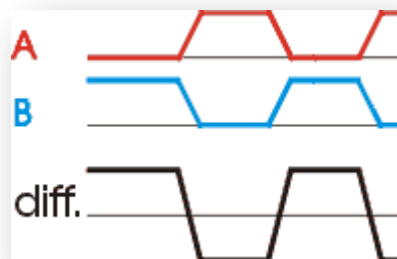
La schermatura risolve solo in parte il problema e ne aggiunge un altro, causato dalla capacità elettrica eccessiva, che determina distorsioni nei fronti e limita la velocità raggiungibile.

E' pertanto divenuto di uso comune l'impiego di linee differenziali bilanciate che utilizzano due conduttori, al posto di uno, per ciascun segnale, oltre a quello di massa, non indispensabile in teoria ma previsto per evitare eccessive differenze di potenziale tra gli apparati.



Linea differenziale bilanciata

Nella linea bilanciata il segnale da trasmettere viene convertito in due segnali uguali e simmetrici (A e B) come mostrato nella figura seguente:



I due stati di ciascuna linea sono definiti nel seguente modo:

quando il terminale A è negativo rispetto a B, la linea rappresenta un uno binario. Tale stato rappresenta anche l'assenza di segnale (idle state);

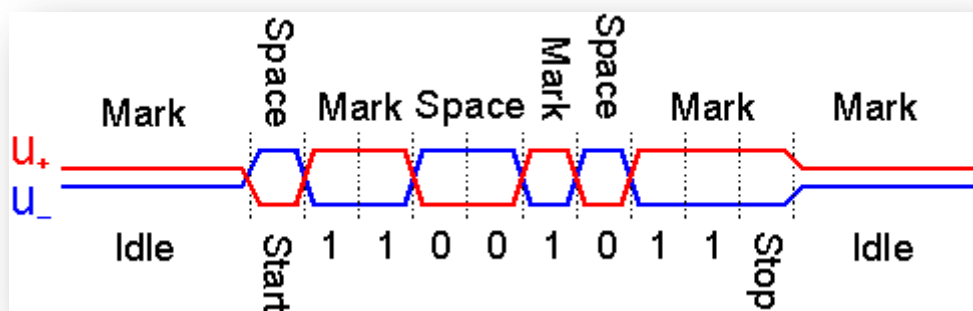
quando il terminale A è positivo rispetto a B, la linea rappresenta uno zero binario.

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	25/48

Il circuito ricevitore, di tipo particolare, presenta alla propria uscita un segnale uguale alla **differenza** dei due segnali in ingresso, che rende tale e quale il segnale di partenza ("diff" nella figura precedente).

Questa caratteristica fa sì che, qualunque sia il livello di rumore raccolto dai cavi, esso si ritrovi in maniera pressoché uguale su ciascuno dei due conduttori. L'operazione differenza, quindi, lo annulla del tutto, restituendo integro il segnale contenente l'informazione.

Nella pratica, ovviamente, il livello massimo di rumore ammissibile è limitato dalle caratteristiche fisiche dei dispositivi.



Andamento dei segnali nella linea bilanciata in assenza di rumore. Nei tratti indicati come "idle" la linea non viene pilotata.

5.6 Interfaccia EIA RS-422

Lo standard USA ANSI/TIA/EIA-422-B (in precedenza RS-422) ed il suo equivalente internazionale "ITU-T Raccomandazione V.11" (conosciuta anche come X.27), sono le normative tecniche che stabiliscono le "caratteristiche elettriche dei circuiti per l'interfaccia digitale a tensione bilanciata".

L'interfaccia RS-422 è logicamente simile alla RS-232 ma utilizza, per ciascun segnale, una linea differenziale bilanciata. Prevede la possibilità di ricevitori multipli ma non di più trasmettitori sulla stessa linea.

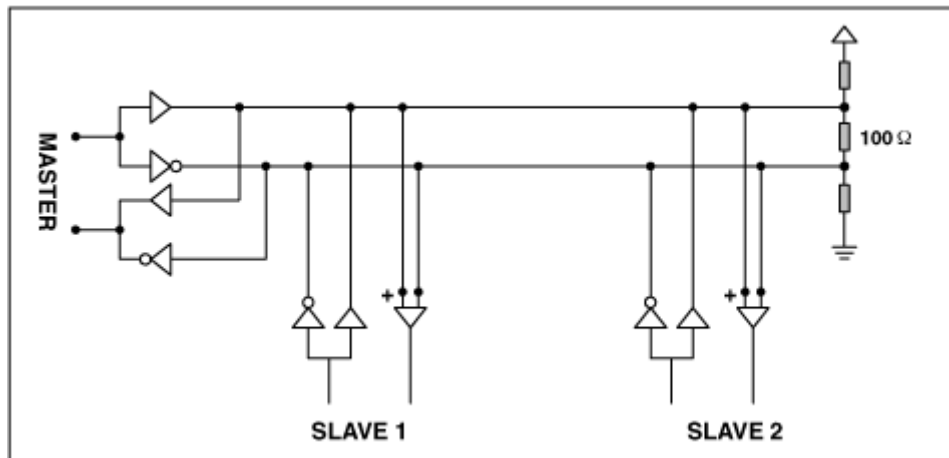
Non è frequentemente utilizzata nell'ambito dei sistemi di bordo, ove si preferisce la più flessibile RS-485 descritta nel prossimo paragrafo.

5.7 Interfaccia EIA RS-485

EIA RS-485, equivalente allo standard Europeo CCITT V11, è una specifica di livello fisico per un'interfaccia seriale a due fili su linea differenziale

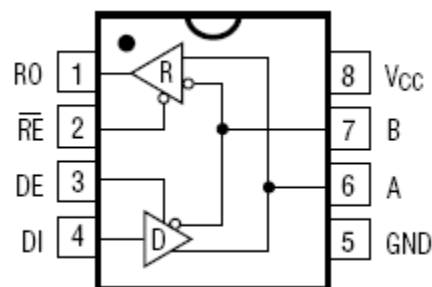
Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	26/48

bilanciata, half-duplex e multipoint, ossia in grado di unire più dispositivi, ciascuno dei quali può ascoltare o parlare.



Una tipica linea RS-485 – solo un trasmettitore alla volta può essere abilitato.

La figura sottostante riporta lo schema di un tipico circuito di interfaccia RS-485 (Maxim MAX485).



In esso si osservano:

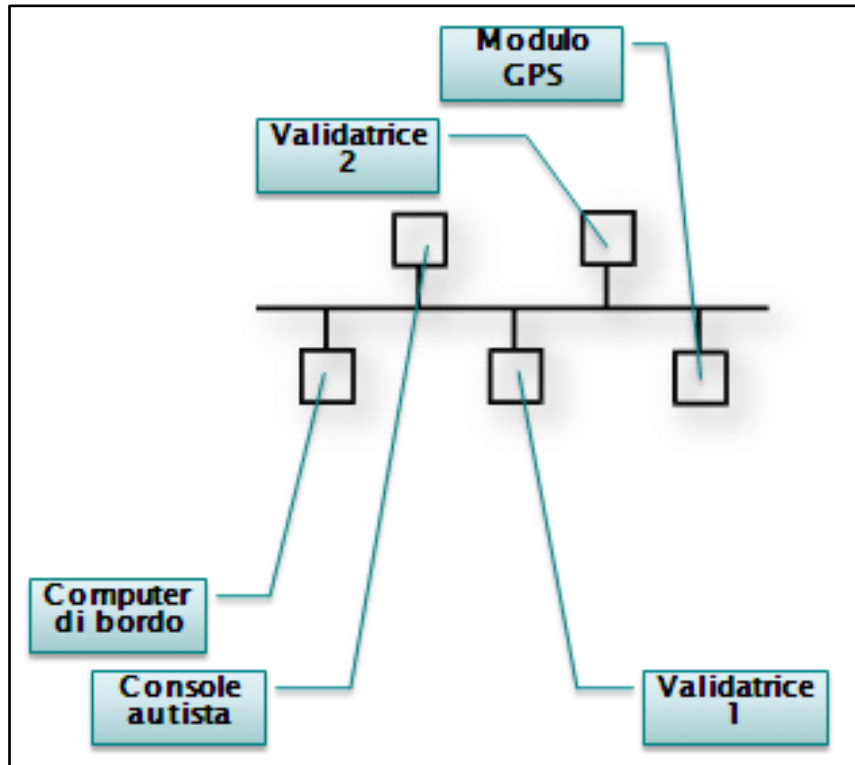
- due pin di alimentazione (Vcc e GND);
- i due pin di collegamento alla linea (A e B);
- l'ingresso del trasmettitore (DI, Data In);
- l'abilitazione del trasmettitore (DE, Data Enable);
- l'uscita del ricevitore (RO, Receiver Output);
- l'abilitazione del ricevitore (\overline{RE} , Receiver Enable).

Si osservi che l'abilitazione del ricevitore può essere di qualche comodità per il progettista ma non rientra logicamente nelle considerazioni precedenti.

EIA RS-485 permette di realizzare semplici reti locali a basso costo con velocità di trasmissione anche molto elevate (35 Mbit/s fino a 10 m e 100 kbit/s a 1.200 m) e si presta ottimamente, quindi, per la costruzione della dorsale di comunicazione del Sistema Di Bordo (esempio nella figura sottostante).

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	27/48

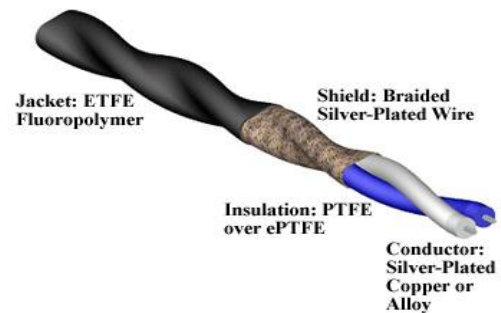
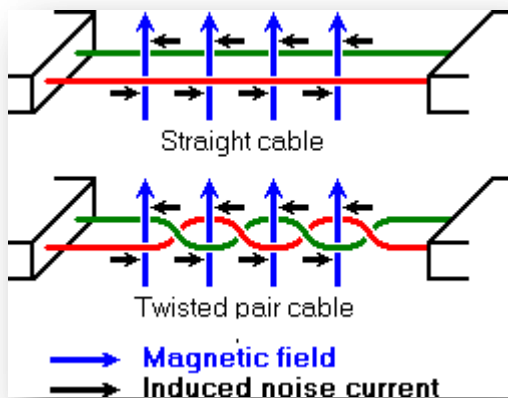
Nei Sistema Di Bordo, comunque, ben difficilmente viene superato il valore di 115.200 baud, anche in considerazione del limitato volume degli scambi da effettuare.



Un tipico sistema di bordo basato su linea RS-485

5.8 Cablaggio di una linea differenziale

Il cablaggio di una linea differenziale, per conseguire i migliori risultati anche dal punto di vista delle emissioni elettromagnetiche, deve di regola avvenire usando un doppino avvitricolato ("twisted pair"), in quanto, come mostrato in figura, le correnti di rumore si annullano su ogni "anello".



5.9 Riepilogo

In questo capitolo sono state esaminate le varie interfacce elettriche comunemente impiegate nelle trasmissioni seriali asincrone.

La tabella sottostante riporta una comparazione tra i vari tipi che sono stati descritti.

	RS232	RS423	RS422	RS485
Differential	no	no	yes	yes
Max number of drivers	1	1	1	32
Max number of receivers	1	10	10	32
Modes of operation	half duplex full duplex	half duplex	half duplex	half duplex
Network topology	point-to-point	multidrop	multidrop	multipoint
Max distance (acc. standard)	15 m	1200 m	1200 m	1200 m
Max speed at 12 m	20 kbs	100 kbs	10 Mbs	35 Mbs
Max speed at 1200 m	(1 kbs)	1 kbs	100 kbs	100 kbs
Max slew rate	30 V/ μ s	adjustable	n/a	n/a
Receiver input resistance	3..7 k Ω	\geq 4 k Ω	\geq 4 k Ω	\geq 12 k Ω
Driver load impedance	3..7 k Ω	\geq 450 Ω	100 Ω	54 Ω
Receiver input sensitivity	\pm 3 V	\pm 200 mV	\pm 200 mV	\pm 200 mV
Receiver input range	\pm 15 V	\pm 12 V	\pm 10 V	-7..12 V
Max driver output voltage	\pm 25 V	\pm 6 V	\pm 6 V	-7..12 V
Min driver output voltage (with load)	\pm 5 V	\pm 3.6 V	\pm 2.0 V	\pm 1.5 V

6. I protocolli

6.1 Generalità

Nei precedenti capitoli sono stati descritti:

- i principi di funzionamento della comunicazione seriale asincrona;
- le interfacce elettriche utilizzate per il collegamento di apparati muniti di interfacce seriali asincrone ed i loro standard di riferimento.

E' importante osservare che gli standard esaminati specificano soltanto le caratteristiche elettriche del trasmettitore e del ricevitore e non indicano né raccomandano alcuna tecnica di composizione e di scambio dei dati.

Nel capitolo corrente esamineremo invece i protocolli di comunicazione, ossia le regole che stanno alla base degli scambi di informazioni.

6.2 Controllo degli errori

La trasmissione basata su segnali elettrici è soggetta a subire vari tipi di interferenza. Se, entro certi limiti, un messaggio testuale può essere facilmente corretto da parte di un operatore sulla base dell'intuizione (es. "QUESTO MESSAGGIO NON CONTIENE ERRORI DI STXMPA"), grazie alla ridondanza dei linguaggi umani, ciò non avviene per le macchine, che, dalla ricezione di un carattere errato potrebbero far derivare comportamenti erronei o addirittura dannosi.

Si deve quindi provvedere un mezzo per il controllo della correttezza dei dati ricevuti.

Un primo metodo elementare, quello del controllo di parità, è già stato esaminato in precedenza, ma, come si è detto, è in grado solo di rilevare errori minimi; già due bit perduti portano all'errato esito positivo del controllo.

Un metodo più evoluto è quello di frazionare il messaggio in "pacchetti" e di aggiungere, in coda a ciascuno di essi, un codice di controllo. Qualcosa di simile avviene per il numero degli assegni: si esegue la somma di tutte le cifre e la si riporta in coda al numero stesso. Esistono metodi più o meno complessi ed affidabili per costruire un codice di controllo e si può

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	30/48

affermare in generale che esiste la maniera di sapere se un certo pacchetto di informazioni è stato ricevuto correttamente o meno.

Come esempio di strutturazione dei dati in pacchetti, si esamini la seguente figura:



Strutturazione dei dati in pacchetti

In esso si riconoscono i seguenti elementi:

STX (Start Of Text) - carattere speciale che indica l'inizio del pacchetto

LEN - numero dei byte che compongono il pacchetto

EXT (End Of Text) - carattere speciale che indica la fine del pacchetto

CKS - codice di controllo

6.3 Regole di comportamento

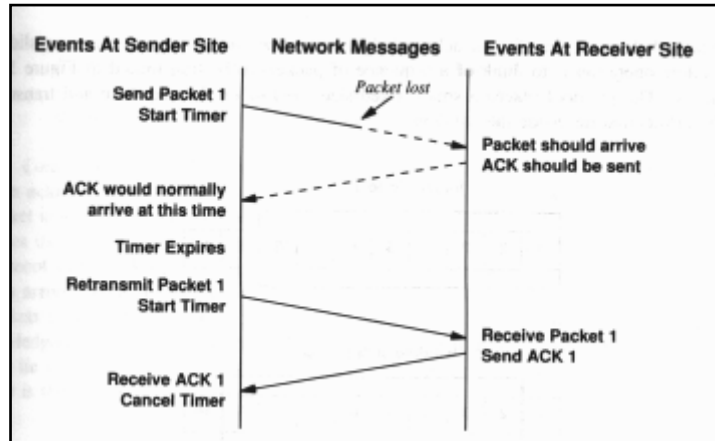
E' opportuno stabilire un "protocollo" per convenire il comportamento del trasmettitore e del ricevitore da adottarsi nei due casi in cui il pacchetto sia stato riconosciuto come giusto o come errato.

Di solito, se il pacchetto è stato ricevuto correttamente, si invia una CONFERMA, viceversa una NON CONFERMA, in modo tale da invitare il corrispondente ad effettuare la ritrasmissione del pacchetto incriminato.

La CONFERMA/NON CONFERMA può essere costituita da un carattere speciale o da un intero pacchetto, a seconda della logica prevista dall'estensore del protocollo. Ma cosa succede se il messaggio CONFERMA/NON CONFERMA non viene ricevuto o ricevuto erroneamente?

E' necessario quindi stabilire una serie di regole complesse che assicurino una funzionalità tanto migliore tanto più accuratamente saranno state studiate.

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	31/48



Un esempio di regola di comportamento di un protocollo (UDP/IP)

6.4 I protocolli

I protocolli sono quindi gli standard che stabiliscono come avvengono i trasferimenti da una macchina ad un'altra. Essi specificano come sono rappresentati i dati, le tecniche per la rivelazione d'errore e il meccanismo di conferma/non conferma per i pacchetti trasmessi.

6.5 Potenzialità del protocollo

Non tutti i protocolli sono adatti a risolvere gli stessi problemi. Si pensi ad esempio al numero dei protocolli utilizzati per il funzionamento di Internet. Per TCP/IP infatti non si intende solo il protocollo di trasmissione TCP ed il protocollo di rete IP, ma una famiglia di protocolli comprendente anche l'UDP, l'ICMP, l'ARP, il RARP ed altri, da cui però sono escluse le applicazioni quali la posta elettronica (E-mail), il trasferimento di file (FTP) e l'emulazione di terminale remota (TELNET).

Il livello di prestazioni richiesto ad un Sistema Di Bordo è tale da richiedere protocolli appositamente studiati; l'uso di protocolli come quelli sopra accennati sarebbe infatti inutilmente pesante.

I protocolli più comunemente impiegati in ambito embedded prevedono che una unità assolva le funzioni di "master", che si cioè quella che avvia i dialoghi con le unità subordinate dette "slave".

Normalmente, un protocollo adatto alla implementazione di un Sistema Di Bordo deve prevedere almeno le seguenti possibili operazioni:

- invio comando;
- richiesta stato;

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	32/48

invio file;
richiesta file.

6.6 Concordanza semantica

Ovviamente i protocolli di comunicazione hanno lo scopo di garantire il corretto trasferimento di dati da una unità ad un'altra.

L'utilità di questi dati è comunque subordinata alla conoscenza del loro significato; è del tutto inutile trasferire perfettamente un file di cui si ignora il significato.

6.7 Complessità e variabilità

Il problema dei protocolli è complesso anche perché:

- esistono molti livelli di prestazioni possibili;
- esistono molti casi e sottocasi da gestire, più di quanto sembri a prima vista;
- esistono più maniere di risolvere lo stesso problema.

Questo significa che, date due diverse gruppi di lavoro, ciascuno tenderà a risolvere il problema della creazione di un protocollo in modo diverso dall'altra, e infatti i protocolli differiscono sostanzialmente da Costruttore a Costruttore e spesso, per vari motivi, anche da apparato ad apparato pur della stessa marca.

E' possibile enunciare la seguente legge: **"dati due apparati, la probabilità che possano parlare tra loro è pressoché nulla"**, ovviamente a meno che non siano stati appositamente progettati. La complessità è accresciuta dai diversi tipi di interfacce elettriche possibili.

L'interoperabilità richiede ad esempio di:

- definire l'interfaccia elettrica (es. RS-232);
- definire velocità di comunicazione (baud rate);
- definire altri parametri fisici (quanti data bit, numero bit di STOP, parità);
- definire regole per i pacchetti e codici controllo;
- definire protocollo;
- definire significato dei dati;
- ecc.

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	33/48

Si può quindi affermare sinteticamente che **“l’interoperabilità non è mai per caso”**.

6.8 Kit di sviluppo

In considerazione delle suddette difficoltà, è auspicabile che tutti gli apparati destinati ad essere integrati con altri dispongano del cosiddetto “Interface kit”, un corredo di documentazione, parti ed accessori destinato a rendere quanto più facile il compito dei tecnici preposti alla integrazione.

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	34/48

7. Il CAN bus

7.1 Generalità

Il Controller Area Network, noto anche come CAN-bus, è uno standard seriale per bus di campo (principalmente in ambiente automotive) introdotto negli anni ottanta dalla Robert Bosch GmbH, per collegare diverse unità di controllo elettronico (ECU). Il CAN è stato espressamente progettato per funzionare senza problemi anche in ambienti fortemente disturbati dalla presenza di onde elettromagnetiche e può utilizzare come mezzo trasmissivo una linea a differenza di potenziale bilanciata come la RS-485. L'immunità ai disturbi EMC può essere ulteriormente aumentata utilizzando cavi di tipo twisted pair (doppino intrecciato).

Sebbene inizialmente applicata in ambito automotive, come bus per autoveicoli, attualmente è usata in molte applicazioni industriali di tipo embedded, dove è richiesto un alto livello di immunità ai disturbi.

IL CAN può quindi costituire il bus per l'interconnessione degli apparati di bordo, anche se non è molto utilizzato in questo tipo di applicazione.

7.2 I livelli ISO-OSI

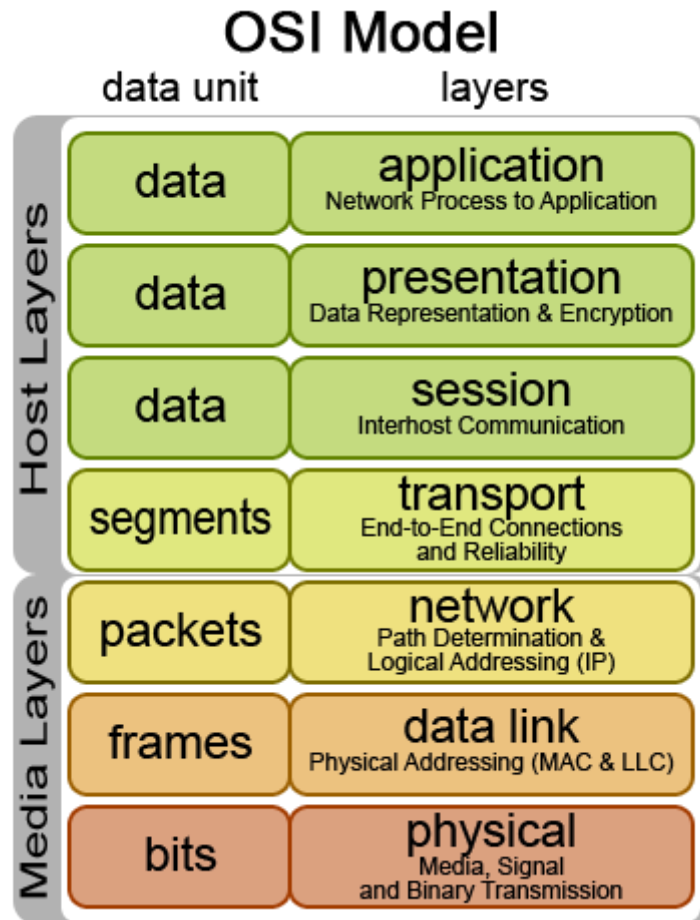
L'Open Systems Interconnection (meglio conosciuto come Modello ISO/OSI) è uno standard stabilito nel 1978 dall'International Organization for Standardization (ISO) che stabilisce una pila di protocolli in 7 livelli.

L'organizzazione sentì la necessità di produrre una serie di standard per le reti di calcolatori ed avviò il progetto OSI come modello standard di riferimento per l'interconnessione di sistemi aperti. Il documento che illustra tale attività è il Basic Reference Model di OSI, noto come standard ISO 7498.

Il modello ISO/OSI è costituito da una pila (o stack) di protocolli attraverso i quali viene ridotta la complessità implementativa di un sistema di comunicazione per il networking. In particolare ISO/OSI è costituito da strati (o livelli), i cosiddetti layer, che racchiudono uno o più aspetti fra loro correlati della comunicazione fra due nodi di una rete. I layers

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	35/48

sono in totale 7 (vedi figura) e vanno dal livello fisico (quello del mezzo fisico, ossia del cavo o delle onde radio) fino al livello delle applicazioni, attraverso cui si realizza la comunicazione di alto livello.



7.3 Standard

Il protocollo di comunicazione del CAN è standardizzato come ISO 11898-1 (2003) che definisce principalmente il Data Link Layer del modello ISO-OSI), composto dai sub layer Logical Link Control e Media Access Control. Definisce inoltre alcuni aspetti dello strato Physical Layer.

I protocolli di tutti gli altri layer sono lasciati alla libera scelta del progettista della rete. e costituiscono quindi elementi di variabilità che impediscono di fatto al CAN di essere uno standard completo, poiché ogni costruttore ha interpretato secondo il proprio criterio i layer non standardizzati.

In altre parole, il CAN definisce solo la comunicazione fisica; il protocollo, inteso come nel capitolo precedente, è ancora una volta demandato al Costruttore.

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	36/48

7.4 Caratteristiche del CAN

Una descrizione dettagliata del funzionamento del CAN bus trascende gli scopi delle presenti note, anche in considerazione del limitato uso fattone nell'ambito del Sistema di Bigliettazione Elettronica. Ci si limiterà pertanto a descriverne i principali aspetti funzionali.

Il bus non viene occupato secondo uno schema predefinito. Tutti i nodi hanno gli stessi diritti, ascoltano in "parallelo" tutti i messaggi ("multicast"), sono sempre pronti a ricevere e, quando necessario, cominciano a trasmettere se nessun altro nodo sta inviando messaggi sul bus. Si tratta quindi di una rete paritetica, in contrapposizione a quelle master/slave viste in precedenza.

Il bit rate può raggiungere 1 Mbit/s per reti lunghe meno di 40 m. Velocità inferiori consentono di raggiungere distanze maggiori (ad es. 125 kbit/s per 500 m).

7.5 Utilizzo delle linee dell'autobus

Anche nel caso di impiego del sistema CAN per l'interfacciamento degli apparati che compongono il Sistema Di Bordo, difficilmente vengono utilizzate le stesse linee elettriche installate a bordo del mezzo quando questo adotta il sistema CAN. Questo per due principali motivi:

come accennato in precedenza, i protocolli degli stati superiori ISO-OSI non sono standardizzati, e quindi ogni marca di autobus prevede protocolli propri. Non sarebbe possibile quindi adottare un unico protocollo per ogni marca/modello.

anche nel caso di superamento dei problemi tecnici, la coesistenza di apparati di terze parti sul bus CAN dell'autobus potrebbe dare luogo ad ambiguità diagnostiche in caso di anomalie, con conseguenti difficoltà di attribuire le relative responsabilità.

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	37/48

8. Comunicazione bordo/terra

8.1 Generalità

In un Sistema di Bigliettazione Elettronica, la comunicazione tra i mezzi e le infrastrutture di terra è di regola indispensabile, ad esempio per le seguenti funzioni:

- consentire il trasferimento di file e/o comandi dal deposito all'unità di bordo e viceversa;
- consentire il trasferimento di file e/o comandi dal deposito alle validatrici e viceversa.

In particolare, possono essere richiesti:

- lo scarico dei file delle transazioni prodotte dalle validatrici di bordo;
- lo scarico dei file di diagnostica delle validatrici;
- il caricamento nelle validatrici di bordo del setup, delle tabelle delle fasce tariffarie, delle linee e delle fermate, dei titoli, delle liste bianche e nere, dei parametri temporali;
- il caricamento nelle validatrici di bordo degli aggiornamenti software delle validatrici;
- il caricamento nelle validatrici di bordo degli eventuali aggiornamenti relativi alle fasce e tabelle tariffarie, al grafo della rete.

In questo capitolo saranno esaminate alcune delle possibili tecniche di comunicazione bordo/terra e viceversa.

8.2 Comunicazione a breve e lungo raggio

Per consuetudine si indica come **comunicazione a breve raggio** (SRDC, Short Range Data Communication) quella che avviene dall'autobus a terra e viceversa nell'ambito del deposito.

I sistemi di comunicazione a breve raggio si suddividono a loro volta in due sotto tipi:

- la comunicazione **a brevissima distanza**, quando il mezzo inizia il dialogo solo a pochi metri dall'antenna fissa;
- la comunicazione **in copertura globale**, quando tutto il deposito, o gran parte di esso, è coperto dal segnale utile per la comunicazione.

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	38/48

In contrapposizione, i sistemi di **comunicazione a lungo raggio** assicurano la copertura anche quando il mezzo si trova in servizio, più o meno ovunque sul territorio.

8.3 Comunicazione a breve raggio

8.3.1 Raggi infrarossi



Comunicazione ad infrarossi tra validatrice e computer palmare

Per quanto sporadicamente utilizzati anche nelle comunicazioni a brevissima distanza, con risultati incerti, essi sono invece spesso impiegati per connessioni locali tra apparati e dispositivi palmari o computer portatili, tanto che, più che di comunicazioni a brevissima distanza, si dovrebbe parlare di semplici sostituti dei cavi.

8.3.2 Comunicazioni radio a banda stretta

La comunicazione radio tradizionale è ottenuta modulando in qualche modo una portante a frequenza fissa con l'informazione che si desidera trasferire. Viene attuata con semplici apparecchi operanti di solito a 433 od 868 MHz.

Questa tecnica, alla semplicità ed al basso costo, unisce importanti svantaggi:

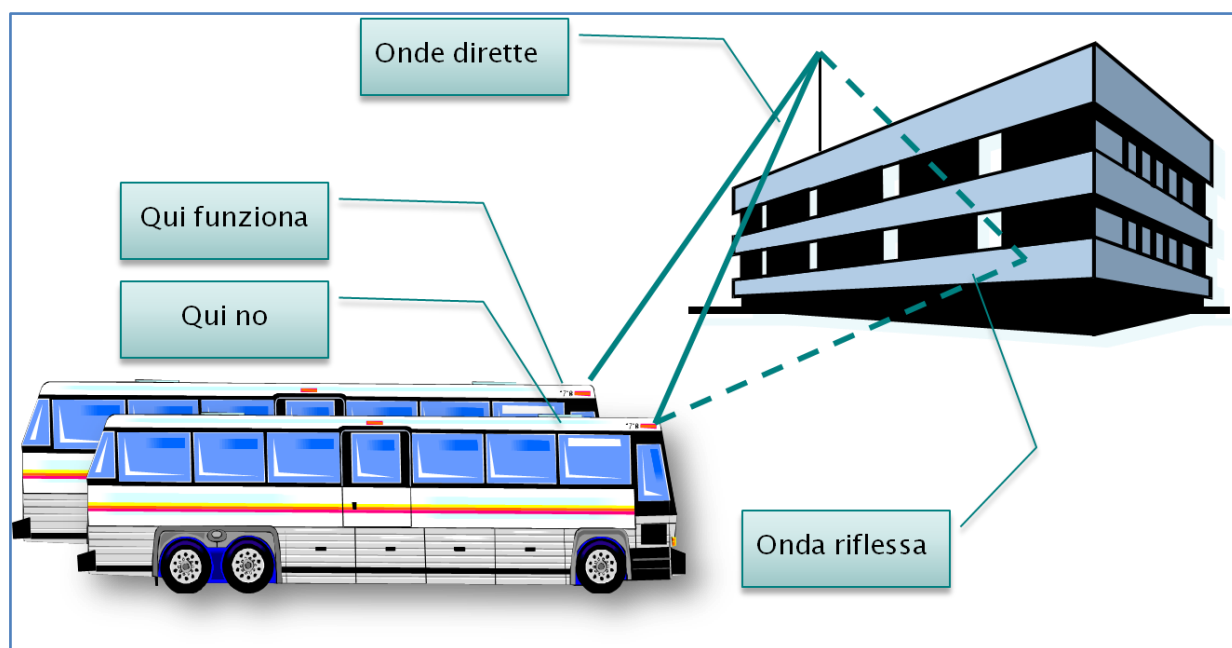
- una portante interferente, casuale o voluta, può impedire la comunicazione;
- la portante utilizzata può interferire a sua volta con altri dispositivi, come aprì cancelli e chiusure centralizzate dei veicoli (effetto "Striscia la notizia");
- le riflessioni dell'onda principale determinano effetti di instabilità e fading; le onde riflesse, infatti, giungono a destinazione con fasi di-

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	39/48

verse e si combinano con l'onda principale fino ad annullarla quando in opposizione di fase (figura sottostante).

il segnale è facilmente rilevabile da parte di terzi, cosa poco importante nell'ambito del Trasporto Pubblico Locale ma assai rilevante da un punto di vista militare.

I sistemi radio a frequenza fissa sono in graduale abbandono.



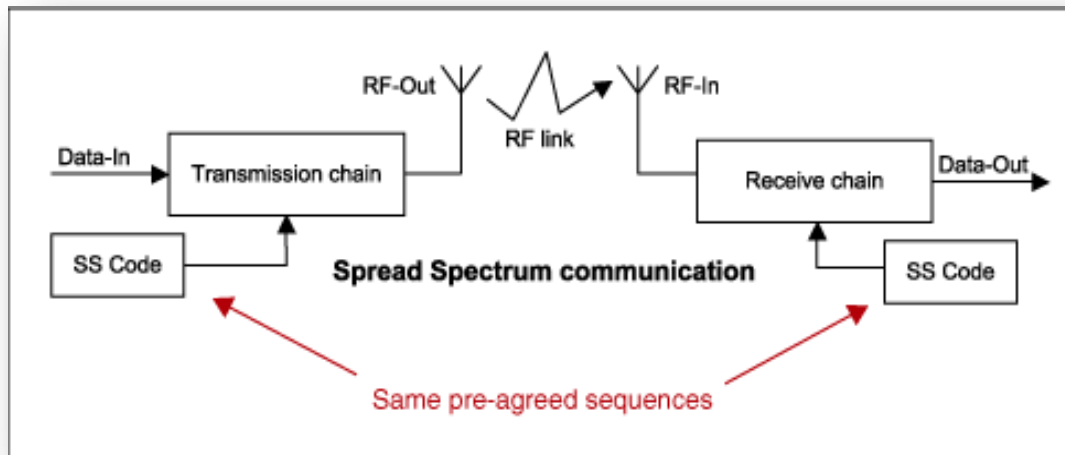
Le combinazioni delle riflessioni con l'onda principale possono arrivare ad annullare il segnale in posizioni del mezzo solo leggermente diverse

8.4 Comunicazioni radio spread spectrum (SS)

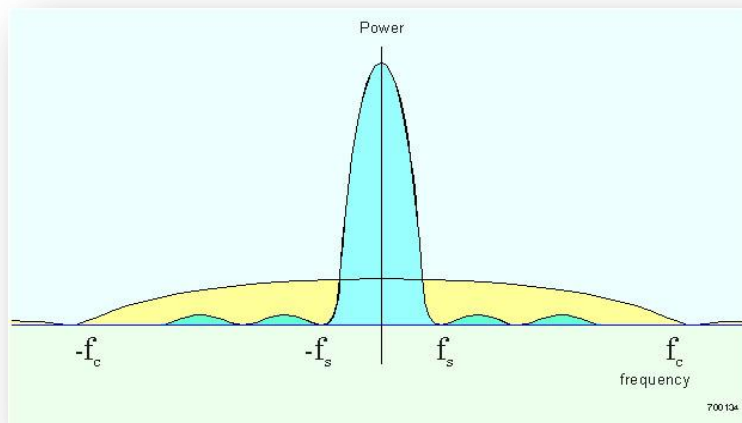
La seconda guerra mondiale aveva evidenziato l'importanza delle comunicazioni in ambito militare e l'inadeguatezza dei metodi fino ad allora utilizzati. E' quindi comprensibile come, già dal primo dopo guerra, gli sforzi di tecnici e scienziati si siano concentrati sul trovare tecniche di trasmissioni più affidabili e sicure.

Una soluzione è la comunicazione "spread spectrum", in italiano espansione di spettro. Con essa il segnale utile viene trasmesso non su una frequenza fissa ma cambiando continuamente la frequenza stessa, "spazzolando" una banda di frequenze che è considerevolmente più ampia di quella dell'informazione contenuta nel segnale.

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	40/48



Con opportune tecniche, il trasmettitore ed il ricevitore si sincronizzano e cambiano di pari passo la frequenza. Essi possono quindi continuare a parlare tra loro, eliminando il maggior numero di interferenze e consentendo l'utilizzo contemporaneo della stessa gamma di frequenze a più utenti. Il segnale radio trasmesso risulta così "mimetizzato", grazie alla inferiore potenza specifica e al fatto di essere difficilmente distinguibile dal rumore di fondo. Come conseguenza, può più facilmente sfuggire al rilevamento da parte delle stazioni di intercettazione.



Lo spettro della comunicazione spread spectrum (in giallo) contro quella tradizionale.

L'espansione di spettro mediante il salto di frequenza (Frequency Hopping) è stata inventata nel 1942 dall'attrice Hedy Lamarr (brevetto USA N. 2.292.387). Ispirandosi alle pianole meccaniche a rullo, proponeva di utilizzare un rullo di carta con cui sincronizzare i salti di frequenza del trasmettitore e del ricevitore.

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	41 / 48

Ironicamente, Mrs. Lamarr è rimasta più famosa per l'apparizione nella prima scena di nudo integrale, nel film cecoslovacco *Estasi*, e come donna gatto nel fumetto Batman.

Lo SS, variando la frequenza, varia le riflessioni e le loro combinazioni, rendendo assai più affidabile la comunicazione.

La comunicazione SS è usata, tra l'altro, dalla telefonia mobile, dal Bluetooth e dal WI-FI.



8.4.1 La Wireless LAN

E' molto nota la Wireless LAN dei PC, detta anche WI-FI, evoluzione assai più comoda della tradizionale rete Ethernet della quale sta raggiungendo le prestazioni. La WI-FI è codificata dallo standard IEEE 802.11b e, più recentemente, 802.11g. Grazie alla tecnica spread spectrum su cui si basa, essa risulta molto affidabile e prevedibile nel suo comportamento.

La WI-FI può operare in varie modalità: la più comune è quella detta "Infrastruttura" dove si usano una o più postazioni fisse, dette Access Point, direttamente collegate ad una rete Ethernet, per coprire un'area che, all'esterno, ha un raggio valutabile in circa cento metri per ogni apparecchio ben installato.

Grazie alle caratteristiche della WI-FI, è possibile assegnare ad ogni Access Point un canale diverso per rendere possibile la copertura di vaste aree.

8.4.2 La sicurezza del WI-FI

Il problema della sicurezza è molto sentito in generale per la WI-FI. Quali contromisure possono essere assunte da una compagnia che utilizza WI-FI nei propri depositi?

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	42/48

WI-FI prevedeva già fin dalla sua origine una forma di crittografia detta WEP (Wired Equivalent Privacy), che però si è rivelata piuttosto inefficace, tanto che, all'inizio del 2002 il noto istituto di ricerche Gartner affermava che "entro il 2002 almeno il 30% di tutte le imprese correranno il rischio di intrusioni per aver realizzato reti WLAN 802.11b, senza le opportune misure di sicurezza".

E' stato quindi introdotto un nuovo standard detto WPA (Wi-Fi Protected Access) che offre un livello di sicurezza nettamente superiore rispetto al WEP e certamente adeguato al tipo di impiego ipotizzato.

E' consigliabile non montare gli AP sulla rete aziendale ma di realizzare una rete separata che fa capo al concentratore di deposito che assume quindi anche la funzione di bridge tra le due reti.

8.4.3 Gli apparati di deposito

Gli Access Point utilizzati per la copertura del deposito sono talvolta del tipo normalmente reperibile nei computer shop; questi apparati non presentano tuttavia stabilità commerciale, in quanto continuamente sostituiti da nuovi modelli, ed hanno spesso anche una scarsa durata ed una limitata affidabilità.

Alcune Compagnie preferiscono invece modelli professionali (immagine a lato), assai più costosi ma più adatti al tipo di impiego.



Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	43/48



Un tipico Access Point da computer shop

8.5 Gli apparecchi di bordo

Gli apparati di bordo che utilizzano la wireless LAN WI-FI possono essere dei normali PC dotati di opportuni moduli di interfaccia o apparati appositamente progettati (figura a lato). In ogni caso essi devono essere dotati delle previste certificazioni 2004/104/CE.

La logica di gestione della comunicazione e delle sincronizzazioni dei file non è univoca e deve essere attentamente studiata per garantire una sufficiente affidabilità del sistema. Essa dipende tanto dal software dell'apparato di bordo che da quello del sistema di deposito.



8.5.1 Bluetooth

Bluetooth è una specifica industriale per reti personali senza fili (WPAN: Wireless Personal Area Network). Fornisce un metodo standard, economico e sicuro per scambiare informazioni tra dispositivi diversi attraverso una frequenza radio a corto raggio. I dispositivi per cui Bluetooth è stato progettato sono ad esempio palmari, telefoni cellulari, personal computer, portatili, stampanti, fotocamere digitali, console per videogiochi. Blueto-

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	44/48

oth cerca i dispositivi coperti dal segnale (10 metri in ambienti chiusi) e li mette in comunicazione tra di loro.

La specifica Bluetooth è stata sviluppata da Ericsson e in seguito formalizzata dalla Bluetooth Special Interest Group (SIG). SIG, la cui costituzione è stata formalmente annunciata il 20 maggio 1999, è un'associazione formata da Sony Ericsson, IBM, Intel, Toshiba, Nokia e altre società che si sono aggiunte come associate o come membri aggiunti.

Il nome è ispirato a Harald Blåtand, re Aroldo I di Danimarca, abile diplomatico, conosciuto con il soprannome di Dente blu.

Il protocollo Bluetooth lavora nelle frequenze libere di 2,45 Ghz. Per ridurre le interferenze il protocollo divide la banda in 79 canali e provvede a commutare tra i vari canali 1600 volte al secondo. La versione 1.1 e 1.2 del Bluetooth gestisce velocità di trasferimento fino a 723,1 kbit/s. La versione 2.0 gestisce una modalità ad alta velocità che consente fino a 10 Mbit/s. Questa modalità però aumenta la potenza assorbita. La nuova versione utilizza segnali più brevi e quindi riesce a dimezzare la potenza richiesta rispetto al Bluetooth 1.2 (a parità di traffico inviato).

Bluetooth opera in modalità master/slave con un massimo di 7 dispositivi. Sono previste tre classi di funzionamento, con diverse potenze e diverse portate:

Classe	Potenza (mW)	Potenza (dBm)	Distanza (Approssimativa)
Classe 1	100 mW	20 dBm	~ 100 metri
Classe 2	2,5 mW	4 dBm	~ 10 metri
Classe 3	1 mW	0 dBm	~ 1 metro

Bluetooth non è uno standard comparabile con il WI-FI dato che questo è un protocollo nato per fornire elevate velocità di trasmissione con un raggio maggiore, a costo di una maggior potenza dissipata e di un hardware molto più costoso. Il Bluetooth può essere paragonato al bus USB e può costituire una valida alternativa alla già citata interfaccia ad infrarossi, mentre il WI-FI può essere paragonato allo standard Ethernet.

Applicazioni con BT a bordo dei mezzi per la comunicazione terra/bordo sono rare ed ormai quasi ovunque soppiantate dal WI-FI.

Nella figura a lato, un modulo integrato Bluetooth in classe 2 che contiene sia il trasmettitore, che il ricevitore che l'antenna.



8.6 Comunicazione a lungo raggio

Per la comunicazione a lungo raggio sono stati storicamente utilizzati i seguenti principali mezzi:

- uso di modem analogico su frequenza radio a banda stretta in concessione; si tratta di un metodo superato, ormai quasi ovunque in disuso;
- uso di modem analogico su canale telefonico GSM. Offre prestazioni limitate (circa 9.600 baud) ed ha un costo legato al tempo di trasmissione; anche questo è in abbandono;
- uso di messaggi SMS. Metodo inaffidabile e costoso; le compagnie telefoniche non garantiscono un tempo sicuro per l'inoltro del messaggio. Pressoché inutilizzabile per le applicazioni tipiche dei Sistemi di Bigliettazione Elettronica.
- uso di modem digitale GPRS, UMTS (o altra emergente tecnologia).

Di quelle sopra elencate, solo l'ultima trova ampia e frequente applicazione. Questa tecnica presenta infatti i seguenti vantaggi:

- costo proporzionato al numero dei dati effettivamente trasferiti;
- possibilità di stipulare contratti "flat" a tariffa fissa;
- costante evoluzione tecnologica degli apparati e delle infrastrutture che garantisce ampiezze di banda sempre più ampie.

8.7 Caratteristiche della comunicazione GPRS

La connessione GPRS, e con essa quella delle tecnologie più evolute, non si comporta come la classica connessione modem "da punto a punto". Essa è invece un connessione da un apparato remoto ad una rete, tipicamente ad Internet o ad un punto di ingresso di una rete privata.

Questa organizzazione ha importanti implicazioni:

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	46/48

il sistema centrale non può chiamare i mezzi; devono essere questi che si collegano al provider, ricevendo dal medesimo un indirizzo IP. Sarà il mezzo che, una volta in rete, provvederà a comunicare alla propria centrale il proprio identificativo sociale e l'indirizzo IP ricevuto.

in un sistema GPRS non vi è un limite al numero dei mezzi che possono mantenere una connessione attiva con il sistema centrale.

8.8 Il concentratore

Il concentratore di deposito è l'apparato che, in deposito o nella centrale operativa, assolve alla funzione di gestione della comunicazione con i mezzi.

Esso si trova in ogni deposito nel caso della comunicazione a breve raggio, mentre può essere centralizzato nella centrale operativa nel caso della comunicazione a lungo raggio.

E' costituito di regola da un PC di buona qualità, dovendo stare acceso molte ore al giorno o addirittura H24, munito di un opportuno applicativo software che ne definisce comportamento e caratteristiche.

Nel caso più comune della rete WI-FI, è prevista, di solito, una doppia scheda di rete, come accennato. La prima è impiegata per il collegamento Ethernet agli Access Point e di conseguenza per il dialogo con i mezzi, mentre la seconda lo collega alla rete aziendale.

Nel caso GPRS, invece, è indispensabile una connessione ad Internet o alla rete privata di comunicazione, ove prevista.

Un applicativo di concentratore può raggiungere anche elevati livelli di sofisticazione e deve poter operare in modalità "unattended" ossia senza operatore. Deve prevedere tutte o parti delle seguenti funzioni:

gestione della comunicazione in sicurezza;

caricamento verso l'autobus dei file contenenti i parametri, le tabelle di configurazione e quanto altro necessario alla corretta operatività degli apparati.

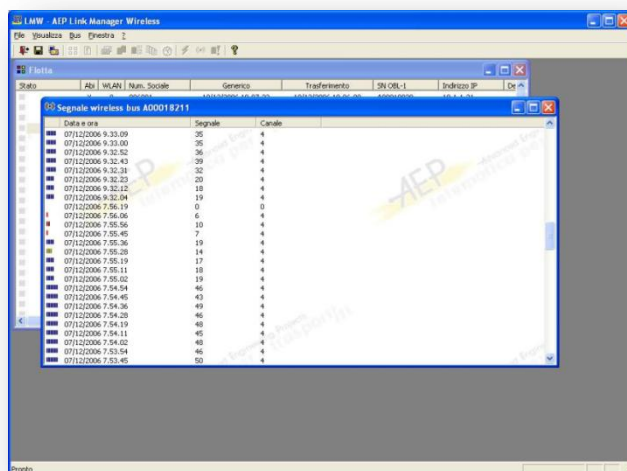
scarico dall'autobus dei file di attività e delle transazioni prodotte dal sistema di bordo;

gestione delle sincronizzazioni;

aggiornamento del software dei dispositivi di bordo;

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	47/48

gestione dei depositi, dei gruppi e dei sottogruppi di autobus;
gestione dei mezzi assenti per manutenzione;
gestione dei canali WI-FI multipli;
gestione del roaming (passaggio da un Access Point ad un altro quando il mezzo si muove in deposito);
gestione degli automatismi (es. chiusura turno);
fornitura delle indicazioni diagnostiche;
registrazione di tutte le operazioni effettuate nell'apposito database delle attività;
segnalazione autobus "smarriti" o in ritardo con il trasferimento dei dati;
gestione dei numeri sociali dei bus;
gestione dei numeri di serie degli apparati e delle loro sostituzioni;
diagnostica e test.



Una finestra di un applicativo per concentratore

Titolo documento	File	Pagina/di
Sistemi Di Comunicazione	701288.E00.IT DISPENSA SDC.DOCX	48/48