



Questo articolo è stato pubblicato su....





# LETTORE DI SCHEDE GSM



Daniele Cappa

Si collega alla porta seriale del PC, legge e scrive le Sim Card dei telefoni cellulari GSM, consentendone la gestione e il backup

Si tratta di una interfaccia seriale in grado di far dialogare il PC, fornito di opportuno software, con la Sim Card del telefono GSM. Lo scopo principale è di evitare la perdita dei dati contenuti nella rubrica, sia a scopo di backup sia per ricopiarli su una nuova Sim senza perdere un pomeriggio a pestar tasti sul telefonino.

L'interfaccia è alimentata esternamente con i soliti 12V stabilizzati, richiede pochissima corrente, il prototipo assorbe meno di 40 mA con i componenti utilizzati; ho effettuato prove utilizzando una pila a 9V non alcalina e anche così tutto funziona a dovere, si iniziano ad avere problemi alimentandola intorno agli 8 V.

## Schema elettrico

Ho voluto mantenere la compatibilità completa con lo standard RS232, evitando eventuali problemi per l'uso su PC portatili (foto 1) il cui seriale è spesso un pochino più "debole" rispetto a quella dei fratelli da tavolo.

Il classico MAX232 assolve benissimo la sua funzione di driver seriale, i quattro condensatori elettrolitici esterni, il cui valore è decisamente poco critico, sono gli unici componenti esterni richiesti da questo chip.

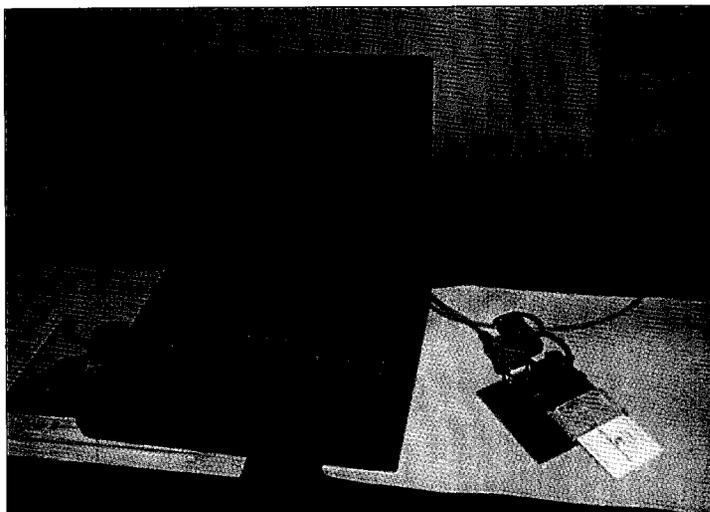


Foto 1

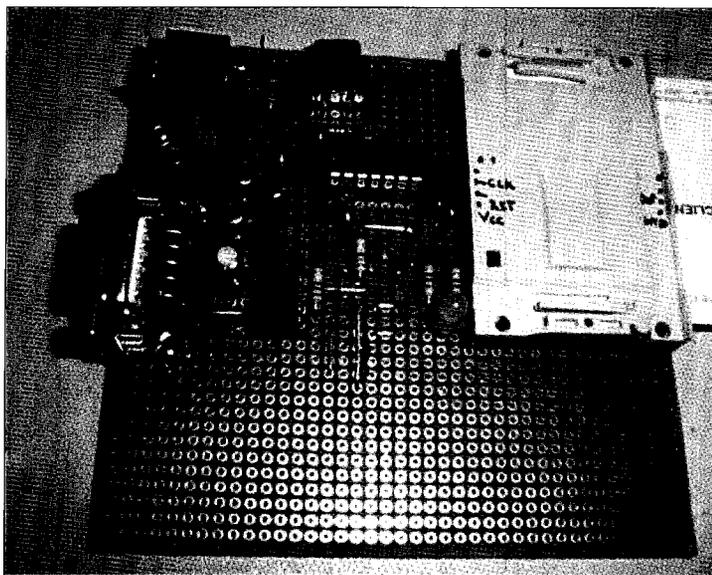


Foto 2

I chip e la carta funzionano a 5 V ottenuti con l'aiuto di un 7805 che nel prototipo ho inutilmente montato su un piccolo dissipatore! (foto 2) Un piccolo 78L05 può tranquillamente fornire la corrente necessaria. Il diodo D1 evita danni da inversioni di polarità mentre il LED D2 funziona da spia di accensione.

Un CD4069 svolge in sostanza tutte le funzioni richieste: oscillatore e il suo buffer, pilota i due LED utili a monitorare il buon funzionamento, capovolge il segnale di reset proveniente dal MAX232. Avanza un inverter utile per future espansioni, magari un oscillatore su un'altra frequenza.

L'oscillatore utilizza un quarzo da 3.579 MHz e fornisce il segnale di clock alla Sim tramite un inverter che funziona da buffer; con questo quarzo la comunicazione PC - SIM avviene a 9600 baud.

Altri due inverter pilotano due LED posti rispettivamente sul pin di reset e sul pin DATA (I della Sim Card). Il Cmos è in verità poco adatto a pilotare LED, ma la disponibilità di porte e la pigrizia di aggiungere un altro chip solo per questo scopo ha fatto sì che mi accontentassi della poca luce prodotta. Del resto basta sostituire pin-to-pin il 4069 con un 74LS04 per guadagnare in luminosità e in

consumo. Se si prevede l'uso alimentandola con una pila è bene non montare nessuno dei tre LED.

I due LED rendono visibile in funzionamento della scheda, quello verde che fa capo al reset si accende nel momento del primo accesso da parte del software del PC verso la scheda, mentre quello rosso lampeggia durante il passaggio dei dati da e verso la scheda GSM.

La Sim dialoga con l'esterno su un solo pin, il diodo D5 si incarica di smistare i segnali in un senso o nell'altro facendo arrivare il Tx sul pin 11 e prelevando l'Rx sul pin 12 del max232. È importante che questo diodo sia di tipo skotty, la

caduta di tensione su un normale diodo al silicio potrebbe pregiudicarne il funzionamento. Sul prototipo è stato usato un BAT42 fornito dal solito cassetto; in alternativa si potrebbe utilizzare un vecchio diodo al germanio, avendo cura di recuperarne uno integro!

Il connettore ISO che ospiterà la Sim sarà adatto alla carta intera, sono reperibili anche connettori per formato francobollo, ma al momento mi sono accontentato di usare un riduttore proveniente da una ex\_sim. Nelle solite fiere del settore sono reperibili slot iso a poco più di due euro, ma aspettatevi prezzi anche pari al doppio nel negozietto sotto casa.

### Montaggio e costi

Come si vede dalle foto (foto 3) il prototipo è stato montato sulla solita millefori, con spazi piuttosto generosi prevedendo future espansioni. I due LED posti sul reset e sul pin data sono stati sostituiti con un LED bicolore a catodo comune, è quello appena dietro il connettore ISO.

I due jumper presenti accanto al CD4069 derivano dalle prove effettuate prima di trovare la giusta polarità del reset e prevedendo un secondo oscillatore a 8.568 MHz (foto 4),

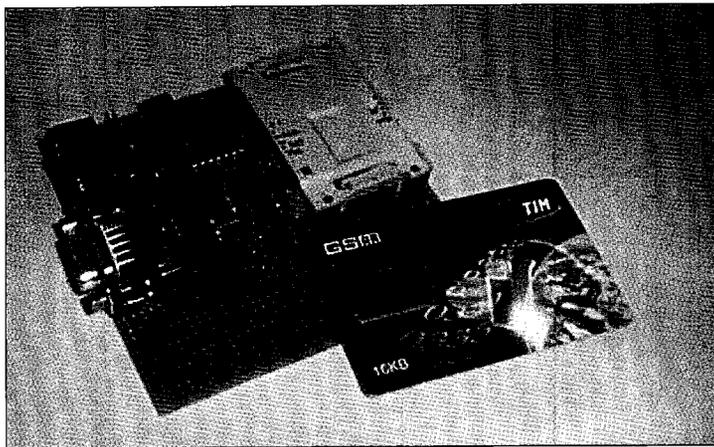


Foto 3

sullo schema definitivo sono stati eliminati perché la maggiore velocità non è, per questi scopi, di alcuna utilità, anzi limita l'uso alle Sim che riescono a "tenere" tale frequenza di clock.

Sul montaggio non c'è molto da dire, attenzione alla polarità dei quattro elettrolitici del MAX232, uno ha il reoforo del negativo collegato al positivo di alimentazione mentre il suo compagno ha il positivo a massa. Questa strana configurazione si chiarisce se misuriamo la tensione presente sui due pin collegati ai condensatori, sono infatti le uscite delle due pompe che generano le tensioni

negative e positive necessarie al funzionamento della RS232 standard. Per confondere meglio le idee occhio al Max che ha i pin di alimentazione disposti in modo non usuale.

Il connettore ISO è reperibile in due modelli differenziati dall'interruttore che si aziona introducendo la carta, il modello che serve a noi è normalmente chiuso, in altre parole si apre quando la carta è inserita. Se il nostro connettore è dotato di interruttore del tipo normalmente aperto possiamo semplicemente scollegarlo da massa simulando così la carta sempre inserita.

Esistono interfacce commerciali con caratteristiche simili a questa il cui costo oscilla intorno a 40 euro, per questa interfaccia siamo sotto i 10 euro, salvo aiuti dal solito cassetto!

## Il software

Prima di iniziare a illustrare cosa deve fare il software una avvertenza importante, questa interfaccia è in grado di leggere e scrivere su una Sim card, spesso il soft permette l'accesso a zone della carta che sono inaccessibili dal telefono o che sono situate nei menù di sicurezza. ATTENZIONE dunque a non intervenire su numeretti di cui non conosciamo il significato. Prima di intervenire sulla carta assicuriamoci di avere disponibili i numeri PIN e PUK, in modo da poter rimediare a eventuali modifiche non volute.

Ho trovato più programmi adatti al nostro uso, alcuni liberi o in versione ridotta, alcuni sono prodotti commerciali per il cui uso è necessario far riferimento al produttore.

Graficamente molto bello è PhoneFile dell'inglese Pipistrel, in versione light e pro, reperibile presso [www.pipistrel.com/phone-](http://www.pipistrel.com/phone-)

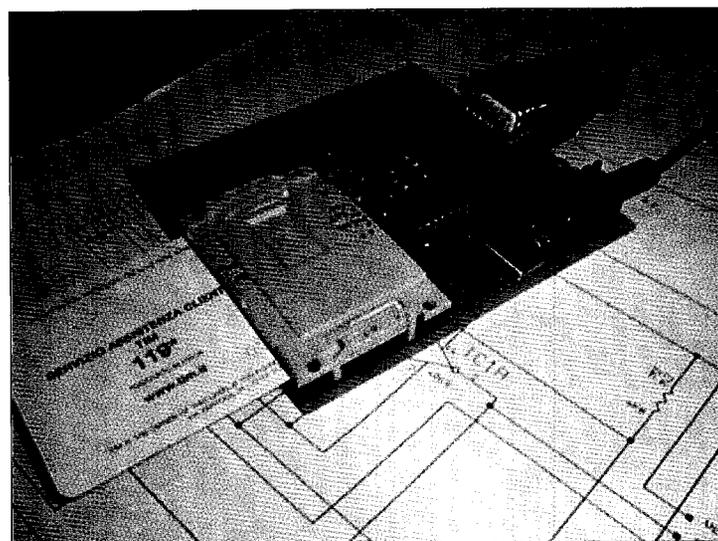
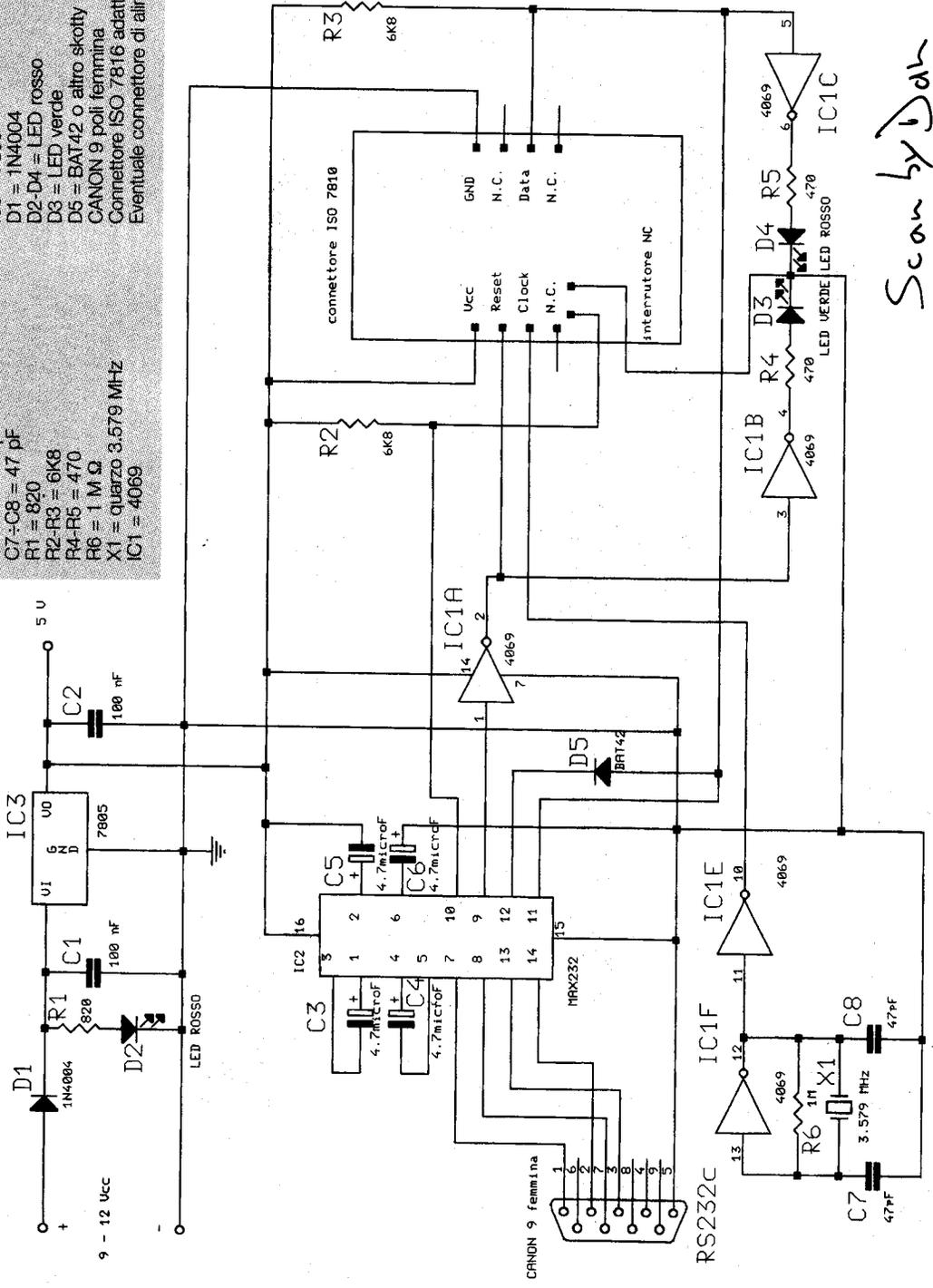


Foto 3



C1- C2 = 100 nF  
 C3- C6 = 4.7 µF 16V elet  
 C7- C8 = 47 pF  
 R1 = 820  
 R2- R3 = 6K8  
 R4- R6 = 470  
 R6 = 1 M Ω  
 X1 = quarzo 3.579 MHz  
 IC1 = 4069  
 IC2 = MAX232  
 IC3 = 7805  
 D1 = 1N4004  
 D2- D4 = LED rosso  
 D3 = LED verde  
 D5 = BAT42 o altro skotky  
 CANON 9 poli femmina  
 Connettore ISO 7816  
 Eventuale connettore di alimentazione



Scan by Doh

Schema elettrico del lettore.



file. La gestione della rubrica consente l'editing diretto della rubrica, il suo salvataggio su disco sia come file proprio sia come file stampabile.

I file da importare possono essere definiti nella forma potendo inserire separatori diversi tra i campi (TAB, virgole, spazi o apici), questa possibilità è di aiuto per poter importare file provenienti da altri programmi.

La gestione dei numeri pin si estende alla riattivazione della scheda tramite codice PUK; è possibile leggere, modificare, stampare e salvare gli SMS presenti sulla Sim.

Di piccole dimensioni, anche questo di provenienza inglese, limitato alla sola rubrica è Phoneman che, dopo avere letto la Sim permette solo di editarla e ricaricarla nuovamente sulla Sim senza nessuna possibilità di backup sul disco... sebbene sia possibile in backup su una vecchia Sim! Nonostante le indubbe limitazioni è un programma molto veloce, intuitivo da usare che assolve pienamente i suoi compiti.

La versione libera di Cardinal nella versione 6.8 gestisce molto bene la rubrica di cui permette sia l'edit diretto sia il backup su disco come file.TXT, fornisce info circa la Sim in uso, ha un'ottima gestione del PIN1 e PIN2, è possibile controllare e cambiare la lingua, non sono disponibili sul programma free la gestione degli SMS e del broadcast. Con questo soft è possibile far danni anche irreversibili alla Sim, dunque prestate molta attenzione a quel che fate. Anche la versione libera permette di importare file di testo nella rubrica con questa sintassi:

**NOME (tab) TELEFONO (invio)**

Il nome e il numero di telefono vanno separati da una tabulazione e al termine ci deve essere un ritorno carrello, senza nessuno spazio. Qualsiasi altra sintassi è rifiutata spesso senza nessun messaggio di errore.

Il setting di questo programma permette di variare la velocità di comunicazione con la SIM dai 9600 baud standard fino a 23040 baud, che si ottengono sostituendo il quarzo con uno da 8.568 MHz. In queste condizioni

una SIM Wind si comporta benissimo e funziona perfettamente, mentre una 16K Tim si rifiuta di funzionare.

Analogamente è possibile diminuire il baud rate, sempre sostituendo il quarzo, avendo cura di scegliere tra le velocità a cui è possibile settare questo software; il limite inferiore è fissato a 5485 baud ottenuti con un quarzo da 2.04 MHz.

È sottinteso che tutti i software citati sono in grado di funzionare esclusivamente sotto Win9x e seguenti.

Ho effettuato prove con Sim di tutti i quattro gestori di telefonia mobile italiani, con memoria da 8, 16 e 32K, tutte le schede si sono comportate benissimo, le uniche differenze sono i numeri in rubrica che gestisce la singola Sim, attenzione a non caricare la rubrica di una schedina da 32K in una vecchia 8K. Assicuratevi anche che la rubrica del vostro telefono sia registrata su memoria Sim, non su memoria telefono!

Come abbiamo visto la gestione della rubrica può avvenire in più modi: il programma legge la rubrica presente sulla Sim, permette l'editing delle voci e il file è salvabile su disco in un formato che fa riferimento al programma stesso. Alcuni soft permettono di esportare il file in formati standard, solitamente in ascii o in excell.

Il file potrà ora essere trattato secondo necessità, per eventualmente importarlo anche con un altro software che potrà riversarlo nuovamente sulla Sim originale come su un'altra.

Le altre opzioni sono un gadget in più, anche il semplice Phoneman assolve benissimo lo scopo che mi ero prefissato.

Non dimentichiamoci che con questa interfaccia possiamo solo interagire con la Sim, non con il telefono cellulare come era stato fatto a suo tempo con i telefoni Nokia della serie 51xx e 61xx e il programma Logomanager. Questo sistema ci impedisce ad esempio di inviare SMS dalla tastiera del PC, oppure gestire anche la rubrica conservata nella memoria del telefono, cosa che era possibile con il cavetto Nokia.

*Davide*