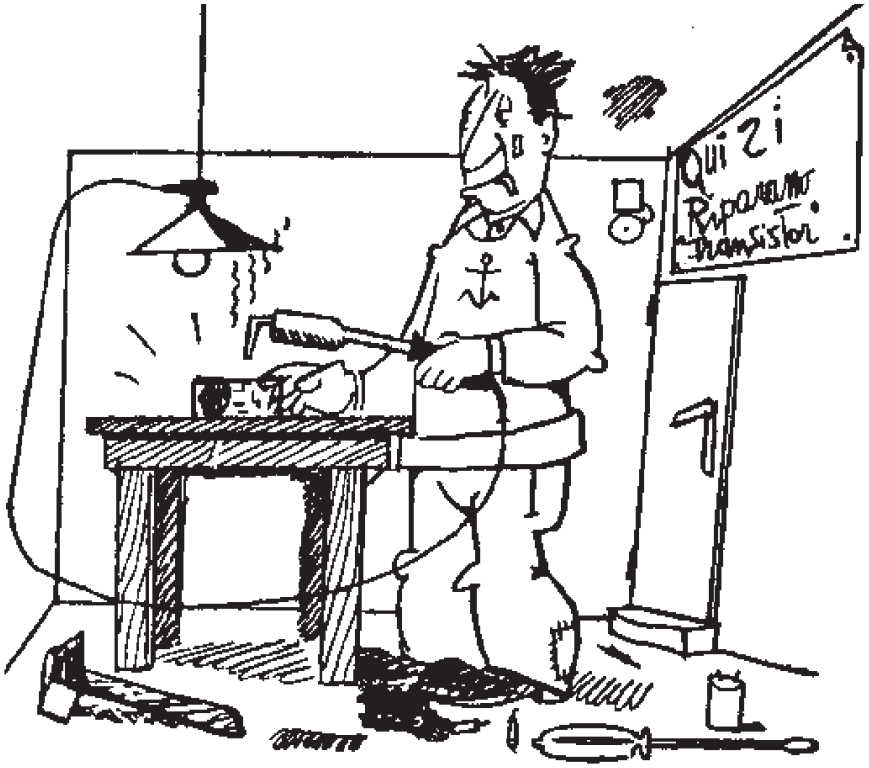


Questo articolo è stato pubblicato su....

ELETTRONICA FLASH

Un antifurto da cellulare

Daniele Cappa, IW1AXR

Recuperare un vecchio cellulare e trasformarlo in un teleavviso da abbinare o sostituire alla sirena di un antifurto di qualsiasi tipo

Tutto è iniziato con l'antifurto elettrico pubblicato su EF Marzo 2003, l'impianto così com'è stato presentato funziona perfettamente, pur con i suoi limiti di progetto.
Il passo successivo è la necessità di essere avvisato, da remoto, se qualcosa ha fatto intervenire l'impianto. Il tutto deve ovviamente rispettare la condizione esposta a suo tempo nell'articolo originale: non deve esserci consumo di energia quando l'impianto è inserito, ma a riposo.
Inizialmente ho pensato di utilizzare un vecchio RTX VHF, poi sono passato a considerare l'uso di un vecchio cellulare, più reperibile, versatile e sicuro.
L'interfaccia proposta è collegata all'impianto con tre fili: massa, positivo permanente e positivo di allarme. Su quest'ultimo basta un impulso positivo di una frazione di secondo per far partire l'intero ciclo di chiamata che si conclude indipendentemente dalla durata del periodo di allarme dell'antifurto.
Per risolvere il problema ho giustiziato alcuni vecchi cellulari buttati via dai proprietari, a questi è stata aggiunta una interfaccia che entra in funzione all'attivazione della sirena tradizionale e compie un ciclo di operazioni finalizzate a far fare le operazioni richieste al cellulare per chiamare un numero memorizzato come ultima chiamata o come "numero breve". Accedere quindi a quelle zone della memoria del telefono che sono richiamabili con poche pressioni di pochi tasti.
Le operazioni necessarie sono comprese in un ciclo che dura alcuni minuti così suddivisi:

- fase di accensione del telefono, tipicamente la pressione di un tasto per 2 o 3 secondi (questo sistema è valido per praticamente tutti i cellulari).
- attesa di un tempo ragionevole per permettere al telefono di cercare e registrarsi sulla propria rete, potrebbe essere rimasto spento anche per alcuni mesi.

La pressione di alcuni tasti in sequenza intervallati da pause, secondo la necessità del cellulare usato, in modo da effettuare una chiamata, o meglio ripetere l'ultima chiamata effettuata.
Pausa di alcune decine di secondi

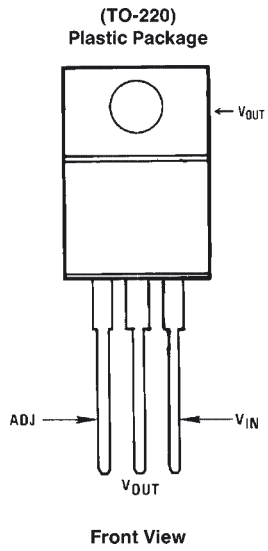
LISTA COMPONENTI

R1 = 10 kΩ
R2 = 22 kΩ
R3 = 150 kΩ
R4 = 1 MΩ
R5 = 10 kΩ
R6 = 1 MΩ
R7 = 270 Ω
R8 = 150 kΩ
R9 = 1 MΩ
R10 = 10 kΩ
R11 = 10 kΩ
R12 = 22 kΩ
R13 = 10 kΩ
R14 = 10 kΩ
P1 = 100 kΩ trimmer mult. vert.
P2 = 1 kΩ trimmer mult. vert.
C1 = 100 nF
C2 = 100 nF
C3 = 220 µF 16V
C4 = 1 µF multistrato
C5 = 22 µF 16V
C6 = 100 nF
D1 = D2 = 1N4004
D3 ÷ D10 = 1N4148
D11 = 1N4148 diodi dei relè
IC1 = CD4040, o 74HC4040
IC2 = CD4017, o 74HC4017
IC3 = CD4069, o 74HC04
IC4 = LM7805 o equivalente stabilizzatore a 5 V
IC5 = LM317
TR1 ÷ TR4 = BC547
RL1 = relè reed per accensione interfaccia
RL2 = relè reed per accensione telefono
Altri relè = secondo il modello del telefono

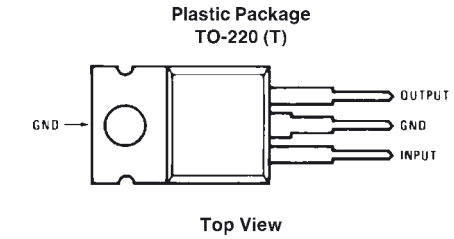
per permettere alla chiamata di avere successo.
Ripetizione di questi ultimi due punti per 3 o 7 volte secondo la presenza o meno il diodo D7.
Fine del ciclo, l'interfaccia si spegne autoscollegandosi dalla fonte di alimentazione, per rispettare la necessità di non avere consumo di corrente in condizioni di non allarme.
L'interfaccia ha la possibilità di simulare la pressione di tre tasti intervallati da altrettante pause. Sullo stampato sono stati previsti due soli tasti più la pressione del tasto di accensione. Di solito la pressione di un solo tasto ripetuta due volte è sufficiente a inoltrare una chiamata.
Il sistema si presta ad essere utilizzato con moltissimi cellulari, sicuramente non su tutti, ETACS o GSM attivi. È importante che la vittima sia in grado di funzionare in modo corretto, non abbia problemi di ricezione o quanto altro pregiudichi il funzionamento intrinseco dell'apparecchio, al contrario tastiera, batteria, carica batteria e antenna rotta non rappresentano un problema.
Come abbiamo visto batteria e carica batteria sono da buttare, l'eventuale antenna rotta è sostituibile da uno stilo di ottone o rame lungo da 76 a 78 mm saldato direttamente al posto della vecchia antenna.
Il telefono deve avere il porta SIM intero con al suo interno una SIM attiva e funzionante di un gestore che offra una buona copertura nella zona interessata.
Al momento dell'allarme avremo una chiamata da parte del numero legato alla SIM impiegata e che avremo memorizzato sul cellulare personale con un nome tipo "antifurto" oppure "garage", magari abbinandola a un tono di suoneria diverso. Se rifiutiamo la chiamata l'interfaccia ci richiamerà fino allo scadere dei tentativi previsti, ma non avremo nessun consumo sul credito della SIM. È necessario prestare attenzione alla data di scadenza e al credito residuo della scheda, che va comunque ricaricata entro i limiti previsti dal gestore.

Lo schema elettrico

Il primo progetto prevedeva l'uso di una eprom, avrebbe permesso l'utilizzo di più tasti, con la possibilità di effettuare ripetizioni e comporre più di un numero, ma la semplicità del progetto, la realizzazione e la modifica veloce del cellulare era essenziale e questa prima soluzione è stata abbandonata.
L'impulso di allarme alimenta l'interfaccia e il telefono, immediatamente scatta il relè reed a 12 Volt che fornisce l'alimentazione prelevandola da un positivo permanente. L'impulso di allarme può cessare in qualsiasi momento, non è più possibile interrompere il ciclo di chiamate se non scollegando l'alimentazione principale. Durante tutto questo tempo il cellulare è alimentato da un LM317 in grado di fornire una tensione che può variare (in sede di taratura agendo su P2) da 1.2 a 6.5 Volt permettendo l'alimentazione di un gran numero di modelli; l'interfaccia è alimentata dai 5 Volt forniti dal solito stabilizzatore positivo 7805.
Il pacco batteria del telefono andrà rimosso, la corrente al cellulare è ora fornita dall'esterno per mezzo di due fili saldati al posto della vecchia pila.
All'accensione iniziano il conteggio due timer basati su una porta Cmos del CD4069 e una rete RC (C5 con R8 e C3 con R3), uno dura pochi secondi e provoca l'accensione del cellulare, l'altro dura 30 secondi circa e mantiene alto il pin di reset del CD4040 che inizierà a funzionare solo dopo che il timer avrà esaurito il suo compito portando a livello 0 il pin 11 del CD4040, questo è il tempo che permette al cellula-



piedinatura LM317



piedinatura LM7805

re di cercare e registrarsi sulla propria rete. I due tempi sono modificabili variando il valore di C5 e di C3.
Il cuore del sistema è un CD4040, contatore binario a 12 bit, il generatore di clock è formato da due porte del CD4069 su una rete RC (P1 in serie a R5 con C4). L'uscita Q2 (o Q1 se vogliamo un ciclo più lungo) del CD4040 fornisce il clock a un contatore decimale (CD4017), dalle cui uscite vengono prelevati i segnali e le "pause" per comandare la tastiera del vecchio cellulare.
Il Pin di reset del CD4017 è controllato da alcuni bit del CD4040 che ne bloccano il funzionamento se non durante sette periodi, oppure tre se decidiamo di avere pause più lunghe, della durata di 7 impulsi di clock, distribuiti durante il tempo totale. Lo spegnimento dell'interfaccia coincide quando l'ultimo bit (Q12) del CD4040 passa a livello logico 1, questo avviene dopo alcuni minuti dall'impulso di avvio.
I comandi verso il cellulare sono realizzati con transistor NPN, in ragione di uno o due per tasto interessato, secondo il modello di cellulare, oppure da relè reed.

L'interfaccia verso il cellulare

Inizialmente dobbiamo controllare che il telefono sia in grado di effettuare una chiamata con pochissime pressioni di pochi tasti, di solito si tratta di premere due volte il tasto OK, oppure un tasto cursore e OK, un numero e OK…
Possiamo anche eseguire una pressione prolungata su un solo tasto collegando due diodi su due uscite consecutive del CD4017 facenti capo ad un solo transistor.
Il telefono va smontato per eseguire l'analisi del sistema di comando della tastiera.
Si presume che questa sia del tipo riga-colonna e che la pressione di ogni tasto colleghi tra loro i terminali di una riga con quelli di una

colonna, rendendo così decodificabile qual è il tasto premuto. Purtroppo non sempre è così, oppure determinare quali siano le righe e quali le colonne non è così immediato. Su un Motorola M3288 ogni tasto riporta tre contatti, uno di massa e due non collegati tra loro. Quando premiamo il tasto mettiamo a massa i due contatti e il telefono esegue quanto richiesto dalla pressione di quel tasto. Altri modelli hanno due soli contatti, con massa in comune oppure no. Le prove possono essere effettuate con il telefono privo della tastiera e alimentato, con un piccolo cacciavite ponticelliamo le piste che compongono le piazzole della tastiera per stabilire tra che punti avviene il contatto utile.

Su un Ericsson GH688, un altro Ericsson A1018s e un vecchio Nokia 21xx visibili nella foto i tasti sono organizzati in righe e colonne, hanno due soli contatti per tasto, ma sono isolati da massa, il problema non è stato neppure analizzato, due micro relè risolvono il problema. Questi telefoni sono adatti a questo tipo di modifica perché la sopportano senza rimuovere la tastiera che continua a funzionare, con l'eccezione dei tasti su cui sono state effettuate le saldature. I 4 fili sono stati fatti uscire nella fessura lasciata libera dal connettore del vivavoce-caricabatterie che è stato rimosso, oppure direttamente dal foro del tasto (brutto, ma veloce). Potrebbe essere una buona idea eliminare i collegamenti originali del connettore del vivavoce e sfruttarne i contatti rimasti liberi per portare all'esterno del telefono i collegamenti dei tasti, l'alimentazione può essere fornita dal guscio di una ex_batteria svuotata.

Se il comando avviene portando a massa uno o due contatti dei tasti la nostra interfaccia utilizzerà uno o due transistor NPN per ogni tasto interessato, se abbiamo dubbi sul livello dei segnali possiamo ricorrere ai soliti microrelè che si incaricheranno di chiudere i contatti necessari.

Sui modelli utilizzati viene premuto per due volte il tasto OK, o il tasto con la cornetta verde.

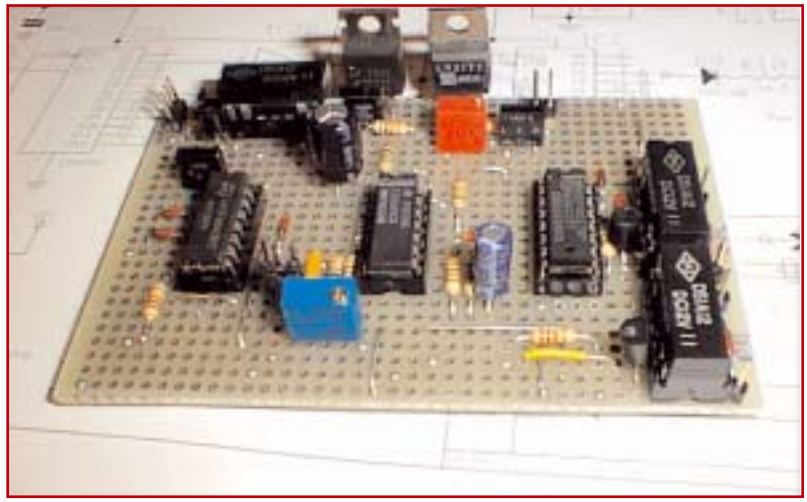
Come già detto il comando dei tasti avviene tramite un contatore decimale, pilotato dagli impulsi di clock provenienti dal pin 7 del CD4040 e regolabili agendo su P1 da 80 a 800 mSec circa, corrispondenti a 20 – 200 mSec misurati su TP1. I pin del CD4017 passano da livello logico 0 a livello logico 1 quando sono trascorsi i corrispondenti impulsi di clock e restano a questo livello per un periodo pari a un impulso di clock: il pin 2 (Q1 del 4017) sarà attivo dopo il primo impulso, il pin 4 (Q2 del 4017) dopo il secondo…. Fino a Q7 che si attiva allo scadere del settimo periodo, l'ultimo prima del reset fornito dai diodi collegati ai bit del CD4040. Attenzione a Q0 il cui livello è sempre alto quando il contatore è in fase di reset ed è attiva l'uscita corrispondente al numero decimale 0. Q1 ha spesso un comportamento anomalo, almeno nel primo ciclo di conteggio, non ho cercato le ragioni di questo strano comportamento, basta utilizzare Q2, Q4 e Q6 come comando per i tasti, Q3, Q5 e Q7 non andranno collegati a nulla e costituiscono le pause tra l'azionamento consecutivo di due tasti.

Il collegamento dei bit di uscita del CD4017 ai diodi collegati alle basi dei transistor sono variabili da un modello all'altro, pertanto sullo stampato saranno necessari alcuni ponticelli di filo per realizzare la combinazione di tasti e la sequenza necessaria al cellulare impiegato.

Nella tabella 1 vediamo i tempi misurati con un periodimetro collegato a TP1, regolabili con il trimmer P1, quello collegato ai pin 2 e 3 del CD4069.

Se viene montato D7 si raddoppia il periodo di ripetizione del ciclo a scapito del numero di tentativi che vengono ridotti da 7 a 3. Personalmente ho preferito un numero maggiore di tentativi più rapidi che mettono al riparo da eventuali disguidi nella composizione del numero; un eventuale "richiamare?" sul display del telefono comporta solo il ritardo di alcuni secondi nella chiamata che sarà eseguita durante il ciclo successivo.

Il clock del CD4017 è prelevato dal Pin 7 (Q2) del CD4040, in realtà è possibile prelevarlo anche dal Pin 9 (Q1), dove ha un periodo pari alla metà, in questo caso tutti i tempi si dimezzano, con P1 riporteremo le temporizzazioni a livelli normali pur raddoppiando il periodo di tempo totale dell'intero ciclo. È importan-



te che tra il Pin di clock e quello del primo diodo di reset (D4 – D7) ci siano tre bit vuoti che permettono al contatore decimale di contare (!) fino a 7. In questo caso dovremo collegare un diodo tra Il Pin 3 del CD4040 e il reset del CD4017. Abbiamo raddoppiato il periodo di funzionamento del telefono, possiamo ora far fare al telefono 3 cicli di chiamata lasciando tutto invariato, 7 cicli eliminando D7 e 15 cicli eliminando anche D6. I Diodi di reset collegati al CD4040 dovranno essere almeno tre per poter avere un periodo di inattività tra una chiamata e la successiva pari a 20 – 30 secondi almeno con un clock il cui periodo misurato sul Pin14 del CD4017 sia di 300 – 450ms. L'aggiunta di un diodo sul successivo bit libero dimezza il numero dei tentativi e raddoppia il periodo di pausa tra due chiamate successive.

Tabella 1

Periodo su TP1	38 mSec	75 mSec	112 mSec
Tasto e pausa	**150 mSec**	**300 mSec**	**450 mSec**
Ripete il ciclo ogni	**10 Sec**	**20 Sec**	**30 Sec**
Ciclo completo per sette tentativi	**1' 20 Sec**	**2' 40 Sec**	**3'**

Montaggio e scelta dei componenti

Come sempre il prototipo è stato montato su un ritaglio di basetta millefori, superata una prima incomprensione con il telefono ha funzionato dopo meno di 48 ore dall'inizio del montaggio del primo prototipo.

I componenti sono tutti della serie CD, perfettamente intercambiabili con la serie 74HC40xx dato che l'alimentazione è a 5V.

I transistor sono tutti NPN da commutazione, BC238, BC547 o simili.

Le due alimentazioni positive sono fornite tramite due diodi 1N4004, sono perfettamente sostituibili con qualsiasi diodo in grado si sopportare da 300 a 500 mA, sono assolutamente indispensabili, la loro assenza impedirebbe alla sirena di smettere di suonare e all'interfaccia di tornare in condizioni di riposo.

Gli altri diodi sono 1N4148, qualsiasi cosa da commutazione va ugualmente bene. I quattro o cinque diodi collegati al Pin 15 del CD4017 è bene siano uguali tra loro.

I relè impiegati sono reed a passo integrato (compatibili con il modello commercializzato dalla RS con Codice 291-9681) con diodo interno, ma qualsiasi modello dal modesto consumo di corrente sarà utilizzabile eliminando o montando il diodo in parallelo alla bobina secondo se questo è presente o meno all'interno del relè.

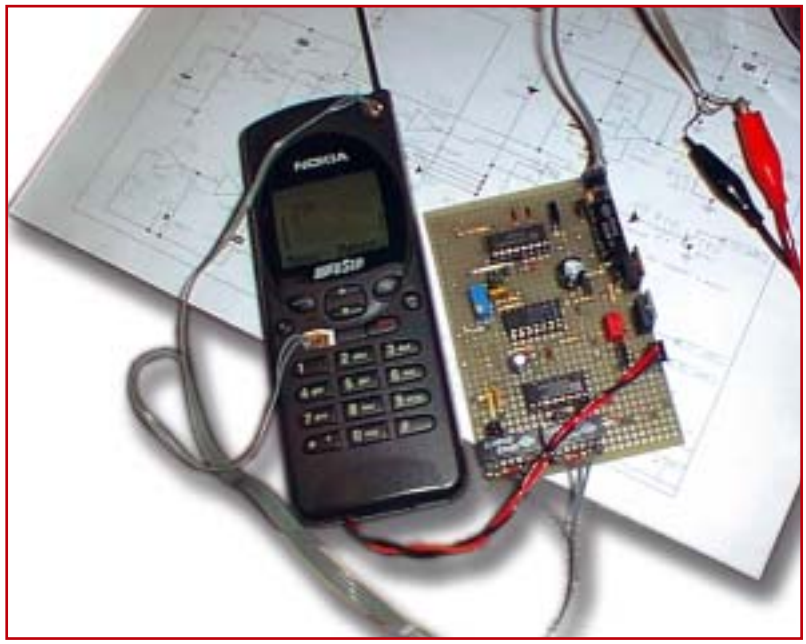
I due stabilizzatori non sono montati su dissipatore, attenzione al LM317 che ha la parte metallica collegata al pin di uscita, non a massa come il 7805, secondo che telefono alimenta potrebbe aver bisogno di un piccolo dissipatore. Il 7805 alimenta solamente i tre chip pertanto un 78L05 potrebbe funzionare senza nessun problema. I tre relè sono alimentati direttamente con i 12 V forniti dalla batteria dell'impianto.

L'intera interfaccia assorbe 27 mA, con il telefono questi salgono a 200-300 mA nei primi momenti di funzionamento poi il consumo scende a pochi milliampere per avere impulsi più consistenti durante le chiamate del cellulare. Siamo in ogni modo su un consumo medio pari a pochi punti in percentuale rispetto ad una sirena elettronica di media potenza.

I prototipi sono stati montati su basetta millefori, l'ultimo seguendo la traccia del circuito stampato presentato. Questo impiega 10 ponticelli a filo che evitano l'impiego di uno stampato a doppia faccia.

L'interfaccia verso il telefono può essere realizzata con transistor o con relè reed, secondo le esigenze nel cellulare che abbiamo deciso di distruggere. Sulla stampato so-

no stati previsti tre relè verso il cellulare, uno di accensione e due per i comandi a due tasti diversi. Se il telefono accetta i comandi che chiudono verso massa questi relè vengono eliminati e il comando è prelevato direttamente dal collettore dei rispettivi transistor. Contemporaneamente vengono eliminati anche i tre diodi in parallelo alle bobine dei relè.



Precauzioni e installazione

Come per l'impianto originale anche qui mancano completamente le protezioni di sicurezza dell'impianto. Tutto andrà realizzato con cura e in modo stabile.

Il telefono andrà posto in luogo riparato dalla polvere e dalla vista, ma NON in un contenitore metallico che potrà invece ospitare la sola interfaccia.

I cavi di collegamento tra interfaccia e telefono è bene siano del tipo schermato, molto sottili, per facilitarne la saldatura sulla tastiera del telefono e il passaggio verso l'esterno, e non eccessivamente lunghi.

Il telefono e la SIM andranno settati in modo da non richiedere all'accensione né il codice di blocco del telefono, né il codice PIN della SIM. La presenza di una di queste protezioni di sicurezza farebbe sì che il telefono, o la SIM, vadano in blocco dopo una o due prove.

Il numero legato alla SIM impiegata dovrà essere estremamente riservato, se fosse chiamato in fase di allarme potrebbe ritardare o annullare del tutto il ciclo di chiamate verso il legittimo destinatario.

Se il nostro impianto non è così spartano come quello citato è probabile che il comando alla sirena sia negativo. Lo è nella quasi totalità dei modelli da auto, Cobra, Ranger, GT, SerpiStar e Piranha hanno spesso una uscita ausiliaria per una sirena aggiuntiva che fornisce un comando negativo. In questi casi è necessario l'impiego di un relè di tipo automobilistico che capovolge il livello del segnale di allarme.

Per una eventuale installazione in auto è necessario prestare la massima attenzione alla presenza, nell'impianto della nostra vettura, del sensore di assorbimento che potrebbe causare allarmi durante lo svolgimento del ciclo di chiamate. Questo tipo di sensore rileva la caduta di tensione provocata dall'accensione di una lampada da almeno 3 W (la luce di cortesia che si accende quando apriamo la porta). Il telefono e l'interfaccia hanno un consumo analogo pertanto l'antifurto potrebbe essere vittima di un circolo vizioso che lo fa suonare quando rileva consumo di corrente provocando così altri cicli di chiamate che lo farebbero nuovamente suonare…

Il periodo di allarme di un antifurto da auto è compreso tra 30 e 45 secondi, pertanto il ciclo di chiamate di questa interfaccia lo supera abbondantemente permettendo che il sensore di assorbimento di corrente dell'antifurto possa essere ingannato dal consumo, di tipo impulsivo, del cellulare durante le chiamate. In questo caso è necessario controllare che pulsanti e sensori volumetrici funzionino a dovere, e coprano lo stesso tutti i vani della vettura per poi disabilitare il sensore ad assorbimento dell'antifurto.

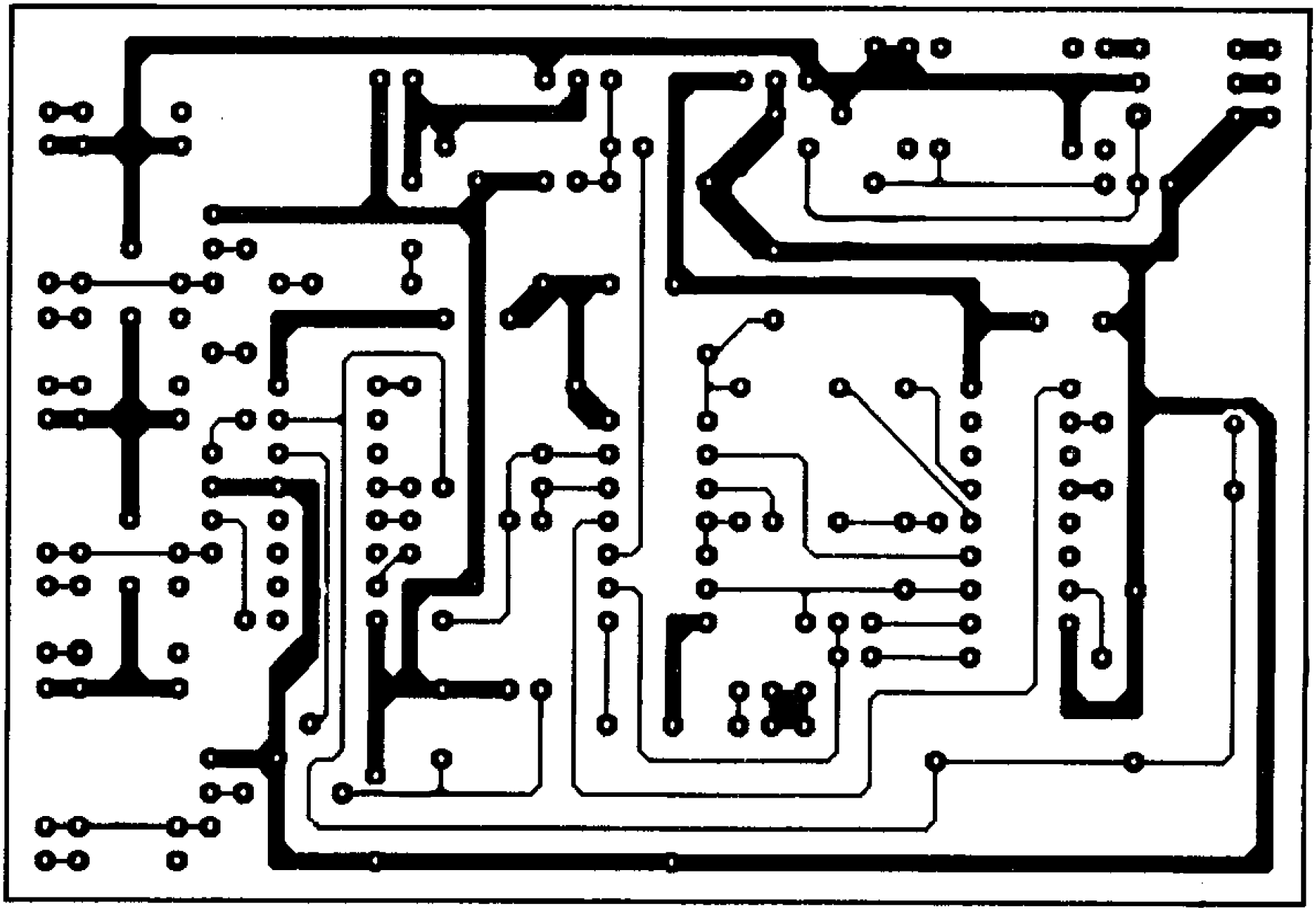
L'impulso di start non è solamente un comando, ma alimenta tutta l'interfaccia e il cellulare per i pochi attimi necessari al relè reed ad entrare in azione, dunque non è possibile impiegare una porta logica, o un transistor per capovolgere questo segnale. L'impiego di un comando elettronico farebbe venire meno uno dei presupposti del progetto, che non deve esserci alcun consumo nei lunghi periodi di inattività.

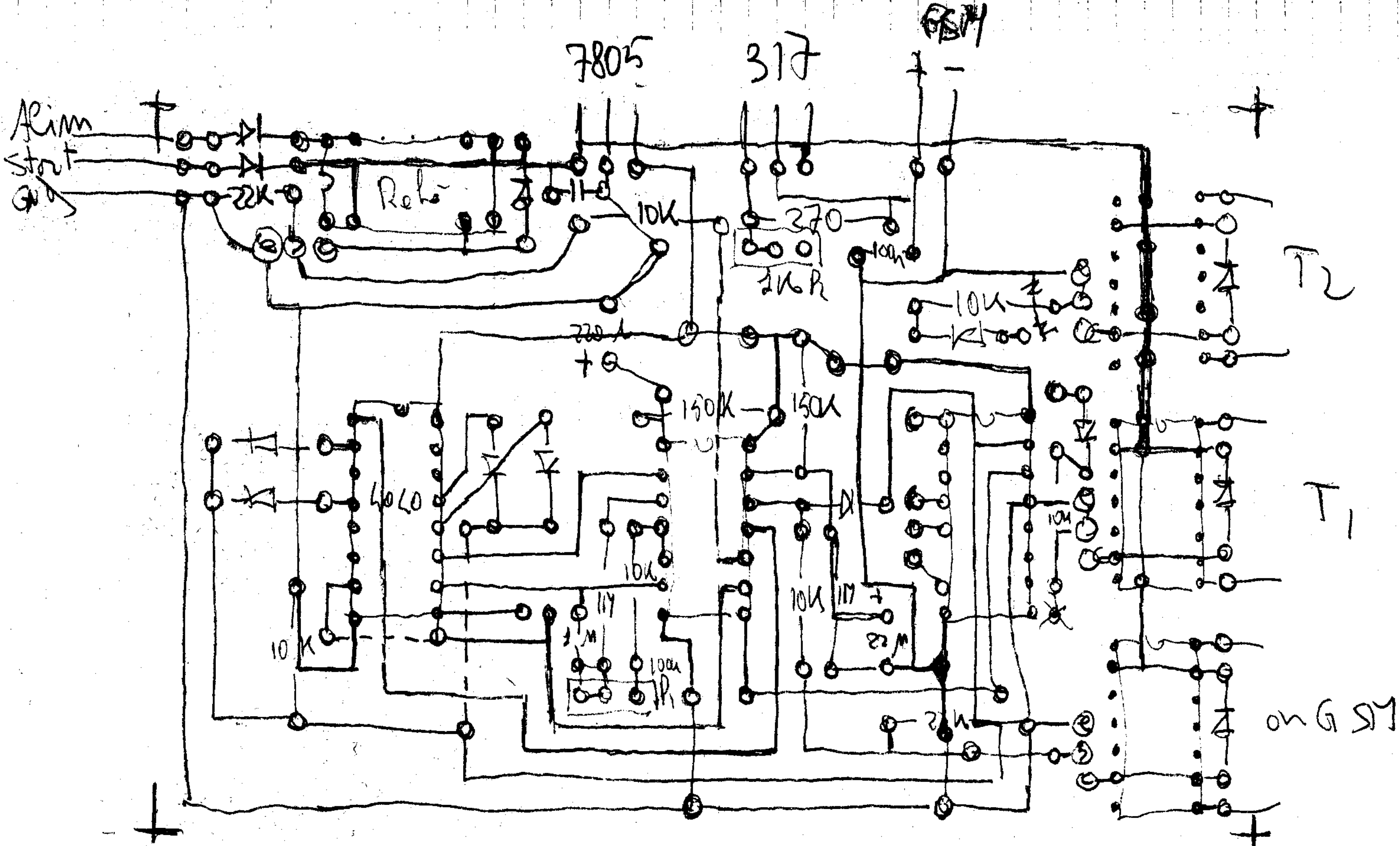
Un ringraziamento a Giulio, I1RCK per l'idea iniziale che ha portato a questa realizzazione, a Salvo IW1AYD, Paolo I1VVP, Marco IW1BIY e Mauro IK1OVY per aver fornito le vittime delle prove.

daniele.cappa@elflash.it

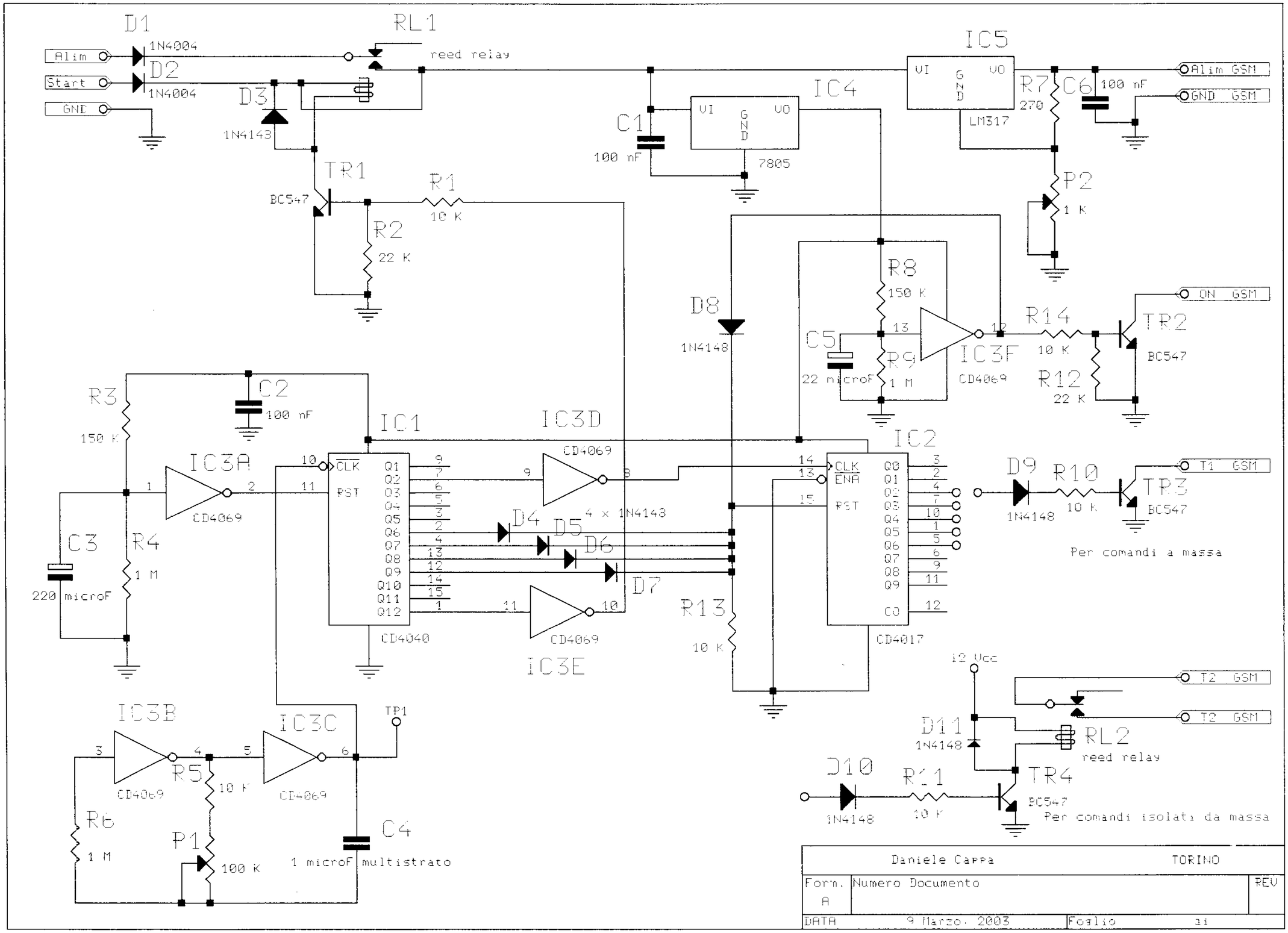
Aggiornamenti all'antifurto elettrico pubblicato su EF marzo 2003

Il Led spia consuma veramente troppo, la batteria defunge dopo due mesi.
Sostituendo il LED originale con un modello lampeggiante dotato di resistenza interna integrata e aggiungendone una esterna la 1Kohm le cose migliorano un poco, ma resta la seccatura di smontare la batteria, ricaricarla e rimontarla.
Per porre rimedio durate uno dei "ponti" tra aprile e maggio ho preparato e montato un minipannello solare da 15V a vuoto per 60 mA proveniente da una bancarella gestita da un simpaticissimo polacco (ha voluto una birra oltre ai soldini) inserendo semplicemente un diodo che impedisce alla batteria di scaricarsi sul pannello. Durante un pomeriggio nuvoloso vengono forniti alla batteria poco più di 10 mA, pochi, ma sufficienti a compensare il consumo del LED che ora potrebbe essere quello originale, molto più luminoso e visibile anche di giorno. Di questa ulteriore modifica non ho purtroppo alcuna foto, il pannello visibile nella foto fornisce 120 mA a 10V, ne ho utilizzate le celle di uno e mezzo per ottenere i 15 V necessari, pur accontentandomi di soli 60 mA. La foto si riferisce all'articolo "illuminazione automatica" pubblicato su EF gennaio 1996, riproduce comunque un gemello di quello da me utilizzato pochi giorni fa durante l'ultimo aggiornamento con il montaggio definitivo di questo teleavviso.

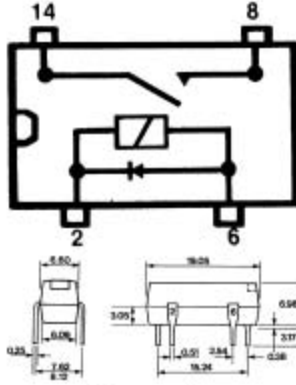



7805
317
GSM
Alim
Start
GND
22K
10K
270
220
150K
150K
4060
T2
T1
on GSM

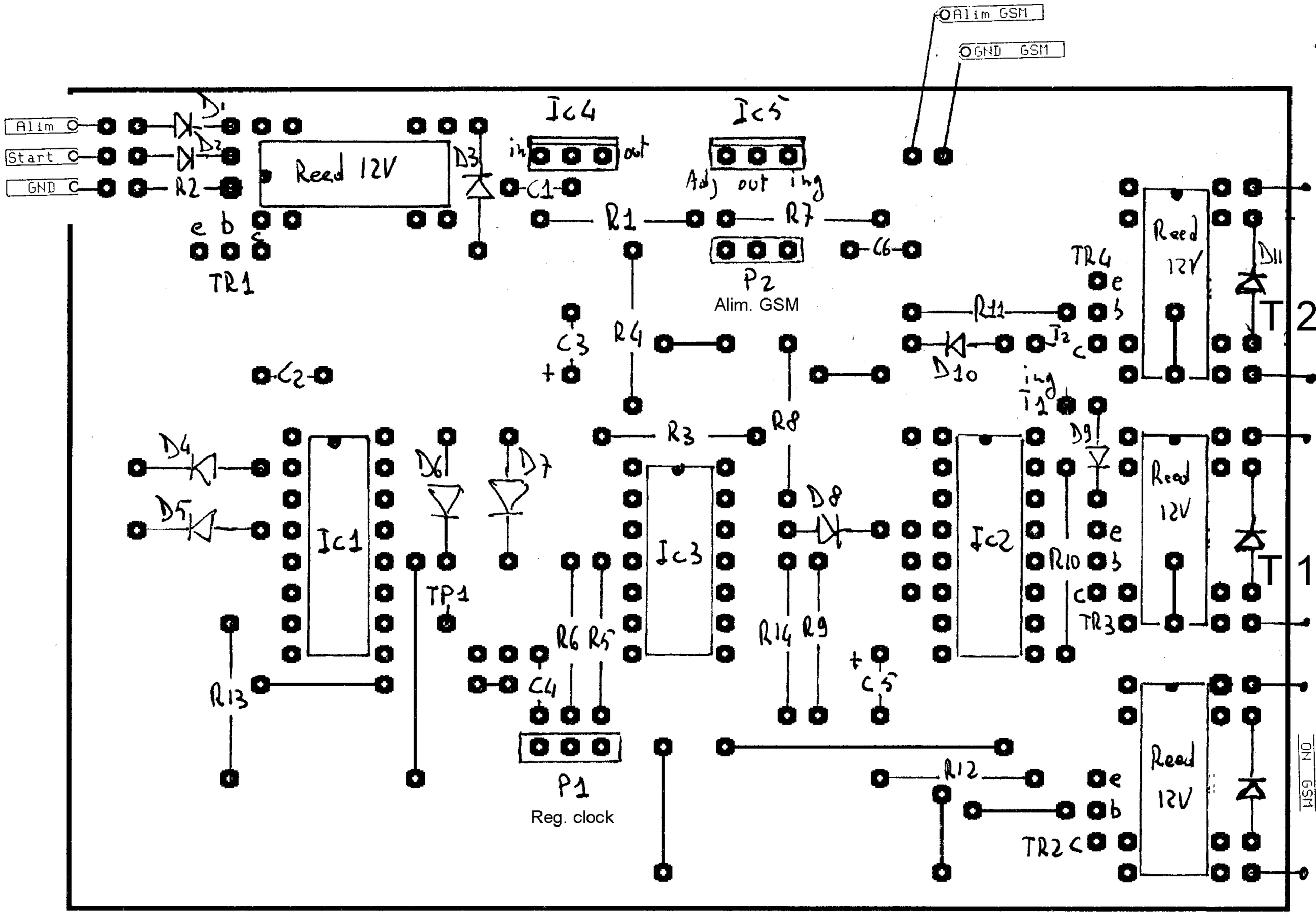
25 x 37 fori



Daniele Cappa		TORINO
Form. A	Numero Documento	REV
DATA	9 Marzo 2003	Foglio 1



Monopolare


Alim GSM
GND GSM
Alim
Start
GND
D1
D2
R2
Reed 12V
D3
Ic4
in
out
C1
Ic5
Adj out ing
R1
R7
C6
P2
Alim. GSM
e b c
TR1
C3
R4
C2
+
R11
D10
T2
TR4
Reed 12V
D11
T 2
ing
T2
R3
R8
D9
D4
D5
Ic1
D6
D7
Ic3
D8
Ic2
R10
Reed 12V
T 1
TP1
R6 R5
R14 R9
C4
C5
TR3
R13
P1
Reg. clock
R12
TR2
Reed 12V
ON GSM