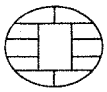
RADIOONDE Aperiodico di scienza e tecnica della radio - N. 35, dicembre 2004

Fotocopiato in proprio, distribuito gratuitamente, è gradita la collaborazione dei lettori - Il N. 34 è stato inviato a 19 lettori
Redazione: Ezio Mognaschi, v.le Gorizia,63 - 27100 Pavia PV, tel. 0382 539522, posta elettronica: mognaschi@fisicavolta.unipv.it
Hanno collaborato a questo numero: E. Mognaschi, P. Romani, R. Romero ed altri.

Notizie: * L'11 dicembre si è svolto a Varese, organizzato dalla locale sezione A.R.I., con il patrocinio della Provincia di Varese, il convegno "*I precursori sismici: stato della ricerca e sperimentazione*" con l'intervento di Mario Alberti, Ezio Mognaschi, Roberto Violi. Il resoconto è a p. 3.

Carte a processore (*Smart Card*)

di P. Romani



La naturale evoluzione delle carte magnetiche ha portato alla nascita di carte con caratteristiche più avanzate grazie all'inserimento nel supporto plastico di un chip semiconduttore o CPU (*Central Processing Unit*). Questo dispositivo è stato chiamato *Smart Card* (carta intelligente).
L'aspetto esterno che diversifica i due supporti è esclusivamente nella presenza di un quadratino di colore oro che può assumere esternamente forme diverse. In questo chip sono memorizzate informazioni, grazie ad un processo esterno, che riguardano il tipo di servizio per cui la carta è stata rilasciata. Un uso tipico è quello di chiave elettronica, il cui possesso e la conoscenza di un codice permettono l'accesso a determinate risorse (servizi di Istituti di credito, emittenti TV via satellite, ecc.).
L'architettura di un chip incorporato nella Smart Card contiene CPU, RAM, ROM, EEPROM, un circuito di sicurezza e dei contatti esterni di Input/Output in formato ISO. Ultimamente sono apparse sul mercato anche delle versioni "*contactless*" dove sono presenti un modulo di comunicazione a radio frequenza (Modem) ed un circuito induttivo d'alimentazione.

CPU - Generalmente si tratta di un microprocessore ad 8-bit con bus d'indirizzamento a 16-bit, ma nuove soluzioni basate su processori a 16-bit (Javacard) o RISC a 32-bit sono attualmente disponibili.

RAM (Memoria volatile) - Fornisce un supporto veloce per immagazzinare dati frequentemente utilizzati durante la comunicazione con il lettore e l'elaborazione delle applicazioni. Valori tipici variano da poche centinaia ad una o due migliaia di byte, poiché le dimensioni del chip non possono superare valori imposti da limiti meccanici (rottura per flessione della carta).

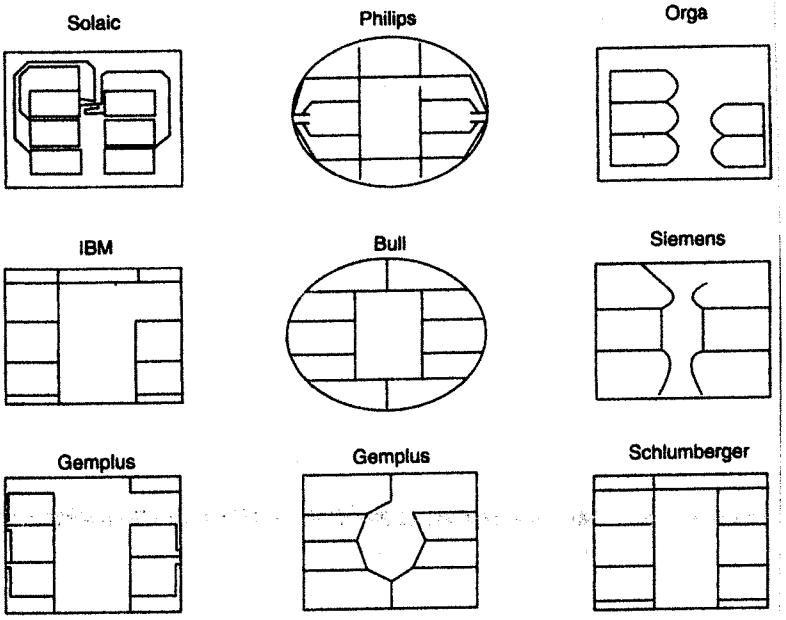
ROM (Memoria a sola lettura) - Questa memoria contiene il Sistema Operativo e viene caricata in fase di produzione della carta. Il software caricato e detto ROM-mask e non può essere modificato in fasi successive. Le dimensioni di questa memoria variano da 2 a 96 kbyte in funzione delle applicazioni per cui la carta è stata sviluppata.

EEPROM (Memoria ROM Elettronicamente Riscrivibile) - Questa memoria non volatile, che contiene i dati statici utilizzati dal Sistema Operativo, può essere modificata durante il normale funzionamento della carta. Nuove applicazioni o aggiornamenti di funzioni del Sistema Operativo possono essere caricate fornendo una notevole flessibilità nello sviluppo di soluzioni basate su Smart Card. I dati riservati sono conservati sotto forma di file e sono accessibili o aggiornabili solo se la carta lo permette. Le dimensioni variano da 2 a 128 kbyte.

Circuito di Sicurezza - Una modalità di elusione delle misure di sicurezza della carta si basa sul funzionamento a valori non nominali di alimentazione e frequenza di clock che consente la lettura dei dati contenuti nella EEPROM. Questo dispositivo controlla le condizioni di funzionamento della carta e ne abilita l'uso (in particolare della memoria EEPROM) solo se queste corrispondono a specifici valori predefiniti.

Porta di I/O - La carta comunica con l'esterno tramite una uscita seriale ad un solo bit, con velocità che variano secondo il tipo e le necessità delle specifiche applicazioni. Valori usuali sono 9600 bit/secondo, ma per le carte contactless (in cui il tempo di interazione con il lettore è ridotto), sono richieste velocità superiori. Nella figura a pagina seguente sono riportati degli esempi in formato ISO di alcuni produttori.

Coprocessori - Alcune card sono dotate di coprocessori dedicati all'elaborazione di operazioni esponenziali su interi (richiesta da algoritmi crittografici), che risulterebbe troppo lenta se implementa a sul processore tradizionale.



Tutto questo "piccolo computer" a bordo della Smart Card permette di eseguire operazioni elementari anche in interscambio con il terminale di servizio a cui viene collegato. A una parte del processore è demandata la delicata e complessa applicazione di particolari algoritmi per la sicurezza stessa del sistema.
Le capacità di memoria delle Smart Card sono imparagonabili se confrontate ai pochi bytes di quelle a banda magnetica.
Le ricerche relative alle Smart Card cominciarono nei primi anni settanta, ma solo nel 1976 Motorola e Bull svilupparono una tecnologia in grado di integrare un chip di silicio all'interno di un supporto plastico. Inizialmente furono prodotte carte con singole funzionalità (pagamento elettronico, carte d'identità, ecc.) definite in fase di produzione e non modificabili dopo la distribuzione. Nel corso degli anni ottanta furono introdotte standardizzazioni fisiche, elettroniche ed architetturali che consentirono lo sviluppo di carte personalizzabili in grado di supportare più funzionalità. Questo tipo di Smart Card, chiamate multi-purpose o multi-funzione, presentavano ancora difficoltà di modifica ed aggiornamento delle funzioni esistenti. La diffusione di questo supporto è ulteriormente dovuta all'intrinseca capacità di sfruttare tecniche crittografiche sempre più complesse (quindi più sicure) che è possibile ricondurre alle seguenti quattro tipologie:

Integrità - ossia la verifica sulla corretta trasmissione dei dati tra la Smart Card e il terminale di servizio, tramite tecniche crittografiche con controllo delle cifre o "*check digits*". Ogni singolo bit del pacchetto dati viene "legato" ad un ulteriore insieme numerico di verifica (valore "*hash*") e non è possibile modificare nessun bit senza alterarne il risultato finale.

Autenticazione - Come nella tecnica precedente di *hashing*, vengono aggiunti dei dati (una specie di "firma digitale") alle normali informazioni da trasmettere per verificare se queste provengono realmente dalla fonte originaria. Per questa tecnica di autenticazione esistono diversi tipi di algoritmi che utilizzano delle chiavi private di lunghezza variabile (512 bit, 1024, 2048, ecc...) ma anche delle chiavi pubbliche per verificare che i dati del mittente siano realmente stati inviati dalla giusta sorgente.

Irriproducibilità - Un aspetto importantissimo nella sicurezza elettronica consiste nel garantire che la "firma digitale" non possa venir copiata permettendo poi transazioni apparentemente autentiche. Infatti il contenuto informativo (ossia l'insieme di 0 e 1) in un sistema digitale risulta identico sia nell'originale che nella copia da questo ottenuta.

Riservatezza - I sistemi operativi per Smart Card devono offrire funzioni crittografiche per garantire la riservatezza dei dati in esse contenuti. Sono utilizzati diversi tipi di algoritmi che si basano principalmente su due tecniche crittografiche (simmetrica ed asimmetrica) per evitare ogni possibile intrusione nel contenuto informativo della card anche durante le transazioni.

Crittografia Simmetrica
Questa tecnica utilizza una singola chiave per codificare e decodificare i dati contenuti nella carta. Il più diffuso algoritmo simmetrico è il DES (*Data Encryption Standard*) che presenta vantaggi in termini di tempo computazionale, sicurezza e facilita di implementazione in hardware (e software). Tale algoritmo opera su un livello di 8 Byte ed opera una codifica utilizzando una chiave di dimensioni variabili. Il testo codificato ha le stesse dimensioni del testo in chiaro (dati iniziali). Conoscendo algoritmo e testo codificato è possibile decodificare il messaggio anche senza il possesso della chiave, ma il tempo necessario alla decifrazione è fortemente influenzato dalla lunghezza della chiave. Dimensioni di 56 bit sono generalmente utilizzate per immagazzinare dati riservati sulla

carta. Anche riuscendo ad ottenere i dati contenuti sulla carta occorrerebbe conoscere la chiave e l'algoritmo utilizzato. Questo tipo di algoritmo può essere utilizzato nella variante Triple DES (3DES), con più livelli di codifica dei dati e chiavi di dimensione doppia, garantendo ancora maggiore sicurezza. Il problema principale di questo tipo di algoritmi è rappresentato dal fatto che la chiave deve essere posseduta sia dal mandante che dal ricevente del messaggio. In tal modo si deve garantire la riservatezza sulla stessa chiave da parte di due entità distinte.

Crittografia Asimmetrica
Con questa tecnica sono utilizzate due chiavi crittografiche, una per codificare i dati ed una per decodificarli. Le due chiavi sono matematicamente correlate in modo che solo i messaggi codificati con una chiave possono essere decodificati con l'altra. L'algoritmo più diffuso è l'RSA (Rivest, Shamir, Adleman). Il messaggio è codificato usando una chiave pubblica distribuita a tutti i mandanti dal ricevente. Tale messaggio è poi decodificato con la chiave privata che resta unica e permette di ottenere un messaggio in chiaro. In questo modo solo il possessore della chiave privata può decodificare i messaggi. La chiave pubblica viene distribuita a tutte le entità che desiderano inviare un messaggio che solo il destinatario può leggere; se una chiave pubblica viene distribuita a terze parti, si possono solo inviare messaggi e non decodificarli come avveniva nel caso precedente. Le Smart Card utilizzano questo tipo di algoritmo in funzioni d'autenticazione di quali digital Signature o in combinazione con la tecnica precedente. La chiave pubblica è contenuta sulla carta in modo che risulti poco accessibile all'esterno. L'algoritmo RSA risulta computazionalmente più complesso del DES e la trasmissione di dati in tale codifica richiederebbe alla carta lunghi tempi di elaborazione. Solitamente si usano algoritmi asimmetrici per trasmettere chiavi per algoritmi simmetrici; una volta che entrambe le parti possiedono una chiave uguale (DES), generata anche come numero casuale, si può stabilire una connessione sicura e trasmettere messaggi codificati simmetricamente.

Nel giro di pochi anni un microchip, chiamato EMV (dalle iniziali di Europay international, MasterCard, Visa), snellirà moltissimo le transazioni di autenticazione. Oggi ci vogliono dai 10 ai 30 secondi mentre con un EMV ne basterà 1 solo e addirittura senza la necessità di collegamento alla banca! Questo sarà reso possibile perché il chip conterrà tutte le informazioni sull'identità del titolare...

La progettazione di un sistema sicuro è spesso compito estremamente difficile per le aziende che sviluppano gli algoritmi e la loro implementazione nei chip. A livello teorico sarebbe possibile attingere al contenuto informativo di qualunque card tramite una comunicazione seriale e un semplice software. I possibili attacchi ai sistemi contenuti nelle Smart Card possono esser di due tipi: tramite tecniche di ingegneria inversa o di analisi delle EEPROM.
Con il primo approccio si tenta di ricostruire la logica interna del chip per trovare un possibile punto debole del sistema, mentre con il secondo tramite un personal computer e un'interfaccia (lettore di smart card), si può leggere il contenuto delle EEPROM per poi tentare di decifrarne il contenuto.

Bibliografia
- "Segreti, Spie, Codici cifrati" di Giustozzi, Monti, Zimuel (Ed.Apogeo)
- siti internet specializzati nel settore
- articolo su mensile FOCUS (novembre 2004)

Convegno "I precursori sismici: stato della ricerca e sperimentazione"

di Ezio Mognaschi

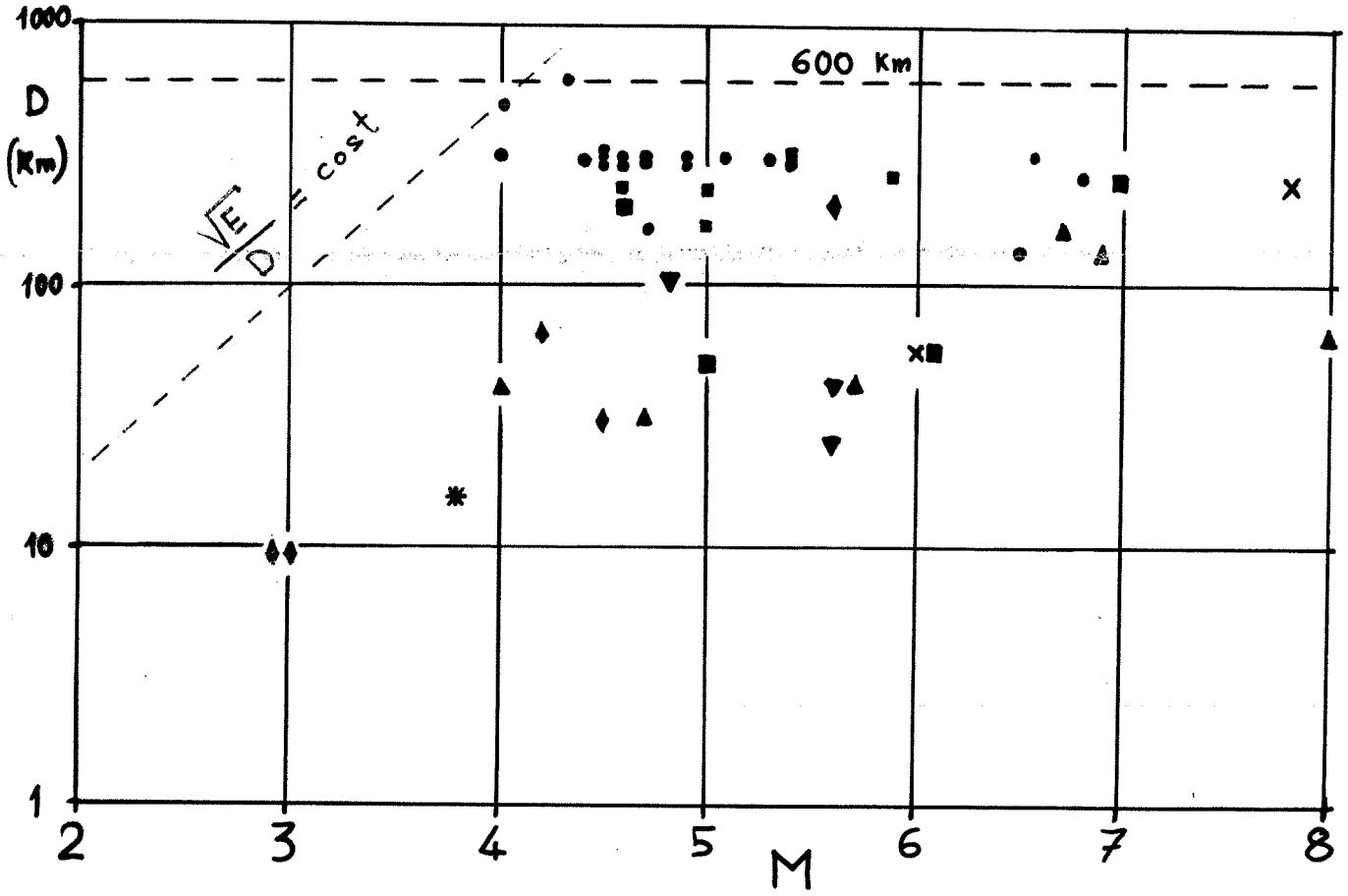
La sezione A.R.I. di Varese, con il patrocinio della Provincia, ha organizzato sabato 11 dicembre 2004 un convegno per fare il punto sulla ricerca e la sperimentazione che alcuni gruppi di sperimentatori stanno conducendo da diversi anni. La manifestazione si è svolta nella sala convegni di villa Recalcati, un palazzo signorile del '700, restaurato dalla Provincia ed adibito a scopi di rappresentanza ed allo svolgimento di incontri e congressi.

Il benvenuto ai partecipanti è stato dato dall'ing. Pietro Gervasini, i2GEK, che ha presentato i relatori e gli ospiti. Per la provincia di Varese è intervenuto il giovane assessore alla Protezione Civile Campiotti che ha sottolineato la cooperazione in atto a Varese tra radioamatori, Protezione Civile ed *Osservatorio Geofisico Prealpino* per la gestione di emergenze idrogeologiche e sismiche. Un assessore comunale ha poi portato il saluto del sindaco ed il presidente della Sezione A.R.I. di Varese Massimo Castelli, iK2NBP, ha portato il saluto dei radioamatori varesini.

La prima relazione, di Mario Alberti, ha riguardato la storia della sperimentazione svolta negli ultimi 5 anni in collaborazione tra la Sezione A.R.I. della Lunigiana, quella di La Spezia ed Ezio Mognaschi per la parte scientifica. Ha poi affermato che il futuro della sperimentazione necessità dello sviluppo di nuovi strumenti e della costituzione di una rete di stazioni, tutte uguali, da collegare tra loro e con un centro di controllo per poter correlare tutti i dati in tempo reale. Questo centro sarà dotato di un software già pronto, ma da collaudare, in modo da analizzare i dati provenienti da diverse stazioni al fine di localizzare la provenienza di eventuali precursori. Alberti ha infine mostrato il prototipo del ricevitore per frequenze inferiori a 40 Hz, realizzato da Alfredo Bernardi, i5JRV. Il ricevitore, che dovrebbe essere adottato dalle stazioni della rete è stato realizzato con un circuito stampato delle dimensioni di 18 ×18

cm^2; la parte più ingombrante del ricevitore è il filtro di ingresso costituito da tre induttanze in serie, su nucleo di ferro, e due condensatori in parallelo da 10 μF.

La seconda relazione, di Ezio Mognaschi, ha riguardato la possibile origine dei precursori elettromagnetici dei sismi in relazione al processo di microfratturazione delle rocce, argomento ben noto ai lettori di *Radioonde* e che pertanto non verrà qui ripetuto. Nella relazione di Mognaschi una novità ha riguardato la distribuzione di alcune decine di precursori (identificati però come tali solo dopo aver avuto notizia dei relativi sismi e perciò denominata "previsione a posteriori") mostrata qui sotto. I dati sono stati ricavati da molti articoli pubblicati su riviste internazionali e da qualche osservazione eseguita a Pavia. In ascissa è riportata la magnitudo M degli eventi sismici, mentre in ordinata la distanza D in km tra epicentro e stazione ricevente, in scala logaritmica. La prima osservazione



importante riguarda la massima distanza D per la ricezione di precursori elettromagnetici: nessuna osservazione è stata sinora riportata, per stazioni terrestri, per D > 600 km. La tratteggiata orizzontale segna, appunto, questo limite. Anzi, ove si escludano i due punti più in alto, dovuti ad osservazioni fatte negli Stati Uniti e molto al di là delle altre osservazioni, la massima distanza scende a circa 300 km, indipendentemente da M per M > 4. Questo fatto dovrebbe essere legato a questioni di propagazione dei precursori lungo la superficie terrestre. La seconda osservazione riguarda i sismi con M < 4, non sono molti non perché questi sismi siano infrequenti, anzi, ma perché sono stati forse oggetto di minore attenzione. Osservando l'andamento complessivo dei punti è venuto spontaneo tracciare una retta, opportunamente inclinata, rispetto alla quale, anche per M < 4 non ci sono osservazioni. Si è partiti dalla magnitudo M e da questa è stata ricavata l'energia in joules del relativo sisma con la relazione empirica log E = 12.24 + 1.44 M. L'autore è consapevole che la relazione è corretta solo per M > 5 e che non esprime direttamente l'energia, bensì il momento del sisma, ma, in mancanza di meglio, l'ha usata lo stesso! Ritenendo poi che la potenza dei segnali elettromagnetici emessi (una piccolissima parte di quella in gioco) fosse proporzionale all'energia perché tutti i sismi hanno durate dello stesso ordine, cioè di circa 10 secondi, e sapendo che un segnale radio ha intensità proporzionale alla radice quadrata della potenza irraggiata ed è inversamente proporzionale alla distanza dalla sorgente, ha provato a rappresentare la retta $\sqrt{E}/D$ = costante, con una costante opportuna. Anche i punti relativi ai precursori di sismi minori (M< 4) stanno al di sotto di questa retta, come si vede dal grafico. Il ragionamento sopra riportato non è rigoroso, ma altre considerazioni non si possono fare attualmente. La pendenza della retta è inoltre abbastanza vicina all'andamento generale delle osservazioni per M < 4.5. Per riassumere, le rette tratteggiate rappresentano la base minore ed un lato di un trapezio che, grossolanamente, definiscono i limiti di osservabilità dei precursori elettromagnetici.

La terza relazione, presentata dal dott. Roberto Violi, iK1XHH, di Sarzana, ha avuto per argomento l'illustrazione del programma di gestione della costruenda rete radioamatoriale. Il programma creato da Violi

permette di gestire le singole stazioni, il nodo cui faranno capo circa sei stazioni e la rete nel suo complesso che potrebbe avere anche migliaia di stazioni. Il programma permette di analizzare i dati di rumore elettromagnetico in funzione del tempo, calcolando il livello medio del rumore per evidenziare automaticamente segnali che poterebbero essere precursori. Da un confronto tra le intensità dei segnali ricevuti dalle singole stazioni di un nodo (che, perciò devono essere tutte identiche come caratteristiche di sensibilità e di banda ricevuta) o, sperabilmente, di più nodi il programma determina automaticamente il punto di provenienza dei segnali. Quello della localizzazione del punto di provenienza dei segnali è il primo passo verso la previsione dei terremoti, in futuro si pensa di poter stimare anche la magnitudo dell'evento, mentre per la determinazione del lasso di tempo tra precursori e sisma occorre ancora acquisire molti dati sulla dinamica del fenomeno.

Molte sono state le domande del pubblico, una sessantina di persone, tra le quali una numerosa rappresentanza di radioamatori del bresciano, resi temporaneamente sensibili alla problematica trattata dal recente sisma del Garda, ed il Direttore del *Centro Geofisico Prealpino* di Varese, prof. Salvatore Furia. Quest'ultimo, anch'egli radioamatore, ha avuto parole di elogio per le attività di sperimentazione in corso e per le nuove proposte. Ha poi messo a disposizione la sede dell'Osservatorio per installare una stazione per il monitoraggio elettromagnetico, mentre la Provincia di Varese ha assicurato la copertura finanziaria per allestire la stazione stessa.

L'impressione generale è stata dell'esistenza di un'atmosfera di collaborazione tra l'ambiente politico che ha la possibilità di disporre dei pur modesti finanziamenti occorrenti e la comunità locale dei radioamatori. Caso unico in convegni di questo tipo è stata la presenza continuata alle prime due relazioni dell'assessore provinciale; di solito i politici, ammesso che prendano parte a queste manifestazioni, si limitano ad un benvenuto di circostanza e poi si disimpegnano con la scusa di altre incombenze improrogabili e, naturalmente, di maggiore rilevanza!

Stagno, piombo e... colofonia

di Ezio Mognaschi

Chi non ha mai giocato con i soldatini di piombo o con modellini di automobili realizzati con leghe di questo metallo? Il piombo, per le sue caratteristiche di malleabilità, discreta conducibilità elettrica e termica, inattacabilità da molti acidi e da tutte le basi è stato ampiamente usato in passato nell'edilizia e nell'idraulica ed è ancora usato in quasi tutte le leghe per la saldatura e per ottenere leghe molto fluide di bronzo. Quest'ultima scoperta è antichissima: per realizzare leggere e leggiadre cavigliere in bronzo per le loro donne, gli antichi Celti usavano aggiungere, già nel V secolo a. C., piombo alla lega rame-stagno. Gli ossidi di piombo (la biacca, conteneva biossido di Pb, il minio è il sesquiossido di Pb) venivano largamente usati nella pittura, nelle decorazioni (le miniature) e nell'industria delle vernici. A partire dagli anni '60 del secolo scorso è divenuto impossibile acquistare sfusa la polvere rossa di minio, mentre rimaneva il minio in alcune vernici antiruggine. Oggi è sparito anche da queste e le vernici antiruggine contengono dei surrogati meno efficienti, ma meno tossici. Dalla benzina è stato tolto il tossico piombo per aggiungere il cancerogeno, se non bruciato completamente, benzene.

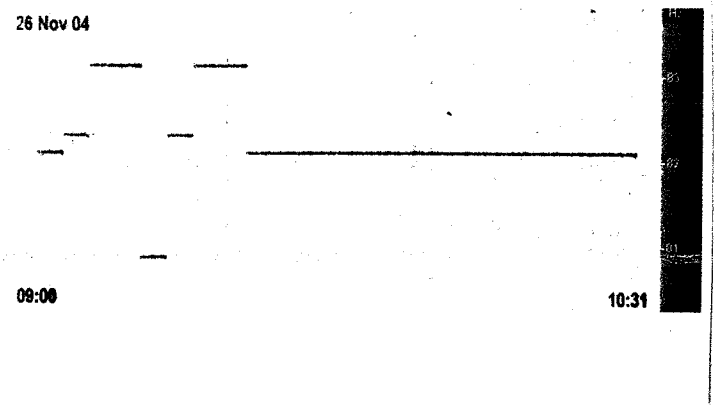
I dati medico-scientifici mostrano gli effetti cumulativi del piombo sul sistema nervoso centrale e sulla formazione di cellule rosse del sangue. Oggi si sa che i bambini sono molto più vulnerabili degli adulti per l'esposizione al piombo. Il limite è fissato in Italia a 25 μg per decilitro di sangue, mentre negli Stati Uniti, dal 1991, il limite è 10 μg per decilitro. Negli U.S.A. regalare ad un bambino un oggetto contenente piombo costituisce reato di abuso sui minori. Ma il piombo è, da sempre, uno dei più diffusi componenti delle leghe per saldatura. Nella costruzione e nella riparazione di circuiti elettronici gli operatori, ove non adeguatamente protetti, rischiano di ingerire piombo. Una lega molto diffusa è la 60/40 che contiene il 60% di stagno ed il 40% di piombo. Diversi sono i meccanismi di ingestione: il principale è attraverso le mani che vengono a contatto con il piombo e, se non accuratamente lavate o se non si usano guanti, quando si porta successivamente il cibo alla bocca si ingerisce inavvertitamente anche del piombo; c'è poi la penetrazione per diffusione attraverso la pelle ed infine l'ingestione attraverso le vie respiratorie se si respirano vapori di piombo rilasciati dal metallo fuso. Questo terzo meccanismo è il meno pericoloso poiché la presenza di piombo nei fumi delle operazioni di saldatura è molto piccola.

Ma il rischio peggiore dall'inalazione di fumi delle saldature non è nel piombo, bensì nel deossidante contenuto nell'anima del filo per saldare o spalmato sulle superfici da saldare. Questo materiale chiamato in inglese "*flux*" viene aggiunto affinché la lega di piombo fusa bagni bene le superfici da saldare e per deossidare le stesse. Per le saldature di tipo elettronico il deossidante è a base di colofonia, in inglese "*rosin*". Si tratta di una resina vegetale prodotta da alcune conifere e nota anche con il nome di pece greca. Sebbene si tratti di una sostanza naturale il suo contatto con altre sostanze chimiche presenti nella pasta per saldare provoca, ad alta temperatura, fumi acidi potenzialmente dannosi. I sintomi da intossicazione di fumi delle saldature sono mal di testa, nausea, irritazione agli occhi e tosse, per arrivare a bronchite cronica ed asma per le persone esposte a lungo per motivi di lavoro. Per eliminare completamente i pericoli da inalazione di fumi prodotti nelle saldature è sufficiente fare in modo di non respirarli e cioè lavorare o all'aria aperta o in presenza di una corrente d'aria che trasporti lontano i fumi. Ma un'altra minaccia incombe su chi usa saldare: dal luglio 2006 l'Unione Europea bandirà l'uso del piombo nelle applicazioni elettriche ed elettroniche. Non è chiaro cosa si userà al posto del piombo, ma è evidente che chi vuole continuare a saldare, pur usando le debite precauzioni, deve fare incetta di filo per saldare prima che zelanti burocrati tolgano dal commercio le leghe a base di piombo.

E-mail alla redazione

A proposito della disattivazione dei TX U.S.A. a 76 Hz (v. *Radioonde* N. 34) Renato Romero conferma la cessazione di queste emissioni ed aggiunge una ulteriore osservazione sulle analoghe emissioni russe a 82 Hz.

"Se è vero che gli USA hanno chiuso il programma a 76 Hz, è stranamente coincidente il fatto che anche i russi non trasmettano più sugli 82 Hz. Stavo dando un'occhiata alle registrazioni di agosto 2004 e delle emissioni a 82 Hz non c'è più traccia! Non ho dubbi sulla cosa: il segnale superava le risonanze di Schumann di quasi 20 dB utilizzando una risoluzione di 5 mHz ... ora più nulla". Il 30 novembre Romero comunica: "i russi sono nuovamente *on air* dopo mesi di inattività". Ecco qui a fianco una registrazione ove si può notare la modulazione in frequenza di un segnale di 91 minuti a 82 Hz, con risoluzione FFT di 27 mHz.



"Mi sembra probabile che la finestra radio sottomarina passi di mano ai vari siti tipo l'HAARP (altrimenti non ne avrebbero costruiti 6 sparsi per tutto il mondo, di cui l'ultimo in costruzione in Svezia) ma mi lascia perplesso il fatto di non ricevere alcun segnale. Forse le modulazioni sono più complesse? Emissioni a *spread spectrum*? Forse".

Per informare cosa sia l'HAARP Renato Romero ha inviato una nota che viene riassunta qui di seguito.

L'HAARP è un programma di ricerca scientifica, attivo dai primi anni '90, per studiare le proprietà ed il comportamento della ionosfera, con particolare riguardo alla sua comprensione ed al suo uso per migliorare le comunicazioni ed i sistemi di sorveglianza sia per uso civile, sia a scopo di difesa. Il centro di ricerca dell'HAARP è situato vicino al villaggio di Gakona, in Alaska, ed effettua il monitoraggio di molti parametri fisici della ionosfera utilizzando TX in HF di grande potenza per eccitare temporaneamente una zona limitata della ionosfera a scopo di studio. Vengono monitorati anche molti altri parametri fisici: dai campi statici alle VHF, il campo elettrico e magnetico terrestre, l'opacità della ionosfera con riometri (*riometer* da *relative ionospheric opacity meter*), ecc. Per avere una panoramica dei dati giornalmente raccolti da HAARP si può visitare il sito: *http://www.haarp.alaska.edu*
L'attività di questo centro ha interessato molte persone, compresi gli ambientalisti, in quanto è dotato di un sistema impressionante di antenne trasmittenti da cui vengono irradiati 3.6 MW in HF da 2.8 a 10 MHz. L'efficienza delle antenne è tale da poter irradiare fasci di solo 5°, con un guadagno d'antenna di 30 dB, allo scopo di eccitare un'area limitata della ionosfera per studiare i processi fisici indotti. Queste eccitazioni generano segnali in banda ELF i quali, per la loro capacità di penetrazione anche nell'acqua marina, sono utilizzabili per comunicazioni con i sottomarini. La tecnica usata è quella di irradiare con radiofrequenza lo strato E della ionosfera (tra 80 e 100 km di quota). Alle alte latitudini la ionosfera è percorsa da correnti di milioni di ampere e l'effetto dell'irraggiamento a radiofrequenza è di ridurre la conducibilità elettrica della ionosfera, sino a quando permane l'eccitazione. Allo spegnimento del campo a radiofrequenza le correnti ionosferiche riprendono. Così è possibile, accendendo e spegnendo il fascio HF ad es. a 3.2 MHz con una frequenza di 12.5 Hz, ottenere una modulazione a 12.5 Hz delle correnti ionosferiche e quindi un segnale in banda ULF. Questo tipo di modulazione è possibile sino alla frequenza di 30 kHz. Il rendimento di questo sistema indiretto di trasmissione è molto basso: da 1 MW in radiofrequenza si possono ottenere circa 10 mW in banda ELF. I segnali a terra sono molto deboli: da 1 a 3 pT per l'intensità del campo magnetico, prossima a quella delle risonanze di Schumann ed al rumore ambientale.
La stazione dell'Alaska è la più nota, ma non la sola; altri impianti sono, dal 1970, a Platteville, Arecibo, Sura, Tromsoe, Hipas, con potenze da 750 kW ad 1.6 MW e frequenze da 2.7 a 25 MHz e guadagni d'antenna sino a 28 dB. L'impianto programmato in Svezia, ad Hiscat, dovrebbe avere un guadagno di 35 dB, con 10 MW di potenza e quindi con un segnale effettivamente emesso di circa 30 GW. Investimenti di questa portata non possono non avere un ruolo militare, magari dissimulato da scopi di ricerca scientifica per... studiare la ionosfera.

Buon Natale e felice Anno Nuovo a tutti i lettori.