

# RFID

Fondamenti di una tecnologia silenziosamente pervasiva

PARTE VI

## STANDARD E PROTOCOLLI DI COMUNICAZIONE



di Paolo Talone, Giuseppe Russo  
Fondazione Ugo Bordoni

*Questa parte è dedicata agli standard di comunicazione, problema di fondamentale importanza per la tecnologia RFID, come per tutte le applicazioni che richiedono interoperabilità tra entità diverse ed intercambiabilità tra apparati di differenti costruttori.*

*L'articolazione della Parte VI è la seguente:*

- *Vengono introdotte dapprima le problematiche internazionali, con particolare attenzione alle diverse condizioni operative nei consorzi privati (EPCglobal) e negli enti pubblici di normativa (ISO), fornendo anche un quadro internazionale degli enti ed associazioni collegate*
- *Successivamente viene illustrata la normativa prodotta dai due grandi enti ISO ed EPCglobal, con particolare interesse per i nuovi TAG RFID passivi "Generation2", i maggiori candidati all'applicazione massiva sui singoli oggetti (corrispondente alla produzione di centinaia di miliardi di TAG da parte dell'industria)*



## VI.1 **NORMATIVA PER LE INTERFACCE DI COMUNICAZIONE**

Si è visto (cfr.§I.2) che la standardizzazione che regola il dialogo tra TAG e Reader vede come protagonisti essenzialmente due temi: la gestione dello spettro radio (frequenze e potenze) e le interfacce di comunicazione. Questo capitolo è dedicato a quest'ultimo tema, ovvero i protocolli di comunicazione per l'interfaccia radio e le prestazioni dei TAG in termini di memoria e capacità di elaborazione.

### VI.1.1 **LA STANDARDIZZAZIONE DELLE INTERFACCE DI COMUNICAZIONE**

La tecnologia RFID è stata ed è oggetto di consistenti attività di normazione sia a livello pubblico (internazionale e regionale), sia privato (consorzi di aziende).

Nei primi anni di vita la standardizzazione non è stata un processo ordinato. La storia degli standard RFID negli ultimi 10 anni, infatti, non ha seguito uno sviluppo ideale, venendo governata da particolari interessi industriali.

Questo anche perché le opinioni sulla necessità di standard unici e pubblici non sono unanimi. Per la maggior parte degli esperti la proliferazione di specifiche di consorzi privati, i cosiddetti “standard de facto”, comporta incrementi nei costi sia per lo sviluppo tecnologico sia per i prodotti finali e comporta, inoltre, una significativa barriera al commercio. Da un altro punto di vista, però, una “libera” competizione (che quindi veda la competizione di specifiche tecniche di consorzi privati senza grande necessità di standard ufficiali emessi dalle organizzazioni di normativa), potrebbe essere vista come uno stimolo a sviluppare tecnologie antagoniste il cui successo sarebbe garantito dalle prestazioni e dal mercato invece che da accordi all'interno delle commissioni.

La linea che si sta affermando vede prevalere gli standard “pubblici”, solo però per quanto riguarda la razionalizzazione del processo produttivo dei TAG e le conseguenti economie di scala. L'azione dei produttori negli organismi di normativa è infatti tale da far strutturare gli standard con una quantità di opzioni spesso ingiustificata sul piano dell'utilizzo. Questo non ostacola la razionalizzazione dei processi produttivi, ma

rende troppo agevole differenziare i prodotti in modo da rendere ardua la cosa che maggiormente interessa l'utilizzatore, ovvero l'intercambiabilità tra fornitori. Si potrebbe quindi concludere che l'affermazione degli standard "pubblici", oggi prodotti dalle organizzazioni internazionali di normativa, va vista come un processo decisamente positivo, ma le contingenze nelle quali si consolida tutelano meglio gli interessi dei produttori, rispetto a quelli degli utilizzatori.

### **VI.1.2 APPLICAZIONI OPEN LOOP VS. CLOSED LOOP**

Le prime applicazioni, standardizzate tra il 1996 ed il 2001, sono quelle che riguardano il cosiddetto "closed loop", ovvero i contesti in cui il medesimo TAG viene riusato per vari oggetti o, in logistica, nel caso di contenitori, in cui il TAG sia riusabile per contenuti differenti.

Gli esempi più celebri di applicazioni closed loop sono le carte senza contatto, per pagamenti e per controllo accessi, ma anche i TAG per lavanderia e quelli, già citati, per contenitori riusabili.

Queste applicazioni vedono, di recente, anche l'impiego dei più costosi TAG attivi accanto ai consueti TAG passivi, per i quali, nelle applicazioni più recenti, la riscrivibilità diventa una caratteristica importante.

Per le applicazioni "closed loop" ISO ha sviluppato le famiglie di standard per carte senza contatto (cfr. §IX.4.4) e per l'identificazione degli animali (cfr. §IX.4.3) oltre a quelle per contenitori riusabili.

Il cosiddetto "open loop", invece, è il contesto di quelle applicazioni nelle quali il TAG segue l'intera vita dell'oggetto al quale è associato. Queste applicazioni impiegano essenzialmente TAG passivi a basso costo.

Le applicazioni cosiddette "open loop" riguardano l'uso degli RFID sui singoli oggetti nel commercio, ma anche gli RFID in contenitori "a perdere" (casse, imballaggi, pallet) e riusabili, quali i "container", se dopo ogni viaggio, il TAG viene sostituito.

Queste applicazioni sono relativamente più recenti, tra il 2003 ed i giorni nostri, e coincidono con la nascita e l'operatività di EPCglobal (e del suo predecessore Auto-ID Center) (cfr. §IX.4.1).

Anche ISO sta sviluppando standard per applicazioni "open loop",

dalla gestione logistica di container, di pallet, di contenitori da trasporto, a quella dei singoli oggetti (incorporando gli standard EPCglobal).

La progressiva riduzione dei costi dei TAG passivi sta rapidamente conducendo quest'ultimi dalle applicazioni "closed loop", per le quali sono nati, verso nuove applicazioni "open loop" in cui il TAG viene associato non al contenitore riusabile, bensì al singolo oggetto, seguendolo per tutta la sua vita e spesso sopravvivendogli. Per questo tipo di applicazioni è previsto il maggior sviluppo in un prossimo futuro.

### **VI.1.3 GLI ENTI DI NORMAZIONE**

Organizzazioni pubbliche e consorzi di aziende hanno portato avanti, in questi anni, l'attività di normazione sui sistemi RFID; tra questi emergono essenzialmente EPCglobal ed ISO.

- EPCglobal nato ed operante come una associazione privata (cfr. §IX.2);
- ISO (ed organismi ad esso collegati) che costituisce l'ente mondiale di normativa in quasi tutti i campi della tecnologia.

Iniziato con specifiche esclusivamente proprietarie, il processo di standardizzazione vede ora la competizione tra i due organismi i cui elaborati stanno convergendo.

Ad esempio, gli standard per l'interfaccia radio sono, ad oggi, proposti sia da ISO che da EPCglobal (probabilmente l'uno orientato su tutti i campi inerenti la gestione degli oggetti, l'altro polarizzato sulle esigenze specifiche della catena di distribuzione).

A questo proposito andrebbe sottolineata l'esistenza di punti di vista differenti relativamente all'approccio normativo di EPCglobal sui temi della proprietà intellettuale.

Il processo di armonizzazione della normativa comunque è in corso e porterà ad una famiglia di standard globali, che garantirà adozione universale. Questo sarà un fattore chiave per la definitiva affermazione della tecnologia RFID. Nel seguito si accenna al quadro dell'articolazione, nelle varie regioni, delle organizzazioni che fanno capo all'ISO.

### **1.3.1 Situazione in Europa**

La normativa ISO viene recepita, a livello europeo, dal Comitato Europeo di Standardizzazione (CEN), per quanto riguarda la parte fisica (hardware) e procedurale (protocolli di comunicazione), mentre l'Istituto Europeo di Standardizzazione nelle Telecomunicazioni (ETSI) emette normativa nelle materie omonime (essenzialmente compatibilità elettromagnetica).

### **1.3.2 Situazione in USA**

L'ANSI (American National Standard Institute) costituisce negli USA l'equivalente del CEN europeo. Il NIST (National Institute of Standards and Technology), invece, è una agenzia del Dipartimento del Commercio Americano che emette standard obbligatori per gli acquisti fatti dal governo degli USA escluso il DoD (Dipartimento della Difesa) che ha standard propri.

### **1.3.3 Situazione in Cina**

Anche in Cina esiste l'organismo che recepisce gli standard ISO, ovvero il Dipartimento per la Standardizzazione della Cina SAC (Standardization Administration of the People's Republic of China) che agisce su autorizzazione governativa (State Council) e sotto il controllo dell'AQSIQ (General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China).

La Cina, che si avvia a costituire uno dei maggiori mercati mondiali, sta iniziando in modo indipendente un lavoro di standardizzazione sugli RFID. Questo può generare criticità nell'etichettatura di beni cinesi destinati oltreoceano, in quanto la Cina che esporta un grande volume di beni, è uno dei maggiori mercati potenziali della tecnologia RFID.

Attualmente il "Ministry of Science and Technology (MOST)" cinese ed altri 13 dipartimenti governativi, inclusi i "Ministry of Information Industry (MII)" ed il già citato SAC, hanno prodotto un "white paper" che traccia le linee guida per lo sviluppo degli RFID nel paese.

L'amministrazione cinese ha incaricato il "National RFID Tags Standards Working Group" di definire quale tecnologia debba essere adottata in Cina. Molto probabilmente verrà deciso di adottare qualcosa

di compatibile con gli standard EPCglobal ed ISO, purché vengano adoperati propri diritti sulla proprietà intellettuale in modo da ottenere standard liberi da royalty.

#### **VI.1.4 LA NORMATIVA ISO ED EPCGLOBAL**

I primi standard RFID sono stati realizzati in ISO, per TAG passivi a bassa frequenza e comprendono:

- Gli standard sui TAG per identificazione degli animali
  - ISO 11784
  - Radio frequency identification of animals - Code structure
  - ISO 11785
  - Radio frequency identification of animals - Technical concept
- Protocolli per l'interfaccia radio per TAG RFID usati nei sistemi di pagamento, smart cards senza contatti e carte di prossimità
  - ISO/IEC 10536
  - Identification cards -- Contactless integrated circuit(s) cards --
    - ISO/IEC 14443
  - Identification cards - Contactless integrated circuit(s) cards - Proximity cards
  - ISO/IEC 15693
  - Identification cards - Contactless integrated circuit(s) cards - Vicinity cards
- Metodi per il test e la conformità di TAG e Reader RFID ad uno standard (ISO/IEC 18047);
- Metodi per il test delle prestazioni di TAG e Reader RFID (ISO/IEC 18046).

Successivamente EPCglobal ha prodotto normative orientate all'uso dei TAG nella logistica, ovvero:

- una tassonomia di classi di TAG;
- standard per protocolli di comunicazione a radio frequenza tra TAG e Reader;
- formato per la memorizzazione delle informazioni di identificazione nei TAG.

Inoltre EPCglobal ha creato standard e specifiche per l'interconnessione di sistemi informatici (server) che consentono di accedere ad informazioni complete su oggetti identificati tramite codici EPC, tramite i codici EPC medesimi ottenuti dai TAG.

Il tutto sulla falsariga dei sistemi per la risoluzione dei nomi simbolici in Internet (DNS - Domain Name Server). I sistemi informativi, detti "EPC Information Services" o EPCIS sono accessibili via Internet con servizi di rete per autorizzazione e sicurezza.

Nel dicembre 2004, EPCglobal ha emesso uno standard lungamente atteso per TAG operanti nelle banda UHF media, che promette la diffusione massiva di TAG passivi a basso costo ed alte prestazioni. Si tratta dei cosiddetti Class 1 Generation 2 (EPC Gen2) RFID. Lo standard copre i protocolli di comunicazione per l'interfaccia a radio frequenza e sta stimolando lo sviluppo di nuove applicazioni.

Il nuovo standard EPC Gen2, recentemente recepito dall'ISO (ISO/IEC 18000-6 Type C), è destinato a superare le preoccupazioni dell'utenza connesse ai diversi standard relativi a TAG per veicolare identificativi EPC ed operanti nelle bande UHF. Si posiziona tra gli standard con carico lieve di diritti per brevetti (è comunque necessario, per ottenere la conformità allo standard di associarsi ad EPCGlobal).



## VI.1.5 STANDARD EPCGLOBAL E LORO EVOLUZIONE

| Classe          | Standard   | Frequenza<br>—<br>Alimentazione<br>—<br>Memoria                                     | Descrizione – Applicazioni   |
|-----------------|--|---|--|
| Class 0<br>Gen1 | 900 MHz Class 0<br>Radio Frequency (RF) Identification<br>Tag Specification  | UHF<br>—<br>Passivi<br>—<br>Solo lettura (read-only)<br>(scritti in fabbrica)       | Sono i tipi più semplici, ove i dati, generalmente il solo identificatore (EPC), sono scritti durante il processo di produzione e non sono possibili modifiche.<br>La classe 0 definisce anche una categoria di TAG chiamati <b>EAS</b> (Electronic Article Surveillance) oppure antifurto (anti-theft). Questi TAG non hanno identificatore completo ma annunciano solo la loro presenza quando transitano nel campo generato dall'antenna del Rader.<br><i>Applicazioni: Identificazione – Antifurto – vedi Nota.</i>  |
| Class 1<br>Gen1 | 13.56 MHz ISM Band Class 1<br>Radio Frequency (RF) Identification<br>Tag Interface Specification   | HF – UHF<br>—<br>Passivi<br>—   | Sono costruiti senza dati scritti in memoria. I dati possono essere scritti una sola volta dall'utente o in fabbrica, successivamente è possibile la sola lettura.<br>Questo tipo di TAG viene principalmente usato come semplici identificatori.<br>Stanno andando in disuso a favore della Gen 2.<br><i>Applicazioni: Identificazione.</i>   |
|                 | 860MHz -- 930 MHz Class 1<br>Radio Frequency (RF) Identification<br>Tag Radio Frequency & Logical<br>Communication Interface Specification | Scrivibili una sola volta<br>– WORM –<br>(write-once, read-many)                    |  |
| Class 1<br>Gen2 | EPCglobal Tag Data Standards<br>Version 1.3  | UHF<br>—  | Comunicano a 860 MHz-960MHz.<br>Di uso globale, comprendono la classe 0, la classe 1 e caratteristiche di ISO/IEC 18000-6.<br><i>Applicazioni: Identificazione.</i>  |
|                 | Class 1 Generation 2 UHF Air Interface<br>Protocol Standard Version 1.0.9  | Passivi<br>—  |  |
|                 | Class-1 Generation-2 UHF RFID<br>Conformance Requirements<br>Specification v. 1.0.2  | Scrivibili una sola volta<br>– WORM –<br>(write-once, read-many)                    |  |
| Class 2         | EPCglobal<br>Hardware Action Group (HAG)<br><br><i>Proposta di Standard</i>  | UHF<br>—<br>Passivi<br>Semi- Passivi<br>Attivi<br>—<br>Riscrivibili<br>(read-write) | Aggiunge caratteristiche addizionali ai Gen 2 in UHF (encryption, read locking, recycle features, sensor support and structured user memory).<br>Dovrebbe introdurre algoritmi di autenticazione e crittografia simili a quelli usati nelle carte senza contatto.<br>Almeno una parte della memoria del TAG è del tipo riscrivibile.<br>È la classe di TAG usata quando l'utente necessita di scrivere "on line" i dati nella memoria del TAG tramite la procedura di interrogazione del Reader. Questo consente di tenere traccia della "storia" della merce (Data logger).<br>Contiene più memoria dei tag delle classi precedenti in quanto, in generale la parte read/write della memoria si affianca alla sezione non volatile EEPROM che continua a contenere l'identificativo o l'EPC.<br><i>Applicazioni: Data loggin.</i> |

**Tabella VI.1**  
Classi di TAG come definite da EPC sulla base  
della memoria del dispositivo e delle capacità  
di trasmissione

Vengono comunemente considerate altre tre classi di TAG, entrambe relative ad apparati attivi o semi-passivi:

- Classe 3 - READ/WRITE - TAG semi-passivi - con sensori a bordo - Applicazioni: Data loggin

Questa classe, in aggiunta alle prestazioni della classe precedente, contiene, a bordo sensori e logica di controllo dei medesimi. I sensori più diffusi sono relativi alla pressione, moto o temperatura (i più diffusi in assoluto, per le esigenze logistiche della "catena del freddo"). Se la logica di controllo dei sensori lo permette, questi possono essere letti e

registrati in memoria anche senza l'intervento del Reader che, quando interrogherà il TAG si vedrà restituita anche la storia delle grandezze misurate. Naturalmente la complessità circuitale ed il relativo consumo di energia richiedono TAG attivi o almeno semi-passivi.

- Classe 4 - READ/WRITE - con trasmettente a bordo - Network Capabilities - Applicazioni: Ad-Hoc Network; Active wireless sensor network

Questa classe di TAG, con trasmettitore a bordo, si comporta come un sistema dotato di logica autonoma, potendo comunicare da TAG a TAG senza la presenza del Reader. In questi casi non solo si è in presenza di TAG attivi, ma l'attività, e di conseguenza l'erogazione di energia dalla batteria, permane anche in assenza di interrogazioni da parte del Reader.

Per il resto sono previste tutte le prestazioni della classe 3.

- Classe 5 - READ/WRITE - con trasmettente a bordo - Network Capabilities.

Oltre alle caratteristiche della classe 4 si ipotizza la possibilità di colloquio con TAG passivi, con funzionalità del tipo di quelle degli NFC (cfr. §V.5).

Nota bene: i sistemi EAS (Electronic Article Surveillance: sistemi elettronici di sorveglianza dell'articolo, antitaccheggio) rappresentano i sistemi più semplici. Questi sistemi verificano e controllano la presenza possibile di un TAG nella zona di interrogazione del lettore usando un semplice risonatore LC accordato ad una fissata frequenza, possono quindi essere realizzati praticamente senza chip.

Sono detti anche 1-bit Tags nel senso che possono restituire solo una informazione binaria (il TAG è/non è nella zona di copertura del Reader).

Molto diffusi nei punti vendita al minuto, necessitano della rimozione fisica dall'oggetto al quale sono associati prima che il cliente che lo ha acquistato transiti attraverso il portale con le antenne del Reader, generalmente posto all'uscita del punto vendita.

## VI.1.6 LA NORMATIVA GLOBALE ISO/IEC 18000

| Standard ISO/IEC 18000: RFID for item Management – Air Interface |  |
|--|--|
| 18000-1  | <p><b>Part 1 - Reference architecture and definition of parameters to be standardized</b><br/>           Definisce i parametri generali dell'interfaccia radio e fornisce una descrizione dell'architettura nella quale questi parametri vanno utilizzati.</p>   |
| 18000-2  | <p><b>Part 2 - Parameters for Air Interface Communications below 135 KHz</b><br/>           Definisce i parametri dell'interfaccia radio per dispositivi RFID operanti sotto i 135 KHz utilizzati per l'identificazione di oggetti.<br/>           Definisce i parametri per l'UpLink ed il DownLink, tra i quali: la frequenza operativa, la canalizzazione, le emissioni spurie, la modulazione, il "Duty Cycle", la codifica dei dati, il BitRate, l'ordine di trasmissione dei bit.<br/>           Inoltre definisce i protocolli di comunicazione usati nell'interfaccia radio. In particolare:</p> <ul style="list-style-type: none"> <li>≡ Lo strato fisico utilizzato nella comunicazione tra Reader e TAG.</li> <li>≡ Il protocollo ed i comandi.</li> <li>≡ Il metodo anti collisione.</li> </ul> <p>Lo standard specifica due tipi di TAG, type A (FDX) e type B (HDX) che differiscono solo per lo strato fisico, implementando i medesimi protocolli e tecniche anti collisione.</p> <ul style="list-style-type: none"> <li>≡ I TAG FDX sono alimentati in permanenza dal Reader anche durante la trasmissione dal TAG al Reader. Operano a 125 KHz.</li> <li>≡ I TAG HDX sono alimentati dal Reader solo durante l'interrogazione. Operano a 134,2 KHz.</li> </ul>                 |
| 18000-3  | <p><b>Part 3 - Parameters for Air Interface Communications at 13,56 MHz</b><br/>           Definisce lo strato fisico, i metodi anti collisione ed il protocollo per per dispositivi RFID utilizzati per l'identificazione di oggetti, conformemente ad ISO/IEC 18000-1. Si riferisce solo a sistemi operanti a 13,56 MHz.<br/>           Lo standard definisce due modi operativi, orientati all'uso in differenti applicazioni, non interoperabili e non interferenti reciprocamente:</p> <ul style="list-style-type: none"> <li>≡ Modo 1, basato su ISO/IEC 15693 (Vicinity Cards cfr.§4.3 e §25.5) con varianti per l'applicazione dei TAG a singoli oggetti.</li> <li>≡ Modo 2, un'interfaccia ad alta velocità.</li> </ul>   |
| 18000-4  | <p><b>Part 4 - Parameters for Air Interface Communications at 2.45 GHz</b><br/>           Definisce i parametri dell'interfaccia radio per dispositivi RFID operanti a 2,45 GHz in banda ISM (Industrial, Scientific, and Medical) per applicazioni di identificazione di oggetti.<br/>           Definisce i parametri per l'UpLink ed il DownLink, tra i quali: la frequenza operativa, la canalizzazione, la massima emissione di potenza, le emissioni spurie, la modulazione, il "Duty Cycle", la codifica dei dati, il BitRate, l'ordine di trasmissione dei bit e, quando appropriato, i parametri per attuare la tecnica del "frequency hopping".<br/>           Inoltre definisce i protocolli di comunicazione usati nell'interfaccia radio.<br/>           ISO/IEC 18000-4 definisce due modalità operative:</p> <ul style="list-style-type: none"> <li>≡ TAG passivi che operano con il Reader che parla per primo.</li> <li>≡ TAG assistiti da batteria che operano con il TAG che parla per primo.</li> </ul>  |
| 18000-6  | <p><b>Part 6 - Parameters for Air Interface Communications at 860 – 960 MHz</b><br/>           Definisce i parametri dell'interfaccia radio per dispositivi RFID operanti a 860 MHz e 960 MHz, in banda ISM (Industrial, Scientific, and Medical) per applicazioni di identificazione di oggetti.<br/>           Definisce i parametri per l'UpLink ed il DownLink, tra i quali: la frequenza operativa, la canalizzazione, la massima emissione di potenza, le emissioni spurie, la modulazione, il "Duty Cycle", la codifica dei dati, il BitRate, l'ordine di trasmissione dei bit e, quando appropriato, i parametri per attuare la tecnica del "frequency hopping".<br/>           Inoltre definisce i protocolli di comunicazione usati nell'interfaccia radio.<br/>           ISO/IEC 18000-6 definisce una modalità operativa (con un protocollo comune per la comunicazione TAG=&gt;Reader e con la modalità nella quale il Reader parla per primo), con due tipi:</p> <ul style="list-style-type: none"> <li>≡ Type A che usa il Pulse Interval Encoding (PIE) nel link Reader=&gt;TAG, e l' "adaptive ALOHA" come protocollo anti collisione.</li> <li>≡ Type B che usa il Manchester nel link Reader=&gt;TAG, e l'"adaptive binary tree" come protocollo anti collisione.</li> </ul> |
| 18000-7  | <p><b>Part 7: Parameters for active air interface communications at 433 MHz</b><br/>           Definisce i parametri dell'interfaccia radio per dispositivi RFID con TAG attivi operanti nella banda dei 433 MHz, per applicazioni di identificazione di oggetti.<br/>           Definisce i parametri per l'UpLink ed il DownLink, tra i quali: la frequenza operativa, la canalizzazione, la massima emissione di potenza, le emissioni spurie, la modulazione, il "Duty Cycle", la codifica dei dati, il BitRate, l'ordine di trasmissione dei bit e, quando appropriato, i parametri per attuare la tecnica del "frequency hopping".<br/>           Inoltre definisce i protocolli di comunicazione usati nell'interfaccia radio.</p>  |

**Tabella V.2**  
**Standard ISO/IEC 18000**

Di recente, nel tentativo di porre fine alla competizione tra standard, l'ISO che costituisce in modo indiscusso l'ente mondiale di normativa, ha portato avanti uno standard costituito da più parti (ISO/IEC 18000) che definisce i protocolli di comunicazione per l'interfaccia radio per tutte le applicazioni e tutte le frequenze comunemente usate nel mondo per identificare gli oggetti nella catena di distribuzione e per ogni altra applicazione.

In quest'ottica ISO cerca di incorporare gli standard EPCglobal e, in particolare, ha recentemente incluso le specifiche EPCglobal Gen2, nella serie ISO/IEC 18000 come ISO/IEC 18000-6 Type C.

Nella tabella precedente sono sinteticamente descritte le parti principali di cui si compone ISO/IEC 18000.

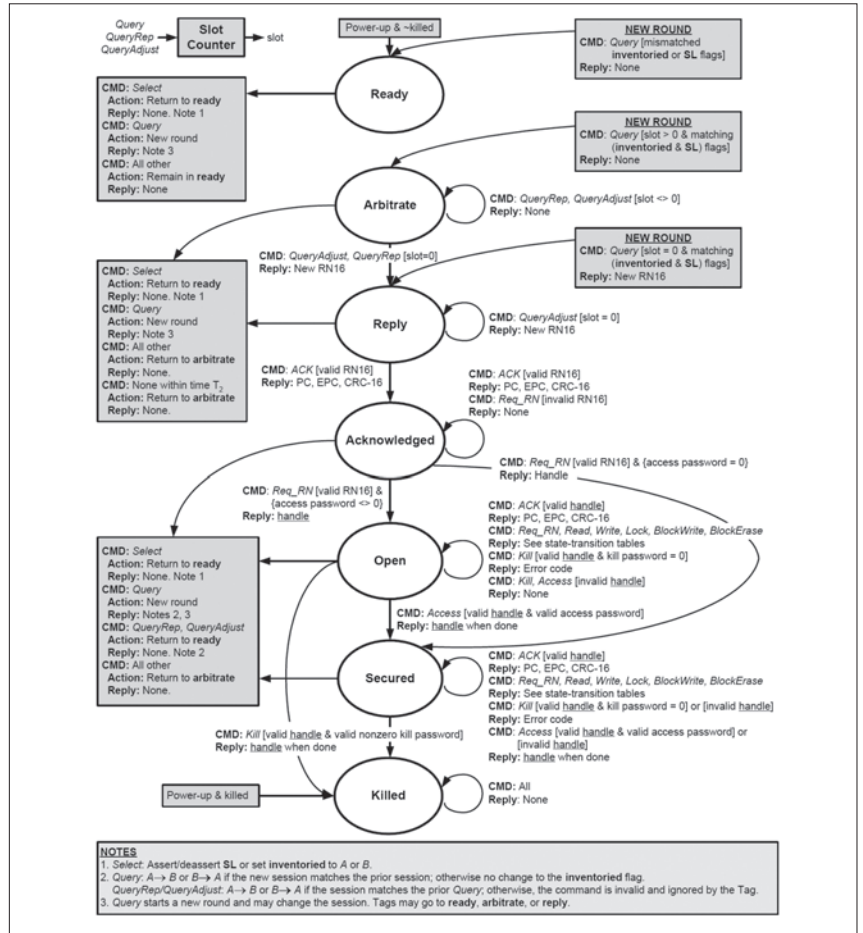
### VI.1.7 I TAG UHF GEN2

Lo standard Gen2 (EPCglobal & ISO/IEC 18000-6) definisce una classe di TAG passivi, operanti in backscatter nelle frequenze 860÷960 MHz ed in modalità HDX (Half Duplex, in cui il Reader parla per primo e continua ad inviare la portante per fornire energia al TAG durante la risposta).

Nelle bande consentite a livello regionale, i sistemi hanno a disposizione 50 canali di 500 kHz a 4 W di potenza negli USA (902÷928 MHz) e 10 canali di 200 kHz a 2 W (più 5 a bassa potenza) in Europa (865÷868 MHz). Da ciò deriva una rilevante diversità di approccio tecnico al problema della possibile presenza di un numero rilevante di Reader nel medesimo ambiente operativo, che si concretizza nell'uso di tecniche di "Frequency Hopping" oppure di "Listen Before Talk" – LBT, nell'interrogazione dei Reader medesimo. Il problema si manifesta quando il TAG, si configura come etichetta intelligente applicata ai singoli oggetti. Sempre in merito a questa strategia, il "Duty Cycle" può variare tra 48% e 82,3% in dipendenza delle tecniche usate (Frequency Hopping opp. LBT).

Lo standard è stato sviluppato per superare le limitazioni delle specifiche precedenti e costituisce la base normativa per una vasta produzione di TAG passivi a basso costo nelle bande UHF. Questo dovrebbe prefigurare una svolta nell'impiego degli RFID nelle applicazioni "open loop" per la logistica ed il commercio, portando l'impiego del TAG a livello dei singoli oggetti.

Figura VI.1  
 Diagramma di stato dei TAG Gen2  
 [EPCglobal]



Gen2 costituisce la prima tecnologia in banda UHF prodotta da tutte le maggiori aziende: Impinj, Philips, Texas Instruments e altri. Anche i produttori di antenne, dispositivi di lettura/scrittura, stampanti/codificatori e computer industriali supportano lo standard Gen2 nelle loro linee di prodotti.

Pur nell'estrema semplicità dell'elettronica associata ad un TAG passivo, un TAG Gen2 riesce a realizzare una macchina a stati finiti abbastanza complessa in cui i comandi ricevuti dal Reader possono provocare, a

seconda dello stato corrente della macchina (TAG), risposte (al Reader) e transizioni di stato (della macchina – TAG) differenti. La complessità della macchina a stati del TAG è dovuta alla necessità di integrare in essa tutte le funzioni del TAG medesimo; dalla generazione di sottoportanti in modulazione, agli algoritmi anti-collisione, alle procedure di sicurezza, ecc. Prevedere un'idea della macchina a stati di un TAG Gen2 viene riportata la Figura V.1, tratta dallo standard [EPC Global].

Vengono ora riassunti alcuni aspetti chiave per i quali lo standard Gen2 ha identificato soluzioni di maggiore efficienza rispetto alle normative precedenti [29], [30]:

- **Modulazioni & Codifiche**

Lo standard prevede l'impiego da parte del TAG delle modulazioni ASK e PSK (cfr. §IV.2) in modo indifferente (non esistono comandi di selezione ed i Reader devono ricevere entrambi). La PSK è stata inclusa perché massimizza il trasferimento di energia (utile nel verso Reader=>TAG) e presenta migliori caratteristiche di robustezza al rumore (utile nel verso TAG=>Reader). Le codifiche di linea previste sono FM0 o Miller (cfr. §IV.1) con generazione di sottoportante attraverso il parametro M. (cfr. §IV.1.3)

Da parte del Reader possono essere impiegate DSB-ASK opp. SSB-ASK oppure PR-ASK con indice di modulazione del 90% e con codifica di linea PIE.

- **Memoria**

Lo standard prevede una capacità di memoria non troppo dissimile dai TAG di classe 1 (EPCglobal). Da 96 a 512 bit di memoria nel TAG contro i precedenti 64÷96 (comunque sufficienti a contenere l'EPC). L'aspetto più interessante consiste nella segmentazione della memoria per contenere maggiori informazioni rispetto al semplice EPC e nella protezione (per segmenti) della memoria di cui si vedrà in seguito.

- **Bitrate vs. identificazione dei TAG**

In genere si riconosce ai TAG Gen2 una velocità superiore alle generazioni precedenti. I bitrate ammessi sono Reader =>TAG 26,7÷128 kbit/s; TAG=>Reader 5÷640 kbit/s. I bitrate vengono gestiti dal Reader nel momento in cui il TAG viene letto/scritto per ottimizzare la

velocità di riconoscimento di TAG con l'affidabilità di trasmissione. Infatti con bitrate alti si aumenta la velocità dell'algoritmo anticollisione, accelerando il riconoscimento dei TAG. Con bitrate bassi si favorisce la robustezza del segnale verso il rumore. Nel verso TAG=>Reader vengono usati 40÷640 kbit/s con codifica FM0 e 5÷320 kbit/s con codifica Miller.

La velocità di lettura è funzione di diverse variabili che comprendono la potenza d'uscita, la densità dei TAG e l'ambiente operativo a radiofrequenza.

Le specifiche Gen2 dovrebbero consentire ai Reader di effettuare, con circa 250 TAG nel raggio di copertura, circa 1500 letture di TAG al secondo in Nord America, e 600 letture per secondo in Europa, dove la potenza irradiata, la banda e il "Duty Cycle" hanno limiti più stretti. Queste velocità di lettura supportano la capacità di identificare oggetti su nastri trasportatori in movimento o trasportati da carrelli elevatori in transito attraverso portali di lettura con velocità anche superiori ai 10 Km/h.

- **Efficienza spettrale**

Vengono definiti tre modi operativi per i sistemi RFID: Reader singolo, Reader multipli, Reader multipli ad elevata densità.

Le specifiche per i Reader che operano in ciascuno di tali ambienti sono state concepite per fornire prestazioni maggiori rispetto a quelli esistenti.

I TAG Gen2 possono essere letti e scritti da Reader di ognuna delle categorie precedentemente elencate.

La modalità operativa di Reader multipli ad elevata densità è la scelta più affidabile ma di maggior complessità; consente un uso efficiente della banda, ottimizza le prestazioni e protegge dalle interferenze.

- **Affidabilità**

Sono previsti miglioramenti essenziali rispetto ai precedenti. Le nuove caratteristiche mirano all'eliminazione di falsi positivi in lettura e in generale all'ottenimento di maggiore affidabilità nella lettura medesima. Vi è anche la possibilità di introdurre meccanismi per incrementare le prestazioni in termini di integrità dei dati. Ad esempio è possibile

la verifica, dopo scrittura, dei dati in memoria del TAG (opzionale da parte del Reader).

- **Raggio di copertura**

Lo standard Gen2 consente ma non obbliga l'uso di tecniche di Frequency Hopping prevedendo canali di 500 kHz nella banda assegnata negli USA (da 902,5 a 927,5 MHz).

Tecniche alternative (Listen Before Talk – LBT) in uso in Europa possono prevedere un “Duty Cycle” più breve e operare con meno potenza, il che può comportare maggiore lentezza di lettura e un raggio di copertura ridotto.

Bisogna comunque ricordare che il massimo raggio di copertura è principalmente funzione della potenza irradiata. Poiché i limiti per tale potenza sono differenti per gli USA, l'Europa e il Giappone, ci si dovrà aspettare valori differenti tra queste aree (in particolare i valori massimi in USA sono maggiori rispetto a quelli in Europa e Giappone).

- **Sicurezza**

I TAG conformi allo standard Gen2 sono protetti da manomissioni. Il cosiddetto “cloaking”, infatti, consente di configurare i TAG in modo tale che prima di rispondere a qualunque interrogazione necessitano di ricevere una password dal Reader. Password possono essere anche richieste per scrivere i TAG o disabilitarli.

Altro requisito di sicurezza supportato dallo standard e particolarmente richiesto è la possibilità di disabilitare definitivamente (“killing”) i TAG in modo tale che i loro dati non possano più essere accessibili. Questo è un requisito essenziale nell'ambito della vendita al dettaglio al fine di dissipare i timori dei consumatori riguardo la loro privacy.

Sono definite password separate (a 32 bit) per il killing, per il cloaking, o per accedere alle diverse sezioni della memoria dei TAG. Maggiori dettagli sono stati illustrati in §VIII.5.4.

Esistono, nell'ambito dello standard, differenti possibilità per realizzare le caratteristiche di sicurezza addizionali, pertanto si può determinare una forte differenziazione tra i prodotti conformi allo standard Gen2.

- **Gestione dei TAG**

Il Reader gestisce la popolazione dei TAG nel proprio raggio di coper-



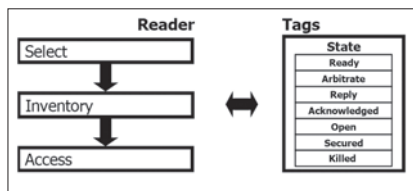


Figura VI.2  
Azioni del Reader sui TAG e stati dei TAG  
[EPCglobal]

tura mediante 3 operazioni fondamentali, che comprendono uno o più comandi:

- *Selezione (Select)*; è il processo con il quale il Reader, sulla base di criteri da lui stabiliti, seleziona gruppi o singoli TAG nella popolazione. La selezione (che non implica risposte da parte dei TAG) avviene allo scopo di operare le successive operazioni di inventario.
  - *Inventario (Inventory)*; è il processo con il quale il Reader identifica i TAG precedentemente selezionati. L'inventariazione avviene con protocollo anticollisione e, in una prima fase, in modo anonimo (con l'uso di RN16 come pseudonimo o "Tag's handle"). Successivamente (cfr.§VIII.5.4) il TAG invia l'identificativo o l'EPC.
  - *Accesso (access)*; è il processo di accesso alla memoria del TAG per operazioni di lettura e scrittura. Viene operato con le misure di sicurezza previste. In questa fase si ottengono l'identificativo, l'EPC o gli altri dati in memoria del TAG. Un particolare tipo di accesso è la disabilitazione definitiva del TAG ("killing").
- **Gestione del protocollo anticollisione (cfr.§IV.3.2.2)**  
Nel protocollo slotted ALOHA impiegato per l'anticollisione, la lunghezza complessiva della trama, ovvero il numero degli slot tra i quali il TAG sceglie di rispondere con algoritmo casuale, viene determinato di volta in volta dal Reader (con il parametro Q, trasmesso ai TAG) sulla base delle condizioni al contorno.
  - **Costi**  
Una delle maggiori spinte che hanno guidato lo sviluppo dello standard Gen2 è stato quello di avere a disposizione una tecnologia RFID con costi tali da poter essere introdotta convenientemente nelle operazioni previste nelle catene di distribuzione. Lo standard Gen2 raggiunge un compromesso tra costo e funzionalità supportate che dovrebbero condurre alla produzione di prodotti competitivi in termini di prezzo che soddisfano le esigenze di applicazioni massive.
  - **Operatività "anywhere"**  
Nei Gen2 è stato anche curato l'aspetto concernente il possibile funzionamento del TAG a larga banda consentendo la compatibilità dell'interfaccia radio e delle tecniche di modulazione con le limitazioni della

porzione di spettro UHF media assegnata agli RFID nelle varie aree geografiche. I TAG, quindi, devono poter operare tra 860 e 960 MHz. La capacità di operare a larga banda del chip conforme a Gen2, però, non implica necessariamente la piena operatività a larga banda dell'intero TAG. Lo standard, infatti, normalizza l'interfaccia radio ma non le antenne. Nei TAG di dimensioni più contenute e di prevalente impiego regionale, pertanto, è possibile l'uso di antenne ottimizzate per una banda stretta. Queste limitano le prestazioni al di fuori delle frequenze consentite nella regione di appartenenza del TAG.

- **Conformità**

Gen2 costituisce un tipo standard dell'ultima generazione. Come accennato all'inizio del capitolo, per questo tipo di normativa il termine "standard" non è tanto sinonimo di uguaglianza tra prodotti quanto di razionalizzazione della produzione dei prodotti medesimi. Diverse caratteristiche dello standard, infatti, sono opzionali e quindi non sono supportate da tutti. Nei punti descritti in precedenza si sono menzionati casi che determinano considerevole differenziazione di prodotti pur nell'ambito della conformità allo standard Gen 2. La focalizzazione su esigenze reali dell'analisi di tali caratteristiche consentirà di selezionare il prodotto in grado di soddisfare maggiormente le prestazioni richieste dalla particolare applicazione, ma non sempre garantirà l'intercambiabilità, per l'applicazione medesima, di TAG di produttori diversi.

- **Comandi**

Lo standard prevede un insieme di comandi (da Reader a TAG) allo scopo di selezionare le differenti funzioni del TAG. I comandi più comuni sono elencati nella tabella seguente:

Esistono anche comandi "avanzati" quali: block write, truncated reply, multiple simultaneous singulation sessions with persistence, selection filtering flexibility, write protection.

| Comando per selezionare il TAG (Select command o singulation) |   |
|---|---|
| <i>Select</i>   | Seleziona un particolare sottoinsieme della popolazione di TAG raggiungibili dall'interrogazione. L'attribuzione o meno del TAG al sottoinsieme, avviene sulla base di porzioni dell'informazione contenuta nella memoria del TAG (Identificatore, EPC o altri dati).   |
| Comandi per inventariare i TAG (Inventory commands)           |   |
| <i>Query</i>  | Indica le caratteristiche del segnale con il quale il TAG deve rispondere all'interrogazione (ad esempio i parametri per la sottoportante generata dal TAG, i parametri dell'algoritmo anti-collisione ed il gruppo di TAG che devono rispondere, quelli selezionati o non dal comando omonimo oppure tutti). |
| <i>QueryAdjust</i><br><i>QueryRep</i>                         | Consente di cambiare i parametri dell'algoritmo anti-collisione e provoca il conseguente cambio di stato dei TAG senza modificare gli altri parametri della Query.  |
| <i>ACK</i>  | Riscontra il riconoscimento di un TAG, reinviando lo pseudonimo RN16.   |
| <i>NAK</i>  | Opera il "reset" di tutti i TAG riportandoli nello stato iniziale dell'operazione di inventario (Arbitrate), a meno che non siano disabilitati (Killed) o pronti per l'operazione di selezione (Ready).   |
| Comandi per accedere alla memoria del TAG (Access commands)   |   |
| <i>Req_RN</i>   | Chiede al TAG di generare e trasmettere un nuovo RN16 con funzioni di pseudonimo. Opera con password di sicurezza e comporta la transizione nello stato "Secured" se la password non risulta corretta.  |
| <i>Read</i><br><i>Write</i>                                   | Lettura/scrittura della memoria del TAG (o parti di essa). In scrittura si opera in sicurezza (cifrando password e dati con un RN16 in funzione di "cover code").   |
| <i>Kill</i>   | Disabilita in modo definitivo il TAG (non sono più possibili altre transizioni di stato).   |
| <i>Lock</i>   | Blocca la memoria (o parti di essa) inibendo successive operazioni di lettura/scrittura. Opera su base password e può essere successivamente annullato nello stesso modo. Viene eseguito quando il TAG è nello stato "Secured"  |
| <i>Access</i>   | Comando opzionale che consente la transizione diretta nello stato "Secured"   |
| <i>BlockWrite</i><br><i>BlockErase</i>                        | Comandi opzionali che permettono la lettura/scrittura di blocchi di memoria. Questo avviene senza misure di sicurezza, per tale motivo queste procedure sono impiegate in ambienti protetti (stampanti di TAG).   |

**Tabella VI.3**  
Principali comandi dello standard Gen2