CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

30

febbraio 2007

i Quaderni

Linee Guida per l'impiego dei sistemi RFId nella Pubblica Amministrazione

30

febbraio 2007

i Quaderni

sommario

i Quaderni n. 30 febbraio 2007
Supplemento al n. 1/2007
di Innovazione

Registrato al Tribunale di Roma
n. 523/2003
del 15 dicembre 2003

Direttore responsabile
Franco Tallarita

Quaderno a cura di:
Gruppo di lavoro RFId
(rfid@cnipa.it)

Redazione
Centro Nazionale
per l'Informatica nella
Pubblica Amministrazione
Via Isonzo, 21b
00198 Roma
Tel. (39) 06 85264.1
pubblicazioni@cnipa.it

I Quaderni del Cnipa
sono pubblicati all'indirizzo:
www.cnipa.gov.it

Stampa:
Stilgrafica srl - Roma

3 PRESENTAZIONE

7 SINTESI DEI CONTENUTI

11 1. PANORAMICA DEI SISTEMI DI IDENTIFICAZIONE A RADIOFREQUENZA
1.1.1 CONTROLLO DEGLI OGGETTI 12
1.1.2 IDENTIFICAZIONE DEGLI ANIMALI 13
1.1.3 AUTENTICAZIONE CON CARTE DI PROSSIMITÀ 14
1.1.4 CONTROLLO DELLE PERSONE 14
1.1.5 NUOVE APPLICAZIONI 15

17 2. LE TECNOLOGIE RFID
2.1 IL SISTEMA RFID 17
2.1.1 TAG (O TRANSPONDER) 18
2.2 CONFRONTO TRA TAG RFID E CODICI A BARRE 25
2.2.1 LETTORI E ANTENNE 27
2.2.2 ARCHITETTURA ACCENTRATA E DISTRIBUITA 33
2.3 MODALITÀ DI SCELTA DEI TAG 39
2.4 IL MERCATO DEI SISTEMI RFID 41
2.4.1 IL MERCATO DEI LETTORI 41
2.4.2 IL MERCATO DEI TAG RFID 42
2.4.3 LA PREVISIONE DEL PREZZO DEI TAG RFID 45
2.4.4 IL MIDDLEWARE RFID 47
2.5 RFID COME GENERAL PURPOSE TECHNOLOGY 49

53 3. SCENARI APPLICATIVI RFID
3.1 INTRODUZIONE 53
3.2 UN MODELLO DI CLASSIFICAZIONE PER LA PUBBLICA AMMINISTRAZIONE 54
3.2.1 IDENTIFICAZIONE DEGLI ANIMALI 56

3.2.2 Logistica 58
3.2.3 Controllo accessi e presenze 59
3.2.4 Gestione rifiuti 59
3.2.5 Le biblioteche 60
3.2.6 Il progetto BRIDGE della UE 62
3.2.7 Le esperienze estere 63
3.2.8 Identificazione e tracciamento dei documenti cartacei con gestione degli archivi 63
3.2.9 Identificazione cespiti e Asset Management 65
3.2.10 Applicazioni ospedaliere 66
3.3 Conclusioni 69

71 4. Standard e regolamentazione
4.1 Standard 71
4.1.1 Premessa 71
4.1.2 Il valore degli standard 71
4.1.3 I principali standard RFId 72
4.2 Regolamentazione 76

81 5. RFId e privacy
5.1 Premessa 81
5.2 Il problema della Privacy nei progetti pilota 82
5.3 Approcci tecnologici 84
5.4 Gli aspetti normativi 87

91 6. La sicurezza dei sistemi RFId
6.1 Le vulnerabilità 91
6.2 Le minacce 92
6.3 Le contromisure 95
6.3.1 Cifratura 95
6.3.2 Autenticazione 96
6.3.3 Mascheramento dell'identificativo 96
6.3.4 Inibizione dell'etichetta 97
6.3.5 Tecniche per contrastare disservizi intenzionali 97
6.3.6 Sorveglianza e disincentivazione 98
6.3.7 Tabella riassuntiva 98
6.4 I rischi connessi all'uso delle tecnologie RFId 99

102 7. Progettazione e realizzazione di una soluzione RFId: un caso pratico

7.1 Descrizione del Modello utilizzato 102
7.2 Possibili Scenari di applicazione 102
7.2.1 Scenario "scaffale aperto no tecnologia" 103
7.2.2 Scenario "scaffale aperto tecnologia bar-code" 104
7.2.3 Scenario "scaffale aperto tecnologia RFId" 104
7.3 I dati di ingresso al modello 105
7.3.1 I dati generali 105
7.3.2 I dati dell'infrastruttura RFId stimata 107
7.4 I risultati dell'applicazione del modello: Analisi Costi-Benefici 108
7.4.1 Il valore dell'investimento 108
7.4.2 I risultati del modello per la biblioteca 110
7.4.3 I risultati del modello per l'utente 115
7.4.4 I risultati del modello per il livello di servizio 116
7.4.5 Analisi di sensitività 118
7.5 Considerazioni sui benefici dell'introduzione delle tecnologie RFId 119
7.5.1 Considerazioni sui benefici di efficienza 119
7.5.2 Considerazioni sui benefici di efficacia 120

121 8. Risultati sperimentali del Laboratorio Cnipa

8.1 Obiettivi della sperimentazione 121
8.2 Affidabilità della lettura e compatibilità dei Tag in ambienti multistandard 122
8.2.1 Descrizione dell'esperimento 122
8.2.2 Risultati e conclusioni 123
8.3 Lettura di Tag in presenza di materiali interferenti 125
8.3.1 Descrizione dell'esperimento 125
8.3.2 Risultati e conclusioni 127
8.4 Robustezza all'interferenza tra antenne 129
8.4.1 Descrizione dell'esperimento 129
8.4.2 Risultati e conclusioni 131
8.5 Robustezza ai principali attacchi 132
8.5.1 Forzatura della password di kill-command 132
8.5.2 Resistenza fisica alle scariche elettriche 134
8.5.3 Risultati e conclusioni 135
8.6 Considerazioni sui tool di sviluppo 136

137 APPENDICI

APPENDICE 1 - APPROFONDIMENTI TECNICI 139
A.1 INTRODUZIONE 139
A.2 BASSE FREQUENZE: LF E HF 139
CAMPO MAGNETICO E INDUTTANZA 139
MUTUA INDUTTANZA: SCAMBIO DI ENERGIA 141
ZONE DI INTERROGAZIONE 142
ACCOPPIAMENTO E TENSIONE INDOTTA 143
A.3 ALTE FREQUENZE: UHF 144
APPENDICE 2 - CONFORMITÀ ALLE NORMATIVE SANITARIE 147
A.1 INTRODUZIONE 147
A.2 NORMATIVE VIGENTI 148
NORMATIVE EUROPEE 148
RESTRIZIONI DI BASE 149
LIVELLI DI RIFERIMENTO DERIVATI 150
NORMATIVE ITALIANE 152
A.3 CRITERI DI VALUTAZIONE 153
LIVELLO 1: MISURE DIRETTE PER VERIFICARE LA CONFORMITÀ AI LIVELLI DI RIFERIMENTO DERIVATI 153
LIVELLO 2: MISURE E ANALISI PER VERIFICARE LA CONFORMITÀ ALLE RESTRIZIONI DI BASE 153
LIVELLO 3: DOSIMETRIA NUMERICA SU MODELLI ANATOMICI DI CORPO UMANO 154
A.4 ESEMPI DI VALUTAZIONE DELL'ESPOSIZIONE A SISTEMI EAS ED RFID 155
SISTEMA EAS A BASSA FREQUENZA (VARCO) 155
SISTEMA RFID A 860-960 MHZ 158
A.5 OSSERVAZIONI CONCLUSIVE 160
APPENDICE 3 - IL PROVVEDIMENTO DEL GARANTE (9 MARZO 2005) 161
APPENDICE 4 - LE SCHEDE DEI PROGETTI RFID 169
A.1 LE SCHEDE RACCOLTE DALLE ASSOCIAZIONI DI CATEGORIA 169
SCHEDE RELATIVE AD APPLICAZIONI ALIMENTARI 169
SCHEDE RELATIVE AD APPLICAZIONI AZIENDALI 171
SCHEDE RELATIVE AD APPLICAZIONI DOCUMENTALI 171
SCHEDE RELATIVE AD APPLICAZIONI OSPEDALIERE 172
SCHEDE RELATIVE AD APPLICAZIONI GESTIONALI 174
SCHEDE RELATIVE AD APPLICAZIONI VEICOLARI 175
SCHEDE AD APPLICAZIONI E ESPERIENZE ESTERE 176
A.2 ESEMPI DI APPLICAZIONI IN AMBITO INTERNAZIONALE 178
IL SETTORE DELL'ABBIGLIAMENTO 178
NATIONAL GALLERY DI LONDRA 178
CONTROLLO DELLE TRASFUSIONI DI SANGUE 178

179 GLOSSARIO

Presentazione

La sigla RFId è comunemente utilizzata per indicare sistemi e applicazioni che consentono l'identificazione remota di oggetti, animali e persone, sfruttando le tecniche di comunicazione attraverso l'etere mediante onde elettromagnetiche.
Il termine tag è utilizzato per individuare tutte le piccole "etichette", di forma e dimensioni più disparate, da palline, a chiodi, a etichette, a microfibre (che possono essere incorporate in tessuti), a inchiostri (utilizzabili per stampare tag su carta).
Già oggi le etichette RFId sono ampiamente utilizzate nei prodotti di largo consumo per semplificare le attività di immagazzinamento e di vendita, parimenti diffuso è il loro uso per il controllo degli animali mentre in altri settori, che pure possono avvantaggiarsi per l'impiego di queste tecniche, si stanno avviando le prime applicazioni pilota.
Gli esperti concordano nel prevedere nel prossimo futuro un consistente incremento dei sistemi RFId che entreranno a far parte dei più svariati processi: dal controllo degli alimenti alle applicazioni mediche, dalla domotica all'automazione di ufficio, dalla gestione dei ricambi al controllo dei processi aziendali.
Il settore pubblico non può ignorare le opportunità offerte da queste nuove tecnologie ed i fenomeni che accompagneranno la loro diffusione. L'interesse è duplice: valutare la possibilità di accrescere l'efficienza dei propri processi e favorire l'innovazione del Paese con opportune attività di impulso e di regolamentazione.
Per rispondere a tale esigenza, il CNIPA ha deciso di presidiare l'argomento delle tecnologie RFId, anche con la formazione di un gruppo di lavoro che ha affrontato l'argomento dal punto di vista del settore pubblico, valutando lo stato dell'arte delle tecnologie, gli sviluppi ipotizzabili, l'effetto sociale della loro diffusione allargata e le possibili applicazioni per migliorare i processi delle amministrazioni. Al gruppo di lavoro hanno partecipato anche esponenti del mondo accademico ed industriale inoltre, per rendere concreta la valutazione delle tecnologie, sono state condotte diverse prove pratiche, sia presso istituti di ricerca che presso il laboratorio sperimentale del CNIPA.
Questo documento di indirizzo è il frutto delle attività del gruppo di lavoro ed ha l'obiettivo di agevolare le amministrazioni pubbliche nella conoscenza dei nuovi strumenti, delle problematiche tecniche e sociali che li caratterizzano e delle opportunità che il mercato offre al settore pubblico e privato.
Si ringraziano tutti coloro che hanno partecipato al gruppo di lavoro che ha consentito il raggiungimento di questo importante risultato ed in particolare,
Le persone del CNIPA:
Emilio Frezza (coordinatore);
Alessandro Alessandroni;

Gabriele Bocchetta;
Indra Macrì;
Carlo Maria Medaglia;
Daniele Mongiello;
Gianfranco Pontevolpe;
Giovanni Rellini Lerz;
Carla Simonetti;
Stefano Venanzi.

Le Pubbliche Amministrazioni:
Università degli Studi di Roma "Sapienza" - CATTID (Centro per le applicazioni televisive e l'insegnamento a distanza);
Politecnico di Milano – Osservatorio RFId della School of Management;
Università degli Studi "Roma Tre" – Area Telecomunicazioni;
Università di Roma "Tor Vergata - Dipartimento di Informatica Sistemi e Produzione;
Università di Torino - Biblioteca Centrale della Facoltà di Economia e la Biblioteca del dipartimento di Scienze Letterarie e Filologiche;
Regione Veneto – Ulss Vicenza 6;
Il Ministero delle Comunicazioni - Direzione Generale Pianificazione e Gestione dello Spettro Radioelettrico.

Le Associazioni/Federazioni ICT:
AIM; Aitech-Assinform; Assintel.

Un particolare ringraziamento va inoltre a:
Francesco Adamo;
Andrea Ardizzone;
Ugo Biader Ceipidor;
Fabrizio Bianchi;
Giulio Camagni;
Giorgio Crescenzi;
Paolo Cursi;
Laura Franchi;
Roberto Macrì;
Gaetano Marrocco;
Giovanni Miragliotta;
Ubaldo Montanari;
Franco Musiari;
Giuseppe Neri;
Lucio Sartori;
Ornella Salvioni;
Antonio Vellucci.

Ai lavori del gruppo hanno assistito Caterina Flick e Cosimo Comella, rappresentante dell'Ufficio del Garante per la protezione dei dati personali, che si ringrazia per la partecipazione, nel quadro della cooperazione istituzionale sugli argomenti trattati.

Floretta Rolleri
Componente del Collegio Cnipa

Claudio Manganelli
Componente del Collegio Cnipa

Sintesi dei contenuti

Il presente documento fornisce le di linee guida, destinate alle pubbliche amministrazioni, relative alle tecnologie RFId e alla loro adozione in seno alle organizzazioni pubbliche. Concepito per offrire un riferimento completo ed immediato in merito, il documento affronta e definisce cosa e quali siano le diverse tecnologie di identificazione in radiofrequenza, descrivendone in dettaglio gli aspetti prettamente tecnologici e funzionali, per passare poi a presentarne gli scenari applicativi e le principali dimensioni di valutazione di questa tecnologia.
Il documento illustra come le tecnologie RFId, nella loro versatilità applicativa, si prestino a numerosi impieghi nell'ambito delle molteplici attività che le Pubbliche Amministrazioni svolgono sia a livello centrale, sia a livello locale, quali:

- logistica, dal trasporto merci alla gestione delle infrastrutture logistiche;
- controllo degli accessi e delle presenze;
- gestione dei processi di raccolta rifiuti, in ottemperanza alla tariffazione puntuale prevista dal Decreto Ronchi del 1997;
- gestione delle biblioteche, per il migliore controllo del patrimonio librario e delle operazioni di prestito;
- identificazione e tracciamento dei documenti cartacei e la relativa gestione degli archivi;
- asset management, per la gestione dei processi di inventariazione e manutenzione dei cespiti;
- applicazioni ospedaliere, dall'accoppiamento farmaco-paziente al tracciamento degli apparati elettromedicali, dal tracciamento delle protesi sanitarie all'identificazione delle sacche di sangue.
- identificazione degli animali mediante tag RFId sottocutaneo;

Nel presentare i suddetti scenari ed ambiti applicativi, il presente documento approfondisce le specifiche soluzioni RFId che si possono adottare a supporto delle attività operative o amministrative delle Pubbliche Amministrazioni, facendo costante riferimento ad esempi reali di efficace implementazione della tecnologia nel panorama italiano ed internazionale. Proprio al confronto con il contesto internazionale viene dedicata particolare attenzione, per tratteggiare le principali linee di evoluzione degli ambiti applicativi.

Al fine di aiutare nella valutazione strutturata del valore delle tecnologie Rfid nelle organizzazioni pubbliche, il documento presenta uno schema di classificazione dei benefici potenziali, di misura dell'impatto sui processi ed un esempio di valutazione quantitativa dei costi / benefici. Questi contenuti permettono di percepire come, oltre alle aspettative di recupero di efficienza, nella Pubblica Amministrazione si rendano sensibili anche tutti i vantaggi legati ai benefici di efficacia del lavoro svolto e al miglioramento del controllo sul processo e sul servizio offerto ai clienti interni ed esterni.

Infine, un ampio spazio viene dedicato ad esporre, in modo semplice ma rigoroso, le principali problematiche tecniche relative alla tecnologia in sé, al suo stato di sviluppo e consolidamento, sia dal punto di vista prettamente tecnologico, sia da quello normativo. Questi contenuti aiuteranno a percepire come molte questioni che l'RFId ha posto negli ultimi anni siano già state ampiamente affrontate. È questo il caso, ad esempio, del tema legato alla Privacy, a proposito del quale non si sono sinora registrati casi rilevanti di infrazioni delle norme, a fronte di un buon quadro normativo e tecnologico a protezione della raccolta e della diffusione di informazioni sensibili.

Più complessa era, fino a poco tempo fa, la situazione degli standard tecnologici, come quelli relativi alle frequenze di trasmissione, ad esempio con alcune limitazioni sull'impiego delle bande di frequenza UHF. Oggi queste difformità sono in corso di risoluzione ed armonizzazione su scala europea, non costituendo più nei fatti un ostacolo all'implementazione.

In conclusione, il documento mostra come un processo ragionato, coordinato e consapevole di introduzione delle tecnologie RFId nella Pubblica Amministrazione, permetta una maggiore efficacia nell'esercizio di molti processi della Pubblica Amministrazione sia a vantaggio dei cittadini, sia a vantaggio degli stessi operatori delle pubbliche amministrazioni.

Il capitolo 1 introduce l'argomento con una veloce panoramica dei sistemi identificativi a radiofrequenza (RFId). Nel capitolo vengono anche fornite indicazioni relative a nuove applicazioni attualmente allo studio. Questa introduzione può essere utile a chi desideri conoscere l'argomento senza approfondirne gli aspetti tecnici.

Il capitolo 2 descrive le caratteristiche tecnologiche e di mercato dei sistemi RFId. Nel capitolo vengono illustrate le tecniche che contraddistinguono le diverse tipologie di sistemi, con riferimento agli standard, ai vincoli di natura fisica ed alle specificità delle applicazioni. Il capitolo è utile per conoscere l'attuale panorama delle tecnologie e delle applicazioni, nonché le loro possibilità d'impiego nei più svariati settori,

Nel capitolo 3 i sistemi RFId sono trattati considerando i possibili scenari applicativi di interesse per il settore pubblico. Nel capitolo vengono presentati alcuni casi pratici di utilizzo degli RFId nel settore pubblico con l'obiettivo di fornire al lettore spunti e modelli di utilizzo.

Il capitolo 4 riporta i principali standard, *de jure* e *de facto*, su cui si basano i sistemi RFId, con l'obiettivo di agevolare la scelta di soluzioni non proprietarie ed interoperabili.

Il capitolo 5 si focalizza sulle implicazioni sociali che possono derivare dall'utilizzo esteso dei sistemi RFId, soprattutto con riferimento al problema della tutela della *privacy*.

Nel capitolo 6 vengono descritti i problemi di sicurezza che possono riguardare le applicazioni RFId, soprattutto in previsione di un uso esteso di tale tecnologia. Nel capitolo vengono anche descritte le soluzioni (contromisure) che permettono di evitare tali problemi laddove si riscontrino rischi significativi.
Il capitolo 7 costituisce una guida pratica alla predisposizione di una applicazione basata su sistemi RFId. Partendo da un caso concreto, vengono illustrati i passi necessari per inquadrare il problema, definire le diverse opzioni e valutare la convenienza economica con analisi di tipo costi/benefici.
Il capitolo 8 illustra i risultati delle prove di laboratorio che sono state condotte per valutare "sul campo" alcune caratteristiche dei sistemi RFId.
Il documento è completato da alcune appendici a cui il lettore può fare riferimento per approfondire temi specifici.

1. Panoramica dei sistemi di identificazione a radiofrequenza

I sistemi di identificazione a radiofrequenza, comunemente noti come RFId (Radio Frequency IDentification), derivano dalla sintesi di più tecniche:

- l'identificazione di persone, animali ed oggetti mediante associazione con i dati gestiti da sistemi informatici ;
- l'impiego di processori specializzati;
- la trasmissione delle informazioni mediante onde radio.

Per ciascuna di queste tecniche è possibile adoperare più soluzioni, dando luogo a varie tipologie di RFId.
Per quanto concerne l'identificazione, occorre distinguere tra l'identificazione di persone e di altre entità.
Nel primo caso il sistema RFId può essere utilizzato:

- per la gestione dell'identità, ossia per identificare il soggetto al fine di concedere o negare l'accesso a specifici servizi informatici (autenticazione);
- per il riconoscimento certo dei soggetti per finalità di controllo e di polizia.

Si tratta di temi non ancora consolidati che coinvolgono, oltre agli aspetti tecnici, argomenti sociali e di privacy.
L'identificazione di animali ed oggetti comporta meno problemi in termini di *privacy*, ma richiede la definizione di un metodo univoco, possibilmente universale, per l'identificazione dell'entità. Per quanto concerne gli oggetti, è possibile fare ricorso agli stessi standard di identificazione già utilizzati per i codici a barre.
Le funzionalità di un sistema RFId sono influenzate principalmente dalle caratteristiche del processore associato all'elemento da identificare.
Si tratta normalmente di processori di dimensioni limitate e poco costosi. Tuttavia, pur rispettando il vincolo del basso costo, il mercato offre svariati prodotti che partono da processori con limitate capacità di elaborazione (capaci comunque di memorizzare e trasmettere un identificativo) fino a processori dotati di una discreta quantità di memoria (64/128 KB) e capaci di effettuare elaborazioni complesse. I processori meno potenti solitamente sono immessi in vere e proprie etichette (*tag*), gli altri sono invece inseriti, a seconda dell'applicazione, in diversi tipi di supporti (etichette, dischetti, contenitori, tessere, ecc.)[1].

[1] Di sovente il termine *tag* viene usato anche per supporti che non hanno la forma di un'etichetta.

Quando il sistema RFId è impiegato per identificare persone, spesso si utilizza una *smart card*, ossia una tessera "intelligente" che può fungere anche da documento di riconoscimento a vista.
La trasmissione in radiofrequenza offre un'ampia gamma di soluzioni che differiscono per frequenza, potenza del segnale, tecniche di modulazione e protocolli di comunicazione.
Per quanto concerne le frequenze, queste possono essere scelte rispettando il vincolo di non interferenza con altre trasmissioni radio, inoltre evitando valori elevati di potenza trasmissiva che potrebbero anche arrivare (se spinti all'estremo) ad essere dannosi per la salute umana. Per questi motivi le caratteristiche di frequenza e potenza sono regolamentate a livello nazionale sulla base di precisi standard. Le frequenze utilizzate per i sistemi RFId, secondo gli standard internazionali, coprono il campo delle medie frequenze (125/134 KHz), delle alte frequenze (13,56 MHz) e delle altissime frequenze (868/915 MHz). E' inoltre allo studio l'impiego di tecniche, sviluppatesi nel campo militare, basate su brevi impulsi di microonde (*Ultra Wide Band* - 2,4 GHz).
La massima distanza di funzionamento dipende dalla frequenza utilizzata e dalle potenze in gioco. Molte applicazioni utilizzano dispositivi di ricezione alimentati dall'energia trasmessa mediante l'accoppiamento induttivo con il dispositivo trasmittente: con questo tipo di dispositivi le distanze operative variano da pochi centimetri a 3-4 metri.
Nelle applicazioni definite con l'espressione *Near Field Communication* (NFC) la distanza operativa è volutamente di pochi centimetri ed il dispositivo trasmittente, spesso di tipo portatile, può essere alimento con una potenza limitata. E' opportuno sottolineare che NFC copre un insieme di protocolli di trasmissione bidirezionale e che quindi è una tecnologia che, pur comprendendo l'identificazione, va oltre il semplice riconoscimento degli oggetti.
Alcuni dei tag RFId offrono la funzione EAS (Electronic Article Surveillance), aumentando così il loro "valore".
L'utilizzo combinato delle tecnologie appena descritte è alla base di un ampio spettro di soluzioni RFId che diviene di giorno in giorno più ricco per effetto dei nuovi sviluppi tecnologici. Nella tabella seguente vengono schematizzate le principali applicazioni distinguendo tra i settori più consolidati e quelli più innovativi.
Nella tabella sono anche riportati i principali standard di riferimento e le relative frequenze, poiché questi sono spesso citati per qualificare l'applicazione.

1.1.1 CONTROLLO DEGLI OGGETTI

Il mercato attuale presenta una consistente offerta di sistemi RFId per il tracciamento degli oggetti. In molti casi le etichette RFId hanno preso il posto dei codici a barre per la gestione del movimento e dell'immagazzinamento delle merci: queste applicazioni richiedono etichette a basso costo, per cui sono di norma utilizzati sistemi di ricezione passivi (non alimentati) con ridotte capacità di immagazzinamento dei dati. Grazie anche alla diffusione di etichette a basso costo, oggi si assiste al proliferare di applicazioni che sfruttano la possibilità di "riconoscere" un oggetto e di acquisirne informazioni in via elettronica. Alcuni

	Oggetti	Animali	Persone	
			Autenticazione	Controllo
Dispositivo associato all'entità	Etichette adesive, processori inseriti in materiali diversi	Dischetti auricolari, capsule, bolo, tag sottopelle	Smart card	Smart card
Applicazioni tradizionali	Logistica, tariffazione, antitaccheggio, tracciamento oggetti, ...	Controllo degli allevamenti, anagrafe animali domestici	Autenticazione per accedere a servizi IT (es. pagamenti, *e-gov*, ecc.)	Documenti di viaggio (es. passaporti, visti), *Badge* aziendale
Impatto su privacy	Basso[2]	Basso	Medio	Alto
Frequenze utilizzate	134 KHz, 13,56 MHZ, 800 MHz	125/134 KHz	13,56 MHZ	13,56 MHZ
Standard di base[3]	ISO 18000 ISO 15693	ISO 14223/1	ISO 14443 ISO 7816-4	ISO 14443
Standard applicativi	*Electronic Product Code* (EPC)[4]	ISO 11784/11785	PKCS#11 PKCS#15	Standard ICAO
Nuove applicazioni	*Networked* RFId Localizzazione di oggetti		*Near Field Communication* (NFC)	Localizzazione di persone
Nuovi standard	ZigBee, Z-Wave, RuBee	RuBee	ISO 18092 (NFC)	

Tabella 1 - Panoramica delle applicazioni RFId

esempi sono: la gestione di biblioteche, la programmazione di elettrodomestici (ad es. lavatrici) in funzione degli oggetti trattati, l'accesso ad informazioni associate ad opere di interesse culturale, il controllo di merci e documenti per la repressione di frodi, ecc. Generalmente si tratta di applicazioni che non hanno particolari requisiti di sicurezza e che richiedono una distanza operativa compresa tra decine di centimetri e qualche metro.

1.1.2 IDENTIFICAZIONE DEGLI ANIMALI

Un settore di applicazione dei sistemi RFId abbastanza consolidato, riguarda l'identificazione ed il controllo degli animali di allevamento.
In questo campo il dispositivo RFId ha preso il posto delle marche auricolari con cui venivano identificati i bovini ed ovini di allevamento: rispetto al sistema tradizionale, l'etichetta RFId può contenere un numero molto più elevato di informazioni, utili per le verifiche incrociate, che possono essere aggiornate facilmente.
Una ulteriore applicazione, ancora non molto diffusa, riguarda il controllo degli animali domestici mediante l'applicazione di etichette (eventualmente sottopelle) con l'indicazione del proprietario, delle vaccinazioni effettuate, ecc.

[2] L'impatto sulla privacy è basso a condizione che l'oggetto non sia direttamente relazionabile ad un soggetto, come nel caso dei braccialetti elettronici per i detenuti.
[3] Per standard di base si intendono le caratteristiche elettriche ed elettroniche, i protocolli e le specifiche di interfaccia
[4] EPC oggi è uno standard commerciale proprietario

1.1.3 AUTENTICAZIONE CON CARTE DI PROSSIMITÀ

L'autenticazione è il processo con cui un soggetto fornisce ad un sistema informatico un identificativo (ad es. lo user-id) e la prova della liceità del suo utilizzo (ad es. la password). L'autenticazione è un passo fondamentale per accedere a servizi informatici critici, quali quelli finanziari, per tale motivo spesso si utilizzano sistemi di autenticazione basati su carte intelligenti o *smart card*. La *smart card* può inoltre essere utilizzata per funzioni locali, quali la memorizzazione di un importo a scalare (borsellino elettronico) o di informazioni sanitarie.

Le tecniche di autenticazione e di accesso ai servizi in rete mediante *smart card* si sono sviluppate in modo indipendente dal sistema di colloquio tra carta e lettore, per cui oggi le stesse tipologie di processori e di applicazioni sono disponibili sia su carte a contatto che su carte di prossimità o RFId[5]. Nelle applicazioni RFId il colloquio tra la carta ed il lettore è quasi sempre cifrato per evitare intercettazioni o contraffazione dei dati scambiati. Di norma si utilizzano carte passive (non alimentate autonomamente) che devono essere posizionate ad una distanza di pochi centimetri dal lettore.

Applicazioni di questo tipo si stanno diffondendo nel settore dei trasporti (biglietti e abbonamenti elettronici), dei pagamenti (borsellino elettronico) e dei servizi di *e-government*. Tra quest'ultimi si citano le applicazioni della Carta Nazionale dei Servizi (CNS) nella sua versione combinata contatti/radiofrequenza[6].

L'accesso ai servizi in rete previa autenticazione non implica il "riconoscimento certo" dell'utente[7], né la trasmissione dei dati personali, per tale motivo l'impatto sulla privacy è generalmente limitato.

1.1.4 CONTROLLO DELLE PERSONE

Gli strumenti per il controllo delle persone sono, per ovvi motivi, progettati per essere adoperati esclusivamente dagli organismi istituzionalmente preposti a tale attività.

Il controllo viene di norma operato verificando la validità di documenti che il soggetto controllato è tenuto ad esibire quali: carta d'identità, permesso di soggiorno, passaporto, visti, ecc. L'impiego di documenti costituiti da smart card di tipo RFId consente di velocizzare i controlli, occorre però accertare al contempo che il documento appartenga realmente al soggetto che lo esibisce e non sia stato contraffatto: per tale motivo molte applicazioni prevedono che sul documento siano presenti dati biometrici che possano essere verificati in modo automatico.

In ogni nazione si stanno sviluppando soluzioni basate su smart card che mirano a migliorare l'efficienza dei controlli senza ridurre le garanzie individuali. In tale ottica molte nazio-

[5] Nelle carte chiamate "combo" lo stesso processore può scambiare dati sia mediante contatti, sia tramite onde radio

[6] Le specifiche della CNS non fissano la modalità di colloquio tra la carta ed il lettore. Il contratto quadro del CNIPA per la fornitura di CNS alla Pubblica Amministrazione prevede comunque carte in grado di operare sia mediante contatti, sia in modalità RFId.

[7] In molte applicazioni può essere fornito solo il codice necessario per ottenere il servizio (ad es. id. di conto bancario) mantenendo l'anonimato.

ni hanno scelto carte a contatto per evitare i pericoli di intercettazione tipici della trasmissione in radiofrequenza[8].
La tecnica di trasmissione in radiofrequenza è stata invece proposte dall'ICAO[9] per la standardizzazione dei documenti di viaggio verificabili automaticamente (*Machine Readable Travel Documents*). Questa proposta, che prevede alcune opzioni di sicurezza per tutelare la privacy, è stata successivamente adottata dall'Unione Europea come standard per il passaporto elettronico.

1.1.5 NUOVE APPLICAZIONI

Le applicazioni descritte non sono ancora pienamente consolidate, ma già si sta pensando a nuovi impieghi della tecnologia RFId.
In particolare, per quanto concerne il controllo degli oggetti, sono allo studio applicazioni relative alla sensoristica distribuita ed alla geo-localizzazione.
In relazione al primo aspetto, si prospettano etichette RFId in grado di misurare e trasmettere dati ambientali come la temperatura, si prevede inoltre che questi sensori "mobili" possano essere collegati stabilmente in rete realizzando veri e propri sistemi di controllo e regolazione di ambienti complessi (*Networked* RFId o NRFID).
Lo standard di collegamento in rete più promettente è lo **ZigBee**, sviluppato da un consorzio di industrie per impieghi in cui è necessario un basso consumo elettrico.
Per quanto concerne le applicazioni, si citano i lavori del consorzio "**Z-wave** alliance" che sta sviluppando standard e prodotti per il controllo degli apparecchi elettrici ed elettronici interni ad un appartamento o ad uno stabile. La peculiarità di questo standard è la possibilità di utilizzare i sensori come "ponte" verso altri sensori, riuscendo così ad aggirare possibili ostacoli che impediscono l'utilizzo delle tradizionali applicazioni *wireless*.
Nel campo degli standard emergenti è opportuno inoltre citare il protocollo denominato **RuBee** (IEEE 1902.1) che è basato sull'impiego di basse frequenze (132 kHz - 450 kHz). L'utilizzo delle basse frequenze comporta una limitata velocità di trasmissione dati (circa 1200 bit/s), ma per contro migliora le capacità trasmissive in situazioni critiche, come nei casi in cui l'etichetta si trova vicina a materiali conduttori o in casi di elevata numerosità e densità dei sensori. Questo standard appare dunque promettente per applicazioni che non richiedono la trasmissione di elevate quantità di dati, ma devono operare in ambienti che possono presentare problemi per i tradizionali sensori RFId.
Una diversa evoluzione dei sistemi RFId, riguarda la possibilità di trasmettere grandissime quantità di dati con l'impiego dell'*Ultra Wide Band* (2,4 GHz).
L'utilizzo di bande elevate facilita inoltre l'impiego delle tecniche di localizzazione, consentendo di realizzare applicazioni in grado non solo di ricevere informazioni dai dispositivo associati agli oggetti, ma anche di calcolare la loro posizione geografica.

[8] In Italia sono attivi i progetti per la Carta d'Identità Elettronica (CIE) ed il permesso di soggiorno elettronico che non utilizzano tecnologie RFId
[9] I documenti tecnici dell'ICAO, l'organizzazione internazionale per l'aviazione civile, spesso danno origine a norme internazionali

L'esigenza di proporre al pubblico apparati in grado di operare in modo estremamente semplice ha portato allo sviluppo della tecnologia definita *Near Field Communication* (**NFC**). Il nome deriva dalla caratteristica del protocollo che attiva la comunicazione tra due dispositivi solo quando questi si trovano sufficientemente vicini (ad una distanza di pochi centimetri o a contatto).
Questa tecnologia è adatta per qualunque tipo di applicazione RFId in cui non sia necessario operare a distanza (ad esempio per la lettura di informazioni presenti su un'etichetta RFId di un articolo in vendita), tuttavia le applicazioni più promettenti sono quelle in cui il sistema trasmittente è presente su un apparecchio telefonico di tipo mobile: infatti, con questa soluzione, il cellulare può diventare uno strumento per accedere ad informazioni di oggetti "etichettati" o per effettuare operazioni di pagamento.
Quest'ultima possibilità rende il sistema NFC un possibile mezzo, alternativo alla smart card, per l'autenticazione e l'accesso ai servizi.
Più in generale, la combinazione delle tecniche di trasmissione in radio frequenza e dei sistemi di identificazione/autenticazione consente oggi più schemi di funzionamento. Nella fattispecie il dispositivo *client* può essere costituito da:

- *smart card* formato tessera senza contatti, alimentata dal lettore mediante accoppiamento induttivo, che colloquia con il *server* per il tramite del lettore RFId;
- *smart card* con contatti alloggiata nel telefono mobile[10] che colloquia con il *server* via rete mobile (ad es. con protocollo GPRS o UMTS);
- telefono mobile NFC[11] che colloquia con il *server* per il tramite di un secondo dispositivo NFC.

Molto è stato detto, soprattutto dalla stampa, relativamente all'impiego di nuove tecnologie RFId per il controllo delle persone. E' infatti possibile, in teoria, adoperare le tecniche di geo-localizzazione anche per controllare gli spostamenti di persone, utilizzando eventualmente ricevitori RFId sottocutanei.
Questo tipo di applicazione ha naturalmente delle implicazioni di carattere etico e sociale che rendono marginale l'aspetto tecnico[12].

[10] In questo caso la *smart card* potrebbe contenere anche il modulo identificativo dell'abbonato (SIM)
[11] Di solito, anche in questo caso, le informazioni personali sono comunque memorizzate in una *smart card* inserita nel telefono
[12] Tali implicazioni sussistono anche nei casi in cui, per controllare la presenza di persone, si utilizzano sensori presenti su oggetti associati alla persona stessa come, ad esempio, braccialetti elettronici.

2. Le tecnologie RFId

L'RFId non è una singola tecnologia, ma è costituita da un vasto insieme di tecnologie, tra loro molto diverse.
Questa eterogeneità è dovuta a fattori strutturali nonché a fattori legati alle specificità del campo applicativo, molto vasto e diversificato. Primariamente, le diversità dipendono dalla frequenza di funzionamento e dal tipo di alimentazione dei tag.
Come già accennato nel capitolo precedente, la trasmissione in radiofrquenza è regolamentata a livello nazionale sulla base di precisi standard. Le frequenze utilizzate per i sistemi RFId, classificate in accordo agli standard internazionali, coprono il campo delle medie frequenze (125/134 KHz), delle alte frequenze (13,56 MHz) e delle altissime frequenze (868/915 MHz).
Sono, proprio la frequenza di utilizzo, la potenza e, di conseguenza, la distanza di funzionamento a determinare i campi applicativi della tecnologia RFId.

2.1 Il Sistema RFId

Un sistema RFId è costituito di tre componenti principali:

- il tag anche definito con il termine transponder;
- il lettore definito anche con il termine transceiver;
- l'infrastruttura software.

Il transponder viene applicato all'oggetto da identificare, memorizza tipicamente un identificativo univoco e opzionalmente ulteriori dati e rappresenta, quindi, il supporto dati primario del sistema. Un transponder può essere considerato come un supporto passivo che viene letto a distanza, senza presentare nessuna capacità di elaborazione propria.
Il lettore è il dispositivo che estrae informazioni dal tag, grazie alla propria antenna, permette la comunicazione con il transponder tramite onde a radiofrequenza, e consente di effettuare operazioni di lettura e, eventualmente, di scrittura.

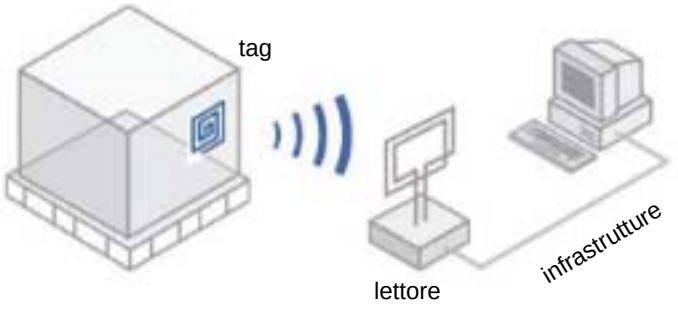

Figura 1 - Sistema RFId

L'infrastruttura software (ad esempio, un singolo PC o un sistema host) filtra i dati letti, rendendoli disponibili per il sistema informativo aziendale.
Il processo di lettura è principalmente legato all'identificazione dei dati di un preciso insieme di asset. I dati relativi all'asset riportati sul tag vengono "recuperati" mediante l'antenna e il lettore, e raccolti da un sistema di gestione delle informazioni.

2.1.1 TAG (O TRANSPONDER)

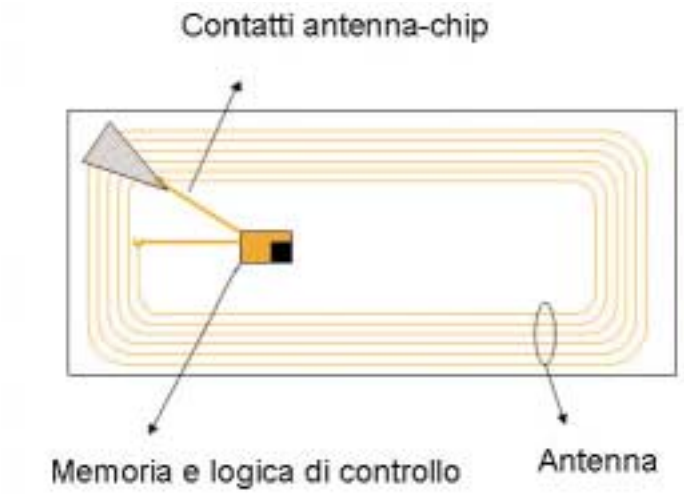

Figura 2 - Esempio di Tag RFId HF con accoppiamento induttivo

Ogni oggetto che deve essere identificato in un sistema RFId, deve essere dotato di un tag.
I tag vengono realizzati con forme diverse a seconda del tipo di oggetto su cui dovranno essere applicati e sulla base delle condizioni ambientali in cui dovranno essere utilizzati. Esiste, infatti, una vasta gamma di tag che si differenziano tra loro per dimensioni, capacità di memoria, resistenza alle temperature e molte altre caratteristiche. Al contrario, quasi tutti i tag sono accomunati dal fatto di essere incapsulati al fine di garantirne l'efficienza ed assicurarne la resistenza agli urti, alla polvere, agli agenti chimici e all'umidità.
Tra i vari tipi di tag che si differenziano dal punto di vista morfologico ci sono quelli flessibili con forma analoga a una carta di credito, quelli con forma di disco e moneta, i tag dedicati (modellati in supporti di plastica usati da contenitori), i tag a forma di chiave, i tag progettati su misura per contenitori e pallet, i tag di carta, e vari altri tipi di tag realizzati a seconda delle esigenze del prodotto su cui devono essere applicati.
I tag risultano immuni alla maggior parte dei fattori ambientali, ma i range di lettura e scrittura possono risentire in modo determinante della vicinanza di metalli, di liquidi o di radiazioni elettromagnetiche che interferiscono con i fenomeni di propagazione radio, disturbando o al limite inibendo le comunicazioni tra gli elementi del sistema. Per queste ragioni è importante progettare e realizzare singolarmente ogni installazione, poiché sistemi ben progettati e installati sono in grado di sopperire a tali difetti.

Figura 3 - Tipologia di Tag

La vera sfida dei prossimi anni sarà quella di portare gli economici tag, passivi e miniaturizzati, ad avere le stesse caratteristiche di range di lettura e di velocità di riconoscimento oggi possedute da elementi di dimensioni considerevoli o addirittura con batteria di alimentazione.
Il range di lettura varia considerevolmente per i vari tipi di tag. In generale ad un range più ampio corrisponde un costo più elevato del tag.
Tag con distanze di lettura limitate a pochi mm possono essere inclusi in documenti cartacei e biglietti per una rapida autenticazione e per un veloce ordinamento.
Tag con range di alcuni metri, capaci di essere letti insieme con altri (risolvendo le cosiddette collisioni) ed anche velocemente sono indicati per la logistica. Altri per la gestione di depositi e per esazione di pedaggi devono arrivare a distanze di decine e centinaia di metri.

Ogni transponder è dotato di un proprio codice identificativo univoco fornito dal produttore. Tale codice non è suscettibile di modifiche e non può essere cancellato o copiato. Ciò fa sì che ciascun transponder sia univocamente identificabile rendendo impossibile ogni tipo di contraffazione. Esiste un ulteriore codice identificativo progressivo che viene attribuito al transponder al momento della prima inizializzazione e assegnazione da parte dell'azienda proprietaria del bene. Un aspetto molto interessante che si presenta, in particolare nelle architetture distribuite è il fatto che i dati del sistema siano contenuti nei tag RFId, che sono fisicamente uniti e pertanto sono collegati e si muovono con essi.

Caratteristiche fisiche dei tag

I formati principali dei tag sono le label (etichette) e le PCB (Printed Circuit Boards, schede a circuito stampato).
Le label sono caratterizzate dalla presenza di una bobina (o un dipolo per frequenze UHF) a radiofrequenza stampata punzonata, impressa o depositata su un substrato di carta o di

poliestere con un chip di memoria. Una label è meno resistente alle condizioni ambientali rispetto a un tag incapsulato, ma risulta più vantaggiosa in termini di costo in ambiti applicativi in cui non sia previsto il riutilizzo del transponder. In quest'ultimo caso la label viene applicata sul prodotto e spedita attraverso tutta la Supply Chain ma non può essere riutilizzata poiché l'oggetto al momento dell'acquisto da parte del cliente, scompare dalla Supply Chain. In alternativa, i tag sono riusabili, per esempio in applicazioni per il tracciamento dei pallet. Per i bassi costi che comporta, una soluzione basata su label risulta estremamente interessante per applicazioni in cui si ha a che fare con alti volumi.

Le PCB sono destinate ad essere costruite appositamente per essere "incorporate" nei prodotti, ma pur presentando ottime caratteristiche di resistenza alle alte temperature, richiedono di essere incapsulate se si usano in condizioni ambientali sfavorevoli come, ad esempio, pioggia o elevata umidità. Una PCB, quindi, presenta soprattutto una grande vantaggio, della robustezza in ambienti in cui una semplice label non sarebbe in grado di sopravvivere.

Un esempio di utilizzo delle PCB è quello della produzione di pallet di plastica. La PCB viene inserita nel pallet di plastica prima della fase di saldatura ultrasonica del ciclo di produzione dello stesso pallet. In questo modo il pallet diventa uno "smart pallet" e i dati possono essere scritti e letti sul pallet attraverso tutta la Supply Chain.

Un tag generalmente si compone, di un chip, di un'antenna e di un supporto fisico. Il chip è il componente elettronico che svolge il compito di gestire la logica di comunicazione e identificazione ed inoltre ha il compito di aumentare la capacità di memorizzazione del transponder. L'antenna è l'apparato che consente al tag di essere alimentato (qualora non sia equipaggiato con una batteria), di ricevere ed, eventualmente, trasmettere informazioni da e per il mondo esterno. Il supporto fisico consiste nel materiale che sostiene e protegge il sistema composto dal tag e dall'antenna.

Il chip dei tag RFId è progettato e realizzato utilizzando alcuni tra i processi più avanzati disponibili, che consentono l'applicazione delle geometrie di silicio più piccole. Il risultato è impressionante, basti pensare che le dimensioni di un chip UHF sono circa pari a 0,5 millimetri quadrati.

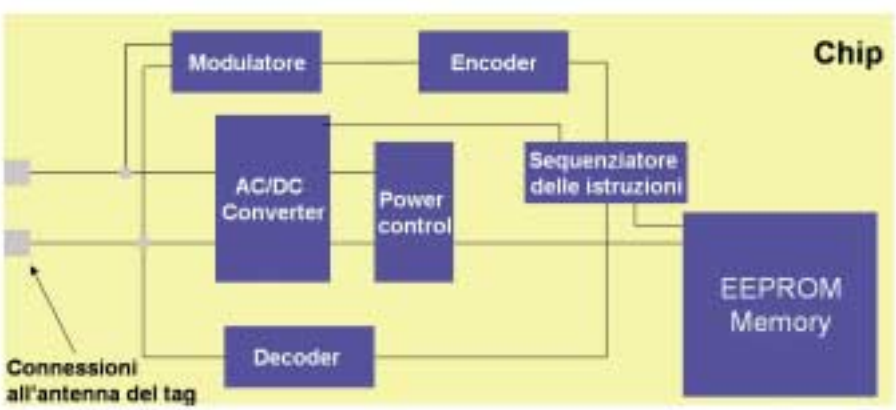

Figura 4 - Struttura di un chip

I tag sono realizzati in tecnologia CMOS e la maggior parte di essi contiene una porzione di memoria non volatile (NVM, Non Volatile Memory), come le EEPROM, al fine di immagazzinare i dati.
La capacità della memoria dipende dalle specifiche del chip e può variare dai 64 bit (Unique IDentification) di un semplice numero identificativo, fino ad alcune decine di kbit. L'aumento della memoria produce un aumento delle dimensioni fisiche del chip e un maggiore costo del prodotto.
Il processo di assemblaggio del tag è una fase molto importante del ciclo di vita e si articola, allo stato attuale della tecnologia, in quattro fasi distinte:

- scelta materiale di substrato che si ritiene più adatto allo scopo (carta, PVC, ecc...)
- posizionamento sul materiale di substrato dell'antenna realizzata con uno dei materiali conduttivi, come ad esempio inchiostro d'argento, d'alluminio e di rame.
- realizzazione del collegamento del chip del tag con l'antenna.
- applicazione di un sottile strato protettivo (di materiale PVC, resina epossidica o carta adesiva) per fare in modo che il tag possa resistere anche in circostanze fisiche non ideali che spesso si verificano durante l'utilizzo, come l'abrasione, gli urti e la corrosione.

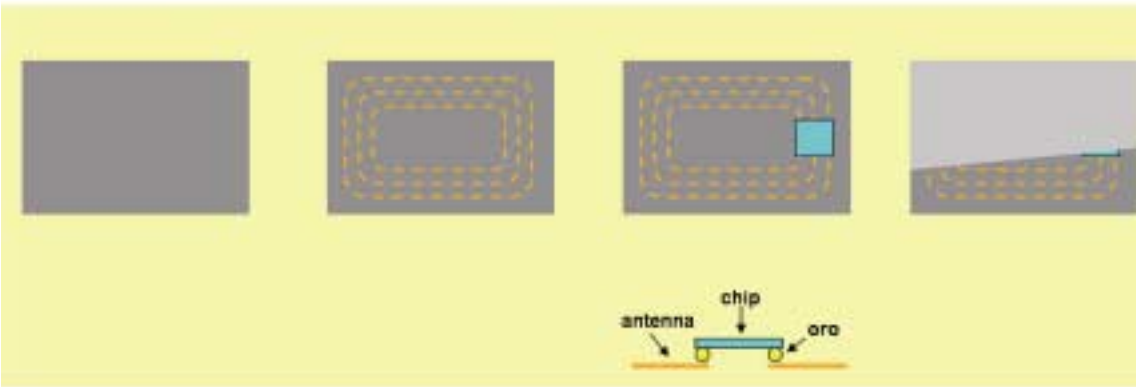

Figura 5 - Le 4 fasi di assemblaggio di un tag RFId

Nelle situazioni in cui sia richiesto un livello di sicurezza piuttosto alto o l'integrità dei dati scambiati, questi ultimi al momento della trasmissione possono essere crittografati. In entrambi i casi, il chip esegue, in modo opportuno, la modulazione del segnale ricevuto per poi inviarlo al lettore, che opera una conversione dei dati, decifrandoli e verificandone l'autenticità..
I "chipless tag" possono essere stampati con inchiostri speciali o costituiti da sottili fibre metalliche, che vengono incorporate nelle fibre della carta, capaci di riflettere le onde elettromagnetiche verso il lettore, entrando in risonanza a determinate frequenze ("resonant signature"). Uno dei problemi è però quello delle difficoltà di miniaturizzazione, dovuto alla "sbavatura" degli inchiostri polimerici (polythiophene) per substrati plastici.

Modalità di alimentazione dei Tag

Ponendo l'attenzione alle modalità di alimentazione elettrica e di trasmissione rispetto al lettore, è possibile distinguere i tag in passivi, semiattivi e attivi.

TAG PASSIVI

Questo tipo di transponder viene utilizzato tipicamente per le applicazioni di massa come mezzi di trasporto a bassa velocità o identificazione di oggetti. Una prima caratteristica distintiva è la fonte di alimentazione dipendente dal lettore, in quanto questi transponder ricevono energia dalla stessa antenna di lettura. Infatti il lettore RFId trasmette un fascio di energia il cui campo elettromagnetico investe il tag e fornisce al chip la potenza necessaria per trasmettere i dati. La capacità di trasmissione risulta quindi limitata ai momenti in cui il tag viene interrogato.
La distanza di comunicazione varia a seconda della frequenza di lavoro e delle potenze dei lettori, e può oscillare da qualche centimetro a qualche metro. Tipicamente, i tag passivi possono essere letti fino ad una distanza di 4-5 metri usando una frequenza nella banda UHF, mentre gli altri possono arrivare a distanze più elevate, nell'ordine dei 100 metri. Questo avviene proprio perchè i transponder passivi utilizzano l'onda a radiofrequenza, generata dal lettore, sia come fonte di energia per alimentare il circuito integrato sia per trasmettere e ricevere dati. La distanza, di questi tipi di tag, è limitata perché la potenza di trasmissione si attenua velocemente con l'aumentare della distanza, ma soprattutto perchè le normative non ammettono ovunque la generazione di campi elettromagnetici con potenze molto elevate, con conseguente distanza di comunicazione limitata.

TAG SEMIATTIVI (O SEMIPASSIVI)

Questa categoria di tag ha batterie incorporate, gestite con attenzione al risparmio energetico: solitamente la batteria alimenta dei sensori e/o memorie presenti sul tag, mentre la lettura continua a sfruttare l' energia proveniente dal campo del lettore. Questi tag sono in grado di trasmettere dati solo se interrogati dal lettore perchè non sono dotati di un trasmettitore integrato e per questo sono ancora costretti ad usare il campo generato dal lettore per effettuare la trasmissione.

TAG ATTIVI

Questa tipologia di tag viene impiegata per applicazioni sofisticate, quali aerei militari e civili e mezzi di trasporto in movimento a velocità elevate. Tali applicazioni richiedono funzionalità evolute come, ad esempio, quando è richiesto un controllo continuo telemetrico di grandezze fisiche. Questo gruppo di tag è caratterizzato da una fonte di alimentazione completamente indipendente dal lettore, in quanto tali transponder sono dotati di una batteria per alimentare i circuiti interni del chip e per le operazioni di trasmissione dei dati al lettore. Quindi i dati possono essere trasmessi senza la necessità di una interrogazione del lettore (processo peer to peer), al contrario di quanto avviene con le altre due tipologie di tag, dal momento che i transponder attivi sono in grado di generare l'energia a radiofrequenza trasmettendo autonomamente i dati. In questo caso, le prestazioni sono caratterizza-

te da comunicazioni effettuate a distanze che vanno dalle decine di metri alle decine di chilometri.

Le differenze tra tag passivi, semiattivi e attivi sono riassunte nella Tabella seguente:

TAG	VANTAGGI	SVANTAGGI	OSSERVAZIONI
Passivi	- tempi di vita più lunghi - vasta gamma di forme - meccanicamente più flessibili - basso costo	- distanze limitate a 4-5 metri - controllati rigorosamente dalle regolamentazioni locali	- sono i più usati nei sistemi RFId - bande LF, HF, UHF
Semiattivi	- grande distanza di comunicazione - possibilità di uso per controllare altri dispositivi come i sensori (temperatura, pressione, ecc..)	- costosi a causa della batteria e del contenitore - affidabilità: impossibile determinare se una batteria sia buona o difettosa, specialmente negli ambienti con tag multipli - la proliferazione di transponder attivi presenta un rischio ambientale, di prodotti chimici potenzialmente tossici usati nelle batterie	usati principalmente nei sistemi in tempo reale per rintracciare materiali di alto valore. I tag sono UHF
Attivi			usati nella logistica per rintracciare container sui treni, camion, ecc… Generalmente lavorano in banda SHF

Figura 6 - Confronto tra varie tipologie di tag

Funzionalità e memoria nei Tag

Uno dei modi principali per classificare i tag RFId è in base alla loro capacità di leggere e scrivere dati. Si giunge alla definizione di cinque classi distinte.

CLASSE 0: Read Only. Questi sono i tag più semplici poichè i dati, che solitamente consistono in un semplice numero identificativo, vengono scritti una volta per tutte nel tag al momento della produzione dello stesso. Non è quindi possibile aggiornare in nessun modo la memoria. La Classe 0 viene usata a volte per indicare una categoria di tag chiamati EAS (Electronic Article Surveillance) o dispositivi anti-furto, che non hanno un identificativo, ma servono esclusivamente per manifestare la propria presenza nel momento in cui attraversano il campo di un antenna. A questa classe appartengono i tag che più si avvicinano ai codici a barre, pur presentando una serie di vantaggi (alcuni per niente trascurabili) che avremo modo di elencare più avanti.

CLASSE 1: Write Once Read Many (WORM). In questo caso il tag viene prodotto senza scrivere nessun dato nella memoria. I dati possono quindi essere scritti sia dal produttore del

tag, sia dall'utilizzatore dello stesso, ma comunque una sola volta. Non è infatti possibile nessuna scrittura successiva: a questo punto il tag può essere solo letto. I tag di questo tipo vengono utilizzati, solitamente, come semplici identificatori.

CLASSE 2: Read Write. Questa classe racchiude i tag più flessibili che consentono agli utilizzatori di leggere e scrivere dati nella memoria. Solitamente, i tag appartenenti a questa classe vengono usati come data loggers e, quindi, possiedono uno spazio di memoria superiore a quello necessario alla memorizzazione di un semplice identificativo, fornendo, ad esempio, la possibilità di immagazzinare anche informazioni utili per le lavorazioni intermedie che un prodotto deve subire (lungo la filiera i PLC o altre tecnologie dedicate alla lavorazione del prodotto, sulla base delle informazioni memorizzate nel tag, decidono quale trattamento eseguire). Altri dati che possono essere contenuti nei transponder potrebbero essere quelli relativi agli indici di qualità o ancora ai problemi riscontrati.
La lettura del tag, invece, consente di valutare le caratteristiche dei prodotti o dei lotti. Nel caso di un uso interattivo lungo la filiera, si può ad un certo punto procedere al recupero del tag per trasferire le informazioni in esso contenute ad altri sistemi informativi.
I tag possono essere applicati sul prodotto durante la fase di lavorazione per essere poi utilizzati in modo interattivo lungo tutta la Supply Chain (dalla produzione alla distribuzione al dettaglio e, a volte, fino al consumatore).
I transponder Read Write possono essere usati a supporto della filiera, svolgendo il ruolo fondamentale di identificare i prodotti per poterne tracciare la storia, di utilizzare le informazioni per automatizzare alcuni processi amministrativi e industriali, di localizzare i diversi modelli presenti in un magazzino e di smistare, nella fase di distribuzione, modelli e prodotti in base al prezzo, alle dimensioni, al packaging. Applicando un tag su un prodotto è possibile gestire in modo automatico l'ingresso-uscita dei pallet in un magazzino, registrare i percorsi e i tempi di transito lungo la filiera e comunicarli al cliente, generare automaticamente le bolle e le fatture e aggiornare il sistema informativo degli attori della Supply Chain. Inoltre è possibile realizzare inventari real time e prevenire furti, fornendo, in entrambi i casi, un supporto valido nella fase di vendita. Nella fase post vendita i tag possono essere riutilizzati per attività di assistenza e manutenzione.

CLASSE 3: Read Write con sensore a bordo. I tag appartenenti a questa classe sono equipaggiati con un sensore che consente di registrare parametri quali temperatura, pressione, umidità (basti pensare alla catena del freddo o del fresco) e spostamenti, scrivendo sulla memoria del tag. Tali tag devono necessariamente essere tag attivi o semiattivi poiché le letture devono poter essere effettuate dal sensore in assenza del lettore.

CLASSE 4: Read Write con trasmettitore integrato. Questi tag sono come dei dispositivi radio in miniatura che possono comunicare con altri tag o altri dispositivi in assenza del lettore. Ciò significa che i tag presi in esame sono completamente attivi e quindi alimentati dalla propria batteria.

	CLASSE 0	CLASSE 1	CLASSE 2	CLASSE 3	CLASSE 4
Passivi/Attivi	Passivo	Passivo	Passivo con funzionalità aggiuntive*	Semipassivo	Attivo
Lettura/Scrittura	Read Only	WORM	Read Write	Read Write	Read Write
Affidabilità di trasmissione	Bassa	Bassa	Bassa	Alta	Alta
Batteria	No	No	No	Litio/ Manganese	Litio/ manganese
Orizzonte di vita	Lungo	Lungo	Corto	Lungo	Lungo
Range di comunicazione	Corto	Corto	Lungo	Medio	Lungo
Applicazioni	Antifurto	Identificazione	Data logging	Sensori	Ad hoc

* (memoria supplementare, crittografia,...)

Figura 7 - Caratterizzazione dei Tag RFId per le modalità di alimentazione e trasmissione e per le capacità di lettura-scrittura

2.2 CONFRONTO TRA TAG RFID E CODICI A BARRE

Quanto illustrato mette chiaramente in evidenza che definire le tecnologie RFId uguali a quelle che stanno alla base dell'identificazione effettuata mediante codice a barre è senza dubbio riduttivo. Infatti, è possibile considerare l'RFId come una "nuova generazione" di codice a barre, senza però dimenticare che essa costituisce, di fatto, un enorme salto tecnologico e funzionale. Allo stesso modo, è importante sottolineare che l'uso del codice a barre, sotto certi aspetti, risulta ancora preferibile e che ciò mostra come il giorno in cui i tag RFId sostituiranno completamente le etichette con codice a barre è ancora molto lontano.
Il codice a barre è attualmente la tecnologia di identificazione più diffusa. È caratterizzato da una pervasività straordinaria, infatti quasi tutti i prodotti di consumo e durevoli hanno etichette con codice a barre. Questa tecnologia comprende, oltre alle etichette, anche tutti gli apparati utili alla loro stampa e lettura e deve la sua affermazione, in tutti i settori industriali e dei servizi, soprattutto al basso costo e alla facilità d'uso. Inoltre, lo sviluppo di sistemi di stampa a getto d'inchiostro con elevata qualità del codice a barre a costi contenuti ha reso possibile la diffusione di questa tecnologia anche nelle linee di produzione e di spedizione. Il codice EAN è, tra i diversi tipi di codici a barre, il più diffuso in Europa e viene utilizzato nella marcatura all'origine dei prodotti finiti. Il codice a barre che ricopre lo stesso ruolo e svolge le stesse funzioni negli Stai Uniti è il codice UPC.
Per mettere in evidenza le differenze esistenti tra un tag RFId e un'etichetta con codice a barre, dovrebbe essere sufficiente riportare le caratteristiche peculiari di entrambe le tecnologie riguardo ad alcuni aspetti cruciali nell'ambito dell'identificazione. Nella tabella di seguito le due soluzioni sono poste a confronto.

	CODICE A BARRE	RFID
Memoria	Capacità limitata	Capacità elevata
Accesso ai dati	Informazioni statiche, sola lettura	Possibilità di riscrittura
Modalità di lettura	Una sola lettura alla volta	Più letture quasi contemporanee
Portata di lettura	Qualche cm manualmente in contatto visivo	Da qualche cm a qualche metro in modo automatico o manuale, senza necessità di linea di vista
Robustezza dispositivo	Facilmente usurabile	Resistente all'usura (con packaging adeguati) e mantenimento delle informazioni per lungo tempo
Modalità di interazione	Necessità di mirare l'etichetta	Lettura omnidirezionale
Qualità supporto	Difficoltà di lettura dovuta allo sporco, al danneggiamento	Immunità allo sporco, maggiore resistenza strutturale
Costo	Economico, costo dell'inchiostro	Da qualche cent a diversi Euro, ancora elevato
Diffusione	Diffusione planetaria omogenea	Ancora in fase di adozione
Disponibilità	Tutti i produttori dispongono di stampanti e lettori	Scarso numero di produttori di tag e lettori
Standard	Consolidati da decine di anni (EAN-UCC)	Ancora in evoluzione
Inserimento nel prodotto	Agevole	Non sempre facile

Figura 8 - Confronto tra RFId e codice a barre

Soprattutto alcuni dei vantaggi di cui godono le tecnologie RFId rispetto al codice a barre coinvolgono degli aspetti che stimolano un grande interesse in molti settori. Tra questi vantaggi ci sono, senza dubbio, la possibilità di identificare univocamente ciascun oggetto, che si ottiene anche grazie alla capacità di immagazzinare un volume di dati enormemente superiore (dai 100 Byte del codice a barre agli 8KB dei tag RFId), il limitato intervento di operatori richiesto per la gestione, l'eliminazione della necessità di "vedere" l'etichetta, la possibilità di disporre di diverse distanze di lettura (da pochi centimetri a diversi metri grazie a frequenze e etichette diverse), la resistenza agli ambienti ostili (alte temperature, umidità, sporcizia, ecc. utilizzando opportuni package.), la capacità di lavorare in ambienti contaminati, la possibilità di effettuare la lettura contemporanea di più codici e di leggere e scrivere sui tag più di una volta, la possibilità di applicare metodi di crittografia e di autenticazione e, infine, la possibilità di disattivare l'etichetta per scopi di sicurezza e di privacy.

Va anche sottolineato che l'RFId penetrerà un numero maggiore di mercati rispetto al codice a barre.
Data l'eliminazione della necessità di "vedere" il tag e la possibilità di leggere anche attraverso la vernice o la plastica, si possono ottenere notevoli benefici in termini di efficienza, di flessibilità e di robustezza. Questa caratteristica può essere sfruttata, ad esempio, inserendo altre stazioni di lettura, come sui nastri dei convogliatori.
Per quel che riguarda la lettura simultanea, sono ovvi i vantaggi relativi all'efficienza derivante soprattutto dall'aumento della velocità di raccolta dei dati, dato che non si deve più fare riferimento a meccanismi di input di tipo sequenziale, come nel caso dei codici a barre che richiedono di essere letti uno per volta.
I range di lettura possibili con le tecnologie RFId garantiscono, maggiore flessibilità visto che aumentano il numero delle modalità con cui i dati possono essere raccolti.
Con riferimento alla capacità di memoria e alla possibilità di lettura-scrittura, è doveroso sottolineare i benefici ottenibili in aspetti cruciali come l'accuratezza ed il controllo d'inventario (visto che si può identificare anche il singolo oggetto), e la gestione dei dati, infatti i tag possono essere scritti e aggiornati in tempo reale.
Altri aspetti cruciali che fanno si che si possano conseguire ulteriori vantaggi sono la possibilità dei tag di operare in ambienti ostili e la maggiore vita utile.
Tuttavia, i codici a barre rimangono ancora il mezzo principale di raccolta automatica di dati, perchè sono una tecnologia molto consolidata e poco costosa. Come accennato in precedenza, prima che i codici a barre vengano eliminati dalla Supply Chain, passeranno diversi anni. Infatti, molte aziende presentano attività operative in ambito logistico basate sull'ausilio dei codici a barre ormai estremamente consolidate e, al di là delle iniziative di compliance, sono molto riluttanti ad implementare una reingegnerizzazione dei processi operativi che risulterebbe molto costosa. È anche questo il motivo per cui si assiste (e si assisterà sicuramente nel prossimo futuro) alla realizzazione di sistemi ibridi che utilizzano sia codici a barre che tag RFId.

2.2.1 LETTORI E ANTENNE

Il lettore rappresenta la porta che consente di mettere in comunicazione il mondo dei transponder con il mondo esterno, ed è in grado di effettuare l'interrogazione del singolo tag, di interfacciarsi con i sistemi informativi e di compiere le operazioni di invio e ricezione dati.
L'interrogazione dei tag da parte del lettore viene effettuata al fine di raccogliere i dati che i chip hanno memorizzati al loro interno. Tale operazione viene realizzata attraverso una interfaccia radio ed una comunicazione che genericamente possiamo dire avvenga a radiofrequenza.
Può capitare che, per mettere a disposizione dell'utente funzionalità aggiuntive, i lettori vengano dotati di una memoria interna, di una capacità di elaborazione o di una connessione a database remoti.

Il lettore può essere dotato di una capacità di elaborazione per eseguire alcune operazioni, come ad esempio la cifratura e la decifratura dei dati e delle trasmissioni.
È possibile distinguere tra il cosiddetto canale diretto (o forward channel o uplink) e quello noto come canale di ritorno (o backward channel o downlink). Il primo è il canale attraverso cui è possibile la comunicazione dal lettore verso il tag, mentre il flusso dei dati in senso opposto è ottenuto grazie al secondo.
Le modalità con cui tag e lettore stabiliscono una comunicazione sono di vario tipo, ma quella più diffusa, è senza dubbio l'accoppiamento induttivo, propria della lettura dei tag passivi funzionanti in bassa frequenza, LF o HF. L'antenna del lettore crea un campo magnetico accoppiato all'antenna del tag che, grazie ad un accumulatore interno, riutilizza l'energia assorbita da questo campo magnetico per modularlo trasmettendo al lettore i dati immagazzinati nella sua memoria. Il lettore, a questo punto, riconverte la risposta in informazione (come il codice identificativo) e la rende disponibile per l'applicazione adeguata.
Un lettore è costituito da un modulo a radiofrequenza (ricetrasmettitore), un'unità di controllo (controller) ed elementi di accoppiamento per il transponder. Inoltre, è dotato di interfacce di comunicazione con l'esterno supplementari (RS 232, RS485, USB, Ethernet, Wi-Fi, GSM, Bluetooth, ecc..) per consentire la trasmissione dei dati ricevuti al sistema di elaborazione.

Il controller

Il controller gestisce le interfacce di comunicazione tra l'antenna e l'infrastruttura software (PC, sistema host, server, Network Interface Module) e consiste in un microcalcolatore con adeguato programma. L'unità di controllo consente di gestire anche fino a otto antenne diverse. In sintesi, il controller rende possibile l'interrogazione dei transponder che attraversano il campo di un'antenna ed è responsabile del funzionamento degli algoritmi di anticollisione per una corretta gestione della ricezione di vari tag, quando presenti contemporaneamente nello stesso range di lettura.
Il sistema host si interfaccia con il controller e dirige l'interrogazione del tag mediante una comunicazione seriale, parallela o via bus. L'unità di controllo RFId può anche essere programmata per eseguire il controllo di processo direttamente dai dati nella memoria del tag.

Figura 9 - Esempio di controller

Alcuni controller presentano interfacce che possono essere attivate dal controller stesso, rendendo possibile una riduzione del carico di lavoro del sistema host.
Riassumendo, le funzioni del controller sono la codifica, la decodifica, il controllo e l'immagazzinamento dei dati, la gestione della comunicazione con i tag e con l'host.

Le antenne

Le antenne sono le interfacce fisiche vere e proprie tra il controller e i tag. Un'antenna è un dispositivo che ottimizza la trasformazione di energia elettrica o magnetica in onde radio per consentire le operazioni a distanza di lettura e scrittura dei dati sui tag (o sulle etichette, o sui PCB). Sul mercato, sono disponibili antenne di diverse forme e dimensioni per rendere possibile l'operatività in spazi ristretti, ma anche per consentire, se necessario, range di lettura e scrittura estesi, generando campi di intensità maggiore o con caratteristiche di direzionalità maggiori che permettano di ricevere meglio i segnali riemessi dai transponder controllati, che spesso sono caratterizzati da livelli di potenza molto bassi.
Le antenne sono realizzate tramite un avvolgimento di filo di rame su un supporto plastico o isolante, presentano dimensioni maggiori rispetto a quelle presenti nei tag e sono dotate di staffe e coperture che le proteggono dagli agenti esterni e atmosferici.
Per valutare le caratteristiche delle antenne è utile porre la propria attenzione su tre parametri principali:

- *Direttività*. È la capacità di concentrare le emissioni a radiofrequenza in una zona più o meno ristretta.
- *Guadagno*. È un importante parametro prestazionale che misura il rapporto tra l'efficacia dell'antenna e quella di un'antenna ideale che irradia con la stessa energia in tutte le direzioni nello spazio circostante. Le antenne direttive presentano un guadagno molto elevato in un determinato spazio e molto basso in tutti gli altri.
- *Polarizzazione*. Indica gli assi (verticale, orizzontale,..) sui quali sono orientate le componenti di campo elettrico e magnetico durante la propagazione in aria. Dipende principalmente dalla forma degli elementi che costituiscono l'antenna di trasmissione. Un tipo di polarizzazione è quella *lineare*, tipica delle antenne che generano un campo monodimensionale e presentano un range di lettura maggiore rispetto agli altri tipi di antenna, a condizione che il tag sia orientato in maniera ottimale. Tali antenne possono avere difficoltà nel trasmettere il segnale oltre alcuni ostacoli. Le antenne con polarizzazione *circolare*, invece, generano un campo tridimensionale e sono meno soggette ai problemi incontrati dalle antenne a polarizzazione lineare.

Creando particolari configurazioni, grazie all'aggregazione di più antenne (array, tunnel), si possono ottenere miglioramenti nelle prestazioni. Tra queste configurazioni, vale la pena citare quella che consiste nell'utilizzare antenne in linea e quella che prevede l'impiego di antenne sotto la stessa copertura.
Nel primo caso, si posizionano in linea più antenne con l'obiettivo di migliorare la lettura di tag che si spostano ad alta velocità. Nel secondo caso, più antenne vengono posizionate

per irradiare nella medesima zona, ma con polarizzazioni differenti per migliorare la lettura indipendentemente dall'orientamento del tag.
Alcuni sistemi sono realizzati integrando insieme in unico lettore (o lettore-scrittore) sia l'antenna che il controller, mentre altri tengono separata la prima dal secondo.
Un'ultima precisazione riguarda un fatto che abbiamo già avuto modo di notare, ovvero che, nel caso di tag passivi, il campo generato dall'antenna risulta necessario per fornire al tag l'energia utile per la trasmissione delle informazioni che contiene.

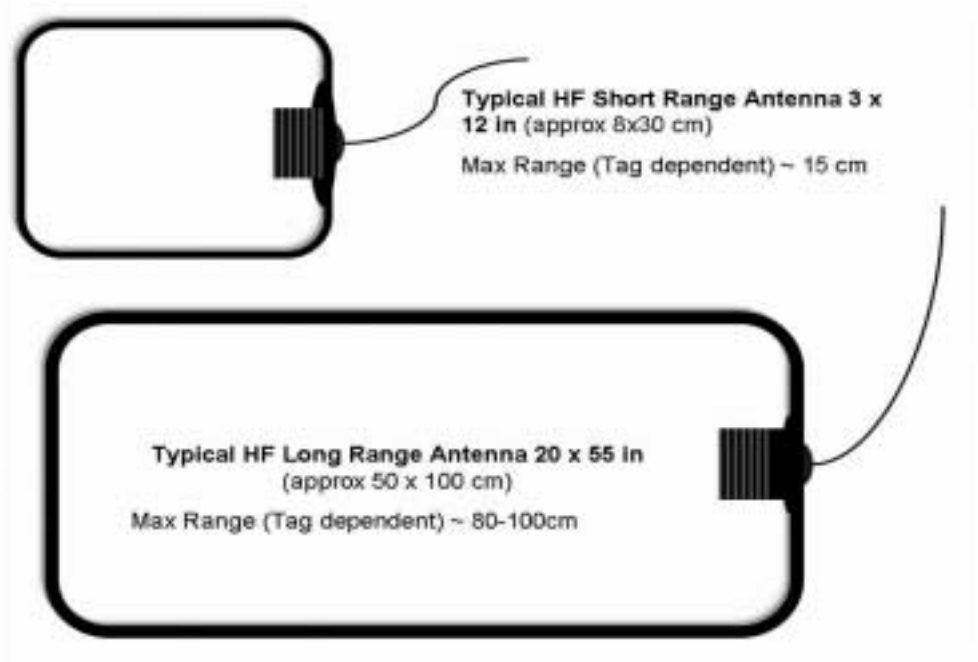

Figura 10 - Antenne esterne per lettori

Tipi di lettore

I lettori di tag possono essere di vari tipi, a seconda dell'applicazione per cui sono destinati.
I dispositivi di lettura possono essere integrati in terminali palmari (hand-held reader) per effettuare rilievi sul campo, laddove ci sia il bisogno di controllare un tag o di aggiornarne il contenuto fuori linea.
Esistono, poi, dispositivi trasportabili che vengono utilizzati quando c'è la necessità di un'installazione su dispositivi mobili.
Infine, un'altra categoria di lettori comprende i dispositivi incorporati in postazioni fisse, che vengono impiegati per controllare ingressi e uscite, linee di produzione o specifiche aree di attività, posizionandoli in punti strategici. Tra le soluzioni di questo tipo figurano colonnine, pedane sensibili, scaffali intelligenti (smart shelves), tunnel e varchi (gate) da cui passano persone, carrelli, muletti e nastri trasportatori. Un lettore fisso può, ad esempio, essere predisposto alle porte di entrata di un magazzino, fissato in un edificio o nella superficie stradale.

Un tunnel consiste in una serie di antenne disposte con diversi orientamenti e accese alternativamente, mentre i gates sono realizzati con due antenne contrapposte con campo sfasato. Gli scaffali intelligenti sono un'applicazione innovativa che permette di rilevare il momento in cui gli articoli vengono aggiunti o rimossi. È ovvia l'importanza del ruolo ricoperto da una soluzione di questo tipo nell'ambito dell'attività di controllo degli inventari, che può essere effettuata real time.
È ovvio che i lettori hand-held possono affiancare i lettori fissi in un tipico scenario di magazzino, ma anche essere il principale strumento di raccolta dati.

Figura 11 - Lettore hand-held (in alto a sinistra), un varco (sotto) e un tunnel

I lettori sono dei dispositivi abbastanza semplici e proprio questa semplicità li rende soggetti a svariati utilizzi: possono essere integrati in dispositivi mobili come cellulari o PDA e, in effetti, è gia possibile trovare in commercio dei telefoni cellulari con lettore RFId incorporato, seppur con una capacità di lettura di pochi centimetri.
È importante sottolineare che, se i tag diventassero comuni sugli articoli di largo consumo, una caratteristica desiderabile per i dispositivi elettronici sarebbe proprio la capacità di leggere i tag RFId.
Un'applicazione futura è quella dei lettori multifrequenza. L'Auto-ID Center del Massachusset Institute of Technology (MIT) ha recentemente definito le specifiche per realizzare dei

lettori che siano in grado di leggere tag che operano a diverse frequenze, anche se la loro realizzazione e il loro utilizzo sembrano ancora abbastanza lontani. Bisogna riconoscere, però, che la prospettiva di utilizzare diversi tipi di tag in svariati ambiti e di essere in grado di leggerli e scriverli senza essere costretti a comprare almeno un lettore per ogni frequenza è piuttosto allettante.
I lettori sono un elemento chiave in ogni sistema RFId e saranno, quindi, parte della valutazione del prodotto e della selezione dei processi. Fino alle recenti ondate negli sviluppi per la Supply Chain e all'esperienza maturata dall'Auto-ID Center, i lettori erano principalmente usati nei sistemi di controllo degli accessi e in altre applicazioni RFId che coinvolgevano bassi volumi, il che significa che i problemi di trattare grandi quantità di tag e alti volumi di dati non rappresentavano problematiche serie e pressanti. Oggi, tutto questo è sicuramente cambiato e molti produttori di lettori stanno iniziando a sviluppare una nuova generazione di prodotti capaci di gestire i problemi che saranno caratteristici della Supply Chain e dell'infrastruttura EPC proposta dall'Auto-ID Center e illustrata più avanti.
In un futuro che secondo alcuni esperti non è poi così lontano, ogni prodotto potrà essere dotato di un tag a radiofrequenza e i lettori raccoglieranno un flusso ininterrotto di codici elettronici durante tutte le fasi di realizzazione, spedizione e vendita. La sfida più stimolante risiederà proprio nelle attività di trasferimento e gestione di questa enorme mole di dati.

Eliminare le collisioni

Nelle operazioni di lettura, uno dei problemi più pressanti che vanno risolti per evitare che tutti gli sforzi di miglioramento che guidano l'implementazione dell'RFId siano vanificati, è l'eliminazione delle collisioni. Le collisioni possono avere una duplice natura: collisioni dei lettori, collisioni dei tag.

COLLISIONE DEI LETTORI

Il problema che porta all'insorgere di questo tipo di collisioni è che il segnale di un lettore RFId può interferire con il segnale di un altro dove la copertura si sovrappone. Un possibile schema di anticollisione è quello proposto e utilizzato dall'Auto-ID Center, chiamato TDMA (Time Division Multiple Access, divisione di tempo con accesso multiplo). Il funzionamento è molto semplice: i lettori vengono programmati per effettuare la lettura in tempi diversi, evitando di leggere i tag allo stesso tempo. In questo modo, è impossibile che i lettori interferiscano uno con l'altro. Una controindicazione sta nel fatto che quando un tag attraversa un'area dove due lettori si sovrappongono, questo tag verrà letto per due volte. Per risolvere il problema della lettura multipla è stato necessario mettere a punto un sistema che consente di cancellare i codici duplicati.

COLLISIONE DEI TAG

Una sfida fondamentale nei sistemi RFId è la prevenzione delle collisioni tra i dati trasmessi dai tag. Se tutti i tag tentano di trasmettere il numero seriale simultaneamente, il risultato potrebbe essere un rumore che conduce, di conseguenza a una lettura errata: potrebbe

essere difficile per il lettore districare i vari segnali che si sovrappongono. Per risolvere questo problema, i protocolli di comunicazione dal lettore al tag impongono un accurato sequenziamento sui messaggi dei tag.
Uno di questi protocolli è noto come tree-walking. Esso si basa sulle possibilità di rappresentare i numeri seriali dei tag a n bit come un albero binario. Se immaginiamo ogni diramazione sinistra etichettata con uno 0 e ogni diramazione destra con un 1, un percorso dalla radice a un nodo posto alla profondità k, otteniamo un numero seriale di k bit.
Il lettore inizia dalla radice dell'albero, chiedendo a tutti i tag di trasmettere il primo bit del loro numero seriale. Se il lettore riceve solo una trasmissione "0", sa che tutti i numeri seriali dei tag iniziano con uno 0 e ricorre al sottoalbero sinistro. Se il lettore rileva una collisione, che consiste sia in uno 0 che in un 1, ricorre a entrambi i sottoalberi del nodo. La stessa procedura viene adottata per ogni nodo interno. All'inizio, tuttavia, trasmette un comando che provoca solo i tag nel sottoalbero corrispondente all'interrogazione fatta. Una volta che il lettore ha completato il processo di analisi dell'albero e ha determinato quali tag sono presenti, può comunicare individualmente con i tag tramite il serial number.
In sintesi, il lettore interroga il tag, richiedendo una risposta solo nel caso in cui le prime cifre del suo codice identificativo corrispondano a quelle comunicate dal lettore stesso. Ad esempio, il lettore invia ai tag un messaggio del tipo: "Rispondi se il tuo codice identificativo inizia con 0". Se la risposta arriva da più di un tag il lettore invia un nuovo messaggio, più preciso del primo: "Rispondi se il tuo codice identificativo inizia con 00". Questa procedura viene reiterata finchè un solo tag risponde alla richiesta del lettore e avviene in modo molto rapido, tale da consentire la lettura di 50 tag in meno di un secondo.

2.2.2 Architettura accentrata e distribuita

Ponendo l'attenzione sui tag passivi, che rappresentano la soluzione più diffusa (soprattutto per ragioni economiche), è possibile individuare due diverse modalità di utilizzo.
La prima, detta architettura accentrata, è caratterizzata dal fatto che all'interno del transponder viene memorizzato solo un numero, lasciando che le informazioni associate a questo numero siano raccolte su server specifici centralizzati.
La seconda, nota come architettura distribuita, presenta la peculiarità di memorizzare le informazioni nel tag stesso applicato al prodotto, dando vita a un vero e proprio sistema informativo distribuito.

Architettura accentrata: EPCglobal

L'Auto-ID Center del MIT ha studiato un sistema con questo tipo di impostazione, prefiggendosi l'ambizioso obiettivo di creare un sistema di identificazione globale dei beni di largo consumo che consenta ad ogni azienda di tracciare i prodotti in ogni paese. Ma per centrare questo obiettivo non si può prescindere dal soddisfacimento di due prerequisiti di base: il primo è quello di contenere il costo dei tag per far sì che sia il più possibile vicino a quello delle etichette con codice a barre, il secondo è sviluppare uno standard mondiale

per l'identificazione dei prodotti. Entrambi questi aspetti richiedono una trattazione più approfondita a sè stante che sarà affrontata nel seguito.

Ciò che differenzia gli altri sistemi RFId da quello proposto dall'Auto-ID Center è l'idea che ogni etichetta abbia memorizzato al suo interno solo l'identificativo del prodotto, ottenendo un tipo di tag estremamente semplice. Introducendo una semplificazione di questo tipo, la strada che conduce allo sviluppo di tag più semplici ed economici sembrerebbe decisamente più praticabile. L'introduzione di un solo numero per ogni tag ha portato a sviluppare un nuovo standard di codifica mondiale dei prodotti, chiamato Electronic Product Code (EPC), che rappresenta il cuore dell'attuale tecnologia RFId secondo l'Auto-ID Center. È fondamentale mettere in evidenza come lo sviluppo dell'EPC non sia finalizzato al rimpiazzamento dei codici a barre, ma, piuttosto, alla creazione di un percorso che le aziende possono seguire per realizzare una "migrazione" dal codice a barre all'RFId. Questa codifica viene sviluppata con il supporto dell'EAN International (in Europa) e dell'UCC (Uniform Code Council, negli USA), le due principali società che sovrintendono a livello internazionale gli standard dei codici a barre.

Recentemente la EPCglobal Inc. ha dovuto prendere atto della diffusione delle tecnologie HF e della impossibilità di rimpiazzarle sempre con quelle UHF. Per questo ha creato un gruppo di lavoro per dettare gli standard Gen 2 anche per le frequenze HF. L'obiettivo è quello di estendere le logiche e le tecnologie comprese nell'attuale Gen2 per UHF anche al campo HF, dove sembrano più promettenti alcune applicazioni farmaceutiche.

Del resto EPCglobal non è una specifica legata a frequenze o tecnologie, ma solo la definizione di strutture di dati e di comando.

Recentemente un test su 56 casi presentati da 23 hardware differenti, ha confermato la possibilità di coesistenza di tag a livello di singolo item, anche con frequenze diverse.

Quando questo standard si aggiungerà a quello esistente, la scelta tra HF e UHF sarà condizionata, come è giusto, solo dalle distanze di lettura richieste per tag passivi (a basso costo): 20 cm per HF e fino ad alcuni metri per UHF.

L'architettura EPC consente un accesso immediato all'informazione e non ottimizza solamente i servizi esistenti, ma ha anche le potenzialità per creare nuovi servizi. Ad esempio: un dettagliante potrebbe abbassare i prezzi automaticamente quando si avvicina la data di scadenza, o un produttore potrebbe rintracciare uno specifico gruppo di prodotti a causa di motivi relativi alla salute e, se necessario, stabilire con esattezza l'origine del problema fino a livello di singolo prodotto.

Ogni blocco in cui può essere suddivisa l'architettura EPC contiene una specifica funzione che si rivela essenziale per garantire un funzionamento rapido ed efficiente dell'intero sistema.

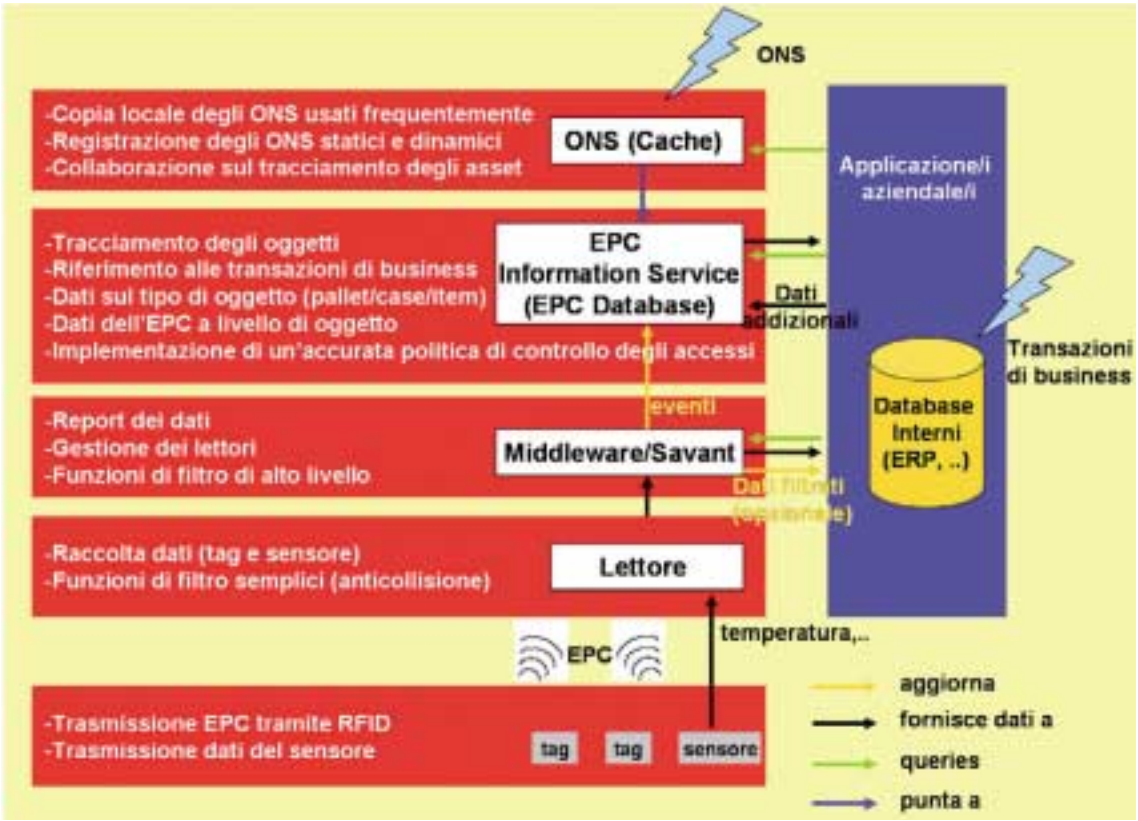

Figura 12 - Architettura di una rete EPC aziendale

EPC: Electronic Product Code

L'EPC è un numero composto da quattro campi: un'intestazione (header) e 3 parti di dati, come illustrato nella Figura 1.10.

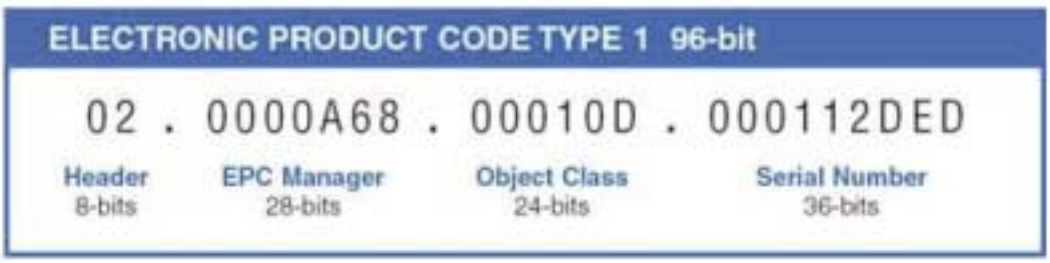

Figura 13 - EPC a 96 bit

L'intestazione (bit 0-7, nel caso di un EPC a 96 bit, come nella Figura 1.10) serve a identificare la versione dell'EPC, data l'esistenza di diverse lunghezze o di diversi tipi di EPC.
La seconda parte del codice (bit 8-35), detta EPC Manager, serve a identificare chi realmente ha realizzato l'articolo in esame e ha installato l'EPC, cioè indica il produttore dell'oggetto.
Il terzo campo (bit 36-59) viene chiamato Object Class ed è relativo al tipo di prodotto. In particolare, ne indica la categoria, il tipo e la versione.

L'ultima parte (bit 60-96) è il numero seriale univoco per l'articolo, che consente di far riferimento con esattezza ai suoi dati, permettendo, ad esempio, una rapida individuazione di quei prodotti alimentari che stanno per scadere.
Come abbiamo già avuto modo di precisare, l'EPC è l'unica informazione che viene memorizzata nel tag, ma il codice può essere associato ad altre informazioni (luogo e giorno di produzione dell'articolo, data di scadenza, luogo di spedizione) che sono memorizzate in un database. È possibile, inoltre, aggiornare in tempo reale tutte le informazioni che riguardano gli spostamenti di un prodotto e le modifiche che esso subisce.
Abbiamo visto che l'intestazione serve a identificare la versione dell'EPC, infatti l'Auto–ID Center ha proposto EPC a 64, 96 e 256 bit. In prospettiva futura, si pensa che sarà possibile ampliare queste versioni, presumendo di disporre di una maggiore quantità di informazioni immagazzinabili nei tag.
Tipicamente l'EPC utilizzato sarà quello composto da 96 bit che consente di conseguire il giusto compromesso tra la necessità di assegnare a tutti gli oggetti un codice univoco e il bisogno di contenere i costi del singolo tag. La versione a 96 bit consente di ottenere un'identificazione univoca per 268 milioni di industrie. Ogni produttore ha 16 milioni di classi di oggetti e 68 miliardi di numeri seriali per ciascuna classe: numeri che consentirebbero di coprire tutti gli articoli realizzati nel mondo in futuro. Va precisato che, probabilmente, fino a quando non sarà necessario utilizzare la maggior parte di questi codici, l'EPC formato da 64 bit rappresenterà una soluzione intermedia ideale. La brevità del codice permette di contenere il prezzo dei Tag RFId nel periodo iniziale e fornisce più numeri univoci EPC delle reali necessità.

		Header	EPC Manager	Object class	Serial number
EPC-64	Tipo I	2	21	17	24
	Tipo II	2	15	13	34
	Tipo III	2	26	13	23
EPC-96	Tipo I	8	28	24	36
EPC-256	Tipo I	8	32	56	160
	Tipo II	8	64	56	128
	Tipo III	8	128	56	64

Figura 14 - Tipi di EPC

Nel sistema proposto dall'Auto-ID Center si possono individuare, oltre all'EPC, tre elementi principali: l'Object Name Service (ONS), il Phisical Markup Language (PML) e il Middleware Savant.
Savant è la tecnologia software sviluppata dall'Auto-ID Center e costituirà il sistema nervoso della nuova rete all'interno di un'azienda, ma anche tra più aziende collegate tra loro.

Nel momento in cui un lettore comunica un EPC a Savant, esso, grazie a un servizio Internet denominato ONS, identifica il prodotto associato allo specifico EPC. Con un funzionamento analogo al DNS (Domain Name Service) che "punta" i computer su determinati siti del web, l'ONS "punta" il Savant su un database aziendale che contiene le informazioni sul prodotto in esame. Informazioni come le caratteristiche di base e la categoria di appartenenza relative ai prodotti vengono memorizzate utilizzando un linguaggio noto come PML, basato su un linguaggio attualmente molto diffuso, denominato XML (eXtensible Markup Language). Il Phisical Markup Language rende possibile lo svolgimento delle normali attività aziendali, che possono andare dalla ricerca in un database d'inventario di tutti i prodotti di una certa categoria, al confronto dei prezzi di un determinato prodotto con date caratteristiche.

MIDDLEWARE/SAVANT

Possiamo generalmente definire con il termine middleware un software intermedio fra i dispositivi di raccolta dei dati e il software applicativo, con svariate funzioni connesse a questo ruolo di "frizione" tra un mondo e l'altro. Nell'ambito delle tecnologie RFId, invece, il middleware assume un significato diverso. Tra i dispositivi che raccolgono dati in elevata quantità e i sistemi multipli che devono farne uso in tempo reale, è necessaria un'intelligenza intermedia capace di trattare, verificare e aggregare questi dati, rendendoli utilizzabili nel modo ottimale. Inoltre, il middleware di un sistema RFId non opera strettamente nella fascia intermedia fra dispositivi periferici e sistemi centrali, ma agisce all'estremità (edge) della rete, cioè a ridosso dei lettori RFId (o addirittura sugli stessi lettori RFId) dove svolge tutte le funzioni di filtraggio e instradamento dei dati.
Le funzioni basilari del middleware RFId sono, quindi, il monitoraggio e la gestione dei dati e dei dispositivi. Esso, infatti, estrae innanzitutto i dati dal lettore RFId e, dopo averli filtrati, aggrega le informazioni e le indirizza verso i sistemi informativi aziendali (ad esempio, un sistema di gestione del magazzino, un sistema ERP, o un sistema di esecuzione della produzione). Il middleware consente inoltre la gestione dei lettori RFId, compreso le condizioni "di salute" del dispositivo e la gestione in remoto.
Non è detto che il middleware in un sistema RFId sia strettamente necessario, infatti, in ogni caso preso in esame, vanno analizzate la dimensione dell'applicazione e la sua complessità. Ad esempio, la raccolta dei dati RFId in applicazioni semplici, che prevedono l'utilizzo di questi per un solo processo e all'interno di un solo sistema, potrebbe non avere bisogno del middleware o potrebbe aver bisogno di un prodotto middleware dotato semplicemente delle funzioni di base, in grado di controllare la veridicità e la qualità dei dati, senza presentare, però, tutte quelle funzioni sofisticate che vanno dalla connessione ad applicativi diversi, alla gestione di lettori diversi, alla possibilità di scrivere nuove applicazioni. Risulta ovvio che il middleware per RFId dipende dal tipo di applicazione presa in considerazione.
Il middleware può essere adatto per i cosiddetti early adopters, coloro che devono adeguarsi ad un obbligo in tempi brevi, o un middleware impostato alla scalabilità e all'integrazione in più applicazioni e più funzioni aziendali, in vista di un prossimo sviluppo dell'RFId.

La focalizzazione sull'hardware, nel caso di progetti RFId, è certamente importante, soprattutto se sussistono ancora incertezze in fatto di prestazioni o di costo, ma il valore dell'hardware RFId diventa inutile se a monte non vi sono degli strumenti software realmente efficaci, capaci di interpretare, aggregare e rendere significativi i dati generati dai lettori e di trasmetterli correttamente al sistema di gestione.
Savant è un sistema software che svolge l'unica funzione di calcolo presente nelle applicazioni EPC. I lettori di tag RFId generano una grande quantità di dati finemente suddivisi, relativi a miliardi di tag, e quindi il lavoro di Savant consiste per lo più nella riduzione dei dati mediante operazioni di filtraggio, aggregazione e conteggio. È proprio Savant che si occupa, quando due antenne leggono lo stesso codice, dell'eliminazione di una delle due letture. Gli altri aspetti rilevanti derivano dalle caratteristiche peculiari dell'architettura EPC, come l'ONS e i componenti del servizio PML. Riguardo alle specifiche di Savant, l'attenzione va posta più sull'estensibilità che sulle specifiche caratteristiche dell'elaborazione, dal momento che fra i specifici requisiti delle varie applicazioni esistono molte differenze.
L'utente ha la possibilità di intervenire, al fine di soddisfare le proprie necessità nelle applicazioni di interesse, combinando le caratteristiche dei vari moduli di Savant. L'obiettivo che sta dietro al progetto di una struttura modulare è quello di evitare la creazione di una sola specifica per soddisfare le necessità di ognuno e di favorire, in questo modo, l'innovazione da parte di gruppi indipendenti di persone.
In sintesi, Savant permette alle aziende di processare i dati relativamente non strutturati dei tag, presi da molti lettori RFId, e inviarli verso il Sistema Informativo appropriato, ed è in grado di compiere operazioni molto differenti, come monitorare i dispositivi di lettura RFId, gestire le false letture, immagazzinare dati e, infine, richiedere un ONS.

Il sottosistema ONS

L'ONS viene utilizzato per fornire un servizio globale di ricerca per la traduzione degli EPC in URL (Uniform Reference Localizzation) di Internet, dove è possibile reperire ulteriori informazioni sull'oggetto considerato. In altre parole, l'ONS viene utilizzato quando un'antenna legge un codice EPC e un computer ha il compito di rintracciare l'informazione relativa a quel codice su Internet. Sono molto frequenti i casi in cui questi URL identificano un Servizio Informazioni EPC, anche se può capitare di imbattersi in casi in cui l'ONS viene utilizzato per effettuare un'associazione tra gli EPC e dei siti web (o altre risorse di Internet) relativi ad un dato oggetto. È già stato provato che tale meccanismo è capace di gestire i volumi di dati attesi in un sistema EPC RFId.
L'ONS consente di disporre di servizi statici e di servizi dinamici: i primi, tipicamente, offrono URL per le informazioni in possesso del produttore di un oggetto, mentre i servizi ONS dinamici servono a registrare una sequenza di dati come fosse un oggetto che si muove attraverso la Supply Chain. Per costruire l'ONS si usa la stessa tecnologia dei DNS di Internet.

Il linguaggio PML

Mentre l'EPC è in grado di identificare il singolo prodotto, le informazioni realmente utili vengono scritte in un nuovo linguaggio software standard, chiamato PML. Lo stesso PML si

basa sul linguaggio XML ampiamente usato e accettato, progettato come un document format per scambiare dati attraverso Internet. Non è sorprendente quindi che, con una così ampia parte dell'infrastruttura EPC che viene presa in prestito da internet (DNS, XML,...), si faccia riferimento ad una "Internet delle cose".
In sintesi, quindi, PML è un linguaggio software i cui vocaboli vengono standardizzati con l'obiettivo di rappresentare le informazioni relative agli oggetti della rete EPC. Il PML viene utilizzato per la descrizione dei prodotti in modo riconoscibile dai computer, eseguendo una standardizzazione del contenuto dei messaggi scambiati nella rete EPC, ed è questo il motivo che sta alla base dello sforzo dell'Auto–ID Center nello sviluppo di interfacce standard e di protocolli per la comunicazione con l'infrastruttura Auto-ID ed all'interno di essa. Il nucleo centrale del PML offre una configurazione standardizzata per lo scambio dei dati catturati dai sensori nell'infrastruttura, come i lettori RFId.
Il PML è progettato per immagazzinare ogni informazione rilevante riguardo al prodotto, ad esempio:

- Informazioni sulla locazione. Ad esempio, il tag X viene rilevato dal lettore Y, che è posizionato alla banchina di carico Z.
- Informazioni telemetriche (proprietà fisiche di un oggetto, ad esempio la sua massa o proprietà fisiche dell'ambiente dove sono posizionati degli oggetti, ad esempio la temperatura dell'ambiente).
- Informazioni sulla composizione. Ad esempio, la composizione di una singola unità logistica.
- Date di scadenza dei prodotti.

Architettura distribuita

Un'architettura che preveda un sistema informatico e i tag applicati sugli oggetti consente di realizzare un sistema informativo distribuito, che può operare secondo modalità e con canali di comunicazione differenti. Questa struttura è dotata di flessibilità e affidabilità e non può essere progettata per ogni applicazione possibile in modo generalizzato. Infatti, deve essere definita per realizzare le specifiche funzionalità richieste ed in base alle peculiarità del settore d'utilizzo preso in considerazione. In questo modo sarà possibile utilizzare al meglio le capacità di elaborazione e di memorizzazione del sistema informatico e del mondo dei tag.
Questo tipo di approccio è più convenzionale (e ancora largamente diffuso, nella maggior parte degli ambiti in cui vengono applicate le tecnologie RFId) e prevede l'impiego di tag sofisticati, dotati di un chip capace di memorizzare tutti i dati necessari (tipicamente si hanno memorie di 8Kb). Le etichette risultano evidentemente più costose.

2.3 MODALITÀ DI SCELTA DEI TAG

Alla luce di quanto descritto finora, la scelta del tipo giusto di tag per una particolare appli-

cazione RFId è di fondamentale importanza, ma non è così agevole, poiché devono essere presi in esame, di volta in volta, una molteplicità di fattori tra cui:

- **Costo unitario**: elemento critico da valutare rispetto al valore degli oggetti e ai benefici marginali ottenuti col sistema RFId
- **Forma e dimensione:** l'insieme delle caratteristiche geometriche
- **Posizione:** se all'interno o all'esterno di involucri o del prodotto stesso. E' importante perché su questa va calibrata la sensibilità che il Tag dovrà avere per interpretare e ritrasmettere segnali a RF provenienti dall'esterno di un eventuale imballo.
- **Durabilità**: generalmente superiore ai 5 anni ma fortemente legata alla tipologia specifica di Tag che si utilizza. Per quanto riguarda i dati eventualmente scritti nella memoria flash, il Data Retention Time è oggi, in genere, di 10 anni.
- **Riusabilità**: la maggior parte dei Tag sono realizzati in supporti o su substrati di materiale plastico, è quindi in media la riusabilità dei tag è alta.
- **Resistenza agli ambienti ostili**: Sono disponibili Tag di ogni genere, ad esempio quelli utilizzati in ambito logistico, hanno un range di funzionamento che va dai -100º a +150 º
- **Polarizzazione:** la maggior parte dei Tag è sintonizzato per polarizzazione circolare, ma si possono realizzare anche tag con diversa polarizzazione.
- **Distanza di comunicazione.**: si va dai pochi centimetri (5-10 per un lettore palmare, 30-50 per un gate di grandi dimensioni) dei dispositivi LF e HF, ad alcuni metri (tipicamente 2-3 per le potenze trasmissive ammesse in Europa fino ai 6-9 negli USA) per dispositivi in banda UHF fino ad alcuni Km per dispositivi attivi nelle bande centimetriche SHF e EHF (limitati solo dalla potenza disponibile per la trasmissione e l'antenna a bordo)
- **Influenza di materiali come i metalli e i liquidi**: Le onde elettromagnetiche soffrono molto gli effetti di interazione con elementi polari (acqua) o metallici, e questi fenomeni di interazione dipendono delle frequenze di funzionamento.
- **Ambiente (rumore elettrico, altri dispositivi radio)**: il grado di disturbo dipende dal tipo di frequenza usata e risulta molto più marcato per le alte frequenze, in cui lo spettro è più affollato di sorgenti trasmissive
- **Frequenze operative (LF, HF, UHF, microonde)**: la frequenza di funzionamento del tag caratterizza sia la distanza di lettura che la loro interferenza con l'ambiente circostante.
- **Protocolli e standard di comunicazione supportati (ISO, EPC)**: i nuovi standard ISO della serie 18000 raccolgono buona parte delle indicazioni emerse dai lavori di EPC nella definizione dello standard GEN2. Manca tuttavia ancora un framework di lavoro unificante per i diversi standard, spingendo ad orientarsi su soluzioni, per applicazioni che richiedano componenti distribuiti,omogenee dal punto di vista dello standard principale supportato.

- **Regolamenti regionali (US, Europa, Asia):** importanti soprattutto per quello che riguarda i dispositivi ad alta frequenza (UHF e superiori) in cui la legislazione europea, e ancor più quella italiana, impongono limiti molto restrittivi sulla potenza utilizzabile.
- **Memoria**: da pochi Byte fino a 2048Byte o più per i soli Tag a basso costo, usati generalmente all'interno di una Supply Chain. Tuttavia, visto il costo ormai irrisorio di questa risorsa, è un parametro largamente ampliabile ed adattabile alle proprie specifiche esigenze
- **Anticollisione**: i meccanismi oggi utilizzati, dettagliati sia in C1G2 che in ISO 18000-3 e 4, permettono la lettura, che all'utente appare contemporanea, fino a 50 Tag al secondo. L'algoritmo più spesso utilizzato è di tipo slotted-aloha, quindi a divisione di tempo. EPC, nelle specifiche G2, prevede anche l'infrastruttura logica per la definizione di 4 sessioni di lettura contemporanee, cioè la possibilità di gestire da parte del Tag interrogazioni provenienti da 4 reader diversi.
- **Crittografia:** la scelta di inserire elementi di cifratura delle informazioni è possibile in diversi punti logici del sistema. Sul mercato è possibile scegliere supporti in grado ad esempio di realizzare una cifratura on-air della trasmissione, o ancora in grado di offrire la possibilità di un three-way hand-shake, con metodi di "challenge-response" per l'autenticazione dei partecipanti alla trasmissione, o infine di proteggere con password tutti i dati presenti sul Tag o solo quelli localizzati in alcune aeree specifiche della memoria.

2.4 IL MERCATO DEI SISTEMI RFID

L'hardware per l'RFId, comprende tutti i prodotti fisici, indispensabili affinché un sistema possa funzionare efficientemente. Di questa categoria, verranno analizzati in particolar modo i lettori e i tag, ponendo l'attenzione sui costi e, in generale, sul mercato attuale e quello futuro. Un discorso a parte verrà affrontato per il middleware, indispensabile anello di congiunzione tra i dati rilevati dall'hardware e i sistemi di gestione.

2.4.1 IL MERCATO DEI LETTORI

Con produttori di lettori si intende un'insieme molto vasto di imprese che vanno dalle aziende multinazionali di tecnologia ai piccoli produttori di lettori portatili.
Il prezzo dei lettori si aggira tra i 20 euro per i lettori grandi come un bottone e può arrivare ai 5000 euro per quelli da applicare sui nastri trasportatori per l'identificazione degli oggetti trasportati alla velocità di 5 metri al secondo.
Il mercato dei lettori RFId è caratterizzato, attualmente, da tre tipi di produttori, le cui caratteristiche sono illustrate nel seguito.

Innanzitutto, esistono i grandi produttori di attrezzature che definiscono gli standard, e che producono sia unità di lettura complete che componenti per altri fornitori che poi costruiranno i loro lettori.
Alcune imprese si concentrano su soluzioni per l'industria, producendo lettori per i nastri trasportatori e lettori di tipo "varco". Le soluzioni sono studiate per i centri di distribuzione delle compagnie di logistica. Altri fornitori completano la loro offerta fornendo oltre alle competenze tecniche, servizi di consulenza sul business.
Il secondo tipo di produttori di componenti RFId sono quelli di medie dimensioni che acquistano qualche componente dai grandi produttori e sviluppano in seguito i loro sistemi originali. Alcune aziende, costruiscono sia i lettori che i tag, pensando che questa combinazione permetta una migliore precisione e si occupano di appoggiare i progetti di prova presso i venditori al dettaglio, sia nei centri di distribuzione che nei negozi finali. Questa categoria di fornitori completa la loro offerta di prodotti con le antenne per gli scaffali intelligenti per i supermercati, ma limitano i servizi di implementazione ai bisogni tecnici.
All'ultimo tipo di produttori appartengono quelli che realizzano dispositivi per l'utente finale e che sono i fornitori più piccoli. Questi fornitori si specializzano soprattutto sui lettori portatili e, oltre al supporto tecnico, di solito, non offrono un servizio di consulenza completo.

2.4.2 IL MERCATO DEI TAG RFID

All'inizio della diffusione di questa tecnologia, si sono studiate le potenzialità derivanti dall'inserire un tag per ogni articolo in commercio. Le complesse tecniche di produzione, i costi di assemblaggio, e la scarsità di domanda hanno fatto sì che molte previsioni stimassero, plausibilmente, che il prezzo dei tag non scenderà fino a 5 centesimi prima dei prossimi otto anni. Si prevede, infatti, che il prezzo dei tag possa scendere in media, solo del 9% ogni anno. Per trovare un'alternativa più economica, i produttori e i distributori di beni di consumo hanno la necessità di ridurre l'utilizzo dei tag, puntando su scenari di utilizzo semplici o aspettando un'innovazione nella produzione. Un'altra prospettiva interessante, che condurrebbe a una notevole riduzione del costo dei tag e, quindi, all'applicazione delle etichette RFId anche ai singoli beni di largo consumo, consisterebbe nell'industrializzazione di nuove tecnologie basate su chip plastici e antenne stampate a getto d'inchiostro conduttivo, che sono ancora in fase di sviluppo e potrebbero portare nei prossimi anni il costo di un tag addirittura intorno al centesimo di euro.
Il trend di abbassamento del prezzo dei tag, è connesso alla crescita dei volumi, favorita dall'apertura dei mercati e al tempo stesso dall'affermarsi, su scala mondiale, di pochi standard consolidati. Secondo uno studio svolto dalla Forrester Research su 18 produttori di tag, si possono fare delle stime sul futuro del mercato delle tecnologie RFId.
In base alla ricerca di mercato, sono stati prodotti solo 276 milioni di tag in totale nel 2003, la maggior parte destinata ai pallet e alle confezioni (case). I produttori si aspettano qualcosa come 7 miliardi di tag prodotti entro il 2008, destinati in gran parte per identificare il singolo prodotto.
In riferimento a tali previsioni è bene precisare che le categorie di fornitori si differenziano in produttori dell'intero tag (dal chip, all'antenna, allo strato di interconnessione, e, per

alcuni modelli, anche all' involucro protettivo), in produttori di chip o in partners che assemblano i tag.

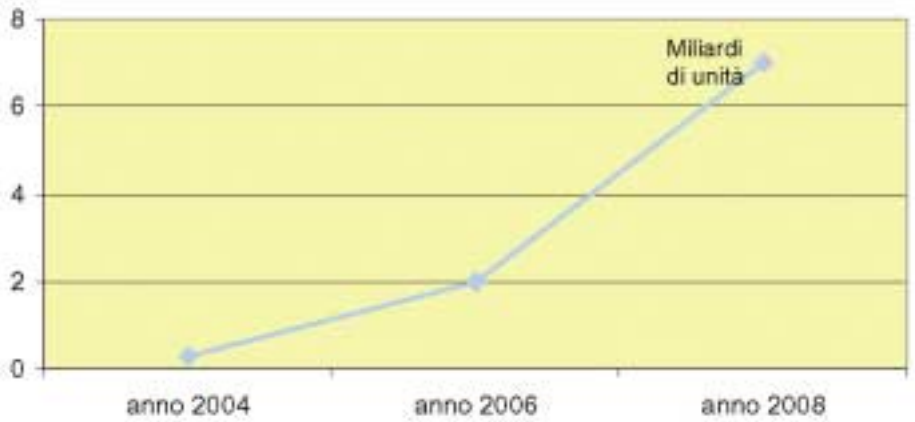

Figura 15 - Proiezione della produzione dei tag pianificata dal 2004 al 2008

La scelta del tag è principalmente guidata dalla capacità dello stesso e non dal prezzo. Le aziende hanno la necessità di comprare tag RFId che si adattino ai loro specifici bisogni, dato che un tag valido per tutte le situazioni non esiste. I produttori di tag cercano di trovare il giusto trade-off tra prezzo e prestazioni. I fornitori di tecnologia considerano gli standard ISO e i regolamenti di conformità come la caratteristica più importante in un tag per soddisfare il cliente, seguita dalla degradazione delle prestazioni.

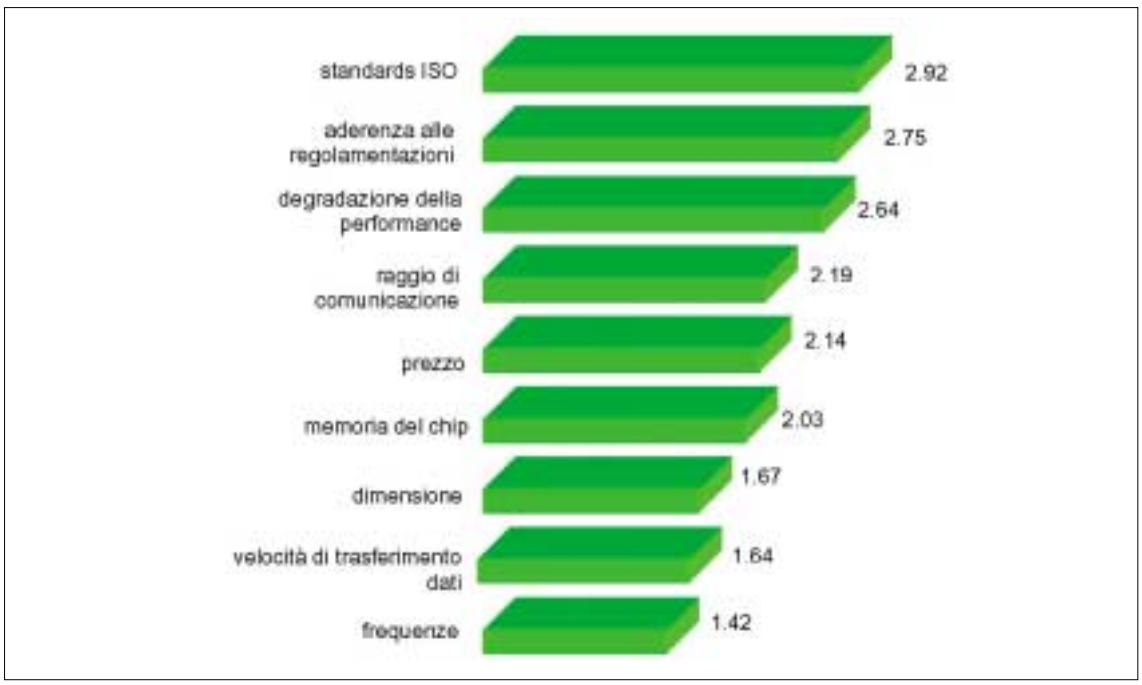

Figura 16 - Le caratteristiche più importanti per chi acquista i tag

Un altro aspetto emerso da non trascurare è che il costo di assemblaggio influenza il costo totale del tag. Il costo di assemblaggio influisce, secondo i produttori, per circa il 35% del totale. Le previsioni sono rivolte all' utilizzo di chip e di antenne più economici, ma cercano di individuare possibilità di risparmio nel processo di assemblaggio.

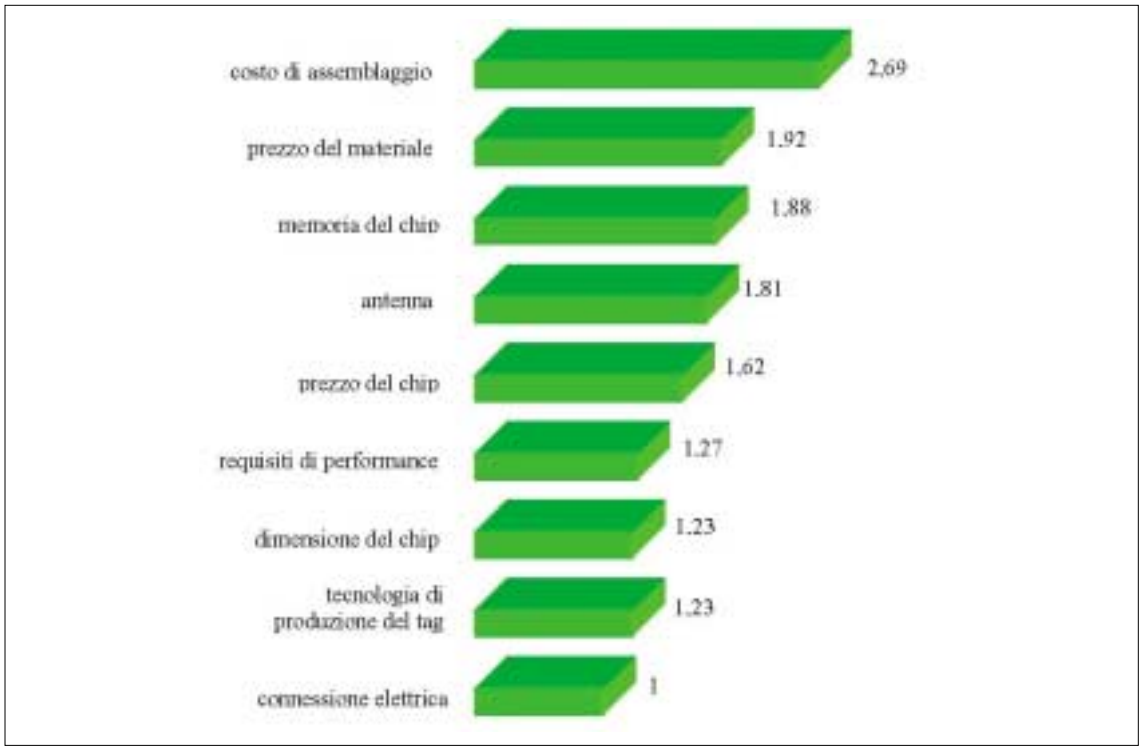

Figura 17 - Principali fattori che influenzano il prezzo del tag
(1 = poco importante, 5 = molto importante)

Va evidenziato che il volume di produzione influenza i prezzi e che il prezzo dei tag scenderà a 5 centesimi solo quando il mercato richiederà 10 miliardi di tag o più. Nei due anni passati, la media degli ordini per tag passivi di sola lettura è stata di 10 milioni di unità, ad un prezzo medio di 0,47 euro per tag. Per valutare le aspettative dei produttori, è sembrato utile indagare anche sulle intenzioni di 10 industrie e di dettaglianti di beni di largo consumo che hanno in corso progetti RFId.
Dall'indagine è emerso che diversi progetti pilota sono in corso e verranno portati avanti nei prossimi anni(vedi figura 18). Alcune organizzazioni pubbliche e private avevano, inizialmente, grandi piani per taggare i singoli articoli, ma hanno abbandonato l'idea a causa dei limiti tecnologici. Quasi tutte le più grandi industrie della grande distribuzione dicono di avere intenzione di applicare l'RFId, e il 60% di queste sta già sviluppando progetti pilota.

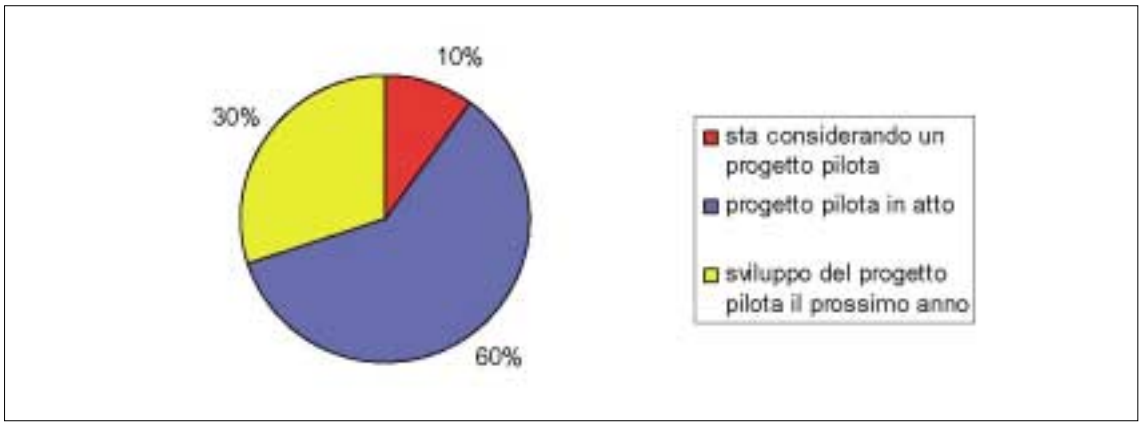

Figura 18 - Pianificazione dell'utilizzo dei tag RFId

Un ulteriore aspetto è quello della scarso impiego delle etichette sui singoli oggetti (vedi figura 19). Il 40% delle aziende pensa di cominciare ad etichettare i singoli articoli tra i due e i sei anni a partire da oggi. Tuttavia, la maggioranza è costituita da imprese che ritengono questa attività piuttosto lontana nel tempo o, addirittura, che non sono certe se l'etichettatura a livello di singolo oggetto verrà da loro mai messa in pratica.

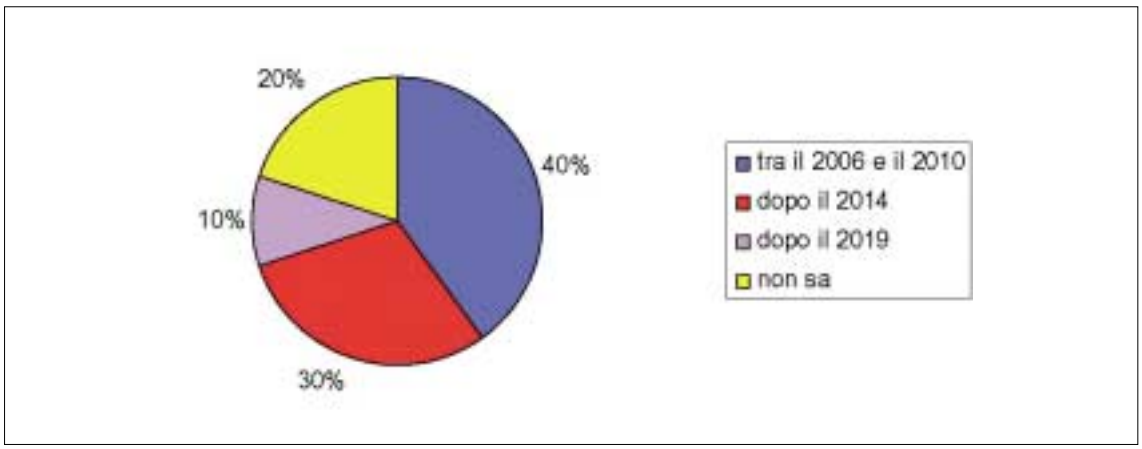

Figura 19 - Etichettatura a livello di singolo prodotto

2.4.3 La previsione del prezzo dei tag RFId

La previsione si basa sulla suddivisione del costo dei tag RFId tra i suoi componenti. Si separano, cioè, i driver di costo tra gli elementi di basso livello come i chip, le antenne, le batterie e il costo di assemblaggio. Basandosi su un trend dei prezzi di 10 anni per le materie prime come silicio, rame e alluminio, si possono estrapolare i prezzi futuri dei materiali fino al 2012. La previsione prende in considerazione anche fattori come il miglioramento delle potenzialità di produzione in settori come le operazioni e i sistemi di fabbricazione, e la gestione dei materiali.
Si assume, inoltre, che ci siano piccoli cambiamenti nella tecnica di produzione dei chip

basati sul silicio. Questa nuova tecnologia aiuta le aziende a posizionare il chip al posto giusto nella fase di assemblaggio, ma non elimina il bisogno di connettere il chip con l'antenna. Dal momento che non ci sono prove che questa rivoluzione tecnologica avverrà, il modello non considera i suoi effetti.
La previsione, infine, esclude gli effetti del ciclo di business sul prezzo dei componenti. I picchi nella domanda dei chip e degli altri componenti, infatti, potrebbero influenzare il prezzo dei tag RFId. Ad esempio, i dati delle industrie mostrano che c'è stato il 30% di capacità produttiva in eccesso nella fabbricazione dei circuiti integrati all'inizio del 2004. Questo implica che un produttore di chip potrebbe incrementare la produzione a costi minimi, con un significativo impatto sul prezzo.
I risultati dell'indagine, mostrano che i tag di Classe 0 e Classe 1 costeranno 0,26 euro nel 2012. Vengono presi in considerazione i tag attualmente più usati il cui costo si aggira intorno agli 0,47 euro e che si stima possa diminuire dell'11% ogni anno (Figura 1.20).

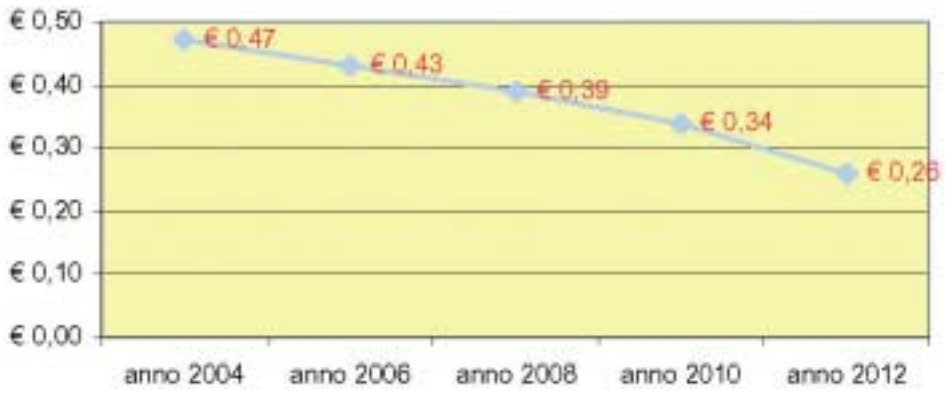

Figura 20 - Previsione del prezzo dei tag Classe 0 e di Classe 1

L'entità della riduzione del prezzo deriva dalla diminuzione del costo dei chip, mentre il costo di assemblaggio rimarrà sostanzialmente lo stesso. A partire dal 2010, al posto delle antenne in rame o alluminio, saranno ampiamente usate antenne stampate più economiche, in modo tale da ridurre il prezzo dei tag del 13%. Il prezzo scenderà del 25% nel 2012, grazie alla capacità dei produttori di chip di aumentare il numero di chip prodotti per wafer.
Nel 2012, i tag di Classe 2 costeranno 0,79 euro. Immagazzinare un numero maggiore di informazioni sul tag, richiede più memoria sul chip, il che porta questo tipo di tag ad essere molto più costosi di quelli di Classe 0 e di Classe 1. Di conseguenza, il loro prezzo non scenderà molto velocemente. Per assicurare che questi tag siano in grado di ricevere e conservare i dati, c'è bisogno, per questa Classe, di un tipo di antenna migliore, il che rende l'intero tag più costoso del 67% rispetto a quelli di Classe 0/1. Il prezzo dei tag di Classe 2 scenderà dell'8% all'anno, ma l'introduzione delle antenne stampate nel 2010 e il miglior sfruttamento dei wafer nel 2012, comporteranno una maggiore riduzione del prezzo.

Figura 21 - Previsione del prezzo dei tag Classe 2

I tag di Classe 4, nel 2012, costeranno 17,14 euro. Il loro costo attuale si aggira intorno ai 24,05 euro l'uno, quindi molto più elevato del costo dei tag di Classe 1/2. La ragione principale di questo prezzo proibitivo è che i tag di Classe 4 sono costruiti per durare diversi anni. Un riutilizzo continuo per un lungo periodo di tempo, rende necessario, per i tag di Classe 4, un involucro robusto: a questo scopo si stima che verranno destinati più di 10 euro (ovvero il 49% del prezzo totale). Nel 2004 l'antenna è risultata venti volte più costosa di un'antenna per un tag di Classe 1, a causa della sua resistenza e del bisogno di un segnale potente per essere in grado di emettere attraverso l'involucro. Gli acquirenti, si aspettano che il prezzo dei tag di Classe 4 scenda del 7% ogni anno, ma i prezzi dipenderanno molto dalle possibilità di utilizzo (Figura 1.22).

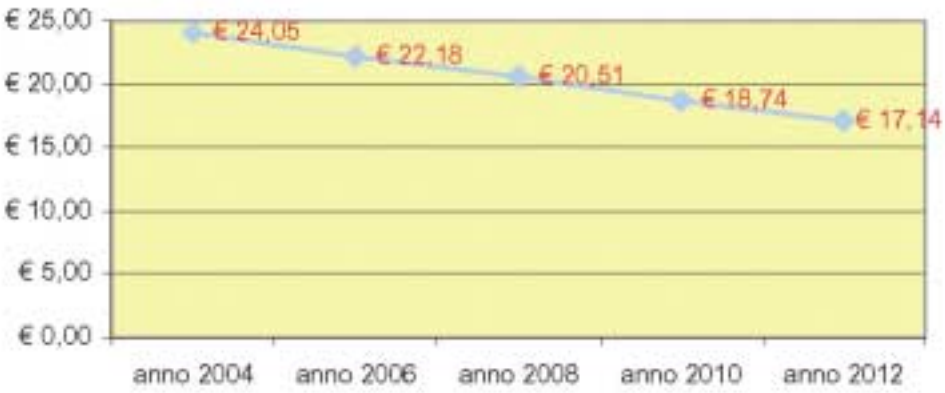

Figura 22 - Previsione del prezzo dei tag di Classe 4

2.4.4 IL MIDDLEWARE RFID

Il middleware gestisce il flusso di dati tra tag, lettori e applicazioni dell'azienda, oltre ad essere responsabile della qualità e quindi della usabilità delle informazioni.
Il mercato del middleware non può essere considerato nuovo, ma, al suo interno, quella del middleware per applicazioni RFId è senza dubbio una nicchia emergente.

Il panorama dei fornitori è tutt'altro che semplice da analizzare: i produttori di middleware stanno nascendo da quattro segmenti chiave, ognuno dei quali ha caratteristiche differenti da mettere in gioco.

PRODUTTORI SPECIALIZZATI DI MIDDLEWARE

I produttori specializzati di middleware presentano un piccolo vantaggio su altri attori del mercato, che consiste nel fatto che essi eseguono la progettazione e l'integrazione di prodotti middleware concepiti per la gestione di volumi di dati notevoli, che sono diretti ad applicazioni riguardanti l'azienda intera.
Le principali funzionalità del middleware RFId sono la raccolta dei dati, l'aggregazione e il filtraggio, oltre all'instradamento. Tuttavia, alcuni prodotti sul mercato presentano delle funzionalità aggiuntive ed estese, come i buffer di dati, la configurazione di eccezioni e il monitoraggio dello stato dei lettori e di altri dispositivi terminali.
Produttori di ERP
La scelta più ovvia, per quegli utenti di tecnologie RFId che hanno investito in un nuovo sistema ERP (o aggiornato una versione precedente), potrebbe essere quella di rivolgersi allo stesso fornitore di ERP per richiedere un middleware RFId.
L'occasione commerciale più grande per i produttori di sistemi ERP scaturisce dal concetto di una piattaforma comune per tutte le applicazioni aziendali con accesso a diversi database e una visione continua dei dati attraverso le applicazioni e attraverso l'azienda. I prodotti per l'integrazione di RFId sono piuttosto nuovi e non sono sperimentati, al di là dell'esperienza del fornitore e dell'affidabilità di un sistema ERP. A volte può capitare che, per ottenere l'integrazione, gli utenti siano costretti a installare qualcosa da soli o a pagare il fornitore di ERP perchè lo faccia. Ad esempio, nel caso in cui un utente decida di installare i lettori in un magazzino o in un centro distribuzione, la scelta migliore potrebbe consistere in un pacchetto middleware di un fornitore ERP. Qualora, però, l'utente desiderasse scambiare i dati RFId con i propri partner commerciali, allora le operazioni RFId in una Supply Chain più aperta potrebbero essere rese più facili con un prodotto middleware indipendente dall'applicazione.

GRANDI INTEGRATORI DI SISTEMA

Un'offerta RFId e i relativi servizi di integrazione e di supporto vengono sviluppati dalla maggior parte dei grandi system integrator.
È indubbio che dare la responsabilità della system integration e dello sviluppo di un sistema RFId ad un partner commerciale affidabile possa agevolare il conseguimento di diversi vantaggi. Infatti, i system integrator che offrono le proprie competenze nell'integrazione dei dati RFId, nella gestione dei progetti e nella riprogettazione dei processi di business (BPR), sono capaci di massimizzare i benefici ottenibili con queste tecnologie. L'esperienza e il know-how industriale hanno pur sempre un costo che molti utenti devono pagare, per ottenere in poco tempo un software RFId e un servizio adeguati, in quanto devono sottostare alle incombenti deadline dei mandati. Deve essere comunque tenuto conto del fatto che non necessariamente la massima esperienza di integrazione coincide con l'esperienza

di sviluppo e integrazione dei dati RFId (nella quale molti di questi fornitori stanno ancora muovendo i primi passi).

PICCOLI INTEGRATORI DI SISTEMA

Diversamente dai grandi integratori di sistema, questi fornitori non presentano di solito un'interfaccia così ampia o una così estesa base di clienti che devono essere serviti. I piccoli system integrator forniscono al cliente un servizio personalizzato e di alto livello e, spesso, costano meno.
Quindi, gli integratori di piccole e medie dimensioni non saranno capaci di eseguire una grande implementazione RFId in decine di siti, anche se con molta probabilità possono rivolgersi con successo ad aziende con progetti RFId più limitati e a quegli utenti che possiedono un numero ristretto di siti in cui implementare dei sistemi RFId.
In conclusione viene riportato lo scenario caratterizzato da diverse possibilità di successo che le imprese interessate ad avventurarsi nel mondo dell'RFId (produttori di componenti o fornitori di servizi) si trovano di fronte.

	SPAZIO PER NUOVE IMPRESE
Tag	Molto poco
Antenne	Buono
Lettori mobili	Medio
Lettori fissi	Medio
Middleware	Buono
Integratori di sistema	Ottimo
Trading di componenti	Buono
Contenitori intelligenti	Ottimo, ma rischioso

Figura 23 - Opportunità per le imprese nel settore RFId

2.5 RFID COME GENERAL PURPOSE TECHNOLOGY

L'implementazione delle tecnologie RFId consente, generalmente, di conseguire diversi vantaggi in termini di risparmio di tempo e di aumento di efficienza. Inoltre, si può notare l'elevato numero di settori ed ambienti cui possono essere applicate queste tecnologie, grazie alle loro caratteristiche peculiari, quali la scarsa invasività e la robustezza.
Le caratteristiche che contraddistinguono la tecnologia RFId posso estendersi a tecnologie di largo impiego definite come : General Purpose Technologies (GPT).

Peculiarità delle General Purpose Technology

Una conoscenza profonda delle tecnologie RFId può consentire di ottenere notevoli benefici nei diversi settori produttivi. Se fosse possibile classificare queste tecnologie in una cate-

goria particolare di innovazioni di cui si conoscono i vantaggi, gli svantaggi e le tempistiche, i benefici citati potrebbero senza dubbio diventare più evidenti.
La categoria che meglio sembra racchiudere le tecnologie RFId sembra essere quella che fa capo alla teoria economica relativa alle General Purpose Technologies. Le GPT portano a profonde modifiche agli equilibri economici globali e sono decisamente rare, basti pensare che è stato possibile identificarne all'incirca una ventina.

LE CARATTERISTICHE DELLE GPT

Le tre caratteristiche principali che denotano le GPT sono la pervasività, il dinamismo e l'esistenza di complementarietà innovative.
Le tecnologie dotate di pervasività presentano funzionalità essenziali per garantire il funzionamento di un esteso segmento di prodotti e sistemi produttivi, dal momento che sono in grado di eseguire varie funzioni generiche, virtualmente applicabili a tutta l'economia.
Il dinamismo è invece la caratteristica che serve a denotare l'evoluzione a cui sono soggette queste tecnologie. Il dinamismo è generato da una spinta continua innovativa e dai miglioramenti ad essa apportati derivanti dall'esperienza e dall'apprendimento.
L'ultima delle caratteristiche distintive delle GPT viene detta "complementarietà innovativa con i settori applicativi" e può essere definita come un legame biunivoco che collega l'evoluzione delle General Purpose Technologies e la convenienza ad innovare di chi la utilizza.
Le "complementarietà innovative" implicano l'esistenza di fenomeni di esternalità verticali e orizzontali.
Le prime consentono di propagare gli effetti legati all'innovazione con maggiore facilità, ma possono anche creare problemi relativi soprattutto all'appropriabilità dei proventi economici oltre al rischio di moral hazard per le due parti. Ad esempio, l'operatore che decide di introdurre la tecnologia (e lo fa con successo), e riesce a renderla determinante in tutta la filiera mediante l'imposizione di uno standard di codifica proprietario, riuscirà a ottenere un controllo pressoché totale sulla stessa filiera.
Le esternalità orizzontali, invece, si ricollegano agli interessi combinati di utilizzatori diversi.
Al crescere del numero di settori applicativi e all'aumentare della consistenza della loro domanda, la tecnologia sarà caratterizzata da uno sviluppo più veloce, data la maggiore intensità dell'impegno in Ricerca e Sviluppo, agevolato da una disponibilità più ampia di fondi.
Come si intuisce dall'esempio precedente, qualora lo standard di codifica non venisse promosso da un singolo soggetto, ma fosse promosso dalla collettività degli operatori di uno stesso settore, ognuno di loro trarrà benefici dall'impiego della tecnologia in tutta la Supply Chain, senza dipendere da terzi clienti, da fornitori o da concorrenti.

LE CRITICITÀ DELLE GPT

È vero che le esternalità sono elementi portanti delle GPT, ma è altrettanto vero che il processo evolutivo e innovativo può risultare frenato dalle problematiche che potrebbero emergere in termini di coordinamento e di tempificazione derivanti dalle stesse esternalità orizzontali e verticali. È ovvio che le istanze provenienti dai vari settori applicativi saranno

differenti per ogni caso preso in esame, sia in termini di prodotto che di tempistica, dal momento che la gamma di tecnologie utilizzate, di mercati serviti e di settori di appartenenza è decisamente vasta.
Le più importanti implicazioni politiche che scaturiscono dalle sopraccitate problematiche sono sostanzialmente due. La prima può esser fatta risalire al concetto di esternalità verticale e si concentra sullo sviluppo di una protezione della proprietà intellettuale che sia adeguata e che allo stesso tempo possa garantire anche la possibilità, per i settori applicativi, di effettuare investimenti complementari. La seconda è, ovviamente, legata alle esternalità orizzontali e ai rischi di free riding, e può essere risolta grazie all'intervento di importanti acquirenti sia privati che pubblici.
Per quanto riguarda i tempi necessari all'affermazione di una tecnologia, se si tratta di una tecnologia in un certo senso rivoluzionaria e profondamente innovativa, si può stimare che essi siano nell'ordine delle decine di anni. Questo è dovuto, innanzitutto, alla necessità di sviluppare adeguati input complementari. Inoltre, se si considera l'eventualità che una nuova tecnologia non venga immediatamente capita e valutata con attenzione, è chiaro che il rischio di un ulteriore dilatamento dei tempi sia più che probabile. Altri aspetti che possono causare dei rallentamenti sono tipicamente legati alle esigenze di evoluzione all'interno delle società clienti e a livello istituzionale.
L'esigenza di valutare e definire con la massima attenzione tutti i meccanismi che regolano l'appropriazione dei risultati economici viene evidenziata dalle caratteristiche complementarietà innovative di queste tecnologie.

L'RFId è una GPT?

Una volta stabilite le peculiarità delle tecnologie RFId e quelle proprie delle GPT, bisogna valutare se le prime possono essere raccolte nella categoria delle seconde. Bisogna cioè valutare se le tecnologie RFId presentano le caratteristiche di pervasività, dinamismo e complementarietà innovativa.
Relativamente alla prima caratteristica, le tecnologie RFId presentano caratteristiche di pervasività in senso ampio, dal momento che possono eseguire alcune funzioni che sono ovunque applicabili nei settori che coinvolgano beni fisici. Per le sue caratteristiche e le sue potenzialità l'RFId può essere utilizzata, come abbiamo avuto modo di evidenziare e come avremo modo di vedere nel seguito, in un numero vastissimo di ambiti applicativi.
Inoltre, è proprio la varietà delle applicazioni disponibili e la flessibilità tipica del sistema che fanno sì che le tecnologie di identificazione a radiofrequenza risultino estremamente utili in un gran numero di settori produttivi, tra cui vanno considerati con particolare attenzione il settore manifatturiero, dei beni di largo consumo, di vendita al dettaglio, dei trasporti, dell'educazione.
Appurata la notevole pervasività delle tecnologie RFId, dovuta principalmente all'applicabilità a qualsiasi settore che preveda le attività di produzione o di gestione di beni fisici, va precisato che se si fa riferimento a un tipo di pervasività "pura", quest'ultima risulta non essere chiaramente una caratteristica di questa innovazione che non può essere utilizzata nelle transazioni in formato esclusivamente digitale.

La seconda caratteristica da verificare, il dinamismo, cioè l'evoluzione a cui le GPT sono sottoposte a causa della continua spinta innovativa, può essere trattata senza dubbi di sorta. Infatti, i sistemi RFId sono soggetti a una continua evoluzione: come abbiamo avuto modo di vedere, dagli anni cinquanta ad oggi hanno subito miglioramenti incredibili e l'attenzione di cui ora godono conduce a sviluppi tecnologici rapidi e significativi. Questa continua evoluzione è resa possibile dai continui miglioramenti nei settori della miniaturizzazione e dei microprocessori, e dagli effetti che scaturiscono dal feedback tra i produttori e gli utilizzatori dei sistemi.

La dimostrazione di esistenza delle complementarietà innovative conduce all'analisi delle esternalità orizzontali e verticali.

Per capire la presenza delle prime è sufficiente porre la propria attenzione sul gran numero di settori e mercati coinvolti dal momento che è importante che un prodotto venduto da un'impresa possa essere identificabile in maniera sicura, veloce, efficace ed efficiente, indipendentemente dalla tipologia.

Le esternalità verticali, invece, sono più difficili da cogliere in modo chiaro e distinto, anche se restano ugualmente piuttosto facili da immaginare.

A parte qualche riserva relativa alle caratteristiche di pervasività delle tecnologie RFId, possiamo considerare dimostrata l'esistenza di tutte e tre le caratteristiche peculiari di una General Purpose Technology. Inoltre è possibile individuare altri importanti elementi che consentono di avvalorare ulteriormente la dimostrazione dell'appartenenza delle tecnologie di identificazione a radiofrequenza alla categoria delle GPT.

Un ulteriore aspetto che sembra ricondurre le tecnologie RFId alla categoria delle GPT è quello per cui una loro implementazione comporta modifiche radicali nell'organizzazione che le adotta. L'identificazione a radiofrequenza, infatti, può servire da spinta e da sostegno per le scelte che un'organizzazione decide di intraprendere a livello strategico.

3. Scenari applicativi RFId

3.1 Introduzione

Molti sono gli scenari applicativi dell'RFId di interesse per l'innovazione dei processi della Pubblica Amministrazione.
Come individuare dei metodi di classificazione di tali applicazioni?
Un contributo in tal senso è offerto dalla Commissione Europea, che ha approfondito dall'inizio dell'anno il tema dell'RFId, pubblicando nella scorsa estate una consultazione pubblica (http://www.RFIdconsultation.eu). L'approccio che viene proposto prende come elemento di classificazione il livello di sensibilità dell'applicazione stessa. La sensibilità è valutata sulla base di due aspetti principali:

- quanto grande sarebbe il danno in caso di errore o di abuso nell'uso dei dati RFId per la specifica applicazione;
- quanto è facile che le cose vadano male a seguito di un abuso o di un guasto del sistema per la specifica applicazione.

Con tale approccio la Commissione Europea intende focalizzare l'attenzione su quegli aspetti critici di privacy che hanno fortemente osteggiato il processo di diffusione della tecnologia RFId negli USA da parte delle associazioni di categoria.
Per valutare le possibili politiche di sicurezza (informatica e privacy) da adottare, vanno analizzati i fattori distintivi che possono determinare il livello di sensibilità del sistema. Tali fattori distintivi sono così suddivisi:

- sistemi chiusi o aperti. In questa classificazione si valuta se il sistema RFId in esame è utilizzato in un ambiente ristretto oppure in un gruppo chiuso di utenti, cioè se il PC o il server che riceve i dati è collegato alla rete, a sua volta collegata ad Internet;
- RFId sempre attivi. In questa classificazione si valuta se i tag RFId che sono utilizzati sono sempre attivi durante tutto il percorso della catena;
- Oggetto dell'identificazione. Questo schema di classificazione suddivide le applicazioni RFId sulla base del fatto che il tag sia utilizzato per identificare cose, animali o persone. In quest'ultimo caso il tag potrebbe sia essere attaccato alla persona stessa, sia a qualche oggetto di appartenenza di una persona (ad esempio il passaporto), in grado di segnalare la presenza e/o la sua identificazione.

Quest'ultimo approccio, basato sull'oggetto dell'identificazione (cose/animali o persone), è comune anche al metodo utilizzato dall'Osservatorio RFId della School of Management

del Politecnico di Milano, che annualmente predispone un resoconto sull'RFId in Italia. Inoltre nel caso delle ricerche da loro condotte sono considerate anche altre variabili, classificando le applicazioni RFId sulla base dei settori di impiego (servizio, manifatturiero, allevamento/agricoltura, etc…), sulla base dello stato di consolidamento di tale applicazione (a regime, sperimentale, futuribile) e sulla base dello sviluppo di questa applicazione.

3.2 UN MODELLO DI CLASSIFICAZIONE PER LA PUBBLICA AMMINISTRAZIONE

A seconda della tipologia di studio che si svolge e delle finalità che ci si pone, sono possibili ulteriori classificazioni. Nella tabella sono proposte alcune categorie che aiutano ad orientarsi tra le diverse applicazioni interessanti per la PA.

		Applicazioni verticali				
		Sanità	**Cultura (Musei, Biblioteche,...)**	**Ambiente Infrastrutture**	**Difesa Forze armate**	**Servizi al Cittadino**
Aree orizzontali	**Supporto attività** (local., accessi, doc.)	Loc. Strumentazione Farmaco-paziente	Info al Visitatore Archivi e Documenti	Tracciabilità alimenti Gestione rifiuti	Armi Doc. classificati	Trasporti Pubblici Biglietteria
	Asset Management (inventario, ...)	Attrezzature, Protesi Farmacia, Sangue	Catalogo museo Biblioteche	Parco auto e attrezzi Animali allevamento	Tracciamento materiali Zona Operativa	Ispezioni Doganali
	Identificazione Autenticazione	Cartella del paziente	Opere "pregiate"	Abilitazione operatori	Accessi/Abilitazioni	Controllo Accessi

Tabella 2 - Categorie di applicazioni

E' importante cercare di prevedere tutte le trasformazioni di processo che sono indotte dall'uso di tecnologie RFId, dato che non è facile prefigurarle semplicemente.
Per esempio l'uso di tecniche RFId aumenta la visibilità e il controllo del prodotto nella catena distributiva.
Ancora la maggiore efficienza in un'area della catena di distribuzione può ridurre le immobilizzazioni di capitale (ad esempio di magazzino) e liberare risorse economiche per altri progetti di investimento (ad esempio differenziazioni).
Con tali strumenti concettuali dovrebbero essere affrontati i progetti RFId, sia quelli di impiego di *tag* passivi HF/UHF al posto dei codici a barre, sia quelli di servizi innovativi (*grid* di localizzazione in interni, anticontraffazione, etc.).
Le applicazioni possono essere ulteriormente classificate, seppur con un certo grado di approssimazione, secondo due criteri:

- il numero di utenti che usufruiscono dell'applicazione o che sono comunque coinvolti nel processo che viene automatizzato per mezzo dell'RFId,

- il grado di fisicità del beni soggetti alla taggatura. Ad esempio i documenti sono intesi a basso grado di fisicità, per la loro "naturale" capacità di trasformarli in beni elettronici.

E' importante fare alcune considerazioni sui benefici che l'adozione della tecnologia RFid può produrre. Va premesso che la valutazione dei benefici può essere stimata induttivamente, vale a dire partendo dallo studio delle applicazioni più largamente usate nel campo industriale o nelle PA degli altri Paesi per valutarne l'applicabilità ed i benefici nel contesto delle PA italiane.
I benefici che le organizzazioni possono conseguire tramite l'adozione della tecnologia RFId sono molteplici: innanzitutto vi sono i benefici di efficienza, che derivano direttamente da un miglioramento della produttività delle risorse o da una riduzione degli effetti della non qualità; in secondo luogo, vi sono i benefici di efficacia, come il miglioramento dell'accuratezza e della tempestività dei processi. I primi sono presenti nella quasi totalità dei progetti e confermano il potenziale di riduzione dei costi delle tecnologie RFId, ma non sempre nell'ambito delle Pubbliche Amministrazioni possono da soli costituire una ragione definitiva verso il processo di adozione. I benefici di efficacia, invece, hanno sempre un peso rilevante, agendo a tutti i livelli ed impattando fattori difficili da valutare in termini di misure economico-finanziarie, come ad esempio il miglioramento della capacità di coordinamento e controllo.
La Figura seguente illustra una classificazione dei benefici ottenibili dalle applicazioni RFId:

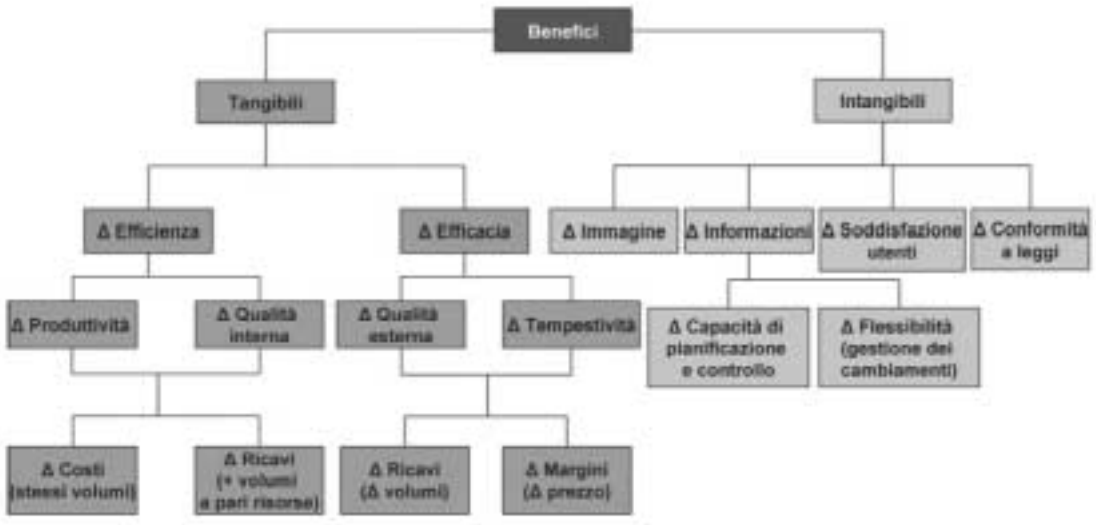

Tabella 3 - Classificazione dei benefici

Due sono i fattori principali che consentono di conseguire benefici di efficienza:

- l'aumento diretto della produttività delle risorse, in particolare di quelle umane;
- l'aumento della qualità dei processi che si traduce in una riduzione delle risorse impegnate a risolvere i problemi della non-qualità.

Questi sono i benefici più facilmente valutabili, anche quantitativamente, e quindi sono solitamente quelli verso cui maggiormente si indirizza l'azione di ricerca e misurazione.
Anche per i benefici tangibili di efficacia si possono individuare due fonti principali:

- l'aumento della qualità esterna;
- aumento della tempestività.

Pur a fronte di una maggior difficoltà di quantificazione e monetizzazione dei benefici, in molti progetti questa categoria di benefici è il reale motore dell'investimento.
Per quanto riguarda i benefici intangibili, essi possono essere classificati in quattro principali categorie:

- benefici riconducibili ad una migliore immagine presso i clienti o gli utenti, e più in generale presso un qualsiasi stakeholder;
- benefici riconducibili ad un aumento della quantità, della qualità e della tempestività dei dati disponibili al management, che consente di rendere più efficace il processo di pianificazione e controllo delle attività e di aumentare la flessibilità nella gestione dei cambiamenti e delle urgenze;
- benefici riconducibili ad una maggiore soddisfazione degli utenti dell'applicazione;
- benefici legati ad una più piena e matura conformità agli obblighi legislativi.

Questa è evidentemente la categoria di benefici più difficile da valutare in termini quantitativi, così da includerli in una valutazione economico-finanziaria. Tuttavia, non è possibile non considerarli perché si finirebbe con l'ostacolare o sottostimare il potenziale di molti progetti RFId, escludendo in molti casi il principale elemento propulsore o comunque una componente rilevante. Ed effettivamente è possibile osservare che la giustificazione all'investimento in molti casi viene in larga parte da un miglioramento delle modalità di lavoro e del controllo sui processi.
E' pertanto essenziale sviluppare modelli ex-ante di valutazione dei benefici, che sappiano cogliere questa multidimensionalità, così da identificare correttamente gli ambiti applicativi prioritari, e guidare nell'allocazione delle risorse disponibili.
Nel seguito, dopo una panoramica sulle principali applicazioni di interesse per la PA, si approfondiscono le applicazioni dell'RFId in ambito bibliotecario, gestione documentale e sanitario per l'identificazione del paziente.
Sono messi in rilievo sia benefici derivanti da ogni caso, che gli aspetti di sicurezza e privacy, nella descrizione di ciascuno scenario, anche se non viene fornita una classificazione delle applicazioni sotto tale profilo.

3.2.1 IDENTIFICAZIONE DEGLI ANIMALI

I sistemi di identificazione degli animali basati su RFId in Italia nascono per la gestione automatizzata delle varie attività di allevamento: dall'alimentazione, all'anagrafe, alla mungitura. Nello specifico sono utilizzati tag a bassa frequenza applicati come marche auricolari o boli alimentari presso gli allevamenti bovini. In particolare per l'identificazione degli animali da compagnia ed ovini/caprini la Commissione europea ha emanati dei regolamenti di seguito riassunti.

Il Regolamento CE n. 998/2003 (art 4, c. 1) ha fissato le condizioni per la movimentazione non commerciale degli animali da compagnia all'interno dell'Unione Europea e ha previsto l'identificazione degli animali mediante microchip.
Il Regolamento CE n. 21/2004 (Allegato A, artt. 4 e 6) per l'identificazione e registrazione degli animali delle specie ovina e caprina ha previsto l'identificazione degli animali mediante microchip.
Rispetto ai metodi utilizzati fino ad oggi per l'identificazione degli animali, con l'applicazione dei tag RFId tutte le informazioni necessarie sono raccolte direttamente "sui" capi di bestiame e, grazie all'emissione di onde elettromagnetiche a bassa frequenza, sono accessibili ovunque si trovi l'animale.
Le etichette RFId possono contenere le informazioni necessarie per garantire la qualità del capo. Alcuni problemi che possono verificarsi con le tecnologie di identificazione tradizionali, come i ritardi nella comunicazione e nell'iscrizione di un capo nella banca dati nazionale, con i sistemi RFId vengono parzialmente limitati, visto che tutte le informazioni possono essere inserite in tempo reale.

Figura 24 - Tracciabilità animale

Per quanto riguarda il resto del mondo, attualmente, esistono delle leggi che regolano l'utilizzo di tag RFId sul bestiame, come ad esempio in Australia, e dei mandati che richiedono di taggare il cibo.
Nel 2003, lo Warrnambool Livestock Exchange è divenuto il primo allevamento che vendeva bestiame e implementava un sistema RFId. Il sistema è stato progettato per aiutare i proprietari di bestiame a conformarsi con lo stringente sistema nazionale di identificazione del bestiame australiano (*National Livestock Identification System*, NLIS). L'NLIS, che è pensato come il più grande e sofisticato sistema di gestione e database di bestiame del mondo, è stato realizzato per soddisfare i requisiti di identificazione e tracciabilità del bestiame posti dall'Unione Europea nel 1999.
La Aleis International ha sviluppato il sistema Aleis MultiRead per l'NLIS. Ogni animale ha un tag auricolare che contiene un chip della Texas Instruments che opera a 134,2 KHz.

Questi tag hanno capacità di lettura e scrittura, e consentono agli allevatori di aggiungere, cambiare o recuperare in tempo reale dettagli relativi a ogni animale, come informazioni sullo stato di salute, l'idoneità al mercato e informazioni commerciali.
Come l'animale si muove attraverso il sistema di pesatura, i lettori installati lungo la linea o all'entrata e all'uscita di esso, leggono i loro tag per identificarli e tracciarne i movimenti. Con questo sistema, più di 3000 capi possono essere registrati ogni giorno, mentre con il precedente era possibile eseguire le stesse operazioni per poche centinaia di animali.

3.2.2 LOGISTICA

Uno dei problemi caratterizzanti le attuali realtà di transito merci, come le frontiera, le zone portuali ed aeroportuali, è l'identificazione delle merci che vengono movimentate, finalizzata alla tracciabilità (e rintracciabilità) interna ed esterna, e alla produzione della documentazione di trasporto. Utilizzando le tradizionali tecnologie di identificazione non è possibile implementare politiche di tracciamento dettagliato delle merci a costi accettabili. Questo obbliga le aziende a limitarsi a tracciare solo le movimentazioni dei lotti.
Sono stati sviluppati sistemi nei quali avviene l'identificazione dei prodotti caricati a bordo di un pallet, consentendo l'identificazione dei singoli colli, ognuno dei quali è dotato di un tag RFId contenente un codice identificativo. Il pallet viene disposto su una rulliera e fatto passare attraverso un varco di rilevazione, capace di eseguire la scansione dei tag e di generare la lista dei prodotti caricati in tempo reale.
L'importanza delle tecnologie RFId, in questo caso è cruciale, dal momento che consente anche l'identificazione delle scatole che sono nascoste alla vista, che non presentano nessun lato verso l'esterno del pallet. L'utilizzo dei diversi sistemi di anticollisione consente di rendere più efficienti le letture, diminuendo i tempi necessari per l'acquisizione delle informazioni in contemporanea.

Figura 25 - Applicazione nella logistica della tecnologia RFId

Tra le attività logistiche più interessanti c'è il controllo delle operazioni di carico e scarico. Grazie ai sistemi RFId è possibile identificare il carico di un mezzo di trasporto, anche se il mezzo dovesse essere in movimento. Un aspetto fondamentale è che non è necessaria la visibilità dei prodotti rispetto al sistema di identificazione impiegato. Le tecnologie RFId trovano proprio in questa qualità il vantaggio maggiore, se poste a confronto con il sistema di identificazione con codice a barre.

3.2.3 CONTROLLO ACCESSI E PRESENZE

L'RFId costituisce una valida alternativa alle tecnologie di identificazione personale tradizionali (come badge e tesserini), e alle tecnologie di *strong authentication* che si basano sul riconoscimento degli attributi biometrici delle persone. Le tecnologie RFId, infatti, non richiedono contatto visivo per l'identificazione e permettono di effettuare un riconoscimento a distanza.
L'identificazione ottenuta con le tecnologie RFId rende più semplice l'impiego di tornelli e varchi motorizzati, consente di distinguere gli ingressi dalle uscite e di verificare l'elenco delle presenze all'interno di una determinata zona in modo completamente automatico. Inoltre, permette l'inizio automatico di una sessione di lavoro, rendendo possibile, ad esempio, l'avvio o l'arresto di un PC a seconda che il proprietario si trovi o meno nei dintorni.
I tag usati in queste applicazioni possono essere stampati o inseriti in oggetti di forma diversa, come ad esempio un badge identificativo. Possono essere, quindi, personalizzati mediante la stampa di immagini, scritte, loghi, fotografie, ecc. Inoltre si possono registrare molte informazioni, tra cui i dati anagrafici, le foto di riconoscimento, la data, l'ora e il verso di transito.
Molte aziende che operano nel campo della sicurezza e del controllo degli accessi hanno deciso di utilizzare le tecnologie RFId nei propri sistemi di sorveglianza perimetrale e di accesso agli edifici, oltre che di controllo dei veicoli che transitano nei parcheggi. Questo è fattibile grazie alla possibilità di montare i tag sul parabrezza delle automobili o di installarli nei portachiavi. I lettori, invece, vengono solitamente inseriti nei muri degli edifici e lungo le vie d'accesso ai parcheggi, all'esterno.

3.2.4 GESTIONE RIFIUTI

La tecnologia RFId viene utilizzata per eseguire in modo efficiente il conteggio degli svuotamenti dei contenitori dei rifiuti in associazione a metodi di tariffazione puntuali. In alcuni casi abbinando l'RFId ad altre tecnologie, quali GPS e metodi di pesatura, si ottimizzano i giri di raccolta degli automezzi. In alcuni casi è stata riorganizzata la modalità di raccolta dei rifiuti, sostituendo i cassonetti stradali di prossimità con la raccolta porta a porta delle diverse tipologie di rifiuti. In ottemperanza al decreto Ronchi del 1997 in alcuni casi i contenitori dei rifiuti indifferenziati sono stati dotati di tag operanti alla frequenza di 125khz il cui codice univoco viene associato al sistema con la matricola del contenitore ed i dati anagrafici dell'utenza. Ogni volta che viene eseguita un'operazione di raccolta l'operatore legge tramite un palmare con lettore RFId il codice del tag. Quando rientra in sede scarica i dati nel

sistema informativo che è così in grado di associare all'utenza i rifiuti prodotti conoscendo il volume del contenitore ad esso associato

3.2.5 LE BIBLIOTECHE

Soluzioni per la gestione delle attività bibliotecarie basate su RFId si stanno diffondendo sempre più. In quanto l'utilizzo dell'RFId consente sia di snellire le operazioni di prestito sia di procedere alle attività di inventario, spesso onerose, senza ricorrere all'interruzione dei servizi bibliotecari. Nel presente paragrafo verrà preso in esame il caso delle biblioteche dell'Università degli Studi di Roma "Tre", che quest'anno ha bandito una gara per l'introduzione della tecnologia. Nel capitolo 7 verrà descritto il caso della Biblioteca Centrale della Facoltà di Economia dell'Università degli Studi di Torino che, in concomitanza con la partecipazione ad un "Gruppo di indagine per l'analisi delle tecnologie RFId nelle biblioteche" attivato dal Sistema Bibliotecario di Ateneo, ha accettato di prestarsi come caso di studio per una ipotesi di applicazione delle tecnologie RFId ad una parte del suo patrimonio librario disposto in scaffali aperti al pubblico, nonché di effettuare una valutazione preliminare all'applicazione tramite il modello di analisi dell'investimento sviluppato dal Politecnico di Milano nell'ambito delle ricerche condotte insieme al CNIPA per comprendere i vantaggi della tecnologia RFId rispetto alla introduzione della tecnologia dei codici a barre. Inoltre si descriverà l'iniziativa danese, conclusasi lo scorso 2005, che ha visto riuniti bibliotecari e fornitori del settore RFId per decidere un modello unico per la codifica dei dati da immagazzinare nelle etichette ad uso bibliotecario.

La biblioteca di Roma Tre

Il progetto dell'Università di Roma Tre prende in esame il sistema per la gestione dell'intero patrimonio librario delle biblioteche delle diverse facoltà di ateneo, per un totale di ca. 400.000 volumi appartenenti a 4 biblioteche dislocate, per adesso, su 11 differenti sedi fisiche. Attualmente di queste 11 sedi 3 svolgono già il prestito automatizzato mediante tecnologie ottiche, 8 sedi invece procedono con prestito non automatizzato. Si stima che nel 2003 le transazioni di prestito automatizzato siano state 7.500 e le transazioni di prestito non automatizzato 44.000.

Il progetto prevede di applicare su ogni documento un'etichetta RFId adesiva di pochi cm quadrati (a seconda del modello scelto) e spessa 0.4 mm ca. Le etichette hanno anche funzione antitaccheggio e sono personalizzabili con il logo della biblioteca. L'adesivo acrilico che verrà utilizzato è stato testato dall'Istituto per la patologia del libro per evitare di danneggiare il libro. Un lettore digitale portatile, leggendo le etichette, agevola le operazioni di verifica dell'esatta collocazione dei volumi, di ricerca di quelli non posizionati correttamente sugli scaffali, di estrazione del materiale richiesto in consultazione o in prestito ed il successivo reinserimento sullo scaffale.

Gli utenti che usufruiranno dei servizi bibliotecari saranno dotati di un tesserino elettronico di riconoscimento. Esso potrebbe coincidere anche con la "carta multifunzione", che è attualmente in fase di progettazione presso l'Ateneo.

La stazione per la gestione del prestito e del rientro effettua la registrazione del prestito o rientro del materiale e contemporaneamente attiva o disattiva la funzione antitaccheggio del microchip del tag. La presenza delle etichette digitali permette di processare contemporaneamente più documenti. La stazione è connessa al sistema informatico della biblioteca e permette la scrittura o la correzione dei dati presenti nelle etichette digitali.
Il progetto prevede anche una stazione automatica di restituzione libri, che è una struttura simile alle postazioni bancomat. Permette la restituzione permanente del materiale preso in prestito. Tale stazione viene installata su uno dei muri perimetrali dell'edificio che ospita la biblioteca e funziona senza la presenza di personale. 24 ore su 24 e 365 giorni l'anno l'utente può riporre nella buca di restituzione il materiale da consegnare, dopo essersi identificato con il proprio tesserino. L'apparecchiatura ritira i libri, automaticamente li riconosce e li divide a seconda del luogo dove dovranno essere poi ricollocati, rilasciando all'utente la ricevuta dell'avvenuta restituzione.
Con il bando di gara emanato l'Amministrazione intende acquisire etichette, lettori digitali portatili, antenne per varchi antitaccheggio, tessere per utenti, stazioni di gestione prestito e restituzione, stazioni di autoprestito necessari per il completamento dell'automazione del servizio prestito nel Sistema bibliotecario dell'Università Roma Tre, tutti basati su tecnologia a radiofrequenza, preservando altresì la compatibilità con il software attualmente in uso per la gestione della biblioteca. L'aggiornamento del sistema informativo e dei moduli web viene realizzato direttamente dall'Amministrazione.
Le scelte tecnologiche per la soluzione RFId di automatizzazione delle biblioteche si sono orientate verso tag passivi utilizzando la frequenza di 13,56 MHz, in considerazione del basso costo, della velocità medio/alta (ca. 106/kbps) scrivibili per 2 Kb e con funzioni antitaccheggio. Tale area di memoria, diversamente da quanto accade nelle tecnologie ottiche, è riscrivibile ed utilizzabile per applicazioni future.
Le caratteristiche tecniche individuate dall'Ateneo per questo progetto sono sintetizzate di seguito.
Per ciò che concerne i sistemi a microchip, dovranno essere rispettate le specifiche di cui allo standard ISO 15693 previsto per i transponder RFId ed allo standard ISO/IEC 18000 per la comunicazione radio (parte 1 e parte 3, ovvero parte 1 e parte 7, per la comunicazione a 13,56 MHz e 433 MHz rispettivamente). Le suddette specifiche valgono per tutte le tipologie di microchip oggetto della fornitura (etichette per materiale librario, per materiale multimediale, per tessere utenti). Per quanto concerne i sistemi di controllo degli accessi/antitaccheggio ovvero i lettori portatili basati sulla tecnologia RFId, questi dovranno aderire allo standard ISO 15693 per ciò che concerne gli apparati riceventi ed allo standard ISO/IEC 18000 per la comunicazione radio (parte 1 e parte 3, ovvero parte 1 e parte 7, per la comunicazione a 13,56 MHz e 433 MHz rispettivamente). Relativamente ai sistemi di gestione del prestito, ovvero di autoprestito, dovranno, per la parte relativa all'identificazione (del materiale librario e/o multimediale oggetto del prestito ovvero dell'utente), essere conformi alle direttive ISO 15693 associate ai sistemi riceventi ed allo standard ISO/IEC 18000 per la

comunicazione radio (parte 1 e parte 3, ovvero parte 1 e parte 7, per la comunicazione a 13,56 MHz e 433 MHz rispettivamente).
Con questa iniziativa l'Ateneo di Roma Tre intende aumentare l'efficienza dei propri servizi, nelle diverse fasi delle attività bibliotecarie, oltre che nell'utilizzo della struttura da parte degli utenti finali. In particolare il sistema consentirà la verifica della disponibilità del materiale da remoto, permettendo all'utente finale di effettuare una prenotazione on-line se il materiale è in prestito a un altro utente, con evidenti vantaggi per studenti disabili o lavoratori.
Inoltre, l'automazione del sistema velocizzerà la verifica della presenza del materiale, senza costringere l'operatore a recarsi fisicamente in magazzino.
Nella fase di prestito, l'utilizzo della tecnologia RFId in modalità integrata consente il controllo dei dati utente (verifica dell'identità, privilegi e restrizioni a seconda della tipologia utente, del numero di volumi già in prestito, delle eventuali sanzioni), oltre che dei dati sul materiale (se è prestabile o meno). L'utente che si reca in biblioteca è consapevole di trovare il materiale prenotato, azzerando così le risposte negative. La registrazione dell'avvenuta transazione e l'emissione della ricevuta di prestito, avvenendo in modo automatico, costituiscono un ulteriore fattore di snellimento delle procedure bibliotecarie. Nella fase di rinnovo del prestito l'utente può effettuare il rinnovo via web, purché il materiale non sia stato prenotato da altri utenti. I solleciti e le eventuali sanzioni sono rilevati automaticamente permettendo così di contattare con sistemi tradizionali (lettera, telefonata) o in alternativa con invio automatico di e-mail di sollecito all'utente in difetto.
Il sistema consentirà delle statistiche periodiche sulla circolazione del materiale utili al miglioramento del servizio e alla politica degli acquisti. Gli utenti da remoto potranno autonomamente verificare la lista storica delle proprie transazioni (libri in prestito, da restituire, restituiti, prenotati).

3.2.6 IL PROGETTO BRIDGE DELLA UE

I sesto programma quadro per la Ricerca e lo Sviluppo Tecnologico della comunità europea si è arricchito nel luglio scorso con il progetto triennale BRIDGE (Building Radio frequencies IDentification solution for Global Environment) di 10 milioni di euro. Al progetto partecipano 31 soggetti, comprese alcune università, anche cinesi, aziende e PMI. Secondo il coordinatore di progetto[13] "RFId non è ancora la panacea per una più efficiente catena distributiva, ma la partecipazione di soggetti complementari, industriali e di ricerca, sarà la chiave del successo".
Obiettivo del progetto è lo sviluppo di un sistema di tracciamento completo per la definizione di un e-pedigree. La Figura 26 mostra un esempio di risultato ottenuto anche senza l'uso di RFId, quale sottolineatura che la prevalenza della sola tecnologia a radio frequenza è ancora tutt'altro che scontata.

[13] H. Bartel, direttore tecnico di EPCglobal

Figura 26 - Esempio di e-pedigree (Data Matrix) operante insieme con il barcode

Il progetto è la risposta europea alla FDA, che ha individuato le RFId come le tecnologie più promettenti per il tracciamento e per la lotta alla contraffazione.

3.2.7 LE ESPERIENZE ESTERE

In Danimarca lo scorso anno si sono concluse le attività del Gruppo di Lavoro sui modelli di dati RFId da utilizzarsi nelle biblioteche. Al Gruppo di lavoro hanno partecipato sia rappresentanti delle biblioteche, sia rappresentanti dei diversi fornitori di tecnologia. I risultati, pubblicati nel 2005, dettagliano il modello dati definendone gli elementi, la struttura, la codifica ed i valori di riferimento. Ulteriori approfondimenti sono disponibili al sito:
http://www.bibliotheca-RFId.com/docs/dokumente/Datenmodell.pdf
Il modello fornisce delle indicazioni sui quattro aspetti che sono stati ritenuti fondamentali:

- i dati, cioè le informazioni che devono essere presentate e per quale scopo;
- i valori e gli intervalli di definizione di tali valori;
- la codifica dei tag RFId, che rappresenta un lavoro delicato, in quanto lo spazio disponibile nel tag è abbastanza limitato per tag di prezzo basso;
- la mappatura fisica delle informazioni sul tag, in quanto il gdl ha riscontrato attraverso dei test che la variazione di questo aspetto può influenzare l'efficienza nella lettura.

Gli esperimenti condotti hanno fornito interessanti indicazioni anche sul numero di libri che si possono leggere al secondo in dipendenza della dimensione dello spazio di memoria. Il numero di libri che si riescono a leggere nell'unità di tempo, come è naturale aspettarsi, è inversamente proporzionale al dimensione della memoria. Altri test, inoltre, hanno correlato la percentuale di successo nella lettura alla dimensione dell'area di memoria, dimostrando come al diminuire della dimensione della memoria la percentuale di successo aumenta.

3.2.8 IDENTIFICAZIONE E TRACCIAMENTO DEI DOCUMENTI CARTACEI CON GESTIONE DEGLI ARCHIVI

L'ottimizzazione nel trattamento dei documenti rappresenta un punto di interesse cruciale per ogni Pubblica Amministrazione che si trovi a gestire grandi moli di incartamenti. La

gestione documentale digitale, che consente la consultazione del materiale in formato elettronico, risolve molte delle problematiche. Recenti normative nazionali vanno in questa direzione ma la necessità di documenti cartacei rimane comunque fondamentale in molti ambiti e lo rimarrà probabilmente per molti anni ancora.

Da queste considerazioni è nata un'applicazione per l'identificazione, il tracciamento e la gestione degli archivi cartacei, oggi in via di sperimentazione presso gli uffici amministrativi dell'Università di Messina. La soluzione sviluppata, personalizzabile in funzione delle necessità dell'utenza, ha l'obiettivo di adottare una strategia mista di gestione, legando la "vita virtuale" del documento in formato elettronico con quella reale, grazie all'utilizzo della tecnologia RFId. Particolare attenzione è stata rivolta alla usabilità del sistema e alla sua integrazione con le procedure ed i sistemi in uso.

Il sistema realizzato consente innanzitutto di mappare la struttura degli uffici (stanze, scrivanie, armadi, scaffalature etc.) nel relativo corrispondente digitale attraverso i sensori a radiofrequenza e i reader RFId. Una volta effettuata la mappatura il sistema consente di definire una gerarchia di figure che possono accedere alla gestione documentale con vari livelli di permessi, di visibilità e di possibilità. Questa gerarchia rispetta a pieno l'organigramma della struttura amministrativa (Capo Area, Capo Settore, Capo Ufficio, Responsabile del Procedimento etc.). Ciascuno avrà accesso ai dati di propria competenza e potrà agire su di essi secondo le proprie responsabilità.

L'architettura del sistema prevede un ufficio protocollo che si occupa di acquisire il documento, di registrarlo sul sistema digitale associandovi le informazioni generali (mittente, destinatario, data ed ora di arrivo, etc.), di associarvi una etichetta RFId e di inoltrarlo all'ufficio o all'area di competenza. Successivamente la documentazione cartacea giunge all'ufficio o all'area di competenza ed è in questa fase che il documento viene classificato in maniera più specifica assegnando alla pratica un workflow definito dal responsabile dell'area. Sempre in questa fase può essere definito un responsabile del documento che sarà informato, attraverso un servizio di messaggistica interno al sistema, di tutti i movimenti che la pratica compirà nel suo iter.

In abbinamento al sistema di identificazione e tracciamento dei documenti è stato realizzato un sistema per la loro gestione dal momento in cui vengono archiviati, sistema che consente di regolamentare, controllare e registrare il prelievo o l'immissione dei documenti negli archivi da parte del personale per avere, in tempo reale, la localizzazione di ciascun documento.

I principali benefici del sistema sono legati al minore impatto di problematiche come lo smarrimento o la difficile reperibilità dei documenti all'interno della struttura di competenza con una conseguente riduzione dei tempi dedicati alla ricerca di fascicoli. Altro vantaggio è la riduzione drastica di errori nel workflow che possono generare, all'interno di una Pubblica Amministrazione, ritardo nei tempi di gestione e impossibilità di stabilire il tempo di disbrigo delle pratiche. Il sistema consente in particolare di fornire servizi quali:

- tracciabilità fino al livello di scrivania o scaffale;
- visualizzazione dello stato di lavorazione del documento;

- sistema di messaggistica integrato fra gli utenti coinvolti nella gestione di ciascuna pratica;
- avvisi multicanale (e-mail, messaggistica, sms, vocale) di eventi quali errore o anomalia nel percorso o rimozione non autorizzata;
- gestione dei tempi di lavorazione e delle priorità delle pratiche;
- localizzazione in tempo reale dei documenti archiviati in appositi armadi.

Per rispondere al bisogno di una maggiore efficienza della soluzione in esame, i documenti cartacei devono essere riposti all'interno di dispositivi quali:

- vaschette porta documenti RFId collocate sulle scrivanie degli addetti agli uffici;
- armadi RFId dotati di antenne integrate.

L'architettura del sistema è a tre livelli: Database Server, Application Server e applicazioni Client. Il sistema è costituito da due applicazioni Client, una per postazioni PC e una per dispositivi mobili. Nell'Application Server è integrato un modulo middleware, per ottimizzare le prestazioni dell'applicativo e consentire l'alta personalizzazione delle funzioni sulla base delle esigenze. Il modulo è stato realizzato utilizzando le tecnologie che rappresentano ad oggi lo stato dell'arte per quanto concerne le architetture e le infrastrutture di comunicazione quali Service Oriented Architecture (WS, REST, HTTP), Enterprise Service Bus (XMPP, JMS), Multichannel Comunication (Jabber, VoIP, SMS, MMS).

3.2.9 IDENTIFICAZIONE CESPITI E ASSET MANAGEMENT

La gestione di asset in realtà estese e dinamiche come le Pubbliche Amministrazioni rappresenta un'attività complessa, con tempi lunghi di gestione e con processi che, se resi in parte automatizzati, possono portare ad una maggiore accuratezza dei dati e ad un risparmio economico.
Da questa considerazione è nato un applicativo basato su tecnologia RFId che consente di ottenere un inventario sempre aggiornato degli asset, organizzato secondo le specifiche del committente (edificio, piano, stanza...) ed un conseguente utilizzo più efficiente.
Questo applicativo, grazie alla tecnologia RFId, con la "taggatura" degli asset coinvolti, consente di:

- localizzare le attrezzature con la possibilità di avere una mappa, anche grafica, della presenza di ogni asset nelle singole stanze;
- analizzarne gli spostamenti tenendo traccia delle precedenti ubicazioni di ogni bene;
- ottimizzare le risorse effettuando statistiche sui beni che sono stati maggiormente soggetti a manutenzione (ad esempio gli asset it);
- automatizzare la registrazione di eventi che riguardano la gestione degli asset, generalmente inseriti manualmente;
- introdurre un ulteriore elemento per la sicurezza, riducendo la possibilità di furti.

Con questo applicativo le operazioni di inventario vengono effettuata da un operatore che, dotato di un reader RFId, periodicamente compie un giro di perlustrazione degli edi-

fici rilevando i tag apposti su ciascun asset. Le operazioni di inventario in questo modo sono rese:

- più agevoli: l'etichetta classica di identificazione è spesso collocata in posizioni di difficile lettura;
- più precise: l'utilizzo di un dispositivo elettronico per raccogliere i dati elimina gli errori di trascrizione dei serial numbers;
- più veloci: per l'operazione di inventario non sarà più necessario avvicinarsi ad ogni bene, dopo averne localizzato visivamente la presenza nella stanza, per trascriverne il serial number. Perché il dispositivo mobile rilevi la presenza dei tag associati ad ogni asset e la colleghi alla stanza in cui si trovano, sarà infatti sufficiente che l'operatore entri ed esca, anche molto velocemente, dalla stanza.

La collocazione di un varco RFId (costituito da due antenne in corrispondenza di ogni tornello di entrata/uscita dagli edifici coinvolti) può rendere più complete le operazioni di inventario, raccogliendo dati relativi alla presenza/assenza degli asset rilevando in tempo reale eventuali sottrazioni indebite.
L'integrazione dell'applicativo con i più diffusi sistemi per la gestione degli interventi tecnici sugli asset IT permette inoltre di integrare e gestire, con un'unica interfaccia utente, le informazioni sull'identità del bene e sulla sua localizzazione insieme a quelle relative al suo ciclo di vita.
Le principale funzionalità messe a disposizione da questa applicazione sono:

- inventario sia in modalità on-line che off-line;
- ricerca di asset all'interno degli edifici;
- gestione rapida degli interventi di manutenzione;
- visualizzazione in mobilità di informazioni presenti sul sistema di asset management.

3.2.10 APPLICAZIONI OSPEDALIERE

Numerose sono le applicazioni della tecnologia RFId in ambito ospedaliero, si va dall'accoppiamento farmaco-paziente al tracciamento degli apparati elettromedicali, dal tracciamento delle protesi sanitarie all'identificazione delle sacche di sangue. Numerosi progetti pilota, ed applicazioni reali sono ormai attive in tutto il mondo, ed anche in Italia l'ambito ospedaliero è stato uno dei più ricettivi all'introduzione di queste nuove tecnologie, ad esempio ricordiamo i casi del Pronto Soccorso dell'AO Ospedale Circolo Fondazione Macchi di Varese, del l'Ospedale San Raffaele di Milano e dell'Azienda Sanitaria Ulss 6 di Vicenza, che analizzeremo in dettaglio nel paragrafo successivo.

Azienda Sanitaria Ulss 6

Di seguito viene descritto il progetto basato su tecnologia RFId in uso presso l'Azienda Sanitaria Ulss 6 di Vicenza. L'applicazione che è stata sviluppata supporta in modalità automatica il processo di identificazione dei pazienti. Il progetto nasce dall'obiettivo di assicurare una corretta identificazione del paziente ed ottimizzazione dei tempi del processo d'iden-

tificazione. Tale applicazione è stata integrata all'interno dei processi di gestione della terapia farmacologia, anche in considerazione del fatto che l'Ulss 6 di Vicenza è una delle strutture coinvolte nel progetto promosso dalla Regione Veneto per la gestione informatizzata della terapia farmacologica.
La soluzione implementata con il progetto regionale prevede la rilevazione del trattamento farmacologico sul singolo paziente ospedaliero tramite l'utilizzo di dispositivi wireless (tabletPC, portatili o palmari) durante la normale attività di reparto. L'Ulss 6 di Vicenza con il supporto dei propri partner tecnologici ha implementato all'interno del progetto regionale un sistema di identificazione del paziente basato su RFId.
Il personale medico e/o infermieristico che accoglie il paziente in reparto al momento del ricovero, consulta l'anagrafica aziendale, contenente i dati che il paziente ha fornito in accettazione e li associa ad un identificativo posto su un tag RFId collocato sul braccialetto che viene consegnato a ciascun paziente ricoverato. Il paziente, indossato il proprio braccialetto, viene accompagnato al letto di degenza.
Nella fase di prescrizione della terapia il medico si avvicina, con un Tablet PC, al letto dell'ammalato e lo identifica leggendo il tag sul braccialetto elettronico indossato dal paziente. La prescrizione farmacologica viene effettuata dal medico sullo stesso tablet PC collegato via wireless al sistema centrale, dove sono immagazzinati i dati di tutti i ricoverati.
La fase di somministrazione è di competenza del personale infermieristico. L'infermiere durante il giro di somministrazione identifica nuovamente il paziente leggendo il tag RFId posto sul braccialetto elettronico con il Tablet PC, effettua la somministrazione dei farmaci e registra sullo stesso tablet PC l'operazione. Le informazioni vengono, quindi, trasmesse per il tramite del collegamento radio al sistema centrale. Finito il giro delle somministrazioni l'infermiere riporta eventuali variazioni registrate in sede di somministrazione nel campo 'note' sul tablet PC. Nel caso specifico il sistema, oltre a garantire un'efficiente uso delle informazioni di identificazione del paziente, consente anche di elaborare dei dati che costituiscono l'input per altri sistemi, quali:

- gestione del magazzino. Le informazioni sui farmaci somministrati e sui farmaci prescritti, consentono di conoscere in tempo reale le necessità del magazzino di reparto e del magazzino centrale, favorendo così un approvvigionamento equilibrato delle scorte.
- osservatorio regionale sul farmaco. Fra gli obiettivi dell'osservatorio regionale del farmaco vi è lo studio dei comportamenti prescrittivi ed il calcolo dell'incidenza del costo del farmaco su DRG (Diagnosis Related Groups o "Raggruppamenti Omogenei di Diagnosi", ROD è un sistema per la classificazione dei pazienti dimessi dagli ospedali per acuti. Tale sistema si fonda appunto sulla classificazione delle malattie, associate ad un numero progressivo che va da 0 a 492, e raggruppate in macrocategorie omogenee di diagnosi. Il raggruppamento in macrocategorie viene effettuato sulla base del consumo di risorse, della durata della degenza e del profilo clinico che le singole malattie richiedono, in modo tale che ciascuna macrocategoria contenga un gruppo di malattie che prevede un impiego omogeneo di queste variabili).

I tag posti all'interno dei braccialetti sono passivi a 13,56 Mhz, ISO 15693. I reader sono delle compact flash che vengono integrate nel tablet PC. La informazioni sul paziente e

sulla cura farmacologia prescritta e somministrata sono raccolte attraverso PC portatili o tablet PC connessi alla LAN attraverso una rete wireless, realizzata con access point distribuiti nei reparti. Alla stessa LAN sono connessi i server su cui sono raccolte le informazioni. Per l'analisi del progetto e per la fase di progettazione è stato impiegato circa un mese. Concluse queste due fasi sono stati avviati dei test di funzionamento della piattaforma che si sono protratti per circa un mese e mezzo. Nel contempo, però, è partita la fase di formazione e gestione del cambiamento, rivolta prevalentemente al personale infermieristico (per la fase di accettazione del paziente) ed al personale infermieristico/medico (per la parte di aggiornamento dati ed applicazione farmacologia). L'obiettivo è di terminare la messa in produzione dei reparti pilota per luglio 2006 e procedere nel 2007 con l'estensione all'intera azienda

Con l'informatizzazione dell'identificazione del paziente mediante RFId l'ULSS 6 di Vicenza mira al raggiungimento dei seguenti obiettivi:

- efficacia, cioè corretta identificazione del paziente e corretta trascrizione delle informazioni che identificano (es.nome e cognome, codice fiscale etc.) o che sono proprie del paziente (es. allergie, gruppo sanguigno etc.). Poiché tutte queste informazioni sono inserite una sola volta nel sistema, i possibili errori di trascrizione sono ridotti al minimo;
- efficienza, cioè ottimizzazione dei tempi di identificazione. In fase di identificazione nei processi di prescrizione o di somministrazione della terapia farmacologica il personale di reparto non deve digitare nulla per richiamare la scheda terapeutica del paziente, perché dal braccialetto viene letto in automatico l'identificativo univoco del paziente. Il personale medico e infermieristico non deve digitare o selezionare alcuna informazione: per identificare il paziente per cui eseguire una prescrizione o una somministrazione è sufficiente che venga avvicinato il tablet PC su cui è installata una scheda flash per la lettura del tag RFId inserito nel braccialetto.

Una stima dei benefici in termini economici va valutata considerando i costi di ciascuna delle singole componenti:

- implementazione hardware e software,
- gestione braccialetto,
- materiali di consumo,
- manutenzione del sistema.

Tale stima va rapportata alla riduzione dei tempi impiegati dal personale medico e infermieristico per svolgere le medesime operazioni, a seguito dell'ottimizzazione dei processi e della lora automazione. Da una stima compiuta presso l'Ulss 6 di Vicenza risulta che, per un reparto di 25 pazienti, il tempo risparmiato dal personale medico e infermieristico in un anno è pari a circa 150 ore (questo nell'ipotesi della prescrizione informatizzata).

L'utilizzo dell'RFId nell'identificazione dei pazienti all'interno dei processi di gestione della terapia farmacologica ha delle ulteriori potenzialità. Nel braccialetto del paziente possono essere memorizzate diverse informazioni, come ad esempio allergie, gruppo sanguigno,

patologia, reparto di appartenenza, etc. Nel braccialetto le informazioni possono essere memorizzate in modo incrementale, es. il gruppo sanguigno del paziente può non essere noto in fase di accettazione, ma può essere disponibile a seguito di esami etc. Le informazioni memorizzate nel braccialetto possono essere utilizzate in alcuni processi per eseguire dei controlli, es. in fase di prescrizione l'informazione sulle allergie potrebbe essere utilizzata per verificare la prescrizione di alcune specialità farmacologiche
Un altro campo di sviluppo che l'identificazione dei pazienti può aprire riguarda la gestione prestazione e referti. In fase di prescrizione di prestazioni l'identificazione del paziente potrebbe essere fatta leggendo il braccialetto del paziente (come per la prescrizione e la somministrazione della terapia farmacologica). Analoga estensione può essere applicata al processo di gestione degli esami di laboratorio. In caso di richiesta di esami di laboratorio le provette potrebbero essere dotate di tag RFId per realizzare l'accoppiamento provetta paziente. Un altro importante campo applicativo riguarda la gestione degli emocomponenti. In caso di trasfusione il paziente potrebbe essere identificato e verificata la corrispondenza tra sacca e paziente con sistemi RFId.

3.3 CONCLUSIONI

Le applicazioni per la Pubblica Amministrazioni che utilizzano l'RFId quando comportano anche un cambiamento del processo riescono realmente ad innovare il sistema. L'adozione delle tecnologie RFId dipende molto dal campo d'applicazione, dalla creazione degli standard e dal successo e dall'influenza di chi li ha già adottati.

4. Standard e Regolamentazione

4.1 Standard

4.1.1 Premessa

RFId è "solo" una tecnologia: la vera innovazione nella Pubblica Amministrazione potrà avvenire solo attraverso la profonda revisione dei processi (dalla logistica, ai sistemi di pagamento, ai sistemi d'accesso, ecc.)
D'altro canto l'innovazione avviene tanto più rapidamente quanto più si aderisce agli standard aperti : senza standard non sarebbe nata Internet, non si sarebbe sviluppata un'innovazione diffusa per la quale comunicare e scambiarsi informazioni è una condizione indispensabile.
Con la tecnologia RFId si potrà realizzare "l'Internet delle cose", i flussi di dati e le informazioni saranno, in termini quantitativi, di diversi ordini di grandezza maggiori rispetto ad oggi.
L'evoluzione degli standard relativi alla tecnologia e l'aderenza ad essi sarà una condizione essenziale da parte della Pubbliche Amministrazioni che si accingono ad affrontare progetti nell'area RFId. Il successo di tali iniziative è fortemente dipendente dalla capacità di rendere interoperabili diverse banche dati e dalla usabilità delle informazioni che se ne potranno ricavare.
La scelta dei prodotti e dei partner con i quali sviluppare progetti nell'area RFId dovrà tenere in debito conto l'aderenza agli standard in vigore e la capacità da parte delle aziende di definire e realizzare progetti che si sviluppino in modo organico rispetto ad essi.

4.1.2 Il valore degli standard

Lo sviluppo di iniziative collettive si basa sulla definizione di standard condivisi dai maggiori operatori sul mercato ed allo stesso tempo la incentiva. Gli standard consolidati hanno sempre rassicurato i clienti sul fatto che le scelte di implementazione fatte minimizzassero i rischi tecnologici.
Tuttavia la standardizzazione, per sua stessa natura, non può essere la soluzione ottimale per tutte le applicazioni perchè rappresenta un intelligente compromesso tra costi e prestazioni. Quindi è senza dubbio vero che la maggior parte delle applicazioni beneficia dalla copertura di uno standard, ma è altrettanto vero che il compromesso prestazionale può diventare un vincolo alla realizzazione di un progetto.

4.1.3 I PRINCIPALI STANDARD RFID

Parecchi organismi di standardizzazione sono coinvolti nel processo di definizione di specifici standard tecnologici ed applicativi per l'RFId al fine di assicurare una piena corrispondenza tra prestazioni ed interoperabilità dei sistemi. A questo proposito è bene specificare subito come l'RFId sia un mondo alquanto variegato, composto da molteplici tecnologie, caratterizzate non solo dalla diversità di frequenze ma, in primo luogo, dalla diversità dell'ambito di applicazione. E' proprio guardando l'ambito di applicazione che si osserva un primo elemento di interesse. Alcuni ambiti applicativi, come ad esempio l'utilizzo delle carte di prossimità per il controllo accessi, per il ticketing nel trasporto persone o per l'identificazione di animali, sono pienamente standardizzati (si vedano rispettivamente lo standard ISO 15693, lo standard Calypso, e ancora gli standard ISO 117984/5 e 14223 per l'identificazione animale). Non a caso, in questi ambiti il consolidamento dello standard ha accelerato la diffusione delle applicazioni, al punto che, queste applicazioni possono definirsi pienamente consolidate. Altri ambiti applicativi, invece, e primo tra questi l'applicazione di tag sui beni di largo consumo, non sono ancora arrivati ad uno standard consolidato, cosa questa che ne sta condizionando il processo di adozione. Concentrandosi quindi su questo secondo ambito, quello su cui si focalizza anche la reale attenzione del business e dei media quando si parla di "problematica standard", è opportuno presentare in dettaglio gli standard che si affrontano in questa arena, ovvero lo standard ISO/IEC e quello EPC.
Prima di fare questo, è bene precisare alcuni aspetti logici comuni sia a ISO che a EPC. In primo luogo, parlando di RFId, si possono individuare quattro diverse aree di standardizzazione:

- gli standard di tecnologia – descrivono le basi tecniche di un sistema RFId, definendo frequenze, velocità di trasmissione, tempistiche, codifiche, protocolli e sistemi di anticollisione, e mirano ad assicurare la compatibilità e/o inteoperabilità nei sistemi prodotti da diversi fornitori;
- standard di dati – si occupano degli accordi sul modo in cui i dati sono strutturati per i requisiti di compatibilità ed interoperabilità. Di conseguenza questi standard descrivono diversi aspetti dell'organizzazione dei dati e sono per lo più indipendenti dalla tecnologia;
- gli standard di applicazione – si occupano di definire l'architettura di una soluzione tecnica rivolta a specifiche applicazioni o per un settore di applicazioni, soluzione all'interno della quale viene poi scelta la soluzione più adatta;
- standard di conformità – si occupano degli accordi e definiscono il modo in cui i sistemi devono comportarsi per essere considerati rispondenti a particolari performance o a test di verifica operativi.

Relativamente a questo quadro, ISO ed EPC sis distanziano soprattutto nella seconda e nella terza area.

4.1.3.1 LO STANDARD ISO

L'ISO ("the International Organization for Standardization"), che è l'organo ufficiale mondiale di standardizzazione, è fortemente coinvolto nella definizione di standard per l'RFId.
L'ISO è composto da un numero molto grande di comitati che sono dedicati alla standardizzazione di una specifica area. Un comitato ISO ha a sua volta una struttura di tipo gerarchico che prevede dall'alto in basso i seguenti livelli :

1) Joint Technical Committee (JTC o JT);
2) Subcommiteees (SC);
3) Workgroups (WG);
4) Subgroups o Task Force (SG/TF)

I sistemi RFId dipendono direttamente dall'area denominate Information Technology a cui si riferisce il JTC1.
L'ISO e l'IEC("Commissione Eletrronica Internazionale) patrocinano insieme il JTC1 per discutere gli argomenti di interesse di entrambe le organizzazioni. Il sottogruppo ISO responsabile per l'identificazione automatica e la raccolta dati (Automatic Identification and Data Capture) è denominato SC31
Di seguito si espone una tabella con i principali standard ISO sull'RFId, già esistenti o in fase di realizzazione, strutturati per sottocomitati SC e per zone di sviluppo :

Sottocomitati	**Standard ISO**
	SC17 Integrated Circuit(s) Cards
ISO 7816	IC Cards with contacts
ISO 10536	Close coupling cards
ISO 14443	Proximity Cards
ISO 15693	Vicinity Cards
ISO 10373	Test methods
	SC19 Animal Identification
ISO 117984/5	Code Structure and Technical Concept
ISO 14223	Advanced Trasponders
	SC31 Item Management
ISO 10374	Freight containers
ISO 15960	Application requirements transaction message profiles
ISO 15961	For item management-data objects
ISO 15962	RFId for item management, data notation
ISO 15963	Unique Identification of RFTag registration Authority to Manage the Uniqueness
ISO 18000	Air interface standards

Per ulteriori dettagli sugli standard ISO si rinvia a documenti specializzati.

4.1.3.2 ELECTRONIC PRODUCT CODE (EPC)

Il progetto EPC (Electronic Product Code) è nato alcuni anni fa grazie agli studi di un gruppo di ricerca del M.I.T. (Boston), denominato Auto-ID Center, che ha visto il contributo di quasi cento fra le più importanti aziende del mondo nel campo della produzione di beni di consumo, della loro distribuzione e della produzione di tecnologia RFId. Nel corso 2003 il progetto ha visto una svolta particolarmente significativa: l'acquisizione della proprietà intellettuale di EPC da parte di EAN International e UCC e l'avvio di una nuova società, EPC Global, nata come joint venture fra EAN International e Uniform Code Council. In questo modo EPC è diventato il particolare sistema RFId che il mondo EAN propone di utilizzare per il trasporto delle informazioni.
Lo standard EPC non definisce solo il tipo di veicolo di identificazione ma anche le tecnologie di rete necessarie per garantire la tracciabilità di questi prodotti lungo la supply chain.

4.1.3.3 OBJECT NAME SERVICE (ONS)

L'ONS è una rete globale aperta per la rintracciabilità delle merci e fornisce l'infrastruttura complementare alla memorizzazione dei dati, dal momento che il trasponder memorizza esclusivamente l'EPC. L'Object Name Service è il legame tra il prodotto "taggato" ed il luogo di memorizzazione delle informazioni relative a quel prodotto. L'Object Name Server presenta funzionalità di networking analoghe al DNS (Domain Name Server): sulla base del codice EPC ricevuto, fornisce l'indirizzo del sistema sul quale risiedono le informazioni relative al prodotto.

4.1.3.4 EPC INFORMATION SERVICE (EPCIS)

Questo standard è progettato per aiutare i produttori a utilizzare la tecnologia RFId in modo da ridurre il sovraccarico di informazioni e ricevere dalla supply chain le informazioni specifiche indispensabili per fruire in maniera innovativa i dati relativi ai prodotti.
Nella figura seguente si intuisce cosa potrebbe accadere al crescere del numero delle banche dati, delle interfacce e delle applicazioni.
Non è un caso che le maggiori aziende del settore aderiscano all'EPCglobal EPCIS Working Group, gruppo di lavoro che ha come obiettivo quello di definire interfacce comuni per il software RFId in grado di porre le aziende nella condizione di scambiare e utilizzare i dati RFId indipendentemente dall'applicazione con la quale sono stati creati o archiviati.
Per le aziende operanti lungo tutte le fasi della supply chain, ciò significa avere la possibilità di acquisire in maniera conveniente grandi volumi di dati dettagliati a ogni livello della supply chain e di condividerli facilmente con i propri partner. Si può intuire facilmente dalla figura seguente l'importanza dell'adozione dello standard Electronic Product Code Information Service (EPCIS) per lo scambio e la consultazione dei dati memorizzati nei tag RFId.

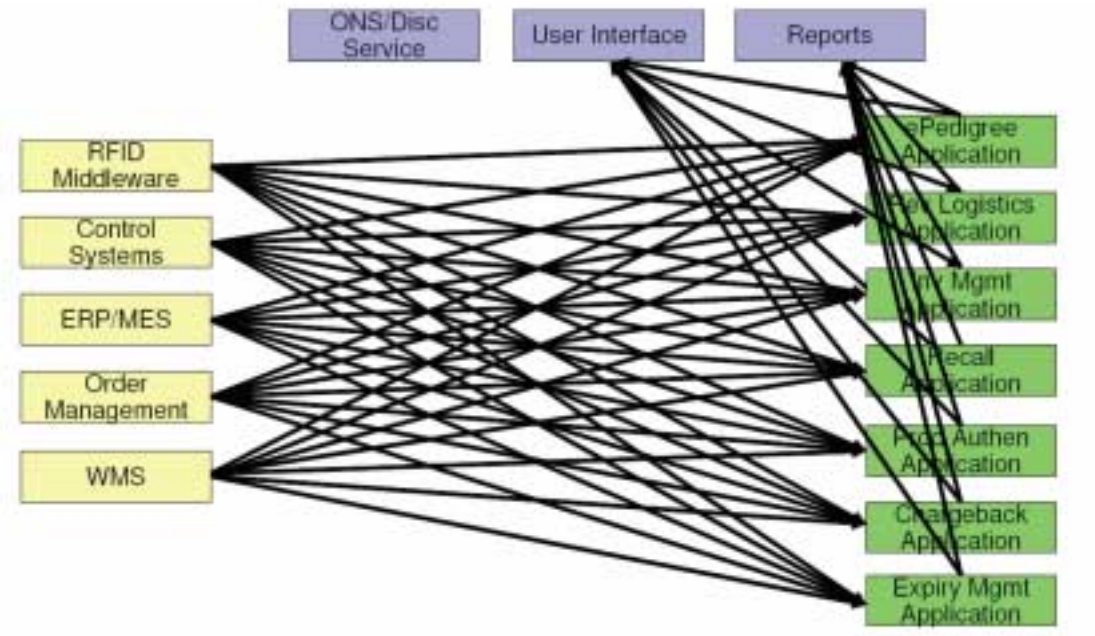

Figura 27 - Aumento del numero delle banche dati, interfacce e applicazioni.

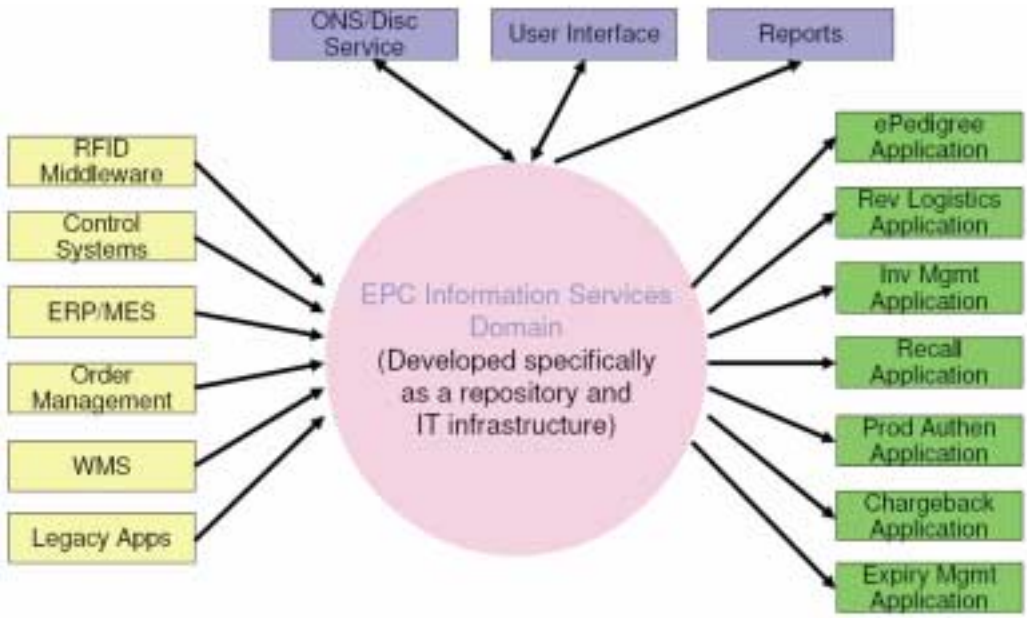

Figura 28 - Standard EPiCS (Electronic Product Code Information Service)

EPICS è quindi il "repository" degli eventi RFId basati sullo standard EPCglobal.
Mediante il Physical Markup Language (PML), vengono descritti gli oggetti fisici, i prodotti e le informazioni al contorno. PML può ad esempio descrivere informazioni costanti, come ad esempio numeri EPC, identificativo del lettore (EPC lettore) e dati barcode, informazioni dinamiche, quali dati di sensori come ad esempio la temperatura di trasporto e temporali,

come la location in cui è transitato il prodotto e l'orario certificato. PML si basa sul diffuso linguaggio XML. Insieme ad EPC ed ONS, PML costituisce la base per la connessione automatica delle informazioni al prodotto fisico. EPC identifica il prodotto, PML lo descrive ed ONS collega i due componenti.

4.1.3.5 SAVANT

Savant è una tecnologia software per la gestione e l'effettiva distribuzione dei dati EPC nelle reti. Savant utilizza un'architettura distribuita, ovvero può girare su un solo computer centrale oppure su diversi computer di una stessa organizzazione. Savant gestisce quindi il flusso delle informazioni del network EPC.
Con Savant si intendono dunque le tecnologie di smistamento, sviluppate su reti nazionali, regionali e locali, le cui terminazioni sono costituite dai lettori RFId, che lavorano nei magazzini, negozi, depositi. Questa tecnologia è costituita da tre moduli : EMS (Event Management System), RIED (real-Time In Memory Data Capture), e TMS (Task Management System). Questi moduli assicurano funzioni e compiti di acquisizione di informazioni, di smistamento, di filtraggio, raccolta e conteggio dei numeri di traspnder, preelaborazione dati, controllo dei lettori, interfaccia ai sensori ed interfaccia ai programmi utente.

4.2 REGOLAMENTAZIONE

Se nella prima fase di sviluppo, si potevano accettare delle soluzioni tecniche cosiddette proprietarie, le applicazioni multi-utente che si prospettano oggi richiedono al contrario delle soluzioni standardizzate, le sole che possono permettere l'interoperabilità dei diversi sistemi proposti dai diversi fornitori di soluzioni, e quindi utilizzabili dalla generalità degli utenti in qualsiasi parte del mondo.
Considerando la globalizzazione dell'economia questa interoperabilità è una necessità assoluta. E, oltretutto, non appena saranno pubblicati in toto questi standard o norme internazionali, anche coloro che utilizzano sistemi in ambiente chiuso potranno avvalersi di questa stessa interoperabilità, per mettere in atto delle opportune dinamiche di concorrenza. La posta in gioco di queste norme è quindi mondiale e pone i lavori della normalizzazione al centro del dibattito attuale sul futuro della RFId. Tutte le ricerche dimostrano che l'assenza di standard è stata uno dei motivi delle incertezze dei potenziali utenti. Ma già oggi, grazie alla significativa opera degli attori della normalizzazione, innanzitutto dell'ISO (International Standard Organization), si possono avere sistemi veramente interoperabili. Le varie frequenze di lavoro sono individuate da organismi internazionali (CEPT - ETSI), che fissano delle regole molto precise per l'utilizzo sia delle frequenze che delle potenze da utilizzare. La tecnologia RFId non può quindi prescindere da queste regolamentazioni, che sono parte integrante dell'ambiente in cui essa opera.
Per questo tipo di applicazioni non esiste una normativa internazionale a livello di Radio Regolamento (UIT) in quanto l'attribuzione delle frequenze per questo tipo di applicazioni

ricade sotto le sovranità nazionali e dipende dagli organismi di gestione dello spettro sovranazionali (CEPT/Commissione Europea). La regolamentazione europea si sviluppa secondo due differenti livelli:

- Raccomandazioni CEPT le cui decisioni non sono vincolanti per i Paesi membri.
- Direttive della Commissione Europea, le cui Decisioni sono vincolanti per i Paesi Membri U.E. e la loro mancata attuazione è soggetta alla procedura di infrazione e conseguenti sanzioni economiche.

È quindi sempre necessario, per ciascun utente, verificare che i prodotti che sta utilizzando rispettino le leggi in vigore. Per semplificare, si potrà dire che i suddetti organismi stabiliscono la frequenza o la banda di frequenza (come nel caso dell'UHF), la potenza di emissione, e il tempo massimo di comunicazione fra etichette e lettori.
Per quanto concerne la potenza RF, conviene precisare che questo termine può dar adito ad una confusione, poiché vi sono diversi tipi di accoppiamento fra etichetta e lettore, a seconda del tipo di frequenza. Per frequenze fino a 13,56 MHz, si tratta di un accoppiamento induttivo, e si dice che il sistema funziona in 'campo vicino'. Si parlerà quindi di intensità massima di campo (H-Field), che si esprime in dBμA/m (decibel-microampère al metro).
Nelle altre frequenze (UHF) l'accoppiamento è elettromagnetico, e si dice che funzioni in 'campo lontano'. Si parlerà allora di potenza massima di emissione, esprimendo tale potenza in Watt. L'unità della potenza RF in Watt può essere espressa sia in e.r.p. (Effective Radiated Power, riferito al dipolo a onda) che in e.i.r.p. (Equivalent Isotropic Radiated Power, riferito ad una antenna isotropica) e dipendono dal tipo di antenna utilizzato. Il rapporto fra le due unità è il seguente: 1 W e.r.p. = 1,62 W e.i.r.p.. Di conseguenza, quando si confrontano i livelli massimi autorizzati in queste due regioni, bisognerebbe utilizzare la stessa unità. Così facendo i 2 Watt e.r.p. autorizzati dalla nuova norma europea di cui parleremo più avanti, corrispondono in realtà a 2 x1,62 cioè a 3,24 Watt e.i.r.p..
La differenza fondamentale tra gli apparati di tipo induttivo (HF/VHF) e quelli con accoppiamento di tipo elettromagnetico operanti in banda UHF consiste nel fatto che nei primi i TAG sono di tipo attivo, nei secondi sono invece di tipo passivo. In particolare nei sistemi UHF l'energia per l'invio del segnale viene fornita ai TAG dal lettore per cui è necessario un livello di potenza RF molto più elevato (fino a 2 W e.r.p.).
In figura è mostrato quanto stabilito da raccomandazione ETSI EN 302 208-1 V1.1.1 (2004-09)
Nella Normativa Europea ed Internazionale gli apparati RFId rientrano nella categoria degli Short Range Devices (SRD) ovvero apparati a corto raggio, apparati radioelettrici destinati ad operare su frequenze collettive, senza diritto a protezione e su base di non interferenza ad altri servizi, per collegamenti a breve distanza (PNRF d.M. 8 luglio 2002). La raccomandazione della CEPT ERC/REC 70-03 stabilisce i requisiti tecnici e regolamentari per l'uso armonizzato degli Short Range Devices (SRD) tra i paesi appartenenti alla CEPT (Conferenza Europea delle Amministrazioni delle Poste e Telecomunicazioni). La raccomandazione viene gestita in ambito CEPT dallo Short Range Devices Maintenance Group (SRD/MG), che dipende dal Working Group FM (Frequency Management). La raccomandazione della

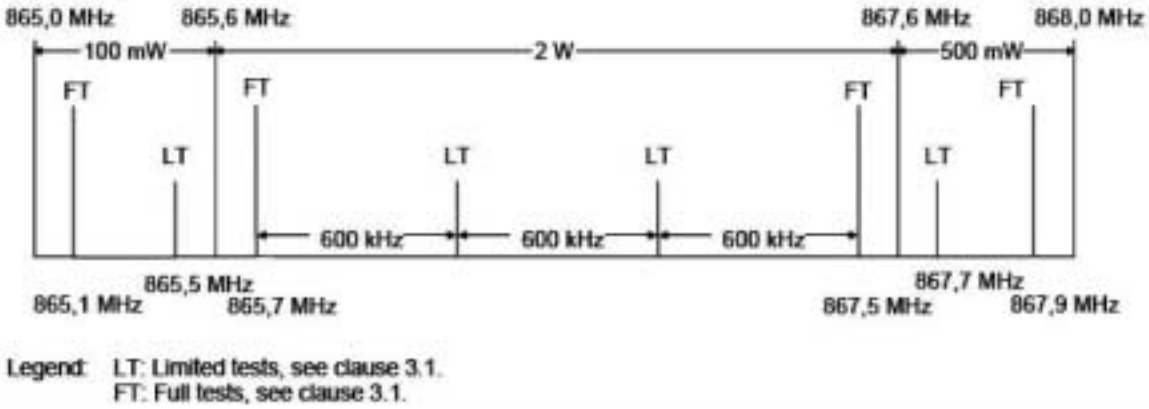

Figura 29 - Frequenze ETSI EN 302 208-1 V1.1.1

CEPT ERC/REC è suddivisa in 13 Annessi, di cui al punto 9 e 11 interessano le applicazioni RFId. L'annesso 9 copre le bande di frequenze e regolamenta i parametri primari per le applicazioni induttive incluso per esempio gli immobilizzatori per autovetture, identificazione di animali, sistemi di allarme, rilevamento di cavi, gestione di materiali, identificazione di persone, controllo accessi, lettori e sensori di prossimità, sistemi antitaccheggio a radiofrequenza ed a induzione, identificazione automatica di articoli, sistemi di controllo senza fili e pagamento stradale automatico. E' da notare che altri tipi di sistemi antifurto possono operare in conformità con altri annessi pertinenti.
Punti fondamentali della CEPT ERC/REC 70-03 a.9 sono:

- f1: 13,553 .13,567MHz per RFId e EAS (Electronic Article Surveillance) only
- Intensity of magnetic field: 60 dBµA/m at 10 m
- Duty cycle: No Restriction
- Channel spacing: No spacing
- Harmonised Standards: EN 300 330

In accordo con tale normativa le bande di frequenze 9-148,5 KHz, 148,5-1600 KHz, 3,155-3,400 KHz, 6,765-6,795 KHz, 7,400-8,800 KHz, 10,200-11,000 KHz, 13,553-13,567 KHz, 26,957-27,283 KHz possono essere impiegate ad uso collettivo da apparati a corto raggio per applicazioni di tipo induttivo aventi le caratteristiche tecniche della raccomandazione.
L'annesso 11 copre le bande di frequenze e regolamenta i parametri primari per applicazioni di identificazione a radiofrequenza (RFId) incluso per esempio sistemi di allarme, di tracciabilità, gestione di materiali, identificazione di persone, controllo accessi, lettori e sensori di prossimità, sistemi antifurto, sistemi di collocazione, trasferimento dati ad apparati portatili e sistemi di controllo senza fili. E' da notare che altri tipi di sistemi RFId possono operare in conformità con altri annessi pertinenti. La banda tra 2446-2454 MHz non è utilizzata in Italia a causa delle applicazioni WAS/R-LAN: 2400-2483,5 MHz 100 mW EIRP (SRD-Annesso 3), Ponti radio privati: 2300-2440 MHz (diritto d'uso delle frequenze), Reti fisse analogiche per il trasporto di segnale audio.

Punti fondamentali della CEPT ERC/REC 70-03 a.11, che individuano tre bande con relativi limiti, sono:

- b1: 865 -868 MHz; b2: 865,6 -867,6 MHz; b3: 865,6 -868 MHz
- Power: b1: 100 mW ERP; b2: 2W ERP; b3: 500mW ERP
- Duty cycle: LBT
- Channel spacing: 200 kHz
- Harmonised Standard: EN 302 208

La banda 865-868 MHz, in accordo al PNRF, è in gestione al Ministero della Difesa ed impiegata per esigenze militari e di polizia connesse con la sicurezza nazionale. A seguito di coordinamento tra il Ministero delle Comunicazioni ed il Ministero della Difesa, porzioni della banda in questione sono attualmente utilizzate per altre applicazioni di debole potenza, ma con potenza massima di 25 mW e.r.p.. La banda 865-868 MHz non è utilizzabile in Italia per applicazioni RFId con potenza superiore a 25 mW e.r.p. (fig 2.42), il Ministero della Difesa non ha dato il proprio consenso a causa del fatto che dispositivi con potenza irradiata più elevata potrebbero compromettere la regolare funzionalità delle applicazioni militari. Pur tuttavia, recentemente vi è stato un cambiamento che ha portato il Ministero della Difesa ad autorizzare l'avvio di una sperimentazione nella banda 865,6÷867,6 MHz, di applicazioni RFId aventi le caratteristiche tecniche dell'Annesso 11 della ERC/REC 70-03 (Università di Parma). Lo scopo è quello di verificare la compatibilità tra le applicazioni RFId ed i servizi del Ministero della Difesa; in particolare si vuole esaminare la possibilità di autorizzare le applicazioni RFId almeno per l'uso indoor, prevedendo di assoggettare tali applicazioni al regime di autorizzazione generale e non di libero uso, ai sensi del Codice delle Comunicazioni. Va però sottolineato come la recente decisione della Commissione Europea (23 novembre 2006) sulla armonizzazione dello spettro radio riguardante proprio la citata EN 302 208 apre la strada alla liberalizzazione delle "selective frequence".
Altre restrizioni sono imposte per il rispetto di normative sulla salute pubblica RTTE 99/05/CE, compatibilità elettromagnetica, privacy ecc. Queste sono soltanto alcune delle normative oggi in vigore, citate per poter far capire come anche restrizioni di utilizzo di una certa frequenza, piuttosto che un'altra, possono orientare lo sviluppo di una tecnologia (ad esempio 13,56 MHz) rispetto ad altre che per certi aspetti talvolta potrebbero essere preferibili.
Gli apparati operanti nelle bande di frequenze di cui all'Annesso 9 e all'Annesso 11 della Rec CEPT 70/03, ai fini della loro immissione sul mercato e del loro utilizzo sul territorio nazionale, devono essere conformi alla Direttiva 99/5/CE, recepita in Italia con il d.lgs. del 09/05/2001, n° 269. In particolare, relativamente all'applicazione del d.lgs. (art 6.4) di cui sopra, il responsabile dell'immissione sul mercato degli apparati di cui trattasi, deve notificare al Ministero delle Comunicazioni, almeno 4 settimane prima, l'intenzione di immettere sul mercato italiano gli apparati medesimi.
La scheda di notifica può essere scaricata dal sito internet del Ministero delle Comunicazioni www.comunicazioni.it.

5. RFId e Privacy

5.1 Premessa

Lo sviluppo delle nuove tecnologie informatiche e la miniaturizzazione dei componenti elettronici hanno accelerato in modo determinante le dinamiche infrastrutturali dell'attuale sistema economico-sociale, rendendo lo scambio di informazioni sempre più semplificato ed economico.
In questo contesto, l'impiego e la progressiva diffusione di sistemi basati sulla identificazione a radiofrequenza (RFId) possono ulteriormente contribuire ad introdurre fattori evolutivi di notevole rilevanza. Tuttavia, come spesso avviene quando si è in presenza di un'accelerazione del processo di innovazione dovuta all'immissione sul mercato di più recenti tecnologie, questi sistemi destano qualche perplessità in quanto sono in grado di trattare informazioni molto specifiche rispetto alla vita privata e sociale di un individuo.
Infatti, non sempre è possibile delimitare il perimetro di propagazione delle informazioni trattate dai dispositivi impiegati e per questo motivo si sente in modo sempre più evidente l'esigenza di una regolamentazione nell'adozione dei sistemi RFId.
Sul piano pratico non si sono registrati casi importanti di infrazioni delle norme in materia di protezione dei dati personali tali da far pensare all'approssimarsi di scenari preoccupanti ma, la questione della compatibilità dei sistemi RFId con le tematiche di sicurezza e riservatezza del trattamento dei dati personali, è senza dubbio l'aspetto più delicato connesso allo sviluppo e alla diffusione di questo tipo di tecnologie, in quanto potrebbe rappresentare una vera e propria barriera al loro impiego su larga scala.
Il pericolo di un abuso delle tecnologie RFId per la creazione di database che raccolgono informazioni sulle abitudini alimentari, sui gusti in termini di abbigliamento o sugli orientamenti politici che potrebbero emergere dalle pubblicazioni acquistate, è legato essenzialmente al fatto che il confine che separa una pratica di questo tipo da una ricerca di mercato è più sottile di quel che si pensi.
Per delimitare il perimetro d'azione dei sistemi RFId che possono essere impiegati nella realtà di tutti i giorni, che sia il posto di lavoro, la catena produttiva, lo spostamento di merci e persone, l'interesse del Garante per la protezione dei dati personali è sicuramente necessario, dal momento che le attuali norme che stabiliscono l'obbligo di garantire l'anonimato al cliente e il consenso informato per i dati raccolti, nel caso dei sistemi RFId, potrebbero non essere così efficaci.

Finora, la via che si è seguita è quella di fornire delle indicazioni "privacy-compatibili" alla tecnologia, poiché una cosa è fornire delle regole sull'impiego della tecnologia, altra cosa è statuire come la tecnologia debba essere costruita utilizzando parametri non in conflitto con il diritto alla riservatezza del dato personale.
Diversamente, cioè in assenza di strumenti regolatori che rendano possibile la convivenza senza conflitti del binomio RFId-Privacy, si delineerebbe uno scenario di applicazione eccessivamente invasivo della sfera personale del soggetto interessato che, potrebbe tradursi nel monitoraggio dello svolgimento della vita privata, sociale e/o commerciale del soggetto interessato, sia esso, a seconda dei casi, cittadino o impresa.
In altre parole, occorre domandarsi se, con la trasformazione dei processi produttivi dovuta all'impiego delle nuove tecnologie, ci si muova nella direzione di integrare e migliorare i processi attuali attraverso il contributo delle tecnologie RFId, oppure nella direzione di stravolgere i processi nella logica di sfruttamento delle piene capacità funzionali che le dette tecnologie sono in grado di offrire, rifluendo così in una sorta di deriva tecnologica sull'onda delle spinte del mercato.

5.2 IL PROBLEMA DELLA PRIVACY NEI PROGETTI PILOTA

Il grande risalto dato alle problematiche della riservatezza del dato personale è dovuto ad alcuni progetti pilota che sono stati promossi a livello internazionale soprattutto nel mondo della grande distribuzione e dalle relative manifestazioni portate avanti da alcune organizzazioni di consumatori, come ad esempio l'americana C.A.S.P.I.A.N. (Consumer Against Supermarket Privacy Invasion and Numbering).
In questi casi è stato evidenziato come i timori legati al mancato rispetto della privacy nei casi di applicazioni RFId siano dovuti soprattutto alla possibilità che i dispositivi di identificazione a radiofrequenza non si disattivino in modo automatico (o quasi) una volta che il cliente abbia lasciato il perimetro del negozio, come invece viene dichiarato dalle aziende che producono tag. Nel caso di mancata disattivazione, tali dispositivi, ad esempio, consentirebbero infatti di tenere traccia degli spostamenti di una persona, soprattutto nel caso in cui quest'ultima abbia utilizzato per l'acquisto una carta di credito o uno strumento analogo, che permetta di associare le informazioni identificative del singolo oggetto etichettato col tag a una determinato individuo.
L'allarme per la privacy non è, quindi, legato solo al fatto che si possa venire a sapere che cosa è stato acquistato da una certa persona, ed il luogo in cui è avvenuto l'acquisto dal momento che il problema è analogo a quello che si pone in innumerevoli altri casi che vanno dalla carta di credito stessa, al semplice scontrino, al codice a barre, ma piuttosto al fatto che essendo il tag un tracciatore di un preciso prodotto, se questo viene associato a un determinato soggetto, diviene anche tracciatore degli spostamenti di quest'ultimo.
Abbiamo visto prima come sia facile associare un tag ai dati identificativi, giacché è sufficiente che il prodotto al quale esso è applicato venga acquistato con un mezzo che implichi l'utilizzo di dati personali (le carte di credito e i bancomat sono gli esempi più diffusi).

Altri scenari negativi che sono stati ipotizzati dalle varie associazioni di consumatori sono, ad esempio, quelli in cui i lettori posti sugli scaffali, dovessero registrare la rimozione di un determinato articolo, con la possibilità di scattare una fotografia di colui che ne prelevi una quantità superiore ad un numero predeterminato; o il caso in cui i tag presenti sulle banconote potrebbero segnalare a un rapinatore chi sta trasportando grandi quantitativi di denaro ed agire di conseguenza.

Uno dei principali aspetti legati ai problemi di privacy che possono derivare dalle applicazioni RFId oltre alla identificabilità ed alla tracciabilità, è la profilabilità.

Quest'ultima consiste in un sistema in grado di fornire, per ogni singolo soggetto, informazioni riguardanti il comportamento attuale e quello atteso, favorendo la produzione di dati preziosi per le analisi di mercato.

Un ulteriore importante aspetto riguarda la sicurezza del dato personale trattato attraverso l'utilizzo della tecnologia RFId.

Uno dei maggiori problemi della sicurezza con i tag RFId, legati alla specifiche ISO 15693, sta nel fatto che si tratta di sistemi promiscui, ovvero che rispondono a qualsiasi lettore tenti di interrogarli. Questo non avviene nel caso di utilizzo di tag RFId che rispondono alle specifiche ISO 14443, che interagiscono esclusivamente con i lettori autorizzati ad interrogarli.

In ogni caso per risolvere i problemi legati anche ai tag ISO 15693, i creatori dello standard EPC hanno messo a punto un comando speciale chiamato "kill": inviando tale comando a un tag quest'ultimo viene "ucciso". In linea teorica, un tag così disattivato non rappresenta più una minaccia sul piano della privacy e, per questo motivo, da molte associazioni di consumatori viene invocata una legge che obblighi i commercianti a rimuovere o disattivare tutti i tag RFId prima che gli articoli a cui sono stati assegnati lascino il negozio.

Secondo alcuni analisti, la disattivazione dei tag genererebbe diversi problemi: sebbene, grazie alla loro disabilitazione si eliminerebbe ogni preoccupazione legata alla privacy, verrebbero a mancare anche i benefici che un'azienda o una pubblica amministrazione potrebbero ottenere con l'uso di tali soluzioni. Ad esempio, disattivando tutti i tag, una volta che i prodotti siano stati acquistati, non sarà possibile tracciare le eventuali restituzioni, compromettendo uno degli scenari più interessanti per gli operatori dell'elettronica di consumo. Potrebbe essere complicato agire anche nella ipotesi in cui debbano essere rintracciati prodotti che mettono a rischio la salute dei consumatori.

È anche importante evidenziare come molti aspetti critici legati alla problematica della privacy scaturiscano dal fatto che l'individuazione dei tag e dei lettori può essere resa piuttosto difficile.

I tag, infatti, possono essere integrati nell'imballaggio delle merci, posti in luoghi inaccessibili all'interno degli oggetti, cuciti nelle stoffe, inseriti fra strati di carta, fusi nella plastica, stampati su supporti eterogenei, senza dimenticare l'esistenza dei chipless tag che, come abbiamo avuto modo di spiegare nel Capitolo 1, consistono in sottili fibre metalliche incorporate nelle fibre della carta capaci di riflettere l'onda elettromagnetica verso il lettore "risonando" a determinate frequenze.

Figura 30 - Un disattivatore di tag

La difficile identificazione, anche nel caso dei lettori, è legata al fatto che essi possono essere molto ben nascosti, ad esempio in mura di edifici, nei pavimenti, nei tappeti, nei mobili, nei veicoli in movimento o nelle strade.
Alcuni esperti, però, sostengono che i tag non possono essere letti a distanza sufficiente per realizzare un'efficace azione di sorveglianza. A tale affermazione altri replicano ricordando che esistono tag attivi che possono essere letti a grandi distanze e che è possibile che ci sia l'interesse a sorvegliare aree anche molto circoscritte.

5.3 APPROCCI TECNOLOGICI

Le soluzioni tecnologiche al problema sono molteplici.
Tra le più interessanti ci sono i cosiddetti blocker tags, semplici dispositivi RFId passivi, simili per costo e forma ai tipici tag RFId. Un blocker tag, ovviamente, presenta anche delle funzioni peculiari: quando un lettore tenta la lettura di tag RFId che sono contrassegnati come "privati", un blocker tag blocca il lettore. Più precisamente, i blocker tag vengono disposti sopra un tag RFId, o comunque interposti tra il tag e il lettore, e "ingannano" il protocollo di comunicazione dal tag verso il lettore in modo che il lettore percepisca miliardi di tag inesistenti e, quindi, va in stallo.
I tag RFId possiedono un bit speciale che serve a distinguerli tra "pubblici" e "privati". Un esempio classico che viene fatto per spiegare il funzionamento dei blocker tag è quello del loro utilizzo nei supermercati, ma tante applicazioni si possono trovare anche nel campo delle pubblica amministrazione. Pensiamo, ad esempio, che tutti i prodotti posizionati sugli scaffali di un supermercato in attesa di essere venduti vengono contrassegnati come "pub-

blici". I lettori nel supermercato possono effettuare la scansione di questi prodotti fino a quando, al momento del passaggio alla cassa per l'acquisto del prodotto, il bit speciale viene cambiato da "pubblico" in "privato". I sacchetti della spesa sono dotati di un blocker tag, cosicché, quando chi effettua l'acquisto si sposta, può beneficiare della protezione del blocker: se un lettore tenta di leggere il contenuto del sacchetto, il blocker tag ne causa lo stallo. Se, ad esempio, chi ha effettuato l'acquisto, rimuove la spesa dal sacchetto, può utilizzare un eventuale frigorifero dotato di tecnologia RFId per leggerli normalmente e sfruttare funzioni come quelle che consentono di individuare i prodotti prossimi alla scadenza, di realizzare una lista della spesa, ecc.

Un protocollo utilizzabile per garantire la riservatezza del dato contenuto nel tag RFId è quello noto come "tree-walking" che agisce simulando una collisione di trasmissione tra i tag. Un blocker tag sfrutta questo protocollo quando il lettore chiede a un sottoinsieme di tag di trasmettere il bit successivo; a questo punto il blocker trasmette sia "0" che "1" simulando la citata collisione di trasmissione tra i tag. Il risultato è che il lettore crede che siano presenti tutti i tag possibili.

Perché un sistema di blocking lavori in modo produttivo, il processo che impedisce la lettura deve essere selettivo. Un blocker tag dovrebbe interdire la scansione da parte di un lettore solo se il lettore prova a leggere un tag "privato". Per far sì che questo sia possibile deve essere usato un sistema di "zonizzazione", in cui metà dell'albero dei numeri seriali è considerata "pubblica" e l'altra metà viene contrassegnata come "privata". Ad esempio, la metà sinistra dell'albero, che comprende tutti i seriali che iniziano per 0, potrebbe essere considerata come zona privata, mentre l'altra come zona pubblica. Il primo bit di ogni numero seriale può indicare lo stato pubblico o privato di un tag. Un blocker dovrebbe simulare delle collisioni solo per il lato privato dell'albero. Per cambiare lo stato di un tag da pubblico a privato, è quindi sufficiente modificare il valore del singolo bit di testa del numero seriale.

I blocker tag presentano, però, le seguenti controindicazioni: risultano poco costosi da produrre solo nel caso di elevati volumi e non sempre sono flessibili come si desidera.

Un approccio alternativo al blocking è il soft blocking che può garantire soluzioni, dal punto di vista "privacy", di flessibilità quasi arbitraria. L'idea è piuttosto semplice: l'interdizione avviene direttamente sul lettore o in un'applicazione software, anziché a livello di protocollo di comunicazione tag-lettore.

Ad esempio, un sistema di soft blocking di tipo opt-in è possibile con gli "unblocker" tag. I lettori RFId, in questo caso, dovrebbero essere programmati solo per effettuare la scansione della zona privata per individuare la presenza di un unblocker tag.

Il soft blocking richiede la cooperazione dei lettori RFId. I meccanismi di verifica per assicurare la conformità dei lettori dovrebbero, quindi, giocare un ruolo chiave nel sistema di soft blocking. D'altro canto, con la giusta configurazione dei lettori, è possibile che la verifica sia condotta senza esaminare ciò che si trova all'interno dei lettori.

A parte i benefici di supporto a una politica flessibile e la verificabilità esterna, l'approccio soft blocking dovrebbe anche permettere la produzione di blocker tag molto economici.

Un soft blocker potrebbe essere un comune tag RFId che, se letto, fornisca un numero seriale in grado di generare un'azione che garantisca il rispetto di determinate norme in materia di protezione del dato personale.
Una tecnica piuttosto diversa rispetto alle precedenti è stata ideata da Fishkin e Roy. Tale tecnica utilizza la distanza fisica tra un lettore e un tag come stima di fiducia. È stato dimostrato che il rapporto segnale/rumore dimostrato durante l'interrogazione tra un lettore, e il tag, dà in prima approssimazione un'indicazione di quanto il tag sia vicino al lettore. Può essere possibile costruire un circuito nel tag RFId che possa misurare la distanza dal lettore.
Un tag, a seconda di come viene configurato può, ad esempio, non rispondere a un'interrogazione trasmessa da più di tre metri di distanza, rivelare il proprio numero seriale quando viene letto da tre metri o meno oppure rispondere al comando "kill" solo ad una distanza predeterminata. Un tag potrebbe anche "trasformarsi" in un blocker se letto da una distanza ritenuta critica.
Un lettore può modificare la potenza di trasmissione per ingannare il tag, ma sembra difficile per un lettore simulare una distanza di lettura più breve in modo efficace. Ovviamente, simulare una distanza più lunga non è vantaggioso per il lettore in termini di energia spesa.
Un'altra soluzione tecnologica è quella nota come crittografia minimale (i tag in grado di realizzare funzioni di crittografia forte sono piuttosto costosi), che prevede la cifratura del codice identificativo, in modo che questo risulti decodificabile solo dal lettore designato, oltre alla re-encryption periodica dell'ID da parte del lettore medesimo e all'operazione di hashing del codice da parte del tag.
Un approccio completamente differente riguarda il problema del tracciamento clandestino. I tag possono cambiare le loro identità dinamicamente: invece di avere un unico numero seriale, un tag potrebbe immagazzinarne diversi. Questi numeri seriali diversi tra loro vengono detti pseudonimi, sono generati off-line e risultano non collegabili tra loro a livello di crittografia.
Si consideri un tag contenente cinque pseudonimi; il tag potrebbe emetterne uno differente ogni volta che viene letto. Tale soluzione permette di garantire la riservatezza del dato personale consistente nel tracciamento del soggetto, venendo meno la correlazione tra il tag letto e le informazioni legate al numero seriale.
Tuttavia l'approccio degli pseudonimi appena descritto presenta delle criticità nel caso in cui si verifichi un attacco con ripetute letture del tag in un breve intervallo di tempo. Questo tipo di attacco potrebbe vanificare completamente la protezione dei dati personali realizzata con gli pseudonimi. Per opporsi a un attacco di questo tipo, un tag RFId può essere configurato per ritardare la rotazione degli pseudonimi: ad esempio, un tag potrebbe trasmettere un nuovo pseudonimo solo dopo tre minuti dall'ultima scansione. Realizzare un tag dotato di un semplice circuito con funzioni di ritardo non presenta difficoltà realizzative né costi eccessivi.
Una evoluzione della soluzione ora descritta prevede che i tag contengano una memoria riscrivibile che consenta di effettuare un refresh degli pseudonimi da parte di lettori a ciò abilitati.

5.4 Gli aspetti normativi

C'è una stretta relazione tra l'uso su larga scala delle tecnologie RFId e il diritto alla protezione del dato personale.
L'Unione europea, da sempre attenta al rispetto dei diritti dei cittadini in tema di trattamento dei dati personali attraverso le tecnologie dell'informazione e della comunicazione, finora ha affrontato queste tematiche attraverso vari strumenti e, tra questi, la "Direttiva sulla protezione degli individui con particolare riferimento al trattamento dei dati personali" (95/46/EC)[14] del 1995 e la cosiddetta Direttiva "e-Privacy" sull'elaborazione dei dati personali e la protezione della Privacy nel settore delle comunicazioni elettroniche del 2002 (2002/58/EC)[15].
La Commissione europea, nel corso del 2006, ha tenuto dei workshop specifici[16] sulle tematiche relative all'utilizzo della tecnologia RFId ed il suo impatto sulla privacy, la sicurezza e la salute dei soggetti coinvolti, allo scopo di trovare risposte concrete finalizzate a produrre un unico documento a integrazione e modifica della citata Direttiva 2002/58/EC.
Le proposte conseguenti ai risultati del workshop sono state di tre tipi:

- legislative;
- tecniche;
- informative/educative e di struttura dei dati.

Sul piano legislativo, è stata proposta l'adozione di un codice di regolamentazione, sviluppato di concerto con le associazioni dei consumatori, mirante a disciplinare varie tematiche, tra le quali la trasparenza nell'acquisizione dei dati, l'interoperabilità, la sostenibilità e l'ergonomia dei sistemi RFId. Inoltre, il codice potrebbe dare indicazioni sulle procedure per rimuovere i tag o disabilitarli in via definitiva dopo la vendita dei prodotti, vietare l'uso di tag e lettori segreti e contenere linee guida sul posizionamento dei lettori.
Le indicazioni che emergono dal workshop evidenziano la circostanza che regole troppo restrittive possano inibire la diffusione della tecnologia RFId e di conseguenza le sue potenzialità; pertanto, l'Unione europea auspica che intervengano **programmi di autoregolamentazione disciplinanti la materia** a partire dalla progettazione e costruzione degli apparati RFId.
Sul piano tecnico, le opzioni prese in considerazione sono state le seguenti:

- la **disattivazione** definitiva del tag;
- la **cifratura** dei dati inseriti nel tag;

[14] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[15] Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronics communications sector
[16] Si sono tenuti cinque workshop cui hanno partecipato esperti, operatori del settore e associazioni di consumatori

- il **tag clipping** ovvero la rimozione dell'antenna dal tag con la conseguente riduzione della distanza di lettura a soli 5 cm.

Sul piano informativo, le proposte prevedono il **consenso informato** rilasciato dal consumatore. Pertanto l'**informazione** fornita al consumatore sulle tecnologie RFId deve essere **chiara, esaustiva** ed **accurata**.
Sulla stessa linea, il Garante per la protezione dei dati personali ha emanato il 9 marzo 2005, un provvedimento a carattere generale che offre un quadro oggettivo, in termini di linee di principio, a cui ci si deve attenere al momento della realizzazione di un'applicazione RFId. Tale provvedimento fa chiarezza sulle modalità di utilizzo delle tecnologie di identificazione a radiofrequenza dal punto di vista degli obblighi relativi alla tutela dei dati personali[17].
Questo provvedimento risulta completo e molto attento non solo al presente ma anche al futuro delle tecnologie RFId per quanto riguarda il grado di utilizzo e le potenzialità tecnologiche.
I punti principali toccati dal provvedimento sono i seguenti.
Si opera innanzitutto una distinzione degli ambiti applicativi in cui non si configura alcun trattamento di dati personali – ad esempio tracciamento dei prodotti nei processi di distribuzione – dagli ambiti nei quali si realizza un simile trattamento.
Il provvedimento, poi, evidenzia alcune soluzioni tecnologiche che presentano profili di criticità legati alla protezione del dato personale. Tra queste il provvedimento cita l'impianto sottocutaneo di microchip, la standardizzazione dei protocolli di lettura/scrittura, l'incremento della potenza del segnale e l'integrazione con altre reti o con altri database esistenti.
Quindi, si richiamano i principi, recati dal "Codice in materia di protezione dei dati personali" che devono essere rispettati anche nel caso di realizzazione di una applicazione RFId. Tali principi sono:

- il principio di necessità (art. 3 del Codice) in base al quale si deve: evitare l'utilizzo di dati personali non strettamente necessari in relazione alla finalità perseguita;
- il principio di liceità (art. 11, comma 1, lettera a) del Codice);
- il principio di finalità e qualità (art. 11, comma 1, lettere b), c), d) ed e), del Codice): "trattare dati personali esclusivamente per scopi determinati, espliciti e legittimi" e "solo per il tempo strettamente necessario";
- il principio di proporzionalità (art. 11, comma 1, lettera d), del Codice): "i dati trattati e le modalità del loro trattamento […]. Non devono risultare sproporzionati rispetto agli scopi […] non risulta di regola giustificato il trattamento che comporti il funzionamento delle etichette apposte su prodotti acquistati […] anche fuori dell'esercizio commerciale, a meno che ciò sia necessario per fornire un servizio specificamente e liberamente richiesto";

[17] Vedi appendice 3

- il principio di dignità (art. 2 del Codice); il provvedimento sancisce che l'applicazione di microchip sottocutanei è giudicata in linea di principio inaccettabile, tranne in casi eccezionali per comprovate e giustificate esigenze a tutela della salute delle persone.

Inoltre, il provvedimento richiama obblighi e condizioni relativi al trattamento dei dati per mezzo di tecnologie RFId. Questi sono:

- l'obbligo di informativa (art. 13 del Codice), che prescrive la chiara indicazione della presenza dell'etichetta e dei lettori, del fatto che il tag può essere interrogato in modo non percepibile e delle modalità mediante le quali il tag può essere disattivato o asportato;
- il consenso, specifico ed espresso, dell'interessato nella ipotesi di trattamento da parte di privati (art. 23 e ss. del Codice).

Si individuano infine le modalità che i produttori dovrebbero predisporre allo scopo di garantire agli interessati un agevole esercizio dei diritti. In particolar modo si fa riferimento alla produzione di tag che agevolino l'esercizio del diritto di rimozione o disattivazione delle etichette, e all'utilizzo di sistemi di crittografia, simmetrica o asimmetrica.
Infine, si richiamano gli obblighi, previsti dal Codice, a carico del titolare del trattamento. In particolare, essi sono:

- notificazione al Garante di trattamenti concernenti dati indicanti la posizione geografica di persone ad oggetto (art. 37, comma 1, lettera a), del codice) ovvero effettuati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato (art. 37, comma 1, lettera d), del Codice);
- adozione delle misure di sicurezza (artt. 31-36 e Allegato B del Codice);
- selezione dei soggetti che, quali incaricati o responsabili del trattamento, sono autorizzati a compiere operazioni di trattamento sulla base di compiti assegnati e delle istruzioni impartite (artt. 29 e 30 del Codice).

Particolare attenzione andrà rivolta al rispetto dei citati obblighi relativi alle misure di sicurezza in quanto, ai sensi di quanto prescritto dall'art. 169 del Codice, la loro mancata adozione è penalmente rilevante.

6. La sicurezza dei sistemi RFId

Prima di affrontare l'argomento della sicurezza dei sistemi RFId, occorre ricordare che le caratteristiche di sicurezza vanno riferite, più che ai prodotti RFId, ai processi ne fanno impiego. Per sicurezza si intende infatti la capacità di gestire eventi non desiderati, prevenendoli oppure attuando misure che ne limitino i danni.
La sicurezza di un processo dipende a sua volta dallo scenario di rischio, ossia dalla probabilità che eventi non desiderati (minacce) arrechino danni a causa di vulnerabilità del sistema.
Per trattare l'argomento della sicurezza nelle applicazioni RFId potremo dunque riferirci:

- alle vulnerabilità dei prodotti RFId;
- alle specifiche minacce nei confronti dei processi che utilizzano tali sistemi;
- ai metodi per ridurre la probabilità di eventi non desiderati (contromisure).

6.1 Le vulnerabilità

Le vulnerabilità di un dispositivo RFId sono quelle tipiche dei sistemi a radiofrequenza e scaturiscono dalla facilità con cui è possibile "comunicare": tale proprietà può essere infatti sfruttata anche per scopi diversi da quelli per cui il sistema è stato progettato.
Molti dispositivi RFId vengono progettati per essere utilizzati in modo particolarmente semplice, senza specifici controlli e procedure di autorizzazione. In questo caso le etichette RFId risponderanno a qualunque interrogazione, senza verificare che questa provenga da un soggetto autorizzato, pertanto sarà possibile leggerne il contenuto, anche non avendone titolo, semplicemente utilizzando un lettore portatile.
Un'altra vulnerabilità, tipica dei dispositivi a radiofrequenza, riguarda la possibilità di intercettare le comunicazioni per venire a conoscenza dei messaggi scambiati. Per intercettare la comunicazione bisogna disporre di un dispositivo di ascolto all'interno del campo d'azione dei dispositivi RFId. E' possibile realizzare dispositivi di ascolto particolarmente efficienti che sono in grado di operare anche con valori molto bassi del campo elettromagnetico per cui, di norma, la distanza massima per le intercettazioni è pari a 3-5 volte la distanza operativa che, come si è visto, può variare tra pochi centimetri e decine di metri.
Una vulnerabilità caratteristica delle etichette meno costose deriva dalla facilità con cui è possibile staccarle dal supporto o danneggiarle.

I dispositivi RFId sono di norma utilizzati in applicazioni che coinvolgono sistemi informatici di tipo tradizionale, nei confronti dei quali si configurano come vere e proprie periferiche di input. I sistemi che gestiscono i dispositivi RFId a loro volta possono essere connessi ad altri sistemi aziendali.
Un dispositivo RFId è dunque un possibile veicolo di ingresso ai sistemi informativi aziendali e, come tale, può essere utilizzato come strumento per attacchi a tale sistema.
Molti articoli hanno evidenziato come teoricamente sia possibile aggirare le protezioni tradizionali dei sistemi informatici sfruttando le vulnerabilità proprie dei sistemi RFId. Ad esempio, se su un'etichetta viene registrato del codice malevolo, questo può arrivare agli elaboratori senza alcun filtro, danneggiando sistemi che non sono stati progettati per resistere a tale attacco.

6.2 LE MINACCE

Le minacce dipendono fortemente dal contesto, dal valore dei beni e dalle tendenze del momento.
Nel caso delle tecnologie innovative di solito le minacce sono limitate per numero e tipologia, per il fatto che i processi che ne fanno uso sono ancora poco diffusi e, soprattutto, poco conosciuti.
Anche nel caso dei sistemi RFId non siamo ancora in presenza di particolari scenari di rischio e, sebbene tali sistemi potrebbero essere oggetto di molte tipologie di attacchi, in pratica non si rilevano ancora effrazioni diffuse.
Ciò nondimeno è prevedibile che, con la diffusione delle applicazioni RFId, si assisterà all'incremento di attacchi basati sulle vulnerabilità specifiche dei sistemi identificativi a radiofrequenza.
Nell'ipotizzare i futuri scenari di rischio, occorre distinguere tra minacce di natura accidentale (errori operativi, guasti, situazioni calamitose, ecc.) o volontaria (furti, truffe, sabotaggi, ecc.).
Le prime possono essere dovute ad utilizzo non corretto dei dispositivi (lettura involontaria di informazioni, danneggiamento dei dispositivi) o a particolari situazioni ambientali (presenza di materiali conduttori, interferenze, ecc.).
In sintesi, le minacce di natura accidentale riguardano:

- la possibilità di uso improprio dei dati nel caso che le informazioni presenti nei sistemi RFId vengano lette al di fuori dei processi ordinari[18];
- la possibilità di disservizi dovuti ad errori nell'utilizzo o a situazioni ambientali particolarmente sfavorevoli.

Queste possibilità possono essere sfruttate anche per azioni illecite (attacchi volontari). Più

[18] Un esempio di minaccia di questo tipo riguarda la possibilità che un'etichetta, utilizzata ad esempio per la gestione della logistica, rimanga sull'oggetto anche quando questo esce dal magazzino e venga letta involontariamente fornendo all'esterno informazioni sull'azienda.

in generale, le minacce verso i processi che utilizzano sistemi RFId possono essere così schematizzate:

a) entrare in possesso di informazioni riservate;
b) contraffare le informazioni presenti su un'etichetta;
c) falsificare l'identficativo del lettore o del trasponder;
d) tracciare un oggetto;
e) tracciare una persona;
f) creare un disservizio.

Le minacce di tipo a) possono riguardare le informazioni presenti sulle etichette, i dati registrati nelle smart card *contactless* o i sistemi utilizzati per le applicazioni RFId.
Nel valutare queste minacce occorre considerare la natura delle informazioni registrate nei dispositivi RFId, l'ambiente in cui i sistemi operano e la tipologia di etichetta.
Nelle applicazioni più diffuse, inerenti la logistica e la gestione degli oggetti, generalmente le etichette riportano informazioni relative ai beni (codici EPS, descrizioni, ecc.) ricavabili anche dalla semplice osservazione dei medesimi, dunque la probabilità di attacchi volti a leggere tali dati è alquanto bassa.
In alcuni casi, la lettura delle informazioni presenti sui dispositivi RFId può fornire indirettamente informazioni sui soggetti entrati in relazione con gli oggetti etichettati (ad esempio sulle abitudini di un soggetto che frequenta una biblioteca dotata di controlli RFId). Questo tipo di minaccia comunque è dovuto all'automazione dei processi, piuttosto che all'uso delle tecnologie RFId, dunque va considerato ed affrontato in ambito più ampio[19].
Analogo discorso vale per la possibilità di accedere ad informazioni riservate, registrate sui sistemi elaborativi interni, mediante attacchi che si avvalgono dei sistemi RFId.
In generale, l'adozione di sistemi RFId non introduce nuovi rischi di lettura di informazioni riservate; vanno invece considerate con attenzione le minacce "tradizionali" nei confronti dei sistemi informativi, minacce che potrebbero sfruttare anche le vulnerabilità dei dispositivi a radiofrequenza.
Le minacce di tipo b) riguardano possibili truffe basate sulla falsificazione dei dati registrati su un dispositivo RFId.
Un caso particolare, che combina le minacce di tipo a) e b), consiste nella clonazione dell'etichetta (ossia nella produzione di un duplicato di un'etichetta esistente mediante la lettura delle informazioni dall'originale e l'inizializzazione di un'etichetta vergine con gli stessi dati).
La consistenza di tali minacce dipende dalla tipologia di applicazioni: quando l'etichetta RFId è utilizzata per proteggere un bene di elevato valore o per assicurare l'integrità di un documento importante, allora il rischio di contraffazione è consistente. Altri casi a rischio sono le applicazioni in cui si utilizzano smart card *contactless* come sistemi di pagamento.

[19] Riprendendo l'esempio della biblioteca, la possibilità di ricavare le abitudini di un soggetto dall'esame dei prestiti deriva dall'automazione del processo ed è indipendente dall'adozione delle tecnologie RFId

La falsificazione dell'identificativo registrato sull'etichetta (minaccia di tipo c) permette di ingannare il sistema sulla natura dell'oggetto etichettato.
Una variante di questa minaccia riguarda la possibilità di "staccare" l'etichetta RFId per poi eventualmente collocarla su un diverso oggetto. In questo caso, anche se i dati registrati nel dispositivo non vengono contraffatti, la falsa associazione con gli oggetti apre la strada a truffe facilmente intuibili.
In alcune applicazioni è importante che il *trasponder* risponda solo a determinati lettori, in questo caso un possibile attacco consiste nella falsificazione dell'identificativo di quest'ultimo, allo scopo di interagire illecitamente con le etichette RFId.
Molto si è detto sulle minacce di tipo d) ed e), soprattutto in relazione alla possibilità di tracciare un individuo seguendo gli spostamenti di un suo capo di abbigliamento dotato di etichetta RFId.
Queste minacce preoccupano giustamente l'opinione pubblica, ma oggi sono alquanto limitate.
Infatti la gran parte dei dispositivi in commercio può essere letta ad una distanza non superiore ai 3 metri, quindi per seguire gli spostamenti di un oggetto dotato di etichetta RFId bisognerebbe disporre, lungo il suo percorso, di una fittissima rete di lettori tra loro interconnessi.
Anche la possibilità di correlare informazioni di etichette lette in luoghi diversi oggi è alquanto remota, anche se con il diffondersi dei sistemi elettronici cresce il rischio che informazioni di carattere personale possano essere registrare in luoghi ed in momenti diversi (pagamenti elettronici, accessi a servizi on line, carte fedeltà, ecc.) e successivamente relazionate e sfruttate per fini malevoli.
Un problema peculiare dei sistemi RFId, riguarda la possibilità di leggere incidentalmente informazioni relative ad oggetti che potrebbero rivelare abitudini dei soggetti che li trasportano (ad esempio informazioni sui farmaci).
I disservizi (minacce di tipo f) possono essere dovuti ad eventi incidentali, a particolari condizioni ambientali oppure a veri e propri attacchi per fini malevoli. Si tratta di un problema serio, soprattutto in ambienti con elevata densità di dispositivi e di lettori (in cui sono probabili problemi accidentali) ed in luoghi non controllati (in cui sono possibili attacchi mirati).
Le tecniche con cui è possibile creare un disservizio sono diverse: la disattivazione del *trasponder* con elevati campi magnetici, con l'uso del comando *kill* o con il danneggiamento materiale dell'oggetto, oppure l'inibizione della trasmissione sia con tecniche di oscuramento che attraverso l'emissione di segnali di disturbo.
Tutte le minacce esposte si riferiscono ad applicazioni che operano in ambienti non controllati o con un basso livello di controllo, come ad esempio all'aperto o in locali pubblici.
Quando le applicazioni RFId operano in locali controllati (ad esempio all'interno di un ufficio) le minacce verso i sistemi RFId hanno la stessa consistenza e probabilità di quelle che caratterizzano altri strumenti di supporto alla normale operatività.
La credenza che un sistema RFId introduca nuovi rischi per la possibilità di operare a

distanza, agendo oscuramente al di fuori dell'ambiente di lavoro, è sostanzialmente infondata per le limitate distanze operative che caratterizzano le tecnologie attuali[20].
Nella figura seguente è riportato lo schema delle possibili minacce per un sistema RFId.

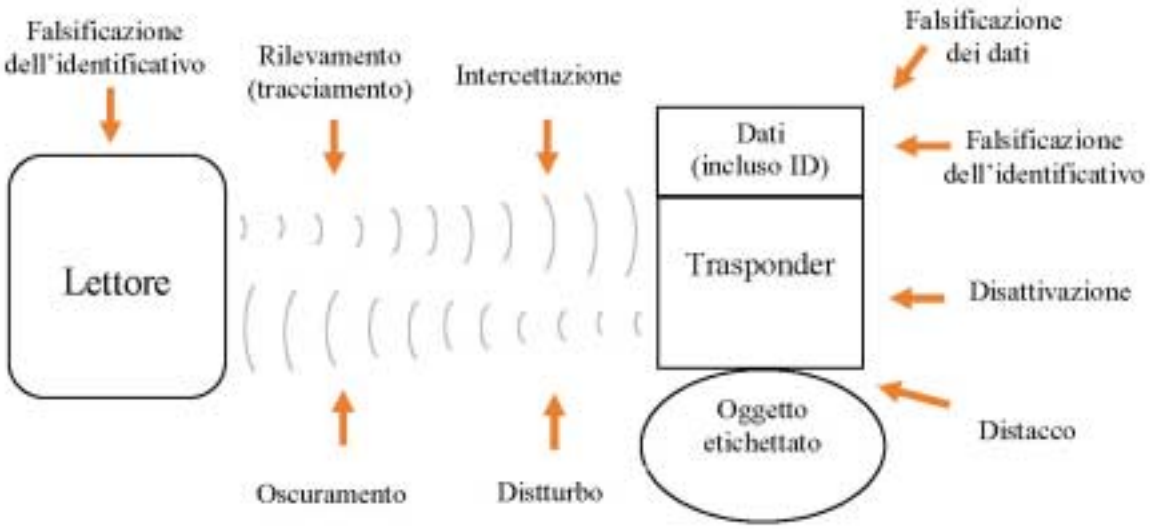

Figura 31 - Schema delle minacce di un sistema RFId

6.3 LE CONTROMISURE

Per ciascuna delle minacce precedentemente esposte esiste almeno una contromisura capace di neutralizzarla o, almeno, di ridurla significativamente.
Una trattazione esaustiva delle possibili contromisure esula dagli obiettivi di questo documento, si vuole invece offrire una veloce panoramica delle soluzioni per la sicurezza e del loro impatto sui costi e sugli aspetti organizzativi.

6.3.1 CIFRATURA

Le contromisure tipiche dei sistemi di trasmissione a radiofrequenza consistono nella cifratura dei dati trasmessi e nell'autenticazione delle entità in comunicazione.
la cifratura consente il mascheramento delle informazioni nei confronti di utenti non autorizzati, nonchè il controllo dell'integrità dei messaggi trasmessi; l'autenticazione permette invece di proteggersi nei confronti dell'uso malevolo di falsi identificativi.

[20] L'utilizzo di particolari lettori in grado di operare a distanze molto superiori a quelle operative è possibile in particolari condizioni ambientali (assenza di schermi e di riflessi) ed a costi molto elevati. Nel caso di sistemi ad accoppiamento induttivo la distanza di un metro è considerata un valore limite. Nel caso dei sistemi UHF, la distanza massima dipende dalla potenza in gioco che è regolamentata per legge (di solito inferiore a 2 Watt), comunque per leggere un'etichetta alla distanza di 20 metri occorrerebbe emettere una potenza di circa 500 Watt, pari a quella di un trasmettitore radiotelevisivo

Le tecniche di cifratura ed autenticazione sono ampiamente utilizzate nelle applicazioni informatiche ed in particolare in tutti i sistemi di trasmissione di segnali in radiofrequenza (GSM, wifi, wimax, ecc.).
L'impiego di queste tecniche nei sistemi RFId è possibile se i dispositivi dispongono di sufficiente memoria e capacità elaborativa, condizione che si verifica nelle etichette attive e nelle smart card di prossimità (ISO 14443 e ISO 18092), anche in questi casi vengono comunque prescelte delle tecniche crittografiche che richiedono un basso impiego di risorse elaborative.
In conseguenza di tale esigenza, al momento non sono molto diffuse le funzioni di autenticazione e di riservatezza basate su chiavi asimmetriche e certificati digitali[21], mentre si utilizzano quasi esclusivamente metodi basati su chiavi segrete simmetriche. L'impiego delle chiavi simmetriche richiede però particolari accorgimenti per la generazione, la distribuzione e la protezione delle medesime. Nel campo delle applicazioni RFId sono stati elaborati diversi metodi aventi l'obiettivo di rendere efficiente e sicura la gestione delle chiavi segrete[22]. Rinviando alla letteratura specialistica per una disamina di tali metodi, si può asserire che le tecniche correntemente impiegate offrono, in generale, garanzie sufficienti per le applicazioni commerciali.

6.3.2 AUTENTICAZIONE

L'autenticazione dei dispositivi di lettura è spesso effettuata con il ricorso alla tradizionale password. Nelle applicazioni che fanno uso di tale tecnica di autenticazione, la password viene immessa nel sistema dall'utente e verificata dalle etichette al fine di abilitare o meno la trasmissione delle informazioni verso il lettore.
Per l'autenticazione delle etichette si ricorre invece a metodi che ricadono nella categoria sfida/risposta. Questi metodi prevedono che il lettore lanci una sfida all'etichetta che, per autenticarsi, deve rispondere in modo opportuno. Un esempio diffuso consiste nella generazione, da parte del lettore, di un numero casuale che viene inviato all'etichetta "sfidandola" a cifrarlo correttamente: l'etichetta utilizzerà una chiave segreta (presente anche sul lettore) per rispondere alla sfida dimostrando la propria autenticità.

6.3.3 MASCHERAMENTO DELL'IDENTIFICATIVO

Le etichette più economiche non dispongono di memoria e potenza sufficiente ad eseguire operazioni crittografiche, per cui gli esperti hanno sviluppato diversi metodi per proteggere le informazioni anche senza l'impiego di tali tecniche.

[21] Tali tecniche sono molto utilizzate per proteggere le informazioni in Internet ma, oltre a necessitare di elevata potenza di calcolo, richiedono la presenza di organizzazioni (*certifiction autority*) per la gestione dell'infrastruttura delle chiavi pubbliche (PKI).
[22] A titolo di esempio si cita la proposta di Henrici and Müller - Tackling Security and Privacy Issues in Radio Frequency Identification Devices. In: Ferscha A., Mattern F.: Pervasive Computing (Proceedings of PERVASIVE 2004, Second International Conference on Pervasive Computing). Springer-Verlag, LNCS 3001: 219-224

Questi metodi consistono nel fare in modo che le informazioni trasmesse non siano inutilizzabili da parte di un eventuale attaccante.
La tecnica più semplice ed efficace consiste nell'utilizzo di identificativi completamente anonimi, ossia non direttamente riconducibili ad alcuna entità se non con metodi attivabili solo dal sistema di *back end*.
Ciò si può ottenere mediante una codifica interna "riservata" oppure con metodi in grado di rendere anonimi gli identificativi per poi ripristinarli ai fini dell'eleborazione.
Gli algoritmi più sofisticati modificano dinamicamente il dato anonimo, in modo tale da proteggere l'etichetta non solo nei confronti dell'identificazione illecita, ma anche dal tracciamento della localizzazione[23].
Il mascheramento dell'identificativo non protegge nei confronti di letture indebite di altre informazioni registrate sull'etichetta e trasmesse a seguito di un'interrogazione.
Per evitare tale problema, la soluzione migliore consiste nello spostare ogni informazione rilevante sul sistema di *back end*, lasciando sull'etichetta il solo identificativo, opportunamente reso anonimo.

6.3.4 INIBIZIONE DELL'ETICHETTA

Le tecniche di inibizione dei dispositivi possono essere utilizzate per evitare la lettura indebita in momenti e situazioni in cui il sistema RFId non è operativo.
I metodi si dividono in due categorie: temporanei e definitivi. I primi sfruttano particolari etichette di tipo attivo (*blocker tags*) in grado di mascherare le etichette da proteggere. I secondi sfruttano il comando di disattivazione[24] (*kill*) per rendere l'etichetta permanentemente inutilizzabile.

6.3.5 TECNICHE PER CONTRASTARE DISSERVIZI INTENZIONALI

Come si è visto, le etichette RFId sono facilmente asportabili e danneggiabili. Per proteggersi nei confronti di queste vulnerabilità è possibile utilizzare particolari tecniche di ancoraggio, oppure "affogare" l'etichetta all'interno del materiale che costituisce l'oggetto.
Quando l'ambito lo consente, i dispositivi possono essere collocati in zone nascoste o difficilmente accessibili.
Per proteggersi dall'uso improprio del comando di disattivazione (*kill*), è possibile introdurre metodi di autenticazione che accettano il comando solo nel caso che esso provenga da una fonte autenticata.

[23] A titolo di esempio si citano i metodi di hash-lock randomico (WEIS, S.A., SARMA, S.E., RIVEST, R.L. und ENGELS, D.W.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. First International Conference on Security in Pervasive Computing, Boppard, März 2003. Springer-Verlag, LNCS 2802: 201-212) e degli hash concatenati (OHKUBO, M., SUZUKI, K. und KINOSHITA, S.: Cryptographic Approach to "Privacy-Friendly" Tags. RFId Privacy Workshop, Massachusetts Institute of Technology, Cambridge, MA, USA).

[24] Per finalità legate alla tutela della privacy, quasi tutti i sistemi rendono disponibile uno specifico comando (*kill*) che disabilita permanentemente l'etichetta

Sulle etichette di tipo attivo sono disponibili sistemi che rilevano automaticamente il distacco o manomissioni ed emettono allarmi o disabilitano il dispositivo; inoltre, per evitare che interrogazioni ripetute scarichino dolosamente le batterie, è possibile utilizzare temporizzatori che sospendono l'operatività dopo un periodo di funzionamento continuato.
Gli attacchi più difficilmente contrastabili sono quelli che mirano a creare disservizi interagendo con il sistema di comunicazione elettromagnetico (disturbi delle comunicazioni, oscuramento del campo, schermatura dei dispositivi, danneggiamento delle etichette con campi particolarmente intensi, ecc.). Benché siano state elaborate tecniche per ridurre le vulnerabilità a tali attacchi (ad esempio particolari tecniche di modulazione), i sistemi che operano in ambienti non controllati difficilmente possono proteggersi nei confronti di attacchi miranti a compromettere la disponibilità delle applicazioni.

6.3.6 SORVEGLIANZA E DISINCENTIVAZIONE

La gran parte delle minacce esposte si basa sulla possibilità di guadagnare l'accesso fisico alle etichette o di utilizzare apparati che emettono forti campi magnetici. Queste azioni possono essere facilmente rilevate e contrastate con un'efficace sistema di sorveglianza.
Un altro modo efficace per contrastare gli attacchi consiste nella disincentivazione alle attività criminose attraverso opportune regole (politiche di sicurezza, norme comportamentali, ecc.) o disposizioni normative (limiti di potenza dei segnali, penalizzazione delle attività di disturbo, divieto di impiego dei dispositivi bloccanti, ecc.).

6.3.7 TABELLA RIASSUNTIVA

La tabella seguente mette in relazione le minacce con le possibili contromisure, inoltre ad ogni contromisura viene associato un livello di costo indicativo.

Minaccia	**Contromisure**	**Costo**
Intercettazione della comunicazione	Cifratura Mascheramento dell'identificativo	medio-alto basso
Lettura/modifica non autorizzata dei dati	Autenticazione, inibizione temporanea delle etichette	medio
Tracciamento di persone ed oggetti	Inibizione permanente dell'etichetta Sistemi di mascheramento dinamici	basso medio
Falsificazione dell'identificativo, clonazione delle etichette	Autenticazione, sistemi di *back end* in grado di rilevare duplicati	medio
Distacco delle etichette	Ancoraggi particolari, etichetta inserita nel materiale, posizione irraggiungibile Sistemi automatici di rilevazione del distacco (solo etichette attive) Sorveglianza	basso medio alto

Minaccia	Contromisure	Costo
Disattivazione delle etichette	Autenticazione del comando *kill*, circuito elettrico in grado di resistere a sovratensioni Sorveglianza	 medio alto
Disturbi delle comunicazioni	Particolari tecniche di modulazione, sistemi di rilevazione dei disturbi, sorveglianza e disincentivazione	 alto
Oscuramento delle comunicazioni	Sorveglianza e disincentivazione (efficace solo in ambienti controllati)	alto

6.4 I RISCHI CONNESSI ALL'USO DELLE TECNOLOGIE RFID

Prima di concludere l'argomento della sicurezza, si vuole ribadire che le vulnerabilità e le minacce illustrate non necessariamente implicano rischi significativi per gli utenti. I rischi vanno infatti determinati in base a considerazioni più ampie che devono tenere in conto l'etica corrente, l'ambiente operativo, il valore dei beni, l'effetto di norme e regolamenti, ecc.

Tali valutazioni ricadono nell'attività che comunemente prende il nome di analisi dei rischi.

I metodi di analisi si basano tuttavia su valori statistici o sulla diretta percezione dei rischi da parte dei responsabili delle applicazioni. Nel caso delle applicazioni RFId oggi non vi sono statistiche accreditate, né esperienze sufficientemente consolidate da consentire una valutazione affidabile dei rischi.

L'unica strada percorribile consiste nel delineare lo scenario di rischio basandosi sul buon senso ed eventualmente sulle indicazioni degli esperti.

Per agevolare il lettore in questo esercizio, si riportano le conclusioni dell'autorevole istituto tedesco BSI circa il probabile scenario di rischio delle applicazioni RFId (il testo che segue è tratto dal documento "Risiken und Chancen des Einsatzes von RFId-Systemen" reperibile sul sito www.bsi.bund.de).

"*E' stato inizialmente chiesto agli esperti di fornire una stima generale sulla rilevanza degli aspetti di sicurezza nelle applicazioni RFId. Sono emersi i seguenti punti:*

- *ad oggi, i problemi causati da attacchi ai sistemi RFId sono di gran lunga inferiori alle difficoltà tecniche che si incontrano nell'utilizzo pratico di tali sistemi;*
- *le potenziali minacce potrebbero crescere se i sistemi venissero impiegati in modo massivo, la loro diffusione potrebbe infatti innescare tentazioni di attacco ai sistemi o di valutazione delle informazioni in modo da compromettere la privacy;*
- *se le applicazioni RFId hanno ripercussioni sulla sicurezza fisica delle persone (ospedali, parti di ricambio di apparati critici per la sicurezza, identificazione personale), è di particolare importanza la sicurezza informatica;*

- *in complesso, la privacy è minacciata dagli attacchi ai sistemi RFId meno di quanto lo sia dalle normali attività operative;*
- *le opinioni in merito ai rischi aggiuntivi per la privacy causati dai sistemi RFId divergono, esse variano da "rischio zero" (è tutto già possibile con i sistemi attuali) a "rischio elevatissimo" (il tracciamento mediante RFId è una nuova forma di sorveglianza);*
- *le contromisure fanno crescere non solo i costi fissi, ma anche quelli variabili; i costi dovuti alle procedure di sicurezza possono essere contenuti solo in caso di volumi elevati.*"

Queste considerazioni sono indicative anche per le applicazioni della pubblica amministrazione, destinate ad operare principalmente in locali controllati e protetti, su dati di natura pubblica, spesso reperibili senza dover sfruttare le vulnerabilità dei sistemi RFId.
Dunque, in genere, le tecnologie RFId possono essere adottate senza particolari precauzioni per la sicurezza.
Occorrerà invece valutare con attenzione gli aspetti di sicurezza in tutti quei casi in cui la riservatezza dei dati e la disponibilità delle applicazioni sono rilevanti per la salvaguardia dei diritti individuali, come nel caso del settore sanitario.

7. Progettazione e realizzazione di una soluzione RFId: un caso pratico

Gli strumenti informatici di supporto alla gestione di un piano di progetto rappresentano un aiuto indispensabile per abbinare una buona efficienza nelle operazioni di stesura iniziale e di successivo aggiornamento del piano, a un'ottima qualità formale della documentazione.
Si rivelano utili anche nella definizione dei contenuti del piano stesso le metodologie di progetto che si prefiggono l'obiettivo di offrire tutte quelle indicazioni che risultano utili anche in merito ai contenuti dell'attività di pianificazione e persino in merito ai contenuti tecnici del progetto stesso.
L'obiettivo più alto che una metodologia può porsi consiste nell'offrire, a chi gestisce il progetto, una guida concreta, che entra nel merito dei contenuti.
In sintesi, quanto più un progetto corrisponde alla tipologia di riferimento di una determinata metodologia, tanto più sarà possibile evitare l'improvvisazione, migliorando, invece, la chiarezza e la qualità generale, e diminuire gli errori e le dispersioni, aumentando enormemente l'efficienza.
L'obiettivo che ci si prefigge nelle prossime pagine è quello di definire una metodologia utile all'implementazione delle tecnologie RFId nel mondo della gestione dei beni bibliotecari, che rappresenta un' applicazione delle tecnologie RFId trasversale a tutto il mondo della pubblica amministrazione centrale e locale, descrivendone i passi salienti. In particolare il modello che andremo ad utilizzare assumerà come riferimento una biblioteca universitaria.
La descrizione dei processi in essa svolti si è basata sull'analisi della Biblioteca Didattica di Architettura del Politecnico di Milano, sede di Milano Bovisa, ed è stata validata presso altri atenei italiani (Torino, Roma, Milano).
Il modello è stato costruito a partire da un'analisi dettagliata dei processi di back-office e di front-office che vengono eseguiti su ciascun bene (libro, rivista o materiale multimediale) dal suo ingresso in biblioteca a seguito di un'acquisizione sino alla sua fruizione da parte degli utenti.
Successive interviste ai responsabili di altre biblioteche comunali ed interne agli enti della Pubblica Amministrazione hanno confermato profonde analogie nella gestione di queste strutture, e hanno dato un contributo per validare il modello nella sua struttura generale e nei suoi risultati. Una volta definito il modello concettuale che si andrà ad utilizzare, si potrà impiegare con i dati reali di scenario per ottenere un'analisi dei costi e dei reali benefici legati all'introduzione delle tecnologie RFId nel processo in questione.

7.1 DESCRIZIONE DEL MODELLO UTILIZZATO

Il modello è stato costruito analizzando i processi all'interno di una biblioteca universitaria caratterizzata dai seguenti elementi:

- appartenenza a un Sistema Bibliotecario d'Ateneo;
- collegamento al Sistema Bibliotecario Nazionale (SBN);
- movimentazione di tre tipologie di documento: libro, rivista e materiale multimediale (CD/DVD);
- orario di apertura al pubblico durante la giornata nei periodi di apertura dell'ateneo e secondo quanto stabilito dalla biblioteca stessa;
- chiusura totale al pubblico in concomitanza dei giorni festivi previsti per le ricorrenze di Natale e Pasqua e ad Agosto.

I servizi principali[25] effettuati sono:

- *consultazione "libera" in sede* di libri e riviste;
- *consultazione in sede* dei materiali custoditi in deposito e non esposti a scaffale aperto;
- *prestito giornaliero* di libri (ed eventuale materiale multimediale);
- *prestito domiciliare* di libri (ed eventuale materiale multimediale);
- *reference* all'utenza, assistenza per l'utilizzo dei servizi offerti;
- *servizi interbibliotecari.*

Il modello è costruito in modo parametrizzato così da permettere la sua applicazione alle strutture universitarie che si vuole prendere in analisi.
Sulla base dell'analisi effettuata, per ciò che concerne lo svolgimento delle attività bibliotecarie, sono state assunte le seguenti ipotesi di funzionamento:

- le attività di back-office sono svolte da personale dipendente, dotato di adeguate competenze biblioteconomiche;
- le attività di front-office sono svolte da personale di cooperativa o da studenti universitari a contratto (le cosiddette "150 ore"), senza competenze specifiche;
- i servizi della biblioteca sono offerti a chiunque in ambito universitario.

7.2 POSSIBILI SCENARI DI APPLICAZIONE

Vengono presentati tre possibili scenari, diversi per modalità e tecnologie utilizzate per l'identificazione dei documenti e la gestione delle attività della biblioteca: gestione manuale con etichetta a codice alfanumerico (scenario "situazione attuale"), gestione con tecnologia

[25] Sono esclusi i servizi "particolari" erogati in bassi volumi (ad es. l'invio dei fascicoli ai dipartimenti)

a codice a barre (scenario "scaffale aperto[26] tecnologia bar-code"), gestione con tecnologia RFId (scenario "scaffale aperto tecnologia RFId").
Le principali caratteristiche comuni ai tre scenari tecnologici presi in esame sono:

- ubicazione documenti: i libri e le riviste sono dislocati su scaffali direttamente accessibili dagli utenti; i libri non disponibili a scaffale aperto ed il materiale multimediale sono conservati in un deposito contiguo al banco per il ricevimento dell'utenza (nello scenario RFId è possibile prevedere che anche il materiale multimediale venga disposto a scaffale aperto);
- ogni utente è identificato grazie al proprio tesserino d'ateneo o al documento d'identità. Per quanto riguarda lo scenario "scaffale aperto tecnologia RFId", sul mercato esistono tessere RFId, tuttavia attualmente tutti gli atenei danno già in dotazione ai propri studenti tessere di riconoscimento a banda magnetica. Non è facile pensare di dotare ogni utente di una nuova tessera RFId per usufruire solo dei servizi bibliotecari e nemmeno che gli atenei sostituiscano immediatamente i loro tesserini a banda magnetica, processo che richiede tempi non brevi per la sua realizzazione;
- il ripristino a scaffale dei materiali in prestito e in consultazione è effettuato periodicamente durante l'orario di apertura; il ripristino dei documenti in deposito è effettuato all'atto di ogni restituzione.

7.2.1 SCENARIO "SCAFFALE APERTO NO TECNOLOGIA"

Non è previsto l'utilizzo di alcuna tecnologia né per la gestione delle operazioni di prestito, né per l'inventario. Le principali caratteristiche di questo scenario sono:

- ogni documento ha il proprio numero d'inventario scritto internamente;
- non sono utilizzate tecnologie per la registrazione dei prestiti e per la gestione dell'inventario; le operazioni vengono eseguite manualmente, eccezion fatta per i prestiti domiciliari che vengono registrati manualmente a sistema (software gestionale);
- l'OPAC (On-line Public Access Catalog) da informazioni solo sull'esistenza di copie del documento nella biblioteca, non sulla disponibilità, perché non collegato al software gestionale;
- libri e riviste sono dotati di sistema antitaccheggio a banda magnetica;
- il materiale multimediale è disponibile solo per il prestito domiciliare e non è dotato di antitaccheggio, perché i sistemi a banda magnetica sono incompatibili con CD e DVD (per questo motivo è conservato a scaffale chiuso);
- è presente una (o più di una) postazione servita da personale di front-office per il prestito e la restituzione assistiti.

[26] Nella configurazione a "scaffale aperto" l'utente può accedere autonomamente alla maggior parte del materiale messo a disposizione, sia esso disponibile in consultazione che in prestito, e si occuperà direttamente del prelievo

7.2.2 SCENARIO "SCAFFALE APERTO TECNOLOGIA BAR-CODE"

Si è scelto di considerare anche questo scenario poiché questa tecnologia è ampiamente diffusa e consolidata nel settore bibliotecario. L'identificazione del documento avviene mediante codice a barre. Le principali caratteristiche di questo scenario sono:

- ogni documento ha il proprio codice a barre corrispondente al numero d'inventario apposto sul retro;
- per la registrazione dei prestiti e per la gestione dell'inventario è utilizzata la tecnologia ottica di lettura dei codici a barre dei documenti combinata alla tecnologia a banda magnetica delle tessere utente; tutte le operazioni vengono registrate automaticamente a sistema (software gestionale);
- l'OPAC (On-line Public Access Catalog) da informazioni sia sull'esistenza di copie del documento nella biblioteca che sull'effettiva disponibilità, perché è aggiornato in tempo reale con il software gestionale;
- libri e riviste sono dotati di sistema antitaccheggio a banda magnetica;
- il materiale multimediale è disponibile solo per il prestito domiciliare e non è dotato di antitaccheggio, perché i sistemi a banda magnetica sono incompatibili con CD e DVD (per questo motivo è conservato a scaffale chiuso);
- sono presenti stazioni automatizzate self-service per il prestito e postazioni servite da personale di front-office per il prestito e la restituzione assistiti. Il loro numero potrebbe variare sulla base delle esigenze della biblioteca.

7.2.3 SCENARIO "SCAFFALE APERTO TECNOLOGIA RFID"

L'identificazione del documento avviene mediante chip basati sulla tecnologia RFId. Le principali caratteristiche di questo scenario sono:

- i libri e il materiale multimediale hanno il proprio chip RFId identificativo apposto internamente. Sul chip, di tipo riscrivibile, vengono scritte solo le informazioni relative al codice d'inventario. Il chip funziona alla frequenza di 13,56 MHz secondo lo standard ISO 15693, come avviene in ogni caso di applicazione della tecnologia RFId in questo ambito, così come emerso dallo studio dei casi di applicazione dell'RFId in biblioteche italiane ed estere;
- per la registrazione dei prestiti e per la gestione dell'inventario è utilizzata la tecnologia RFId dei documenti combinata alla tecnologia a banda magnetica delle tessere utente; tutte le operazioni vengono registrate automaticamente a sistema (software gestionale);
- l'OPAC (On-line Public Access Catalog) da informazioni sia sull'esistenza di copie del documento nella biblioteca che sull'effettiva disponibilità, perché è aggiornato in tempo reale con il software gestionale;

- le riviste sono dotate di chip RFId "economici" non scrivibili: il loro codice univoco non è associato al loro codice d'inventario, non è dunque possibile il riconoscimento automatico a sistema;
- tutti i documenti sono dotati del sistema antitaccheggio E.A.S. (Electronic Article Surveillance) contenuto nei chip RFId (le riviste sono dotate di chip economici con la funzione E.A.S. sempre attiva perché disponibili solo in consultazione);
- sono presenti stazioni automatizzate self-service per il prestito, postazioni servite da personale di front-office per il prestito e la restituzione assistiti e postazioni esterne automatizzate ("buca") per la restituzione. Il loro numero potrebbe variare sulla base delle esigenze della biblioteca.

7.3 I DATI DI INGRESSO AL MODELLO

7.3.1 I DATI GENERALI

Nel seguito si riportano i dati utilizzati per il funzionamento del modello sulla base delle informazioni fornite dalla Biblioteca mediante il questionario preparato dal Politecnico di Milano e mediante gli incontri avvenuti nel corso del lavoro.

DATI DELLA STRUTTURA			
patrimonio librario [documenti]		**60.000**	
n° totale fascicoli [documenti]		**10.000**	
patrimonio multimediale [documenti]		**1.000**	
n° medio libri in prestito domiciliare per utente [libri/utente]		**2**	
n° medio multimediali in prestito per utente [multimediali/utente]		**1**	
n° ore giornaliere front-office pre-RFId [ore/g]		**28**	
N° ore giornaliere front-office post-RFId [ore/g]		**28**	
giorni di apertura annui [giorni/anno]		**276**	
costo orario Manodopera front-office [€/h]		**15**	
costo orario Manodopera back-office [€/h]		**18**	
n° postazioni prestito assistito (attive nel picco di frequentazione della biblioteca)	**Scenario non RFId**	**3**	
	Scenario RFId	**2**	

Tabella 4 - Dati in ingresso al modello (continua nella pagina seguente)

DATI DI FLUSSO		
n° libri acquistati [documenti/anno]	**1.500**	
n° testate in abbonamento [documenti/anno]	**650**	
n° fascicoli acquistati [documenti/anno]	**6.500**	**Modello**
n° multimediali acquistati [documenti/anno]	**n.d.**[27]	
n° ordini [ordini/anno]	**2.200**	
n° libri restaurati [documenti/anno]	**0**	
n° consultazioni [documenti/anno]	**88.000**	
n° consultazioni deposito [documenti/anno]	**2.500**	
n° consultazioni chiuso [documenti/anno]	**0**	
n° prestiti giornalieri [documenti/anno]	**0**	
n° prestiti domiciliari [documenti/anno]	**7.300**	
n° prestiti multimediali [documenti/anno]	**500**	
n° schede consultazione chiuso [schede/anno]	**0**	
n° schede materiale in deposito [schede/anno]	**2.500**	
n° schede prestito giornaliero [schede/anno]	**0**	
n° ripristini giornalieri materiale consultazione [ripristini/giorno]	**16**	
n° ripristini giornalieri materiale prestato [ripristini/giorno]	**6**	
n° ripristini giornalieri materiale multimediale prestato [ripristini/giorno]	**0**	
% autoprestito	**60%**	**Modello**
% autoconsegna (mediante postazione self-service)	**10%**	**Modello**
% autoconsegna (mediante buca 24h/24)	**60%**	**Modello**

Segue: *Tabella 4 - Dati in ingresso al modello*

[27] 20 è il numero di multimediali acquistati ogni anno relativi a banche dati non concesse in prestito, mentre non è possibile individuare il numero di multimediali annui acquisiti poiché allegati ad una monografia. Poiché tale dato è quello che serve per alimentare il modello, al momento lo si pone pari a 0

Di seguito vengono riportati i dati di afflusso degli utenti presso la sede bibliotecaria

	GEN	FEB	MAR	APR	MAG	GIU	LUG	AGO	SET	OTT	NOV	DIC	TOT
Giorni di apertura della biblioteca	24	24	27	24	25	25	26	CHIU-SA	27	26	25	23	276
Numero utenti	8111	4867	5840	6489	10815	14870	8084	0	8760	7733	10139	8706	94414
Numero utenti (che effettuano prestiti) = 4150	356	214	257	285	475	654	356	0	385	340	446	382	4150

Tabella 5 - Dati di afflusso degli utenti presso la sede bibliotecaria

7.3.2 I DATI DELL'INFRASTRUTTURA RFID STIMATA

Lo studio di un modello prevede una analisi propedeutica per la gestione dell'ambiente in cui si deve applicare la struttura RFId. Nel caso della biblioteca di economia le principali caratteristiche dell'ambiente in cui si applicherà la struttura RFId sono:

COMPONENTE	QUANTITÀ
Unità RFId per inizializzazione, prestito e restituzione assistiti	2
Postazione RFId per prestito/restituzione non assistiti, inclusa stampante per ricevuta	1
Buca esterna per restituzione 24h/24	1
Varco antitaccheggio RFId incluso contapersone	2 coppie
Terminale RFId portatile	1
Etichette RFId per libri, neutre	60.000
Etichette RFId per periodici, neutre	10.000
Etichette RFId per supporti multimediali	1.000
Stampanti termiche	0[28]
Numero medio di utenti (card RFId)	0[29]
Numero di giorni per installazione e addestramento	10
Installazione hardware forfait	500€/gg
Eventuali altri costi	0

Tabella 6 - Dimensionamento del sistema RFId

- Le unità di prestito assistito sono assunte pari a 2 così come indicato dal personale della Biblioteca Centrale di Economia in modo che possano essere utilizzate anche per l'inizializzazione dei tag RFId.

[28] Pari a 1 nel caso in cui si ipotizzi di dotare gli utenti di tessere RFId
[29] Pari a 3000 nel caso in cui si ipotizzi di dotare gli utenti di tessere RFId

- Si ipotizza una sola stazione di autoprestito dati i volumi di libri che si prevede di taggare e il numero di prestiti annui effettuati.
- Si pone quindi a 0 Il valore delle card per gli utenti e delle stampanti termiche necessarie per la loro personalizzazione è posto a 0, giacchè la Biblioteca non intende fornire agli utenti una card RFId in sostituzione dell'attuale badge magnetico. (Verranno presentati i risultati del modello anche nel caso in cui si ipotizzi di utilizzare card RFId per gli utenti).
- Si assume pari a 10 il numero di giorni per l'installazione e la formazione del personale, per i quali, concordemente anche al parere espresso dalla Biblioteca, si assume un costo unitario di 500 euro.

7.4 I RISULTATI DELL'APPLICAZIONE DEL MODELLO: ANALISI COSTI-BENEFICI

Il modello permette di confrontare i tre scenari tecnologici descritti in precedenza. Si presentano pertanto anche i risultati che si ottengono nello scenario "scaffale aperto tecnologia bar code" anche se l'intenzione della Biblioteca è di passare alla tecnologia RFId.
Si ricorda che si è ipotizzato che i 60.000 tag acquistati per la taggatura dei volumi vengono utilizzati esclusivamente per l'identificazione dei libri posizionati a scaffale aperto (si assumono 28 ore di front-office, la consultazione a deposito continua a essere gestita come nello scenario "scaffale aperto", 4.150 sono gli utenti che usufruiscono delle attrezzature RFId installate). In questo caso devono essere probabilmente mantenuti con funzione antitaccheggio i varchi già esistenti.

7.4.1 IL VALORE DELL'INVESTIMENTO

N.B. I valori di investimento a seguire sono stati acquisiti con la massima cura, ma vanno comunque considerati come un dato indicativo.

- L'infrastruttura tecnologica nello scenario "scaffale aperto tecnologia bar-code" comprende:

COMPONENTE	QUANTITÀ	VALORE UNITARIO [€]	TOTALE [€]
Postazione bar-code per prestito e restituzione assistiti e per inizializzazione	*2*	*4.000*	*8.000*
Postazione bar-code per prestito non assistito, inclusa stampante per ricevuta	*1*	*15.000*	*15.000*
Varco antitaccheggio tecnologia banda magnetica incluso contapersone	*0*[30]	-	
Terminale bar-code portatile	*1*	*1.000*	*1.000*
Stampante bar-code	*1*	*400*	*400*
Installazione hardware forfait e addestramento	*10*	*500*[31]	*5.000*
Totale			***29.400***

Tabella 7 - Caratteristiche e costi per l'infrastruttura tecnologica nello scenario "scaffale aperto tecnologia bar-code"

[30] La Biblioteca è già dotata di varchi antitaccheggio per la banda magnetica. Non è, quindi, necessario attrezzare nuovi varchi nello scenario "scaffale aperto tecnologia bar code"
[31] Dato indicato dalla Biblioteca di Economia

A questi costi, se ne aggiungono altri necessari per mettere a regime il funzionamento dell'infrastruttura:

COMPONENTE	QUANTITÀ	VALORE UNITARIO [€]	TOTALE [€]
Etichette bar-code	*71.000*[32]	*0,02*	*1.420*
Ore di manodopera per applicazione barcode al pregresso	*1183*	*15*	*17.750*
Totale			*19.170*

Tabella 8 - Caratteristiche e costi per l'infrastruttura tecnologica nello scenario "scaffale aperto tecnologia bar-code"

- L'infrastruttura tecnologica nello scenario "scaffale aperto tecnologia RFId" comprende:

COMPONENTE	QUANTITÀ	VALORE UNITARIO [€]	TOTALE [€]
Postazione RFId per prestito/restituzione non assistiti, inclusa stampante per ricevuta	*1*	*6.000*	*6.000*
Buca esterna per restituzione 24h/24	*1*	*6.000*	*6.000*
Varco antitaccheggio RFId incluso contapersone	*2*	*7.000*	*14.000*
Terminale RFId portatile	*1*	*4.000*	*4.000*
Installazione hardware forfait e addestramento	*10*	*500*	*5.000*
Totale			***39.000***

Tabella 9 - Caratteristiche e costi per l'infrastruttura tecnologica nello scenario "scaffale aperto tecnologia RFId"

A questi costi, se ne aggiungono altri necessari per mettere a regime il funzionamento dell'infrastruttura:

COMPONENTE	QUANTITÀ	VALORE UNITARIO [€]	TOTALE [€]
Etichette RFId per libri, neutre	*60.000*	*0,5*	*30.000*
Etichette RFId per CD/DVD circolare, neutre	*1.000*	*0,6*	*600*
Etichette RFId per periodici, neutre	*10.000*	*0,1*	*1.000*
Ore di manodopera per taggatura del pregresso	*1.100*	*15*	*16.500*
Totale			***48.100***

Tabella 10 - Caratteristiche e costi per l'infrastruttura tecnologica nello scenario "scaffale aperto tecnologia RFId"

- I valori degli investimenti presentati rappresentano un valore medio ricavato dal lavoro di analisi eseguito dal Politecnico di Milano, sulla base di interviste a biblioteche che hanno applicato la tecnologia RFId e a fornitori di soluzioni tecnologiche;

[32] Il dato è ricavato dalla somma delle etichette da apporre su libri, periodici e multimediali

- Il valore delle giornate di installazione hardware e addestramento è stato indicato dalla Biblioteca stessa ed è assunto pari a 500 euro al giorno;
- Il valore della postazione di autoprestito bar code è stato indicato dalla Biblioteca a seguito di un'offerta ricevuta da una ditta fornitrice di tecnologia;
- Il costo unitario della manodopera necessaria per la taggatura del pregresso è assunto pari al costo della manodopera di front-office, dato fornito dalla Biblioteca;
- I risultati economici presentati possono pertanto risentire dei valori di costo che il provider che la Biblioteca selezionerà per la fornitura applicherà alla Biblioteca stessa.

7.4.2 I RISULTATI DEL MODELLO PER LA BIBLIOTECA

Le prime considerazioni sul modello bibliotecario sono le seguenti:

- Il personale di front-office è considerato una risorsa scalabile;
- La scelta di etichettare 60.000 dei 173.000 volumi presenti nella struttura, fa ipotizzare che i libri presenti in deposito non vengano etichettati e quindi che la consultazione/prestito di questo materiale avvenga come nello scenario attuale;
- Tenimento degli scenari tecnologici con bar code e con RFId il valore del tempo dedicato all'assistenza agli utenti pari a quello attuale;
- I risultati riportati nel seguito derivano dalla modellizzazione delle attività che si svolgono in biblioteca così come elaborata nel modello del Politecnico di Milano.

Da queste premesse si ottengono i seguenti risultati:

BIBLIOTECA	APERTO	BAR-CODE	RFID	ΔRFID[33]	Δ%RFID[34]
INVESTIMENTO	€ -	€ 48.570	€ 87.100		
COSTI CORRENTI					
Attività di back-office	€ 37.125	€ 37.949	€ 34.498	- € 2.627	-7%
Attività di front-office	€ 58.920	€ 56.026	€ 46.393	- € 12.527	-21%
Materiali	€ 1.253	€ 1.440	€ 1.871	€ 618	49%
Revisione inventariale	€ 13.313	€ 9.482	€ 4.157	- € 9.156	-69%
Reference	€ 57.000	€ 57.000	€ 57.000	€ -	0%
Totale	€ 167.611	€ 161.897	€ 143.919	- € 23.692	-14%

Tabella 11 - Risultati del modello

[33] Variazione assoluta tra il valore nello scenario con tecnologia RFId e quello nello scenario scaffale aperto senza tecnologia

[34] Variazione % tra il valore nello scenario con tecnologia RFId e quello nello scenario scaffale aperto senza tecnologia

Il valore dell'investimento è dato dalla somma dei valori riportati nelle tabelle 8 e 9 per la tecnologia bar code e 10 e 11 per la tecnologia RFId.
I costi correnti presentano il seguente andamento nei tre scenari tecnologici considerati:

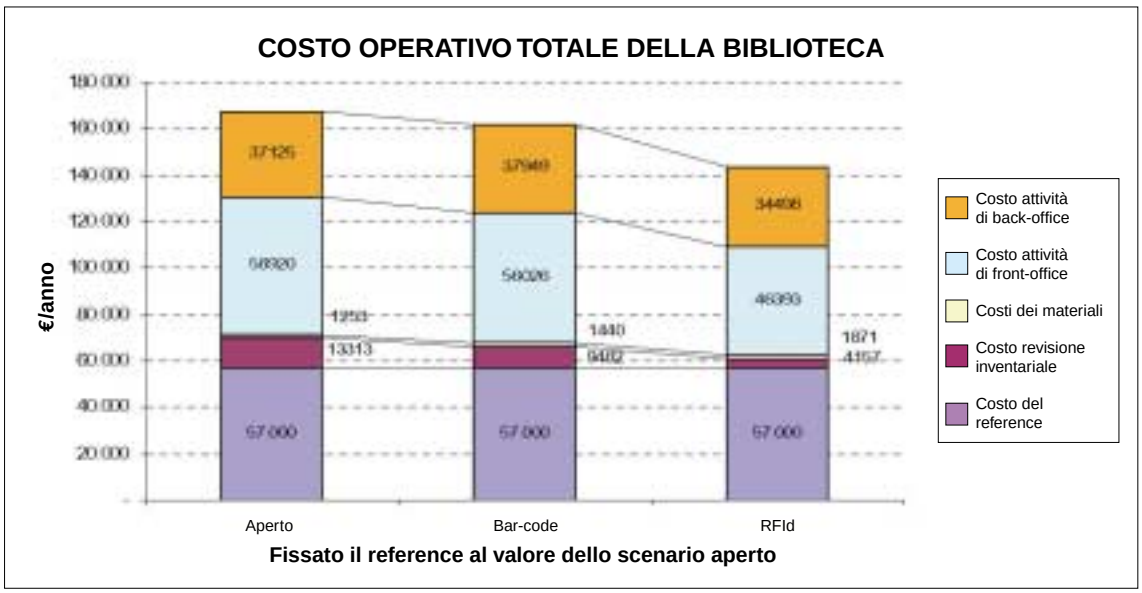

Figura 32 - Costo operativo totale della biblioteca per i tre scenari prospettati

Nello specifico:

- Il passaggio alla soluzione "scaffale aperto tecnologia bar-code" permette un risparmio annuo di circa 5.715 euro, pari al 3,4% dei costi totali;
- Il passaggio alla soluzione "scaffale aperto tecnologia RFId" permette un risparmio annuo di circa 23.692 euro, pari al 14% dei costi totali.

A fronte di questi risparmi, sulla base dell'investimento iniziale sono stati calcolati il tempo di payback (non attualizzato) e il Net Present Value (NPV) delle soluzioni tecnologiche bar-code e RFId rispetto alla situazione attuale. Per il calcolo si è ipotizzato un tasso di attualizzazione del 9% e un orizzonte temporale pari a 5 anni.

	TEMPO DI PAY BACK [ANNI]	NPV [€]
Bar-code	8,50	€ -26.342
RFId	3,68	€ 5.054

Tabella 12: Pay back e NPV per l'investimento in tecnologia bar-code e RFId

Come si evince dalla tabella sopra riportata, l'investimento in tecnologia bar-code all'interno della struttura bibliotecaria considerata non è economicamente conveniente, mentre l'investimento in tecnologia RFId ha un tempo di pay-back compreso all'interno dei 5 anni di valutazione ed un NPV positivo.

Tali valori risultano coerenti con i dati inseriti in input, in particolar modo con il numero di prestiti. E' ovvio, infatti, che i benefici di una tecnologia di identificazione automatica sono tanto maggiori quanto più i documenti subiscono delle movimentazioni per le quali è necessario provvedere ad una loro identificazione. Variando, infatti, tale parametro i risultati sono ancora più positivi per la tecnologia RFId.
Nel seguito si riporta il valore, espresso in ore/anno, del tempo dedicato in biblioteca a ciascuna attività sopra individuata.

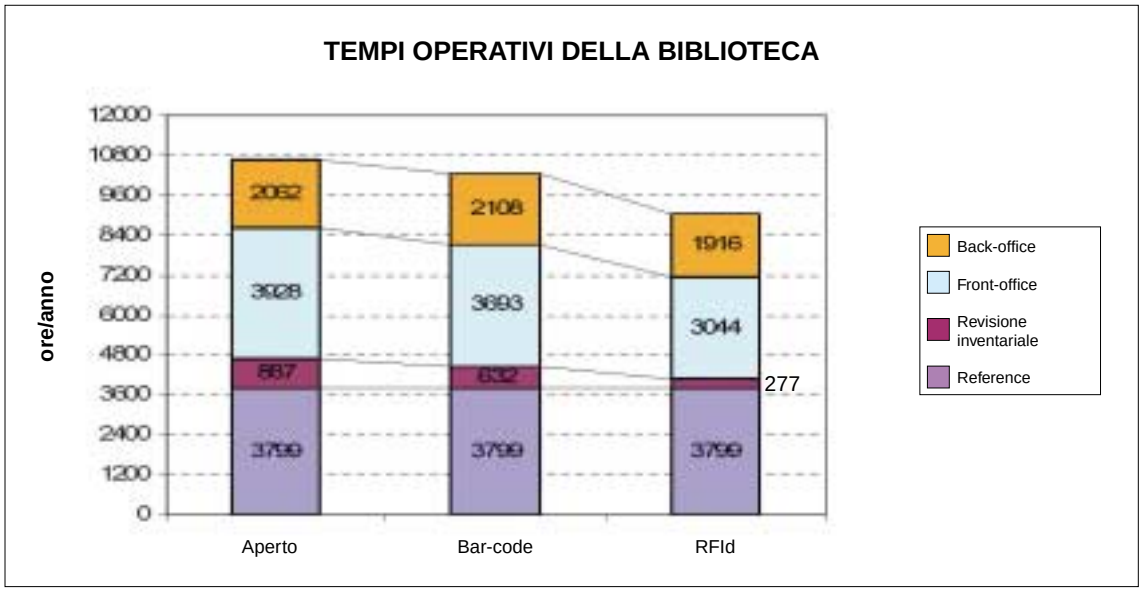

Figura 33 - Tempi operativi stimati per i diversi tipi di soluzione

E' possibile analizzare nel dettaglio le componenti del costo e del tempo annuo della biblioteca.
Il costo delle attività di back office (acquisizione, catalogazione, gestione dei seriali e conservazione) riporta leggere variazioni al variare dello scenario tecnologico così come il tempo dedicato allo svolgimento di queste attività.

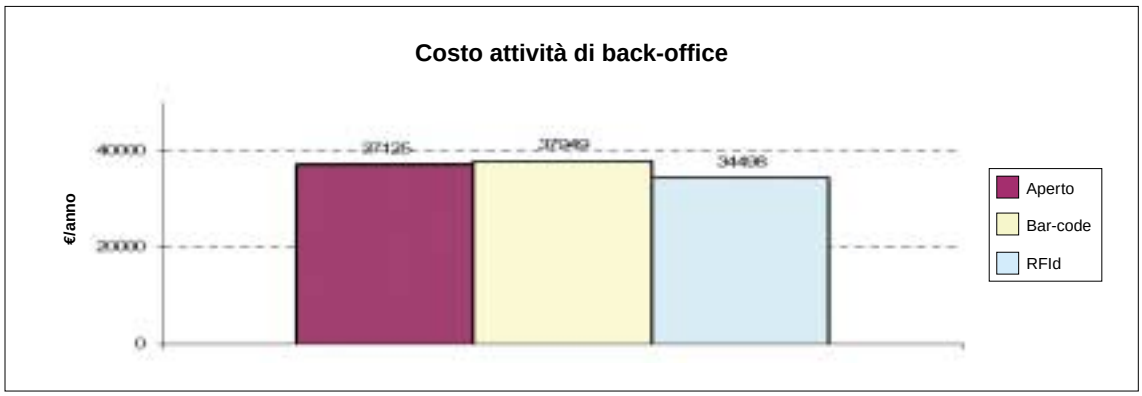

Figura 34 - Costo delle attività di back office

Figura 35 - Tempo dedicato alle attività di back office

Il costo corrente dei materiali si incrementa a causa del maggiore costo del tag relativo ai materiali che vengono acquistati annualmente.

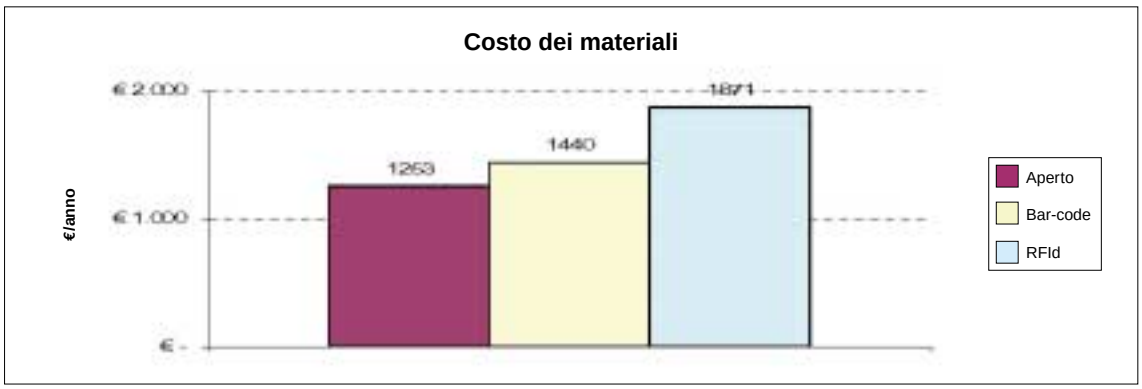

Figura 36 - Costo dei materiali

Si riduce notevolmente il costo della revisione inventariale alla quale corrisponde un notevole risparmio di tempo necessario per la sua esecuzione. Con la tecnologia bar-code è possibile ridurre del 29% il tempo necessario per una ricognizione inventariale, mentre con

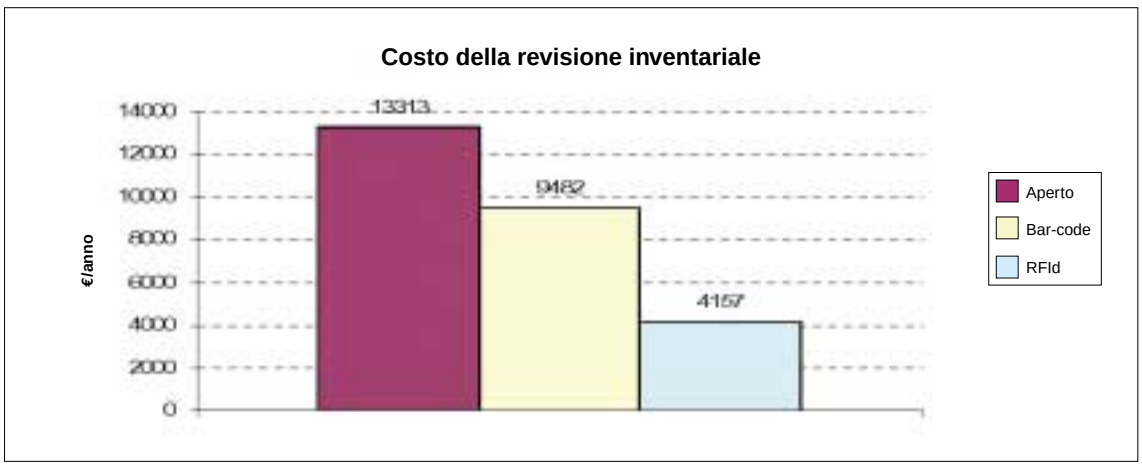

Figura 37 - Costo dell'operazione di revisione inventariale

l'ausilio dell'RFId tale valore si riduce del 69%. Si deve naturalmente ricordare che tale valore è riferito alla parte di materiale librario etichettato mediante tecnologia RFId. Si ricorda, inoltre, che si ipotizza un funzionamento affidabile dei sistemi portatili di lettura dei tag RFId sui libri.

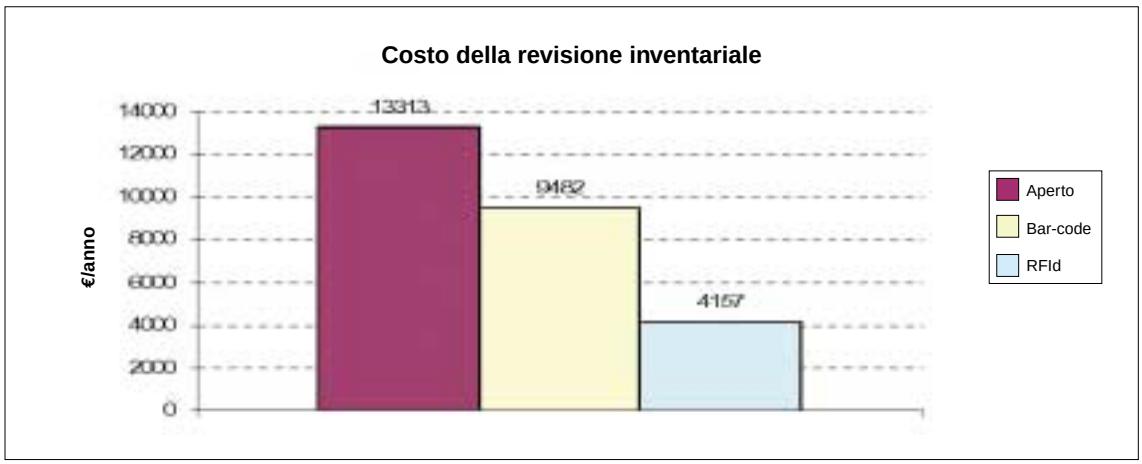

Figura 38 - Tempo necessario per l'operazione di revisione inventariale

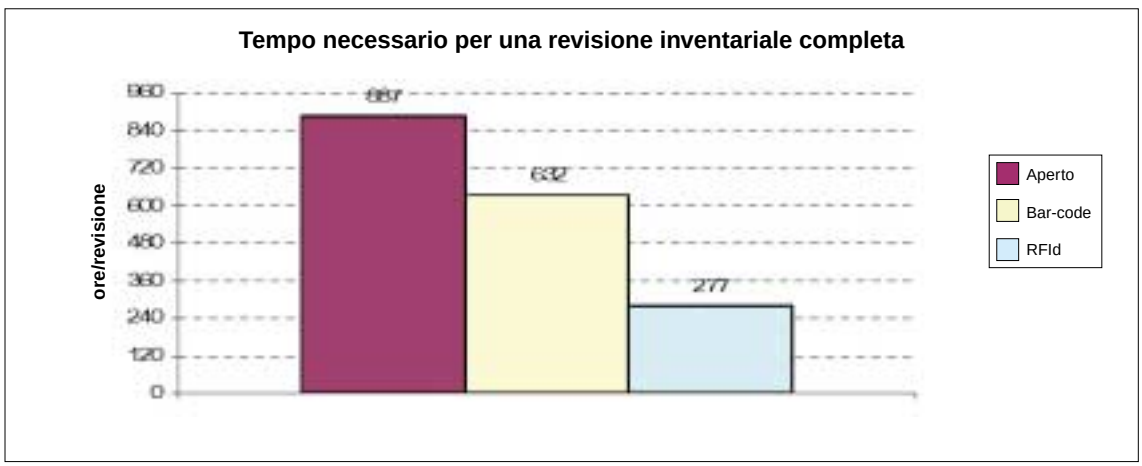

Figura 39 - Costo per le attività di front-office

E' interessante approfondire nel dettaglio le componenti del costo delle attività di front-office in modo da comprendere su quali di esse ha maggiore impatto la tecnologia RFId.
Come si nota dalla figura seguente, i benefici maggiori si hanno nell'attività di riordino, maggiormente automatizzata grazie all'ausilio del palmare RFId, e di prestito.
Come si nota, il valore della consultazione è assunto costante ipotizzando che i libri in deposito non vengano etichettati con RFId oppure bar-code.

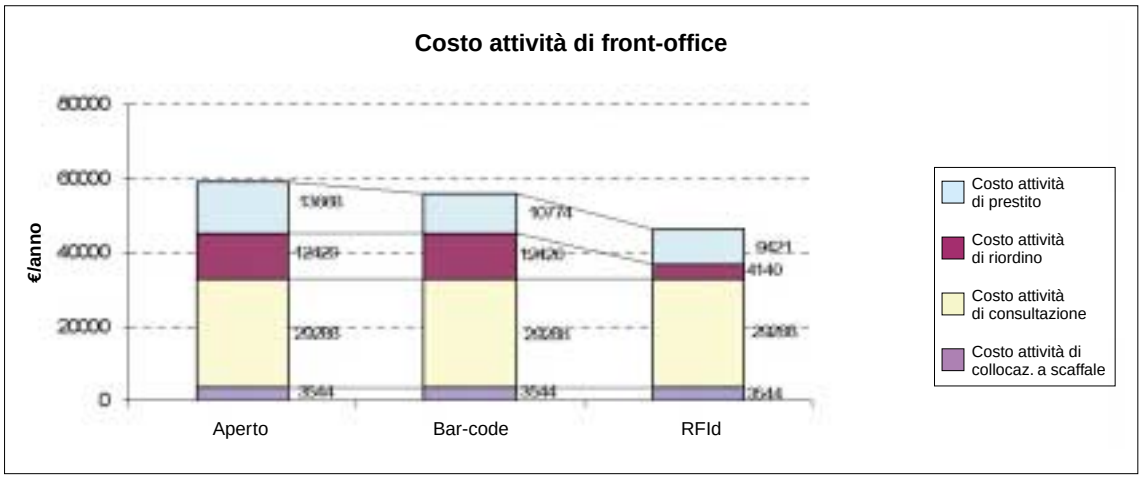

Figura 39 - Costo per le attività di front-office

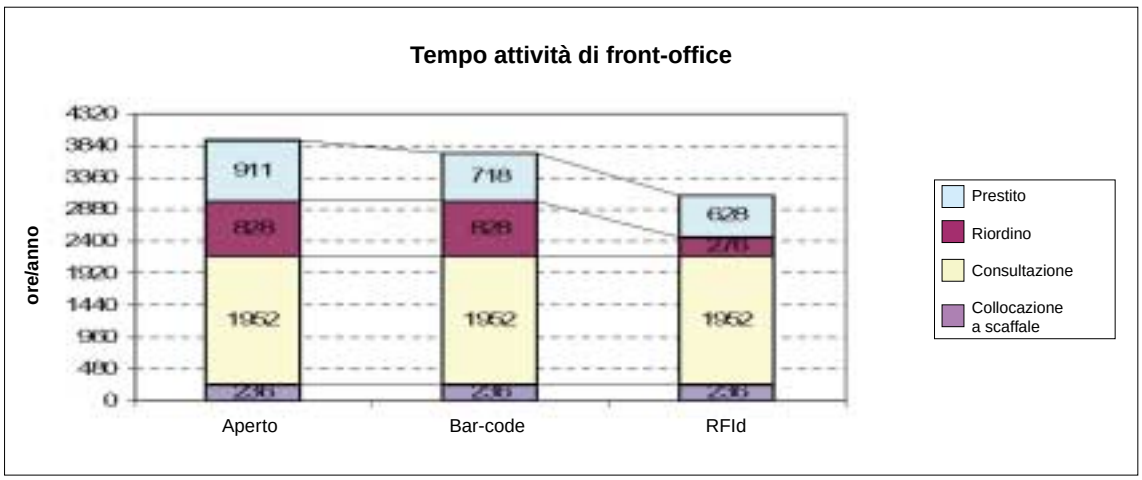

Figura 40 - Tempo necessario per le attività di front-office

I risultati economici qui descritti non variano nel caso in cui si ipotizzi un livello di reference ideale per ciascun utente e pari a 4 minuti. In questo caso diminuisce naturalmente il costo del reference che è già sufficiente per ottenere tale valore nello scenario attuale, portandosi a 6.150 euro all'anno.

7.4.3 I RISULTATI DEL MODELLO PER L'UTENTE

Il modello consente di stimare anche i vantaggi che la tecnologia RFId apporta all'utente e non solo ai costi operativi della biblioteca. Delle diverse misure di servizio, quella relativa alla misura del tempo in coda in corrispondenza del banco del prestito è certamente la principale. L'analisi del tempo medio dell'utente nel sistema nei momenti di picco mostra come sia possibile una notevole riduzione dei tempi grazie all'impiego della tecnologia RFId[35]. L'RFId consente in questo caso un risparmio di tempo analogo al bar-code e pari circa il 20%.

[35] Tale analisi è stata eseguita avvalendosi all'interno del modello del Politecnico di Milano sulla teoria delle code

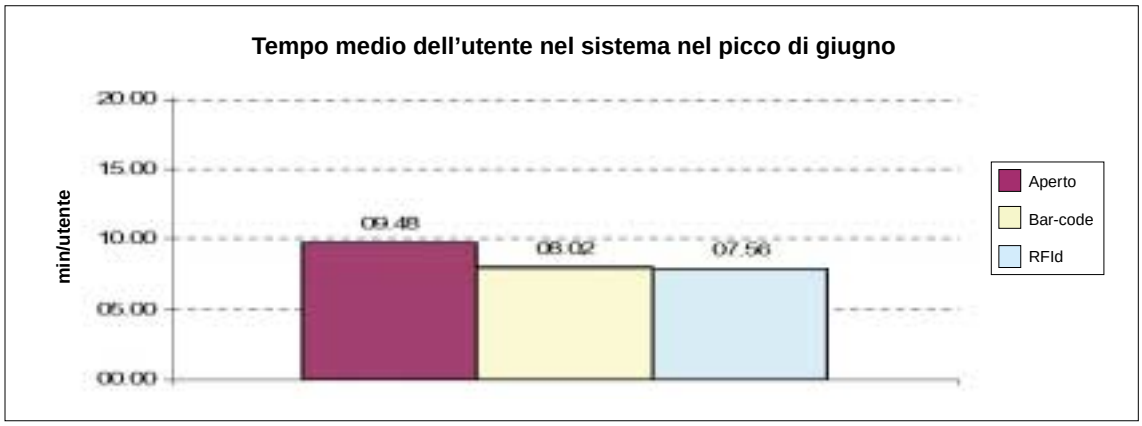

Figura 41 - Tempo medio di permanenza dell'utente nel momento di massimo picco

Quale ulteriore beneficio, il modello mostra come complessivamente il tempo per l'assistenza agli utenti si incrementi notevolmente al passaggio alla tecnologia RFId, poiché si solleva il personale di front-office di parte delle operazioni di registrazione dei prestiti.

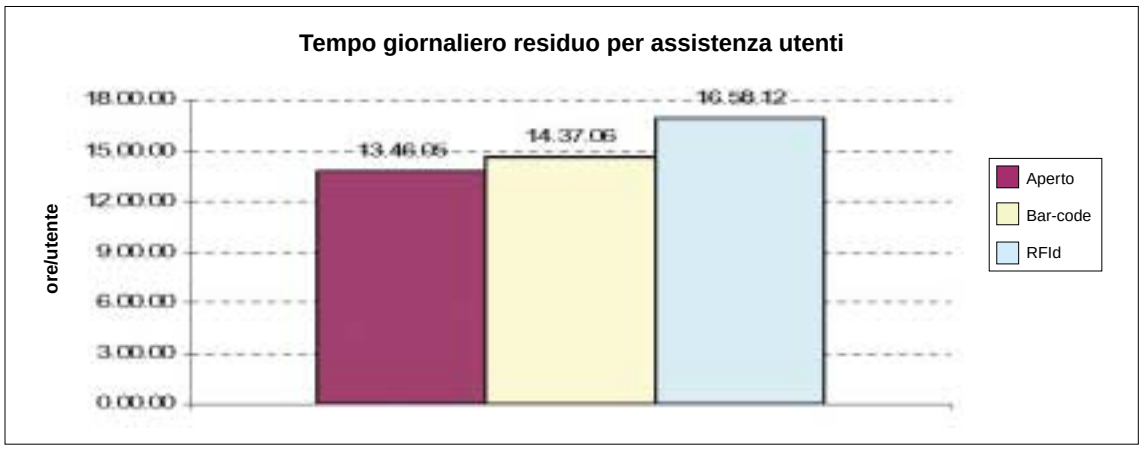

Figura 42 - Tempo residuo dedicabili all'assistenza clienti

7.4.4 I RISULTATI DEL MODELLO PER IL LIVELLO DI SERVIZIO

Il livello di servizio viene valutato tramite una media che pesa allo stesso modo il punteggio attribuito al tempo medio trascorso da un utente nel sistema nel picco e al tempo di reference per utente.
La formula utilizzata è la seguente:

$$Livello\ servizio = 0{,}5*Punteggio\ t_{medio}\ nel\ sistema + 0{,}5*Punteggio\ t_{reference}\ per\ utente$$

Nel modello elaborato sono stati individuati degli intervalli di variazione rispettivamente del tempo trascorso nel sistema e del tempo di reference a ciascuno dei quali è stato attribuito un punteggio su una scala che varia da 0 a 1. Ad esempio, per un tempo trascorso nel sistema superiore ai 30 minuti si associa un punteggio pari a 0.

Se ne valuta l'andamento in relazione a:

- Caso base: scenario scaffale aperto no tecnologia;
- RFId reference fissato all'aperto: costo annuo e livello di servizio valutati fissando il livello di reference pari a quello ottenuto nello scenario "scaffale aperto no tecnologia";
- RFId reference fissato a 4 minuti: costo annuo e livello di servizio valutati fissando a 4 minuti per utente il valore del reference;
- RFId: costo annuo e livello di servizio a risorse fissate.

Lo stesso procedimento è stato seguito nel caso in cui si prenda in considerazione la tecnologia bar-code.
L'andamento che si ottiene, funzione dei dati inseriti in input (in particolare le ore di front office e il numero di prestiti annui) ha un andamento particolare, diverso da quello registrato in altre strutture bibliotecarie.
Si ottiene un livello di servizio pari a 0,9 già nello scenario attuale così come nello scenario con tecnologia bar-code o con tecnologia RFId (a risorse fissate oppure fissato il livello di reference al caso dello scenario scaffale aperto no tecnologia). La ragione di tale risultato risiede nel fatto che con gli attuali livelli di prestiti, e quindi di numero di utenti che richiedono un prestito, l'attuale struttura non appare congestionata.

L'attuale livello di reference è superiore ai 4 minuti desiderabili ed è per questo motivo che nella situazione 3 il livello di servizio diminuisce.

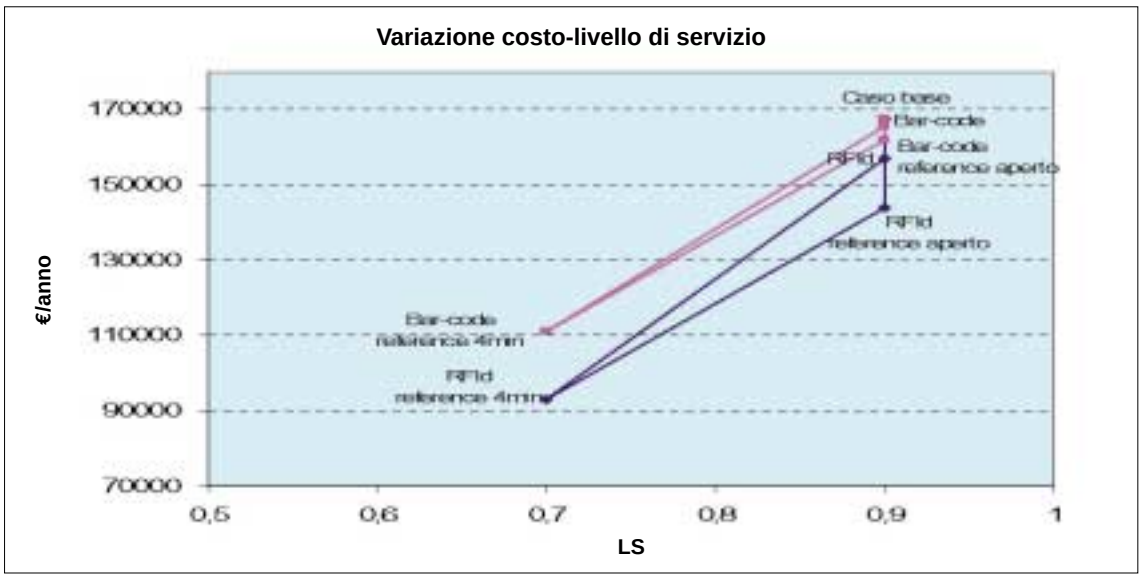

Figura 43 - Andamento Livelli di servizio / Costi

Si ricorda che agli utenti non viene distribuita una card RFId, ma sono identificati in biblioteca mediante la card a banda magnetica fornita dall'Ateneo. Nel caso in cui si volesse dotare

gli utenti di card RFId non varierebbero di gran lunga i benefici in termini di efficienza (si otterrebbe probabilmente una maggiore facilità nell'utilizzo della tessera da parte degli utenti), ma aumenterebbe l'investimento. In particolare si dovrebbero provvedere ad acquistare:

COMPONENTE	QUANTITÀ	VALORE UNITARIO [€]	TOTALE [€]
Stampante termica a colori	*1*	*1.250*	*1.250*
Smart card RFId	*3.000*	*1,29*	*3.870*
Totale			***5.120***

Tabella 13 - Costo componenti aggiuntivi da acquistare per un sistema RFId con smart card

Si ottiene un NPV di poco negativo (-66 euro). Oltre a ciò potrebbero essere previsti dei costi per l'installazione del middleware, che potrebbero non venire sostenuti interamente dall'Ateneo.

7.4.5 ANALISI DI SENSITIVITÀ

Come emerso dagli incontri con la Biblioteca e come riportato in allegato, si è deciso di effettuare analisi di sensitività sul numero di consultazioni del materiale a scaffale aperto poiché spesso gli utenti si recano presso la struttura per trovarvi un luogo tranquillo in cui studiare, anche usufruendo dei propri libri di testo o appunti.
Per tale motivo si apportano le seguenti variazioni ai parametri:

- n° consultazioni [documenti/anno]: da 88.000 a 44.000;
- n° ripristini giornalieri materiale consultazione [ripristini/giorno]: da 16 a 8.

Si ottengono i seguenti valori di costo:

BIBLIOTECA	APERTO	BAR-CODE	RFID	ΔRFID[36]	Δ%RFID[37]
INVESTIMENTO	€ -	€ 48.570	€ 87.100		
COSTI CORRENTI					
Attività di back-office	€ 37.125	€ 37.949	€ 34.498	- € 2.627	-7%
Attività di front-office	€ 47.776	€ 43.882	€ 34.249	- € 12.527	-27%
Materiali	€ 1.253	€ 1.440	€ 1.871	€ 618	49%
Revisione inventariale	€ 13.313	€ 9.482	€ 4.157	- € 9.156	-69%
Reference	€ 69.144	€ 69.144	€ 69.144	€ -	0%
Totale	€ 167.611	€ 161.897	€ 143.919	- € 23.692	-14%

Tabella 14 - Confronto costi complessivi per gli scenari considerati

[36] Variazione assoluta tra il valore nello scenario con tecnologia RFId e quello nello scenario scaffale aperto senza tecnologia

[37] Variazione % tra il valore nello scenario con tecnologia RFId e quello nello scenario scaffale aperto senza tecnologia

Rispetto ai risultati presentati nei paragrafi precedenti si nota che permangono invariati i costi delle attività di back-office, dei materiali e della revisione inventariale, mentre diminuisce il costo delle attività di front-office ed aumenta quello del reference.
Infatti, al diminuire del numero di consultazioni del materiale a scaffale aperto, e di conseguenza del numero di ripristini necessari per riordinare i documenti, si rende disponibile una percentuale di tempo maggiore da dedicare all'assistenza agli utenti.
Evidenziando in dettaglio le diverse voci che compongono il costo dell'attività di front-office, infatti, si nota che diminuisce del 41% il costo della consultazione proprio perché è stato decrementato il numero di riordini del materiale consultato. Tale variazione corrisponde ad un'altrettanta riduzione del tempo dedicato a questa attività ed ad un incremento di quello dedicato al reference.

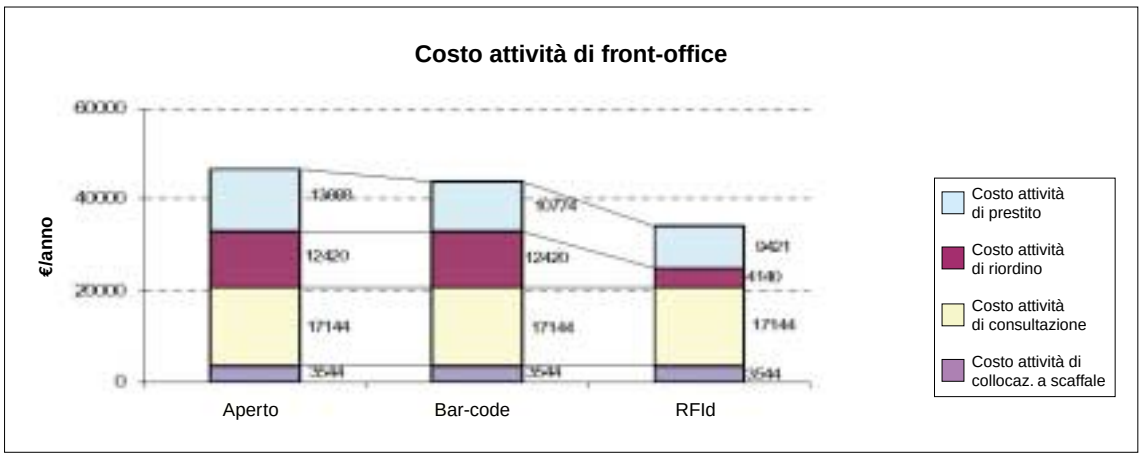

Figura 44 - Costo attività di front office

L'analisi economica (NPV e tempo di pay back) non subisce variazioni rispetto a quanto presentato in precedenza poiché rimane costante la variazione tra i costi correnti nello scenario attuale e nei due scenari tecnologici analizzati. In particolare, nel caso dell'RFId si ottiene, come in precedenza, una riduzione dei costi totali di gestione pari a circa 23.692 euro.

7.5 CONSIDERAZIONI SUI BENEFICI DELL'INTRODUZIONE DELLE TECNOLOGIE RFID

7.5.1 CONSIDERAZIONI SUI BENEFICI DI EFFICIENZA

Dall'analisi condotta a partire dai dati forniti in input dal personale della biblioteca, è possibile fare le seguenti considerazioni sui risultati del modello:

- Al momento il valore economico generato dall'adozione del RFId appare molto modesto. Questo valore aumenta al crescere del numero di movimentazioni dei documenti;

- In valore assoluto il maggiore beneficio economico della tecnologia si manifesta nelle attività di front-office, specialmente nelle attività di prestito, grazie alla possibilità di utilizzare il prestito self-service, e di riordino;
- In termini percentuali il maggior impatto economico si ottiene nell'attività di revisione inventariale, ma è doveroso ricordare che tale impatto è calcolato nell'ipotesi che la funzionalità di inventario automatico sia funzionante ed efficace.

7.5.2 CONSIDERAZIONI SUI BENEFICI DI EFFICACIA

L'adozione dell'RFId offre i seguenti benefici di efficacia per gli utenti del sistema librario e per il personale addetto alla sua gestione:

- L'utente sperimenta un incremento del livello di servizio, misurato come riduzione dei tempi di attesa. L'effetto è crescente al crescere del volumi di prestito e al concentrarsi dell'afflusso degli utenti;
- Il minor impegno dei bibliotecari in attività di registrazione dei prestiti o consultazioni può agevolare un'assistenza più approfondita e qualitativamente superiore all'utente, incrementando il livello di servizio fornito;
- Il sistema è in grado di registrare il numero univoco associato ad eventuali libri che escono dalla biblioteca senza permesso, con un conseguente incremento del grado di controllo sul patrimonio librario;
- La possibilità di eseguire più frequentemente la revisione inventariale accresce ulteriormente il controllo sul patrimonio librario;
- La soluzione RFId per il riordino continuo garantisce un maggiore ordine negli scaffali e diminuisce le difficoltà di ricerca per l'utente e il bibliotecario.

8. Risultati sperimentali del Laboratorio Cnipa

In questo capitolo sono illustrati i risultati di una campagna di sperimentazione realizzata dal Laboratorio sperimentale del Cnipa in collaborazione con i laboratori del CATTID (Centro per le Applicazioni della Televisione e delle Tecniche di Istruzione a Distanza) dell'Università "Sapienza" di Roma.
L'attività sperimentale è stata specificatamente orientata alla verifica delle caratteristiche di interoperabilità e sicurezza in ambienti RFId multivendor e multistandard. L'esperienza condotta in laboratorio, durata oltre sei mesi, ha consentito di acquisire elementi concreti circa la funzionalità e le prestazioni dell'RFId in alcune situazioni di utilizzo tipiche della Pubblica Amministrazione. Nel seguito, sono illustrati in maniera sintetica gli ambienti sperimentali ed i risultati più significativi tra quelli osservati.

8.1 Obiettivi della sperimentazione

I campi di applicazione della tecnologia RFId nella Pubblica Amministrazione sono molto vari, con esigenze molto eterogenee in termini di *interoperabilità*, di *sicurezza* e *privacy*. L'esistenza di diversi standard di comunicazione Tag/reader, molti dei quali proprietari (e.g. Tag-IT, I-CODE ecc.), la possibilità di avere dei Tag con diverse prestazioni anche all'interno dello stesso standard (riconducibili ad esempio al particolare procedimento costruttivo), potrebbero vincolare alla scelta di una ben specifica tipologia di Tag, se non addirittura a quella di uno specifico produttore. Si pensi ad esempio ad un'applicazione in ambito sanitario in cui un paziente deve essere identificato (e collegato ai suoi dati clinici) attraverso il suo bracciale RFId in diverse unità sanitarie dislocate sul territorio: la compatibilità del Tag con i diversi lettori presenti sul territorio è fondamentale.
L'interoperabilità è quindi la principale e fondamentale caratteristica richiesta nei sistemi altamente distribuiti e cooperanti della Pubblica Amministrazione (e.g. unità sanitarie, magazzini doganali, tracciamento alimenti ecc.) e in cui in generale non esiste la possibilità del controllo centralizzato.
Pertanto, l'ambiente di riferimento per le sperimentazioni realizzate è, per quanto possibile, volutamente caratterizzato da dispositivi "multi-vendor". In questo tipo di scenario è lecito attendersi alcuni problemi di interoperabilità, legati principalmente alla parziale frammentazione degli standard tecnologici adottati per le comunicazioni ed è prevedibile anche una disomogeneità di prestazioni rispetto ai valori operativi dichiarati dai fornitori. In questo

senso, l'osservazione dei valori effettivamente riscontrabili sul campo evidenzia fluttuazioni prestazionali non trascurabili, anche per dispositivi appartenenti ad una medesima classe funzionale e con fattori di forma simili. La cause di tali fluttuazioni potrebbero essere riconducibili a ragioni che possono essere le più varie e legate, ad esempio, allo specifico produttore, al particolare procedimento costruttivo e a fattori ambientali.
Nei test sono stati utilizzati dispositivi RFId progettati per il funzionamento in due diverse porzioni di spettro: elementi funzionanti in HF (13,56Mhz se non specificato diversamente) e UHF (868Mhz, in conformità con le attuali normative in materia).
Il piano di sperimentazione è composto di quattro serie di esperimenti:

- misura dell'affidabilità della lettura e valutazione del livello di compatibilità tra lettori e Tag multistandard e multivendor;
- misura dell'affidabilità della lettura di Tag in situazione "ideale" ed in presenza di materiali interferenti;
- misura della capacità di lettura dei Tag in condizioni di interferenza tra lettori;
- valutazione della robustezza dei Tag ad attacchi "semplici".

8.2 AFFIDABILITÀ DELLA LETTURA E COMPATIBILITÀ DEI TAG IN AMBIENTI MULTISTANDARD

L'esperimento è consistito nella verifica della capacità di un reader di leggere correttamente un insieme di Tag di diversi produttori. Tutti i sistemi utilizzati in questo esperimento operano in banda HF.
L'esperimento ha i seguenti obiettivi specifici:

1. misurare, in una situazione ideale, l'affidabilità di un reader nella lettura di un Tag;
2. misurare la compatibilità, da parte di ciascun reader, nella lettura di Tag multistandard o multivendor;
3. sperimentare la possibilità di sviluppare dei software che migliorino le prestazioni dei reader, come misurati al punto precedente.

Sono stati studiati, inoltre, i meccanismi che consentono di configurare la modalità di lettura di ciascun reader.

8.2.1 DESCRIZIONE DELL'ESPERIMENTO

Il test è stato effettuato utilizzando sette diversi reader commerciali. Nello specifico:

1. antenna planare A, con controller esterno indipendente, interfaccia comandi vs PC su collegamento seriale (anno di produzione 2001);
2. antenna Gate B, con controller esterno indipendente, interfaccia comandi vs PC su collegamento seriale (anno di produzione 2001);

3. antenna planare C, con controller emulato via software e interfaccia comandi vs PC su collegamento USB (anno di produzione 2004);
4. lettore portatile D, modello palmare ad antenna integrata con software di gestione proprietario (anno di produzione 2002);
5. lettore portatile E, modello palmare ad antenna integrata con software di gestione realizzato su piattaforma WindowsCE (anno di produzione 2005);
6. lettore portatile F, modello PC palmare con hardware di lettura su scheda SD e software di gestione realizzato su piattaforma WindowsCE (anno di produzione 2006).

I Tag selezionati per questo esperimento appartengono alle seguenti tipologie:

- I-Code 1
- I-Code SLI
- ISO 15693 – 18000-3
- TI Tag-It
- MiFare

L'insieme dei Tag utilizzato nell'esperimento, e pertanto appartenenti alle categorie sopra elencate, è detto nel seguito Tag-set.

Il setup dei test è consistito in:

- preparazione e test di funzionalità degli apparati, e specificatamente:
  - studio dell'interfaccia di gestione dello specifico reader;
  - predisposizione del firmware di controllo, ove fosse necessario;
- configurazione ambiente per l'interfaccia software di gestione, ove fosse necessario;
- sviluppo del software di lettura, ove possibile, per consentire in maniera automatica la lettura dell'intero Tag set;
- debugging e ottimizzazione.

La procedura di test per i singoli apparati è consistita in:

- selezione di una modalità di lettura;
- posizionamento del Tag-set nella zona di lettura "ideale";
- rilevazione dell'esito della lettura per ciascun Tag componente il set.

Sono stati effettuati, complessivamente, 21 test, dove per test si intende la lettura dell'intero Tag-set con uno dei reader selezionati.
Il gruppo di test è stato effettuato in un periodo di 7 giorni, impegnando una media di 3 ore per lo svolgimento di ogni test.

8.2.2 RISULTATI E CONCLUSIONI

Prima di tutto, si osserva che tutti i reader in prova sono stati in grado di leggere correttamente i Tag per i quali erano configurati. Pertanto, tutti i reader hanno realizzato la funzione di lettura correttamente e secondo le aspettative.

Le valutazioni di interoperabilità hanno consistito nella verifica della capacità dei reader di modificare, con un'operazione manuale o automatica, la modalità (cioè lo standard) di lettura.

Pertanto, i lettori sottoposti a prova sono stati classificati come segue, sulla base della capacità di leggere Tag multiprotocollo:

- lettori monoprotocollo, incapaci cioè di commutare da una modalità di lettura ad un'altra;
- lettori multiprotocollo non adattativi: la commutazione da uno standard ad un altro avviene attraverso un comando manuale dell'operatore;
- lettori multiprotocollo, che utilizzano ciclicamente più protocolli per tentare di leggere i Tag.

Di conseguenza, con i lettori in dotazione al laboratorio ed il software fornito a corredo, solo in alcuni casi è stato possibile effettuare una lettura contemporanea dei diversi Tag senza un intervento diretto dell'operatore.
La maggior parte degli apparati di lettura, ed in particolar modo quelli prodotti precedentemente al 2001, non prevedono un supporto multiprotocollo o "hot-swap". Per gli apparati sottoposti a test in questo ambito ed in particolare per le due antenne di più vecchia produzione, la configurazione di una data modalità di lettura si realizza caricando il firmware e riavviando il controller (Apparati A e B). Questa operazione richiede l'intervento di un tecnico specializzato e può durare anche decine di secondi[38].
Per tutti i restanti reader è stato possibile sviluppare una semplice procedura software che configura ciclicamente la modalità di lettura dei Tag. È stato misurato il tempo necessario al reader per effettuare il cambio della modalità di trasmissione e riportare l'avvenuta lettura del Tag. Questo è risultato variabile da circa 2 secondi (modello C) fino a qualche frazione di secondo per il modello palmare ad antenna integrata (modello D), per il quale è stato quindi possibile realizzare un'applicazione, per quanto essenziale, in grado di consentire la lettura semi-contemporanea del Tag set mascherando la complessità sottostante.
Nei test condotti sui sei lettori utilizzati, solo in tre di questi è stata riscontrata una incompatibilità verso un tipo specifico di Tag. In particolare, per questi tre apparati, non è stato possibile reperire librerie software che consentissero la lettura di Tag di tipo MiFare. Va notato comunque che sono gli unici Tag appartenenti al set che comprendono funzionalità per la cifratura del canale on-air, adatti quindi ad applicazioni particolari.
Per i restanti lettori è sempre stato possibile reperire i componenti software necessari a consentire la lettura dell'intero Tag-set.
Dall'osservazione dei risultati è evidente che il progresso tecnologico degli ultimi quattro-cinque anni ha messo a disposizione pacchetti di sviluppo che permettono una personalizzazione rapida e flessibile secondo le proprie esigenze, offrendo trasparenza rispetto alle complessità tecnologiche. Apparati risalenti al 2000-2001 o precedenti risentono molto della

[38] Il caricamento del firmware sul controller si fa attraverso la connessione seriale del controller di antenna ad un PC

frammentazione degli standard costruttivi e dei problemi di incomunicabilità relativi, fatto che può in parte essere ovviato tramite l'utilizzo di apparati di lettura di ultima generazione, più sofisticati dal punto di vista hardware.

8.3 LETTURA DI TAG IN PRESENZA DI MATERIALI INTERFERENTI

L'esperimento ha l'obiettivo di misurare la probabilità di errore nella lettura di Tag in funzione del tipo di imballaggio che li contiene. In particolare, sono state eseguite prove con i seguenti imballaggi:

- imballi vuoti (carta);
- imballi liquidi;
- imballi di metallo;
- Tetra-Pak.

Secondariamente, è stata misurata la distanza massima alla quale è possibile effettuare correttamente la lettura di un Tag, in funzione del tipo di imballaggio che lo contiene.

8.3.1 DESCRIZIONE DELL'ESPERIMENTO

Il test è stato effettuato utilizzando un'antenna in configurazione gate (A) ed un'antenna planare da tavolo (B). La Figura 45 illustra lo scenario del test ed evidenzia il gate e l'antenna da tavolo.

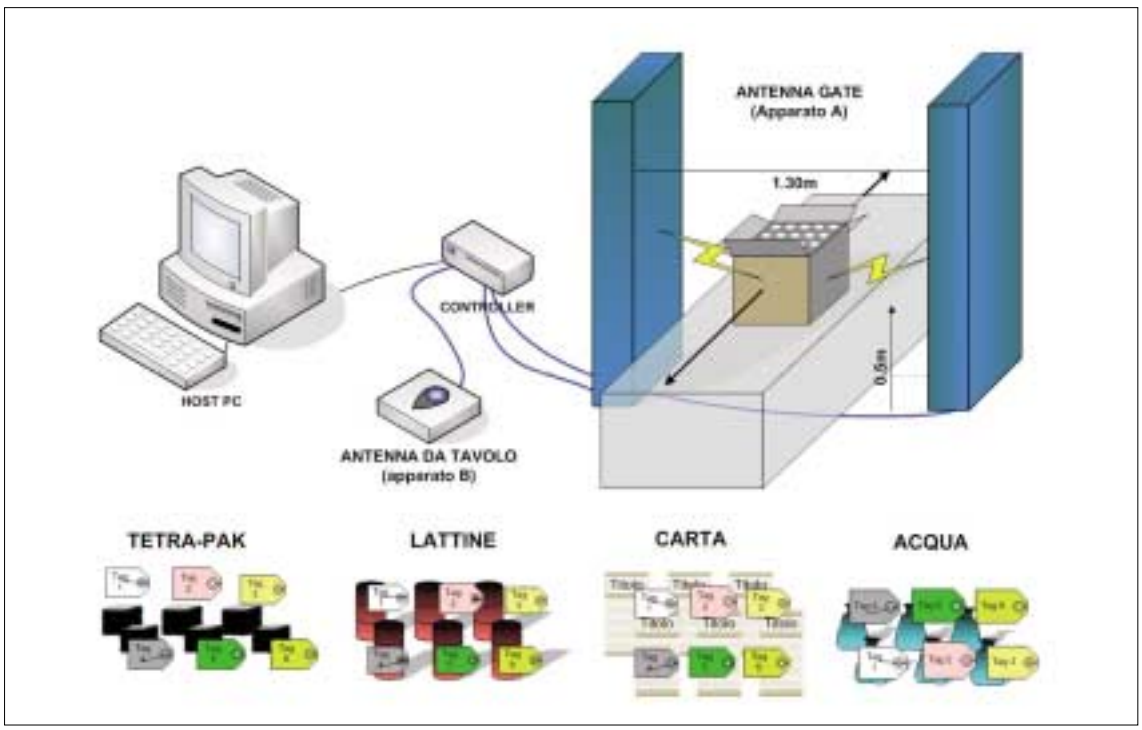

Figura 45: Schema dell'apparato sperimentale

Il setup della prova ha previsto:

- Selezione del Tag-set che comprende Tag conformi ai seguenti protocolli in dettaglio:
  - Tag I-Code 1
  - Tag I-Code SLI
- In particolare sono stati usati due Tag-set:
  - il Tag-set 1 è composto da 10 Tag di tre differenti produttori ed è stato utilizzato nelle prove con attraversamento del gate;
  - il secondo è composto da 9 Tag, tutti differenti tra loro per dimensioni, forma e materiale costruttivo. Il Tag set 2 è stato utilizzati solo nelle prove di stima della distanza di lettura.
- Preparazione e test di funzionalità degli apparati:
  - posizionamento delle antenne del gate a 1,3m di distanza reciproca;
  - posizionamento dell'antenna planare in posizione verticale;
  - verifica di corretto funzionamento del firmware di controllo;
  - reinstallazione interfaccia software per i comandi, ove fosse necessario.

La procedura di test ha previsto:

- preparazione degli oggetti campione da utilizzare nelle singole prove. Nel dettaglio, i Tag sono stati applicati sui seguenti quattro materiali:
  - materiale non interferente (cartaceo);
  - sacchetti in plastica riempiti con acqua;
  - lattine da 33cl vuote e riempite con liquido acquoso;
  - tetra-Pak riempiti con liquido acquoso.
- Preparazione dell'imballo in cartone, delle dimensioni di 1m x 1m, in cui sono di volta in volta inseriti i Tag applicati sugli oggetti, descritti al punto precedente, come di seguito illustrato:
  - inserimento casuale dei Tag nella scatola, senza ricercare l'ortogonalità con l'asse delle antenne;
  - riposizionamento dei Tag, con lo stesso criterio, ad ogni passaggio;
  - viene imposta una distanza di almeno 10cm tra Tag per evitare interferenze reciproche;
  - percorso guida su cui far scorrere l'imballo posto ad 1 m da terra.
- Passaggio dell'imballo per 12 volte in tutto, come di seguito:
  - velocità di attraversamento longitudinale del gate variabile tra 0,25 e 1,5 metri al secondo;
  - sei passaggi per direzione ("ingresso" e "uscita")
  - rilevazione dell'esito della lettura per ogni passaggio, attraverso la misura del rap-

porto tra il numero delle letture correttamente eseguite ed il numero di Tag componenti il Tag-set (denominato nel seguito tasso di successo).

- Nei soli casi in cui il tasso di successo è risultato inferiore al 100%, si è proceduto come segue:
  - sono stati estratti tutti i Tag non letti, mantenendoli applicati all'imballo;
  - l'apparato di lettura B (antenna planare) è stato progressivamente avvicinato al Tag fino a raggiungere l'esito positivo della lettura;
  - è stata misurata e registrata la distanza massima alla quale la lettura è avvenuta correttamente.

Sono stati effettuati complessivamente 40 test (20 riguardanti le distanze di lettura e 20 riguardanti l'attraversamento del gate). Il gruppo di test è stato effettuato in un periodo di 20 giorni, impegnando una media di 4 ore per lo svolgimento di ciascun test.

8.3.2 RISULTATI E CONCLUSIONI

È stato possibile osservare, tramite le prove eseguite, che l'impatto sulla trasmissione elettromagnetica dei materiali metallici e dei liquidi polari è fortemente distorsivo. La Figura 46 illustra il tasso di successo medio misurato utilizzando il Tag-set 1 e l'apparato di lettura A, in funzione del tipo di materiale su cui i Tag sono applicati. La media dei risultati si riferisce a 12 passaggi, con velocità diverse e nei due versi di attraversamento del gate, come precedentemente descritto.
Nelle condizioni ideali, in cui i Tag sono applicati su materiali elettromagneticamente non

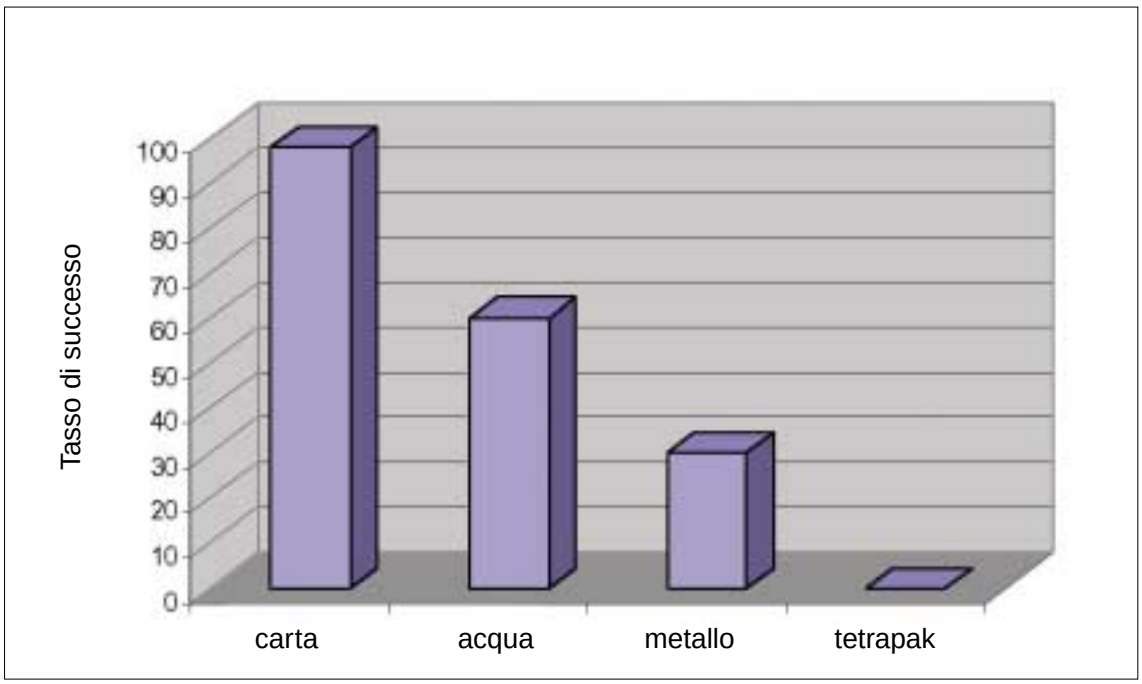

Figura 46: Tasso di successo su materiali interferenti (Tag-set 1)

interferenti (carta), il tasso di successo è stato molto prossimo al 100%. Solo in alcuni passaggi non sono stati letti i Tag di dimensioni più piccole.
Nel caso in cui si sono utilizzati i Tag su oggetti (sacchetti di plastica) riempiti con acqua il tasso di successo, per lo stesso gruppo di Tag di riferimento, è sceso nei dodici passaggi, al 50-60%.
Un ulteriore peggioramento si è riscontrato nel caso di involucri metallici (lattine) con un 20-30% di Tag letti per passaggio e la comparsa di un primo passaggio con 0 Tag letti.
Infine, nella configurazione di test elaborata, si è arrivati all'inibizione quasi totale della lettura nel caso di involucri di Tetra-Pak.
Successivamente è stata misurata la massima distanza alla quale un Tag risulta leggibile da parte dell'antenna planare da tavolo (B), in funzione del materiale su cui il Tag è applicato. L'esperimento è stato realizzato su tutti i Tag appartenenti al Tag-set 2.
Il grafico seguente (Fig. 47) indica, in ascissa, la dimensione fisica di ciascuno dei Tag oggetto dell'esperimento, in ordine crescente. L'asse delle ordinate misura la variazione percentuale della distanza di lettura rispetto a quella ideale misurata quando il Tag è applicato su materiale cartaceo. Ciascuna delle tre curve illustra pertanto la degradazione della distanza di lettura quando il Tag è applicato rispettivamente a contatto con materiale acquoso, metallo e tetrapak. L'osservazione mostra che la riduzione della portata rispetto al caso ideale (imballo vuoto contenente i soli Tag) è dell'ordine del 10% circa per Tag applicati su oggetti contenenti acqua (ed indipendentemente dalle dimensioni del Tag), varia tra il 40% ed il 100% per involucri metallici e, nel caso del Tetra-Pak, provoca una "inibizione" vera e propria della lettura della gran parte dei Tag[39] con dimensione inferiore a 5mm x 5mm.

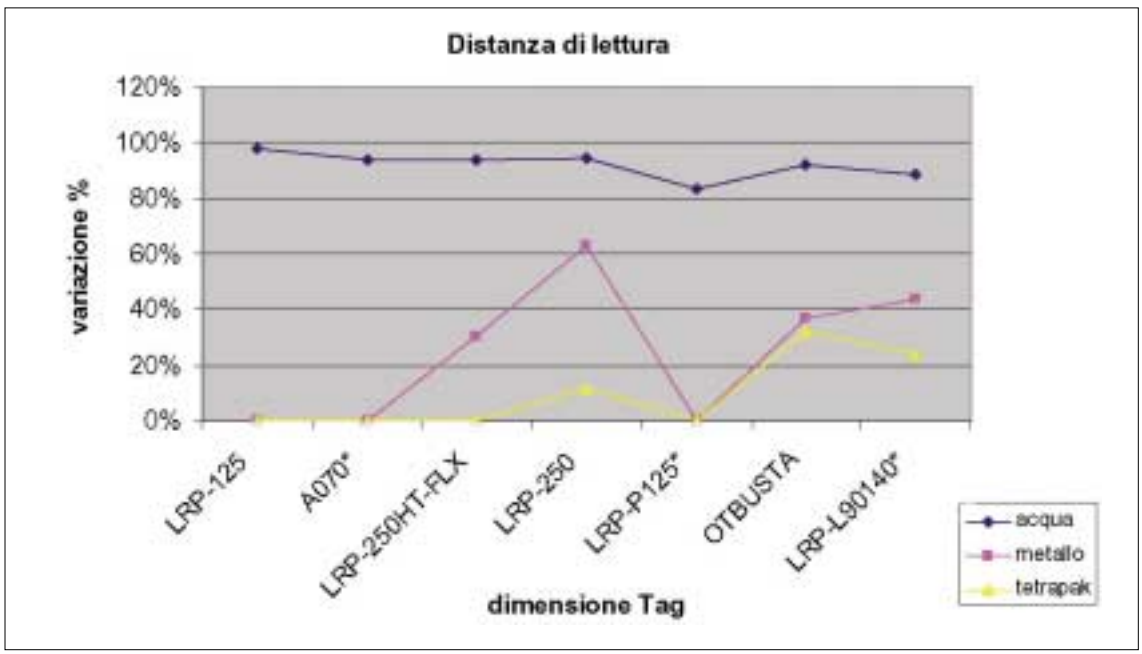

Figura 47 - Degradazione distanza di lettura secondo i materiali

[39] Esistono Tag appositamente costruiti per l'utilizzo su materiali speciali, quali il Tetrapak, che non sono stati inclusi nei Tag-set oggetto della sperimentazione

Anche la velocità di attraversamento del gate ha avuto un effetto di degradazione sensibile delle prestazioni misurate. Una lettura completa del set, pertanto senza errori, è stata possibile unicamente nel caso ideale (Tag applicati su carta) e con velocità non superiori a circa 1 m/s.
La conclusione è che, in scenari simili a quello di prova, il disturbo dovuto alla presenza di materiali specifici comporta un forte degradamento del tasso di successo nella lettura automatizzata. Di contro, in scenari di lettura in cui non siano coinvolti elementi elettromagneticamente non trasparenti, lo stesso sistema può funzionare con buoni livelli prestazionali.

In conclusione, si può affermare che, in fase di progettazione, debbono essere tenute in conto nell'ordine:

1) le condizioni ambientali di utilizzo della tecnologia RFId, con specifico riferimento primariamente alla natura dei materiali su cui i Tag sono apposti;
2) la velocità di movimento degli oggetti "taggati" quando attraversano le zone di lettura;
3) la dimensione e le caratteristiche fisiche dei Tag utilizzati.

8.4 ROBUSTEZZA ALL'INTERFERENZA TRA ANTENNE

L'esperimento ha l'obiettivo di misurare la probabilità di errore nella lettura di un Tag da parte di un lettore di riferimento, quando è presente un lettore interferente.
A tale scopo è stato posto sotto osservazione il comportamento di un reader palmare HF quando nelle vicinanze è presente un'antenna Gate funzionante alla medesima frequenza. In questo scenario, è stata misurata la massima distanza di lettura di Tag passivi da parte dell'apparato HF con antenna Gate in prossimità del reader palmare HF funzionante in modalità CR (Continuos Reading).

8.4.1 DESCRIZIONE DELL'ESPERIMENTO

Questo test è stato realizzato per valutare sperimentalmente quanto segue:

- la riduzione della massima distanza di lettura di un Tag HF passivo a 13,56MHz, posto nel campo generato da due reader interferenti, rispetto ad una situazione di non interferenza;
- la minima distanza a cui due reader, in condizioni di interferenza reciproca, sono in grado di operare entrambi correttamente.

Per effettuare le prove è stato posto un lettore palmare, in modalità lettura continua, nel campo generato da un lettore con una singola antenna appartenente ad una configurazione a Gate. Quest'ultima è configurata per inviare una richiesta di lettura con tempi di interlettura di: 100ms, 200ms, 300ms. La Figura 50, a pagina seguente, illustra lo scenario della prova.

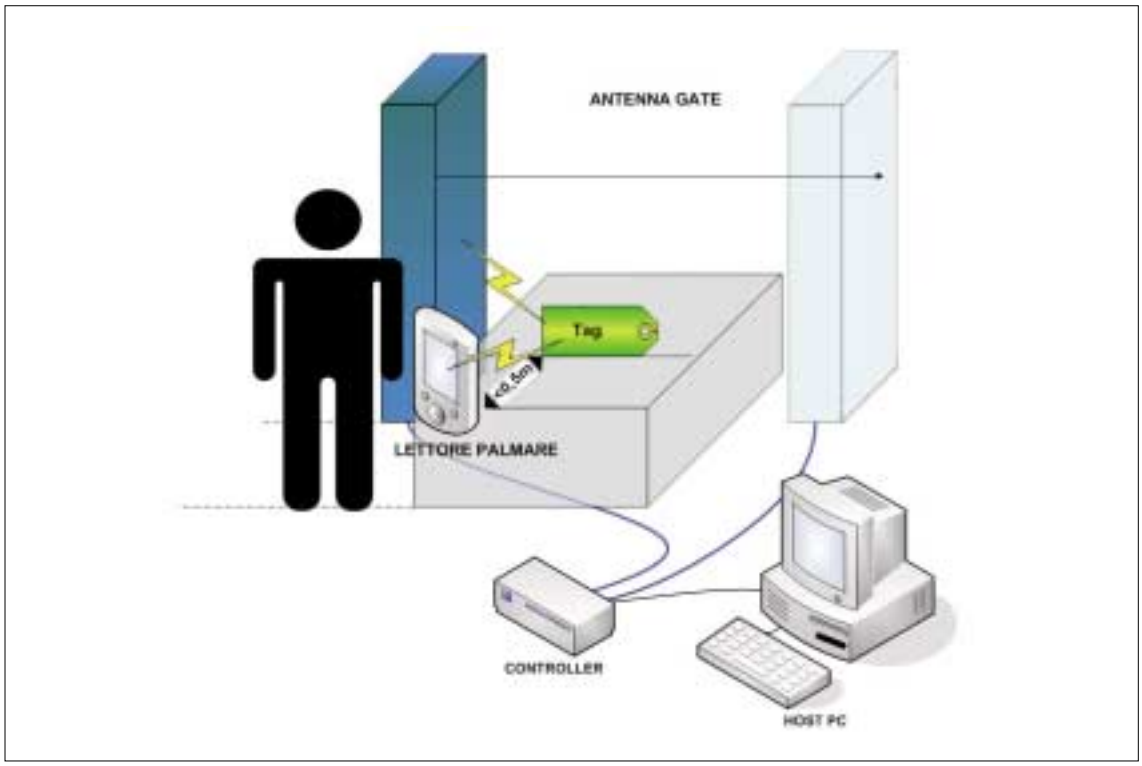

Figura 50 - Schema dell'apparato sperimentale per la valutazione dell'interferenza

Il test è stato eseguito utilizzando i seguenti Tag a 13,56 MHz:

1. Tag i-code SLI II;
2. Tag ISO 15693;

e i seguenti apparati:

- controller con singola antenna di Gate (nel seguito R1), ERP 500mW;
- reader palmare (nel seguito R2) in modalità lettura continua;
- asta graduata per la misurazione delle distanze.

La procedura di test è stata eseguita separatamente per i Tag indicati sopra (punti 1 e 2), per i seguenti tempi di interlettura[40] del reader R1:

1. til=300 ms
2. til=200 ms
3. til=100 ms

per le seguenti distanze tra R1 e R2:

1. distanza(R1,R2)=10 cm

[40] Il tempo di interlettura misura l'intervallo di tempo che intercorre tra due successivi invii del segnale di interrogazione (detto anche intervallo di polling). Lo stato di Continuous Reading, per l'apparato palmare utilizzato, corrisponde ad un intervallo di interlettura pari a 50 ms.

2. distanza(R1,R2)=20 cm
3. distanza(R1,R2)=30 cm
4. distanza(R1,R2)=40 cm

Procedura di test:

- misura della massima distanza tra i due apparati in cui è possibile ottenere una lettura corretta tramite l'apparato R1 con tempo di interlettura fissato;
- misura della massima distanza palmare R2 in modalità lettura continua;
- posizionamento degli apparati R1 e R2 in condizione di massima interferenza e distanza (R1,R2) fissa;
- posizionamento del Tag tra gli apparati, il Tag è stato posto tra i due apparati R1 e R2 con l'orientamento dell'antenna più favorevole alla lettura, variando la distanza:

  - distanza (Tag,R1);

  - distanza (Tag,R2)= distanza(R1,R2)-distanza (Tag,R1) con scarti di 5 cm partendo dal lettore R1;
- verifica dell'avvenuta lettura del Tag da parte dei lettori R1 e R2.

Per tutti i test è stato definito un sistema di riferimento in cui la posizione del lettore R1 è stata presa come punto di riferimento (coordinata X=0) per la misura delle distanze. A tale scopo è stata posizionata un'asta graduata perpendicolarmente al piano dell'antenna del lettore R1 in coincidenza dell'asse centrale dell'antenna stessa.
La distanza tra R1 e R2 è stata variata mantenendo fissa la posizione di R1.

Sono stati eseguiti i test con i seguenti setup sperimentali:

A. reader palmare in CR, controller con antenna Gate e tempo di interlettura 300ms, distanza tra i lettori: 10-20-30-40 cm per un totale di 60 letture;
B. reader palmare in CR, controller con antenna Gate e tempo di interlettura 200ms, distanza tra i lettori: 10-20-30-40 cm per un totale di 60 letture;
C. reader palmare in CR, controller con antenna Gate e tempo di interlettura 100ms, distanza tra i lettori: 10-20-30-40 cm per un totale di 60 letture.

Sono stati effettuati, complessivamente, 6 test (2 per ogni tipo di setup sperimentale, utilizzando rispettivamente Tag i-code SLI II e Tag ISO 15693).
Il gruppo di test è stato effettuato in un periodo di 6 giorni, impegnando una media di 1 giornata per lo svolgimento di ogni singola prova.

8.4.2 RISULTATI E CONCLUSIONI

Il primo risultato è che, seppure in presenza di campi d'interferenza reciproca ed azioni di lettura concorrenti, gli apparati Reader, anche se caratterizzati da livelli di potenza elettromagnetica molto diversi (e quindi da una diversa capacità di "controllare" il Tag), riescono comunque a leggere il valore corretto dell'Id del Tag.

Tuttavia, l'esperienza ha mostrato che, in ambienti in cui siano presenti più sistemi di lettura RFId indipendenti e di diversa tipologia, ad esempio quando alle postazioni fisse si aggiungano apparati per letture in mobilità, i problemi di interferenza sono evidenti:

- la riduzione della portata del lettore portatile utilizzato nei test quando posto a meno di un metro dall' apparato più potente, come il gate utilizzato, è consistente e misurata nell'ordine del 50%;
- durante la sperimentazione sono state rilevate delle "letture incerte" nella zona di sovrapposizione dei campi elettromagnetici generati dai due reader che quindi interferiscono reciprocamente. La visualizzazione dell'Id del Tag, sebbene decifrabile, risulta instabile e intermittente mentre in modalità CR (Continuos Reading) dovrebbe rimanere statica e fissa sul display;
- al di sotto dei 0,5 m di distanza tra i due lettori il dispositivo meno potente, quello palmare non riesce più a leggere correttamente i Tag selezionati.

8.5 ROBUSTEZZA AI PRINCIPALI ATTACCHI

L'esperimento ha l'obiettivo di valutare la robustezza dei Tag ad alcuni semplici attacchi di tipo logico e fisico. Le prove sono state suddivise in due gruppi con differenti finalità sperimentali relative a:

- sicurezza logica:
  - forzatura della password a protezione del kill-command deputata alla disattivazione del Tag;
- sicurezza fisica:
  - disattivazione/danneggiamento del Tag per mezzo di impulsi elettrici diretti e di impulsi elettromagnetici.

8.5.1 FORZATURA DELLA PASSWORD DI KILL-COMMAND

Il kill-command è un particolare comando che provoca la disattivazione permanente e definitiva del Tag a cui esso viene inviato.
I Tag utilizzati nelle prove eseguite in laboratorio sono conformi alle specifiche EPCGlobal C1G1. Questo tipo di Tag, in una configurazione minimale, ha una memoria interna di 128bit, di cui 96 sono destinati a contenere l'Id di identificazione, 8bit/16bit contengono la password di kill, 16bit un CRC calcolato secondo CCITT CRC-16 ed i restanti 8bit un lock-code opzionale il cui scopo è rendere "opache" alcune zone di memoria. La kill command key dei Tag UHF C1G1 utilizzati per i test è costituita da una stringa lunga 2 byte, precedentemente registrata in una speciale area di memoria. Una chiave di soli 2 byte significa che vi possono essere al massimo 2^{16ma} ovvero 65536 chiavi.
Visto il limitato range di valori che la chiave di protezione può assumere, la sicurezza garantita a fronte di un "attacco di forza bruta" mirato alla disattivazione dei Tag tramite un reader "intruso" è, relativamente, piuttosto debole.

Le specifiche EPCGlobal C1G2 prevedono invece che sui Tag sia memorizzata una password statica di 32bit che inibisce l'esecuzione del kill command. Viene inoltre aggiunto un meccanismo di protezione della memoria, opzionale, con una ulteriore password di 32bit che il reader dovrà fornire per avere diritti di lettura/scrittura sul Tag in determinate aree.
La protezione offerta per questa versione delle specifiche EPC, che prevede password statiche per un gruppo omogeneo di Tag esposti ad un attaccante determinato, è sicuramente migliore in quanto richiede range temporali di gran lunga superiori (2^{32} ovvero circa 16M di chiavi possibili).
I test di sicurezza logica sono stati effettuati con l'ausilio di un dispositivo di lettura UHF composto da:

- due antenne di lettura formato "patch" delle dimensioni di 40x40cm;
- controller separato per entrambe le antenne con collegamento USB.

Le prove di laboratorio hanno richiesto lo sviluppo di una semplice applicazione in linguaggio Java per la generazione ricorsiva delle password e del tentativo di attacco mediante kill-command. A tale scopo si è fatto uso dello SDK (Software Development Kit) a corredo, che include le librerie software di gestione degli apparati di trasmissione e il supporto per i protocolli relativi ai Tag utilizzati[41].
Il setup della prova ha previsto:

- setup della macchina di sviluppo;
- studio del pacchetto SDK;

  - Vendor 1 SDK Java
- scelta dei Tag da porre in test, in dettaglio:

  - EPC C1G1

  - EPC C1G2[42]
- realizzazione del codice necessario;
- debugging e ottimizzazione.

La procedura di test ha previsto:

- posizionamento dei Tag in zona di lettura;
- lettura del Tag prima dell'esperimento;
- avvio del ciclo di scansione delle password possibili per l'invio e l'esecuzione del comando di Kill;
- lettura del Tag per verificarne l'eventuale disattivazione.

[41] Lo studio e la codifica del software che realizza la ricerca esaustiva delle password è stata condotta con l'ausilio del personale tecnico della casa costruttrice dell'apparato di lettura. Parte del listato relativo al codice utilizzato proviene da codice già realizzato internamente al CATTID per altre sperimentazioni sulle stesse tecnologie

[42] Pur avendo inserito nello scenario di test questa tipologia di Tag, in fase di set up delle strumentazioni, si è riscontrata la mancanza delle librerie di controllo funzionanti che non hanno consentito la corretta esecuzione del codice di ricerca della password di kill command

8.5.2 RESISTENZA FISICA ALLE SCARICHE ELETTRICHE

L'esperimento ha l'obiettivo di misurare la robustezza dei Tag alla scarica elettrica indotta da una batteria di condensatori caricati attraverso una rete elettrica appositamente realizzata e alla scarica elettrica indotta da dispositivo piezoelettrico. I Tag selezionati sono tutti operanti a 13.56 MHz.

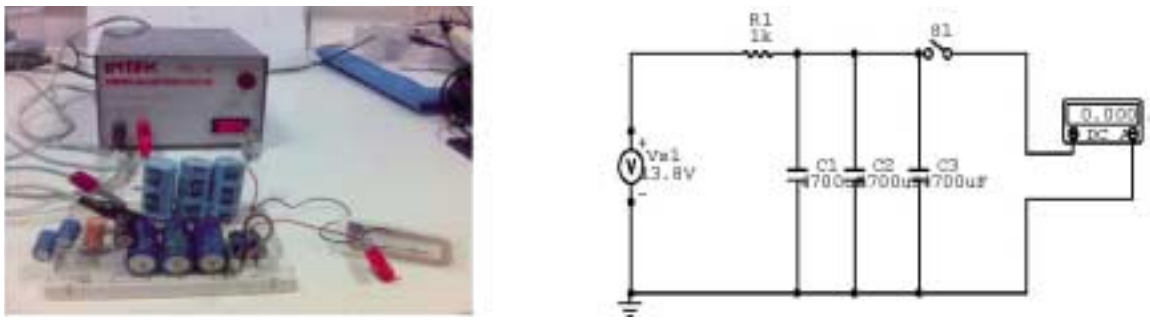

Figura 49 - Immagine e schema dello scenario di prova

La robustezza è stata valutata andando a verificare il corretto funzionamento del Tag colpiti da una scarica ed ispezionando a vista la presenza di ustioni sul packaging. Il Tag si ritiene funzionante dopo la scarica se viene correttamente letto dal reader e se il valore dell'identificativo letto coincide con quello letto prima della scarica.

Il test è stato eseguito utilizzando i seguenti Tag:

- Tag Vendor 1 ISO 15693 ICODE SL2 (5x5 cm);
- Tag Vendor 2 ISO 15693 (8,5x5,5 cm);
- Tag Vendor 3 ISO 15693 (8x2,5 cm);
- Tag Vendor 4 ISO 15693 ICODE SL2 (7,5x4,5 cm);
- Tag Vendor 5 ISO 15693 (8x5 cm);

e i seguenti apparati e dispositivi:

- reader palmare utilizzato per eseguire letture dei Tag elencati sopra;
- dispositivo piezoelettrico;
- condensatori con capacità singola di 4700 µF (*micro Farad*);
- alimentatore 13,8 V DC 3A;
- breadboard e componenti elettrici aggiuntivi per la realizzazione del circuito di carica dei condensatori.

Le prove sono state eseguite con apparati di scarica "portatili", ossia di dimensioni contenute, di facile realizzazione e con alimentazione portatile. Si consideri che i circuiti a condensatori che realizzati allo scopo possono essere efficacemente alimentati a batteria.

La procedura di test ha previsto:

- realizzazione dei circuiti di scarica con capacità:
  A. C=4700 µF;
  B. C=9400 µF;
  C. C=14100 µF.
- selezione sul reader dello standard di lettura del Tag sotto test;
- lettura e registrazione dell'identificativo del Tag prima del test;
- scarica elettrica sul packaging del Tag in prossimità del chip, attraverso conduttori a punta che prelevano la carica:
  - ai capi della batteria di condensatori (circuiti A,B,C);
  - dal dispositivo piezoelettrico;
- lettura del Tag dopo la scarica per verificarne il funzionamento.

Sono state effettuate, complessivamente, venti prove di scarica su ogni Tag per un totale di 100 prove. Il gruppo di test è stato effettuato in un periodo di 5 giorni, impegnando in media 20 minuti per lo svolgimento di ciascun test.

8.5.3 RISULTATI E CONCLUSIONI

L'esperimento di attacco tramite kill-command ha sempre avuto successo. Relativamente ai Tag C1G1 l'attacco è stato portato a compimento in un massimo di circa 5800 secondi circa (su un tempo massimo teorico di 6030 secondi circa, ottenuto considerando un tempo di esecuzione complessivo del singolo comando di circa 90ms moltiplicato per il totale delle chiavi possibili).
Per i test riguardanti i Tag C1G2, per problemi emersi con il tool di sviluppo del codice (v. paragrafo seguente), è stato possibile affrontare solo uno studio approssimato dei tempi di successo attesi per la ricerca della password di kill. Tale studio, prendendo in considerazione le stesse modalità di esecuzione e password di 4 Byte, ha indicato comunque un tempo di esecuzione massimo di molto superiore[43].

Pertanto, l'utilizzo di Tag UHF EPC C1G1 e G2 in applicazioni in cui siano coinvolti dati sensibili su scenari aperti o comunque non "supervisionati" è una scelta da valutare con attenzione[44].

Nella composizione del Tag set per la sperimentazione sulla sicurezza fisica, sono stati selezionati i Tag maggiormente diffusi nelle applicazioni RFId, ossia tag ad alimentazione passiva ed a basso costo.

[43] Va tenuto conto, comunque, che la sicurezza assicurata da un sistema che si affidi unicamente a chiavi simmetriche resta comunque bassa. Sono state dimostrate in letteratura tecniche di analisi del segnale riflesso dal Tag che permettono la ricostruzione corretta di parte delle sequenze numeriche inviate on-air in chiaro.

[44] Sulla base delle specifiche sulla password di identificazione dei reader per la scrittura sono state proposte soluzioni basate su un servizio directory per le chiavi di lettura

Il Tag set ha evidenziato una rilevante robustezza all'induzione di scariche elettriche indotte dagli apparati utilizzati. In particolare nelle prove eseguite, pur in presenza di ustioni e segni permanenti sulla pellicola di protezione dei Tag, essi hanno continuato a funzionare correttamente.

8.6 CONSIDERAZIONI SUI TOOL DI SVILUPPO

Le attività sperimentali hanno portato ad utilizzare i kit di sviluppo software (SDK) forniti a corredo per il pilotaggio degli apparati reader. Nel seguito sono riportate alcune considerazioni che vengono dall'esperienza realizzata in laboratorio.

La prima esperienza ha riguardato lo sviluppo di semplici procedure per la configurazione della modalità di lettura dei reader. La qualità dell'applicazione e la semplicità di sviluppo sono risultate essere fortemente dipendenti dalla qualità tecnica e dal livello di aggiornamento ed assistenza del Software Development Kit fornito. In uno specifico caso, ad esempio, le librerie in dotazione non hanno consentito il controllo completo della configurazione dell'apparato.
Durante la fase di sviluppo e nel debugging dell'applicazione compiuto su alcuni Tag C1G1 di prova, sono emersi problemi di incompatibilità legati alla mancanza di alcune delle funzioni documentate nei manuali d'uso. Comunque, il test ha avuto successo grazie alle correzioni fornite su richiesta dalla casa costruttrice degli apparati.
Relativamente allo sviluppo per il tipo C1G2, sono stati riscontrati errori di run-time, e problemi legati alla non completa corrispondenza tra le funzioni documentate nei manuali d'uso e quelle effettivamente presenti nelle librerie destinate alla gestione dell'interfaccia del reader. Si tratta di difficoltà imputabili ad uno stadio ancora iniziale di sviluppo delle tecnologie UHF, almeno in Italia, ed a problemi legati alla localizzazione del software, diversa per ciascun Paese europeo in conseguenza delle differenze di allocazione dello spettro radioelettrico.

Appendici

Appendice 1 - Approfondimenti tecnici

A.1 Introduzione

Genericamente si dice che un sistema RFId scambia energia e informazioni a radiofrequenza, concetto che coinvolge idealmente un processo di propagazione di un'onda elettromagnetica. Perchè questo possa avvenire, la struttura che lancia l'energia elettromagnetica deve avere dimensioni adeguate alla lunghezza d'onda del segnale da trasmettere, più esattamente pari almeno ad 1/4 di l.
Le bande di frequenza d'interesse per applicazioni RFId sono principalmente tre, tralasciando gli apparati attivi con frequenze di funzionamento sopra i 2 GHz: LF a 125 Khz, HF a 13.56 Mhz e, in Italia, UHF a 868 Mhz. La banda dei 13.56 MHz fa parte della dozzina di bande comprese 6 MHz e i 250 GHz riservate a livello internazionale dalla ITU in collaborazione con lo IEC (International Electrotechnical Commission) per l'uso di dispositivi Industriali Scientifici e Medici (ISM) che hanno caratteristiche di radiazione a banda stretta.
A 13.56 Mhz la lunghezza minima dell'antenna perché si abbia una onda propagante risulta essere di circa 22 metri, irrealizzabile in pratica. Il campo elettrico o magnetico comunque generato dalla struttura rimane vincolato alle immediate prossimità dell'antenna. I sistemi funzionanti a 125 Khz e a 13.56 Mhz si basano sul fenomeno dell'accoppiamento induttivo, ovvero per effetti riconducibili al campo magnetico. Oltre i 30 Mhz, quindi per i sistemi UHF, sono coinvolte onde elettromagnetiche e fenomeni di propagazione classica. Per comprendere le modalità di trasferimento dell'energia e dei dati si daranno alcuni cenni dei principi fisici legati ai fenomeni magnetici ed elettromagnetici.

A.2 Basse Frequenze: LF e HF

Campo magnetico e induttanza

Qualsiasi flusso di carica in movimento (elettroni in un filo o nel vuoto) è associato ad un campo magnetico, cioè ad una forma di energia che viene generata nel suo intorno ed in grado di esercitare un'azione a distanza su oggetti interessati dal fenomeno magnetico. Questo avverrà per ogni conduttore che sia percorso da corrente, indipendentemente dalla sua forma. La presenza di questo campo può essere banalmente verificata con il classico ago della bussola posto in prossimità del conduttore.

Per un conduttore filare percorso da corrente, rispettando l'enunciato classico nella forma generale[45], il campo magnetico lungo una linea di flusso circolare a distanza r è costante e può essere calcolato come:

$$H = \frac{1}{2\pi r}$$

Se il conduttore si presenta invece con una forma circolare chiusa, il campo magnetico è particolarmente intenso.Una serie di "circoli" chiusi costituiti dal conduttore filare formano una spira cilindrica corta. Se questa viene percorsa da una corrente dunque, il modulo del campo magnetico ad una distanza x lungo l'asse è definibile come:

$$H = \frac{I \cdot N \cdot R^2}{2 \cdot \sqrt{((R^2 + x^2)^3)}}$$

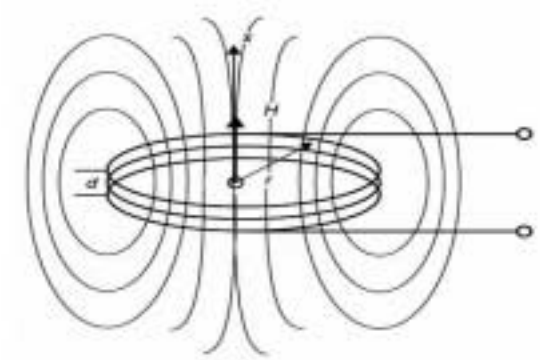

Figura 50 - Rappresentazione campo magnetico generato da una spira

Nella equazione precedente vengono anche menzionate N, numero di spire e R, raggio della spira.
Studiando l'andamento del modulo del campo magnetico all'aumentare della distanza x lungo l'asse, si può notare che questo rimane costante fino ad una certa distanza, legata al raggio della spira, per poi decadere rapidamente in ragione del cubo della distanza. Per questo motivo sistemi RFId a basse frequenze in genere sono limitati a distanze dell'ordine delle decine di centimetri.
Il campo qui espresso non è ancora legato alle caratteristiche fisiche del mezzo in cui viene propagata l'energia. Ad esempio, se invece del vuoto la spira è avvolta su di un nucleo ferroso, la forza agente sull'ago di test menzionato prima aumenterà, anche a parità di prodot-

[45] L'integrale di linea (circuitazione) campo magnetico come uguale alla somma delle intensità di correnti comprese all'interno della curva chiusa. $\sum I = \oint \bar{H} \cdot \bar{ds}$

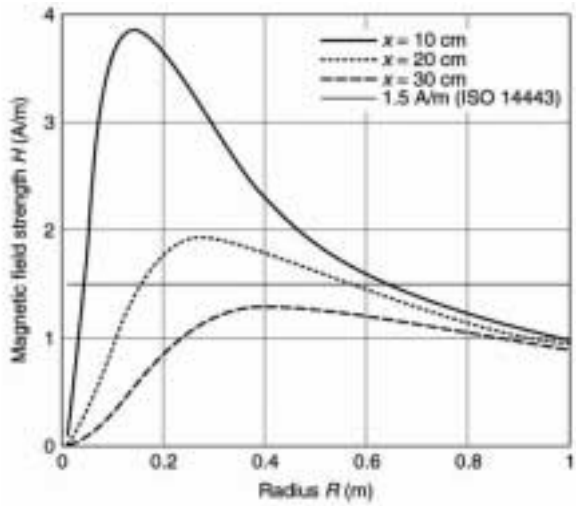

Figura 51 - Intensità di campo per I = 1 e N = 1 e raggio della spira variabile

to I x N. Quello che è aumentato è la densità di flusso magnetico, grandezza definita come B (spesso definita anche come induttanza magnetica).

$$B = \mu_0 \mu_r H$$

in cui le due costanti sono dette rispettivamente permeabilità magnetica del vuoto e permeabilità magnetica relativa, riferita al materiale specifico. Attraverso **B** si può quantificare il flusso attraverso una superficie A, grandezza indicata con **Φ** e pari al prodotto **B**xA
Il conduttore a spira può essere caratterizzato tramite una grandezza chiamata induttanza. Questa dipende totalmente dalle caratteristiche del materiale (permeabilità) di cui è costituito lo spazio racchiuso dal conduttore, e quindi attraversato dal flusso magnetico, e dalle caratteristiche geometriche del conduttore stesso. Come menzionato ad esempio, per ridurre le dimensioni della spira stessa ma convogliare lo stesso un buon numero di linee di flusso, questa spesso viene realizzata con un piccolo nucleo di ferrite.
Per quello che riguarda quindi gli RFId, la spira, costituita da un avvolgimento di rame, è l'elemento costituente sia l'antenna del reader che quella del Tag. Essa è lo "strumento" che permette sia lo scambio di energia, come si vedrà tra poco, che la comunicazione.

MUTUA INDUTTANZA: SCAMBIO DI ENERGIA

Consideriamo quindi una spira percorsa da corrente posta nello spazio libero. Se una seconda spira è presente nelle vicinanza della prima, l'area A2 di questa spira (che si suppone minore della prima per garantire l'omogeneità del campo magnetico sulla superficie) sarà attraversata da alcune linee del flusso magnetico generato dalla prima. I due circuiti sono quindi connessi tra loro tramite un flusso di accoppiamento. L'accoppiamento di due circuiti tramite campo magnetico, l'antenna di lettura del reader e l'antenna passiva del Tag, è il principio fisico alla base del funzionamento di sistemi RFId.
E' possibile definire una grandezza definita mutua induttanza tra le due spire, legata anzitutto alle caratteristiche geometriche reciproche delle spire coinvolte, quindi alla distanza ed

alle permeabilità relative dei mezzi coinvolti tramite B, e che dia una descrizione quantitativa di quanto il flusso magnetico sia concatenato alle due spire. Matematicamente questo può essere espresso come:

$$M_{21} = \frac{\Psi_{21}(I_1)}{I_1} = \int_{A2} \frac{B_2(I_1)}{I_1} dA_2$$

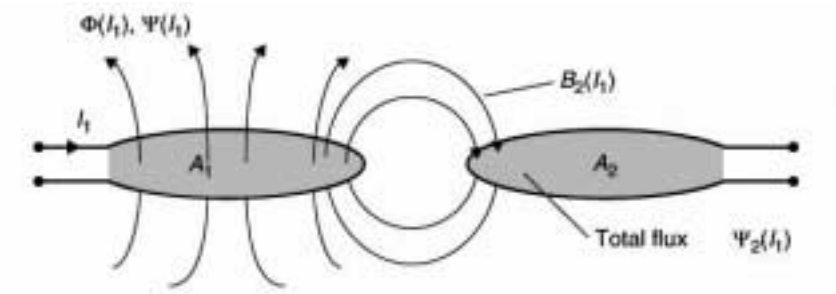

Figura 52 - Concatenazione dei flussi

Per dare invece una descrizione qualitativa dell'accoppiamento conseguito si usa un coefficiente detto appunto coefficiente di accoppiamento K, che da una misura dell'efficienza dello scambio energetico in atto tra reader e Tag, in questo caso. Esso è compreso tra 0 (nessun accoppiamento) ed 1 (accoppiamento perfetto, situazione in cui i centri delle spire dovrebbero teoricamente coincidere in x=0), è legato sia alle dimensioni del raggio delle spire d'antenna del reader e del Tag e sia ovviamente alla distanza tra le due.
Per sistemi RFId a frequenze HF in condizioni operative in genere K non supera mai lo 0,25 (25%) ma generalmente è funzionale già per valori dello 0,01 (1%).

ZONE DI INTERROGAZIONE

Il campo magnetico è un campo vettoriale, ovvero descritto da un modulo e verso di azione. Fino ad ora ci si è riferiti al caso ideale di campo H omogeneo parallelo all'asse della

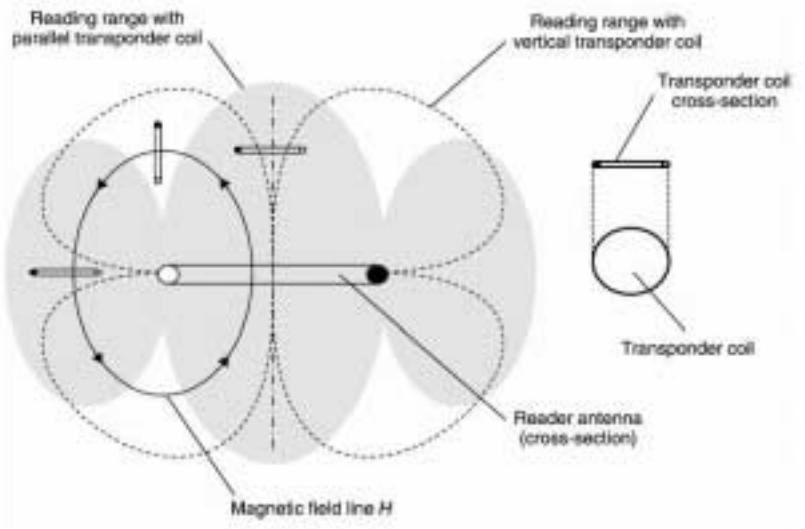

Figura 53 - Zone d'interrogazione risultanti dalle diverse posizioni relative degli assi delle spire Tag-Reader

spira, ovvero ad un caso in cui gli assi delle antenne del Reader e del Tag siano collineari. Se l'asse del trasponder si trova su un'altra retta, la condizione non è più soddisfatta e la tensione indotta per accoppiamento si ridurrà di un fattore approssimativamente proporzionale al coseno dell'angolo formato tra i due assi.
Questo aspetto è reso ancora più critico nel caso comune di transpoder ad etichetta, in cui la spira è caratterizzata dall'essere disposta su tutta la lunghezza del Tag ed schiacciate.

ACCOPPIAMENTO E TENSIONE INDOTTA

Descritto il meccanismo di base tramite il quale l'energia viene trasferita, vanno adesso descritte le reali condizioni in cui questo avviene. Qualsiasi variazione del flusso magnetico Ψ, generata da una variazione della corrente che fluisce nel conduttore, genera l'insorgere di un campo elettrico **E**, come previsto dalla legge di Faraday. Nel caso in cui l'oggetto in cui avviene la variazione di corrente sia una singola spira conduttrice con i morsetti finali aperti è possibile rilevare ai capi di questi una certa differenza di potenziale elettrico, chiamata solitamente tensione indotta[46]. Come illustrato in figura, in un sistema RFId ad accoppiamento induttivo L1 rappresenta l'antenna trasmittente ed L2 l'antenna del transponder. Nel circuito equivalente semplificato R2 è la resistenza della spira mentre RL è la resistenza di carico.

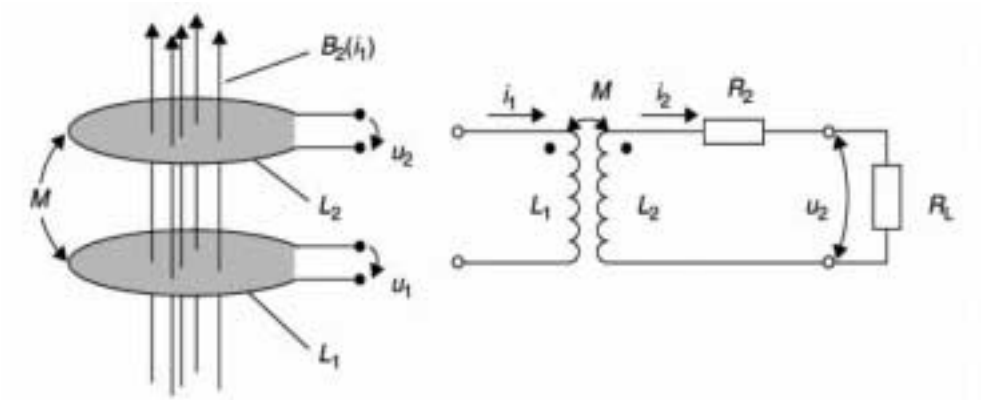

Figura 54 - Accoppiamento Reader-Tag e circuito equivalente

Un flusso variabile generato nel loop L1 induce una tensione v2 nel loop L2 dovuto alla presenza di una certa mutua induttanza. Il flusso è misurabile ai capi della spira L2 come caduta di tensione dovuta alle resistenza interna ai capi di R2 o tramite la misura di una corrente i2 attraverso la resistenza di carico. La semplificazione illustrata non tiene conto di tutti i fenomeni elettromagnetici aggiuntivi (legge di Ampere) e le aggiuntive specifiche circuitali su risonanza e tuning che sarebbero necessarie. Tuttavia si è illustrato il modo in cui avviene lo scambio energetico alla base della comunicazione tra reader e Tag.
A titolo d'esempio si riporta in figura un semplice circuito di un transponder passivo.

[46] Tensione che corrisponde matematicamente all'integrale di linea del campo elettrico lungo il conduttore.

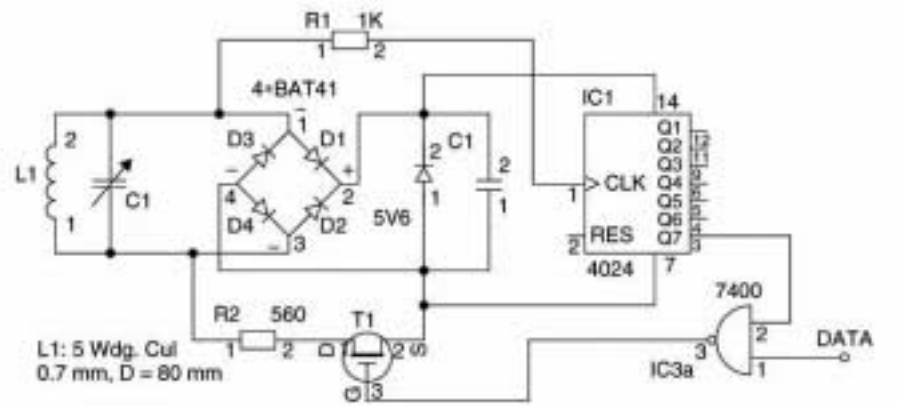

Figura 55 - Circuito di un transponder passivo

Possiamo distinguere quattro componenti principali:

- Un circuito LC di accoppiamento e accumulazione dell'energia, sulla sinistra
- Un ponte raddrizzatore per fornire l'alimentazione necessaria, al centro
- Una parte di logica che contiene il chip ed è responsabile della gestione delle risorse a bordo, sulla destra
- Una parte dedicata alla modulazione del canale di ritorno, costituita dalla resistenza di carico R2 in basso e dalla porta logica sulla destra. Tra i tanti metodi di modulazione per il canale di ritorno dal Tag al reader, una delle più utilizzate è la cosiddetta modulazione di carico. Si attua variando i parametri circuitali del circuito risonante del Tag in maniera sincronizzata con il flusso dati da trasmettere. Due sono le tecniche principali di operazione: ohmica (o reale) e capacitiva. Questo si traduce principalmente in una modulazione di ampiezza nel primo caso ed in una combinazione di modulazione di fase e frequenza nel secondo caso.

A.3 ALTE FREQUENZE: UHF

A frequenze di qualche centinaio di Mhz, in cui la lunghezza d'onda (ovvero la frequenza) operativa dei dispositivi utilizzati diventa paragonabile alle dimensioni fisiche dell'antenna[47] il meccanismo di scambio dell'energia è diverso.
Semplificando, l'antenna è in grado di emettere un'onda elettromagnetica che si propaga lungo un tubo di flusso, con fronte sferico ed origine nella sorgente, lungo direzioni determinate dalla struttura fisica dell'antenna stessa che vengono identificate come lobi di radiazione. L'energia trasportata da un'onda elettromagnetica è conservata nel campo magnetico ed elettrico costituenti l'onda stessa, ortogonali tra loro ed oscillanti, generalmente in fase, ad una frequenza che costituisce in genere il principale parametro di riferimento. L'orientazione che assumono in un periodo i versori dei vettori di campo magnetico ed elettrico caratterizzano la polarizzazione risultante dell'onda.

[47] Per frequenze di 868 Mhz parliamo di dimensioni d'antenna di circa 34 cm.

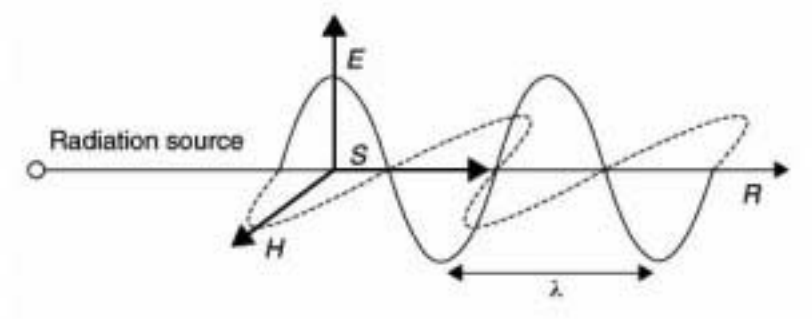

Figura 56 - Esempi di campi E-H a grande distanza dall'antenna

L'energia che è possibile "raccogliere" in un qualsiasi punto dell'onda a distanza d dalla sorgente è inversamente proporzionale al quadrato della distanza. La potenza massima che una struttura ricevente è in grado di assorbire dipende da diversi fattori: dall'adattamento che la struttura di questa ha nei confronti della polarizzazione del campo incidente, dall'allineamento rispetto alla sorgente e da un fattore di proporzionalità che ha le dimensioni di un'area è rappresenta l'area efficace dell'antenna in grado di "intercettare" un'onda piana incidente

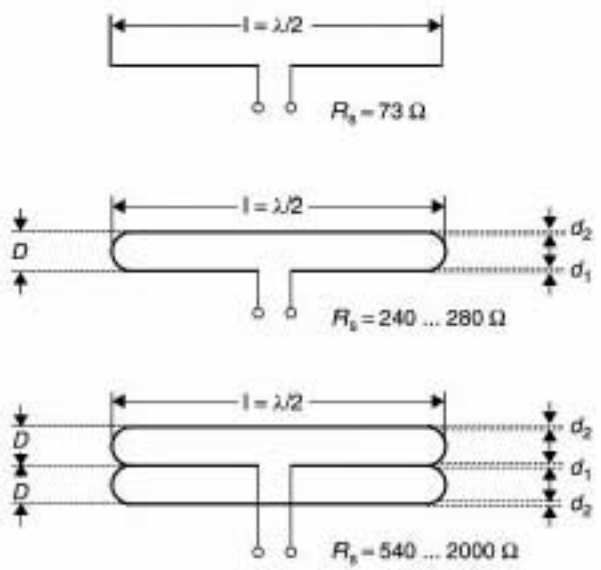

Figura 57 - Dipoli ripiegati, per aumentare la lunghezza effettiva dell'antenna

Appendice 2 - Conformità alle normative sanitarie

Conformità dei sistemi EAS/RFId alle normative in materia di esposizione della popolazione ai Campi Elettromagnetici

A.1 Introduzione

I sistemi di sorveglianza elettronica (EAS) e di identificazione a radiofrequenza (RFId) operano in un intervallo esteso di frequenza, che va da decine di hertz fino ad alcuni gigahertz utilizzando trasmissioni impulsive o in onda continua.
Tali sistemi hanno alcune caratteristiche comuni:

- fanno ricorso ai campi elettromagnetici per comunicare o rivelare oggetti entro distanze relativamente piccole (da pochi centimetri fino ad una decina di metri nelle applicazioni UHF);
- richiedono che gli oggetti o le persone che si vuole monitorare si trovino in una zona ben definita in prossimità del sistema di lettura;
- comportano tempi di esposizione brevi per la popolazione comune (dell'ordine di secondi o frazioni di secondo), mentre l'esposizione del personale addetto può prolungarsi anche per tutta la durata di un turno di lavoro.

Nel progetto di una applicazione RFId, e nella panificazione dell'apparato, è quindi opportuno tenere in considerazione le problematiche di conformità alle normative sanitarie in merito alla esposizione del corpo umano ai campi elettromagnetici. Nell'ipotesi di lavorare con tag passivi, che quindi comunicano con il reader solo tramite la retrodiffusione dell'energia da esso trasmessa, i requisiti di conformità sanitaria vanno principalmente riferiti alle caratteristiche elettromagnetiche del reader stesso. Nelle applicazioni ove si faccia uso anche di tag attivi, le osservazioni che seguiranno devono essere estese anche a questo componente.
Gli apparati di interrogazione dei sistemi RFId possono essere di tipo portatile (palmare, telefono cellulare) o di tipo fisso (varchi, access point). Nel primo caso tali dispositivi sono tenuti in mano dall'operatore e quindi l'interazione tra il campo elettromagnetico irradiato ed il corpo umano può essere importante. Nei sistemi fissi sono le persone e gli oggetti da monitorare a muoversi rispetto al reader, ed in tal caso l'esposizione è in linea di principio ridotta ma non necessariamente trascurabile.
Da un punto di vista operativo, valutare la conformità sanitaria di un apparato EAS/RFId equivale ad indicare la minima distanza di sicurezza tra questo e persone che siano soggette ad una esposizione prolungata e continuativa.
In questa Appendice vengono introdotte e discusse le linee guide generali delle normative europee ed italiane in materia di esposizione elettromagnetica che siano applicabili ai siste-

mi EAS/RFId. Sono descritte le procedure di valutazione dell'esposizione e sono infine riportati alcuni esempi di caratterizzazione di impianti a bassa ed alta frequenza.

A.2 NORMATIVE VIGENTI

I campi elettromagnetici interagiscono con la materia vivente principalmente tramite meccanismi termici e non-termici. A frequenze al disotto di 100 kHz i campi magnetici esterni inducono nel corpo umano campi elettrici e distribuzioni di corrente elettrica. I campi elettrici nel corpo possono portare ad una variazione dei potenziali di membrana a livello cellulare, con il rischio di provocare possibili effetti sulle funzioni del sistema nervoso centrale. Oltre 10 MHz il fenomeno dominante di interazione con la materia vivente diviene l'assorbimento della radiazione elettromagnetica, che ha come conseguenza il riscaldamento dei tessuti, come pure altri effetti a livello cellulare. Mentre l'eccitazione della membrana è un processo rapido (dell'ordine di millisecondi) e richiede stimoli energetici rilevanti, il danneggiamento delle cellule per effetto termico è invece un processo molto più lento.
Negli ultimi due decenni gli intensi studi compiuti per la comprensione qualitativa e quantitativa dell'interazione elettromagnetica con i tessuti viventi e sulle conseguenze sanitarie ha costituito la base scientifica di una articolata attività di normazione in ambito Europeo. I vari Stati membri, tra i quali l'Italia, hanno recepito le raccomandazioni comunitarie con alcune modifiche, in generale più cautelative.

NORMATIVE EUROPEE

Le normative e le raccomandazioni europee in materia di esposizione ai campi elettromagnetici prodotti da EAS e RFId sono di seguito indicate

- Linee guida ICNIRP[48]: "Guidelines for limiting exposure in time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz", Health Physics, Volume 24, Number 4, April 1998, p.494. Questo documento introduce i limiti di esposizione per la popolazione generica ed in ambiente lavorativo. I valori massimi indicati sono discussi in relazione alle attuali conoscenze degli effetti biologici dei campi elettromagnetici.
- Raccomandazioni della Comunità Europea[49]: "European Council Recommendation 1999/519/EC of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz", Official Journal, L199, 30.7.1999., p.59). Vengono definite le tabelle con i limiti di esposizione ai campi elettromagnetici per la popolazione.

[48] International Commission on Non.Ionising Radiation Protection, http://www.icnirp.de/documents/-emfgdl.pdf.
[49] http://ec.europa.eu/enterprise/electr_equipment/lv/rec519.pdf.

- Standard di base: EN 50357, anche Norma CEI EN 50357, "Evaluation of human exposure to electromagnetic fields (EMFs) from devices used in electronic article surveillance (AS), radio frequency identification (RFId) and similar applications". Sono dettagliatamente descritte le procedure di simulazione e di misura per valutare i livelli di esposizione ai campi elettromagnetici dovuti a dispositivi di sorveglianza elettronica e di identificazione a radiofrequenza.
- Standard EN 50364, anche Norma CEI EN 50364 "Limitation of human exposure to electromagnetic fields from devices operating in the frequency range 0 to 10GHz, used in Electronic Article Surveillance (EAS), Radio Frequency Identification (RFId) and similar applications. La norma può essere usata per la dimostrazione di conformità ai requisiti delle Direttive Europee 1999/5/EC e 72/73/ECC, relative alla limitazione dell'esposizione umana ai campi elettromagnetici, e alla Raccomandazione Europea 1999/519/EC e delle Linee Guida ICNIRP del 1998.

Nella valutazione dell'esposizione ai campi elettromagnetici sono importanti due tipologie di limiti indicate come Restrizioni di Base e Livelli di Riferimento Derivati. I primi, difficilmente verificabili, sono direttamente correlati agli effetti biologici. I secondi sono ottenuta per via indiretta ma si riferiscono a grandezze facilmente misurabili.

RESTRIZIONI DI BASE

Restrizioni sull'entità dell'esposizione ai campi elettromagnetici, con considerabili margini di sicurezza, basate su provati effetti sulla salute dell'uomo. Alle basse frequenze (inferiori a 10MHz) la grandezza da monitorare è la densità di corrente indotta nei tessuti, mentre ad alte frequenze (superiori a 100kHz) si fa riferimento al tasso di assorbimento specifico (Specific Absorption Rate - SAR) definito come la densità di potenza assorbita dal corpo umano per unità di massa. Queste grandezze dipendono dall'intensità di campo elettromagnetico emesso dal dispositivo e dalla posizione di quest'ultimo rispetto al corpo umano. Vengono indicate soglie distinte per la popolazione comune ed il personale addetto. Il personale lavorativo consiste di adulti che sono generalmente esposti ai campi elettromagnetici in condizioni note e sono consapevoli dei potenziali rischi per la salute umana e delle precauzioni da prendere per minimizzare gli effetti. La popolazione generica comprende invece individui di qualunque età e stato di salute, non necessariamente informati o resi consapevoli della propria esposizione ai campi elettromagnetici e quindi non nelle condizioni di prendere opportune precauzioni per minimizzare l'esposizione. Vengono di conseguenza considerati limiti di esposizione più severi per la popolazione generica rispetto al personale lavorativo, come presentato in Tabella 15.

EXPOSURE	FREQUENCY RANGE	CURRENT DENSITY J FOR HEAD AND TRUNK mA/m^2	WHOLE-BODY AVERAGE SAR W/KG	LOCALIZED SAR FOR HEAD AND TRUNK W/KG	LOCALIZED SAR (HMBS) W/KG
Occupational exposure	Up to 1 Hz 1-4 Hz 4 Hz/1 kHz 1-100 kHz 100 kHz-10 MHz 10 MHz-10 GHz	40 40/*f* 10 *f*/100 *f*/100 –	– – – – 0.4 0.4	– – – – 10 10	– – – – 20 20
General public exposure	Up to 1 Hz 1-4 Hz 4 Hz-1kHz 1-100 kHz 100 kHz-10 MHz 10 MHz-10 GHz	8 8/*f* 2 *f*/500 *f*/500 –	– – – – 0.08 0.08	– – – – 2 2	– – – – 4 4

Tabella 15 - Restrizioni di Base indicate da ICNIRP per campi elettrici e magnetici variabili, per frequenze fino a 10 GHz per il personale lavorativo (Occupational exposure) e per la popolazione generica (General public exposure)

Il parametro f rappresenta la frequenza in Hertz; la densità di corrente J deve essere mediata su di una sezione trasversale di $1cm^2$ perpendicolare alla sua orientazione. Il SAR massimo localizzato è riferito ad una massa di 10 g di tessuto contiguo.

LIVELLI DI RIFERIMENTO DERIVATI

Fanno riferimento a grandezze fisiche non direttamente associabili ad un effetto biologico ma che possono essere facilmente misurate o stimate in assenza del corpo umano. Questi livelli sono dedotti dalle Restrizioni di Base, a seguito di calcoli e sperimentazioni supponendo condizioni di massimo accoppiamento tra campo elettromagnetico ed individuo. Per il confronto con le soglie indicate bisogna considerare il valore medio delle grandezze, misurate o calcolate in assenza di persone, in un volume di dimensioni simili a quelle di un corpo umano. La conformità di un apparato ai Livelli di Riferimento Derivati comporta automaticamente la sua conformità alle Restrizioni di Base, mentre il fatto che i Livelli di Riferimento vangano superati dal particolare dispositivo non risulta necessariamente in una mancanza di conformità alle Restrizioni di Base. In questo caso sono richieste misure o calcoli addizionali per verificare i suddetti limiti. In alcune condizioni, quando l'esposizione è particolarmente localizzata, come nel caso di dispositivi portatili (telefoni cellulari, palmari), il ricorso ai Livelli di Riferimento di Base non è appropriato ed è richiesto di verificare direttamente le Restrizioni di Base.
Anche per i Livelli di Riferimento vengono indicate soglie differenti per la popolazione e per il personale lavorativo.

FREQUENCY RANGE	E-FIELD STRENGTH (V m^{-1})	H-FIELD STRENGTH (A m^{-1})	B-FIELD (μT)	EQUIVALENT PLANE WAVE POWER DENSITY S_{eq} (W m^{-2})
up to 1 Hz	–	1.63×10^5	2×10^5	–
1-8 Hz	20,000	$1.63 \times 10^5/f^2$	$2 \times 10^5/f^2$	–
8-25 Hz	20,000	$2 \times 10^4/f$	$2.5 \times 10^4/f$	–
0.025-0.82 kHz	500/*f*	20/*f*	25/*f*	–
0.82-65 kHz	610	24.4	30.7	–
0.065-1 MHz	610	1.6/*f*	2.0/*f*	–
1-10 MHz	610/*f*	1.6/*f*	2.0/*f*	–
10-400 MHz	61	0.16	0.2	10
400-2,000 MHz	$3f^{1/2}$	$0.008f^{1/2}$	$0.01f^{1/2}$	*f*/40
2-300 GHz	137	0.36	0.45	50

Tabella 16 - Limiti di Riferimento Derivati in Europa per personale lavorativo per campi elettrici e magnetici imperturbati. Si fa riferimento ad una misura mediata su 6 minuti. I livelli sono espressi in valore efficace

FREQUENCY RANGE	E-FIELD STRENGTH (V m^{-1})	H-FIELD STRENGTH (A m^{-1})	B-FIELD (μT)	EQUIVALENT PLANE WAVE POWER DENSITY S_{eq} (W m^{-2})
up to 1 Hz	–	3.2×10^4	4×10^4	–
1-8 Hz	10,000	$3.2 \times 10^4/f^2$	$4 \times 10^4/f^2$	–
8-25 Hz	10,000	4,000/*f*	5,000/*f*	–
0.025-0.8 kHz	250/*f*	4/*f*	5/*f*	–
0.08-3 kHz	250/*f*	5	6.25	–
3-150 KHz	87	5	6.25	–
0.15-1 MHz	87	0.73/*f*	0.92/*f*	–
1-10 MHz	$87/f^{1/2}$	0.73/*f*	0.92/*f*	–
10-400 MHz	28	0.073	0.092	2
400-2,000 MHz	$1.375f^{1/2}$	$0.0037f^{1/2}$	$0.0046f^{1/2}$	*f*/200
2-300 GHz	61	0.16	0.20	10

Tabella 17 - Limiti di riferimento Derivati in Europa per la popolazione comune per campi elettrici e magnetici imperturbati. Si fa riferimento ad una misura mediata su 6 minuti. I livelli sono espressi in valore efficace

Nei casi in cui ci siano esposizioni simultanee a più frequenze, è richiesto di considerare l'additività degli effetti. L'additività va implementata riferendo ciascuna grandezza da controllare al suo valore limite. Per esempio, le correnti indotte fino a 10 MHz vanno sommate secondo la formula seguente:

$$\sum_{i=1Hz}^{10\,GHz} \frac{J_i}{J_{L,i}} \leq 1$$

dove Ji è la densità di corrente indotta alla frequenza i, e JL,i è la Restrizione di Base sulla densità di corrente indotta alla frequenza i contenuta nella Tabella.1. Analoghe considerazioni valgono per le altre grandezze relative sia alle Restrizioni di Base che ai Livelli di Riferimento Derivati (linee guida ICNIRP).

NORMATIVE ITALIANE

Lo Stato Italiano ha stabilito con la legge quadro sulla "Protezione dalle esposizioni a campi elettrici, magnetici ed elettromagnetici", n.36 del 22/02/2001 limiti più stringenti rispetto alle normative europee nella convinzione che sia opportuno indicare valori di attenzione o obiettivi di qualità che tengano conto anche degli effetti a lungo termine, possibili ma non ancora dimostrati. Si propone pertanto di garantire, nel dubbio, un livello di sicurezza ancora più elevato. Di seguito sono riportate le tabelle indicate nel D.P.C.M dell'8 luglio 2003.

LIMITI DI ESPOSIZIONE	INTENSITÀ DI CAMPO ELETTRICO W (V/M)	INTENSITÀ DI CAMPO MAGNETICO H (A/M)	DENSITÀ DI POTENZA (W/m^2)
0.1 < f < 3 MHz 3 < f < 3000 MHz 3 < f < 300 GHz	60 20 40	0.2 0.05 0.01	– 1 4

Tabella 18 - Limiti di Esposizione, in valore efficace, indicati dallo Stato Italiano nel D.P.C.M. dell'8 luglio 2003 [ex Legge 22 febbraio 2001 n. 36)

A titolo di cautela per la protezione da possibili effetti a lungo termine, eventualmente connessi con le esposizioni ai campi generati alle suddette frequenze all'interno di edifici adibiti a permanenze non inferiori a quattro ore giornaliere, e loro pertinenze esterne che siano fruibili come ambienti abitativi quali balconi, terrazze e cortili esclusi i lastrici solari, si assumono i Valori di Attenzione indicati in Tabella 19.

VALORI DI ATTENZIONE	INTENSITÀ DI CAMPO ELETTRICO W (V/M)	INTENSITÀ DI CAMPO MAGNETICO H (A/M)	DENSITÀ DI POTENZA (W/m^2)
0.1 < f < 300 GHz	6	0.016	0.10 (3 MHz-300 GHz)

Tabella 19 - Valori di Attenzione, in valore efficace, dallo Stato Italiano nel D.P.C.M. dell'8 luglio 2003 [ex Legge 22 febbraio 2001 n. 36]

È indicato che i valori in Tabella 18 e Tabella 19 devono essere mediati su un'area equivalente alla sezione del corpo umano e su qualsiasi intervallo di sei minuti.
La normativa italiana, negli stessi documenti prima citati, individua anche Obiettivi di Qualità. Ai fini della progressiva minimizzazione della esposizione ai campi elettromagnetici, i valori calcolati o misurati all'aperto nelle aree intensamente frequentate, e cioè superfici edificate ovvero attrezzate permanentemente per il soddisfacimento di bisogni sociali, sanitari e ricreativi, non devono superare i valori indicati in Tabella 20.

OBIETTIVI DI QUALITÀ	INTENSITÀ DI CAMPO ELETTRICO W (V/M)	INTENSITÀ DI CAMPO MAGNETICO H (A/M)	DENSITÀ DI POTENZA (W/m^2)
0.1 < f < 300 GHz	6	0.016	0.10 (3 MHz-300 GHz)

Tabella 20 - Valori massimi, in valore efficace, indicati come Obiettivi di Qualità nel D.P.C.M. dell'8 luglio 2003 [ex Legge 22 febbraio 2001 n. 36]

A.3 CRITERI DI VALUTAZIONE

Le procedure di misura e/o di calcolo da seguire per certificare la conformità dei sistemi EAS e RFId ai limiti delle Tabelle.1-3, e per estensione alla normativa italiana, sono dettagliatamente indicate nella norma EN50357:2001. E' previsto un meccanismo di verifica della conformità in tre fasi distinte e successive, che si basa sull'idea che, qualora sia accertata la non conformità di un dispositivo ai Livelli di Riferimento Derivati, è necessario eseguire specifici calcoli su configurazioni a complessità crescente in modo da verificare la conformità alle Restrizioni di Base. Il primo passo della certificazione è pertanto il confronto tra le misure dei campi elettromagnetici in assenza del corpo umano ed i corrispondenti Livelli di Riferimento Derivati. Se il dispositivo risulta conforme non è richiesta alcuna verifica ulteriore. Diversamente, bisogna procedere al secondo passo che comporta il ricorso a modelli di calcolo analitici o numerici che includano la variazione spaziale del campo elettromagnetico nel volume occupato dal corpo umano, mentre quest'ultimo viene rappresentato con geometrie semplici di permettività e conducibilità elettrica uniforme. Qualora anche le Restrizioni di Base risultino superate, è ancora ammesso di poter dimostrare la conformità del dispositivo passando al terzo livello della validazione che richiede di considerare modelli non uniformi e realistici del corpo umano e fare uso della Dosimetria Computazionale.

LIVELLO 1: MISURE DIRETTE PER VERIFICARE LA CONFORMITÀ AI LIVELLI DI RIFERIMENTO DERIVATI

È prevista la misura delle ampiezze di campo elettromagnetico in prossimità del dispositivo sotto test, in assenza del corpo umano, ad un distanza che è indicata dalla normativa per diverse configurazioni di utilizzo. Qualora siano richiesti valori mediati sul volume occupato dal corpo umano, la norma indica la geometria e la posizione di griglie di misura (esempi in Figura 61), in genere relative al torso e alla testa.

LIVELLO 2: MISURE E ANALISI PER VERIFICARE LA CONFORMITÀ ALLE RESTRIZIONI DI BASE

E' richiesto di tenere in conto della variazione spaziale del campo elettromagnetico e del fatto che l'esposizione avvenga in zona vicina o in zona lontana. Il campo elettromagnetico prodotto dal dispositivo può essere misurato su di un reticolo, tipicamente più fitto di quelli

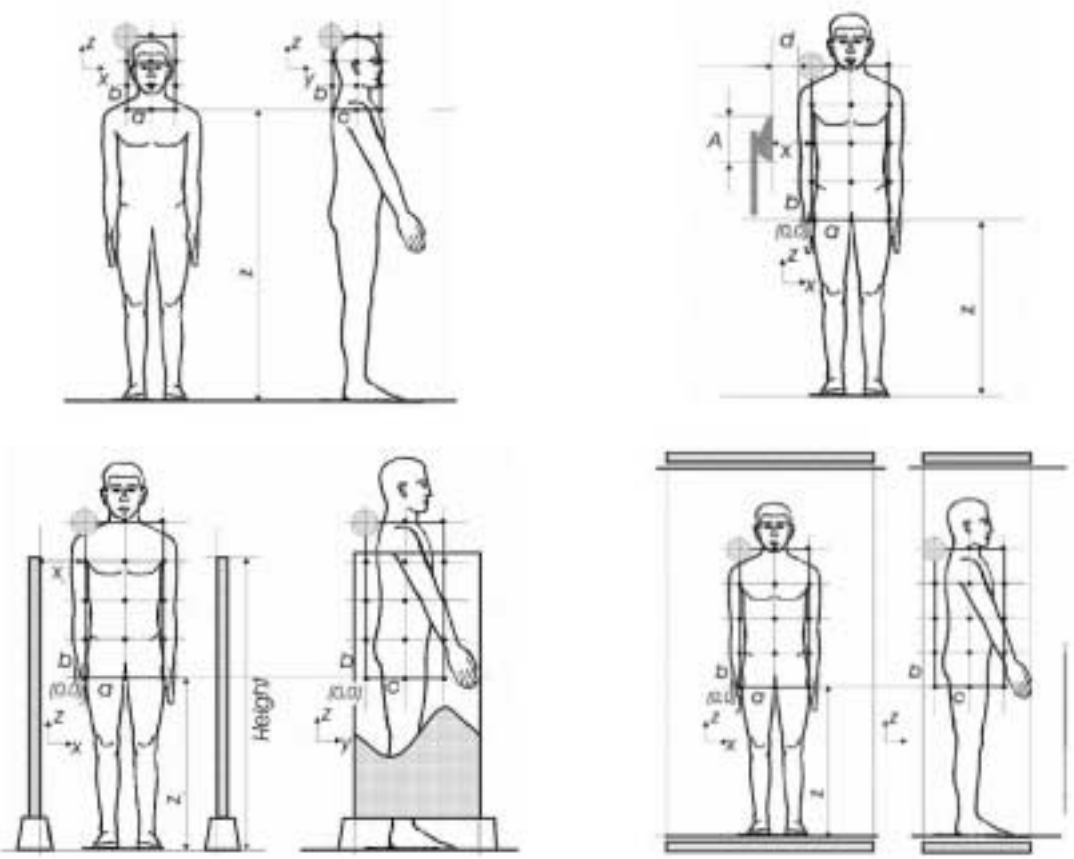

Figura 58 - Esempi di griglie ove eseguire, in assenza del corpo umano, le misure delle grandezze elettromagnetiche al fine di valutare il valore medio da confrontare con i Livelli di Riferimento Derivati. A partire dalla figura in alto a sinistra ed in senso orario

indicati in Figura 61, oppure stimato tramite programmi di simulazione elettromagnetica una volta noti i dettagli elettrici e geometrici del reader. La norma standardizza anche la forma del modello semplificato di corpo umano, e la sua conducibilità uniforme, da usare assieme ad un programma di calcolo elettromagnetico per valutare la densità di correnti indotte (bassa frequenza) oppure il SAR (alta frequenza) per il confronto con le Restrizioni di Base. In particolare sono indicate le dimensioni di un ellissoide prolato rappresentative dell'intero corpo o della sola testa. Non è invece posta alcuna limitazione al tipo di strumento di simulazione numerica da usare, ma è comunque richiesto che l'accuratezza del simulatore sia stata almeno una volta verificata per confronto ad altre soluzioni di riferimento disponibili nella letteratura scientifica.

LIVELLO 3: DOSIMETRIA NUMERICA SU MODELLI ANATOMICI DI CORPO UMANO

È ammesso di verificare la conformità del dispositivo utilizzando la dosimetria computazionale che richiede sofisticati modelli numerici del corpo umano con risoluzione millimetrica. Tali modelli sono spesso ottenuti da immagini tridimensionali provenienti da Risonanza Magnetica Nucleare oppure da foto di sezioni anatomiche e contengono mappe dettagliate dei tessuti associate ad un database di parametri fisici (conducibilità e percettività elettrica,

densità di massa). Il campo elettromagnetico incidente (cioè in assenza del corpo umano) può essere ottenuto come al punto precedente. L'interazione con il modello di corpo umano è infine calcolata utilizzando appositi simulatori elettromagnetici, anch'essi di accuratezza certificata. Nella norma si fa riferimento ad un "uomo standard" di altezza 1.76m ± 5% e peso 73kg ± 5%. La posizione del corpo rispetto al dispositivo sotto test è dedotta dalle indicazioni fornite al Livello 2 (esempi in Figura 61). Le grandezze di confronto con le Restrizioni di Base sono ancora la densità di corrente indotta, a bassa frequenza, e il SAR per dispositivi operati ad alta frequenza.

A.4 ESEMPI DI VALUTAZIONE DELL'ESPOSIZIONE A SISTEMI EAS ED RFID

I sistemi EAS ed RFId funzionanti a bassa frequenza (inferiore a 10 MHz), producono campi principalmente reattivi, con trascurabili effetti propagativi. L'esposizione della popolazione è quindi generalmente limitata al campo magnetico vicino del reader e la sua intensità si attenua molto rapidamente con la distanza. Tale campo risulta quindi estremamente localizzato e quindi, qualora siano presenti più sistemi reader, potrebbe essere lecito valutare l'esposizione dovuta ad un dispositivo alla volta.
I sistemi RFId funzionanti nella gamma UHF (300 MHz - 3 GHz) emettono invece microonde ed il fenomeno propagativo va comunque tenuto in conto ed è necessario verificare le soglie di esposizione anche a qualche metro di distanza dal reader.
Le possibili configurazioni di esposizione ai campi elettromagnetici prodotti da sistemi EAS ed RFId possono differire per le diverse caratteristiche spaziali e temporali dell'emissione (frequenza, potenza, modulazione) e per la tipologia e per l'installazione dell'apparecchiatura. Esiste attualmente poca documentazione disponibile sulla casistica di scenari espositivi di riferimento, sulla base della quale derivare indicazioni progettuali che siano utili alla definizione di dispositivi e di impianti EAS/RFId con caratteristiche di conformità alle normative.
Solo a titolo esemplificativo, vengono di seguito riportati due casi di studio relativi ad un sistema a bassa frequenza EAS ed alla valutazione preliminare di esposizione ad sistemi RFId UHF a 860-960 MHz.

SISTEMA EAS A BASSA FREQUENZA (VARCO)

Si considera un varco EAS operante a 30 kHz, schematizzato come un insieme di due avvolgimenti (coil) rettangolari[50], parzialmente sovrapposti e alimentati in fase con una corrente di 100 A ciascuno (Figura 62).
Il modello anatomico di corpo umano usato per le valutazione dosimetriche ha risoluzione 1.974x1.974x2.93 mm e fa riferimento ad un maschio adulto. Con opportuni ridimensionamenti sono stati derivati modelli di bambini di 10 e 5 anni (Figura 63).

[50] O.P. Gandhi, "Electromagnetic fields: human safety issues", *Annu. Rev. Biomed. Eng.,* Vol. 4, pp. 211-234, 2002

A partire da una stima della corrente sui coil, e applicando la legge di Biot-Savart è preliminarmente calcolata la densità di flusso magnetico B in assenza del corpo umano. Le tre componenti cartesiane ed il modulo di B sono rappresentati in Figura 63 lungo una linea verticale a 20cm dagli avvolgimenti, come indicato nelle raccomandazioni ICNIRP. Confrontando i valori con i Livelli di Riferimento Derivati, si deduce che la densità del flusso magnetico nella regione corrispondente alla testa del modello di 5 anni e di quello di 10 anni è rispettivamente 4-5 volte e 2-3 volte più intensa che nel caso dell'adulto, e comunque superiore al limite ICNIRP di 6.25 mT per la popolazione generica.

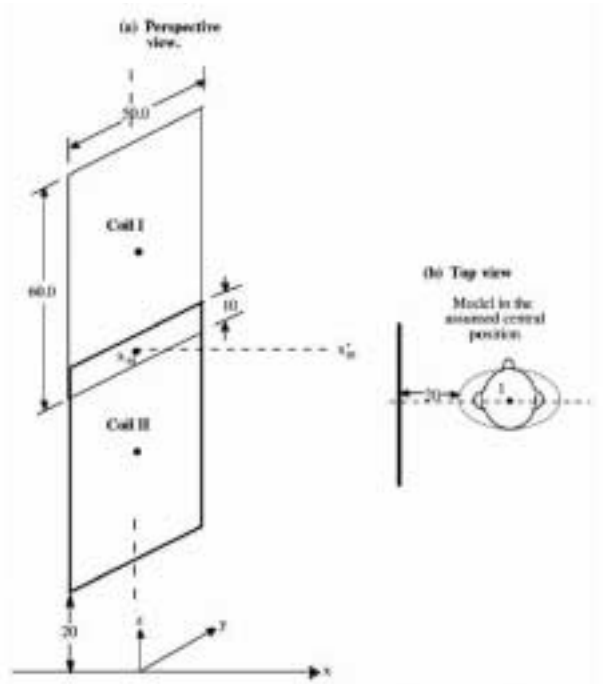

Figura 59 - Schematizzazione di un varco EAS costituito da due coil. Le dimensioni sono in cm. A destra è indicata la posizione mutua varco-corpo umano

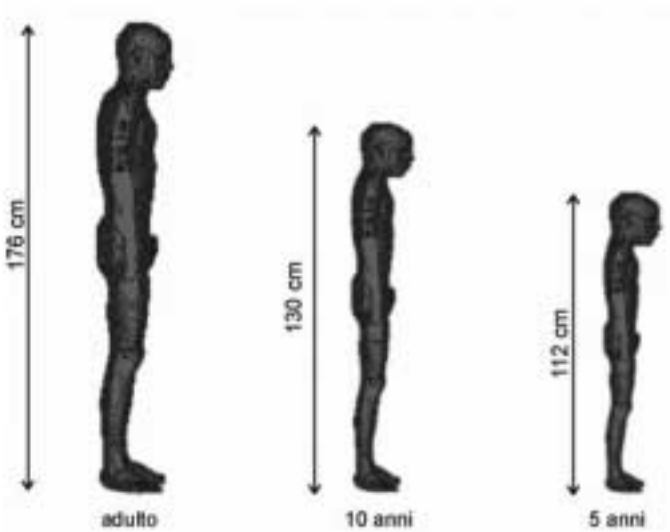

Figura 60 - Tre modelli anatomici usati per il calcolo del campo elettrico indotto e delle densità di corrente in seguito ad esposizione a campi elettromagnetici a bassa frequenza

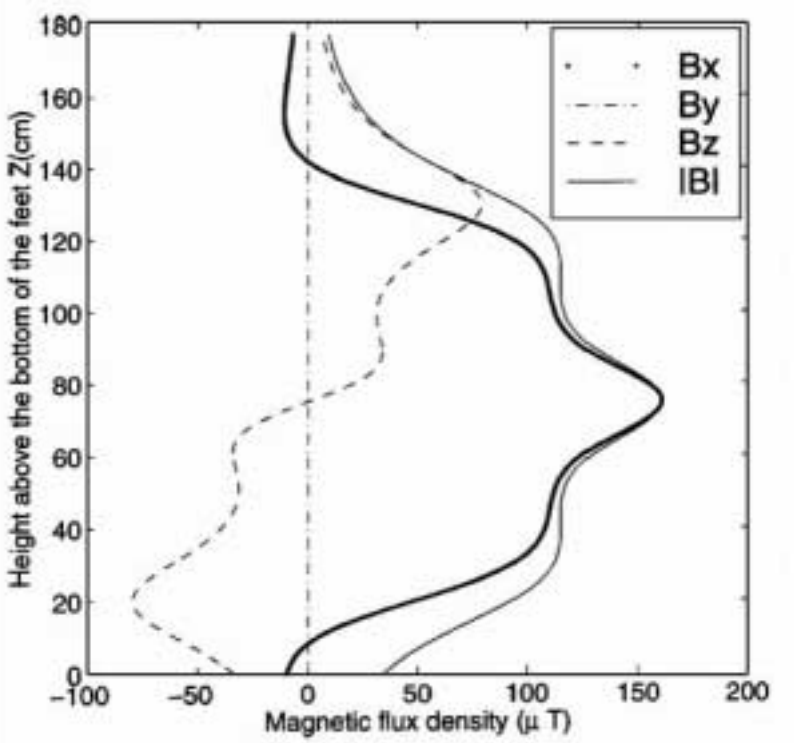

Figura 61 - Andamento spaziale della densità di flusso magnetico B prodotta dal modello di varco EAS in Figura 59, valutata su una linea verticale parallela alla posizione ipoteticamente occupata dal corpo umano, a 20 cm di distanza dalla spalla

Il campo elettrico e le densità di corrente elettrica indotta nel corpo umano sono calcolati utilizzando il Metodo delle Impedenze[51] applicato a modelli volumetrici di adulto e bambino, assumendo la densità di flusso magnetico, precedentemente stimata in assenza di persone, come grandezza d'ingresso. I valori massimi e medi di corrente e di campo elettrico nei vari organi dei tre modelli anatomici sono riportati in Tabella 21. I valori massimi di corrente indotta possono essere direttamente confrontati con le Restrizioni di Base in Tabella 15. Si osserva che nel caso di modello anatomico di soggetto adulto, i livelli nel cervello e nel nervo spinale sono considerevolmente inferiori ai limiti ICNIRP per l'esposizione non controllata della popolazione (a 30 kHz la massima densità di corrente ammissibile e di 60 mA/m2). Nel caso dei modelli di bambini, i valori massimi di corrente nel cervello sono vicini (64.6 mA/m2, bambino di 10 anni) o superiori (98.9 mA/m2, bambino di 5 anni) alle indicazioni della norma. Ad ogni modo, a differenza di quanto accadeva per i livelli di densità di flusso magnetico che risultavano eccedere i Livelli di Riferimento Derivati di oltre cinque volte, la non conformità alle Restrizioni di Base si quantifica per una eccedenza di solo il 60% i valori massimi consentiti.

[51] J.F. DeFord, O.P. Gandhi, "An impedante method to calculate currents in biological bodies exposed to quasi-static electromagnetic fields", *IEEE Transaction on Electromagnetic Compatibility,* N. 27 pp. 168-173, 1985.

ORGAN		ADULT		10-YEAR-OLD		5-YEAR-OLD	
		J (mA/m^2)	E (MA/m^2)	J (mA/m^2)	E (mV/m^2)	J (mA/m^2)	E (mV/m)
Brain	Organ-average max (1 cm^2)	4.75 17.63	47.89 177.83	23.20 64.64	234.13 652.23	40.70 98.93	410.71 998.27
Pineal gland	Organ average max (1 cm^2)	0.92 –	9.29 –	17.42 –	175.73 –	36.27 –	365.95 –
Spinal cord	Organ average max (1 cm^2)	– 32.64	– 538.61	– 40.19	– 663.20	– 43.71	– 721.29
Heart	Organ average max (1 cm^2)	92.69 234.69	185.39 469.38	120.08 296.86	240.16 593.71	130.33 316.80	260.66 633.59
Liver	Organ average max (1 cm^2)	18.15 86.68	277.56 1325.33	23.63 114.57	361.24 1751.76	24.66 121.11	377.11 1851.78
Kidneys	Organ average max (1 cm^2)	36.41 88.08	239.41 579.09	38.06 81.26	250.23 534.26	38.05 78.07	250.19 513.26
Bladder	Organ average max (1 cm^2)	85.11 234.21	394.75 1086.33	86.84 222.24	402.80 1030.81	68.55 170.34	317.93 790.09
Pancreas	Organ average max (1 cm^2)	28.61 86.33	188.08 567.63	38.64 94.74	254.02 622.87	46.72 85.43	307.19 561.64

Tabella 21 - Valori di densità di corrente elettrica e di campo elettrico indotti nei tre modelli anatomici di corpo umano. Per i vari organi sono riportati i valori medi ed i valori massimi, questi ultimi relativi ad una media su una superficie di 1 cm^2

SISTEMA RFID A 860-960 MHZ

Non sono attualmente disponibili casi di studio specifici sulla esposizione a sistemi RFId a bassa o alta frequenza. Nel dominio UHF 860-960MHz potrebbero essere parzialmente applicati gli studi compiuti sull'esposizione ai telefoni cellulari di prima generazione, supponendo che siano assimilabili a dispositivi reader portatili anche se non necessariamente posti a contatto con la testa e funzionanti con potenze differenti. In questo paragrafo si riporta, a titolo puramente illustrativo, una analisi preliminare[52] che permette di stimare i livelli di SAR nel corpo umano esposto all'irradiazione di una postazione RFId posta per esempio su una parete. Per questa analisi è stato utilizzato un modello realistico di corpo umano, con risoluzione di 4mmx4mmx4mm, che comprende testa e torace e include la geometria e le caratteristiche di più di quaranta tessuti differenti[53]. Nell'ipotesi che il corpo umano si trovi a sufficiente distanza del reader, il campo elettromagnetico da questo irradiato verso il corpo umano, può essere approssimato con un'onda piana avente polarizzazione verticale. Questo modello è estremamente semplificato perché non tiene conto in maniera realistica delle caratteristiche delle antenne del reader, del tipo di modulazione e soprattutto dell'interazione con l'ambiente circostante e cioè con soffitto, pavimenti e pareti, ne tanto meno degli oggetti che normalmente si trovano in uno scenario indoor e che

[52] In parte presentata in: G. Marrocco, "Body-matched RFId antennas for wireless biometry", European Conference on Antennas and Propagation, 2006.

[53] M.J. Ackerman, "The visible human project: a resource for education", *J. Acad. Med.* N. 74, pp. 667-670, 1999.

possono notevolmente modificare la distribuzione di campo. Si ipotizza cioè di trovarsi nella situazione di spazio libero e in una modalità di interrogazione di tipo continuativo. Nonostante le suddette semplificazioni, i risultati descritti possono essere comunque utili per avere una prima idea sugli ordini di grandezza delle distribuzioni di SAR e di campo elettromagnetico.
L'onda piana che investe il corpo umano, in direzione del torace trasporta una densità di potenza $EIRP_R/(4\pi d^2)$, dove $EIRP_R$ è la potenza irradiata dal reader (Effective Isotropic Radiated Power[54]) e d è la distanza dal reader. Nell'ipotesi di spazio libero, il modulo del campo elettrico a distanza d si può calcolare dalla formula $|E| = \sqrt{120 EIRP} / d$. Questo modello semplificato per l'emissione del reader è da considerarsi affidabile oltre un paio di lunghezze d'onda da esso, e quindi per una distanza reader-corpo superiore a circa 0.5m.
La potenza assorbita dal corpo umano è valutata con un simulatore elettromagnetico[55] basato sul metodo delle Differenze Finite nel Dominio del Tempo (FDTD), nell'ipotesi in cui il reader irradi una potenza di 3.2 W EIRP (2 W ERP), corrispondente al limite massimo fissato dalle normative europee per questa classe di dispositivi.

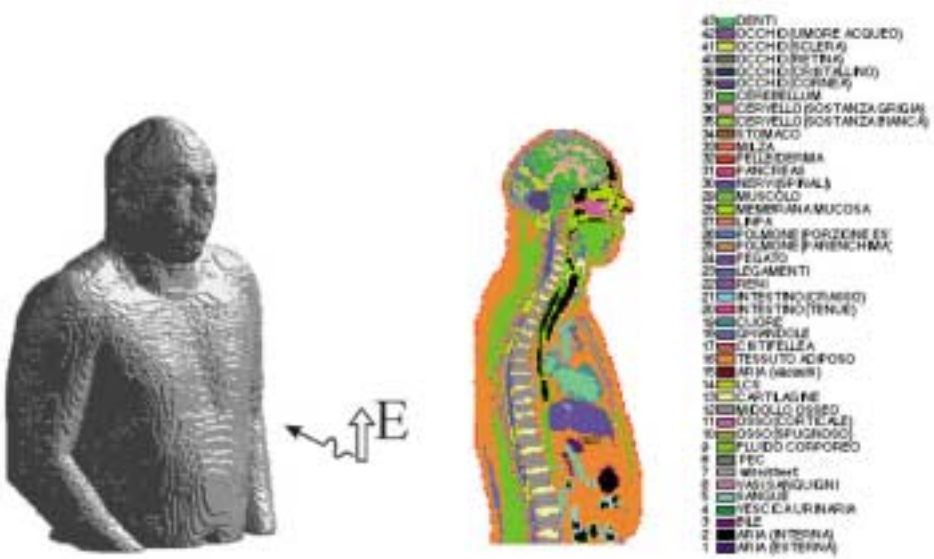

Figura 62 - Mappa anatomica di soggetto adulto con risoluzione di 4mmx4mmx4mm investito da un'onda piana che si può pensare proveniente dal reader posto su una parete. La freccia bianca indica la polarizzazione del campo elettrico incidente

In Tabella 22 sono riportati, per la frequenza di 900 MHz, i valori ottenuti di campo elettrico e di SAR massimo nella testa e nel tronco ed il valore medio di SAR sull'intero corpo. Questi dati devono essere confrontati con i valori limite previsti dalle normative. Considerando le indicazioni italiane, che sono più severe di quelle europee, si osserva che l'intensità di campo elettrico, secondo il modello di propagazione in spazio libero, diventa infe-

[54] Prodotto tra la potenza fornita all'antenna ed il suo guadagno, nella direzione di massima radiazione, relativo ad un'antenna isotropa. È comune anche l'utilizzo della grandezza *ERP*, Effective Radiated Power, definita come l'*EIRP* ma con riferimento al guadagno di un dipolo a mezz'onda. Vale la relazione *EIRP* = 1.6 *ERP*.
[55] G. Marrocco, F. Bardati, "BEST: a finite-difference solver for time electromagnetics", Simulation Practice Theory, vol. 7, pp. 279-293, Jul. 1999.

riore a 20 V/m oltre 0.5m dalla sorgente, ed inferiore a 6 V/m dopo circa 2m. Prendendo in considerazione le Restrizioni di Base (Tabella 15) sulla potenza assorbita (SAR) nel corpo, nel caso di popolazione generica, il limite di 0.08 W/kg viene ragionevolmente rispettato per una distanza tra sorgente e corpo umano superiore a 0.5m. Di conseguenza, sempre nell'ambito delle forti limitazioni del modello considerato, che comunque non tiene conto del tipo di modulazione, e nell'ipotesi peggiorativa di esposizione prolungata, la minima distanza del reader dal corpo umano è plausibilmente dell'ordine della frazione di metro.

d (m)	Imperturbed r.m.s. (E)	Localized SAR in the head (mW/kg)	Localized SAR in the trunk (MW/kg)	Body averaged SAR (mW/kg)
0.5	20	13	8	6
1.0	10	3	2	1.5
2.0	5	1	1	<1
3.0	3	<1	<1	<1
4.0	2	<1	<1	<1

Tabella 22 - Valori di campo elettrico imperturbato (in assenza del corpo umano) e valori di SAR calcolato nel modello realistico del corpo umano in funzione della distanza dalla sorgente. Dati riferiti alla frequenza di 900 MHz

A.5 Osservazioni conclusive

La realizzazione di piattaforme RFId e AES richiede, come per qualunque altra apparecchiatura radiante, la certificazione di conformità alle normative in materia di salvaguardia dell'uomo dall'esposizione ai campi elettromagnetici. La documentazione disponibile in ambito Comunitario descrive in maniera dettagliata le procedure di misura e di calcolo da eseguire per valutare l'emissione elettromagnetica dell'apparato ed indicare la eventuale distanza di sicurezza entro la quale sia inibita l'esposizione continuativa o prolungata di persone. Tali attività possono essere svolte da Enti specializzati oppure direttamente dal costruttore qualora sia provvisto della adeguata strumentazione e degli opportuni modelli di calcolo la cui accuratezza sia stata in qualche modo certificata.

Bisogna inoltre osservare che il produttore di uno specifico componente dell'apparato non è tenuto ad essere a conoscenza dei livelli di esposizione complessiva nei quali l'intero apparato si troverà a funzionare. Non c'è inoltre nessuna indicazione nelle normative europee, recepite anche nelle norme italiane (CEI EN 50364, punto 5.4), sulla necessità di eseguire una valutazione di conformità dopo l'istallazione dell' apparato. L'installatore dovrebbe però farsi carico di eseguire i test che siano stati specificati dal produttore per assicurarsi che l'apparecchiatura stia funzionando in accordo con le modalità di progetto. Qualora ci fossero dei parametri dell'apparecchiatura che necessitino di essere definiti all'atto dell'installazione al fine di assicurare la conformità agli standard, tali modifiche vanno eseguite e deve restarne traccia nella documentazione dell'apparato, assieme a qualunque tipo di test necessario ad assicurare che le modifiche richieste siano state implementate correttamente.

C'è, infine, una notevole carenza di casistica di scenari tipici, analizzati in dettaglio, che permetterebbero per analogia di avere indicazioni specifiche utilizzabili nella fase di progetto del singolo dispositivo o ancor più nel dispiegamento dell'apparato, in modo da ridurre al minimo il ricorso a specifiche attività di misura e simulazione.

Appendice 3 - Il provvedimento del Garante (9 Marzo 2005)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello vice-presidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;
VISTI gli articoli 3, 7 e 8 della Carta dei diritti fondamentali dell'Unione europea;
VISTO il Codice in materia di tutela dei dati personali (d.lg. 30 giugno 2003, n. 196);
RITENUTA la necessità di prescrivere alcune misure al fine di rendere il trattamento dei dati personali nell'ambito dei sistemi di Radio Frequency Identification conforme alle disposizioni vigenti, anche in relazione al principio di dignità della persona (art. 1 Carta dei diritti fondamentali dell'Unione europea; artt. 2 e 154, comma 1, lett. c), del Codice in materia di protezione dei dati personali);
VISTI i commenti e le osservazioni pervenuti a seguito della consultazione pubblica indetta da questa Autorità riguardo alle tecniche di Radio Frequency Identification;
VISTI gli atti d'ufficio e le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento n. 1/2000;
RELATORE il prof. Stefano Rodotà;

PREMESSO

La *Radio Frequency Identification* ("RFId") si diffonde rapidamente in numerosi settori.
L'utilizzo di tale tecnologia può risultare utile, ad esempio, per garantire una migliore gestione dei prodotti aziendali, per incrementare la rapidità di operazioni commerciali anche a vantaggio dei consumatori, per rintracciare l'origine di prodotti particolarmente delicati, per controllare accessi a luoghi riservati e per altri usi nei luoghi di lavoro.
Tuttavia, determinati impieghi della *RFId* possono costituire una violazione del diritto alla protezione dei dati personali (art. 1 del Codice) ed avere serie ripercussioni sull'integrità e la dignità della persona, anche perché, per le ridotte dimensioni e l'ubicazione delle cd. "etichette intelligenti" e dei relativi lettori, il trattamento dei dati personali attraverso la *RFId* può essere effettuato all'insaputa dell'interessato.
In particolare, come rilevato anche dal Gruppo dei garanti europei *(documento di lavoro adottato il 19 gennaio 2005 dal Gruppo costituito ai sensi dell'art. 29 della direttiva n. 95/46/CE, in http://europa.eu.int/...),* l'impiego di tecniche di RFId, da parte sia di sog-

getti privati, sia di soggetti pubblici, può determinare forme di controllo sulle persone, limitandone le libertà. Attraverso l'impiego della *RFId,* potrebbero, ad esempio, raccogliersi innumerevoli dati sulle abitudini dell'interessato a fini di profilazione, tracciare i percorsi effettuati da quest'ultimo o verificare prodotti (vestiti, accessori, medicine, prodotti di valore) dallo stesso indossati o trasportati.

In alcune ipotesi, l'impiego della *RFId* può essere finalizzato esclusivamente al tracciamento di prodotti, per garantire una maggiore efficienza nel processo di produzione industriale. In particolare, ove tali sistemi siano impiegati da produttori o distributori solo all'interno di una catena di distribuzione, l'informazione contenuta su ciascuna etichetta del prodotto può costituire un dato personale (di per sé sola, o per effetto della connessione con ulteriori informazioni quali stato di conservazione, stabilimento di produzione, sussistenza di difetti, appartenenza a partite avariate, ecc.) relativo ai soli produttori o distributori.

Questo tipo di trattamento di dati non pone particolari problemi di liceità e sotto il profilo della tutela dei soggetti interessati.

In altri casi, invece, l'utilizzo dei sistemi di *RFId* può comportare il trattamento di dati personali relativi a terzi, persone fisiche o giuridiche, enti o associazioni *(art. 4, comma 1, lett. a) e b) del Codice).*

Infatti, le "etichette" potrebbero contenere esse stesse dati personali, o essere impiegate in modo tale da rendere comunque identificabili gli interessati attraverso il raffronto con altre informazioni.

I sistemi informativi cui esse sono collegate possono permettere, altresì, di individuare la posizione geografica di chi detiene l'etichetta o l'oggetto su cui essa è apposta, con considerevoli ripercussioni sulla libertà di circolazione delle persone.

La *RFId* può essere inoltre adoperata nelle tecniche di impianto di *microchip* sottocutaneo, anche su individui: l'inserimento di microprocessori sottopelle, per l'evidente delicatezza delle implicazioni che ne derivano sui diritti delle persone, rende quindi necessaria la predisposizione di particolari cautele.

Ulteriori pericoli per gli interessati possono altresì derivare - specie, in prospettiva, con l'adozione di *standard* comuni - dalla possibilità che terzi non autorizzati "leggano" i contenuti delle etichette o intervengano sugli stessi (mediante, ad esempio, "riscrittura"). Ciò, tenendo anche conto che lo sviluppo tecnologico può comportare un aumento della potenza dei sistemi di *RFId,* rendendo possibile una "lettura" delle etichette a distanze sempre maggiori; parallelamente, il progressivo contenimento dei costi di produzione dei dispositivi in questione agevola la crescita dell'impiego di tali tecniche di identificazione.

Infine, i rischi per la vita privata dei cittadini possono accrescersi nel caso di un'integrazione della *RFId* con infrastrutture di rete (telefonia, Internet, ecc.).

È quindi necessario che l'implementazione e l'utilizzo della *RFId,* ove si configuri un trattamento di dati personali, avvenga nel rispetto dei principi dettati dal Codice e, in particolare, delle libertà, dei diritti fondamentali e della dignità degli interessati *(art. 2, comma 1, del Codice).*

Il Garante, a garanzia degli interessati e in conformità a quanto previsto dal Codice, prescrive pertanto alcune prime misure che devono essere approntate da parte di coloro che, a diverso titolo, si avvalgano di tecniche fondate sulla *RFId;* ciò, anche al fine di consentire ad operatori e produttori di predisporre dispositivi offerti alla conformità alla normativa in materia di tutela dei dati personali.
Tali prescrizioni si applicano ai casi in cui, per effetto dell'impiego di sistemi RFId, si trattino dati personali relativi a terzi identificati o identificabili *(art. 4, comma 1, lett. b)* del Codice); non operano invece nei casi - che non pongono particolari problemi sul piano della protezione dei dati - in cui la *RFId* non comporti il predetto trattamento e sia utilizzata, ad esempio, in una catena di distribuzione aziendale al solo fine di garantire una maggiore efficienza del processo di produzione.
L'Autorità si riserva peraltro di impartire ulteriori prescrizioni che potrebbero rendersi necessarie in relazione a specifici trattamenti di dati personali effettuati mediante RFId, anche in vista dell'evoluzione rapida e costante che contraddistingue questa tematica.

PRINCIPI GENERALI

L'utilizzo della RFId può comportare condizionamenti e vincoli per gli interessati. Si rende pertanto necessario assicurare il rigoroso rispetto di tutti i principi dettati dal Codice, tra i quali, vanno qui richiamati, in particolare:
I sistemi di RFId devono essere configurati in modo tale da evitare l'utilizzazione di dati personali oppure, a seconda dei casi, l'identificabilità degli interessati, quando non siano strettamente necessarie in relazione alla finalità perseguita.
Tale valutazione deve essere condotta tenendo presente che nella maggior parte degli impieghi, ad esempio nella catena di distribuzione di prodotti, non è necessario trattare dati personali relativi a terzi.

LICEITÀ (ART. 11, COMMA 1, LETT. A), DEL CODICE)

Il trattamento mediante RFId è lecito solo se si fonda su uno dei presupposti che il Codice prevede, rispettivamente, per i soggetti pubblici da un lato (svolgimento di funzioni istituzionali: artt. 18-22) e, dall'altro, per soggetti privati ed enti pubblici economici (ad es., adempimento ad un obbligo di legge, o consenso libero ed espresso: artt. 23-27).
L'utilizzo di tali tecniche deve svolgersi anche nel rispetto di altre leggi e regolamenti che possono di volta in volta rilevare a seconda del loro settore di impiego. In ambito lavorativo, l'uso di tecniche RFId deve in particolare rispettare il divieto di controllo a distanza del lavoratore (art. 4 l. 20 maggio 1970, n. 300; art. 114 del Codice).

FINALITÀ E QUALITÀ DEI DATI (ART. 11, COMMA 1, LETT. B), C), D) E E), DEL CODICE)

Il titolare (art. 4, comma 1, lett. f)) può trattare dati personali esclusivamente per scopi determinati, espliciti e legittimi (art. 11, comma 1, lett. b)).

I dati possono essere inoltre utilizzati soltanto in termini compatibili con la finalità per la quale sono stati originariamente raccolti; devono essere conservati per il tempo strettamente necessario a perseguire tale finalità, decorso il quale devono essere cancellati o resi anonimi (art. 11, comma 1, lett. b) e e) del Codice).
Il titolare deve altresì curare la pertinenza e non eccedenza, l'esattezza e l'aggiornamento dei dati personali (art. 11, comma 1, lett. c) e d) del Codice).

PROPORZIONALITÀ (ART. 11, COMMA 1, LETT. D), DEL CODICE)

Il titolare deve verificare il rispetto del principio di proporzionalità in tutte le diverse fasi del trattamento.
I dati trattati e le modalità del loro trattamento, anche con riferimento alla tipologia delle infrastrutture di rete adoperate, non devono risultare sproporzionati rispetto agli scopi da prefissare.
Non risulta di regola giustificato il trattamento che comporti il funzionamento delle etichette apposte su prodotti acquistati dall'interessato anche fuori dell'esercizio commerciale, a meno che ciò sia necessario per fornire un servizio specificamente e liberamente richiesto dall'interessato stesso.

INFORMATIVA (ART. 13 DEL CODICE)

Il titolare del trattamento, nel fornire agli interessati la prescritta informativa precisando anche le modalità del trattamento (art. 13 del Codice), deve indicare la presenza di etichette RFId e specificare che, attraverso i sistemi connessi, è possibile raccogliere dati personali senza che gli interessati si attivino al riguardo. Analogamente, deve essere segnalata mediante informativa l'esistenza di lettori in grado di "attivare" l'etichetta (lettori i quali possono comunque essere posti in essere solo in quanto strettamente necessari in rapporto alla finalità del trattamento).
Chiara evidenza deve essere data anche alle modalità per asportare o disattivare l'etichetta, o per interrompere in altro modo il funzionamento del sistema di RFId.
L'informativa potrebbe essere altresì fornita attraverso appositi avvisi agevolmente visionabili nei luoghi in cui le tecniche RFId sono adoperate, con un formato ed un posizionamento tale da risultare chiaramente visibile.
La presenza di avvisi non esime i titolari del trattamento dall'apporre un'idonea informativa sugli oggetti o sui prodotti recanti le "etichette intelligenti", qualora le stesse rimangano attive dopo che è stato reso possibile associarle con dati relativi a terzi identificati o identificabili, in particolare al di fuori dei luoghi (ad esempio esercizi commerciali) in cui si fa uso della RFId.

TRATTAMENTO DA PARTE DI PRIVATI: IL CONSENSO (ARTT. 23 E SS. DEL CODICE)

In generale, l'utilizzo di RFId che implichi un trattamento di dati personali da parte di privati può essere effettuato solo con il consenso dell'interessato (art. 23), a meno che ricorra un altro presupposto equipollente del trattamento (art. 24).

In presenza di un trattamento di dati personali, il consenso, ove necessario, deve avere i requisiti previsti (art. 23 del Codice). In particolare, esso deve essere specifico ed espresso, non rilevando a tal fine il semplice comportamento concludente dell'interessato (art. 23, commi 1 e 3).
Il consenso non è altresì valido se ottenuto sulla base di pressioni o condizionamenti sull'interessato (art. 23, comma 3). Ove non acconsenta al trattamento, l'interessato non dovrà incorrere in conseguenze pregiudizievoli o limitazioni che non siano diretta conseguenza dell'impossibilità di effettuare il trattamento dei dati che lo riguardano.
Se il trattamento riguarda dati di carattere sensibile (art. 4, comma 1, lett. d)), il consenso deve essere manifestato per iscritto e il trattamento può essere effettuato solo previa autorizzazione del Garante (art. 26 del Codice).
Anche in presenza del consenso dell'interessato o di un altro presupposto del trattamento, il trattamento dei dati personali mediante RFId deve comunque svolgersi nel rispetto dei menzionati principi di finalità, proporzionalità e dignità (artt. 2, comma 1, e 11, comma 1).
Tutto ciò premesso, e nella consapevolezza della prevedibile diffusione della *RFId* in diversi settori ed impieghi, possono sin da ora distinguersi - con riferimento al profilo del consenso - alcuni casi specifici:

a) qualora le tecniche di *RFId* siano adoperate, in esercizi commerciali, nel quadro delle modalità di pagamento (ad es. cd. carrello elettronico), e tale impiego non comporti alcuna riconducibilità dei prodotti ad acquirenti identificati o identificabili, non sussiste, in generale, la necessità di richiedere un consenso, in base alla normativa sulla protezione dei dati personali, ai clienti stessi;

b) nel caso in cui le tecniche di *RFId* siano associate all'utilizzo di carte di fidelizzazione della clientela e al trattamento di dati relativi a clienti a fini di profilazione commerciale, valgono anche i principi di protezione dei dati - con specifico riferimento a informativa, consenso, necessità e proporzionalità - esplicitati da questa Autorità nel provvedimento del 24 febbraio 2005 (in www.garanteprivacy.it);

c) fermo restando, come sopra rilevato, che non è di regola lecita l'installazione di etichette *RFId* destinate a rimanere attive anche oltre la barriera-cassa dell'esercizio commerciale in cui sono utilizzate, tale ipotetico impiego, ove lecito, presuppone comunque il necessario consenso dell'interessato, a meno che possa operare un altro presupposto equipollente del trattamento *(art. 24 del Codice);*

d) nei casi di impiego di *RFId* per la verifica di accessi a determinati luoghi riservati devono essere predisposte idonee cautele per i diritti e le libertà degli interessati. In particolare,

d1) ove si intenda utilizzare tali tecniche per verificare accessi a luoghi di lavoro, o comunque sul luogo di lavoro, va tenuto conto che lo Statuto dei lavoratori vieta l'uso di impianti e apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori e, nel caso in cui il loro impiego risulti necessario per altre finalità, prescrive alcune garanzie *(art. 4 l. 20 maggio 1970, n. 300; art. 114 del Codice)*

alle quali si affianca l'osservanza dei richiamati principi di necessità, finalità e proporzionalità del trattamento dei dati;

d2) qualora la *RFId* sia adoperata per controllare l'accesso occasionale di terzi a determinati luoghi, occorre predisporre un meccanismo che, in caso di indisponibilità dell'interessato, permetta a quest'ultimo di entrare comunque nel luogo in questione, con eventuale adozione - e solo se necessario - di misure di cautela rimesse alla ragionevole valutazione del titolare.

ESERCIZIO DEI DIRITTI (ARTT. 7-10 DEL CODICE)

Il titolare del trattamento deve agevolare l'esercizio, da parte dell'interessato, dei diritti di cui all'art. 7 del Codice, semplificando le modalità e riducendo i tempi per il riscontro al richiedente (art. 10, comma 1 del Codice). Già nella fase di progettazione delle tecnologie, i produttori di sistemi RFId dovrebbero opportunamente predisporre modalità idonee a garantire agli interessati un agevole esercizio dei diritti.

DISATTIVAZIONE O RIMOZIONE DELLE ETICHETTE

All'interessato deve essere riconosciuta la possibilità di ottenere, gratuitamente e in maniera agevole, la rimozione o la disattivazione delle etichette RFId al momento dell'acquisto del prodotto su cui è apposta l'etichetta o al termine dell'utilizzo del dispositivo.
Le etichette devono essere posizionate in modo tale da risultare, per quanto possibile, facilmente asportabili senza danneggiare o limitare la funzionalità del prodotto o dell'oggetto a cui si riferiscono (ad esempio, disponendone la collocazione sulla sola confezione).

IMPIANTO SOTTOCUTANEO DI MICROCHIP

L'impianto sottocutaneo di microchip in esseri umani solleva problematiche, particolarmente delicate, che hanno già indotto altre autorità garanti in Europa a considerarlo inaccettabile sul piano della protezione dei dati.
Anche nei casi in cui un limitato impiego di microprocessori sottocutanei è stato permesso (ad es., negli Stati Uniti: Food and Drug Administration, 12 ottobre 2004) sono stati comunque messi in evidenza i potenziali rischi di tali operazioni, sia per la salute dei soggetti che si sottopongono all'impianto, sia per la sicurezza dei dati personali trattati.
Gli impianti sottocutanei di microchip devono ritenersi in via di principio esclusi, in quanto contrastanti, con riferimento alla protezione dei dati, con il principio di dignità (art. 2 del Codice), ferme restando le altre norme dell'ordinamento a garanzia dell'integrità fisica e dell'inviolabilità della dignità della persona, contenute anche nella Carta dei diritti fondamentali dell'Unione europea (artt. 1 e 3).
Fatte salve le previsioni della normativa sulla protezione dei dati e le prescrizioni del presente provvedimento, l'impiego di microchip sottocutaneo può essere quindi ammesso solo in casi eccezionali, per comprovate e giustificate esigenze a tutela della salute delle persone, in stretta aderenza al principio di proporzionalità (art. 11 del Codice), e nel rigoroso rispetto della dignità dell'interessato (art. 2, comma 1).

L'interessato dovrebbe poter essere in grado di ottenere di regola, in qualunque momento e senza oneri, la rimozione del microchip e l'interruzione del relativo trattamento dei dati che lo riguardano.
I titolari del trattamento devono inoltre predisporre modalità di impianto e di impiego delle etichette sottocutanee tali da garantire la riservatezza circa la presenza delle stesse etichette nel corpo dell'interessato.
I trattamenti di dati sensibili, oltre che effettuati nell'osservanza dei presupposti e dei limiti stabiliti dal Codice (artt. 22 e 2; Parte II, Titolo V del Codice), devono essere, ove prescritto (artt. 26 e 76), preventivamente autorizzati dal Garante.
Il Garante si riserva di prescrivere ai titolari del trattamento, ai sensi dell'art. 17 del Codice, di sottoporre alla verifica preliminare di questa Autorità (anche con eventuali provvedimenti di carattere generale) i sistemi di RFId destinati all'impianto sottocutaneo che, in quanto tali, presentano rischi specifici per i diritti, le libertà fondamentali e la dignità degli interessati.

ULTERIORI PRESCRIZIONI

Restano, fermi, in aggiunta alla prescrizioni del presente provvedimento, gli obblighi che il Codice detta ai titolari del trattamento.
Ci si riferisce, in particolare:

a) all'obbligo di notificazione al Garante dei trattamenti
   - concernenti dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica *(art. 37, comma 1, lett. a))*
   - effettuati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzarne abitudini e scelte in ordine ai prodotti acquistati *(artt. 37, comma 1, lett. d));*

b) agli obblighi relativi alle misure di sicurezza (artt. 31-36 e Allegato B) del Codice), affinché siano ridotti al minimo i rischi di distruzione o perdita anche accidentale dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

c) alla selezione dei soggetti che, in qualità di incaricati o responsabili del trattamento, sono autorizzati a compiere operazioni di trattamento sulla base dei compiti assegnati e delle istruzioni impartite (artt. 29 e 30 del Codice).

TUTTO CIÒ PREMESSO IL GARANTE:

ai sensi dell'art. 154, comma 1, lett. c) del Codice, prescrive ai soggetti che, a diverso titolo, effettuino trattamenti di dati personali avvalendosi della *RFId,* le misure necessarie od opportune indicate nel presente provvedimento al fine di rendere il trattamento conforme alle disposizioni vigenti.

Roma, 9 marzo 2005

Appendice 4 - Le schede dei progetti RFId

A.1 Le schede raccolte dalle associazioni di categoria

Il CNIPA ha provveduto ad inviare ad alcune associazioni di categoria, scelte in modo da poter ottenere una fotografia completa dei campi applicativi, un questionario complesso, relativo alle applicazioni ad oggi in essere nel campo RFId.
Alcune delle risposte ottenute, riassunte sotto forma di schede, sono di seguito riportate, al fine di rendere maggiormente esplicita la disomogeneità oggi esistente tra i diversi utilizzatori di tale tecnologia. In particolare sono di seguito riportate le principali aree applicative a cui le schede fanno riferimento:

- Campo Alimentare (es. tracciamento dei capi da macello, tracciamento delle trasformazioni alimenti);
- Campo Aziendale (es. tracciamento degli asset aziendali);
- Campo Documentale (es. tracciamento della movimentazione di volumi cartacei);
- Campo Ospedaliero (es. gestione del blocco operatorio, associazione mamma - neonato);
- Campo Gestionale (es. gestione cespiti);
- Gestione Veicolare (es. gestione dei parcheggi).

Per completezza, in coda alle schede italiane, vengono riportate anche alcune esperienze estere, rientranti nel campo sanitario/ospedaliero, relative all'ospedale di Jena e alla Purdue Pharma (relativamente al tracciamento dei farmaci).

Schede relative ad applicazioni alimentari

La prima scheda, di seguito riportata, è relativa, nello specifico, alla tracciabilità di un animale durante l'intero processo di macellazione.

Campo Applicativo	ALIMENTARE
Nome del Progetto	TRACCIABILITÀ MACELLO SUINI
Referente del Progetto	
Caratteristiche Tecniche Frequenze Utilizzate Tipologie di tag (attivi, passivi, semipassivi) Distanza massima lettore/tag	 13.56 MhZ attivi 150 mm

Dimensioni del Progetto Numero di utenti attuali e previsti Num. di sedi ed unità organizzative coinvolte	 20 2
Impatto sociale ed organizzativo Impatto sulla privacy Impatto sull'organizzazione aziendale	 No Limitato
Percorso di Attuazione Studio di fattibilità Prototipo Pilota	 Si/No - Commenti Si/No - Commenti Si/No - Commenti
Tempi di Implementazione	30 giorni
Costi	€ 50.000,00
Benefici	acquisizione puntuale dei dati di tracciabilità prodotto
Eventuali criticità emerse	

Tabella 23 - Scheda di progetto per la tracciabilità del macello suini

Un ulteriore impiego della tecnologia RFId si verifica per il tracciamento dei prodotti alimentari.

Campo Applicativo	TRACCIABILITÀ/RINTRACCIABILITÀ SU TRASFORMAZIONE PRODOTTI ALIMENTARI
Nome del Progetto	Tracciabilità RFId
Referente del Progetto	
Caratteristiche Tecniche Frequenze Utilizzate Tipologie di tag (attivi, passivi, semipassivi) Distanza massima lettore/tag	 HF 13.56 MHz Tag passivi: adesivi cartacei circa 30 cm
Dimensioni del Progetto Numero di utenti attuali e previsti Numero di sedi ed unità organizzative coinvolte	 circa 20 utenti 1
Impatto sociale ed organizzativo Impatto sulla privacy Impatto sull'organizzazione aziendale	 No Si
Percorso di Attuazione Studio di fattibilità Prototipo Pilota	 Si No – in fase di definizione No
Tempi di Implementazione	60 gg
Costi	€ 15.000,00
Benefici	tracciabilità e gestione dei lotti sulla linea di trasformazione prodotti alimentari
Eventuali criticità emerse	costo tag applicabili a confezioni di prodotti alimentari

Tabella 24 - Scheda di progetto per la trasformazione dei prodotti alimentari

SCHEDE RELATIVE AD APPLICAZIONI AZIENDALI

La scheda successiva prevede l'impiego della tecnologia RFId per la gestione degli asset nel progetto per le metropolitane di Roma.

Campo Applicativo	ASSET MANAGEMENT
Nome del Progetto	ASSET MANAGEMENT PER METROPOLITANE DI ROMA
Referente del Progetto	
Caratteristiche Tecniche Frequenze Utilizzate Tipologie di tag (attivi, passivi, semipassivi) Distanza massima lettore/tag	 13.56 MHz Tag passivi 50 cm a 50 km/h
Dimensioni del Progetto Numero di utenti attuali e previsti Num. di sedi ed unità organizzative coinvolte	
Impatto sociale ed organizzativo Impatto sulla privacy Impatto sull'organizzazione aziendale	 No
Percorso di Attuazione Studio di fattibilità Prototipo Pilota	 Si/No - Commenti Si/No - Commenti Si - 1 stazione 6 treni
Tempi di Implementazione	3 mesi
Costi	€ 100.000,00
Benefici	ottimizzazione processo di manutenzione
Eventuali criticità emerse	

Tabella 25 - Scheda di progetto per asset management

SCHEDE RELATIVE AD APPLICAZIONI DOCUMENTALI

La tabella di seguito riportata mostra l'applicazione della tecnologia alla gestione documentale dei fascicoli.

Campo Applicativo	RFId APPLICATO AMBITO DOCUMENTALE
Nome del Progetto	TRACCIAMENTO MOVIMENTAZIONE FASCICOLI CON SISTEMA RFId
Referente del Progetto	
Caratteristiche Tecniche Frequenze Utilizzate Tipologie di tag (attivi, passivi, semipassivi) Distanza massima lettore/tag	 HF 13.56 MHz Tag passivi 30cm

Dimensioni del Progetto Numero di utenti attuali e previsti Num. di sedi ed unità organizzative coinvolte	 circa 15 utenti sono coinvolti nella movimentazione coinvolti 8 uffici per un totale di 2460 fascicoli (2004-2005-2006)
Impatto sociale ed organizzativo Impatto sulla privacy Impatto sull'organizzazione aziendale	 No processo di movimentazione fascicoli invariato e impatto organizzativo solo nella fase di taggatura fascicoli
Percorso di Attuazione Studio di fattibilità Prototipo Pilota	 Si - valutazione per ridurre impatti sui processi Si - test vincoli "fisici" e ambientali Si
Tempi di Implementazione	luglio-novembre 2005 = sperimentazione; da dicembre produzione
Costi	progettazione 20%; HW 40%; SW 40%
Benefici	riduzione tempi di ricerca fascicoli - migliore gestione pratiche urgenti
Eventuali criticità emerse	

Tabella 26 - Scheda di progetto per i tracciamento dei fascicoli

Schede relative ad applicazioni ospedaliere

Di seguito viene riportata la scheda di progetto per una esperienza di gestione in ambito ospedaliero di due realtà, la prima di gestione del blocco operatorio, la seconda esperienza impiega gli RFId per il riconoscimento mamma – neonato.

Campo Applicativo	SANITÀ
Nome del Progetto	Gestione del Blocco Operatorio
Referente del Progetto	
Caratteristiche Tecniche Frequenze Utilizzate Tipologie di tag (attivi, passivi, semipassivi) Distanza massima lettore/tag	 13.56MHz Tag Passivi lettura in prossimità.
Dimensioni del Progetto	
Numero di utenti attuali e previsti	I posti letto accreditati sono 506 in regime ordinario e 70 per ricoveri in day hospital, mentre ogni anno i ricoveri in regime ordinario sono oltre 18.000 e 10.000 in day hospital, con una media di circa 4.000 parti
Num. di sedi ed unità organizzative coinvolte	22 poliambulatori territoriali.

Impatto sociale ed organizzativo Impatto sulla privacy	I dati sono stati crittografati e memorizzati sul braccialetto del paziente in base allo standard Iso 15693. Tale sistema impedisce l'accidentale letture di informazioni riservate e la loro diffusione. I pazienti si sono mostrati ben disposti ad utilizzare componenti di questo tipo proprio perchè impattano sulla loro sicurezza e riducono ulteriormente il già basso errore dovuto all'erronea identificazione.
Impatto sull'organizzazione aziendale	L'organizzazione ha beneficiato di una maggiore efficienza su l'uso delle strutture chirurgiche e ha garantito ulteriormente i medici sull'identificazione del paziente
Percorso di Attuazione Studio di fattibilità Prototipo Pilota	 No No Si - Il sistema è attualmente in esercizio ed ha concluso la fase pilota.
Tempi di Implementazione	3 mesi
Costi	Non disponibile
Benefici	L'introduzione dei nuovi sistemi basati su tecnologia RFId volti a supportare le interazioni tra paziente ed ente ospedaliero ha contribuito in maniera significativa anche a valorizzare e responsabilizzare sempre di più le risorse interne. L'introduzione dei nuovi sistemi, inoltre, non ha comportato alcun problema, né in termini di difficoltà operative né d'accettazione da parte degli operatori coinvolti, che hanno recepito positivamente i nuovi strumenti, grazie anche alla loro semplicità d'uso. La tecnologia RFId si è quindi rivelata vincente per diminuire i margini di errore e le casistiche di mal practice all'interno dei reparti in cui è stata introdotta; inoltre sono allo studio ulteriori estensioni della stessa.
Eventuali criticità emerse	Non Applicabile

Tabella 27 - Scheda di progetto per la gestione del blocco operatorio

Campo Applicativo	OSPEDALI - LOCALIZZAZIONE PAZIENTI
Nome del Progetto	DOVE
Referente del Progetto	
Caratteristiche Tecniche Frequenze Utilizzate Tipologie di tag (attivi, passivi, semipassivi) Distanza massima lettore/tag	 868 Mhz Tag attivi 6 m

Dimensioni del Progetto Numero di utenti attuali e previsti Numero di sedi ed unità organizzative coinvolte	 circa 100 pazienti - 10 clients attivi 1
Impatto sociale ed organizzativo Impatto sulla privacy Impatto sull'organizzazione aziendale	
Percorso di Attuazione Studio di fattibilità Prototipo Pilota	 Si Si Si
Tempi di Implementazione	circa 10 mesi
Costi	
Benefici	
Eventuali criticità emerse	

Tabella 28 - Scheda di progetto per la localizzazione pazienti

SCHEDE RELATIVE AD APPLICAZIONI GESTIONALI

Di seguito viene riportata la scheda progetto realizzata per la gestione dei cespiti.

Campo Applicativo	RISOLUZIONE PROBLEMA CESPITI
Nome del Progetto	TC EASY ASSET MANAGEMENT
Referente del Progetto	
Caratteristiche Tecniche Frequenze Utilizzate Tipologie di tag (attivi, passivi, semipassivi) Distanza massima lettore/tag	 HF 13.56 MHz Tag passivi: adesivi cartacei e "on metal" circa 30 cm
Dimensioni del Progetto Numero di utenti attuali e previsti Numero di sedi ed unità organizzative coinvolte	 circa 100 utenti 2 sedi coinvolte
Impatto sociale ed organizzativo Impatto sulla privacy Impatto sull'organizzazione aziendale	 No Si
Percorso di Attuazione Studio di fattibilità Prototipo Pilota	 Si Si No
Tempi di Implementazione	1mese
Costi	€ 30.000,00

Benefici	ogni oggetto ha la sua storia all'interno di un'etichetta
Eventuali criticità emerse	a seconda del materiale dell'oggetto da inventariare sono stati utilizzati i tag più adatti

Tabella 29 - Scheda di progetto per la gestione dei cespiti

SCHEDE RELATIVE AD APPLICAZIONI VEICOLARI

Di seguito viene riportata la scheda progetto realizzata per la gestione dei parcheggi ad elevata problematica di sicurezza.

Campo Applicativo	SISTEMA DI GESTIONE DI PARCHEGGI VEICOLARI CON ELEVATA PROBLEMATICA DI SICUREZZA COSTITUITO DA SISTEMI INTEGRATI PER IL CONTROLLO E LA TRACCIATURA DEGLI ACCESSI ALL'INTERNO DI UNA STRUTTURA (RFId per identificazione conducente associato a lettura targhe del mezzo)
Nome del Progetto	Gestione parcheggi
Referente del Progetto	
Caratteristiche Tecniche Frequenze Utilizzate Tipologie di tag (attivi, passivi, semipassivi) Distanza massima lettore/tag	 13,56 MHz read/write tecnology, con possibilità fino a 127 applicazioni sulla tessera, compresa la crittografia dei dati e nella memorizzazione La carta contiene un RFId passivo 40 cm
Dimensioni del Progetto Numero di utenti attuali e previsti Numero di sedi ed unità organizzative coinvolte	 Parcheggi di capienza superiore a 500 posti auto 2
Impatto sociale ed organizzativo Impatto sulla privacy Impatto sull'organizzazione aziendale	 medio basso (per effetto della gestione dei picchi di flusso veicolare)
Percorso di Attuazione Studio di fattibilità Prototipo Pilota	 No No No
Tempi di Implementazione	3 Mesi
Costi	
Benefici	- Maggiore sicurezza, - Sveltimento delle procedure - Minori costi di esercizio
Eventuali criticità emerse	

Tabella 30 - Scheda di progetto per la gestione dei parcheggi

SCHEDE AD APPLICAZIONI E ESPERIENZE ESTERE

Le ultime due schede sono relative alle esperienze fatte, presso l'ospedale universitario di Jena e presso una azienda farmaceutica. Il primo è relativo alla gestione ospedaliera, la seconda alla tracciabilità dei farmaci prodotti.

Campo Applicativo	SANITÀ
Nome del Progetto	TRACCIABILITÀ RFId
Referente del Progetto	JENA UNIVERSITY HOSPITAL (Germania)
Caratteristiche Tecniche Frequenze Utilizzate Tipologie di tag (attivi, passivi, semipassivi) Distanza massima lettore/tag	Tag passivi
Dimensioni del Progetto	L'Ospedale universitario di Jena è una struttura articolata, localizzata nello Stato federale della Turingia (Germania) e che raccoglie sotto di sè diverse strutture sparse sul territorio federale per un totale di circa 1.400 posti letto. Attualmente la struttura occupa circa 4.000 dipendenti ed eroga circa 250.000 trattamenti ogni anno.
Numero di utenti attuali e previsti Numero di sedi ed unità organizzative coinvolte	Il progetto nasce con l'obiettivo principale di introdurre una nuova metodologia di gestione delle informazioni per aumentare l'efficienza dei processi ospedalieri. Oggi l'Ospedale di Jena è diventato un punto di riferimento nell'ambito dell' applicazione di scenari innovativi alla sanità grazie all'utilizzo di applicazioni integrate accessibili tramite palmari e soprattutto grazie all'introduzione della tecnologia RFId. Il progetto è stato avviato a partire dall'unità di chirurgia di pronto soccorso, in cui è stata attività da ottobre del 2002 una stazione di lavoro. Il progetto pilota ha coinvolto inizialmente una team composto da 25 infermiere. In questa fase sono state testate le procedure per allineare i sistemi sin dal momento dell'accettazione del paziente con l'inserimento dei servizi resi, delle diagnosi e con la rilevazione dei medicinali utilizzati su un braccialetto identificativo del paziente con TAG RFId.
Num. di sedi ed unità organizzative coinvolte	Prima dell'introduzione della soluzione era necessario compilare circa 12 schede con i dati necessari alla gestione del paziente. Con la nuova soluzione la maggior parte delle informazioni possono direttamente essere inserite nel sistema gestionale in tempo reale al letto del paziente.

Impatto sulla privacy Impatto sull'organizzazione aziendale	I dati che riguardano l'episodio di cura sono inseriti nella cartella clinica elettronica, basata sulla soluzione ERP per la gestione Ospedaliera. Il percorso di cura del paziente viene gestito dal sistema che raccoglie i dettagli dei trattamenti e dei medicinali somministrati.
Percorso di Attuazione Studio di fattibilità Prototipo Pilota	 No Si - Scenario prototipale iniziale limitato ad una unità di chirurgia di urgenza No
Tempi di Implementazione	
Costi	- Investimento iniziale nel progetto e nella sperimentazione ; - Costi relativi al nuovo disegno organizzativo; - Gestione del cambiamento organizzativo e gestionale ; - Costi di Formazione ;
Benefici	- Aggiornamento informazione del paziente sul punto di cura. - Maggior qualità di dati per statistiche, analisi e gestione dei magazzini di medicinali. - Ottimizzazione costi di gestione dei magazzini e delle farmacie. - Maggiori info per la gestione delle fatturazioni per i gruppi diagnosi-relativi (DRGs). - Aggiornamento in tempo reale. - Minore possibilità di errore nella somministrazione di medicinali. - Sicurezza di gestione dei dati personali e di cura nei confronti del paziente.
Eventuali criticità emerse	

Tabella 31 - Scheda di progetto Jena University Hospital

Campo Applicativo	SANITÀ
Nome del Progetto	TRACCIABILITÀ FARMACO
Referente del Progetto	
Caratteristiche Tecniche Frequenze Utilizzate Tipologie di tag (attivi, passivi, semipassivi) Distanza massima lettore/tag	 900 MHz 1in x 1in 915 MHz Class 0 tags circa 30 cm
Dimensioni del Progetto Numero di utenti attuali e previsti Num. di sedi ed unità organizzative coinvolte	 100 fornitori 1
Impatto sociale ed organizzativo Impatto sulla privacy Impatto sull'organizzazione aziendale	 No Si

Percorso di Attuazione Studio di fattibilità Prototipo Pilota	 No No Si
Tempi di Implementazione	
Costi	- Investimento per progetto Cambiamenti organizzativi e reengineering dei processi
Benefici	- Riduzione ed eliminazione di casi di furto, contraffazioni, irregolarità nel processo di produzione e consegna. - Normativa: rispetto della normativa e delle direttive (FDA e DEA)
Eventuali criticità emerse	

Tabella 32 - Scheda di progetto della Purdue Pharma

A.2 ESEMPI DI APPLICAZIONI IN AMBITO INTERNAZIONALE

IL SETTORE DELL'ABBIGLIAMENTO

Negli USA le tecniche RFId sono particolarmente diffuse nel settore dell'abbigliamento, in particolare per ciò che concerne:

- automazione del ricevimento della merce: si riduce, e qualche volta si evita, il tempo di raccolta e immagazzinamento, con incremento delle vendite dei pezzi;
- allarme di sotto scorta: è garantito il rifornimento anche in spazi di vendita limitati, con riduzione dei costi di esposizione;
- inventario automatico: è possibile contare i pezzi in tempo reale e affinare le politiche di rifornimento dei punti vendita, anche di quelli in affiliazione, rendendo più appetibile il franchising;
- lettura diretta al POS: si semplifica il "conto" al cliente, con riduzione del personale necessario e dei tempi di attesa;
- antitaccheggio e riduzione dei ritorni per addebito errato.

NATIONAL GALLERY DI LONDRA

La Galleria Nazionale di Londra ha ridotto drasticamente i costi di sorveglianza con un investimento assai ridotto. Ogni opera esposta è stata dotata di un tag RFId attivo che incorpora un sensore di vibrazione e di shock. I tag trasmettono ogni 15 secondi permettendo di ridurre le persone addette alla sorveglianza.

CONTROLLO DELLE TRASFUSIONI DI SANGUE

Dalle statistiche emerge che l'8,6% delle schede identificative dei pazienti negli ospedali sono sbagliate e il 5,7% sono illeggibili. Durante le trasfusioni necessarie nelle sale operatorie è fondamentale controllare la compatibilità del sangue con il paziente.
Nel Massachusset General Hospital è in corso una sperimentazione che usa un lettore di tag RFId inglobato nel tavolo operatorio. Il paziente è a sua volta dotato di un braccialetto RFId e così è possibile controllare la compatibilità in modo immediato e accurato.

Appendice 5 - Glossario

A

AIDC
Automatic Identification and Data Capture – *Identificazione automatica e raccolta dati*.
Con AIDC si fa riferimento a tutte le tecnologie adottate per l'identificazione automatica e la raccolta (automatica) dei dati. Codici a barre, RFId, biometria alcune delle tecnologie considerate nell'AIDC.

Air Interface Protocol
Protocollo Interfaccia a Radiofrequenza.
Parametri e regole (frequenza, modulazione, codifica dei dati, ecc.) che governano il colloquio tra tag e lettore nell'ambito della radiofrequenza.

Antenna
L'antenna svolge, alternativamente, due funzioni: • trasmettere ovvero trasformare un segnale elettrico di frequenza opportuna in un campo elettromagnetico in grado di propagarsi nello spazio circostante, • ricevere ovvero trasformare il campo elettromagnetico da cui sono investite in un segnale elettrico da inviare al ricevitore per la relativa elaborazione. Dimensione e forma delle antenne sono strettamente collegate alle frequenze a cui devono operare, alla direzionalità che si vuole ottenere.

Anticollisione
Sono diverse tecniche che consentono ad un lettore di individuare e colloquiare singolarmente (singulation) con ognuno dei tag che si presenta contemporaneamente ad altri nel suo raggio di azione.

Attivi (tag)
Sono definiti attivi i tag che contengono una propria sorgente di energia (batterie, accumulatori,...) che consente una autonomia trasmissiva.

B

Backscatter
È il metodo più usato dai tag passivi per comunicare con il lettore, consiste nel cortocircuitare l'antenna del tag secondo cadenze e sequenze definite dal protocollo di comunicazione

Barcode
Codice a barre caratterizzato da un insieme di 1
Uno tra i metodi oggi più diffuso per l'identificazione automatica degli oggetti. Adottato a partire dall'inizio degli anni 70 per la semplicità di realizzazione dei sistemi ottici di lettura delle barre (rispetto ad altre simbologie) è caratterizzato oggi da una molteplicità di standard, per settori merceologici, applicativi e settoriali, adottati a livello globale. Il più grosso inconveniente del Barcode è la necessita del contatto ottico con il lettore.

C

C1G1 - C1G2
Per esteso significano Class1Generation1 e Class1Generation2. Sono sigle che identificano le due versioni successive degli standard pubblicati dal gruppo di lavoro EPCGlobal. Le specifiche della Generation1 comprendono Tag funzionanti sia in HF che UHF. Descrivono Tag WORM privi di zone di memoria su cui sia possibile scrivere dati. I tag di questo tipo stanno andando rapidamente in disuso a favore della Generation2. Le specifiche Generation2 sono rivolte invece a Tag in banda UHF con caratteristiche analoghe a ISO/IEC 18000/6.

Capacità (di memoria)
Espressa normalmente in numero di bit (o di Byte) rappresenta la quantità di informazione che il tag può supportare. Può rappresentare sia

il numero di bit netti disponibili all'utilizzatore che quelli totali, compresi quelli riservati dal produttore, per esempio, per la parità o per l'*ECC*.

Chip
Termine con cui si definisce la parte attiva del tag. Ad oggi, nella stragrande maggioranza dei casi, è realizzato con la tecnologia dei semiconduttori, tecnologia con cui vengono realizzati i circuiti integrati usati in molte apparecchiature elettroniche.

Chipless
'Senza Chip'.
Tag speciali senza chip dedicati tipicamente all'*EAS*.

CMOS
Complementary Metal Oxide Semiconductor
Tecnologia per la realizzazione di chip caratterizzata dalla dissipazione statica di potenza idealmente nulla grazie alle piccole dimensioni.

Contactless
'Senza Contatto'
Termine spesso riferito alle 'Smart Card' in cui il colloquio tra lettore e card avviene per mezzo delle onde radio e quindi senza contatto. Richiede comunque che lettore e 'card' siano in prossimità l'uno all'altro. Vedi anche Wireless.

CRC
Cyclic Redundancy Check. Indica un algoritmo matematico che, eseguito su alcuni Byte campionati in determinati punti del flusso informativo, genera un hash di controllo che consente di verificare la correttezza della trasmissione.

D

Database
Basi di Dati.
Insieme di dati strutturati in modo da rendere la ricerca delle informazioni efficiente e veloce.

E

EAN
European Article Number(ing)
Standard di codifica per codici a barre utilizzato nel mondo della grande distribuzione per articoli di consumo (e non). L'EAN 13 e l'EAN 8 sono due versioni rispettivamente con 8 e 13 caratteri.

EAS
Electronic Article Surveillance – *Sorveglianza elettronica degli oggetti*.
Sistema antitaccheggio che fa uso di tag tipicamente chipless (senza chip) costituiti nella maggior parte dei casi da una piccola striscia di materiale che può assumere solamente due stati: Attivo/Disattivo.

ECC
Error Correcting Code – *Codice di correzione d'errore*.
Sequenza di bit aggiunta in coda alla trasmissione dei dati calcolata, partendo dai dati stessi, con particolari algoritmi polinomiali che consentono al ricevitore di rilevare, usando lo stesso algoritmo, se durante la trasmissione si sono avuti errori ed eventualmente correggerli.

EDI
Electronic Data Interchange - *Scambio Elettronico di Dati*.
Scambio di dati strutturati tra sistemi informatici per via elettronica e con interventi manuali limitati. Si basa su messaggi standard concordati tra le parti o codificati da standard nazionali, internazionali o di settore.

EEPROM
Electrically Erasable Programmable Read Only Memory
Tecnologia con cui viene realizzato un tipo di memoria per i chip usati nei tag R/W caratterizzata da: ü possibilità di cancellare i dati per riscriverli, ü mantenimento dell'informazione anche in assenza di alimentazione.

EIRP
Effective Isotropic Radiated Power.
Rappresenta la potenza di uscita dall'antenna di un lettore RFId secondo lo standard Americano. E' normalmente espressa in Watt (W). E' la potenza che dovrebbe essere emessa da una antenna isotropica (antenna ideale che distribuisce la potenza in modo uniforme in tutte le direzioni) per produrre la densità di potenza di picco osservabile nella direzione di massimo guadagno dell'antenna reale.

EPC
Electronic Product Code - *Codice elettronico di prodotto.*
Un 'codice a barre' elettronico che identifica il produttore, il prodotto, la versione ed il numero di serie di ogni singolo oggetto. Descritto nel documento "EPC Tag Data Specification Version 1.1 Rev. 1.27", pubblicato nel Maggio 2005. L'identificatore EPC è infatti uno schema di metacodifica progettato per supportare le necessità di diversi settori industriali sia incorporando schemi già esistenti che definendo, se necessario, nuove codifiche.

ERP
Effective Radiated Power. Potenza irradiale efficace
Rappresenta la potenza di uscita dall'antenna di un lettore RFId secondo lo standard Europeo. È normalmente espresso in Watt (W). $1W_{ERP} \cong 1{,}64W_{EIRP}$.

F

Frequenza
In un segnale periodico (e ripetitivo) rappresenta il numero di ripetizioni di una completa forma d'onda nel tempo di un secondo. Si misura in cicli al secondo ovvero Hertz (Hz).

Frequenza portante
Nei segnali a modulazione di ampiezza rappresenta la frequenza del segnale. Più in generale rappresenta la frequenza centrale della banda occupata dal segnale a radiofrequenza.

H

HF
High Frequency – *Alta Frequenza.*
Il termine HF individua l'area 3–30 MHz. All'RFId è assegnata su base mondiale la frequenza di 13,56 MHz

I

I-Code 1
I- Code SLI I e II
Inlay
Un microchip RFId collegato alla sua antenna e montato su un substrato. Sono sostanzialmente delle etichette non ancora finite e vengono solitamente fornite a produttori che le convertono poi in etichette RFId.

Inlet
vedi 'inlay'

ISM
Industrial, Scientific, Medical – *Industriale, scientifico, medico.*
Si individuano con questa sigla alcune bande dello spettro RF che sono di libero accesso (senza necessità di licenze), rispettando alcune limitazioni sul segnale emesso (p.e. la potenza).

L

Lettore
Il dispositivo elettronico che colloquia con il tag, ne legge le informazioni contenute e, eventualmente, le modifica. In varie configurazioni, per esempio le unità portatili, lettore ed antenna formano un tutt'uno; in altri casi sono separati dall'antenna a cui vengono collegati con cavi adatti alla RF. Si collegano al resto del sistema tipicamente con collegamenti seriali o di rete.
Sinonimi: interrogator, reader, controller.

LF
Low Frequency – *Bassa Frequenza.*
Il termine LF individua l'area 30–300 kHz. Per l'RFId le frequenze tra 120 e145 KHz. In realtà le frequenze operative più utilizzate sono due: 125,5 kHz e 134,2 kHz.

M

Middleware (M/W)
Nel contesto dei sistemi RFId fa riferimento al software che viene utilizzato per filtrare i dati forniti dai lettori e passare al sistema centrale solamente le informazioni utili e necessarie per le successive elaborazioni.

Mifare
Modulazione
Il metodo con cui viene alterata la frequenza della portante al fine di codificare le informazioni ed i comandi da trasmettere al tag. I metodi usati sono diversi e comprendono principalmen-

te: AM (modulazione di ampiezza), FM (modulazione di frequenza). In alcuni casi vengono usate tecniche di modulazione diverse in ogni direzione (da/verso il tag).

Modulazione di Ampiezza
Tecnica di modulazione in cui viene variata l'ampiezza del segnale trasmesso. Nella trasmissione digitale, dove si hanno due soli livelli dell'ampiezza, si parla di ASK (Amplitude Shift Keyng).

Modulazione di Frequenza
Tecnica di modulazione in cui viene variata la frequenza del segnale trasmesso. L'FSK (Frequency Shift Keying) ne è un caso particolare.

O

Open System
Sistema aperto, vedi.

P

Passivi (tag)
Sono definiti passivi i tag che non contengono alcuna sorgente di energia e che, per poter operare, acquisiscono l'energia necessaria dal campo a radio frequenza del lettore.

Protocollo
Insieme di regole che determinano il comportamento di unità funzionali per ottenere una comunicazione [ISO/IEC 2382-9]. Collettivamente, le specifiche del livello fisico (p.e. frequenza, modulazione, ecc.) e del primo livello di identificazione del tag.

R

R/O
Read/Only – *Sola Lettura.*
Vengono definiti R/O quei tag il cui contenuto viene stabilito al momento della produzione del chip che li compone e rimane quindi immodificabile. Il chip contiene un codice identificativo univoco (UID)

R/W
Read/Write – *Lettura/Scrittura.*
Vengono indicati come R/W i tag i cui contenuti possono essere sia letti che modificati (scritti) attraverso un lettore.

Reader
vedi 'Lettore'

RFId
Radio Frequency Identification – *Identificazione a Radio Frequenza.*

S

Sistema aperto
Open System
Viene definito aperto un sistema in grado di scambiare alcuni dei suoi componenti con altri sistemi equipollenti mantenendo inalterata la sua funzionalità. Si contrappongono ai 'sistemi chiusi' che non accettano al loro interno componenti estranei.

Smart Card
'Carta Intelligente'
Si compone di un supporto plastico, di dimensioni e fattura identiche o simili a quelle delle carte di credito (formato ISO), in cui la banda magnetica è sostituita da un chip che può contenere, insieme alla capacità di memorizzare dati, anche capacità di elaborazione (microprocessore).

Supply Chain
Filiera di Fornitura
Una supply chain (o rete logistica) è un sistema coordinato di organizzazioni, attività, flusso di informazioni e risorse coinvolte nel trasferire un servizio o un prodotto da un produttore/fornitore al cliente finale. Le entità di una supply chain sono tipicamente produttori, fornitori di servizi (p.e. operatori della logistica), distributori, canali di vendita e, alla fine, il cliente finale.

T

Tag
letteralmente *'cartellino', 'etichetta'*
È ormai entrato nell'uso comune per indicare un'etichetta RFId.
Dispositivo elettronico composto da un microchip e un'antenna. Può essere dotato, nel caso di tag attivi, di una batteria.

Sinonimi: Smart-tag, etichetta intelligente, electronic label, etichetta elettronica, transponder.

Tag-It
Altro termine per definire i tag

U

UCC
Uniform Code Council.
Organizzazione nonprofit che controlla e definisce gli standard dei codici a barre nel nord-America.

UHF
Ultra High Frequency – *Frequenza Ultra Alta*.
Il termine UHF individua l'area 300–3000 MHz (3GHz). Per motivi diversi di sovrapposizione con altri servizi le frequenze assegnate all'RFId sono diverse a seconda dell'area geografica:
- Europa: 865-868 MHz,
- Americhe: 915-930 MHz,
- Asia-Pacifico: 930-960 MHz

UID
Unique IDentity – *Identità univoca*.
Codice identificativo univoco presente in ogni chip utilizzato per la realizzazione di tag RFId. Viene inserito dal produttore del chip al momento della sua fabbricazione ed è immodificabile.

UPC
Unique Product Code
Lo standard per codici a barre usato in Nord America e gestito dall'UCC.

W

Wireless
'Senza Fili'
Fa riferimento a collegamenti che avvengono per mezzo delle onde radio ma su distanze più significative di quanto viene definito 'contactless'.

WORM
Write Once Read Many – *Scrivere una volta Leggere molte (volte)*.
Vengono definiti WORM quei tag il cui contenuto può essere modificato una volta (in realtà alcune volte) per poi divenire immodificabili (ovvero R/O).

X

XML
eXtensible Markup Language.
Linguaggio ampiamente adottato per la condivisione di informazioni attraverso Internet indipendentemente dal sistema operativo usato dai sistemi (computer) collegati.

XQL
XML Query Language
Un metodo di ricerca all'interno di basi di dati dati (database) basaTo sul linguaggio XML. XQL può essere usato per il recupero dei dati da file generati con il Physical Markup Language creato dall'Auto-ID Center.

CNIPA
Centro Nazionale per l'Informatica
nella Pubblica Amministrazione

via Isonzo, 21/b - 00198 Roma
tel. 06 85264.1
www.cnipa.gov.it