Consiglio Nazionale delle Ricerche

Istituto di Calcolo e Reti ad Alte Prestazioni

INTEGRAZIONE DI TECNOLOGIE RFID E FOTOSENSORI PER IL MONITORAGGIO DI UTENTI MOBILI IN AMBIENTI PERVASIVI

Gennaro Della Vecchia – Massimo Esposito – Raffaele Zuccaro

RT-ICAR-NA-02-09 aprile 2009

Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR)
Sede di Napoli, Via P. Castellino,111, 80131 Napoli, URL: *www.na.icar.cnr.it*

Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni

INTEGRAZIONE DI TECNOLOGIE RFID E FOTOSENSORI PER IL MONITORAGGIO DI UTENTI MOBILI IN AMBIENTI PERVASIVI

Gennaro Della Vecchia[1] – Massimo Esposito[1] – Raffaele Zuccaro[1]

Rapporto Tecnico N.:
RT-ICAR-NA-02-09

Data:
aprile 2009

---

[1] Istituto di Calcolo e Reti ad Alte Prestazioni ICAR-CNR, Sede di Napoli, Via P. Castellino,111, 80131 Napoli, URL: *www.na.icar.cnr.it*

Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR)
Sede di Napoli, Via P. Castellino 111, 80131 Napoli, URL: *www.na.icar.cnr.it*

INTEGRAZIONE DI TECNOLOGIE RFID E FOTOSENSORI PER IL MONITORAGGIO DI UTENTI MOBILI IN AMBIENTI PERVASIVI

Gennaro Della Vecchia, Massimo Esposito, Raffaele Zuccaro

ABSTRACT

In un ambiente di Pervasive Computing ruolo fondamentale assumono posizione e identificazione univoca di dispositivi o utenti mobili in ambienti noti. La capacità di acquisire tali informazioni di contesto in maniera automatica, non invasiva e trasparente all'utente, costituisce quindi un requisito imprescindibile nella realizzazione di applicazioni in cui le interazioni uomo/macchina evolvano secondo il paradigma della pervasività. In quest'ottica, nel presente lavoro viene proposta una infrastruttura per il monitoraggio automatico degli accessi in ambienti circoscritti mediante localizzazione e identificazione di utenti mobili. Seguendo una metodologia imperniata su un'innovativa tecnica di integrazione di tecnologie di posizionamento wireless, si è progettato un sistema che utilizza rilevatori RFID e sensori fotoelettrici per inferire informazioni di contesto relative agli ambienti monitorati. Un prototipo sperimentale implementato per valutare il comportamento del sistema ha dimostrato la validità delle scelte effettuate e l'effettiva fattibilità di impiego in uno scenario di applicazione reale.

Keywords: Pervasive Computing, RFID, sensori fotoelettrici, localizzazione, identificazione

1. INTRODUZIONE

Negli ultimi anni, grazie ai continui progressi tecnologici, si è assistito ad un proliferarsi di dispositivi di calcolo di dimensioni sempre più piccole e a basso costo che, accoppiato con i progressi delle tecnologie di comunicazione, ha portato all'approccio "Pervasive Computing". Questo nuovo paradigma si basa su ambienti dotati di proprietà computazionali e comunicative che contengono un gran numero di componenti hardware e software, autonomi ed eterogenei, che necessitano di cooperare tra loro e che tendono ad essere altamente dinamici. Di conseguenza si è spianata la strada per nuovi scenari applicativi che stanno sempre più concretizzandosi e integrandosi nella realtà quotidiana.
Scopo del presente lavoro è lo sviluppo di un sistema che permetta la localizzazione e l'identificazione di utenti mobili all'interno di un ambiente pervasivo. Entrambe le funzionalità di localizzazione e identificazione saranno implementate in maniera automatica e trasparente, senza intervento diretto dell'utente, secondo i canoni del Pervasive Computing.
L'obiettivo finale è quello di monitorare il flusso di utenti mobili relativo ad uno specifico ambiente target, segnalando ingressi e uscite, e tenendo traccia delle persone attualmente presenti. Il sistema si basa sull'integrazione di tecnologia RFID e fotosensori, tecnologie poco invasive, funzionanti a distanza e capaci di recepire variazioni nel contesto dell'ambiente di lavoro. Inoltre, il sistema sarà

in grado di riconoscere e segnalare eventuali anomalie quali ad esempio accessi non autorizzati o la presenza di ostacoli nei varchi di accesso.
Tale integrazione consente di minimizzare la probabilità di errore (gli ingressi e le uscite sono registrati e identificati attraverso i sensori posti sul varco di accesso, mentre l'impiego della tecnologia RFID consente l'identificazione univoca delle persone presenti) e di lavorare in tempo reale (la localizzazione e l'identificazione delle persone presenti sono fatte contestualmente all'ingresso/uscita dall'ambiente di lavoro, senza ritardi), utilizzando soluzioni tecnologiche a basso costo.
Il presente rapporto tecnico è strutturato come segue. Il Capitolo 2 presenta una panoramica sulle tecnologie RFID, analizzandone i componenti fondamentali e il loro funzionamento. Il Capitolo 3 descrive sinteticamente le principali tecnologie di sensori di posizionamento e movimento. Nel Capitolo 4 vengono brevemente illustrate metodologie e tecniche impiegate nei sistemi di identificazione e localizzazione più diffusi. Il Capitolo 5 descrive le fasi della progettazione del sistema e l'implementazione del prototipo sperimentale. Infine, le Conclusioni e la sezione dedicata alla Bibliografia terminano il lavoro.

2. TECNOLOGIA RFID

Quella nota come RFID è una tecnologia wireless che rappresenta una soluzione innovativa nel campo dell'automazione dei processi. Sebbene la sua origine non sia recente, essa è ancora considerata una tecnologia in piena evoluzione, anche se ormai è abbastanza consolidata nelle sue applicazioni tipicamente orientate a problemi di logistica, tanto che nei prossimi anni è destinata a provocare una vera e propria rivoluzione in ogni settore produttivo.
La definizione stessa dell'acronimo, *"Radio Frequency IDentification"* (Identificazione mediante Radiofrequenza), è molto chiara nel precisare e delimitare la tecnologia impiegata: essa permette l'identificazione (ossia il riconoscimento univoco) di un oggetto mobile mediante l'impiego di onde elettromagnetiche a radiofrequenza.
Il processo di identificazione di un qualunque tipo di oggetto, sia esso un prodotto, un animale o una persona, avviene attraverso l'interazione con apposite etichette "intelligenti" (dette *Tag* o *Transponder*) senza alcuna necessità di collegamento fisico, ossia a distanza. Tali transponder, a differenza della tecnologia dei precedenti codici a barre, possono avere anche la capacità di memorizzare informazioni suscettibili di essere trasmesse tramite onde radio ad opportuni dispositivi di lettura (detti *Reader* o *Interrogator*). Nel corso del presente lavoro, i termini "tag" e "transponder" sono considerati sinonimi.
Attualmente, possiamo considerare come componenti principali di un sistema RFID (Figura 1):

a) i tag, di tipo, dimensioni e caratteristiche variabili
b) una o più antenne ricetrasmittenti, di potenza e dimensioni variabili
c) uno o più dispositivi per l'interazione con i tag (reader).

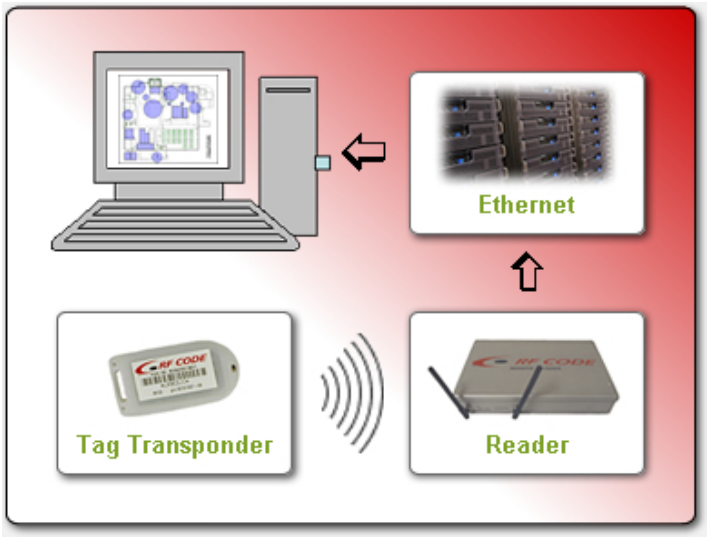

Figura 1 - Schema di un tipico sistema RFID

2.1 Tag RFID

I tag sono i data-carrier device che immagazzinano i dati e che vanno posti sugli oggetti o prodotti da identificare; vengono letti dal reader con una comunicazione di tipo wireless. Sono contrassegnati da un numero di identificazione (*UID* o *ID*), memorizzato dal costruttore in una ROM e non manipolabile; sono inoltre in grado di immagazzinare nella memoria interna un certo numero di informazioni specifiche dell'applicazione e di comunicarle al lettore. L'UID può essere incluso in comandi diretti ad uno specifico tag e rappresenta pertanto un mezzo per condurre una comunicazione separata ed unica con quel tag, anche in presenza di multipli data-carrier device.
I tag costituiscono il supporto fisico alle informazioni, e il loro layout risulta fortemente influenzato dal tipo di utilizzo e dalle prestazioni che si desiderano ottenere, generando così una molteplicità di configurazioni possibili che, pur basandosi sulla medesima tecnologia, risultano visivamente tutte differenti (etichette, carte, supporti rigidi, etc.). La maggior parte dei tag è incapsulata per assicurarne la resistenza agli urti, agli agenti chimici, all'umidità e allo sporco.
In base al tipo di alimentazione, si hanno:

- *Tag passivi*. Sono dotati solo di un chip e un'antenna, non richiedono alcuna sorgente di alimentazione interna (si dice infatti che sono dotati di alimentazione "on board"): il tag viene alimentato dalla potenza estratta dalle onde elettromagnetiche in radiofrequenza emesse dalle antenne. Quando un tag passivo non è all'interno del range di azione del reader, è totalmente spento, ed è attivato solamente nel momento in cui si porta nella zona di interrogazione. La potenza richiesta per tutte le operazioni interne, così come i dati, sono forniti al tag tramite l'antenna. La parte intelligente di ogni tag passivo è costituita da un solo circuito di trasmissione del segnale e da una memoria non volatile contenente un codice unico, il quale viene trasmesso al lettore, oppure da un completo microprocessore, capace di elaborare in proprio i segnali provenienti dai lettori e ritrasmettere in proprio i risultati così ottenuti. I tag passivi possono operare a bassa frequenza (LF, 125-135KHz), ad alta frequenza (HF, 13.56 MHz), oppure a frequenze molto alte (UHF, 868-915 MHz); le dimensioni possono essere anche molto piccole, anche dell'ordine dei centimetri. In genere il loro costo è di gran lunga inferiore rispetto a quello dei tag attivi.
- *Tag semi-passivi*. Sono dotati di una batteria che alimenta direttamente i circuiti interni del Tag durante la comunicazione, ma non è usata per generare onde radio (in altri termini il trasferimento di informazioni avviene estraendo la potenza emessa dal reader), allo scopo di migliorare le performance, soprattutto in termini di portata operativa. Vengono usati per applicazioni speciali come il telepass per auto od il monitoraggio di vagoni ferroviari; essi

trasmettono solo se interrogati dal reader e comunicano a distanze di decine di metri.

- *Tag attivi*. Contengono una sorgente di alimentazione propria, di solito una piccola batteria al litio, che, oltre che ad alimentare i circuiti di ricetrasmissione, può servire per tenere attiva una memoria RAM statica nella quale si memorizzano i dati. Il vantaggio di utilizzare un'alimentazione interna consiste nella possibilità di realizzare sistemi che lavorino con frequenze più elevate e che abbiano un raggio di azione maggiore. Tali tipi di tag attivi sono per esempio usati per l'identificazione automatica di oggetti in movimento, come autoveicoli in marcia, per i quali la distanza di rilevamento può essere abbastanza grande e variabile. Alcuni tag attivi lavorano con una frequenza del segnale nella banda dei 900 MHz, ma è previsto l'uso di frequenze anche più elevate, dell'ordine dei GHz: per esempio, negli Stati Uniti è stato proposto alla FCC, l'autorità che regola l'uso delle frequenze, di destinare la frequenza di 2,45 GHz ai tag RFID. In Europa vi sono altre proposte per definire l'uso delle frequenze intorno a 5,8 GHz.

2.2 Antenne

In un sistema RFID sono presenti due tipi di antenne, che svolgono due funzioni completamente differenti: le antenne presenti nei tag e le antenne collegate ai reader, queste ultime impiegate per sollecitare la risposta dei tag presenti nel loro raggio di azione. Ogni reader può governare simultaneamente una o più antenne.

Le antenne hanno tre parametri che ne identificano le caratteristiche:

- direttività, ovvero la capacità di concentrare le emissioni in radiofrequenza dell'antenna in uno spazio più o meno ristretto
- guadagno, il coefficiente prestazionale dell'antenna
- polarizzazione, che può essere di due tipi:
    - *polarizzazione lineare*: generano un campo monodimensionale e presentano solitamente un range di lettura superiore rispetto agli altri tipi di antenne, a condizione che il tag sia orientato in maniera ottimale, ma possono incontrare difficoltà nel trasmettere il segnale oltre alcuni ostacoli
    - *polarizzazione circolare*: generano un campo tridimensionale, sono meno soggette a problemi di lettura dovuti alla variabilità nell'orientamento del tag e risultano molto più flessibili anche nel superamento di ostacoli.

Inoltre, possiamo distinguere le antenne dei lettori RFID in mobili e fisse, a seconda se sia l'antenna (tipicamente integrata in un reader tipo palmare o a pistola) a muoversi verso il tag da identificare, o, viceversa, sia l'oggetto a spostarsi nel range di lettura dell'antenna.

2.3 Reader

In un sistema RFID i reader sono gli elementi che interagiscono sia con i tag, leggendo ed eventualmente modificando le informazioni ivi presenti, che con il sistema di gestione, tipicamente un host connesso in LAN o WLAN.

Un reader è essenzialmente composto da:

- interfaccia di connessione e comunicazione
- meccanismo di alimentazione
- sistema di generazione del campo RF
- sistema di comunicazione mediante RF.

3. SENSORI DI POSIZIONAMENTO E MOVIMENTO

I sensori di posizione e movimento, come dice il nome stesso, servono a rilevare la posizione e il movimento di un oggetto nel loro raggio d'azione, eventualmente rilevando anche velocità e verso di percorrenza. Amplissima è la gamma delle possibilità offerte dalla tecnologia corrente, ma per gli scopi del presente lavoro considereremo solo i sensori fotoelettrici.

3.1 Sensori Fotoelettrici

Le fotocellule, o sensori fotoelettrici, sono dispositivi elettronici che utilizzano il principio dell'emissione luminosa. Sono sicuramente tra i più versatili, costituendo una famiglia di sensori impiegata nei più svariati settori dell'automazione industriale: rivelazione e conteggio di oggetti, lettura di contrasti, misure, rilevazione della presenza di materiali non conduttori come legno, plastica, vetro, etc. e di metalli ferrosi e non ferrosi.
In generale un sensore fotoelettrico, consiste di una sorgente luminosa (o emettitore), un ricevitore, un amplificatore/demodulatore e uno stadio di uscita. Quando il fascio luminoso generato dai fotoelementi viene interrotto, lo stadio di uscita della fotocellula cambia il proprio stato logico.

Figura 2 - Fotocellula cilindrica con involucro metallico

Alcuni tipi di fotocellule, divise per tipo di funzionamento, sono:

- *Tipo proiettore/ricevitore (o sbarramento)*: in queste fotocellule, il proiettore e il ricevitore costituiscono due dispositivi separati, tipicamente montati l'uno davanti all'altro. Ogni oggetto tra i due dispositivi interrompe il raggio di luce e viene rilevato.
- *Tipo sbarramento a riflessione (o riflessione)*: questo tipo di fotocellule comprende dispositivi nei quali i fotoelementi di emissione e ricezione sono contenuti nello stesso corpo meccanico. Il fascio di luce emesso è riflesso da un riflettore prismatico (catarifrangente) che lo ritorna al ricevitore. Quando un oggetto attraversa il percorso del raggio di luce, esso viene rilevato. Funzionano con l'ausilio di riflettori prismatici e riflettori "scotch tape", che hanno la caratteristica di rinviare parallelamente la luce ricevuta, grazie alla loro particolare struttura a "nido d'ape".
  Questo tipo di sensore è molto diffuso, in quanto offre buone distanze operative con semplicità di allineamento sensore/riflettore e facilità d'installazione anche in spazi ristretti.

4. TECNICHE DI LOCALIZZAZIONE E IDENTIFICAZIONE

In un ambiente di Pervasive Computing assumono un ruolo fondamentale la posizione e l'identificazione univoca di un dispositivo o di un utente. In questo senso, tipicamente la maggior parte dei servizi in ambienti pervasivi si distinguono in "*location-aware*" e "*context-aware*". Con il termine "contesto" si fa riferimento un certo numero di fattori come identità di un utente, posizione fisica corrente, condizioni atmosferiche, ora del giorno, data, etc. Quindi, l'obiettivo dei "*context-aware services*" è quello di acquisire ed utilizzare informazioni riguardanti il contesto di un dispositivo al fine di fornire servizi appropriati per un determinato gruppo di persone, luogo, evento, etc.

4.1 Principi di localizzazione

Nel corso degli anni sono stati proposti molti sistemi di posizionamento progettati per rilevare la posizione di un oggetto mobile, determinandone quindi la *localizzazione* in un ambiente noto a priori. Essenzialmente due sono gli approcci seguiti:

- sistemi di localizzazione "Network-based", ove è l'infrastruttura che calcola e conosce la posizione del terminale mobile, comunicandola eventualmente a quest'ultimo
- sistemi di localizzazione "Handset-based", ove, viceversa, è il dispositivo mobile stesso che riesce a calcolare la propria posizione mediante le informazioni inviategli dai terminali componenti l'infrastruttura.

Un sistema di localizzazione prevede di determinare la posizione di un oggetto mediante la sua "prossimità", "vicinanza" rispetto a locazioni note. La presenza dell'oggetto deve essere percepita dal sistema mediante fenomeni fisici dalla portata limitata, quali ad esempio quelli utilizzati nella tecnologia RFID. In questo caso, la localizzazione avviene attraverso il monitoraggio dei punti di accesso all'ambiente, dove è prevista una infrastruttura composta da terminali ai quali l'oggetto si "connette" in base alla vicinanza. Se la connessione è individuata, allora si può stabilire in prima approssimazione la "zona" in cui si trova l'oggetto.

4.2 Identificazione

Per identificazione si intende la capacità di distinguere, senza possibilità d'errore, persone o oggetti simili tra loro sulla base di un elemento di distinzione univocamente determinabile. L'identità della persona o dell'oggetto, pertanto, può essere verificata mediante l'impiego di un apposito dispositivo manuale o automatico in grado di analizzare quel particolare univoco, che tipicamente è associato ad un codice di identificazione.
Le tecniche di identificazione automatica - in anglosassone *AIDC* (*Automatic Identification and Data Capture*) *technologies* – stanno rapidamente diventando quelle principalmente usate, e tra esse quelle che utilizzano l'identificazione automatica tramite RFID. L'oggetto da identificare è univocamente e solidalmente associato ad un tag: allorché il tag viene rilevato nel raggio d'azione di un reader, attraverso l'ID si risale immediatamente all'oggetto ad esso associato, identificandolo in maniera non ambigua.
Mediante RFID, quindi, è possibile determinare non soltanto l'identità di un oggetto o di una persona, ma anche la sua posizione nello spazio e nel tempo. Questa capacità di localizzazione ed identificazione rappresenta il punto di forza dei vantaggi offerti da questa tecnologia.

4.3 Controllo accessi e RFID

L'uso di sistemi RFID costituisce una valida alternativa sia alle tecnologie di personal identification tradizionali (badge, tesserini, etc.), sia alle tecnologie di *strong authentication* basate sul riconoscimento di *smart card* o degli attributi biometrici di un individuo. A differenza di tali tecnologie, l'RFID non richiede contatto visivo per l'identificazione e permette il riconoscimento anche a distanza ed in presenza di ostacoli.
L'identificazione tramite RFID oltre a rendere più agile l'impiego di varchi motorizzati, distinguere gli ingressi dalle uscite e verificare automaticamente l'elenco delle presenze all'interno di una determinata zona, permette ad esempio l'avvio e/o l'arresto automatici di un dispositivo a seconda che il legittimo utente si trovi o meno nelle vicinanze.

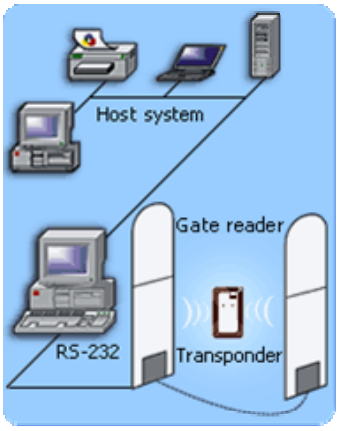

Figura 3 - Schema di un controllo accessi mediante RFID

I tag possono essere stampati o inseriti in oggetti di forma diversa, come ad esempio badge identificativi, braccialetti, etichette, ecc. e quindi, personalizzati con stampe di immagini, scritte, loghi, fotografie e codici a barre. Mediante la scrittura su tag, è possibile registrare diverse informazioni relative all'identità della persona o dell'oggetto *tagged*, come dati anagrafici, foto di riconoscimento, data e ora di transito, verso di transito e altre informazioni.

5. UN SISTEMA PER IL MONITORAGGIO DI OGGETTI MOBILI IN AMBIENTE PERVASIVO

In questo capitolo verranno descritte la progettazione e l'implementazione di un sistema che, mediante l'uso integrato delle tecnologie RFID e sensori viste in precedenza, permette la localizzazione e l'identificazione univoca di utenti in movimento all'interno di un ambiente pervasivo.
Si mostrerà dapprima il contesto nel quale va a collocarsi questa applicazione, passando successivamente alla descrizione dell'architettura e dei componenti hardware utilizzati, e concludendo con le varie fasi della progettazione dei componenti software impiegati. L'obiettivo finale è quello di conferire all'utilizzatore del sistema la capacità di monitorare il movimento di oggetti o persone in un ambiente noto, fornendo automaticamente ed in maniera sicura ed affidabile informazioni di localizzazione ed identificazione e consentendo il rilevamento di anomalie (accessi non autorizzati, presenza di ostacoli nei varchi, etc.).

5.1 Scenario applicativo

Consideriamo un ambiente circoscritto di lavoro, costituito da un varco, una coppia orientata di fotocellule, un reader e due antenne RFID. Il nostro obiettivo è quello di monitorare l'ambiente di lavoro, segnalando ingressi e uscite, e tenere traccia delle persone attualmente presenti.
L'assunto di base è che le persone autorizzate all'accesso siano munite di tag RFID indossabili,

tipicamente braccialetti, badge o similari, preventivamente registrati.
Un primo problema riguarda la necessità di identificare il "tipo" di persona che accede all'interno dell'ambiente. Nel caso di una persona autorizzata, ossia munita di tag registrato, il riconoscimento avviene attraverso il sistema RFID; nel caso in cui invece si è in presenza di accessi non autorizzati occorre prevedere opportuni meccanismi atti a rilevare tale circostanza. E' in quest'ottica, quindi, che si è pensato di integrare il sistema RFID con la tecnologia dei sensori fotoelettrici; saranno le fotocellule, infatti, posizionate opportunamente nel varco, a segnalare il passaggio di un qualunque individuo, la cui presenza sarà eventualmente validata dalla rilevazione contestuale di un tag da parte delle antenne RFID. Inoltre, grazie alla particolare installazione e gestione della coppia di fotosensori, è possibile rilevare anche il verso di percorrenza del movimento, ossia se l'individuo stia entrando o uscendo dall'ambiente. Infine, l'utilizzo delle fotocellule consente di *triggerare* il funzionamento delle antenne RFID, che saranno attivate –e per breve tempo- solo in presenza di movimenti rilevati, riducendo i tempi di esposizione alle radiofrequenze e limitando il consumo energetico.

5.2 Architettura hardware

Un prototipo sperimentale del sistema descritto è stato realizzato presso il laboratorio RFID dell'ICAR sede di Napoli. I componenti hardware impiegati sono (Figure 4 e 5):

- Reader RFID mod. ISC-LRU2000 della FEIG Electronic. E' un lettore long-range a tecnologia RFID passiva nello spettro UHF, in grado di pilotare fino a quattro antenne ed interfacciabile via LAN, WLAN, RS232-C; dotato di firmware per l'interazione con tag passivi e la gestione automatica delle collisioni
- Antenne UHF mod. ISC.ANTU250/250-EU, a polarizz. circolare, max range di lettura 5 m
- Tag RFID passivi standard EPC Class1 Gen2 a 96 bit.
- Fotocellule del tipo cilindrico M18 della Omron Industrial Automation.

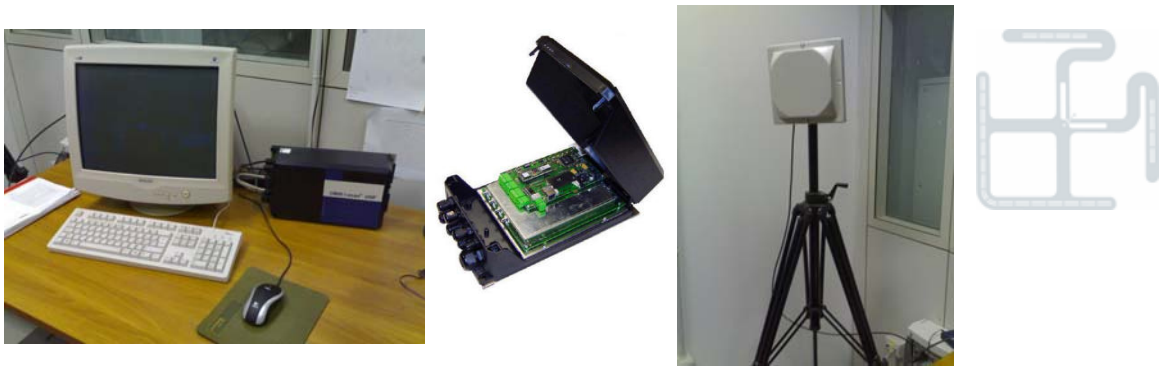

Figura 4 – Reader LRU, antenna UHF e tag passivo EPC Gen. 2

Figura 5 – Coppia di fotocellule e particolari dell'installazione al varco di accesso

5.3 Architettura software

La progettazione del sistema software adotta un approccio a componenti. Seguendo questo approccio, il processo di sviluppo del software si articola nella serie di workflow:

- workflow dei requisiti: si descrive il dominio applicativo
- workflow di specifica: si modellano le specifiche dei singoli componenti
- workflow di provisioning: si realizzano i singoli componenti
- workflow di integrazione: tutti i componenti sono integrati in un middleware o software preesistente.

Nei prossimi paragrafi saranno illustrate le varie fasi del processo di sviluppo.

5.3.1 Definizione dei requisiti

L'obiettivo di questo workflow è comprendere i requisiti del sistema, ovvero capire il dominio applicativo, le funzionalità che deve offrire, gli attori coinvolti ed i processi di business dell'organizzazione. Questa fase produrrà i seguenti *artifact*:

- Business Concept Model
- Use Case Model.

5.3.1.1 Descrizione di attività e del dominio applicativo

Una prima fase molto importante, e spesso molto sottovalutata, è la definizione dei confini del sistema software. Questa viene spesso chiamata visione del sistema (*System Envisioning*).

"Viene realizzato un sistema software per la localizzazione e l'identificazione di soggetti mobili in un ambiente pervasivo, che si basa sul rilevamento dell'attraversamento da parte di tali soggetti di un varco di accesso. L'utente del sistema accede in maniera automatica e trasparente alle informazioni pertinenti ai soggetti identificati nell'ambiente. L'identificazione del soggetto avviene attraverso un tag RFID ad esso univocamente associato. Inoltre, il sistema è in grado di rilevare anomalie quali accessi non autorizzati, presenza di ostacoli nel varco, ecc."

5.3.1.2 Individuazione e rappresentazione dei concetti

In Figura 6 è rappresentato il Business Concept Model. In questo diagramma sono riportati i concetti e le relazioni rilevanti per il dominio applicativo rappresentati con la notazione dei Class Diagram UML.

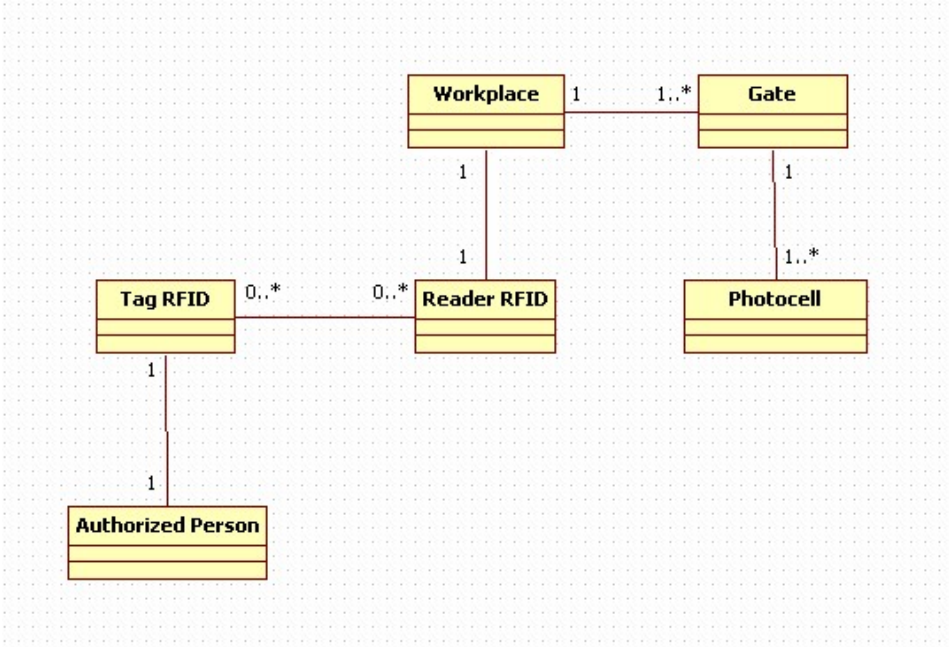

Figura 6 – Business Concept Model

5.3.1.3 Individuazione e descrizione dei casi d'uso

I casi d'uso sono il meccanismo principale usato da UML per la definizione dei confini del sistema software. Essi permettono di indicare il modo in cui il software implementa le funzionalità richieste. Gli Use Case Diagram riportati nelle Figure 7.a, 7.b e 7.c rappresentano le specifiche funzionali del sistema.

Associazione Persona - tag RFID

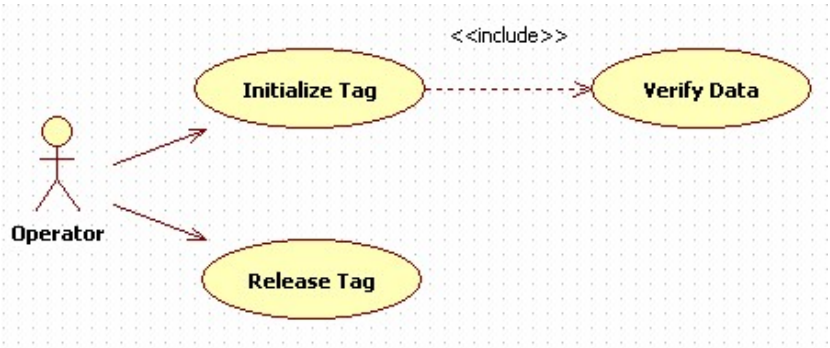

Figura 7.a Diagramma dei casi d'uso per l'associazione Persona/tag RFID

Nome: **Initialize Tag**

Iniziatore: Operator

Scopo: Inserire una nuova associazione Persona-Tag.

Scenario principale di successo:

1. L'utente chiede di aggiungere una nuova associazione tra una persona e un tag.

2. L'utente inserisce i dati relativi alla nuova associazione Persona-Tag.

3. Viene eseguito lo Use Case "Verify Data".

4. Il sistema inserisce la nuova associazione Persona-Tag nell'elenco di quelle già presenti.

Inclusioni: “Verify Data”.

Nome: **Verify Data**

Iniziatore: Initialize Tag

Scopo: Verificare che i dati della nuova associazione Persona-Tag siano corretti.

Scenario principale di successo:

1. Il sistema riceve i dati della nuova associazione Persona-Tag.

2.Il sistema confronta i dati della nuova associazione con quelli delle altre associazioni presenti, verificando che non vi siano incongruenze (per es. che a quella persona sia già associato un tag RFID).

3. Il sistema permette l'inserimento della nuova associazione.

Nome: **Release Tag**

Iniziatore: Operator

Scopo: Rilasciare una associazione Persona-Tag.

Scenario principale di successo:

1. L'utente chiede di rilasciare una associazione Persona-Tag.

2. Il sistema provvede a rimuovere le associazioni Persona-Tag indicate dall'utente.

3. Il sistema aggiorna l'elenco delle associazioni Persona-Tag.

Localizzazione e Identificazione Persone

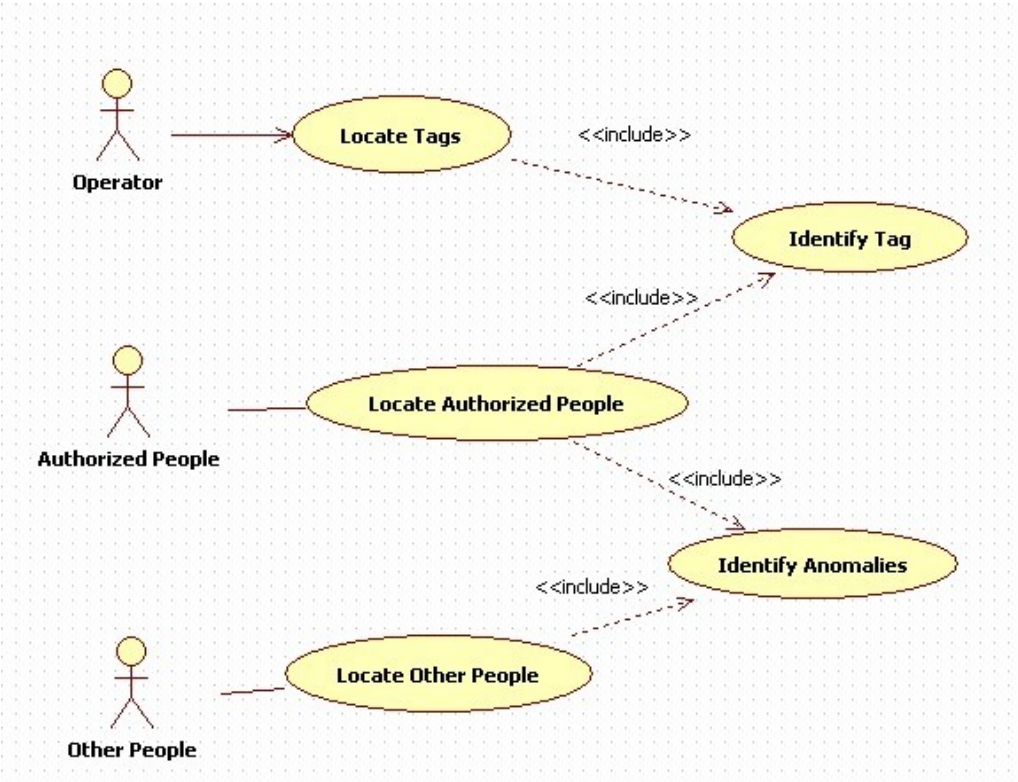

Figura 7.b Diagramma dei casi d'uso per la Localizzazione e l'Identificazione delle Persone

Nome: **Locate Tags**

Iniziatore: Operator

Scopo: Localizzare le persone autorizzate attualmente presenti nell'ambiente di lavoro.

Scenario principale di successo:

1. L'utente chiede di conoscere le persone presenti in quell'istante nell'ambiente di lavoro.

2. Il sistema rileva i tags RFID attualmente presenti nell'ambiente di lavoro.

3. Viene eseguito lo Use Case "Identify People".

4. Il sistema aggiorna l'elenco delle persone autorizzate attualmente presenti nell'ambiente di lavoro.

Inclusioni: "Identify People".

Nome: **Locate Authorized People**

Iniziatore: Authorized People

Scopo: Localizzare persone autorizzate nell'ambiente di lavoro.

Scenario principale di successo:

1. Una persona autorizzata, ossia dotata di un tag RFID di identificazione, attraversa il varco controllato dal sistema.

2. Viene eseguito lo Use Case "Identify Anomalies".

3. Il sistema identifica nell'ambiente l'ingresso o l'uscita di un tag RFID.

4. Viene eseguito lo Use Case "Identify People".

5. Il sistema aggiorna l'elenco delle persone autorizzate attualmente presenti nell'ambiente di lavoro.

Inclusioni:"Identify People"; "Identify Anomalies".

Nome: **Locate Other People**

Iniziatore: Other People

Scopo: Localizzare persone NON autorizzate nell'ambiente di lavoro.

Scenario principale di successo:

1. Una persona non autorizzata, ossia sprovvista di un tag RFID di riconoscimento, attraversa il varco controllato dal sistema.

2. Viene eseguito lo Use Case "Identify Anomalies".

3. Il sistema aggiorna un contatore indicante il numero di persone non autorizzate presenti nell'ambiente di lavoro.

Inclusioni: "Identify Anomalies".

Nome: **Identify Tag**

Iniziatore: Locate Authorized People

Scopo: Identificare le persone presenti nell'ambiente di lavoro in base ai rispettivi Tag RFID.

Scenario principale di successo:

1. Il sistema identifica gli ID dei tag localizzati con quelli nell'elenco delle associazioni Persona-Tag.

2. Il sistema restituisce i dati delle persone associati agli ID dei tag localizzati.

Nome: **Identify Anomalies**

Iniziatore: Locate Authorized People, Locate Other People.

Scopo: Identificare le eventuali anomalie.

Scenario principale di successo:

1. Il sistema identifica una delle seguenti anomalie:

- una persona non autorizzata ha effettuato un ingresso o un'uscita dall'ambiente di lavoro;

- una persona, autorizzata o non autorizzata, attraversa il varco di ingresso/uscita dell'ambiente di lavoro non completamente in un verso di percorrenza, e lo ripercorre nel verso opposto, ritornando nella posizione iniziale;

- una persona o un ostacolo è fermo davanti al varco di ingresso/uscita dell'ambiente di lavoro.

2. Il sistema notifica l'anomalia.

Funzionalità avanzate Reader RFID

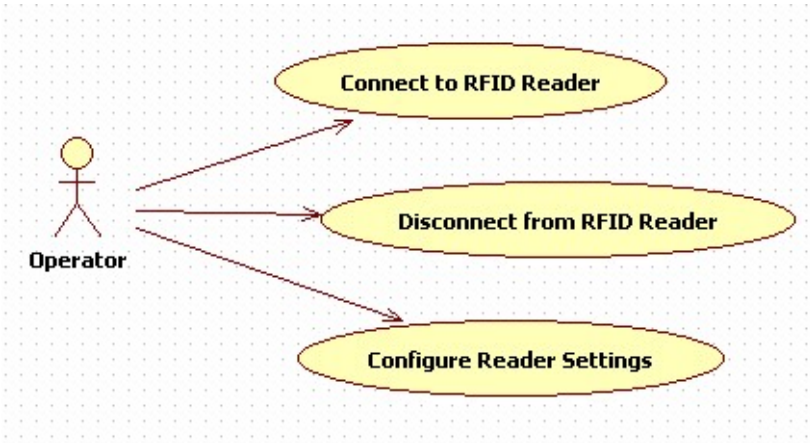

Figura 7.c Diagramma dei casi d'uso delle Funzionalità avanzate Reader RFID

Nome: **Connect to RFID Reader**

Iniziatore: Operator

Scopo: Effettuare la connessione al Reader RFID.

Scenario principale di successo:

1. L'utente richiede di connettersi ad un Reader RFID.

2. L'utente inserisce i dati richiesti per la connessione.

3. Il sistema permette la connessione al Reader RFID.

Nome: **Disconnect from RFID Reader**

Iniziatore: Operator

Scopo: Effettuare la disconnessione dal Reader RFID.

Scenario principale di successo:

1. L'utente chiede la disconnessione dal reader RFID in uso.

2. Il sistema consente la disconnessione.

Nome: **Configure Reader Settings**

Iniziatore: Operator

Scopo: Gestire le impostazioni avanzate del Reader.

Scenario principale di successo:

1. L'utente chiede di configurare le impostazioni avanzate del reader.

2. Il sistema permette la configurazione delle impostazioni avanzate del reader.

5.3.2 Specifica dei componenti

Il workflow di specifica è la fase in cui si modellano le specifiche dei singoli componenti. Esso prevede tre fasi distinte:

- identificazione dei componenti
- interazione tra componenti
- specifica dei componenti.

5.3.2.1 Identificazione dei componenti

L'identificazione dei componenti è la prima fase del workflow di specifica. Segue direttamente il workflow dei requisiti, prendendo come input il business concept model e lo use case model.
Lo scopo dell'identificazione dei componenti è creare un primo insieme di specifiche di interfacce e di componenti, che riunite insieme costituiscano un tentativo iniziale di architettura di componenti.
In questa fase saranno realizzati i seguenti "artifacts":

- Business Type Model
- System Interfaces
- Business Interfaces
- Component Specification & Architecture.

5.3.2.1.1 Il Business Type Model

Il primo passo nell'identificazione dei tipi specifici del business richiede la conversione del modello concettuale di business, prodotto all'interno del workflow dei requisiti, in un modello di tipo di business (Business Type Model). Quest'ultimo è rappresentato da un diagramma delle classi UML, come il modello concettuale, ma il suo scopo è differente (Figura 8).

Laddove il modello concettuale è semplicemente una mappa delle informazioni pertinenti al dominio del problema, il modello di tipo di business contiene l'informazione specifica al business che deve essere mantenuta in memoria dal sistema in via di costruzione.
Un modello di tipo di business viene costruito a partire dal modello concettuale, ridefinendo il campo d'azione ed eliminando elementi (o aggiungendone altri che erano stati omessi a livello concettuale) fino a quando la sua estensione è quella corretta per il sistema.

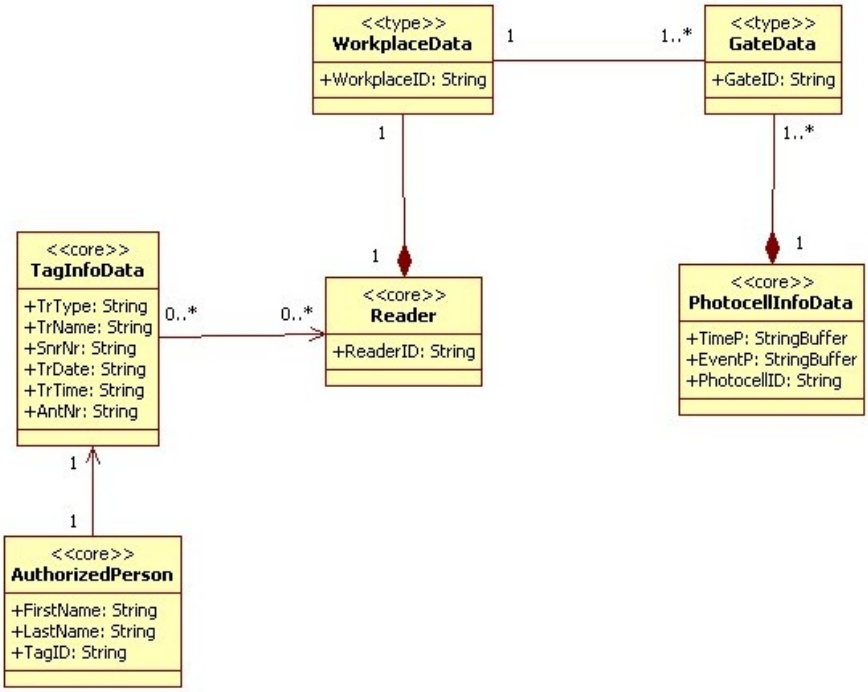

Figura 8 – Business Type Model

5.3.2.2 System Interfaces

Le interfacce di sistema vengono individuate a partire dal modello dei casi d'uso realizzato nel workflow di specifica. In particolare, si considerano tutte le funzionalità del sistema individuate nel modello dei casi d'uso e per ognuna di esse si costruisce un'interfaccia, in quanto esse rappresentano il meccanismo di accesso alle funzionalità stesse.
Dall'analisi del modello dei casi d'uso realizzato precedentemente si sono individuate le seguenti interfacce (Figura 9):

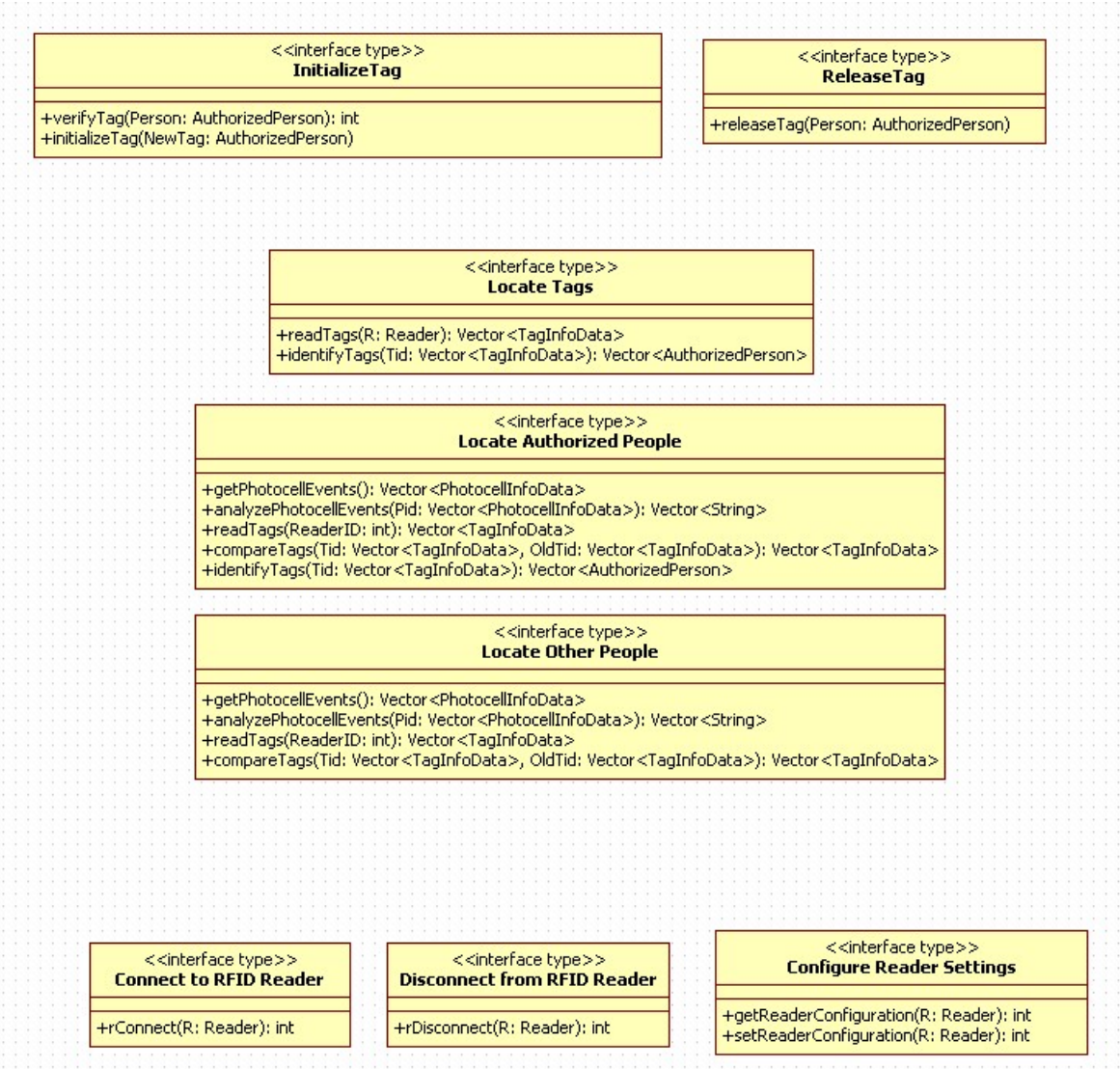

Figura 9 – System Interfaces

5.3.2.3 Business Interfaces

Le interfacce di business gestiscono le informazioni rappresentate dai tipi base, individuati nel Business Type Model, e dai tipi che rappresentano i suoi dettagli. Per ognuno dei tipi base, quindi, verrà creata un'interfaccia di business. Un tipo base è un tipo di business che esiste all'interno del business in modo indipendente, ed è caratterizzato dalle seguenti proprietà:

- Identificatore del business
- Esistenza indipendente

Per quanto riguarda l'esistenza indipendente, essa significa che il concetto può esistere nel nostro dominio applicativo indipendentemente dagli altri. Per creare le interfacce di business bisogna analizzare il business type model e vedere quali tipi base hanno le due proprietà sopra elencate. Analizzando il nostro business type model si ha che le interfacce create sono le seguenti (Figura 10):

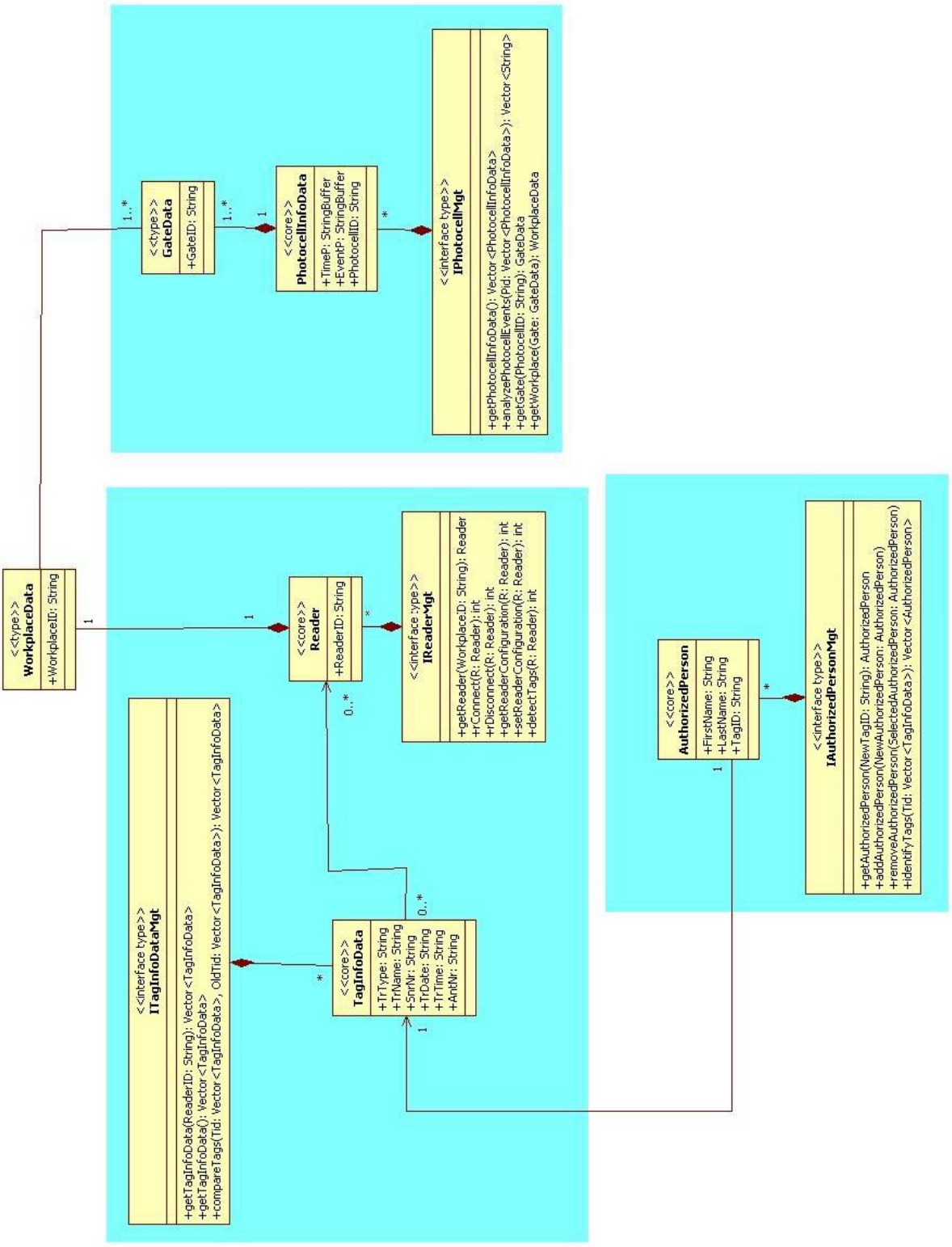

Figura 10 – Business Interfaces

5.3.2.4 Architettura dei componenti

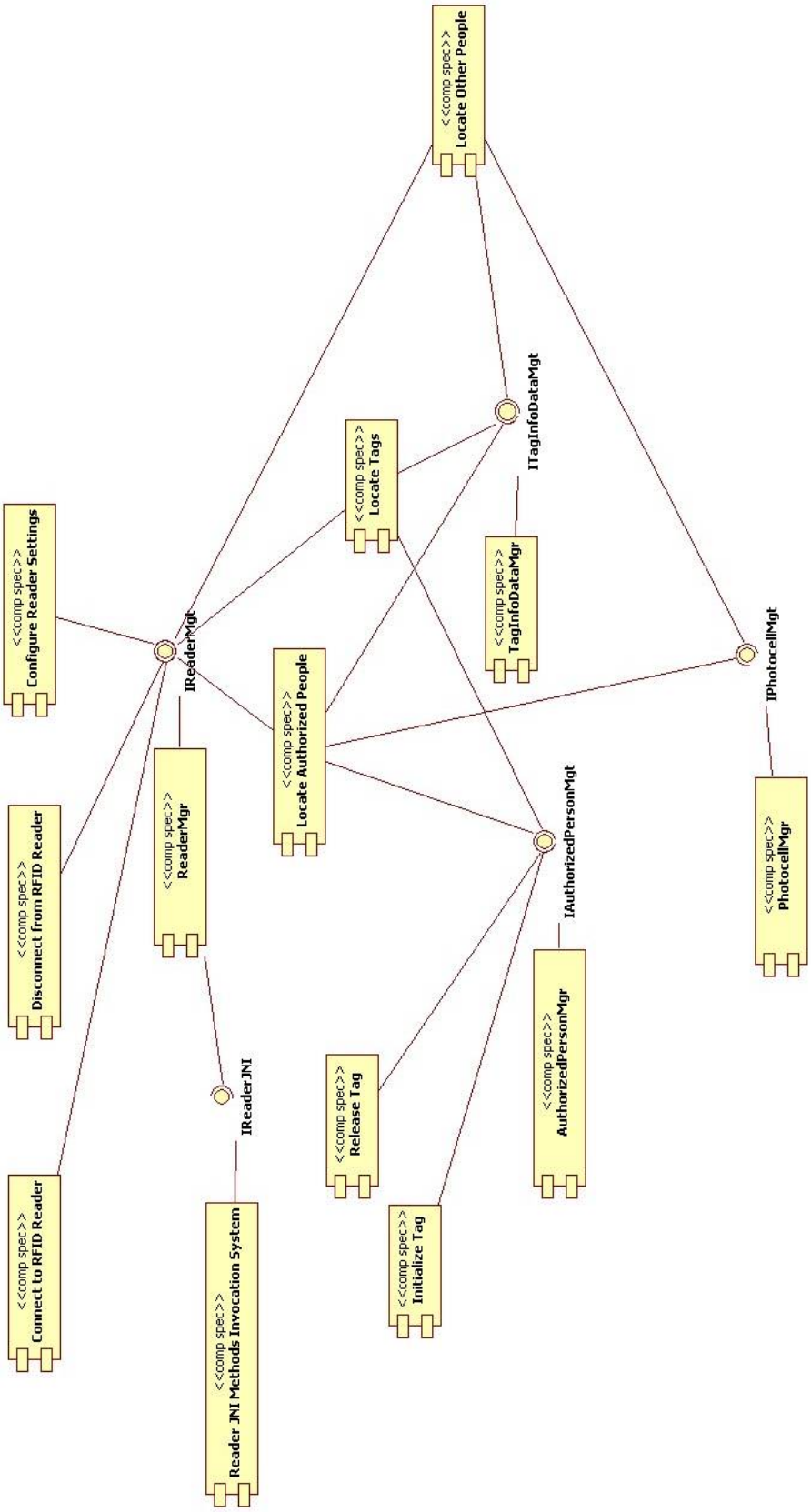

Figura 11 – Architettura dei componenti

A questo punto è possibile avere una specifica iniziale dei componenti e dell'architettura. Si ricorda che un componente è l'unità di distribuzione di un sistema a componenti, ed identifica anche la dimensione dei "frammenti" che si possono sostituire durante la manutenzione del sistema.
Nel caso specifico (Figura 11), l'interazione a basso livello con il reader RFID è ottenuta attraverso una dll esterna, rappresentata nel diagramma seguente dal componente "Reader JNI Methods Invocation System", la quale contiene l'implementazione in codice C++ dei metodi di comunicazione di basso livello verso il reader, necessari per il funzionamento del sistema. L'uso di questa dll per l'invocazione di questi metodi e il prelievo di eventuali parametri di ritorno avviene attraverso la Java Native Interface, un'interfaccia offerta da Java per l'utilizzo di codice scritto in altri linguaggi da o verso l'applicazione Java.
Una breve trattazione di questa libreria offerta da Java sarà introdotta nel seguito.

5.3.3 Interazione tra componenti

L'obiettivo di questa fase del workflow di specifica è capire come i componenti, identificati nella fase precedente, devono collaborare per fornire le funzionalità richieste.
Per ogni interfaccia di sistema verranno riportati i Collaboration Diagram, mostrando le interfacce di business e i loro metodi che risolvono le chiamate.

Initialize Tag:

- *InitializeTag*: il sistema dapprima verifica che i dati della nuova associazione Persona-Tag siano validi, ossia che non sia già presente un tag associato a quella persona, o viceversa (getAuthorizedPerson); in caso affermativo la nuova associazione Persona-Tag viene inserita nel sistema (addAuthorizedPerson) (Figura 12.a).

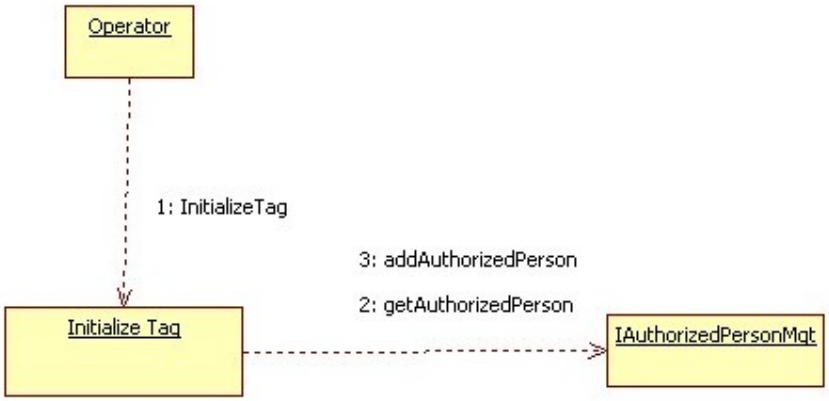

Figura 12.a – Collaboration diagram per l'interfaccia Initialize Tag

- *VerifyTag*: il sistema verifica se i dati di una associazione Persona-Tag non siano già presenti nel sistema, come spiegato prima (getAuthorizedPerson) (Figura 12.b).

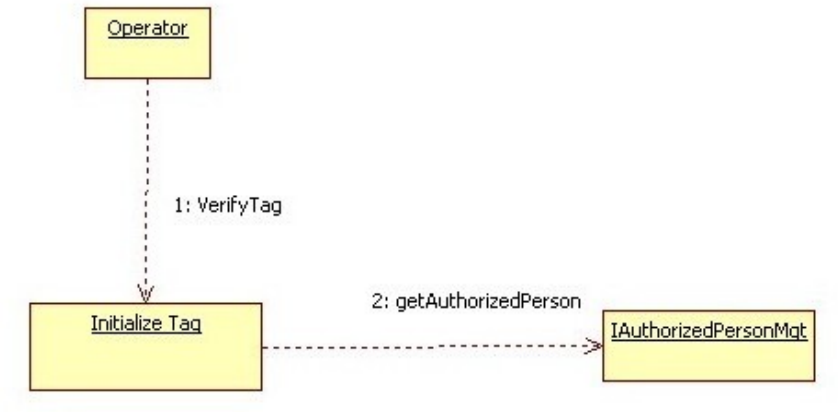

Figura 12.b – Collaboration diagram per l'interfaccia Initialize Tag

Release Tag:

- *ReleaseTag*: il sistema ricerca l'associazione Persona-Tag da rimuovere (getAuthorizedPeople), e la rimuove dall'elenco (removeAuthorizedPeople) (Figura 13) .

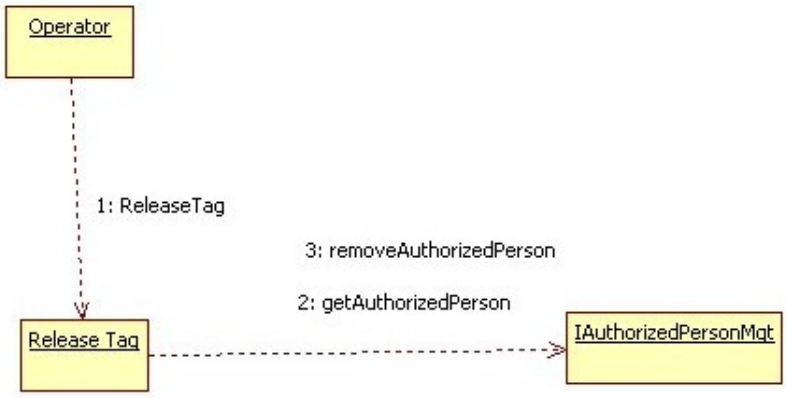

Figura 13 – Collaboration diagram per l'interfaccia Release Tag

Locate Tags*:*

- *readTags:* viene ordinato al reader di accendere le antenne RF, registrare i dati dei tag presenti (detectTags) e prelevarli dal reader stesso (getTagInfoData) (Figura 14.a).

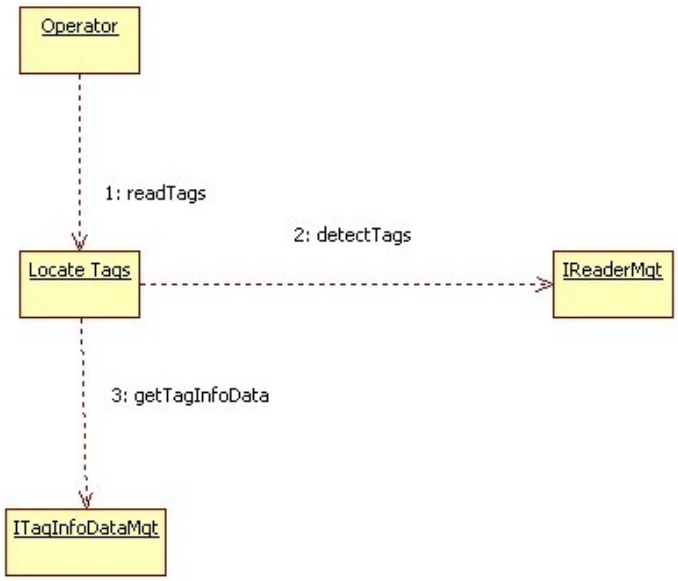

Figura14.a – Collaboration diagram per l'interfaccia Locate Tags

- *identifyTags*: viene effettuata l'associazione tra gli ID dei tag rilevati e i dati anagrafici delle persone cui appartengono (identifyTags) (Figura 14.b) .

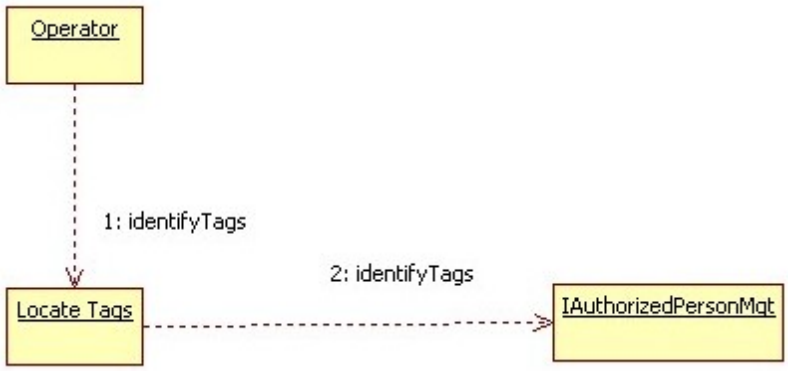

Figura14.b – Collaboration diagram per l'interfaccia Locate Tags

Locate Authorized People:

- *getPhotocellEvents:* vengono prelevati i dati relativi all'interruzione del raggio di una o di entrambe le fotocellule (getPhotocellInfoData) (Figura 15.a) .

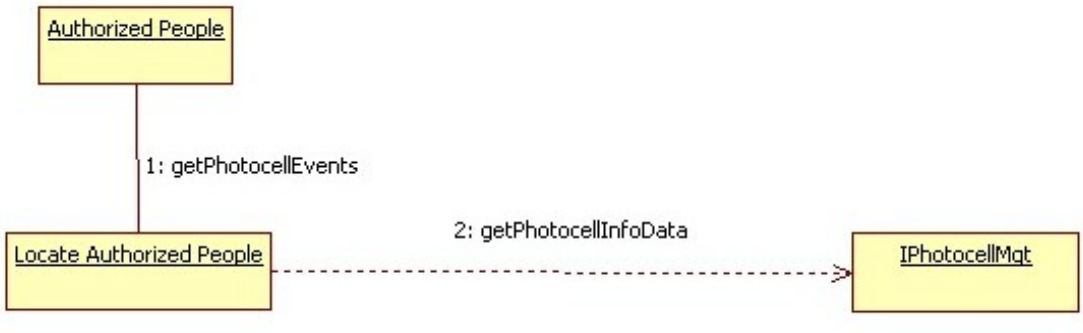

Figura 15.a Collaboration diagram per l'interfaccia Locate Authorized People

- *analyzePhotocellEvents*: i dati delle fotocellule registrati prima vengono analizzati per capire che tipo di evento si è verificato, regolare (ingresso/uscita) o anomalo (tentativo d'ingresso/uscita, varco ostruito) (Figura 15.b) . Nel prossimo paragrafo approfondiremo questo aspetto.

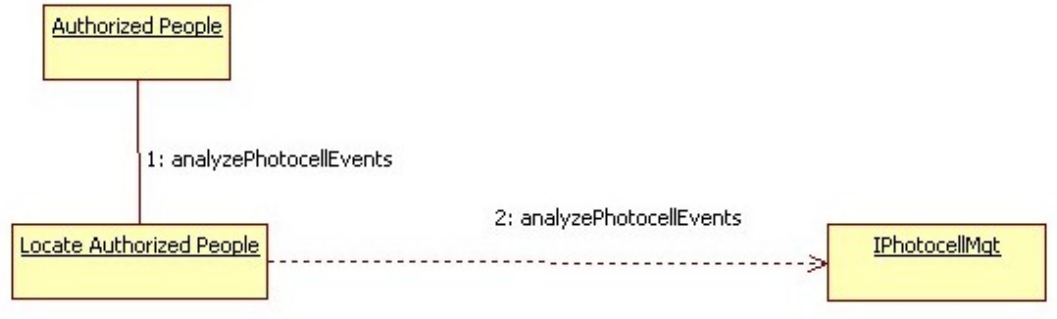

Figura 15.b Collaboration diagram per l'interfaccia Locate Authorized People

- *readTags*: il sistema identifica dapprima qual è il varco dov'è avvenuto l'evento (getGate) e l'ambiente di lavoro associato a quel varco (getWorkplace). Poi, mediante l'interfaccia di business IReaderMgt, identifica il Reader associato a quel Workplace (getReader), gli ordina di registrare i dati dei tags ivi presenti (detectTags) che poi vengono prelevati (getTagInfoData) (Figura 15.c).

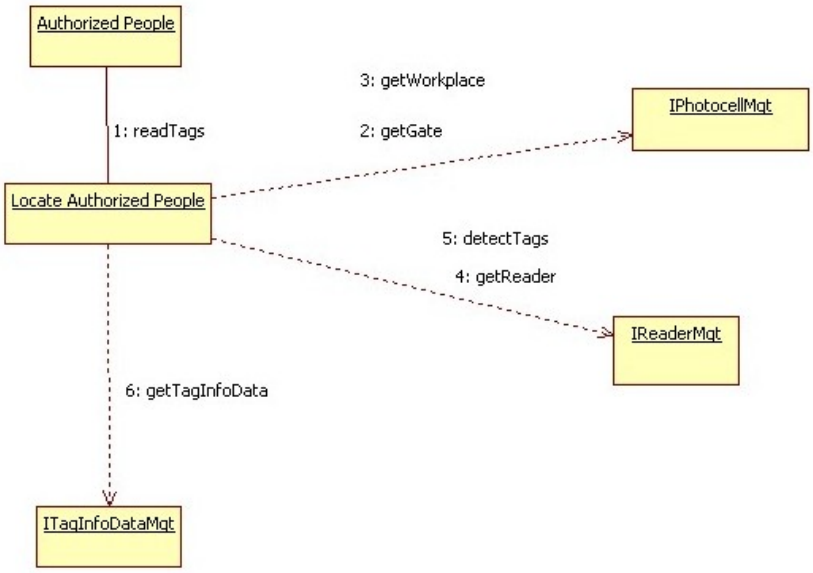

Figura 15.c – Collaboration diagram per l'interfaccia Locate Authorized People

- *compareTags:* i dati dei tags localizzati dal reader vengono confrontati con quelli localizzati precedentemente, per vedere se c'è qualche tag in più (è entrato qualcuno), se ne manca qualcuno (è uscito qualcuno) oppure se non vi è stata alcuna variazione nel numero e nell'identificativo dei tags (l'evento è stato innescato da una persona non autorizzata) (Figura 15.d).

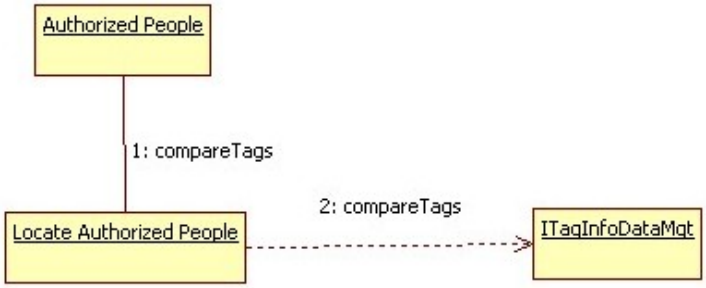

Figura 15.d – Collaboration diagram per l'interfaccia Locate Authorized People

- *identifyTags:* viene effettuata l'associazione tra gli ID dei tag rilevati e i dati anagrafici delle persone cui appartengono (identifyTags) (Figura 15.e).

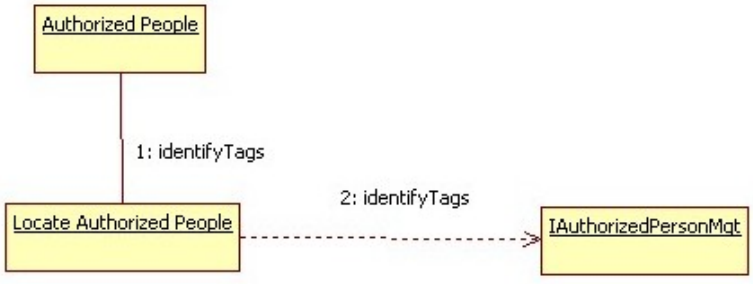

Figura 15.e – Collaboration diagram per l'interfaccia Locate Authorized People

Locate Other People:

- *getPhotocellEvents:* vengono prelevati i dati relativi all'interruzione del raggio di una o di entrambe le fotocellule (getPhotocellInfoData) (Figura 16.a) .

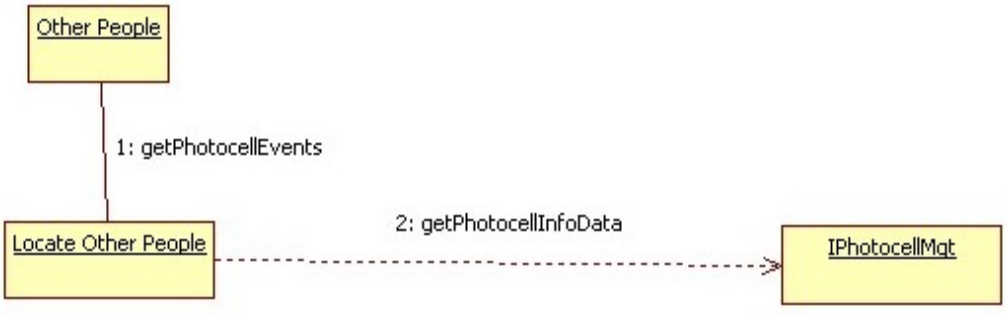

Figura 16.a – Collaboration diagram per l'interfaccia Locate Other People

- *analyzePhotocellEvents*: i dati delle fotocellule registrati prima vengono analizzati per capire che tipo di evento si è verificato, regolare (ingresso/uscita) o anomalo (tentativo d'ingresso/uscita, varco ostruito) (Figura 16.b). Nel prossimo paragrafo approfondiremo questo aspetto.

Figura 16.b – Collaboration diagram per l'interfaccia Locate Other People

- *readTags*: il sistema identifica dapprima qual è il varco dov'è avvenuto l'evento (getGate) e l'ambiente di lavoro associato a quel varco (getWorkplace). Poi, mediante l'interfaccia di business IReaderMgt, identifica il Reader associato a quel Workplace (getReader), gli ordina di registrare i dati dei tags ivi presenti (detectTags) che poi vengono prelevati (getTagInfoData) (Figura 16.c).

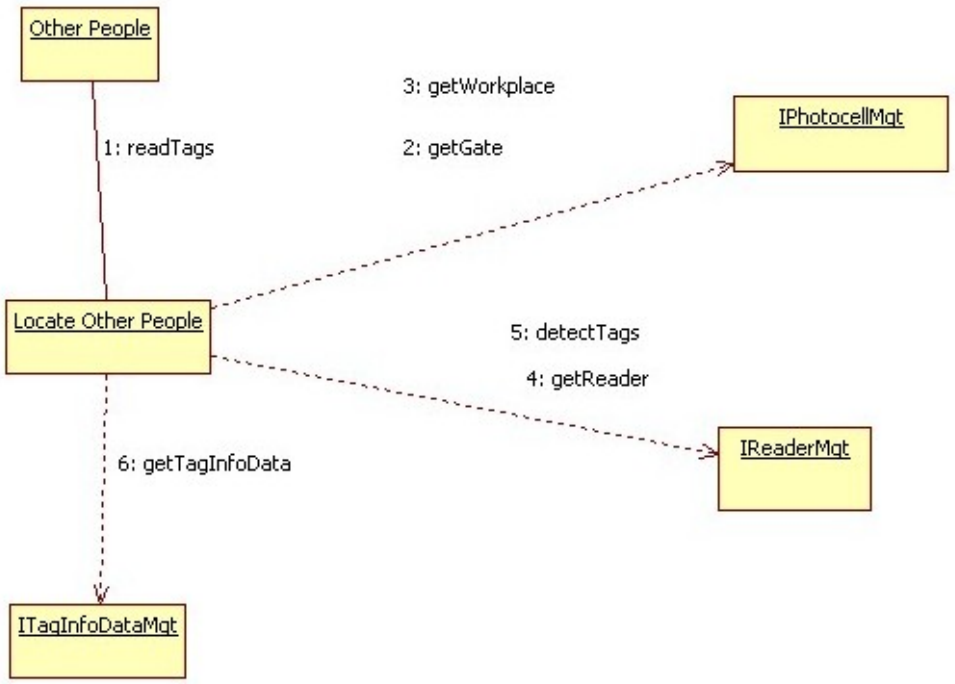

Figura 16.c – Collaboration diagram per l'interfaccia Locate Other People

- *compareTags:* i dati dei tags localizzati dal reader vengono confrontati con quelli localizzati precedentemente, per vedere se c'è qualche tag in più (è entrato qualcuno), se ne manca qualcuno (è uscito qualcuno) oppure se non vi è stata alcuna variazione nel numero e nell'identificativo dei tags (l'evento è stato innescato da una persona non autorizzata) (Figura 16.d).

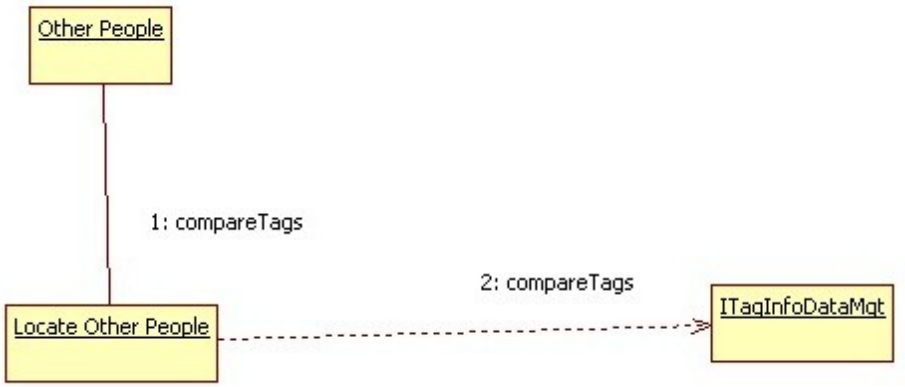

Figura 16.d – Collaboration diagram per l'interfaccia Locate Other People

Connect to RFID Reader:

- *rConnect:* il sistema effettua la connessione al Reader (rConnect) (Figura 17).

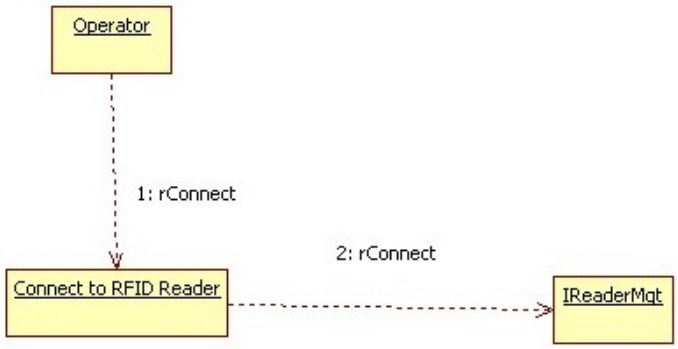

Figura 17 – Collaboration diagram per l'interfaccia Connect to RFID Reader

Disconnect to RFID Reader:

- *rDisconnect:* il sistema effettua la disconnessione dal Reader (rDisconnect) (Figura 18).

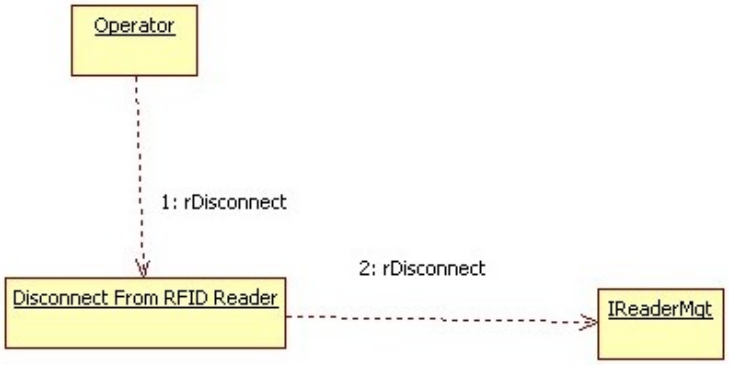

Figura 18 – Collaboration diagram per l'interfaccia Disconnect From RFID Reader

Configure Reader Settings:

- *getReaderSettings*: vengono prelevati i dati relativi alle impostazioni avanzate del Reader (getReaderSettings) (Figura 19.a).

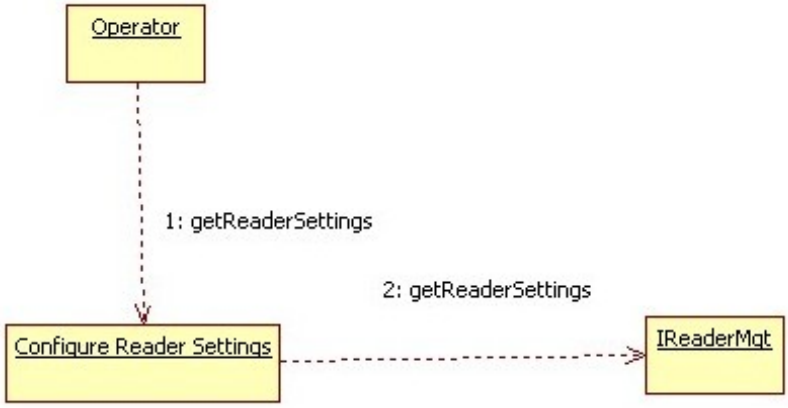

Figura 19.a – Collaboration diagram per l'interfaccia Configure Reader Settings

- *setReaderSettings*: vengono settati i dati relativi alle impostazioni avanzate del Reader (setReaderSettings) (Figura 19.b).

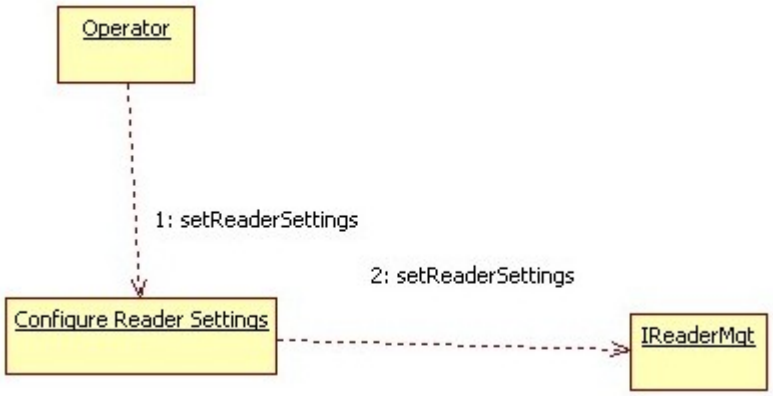

Figura 19.b – Collaboration diagram per l'interfaccia Configure Reader Settings

5.4 Riconoscimento degli eventi di varco

In questo paragrafo approfondiremo il discorso su come il sistema rileva gli eventi rilevati dalle fotocellule, e come ne stabilisce il tipo.
Anzitutto, ricordiamo che le fotocellule sono state installate in modo tale che sia impossibile attraversare il varco senza interrompere il raggio di almeno una di esse.
Posto che ogni fotocellula ha due stati, indicati come "raggio attivo" e "raggio interrotto", si ha che:

- ognuna delle due fotocellule invia al sistema un valore diverso per lo stato "raggio interrotto", permettendo così al sistema di identificare su quale fotocellula si è registrato l'evento
- entrambe le fotocellule inviano al sistema un unico valore per lo stato "raggio attivo", nel momento in cui entrambe le fotocellule si trovino in questo stato
- inoltre, il sistema registra un valore anche nel caso entrambe le fotocellule siano nello stato "raggio interrotto".

Con queste premesse, è stato implementato un automa a stati finiti in grado di analizzare la sequenza di valori inviata dalle fotocellule ogni volta in modo rapido e preciso, e decodificare così il tipo di evento associato a quella sequenza.
Posto che F1 (F2) indichi che la prima (seconda) fotocellula nel verso d'ingresso si trova nello stato "raggio interrotto", e che lo stato "raggio attivo" sia indicato come '0', si ha ad esempio che la sequenza *F1, F1+F2, F2,'0'* indicherà un ingresso avvenuto con successo.
Se invece l'evento avvenuto fosse un tentativo d'ingresso non portato a termine, una possibile sequenza potrebbe essere: *F1, F1+F2, F1, '0'*.
Considerando invece il verso d'uscita, valgono gli esempi fatti prima a patto di scambiare tra loro F1 e F2.
Infine, per il riconoscimento dell'evento anomalo "varco ostruito", il sistema fa partire un timer appena una delle fotocellule passa nello stato "raggio interrotto": se non viene inviato l'evento "raggio attivo" prima di un prefissato limite di tempo, l'evento "varco ostruito" viene notificato.
In Figura 20 è rappresentato lo Statechart Diagram per l'ingresso nell'ambiente di lavoro. I vari stati sono indicati con la terminologia descritta precedentemente. Per l'uscita il procedimento è analogo, a patto di scambiare in figura gli stati F1 e F2.

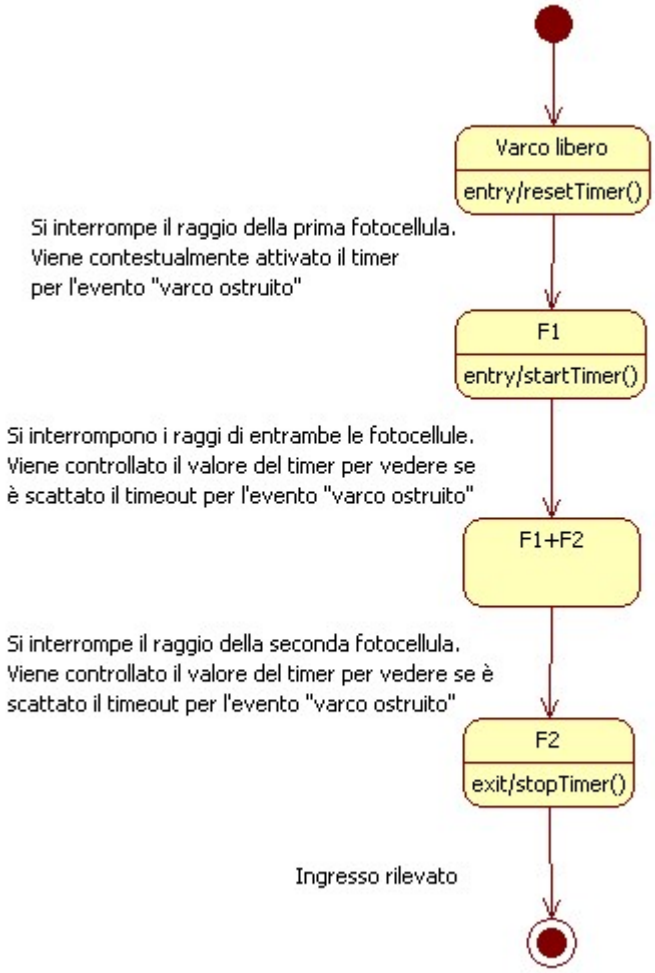

Figura 20 – Statechart Diagram per l'ingresso nell'ambiente monitorato

5.5 Implementazione

Per l'utilizzo del reader è stata implementata una libreria in linguaggio C++, in cui sono presenti le strutture dati necessarie e i metodi principali per la comunicazione a basso livello con il reader, ad esempio per la lettura dei tag presenti nell'ambiente di lavoro e per il prelievo dei dati su di essi presenti, per la connessione e la disconnessione dal reader, per accedere alle impostazioni avanzate di configurazione, etc. Per la comunicazione con il reader dall'applicazione Java, attraverso l'invocazione dei metodi della dll, è stata utilizzata come tramite tra i due linguaggi di programmazione la Java Native Interface.
La Java Native Interface (JNI) è una infrastruttura di programmazione che permette al codice Java in esecuzione nella Java Virtual Machine (JVM) di invocare ed essere invocato da applicazioni in linguaggio nativo (programmi specifici dell'hardware o del sistema operativo in uso) e librerie scritte in altri linguaggi, così come ad esempio C, C++ e Assembly. L'infrastruttura JNI permette ad un programma scritto in linguaggio nativo di utilizzare oggetti Java allo stesso modo di un programma Java. Un metodo nativo può creare oggetti Java e quindi verificare il loro stato e usarli per compiere operazioni. Un metodo nativo può anche ispezionare e usare oggetti creati da un programma Java.

JNI viene talvolta definita come “via di fuga" per gli sviluppatori Java, perché permette loro di estendere le funzionalità delle API Java standard. E’ anche usata per applicazioni *time-critical*, o per operazioni come la risoluzione di equazioni matematiche particolarmente complicate, visto che il codice nativo può essere più rapido della JVM (Figura 21).

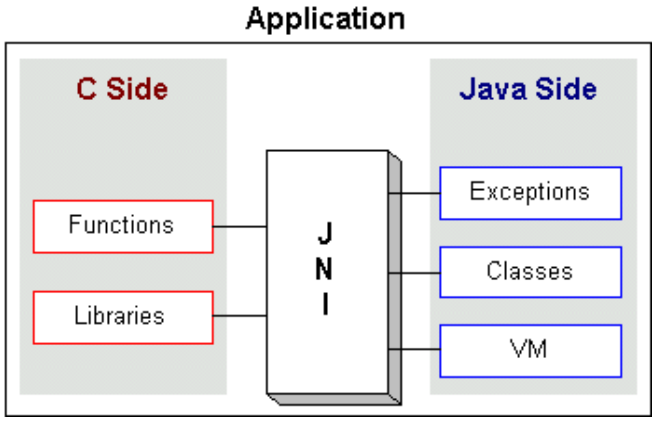

Figura 21 – Dettaglio del rapporto tra Java e il mondo nativo attraverso JNI

I programmatori che si trovano ad usare la JNI devono tener presente che:

- JNI non è una API immediata da usare, richiede uno sforzo considerevole per imparare ad usarla
- piccoli errori nell’utilizzo di JNI possono destabilizzare l’intera JVM in modi difficili da individuare e risolvere
- solo applicazioni e applet verificate possono invocare metodi tramite JNI
- un’applicazione che sfrutta JNI perde la portabilità tra varie piattaforme offerta da Java (comunque, è sempre possibile scrivere diverse implementazioni del codice JNI per ogni piattaforma, e far sì che Java determini il sistema operativo su cui sta operando e carichi l’implementazione giusta a run-time)
- non è prevista alcuna *garbage collection* dal lato JNI del codice (ossia, il codice JNI deve esplicitare la deallocazione dopo il suo utilizzo);
- il controllo degli errori è assolutamente necessario, pena la possibilità di crash sia della JNI che la JVM stessa.

In Figura 22 vengono mostrati i vari passi necessari per la creazione di un’applicazione Java che sfrutti la JNI.

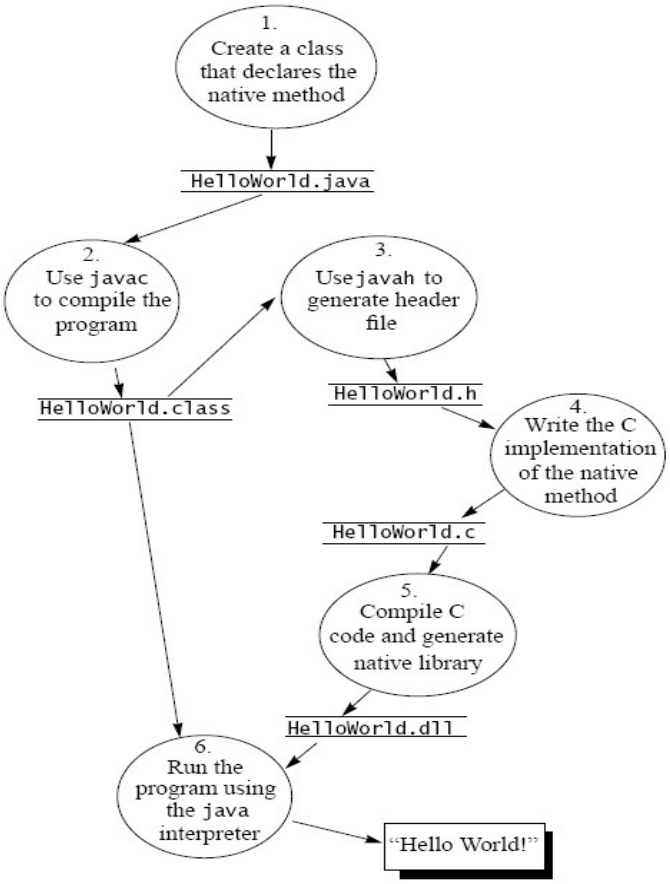

Figura 22 – Creazione di un'applicazione Java "Hello world!" sfruttando JNI

Di seguito vengono riportati alcuni screenshots della GUI dell'applicazione realizzata.
Appena lanciata, dal menù principale è possibile visualizzare i campi principali e accedere agli altri menù dalla pulsantiera a lato.

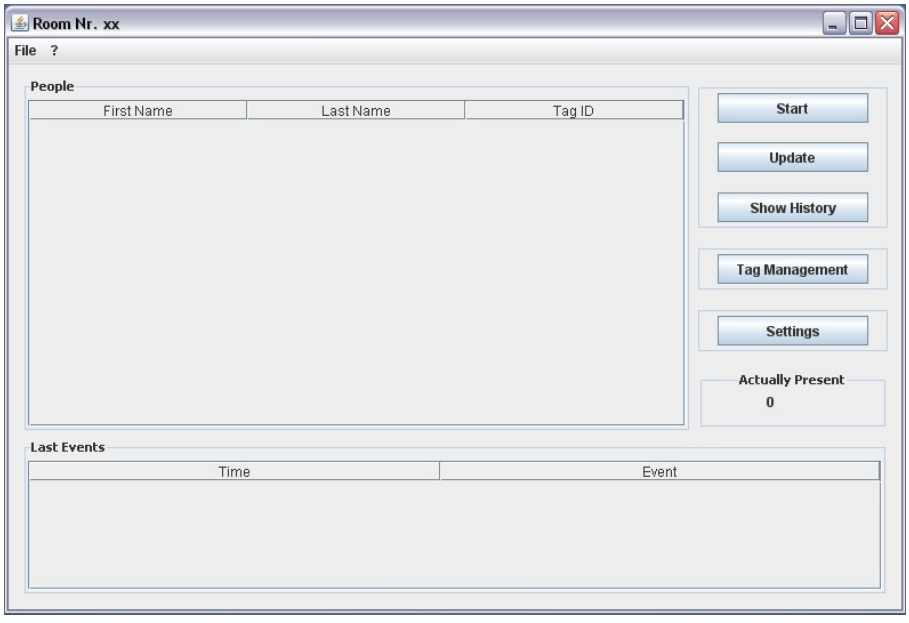

Figura 23 – Il programma appena avviato

Durante la sua esecuzione, in alto vengono mostrate le informazioni sulle persone autorizzate attualmente presenti nell'ambiente di lavoro, mentre in basso vengono mostrati gli ultimi eventi del varco controllato dal sistema. Sulla destra, sotto i pulsanti, è presente un contatore delle persone attualmente presenti.

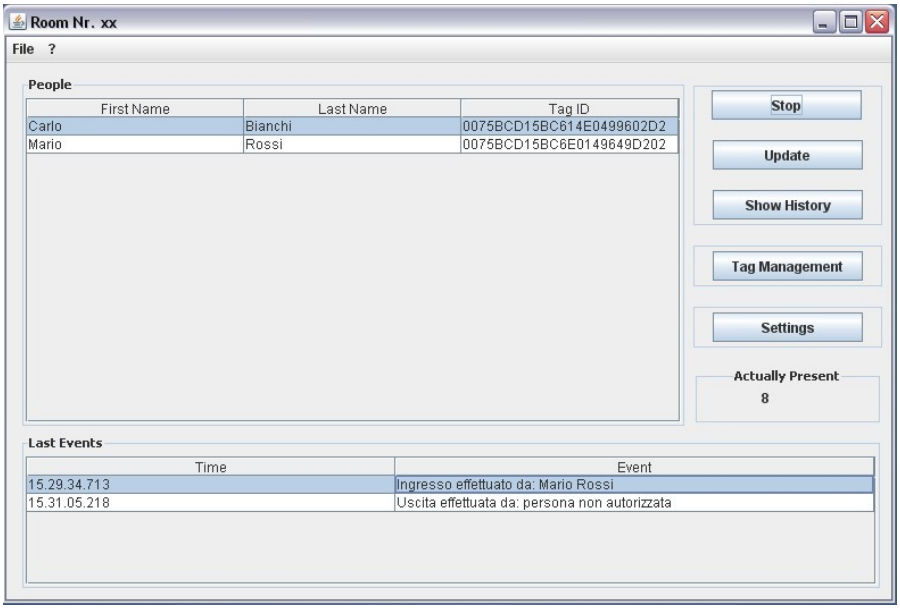

Figura 24 – L'applicazione in esecuzione

Nel menù "Tag Management" è possibile inserire nuove associazioni tra i dati di una persona e l'ID del tag univoco ad essa associato. Le associazioni vengono salvate in un file esterno, in modo da essere conservate una volta chiuso il programma, e richiamate una volta aperto di nuovo.

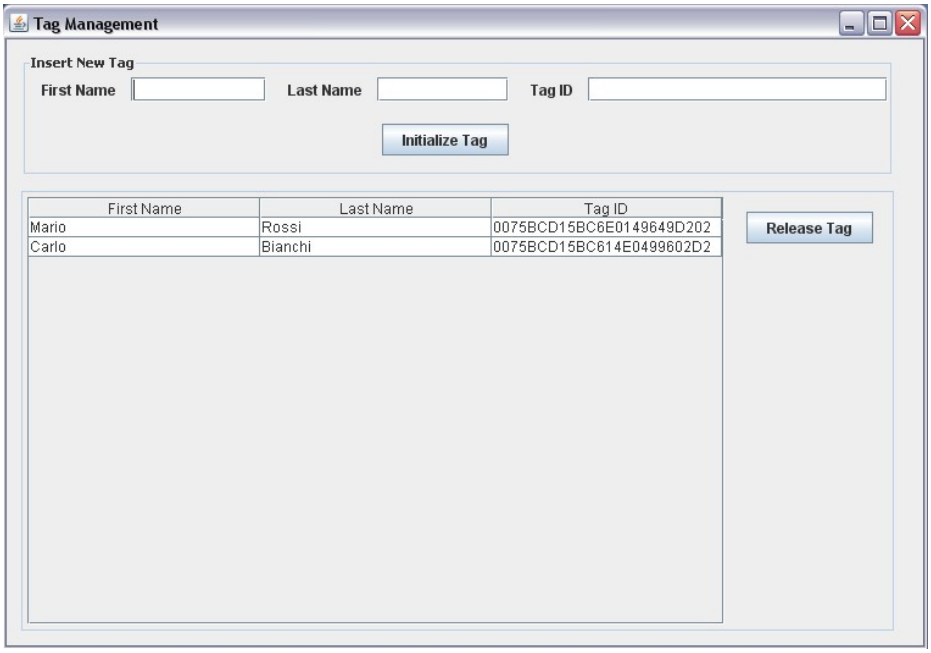

Figura 25 – La finestra di gestione delle associazioni Persona-Tag

6 CONCLUSIONI

Nel presente lavoro è stato descritto lo sviluppo di un sistema che consente di monitorare gli accessi ad ambienti circoscritti attraverso l'acquisizione, in maniera automatica e trasparente all'utente, di informazioni di localizzazione e identificazione di persone in movimento. Il sistema è stato progettato seguendo una metodologia basata su un'innovativa tecnica di integrazione di tecnologie di posizionamento wireless, in particolare RFID e sensori fotoelettrici.
Dopo una sintetica *overview* delle tecnologie di posizionamento wireless disponibili, si è valutata la fattibilità del sistema e si è quindi proceduto ad effettuare l'analisi dei requisiti, individuando in tal modo le funzionalità richieste. La definizione dell'architettura hardware e dei workflow in cui si articola la fase di progettazione dell'architettura software, che ha utilizzato l'approccio a componenti, ha poi consentito di individuare le specifiche ed implementare i componenti necessari. Un prototipo sperimentale del sistema proposto è stato realizzato presso i laboratori dell'ICAR – sede di Napoli – e la conseguente attività di testing di cui è stato oggetto ha dimostrato la validità delle scelte effettuate e l'effettiva fattibilità di impiego in uno scenario di applicazione reale.

BIBLIOGRAFIA

- M. Satyanarayanan, *"Pervasive Computing: Vision and Challenger"*, Carnegie Mellon University.
- M. Weiser, *"The Computer for the 21st Century"*, Scientific Am., Sept., 1991, pp. 94-104.
- S. Maffioletti, *"Requirements for an Ubiquitous Computing Infrastructure"*, Department of Informatics, University of Fribourg.
- D. Salber, A.K. Dey, G.D. Abowd, *"Defining an HCI Research Agenda for an Emerging Interaction Paradigm"* Technical report, GVU Center and College of Computin, Georgia Tech, 1999.
- Davies N., Gellersen H.-W., *"Leaving the Lab: Issues in Deploying Ubiquitous Computing Systems and Applications"*, 2002.
- Michel Barbeau, *"Mobile, Distributed, and Pervasive Computing"*.
- Mascolo C., Capra L., Emmerich W., *"Mobile Computing Middleware"*, Dept. of Computer Science, University College London, 2002.
- Roman M., *"An Application Framework for active space applications"*, 2003.
- Wallbank N., *"A Requirements Analysis of Infrastructures for Ubiquitous Computing Environments"*, Computing Department Lancaster University, 2002.
- Banavar G., *"Challenges in Design and Software Infrastructure for Ubiquitous Computing Applications"*, IBM TJ Watson Research Center, University of Zurich.
- Pervasive Computing Group, *"A Middleware Infrastructure for Active Surroundings"*, Information & Communications University, Korea.
- Gaia Home Page, *http://choices.cs.uiuc.edu/2k/Gaia/*
- Roman M., *"An Application Framework for active space applications"*, 2003.
- Kagal L., Korolev V., Avancha S., Joshi A., Finin T., Yesha Y., *"Centaurus: An Infrastructure for Service Management in Ubiquitous Computing Environments"*, Dept. of Computer Science and Electrical Engineering, University of Maryland Baltimore Conty, USA, 2002.
- Chen H., Finin T., *"An Ontology for Context Aware Pervasive Computing Environments"*, University of Maryland, Baltimore County, USA, 2003.
- Patierno C., *"Italia, semaforo verde per RFID UHF"*, Punto Informatico, 7 Dicembre 2006, *http://punto-informatico.it/1800430_2/PI/News/italia-semaforo-verde-rfid-uhf.aspx*
- Bottà G., *"No, gli europei non si fidano degli RFID"*, Punto Informatico, 18 Ottobre 2006, *http://punto-informatico.it/1704590_all1/PI/News/no-europei-non-si-fidano-degli-rfid.aspx*

- Patierno C., *"Viaggio nel mondo RFID"*, Punto Informatico, 17 Settembre 2004, *http://punto-informatico.it/578577_2/Hardware/News/tecnologie-viaggio-nel-mondo-rfid.aspx* .
- *"Radio Frequency IDentification"*, Wikipedia, *http://it.wikipedia.org/wiki/Radio_Frequency_IDentification*
- *"RFID e sensori ovunque: verso un mondo sinergico, efficiente e interattivo"*, Confindustria, Progetto "IxI - Imprese x Innovazione", *http://www.confindustria.it/Aree/docIXI.nsf/0B60220FD8A8F603C1257141006D5A6D/$File/RFID.pdf*
- *"Sensore"*, Wikipedia, *http://it.wikipedia.org/wiki/Sensore*
- Mauro M., *"Sensori"*, AutoMik - Sito web di informazioni utili sui componenti più utilizzati nell'automazione industriale, *http://digilander.libero.it/mikimoni/sensori.htm*
- Fraden J., *"Handbook of modern sensors: Physics, Designs, and Applications"*, 2003
- Wilson J., *"Sensor Technology Handbook"*, 2005
- Cascetta F., De Luccia M., *"Sistemi di identificazione personale"*, Mondo Digitale n.1, Marzo 2004, pp.44-55, *http://www.mondodigitale.net/Rivista/04_numero_due/Cascetta_p.44-55.pdf*
- Ficco M., *"Localizzazione, molti vantaggi"*, CRIAI Consorzio Campano di Ricerca per l'Informatica e l'Automazione Industriale, 2005, *http://www.criai.it/index.php?option=com_content&task=view&id=28&Itemid=1*
- *"Controllo Accesso - Sistemi di controllo degli accessi"*, http://www.controllo-accesso.com/
- *"Wi-Fi, RFID e 802.11n: quali scenari per il futuro?"*, Network World Online, 6 Febbraio 2008, *http://www.nwi.it/showPage.php?template=approfondimenti&id=7014*
- *"Sistemi Informativi Pervasivi"*, Giornata di studio sul tema "Sistemi Informativi Pervasivi", AICT – Associazione per la Tecnologia dell'Informazione e delle Comunicazioni della Federazione AEIT, 2008, *http://www.associazioneaict.it/asp_getfile.aspx?f=760&io=1&s=808402989*
- *"Controllo elettronico della stabilità"*, Wikipedia, *http://it.wikipedia.org/wiki/Electronic_Stability_Program*
- *"Gem-Where: RFID Jewelry Tracking Solution"*, *http://www.gemwhere.com/index.html*
- Patierno C., *"Viaggio nel mondo dell'RFiD"*, RFiD Guru, 24 Settembre 2004, *http://rfidguru.eu/blogs/rfid/archive/2004/09.aspx*
- *"Linee guida per l'impiego dei sistemi RFID nella Pubblica Amministrazione"*, CNIPA - Centro Nazionale per l'Informatica nella Pubblica Amministrazione, 2007, *http://www.scribd.com/doc/2188740/GuidaRFID-PA*
- *"Soluzione per la gestione e il controllo degli accessi"*, *Essecome, Novembre 2008, pp.195-200*, *http://www.securindex.com/articoli/applicazioni/SOLUTION_NUOVA_VETRO_e_11_08.pdf*
- Liang S., *"The Java™ Native Interface: Programmer's Guide and Specification"*, 1999.
- *"Wireless"*, Wikipedia, http://it.wikipedia.org/wiki/Wireless
- *"Controller RFID – Long Range UHF LRU2000"*, *http://www.work-tag.eu/Prodotti/ISC.RU2000-LongRangeUHF.htm*