UNIVERSITÀ DEGLI STUDI DI PARMA

Dottorato di Ricerca in Tecnologie dell'Informazione

XXI Ciclo

INTELLIGENZA AMBIENTALE PER IL MONITORAGGIO E L'ASSISTENZA DOMESTICA: UN'INFRASTRUTTURA DI CONTROLLO BASATA SU COMUNICAZIONE IP

Coordinatore:

Chiar.mo Prof. Carlo Morandi

Tutor:

Chiar.mo Prof. Ilaria De Munari

Dottorando: *Ferdinando Grossi*

Gennaio 2009

Alla mia famiglia
ed a tutti coloro
che hanno creduto in me

Sommario

Elenco delle figure

Introduzione

Le tecnologia è ormai una realtà nella nostra società da molti anni. Ha, poco a poco, pervaso quasi tutti gli aspetti della nostra vita: ci permette di comunicare a distanza in modo rapido ed efficace, ci consente di lavorare in modo efficiente, di spostarci in modo più rapido e sicuro. È un supporto indispensabile per lo sviluppo della scienza e della medicina, pur non essendo sempre considerata da tutti come un aspetto positivo. Di sicuro ha cambiato i rapporti fra le persone e le dinamiche del mercato.
Un ambito nel quale la tecnologia si inserisce con relativa difficoltà è quello dell'automazione delle abitazioni. La casa è vista come un luogo molto intimo, legato ad abitudini e necessità personali. L'introduzione della tecnologia in questo contesto può essere problematica: la tecnologia può essere ritenuta "invadente" oppure sorgente di rischi o difficoltà, senza che ne vengano percepiti i potenziali benefici.

Le tecnologie dell'informazione sono invece mature per essere introdotte in contesti domestici senza dover temere effetti negativi sulle nostre abitudini o sulle funzioni di cui abbiamo necessità, analogamente a quanto accaduto in diversi contesti della nostra vita quotidiana. Si pensi, per esempio, a quanto accaduto con l'introduzione dell'elettronica nei mezzi di trasporto. Essa ha portato senza dubbio innumerevoli vantaggi: l'ABS, gli air-bag, il controllo di stabilità, gli immobilizer, sono tutte tecnologie con impatto diretto molto positivo sulla vita di tutti gli automobilisti. E' interessante anche notare che l'introduzione di elementi tecnologici non sempre è direttamente percepita dall'utilizzatore, nè necessariamente gli richiede maggiore competenza. Ad esempio, il sistema ABS consente di ridurre considerevolmente gli

spazi di arresto in condizioni critiche, ma l'utente aziona comunque il comando tradizionale del freno, non modificando il proprio abituale comportamento. Certamente tali tecnologie hanno comportato una maggiore complessità dei veicoli, e la necessità di personale maggiormente specializzato per la loro manutenzione; questo ha un impatto sui costi, che deve essere compensato dalla chiara percezione del benificio ottenuto.

Anche per l'abitazione una simile trasformazione, in parte nascosta, è già iniziata. Sono molte le case dotate di sistemi di controllo del riscaldamento evoluto, in grado di pianificare temperature diverse in base alle ore del giorno, in modo diverso giorno per giorno, ad esempio su base settimanale. I sistemi di segnalazione delle intrusioni sono diffusi e sofisticati. Quelli per la gestione di automazioni per l'apertura di cancelli ed autorimesse sono ormai una dotazione comune.
L'automazione domestica si propone come elemento in grado di orchestrare in modo efficiente ed integrato tutte queste funzioni, ed altre ancora, che sono rese possibili solo dall'interazione fra i sistemi.

Le necessità specifiche di persone con difficoltà di tipo motorio, sensoriale o cognitivo possono essere significativamente sostenute da un uso accorto di questo tipo di tecnologie: esse possono favorire l'autonomia, riducendo la necessità di assistenza e permettendo maggiori possibilità di vivere in maniera indipendente nella propria casa, con evidente vantaggio sia in termini di qualità della vita che di costi (individuali e collettivi).

Per questo il progetto sviluppato ha una particolare attenzione alle esigenze di integrazione degli ausili di automazione di ogni genere, per poter essere aperto a qualunque necessità, presente e futura. Il problema ha dimensioni rilevanti: in Europa vivono oltre 39 milioni di persone disabili; in Italia esse sono circa 2.8 milioni [1]. Di queste, oltre il 92% vivono in famiglia, mentre il rimanente 8% vive in strutture dedicate. L'ambiente domestico è quindi lo scenario entro il quale prevalentemente si manifestano le limitazioni di autonomia e indipendenza connesse a malattia e disabilità.
E' importante anche notare che la prima causa di disabilità è l'invecchiamento e le patologie a questo connesse. Dai dati disponibili risulta evidente come la possibi-

lità di subire limitazioni alla propria autonomia e indipendenza cresca rapidamente con l'età oltre i 55-60 anni. Per questo motivo, quindi, le soluzioni volte a favorire una soddisfacente permanenza nell'ambiente domestico di persone anziane e disabili hanno evidenti tratti in comune, e possono avere ricadute sociali ed economiche di rilievo.
Più in generale, si può osservare che l'invecchiamento è una delle più importanti sfide che il mondo (in particolare le regioni occidentali più industrializzate) deve affrontare. Da un lato l'aumento dell'aspettativa di vita è un importante risultato della scienza e della medicina, ma dall'altro ciò incide significativamente su molti aspetti di tipo economico e sociale. Infatti la riduzione del rapporto fra la giovane popolazione "attiva" e quella più anziana che ormai si trova in pensione rappresenta, come è noto, una minaccia per la stabilità economica dei sistemi previdenziali di tutti gli Stati. La stessa causa, tuttavia, rischia di compromettere i modelli attuali dei sistemi di assistenza agli anziani e ai bisognosi di cure. La modificazione dei modelli sociali e lavorativi, inoltre, sempre più frequentemente porta alla frammentazione dei nuclei familiari e alla carenza di assistenza domiciliare. Ciò porta sempre più spesso alla necessità di spostare persone anziane con problemi di autosufficienza (a volte anche lievi) verso strutture attrezzate, con evidente riduzione della qualità della vita percepita dagli anziani ed elevato peso economico a gravare sui familiari e sul sistema sanitario.

Strumenti tecnologici possono essere efficacemente impiegati per ridurre le necessità di assistenza: la tecnologia, ovviamente, non può sostituirsi all'assistenza dei familiari o di personale specializzato, ma ne può integrare e completare l'attività, fornendo ausili importanti alla sicurezza personale ed ambientale, coadiuvando l'esecuzione delle funzioni più faticose o ripetitive, consentendo attività di controllo e monitoraggio continuato. L'effettiva diffusione di tali sistemi è ovviamente vincolata a considerazioni di sostenibilità economica. Il costo dei sistemi attualmente in commercio è spesso molto elevato, in parte a causa del fatto che il mercato di riferimento è ancora di ridotte dimensioni, e quindi considerato ancora di tipo "elitario". Nella ricerca condotta, quindi, particolare attenzione è stata dedicata al contenimento dei costi. In particolare, l'impiego della tecnologia di comunicazione IP, in luogo di pro-

tocolli “domotici” dedicati, può permettere una significativa riduzione dei costi associata ad un livello elevato di prestazioni e potenzialità di innovazione. Infatti, tale tecnologia è caratterizzata da costi relativamente bassi grazie alla sua ampia diffusione e ai grandi volumi di mercato. Essa, inoltre, è in costante e rapido sviluppo per supportare l'evoluzione dei sistemi informatici e di telecomunicazioni,garantendo la sostenibilità futura dell'approccio, e permette di basarsi su un'infrastruttura aperta e standardizzata, favorendo la convergenza dei servizi che si vogliono fornire all'interno dell'abitazione ed al tempo stesso condividerne i costi di implementazione.

Oltre alle funzionalità di automazione e gestione, l'introduzione di un sistema in grado di controllare in modo capillare le funzioni dell'abitazione consente inoltre di ricavare informazioni di grande rilevanza ai fini del monitoraggio delle condizioni ambientali e della salute dei residenti. In prospettiva, è possibile ipotizzare funzioni di analisi comportamentale, utili all'introduzione di funzionalità adattative o al riconoscimento di condizioni di anomalia potenzialmente connesse a patologie incipienti o in corso di evoluzione, al declino associato a malattie legate all'età o alla disabilità. L'utilizzo del protocollo IP, come livello di trasporto per le informazioni del sistema sviluppato, lo rende nativamente integrabile con una serie sempre più vasta di servizi, che si stanno spostando verso la direzione dell'integrazione con le tecnologie informatiche, quali ad esempio la telefonia (con il VoIP, ovvero Voice over IP) e l'intrattenimento (con l'IPTV, ovvero la TV su IP ed il DVB, cioè il Digital Video Broadcasting).

La struttura di questa tesi è pensata per fornire inizialmente una panoramica delle necessità cui un sistema di automazione deve dare una risposta (capitoli 1 e 2), per proseguire poi con una descrizione di alcuni dei principali sistemi attualmente disponibili (capitolo 3), continuando con una descrizione delle tecnologie alla base del sistema progettato (capitolo 4). Quindi viene descritto il sistema vero e proprio (capitolo 5), il modulo chiave su cui esso si basa (capitolo 6), l'ambiente di sviluppo e collaudo (capitolo 7). In seguito viene descritta un'installazione pilota, che dimostra la fattibilità dell'approccio (capitolo 8) e vengono quindi tratte le conclusioni e descritti gli sviluppi futuri attualmente previsti (capitolo 9).

Capitolo 1

Cosa si può chiedere ad una casa?

Un uomo percorre il mondo intero
in cerca di ciò che gli serve
e torna a casa per trovarlo.

– George Moore

La casa è un luogo centrale della vita della maggior parte delle persone. È un luogo dove riposare, rilassarsi, godersi un ambiente confortevole, sentirsi al sicuro. Perché tutto questo sia possibile è necessario che una serie di requisiti siano soddisfatti, altrimenti il luogo nei nostri sogni può rivelarsi una delusione continua. Tutto ciò conduce alla conclusione che noi tutti chiediamo molto alle nostre case, e chi ha difficoltà di ordine fisico o psichico ha un'esigenza ancora superiore di sentirsi a proprio agio nella propria abitazione. In questo capitolo verranno ricordati una serie di aspetti che sono di fondamentale importanza nel vivere la propria casa: esigenze cui l'automazione domestica cerca di trovare sempre migliori risposte ogni giorno.

1.1 Sicurezza

La sicurezza è un'esigenza primaria cui la casa deve rispondere. Sicurezza è inteso sia come protezione dalle possibili insidie che si possono manifestare all'interno del-

l'edificio, quali incendi ed allagamenti, sia come segnalazione di intrusioni da parte di estranei.

1.1.1 Ambientale

All'interno delle nostre case, nonostante tutti gli accorgimenti sempre più presenti per ridurre i pericoli, si annidano diverse insidie, legate ai materiali ed ai dispositivi che utilizziamo tutti i giorni. Fornelli, stufe, lavatrici e lavastoviglie sono elettrodomestici ormai entrati nella vita quotidiana, che però in caso di incuria, distrazione o malfunzionamenti, posso anche rappresentare dei pericoli per le persone. Infatti sia i fornelli che le stufe portatili possono essere fonte di incendio, se non correttamente utilizzate; lavatrici e lavastoviglie, in caso di guasto, possono essere causa di allagamenti dei locali in cui sono installate. Questi sono solo un paio di esempi delle possibili insidie, dovute a elettrodomestici di uso comune, cui possiamo andare incontro nella vita di tutti i giorni. È evidente come una casa per essere veramente un luogo sicuro abbia l'esigenza di ridurre al minimo i rischi connessi a queste situazioni.

In questo contesto l'automazione domestica fornisce non solo la possibilità di avvisare, anche a distanza, gli abitanti dell'edificio della condizione di rischio o di pericolo, ma anche di intervenire attivamente per prevenire l'aggravarsi dei danni. Ad esempio un sistema di rilevazione delle condizioni di allagamento è in grado di rilevare la condizione anomala, quando sono presente ancora pochi millimetri di acqua sul pavimento, localizzati nellŠintorno di un sensore opportunamente collocato, e può interrompere l'erogazione di acqua all'elettrodomestico o al locale dove l'allagamento si è verificato, limitando quindi moltissimo i danni correlati, mentre contemporaneamente viene segnalata la condizione di anomalia, mediante allarmi locali e remoti. In modo del tutto analogo un sistema di rilevazione di fumo può segnalare che qualcosa sta bruciando in un ambiente ed intervenire interrompendo il flusso di combustibili verso l'abitazione, per ridurre i rischi di esplosione o di aggravamento dell'incendio, ed al tempo stesso segnalare la condizione di allarme.

1.1.2 Anti-effrazione

La sicurezza del domicilio è un'esigenza primaria, sia quando ci si trova all'interno, sia quando si è lontani. Per garantire l'inviolabilità della propria abitazione è necessario dotarsi di sistemi che rendano quanto più difficoltoso possibile l'accesso a persone non autorizzate, ricorrendo a mezzi fisici quali recinzioni, porte blindate, inferriate, ecc. Ma tutto questo rappresenta solo una parte della soluzione, in quanto nessuno di questi sistemi rappresenta una barriera insuperabile. Per completare la protezione è quindi necessario aggiungere un sistema di rilevazione dell'intrusione, per segnalare se questi sistemi falliscono. La funzione del sistema è in genere duplice: da un lato rappresenta un deterrente, in quanto i sistemi di segnalazione acustica (sirene) hanno la funzione di allertare quante più persone possibili dell'effrazione in atto e di mettere così in fuga l'intruso, ma unitamente a questo il sistema in genere esegue una serie di segnalazioni sia al proprietario, sia eventualmente alle forze dell'ordine, per notificare la violazione.
Questo tipo di sistemi si avvale di vari tipi di sensori, dai contatti magnetici che rilevano l'apertura degli infissi, ai sensori di movimento a infrarossi passivi (comunemente noti come PIR, ovvero Passive Infra Red), che rilevano quando un corpo caldo si trova in movimento in un ambiente controllato, a sensori di rottura vetri, ecc.

1.1.3 Videosorveglianza

L'utilizzo di telecamere collegate ad un sistema a circuito chiuso può essere utilizzato al fine di registrare le attività nei pressi dell'abitazione. Ciò costituisce da un lato un deterrente nei confronti dell'effrazione stessa, dall'altro uno strumento utile, se viene eseguita una registrazione remota, per identificare le modalità di infrazione ed eventualmente i colpevoli.
L'utilizzo di sistemi di videosorveglianza in genere richiede la presenza di personale addetto alla sorveglianza che sia in grado di reagire prontamente in caso di accesso non autorizzato.

1.2 Comfort

Per godersi appieno la casa è necessario che questa possa garantire un ambiente confortevole ed accogliente. Questo obbiettivo può essere raggiunto solamente se una serie di requisiti sono raggiunti, non tutti di natura tecnologica ovviamente. Fra i requisiti che un sistema di controllo tecnologico può gestire i principali sono legati al condizionamento della temperatura e dell'illuminazione, oltre alla possibilità di automatizzare infissi e serramenti.

1.2.1 Controllo riscaldamento e raffrescamento (HVAC)

Il controllo del riscaldamento è stata una delle prime applicazioni di quella che potremmo definire la "domotica di livello 0", ovvero l'automazione indipendente dei sistemi tecnologici della casa. Nella sua accezione minima anche un semplice termostato permette di mantenere una temperatura relativamente costante nella casa. Con il passare degli anni questi dispositivi sono evoluti in sistemi di controllo che prendono in considerazione le ore della giornata ed i giorni della settimana, permettendo di risparmiare sul riscaldamento quando nessuno si trova nell'abitazione o di avere un profilo di temperatura che si adatta alle attività normalmente svolte nel periodo di tempo selezionato. Questo controllo ora può prendere in considerazione anche dati aggiuntivi, quali la temperatura esterna, il livello di insolazione della singola stanza, ed ottimizzare così l'impiego di energia sfruttando sistemi di parzializzazione della distribuzione del calore in modo più capillare. Tutto questo conduce a risparmi energetici significativi.

L'uso di nuovi sistemi di riscaldamento e raffrescamento combinati, basati ad esempio su pompe di calore, permette di avere un'efficienza maggiore rispetto ad altri sistemi tradizionali, e sfruttando un coordinamento a livello di abitazione possono essere molto efficienti anche dal punto di vista del comfort degli abitanti, potendo anche controllare il livello di umidità atmosferica.

1.2.2 Illuminazione

L'illuminazione degli ambienti è un punto fondamentale per un corretto sfruttamento degli ambienti abitativi. Un'illuminazione inadatta all'attività svolta può essere molto fastidiosa ed al tempo stesso essere inutilmente dispendiosa.
Al fine di razionalizzare i consumi è necessario utilizzare lampade dall'elevata efficienza energetica, quali ad esempio le lampade fluorescenti, che hanno un'efficienza energetica in genere cinque volte superiore a quelle ad incandescenza. È però da notare che questo tipo di lampade hanno condizioni operative molto diverse da quelle tradizionali e quindi anche l'utilizzo deve essere leggermente differente, per non ridurne drasticamente la vita utile. Un sistema di controllo automatico correttamente configurato può aiutare a rispettare le condizioni ottimali di utilizzo.
L'uso di regolatori di luminosità può essere utile per ridurre i consumi di lampade tradizionali (che saranno però progressivamente abbandonate entro il 2020 secondo una recente norma dell'Unione Europea), quando vengono utilizzate ad integrazione della luce naturale proveniente dall'esterno, oppure possono essere usati per regolare l'illuminazione ottimale negli ambienti di fruizione delle trasmissioni televisive.

1.2.3 Automazione infissi

Le automazioni degli infissi possono essere una comodità per chiunque, ma per coloro che hanno problemi motori possono rappresentare un vero sollievo nella vita quotidiana, o una necessità inderogabile ai fini dell'autonomia. L'automazione può riguardare le tapparelle, le imposte, le finestre o anche le porte, interne ed esterne. Il controllo di queste automazioni può essere fatto in vari modi, a seconda di quale interfaccia si addice meglio all'utilizzo da parte dell'utente. Possono essere ad esempio semplici pulsanti posti nei pressi dell'infisso, telecomandi, rivelatori di movimento, sistemi a controllo vocale, ...

1.3 Gestione dell'energia

Il tema energetico sta prepotentemente facendo il suo ingresso in ogni momento della nostra vita, dal controllo efficiente del riscaldamento alla razionalizzazione dell'illuminazione, controllo dello spreco di acqua all'utilizzo intelligente degli elettrodomestici.
Queste tematiche hanno impatto primario sulle spese per la gestione della casa, ma hanno collettivamente un impatto non trascurabile su sistemi più ampi e complessi, sia di tipo tecnologico (ad esempio il sistema di generazione e distribuzione dell'energia elettrica), sia di tipo naturale (inquinamento ambientale). Anche una corretta (e dettagliata) contabilizzazione dell'energia può essere un utile ausilio per il risparmio energetico.

1.3.1 Gestione intelligente del sistema di illuminazione

Oltre ad un controllo che permetta il massimo comfort possibile, un sistema di automazione domestico può permettere di ridurre gli sprechi di energia in modo significativo, ad esempio spegnendo le luci nei locali dove non è presente nessuno da una certa quantità di tempo, riducendo l'illuminazione se quella proveniente dall'esterno e sufficiente, avvisando ad esempio se si accendono le luci con le tapparelle abbassate quando all'esterno è presente luce sufficiente ad illuminare la stanza. Possono essere accese automaticamente le luci quando una persona si alza dal letto durante la notte e molte altre situazioni possono essere prese in considerazione. Questi sono solo esempi di quello che è possibile fare, e quindi come tali non sono applicabili alla totalità delle situazioni, come sono possibili ulteriori e più complessi servizi che possono essere implementati, se il sistema di controllo è sufficientemente flessibile.

1.3.2 Coordinamento del sistema di riscaldamento e raffrescamento

In modo analogo al controllo di illuminazione è possibile pensare a servizi complessi di razionalizzazione del riscaldamento e raffrescamento, al fine di ridurre gli sprechi, per esempio avvisando se si aprono le finestre in un locale dove è attivo il sistema

di condizionamento e quindi disattivandolo, se previsto. Oppure è possibile pensare all'impostazione di profili di riscaldamento e raffrescamento che riducano al massimo gli sbalzi termici e quindi lo stress per l'organismo degli occupanti.

È possibile controllare in modo capillare la distribuzione del calore anche in relazione al calore disperso o assorbito verso l'esterno, ad esempio per sfruttare il calore assorbito dai locali esposti a sud nelle ore diurne dei mesi invernali, evitando di fornire calore non necessario. Questo ovviamente richiede l'utilizzo di sonde termiche in tutti i locali, per ottenere il controllo capillare descritto.

1.3.3 Coordinamento degli elettrodomestici

Gli elettrodomestici in una casa sono ormai in numero sempre più rilevante. Coordinarne il funzionamento, e con esso l'assorbimento, permette di ottenere un risparmio in termini di massima potenza contrattuale richiesta ed anche un risparmio in termini di costo dell'energia consumata, in caso di tariffe biorarie, in quanto è possibile fare in modo che i sistemi di controllo facciano attivare, ad esempio, la lavatrice e la lavastoviglie nelle ore notturne, quanto l'energia è meno costosa, anche senza l'intervento dell'utente, razionalizzando quindi i consumi. Il coordinamento è anche fondamentale per le funzioni anti black-out di seguito descritte.

1.3.4 Funzioni anti black-out

Quando il consumo di energia elettrica supera la massima potenza contrattuale il contatore dell'energia interrompe l'erogazione. È una situazione della quale siamo bene o male stati tutti vittime almeno una volta nella vita. Oltre ad essere una seccatura, perché ci costringe a recarci dove è installato il contatore per riarmare l'interruttore, è un inconveniente che può essere fonte di infortuni, in quanto, a seconda delle situazioni, può costringere a fare diversi piani di scale o a muoversi nell'oscurita per raggiungere il contatore stesso, che in genere non si trova all'interno dell'abitazione. AL fine di prevenire questo tipo di situazioni un opportuno coordinamento dei dispositivi che assorbono grandi quantità di energia è necessario. Un sistema di questo tipo consiste in genere di un rilevatore dell'assorbimento dell'energia, più o meno suddi-

viso per gruppi di elettrodomestici, ed un sistema di controllo degli elettrodomestici stessi, che può colloquiare direttamente con elettrodomestici "intelligenti" o interagire con altri elettrodomestici "tradizionali" mediante relè, che intercettano direttamente la presa elettrica, permettendo l'esclusione dell'utenza. Una definizione delle priorità fra i carichi permette di razionalizzare l'intervento al fine di minimizzare l'impatto della parzializzazione all'avvicinarsi del consumo alla potenza contrattuale massima.

1.3.5 Gestione delle fonti di energia alternative

L'integrazione di fonti di energia alternative nel sistema energetico dell'abitazione è un'alternativa che viene ultimamente incoraggiata come risposta ai crescenti problemi ecologici ed economici. In particolare l'integrazione di pannelli fotovoltaici è attualmente in fase di lenta diffusione anche nell'utenza domestica. Questo tipo di sistemi, per operare in modo efficiente, necessitano di sistemi di controllo che ne regolino l'immissione di energia nella rete elettrica dell'abitazione ed anche in quella nazionale, se il gestore lo consente.
Un'accurata pianificazione del consumo e sistemi di immagazzinamento temporaneo dell'energia, ad esempio mediante batterie ad alta efficienza, possono ridurre al minimo gli sprechi di energia, massimizzando quindi i vantaggi che possono essere tratti dall'impiego di queste nuove tecnologie.

1.4 Contenuti multimediali

Le forme di intrattenimento che possono essere fruite in casa sono molteplici, dalla televisione alla musica, ai videogiochi, ... Queste attività possono essere rese più efficaci e gratificanti se sono correttamente integrate in un contesto abitativo che tenga conto delle possibilità di distribuzione delle informazioni, delle immagini e dei suoni.

1.4.1 Televisione e contenuti on-demand

L'intrattenimento televisivo è ormai parte integrante della nostra vita di tutti i giorni. Gli apparecchi televisivi sono oggi elementi quasi immancabili nelle abitazioni moderne, però anch'essi sono evoluti verso forme e caratteristiche innovative. Negli ultimi anni non sono più a tubo catodico, ma sono "piatti", ovver basati su tecnologie LCD o plasma. Hanno aree visibili maggiori e spessori inferiori, ma anche i requisiti energetici sono cambiati, non sempre riducendosi... Anche i sistemi di diffusione acustica sono diventati più evoluti, coinvolgendo spesso sistemi multicanale (sistemi Dolby Sorround 4+1, 5+1, ...).

Al fine di godere appieno dell'esperienza visiva ed uditiva questi sistemi devono essere correttamente installati ed anche i sistemi di illuminazione dovrebbero essere studiati per evitare inopportune riflessioni o illuminazioni fastidiose.
Inoltre negli ultimi anni si stanno diffondendo sistemi di distribuzione dei contenuti multimediali non più basati sui canali tradizionali, quali le antenne per le trasmissioni terrestri e satellitari, ma anche tramite internet. Per questo motivo oltre ai normali videoregistratori e lettori di DVD (Digital Versatile Disk) si stanno anche diffondendo i cosiddetti "media center", ovvero piccoli elaboratori collegati direttamente alla rete Internet o ad una rete locale (LAN, Local Area Network) dalla quale attingono le informazioni che vengono poi trasmesse al televisore ed ai sistemi Hi-Fi (High Fidelity, alta fedeltà).

1.4.2 Diffusione della musica

La diffusione sonora in più ambienti è una funzione che, pur non essendo particolarmente diffusa, può essere annoverata fra le possibilità di entertainment offerte da un sistema abitativo evoluto. I metodi possono basarsi su vari e diversi sistemi, che si distinguono in base al tipo di trasporto delle informazioni (digitale o analogico) e per la possibilità o meno di avere diversi canali a seconda degli ambienti.

1.5 Comunicazione

La nostra società viene a volte definita “società dell’informazione”, altre volte “società della comunicazione”. Questo connubio è senza dubbio di grande importanza nel contesto moderno. I mezzi di comunicazione sono sempre più pervasivi ed è sempre più vero se pensiamo alla diffusione attuale della telefonia cellulare e di Internet.
La comunicazione si sta spingendo sempre più da un rapporto di tipo scritto o parlato a contesti più multimediali, che includono anche immagini o altri tipi di dati applicativi, che vengono condivisi fra gli interlocutori anche grazie alle elevate velocità di comunicazione, che permettono di scambiarsi anche grandi moli di dati in breve tempo.

1.5.1 Telefonia e videotelefonia

La telefonia è un servizio che ormai viene dato per scontato all’interno di una casa, quindi viene spesso sottovalutato. L’utilizzo di sistemi evoluti all’interno dell’abitazione può consentire di rendere il telefono un oggetto intelligente, in grado non solo di permettere una comunicazione vocale con un interlocutore esterno o interno all’abitazione, ma anche una comunicazione video, oppure di inviare SMS (Short Message System), ma anche di controllare alcune funzioni della casa, trasformando quindi il telefono in un un semplice pannello di controllo. L’utilizzo di tecnologie di tipo VoIP (Voice over IP, trasmissioni telefoniche su rete dati) permette di beneficiare di risparmi in termini di spesa per le telefonate, specialmente se indirizzate verso destinazioni estere.

1.5.2 Citofonia evoluta

La citofonia, come la telefonia, può essere integrata mediante immagini provenienti dal posto di chiamata e, se basata su sistemi evoluti, anche di ricevere l’informazione sul proprio PC (Personal Computer), su terminali mobili, o di registrare le chiamate, proprio come se si trattasse di una segreteria telefonica, per sapere chi ha suonato

anche se si è fuori, o addirittura di ricevere le informazioni in tempo reale sul proprio telefono cellulare anche se non si è a casa.

1.6 Assistenza

Le possibilità messe a disposizione dai sistemi di comunicazione evoluti permettono di concepire un modello di assistenza alla persona differente da quello finora considerato. I sistemi di diagnostica a distanza permettono di avere diagnosi sullo stato di salute anche da parte di medici a distanza, con un aumento complessivo dell'efficienza e della rapidità di risposta ed al contempo con una riduzione del numero di spostamenti da parte di pazienti e medici.
Le richieste di soccorso possono essere automatizzate utilizzando sistemi di rilevazione di condizioni biologiche anomale, rendendo più sicura la vita di persone che vivono sole o che devono rimanere sole per prolungati periodi di tempo durante la giornata.

1.6.1 Richieste di soccorso

Quando una persona si trova sola nella propria abitazione, un sistema semplice ed eventualmente automatico per la richiesta di soccorso può essere molto utile. Questo permette a persone con problemi di salute non gravi di rimanere nelle proprie abitazioni in autonomia, avendo però una sistema che rassicura sia la persona che, eventualmente, i suoi parenti. Questo tipo di servizio può essere configurato per collegarsi con i parenti, i vicini o centri servizi, che si occupando di inviare i soccorsi adeguati in base alle necessità.
I sistemi automatici di chiamata devono essere presi in considerazione solo in casi particolari, in quanto i falsi allarmi sono un problema che deve essere attentamente considerato in fase di installazione e configurazione, sia del sistema che del servizio nel suo complesso.

1.6.2 Telemedicina

La possibilità di collegare normali strumenti di autodiagnosi ai PC permette di realizzare servizi di telemedicina che possono essere utilizzati anche nelle singole case, senza la necessità di personale infermieristico addestrato. Ad esempio è possibile rilevare personalmente parametri quali il peso corporeo, la pressione sanguigna e la glicemia ed inviare questi parametri al medico curante, perché possa intervenire prontamente in caso di anomalie, o anche solo al fine di un controllo più efficace dello stato di evoluzione di patologie croniche (spesso legate all'avanzare dell'età), quali l'ipertensione ed il diabete.

1.7 Convergenza

La grande maggioranza dei servizi descritti in questo capitolo hanno punti di contatto ed intersezione non trascurabili. In particolare molti servizi possono condividere diversi sensori ed attuatori, al fine di rendere più razionale ed efficiente l'intero sistema casa.

La convergenza fra questi servizi è possibile se viene realizzato un unico sistema di controllo che li realizzi e coordini nel migliore de modi. In questa ricerca è stata valutata la possibilità di utilizzare una sola rete di comunicazione per il trasporto delle informazioni relative a tutti questi diversi sistemi, sfruttando la rete per antonomasia: Ethernet.

Capitolo 2

Tecnologie Assistive

Non è tanto l'aiuto dei nostri amici ad aiutarci,
quanto la consapevolezza che essi ci aiuteranno.

– Epicuro

Progettare una casa è una responsabilità molto grande, poiché le scelte che vengono fatte in questa fase hanno un'influenza diretta su come la casa sarà vissuta, ora ed in futuro. Considerare una serie di aspetti che riguardano la struttura architettonica ed impiantistica è fondamentale, al fine di permettere l'eventuale adattamento degli ambienti al presentarsi di condizioni nuove. Per questa ragione è nata una "filosofia" del "progettare per tutti" (Design For All), che richiede ai progettisti uno sforzo per considerare quanto più possibile le esigenze non solo degli attuali occupanti degli edifici, ma anche di quelli futuri.

Le tecnologie assistive sono un insieme di tecnologie che possono fornire supporto a quelle fasce di popolazione che hanno difficoltà correlate all'avanzare dell'età o ad altre patologie, che ne limitano le possibilità di godimento di un edificio non correttamente strutturato. Queste tecnologie possono essere molto semplici, basate su sensori ambientali ed attuazioni meccaniche degli infissi, o essere più complesse, sfruttando ad esempio sensori e trasmettitori indossabili. In questo capitolo verranno ricordati i vantaggi che possono derivare dall'automazione domestica in questa sfida

continua.

2.1 Progettare per tutti

Progettare le abitazioni prendendo in considerazione le esigenze della maggior parte possibile di individui è ormai un requisito fondamentale. Quando si pensa a come realizzare determinati servizi e infrastrutture è necessario progettare "per tutti", ovvero considerando le esigenze degli occupanti previsti e di quelli futuri, che possono avere vari tipi di limitazioni, che devono essere rese quanto più possibile ininfluenti nelle normali operazioni quotidiane. Questo implica l'abbattimento di ogni barriera architettonica, ovviamente, ma si deve estendere il concetto anche ad altri particolari, quali il posizionamento di prese di corrente ed interruttori, la predisposizione di automazioni di infissi e varchi e molti altri accorgimenti, che possono rendere la vita più facile e confortevole a tutti, ma possono essere fondamentali per chi ha particolari esigenze.

2.2 La casa come elemento fondamentale di autonomia

La casa è un punto di riferimento fondamentale nella vita di ogni persona. Per molti, vivere come persone indipendenti nella propria abitazione rappresenta un punto fondamentale per la propria sicurezza ed autostima. Perché sia possibile vivere in modo autonomo in una casa è necessario che questa possa fornire tutto (o quasi) il supporto necessario ai suoi occupanti. Per questo il tipo e la complessità dei servizi richiesti dipende dalle esigenze di chi la vive, e per questo, nell'ottica del "design for all", è fondamentale che la casa sia, quanto meno, predisposta per il supporto delle necessità di una vasta gamma di persone, di varia età e differenti livelli di autonomia psico-fisica.

Per questi motivi, più la casa risulta essere "intelligente" e maggiore sarà il livello di autonomia che possono aspettarsi le persone che vi abitano. Inoltre anche con l'avanzare dell'età, l'autonomia potrà essere mantenuta per un periodo di tempo più lungo rispetto a quello atteso se l'abitazione fosse di tipo "tradizionale". Questa

possibilità di permanenza nel proprio ambiente domestico ha vantaggi in termini psicofisici, sia per gli occupanti, sia per i familiari ed incidentalmente comporta un non trascurabile risparmio in termini economici, rispetto all'esigenza di un trasferimento in una residenza protetta o in altra struttura assistenziale [2, 3].

2.3 Studio del comportamento mediante sensori non invasivi

Lo studio del comportamento degli abitanti di un edificio può avere diversi vantaggi, in termini di comfort complessivo ed in termini clinici. Perché questi benefici siano però veramente percepiti, è necessario che i dati siano acquisiti senza perturbare l'ambiente e le abitudini.

2.3.1 Perché studiare il comportamento?

Tutti i sensori che sono presenti nella casa, se utilizzati in modo coordinato, permettono di rilevare dei profili di comportamento, ma perché dovremmo farlo? Le risposte a questa domanda possono essere molte, ma in particolare ci soffermeremo su due aspetti: quello della sicurezza e quello dell'analisi clinica.

Sicurezza predittiva

La creazione di profili di abitudini da parte del sistema di automazione è un'attività di particolare complessità. Essa infatti prevede la possibilità di estrarre indicatori di attività globali o specifici, relativi al modo di vivere la casa tipico di ogni individuo [4].
Quest'attività di ricerca è ancora in fase altamente sperimentale, ma sembra che possa effettivamente condurre allo sviluppo di algoritmi di elaborazione delle informazioni che provengono dalla miriade di sensori elementari normalmente disseminati nell'abitazione, al fine di estrapolare indici e relativi intervalli di variabilità. La deviazione imprevista e decisa da tali schemi può essere impostata come una condizione di atten-

zione. Tale condizione può essere riportata direttamente all'utente o a chi si occupa della "sorveglianza" dell'utente, siano essi i familiari o personale sanitario.

La capacità del sistema di apprendere le abitudini potrebbe, in teoria, essere anche utile per ridurre la necessità di compiere azioni ripetitive da parte di persone con particolari tipi di patologie debilitanti, che quindi ne potrebbero avere un vantaggio in termini di minore affaticamento e minori probabilità di errori. Ad esempio se fosse possibile per il sistema determinare che una persona, quando si alza dal letto fra le ore otto e le ore nove del mattino, nel giro di pochi minuti accende la televisione e poi la macchina per fare il caffè, esso potrebbe trarne una sorta di "regola" e svolgere autonomamente alcune o tutte queste funzioni, quando ne ricorrono le condizioni. Ovviamente si tratta di funzioni banali e probabilmente di scarsa utilità effettiva, ma possono dare un'idea delle potenzialità dell'approccio.

Monitoraggio delle derive delle abitudini

Attualmente sono in svolgimento studi clinici per la determinazione di parametri di attività, che possano essere valutati al fine di rilevare malattie incipienti dalla modificazione delle abitudini delle persone [5, 6].
La strutturazione di un sistema in grado di registrare ed elaborare, eventualmente in tempo reale, queste informazioni al fine di estrapolarne i parametri utili può essere considerato un notevole passo nella direzione della creazione di indicatori di attenzione, che possono essere utili nella prevenzione o nella diagnosi precoce di varie malattie, sia dell'apparato motorio, sia cardiovascolare, sia di altre patologie.

Un sistema di questo tipo ha il vantaggio di eseguire valutazioni oggettive e di essere sensibile anche a derive delle abitudini tanto lente da sfuggire agli operatori quotidianamente a contatto con gli utenti, in quanto queste possono sfuggire a chi ha modo di abituarsi involontariamente alle quotidiane attività delle persone, ma un sistema opportunamente configurato è in grado, teoricamente, di rivelare anche queste derive, quando arrivano ad avere significato per gli studi in atto [7].

2.3.2 I sensori

Nelle nostre abitazioni sono presenti un gran numero di sensori ed attuatori, con i quali interagiamo quotidianamente in modo ormai molto naturale. Ci siamo abituati nel tempo a vedere vari tipi di sensori di movimento utilizzati nei sistemi antifurto, sensori di fumo, contatti magnetici su porte e finestre. Ci stiamo abituando a vedere sensori di allagamento nei locali dove sono presenti elettrodomestici, sensori di gas collegati ad elettrovalvole per intercettare i combustibili in caso di fughe.
Diamo ormai per scontati gli interruttori delle luci, i sensori di temperatura per la regolazione dell'impianto di riscaldamento, i sensori di luminosità con i quali vengono controllate le luci esterne con funzionalità crepuscolare.
Interagiamo quotidianamente con i telecomandi di svariati elettrodomestici, dalla televisione allo stereo, ed ultimamente anche alle console ludiche.
Tutti questi dispositivi rappresentano di fatto sensori con cui interagiamo in modo del tutto naturale, e quindi sono sensori definibili come non invasivi, perché non sono percepiti come estranei alla vita quotidiana.
Ciò che risulta importante notare è che se un sistema di automazione deve controllare sostanzialmente la maggioranza, se non la totalità, dei servizi tecnologici forniti all'abitazione, è anche necessario che esso interagisca, in modo più o meno complesso, con tutti questi sensori, al fine di ricavarne le informazioni necessarie al funzionamento che noi ci attendiamo. Al contempo, però, un sistema sufficientemente aperto e flessibile può utilizzare questi sensori, oltre che per implementare le funzioni primarie e più banali, anche per rilevare abitudini e comportamenti. Ciò consente di sviluppare servizi evoluti, che possono scaturire dall'analisi dello stato di più sensori, che sono stati posti per motivi diversi nell'ambiente. Il tutto senza che l'utente debba necessariamente esserne al corrente o debba modificare le proprie abitudini di interazione con le interfacce cui è ormai abituato.
In questo contesto i semplici interruttori della luce possono essere utilizzati come indicatori di attività nella stanza, come lo possono essere i sensori di movimento normalmente utilizzati per la rilevazione delle intrusioni. Il monitoraggio dei consumi elettrici, effettuato in modo più o meno capillare, può essere utilizzato per determinare se si verificano situazioni di anomalia, quali ad esempio un consumo prolungato

molto più del solito da parte di un particolare elettrodomestico [8, 9, 10].

2.4 Sensori indossabili

L'utilizzo di sensori indossabili, ovvero dispositivi sensibili che vengono ingegnerizzati al fine di poter essere portati con se dalle persone, senza che provochino alterazioni delle abitudini quotidiane, permette di fornire servizi evoluti volti alla diagnostica clinica, alla prevenzione delle situazioni di rischio ed alla pronta segnalazione delle condizioni di emergenza che possono coinvolgere la persona che li porta.
L'utilizzo di questi sensori risulta tanto più invasivo, tanto più è complesso l'oggetto da indossare e quanto meno questo è compreso dalla persona che lo indossa.
Un semplice sensore in grado di determinare l'accelerazione istantanea della persona che lo porta può essere utilizzato per una molteplicità di funzioni, dalla rilevazione della caduta, all'analisi della camminata. Inoltre, integrando un pulsante per la richiesta di soccorso, è anche possibile farlo diventare un dispositivo di segnalazione di emergenza personale. L'aggiunta di un sistema di rilevazione della posizione all'interno dell'edificio può consentire di rendere più tempestivo l'intervento dei soccorsi in caso di necessità, ma può permettere di attivare anche altre funzioni più evolute, dal context awareness dell'ambiente nei confronti della persona, adattando cioè alcuni parametri ambientali, quali l'illuminazione ed il riscaldamento, in base alle persone che sono presenti, come alla segnalazione di allarme nel caso persone con problemi di orientamento si vengano a trovare in posizioni che risultano essere per loro anomale o pericolose [11, 12].

Capitolo 3

Breve storia delle tecnologie di automazione

La grande storia vera
è quella delle invenzioni;
sono infatti le invenzioni
che provocano la storia.

– Raymond Queneau

In questa sezione verranno descritti i principali approcci all'automazione domestica e di edificio utilizzati nel corso degli anni in vari contesti. Si cercherà di descriverne le caratteristiche principali e di evidenziarne punti di forza e limiti

3.1 L'approccio a sistemi indipendenti

Tradizionalmente, nelle abitazioni i sistemi tecnologici necessari sono stati trattati come sistemi autonomi, ciascuno con specifiche funzioni e con pochi o nessun punto di contatto gli uni con gli altri. Ad esempio il sistema di controllo del riscaldamento è a se stante, comprendente la caldaia, gli scambiatori di calore (termosifoni) ed il sistema di regolazione della temperatura, in genere un termostato. Un altro esempio

di sistema è quello anti-intrusione, che si compone di una varietà di sensori per la rilevazione dell'accesso o della presenza di intrusi, di una centrale di controllo e di un sistema di avvisatori sonori ed acustici. Un ulteriore esempio può essere il sistema di rilevazione incendi, come molti altri... Tutti questi sistemi sono in grado di operare in modo autonomo ed indipendente, al fine di assicurare ciascuno la funzione ad esso affidata. La loro gestione risulta però particolarmente inefficiente, in quanto è necessario che ciascuno di essi sia manutenuto in modo indipendente, supervisionato singolarmente e gestito secondo interfacce a volte molto dissimili. Inoltre non vi è nessun tipo di economia possibile che derivi dalla sovrapposizione di parti comuni ai sistemi, quali ad esempio le sirene di allarme o i sistemi di comunicazione a distanza delle condizioni di emergenza.

3.2 La supervisione comune

Un primo passo nella direzione dell'integrazione fra i vari sistemi è stata l'introduzione dei gestori di supervisione. Sebbene siano scarsamente diffusi a livello domestico, essi sono fondamentali in molti casi nell'automazione di edifici commerciali di medie e grandi dimensioni.
Questo tipo di sistemi consente di avere un quadro della situazione di tutti i sistemi tecnologici da un'unica postazione, consentendo una più rapida ed efficace gestione degli eventi correlati alla manutenzione o alle emergenze. Nonostante la supervisione comune, i singoli sistemi continuano ad operare in modo indipendente, ciascuno con le proprie specifiche funzioni. Non è ancora possibile ottenere una condivisione dispositivi o sottosistemi, in generale, ma si tratta di un importante passo nella direzione di una razionalizzazione delle risorse.

3.3 I sistemi a BUS

L'integrazione di più sistemi tecnologici in modo efficiente richiede che tutti i dispositivi coinvolti utilizzino un unico protocollo di comunicazione e siano gestiti da un solo sistema di controllo. Anche se i mezzi di comunicazione possono essere diver-

si, e l'intelligenza del sistema di controllo può essere distribuita su più dispositivi nel sistema, quando i dispositivi interagiscono direttamente fra loro e consentono di condividere le informazioni, allora si ha quello che viene definito un sistema a BUS, intendendo come BUS il mezzo di comunicazione (sia esso fisico o logico) che consente a tutti i componenti del sistema di scambiarsi le informazioni in modo diretto ed omogeneo.
Vari sistemi a BUS sono stati sviluppati nel corso degli anni, fin dalla metà degli anni '70. Nel tempo varie soluzioni sono state proposte e vari tentativi di standardizzazione sono stati avanzati, anche se finora nessuno di questi è effettivamente riuscito ad imporsi.
Di seguito sono descritti alcuni dei principali (e più diffusi) standard attualmente in commercio [13, 14].

3.3.1 X10

Il sistema di automazione X10 si basa su una tecnologia di trasmissione di informazioni che sfrutta la normale linea elettrica a tensione di rete.
Il marchio è registrato dalla X-10 Incorporated negli USA e dalla X-10 Home Controls Incorporated in Canada. I brevetti sono sviluppati dalla Pico Electronics Limited, Scozia, UK, ora parte della X10 ltd. [15].

Principio di funzionamento

In sintesi il protocollo si basa sulla sovrapposizione di brevi impulsi alla frequenza di 120 kHz, sincronizzati con il passaggio per lo zero della tensione di rete, alla tensione di rete stessa. Tali impulsi vengono trasmessi dai dispositivi di comando e ricevuti dagli attuatori. La presenza di un impulso in corrispondenza del passaggio per lo zero prima della semionda positiva e la successiva assenza nel successivo passaggio per lo zero prima della semionda negativa, viene interpretato come un 1 logico. La condizione duale viene interpretata come uno 0 logico.
Il protocollo prevede un pacchetto dati che include un preambolo, un identificativo dell'abitazione a 4 bit, un identificativo del codice o della funzione a 5 bit. Esiste

una variante su radiofrequenza del protocollo X10, che utilizza la frequenza radio a 310 MHz per il collegamento con dei telecomandi [16].

Punti di forza

Uno dei principali vantaggi del sistema X10 è la semplicità: l'utilizzo della rete di potenza per la trasmissione dei dati rende possibile la realizzazione senza ulteriori cablaggi di semplici controlli di illuminazione e di attivazione di semplici apparati, come sistemi di irrigazione e porte automatiche. L'utilizzo di altre interfacce evolute, quali sistemi di controllo vocale, telecomandi infrarossi o schede per personal computer, rendono possibile la realizzazione di sistemi più complessi.
L'indicizzazione dei dispositivi è effettuata mediante selettori rotanti manuali, che non richiedono alcuna competenza tecnica per poter essere configurati. Ciò li ha resi particolarmente diffusi fra gli hobbisti, specialmente negli USA.

Limiti

L'utilizzo della rete elettrica rappresenta anche uno dei maggiori limiti dell'approccio, non tanto per il mezzo in sé, quanto per le interferenze che questo mezzo comporta. Sulla rete elettrica sono normalmente presenti molte interferenze, dovute all'inserimento e disinserimento di vari carichi di potenza, quali motori elettrici e resistenze di riscaldamento, che perturbano fortemente l'alimentazione. Inoltre vi sono interferenze che possono provenire dalla rete elettrica esterna. Per questo motivo la comunicazione, per essere affidabile, deve avvenire a velocità molto contenute e con sistemi di identificazione degli errori di trasmissione, che però non sempre operano al meglio e quindi questo tipo di tecnologia ha un livello di affidabilità che, anche nelle ultime varianti, non è in generale comparabile con quello di altri sistemi che utilizzano mezzi di comunicazione dedicati o tecnologie di modulazione più moderne, quali ad esempio l'OFDM (Orthogonal Frequency Division Multiplexing).
La semplicità di installazione si coniuga con una estrema semplificazione del sistema di indirizzamento, che però limita il numero massimo di dispositivi controllabili all'interno dell'abitazione e richiede opportuni filtri che impediscano l'interferenza

con i sistemi elettrici di altre abitazioni, in quanto non è prevista una codifica univoca per gruppo di dispositivi, visto appunto il ridotto numero di dispositivi indirizzabili, e si fa quindi affidamento sul fatto che i segnali non possano superare il contatore di alimentazione dell'appartamento, in genere grazie anche ad opportuni filtri di rete.

3.3.2 BACnet

Il Building Automation and Control Networking Protocol (BACnet) [17, 18] è stato sviluppato specificamente per la gestione delle necessità relative all'automazione di edificio ed al controllo di sistemi di automazione di ogni dimensione. Lo sviluppo cominciò nel 1987 ad opera dell'American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE), per sopperire all'assenza di un protocollo che rispondesse alle esigenze di automazione definite da un comitato di progetto che aveva il compito di definire le specifiche di comunicazione fra i dispositivi degli aderenti al consorzio. Il primo rilascio delle specifiche è avvenuto nel 1995 ed è stato identificato come Standard ASHRAE 135-1995. Successivamente lo standard è stato approvato dall'ANSI ed è quindi diventato ANSI/ASHRAE 135-2005. Sono seguite ulteriori revisioni nel 2001 e nel 2004. Nel 2003 lo standard è stato inserito fra gli standard ISO (International Standard Organization) e registrato come ISO 16484, del quale ora sono disponibili varie revisioni, l'ultima è del 2007 (ISO 16484-5:2007). Nel 2003 lo standard ha anche iniziato il percorso di registrazione presso il CEN (Comité Européen de Normalizazion), percorso che si è concluso con la registrazione dello standard EN ISO 16484, la cui ultima revisione è del 2008 (EN ISO 16484-5:2008). BACnet è stato anche adottato come standard da altre Nazioni, quali la Korea.
Lo standard è aperto e gratuito: non sono richieste royalty di nessun genere, né l'iscrizione ad un consorzio per poter produrre o utilizzare dispositivi conformi alle specifiche del protocollo. È sufficiente acquistare le specifiche presso uno degli enti che le hanno standardizzate.
Esistono gruppi di interesse che svolgono parti attive nel miglioramento del protocollo, nella promozione dello stesso e delle attività di istruzione in tutto il mondo.

Principio di funzionamento

In teoria il protocollo di comunicazione può essere trasmesso su qualunque mezzo, ma solo alcuni sono stati standardizzati, al fine di ottenere una più alta probabilità di corretta comunicazione fra dispositivi di diversi produttori. Attualmente sono contemplate le seguenti opzioni di rete standard: Ethernet (ISO 8802-3, IEEE 802.3), ARCNET (ATA/ANSI 878.1), LonTalk (ANSI/CEA 709.1) oltre a due proprietarie: Master-Slave/Token-Passing (MS/TP) su EIA-485 e Point-To-Point (PTP) su EIA-232. Lo standard proprietario MS/TP, progettato ad hoc per questa applicazione,

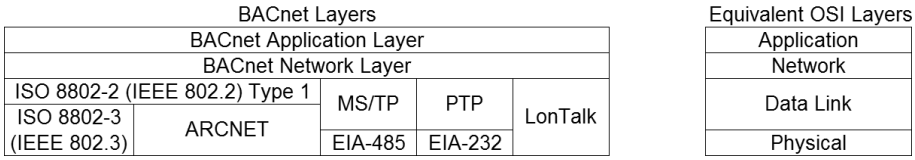


Figura 3.1: Stack BACnet confrontato con la porzione di stack ISO/OSI.

è stato concepito per permettere ai produttori di dispositivi di realizzare una rete a costi competitivi con altri standard proprietari, in generale senza richiedere specifici chip per l'interfacciamento di rete, potendo utilizzare i microcontrollori comunque necessari all'applicazione. Anche per questo lo standard fisico sul quale poggia è l'EIA-485. Lo standard PTP è invece concepito per una comunicazione full-duplex con un modem per l'accesso remoto al sistema dell'edificio.
In generale in un'installazione sono presenti diversi mezzi di comunicazione, collegati fra loro mediante gateway. Usualmente si hanno più tronconi collegati ai vari dispositivi mediante reti di tipo MS/TP [19] o LonTalk ed una dorsale realizzata mediante Ethernet o ARCNET [20].

Il riconoscimento dell'ampia e crescente diffusione dello standard IP in molte applicazioni abitative e la diffusione di internet ha portato all'inizio del 1999 alla definizione dei una nuova implementazione dello standard: il BACnet/IP. Tale implementazione consente di utilizzare il livello IP (o UDP) come livello di trasporto, senza la necessità di gateway. Ciò permette una maggiore efficienza delle comunicazioni e l'utilizzo diretto di Internet come mezzo di comunicazione per le funzioni di supervi-

sione. Il tutto è reso possibile dall'introduzione di una "BACnet Virtual Link Layer" (BVLL). Le specifiche di questa implementazione sono ora descritte nell'Annex J dello standard ANSI/ASHRAE 135-2004.

Il livello applicativo dello standard lascia la massima libertà di implementazione interna dei dispositivi. Deve quindi garantire l'interoperabilità, definendo un'interfaccia chiara ed uniforme fra gli stessi. A questo scopo attualmente definisce 25 tipi differenti di oggetti, fra i quali: "Binary Input", "Binary Output", "Analog Input", "Device", "Schedule", ... Le funzioni di ciascun oggetto BACnet sono standardizzate e definiscono quindi le informazioni fornite dall'oggetto e le azioni che esso può compiere. Di tutti gli oggetti il solo oggetto obbligatorio per ogni dispositivo è l'oggetto "Device". Attualmente gli oggetti definiti sono sufficienti a descrivere praticamente ogni funzione sia necessario rendere disponibile nell'automazione di un edificio. Ogni oggetto contiene una certa quantità di informazioni, al fine di autodocumentare le proprie funzioni al sistema di supervisione.
Lo standard si basa su un modello di tipo "Client-Server" e definisce quindi 40 differenti servizi, che vengono utilizzati per lo scambio di informazioni fra i vari oggetti del sistema complessivo. Questi servizi sono suddivisi in cinque categorie: "Alarm and Event Services", "File Access Services", "Object Access Services", "Remote Device Management Services" e "Virtual Terminal Services". Fra i servizi per l'accesso agli oggetti vi sono anche i servizi (funzioni) per la lettura e scrittura delle proprietà, mediante i quali si interagisce direttamente con gli oggetti e quindi con i dispositivi ad essi associati.

Sono previsti tre diversi tipi di notifica della variazione delle grandezze di interesse verso il sistema di supervisione, utilizzate per la segnalazione della variazione di parametri, come per la segnalazione di allarmi. La prima modalità ("Intrinsic Reporting") prevede la segnalazione di condizioni specifiche (ne sono state definite finora 9, fra le quali "OUT_OF_RANGE" e "CHANGE_OF_STATE") di proprietà specifiche di ciascun oggetto. La seconda ("Algorithmic Change Reporting") prevede che uno specifico oggetto di tipo "Event Enrollment" generi le notifiche al variare di una qualunque delle proprietà dell'oggetto preso in considerazione. Ciascuno di questi

due tipi di notifica si può appoggiare ad un oggetto di tipo “Notification Class”, al fine di definire specifici paradigmi di segnalazione degli eventi ai sistemi che ne fanno richiesta, fornendo segnalazioni che possono richiedere o meno una conferma di ricezione. Un terzo tipo di segnalazione è detto “Change of Value (COV)”: si tratta di una segnalazione che viene inviata agli oggetti che si registrano per riceverla mediante opportune chiamate mediante il servizio “SubscribeCOV” o “SubscribeCOVProperty”, a seconda che si vogliano ricevere segnalazioni sui valori delle proprietà standard o specifiche di un oggetto.

Punti di forza

Il protocollo è aperto, standardizzato sia a livello internazionale, sia a livello nazionale in molti Paesi ed è stato utilizzato in numerose installazione nel corso degli ultimi anni. La presenza di comitati per lo sviluppo in doversi continenti rappresenta un punto di forza per la versatilità e possibile longevità del protocollo. [21]
La possibilità di utilizzare diversi mezzi di trasmissione, sia ad alta velocità, sia a basso costo, lo rende adatto sia alla realizzazione di sezioni per la supervisione, sia per il campo [22]. La possibilità di utilizzare nativamente il protocollo IP (ed UDP) come livello di trasporto rappresenta un elemento particolarmente apprezzabile nella direzione di una forte integrazione fra i sistemi tecnologici e di ICT nelle abitazioni [23].
L’interoperabilità fra i dispositivi è garantita dalla presenza di “BACnet Testing Lab” (BTL), che si occupano di verificare il rispetto dello standard da parte dei prodotti che stanno per essere immessi sul mercato, al fine di garantire in modo efficace l’interoperabilità fra gli stessi [24].

Limiti

Il protocollo risulta essere molto versatile, ma al tempo stesso relativamente complesso anche per la realizzazione di comunicazione di valori semplici, quali lo stato di contatti.
La standardizzazione a livello globale è avvenuta in tempi relativamente recenti e

quindi si può ancora considerare uno standard “giovane”, di conseguenza la sua diffusione è ancora relativamente scarsa rispetto ad altri standard quali LonTalk.
L’assenza di uno strumento di configurazione unico per tutte le installazione rappresenta un forte elemento di flessibilità, ma anche un limite alla diffusione, in quanto rappresenta un elemento di difformità per chi si deve occupare di manutenzione o successive integrazioni di impianti esistenti.

3.3.3 LonWorks

Il protocollo LonWorks è stato sviluppato dalla Echelon Corp. Il sistema [25] è costituito dal protocollo di comunicazione, LonTalk, da un dispositivo di interfacciamento, il “Neuron Chip”, e da uno strumento di gestione della rete. Inizialmente mantenuto privato e proprietario, LonTalk è stato pubblicato come standard ANSI nel 1999 (ANSI/EIA-709) e rivisto l’ultima volta nel 2002. È stato anche standardizzato dal CEN come EN 14908, con ultima revisione nel 2006, ed è attualmente stato proposto come standard ISO (anche se al momento della redazione di questa dissertazione non è ancora stato approvato come tale e le votazioni iniziali sono state negative).
Lo standard è aperto, ma attualmente sono richieste delle royalty per ogni dispositivo “commissionato”, ovvero inserito in una rete, utilizzando il software di riferimento fornito dalla Echelon: LonMaker.

Principio di funzionamento

LonTalk è un protocollo standardizzato su molti mezzi di trasmissione, fra i quali i più diffusi sono il doppino ritorto (ANSI/EIA709.3 per gli USA e EN 14908-2 per l’Europa) e la powerline (trasmissione su linea elettrica di alimentazione a corrente alternata, ANSI/EIA709.3 per gli USA ed EN 14908-3 per l’Europa), ma è possibile utilizzare anche fibre ottiche, onde radio o protocollo IP (ANSI/EIA-852 conosciuto anche come LonWorks/IP).
Ci si riferisce alle reti realizzate utilizzando il protocollo di comunicazione LonTalk con il termine di reti LON (Local Operating Network).
Il protocollo prevede una comunicazione peer-to-peer (P2P), con indirizzamento di-

retto fra dispositivi che consente di creare domini con fino a 32385 dispositivi, che possono essere suddivisi in subnet di 127 nodi, per un totale di 255 subnet per dominio. Ogni nodo ha un ID univoco a 48 bit, utilizzato per la configurazione iniziale della rete. I nodi sono in genere dei dispositivi che includono un Neuron Chip, ma lo stack può anche essere implementato via software all'interno di chip utilizzati nelle applicazioni dei componenti interfacciati alla rete.
L'utilizzo della rete in genere prescinde dalle conoscenze dell'indirizzamento dei nodi, che viene gestito direttamente dallo stack, e si basa sul concetto di "network variable", ovvero variabili di rete, e "binding", ovvero un collegamento logico fra variabili all'interno della rete. Un qualunque nodo della rete pubblica delle variabili, che possono essere lette o scritte, chiamate SNVT (pronunciato usualmente "snivit"), e tramite tali variabili i dati vengono scambiati sulla rete fra un nodo che le pubblica ed uno che si registra per riceverne le variazioni o esegue delle letture dirette delle stesse (polling). I tipi di variabili sono standardizzate dal protocollo LonTalk e la definizione di nuovi tipi è coordinata dal consorzio LonMark, che fra le altre cose si occupa anche di mantenere e certificare la compatibilità dei dispositivi prodotti.

Punti di forza

Il Neuron Chip rappresenta un'interfaccia ideale per i nodi di automazione, integrando sia l'hardware che il software per la connessione in rete in una soluzione compatta ed efficiente. La politica di pubblicazione in rete delle informazioni e la modalità di segnalazione delle variazioni rappresenta un modo efficiente di trasmettere dati anche in reti di dimensioni di grande estensione e complessità.

Limiti

L'utilizzo di un unico software per la configurazione e gestione della rete rappresenta da un lato un vantaggio a livello di apprendimento, dall'altro una limitazione, in quanto la qualità del software non beneficia della presenza di concorrenti. Grazie all'apertura del protocollo negli ultimi anni sta emergendo qualche alternativa. La necessità di pagare royalty su ogni singolo nodo installato e configurato (all'incirca 5 $

per ognuno) rappresenta una limitazione alla riduzione effettiva dei costi di installazione, rendendo l'approccio ancora troppo costoso per installazioni medio-piccole. Non esistono sistemi diretti semplici per l'implementazione della sicurezza [26].

3.3.4 Konnex

Il protocollo Konnex (KNX) è nato dalla convergenza di 3 standard di automazione europei: EIB, Batibus ed HES [27]. I tre standard sono stati sviluppati indipendentemente a partire dai primi anni '90, ciascuno con caratteristiche relativamente simili agli altri. Nel 1996 i consorzi a supporto dei tre standard hanno siglato accordi di convergenza che hanno dato inizio ad un cammino che ha poi portato alla costituzione dell'associazione Konnex ed all'inizio del processo di standardizzazione a livello Europeo (CENELEC) con la stesura delle norme EN 50090 all'inizio del 2000. I primi standard approvati sono stati pubblicati nel 2003. Il processo è tutt'ora in corso, e sebbene alcune norme siano state pubblicate, non tutto lo standard Konnex è stato ancora incluso nelle norme CENELEC.
Semplificando, si può affermare che si è trattato di una fusione per incorporazione all'interno dello standard EIB di alcune caratteristiche degli altri due standard, in quanto al termine del processo di convergenza i dispositivi EIB sono sostanzialmente compatibili con quelli KNX.
Il protocollo, in conseguenza della standardizzazione, è aperto e royalty free, ma solo per i membri della Konnex Association.

Principio di funzionamento

Il protocollo Konnex utilizza come mezzo trasmissivo prevalentemente un doppino schermato, utilizzato per trasportare sia l'alimentazione a 29 V corrente continua, sia il segnale. Sono comunque standardizzati altri mezzi trasmissivi, quali le powerline, i raggi infrarossi e le onde radio [28].
Il protocollo prevede una comunicazione diretta fra i dispositivi connessi al medesimo bus, o anche a bus fra loro collegati logicamente mediante opportuni dispositivi, utilizzando un paradigma di tipo P2P, che quindi non richiede un dispositivo di super-

visione o coordinamento per operare. Ogni dispositivo è accoppiato alla linea, dalla quale riceve alimentazione e sulla quale comunica, mediante una BCU (Bus Coupling Unit).
Ogni nodo nella rete è identificato da un codice univoco (indirizzo fisico). Ogni linea può avere fino a 64 dispositivi. Fino a 12 linee possono essere accoppiate fra loro mediante opportuni dispositivi chiamati "accoppiatori di linea" a creare un'area. Ogni sistema può a sua volta comprendere fino a 15 aree, per un totale massimo teorico di 11520 dispositivi. L'indirizzamento fisico riflette questa topologia: è infatti suddiviso su 3 numeri, che identificano campo, linea e dispositivo.
I messaggi scambiati sulla rete sono detti "telegrammi" ed ognuno di essi comprende: l'indirizzo fisico del mittente, l'indirizzo di gruppo del (o dei) destinatari ed i dati che devono essere trasferiti. La velocità di comunicazione sul normale doppino schermato è di 9600 bps.
La creazione delle funzioni avviene includendo i dispositivi che si devono scambiare dati per una specifica funzione all'interno del medesimo gruppo logico. Ad esempio se si vuole che un pulsante attivi una o più luci è necessario includere l'oggetto pulsante e gli oggetti luci nel medesimo gruppo, in modo che nel momento in cui il pulsante invia un telegramma in conseguenza di una variazione dello stato, il telegramma venga ricevuto dagli oggetti luce che lo devono ricevere ed interpretare.
L'indirizzamento dei gruppi è a 15 bit, suddivisibili in due insiemi: 4 bit (16 gruppi principali) e 11 bit (2048 sottogruppi), oppure in 3 insiemi: 4 bit (16 gruppi principali), 3 bit (8 gruppi intermedi) e 8 bit (256 sottogruppi).
La comunicazione è di tipo "event-driven", ovvero vengono inviati messaggi sulla base dell'accadimento di eventi predefiniti per ciascun dispositivo [29, 30].
Per la creazione delle reti e la conseguente configurazione dei singoli dispositivi è reso disponibile dall'associazione Konnex un software ad hoc: ETS3.

Punti di forza

L'approccio del sistema Konnex è di facile implementazione, grazie alla libertà di topologia ed alla distribuzione dell'alimentazione insieme ai dati sul medesimo mezzo.
Essendo in fase finale di standardizzazione a livello europeo ed essendo supporta-

to da diverse importanti case produttrici di dispositivi per l'automazione domestica, rappresenta una scelta di continuità di supporto ragionevole, sebbene ancora oggi non particolarmente diffusa. L'utilizzo di un solo software di configurazione rappresenta un elemento di uniformità per progettisti ed installatori, indipendentemente dalla marca dei dispositivi (analogamente a quanto avviene con LonMaker per LON).

Limiti

Anche per Konnex, come per LON, il software di configurazione unico rappresenta un ostacolo, sia di tipo economico (sebbene ETS3 non richieda royalty per singolo nodo incluso), sia di tipo operativo, non esistendo attualmente alternative pratiche all'approccio imposto dal software stesso.
Il meccanismo di indirizzamento utilizzato rappresenta un limite al numero massimo di connessioni che possono essere rappresentate dal protocollo, ed un elemento che in parte ostacola le procedure di supervisione della rete da parte di personal computer, o altri mezzi che devono interfacciarsi con la rete. Infatti collegarsi e monitorare il traffico è l'unico mezzo per determinare lo stato dei dispositivi e per ricevere le segnalazioni degli eventi. Inoltre aggiungere molte funzioni richiede l'aggiunta ripetitiva e complessa di diversi gruppi, uno per ogni funzione che si intende implementare. L'utilizzo del software ETS3 non rende purtroppo particolarmente agevole questa operazione.
È inoltre da notare che per sfruttare al meglio l'organizzazione gerarchica dell'indirizzamento di gruppo (e ridurre di conseguenza la complessità della configurazione e delle manutenzione) è necessario fare ampio uso di gruppi principali e spesso dell'indirizzamento a tre livelli. Così facendo, però, le potenzialità del sistema crollano velocemente a causa del ridotto numero di bit a disposizione per la codifica, che rende quindi l'approccio inadatto ad installazioni che includano nel medesimo sistema poco più di un appartamento di medie dimensioni o un edificio commerciale con un livello di automazione modesto. A questo problema è possibile sopperire utilizzando un sistema di supervisione basato su computer, che però fa venire meno i vantaggi intrinseci dell'intelligenza distribuita.
Un'altra limitazione, comune anche ad altri tipi di bus proprietari, è rappresentata

dal fatto che i dispositivi, nonostante il tentativo di semplificazione dell'approccio, per essere inseriti nella rete devono essere ogni volta programmati con il software, altrimenti non possono operare. Questo significa che in caso di guasto è necessaria una nuova configurazione ad opera di un progettista o installatore qualificato, non è possibile semplicemente sostituire fisicamente il modulo guasto.

3.3.5 Sistemi e bus proprietari

Alcune ditte hanno sviluppato negli anni sistemi di automazioni interamente proprietari, ovvero non basati su tecnologie standardizzate o a specifiche aperte. Un esempio è il sistema MyHome di Bticino [31].
Esistono poi diversi altri sistemi di automazione domestica e di edificio che si basano su bus di campo aperti, quali CANOpen [32, 33] o EIA-485, sui quali sono poi stati sviluppati protocolli di livello superiore di tipo proprietario. Questi standard sono per molti versi il risultato dell'assenza di standard diffusi e condivisi durante gli anni di diffusione iniziale dell'automazione domestica.
Nell'ultima decina d'anni alcuni standard emergenti stanno cominciando ad avere un riconoscimento a livello internazionale che può essere un punto di partenza per una maggiore protezione degli investimenti e quindi possono essere una base per futuri sviluppi, che però tardano ancora a manifestarsi.

Capitolo 4

Le reti Ethernet/IP

Comunicare l'un l'altro, scambiarsi informazioni è natura;
tener conto delle informazioni che ci vengono date è cultura.

– Johann Wolfgang Goethe

La rete Ethernet è ormai uno standard di fatto per la comunicazione fra computer in tutto il mondo. L'utilizzo è sia su base locale che su base geografica e la sua evoluzione è estremamente rapida, in quanto legata all'evoluzione stessa dei computer, ma anche a quella dei contenuti informativi che devono essere veicolati. In questo capitolo verranno descritte le caratteristiche della rete ed i principali protocolli utilizzati, al fine di costituire una base fondamentale per la comprensione del lavoro di progettazione svolto.

4.1 Convergenza

Il numero dei sistemi tecnologici ormai presenti all'interno delle abitazioni sta crescendo sempre di più. Abbiamo il sistema telefonico (anche se negli ultimi anni la telefonia cellulare lo sta lentamente soppiantando nel nostro Paese), abbiamo sistemi anti-intrusione, di rilevazione incendi, allagamenti, controllo del riscaldamento e condizionamento (HVAC, Heating, Ventilation and Air Conditioning). C'è poi l'im-

pianto televisivo, terrestre e satellitare, con relativi decoder. Inoltre abbiamo reti per il trasporto di dati, sia cablate (Ethernet LAN), sia senza fili (Wi-Fi).
Tutti questi sistemi sono indipendenti, e ciascuno di essi si poggia su meccanismi e supporti cablati indipendenti e, spesso, incompatibili. Ciò rende necessario installare in modo indipendente diverse serie, non solo di sensori ed attuatori, ma anche di cavi differenti, con adeguate regole di posa per limitare le interferenze reciproche. A tutto questo, utilizzando approcci tradizionali, è necessario affiancare un cablaggio apposito per l'automazione domestica (cfr. cap. 3).

Un nuovo approccio che si sta affermando negli ultimi anni è quello di fare convergere i vari sistemi verso un unico mezzo di comunicazione: Ethernet, nelle sue varie incarnazioni. Ciò comporta la necessità di un unico cablaggio (detto "strutturato") che consente il trasporto efficiente di una grande quantità di informazioni. Per ottenere questo sono stati sviluppati vari protocolli di comunicazione, che permettono alle informazioni di viaggiare su questo mezzo, senza creare interferenze fra di loro. Il protocollo fondamentale per questa coesistenza è il protocollo IP (Internet Protocol, cfr. sez. 4.5.1), sul quale ne operano altri di livello superiore, a seconda dell'informazione che si vuole fare circolare, sia essa VoIP (Voice over IP), DVB (Digital Video Broadcasting), o anche di automazione, in quanto molti protocolli di supervisione sono già in grado di operare anche su IP (cfr. sez. 3.3.2 e 3.3.3).

In questa ricerca è stata messa a punto un'infrastruttura in grado di spingere il concetto di convergenza ancora di più verso il campo, con la progettazione di un modulo di interfacciamento intelligente fra Ethernet (cfr. sez. 5.2.2 e 6) ed i sensori operanti con protocolli "semplici" nativi. Ciò comporta un'integrazione ancora superiore dei dispositivi e dei sistemi all'interno dell'abitazione, potendo far funzionare anche i sistemi anti-intrusione, di rilevazione incendi, HVAC, etc. sul medesimo mezzo usato per gli altri servizi.

4.2 Il concetto di rete

Nell'accezione utilizzata in questa trattazione, una rete è sistema di comunicazione in grado di permettere l'interconnessione (fisica o logica) di più dispositivi. È da

notare che le reti possono essere classificate in vario modo, a seconda dei parametri che vengono presi in considerazione: topologia, estensione e distanza fra i nodi, mezzo fisico di collegamento, protocollo di comunicazione ... Di seguito verranno riepilogate rapidamente alcune di queste distinzioni.

4.2.1 Topologie di rete

A seconda di come sono collegati i nodi gli uni con gli altri si possono avere vari tipi di rete: le reti lineari (line), ad anello (ring), a bus, ad albero (tree), a stella (star), a maglia (mesh), completamente connesse (fully connected) e miste (mixed).

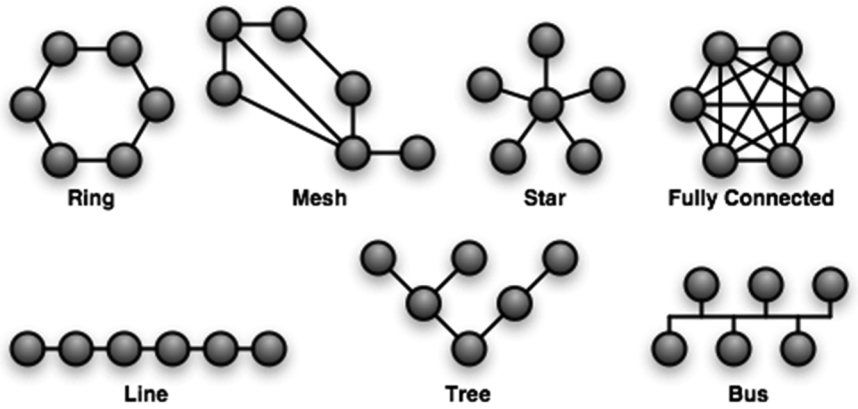


Figura 4.1: Schemi di topologie di rete.

Lineari Ogni nodo riceve e ritrasmette a quello successivo i dati che non sono a lui indirizzati: questo crea problemi di affidabilità, in quanto il guasto di un qualunque nodo comporta la separazione della rete in due tronconi. Inoltre introduce dei ritardi di trasmissione, dovuti al fatto che ogni messaggio viene prima ricevuto e poi ritrasmesso.

Anello Sono in tutto e per tutto simili a quelle lineari, con la differenza che se un nodo si guasta, a seconda del protocollo, è ancora possibile una comunicazione fra tutti i rimanenti nodi.

Bus Consentono una comunicazione arbitraria fra due nodi nella rete, senza che il guasto di uno qualunque dei nodi pregiudichi la possibilità per gli altri di comunicare fra loro. È necessario un protocollo di arbitrazione per l'accesso al mezzo, che impedisca o risolva le condizioni di concorrenza.

Albero I nodi che ricevono un'informazione non a loro destinata la ritrasmettano a tutti i nodi sotto di loro, o solo a quelli indirizzati, se possono risolvere il destinatario. Ciascun nodo, tranne quelli senza nodi di livello inferiore, in caso di guasto, isola i nodi sottostanti.

Stella Tutti i nodi sono in comunicazione con un singolo nodo centrale, spesso indicato come "centro stella", che funge da nodo di smistamento per tutte le comunicazioni. Il guasto del centro stella provoca ovviamente il blocco completo della rete.

Maglia Prevedono percorsi multipli fra due o più nodi. Ciò assicura una maggiore efficienza di comunicazione ed una riduzione degli effetti negativi dei guasti. Devono però essere utilizzati protocolli di comunicazione in grado di risolvere il problema dei cammini multipli.

Completamente connesse Hanno una connessione diretta fra ogni coppia di nodi nella rete. Il livello di affidabilità è massimo in caso di guasto, ma sono estremamente dispendiose in termini di risorse assegnate alla realizzazione delle connessioni.

Miste Presentano tratti di due o più dei tipi di rete descritti. In genere sono rappresentate da più reti dei tipi descritti, aventi alcuni nodi che fungono da punti di

contatto. Per la loro gestione è necessario che il protocollo di comunicazione tenga conto dei problemi di cammini multipli ed eventualmente di problemi di accesso concorrente al mezzo.

4.2.2 Estensione delle reti

L'estensione è un differente fattore distintivo delle reti. Sulla base dell'estensione, della tipologia e della dislocazione delle reti possiamo distinguere:

- BAN: Body Area Network. Sono reti che collegano fra loro diversi sensori personali che rilevano parametri vitali.
- PAN: Personal Area Network. Sono reti pensate per la connessione di pochi dispositivi (in genere dell'ordine della decina), tutti relativi all'attività di una sola persona, o al limite di un ristretto gruppo di persone. Ad esempio possono collegare i dispositivi presenti su una scrivania o in una postazione di lavoro.
- LAN: Local Area Network. Includono un numero di dispositivi variabile, in genere contenuti nella medesima unità abitativa, operativa o di edificio. Ad esempio la rete Ethernet di un ufficio.
- CAN: Campus Area Network. Sono reti che spaziano su più edifici tra loro connessi.
- MAN: Metropolitan Area Network. Sono reti che includono specifiche aree di una città.
- WAN: Wide Area Network. Sono reti a diffusione globale, ad esempio la rete Internet.

4.2.3 Mezzi fisici di collegamento

Sulla base del mezzo fisico possiamo avere:

- Reti cablate: un cavo elettrico o una fibra ottica si collega ad ogni singolo nodo.

- Reti wireless: un mezzo trasmissivo senza fili è usato, ad esempio le onde radio o gli infrarossi.
- Reti miste: porzioni della rete sono realizzate con ambedue i metodi precedenti.

4.3 La rete per eccellenza: Ethernet

Nonostante siano possibili molti tipi di reti di comunicazione fra calcolatori, e siano tutt'ora impiegati svariati mezzi e protocolli di comunicazione fra dispositivi, quando si parla di rete in ambito informatico ci si riferisce in genere implicitamente alla rete Ethernet.
Ciò deriva dal fatto che tale connessione, standardizzata come IEEE 802.3 (ISO 8803) nel 1983, ha avuto da allora una diffusione a livello mondiale che è cresciuta esponenzialmente. Attualmente Ethernet, nelle sue varie implementazioni fisiche, rappresenta uno degli standard più diffusi per la comunicazione fra personal computer e periferiche ICT in genere. La velocità di comunicazione varia a seconda del tipo di cablaggio, ma nelle attuali implementazioni si va da un minimo di 10 Mbps full-duplex su doppino intrecciato non schermato (UTP, Unshielded Twisted Pair) con lo standard 10BASE-T (IEEE 802.3i), ad un massimo di 10 Gbps (10GBASE-T, IEEE 802.3an). Sono in oltre in corso di definizione standard a velocità superiori, in particolare sono allo studio 40 Gbps e 100 Gbps (IEEE 802.3ba in corso di definizione).

Lo standard Ethernet prevede anche la possibilità di fornire energia sfruttando il cablaggio UTP di segnale, secondo uno standard noto come PoE (Power over Ethernet, IEEE 802.3af fino a 12.95 W per dispositivo, e IEEE 802.3at per potenze maggiori, in corso di definizione) [34].

4.3.1 Standard Ethernet

A livello internazionale è stato standardizzato un modello protocollare detto stack ISO/OSI [35]. Tale modello permette la descrizione in modo astratto di qualunque protocollo di comunicazione come una serie di strati (layer) sovrapposti, che forniscono ciascuno dei servizi al livello immediatamente superiore, rendendo a quest'ultimo trasparente il funzionamento dei livelli sottostanti. Questo modello è molto utile

in astratto, ma risulta di difficile implementazione nei casi reali. Il modello ISO/OSI definisce 7 diversi livelli, dal livello fisico a quello di applicazione: Physical (fisico), Data Link (collegamento dati), Network (rete), Transport (trasporto), Session (sessione), Presentation (presentazione), Application (applicazione).
Il comitato tecnico incaricato della definizione degli standard della famiglia IEEE 802 (ISO 8802) ha quindi definito un modello che risulta essere definito sempre a strati, ma con una suddivisione leggermente differente: esso infatti introduce gli strati MAC ed LLC come suddivisioni dello strato Data Link. Lo strato fisico è definito dai vari sotto standard dell'IEEE 802.3, lo strato MAC è definito dallo standard IEEE 802.3, mentre quello LLC è definito dall'IEEE 802.2 (Figura 4.2).

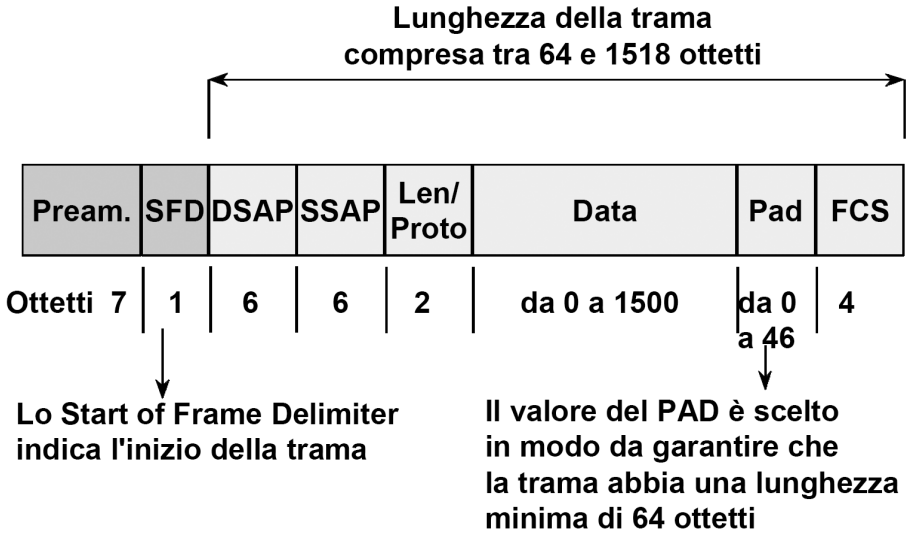


Figura 4.2: Trama secondo lo standard IEEE 802.3.

4.3.2 Mezzi fisici

Attualmente sono stati standardizzati diversi mezzi fisici per l'Ethernet:

- cavo coassiale spesso (RG213, IEEE 802.3);
- cavo coassiale sottile (RG58, IEEE 802.3a);

- fibra ottica (IEEE 802.3d, IEEE 802.3j, IEEE 802.3z, IEEE 802.3aq);
- cavo UTP (di differenti categorie[1], IEEE 802.3i, IEEE 802.3ab, 802.3an);
- cavo FTP/SFTP (di differenti categorie, utilizzati analogamente ai cavi UTP).

4.3.3 Accesso al mezzo

Il protocollo Ethernet prevede un accesso fisico al mezzo di tipo Carrier Sensing Multiple Access / Collision Detection (CSMA/CD), che prevede per la trasmissione il seguente processo:

1. verifica che nessuna comunicazione sia già in corso;
2. inizio della trasmissione della trama;
3. verifica se è avvenuto l'inizio contemporaneo di una trama da parte di un'altro dispositivo (collisione):
    - se è avvenuta una collisione, interrompe la comunicazione e ritenta la trasmissione dopo un intervallo di tempo casuale;
    - se non è avvenuta collisione, il processo è concluso.

È da notare che l'insieme di dispositivi che si trova a dover eseguire questa procedura, per determinare se la trasmissione è andata a buon fine, si dicono all'interno dello stesso "dominio di collisione". Se viene utilizzato come mezzo trasmissivo un mezzo di tipo half-duplex, quale ad esempio un cavo coassiale, siamo in presenza di una rete con topologia a bus e tutte le interfacce collegate condividono il medesimo mezzo, sia per la trasmissione, sia per la ricezione. È quindi necessario limitare e rilevare le collisioni. Ciò limita ovviamente la velocità massima di comunicazione effettiva dei singoli dispositivi, in quanto oltre a dover condividere la medesima banda massima, deve essere considerata nel computo anche la banda persa a causa delle collisioni.

[1] Sono standardizzate diverse categorie di cavi UTP. Per la comunicazione Ethernet sono utilizzati i cavi di categoria 5e (TIA/EIA-568-B), 6 (TIA/EIA-568-B.2), 6a (ANSI/TIA/EIA-568-B.2-10). Tutte queste categorie sono state definite anche nello standard internazionale ISO 11801 ed europeo EN 50173.

In casi reali è quindi in generale buona norma considerare la banda come dimezzata rispetto a quella teorica.

Appositi dispositivi sono in grado di ricevere informazioni da una porta (interfaccia di comunicazione) e riportarle su tutte le altre, al fine di rigenerare il segnale o di ampliare il bus. Questi dispositivi prendono il nome di "repeater", se hanno solo due porte, di "multiport repeater", se hanno più di due porte, o "hub", se gestiscono cablaggi a coppie simmetriche UTP. Tali dispositivi non fanno altro che ricevere e ritrasmettere su tutte le loro porte ciò che ricevono. Per questo motivo, di fatto, pongono tutti i dispositivi all'interno del medesimo dominio di collisione. Gli hub non hanno alcuna cognizione degli indirizzi MAC, operano quasi unicamente al livello fisico[2]. L'uso di questo tipo di dispositivi è quasi del tutto scomparso con l'introduzione del cavo UTP a sostituire i cavi coassiali e con l'introduzione degli switch Ethernet.

Con l'introduzione degli "switch" Ethernet, la situazione è radicalmente mutata: tali dispositivi, sebbene utilizzati con la medesima funzione degli hub, hanno la capacità di memorizzare i pacchetti Ethernet ricevuti da più porte contemporaneamente e di ritrasmetterli successivamente sulle porte alle quali sono connessi i dispositivi cui sono destinati. Per fare ciò gli switch operano al livello MAC, sono quindi in grado di eseguire richieste ARP (Address Resolution Protocol, protocollo utilizzato per richiedere a livello MAC quali dispositivi hanno un determinato indirizzo IP, cfr. sez. 4.5.1) ed indirizzare i pacchetti solo verso la porta alla quale è direttamente o indirettamente collegato il dispositivo che deve ricevere quel pacchetto. Gli switch Ethernet sono quindi in grado non solo di separare i domini di collisione e supportare comunicazioni di tipo full-duplex su tutte le connessioni, ma anche di sgravare le connessioni non interessate da uno specifico traffico dei pacchetti non interessanti. L'introduzione di questi dispositivi, certamente più complessi di un hub, ma ormai caratterizzati dai costi estremamente ridotti ed affidabilità ed efficienza molto elevate, ha permesso di rendere le reti LAN molto più performanti. Ciò ha ridotto grandemente gli svantag-

[2] In realtà gli hub sono in grado di rilevare attivamente le collisioni e di generare su tutte le porte un messaggio di "jamming" appositamente studiato per garantire che la collisione sia rilevata con certezza da tutti i dispositivi connessi

gi di un accesso al mezzo di tipo CSMA/CD, incrementando la velocità massima di trasmissione, anche in caso di reti ad alto traffico, molto vicino alla massima velocità teorica di comunicazione.

4.3.4 Trama Ethernet

La trama Ethernet è rappresentata in Figura 4.3. L'indirizzamento dei dispositivi a

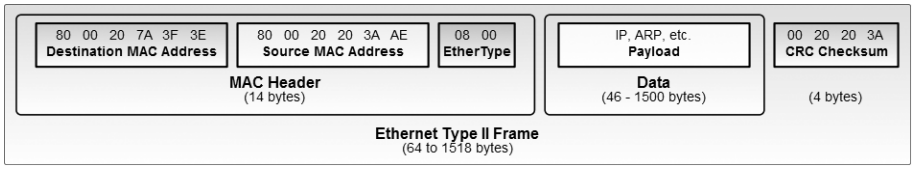


Figura 4.3: Trama Ethernet II.

questo livello avviene utilizzando un codice a 48 bit denominato MAC (Media Access Control) address, cui ci si riferisce comunemente solo come MAC. Esso è suddiviso in 6 ottetti (byte), di cui i primi tre sono definiti OUI: Organizationally Unique Identifier e sono assegnati dall'IEEE, mentre i restanti 3 sono definiti dal produttore, in modo univoco per ogni interfaccia di rete. Tale indirizzo così formato è univoco per ogni interfaccia di rete. L'IEEE è stata incaricata dall'ISO come autorità per l'assegnazione degli indirizzi MAC, sia in forma individuale (se necessario), sia in forma di 3 ottetti che identificano un produttore, il quale poi impone in modo progressivo ed univoco i restanti 3 ottetti in ogni scheda o dispositivo prodotto [36].

4.3.5 Wireless

Il protocollo Ethernet opera anche su mezzi non cablati, grazie allo standard Wi-Fi[3] (IEEE 802.11a/b/g/n) ed allo standard appena introdotto WiMAX (IEEE 802.16).
Grazie a questi standard, in particolare a quello Wi-Fi, è possibile realizzare delle reti WLAN (Wireless LAN), che hanno proprietà di connessione simili alle reti LAN

[3]Wi-Fi: Wireless Fidelity, termine che si riferisce ai dispositivi conformi alle norme IEEE 802.11 che abbiano superato le prove di certificazione della Wi-Fi Alliance (Wireless Ethernet Compatibility Alliance)

cablate, quindi impiegando i medesimi protocolli di comunicazione di livello superiore al livello fisico. Ovviamente l'utilizzo della comunicazione radio al posto dei cavi rende necessario l'utilizzo di una serie di protocolli e procedure di livello MAC opportuni, ma questi risultano trasparenti alle applicazioni già a partire dal livello superiore al livello MAC.

4.4 Non solo LAN: l'integrazione nativa con Internet

È da notare che le reti LAN sono sempre più spesso concepite per integrarsi o collegarsi a reti più ampie a rilevanza geografica, ma in particolare per interconnettersi alla rete per eccellenza: Internet. Questa connessione è possibile, perché esistono protocolli per l'instradamento ed il trasporto comuni alle reti coinvolte (cfr. sez. 4.5).

La capacità di comunicazione nativa fra i dispositivi e le applicazioni che operano in reti LAN ed i servizi internet, rende sostanzialmente immediata la possibilità di fornire e ricevere informazioni da ogni parte del mondo, senza dover modificare le applicazioni sviluppate. Questo è un vantaggio importante di ogni sistema di supervisione: se questo opera sfruttando una rete LAN, allora può operare con la medesima efficenza ed efficacia da ogni punto del mondo, ammesso che la banda di comunicazione e le latenze si mantengano entro livelli accettabili per l'applicazione specifica.

4.5 Protocolli ampiamente diffusi per le comunicazioni Ethernet ed Internet

Dopo aver discusso del protocollo Ethernet, passiamo ora alla descrizione dei livelli superiori dello stack ISO/OSI, in particolare i livelli di rete e di trasporto. Questi livelli sono infatti le basi per una comunicazione efficiente ed affidabile fra due applicazioni, sia che queste operino su LAN che su WAN. Di seguito sono quindi descritte le caratteristiche principali dei protocolli IP, TCP ed UDP.

4.5.1 IP

Il protocollo IP (Internet Protocol, RFC[4] 791, 919, 922, 950, 1349) è un protocollo dello strato di rete, secondo il modello ISO/OSI. Esso permette la comunicazione trasparente di pacchetti di dati fra sottoreti diverse in modo non gerarchico, fra reti locali (LAN, WLAN) e reti più ampie (CAN, MAN, WAN), sfruttando collegamenti permanenti o dial-up su PTSN/ISDN. Appositi apparati di rete, detti "router", basandosi sul protocollo IP, consentono il corretto indirizzamento dei pacchetti.

In questa trattazione verrà considerata la versione 4 del protocollo (IPv4), in quanto è quella utilizzata nel progetto ed attualmente è quella utilizzata nella stragrande maggioranza delle applicazioni nel mondo. Una nuova revisione del protocollo, denominata IPv6, è stata definita diversi anni fa, allo scopo di superare alcune limitazioni chiave della versione 4 nel contesto moderno mondiale, ma a tutt'oggi la sua diffusione è ridotta a poche dorsali ed alcuni casi industriali o accademici isolati.

Gli scopi fondamentali del protocollo IP sono:

- definire l'unità base per il trasferimento delle informazioni, standardizzando il "datagramma", la cui dimensione massima è 65535 byte;
- definire lo schema di indirizzamento dei datagrammi;
- definire la modalità di indirizzamento dei datagrammi;
- eseguire la frammentazione e riassemblaggio dei datagrammi, se necessario per la trasmissione, in base alle necessità del livello inferiore.

In Figura 4.4 è rappresentato lo schema del pacchetto IP. Gli indirizzi IP sono costituiti da 4 byte, rappresentati usualmente in notazione decimale separata da punti (es. 192.168.0.1). Al fine di determinare il corretto instradamento dei pacchetti IP è necessario che vengano definite le maschere di rete (e sottorete), ovvero gruppi di 4 byte che agiscono da maschere per definire quale gruppo di indirizzi fa parte

[4]RFC: Request For Comment. È l'insieme dei protocolli standard per Internet. Il nome deriva dall'origine degli standard stessi, che erano redatti come proposte da presentare ad una costituenda entità di standardizzazione, che però non si è mai costituita.

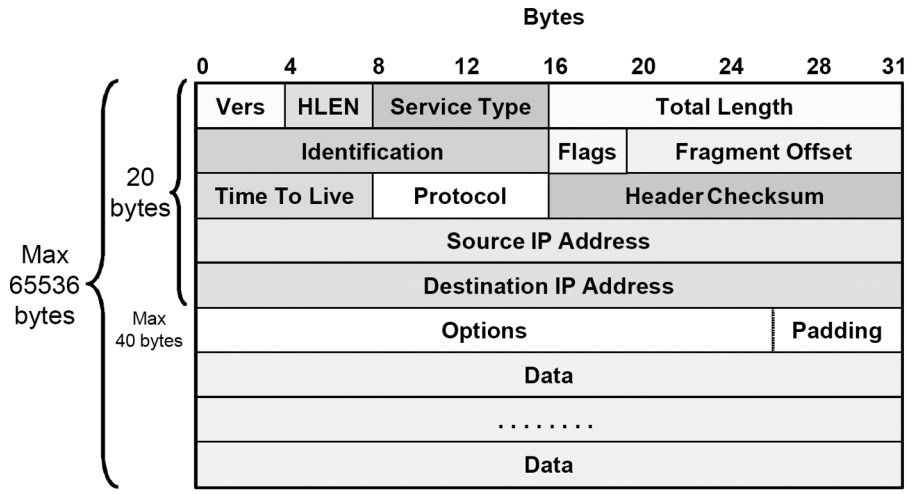


Figura 4.4: Pacchetto IP.

della rete, e può quindi essere raggiunto direttamente, e quali invece devono essere raggiunti grazie ad un router, che si occupi di instradare i pacchetti verso la rete di destinazione. Lo schema prevede la possibilità di impostare reti in varie classi, come mostrato in Figura 4.5. Esistono indirizzi particolari, utilizzati per particolari

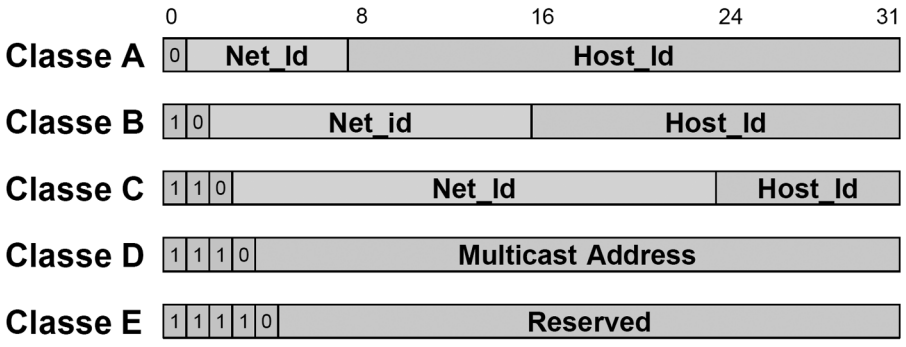


Figura 4.5: Classi di indirizzamento.

comunicazioni, riportati in Figura 4.6.

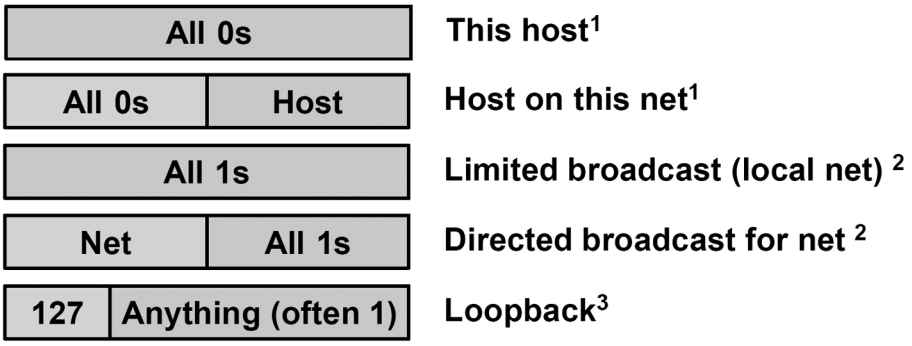


Figura 4.6: Indirizzi IP speciali.

Al fine di razionalizzare l'utilizzo di indirizzi IP, alcuni indirizzi di rete sono stati riservati per l'utilizzo in reti LAN ad uso privato (RFC 1918):

- 10.0.0.0 – 10.255.255.255 (10/8 prefix);
- 172.16.0.0 – 172.31.255.255 (172.16/12 prefix);
- 192.168.0.0 – 192.168.255.255 (192.168/16 prefix).

Questi indirizzi privati vengono trattati come tali dai router che gestiscono la comunicazione verso l'esterno della rete LAN, non propagandoli.
Ulteriori dettagli sul protocollo sono reperibili nelle RFC citate.

Al di sopra dello strato di rete, gestito mediante il protocollo IP, ci possono essere diversi protocolli dello strato di trasporto. I più diffusi sono TCP ed UDP, di seguito descritti.

4.5.2 TCP

Il protocollo Transmission Control Protocol (TCP) è definito dalla RFC 793. Si tratta di un protocollo bidirezionale che instaura un flusso di comunicazione basato sui singoli byte, ovvero il canale virtuale creato non richiede la strutturazione dei messaggi

trasmessi.
La comunicazione è "orientata al flusso" (stream oriented), ovvero instaura un canale virtuale di comunicazione fra due entità e ne gestiste la stabilità ed affidabilità occupandosi del:

- controllo e recupero di errore;
- controllo di flusso;
- controllo di congestione;
- ri-ordinamento delle unità informative;
- indirizzamento di uno specifico utente all'interno di un host.

Nella comunicazione di tipo stream (flusso) le informazioni sono interpretate come un unico flusso di byte. Il protocollo TCP si occupa della loro suddivisione in più pacchetti IP (segmenti), se necessario, e del loro riassemblaggio nell'ordine corretto in sede di ricezione.
Lo stream è stabilito fra una "porta" dell'host mittente verso una "porta" dell'host destinatario. Lo standard definisce un numero massimo di 65535 porte per ogni host. Una porta può essere impegnata in più flussi contemporaneamente, ma non possono essere instaurate due connessioni TCP che abbiano in comune contemporaneamente le stesse porte ed host da entrambi i lati.
Il formato di un pacchetto TCP è riportato in Figura 4.7. Il TCP è un protocollo di tipo "affidabile", ovvero si occupa di garantire la consegna dei messaggi inviati, mediante la verifica dell'integrità e della ricezione, e segnala al mittente le condizioni di errore irrecuperabile, quando cioè il pacchetto non viene ricevuto correttamente nonostante la correzione di errore ed i tentativi di ritrasmissione. Il protocollo prevede che una connessione stabilita sia permanente, fino al termine della comunicazione, e segnala quindi quando la connessione risulta essere chiusa o interrotta. Ulteriori dettagli sui meccanismi che consentono al protocollo di operare in questo modo sono reperibili nella RFC citata.

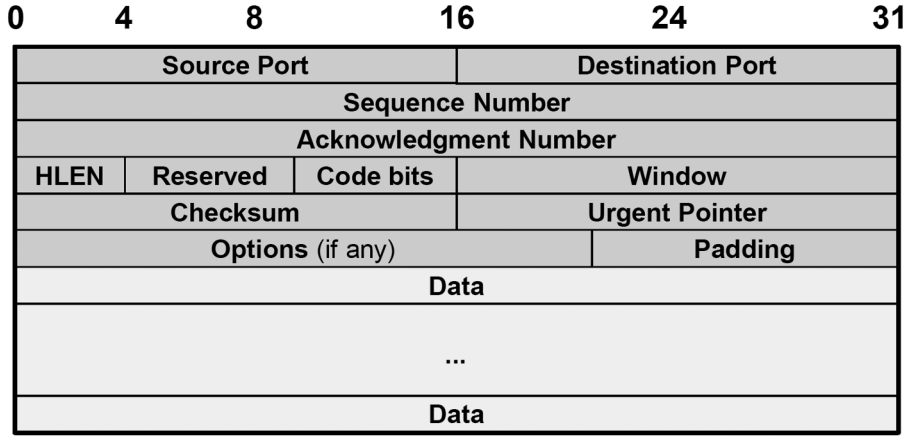


Figura 4.7: Pacchetto TCP.

4.5.3 UDP

Il protocollo User Data Protocol (UDP) è definito dalla RFC 768. Si tratta di un protocollo molto più semplice rispetto al TCP e fornisce servizi minimi di comunicazione. È di tipo "orientato ai messaggi" (message oriented), ovvero si occupa di trasmettere singoli messaggi da un host ad un altro.
UDP fornisce controllo di errore sull'intero messaggio, ma non si occupa della correzione di errore o della ritrasmissione dei pacchetti. È quindi un protocollo definito "non affidabile", in quanto il mittente non è in grado, basandosi solo sulle informazioni fornite da questo protocollo, di sapere se un pacchetto è stato ricevuto o meno. Non instaura una connessione stabile, come fa invece il TCP, fra i due host, ma mantiene il concetto di porta, utilizzandola per identificare mittenti e destinatari negli host coinvolti.
Un vantaggio della connessione UDP è la possibilità di trasmettere messaggi di tipo "multicast", ovvero indirizzati a più destinatari, cosa che il TCP non consente. Ciò permette di ridurre il traffico complessivo, nel momento in cui un messaggio è indirizzato a molti destinatari, ad esempio nel caso dell'invio di immagini televisive a più utenti.

Il formato di un pacchetto UDP è riportato in Figura 4.8. Complessivamente il TCP ha

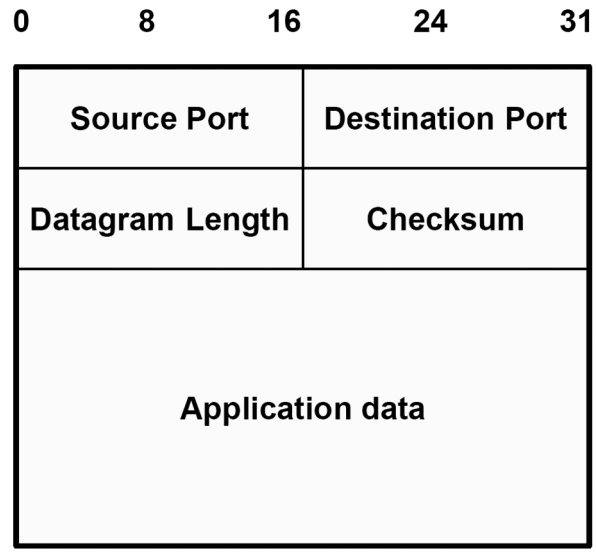


Figura 4.8: Pacchetto UDP.

un overhead maggiore rispetto all'UDP, dovuto alla necessità di instaurare una connessione ed alla gestione di errori e ritrasmissioni. Questo overhead è giustificabile nel caso di comunicazioni fondamentali non frequenti fra due entità, o per comunicazioni di grandi quantità di dati fra le stesse entità all'interno di un'unica connessione. Ciò perché in questi casi l'overhead è ammortizzabile. Nel caso invece di frequenti comunicazioni di tipo "event-driven", la connessione di tipo UDP, con una verifica di corretta ricezione gestita a livello superiore, è preferibile, in quanto l'overhead con connessioni brevi è significativo.

4.5.4 ARP

Il protocollo Address Resolution Protocol (ARP) è definito dalla RFC 826. Lo scopo è quello di consentire ad ogni dispositivo connesso alla rete di ottenere la corrispondenza fra un indirizzo IP ed un indirizzo MAC, al fine di indirizzare i pacchetti IP verso l'interfaccia corretta. È utilizzato ad esempio dai personal computer per impo-

stare correttamente l'indirizzo MAC di destinazione dei pacchetti di trama Ethernet da inviare, ma anche dagli switch al fine di indirizzare correttamente i pacchetti IP verso la connessione relativa all'host di destinazione, evitando di inviare le informazioni sulle porte cui non sono collegati host coinvolti nella comunicazione.
Per poter funzionare questo protocollo richiede che sia possibile la trasmissione di pacchetti broadcast a livello data link, ovvero è supportato su protocollo Ethernet, ma non è supportato su altri tipi di protocollo.

4.5.5 DHCP

Il Dynamic Host Configuration Protocol (DHCP) è definito nella RFC 2131 ed integrato dalle RFC 1533, 1497, 2132. Lo scopo del protocollo (aggiornamento ed integrazione del Bootstrap Protocol, BOOTP, RFC 951) è quella di consentire la configurazione dinamica di host che si connettono ad una rete in cui è presente un server di configurazione, definito DHCP Server.
Il protocollo prevede una serie di fasi successive, che consentono ad un host privo di indirizzo IP e di informazioni sulla rete di ricevere tutte le informazioni necessarie a sfruttare al meglio la comunicazione nella rete nella quale si va ad inserire. Il DHCP è anche molto versatile, in quanto oltre a prevedere oltre cinquanta parametri (molti dei quali opzionali) preconfigurati e standardizzati, consente anche l'inclusione di informazioni specifiche per ogni produttore, al fine di migliorare l'integrazione e la versatilità dell'approccio. È da notare che, in quanto estensione del BOOTP, il DHCP consente anche a macchine prive di sistema operativo di ottenere le informazioni necessarie a scaricare dalla rete l'immagine necessaria al loro avvio o funzionamento, sfruttando il protocollo di trasferimento file TFTP.
Ogni parametro fornibile è identificato da un numero progressivo detto di opzione, le cui più utilizzate sono:

- 1 - Subnet
- 6 - Domani name server
- 7 - Log server

- 12 - Host name
- 13 - Boot file size
- 15 - Domain name
- 28 - Broadcast address
- 42 - NTP server
- 50 - Requested IP address
- 51 - IP address lease time

4.5.6 TFTP

Il protocollo Trivial File Transfer Protocol (TFTP) è definito nella RFC 1350. Il suo scopo è quello di permettere il trasferimento di file nel modo più semplice possibile. Si basa sul trasferimento di singoli pacchetti UDP, di cui viene confermata singolarmente la ricezione fino al ricevimento dell'intero file richiesto. Attualmente è utilizzato anche per la trasmissione dei file necessari all'avvio di personal computer o altri dispositivi tramite la rete, configurati mediante il protocollo DHCP (o BOOTP).

4.6 Altri protocolli

Sono molti i protocolli che hanno un'importanza più o meno grande sul funzionamento delle reti LAN (intranet) e sulle reti WAN (Internet). In questo breve excursus sono stati ricordati solamente i protocolli più importanti per la comprensione della trattazione del tema proposto in questa dissertazione, ma molti altri sono importanti per il funzionamento delle reti LAN ed Internet. A titolo di esempio possiamo ricordare il protocollo Domain Name System (DNS), utilizzato essenzialmente per ottenere un indirizzo IP a partire da un nome mnemonico opportunamente costituito in modo gerarchico, il protocollo Internet Control Message Protocol (ICMP), per la diagnostica di rete e delle connessioni, l'Hyper Text Transfer Protocol (HTTP) per l'accesso alle pagine web, e molti altri [37].

4.7 Reti private virtuali (VPN)

L'utilizzo di reti LAN è oggi ampiamente diffuso in molte realtà commerciali ed industriali. Tutti i PC all'interno della rete comunicano condividendo risorse interne alla rete stessa. Le reti LAN sono collegate verso l'esterno mediante appositi dispositivi, detti gateway, che fungono da punti di contatto fra diverse reti LAN o fra la rete LAN e la rete WAN. Nella quasi totalità dei casi questi gateway includono altre funzioni, oltre a quella di router, in particolare spesso implementano funzioni di NAT (Network Address Translator), funzione necessaria alla comunicazione verso Internet quando all'interno della rete LAN sono utilizzati IP privati, e funzioni di firewall, ovvero programmi o dispositivi con lo scopo di fungere da barriere di regolamentazione del traffico in ingresso ed in uscita dalla LAN.

Nel caso in cui un utente esterno alla rete LAN volesse poter condividere delle risorse private della rete stessa, sarebbe necessario rendere queste risorse accessibili anche all'esterno della rete stessa: questo pone grossi problemi relativi alla sicurezza ed all'autenticazione degli accessi, oltre che alla protezione dei dati in transito su una rete pubblica che non può essere controllata dall'entità che possiede la rete LAN.
Al fine di risolvere questa problematica sono stati messi a punto vari tipi di protocollo che hanno però tutti lo stesso scopo: instaurare una connessione protetta ed autenticata fra un host esterno ad una rete LAN e la rete LAN stessa, consentendo ad un host esterno l'accesso alle risorse della rete interna, come se si trovasse fisicamente direttamente collegato alla rete stessa. Una rete così costituita è detta Virtual Private Network (VPN, rete privata virtuale). Grazie a questi protocolli è possibile per un nodo che si trovi collegato alla rete LAN mediante una rete esterna, tramite un firewall ed un apposito processo di "attestazione", autenticarsi ed instaurare una comunicazione bidirezionale protetta mediante cifratura, che consente al nodo stesso di operare nella rete, a livello funzionale, come se fosse fisicamente nella rete stessa.

4.8 Qualità del servizio (QoS)

La coesistenza di diversi flussi dati sul medesimo canale di comunicazione, anche se

si tratta di canali ad elevata capacità come possono essere gli odierni mezzi fisici per la comunicazione Ethernet, viene a porre dei problemi di qualità del servizio per le trasmissioni dati sensibili, ad esempio, alle latenze di comunicazione o al jitter delle stesse (variazioni istantanee delle latenze) [38]. Un esempio classico del problema sono i servizi di telefonia su IP (VoIP).
Semplificando la trattazione di un problema molto complesso si può dire che al fine di massimizzare l'efficenza del trasporto delle informazioni sono state sviluppate opportune tecniche di marcatura dei pacchetti, a vari livelli dello stack protocollare, per indicare la priorità di invio dei pacchetti stessi e ridurre quindi la latenza per i pacchetti relativi a servizi particolarmente sensibili a questo parametro. Queste informazioni sono interpretate dai vari apparati posti sulla rete (in particolare access point wireless, switch, router e firewall) al fine di cercare di garantire la massima efficienza nel trasporto delle varie informazioni che devono condividere l'infrastruttura di comunicazione. Alcuni degli standard che definiscono politiche di tipo QoS sono: IEEE 802.1p, IEEE 802.1q e IEEE 802.11e.

Capitolo 5

Un sistema di automazione su Ethernet

La verità si ritrova sempre nella semplicità,
mai nella confusione.

– Isaac Newton

In questa sezione verranno descritte la struttura, le componenti ed il funzionamento del sistema progettato nel corso dell'attività del dottorato.
Per prima cosa verrà descritta l'astrazione utilizzata per eseguire il progetto. Si passerà poi ad una descrizione della gerarchia fisica, ovvero dei dispositivi che si occupano delle varie funzioni. In seguito verrà riportata una spiegazione dettagliata del funzionamento delle componenti logiche del sistema, che implementano le funzioni sfruttando la gerarchia fisica espressa. Successivamente verrà riportata una descrizione dell'architettura di rete necessaria alla comunicazione fra i vari elementi (sia fisici che logici) e dei protocolli di comunicazione sfruttati per la stessa. Infine si presenteranno gli strumenti e le procedure di progettazione e configurazione del sistema, seguite dall'esposizione delle politiche di gestione.
Nel corso della lettura sarà importante mantenere presenti i paradigmi di astrazio-

ne descritti nel primo paragrafo, in quanto rappresenteranno il riferimento costante per comprendere sia le dinamiche di comunicazione, sia quelle di attuazione e configurazione.

5.1 Filosofia

Premessa fondamentale alla comprensione della struttura del sistema è la volontà di utilizzare sensori ed attuatori a larga diffusione nel mercato dell'automazione domestica ed industriale in un sistema integrato basato sulla rete Ethernet. Per ottenere questo è stato necessario progettare e realizzare un dispositivo di interfacciamento fra i protocolli di campo attualmente utilizzati ed un protocollo di livello più alto, adatto alla gestione integrata dell'intero sistema, sia dal punto di vista della supervisione, sia dal punto di vista della gestione ed automazione.

Elemento chiave del processo è l'astrazione di ogni elemento del sistema, che diviene un "oggetto", con indirizzamento univoco e caratteristiche comuni standardizzate. Ciò consente di ottenere una gestione efficiente ed uniforme delle risorse, lasciando al tempo stesso un'ampia flessibilità per la gestione delle specifiche caratteristiche dei vari dispositivi utilizzabili [39, 40, 41, 42, 43, 44].

5.2 Gerarchia Fisica

La struttura fisica del sistema è di tipo intrinsecamente gerarchico ed è schematizzato in Figura 5.1. Gli elementi fisici del sistema sono:

- i sensori e gli attuatori (PN, Peripheral Node, Nodi Periferici) che si trovano al livello di campo ed hanno la funzione di interfacciarsi con l'ambiente;
- i FEIM (Field Ethernet Interface Module, cfr. sez. 5.2.2);
- i server locali, ovvero degli elaboratori dedicati alla gestione di aree specifiche;
- il supervisor, ovvero un server che ha la funzione principale di coordinare a livello alto l'intero sistema.

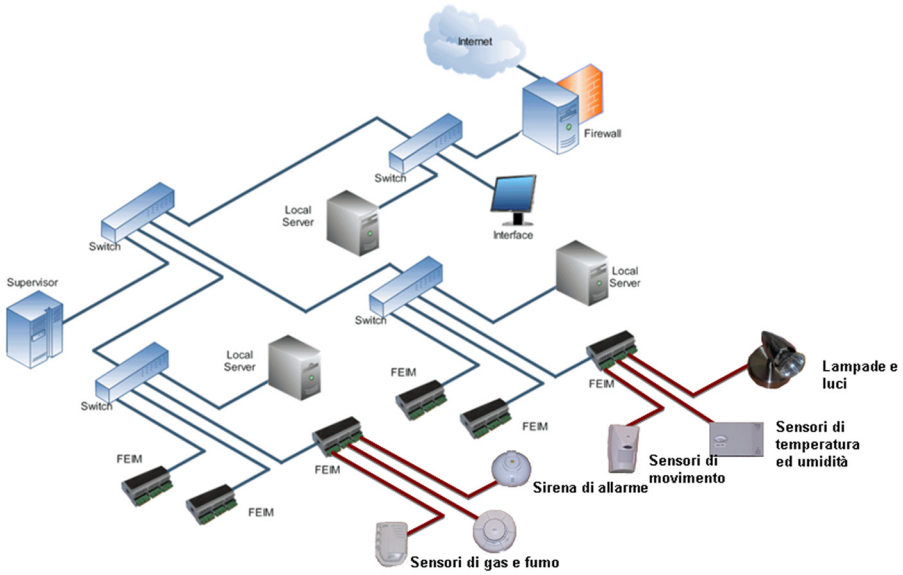


Figura 5.1: Schema della gerarchia fisica del sistema.

La gerarchia fisica del sistema è pensata per consentire un'adeguata ripartizione del carico di elaborazione e trasmissione dati, garantendo l'efficenza, la scalabilità e la tolleranza ai guasti dei vari elementi del sistema (cfr. sez. 5.7.4).
Di seguito sono descritti nel dettaglio gli elementi fisici del sistema.

5.2.1 Livello di campo

Al livello più basso della gerarchia troviamo gli elementi di campo, ovvero sensori ed attuatori installati all'interno della struttura.
Il sistema è progettato per accogliere dispositivi con interfacce di comunicazione su protocolli standard dell'automazione domestica e di edificio. In particolare sono previsti alcuni sensori ed attuatori standard:

- sensori di condizioni ambientali, ad esempio temperatura ed umidità;
- sensori per la sicurezza ambientale, ad esempio fumo ed allagamento;

- sensori di sicurezza anti-intrusione, ad esempio movimento ed apertura varchi;
- pulsanti per luci, campanelli e chiamate infermieristiche;
- sensori di luminosità;
- relè e dimmer (regolatore di corrente pilotato da un segnale che permette di variare la luminosità di un corpo illuminante) per il controllo dell'illuminazione;
- sensori di potenza assorbita;
- relè per l'intercettazione delle prese di alimentazione;

Questi sensori presentano in genere un'interfaccia standard, rappresentata da un contatto pulito, oppure (se analogici), da un'uscita in tensione in standard 0–10 V o 4–20 mA. L'alimentazione nella maggior parte dei casi è a 12 V corrente continua. Ciò consente quindi di avere a disposizione per l'installazione un insieme considerevole di dispositivi ad ampia diffusione, e quindi a costi contenuti, che possono essere anche fra loro intercambiabili.
In definitiva, il vantaggio nell'utilizzo di questo genere di sensori di campo è l'assenza di un'interfaccia proprietaria dedicata e di elettronica di comunicazione complessa a bordo. Ciò riduce i costi, allarga l'offerta di prodotti compatibili ed evita di legare il funzionamento del sistema ad una specifica cerchia di produttori.
È da notare che fra i sensori vengono inclusi anche tutti i pulsanti utilizzati per accendere le luci e suonare i campanelli. Inoltre sono previsti come sensori anche contatti ausiliari affiancati agli interruttori automatici modulari da quadro elettrico, che permettono di includere nel sistema informazioni sullo stato degli stessi.
A livello logico (cfr. sez. 5.3) sensori ed attuatori di campo sono suddivisi in: pulsanti (button), interruttori (switch), sensori analogici (analog in), relè monostabili (relè mono), relè bistabili (relè bi) e uscite analogiche (analog out). Il significato di queste astrazioni ed i motivi delle scelte sono descritti nel paragrafo relativo agli Oggetti (5.3.1).

5.2.2 Gestione del campo: il FEIM - Field Ethernet Interface Module

Per rendere possibile la comunicazione fra i sensori di campo con interfaccia standard ed il sistema, utilizzando la rete Ethernet, si è reso necessario progettare (cfr. cap. 6) un elemento di interfacciamento: il FEIM. Il modulo non è però meramente un'interfaccia di comunicazione e conversione di protocollo: si tratta di un elemento intelligente di elaborazione delle informazioni, in grado di operare decisioni locali sulla base di regole predeterminate e di modificare il proprio comportamento in base alle condizioni di funzionamento del resto del sistema, al fine di garantire il massimo dell'affidabilità, anche in caso di guasto parziale o totale del sistema di supervisione o comunicazione (cfr. sez. 5.7.4).
In sintesi, le funzioni del FEIM sono:

- leggere fino a 21 ingressi digitali a contatto pulito;
- leggere fino a 8 ingressi analogici (4 in standard 0–10 V, 4 in standard selezionabile 4–20 mA o 0–10 V);
- controllare fino a 12 uscite di potenza (corrente massima 240 mA, tensione massima 24 V);
- fornire 4 uscite analogiche in standard 0–10 V;
- alimentare i sensori a 12 V partendo dall'alimentazione a 24 V fornita al sistema;
- comunicare via TCP/IP verso il server locale tutte le variazioni dello stato del campo;
- eseguire le attuazioni richieste tramite TCP/IP dai server locali;
- elaborare le regole locali sulla base della configurazione impostata e sulla base del profilo di funzionamento attivo (cfr. sez. 5.7).

I moduli sono progettati fondamentalmente per fornire lo stato aggiornato istante per istante del campo al sistema di supervisione e per eseguire le procedure di attuazione sullo stesso sulla base dei comandi impartiti dagli LMP. Sono però anche in

grado di comunicare direttamente gli uni con gli altri, sfruttando una comunicazione di tipo P2P, ovvero una comunicazione di tipo paritario fra nodi appartenenti ad un sistema o ad una rete, che quindi sono in grado di interagire senza la necessità di server di coordinamento o interfacciamento, quindi sono capaci di eseguire regole che coinvolgono attuazioni anche su oggetti controllati da altri moduli. Questa potenzialità è sfruttata per l'implementazione a bassa latenza di operazioni che si devono svolgere in breve tempo, quali ad esempio l'accensione di un elemento di illuminazione alla pressione del relativo pulsante, o il controllo di un sistema di intercettazione dell'acqua nel caso venga rilevato un principio di allagamento. Inoltre questa funzione può essere sfruttata, abilitando eventualmente anche ulteriori regole, in caso di malfunzionamento del collegamento con il sistema di supervisione, sia esso causato da un problema sull'unità di supervisione o dal collegamento di rete con la stessa, sia da un eventuale mancanza di energia che coinvolga solo una parte del sistema. In tutti questi casi il modulo, grazie al meccanismo dei profili (cfr. sez. 5.7) può continuare a garantire il massimo livello di efficienza e funzionalità possibili con gli elementi raggiungibili e funzionanti, istante per istante, all'interno dell'intero sistema.

Funzione intrinseca di ciascun FEIM è anche l'astrazione del livello di campo verso l'architettura logica (cfr. sez. 5.3), quindi ogni valore letto dal campo, sia esso di tipo digitale o analogico, viene condizionato (se necessario) e poi riportato all'LMP (Local Management Process, cfr. sez. 5.3.3) come valore già significativo all'interno del sistema. Per fare questo, mediante configurazione tramite rete, i valori logici letti dal campo possono essere intesi come diretti oppure negati, ovvero si può avere che un contatto pulito chiuso corrisponda ad una variabile logica al valore 1 (se diretto) oppure 0 (se negato). Lo stesso vale per le uscite binarie, che possono essere viste come normalmente aperte o normalmente chiuse, mentre a livello logico con il valore 1 si indica sempre chiuso (attivato) e con 0 sempre aperto (disattivato).
Per quanto riguarda ingressi ed uscite analogiche, il FEIM si occupa di tutte le procedure di correzione di errori di offset e guadagno, oltre che dell'eventuale linearizzazione fosse necessaria (mediante interpolazione su tabella di look-up). I parametri di offset e guadagno vengono anche utilizzati per la conversione dei valori di tensione

(ad esempio in rage 0–10 V) o di corrente (ad esempio 4–20 mA) nelle rispettive grandezze rappresentate, ad esempio gradi centigradi o percentuale di umidità relativa, o ancora luminostià ambientale in lux. In questo modo vengono comunicati al sistema di supervisione solamente dati direttamente gestibili e del tutto indipendenti dallo specifico sensore. In caso di sostituzione del sensore, se necessario, è sufficiente riconfigurare il FEIM, senza intervenire sui livelli superiori dell'architettura.

Il modulo viene alimentato a 24 V in corrente continua mediante un opportuno sistema di alimentazione (cfr. sez. 5.2.6). Questa tensione non è però adatta alla maggior parte dei dispositivi di sicurezza comunemente in commercio, i quali operano normalmente a 12 V. Per questo motivo il FEIM integra una sezione di alimentazione che, oltre a consentire il funzionamento del modulo stesso, fornisce anche una uscita di potenza a 12 V per tutti i moduli sensori ad esso connessi. Ciò riduce i cablaggi necessari ed è in linea con l'ottica gerarchica del sistema.

All'interno di un'abitazione di medie dimensioni (circa 100 m^2 di superficie) sono necessari in media circa 5 moduli. Il numero ovviamente dipende dalle funzionalità che si richiedono e dal tipo di intervento (se si opera in fase di progettazione degli impianti o in fase di conversione ed integrazione di un impianto esistente).

5.2.3 Server Locali

I server locali sono dispositivi di elaborazione incaricati della gestione di uno specifico gruppo di FEIM e degli oggetti da loro controllati. Si può trattare di normali PC (Personal Computer), oppure possono essere elaboratori di tipo embedded, quali ad esempio PC con motherboard formato mini-ITX [45].
Su ciascun server locale sono in esecuzione uno o più processi di gestione locale, chiamati LMP (Local Management Process, cfr. sez. 5.3.3).
Il funzionamento degli LMP verrà descritto in seguito nel corso della trattazione, ma le funzioni principali riguardano la registrazione degli eventi di campo, l'interfacciamento, sia con il sistema di supervisione centrale, sia con le interfacce grafie di gestione (GUI, Graphic User Interface), l'implementazione di regole sofisticate, che possono tenere in considerazione svariati parametri correlati con lo stato presente e passato del sistema, l'orario, configurazioni dinamiche fornite dal sistema di gestione

gerarchicamente superiore.
I server locali sono l'elemento chiave per la scalabilità e la gestione efficiente del sistema. Ciascun server locale può gestire uno o più gruppi di FEIM, a seconda di quanti LMP sono in esecuzione. Essi dovrebbero essere collegati in prossimità dei FEIM da controllare, non perché non sia possibile farli operare anche a distanza elevata, visto che comunque operano su rete Ethernet, ma per maggiore affidabilità: ciascuno di essi dovrebbe essere collegato in prossimità del centro stella Ethernet che collega fra loro i FEIM controllati. In questo modo, se anche dovesse esserci un problema di connessione verso il resto della rete, le funzionalità di gestione del gruppo di FEIM controllati rimarrebbero inalterate (cfr. sez. 5.2.7).
Un particolare da notare è che i server locali sono normali PC di tipo x86 (o x86-64), quindi per questa funzione possono eventualmente essere utilizzati anche dei normali PC desktop già presenti in un'abitazione, o macchine virtuali che vengono eseguite su PC desktop o su server che hanno anche altre funzioni, legate ad esempio a servizi VoIP o di intrattenimento.

5.2.4 Server Supervisor

Il server di supervisione è un server dedicato alla gestione a livello di edificio. Su di esso è in esecuzione il processo di supervisione (SP, cfr. sez. 5.3.5). Esso può anche fungere da gateway verso la rete internet, ma non è obbligatorio. Inoltre il server di supervisione può coincidere con un server locale, sia che questo sia un normale PC o un PC embedded, visto che le risorse fisiche necessarie sono comunque proporzionali alla complessità della rete da controllare. È da notare che il Server Supervisor, in quanto unico ad eseguire il processo SP, deve essere particolarmente affidabile, oppure deve essere previsto un meccanismo di ridondanza fisica (o logica) che permetta di rilanciare il processo SP su un'altra macchina in caso di guasto grave. È comunque importante osservare che in caso di guasto, il resto del sistema, ed in particolare il server locali e quindi gli LMP, continuano ad operare normalmente, garantendo la quasi totalità delle funzioni.
Il Supervisor è indispensabile in sistemi particolarmente estesi, che comprendono diversi Server Locali o prevedono la connessione contemporanea di svariate interfac-

ce grafiche utente. In queste situazioni il processo SP richiede intrinsecamente una quantità di risorse (memoria e velocità di elaborazione) che mal si conciliano con elaboratori embedded a basso costo e consumo. Questa esigenza si prevede si manifesti solamente nel caso di infrastrutture di dimensioni medio-grandi, che quindi sono anche adatte all'installazione di PC server dedicati alle funzioni di coordinamento ed accesso verso l'esterno.

5.2.5 Interfacce utente

Le interfacce utente sono qui intese come postazioni dedicate all'interazione con il sistema da parte dell'utente. Sebbene i processi di interfacciamento possano operare su qualunque PC in grado di eseguire applicazioni Java SE[1] (cfr. sez. 5.3.6), all'interno delle installazioni sono in genere previste una o più postazioni che presentano un'interfaccia sempre attiva, per la supervisione ed il controllo del sistema. Le postazioni sono previste come Panel PC, ovvero PC on monitor a cristalli liquidi (LCD) e dotate di tecnologia touch-screen (schermo tattile) per semplificare al massimo l'interazione, anche da parte di personale non addestrato all'uso dei PC in generale.
Le interfacce utente possono però essere anche implementate su terminali mobili aventi connessione Wi-Fi, ad esempio PDA (palmari) o telefoni cellulari con connessione Wi-Fi. Per ottenere questo è però necessario utilizzare interfacce semplificate, adatte a schermi molto piccoli, eventualmente non touch-screen. Tali interfacce sono attualmente in fase di sviluppo.

5.2.6 Alimentazione

Un particolare riguardo deve essere prestato alla progettazione del sistema di alimentazione, in un contesto di automazione domestica, ed in particolare in contesti dove il sistema si vuole sia un supporto alla sicurezza anche di persone con difficoltà.

[1] Java SE: Java è un linguaggio di programmazione progettato per la produzione di codice che viene compilato per l'esecuzione su specifiche macchine virtuali, dette Java Virtual Machine. La versione SE è la Standard Edition e si differenzia dalla ME, Mobile Edition, per una serie di funzionalità, sia in termini di librerie che grafiche. Per questo motivo è necessario specificare il framework di riferimento.

Il primo elemento da considerare è la gestione delle condizioni di mancanza di alimentazione, in quanto si tratta di condizioni che, pur non frequenti nella maggior parte delle zone, caratterizzano momenti di criticità elevata. Per gestire tali condizioni ogni elemento del sistema deve possedere una riserva di alimentazione, che ne consenta l'operatitivà per un periodo di tempo maggiore della durata media prevista delle interruzioni di corrente. Ad esempio nelle zone urbane le durate dei periodi di interruzione sono in genere ridotte, sia per la presenza di personale tecnico nelle vicinanze, sia per la molteplicità di interessi economici che vengono ad essere compromessi in caso di estesi black-out; viceversa nelle zone rurali o montane le interruzioni possono avere durate superiori. Per questo è necessario progettare opportunamente i sistemi di continuità.

Il sistema progettato prevede un'alimentazione a 24 V corrente continua, che alimenta tutti i moduli FEIM, i relè e, tramite i FEIM, tutti i PN. L'alimentazione è fornita mediante un modulo di conversione di energia che può erogare 10 A a 24 V e ne viene installato uno ogni 5–7 moduli, al fine di garantire uno sfruttamento ottimale del dispositivo, lasciando comunque margini per espansioni e sovraccarichi istantanei durante le commutazioni degli elementi elettromeccanici. Ad ogni alimentatore viene affiancato un gruppo di continuità operante alla tensione di uscita, di estrazione industriale, che risulta estremamente efficace, in quanto durante la mancanza di alimentazione non viene richiesta nessuna conversione di energia, che andrebbe a ridurre l'efficienza del processo e conseguentemente la durata del funzionamento. È inoltre da notare che i FEIM ed i sensori ad esso collegati possono operare a tensioni inferiori ai 24 V, anche se i relè in genere non possono attivarsi al di sotto dei 20 V, il FEIM ed i sensori a 12 V ad esso collegati continuano ad operare anche quando la tensione scende al di sotto dei 18 V, prolungando di fatto il funzionamento fino alla tensione minima di sicurezza delle batterie (di solito nell'ordine dei 18–19 V appunto). Per tutti questi motivi è preferibile questo approccio rispetto all'utilizzo di UPS (Uninterruptible Power Supply) operante alla tensione di rete (230 V), che comporta una doppia conversione di energia dalla tensione di batteria interna all'UPS, poi a 230 V corrente alternata ed infine di nuovo a 24 V corrente continua.

Al fine di aumentare al massimo la durata delle batterie dei gruppi di continui-

tà i FEIM hanno profili di funzionamento (cfr. sez. 5.7) particolari che, attivati nel caso di una mancanza di alimentazione di rete, permettono di disattivare (secondo le configurazioni preimpostate) i relè relativi ai carichi che senza l'alimentazione di rete non possono comunque operare, quali ad esempio le luci, e risparmiare quindi potenza necessaria a mantenere i relativi relè eccitati, ripristinando poi le condizioni precedenti di attivazione al termine del black-out.

Per quanto riguarda l'alimentazione degli apparati di rete e di quelli di supervisione è invece necessario, in generale, affidarsi ad UPS classici, che possano garantire l'operatività anche in assenza di alimentazione. Ovviamente i componenti più critici sono gli apparati di rete, in quanto in caso di spegnimento delle unità di supervisione il sistema è comunque in grado di funzionare, grazie alle capacità di comunicazione P2P dei FEIM ma, se gli apparati di rete vengono a disattivarsi, solamente le regole che coinvolgono sensore ed attuatore connessi al medesimo FEIM possono essere attive, venendo meno le possibilità di comunicazione fra i moduli. Al fine di ridurre gli effetti di una tale evenienza è possibile adottare politiche opportune di dimensionamento degli UPS ed è utile, anche per questioni di affidabilità ed ove possibile, utilizzare apparati indipendenti per la continuità degli apparati di rete e per le unità di supervisione.

La strutturazione gerarchica a più livelli degli apparati di rete (cfr. sez. 5.2.7), può essere un'opportunità per aumentare la tolleranza ai guasti, non soltanto degli apparati stessi, ma anche ai black-out. Una possibilità aggiuntiva potrebbe essere quella di porre piccoli switch di rete, che mettano in contatto solo i vari FEIM all'interno di un gruppo fra di loro, alimentandoli poi con un'UPS indipendente, o addirittura direttamente alla tensione 24 V che alimenta i FEIM stessi, utilizzando moduli pensati per il mondo industriale.

L'utilizzo di apparati di tipo PoE (cfr. sez. 4.3) permette di alimentare diversi dispositivi (in futuro anche i FEIM si prevede possano utilizzare questa tecnologia) semplicemente utilizzando i cavi di segnale. Ciò evita di dover portare alimentazione di rete a diverse prese nelle vicinanze dei singoli apparati, quali access point Wi-Fi, telefoni e cordless VoIP, videocamere di sorveglianza, ... tutti dispositivi cui deve

in generale essere garantito il funzionamento anche in caso di black-out e che quindi avrebbero richiesto la distribuzione di un'alimentazione di rete preferenziale sotto UPS, che in questo modo ricevono invece un'alimentazione che proviene dal loro switch, che funge da dispositivo di alimentazione e può essere posto centralmente sotto UPS, direttamente nel rack dove sono installati tutti gli apparati. Anche questo è un'importante elemento di affidabilità e di riduzione dei costi complessivi di installazione e manutenzione, in quanto non sono presenti tutti gli adattatori di rete per ogni singola apparecchiatura e la manutenzione è centralizzata in un solo punto accessibile.

Un'ultima nota di crescente importanza riguarda la protezione degli apparati dalle scariche atmosferiche, che possono propagarsi attraverso le linee alimentazione, come anche attraverso le linee dati provenienti dall'esterno [46]. Per proteggere le funzionalità del sistema e l'investimento fatto è necessario prevedere opportuni scaricatori di sovratensioni transitorie, secondo uno schema distribuito adatto, che protegga tutti gli apparati collegati, dai moduli di alimentazione di campo, a quelli di rete, a quelli di supervisione.

5.2.7 Organizzazione della struttura di rete

La struttura della rete Ethernet, a livello meramente funzionale, è del tutto ininfluente ai fini del funzionamento del sistema. Tuttavia, nella pratica, un'attenta progettazione di questo elemento fondamentale può portare grandi benefici, sia in termini di efficienza nello sfruttamento della banda, sia in termini di affidabilità complessiva del sistema sotto diversi punti di vista. Inoltre la scelta degli apparati stessi deve essere oculata e vagliata in funzione non solamente dell'automazione, ma anche degli altri servizi aggiuntivi che si vogliono vengano veicolati dalla rete stessa. In particolare, ad esempio, al fine consentire un funzionamento ottimale dei sistemi di tipo VoIP è necessario che venga correttamente supportato il QoS (cfr. sez. 4.8).

La struttura delle reti Ethernet moderne è intrinsecamente gerarchica: questo perché i collegamenti sono realizzati mediante cavi UTP (o FTP) Cat. 5e o superiori, fra loro collegati mediante switch (cfr. sez. 4.3.3) che quindi agiscono ciascuno come centro stella di rete, smistando i vari pacchetti Ethernet/IP a seconda delle necessità.

È quindi possibile, secondo questo paradigma, avere un unico switch che collega fra loro tutti i FEIM con tutte le unità di supervisione ed eventualmente con tutte le altre apparecchiature presenti nell'abitazione. Questo approccio, seguito a volte nelle realtà commerciali, ha certamente il vantaggio della semplicità e della riduzione delle latenze complessive. Ha però lo svantaggio di richiedere collegamenti mediamente più lunghi e di introdurre un singolo punto di guasto critico nel sistema (single point of failure), in quanto un guasto dello switch comporta l'immediata interruzione di tutte le comunicazioni di rete.
Al fine di ridurre l'effetto di un guasto è quindi auspicabile l'utilizzo di più apparati fra loro connessi in modo gerarchico, cosicché il guasto di uno di essi comporti l'interruzione di un solo servizio, o di una parte di esso, lasciando possibilità agli altri di operare.
In particolare è quindi possibile ipotizzare, solo a titolo di esempio, uno switch che gestisca i servizi di automazione, uno che gestisca la telefonia, uno che colleghi fra loro tutte le prese dedicate ai PC ed agli access point Wi-Fi. Tutti questi switch sono poi collegati fra loro ad un unico switch, che collega anche il router verso l'esterno (ADSL o altro). In questo modo il guasto dello switch gerarchicamente superiore isola i sottosistemi gli uni dagli altri, ed anche dall'esterno, ma i servizi interni rimangono operativi: sono operative le telefonate interne, è attiva la connessione fra i PC interni e le loro periferiche di rete, quali stampanti, NAS (Network Attached Storage), ... ed il sistema di automazione continua ad operare inalterato, in quanto i FEIM sono connessi fra loro ed ai server di gestione. In caso di un guasto di uno degli switch di livello gerarchico inferiore, solo il sistema interessato sarà fuori uso, ma gli altri non ne risentiranno.
Un altro approccio può essere di tipo topologico, anziché funzionale: è possibile collegare sotto il medesimo switch tutti gli apparati di un'area dell'edificio, sia esso un appartamento in un condominio, un insieme di uffici o laboratori, ... In questa configurazione, in caso di guasto dello switch gerarchico superiore, la situazione è la stessa descritta nel caso precedente ma, nel caso di malfunzionamento di uno switch di livello inferiore, si avrà l'isolamento di tutti gli apparati in una determinata area, anziché quelli afferenti ad un singolo servizio. Anche questa è una scelta pos-

sibile, come sono possibili vari livelli intermedi fra le due. Ciò che è importante è fare una scelta che tenga conto delle specifiche necessità della singola installazione e prevedere i vantaggi ed i disagi di ciascuna scelta in caso di guasto.

Un altro punto da considerare è che, se possibile, è utile mantenere sempre una riserva di porte inutilizzate su uno switch, al fine di mantenere spazio per futuri ampliamenti. Se più switch sono posti nel medesimo armadio, lasciare uno spazio complessivo in numero di porte libere pari al numero di porte mediamente utilizzato su ciascuno di essi consente, in caso di emergenza dovuta al guasto di uno di essi, di spostare temporaneamente tutte le connessioni dello switch guasto sulle posizioni libere degli altri, ripristinando così immediatamente le funzionalità della rete, in attesa che possa essere installato il sostituto di quello danneggiato.
Una scelta che può aumentare l'affidabilità del sistema è quella di mettere piccoli switch (eventualmente installabili nei quadri elettrici standard) che connettono fra loro i FEIM di aree dell'edificio, poi fra loro connessi da switch da rack o di altro tipo a livello gerarchico superiore. Ciò consente di elevare l'affidabilità del sistema, in quanto in caso di guasto dello switch gerarchicamente superiore essi possono mantenere il contatto fra i FEIM dell'area specifica e mantenere quindi inalterate tutte le funzioni di base, grazie alla comunicazione P2P. Inoltre questo genere di switch può essere alimentato direttamente dalla tensione a 24 V che alimenta i FEIM, così da avere anche una maggiore indipendenza dal punto di vista energetico (cfr. sez. 5.2.6).

5.3 Gerarchia Logica

A livello logico il sistema astrae completamente tutto quello che riguarda i singoli dettagli di sensori ed attuatori. Le informazioni necessarie all'astrazione sono fornite in fase di configurazione del livello di campo e sono ignote al resto del sistema, che opera solamente sul livello astratto.

L'elemento fondamentale dell'astrazione è la definizione del concetto di "oggetto logico", cui ci riferimento di seguito semplicemente come *Oggetto*. Un *Oggetto* è un elemento del sistema che può essere, in senso più ampio, letto e/o scritto. Divengono quindi *Oggetti* tutti i sensori, ma anche i FEIM o gli altri processi di gestione di se-

guito descritti. Ciascuno ha delle proprietà specifiche, che vengono riassunte sotto il termine di "variabili logiche" o semplicemente *Variabili*. Ciò consente di interagire con qualunque elemento del sistema a livello astratto (logico) utilizzando un indirizzamento a 32 + 32 bit: 32 sono utilizzati per identificare univocamente un *Oggetto* nel sistema, mentre gli altri 32 identificano la *Variabile* dell'*Oggetto* stesso (anche se esistono eccezioni a questo approccio, che saranno spiegate nelle sezioni relative).
Una rappresentazione grafica generica della gerarchia logica è presentata in Figura 5.2. Le varie componenti saranno descritte nei prossimi paragrafi.

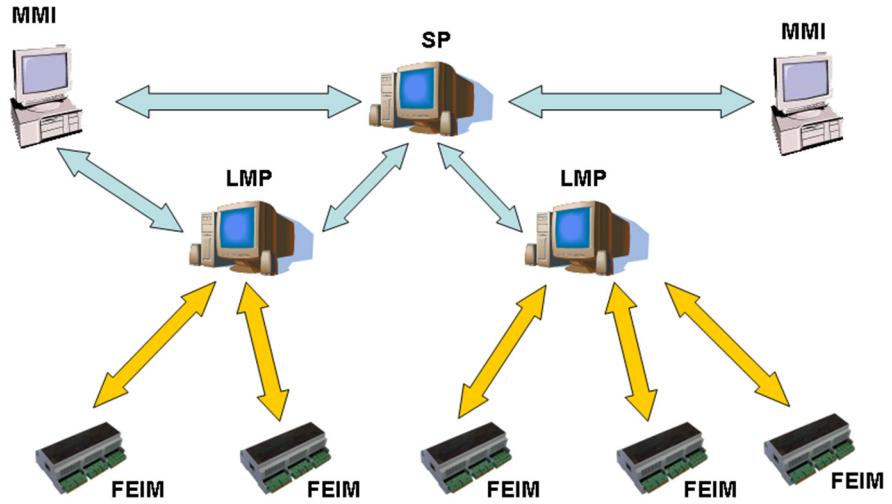


Figura 5.2: Schema della gerarchia logica del sistema.

5.3.1 Oggetti

Un oggetto logico, o *Oggetto*, è l'unità fondamentale di interazione e memorizzazione del sistema. Lo stato del sistema non è altro che il valore complessivo di tutti gli *Oggetti* e delle loro *Variabili*.
Ogni *Oggetto* è identificato univocamente a livello di sistema mediante una varia-

bile a 32 bit. Fanno eccezione i valori da 0xFFFFFF00[2] a 0xFFFFFFFF, che sono considerati oggetti privati e quindi non accessibili dall'esterno dell'*Oggetto* stesso. Questa scelta è stata fatta per ridurre la complessità dei firmware dei FEIM e degli altri elementi del sistema, consentendo loro di gestire alcuni elementi interni alla stregua degli altri *Oggetti*, sfruttando l'astrazione implementata, senza che questi fossero accessibili dall'esterno e senza che dovessero occupare (inutilmente, dato che non sarebbero accessibili) posizioni univoche all'interno dello spazio di indirizzamento del sistema. Un esempio è il pulsante di reset logico dei FEIM (cfr. sez. 6.6).

Per poter interagire in modo completo con un oggetto complesso sono state definite le variabili logiche, cui ci si riferisce in seguito come *Variabili*. Anch'esse sono identificate univocamente mediante un valore a 32 bit ed analogamente agli oggetti le ultime 256 sono riservate per uso privato interno del software/firmware degli oggetti stessi.
Ogni oggetto ha almeno la variabile 0, che ne rappresenta in generale il valore del parametro fondamentale. Quando si dice che un oggetto ha un determinato valore, si sottintende che la *Variabile* 0 di tale *Oggetto* ha quel valore.
Il numero ed il tipo di dato rappresentati dalle *Variabili*sono liberi e devono essere quindi definiti in sede di configurazione. I tipi di dato possibili sono:

- booleano (bool)
- intero a 8 bit (char)
- intero senza segno a 8 bit (byte)
- intero a 16 bit (short int)
- intero senza segno a 16 bit (unsigned short int)
- intero a 32 bit (int)
- intero senza segno a 32 bit (unsigned int)
- valore in virgola mobile a singola precisione, 32 bit formato IEEE 754 (float)

[2] Valori esadecimali: la preposizione dei caratteri "0x" indica che il valore numerico è espresso in formato esadecimale.

Ad ogni valore inserito nel sistema come valore di una *Variabile* viene sempre associato un timestamp[3], al fine di avere informazioni corrette circa la successione degli eventi e poter utilizzare queste informazioni nella definizione delle regole operative del sistema. Ciò si è reso necessario al fine di eliminare possibili problemi di acronicità introdotti dalle latenze di rete nelle comunicazioni fra i vari elementi del sistema.

Non tutti gli *Oggetti* sono leggibili o scrivibili. Alcuni, ad esempio quelli che rappresentano gli interruttori, non possono essere scritti, ma solamente letti. Altri non possono essere neanche letti, ad esempio i pulsanti. Ciò perché lo stato di un pulsante non ha significato, in quanto l'informazione risiede nel fatto che questo sia premuto e rilasciato, quindi le probabilità di leggere il suo valore esattamente nel momento in cui viene premuto sono trascurabili. Ciò che è importante è l'evento associato alla pressione, non il valore istantaneo. Per questo motivo per gli *Oggetti* pulsanti (button) non è consentita la lettura, ma le regole (cfr. sez. 5.6) possono prenderli in considerazione, in quanto al momento della pressione (o del rilascio, a seconda della configurazione) il FEIM genera un messaggio di variazione, che può scatenare le regole che coinvolgono lo stato del pulsante. Altri oggetti possono essere sia letti che scritti, ad esempio i relè bistabli, utilizzati ad esempio per il controllo delle luci. Di questi oggetti è possibile conoscere lo stato attuale mediante lettura ed operarne l'accensione o lo spegnimento mediante la scrittura del valore relativo sull'*Oggetto* stesso.

5.3.2 Oggetti di campo

Si definiscono oggetti di campo gli *Oggetti* che rappresentano lo stato corrente di sensori ed attuatori collegati ai FEIM o eventualmente direttamente collegati ad Ethernet.

[3]Timestamp: numero che rappresenta il numero di secondi trascorsi dall'epoch, ovvero dal punto di origine del sistema di datazione in uso in un sistema informatico. Nel sistema progettato non è importante quale sia preso come epoch, in quanto sono operate le opportune conversioni al momento dell'invio e della ricezione dei pacchetti da altri sistemi. Attualmente viene preso come riferimento il 1 gennaio 1980 ed il valore è rappresentato come un numero a 32 bit per le comunicazioni con i FEIM, mentre sui sistemi Linux la base è rappresentata dal 1 gennaio 1970 ed il valore è rappresentato a 64 bit.

La scrittura di un valore su un oggetto di campo comporta l'immediata variazione del suo stato. Ciò avviene mediante la trasmissione di opportuni messaggi di rete, che richiedono la scrittura e quindi l'operazione stessa. Il FEIM che ha in carico la gestione dell'*Oggetto* trasmetterà una conferma al messaggio di scrittura, per informare il mittente se l'*Oggetto* è scrivibile o meno. Questa però non deve intendersi come effettiva conferma di scrittura, ma solo come correttezza formale del comando. Al momento (immediatamente successivo) della scrittura effettiva verrà inviata una notifica all'LMP di riferimento, per segnalare la reale variazione dello stato dell'attuatore.

Nel caso della lettura, invece, la risposta contiene già il valore letto, che si riferisce al valore più aggiornato attualmente disponibile della grandezza monitorata. Dipendentemente dalla configurazione del FEIM, questo può eventualmente differire dal valore attuale a meno di una soglia impostata e si riferisce all'ultimo istante di campionamento della grandezza stessa, secondo gli intervalli di campionamento impostati per lo specifico *Oggetto*.

Il comportamento degli oggetti di campo può essere verificato o modificato accedendo alle variabili diverse dalla 0 dell'oggetto stesso. Ciò permette al sistema di alterare alcune politiche di funzionamento rispetto alle configurazioni fornite al fine di ottenere comportamenti differenti in caso di necessità.
Il comportamento degli oggetti è inoltre determinato anche dal profilo di funzionamento del FEIM che li controlla, quindi le politiche di segnalazione degli eventi possono cambiare a seconda delle condizioni impostate. Tutto questo è trasparente al sistema di supervisione, in quanto implementato direttamente ed autonomamente dal FEIM.

Nell'astrazione degli oggetti di campo verso il sistema sono definiti, a livello di modulo FEIM, sei differenti tipi di oggetto, con caratteristiche specifiche, che possono rappresentare astrazioni di tutti i sensori ed attuatori attualmente previsti nel sistema.

Button Sono ingressi digitali dei quali non interessa sapere quando commutano da attivo a disattivo e viceversa, ma dei quali è interessante solamente un ciclo di attivazione, ovvero il passaggio dall'inattivazione all'attivazione e ritorno. Questi oggetti

generano una notifica solamente una volta per ogni ciclo e questa segnalazione può avvenire, a seconda della configurazione, al momento dell'attivazione o della disattivazione, ma in entrambi i casi la notifica è di attivazione, in quanto significa che è in corso un ciclo. Un esempio può essere un pulsante che serve ad accendere una luce, oppure un sensore di movimento, che genera fronti di salita multipli anche se lo stato di occupazione permane: anche in questo caso l'informazione riguarda il fatto che è stato rivelato un movimento, non che è presente un movimento e poi è cessato: l'assenza di fronti e quindi di segnalazioni indica che il movimento è cessato. L'uso di questa astrazione riduce del 50% le segnalazioni, evitando informazioni inutili. Non possono essere letti direttamente, in quanto lo stato di attivazione in questo caso è generalmente molto ridotto nel tempo e quindi conta solamente la segnalazione dell'avvenuto ciclo di attivazione.

Switch Sono ingressi digitali dei quali è importante lo stato. Sono quindi oggetti che possono essere letti e dei quali è possibile configurare la segnalazione sia dell'attivazione, sia della disattivazione. Un esempio sono tutti i sensori di sicurezza, ad esempio i sensori di fumo, quelli di allagamento, quelli di fuga gas combustibili, oppure i campanelli di richiesta di assistenza, in quanto in quel caso è utile fare riportare sull'attuatore, in genere un campanello o un buzzer, effettivamente la durata della pressione del campanello stesso, anche per mutuare in modo più naturale il comportamento atteso dagli utenti.

Analog in Sono ingressi analogici e possono essere letti in qualunque momento. Possono inoltre segnalare le variazioni della grandezza monitorata quando questa varca una soglia specificata in salita o discesa, oppure quando il valore corrente si discosta dall'ultimo valore segnalato più di una quantità assoluta impostabile. L'intervallo di aggiornamento delle letture è impostabile mediante le configurazioni dell'*Oggetto* memorizzate nel FEIM ed eventualmente modificate dinamicamente dall'LMP, se necessario.

Relè mono Sono uscite digitali che rappresentano dispositivi che devono essere attivati per un periodo di tempo preimpostato. Un esempio può essere il controllo di una luce in una parte comune, che dopo l'accensione si spegne automaticamente dopo un intervallo di tempo predefinito. Se l'intervallo di tempo è molto breve allora, come nel caso dei Button, non è sensato che venga consentita la lettura e la segnalazione di attivazione avviene solamente al termine dell'intervallo stesso. Se invece l'intervallo è sufficientemente lungo (al di sopra dei cinque secondi orientativamente), allora è possibile impostare un flag, che imposta il modulo per mandare una doppia notifica, di attivazione e disattivazione. I relè monostabili possono solo essere attivati con un comando, non possono essere disattivati. La loro disattivazione avviene solo al termine dell'intervallo impostato. Se vengono attivati nuovamente prima del termine dell'intervallo, al tempo di disattivazione viene sommato un nuovo periodo di tempo pari al periodo impostato, una sola volta per ogni intervallo. Quindi se alla scadenza manca meno di un intervallo di tempo e viene inviata una nuova richiesta di attivazione, l'istante di disattivazione viene aggiornato sommandovi un nuovo intervallo. Se invece l'istante di disattivazione è già stato aggiornato una volta, verranno ignorate ulteriori attivazioni, finché il nuovo tempo alla scadenza non scenderà al di sotto della durata di un intervallo originale.

Relè bi Sono uscite digitali che vengono utilizzare per controllare dispositivi che devono essere accesi e spenti in modo arbitrario. Possono controllare luci o prese di corrente, o ogni altro elemento controllabile con un relè. Possono essere letti o scritti senza restrizioni ed inviano segnalazioni sia in caso di attivazione, sia alla disattivazione.

5.3.3 Processi di gestione locale e loro gerarchia

I processi di gestione locale (LMP: Local Management Process) si occupano di gestire un gruppo (cluster) di FEIM ed i relativi PN collegati. Le funzioni svolte sono diverse, ma in particolare ciascun LMP hai il compito di gestire il proprio cluster eseguendo:

- acquisizione costante dello stato del campo, ovvero degli oggetti di campo e dei FEIM di sua pertinenza, mediante la ricezione delle notifiche di variazione di stato provenienti dai FEIM (e dagli eventuali oggetti dotati di interfaccia Ethernet nativa);
- registrazione (logging) di tutti gli eventi di campo o di gestione rilevanti;
- gestione delle regole di attuazione relative al cluster gestito;
- predisposizione ed invio delle configurazioni iniziali ai FEIM gestiti, sulla base della configurazione generale fornita.

Un LMP è in esecuzione su un'unità di supervisione, da solo o insieme ad altri processi che gestiscono altri cluster.
Gli LMP possono comunicare fra di loro utilizzando la rete Ethernet, ma in particolare essi devono comunicare con il processo di supervisione (SP, cfr. sez. 5.3.5) al fine di fornire a quest'ultimo informazioni riassuntive circa le condizioni del campo di loro pertinenza. Questa capacità di comunicazione P2P fra i server è simile a quella di comunicazione fra i FEIM ed ha gli stessi vantaggi: capacità di gestione diretta di condizioni che richiedono basse latenze e gestione delle situazioni di criticità, in cui non è possibile comunicare temporaneamente con l'SP.
Gli LMP non sono vincolati all'esecuzione su una specifica unità di supervisione. Ciò rende possibile la coesistenza di più processi sulla medesima macchina fisica, ma anche la "migrazione" dei processi da una macchina ad un'altra in caso di guasto. Ciò è possibile poiché il processo di supervisione verifica periodicamente la connessione con tutti gli LMP. Nel caso in cui non verifichi più la presenza nella rete di un dato processo può richiederne, in modo remoto, l'avvio su un'altra unità di supervisione (tenendo conto dello stato attuale di carico delle unità stesse) o anche avviarlo direttamente sulla propria unità di supervisione.
Gli LMP possono essere (se necessario) configurati anche su livelli gerarchici multipli, ovvero un LMP può essere configurato per gestire gruppi di LMP e non solo gruppi di FEIM. In questo modo è possibile fare scalare la complessità del sistema anche a strutture particolarmente estese, in cui la gestione di politiche di supervi-

sione che coinvolgano svariate decine di moduli possano beneficiare di un livello intermedio di gestione, che semplifichi il coordinamento ai livelli sia inferiori (che si occupano di politiche locali al cluster), sia superiori, che beneficiano di un maggior livello di astrazione nella gestione delle politiche di interi edifici o complessi di edifici.
Gli LMP, comunicando con lo stesso protocollo utilizzato per comunicare fra loro e con l'SP (cfr. sez. 5.4.3) e possono essere anche in contatto con una o più interfacce grafiche utente (GUI, cfr. sez. 5.3.6).

5.3.4 Oggetti virtuali

Oltre agli oggetti di campo ed ai vari *Oggetti* del sistema di supervisione, possono anche essere definiti degli oggetti virtuali. Tali *Oggetti* rappresentano funzioni avanzate che possono essere utili nella gestione del funzionamento del sistema, ma che non sono oggetti fisici o processi a se stanti. Tali *Oggetti* sono quindi definiti virtuali e sono privati di ciascun LMP.
Gli oggetti virtuali attualmente previsti sono:

- l'orologio: si tratta di un *Oggetto* che tramite le proprie variabili fornisce accesso al timestamp corrente, a ore, minuti, secondi, giorno, mese, anno, giorno della settimana. È necessario per la definizione di regole che tengano conto del tempo. È unico per ogni LMP;

- timer: *Oggetti* che si comportano come timer fisici per conto alla rovescia: possono essere impostati al valore voluto in secondi, avviati, fermati, riavviati o resettati;

- timeout: *Oggetti* compositi che hanno al loro interno variabili relative ad un numero arbitrario di timeout tutti della medesima durata. Sono utili nelle regole che prevedono una verifica di esecuzione di un'azione entro un tempo specificato.

5.3.5 Processo Supervisore

Il processo di supervisione (SP, Supervisor Process) è per molti versi molto simile ad un LMP, con la differenza che in generale non gestisce direttamente FEIM, ma coordina le politiche di gestione al massimo livello previsto nella struttura. Si occupa quindi della gestione degli allarmi a livello di struttura, di gestire le emergenze al livello più alto, coordinando gli interventi effettivi di campo demandati agli LMP e da questi ai FEIM.
Di fatto il processo SP ha il medesimo codice oggetto dell'LMP, ciò che cambia sono le configurazioni ricevute.

Unica funzione demandata in esclusiva all'SP è quella di permettere la connessione delle interfacce grafiche (GUI, cfr. sez. 5.3.6). Questa scelta è dovuta al fatto che le GUI devono registrarsi al fine di ricevere inizialmente un ID temporaneo dinamico, che le possa identificare all'interno del sistema nelle comunicazioni con gli altri oggetti, e successivamente devono ricevere informazioni riepilogative sullo stato del sistema e sulla presenza di allarmi. Tali informazioni sono contenute nel database aggiornato in tempo reale dall'SP e quindi è normale che sia il primo punto di connessione. Ciò consente anche alle interfacce di instaurare una sola connessione TCP/IP con il solo SP, senza avere la necessità di contattare ogni LMP nel sistema per estrapolare le informazioni necessarie.

È però da notare che nel momento in cui tramite l'interfaccia si vogliono avere informazioni dettagliare su un'area specifica della struttura, allora l'interfaccia grafica richiede all'SP le informazioni necessarie a contattare direttamente LMP incaricato di gestirla, per collegarsi direttamente ad esso ed ottenerne gli aggiornamenti in tempo reale. Questa politica è stata adottata al fine di impedire che il processo di supervisione divenisse un collo di bottiglia per tutte le comunicazioni fra le interfacce grafiche ed il sistema, anche nell'ispezione capillare dello stesso. Inoltre la capacità dell'interfaccia di collegarsi ai singoli LMP risulta utile nel caso in cui, una volta persa la connessione con l'SP a seguito di un problema di comunicazione o di un guasto, si renda necessario fornire tutte le informazioni ancora raggiungibili, collegandosi direttamente agli LMP noti.

5.3.6 Interfacce grafiche di gestione

Le interfacce grafiche di gestione (GUI, Graphic User Interface) sono processi (realizzati attualmente in linguaggio Java per piattaforma SE) che permettono all'utente di interagire con il sistema. Mediante le GUI è possibile avere informazioni riassuntive sullo stato dell'intero sistema, sulla presenza di condizioni di allarme o guasto e di interagire con i singoli oggetti controllati dal sistema presenti nell'edificio.
Le informazioni sono rappresentate mediante interfacce grafiche a pulsanti e mappe di tipo intuitivo, adatte ad essere presentate su monitor a cristalli liquidi (Liquid Crystal Display, LCD) con interfaccia sensibile al tatto (touch-screen).
Dalla schermata iniziale è possibile avere in un colpo d'occhio la situazione di allarmi e guasti attuale, mentre selezionando aree specifiche dell'edificio è possibile accedere a mappe grafiche nelle quali opportune icone rappresentano i vari oggetti e consentono di interagire con quelli modificabili, semplicemente toccando le icone relative. In Figura 5.3 e 5.4 sono riportati alcuni screen-shot del programma, relativi ai due locali tipo che sono stati rappresentati nel laboratorio per i test (cfr. sez. 7.1).
Le interfacce grafiche si registrano al sistema utilizzando il medesimo protocollo

Figura 5.3: Screen-shot del programma GUI: visualizzazione di una cucina.

Figura 5.4: Screen-shot del programma GUI: visualizzazione di una camera da letto con bagno.

di supervisione degli LMP e dell'SP. Da ques'ultimo ricevono un ID dinamico, che permette loro di interagire con il sistema fino alla disconnessione. Se necessario, le interfacce possono anche scaricare un opportuno file di configurazione, che permette di avere informazioni aggiornate sulla mappatura degli oggetti all'interno del sistema e sulle grafiche rappresentative della struttura, oltre alla struttura degli allarmi (cfr. sez. 5.5).

5.4 Protocolli di comunicazione

Al fine di ottenere una comunicazione efficiente fra i vari componenti del sistema è stato necessario decidere due protocolli con livelli di complessità differenti: uno per il livello di campo, ovvero per la comunicazione con i FEIM, ed uno per il livello di supervisione, ovvero per la comunicazione fra le unità di supervisione e con le interfacce grafiche.

Entrambi i protocolli utilizzano connessioni di tipo TCP/IP e quindi sono perfettamente compatibili ed integrabili in una rete Ethernet/IP standard.

5.4.1 Protocolli a livello di campo

A livello di campo i protocolli più diffusi nell'automazione industriale e domestica sono essenzialmente:

- contatto pulito;
- 0–10 V;
- 0–1 V;
- 4–20 mA;
- 0–20 mA;
- RS-485.

Un contatto pulito non è altro che un interruttore comandato, sul quale non è presente una tensione imposta dal dispositivo. Possono quindi essere letti dai sistemi di supervisione come circuiti aperti o chiusi senza nessuna restrizione, se non nelle tensioni e correnti massime e minime supportate. In pratica la quasi totalità dei dispositivi di sicurezza, ovvero sensori di movimento, contatti magnetici, barriere a infrarossi, sensori di fumo per sistemi di sicurezza (non di tipo analogico indirizzato), sensori di allagamento, ... utilizzano come uscite di campo uno o più contatti puliti per segnalare le condizioni di allarme, guasto, manomissione. Per quanto riguarda i sensori con uscita analogica, quali sensori di temperatura, umidità relativa, luminosità, ... essi utilizzano vari standard, che possono essere suddivisi a grandi linee in: uscite in tensione ed uscite in corrente.
Nel mondo industriale vengono utilizzate sovente uscite in corrente, in quanto hanno una maggiore immunità ai disturbi elettromagnetici anche su distanze elevate. Inoltre l'utilizzo di standard "a zero vivo", ovvero nei quali il valore minimo della grandezza misurata non corrisponde ad un'assenza di corrente, permettono di alimentare il dispositivo utilizzando il cavo di segnale e al tempo stesso verificare la condizione di guasto, in cui il cavo è interrotto o il dispositivo è guasto, in quanto il valore nullo di

corrente non è un valore ammesso nel normale funzionamento.
Nel mondo dell'automazione domestica sono invece diffusi gli standard in tensione, in quanto i collegamenti sono in genere più corti ed in ambiente meno ostile di quello industriale dal punto di vista delle interferenze. Inoltre questo standard consuma meno energia ed i dispositivi di lettura non richiedono resistenze tarate per una conversione precisa dei valori letti.
Il protocollo RS-485 viene utilizzato per il collegamento con strumenti di misura utilizzati nel mondo industriale o con piccoli pannelli di interazione utente che utilizzano poi protocolli standard di livello superiore, come ad esempio il Modbus [47].

5.4.2 Protocollo di gestione del campo

Per la scelta del protocollo del livello di campo sono stati vagliati diversi protocolli standard, fra i quali il più adatto sembrava essere l'SNMP (Simple Network Management Protocol, RFC 1157) [48, 49]. Il limite di quel protocollo risiede però nella necessità di codificare i messaggi trasmessi utilizzando una speciale codifica: ASN.1 (ISO 8824-1:2002). Tale codifica risultava essere relativamente complessa per il tipo di applicazione che si stava sviluppando e la richiesta di risorse di elaborazione e memoria non erano giustificate per le necessità di comunicazione. Inoltre l'uso standardizzato dell'SNMP richiedeva la costruzione di un albero di definizione relativamente complesso, cui doveva essere ufficialmente richiesta l'aggiunta di un nodo specifico per la nostra applicazione.
Sulla base di queste considerazioni si è deciso di sviluppare un semplice protocollo di livello applicazione, che sfruttasse la garanzia di consegna ed integrità del TCP/IP per trasmettere le informazioni. Il protocollo è di tipo binario e supporta un modello di tipo master-slave, in cui i sistemi di supervisioni operano come master, inviando comandi, ed i FEIM operano come slave, eseguendo i comandi. I FEIM possono inviare notifiche non sollecitate su variazioni di eventi di campo predefiniti secondo le configurazioni fornite. Inoltre, il protocollo, oltre al paradigma master-slave, supporta anche un paradigma P2P, che consente a ciascun modulo di agire come master nei confronti degli altri, nel momento in cui deve richiedere la scrittura di nuovi valori su

altri oggetti in conseguenza delle regole impostate. Le operazioni consentite in modalità P2P sono limitate, al fine di garantire l'esecuzione dei soli comandi strettamente indispensabili in condizioni specifiche. In particolare non sono accettate variazioni di configurazioni non provenienti dall'unità LMP preposta alla gestione di quello specifico FEIM.
Oltre ai normali comandi per il controllo del FEIM è anche definito nel protocollo uno specifico pacchetto, definito di "Keep Alive", che deve essere inviato dall'LMP a tutti i FEIM connessi, se questi non sono stati contattati da più di uno specifico intervallo di tempo (timeout). Ciò serve a dimostrare al FEIM che la connessione con l'LMP è ancora possibile. Se non viene ricevuto un comando od un pacchetto di Keep Alive entro il timeout, il modulo cambia profilo di funzionamento ed entra in modalità "Orphan" (orfano) (cfr. sez. 5.7).
Attualmente il protocollo è di tipo binario in chiaro, senza crittografia o autenticazione, sebbene venga supportata l'identificazione di mittente e destinatario.

5.4.3 Protocollo di supervisione

Il protocollo di supervisione realizzato è simile, nella filosofia, a quello progettato per il livello di gestione del campo. Si tratta di un protocollo basato sull'XML (eXtensible Markup Language, un formato di file di testo mediante il quale è possibile rappresentare le informazioni in modo gerarchico e mediante il quale è anche possibile rappresentare complesse basi di dati) che utilizza il TCP/IP come livello di trasporto. In questo caso un entità stabilisce una connessione TCP con un'altra, dopo di che quest'ultima stabilisce a sua volta una connessione verso la prima. La connessione iniziale viene utilizzata per l'invio di comandi e la ricezione delle risposte, mentre la seconda viene utilizzata per la ricezione di eventi da parte dell'unità contattata. In questo modo vengono limitati al minimo i problemi di concorrenza nella comunicazione.
Definita "connessione comandi" la prima connessione instaurata e "connessione trap" la seconda, si può descrivere a grandi linee il funzionamento del protocollo: sulla connessione comandi un'entità può richiedere letture o scritture di variabili su *Oggetti* presenti sull'entità contattata o può richiedere di registrarsi per la ricezione di varia-

zioni dello stato di alcune *Variabili*. Se viene inviata una richiesta di notifica, ogni volta che avviene una variazione delle *Variabili* registrate, il server contattato invierà una notifica utilizzando la connessione trap.
Se l'entità contattata è il SP, allora possono anche essere richieste informazioni (IP ed ID) dei server in carico per la gestione di specifici *Oggetti*, al fine di permettere all'unità di contattare direttamente tali server per ottenere informazioni o controllare gli *Oggetti* in questione.
Nel caso la connessione venga effettuata da una GUI verso l'SP è anche possibile, sempre utilizzando questo protocollo, richiedere l'assegnazione di un ID dinamico, che rimane assegnato all'interfaccia finché la connessione comandi con la stessa è attiva.
Nel momento in cui, per qualunque motivo, una delle due connessioni viene chiusa, anche l'altra viene interrotta e tutte le registrazioni per la ricezione delle variazioni delle *Variabili* vengono annullate. Se viene interrotta la connessione fra la GUI e l'SP, il sui ID dinamico viene rilasciato.

5.5 La configurazione del sistema

La configurazione del sistema è pensata per essere quanto più possibile versatile e compatibile con varie piattaforme operative. Per questo motivo è stato scelto di utilizzare dei file XML per la definizione di ogni aspetto configurabile del sistema. L'unico elemento che (per il momento) non viene direttamente configurato mediante file XML è il FEIM, che riceve invece la configurazione sotto forma di un file di testo delimitato a formato fisso, per semplificarne l'elaborazione. Tutti gli altri elementi, dagli LMP all'SP, alle GUI sono configurate a partire da file XML. Non solo, anche i file per i FEIM vengono generati come prodotto di conversione a partire dai file XML generali di configurazione.

5.5.1 Configurazione dei FEIM

I FEIM sono programmati tutti con il medesimo firmware in fase di produzione. Non vi sono configurazioni preimpostate. Le informazioni necessarie al loro funziona-

mento all'interno del sistema vengono scaricate nello stesso sfruttando i protocollo DHCP e TFTP. Questo è possibile, perché ogni modulo ha un indirizzo MAC univoco, requisito indispensabile alla connessione in rete, e tale MAC è la base per la distinzione di ciascun modulo al momento della sua connessione.
Grazie al protocollo DHCP è possibile fornire a ciascun modulo una configurazione di rete individuale, oltre alle informazioni sul file di configurazione che devono scaricare dal server TFTP che le detiene, sulla base del MAC contenuto nel pacchetto Ethernet di richiesta. Dunque il server di configurazione dei FEIM non è altro che l'insieme di due server (DHCP e TFTP), assolutamente standard, correttamente configurati. In particolare vengono utilizzate le seguenti opzioni DHCP (cfr. sez. 4.5.5) per fornire informazioni specifiche:

- IP ADDRESS: è l'indirizzo IP del FEIM
- SUBNET: è la net mask della rete del FEIM
- HOST NAME: è l'ID del FEIM
- LOG SERVER: è l'indirizzo IP dell'LMP
- DOMAIN NAME: è l'ID dell'LMP
- BOOTP FILENAME: è il nome del file di configurazione che il FEIM deve scaricare ed utilizzare
- BOOTP SERVER: è l'indirizzo IP del server TFTP a cui richiedere il file di configurazione

In questo modo il modulo riceve tutte le informazioni in modo del tutto standard e compatibile anche con altri host, che possono usare lo stesso server DHCP per ricevere le rispettive configurazioni, senza generare conflitti di sorta.
Il server TFTP è in grado in generale di sopportare diverse richieste contemporanee, ma in caso di congestione i FEIM che si trovassero impossibilitati a ricevere la configurazione, attendono un intervallo di tempo casuale prima di ritentare lo scaricamento, al fine di ridurre il carico contemporaneo di accesso al server. Queste problematiche si possono comunque verificare solamente alla prima accensione dell'intero sistema, in quanto ogni modulo, dopo la ricezione della configurazione, la memorizza in una memoria non volatile di tipo FLASH e non richiede quindi più

informazioni, né al DHCP, né al server TFTP, a meno che questa non venga esplicitamente invalidata in caso sia necessario un aggiornamento. Questo può avvenire da remoto mediante uno specifico comando via rete o mediante un accesso fisico diretto al modulo, utilizzando un apposito pulsante indicato come SW RESET (Software Reset). Se la configurazione viene invalidata, la procedura di prima installazione avviene nuovamente come descritto precedentemente.

5.5.2 File di configurazione dei FEIM

Per la configurazione completa dei FEIM è necessario fornire un file contenente informazioni circa gli *Oggetti* che il modulo dovrà gestire. In particolare devono essere indicati:

- ID logico
- tipo logico:
  - button
  - switch
  - analog input
  - relè mono
  - relè bi
  - analog out
- flag di configurazione relativi alle segnalazioni di variazione dello stato di campo
- condizioni iniziali dell'oggetto
- informazioni circa eventuali regole da eseguire in conseguenza di specifiche variazioni dell'oggetto (cfr. sez. 5.6.1)

Il file contiene poi anche fino a 12 tabelle di linearizzazione, per l'eventuale linearizzazione di ingressi o uscite analogiche. Le informazioni sono contenute nel file sotto forma di campi di testo delimitati e sono quindi facilmente editabili manualmente e al tempo stesso facilmente interpretabili dal modulo. In futuro è previsto l'utilizzo di file XML anche per la configurazione del modulo, ma per il momento non è stato

fatto in quanto un parser XML interno al modulo richiederebbe una quantità di memoria, sia di programma che RAM, non giustificabile con i benefici dell'utilizzo di questo formato.
I file possono essere generati come elaborazione di due file XML di livello astratto superiore: uno di descrizione della scheda ed uno di descrizione degli *Oggetti*. Tale elaborazione può essere fatta dal server LMP in coincidenza con aggiornamenti della configurazione, producendo nuovi file di testo da porre a disposizione del server TFTP per successivi aggiornamenti dei FEIM coinvolti.

5.5.3 File di configurazione di LMP e SP

I file di configurazione del sistema di controllo sono tutti di tipo XML. Un unico file XML viene generato dai programmi di configurazione (cfr. sez. 5.5.5) e viene definito "File di configurazione logica". Questo file XML contiene tutte le informazioni relative a tutto il sistema, fino alla definizione delle configurazioni degli oggetti di campo. Al momento del parsing (il parsing è un'operazione di lettura ed interpretazione di un file, in particolare riferito ai file di tipo XML) ciascun LMP o SP (che riceve da linea di comando il proprio ID) interpreta le informazioni contenute dal proprio "punto di vista", ovvero interpretando come oggetti di propria competenza quelli attribuiti all'oggetto con il proprio ID e come oggetti accessibili dall'esterno gli altri oggetti descritti. Inoltre, l'LMP può generare i file di configurazione dei vari FEIM (se necessario) utilizzando le informazioni contenute nel medesimo file. Ciò porta ad una maggiore coerenza intrinseca del sistema di configurazione ed a minori probabilità di incoerenza nella configurazione dei vari elementi.
All'interno del file di configurazione logica sono definite tutte le variabili di ciascun LMP e tutti gli oggetti virtuali.
Nella sezione relativa alla configurazione del server SP è anche indicato l'elenco delle interfacce autorizzate alla connessione ed il numero ed i valori degli oggetti dinamici assegnabili.
Anche le regole 5.6 sono definite nel medesimo file, gerarchicamente dipendenti dall'LMP che le deve predisporre ed eseguire.

5.5.4 File di configurazione di interfacciamento

Al fine di consentire un interfacciamento verso il sistema da parte di altri sistemi di supervisione o da parte di interfacce grafiche è stato pensato un formato XML per fornire all'esterno informazioni necessarie e sufficienti ad interagire con il sistema, senza doverne conoscere i dettagli implementativi interni. Questo file può anche contenere informazioni riguardanti la grafica di pannelli sinottici per la gestione delle aree dell'edificio, come la definizione della gerarchia degli allarmi, oltre a tutti gli ID ed i tipi di *Oggetti* e *Variabili* contenute nell'intero sistema o nella porzione che si vuole rendere disponibile. Questo file può essere in gran parte ricavato a partire dal file di configurazione logica e viene attualmente impiegato per la configurazione delle GUI (cfr. sez. 5.3.6).

5.5.5 Strumenti di configurazione

Gli strumenti di configurazione attualmente realizzati sono software, per piattaforma Microsoft™ Windows™, in grado di assistere il progettista nella configurazione del singolo FEIM e nella stesura della configurazione logica del sistema e delle regole. Tali software presentano interfacce grafiche che semplificano le operazioni di aggiunta e definizione degli *Oggetti*, ma non rappresentano ancora un supporto adatto allo sviluppo da parte di personale non specificamente addestrato. È in corso di realizzazione un ambiente CAD (Computer Aided Design, progettazione assistita al computer) in grado di semplificare grandemente le procedure di realizzazione delle configurazioni, in quanto permette di caricare gli sfondi dei pannelli sinottici, sui quali vengono posizionati gli oggetti di campo presi da una libreria. Tali oggetti vengono poi assegnati mediante una procedura guidata ai FEIM necessari al loro interfacciamento. In questa fase vengono anche impostate le regole di livello FEIM e definiti i collegamenti fisici effettivi fra il FEIM e gli *Oggetti*. A questo punto, una volta definito il campo, viene avviata una procedura di bilanciamento del carico di elaborazione per la supervisione e vengono proposte alcune configurazioni possibili sulla base degli elaboratori disponibili e delle restrizioni in termini di spazi e distanze. Al termine il programma genera sia il file XML di descrizione logica, sia quello di inter-

facciamento con le informazioni ricavate dagli inserimenti degli oggetti sui pannelli sinottici utilizzati per la configurazione. Il programma è ancora attualmente in uno stadio iniziale dello sviluppo.

5.6 Le regole

Con il termine "regole" si indicano collettivamente tutte le configurazioni atte a definire il comportamento del sistema in corrispondenza del verificarsi di variazioni dello stato del campo o del verificarsi di altri eventi, ad esempio lo scadere di un timer interno o una variazione di una *Variabile* voluta da un utente. In corrispondenza di tali evenienze il sistema valuta una serie di regole impostate che determinano se e quali eventi si devono verificare come conseguenza.
Il meccanismo di valutazione delle regole è estremamente flessibile e configurabile, potendo prendere in considerazione ogni valore di ogni *Variabile* presente nell'intero sistema, sia che siano direttamente accessibili, in quanto locali all'LMP che sta eseguendo le regole, sia che siano presenti su altri LMP o su oggetti di campo gestiti dai FEIM.
Sfruttando il paradigma di astrazione sviluppato e con l'ausilio degli oggetti virtuali, è possibile realizzare relazioni di verifica del valore di ogni grandezza accessibile dal sistema semplicemente utilizzando la *Variabile* relativa.
Il paradigma ad intelligenza distribuita prevede che esistano essenzialmente due livelli di regole: regole in esecuzione a livello di FEIM e regole a livello di supervisione, in esecuzione sui vari LMP e sull'SP.

5.6.1 Le regole dei FEIM

Le regole gestiste dal FEIM sono regole molto semplici, si tratta infatti di relazioni di azione-reazione.
Ogni qual volta uno dei sensori monitorati cambia stato, viene verificato se il nuovo stato prevede l'esecuzione di azioni. Sono previste fino a due azioni per ogni oggetto. Le azioni possono essere scatenate dallo stesso stato o da stati diversi. Ad esempio è possibile impostare una regola per la quale quando viene premuto un pulsante una

determinata luce viene accesa. Oppure è possibile realizzare una regola che quando viene premuto un pulsante di richiesta di assistenza un campanello venga fatto attivare e quando il pulsante viene rilasciato il campanello torni nuovamente in condizione di riposo.
Le regole possono inoltre essere attivate o disattivate sulla base del profilo di funzionamento del modulo FEIM (cfr. sez. 5.7) attivo in quel momento. In questo modo è possibile fare si che alcune azioni vengano intraprese solamente in specifiche condizioni.
Le regole dei FEIM non possono tenere conto del tempo o dello stato di più di un sensore contemporaneamente. Per questo motivo si tratta di regole estremamente semplici, che sono pensate per l'esecuzione di livello molto basso, legate a funzioni basilari o di sicurezza intrinseca, quali appunto la gestione dell'illuminazione o la segnalazione e gestione essenziale di condizioni di allarme o emergenza. Possono infatti fare attivare le elettrovalvole di intercettazione in caso di fughe di acqua o gas. Tutte le azioni intraprese sulla base delle regole vengono comunque segnalate al sistema di supervisione esattamente come se fossero eventi indipendenti e quindi il sistema si supervisione può integrare le azioni intraprese autonomamente dai moduli, se necessario.

5.6.2 Le regole degli LMP e dell'SP

Le regole gestite dai "motori" di valutazione (sono così definiti i processi che si occupano di ricevere le segnalazioni delle variazioni di stato ed eseguire le opportune azioni relativamente alle regole impostate) dei server sono molto più complesse e versatili rispetto a quelle dei FEIM.
Queste regole possono prendere in considerazione qualunque *Variabile* di qualunque *Oggetto* presente nel sistema ed accessibile all'LMP (sono quindi esclusi gli *Oggetti* e le *Variabili* private di altri *Oggetti*).
Ogni regola è rappresentata da un albero XML binario, in cui il ramo sinistro rappresenta un'espressione in notazione prefissa che coinvolge le *Variabili* e che viene valutata dal motore come *vera* o *false*. Nel caso in cui sia valutata *false*, l'elaborazione della regola è conclusa ed il motore passa alla regola successiva. Nel caso in

cui sia valutata come *vera*, allora viene valutato il ramo destro della regola, nel quale sono inserite le operazioni di assegnazione di nuovi valori ad una o più *Variabili*.
Per ogni *Variabile* inserita nelle regole viene definito se si tratta di una *Variabile* scatenante la valutazione o meno. Se è scatenante allora, al momento dell'inserimento della regola nel motore, essa viene inserita nell'elenco delle *Variabili* da monitorare (se non era già presente in conseguenza di altre regole caricate precedentemente), viene poi inserito l'ID della regola nella lista delle regole da valutate nel momento in cui viene rilevata una variazione della *Variabile* in oggetto. In questo modo viene gestita in modo efficiente l'esecuzione delle operazioni di valutazione. Infatti il procedimento di valutazione si svolge secondo le seguenti fasi:

1. rilevazione della variazione di una delle *Variabili* monitorate;
2. lettura e salvataggio di tutte le *Variabili* coinvolte nelle regole (comprese le *Variabili* non scatenanti);
3. valutazione di tutte le regole relative alla *Variabile* variata e conseguente aggiornamento delle *Variabili*.

Se al termine del primo "giro" sono state variate *Variabili* monitorate, allora la sequenza verrà eseguita nuovamente con i valori aggiornati. In questo modo gli eventi vengono valutati nel contesto più vicino possibile ad una fotografia dell'istante nel quale si sono verificati, indipendentemente dall'ordine di valutazione delle regole e dal tempo di esecuzione delle valutazioni da parte del motore.
La possibilità di definire alcune variabili come "non scatenanti" consente di evitare la valutazione di regole che non ha senso vengano valutate in coincidenza di eventi molto comuni. Ad esempio le *Variabili* relative al tempo in genere non sono scatenanti, in quanto normalmente vengono utilizzate per verificare se un dato evento scatenante, nell'istante corrente, deve o meno comportare determinati assegnamenti. Se l'evento non si verifica, non ha senso rivalutare la regola ogni minuto, solo perché la *Variabile* relativa al minuto corrente viene aggiornata.
Le regole comprendono attualmente gli operatori logici (*and*, *or*, *not* e *xor*), quelli aritmetici (*somma*, *sottrazione*, *moltiplicazione*, *divisione* e *modulo*), quelli di confronto (*maggiore*, *maggiore o uguale*, *uguale*, *minore o uguale*, *minore* e *diverso*) e

quelli di assegnazione per l'aggiornamento delle variabili. È inoltre possibile definire delle "sotto-procedure", che vengono valutate di volta in volta e che possono essere utilizzate da più regole, al fine di ridurre i tempi di valutazione nel caso di molte regole con porzioni uguali. Le regole possono ovviamente prendere anche in considerazione costanti di riferimento, sia per i confronti, sia per le operazioni aritmetiche o logiche.

5.7 Politiche di gestione

Il sistema è estremamente versatile, ed in quanto tale si presta ad un'ampia gamma di funzionalità. L'organizzazione delle funzioni è del tutto configurabile e deve essere attentamente pianificata al fine di non avere interazioni non volute fra le varie attività. In questa sezione verranno descritte le politiche secondo le quali è possibile configurare il sistema per la gestione efficace delle situazioni che si vengono a verificare in un edificio. Verranno inoltre descritte le modalità di funzionamento dei vari elementi del sistema che sono alla base della gestione efficace delle varie evenienze, per esempio nella gestione degli allarmi o dei guasti.

5.7.1 I profili di funzionamento dei FEIM

Come già più volte ricordato, i FEIM non sono mere interfacce, ma elementi in grado di elaborare le informazioni ricevute ed agire di conseguenza, secondo opportune regole preimpostate (cfr. sez. 5.2.2 e 5.6.1). Questa capacità elaborativa sta alla base del modello di intelligenza distribuita utilizzato nel sistema.
Per poter operare nel modo più flessibile possibile è stato ideato un meccanismo di configurazione strutturato in insiemi funzionali, chiamati profili.
Ogni profilo contiene una configurazione specifica per tutti gli oggetti, quindi può avere politiche di segnalazione delle variazioni diverse da quelle di altri profili. Inoltre le regole, che sono uguali per tutti i profili, possono però essere attivate o disattivate.
Attualmente il firmware prevede sette diversi profili di funzionamento, ciascuno attivo in particolari circostanze:

1. Default: è il profilo di normale funzionamento;
2. Custom: è un profilo alternativo a quello di default;
3. Orphan: è il profilo che si attiva nel momento in cui il FEIM non riesce a comunicare con l'LMP, ma ha ancora capacità di comunicazione in rete;
4. EthDown: è il profilo che si attiva quando viene a mancare il link di rete;
5. Passive: è il profilo attivato dall'LMP quando tutte le regole devono essere disattivate;
6. Fault: è il profilo attivato dall'LMP quando viene rilevato un grave malfunzionamento del FEIM stesso, al fine di disattivarlo;
7. NoLine: è il profilo attivato dall'LMP quando viene a mancare l'alimentazione di rete.

A questi sette profili si aggiunge un profilo di funzionamento solo interno, il profilo di reset. I profili da 1 a 6 sono mutuamente esclusivi, ovvero solamente uno di essi può essere in funzione in un dato istante, ed in base a quale di essi è attivo le configurazioni di segnalazione e le regole relative sono attive. Il profilo 7 è invece un profilo di tipo "trasversale", ovvero sovrappone le sue attività a quelle degli altri, indipendentemente da quale di essi sia attivo.
Di seguito sono descritte in dettaglio le funzioni dei singoli profili.

Default Questo profilo viene attivato subito dopo l'avvio o un reset. Configura i sensori per il normale funzionamento e per la segnalazione delle variazioni secondo il profilo previsto per le normali attività. Le regole sono attive secondo il funzionamento normale.

Custom Il profilo Custom è stato introdotto per permettere la memorizzazione di una configurazione alternativa a quella del profilo Default, che possa essere utilizzata in particolari condizioni di funzionamento dell'intero sistema. È l'LMP di riferimento che abilita o disabilita questo profilo e le configurazioni introdotte possono essere di qualunque tipo. Le regole sono attivate o disattivate sulla base della configurazione.

Orphan Quando il FEIM non riesce ad inviare una segnalazione di variazione del valore di un *Oggetto*, o quando non riceve pacchetti di comando o di Keep Alive dall'LMP per più di un tempo di timeout impostato, allora viene attivato automaticamente il profilo Orphan (orfano). In questo profilo tutte le segnalazioni verso l'LMP sono sospese, al fine di non sprecare tempo con le ritrasmissioni, vista l'impossibilità di raggiungerlo. I messaggi di segnalazione vengono memorizzati nella memoria interna, per una successiva trasmissione al ristabilimento della comunicazione. Se il numero di messaggi da memorizzare supera la capacità di memorizzazione, i messaggi più recenti vengono persi e viene però memorizzata la condizione, per poter segnalare all'LMP, al momento della riconnessione, che è necessario un aggiornamento di campo completo, perché alcune segnalazioni sono andate perse. In questa modalità è quindi possibile, mediante opportuna configurazione, disattivare le notifiche di eventi che non sono utili se non elaborati dall'LMP, quali ad esempio informazioni sull'occupazione delle stanze, se queste non scatenano regole locali. È possibile che vengano abilitate regole per la gestione diretta di condizioni di emergenza, che normalmente sarebbero gestite dall'LMP. Ciò è possibile sfruttando le possibilità di comunicazione P2P fra i FEIM. Quando l'LMP ritorna raggiungibile o si accorge che il modulo è entrato in Orphan (ad esempio, perché il modulo risponde ad un Keep Alive con un pacchetto di errore, che informa l'LMP del suo attuale profilo di funzionamento) viene avviata una procedura di ripristino, che prevede come prima cosa la richiesta di invio degli eventi memorizzati e poi il ripristino del profilo precedente. A questo punto il modulo torna nel profilo Default o Custom, a seconda di quale dei due era attivo al momento della perdita di comunicazione. Se è presente il messaggio di avviso della perdita di segnalazioni, viene anche avviata una procedura di aggiornamento completo dello stato del campo, al fine di avere una informazione coerente nel sistema di supervisione.

EthDown In caso venga completamente perso il link Ethernet e sia quindi impossibile per il FEIM comunicare con altri FEIM o LMP si attiva questo profilo. Tutte le segnalazioni sono sospese ed i messaggi sono memorizzati come nel caso del profilo Orphan. Anche in questo caso possono essere sospese rilevazioni di variazioni non

utili, e vengono disattivate tutte le regole che per l'attuazione richiedono la comunicazione con altri FEIM, ora impossibile. Possono essere attivate (o rimanere attive) regole che coinvolgano solamente elementi direttamente controllati dal FEIM stesso. Al ripristino della connessione il modulo non passa direttamente al profilo precedente, ma passa al profilo Orphan, ed attene l'inizio della procedura di ripristino da parte dell'LMP.

Passive Il profilo Passive (passivo) è utilizzato in condizioni di emergenza, quando si vogliono disabilitare immediatamente e completamente tutte le regole locali. Una tale evenienza si può verificare quando viene rilevata una fuga di gas combustibile, che pone rischi di deflagrazione, e si vuole evitare che l'attivazione di un'uscita possa essere l'innesco di un'esplosione. In questo caso tutte le regole sono disattivate e lo stato delle uscite non viene alterato. Solo l'LMP può impartire ordini di modifica dello stato delle uscite. Gli ingressi continuano ad operare normalmente. Per uscire da questo profilo è necessario un comando da parte dell'LMP.

Fault Il profilo fault (guasto) è utilizzato da parte dell'LMP per disattivare un modulo che produca messaggi di errore che possono generare intralcio alle comunicazioni o che non si comporti in modo prevedibile secondo il sistema di supervisione. Sebbene non si sia mai verificata la necessità di utilizzare tale profilo, questo è stato previsto come ultima risorsa in caso di gravi malfunzionamenti, al fine di mantenete l'operatività degli altri elementi della rete. Per uscire da questo profilo è necessario un reset hardware manuale.

NoLine Il profilo NoLine è attivato dall'LMP in caso venga rilevato un black-out. Ogni relè viene marcato in fase di configurazione come "mascherabile" o "non mascherabile", ovvero rispettivamente disattivabile o meno in caso di mancanza di alimentazione. All'ingresso in questo profilo vengono salvati gli stati di tutti i relè mascherabili e poi vengono disattivati, al fine di non sprecare corrente di alimentazione a bassa tensione per mantenere attive utenze che, senza alimentazione, non possono comunque funzionare. Non vengono disattivate le uscite che pilotano carichi a bassa

tensione o sotto gruppo di continuità, che possono quindi continuare a funzionare anche in caso di black-out. All'uscita dal profilo gli stati vengono ripristinati. Le regole che coinvolgono uscite mascherabili dovrebbero essere disattivate, ma anche se non vengono disattivate, ogni comando che tenti di agire su uscite mascherate viene ignorato e viene restituito un errore che specifica il motivo.

5.7.2 Gestione degli eventi immediati

Nel controllo di un edificio esistono azioni alle quali l'utente si aspetta una reazione con una latenza molto bassa, mentre altre possono avere tempi di ritardo superiori. Un evento che deve avere una latenza molto bassa, ad esempio, è l'accensione della luce di una stanza, come conseguenza della pressione del pulsante relativo. Questo evento ci si aspetta essere pressoché immediato. Tuttavia, se questo evento deve essere controllato per mezzo delle regole dell'LMP relativo, essendo necessaria una comunicazione via rete per la richiesta, un'elaborazione della regola (o delle regole) relative ed una seconda comunicazione via rete, per richiedere l'attuazione, il tempo di latenza può essere variabile ed in teoria non prevedibile. Nella pratica questo richiede molto meno di un secondo, ma in caso di reti o unità di elaborazione congestionate non è possibile garantirlo. I FEIM possono essere configurati al fine di eseguire semplici regole di azione e reazione e quindi questo tipo di regola può essere implementata direttamente a livello di controllo di campo. Nel caso in cui lo stesso modulo controlli sia i pulsanti che la luce, la regola si troverà ad agire internamente al modulo, quindi non coinvolgerà nessuna latenza di rete. Nel caso in cui il controllo della lampada si trovi su un altro FEIM, la latenza complessiva coinvolgerà la latenza di una sola comunicazione su Ethernet fra il modulo che controlla il (o i) pulsanti ed il modulo che controlla la luce, riducendo quindi comunque di molto le possibilità di un forte incremento del ritardo.
Per questa ragione, tutti gli eventi che l'utente si aspetta essere "immediati" dovrebbero essere configurati a livello di logica di elaborazione di campo, ovvero all'interno delle configurazioni dei FEIM.
Per quanto riguarda eventi a latenza attesa imprecisata, quali ad esempio i controlli sul sistema di riscaldamento, le regole possono essere eseguite a livello di processi di

supervisione e demandati al livello FEIM solo in caso di guasto, ad esempio attivando le regole nel profilo Orphan.

5.7.3 Gestione degli allarmi

La gestione delle condizioni di allarme deve avvenire a vari livelli. A livello di campo possono essere attivate immediatamente le contromisure possibili nel caso di allarmi ambientali, quali allagamenti ed incendi, mediante l'attivazione di valvole di intercettazione e segnalazioni acustiche e visive. A livello di supervisione possono essere attivate regole di coordinamento per l'attivazione di ulteriori misure di protezione, quali l'isolamento dell'energia elettrica in zone allagate o le segnalazioni mediante sistemi di composizione telefonica, sistemi GSM per l'invio di messaggi SMS di allarme, trasmissione di segnalazioni via web a postazioni di sorveglianza remota e altro (cfr. sez. 5.8).
In caso di guasto del sistema di supervisione o della connessione con lo stesso il livello di campo, grazie al meccanismo dei profili può intervenire in modo adeguato, dipendentemente dal livello di guasto riscontrato.
Altri tipi di allarmi, quali allarmi evoluti legati ad attività inusuali da parte di persone con problemi di indebolimento delle facoltà psichiche, possono essere segnalate al personale di assistenza. Per esempio è possibile per il sistema rilevare se una porta che porta verso l'esterno dell'abitazione viene aperta ad orari inusuali della notte, da parte di persone affette da problemi di disorientamento, e possono quindi essere avvisati gli assistenti mediante uno dei canali di comunicazione (cfr. sez. 5.8).
L'intera gamma degli allarmi ipotizzabili può essere impostata opportunamente sfruttando le regole a livello di FEIM ed a livello di LMP / SP.

5.7.4 Gestione dei guasti

La gestione delle emergenze, come dei guasti, è un elemento fondamentale di un sistema di automazione domestico [50, 51].
Il sistema progettato è stato ideato per ottenere un livello molto elevato di affidabilità e di tolleranza ai guasti. In particolare è stata utilizzata una filosofia definita "grace-

ful degradation", ovvero le funzionalità del sistema si degradano progressivamente all'aumentare dei guasti, ma senza che le parti che non sono interessate direttamente vengano coinvolte negativamente. Questo approccio prevede la fornitura del massimo delle funzionalità possibili con i dispositivi funzionanti, evitando che il guasto di un singolo elemento possa avere ripercussione a catena su tutte le parti o funzionalità dell'intero sistema.

Il primo passo nella garanzia di una corretta gestione della situazione è rappresentato dall'utilizzo di dispositivi di campo intelligenti, i FEIM, che consentono un'elaborazione distribuita, che risulta fondamentale in caso di guasto dei sistemi di comunicazione o delle unità di supervisione. Infatti, grazie alla possibilità di eseguire regole locali ed al meccanismo dei profili (cfr. sez. 5.7.1) i moduli sono in grado di garantire le funzionalità di base anche in caso di guasti alle unità di supervisione o in caso di problemi di connessione con le stesse. Al fine di minimizzare i disagi in caso di guasto dei dispositivi di rete è opportuna una progettazione attenta, che ponga tutti o gran parte degli ingressi che controllano un'uscita, e l'uscita stessa, sul medesimo modulo, se possibile, in modo che le regole possano mantenere attive le funzioni perfino in caso guasto dello switch che collega fra loro i moduli.
Le funzioni di supervisione sono affidate a processi LMP che sono in esecuzione su PC o elaboratori embedded. L'installazione di più moduli di elaborazione nella struttura permette di fornire ridondanza a questi processi, che grazie ad un processo di "migrazione", ovvero di riavvio su un'altra macchina, permettono di mantenere operative le funzioni di controllo operative anche in caso di guasto fisico di un'unità di elaborazione (ad eccezione di un breve intervallo di tempo necessario al processo di rilevazione dell'anomalia ed al riavvio sull'altro elaboratore).

Per quanto riguarda l'SP, pur non essendo indispensabile al funzionamento normale del sistema, esso rappresenta un punto centrale per la connessione verso l'esterno e per la gestione delle politiche di livello massimo della struttura e quindi anche per questo processo è previsto un processo di replicazione, che però, non potendo essere gestito da processi di livello superiore, deve essere eseguito mediante tecniche più complesse di verifica della funzionalità, attualmente in fase di definizione. Le interfacce grafiche, in caso blocco dell'SP, possono collegarsi direttamente agli LMP

(se raggiungibili) e fornire comunque informazioni circa lo stato del sistema fino al ripristino della connessione con il processo stesso.
È importante che la progettazione della struttura di rete tenga conto dei criteri che permettono di ridurre l'impatto del guasto di un singolo apparato di rete sulle funzionalità complessive del sistema (cfr. sez. 5.2.7).

5.7.5 Registrazione eventi

Il sistema è progettato per mantenere una traccia permanente e dettagliata degli eventi che si verificano all'interno dell'area controllata. Per fare ciò tutti i FEIM inviano verso l'LMP di riferimento le notifiche di variazione di tutti gli ingressi e delle uscite controllate, cosicché possano essere registrate in un file di log o in un database. Possono essere anche impostate le registrazioni delle variazioni delle Variabili interne ai vari LMP e SP. Tutto questo è utile a livello di debug del sistema, ma anche al fine di ottenere informazioni fondamentali all'estrapolazione di modelli di comportamento degli abitanti, la cui analisi può portare alla determinazione di patologie incipienti o di anomalie nel comportamento, che indicano la degradazione delle condizioni psicofisiche degli utenti.
Il sistema di logging è estremamente configurabile in modo dettagliato e permette di ripartire o duplicare le informazioni su più destinazioni, quali ad esempio file di testo semplice, file XML con relativo file di stile XSLT (Extensible Stylesheet Language Transformations, un file di testo con sintassi specifica, utilizzato ad esempio per la trasformazione di file XML in file XHTML) per la rappresentazione, database MySQL, server di logging secondo lo standard Syslog, ... È anche possibile filtrare le informazioni da registrare in base al livello di logging o in base alle aree di attinenza delle informazioni. Il meccanismo di definizione di questi parametri è dinamico ed è basato su un file XML di configurazione specifico.

5.8 La comunicazione con l'utente

La comunicazione fra l'utente ed il sistema può avvenire sfruttando vari canali di comunicazione. Essendo un sistema basato su Ethernet si può agire nativamente sfrut-

tando le interfacce grafiche, sia a livello locale (mediante la rete LAN), sia da remoto tramite Internet, eventualmente sfruttando una connessione protetta mediante sistemi VPN. È poi possibile utilizzare applicativi che operano su dispositivi palmari (PDA), grazie all'integrazione nativa della rete Ethernet con i sistemi Wi-Fi. Inoltre, grazie ad opportuni combinatori telefonici, sia con interfaccia verso rete telefonica commutata (PTSN o ISDN), sia tramite reti cellulari (GSM, GPRS, UMTS), è possibile inviare messaggi vocali o SMS verso numeri predefiniti in caso di emergenza.
Le interfacce utente sviluppate finora sono pensate per l'interazione con assistenti che si trovano nella struttura o che devono gestire una sola struttura a distanza. È però possibile realizzare interfacce in grado di gestire una molteplicità di siti da un unico centro servizi, ponendo le basi ad esempio per un supporto, sia di tipo tecnico, sia sociale e sanitario, a più installazioni, che possono anche essere case singole all'interno di vaste aree rurali o montane.
Tutti questi sistemi si aggiungono naturalmente alla serie di avvisatori visuali ed acustici normalmente previsti in sistemi di sicurezza ambientale e che servono a segnalare condizioni di pericolo immediato, quali incendi, allagamenti ed intrusioni.
La possibilità di installare sulle unità di controllo anche altre applicazioni sviluppate per le normali piattaforme GNU/Linux (o Microsoft Windows) permette di espandere le funzionalità del sistema integrando altri applicativi, quali ad esempio sistemi di comando vocale.

Capitolo 6

La progettazione del FEIM

Il valore di un uomo si misura dalle poche cose che crea,
non dai molti beni che accumula.

– Kahlil Gibran

Il FEIM (Field Ethernet Interface Module) è stato progettato come elemento intelligente di interfacciamento con sensori di tipo standard per l'automazione domestica ed industriale e per l'implementazione di un livello di astrazione, che consenta al sistema di gestirli direttamente come Oggetti (cfr. sez. 5.3.1).
Perché il dispositivo fosse adatto allo scopo è stato necessario definire delle specifiche, sia in termini funzionali, sia in termini di costo e modalità di installazione in ambiente domestico.

6.1 La definizione dei requisiti

Il modulo da progettare doveva avere la capacità di interfacciarsi con sensori per automazione domestica ed industriale a basso costo, quindi doveva avere la capacità di leggere contatti puliti ed ingressi analogici in standard 0–10 V, 0–1 V e 4–20 mA. Inoltre era richiesto l'interfacciamento in uscita verso le utenze domestiche e, vista la necessità di gestire una grande varietà di carichi ed utenze, si è deciso di optare per la

gestione di vari tipi di relè, quindi il modulo doveva poter gestire una corrente continua di intensità fino a 240 mA, per poter eccitare relè con tensione di alimentazione fino a 24 V.

Un altro requisito fondamentale riguardava il fattore di forma del dispositivo, in quanto era necessario che potesse essere installato nei quadri di alimentazione domestici e doveva anche permettere la connessione di un gran numero di dispositivi, al fine di ridurre al minimo il numero di connessioni Ethernet necessarie per l'automazione.

L'alimentazione prevista è a 24 V in corrente continua, in quanto questa alimentazione risulta essere la tensione di alimentazione più indicata per la distribuzione di energia ai sistemi elettronici in una rete estesa a tutta l'abitazione, ed infatti è anche la tensione utilizzata nei sistemi industriali di automazione. Tale livello di tensione permette di sfruttare alimentatori e gruppi di continuità utilizzati proprio in quelle realtà.

6.2 Scelta del microcontrollore

La scelta del microcontrollore è caduta sul micro Rabbit 3000™ della Rabbit Semiconductors. Questo perché al momento della scelta la Rabbit Semiconductors era sostanzialmente una delle poche ditte a fornire un modulo di comunicazione Ethernet a basso costo, l'RCM3700, dotato di librerie di supporto complete per lo sviluppo di applicazioni di media complessità. Il modulo include il microcontrollore Rabbit 3000, 512 kByte di memoria Flash di programma, 512 kByte di RAM, 1 MByte di memoria flash su bus SPI (Serial Peripheral Interface) per la memorizzazione di dati. L'interfaccia Ethernet è di tipo 10Base-T, quindi con una velocità massima di comunicazione pari a 10 Mbps full-duplex. Il modulo è alimentato alla tensione di 5 V ed include anche il generatore di clock a 22.1 MHz ed un quarzo ausiliario per l'RTC (Real Time Clock, orologio a tempo reale) integrato nel microcontrollore. Il consumo complessivo di corrente del modulo è pari a 100 mA. Il modulo presenta in uscita interfacce per collegare fino a 33 linee di I/O digitali, ma non presenta interfacce analogiche.

6.3 Scelta dell'involucro

Per l'involucro è stato scelto un contenitore adatto all'alloggiamento nei quadri elettrici civili standard, quindi è stata utilizzata una scatola plastica per il fissaggio su guide omega secondo lo standard EN 50022, da 9 moduli. Le dimensioni dell'involucro sono di 160 mm per 90 mm per 58 mm. Questo tipo di contenitore permette di esporre connettori su entrambi i lati lunghi, paralleli alla barra omega, e quindi massimizzano le possibilità di connessione delle periferiche. Purtroppo la connessione del modulo Rabbit ha richiesto la foratura della scatola sul fianco, al fine di permettere l'esposizione del connettore Ethernet. Questo costringe l'installazione del modulo nel lato estremo destro o sinistro del quadro, per non impedire la connessione della rete. La scatola presenta inoltre delle feritoie laterali che facilitano la ventilazione, caratteristica importante, in quanto il modulo FEIM integra una sezione di alimentazione, che deve convertire l'energia a 24 V ricevuta per l'alimentazione della circuiteria interna (a 5 V), ma anche della sensoristica esterna a 12 V.

6.4 Il progetto elettrico

Nei paragrafi che seguono viene descritta la progettazione elettrica del modulo, dalla definizione degli schematici, alla realizzazione del layout per la produzione del circuito stampato (PCB, Printed Circuit Board).

6.4.1 Schematico

Il FEIM include essenzialmente sei differenti sezioni:

- alimentazione, per la conversione della tensione a 24 V corrente continua nelle tensioni interne ed esterne a 12 V, 5 V e 3.3 V;
- modulo microcontrollore e sezione Ethernet;
- sezione di conversione analogico-digitale;
- sezione di conversione digitale-analogica;

- sezione di lettura contatti puliti;
- sezione di comando uscite di potenza.

Di seguito sono descritte le componenti fondamentali delle singole sezioni.

Alimentazione La sezione di alimentazione è composta da due regolatori DC/DC di tipo switching. Il primo è basato sull'integrato LM2596-12 della National Semiconductors: si tratta di un convertitore operante alla frequenza fissa di 150 kHz che integra il sistema di controllo ed il MOS per la commutazione generando, in uscita una tensione controllata di 12 V. A valle di questo primo convertitore è presente un altro integrato di regolazione switching della National Semiconductors: l'LM2575-5, operante alla frequenza fissa di 52 kHz ed integrante anch'esso logica di controllo e MOS di commutazione. Ciascuno dei due integrati richiede pochi componenti esterni, in particolare: capacità di uscita, diodi di ricircolo e induttanza.
A causa delle pesanti distorsioni di ingresso generate è stato necessario inserire un blocco di filtraggio di modo comune all'ingresso, al fine di rispettare le norme sulla compatibilità elettromagnetica riguardanti le emissioni condotte (cfr. sez. 6.7). Tale blocco è costituito da un filtro a due celle, comprendenti ciascuna una bobina di blocco di modo comune ed una capacità in poliestere.
All'ingresso della sezione è poi presente un diodo per la protezione contro le inversioni di polarità ed un fusibile autoripristinabile che protegge il circuito e la rete di alimentazione esterna in caso di sovraccarico o corto circuito.

Modulo microcontrollore Il modulo a microcontrollore è l'RCM3700 della Rabbit Semiconductors, appena descritto. Sulla scheda è previsto un connettore per il fissaggio del modulo stesso.

Conversione analogico-digitale Per la realizzazione della conversione analogico-digitale degli ingressi provenienti dai sensori analogici è stato utilizzato il sistema di conversione on-chip: l'ADS7871 della Texas Instruments. L'integrato include un riferimento di tensione, un amplificatore a guadagno programmabile, un multiplexer

per la lettura di otto ingressi ed un convertitore analogico-digitale ad approssimazioni successive (SAR) a 14 bit (13 bit nella modalità single-ended utilizzata). La connessione con il modulo a microcontrollore avviene mediante una linea SPI full-duplex.
È stato realizzato un front-end di conversione dei livelli di tensione da 0–10 V a 0–2 V fisso per quattro ingressi, mentre per gli altri quattro è stata adottata una soluzione che permette di leggere segnali di tipo 0–10 V, 0–1 V e 4–20 mA mediante la selezione fisica mediante ponticelli della rete di riduzione della tensione, mediante partitore resistivo, o di conversione corrente-tensione, mediante resistenza di precisione.
In ogni caso le necessarie tarature possono essere effettuate utilizzando i parametri di compensazione degli errori di guadagno ed offset previsti nel firmware.

Conversione digitale-analogico Il modulo comprende anche quattro canali di uscita in tensione in standard 0–10 V, per in controllo di attuatori proporzionali. L'uscita è generata sfruttando il convertitore AD5304 della Analog Devices, collegato ad un amplificatore operazione OP496, sempre della Analog Devices.

Lettura contatti puliti Per la lettura dello stato dei contatti puliti sono previsti dei partitori di tensione, che convertano il livello di tensione a 12 V, utilizzato per l'alimentazione dei contatti, in un livello compatibile con gli ingressi del modulo RCM3700, che sono ingressi in standard CMOS 3.3 V (tolleranti tensioni fino a 5 V). Per questo motivo il partitore opera una riduzione di un fattore 0.248, che porta quindi la tensione di alimentazione da 12 V ad un valore di circa 3 V, facendo scorrere una corrente di circa 1 mA. In questo modo le interferenze elettromagnetiche non comportano variazioni che possano portare a false letture di variazioni dello stato. Inoltre il firmware include funzioni di sicurezza, che verificano la durata minima dell'impulso di ingresso al fine di discriminare false letture da effettive variazioni.

Comando uscite di potenza Le uscite di potenza sono realizzate utilizzando dei MOS FDN337N della Fairchild Semiconductors, in gradi di sopportare una corrente massima di 2.2 A ed una tensione massima di 30 V in un case estremamente ridotto: SOT-23, con una tensione di soglia pari a 1 V massimo. Questo consente di gestire il

controllo diretto dei relè a 24 V senza bisogno di ulteriori strutture di amplificazione, con un controllo diretto da parte del microcontrollore.

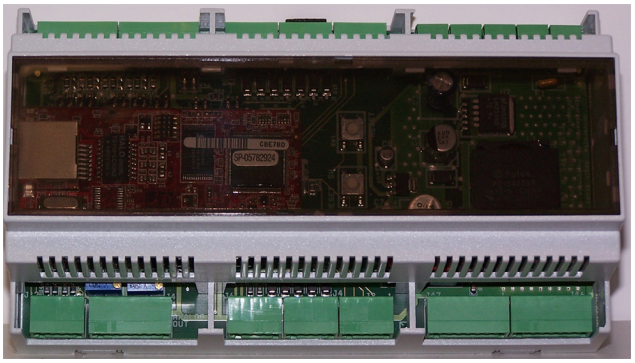
Ingressi ed uscite configurabili Delle dodici uscite di potenza, sei possono essere configurate in modo da operare come ingressi supplementari, anziché come uscite, mediante appositi ponticelli presenti sulla scheda. Questo permette di ampliare la flessibilità dell'installazione e della configurazione fisica del sistema, anche in sede di ampliamento successivo.

Layout

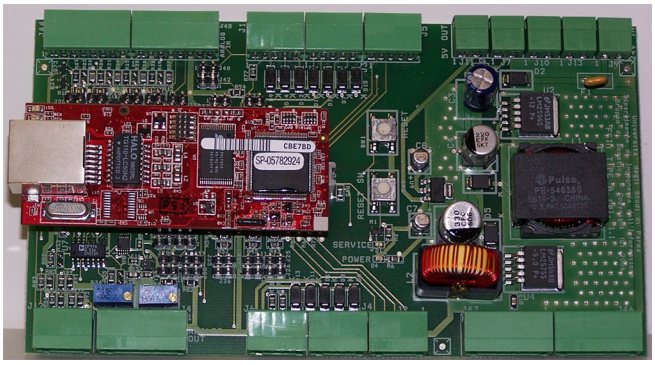
Il Layout della scheda è stato realizzato su un supporto a due strati, in modo da permettere l'installazione solamente su una faccia dei componenti, al fine di ridurre i costi. La tecnologia utilizzata è una tecnologica ad isolamento minimo e pista minima 150 ţm (anche detta tecnologia 6/6, 6 mils pista minima, 6 mils isolamento minimo). Non è stata realizzata una scheda a quattro strati per motivi di costo, ma questo ha reso difficili le procedure relative alla certificazione di compatibilità elettromagnetica, in particolare per quanto riguarda le emissioni radiate (cfr. sez. 6.7), quindi la prossima revisione verrà progettata per l'impiego di una scheda a quattro strati. In Figura 6.1 si può vedere il modulo realizzato.

6.5 Caratteristiche elettriche

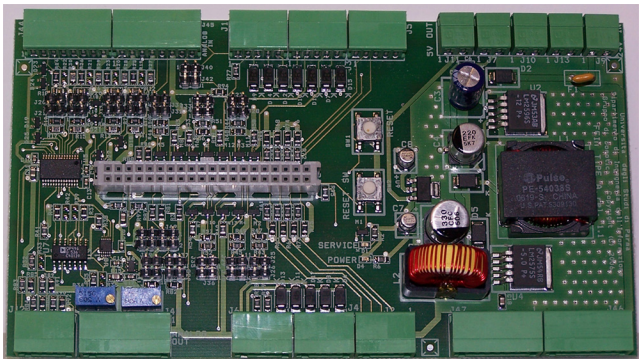
Il modulo ha un assorbimento massimo alla tensione di alimentazione a 24 V di 1 A. L'intervallo di valori della tensione di alimentazione che garantisce il corretto funzionamento è da 13 V a 29 V.
Le uscite di tensione a 12 V hanno una precisione di più o meno il 5% ed una corrente massima di uscita complessiva di 1 A.
Le uscite di tensione a 5 V hanno anch'esse una precisione di più o meno il 5% ed una corrente massima complessiva di 200 mA.
Le uscite di potenza del modulo possono controllare tensioni fino ad un massimo di 24 V e corrente massima per ciascun canale di 240 mA. È possibile controllare relè a



(a) Vista esterna.



(b) Le schede.



(c) La base senza il modulo Rabbit Semiconductors.

Figura 6.1: Alcune foto del modulo FEIM.

24 V sfruttando dei diodi di ricircolo interni, che si attivano collegando l'opportuno terminale alla tensione di alimentazione dei relè e consentono così un controllo diretto degli stessi senza bisogno di componenti esterni.
Gli ingressi per la lettura dei contatti puliti operano solamente rilevando la presenza o meno di una tensione di 12 V sull'ingresso stesso. La corrente che scorre a contatto chiuso è di circa 1 mA.

6.6 Firmware

Il firmware del FEIM è stato sviluppato in linguaggio C, utilizzando come ambiente di sviluppo il compilatore standard della Rabbit Semiconductors: il Dynamic C™. Questo compilatore mette a disposizione anche una serie di costrutti per il supporto all'implementazione di meccanismi di concorrenza cooperativa, consente cioè di definire dei sottoprogrammi (task) che possono essere sospesi e ripresi, mediante opportune istruzioni. In questo modo è possibile avere un controllo simile a quello possibile in un sistema operativo non preemptive[1]. Purtroppo queste istruzioni sono specifiche del compilatore utilizzato e non sono quindi portabili verso altri compilatori o piattaforme, mentre il resto del codice è compatibile con lo standard ANSI C, utilizzato da molti altri compilatori per altri microprocessori e microcontrollori.
Il firmware è stato organizzato in modo modulare, al fine di ottenere la massima efficenza, sia in fase di esecuzione, sia in fase di aggiornamento e debug. La struttura del codice è rappresentata in Figura 6.2.
La struttura prevede la suddivisione generale del codice in cinque gruppi funzionali:

- Programma Principale;
- Gestione Oggetti;
- Rete;
- Profili;
- Configurazione.

[1] Preemptive: i sistemi operativi in grado di interrompere un processo in esecuzione quando il proprio quanto di tempo è scaduto sono detti preemptive.

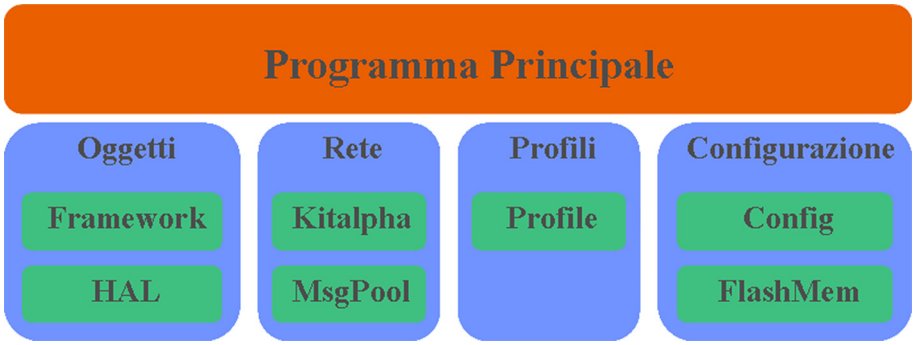


Figura 6.2: Struttura del firmware del FEIM.

Programma Principale Si occupa dell'inizializzazione del sistema interno e del coordinamento dell'esecuzione dei vari task. Di fatto presenta un loop infinito che manda in esecuzione i vari task ed esegue la verifica delle condizioni di anomalia.

Gestione Oggetti La gestione del paradigma di astrazione ad oggetti è affidata ad uno stack che include due livelli: un livello di astrazione dall'hardware (HAL, Hardware Abstraction Level) ed un livello di gestione delle funzioni dei singoli tipi di oggetto (Framework).
L'HAL a sua volta è rappresentato da uno stack a tre livelli:

- User Level;
- Peripheral Level;
- Device Level.

Il Device Level si interfaccia direttamente con le periferiche hardware, mentre lo User Level è l'interfaccia verso il livello Framework. La suddivisione su tre livelli dell'HAL consente la massima flessibilità in termini di gestione e portabilità del firmware verso altri microcontrollori della stessa famiglia o verso microcontrollori completamente differenti, in quanto è possibile alterare il livello Device Level, per gestire altri tipi di periferiche analoghe a quelle gestite ora, ed il Peripheral level, per aggiungere nuovi tipi di periferica, lasciando però inalterato lo User Level, che

permette l'interfacciamento con il Framework, che non viene quindi influenzato dal porting, così come non vengono influenzati i livelli superiori dello stack.

Rete La gestione della rete è suddivisa in due sezioni: una sezione si occupa dell'implementazione del protocollo di comunicazione su Ethernet (il Kitalpha) ed esegue quindi le procedure di creazione dei messaggi e decodifica degli stessi. Per la trasmissione e ricezione vengono sfruttate le librerie di comunicazione TCP/IP fornite con l'ambiente di sviluppo. La seconda sezione si occupa della gestione delle code per l'invio dei messaggi non sollecitati e di quelli di risposta a comandi inviati, o dall'LMP o da un altro FEIM.
La suddivisione dei messaggi da inviare in tre code distinte consente una gestione molto efficiente della comunicazione in caso di problemi di connessione con l'LMP, in quanto in questi casi vengono bloccate solo la coda relativa ai messaggi di trap ed eventualmente quella di risposta ai comandi dall'LMP, se l'interruzione si verifica prima della conclusione di un comando impartito, lasciando però correttamente funzionante la coda dei messaggi da inviare agli altri FEIM, garantendo quindi l'indipendenza del meccanismo di comunicazione P2P da eventuali problemi di comunicazione con l'LMP.

Profili L'intero sistema di gestione dei profili è gestito da un unico modulo, che viene utilizzato dai vari elementi del firmware al fine di determinare se le operazioni che devono essere effettuate (trasmissione di messaggi, scrittura su oggetti, ...) possono essere effettuate nel profilo corrente. Ovviamente il modulo viene aggiornato sia dal modulo di rete, alla ricezione di comandi di modifica del profilo da parte dell'LMP o in caso di errori permanenti di comunicazione con lo stesso, sia da parte del programma principale, nel momento in cui venga perso il link di connessione o venga richiesto il reset del modulo.

Configurazione Il modulo di configurazione è suddiviso in due sottomoduli: uno si occupa effettivamente dell'interpretazione del file di configurazione ricevuto in fase di prima accensione, o in caso di invalidazione della configurazione, l'altro è un

modulo di basso livello per la gestione della memoria flash esterna, che ne verifica la coerenza e ne valida il contenuto mediante l'uso di hash MD5. Nel caso in cui, durante un riavvio, la configurazione risultasse non valida, genera un allarme che porta il programma principale a riavviare la procedura di configurazione di rete e degli Oggetti.

6.7 Collaudo funzionale e prove CE

Il collaudo funzionale è stato eseguito sia per quanto riguarda la sezione di alimentazione, sia per quanto riguarda il funzionamento complessivo del modulo. Le modalità di collaudo funzionare in laboratorio e sul campo sono descritte nelle sezioni 7.1 e 8. Il passo finale per verificare se un dispositivo può essere immesso in commercio è la verifica dei requisiti per la marcatura CE. Per il dispositivo in questione, trattandosi di un circuito alimentato in bassa tensione e che non controlla direttamente carichi a tensione di rete, non è richiesta che la verifica di compatibilità elettromagnetica (EMC), secondo le norme CEI EN 61000-6-1 e CEI EN 61000-6-3.
Le prove svolte hanno dimostrato che il dispositivo risulta essere conforme, se dotato di opportune ferriti di blocco sul cavo Ethernet e sui cavi di connessione con i sensori analogici. La causa delle interferenze è da ricercarsi nella progettazione del modulo RCM3700, che risulta propagare grandi livelli di interferenza attraverso il cavo Ethernet e attraverso la massa del modulo. Essendo il modulo non di nostra progettazione, non è possibile intervenire sullo stesso direttamente, sono quindi necessari dei mezzi di blocco delle interferenze prima che queste si possano propagare lungo i cavi di segnale, ovvero le ferriti.

Capitolo 7

Test in laboratorio

Con i "vorrei" non si è mai fatto niente.
Con i "proverò" si son fatte grandi cose.
"Voglio" ha fatto miracoli.

– Xavier de Ravignan

AL fine di collaudare correttamente il modulo FEIM e di avere un supporto per lo sviluppo del firmware e del software, è stato sviluppato un ambiente di test all'interno del laboratorio del dipartimento. L'ambiente è stato realizzato in modo quanto più possibile realistico e simile alle effettive installazioni previste.

7.1 Pannelli da laboratorio

Al fine di ottenere un ambiente di test realistico, ma indipendente dagli impianti del laboratorio, sono stati realizzati due pannelli, sui quali sono rappresentate le planimetrie di un mini-appartamento, composto da una cucina, una camera da letto ed un bagno. Ciascun pannello ha la dimensione di 1 m per 1.4 m. Sul pannello che

rappresenta la cucina (Figura 7.1) sono installati:

- 1 lampada;
- 2 contatti magnetici;
- 1 sensore di fumo;
- 1 sensore di gas metano;
- 1 sensore di movimento a doppia tecnologia (PIR e microonde);
- 1 sensore integrato di temperatura ed umidità relativa;
- 1 set point di temperatura;
- 3 pulsanti;
- 2 spie a 220 V;
- 1 buzzer;
- 1 presa di corrente.

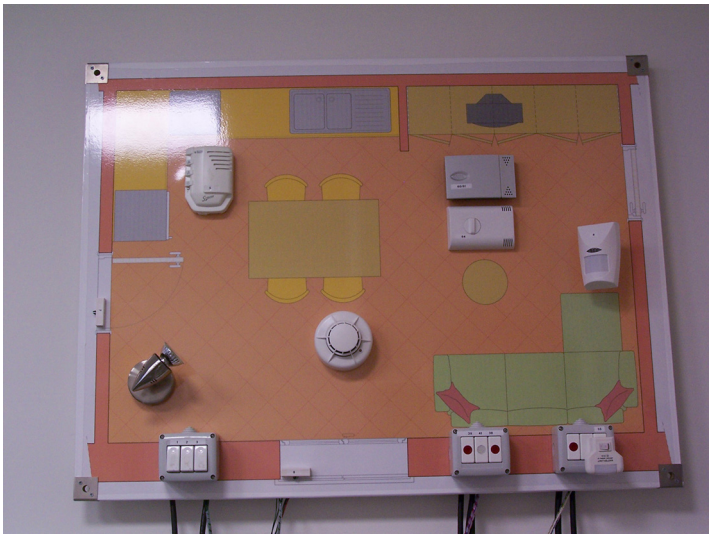


Figura 7.1: Foto del pannello di test rappresentate una cucina.

Mentre su quello che rappresenta la camera da letto (Figura 7.2) sono installati:

- 1 lampada;
- 3 contatti magnetici;
- 1 sensore di allagamento;
- 1 sirena di allarme;
- 1 sensore di movimento;
- 1 sensore integrato di luminosità e temperatura;
- 4 pulsanti;
- 3 spie a 220 V;
- 2 prese di corrente.

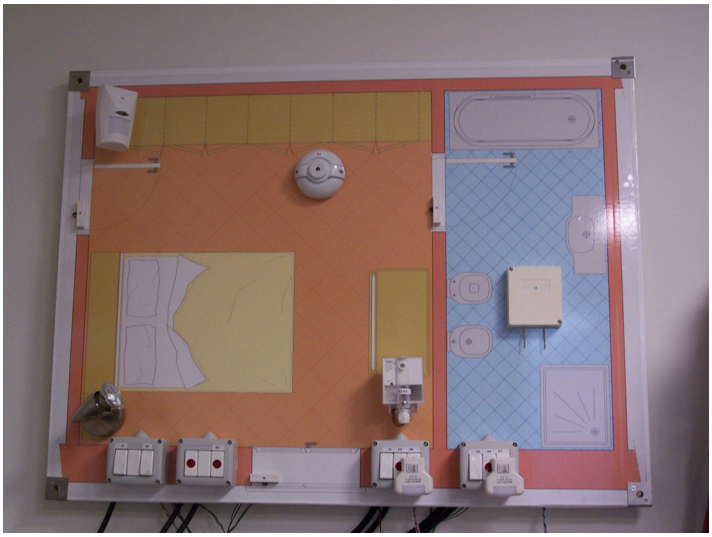


Figura 7.2: Foto del pannello di test rappresentate una camera da letto ed un bagno annesso.

I due pannelli sono poi collegati tramite opportuni cavi di potenza e segnale ad un terzo pannello (Figura 7.3) che rappresenta un quadro elettrico e su di esso sono installate la sezione di alimentazione con UPS, gli interruttori automatici di sicurezza

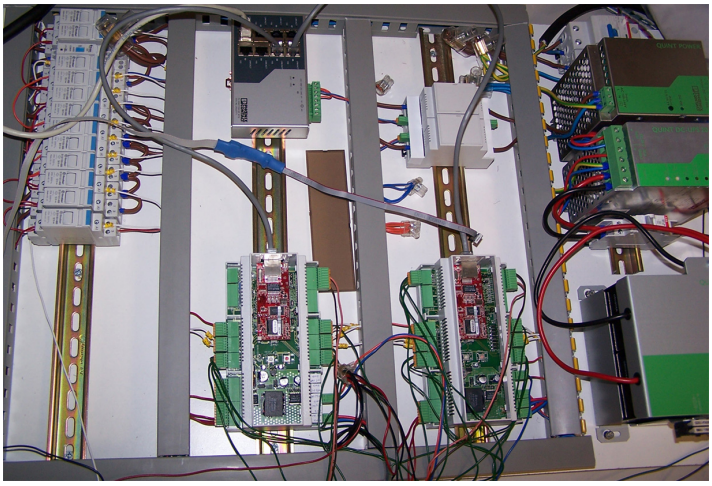


Figura 7.3: Foto del pannello di test con installati i moduli di automazione, uno switch da quadro, i relè e la sezione di alimentazione.

(magnetotermico e differenziale), uno switch alimentato a 24 V, due moduli FEIM e 13 relè modulari per montaggio a pannello, per il controllo delle prese di corrente, delle luci, delle spie, della sirena e del buzzer.

7.2 Prove funzionali

Al fine di provare il corretto funzionamento del modulo è stato necessario ricreare le situazioni di funzionamento nel modo più realistico possibile. Sfruttando i pannelli del laboratorio è stato possibile simulare normali operazioni, sia dei pulsanti, sia di tutti i vari sensori installati. L'utilizzo dei sensori e l'impostazione di vari parametri per il funzionamento del FEIM hanno condotto alla creazione di una serie di configurazioni standard, che possono essere applicate in ambienti reali.
Per determinare se le varie regole venissero implementate correttamente, sono state svolte lunge e complesse prove, nelle quali sono state simulate situazioni di concorrenza di eventi, più o meno probabili, al fine di determinare se vi fossero interazioni impreviste fra sezioni diverse del programma, o fra linee di lettura e/o scrittura a li-

vello hardware.
Le prove svolte hanno portato all'individuazione di alcune condizioni di anomalia in casi particolari, specialmente per quanto riguarda la comunicazione fra i moduli in caso di guasti di rete in momenti specifici del funzionamento. Tali anomalie sono state isolate e risolte, anche modificando l'architettura del firmware, ad esempio con l'introduzione delle tre code messaggi distinte (cfr. sez. 6.6).

7.3 Prove di stabilità

Un elemento fondamentale delle prove di funzionamento di un sistema di questo tipo sono le prove di stabilità nel tempo, ovvero è necessario mantenere il sistema attivo costantemente in un ambiente quanto più possibile reale (eventualmente anche più "stressante", se possibile) al fine di identificare problemi a bassa frequenza di incidenza. Per questo motivo il sistema è costantemente attivo nel laboratorio, e sono stati svolti alcuni mesi di test prima di passare all'implementazione effettiva in un contesto reale (cfr. cap. 8).

7.4 Prove in condizioni di congestione Ethernet

Al fine di determinare l'impatto di un alto traffico Ethernet sulla rete che deve trasmettere anche le informazioni necessarie al controllo del sistema di automazione, è stato realizzato un esperimento per determinare l'impatto del traffico sulla latenza di esecuzione di un comando diretto fra FEIM e FEIM.
L'esperimento si è utilizzando una rete composta da due switch collegati fra loro da un unico cavo Ethernet. Su uno di essi è stato collegato un PC che trasmetteva dati ad un bitrate medio di circa 100 Mbps utilizzando il protocollo TCP/IP ad un altro PC, collegato invece al secondo switch. Contemporaneamente veniva variato l'ingresso di un FEIM collegato sul primo switch che, secondo una regola interna, generava un comando di attuazione di un relè collegato ad un FEIM connesso al secondo switch. In questo modo sia il traffico ad alta velocità, che il traffico di automazione dovevano condividere il cavo di connessione fra i due switch. I risultati dell'andamento della

latenza sono riportati in Figura 7.4. Durante l'esperimento il tempo di latenza non ha

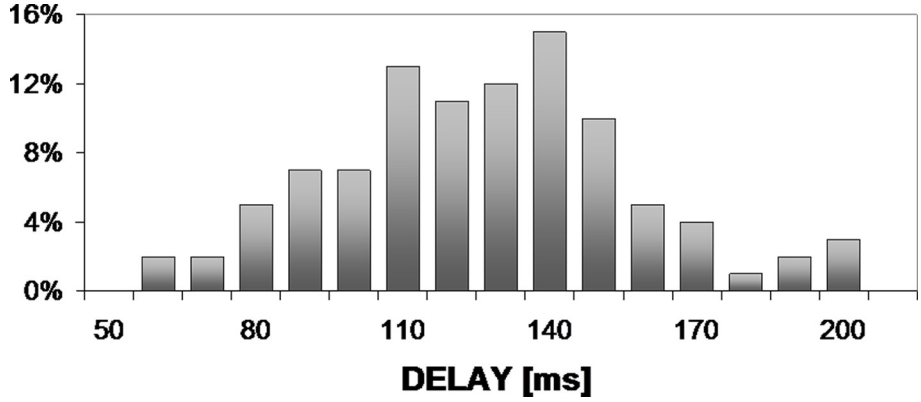


Figura 7.4: Distribuzione delle latenze di esecuzione del comando nell'esperimento ad alta congestione di rete.

mai superato i 200 ms e deve essere considerato anche che, trattandosi di un esempio reale, la latenza rilevata non è determinata solo dalla rete, ma anche dalla latenza intrinseca di rilevazione ed elaborazione dei comandi da parte dei due FEIM.
Tali rilevazioni indicano chiaramente come le latenze, introdotte dal sistema di automazione e dalla rete, sono del tutto compatibili con un normale utilizzo delle utenze domestiche.

Capitolo 8

Sperimentazione del sistema e dell'approccio

Una teoria può essere provata da un esperimento,
ma nessun percorso guida dall'esperimento
alla nascita di una teoria.

– Albert Einstein

In questo capitolo viene descritta la prima installazione in ambiente reale del sistema di automazione sviluppato.

8.1 Prima sperimentazione: residenza protetta

Come prima installazione pilota per il sistema progettato è stata scelta una residenza protetta per anziani parzialmente autosufficienti, in cui è presente personale di assistenza ventiquattr'ore su ventiquattro. In questo modo anche in caso di problemi gli utenti con difficoltà non sarebbero stati soli, ma avrebbero avuto comunque il supporto degli assistenti.

La sperimentazione è stata svolta nell'ambito del progetto "A Nostra Ca' "[1] ed è stata svolta presso la residenza protetta di Ca' Bonaparte, in Comune di Neviano degli Arduini, sulle colline vicino a Parma.
In questo capitolo verranno descritte le caratteristiche fisiche e funzionali dell'impianto realizzato e verranno anche illustrati i risultati ottenuti dopo quasi due anni di sperimentazione del sistema.

8.1.1 Struttura dell'edificio

L'edificio automatizzato è una struttura su tre piani, con cinque mini appartamenti ed alcune parti comuni, in parte utilizzate come centro diurno per anziani ed in parte come strutture di supporto alle attività quotidiane degli utenti della struttura (cucine, infermeria, lavanderia, ...). L'estensione media dei mini-appartamenti è di circa 40 m^2.

Piano Terra Sono presenti l'ingresso, un androne, una sala comune, l'infermeria con funzioni anche di ufficio, con annessi servizi igienici, la cucina con annessa dispensa, i bagni comuni ed un bagno attrezzato per persone con disabilità motorie.

Primo Piano Sono presenti tre mini appartamenti. Il primo ha due stanze: una soggiorno con angolo cottura ed una camera da letto doppia, un disimpegno ed i servizi igienici. Il secondo ed il terzo sono invece due monolocali, con disimpegno e servizi.

Piano Secondo Sono presenti due appartamenti: uno monolocale con servizi ed un appartamento per i custodi, che prestano assistenza nelle ore notturne e nei giorni festivi. Il loro appartamento è più grande, in quanto comprende, oltre ad un grande soggiorno con angolo cottura (ed un posto letto) anche una camera da letto doppia ed un disimpegno d'ingresso.

[1] Il progetto "A nostra ca' " è stato parzialmente finanziato da varie entità pubbliche: Regione Emilia-Romagna, Provincia di Parma, Comune di Neviano degli Arduini, Comune di Tornolo, Comune di Borgo Val di Taro, Azienda ASL di Parma

Figura 8.1: Foto della struttura oggetto del test.

Seminterrato Sono collocate la lavanderia ed un magazzino, oltre al locale tecnico dell'ascensore.

L'intervento di modifica dell'impianto è stato eseguito mentre l'edificio era abitato e questo ha richiesto alcune scelte di compromesso, fra le quali l'utilizzo di canalizzazioni esterne, invece della modifica dell'impianto sotto-traccia.

8.1.2 Struttura fisica dell'impianto

La struttura fisica dell'impianto di automazione è suddivisa in blocchi funzionali, sulla base dell'uso o dell'estensione delle aree. Ogni appartamento è energeticamente indipendente, mentre le parti comuni sono suddivise per gruppi funzionali e topografici, al fine di garantire l'alimentazione a tutti i moduli necessari.
Trattandosi di un'installazione sperimentale sono state previste ed installate tutte le

dotazioni che erano economicamente compatibili con il progetto, al fine di permettere il più ampio spettro di servizi sviluppabili, sia ora, sia in futuro. Ciò ha portato alla necessità di interfacciare un numero considerevole di dispositivi, complessivamente superiore alle 600 unità (comprendendo fra i sensori anche tutti i pulsanti di illuminazione e richiesta di assistenza).
Ogni appartamento è gestito da un numero di FEIM compreso fra 3 e 5 ed è alimentato da un singolo alimentatore a 24 V con UPS in bassa tensione e batteria da 7.2 Ah, sufficiente a mantenere il sistema attivo per oltre due ore in caso di black-out.
In ogni appartamento è poi installato, nel quadro di distribuzione principale, uno switch di rete Ethernet ad 8 porte, alimentato a 24 V dalla stessa linea di alimentazione dei FEIM.

Dotazione standard di ogni appartamento

Ogni appartamento ha, oltre a quanto già descritto, anche la seguente dotazione:

- sensori di movimento di tipo PIR (Passive Infra Red, sensori ad infrarossi passivi) in ogni ambiente, in alcuni casi anche più di uno, se necessari a garantire la copertura dell'intera area;
- contatti magnetici per la rilevazione dell'apertura delle porte, sia interne che esterne;
- contatti magnetici per la rilevazione dell'apertura delle finestre e delle imposte esterne (se presenti);
- un sensore di temperatura ed umidità relativa;
- una manopola per l'impostazione del set-point di temperatura;
- un sensore integrato di luminosità ambientale e temperatura in ogni ambiente;
- un sensore di posizione per ogni interruttore automatico presente nel quadro di appartamento, per la rilevazione dello stato degli interruttori magnetotermici;

- relè da barra DIN installati nei quadri di distribuzione, uno per ogni presa di corrente ed uno per ogni lampada;
- un sensore di corrente per ognuna delle tre linee di alimentazione (luci, prese da 10 A, prese da 16 A);
- pulsanti monostabili per il controllo delle luci, tiranti bagno per la richiesta di assistenza;
- un pulsante (a strappo[2]) vicino ai letti per la richiesta di soccorso;
- un campanello collegato ad un pulsante fuori dalla porta dell'appartamento;
- un buzzer per la segnalazione locale di richieste di soccorso.

I relè scelti per l'installazione sono relè a basso consumo, alimentati a 24 V corrente continua e sono di due tipi: uno ha una corrente massima gestibile di 20 A e presenta un pulsante di test per verificare il funzionamento, mentre l'altro ha un interruttore azionabile per eseguire un controllo manuale sul relè, indipendentemente dalla presenza o meno del segnale di controllo, ed un LED per la segnalazione dello stato di eccitazione del relè. Quest'ultimo relè è in grado di gestire fino a 10 A.
È importante notare il fatto che non tutti i relè disponibili in commercio hanno consumi al di sotto di 1.5 W e questo deve invece essere considerato come parametro nella scelta, in quanto l'elevato numero di moduli ha incidenza complessiva, sia in termini di consumi, sia di dissipazione termica dei quadri di controllo.

Dotazione delle parti comuni

Nelle parti comuni la dotazione è del tutto simile a quella degli appartamenti, con la differenza che non è presente un monitoraggio delle porte interne, ma solo delle porte perimetrali.

[2]Pulsante a strappo: un pulsante collegato ad un filo della lunghezza di circa 2 m collegato ad una presa di segnale posta nelle vicinanze, che permette la disconnessione automatica nel caso in cui il cavo venga tirato, al fine di evitare che ci siano danni accidentali. Dopo lo sfilamento la presa può essere facilmente reinserita.

Le sezioni di alimentazione sono complessivamente tre: una per l'infermeria e la sala comune, una per i bagni, le cucine e l'androne ed una per le cantine.
I sensori di fumo e di movimento presenti sulle scale e sui pianerottoli del secondo e terzo piano sono collegati a FEIM presenti nell'appartamento più vicino al sensore stesso.
Nell'androne è installato un avvisatore acustico per la segnalazione di condizioni di allarme.

8.1.3 Le interfacce

Le interfacce di controllo del sistema sono rappresentate da monitor LCD touch-screen. Nell'androne è presente un pannello di estrazione industriale da 12 pollici (Figura 8.2), mentre nell'appartamento dei custodi è presente un pannello di estrazione automobilistica da 8 pollici (Figura 8.3).

Ciascuna delle unità di interfacciamento è controllata da un PC industriale basato su motherboard con fattore di forma mini-ITX, basato su processore VIA Eden senza ventola, per motivi di rumorosità ed affidabilità. L'unità ha un consumo di potenza modesto, quasi dominato dal consumo dei pannelli LCD.
Gli utenti del sistema, ovvero gli ospiti della struttura, utilizzano ancora l'appartamento senza l'ausilio di interfacce dedicate, servendosi come sempre degli interruttori della luce e delle altre interfacce cui sono abituati. Ciò ha reso l'impatto psicologico dell'intervento molto ridotto.

8.1.4 La struttura di rete e le unità di supervisione

La struttura di rete è relativamente semplice e prevede uno switch di rete ad 8 porte in ogni appartamento, in infermeria, nei bagni comuni ed in cantina. Agli switch degli appartamento degli ospiti sono collegati solamente i FEIM, mentre a quello dei custodi è collegata anche l'unità di controllo dell'interfaccia grafica. Allo switch dell'infermeria, oltre ai FEIM sono collegate anche l'unità di controllo dell'interfaccia grafica dell'androne e tre prese Ethernet, ad una delle quali è connesso un PC ad uso

stazione di telemedicina. Tutti gli switch "locali" sono poi collegati ad uno switch di edificio a 20 porte che connette tutta la rete. Allo switch di edificio sono anche connessi direttamente due PC server, che operano come unità di supervisione e gateway verso una linea HDSL (da 2 Mbit nominali), posizionati in cantina. Inoltre allo stesso switch sono anche collegati una presa che va alla sala comune, dove è posto un PC ad uso stazione di video-comunicazione e quattro predisposizioni per l'installazione di access point Wi-Fi, per la copertura wireless dell'intera struttura.
All'interno del rack posto nel seminterrato, nel quale sono alloggiati i due server, è anche installato il router per la connessione HDSL, il modem ed un gruppo di continuità da 2200 VA per il mantenimento dell'alimentazione a tutti gli apparati di rete di edificio (esclusi gli switch locali, che sono alimentati a 24 V e quindi posti sotto l'UPS della singola zona di automazione) e l'interfaccia grafica dell'androne. L'interfaccia grafica dell'appartamento dei custodi è invece posta sotto un UPS indipendente da 600 VA.

8.1.5 Funzioni basilari implementate

Le funzioni basilari attualmente implementate riguardano la gestione dell'illuminazione degli ambienti, la segnalazione delle condizioni di emergenza, quali incendi ed allagamenti, mediante la segnalazione acustica e l'intervento, se necessario, di una valvola di intercettazione dell'erogazione idrica.
Sono state implementate funzioni di accensione automatica delle luci sulle scale interne e nei bagni degli ospiti che ne hanno fatto richiesta. Inoltre il sistema si occupa della gestione del riscaldamento, agendo sulle elettrovalvole che controllano la circolazione dell'acqua negli elementi radianti di ciascun appartamento.
Sono state predisposte anche funzioni per l'accensione automatica delle luci nel momento in cui una persona si alza dal letto e passa sopra un tappeto sensibile, ma questa funzione non è attualmente in uso, in quanto l'utilizzo del tappeto per la rilevazione della presenza non è consentita dalle direttive della AUSL, in quanto vi è il rischio di caduta. Per questo è in fase avanzata di sviluppo un sensore di presenza a letto che possa assolvere ad una funzione simile, senza la necessità di porre sensori che pos-

sano rappresentare un rischio di inciampo. Questo nuovo tipo di sensore avrebbe il vantaggio di fornire informazioni più attendibili sullo stato di occupazione del letto.

8.1.6 Funzioni evolute in sperimentazione

Le funzioni evolute si basano sul funzionamento delle regole a livello di LMP ed SP. Attualmente sono attive solamente funzioni di segnalazione su pannello delle condizioni di emergenza, ma sono in fase di sperimentazione servizi di allerta in caso di persone che si aggirano nelle parti comuni nelle ore notturne (wandering), utili se qualcuno degli ospiti, a causa di un momentaneo disorientamento, esce dal proprio appartamento senza rendersene conto.
Una funzione che può risultare particolarmente utile nel caso di appartamenti occupati da anziani è una funzione per la prevenzione del distacco dell'energia per superamento della potenza contrattuale (sistema anti black-out), che può operare con un avviso acustico all'avvicinarsi della soglia di distacco ed operare autonomamente un distacco dei carichi noti, secondo una priorità preimpostata, al fine di evitare che un sovraccarico, dovuto all'utilizzo contemporaneo di più elettrodomestici ad alto assorbimento, comporti il distacco della fornitura e quindi il disagio del trovarsi senza energia (e magari al buio) e dover raggiungere il punto di installazione del contatore (spesso all'esterno dell'appartamento) per poter ripristinare l'erogazione.
Altre funzioni riguardano l'attivazione di allarmi nel caso in cui l'utilizzo delle piastre elettriche superi di molto il tempo medio, al fine di segnalare condizioni di potenziale pericolo.
Un'altra funzione di grande importanza in fase di studio riguarda l'analisi (per il momento off-line, ovvero a posteriori) delle informazioni contenute nei log di attività, al fine della determinazione di profili di comportamento, con l'estrazione di indici di attività che possano essere utilizzati come parametri per la definizione di soglie di attenzione nella deriva di comportamenti. Ciò rappresenta un punto di partenza importante per l'utilizzo dei dati di monitoraggio indiretto, per la determinazione di degradazione di condizioni di salute incipienti o molto lenti.

8.1.7 Stabilità del sistema

Le procedure di installazione del sistema sono iniziate nel gennaio del 2007 e sono state concluse nel settembre dello stesso anno. Da allora l'intero sistema sta operando in modo autonomo. Sono state registrate informazioni relative allo stato del sistema a partire dal momento del completamento del sistema e tali dati sono alla base degli attuali studi per l'analisi dei dati.
Fino all'ottobre del 2008 non è stata installata nessuna unità di supervisione con funzioni diverse dalla mera registrazione degli avvenimenti. Quindi il sistema ha operato semplicemente sfruttando le funzionalità P2P dei moduli. Ciò ha consentito di verificare l'effettiva stabilità delle unità in un contesto reale particolarmente gravoso per le unità stesse, in quanto tutte le attività erano governate solamente dalle regole ivi impostate. Nell'intervallo di tempo considerato è stato riscontrato il guasto di un solo FEIM sui 31 installati. Il guasto si è verificato dopo circa 18 mesi dall'installazione ed è stato determinato che si è trattato del diodo di ricircolo di del convertitore DC/DC che fornisce l'alimentazione a 12 V. Dato che l'unità aveva un carico di alimentazione molto modesto, specialmente se confrontato con quello delle altre unità, si assume che il guasto sia ascrivibile ad un problema di fabbricazione del singolo diodo. L'unità è già stata riparata ed è ora in fase di collaudo nel laboratorio di test per determinare se vi sono altre concause.
Il firmware dei moduli è risultato stabile durante il periodo di attività, sebbene siano state riscontrate tre occasioni difficoltà di comunicazione con l'unità di controllo, le cui cause sono attualmente in fase di determinazione. In ogni caso i FEIM hanno continuato ad operare correttamente ed a fornire le funzionalità richieste, senza che gli ospiti si siano accorti di nulla, grazie al meccanismo automatico di gestione delle anomalie descritto nel paragrafo 5.7.1.

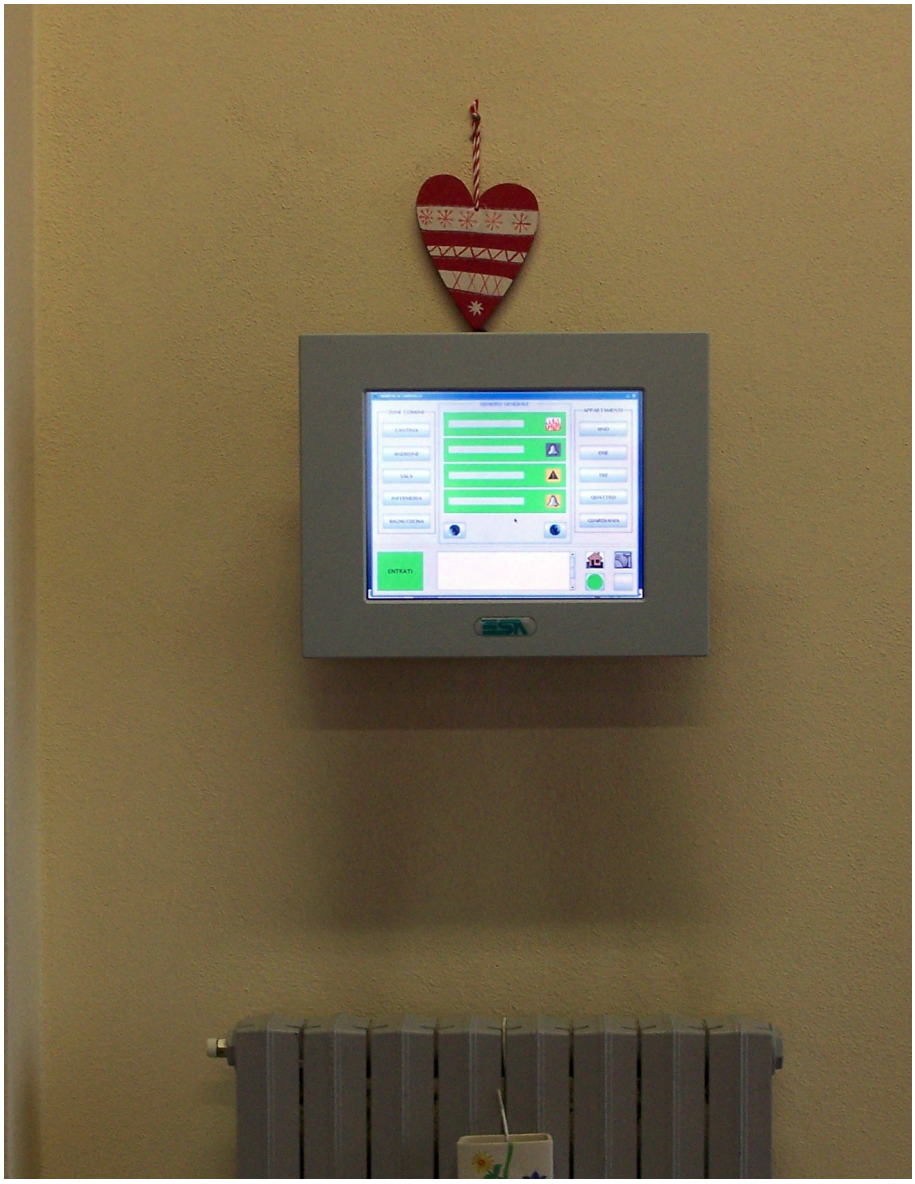


Figura 8.2: Pannello LCD con touch-screen installato nell'atrio della struttura.

Figura 8.3: Pannello LCD con touch-screen installato nell'appartamento dei custodi. Si vede in basso anche l'unità PC embedded su un mobile.

Capitolo 9

Conclusioni e sviluppi futuri della ricerca

Non penso mai al futuro.
Arriva così presto.

– Albert Einstein

In questo capitolo verranno ripresi i concetti fondamentali della ricerca, evidenziandone i punti di forza e le possibili evoluzioni ed integrazioni future.

9.1 Convergenza verso la rete Ethernet ed altri protocolli ampiamente diffusi

In questo lavoro di ricerca è stato sviluppato un sistema di automazione basato sulla rete Ethernet, che utilizza IP come protocollo di comunicazione fra unità di interfacciamento con sensori a basso costo (FEIM), aventi interfacce standard per l'automazione domestica ed industriale. Il sistema sviluppato si basa su un approccio di gestione gerarchico ad intelligenza distribuita, che permette un'elevata scalabilità ed

al tempo stesso un'efficiente gestione dei guasti, al fine di garantire in ogni momento le funzioni di base.

L'utilizzo della rete Ethernet, come mezzo di trasporto per le informazioni di automazione, ha intrinsecamente il vantaggio di utilizzare una tecnologia standard, aperta, ampiamente diffusa ed a basso costo. Inoltre altri servizi fondamentali nell'ambito domestico stanno convergendo verso il trasporto su IP, quali ad esempio la telefonia (VoIP) e l'intrattenimento (IPTV), con il vantaggio di ridurre drasticamente il numero di connessioni necessarie all'interno degli edifici. Ciò perché il solo cablaggio strutturato mediante cavi Ethernet, o copertura Wi-Fi, potrà sostituire i cablaggi per la telefonia, per la televisione, sia terrestre sia satellitare, e consentire al tempo stesso la trasmissione dati fra i vari dispositivi informatici utilizzati normalmente, quali PC e PDA.

La grande apertura del sistema ai maggiori protocolli standard di comunicazione offre ampie garanzie di compatibilità con diversi produttori di dispositivi, sia sensori che attuatori, sia presenti che futuri, permettendo quindi di mantenere bassi i costi di installazione e manutenzione futura, senza legarsi in modo stretto ad un singolo produttore di dispositivi.

L'architettura di controllo del sistema è basata su normali PC, permettendo quindi l'integrazione di applicativi basati sulla stessa piattaforma per ampliare le funzioni di supervisione, permettendo ad esempio l'implementazione di controlli vocali.

9.2 Controllo locale, mobile e remoto

Il fatto che il sistema utilizzi IP come protocollo di comunicazione consente un'integrazione nativa con internet, permettendo quindi una semplice ed efficiente gestione da remoto del sistema, sia per quanto riguarda la supervisione che il controllo, sia per finalità di manutenzione o monitoraggio tecnico, sia per la ricezione di richieste di intervento legate ad emergenze sanitarie.

L'utilizzo di reti Wi-Fi consente l'integrazione di terminali mobili nel sistema, esattamente come se questi fossero collegati alla rete LAN, ancora una volta in modo efficiente e senza apportare modifiche al sistema di automazione stesso.

È inoltre possibile pensare di espandere il sistema integrando sistemi wireless pensati esplicitamente per l'automazione domestica, ad esempio basati sullo standard IEEE 802.l5.4/ZigBee [52]. Ciò può avvenire tramite un gateway che, dotato di porta di comunicazione Ethernet, faccia da tramite per la trasmissione dei pacchetti di livello applicativo, o anche di livello IP. La realizzazione di un'infrastruttura wireless basata sul protocollo ZigBee consente di utilizzare terminali mobili alimentati a batterie e dotati di un'elevata autonomia, ad esempio per la realizzazione di telecomandi o sistemi di monitoraggio personale.

9.3 Integrazione del wireless per il monitoraggio personale

La tecnologia ZigBee può essere la chiave per la realizzazione di sistemi di monitoraggio personale, che possono aggiungere alle capacità di monitoraggio indiretto e non invasivo, intrinseche del sistema cablato, anche la capacità di acquisire informazioni biologiche dagli utenti che necessitano di un controllo più stretto, e che possono beneficiare delle funzioni aggiuntive che questo può offrire. Ad esempio si possono realizzare sistemi per la richiesta di soccorso personali, sistemi per la segnalazione delle cadute o di condizioni di deambulazione compromessa, che possono essere rischiose. Possono consentire, con reti sufficientemente estese, di aggiungere funzioni di localizzazione all'interno di edifici particolarmente estesi, quali ad esempio residenze protette o strutture ospedaliere, consentendo, in caso di emergenza, di dirigere i soccorsi subito nella posizione dell'utente che necessita di aiuto, o anche di segnalare situazioni di potenziale pericolo, quando un soggetto si sta allontanando dalla propria casa o si sta avvicinando ad aree pericolose, se le condizioni lo richiedono. L'integrazione di tecnologie di tipo RFID[1] permette di incrementare la precisione e l'efficienza di tale approccio, ad esempio consentendo di monitorare varchi critici.

[1] RFID: Radio Frequency Identification, tecnologie di identificazione radio, realizzate mediante dispositivi estremamente piccoli e privi di proprie fonti di alimentazione, che vengono letti ed alimentati da un'onda radio generata da un apposito lettore.

9.4 Sicurezza: autenticazione e crittografia

Il sistema attualmente impiega il mezzo di comunicazione assumendo che questo sia protetto dall'accesso da parte di terzi. Non sono state quindi ancora implementate politiche di autenticazione e crittografia delle informazioni trasmesse e ricevute, a nessun livello. Nel caso di comunicazioni verso l'esterno sono utilizzate tecnologie di protezione (VPN) che consentono di mantenere il livello di sicurezza anche con connessioni remote.
È però ovvio come sia necessario prendere in debita considerazione questi aspetti nel momento in cui si pensa ad un'espansione dell'approccio a sistemi di maggiore estensione o complessità, che coinvolgano più di un'utenza di test o domestica.
L'introduzione di queste funzionalità nel sistema risulta sostanzialmente semplice al livello di supervisione, in quanto la potenza di calcolo a disposizione rende possibile l'implementazione di politiche di cifratura a chiave pubblica particolarmente efficaci.
Per quanto riguarda invece il livello di campo è necessario studiare politiche meno esigenti dal punto di vista delle risorse di elaborazione e della memoria necessaria, data l'attuale architettura dei FEIM.
Non è comunque esclusa una successiva revisione del core dei moduli FEIM a favore di dispositivi più performanti, e nonostante ciò economici, che permetterebbero di ridurre i vincoli in termini di potenza di elaborazione, aprendo la strada a soluzioni differenti.

Bibliografia

[1] ISTAT. Indagine sulle condizioni di salute e ricorso ai servizi sanitari. Technical report, ISTAT, 2004-2005.

[2] Paolo Ciampolini, Ilaria De Munari, Guido Matrella, Ferdinando Grossi, and Valentina Bianchi. An "assistance over ip" network for monitoring and support of daily living activities. In *Challenges for Assistive Technology. 9th European Conference for the Advancement of Assistive Technology in Europe*, volume 20, pages 743–747, AMSTERDAM – NLD, 3-5 October 2007. IOS PRESS.

[3] Paolo Ciampolini, Ilaria De Munari, Guido Matrella, Ferdinando Grossi, and Valentina Bianchi. *Progettare per l'autonomia. Ausili e ambiente per la qualità della vita*, volume 1, chapter Favorire l'indipendenza attraverso l'uso dell'intelligenza distribuita in una casa domotica, pages 44–55. GIUNTI, ITA, 2008.

[4] D. Dietrich, W. Kastner, T. Maly, C. Roesener, G. Russ, and H. Schweinzer. Situation modeling. In *IEEE International Workshop on Factory Communication Systems. Proceedings 2004*, volume 1, pages 93–102, 2008.

[5] Majd Alwan, David C. Mack, Siddharth Dalal, Steve Kell, Beverely Turner, and Robin A. Felder. Impact of monitoring technology in assisted living: outcome pilot. *IEEE Transaction On Information Technology in Biomedicine*, 10(1):192–198, January 2006.

[6] Gilles Virone, Majd Alwan, Siddharth Dalal, Steven W. Kell, Beverely Turner, John A. Stankovic, and Robin Felder. Behavioral patterns of older adults in assisted living. *IEEE Transaction On Information Technology in Biomedicine*, 12(3):387–398, May 2008.

[7] A.M. Cole and B.Q.Tran. Home automation to promote independent living in elderly populations. In *Proceedings of the Second Joint EMBS/BMES Conference*, volume 3, pages 2422–2423, 2002.

[8] O.O. Brdiczka, J.J. L. Crowley, and P.P. Reignier. Learning situation models in a smart home. *IEEE Transactions on Systems, Man, and Cybernetics, Part B. Accepted for future publication*, PP:56–63, 2003.

[9] Gerhard Pratl, Walter T. Penzhorn, Dietmar Dietricht, and Wolfgang Burgstaller. Perceptive awareness in building automation. In *IEEE 3rd International Conference on Computational Cybernetics. ICCC 2005.*, volume 1, pages 259–264, 2005.

[10] Gerhard Pratl, Dietmar Dietrich, Gerhard P. Hancke, and Walter T. Penzhorn. A new model for autonomous, networked control systems. *IEEE Transactions on Industrial Informatics*, 3(1):21–32, Feb 2007.

[11] Valentina Bianchi, Ferdinando Grossi, Guido Matrella, Ilaria De Munari, and Paolo Ciampolini. Fall detection and gait analysis in a smart home environment. In *GERONTECHNOLOGY - International journal on the fundamental aspect of technology to serve the ageing society - Conference issue Pisa, June 4-6, 2008*, volume 7(2), page 73, 4-6 Giugno 2008.

[12] Valentina Bianchi, Ferdinando Grossi, Guido Matrella, Ilaria De Munari, and Paolo Ciampolini. A wireless sensor platform for assistive technology applications. In *Proceeding of the 11th Euromicro Conference On Digital System Design*, pages 809–816, September 3-5 2008.

[13] Deborah Snoonian. Smart buildings. *IEEE Spectrum*, 40(8):18–23, Aug 2003.

[14] Wolfgang Kastner, Georg Neugschwandtner, Stefan Soucek, and H. Michael Newman. Communication systems for building automation and control. *Proceedings of the IEEE*, 93(6):1178–1203, Jun 2005.

[15] Harrison Cooper. X10 FAQ [online]. 2008. Disponibile a: `http://www.nomad.ee/micros/x10faq.html` [citato 31-11-2008].

[16] Phillip Kingery. Digital X-10 [online]. 2008. Disponibile a: `http://www.hometoys.com/htinews/feb99/articles/kingery/kingery13.htm` [citato 30-11-2008].

[17] S. T. Bushby. BACnet: a standard communication infrastructure for intelligent buildings. *Autom. Construction*, 6(5–6):529–540, 1997.

[18] Wolfgang Kastner, Georg Neugschwandtner, Stefan Soucek, and H. Michael Newman. Communication Systems for Building Automation and Control. *Proceedings of IEEE*, 93(6):1178–1203, June 2005.

[19] Tae-Jin Park, Young-Chan Kwon, and Seung-Ho Hong. Performance evaluation of BACnet MS/TP protocol using experimental model. In *IEEE International Conference on Industrial Technology, ICIT 2005.*, 2005.

[20] Larry K. Haakenstad. The Open Protocol Standard for Computerized Building Systems: BACnet. In *IEEE International Conference on Control Applications*, volume 2, pages 1585–1590, August 1999.

[21] S.U.Cho and S.H. Hong. Fault Tolerant BBMD in the BACnet/IP Protocol. In *IEEE International Conference on Industrial Technology, ICIT 2006.*, 2006.

[22] Ziyan Jiang. An information platform for building automation system. In *IEEE International Conference on Industrial Technology. ICIT 2005*, volume 1, pages 1391–1396, Dec 2005.

[23] Chetan Tamboli and Constantine N. Mani kopoulos. Determination of the optimum packet length and buffer sizes for the industrial building automation

and control networks. In *Proceedings of the IEEE International Symposium on Industrial Electronics ISIE '95.*, volume 2, pages 831–836, 1995.

[24] Tae Jin Park and Seung Ho Hong. Development of an Experimental Model of BACnet-based Lighting Control System. In *IEEE International Conference on Industrial Informatics*, volume 1, pages 114–119, 2006.

[25] D. Loy, D. Dietrich, and H. Schweinzer. *Open Control Networks*. Kluwer, Norwell, MA, USA, 2004.

[26] Peter Fischer, Michael Holz, and Martin Menzel. Network management for a safe communication in an unsafe environment. In *5th IEEE International Conference on Industrial Informatics*, volume 1, pages 131–136, 2007.

[27] Stefano Bellintani. *Manuale della Domotica.* Il Sole 24 Ore, Milano, 2004.

[28] Konnex. Associazione konnex italia [online]. 2008. Disponibile a: `http://www.konnex.it/` [citato 4-12-2008].

[29] W. Kastner and G. Neugschwandtner. Service interfaces for field-level home and building automation. In *IEEE International Workshop on Factory Communication Systems, 2004. Proceedings.*, volume 1, pages 103–112, 2004.

[30] W. Kastner. Jini connectivity for fieldbus systems. In *Proceedings of the 2000 IEEE International Symposium on Intelligent Control*, volume 1, pages 229–234, 2000.

[31] Bticino. MyHome Bticino [online]. 2008. Disponibile a: `http://www.myhome-bticino.it/` [citato 2-12-2008].

[32] CAN in Automation CiA. CANOpen [online]. 2008. Disponibile a: `http://www.can-cia.org/` [citato 4-12-2008].

[33] Kyung Chang Lee and Hong-Hee Lee. Network-based fire-detection system via controller area network for smart home automation. *IEEE Transactions on Consumer Electronics*, 50(4):1093–1100, Nov 2004.

[34] Takao Kashiwamura, Hisao Koga, and Yasuji Murakami. Telecommunications aspects of intelligent buildings. *IEEE Communications Magazine*, 29(4):28–32,39–40, Apr 1991.

[35] ISO/IEC 7498-1:1994. *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*. ISO, Geneva, Switzerland, 1994.

[36] IEEE. IEEE Registration Authority - IEEE OUI and Company_id Assignments [online]. 2008. Disponibile a: `http://standards.ieee.org/regauth/oui/index.shtml` [citato 4-12-2008].

[37] S. Knauth, R. Kistler, D. KÍaslin, and A. Klapproth. SARBAU Towards Highly Self-Configuring IP-Fieldbus Based Building Automation Networks. In *22nd International Conference on Advanced Information Networking and Applications. AINA 2008.*, volume 1, pages 713–717, 2008.

[38] Stefan Soucek and Thilo Sauter. Quality of service concerns in IP-based control systems. *IEEE Transactions on Industrial Electronics*, 51(6):1249–1258, Dec 2004.

[39] Ferdinando Grossi, Guido Matrella, Ilaria De Munari, and Paolo Ciampolini. A flexible home automation system applied to elderly care. In *ICCE07 Digest of Technical Papers*, volume 1, pages 341–342, TAMPERE – FIN, 10-14/01/2007. Suvisoft Oy Ltd.

[40] Ferdinando Grossi, Valentina Bianchi, Guido Matrella, Ilaria De Munari, and Paolo Ciampolini. An assistive home automation and monitoring system. In *ICCE08 Digest of Technical Papers*, pages 1–2, 11-13 January 2008.

[41] Ferdinando Grossi, Valentina Bianchi, Guido Matrella, Ilaria De Munari, and Paolo Ciampolini. A versatile home control and monitoring network. In *GERONTECHNOLOGY - International journal on the fundamental aspect of technology to serve the ageing society - Conference issue Pisa, June 4-6, 2008*, volume 7(2), page 116, 4-6 Giugno 2008.

[42] Guido Matrella, Ferdinando Grossi, Valentina Bianchi, Ilaria De Munari, and Paolo Ciampolini. An environmental control hw/sw framework for daily living of elderly and disabled people. In *Telehealth and Assistive Technologies TeleHealth/AT 2008*, volume 1, pages 103–108. R. Merrell, R.A. Cooper, April 16-18, 2008.

[43] Ferdinando Grossi, Valentina Bianchi, Guido Matrella, Ilaria De Munari, and Paolo Ciampolini. A lan-based home control system. In *Building Comfortable and Liveable Environment for All*, pages –, 15-16 May 2008.

[44] Ferdinando Grossi, Guido Matrella, Ilaria De Munari, and Paolo Ciampolini. A lan-based home automation and monitoring system. In *Proceeding of the International Conference on Aging, Disability and Independence*, GAINESVILLE – USA, February 20-23 2008. University of Florida.

[45] VIA. VIA Mini-ITX Mainboard Form Factor: 17cm x 17cm - VIA Technologies, Inc. [online]. 2008. Disponibile a: `http://www.via.com.tw/en/initiatives/spearhead/mini-itx/` [citato 23-12-2008].

[46] Fabio Fiamingo, Carlo Mazzetti, and Zdobyslaw Flisowski. Smart building and lightning risk assessment: an approach to the protection of building automation systems high exposed to overvoltage failure. In *IEEE Power Tech Conference Proceedings*, volume 4, 2003.

[47] Modbus-IDA. Modbus-IDA Technical Resources [online]. 2008. Disponibile a: `http://www.modbus.org/tech.php` [citato 13-12-2008].

[48] Ran Giladi. Heterogeneous building automation and IP networks management. In *24th International Conference on Distributed Computing Systems Workshops, 2004. Proceedings.*, volume 1, pages 636–641, 2004.

[49] S. Knauth, D. Kaslin, R. Kistler, and A. Klapproth. UPnP Compression for IP based Field Devices in Building Automation. In *IEEE Conference on Emerging Technologies and Factory Automation, 2006. ETFA '06.*, volume 1, pages 445–448, 2006.

[50] Pan Dongbo, Liu Feng, Zhou Xuelian, and Li Tao. Functional safety in building automation and control systems. In *3rd IEEE Conference on Industrial Electronics and Applications, ICIEA 2008.*, volume 1, pages 467–470, 2008.

[51] Peter Palensky Thomas Novak, Albert Treytl. Common approach to functional safety and system security in building automation and control systems. In *IEEE Conference on Emerging Technologies & Factory Automation, 2007. ETFA.*, 2007.

[52] David Egan. The emergence of ZigBee in building automation and industrial control. *Computing & Control Engineering Journal*, 16(2):14–19, Apr-May 2005.

Ringraziamenti

Innanzitutto ringrazio di cuore la professoressa Ilaria De Munari ed il professor Paolo Ciampolini, per avermi dato l'opportunità di svolgere quest'attività di ricerca e per il costante supporto, sia scientifico che personale, che mi hanno dato in questi anni.

Desidero inoltre ringraziare il Comune di Neviano, nelle persone del Sindaco Dott. Giordano Bricoli e della Signora Roberta Ferzini, per avere creduto e sostenuto il progetto di Ca' Bonaparte, non facendo mai mancare il loro aiuto e la loro collaborazione nelle fasi di realizzazione della struttura sperimentale. Ringrazio inoltre gli ospiti e il personale di assistenza di Ca' Bonaparte, per l'accoglienza sempre calorosa ed amichevole e per la pazienza e la disponibilità mostrata durante i lavori di installazione e collaudo.

Uno speciale ringraziamento va alla mia famiglia, che mi ha sopportato con coraggio durante quest'avventura, nonostante i momenti di difficoltà incontrati durante il lungo cammino, che culmina ora con la discussione della tesi, ma non si ferma qui.

Ringrazio tutti i miei compagni di palazzina, per la simpatia ed i momenti di divertimento che abbiamo condiviso. In particolare ringrazio Paolo e Alessandro, con i quali condivido l'ufficio e con cui è sempre possibile discutere di qualunque cosa, dalla storia alternativa del mondo alla fantascienza. Ringrazio Valentina, per il prezioso supporto scientifico e morale, Matteo, per il suo punto di vista schietto veritiero, che mi ha aiutato a vedere le cose in modo diverso e Andrea Ricci, per le interessanti discussioni. Ringrazio sentitamente Guido per la simpatia e le lunghe chiacchierate. Non posso dimenticare Andrea Crinto, per la cara amicizia e la disponibilità sempre

dimostrata.

Ringrazio i tesisti che si sono avvicendati negli anni a supporto delle attività della ricerca, che hanno portato preziosi contributi a questa grande avventura che stiamo portando avanti. In particolare ricordo Andrea Camurri, che insieme a Fulvio Mazzamuto, era presente all'inizio del viaggio, e che ci ha raggiunto ancora nei pressi della conclusione, Andrea Rossini, Alberto Rizzi, Jacopo Bocchialini e Niccolò Mora, che hanno dedicato molto tempo ed energie alla buona riuscita del progetto. Un particolare ringraziamento va ad Andrea Zurla, non solo per il grande contributo tecnico dato al progetto durante la tesi e successivamente, ma anche per l'amicizia ed il supporto accordato durante le avventure che lo hanno accompagnato.

Ringrazio di cuore Roberto, che pur essendo letteralmente dall'altra parte del mondo mi ha donato la sua amicizia, tenuto compagnia e dato preziosi consigli per via telematica. Ricordo Paolo Baroncini, per la simpatia e gli interessanti confronti sui progetti svolti insieme.

Vorrei poi ringraziare tutti i miei amici, che pur non avendo contribuito direttamente a questo lavoro, mi hanno aiutato a non perdere (del tutto) la sanità mentale, in particolare Vitto, Pongo, Pierpa, Erika, Aldo, Mana, Elena, Oscar, Pera, Max ed Elisa.

Molte altre persone meriterebbero di essere ricordate qui, ma forse non c'è lo spazio e non voglio rischiare di dimenticare qualcuno, quindi le ringrazio collettivamente per i consigli e l'amicizia che mi hanno dimostrato.

Ringrazio tutti per aver sopportato le spigolosità del mio carattere... e per avermi aiutato a limarle almeno un po'.