POLITECNICO DI MILANO
Corso di Laurea Magistrale in Ingegneria Informatica
Dipartimento di Elettronica e Informazione

REALIZZAZIONE DI UN SISTEMA DI RICEZIONE ALLARMI E TELEGESTIONE UNIFICATO PER CENTRALI ANTI-INTRUSIONE

Relatore: Prof. William Fornaciari
Correlatore:

Tesi di Laurea di:
Matteo Gianello, matricola 771166

Anno Accademico 2014-2015

A Ilaria

Sommario

Ringraziamenti

Ringrazio .....

Indice

Capitolo 1

Introduzione

La diffusione di connessioni a banda larga, il progressivo abbandono di reti telefoniche convenzionali e il passaggio su linee telefoniche VoIP hanno costretto le vigilanze private a trovare nuovi meccanismi di comunicazione verso gli apparati remoti di sicurezza da loro gestiti. Inoltre la richiesta di tempi di intervento più brevi e contatto con il cliente solo quando è indispensabile richiedono strumenti di controllo e verifica immediati e di facile utilizzo.

1.1 Inquadramento generale

Questa tesi è stata sviluppata in collaborazione con *LIS s.r.l.*, vigilanza privata che si distingue per i tempi di intervento ridotti e la possibilità di gestione degli impianti da remoto. Queste caratteristiche distinguono *LIS* già dai primi anni di attività quando ancora la ricezione degli allarmi e la tele-gestione avveniva tramite linee telefoniche tradizionali.
Negli ultimi anni tuttavia ci siamo trovati in difficoltà in quanto molte delle linee telefoniche tradizionali stanno scomparendo sostituite da fibre ottiche e linee VoIP questo impedisce la normale gestione. Si è deciso perciò di effettuare un aggiornamento del sistema in modo da permettere a *LIS* di gestire gli impianti tramite le connessioni a banda larga o tramite linee telefoniche mobili. Oltre alla gestione degli impianti un altro punto sul quale ci focalizzeremo è quello della ricezione degli allarmi in modo tale da permettere una ricezione quasi istantanea della segnalazione di allarme e quindi una gestione immediata dell'eventuale situazione di emergenza.

1.2 Breve descrizione del lavoro

Questa tesi si sviluppa nell'ambito della sicurezza privata. Prima di addentrarci nello specifico dobbiamo capire come lavora una vigilanza privata.

Possiamo distinguere due operazioni principali che una vigilanza privata svolge, la prima è il lavoro di ricezione e verifica delle segnalazioni d'allarme provenienti dalle varie centrali di sicurezza e gli operatori, tramite l'ausilio di immagini provenienti da eventuali sistemi di videosorveglianza, valutano e gestiscono i vari eventi.
La seconda funzione è quella di gestire gli impianti come ad esempio l'inserimento delle centrali antintrusione o l'esclusione di sensori guasti.
In LIS era già presente un sistema di che permetteva all'operatore di gestire

1.3 Struttura della tesi

La terza parte contiene la descrizione della struttura della tesi ed è organizzata nel modo seguente. "La tesi è strutturata nel modo seguente.

Nella sezione due si mostra ...

Nella sez. tre si illustra ...

Nella sez. quattro si descrive ...

Nelle conclusioni si riassumono gli scopi, le valutazioni di questi e le prospettive future ...

Nell'appendice A si riporta ... (Dopo ogni sezione o appendice ci vuole un punto)."

I titoli delle sezioni da 2 a M-1 sono indicativi, ma bisogna cercare di mantenere un significato equipollente nel caso si vogliano cambiare. Queste sezioni possono contenere eventuali sottosezioni.

Capitolo 2

La sicurezza privata

> *"Giuro di osservare lealmente le leggi e le altre disposizioni vigenti nel territorio della Repubblica e di adempiere le funzioni affidatemi con coscienza e diligenza, nel rispetto dei diritti dei cittadini."*
>
> Giuramento di una guardia particolare giurata

La sicurezza (dal latino sine cura: senza preoccupazione) può essere definita come la conoscenza che l'evoluzione di un sistema non produrrà stati indesiderati. In termini più semplici è: sapere che quello che faremo non provocherà dei danni.[3]

2.1 Le vigilanze private

La vigilanza privata è l'attività, posta in essere da persone o da enti di coloro che operano nel campo della sicurezza privata, a tutela di persone, beni e/o enti pubblici o privati [4].
Le vigilanze private sono aziende che si occupano della protezione di persone e di beni mobili ed immobili, esse derivano direttamente dalle milizie cittadine del medioevo che, in tempo di pace svolgevano il compito di controllare e garantire la sicurezza dei cittadini durante la notte, nelle fiere e nei mercati. Oggi le vigilanze private si occupano di diversi aspetti della sicurezza tramite l'utilizzo di tecnologie all'avanguardia. Tra queste attività troviamo:

Piantonamento: questo tipo di attività consiste nel presidio fisso da parte di una o più guardie particolari giurate (GPG) dotate di protezione anti proiettile e solitamente armate, esse sono collegate in modo costante con una centrale operativa. Solitamente tale attività viene svolta presso istituti di credito e enti pubblici. Possiamo distinguere tra piantonamenti diurni, piantonamenti notturni o piantonamenti per brevi periodi. Tale attività viene svolta in quei luoghi nei quali esiste un pericolo costante.

Servizio ispettivo: questa attività consiste nell'ispezione saltuaria di alcune zone come piccole imprese, locali e aree circoscritte. Solto principalmente durante le ore notturne consiste in una visita della zona e nell'esame degli ingressi, degli infissi e del perimetro. Se la GPG durante l'ispezione nota delle anomalie provvede a contattare la centrale operativa che effettuerà gli opportuni controlli ed ad avvisare eventualmente le forze dell'ordine.

Trasporto valori: in questo caso si tratta di un servizio di scorta effettuato da personale armato e dotato di protezioni antiproiettile ed effettuato tramite l'ausilio di mezzi blindati.

Sala conta: questa attività è destinata soprattutto agli istituti di credito e ai centri commerciali. Il denaro viene prelevato dalla sede del cliente e prima di essere custodito nel *caveau* dell'istituto di vigilanza vine ricontato trattato e confezionato secondo precise istruzioni.

Localizzazione satellitare: tramite il sistema GPS è possibile localizzare a distanza un mezzo, inoltre è possibile effettuare alcune operazioni per gestire il mezzo in tempo reale. Tale servizio è rivolto soprattutto ai possessori di auto di valore, ad aziende di trasporto, ai mezzi blindati, e a chiunque abbia necessità di tenere sotto controllo la propria flotta di veicoli. Tale servizio è possibile grazie ad un apparecchio dotato di ricevitore GPS e di un interfaccia GSM o UMTS per la comunicazione dei dati.

Teleallarme: questo servizio consiste nell'installazione di un sistema antintrusione in abbinata ad un sistema di teleallarme dove è necessario, collegati alla centrale operativa in modo da ricevere le eventuali segnalazioni di allarme e gestirle di conseguenza.

Telesoccorso: molto simile al teleallarme ma questa volta la periferica invia le segnalazioni di allarme alla centrale solo nel caso in cui la persona prema un pulsante di allarme e non in modo automatico.

Videosorveglianza: sistema complementare a quello di teleallarme o di telesoccorso avviene tramite l'utilizzo di telecamere collegate con la centrale operativa dell'istituto di vigilanza. Tale meccanismo permette di valutare la reale presenza di eventuali pericoli e di guidare i controlli.

Nella nostra trattazione ci occuperemo solo alcuni di questi servizi in particolare del teleallarme e della videosorveglianza oltre ad alcune funzionalità complementari e di supporto a queste attività.

2.1.1 La vigilanza di LIS

Fondata nel 1982, LIS si contraddistingue nel panorama italiano per l'eccellente qualità dei servizi e prodotti offerti, per l'elevato standard della

Figura 2.1: Foto di una Webu All-In-One

tecnologia usata e per la completezza dell'offerta proposta.[2].
LIS, non si occupa di tutti gli aspetti di vigilanza visti in precedenza, si concentra invece su quegli aspetti che permettono agli operatori LIS di individuare in modo rapido le minacce ed i pericoli ed agire di conseguenza inviando sul posto delle guardie giurate o contattando direttamente le forze dell'ordine nei casi più gravi cercando tuttavia di non contattare inutilmente il cliente.
I servizi di LIS si concentrano perciò principalmente sul teleallarme e telesoccorso affiancati nella maggior parte dei casi da meccanismi di videosorveglianza. Inoltre, LIS non sfrutta i normali ponti radio per la comunicazione con le centrali di sicurezza, ma sfrutta i mezzi di comunicazioni preesistenti nelle sedi da controllare in modo da avere sempre a disposizione più di un canale di comunicazione come ad esempio, linee PSTN e GSM utilizzate una come backup dell'altra; in alcuni casi più critici vengono, inoltre, installate anche periferiche di comunicazione supplementari per trasmettere eventuali guasti della centrale principale.

2.2 Le tecnologie di LIS

LIS sfrutta una serie di tecnologie innovative in tutti i settori del controllo di sicurezza, si parte dall'installazione dell'hardware dal cliente che solitamente comprende una centrale antintrusione di ultima generazione tra cui:

- Tecnoalarm
- UTC Fire & Security
- Bentel

Tutte centrali che permettono la ricezione degli allarmi tramite connessioni ADSL e GPRS, ed inoltre forniscono dei software di telegestione tramite gli stessi canali di comunicazione.
Affiancato alla centrale antintrusione solitamente LIS installa una centrale di backup come ad esempio la *Webu All-In-One* della *Urmet* questa centrale viene utilizzata come backup della centrale di sicurezza avendo alcuni ingressi programmabili, inoltre viene utilizzata come ponte per il vettore PSTN. Infine, dove possibile, viene installato anche un sistema di videosorveglianza che permette un analisi più approfondita della situazione. In particolare, dove il budget lo permette, viene installato un sistema *Dallmeier* che offre meccanismi di compressione delle registrazioni quando queste vengono consultate da remoto[1].

Figura 2.2: Schermata del software E-Pro

Quanto visto fino ad ora è quello che LIS installa dal cliente; vediamo adesso, invece, come LIS riceve e gestisce gli allarmi. In primo luogo, prima del nostro intervento, LIS utilizzava solo i vettori PSTN, GSM e solo per alcuni modelli della *UTC*, il vettore GPRS nonché per le periferiche di backup interne. Per ricevere gli allarmi su questi vettori utilizzavano due sistemi, il primo chiamato *System III* è un sistema di ricezione allarmi su PSTN che permette di ricevere gli allarmi tramite il protocollo Contact-ID o SIA su PSTN e quindi su linea telefonica tradizionale tramite i toni. Il secondo sistema è chiamato Osborne Hoffman LAN che permette, tramite un protocollo proprietario, di ricevere gli allarmi sul canale GPRS per alcuni modelli della *UTC Fire & Security*.
Questi due ricevitori permettono la ricezione degli allarmi, tuttavia, per permettere la gestione di tali allarmi LIS sfrutta un programma proprietario denominato *E-Pro* che permette la gestione degli allarmi presentando l'anagrafica del cliente, il posizionamento del sensore che è andato in allarme, una segnalazione esaustiva della tipologia di allarme ed altre informazioni che possono essere utili all'operatore, il quale una volta preso in carico una segnalazione la gestisce e compila un rapporto di gestione.

2.3 Cosa offre il mercato

Al nostro arrivo in LIS la situazione presente era quella specificata in precedenza e quindi le centrali supportate erano molto poco ed inoltre il vettore di comunicazione principale era il PSTN. Si è quindi deciso di analizzare che cosa offrisse il mercato per valutare se sostituire il software E-Pro o aggiornarlo per renderlo più competitivo rispetto alla concorrenza.
Adesso analizzeremo quali sono i principali prodotti che avrebbero potuto sostituire il software di Lis analizzando in dettaglio i punti a favore e quelli a sfavore della scelta. I software che analizzeremo sono:

- AteArgo di Urmet
- WebSat Enterprise di AMA Software
- Advisor Managment di UTC Fire & Security
- Mastermind e x-View di Enai

2.3.1 AteArgo

AteArgo è un prodotto che ha alle spalle vent'anni di sviluppo da parte di *Urmet*, esso si basa su un sistema Unix/Linux ed è stato il primo software per vigilanze private creato in Italia. Il continuo confronto con il mercato e l'aggiornamento tecnico costante anno permesso di perfezionare sempre più AteArgo e adattarlo alle reali esigenze delle centrali operative degli istituti di vigilanza.
La centrale AteArgo è composta da due server uno principale e uno di backup con allineamento automatico dei dati in maniera trasparente all'operatore. Il software è multi-operatore e multi protocollo e prevede di base la gestione dei teleallarmi radio, PSTN e GSM, inoltre per le centrali Urmet permette anche la ricezione degli allarmi tramite vettori GPRS e TCP/IP. Il software permette di gestire delle periferiche mobili GPS per applicazioni di teleallarme come l'invio della pattuglia più vicina in caso di allarme o la verifica del servizio di ronda. Nell'ultima versione del software è possibile, tramite l'ausilio di periferiche aggiuntive, l'acquisizione video automatica dalle centrale AteArgo a seguito di un evento di allarme. Infine è possibile la gestione di sistemi video navigabili via browser.
Oltre a queste funzionalità il sistema è in grado di eseguire alcune funzioni automatizzate come effettuare chiamate automatiche per particolari segnalazioni effettuare il backup a caldo sia della centrale principale che quella di riserva, invio di segnalazioni direttamente al cliente tramite SMS, gestione automatica di un call-center e di un agenda cliente.
AteArgo fornisce anche la possibilità di rilevazioni statistiche sia in formato elettronico sia via Web. possibilità di creare report personalizzati o l'interazione con altri sistemi di centralizzazione.
Per quanto riguarda la gestione multi operatore ad ogni operatore viene assegnato un profilo specifico in base al suo livello di specializzazione. Per accedere al sistema ogni operatore si identifica tramite login e password con le quali attiva le funzioni a lui destinate.
L'interfaccia utente permette di intervenire all'arrivo di un allarme con il minor numero di azioni. Inoltre vi è un costante monitoraggio del sistema e dei collegamenti periferici.
Oltre a queste funzionalità di base il sistema può essere espanso tramite moduli software aggiuntivi tra cui:

- comunication server: il sistema permette la comunicazione con altri sistemi informativi in modo bidirezionale assumendo la funzionalità di front-end.

- Utente ricaricabile: consente alla vigilanza di gestire clienti di tipo - ricaricabile ovvero con la possibilità da parte del cliente di attivare o disattivare il servizio di vigilanza solamente tramite l'invio di un SMS.

- Verbali: garantisce la rintracciabilità di tutte le azioni della centrale operativa e legate ad un allarme e supporta l'operatore nella gestione degli eventi.
- ArgoSound: permette la gestione di determinate segnalazioni tramite una chiamata vocale automatica.
- Fast call: compone automaticamente un numero dalla lista dei contatti del cliente in allarme evitando errori o perdite di tempo.
- Messaging: permette alla centrale di inviare automaticamente SMS, FAX o E-Mail verso recapiti preimpostati nel caso di particolari eventi.
- Modulo database: relaziona e rende disponibili tutti i dati archiviati e permette di eseguire qualsiasi tipo di ricerca, inoltre permette di interfacciarsi con altri sistemi. Permette la creazione di indici per la stima e la valutazione degli interventi.
- Modulo installatore: questo modulo permette di sollevare l'operatore dal supervisionare una nuova installazione dando la possibilità al tecnico di collegarsi alla centrale mediante portatile o smartphone e verificare la corretta ricezione degli allarmi dell'impianto sul quale sta intervenendo.
- Modulo GPS: permette di ricevere in centrale la posizione in tempo reale del parco pattuglie e di inviare sul sito in allarme la pattuglia più vicina.
- Modulo video: permette alla postazioni operatore di collegarsi a video server e telecamere IP in tempo reale.

2.3.2 WebSat Enterprise

WebSat Enterprase è un software sviluppato da AMA per la gestione di problemi di sicurezza ed emergenza degli ambienti, delle persone e dei veicoli. Esso consente la gestione di diverse tipologie di dispositivi di teleallarme come combinatori telefonici digitali (Contact ID, SIA, Fast Format), combinatori telefonici a sintesi vocale, teleallarmi radio. Inoltre tramite l'ausilio di periferiche AMA è possibile la gestione di teleallarmi via GSM/GPRS o IP, video allarmi, video sorveglianza con telecamere IP ed anche localizzazione satellitari per il controllo delle pattuglie, dei furgoni per il trasporto valori e qualsiasi tipo di veicolo.
Oltre a queste caratteristiche il software *WebSat Enterprise* permette un'interazione automatizzata verso il cliente tramite SMS o chiamate pre-registrate. Gestisce, inoltre, i servizi di pattuglia e di ronda tramite il sistema di localizzazione satellitare. Infine permette la gestione della videosorveglianza.

Per quanto riguarda l'aspetto amministrativo il software permette l'integrazione con i software amministrativi e gestionali già presenti in azienda ed è possibile predisporre un interfacciamento per la ricezione di allarmi provenienti da altri software.
Il software WebSat Enterprise è:

Multifunzionale: in quanto permette all'operatore di gestire tramite un unica interfaccia sia gli allarmi provenienti da periferiche mobili sia da impianti di allarme fissi.

Geo-referenziato: per ogni tipo di allarme sia esso fisso o mobile, vengono messe a disposizione dell'operatore il maggior numero di informazioni possibili.

Gestione delle pattuglie: Tramite la periferica WebSat Patrol la centrale permette di gestire in modo automatizzato le pattuglie in modo da ottimizzare le pattuglie sul territorio.

Report di comunicazione verso i clienti: la centrale è in grado di inviare avvisi di stato di allarme in modo automatico via SMS , invio automatico di report mensili, possibilità da parte del cliente di richiedere report parziali tramite l'invio di SMS.

Interfacciamento automatico con centralino telefonico: WebSat Enterprasie consente l'automazione delle chiamate verso i contatti telefonici del cliente in caso di allarme.

Interfacciamento con altri ricevitori: oltre ai ricevitori di AMA la Websat enterprise è in grado di interfacciarsi con tutti i ricevitori telefonici che implementano i protocolli ADEMCO 685, standard SurGuard, per ricevere gli allarmi in codice Contact ID, SIA level 2 e Ademco high Speed.

Ricezione allarmi da combinatori con sintesi vocale: la centrale di AMA è in grado di ricevere allarmi tramite chiamate effettuate da combinatori telefonici con sintesi vocale, solamente assicurandosi che il numero del chiamante sia in chiaro.

Gestione telecamere Axis: ad ogni sistema di teleallarme è possibile combinare una o più telecamere Axis con connessione diretta via Internet in modo da mettere a disposizione dell'operatore un sistema di videosorveglianza ad un costo contenuto.

Polling GPRS: per quelle periferiche che sono connesse tramite canale GPRS o TCP/IP la centrale è in grado di effettuare un polling ad intervalli molto brevi per verificare l'esistenza in vita della periferica e rilevare in modo tempestivo eventuali problemi di connessione.

2.3.3 Advisor Managment

Advisor Managment è una soluzione di UTC Fire & Security pensata per centralizzare la gestione della sicurezza di uno o più siti facenti riferimento ad un unica centrale di sicurezza. Tuttavia questo prodotto non è pensato specificatamente per le vigilanze bensì per piccoli complessi residenziali o commerciali aventi un unica centrale di monitoraggio.
Questo sistema si concentra sulle caratteristiche necessarie alla gestione della sicurezza in ambienti particolari nel quale accedono dipendenti e lavoratori, nel quale si hanno orari di lavoro flessibili. Solo la gestione integrata di controllo accessi, sicurezza antincendio e videosorveglianza permette ai security manager di avere una visione chiara e completa di tutto il sistema.
L'advisor managment offre un interfaccia intuitiva per la gestione di ambienti differenti, un'unica interfaccia per funzioni multiple, consente la creazione di report e rivolto alla gestione efficiente degli allarmi qualunque essi siano. Per quanto riguarda la videosorveglianza l'advisor managment è in grado di supportare tutti i videoregistratori di rete TrueVison, questa integrazione permette agli operatori di avere accesso sia alle telecamere in tempo reale sia agli eventi registrati consentendo così una verifica immediata degli eventi di allarme.
L'advisor management supporta le centrali antintrusione della linea advisor management e advisor advance questo permette una gestione combinata di sistemi antintrusione e di videosorveglianza, inoltre è possibile configurare aree ad accesso limitato. Nel caso di rilevazione di un allarme, questo viene evidenziato nell'area di competenza e le immagini vengono mostrate in modo automatico all'operatore. Advisor management permette inoltre l'integrazione con le centrali di rilevazioni incendi della serie FP sia per il monitoraggio degli eventi sia per tutto quello che riguarda la gestione dell'impianto. Tutto questo integrato in un unico software permette di intervenire in modo tempestivo in caso di incendio; infatti, in caso di allarme la posizione del sensore viene mostrata dinamicamente e viene attivato il flusso video in tempo reale per verificare la presenza dell'incendio. Inoltre, grazie al sistema di controllo accessi è possibile sbloccare tutte le porte in modo automatico, e gli ascensori portati a terra.

2.3.4 Mastermind e X-View

Mastermind è uno dei prodotti più utilizzati dalle maggiori industrie di sicurezza principalmente in US ma ultimamente anche nel resto del mondo sia nel settore privato che in quello pubblico. Questa diffusione è dovuta alla grande sicurezza e affidabilità del sistema unita alla possibilità di gestire sistemi su larga scala. I punti di forza di mastermind sono la possibilità di lavorare sia con ambienti di piccola scala sia con ambienti più grandi. Possibilità di configurazione multi sito con ridondanza a caldo. Integrazione

di molti sistemi in un unica interfaccia di sistema.
Mastermind è un sistema ad architettura aperta per fare in modo che i compratori possano adattare le loro tecnologie al sistema; esso permette la comunicazione tramite rete locale LAN e mette a disposizione degli SDKs per supportare al meglio lo sviluppo da parte di venditori di terze parti. come vendor di videosorveglianza.
Il sistema si suddivide in due parti slegate, una parte tratta il monitoring degli allarmi, l'altra parte, denominata *business suite* si occupa del contatto e della gestione del cliente. Tutte queste funzioni sono supportate da una serie di applicazioni che permettono una gestione ottimale del sistema come il MASVideo che permette di registrare sui server le immagini associate ad un allarme o il MASWeb utilizzato per consentire un accesso remoto alla reportistica a clienti con particolari esigenze. Oppure X-View un software affiancato a MasterMind che permette all'operatore di costruire la propria interfaccia personale e mette a disposizione maggiori informazioni come la localizzazione GPS o la piantina dell'edificio.
A differenza degli altri prodotti analizzati mastermind risponde alle esigenze impostate dal cliente tramite l'utilizzo di workflows che gestiscono tutti gli eventi in modo tale da guidare l'operatore lungo una sequenza predefinita di operazioni. Inoltre questo meccanismo permette di gestire in modo automatico le operazioni più semplici e che non richiedono la necessità dell'interazione con l'operatore.
La parte di *business suite* comprende tre sotto sezioni, la prima per definire le promozioni ed i prezzi da applicare ai clienti e organizza gli appuntamenti per le vendite. La seconda parte si occupa della relazione col cliente contenendo i dati del contratto la fatturazione dei servizi e il controllo dei pagamenti. l'ultima parte invece si occupa dell'organizzazione dell'installazione e dell'attivazione del servizio, si può occupare della gestione del magazzino mantenendo un inventario aggiornato. Le funzionalità di Mastermind sono:

VRT/IVR ovvero la possibilità di sfruttare un centralino automatico che risponde alle richieste più comuni dei clienti senza tenere occupato inutilmente un operatore di centrale, inoltre questa funzionalità può essere sfruttata per creare chiamate automatizzate verso il cliente nel caso di allarmi specifici.

Voice Recorder Integration: tutte le chiamate in entrata ed in uscita possono essere registrate e immagazzinate per un successivo controllo sia da parte del cliente che da parte della vigilanza nel caso in cui sia necessaria una verifica.

Report Server: questa funzionalità permette l'invio di email o messaggi periodici con il riassunto degli allarmi e degli interventi.

MASWeb: questa funzionalità permette ai clienti e ai tecnici di accedere alle loro informazioni per generare report o modificare i dati. Le pagine

web sono strutturate per includere i servizi di monitor e reportistica, l'elenco dei servizi e le informazioni di fatturazione. I tecnici possono modificare uno stato dell'impianto e inserirlo in modalità test per ricevere sul proprio browser o sull'app l'esito dei test effettuati durante una manutenzione o installazione.

MASmobile: questa app permette di controllare lo stato del sistema effettuare controllare lo storico eventi, agli installatori permette di mettere il sistema in modalità test per ricevere gli esiti.

Controllo accessi: è possibile integrare la ricezione degli allarmi con sistemi di controllo accessi

Capitolo 3

Obiettivi della tesi

L'obiettivo di questa tesi è quello di illustrare le modifiche, le aggiunte ed i cambiamenti effettuati al software di LIS per permettere un integrazione dei ricevitori di allarme in maniera più veloce e standard, una seconda parte della tesi complementare alla prima si focalizza invece sulla telegestione del delle centrali di allarme. Marginalmente tratteremo la videosorveglianza ed altri aspetti più pratici che riguardano la gestione di un allarme.

3.1 La situazione iniziale

Al nostro arrivo in LIS la situazione che si presentava era poco chiara e non ben definita. Gli operatori di centrale che gestivano gli allarmi utilizzavano un software denominato *E-Pro*. Questo programma è un adattamento di un programma utilizzato da Cobra SPA per la gestione degli allarmi provenienti da veicoli ed è stato adattato negli anni alla gestione degli impianti fissi.
Questo software è un formato da un insieme di moduli alcuni scritti in C ed altri in Java, la parte che riguarda la ricezione degli allarmi il loro immagazzinamento nel database e la logica che gestisce il comportamento da intraprendere per la loro gestione è implementato in una serie di moduli scritti in C; questi moduli sono chiamati:

- cp220_3
- cp220_4
- MTSfe_fissi

Questi tre moduli si occupano della ricezione degli allarmi dai vettori PSTN e GPRS/GSM per fare questo utilizzano dei ricevitori fisici chiamati

System III: si occupa della ricezione degli allarmi sul vettore PSTN tramite protocollo Contact ID.

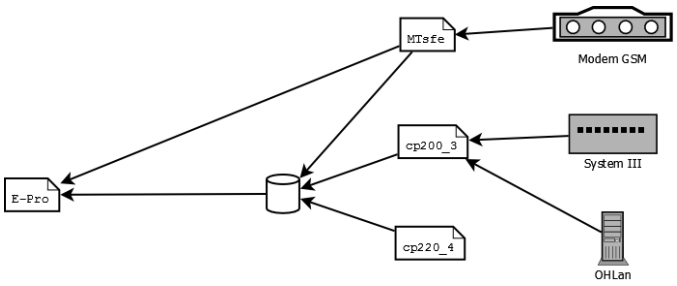

Figura 3.1: Schema dei moduli applicativi di LIS

OHLan: questo ricevitore è un PC fisico collegato in LAN sul quale è installato un software della UTC Fire & Security che si occupa della ricezione tramite protocollo proprietario degli allarmi provenienti dalle centrali UTC.

Modem GSM: più di un modem GSM è collegato ad una porta multiseriale connessa nella rete locale questi modem permettono la ricezione degli allarmi tramite vettore GSM e GPRS.

Per quanto riguarda la parte Java essa si occupa dell'interazione con l'operatore e quindi il compito di questi moduli è quello di prelevare gli allarmi dal database e mostrarli all'operatore, inoltre, questi moduli si occupano di tenere traccia di tutte le azioni eseguite dall'operatore. Infine, questa parte è strutturata in modo da garantire la multiutenza, infatti, questi moduli sono scritti in Java EE e sono eseguiti su di un server JBoss in modo da permettere l'esecuzione di più sessioni contemporaneamente.

3.1.1 cp220_3

Il *cp220_3* ha la funzione di leggere e trasformare gli allarmi provenienti dai sistemi di ricezione come il *System III* o lo *OHLan* e di immagazzinarli in un database non prima di averli trasformati in un formato interpretabile dall'E-Pro. questo formato è derivato direttamente dal Contact ID il prevedere diversi campi

```
ACCT MT QXYZ GG CCC S
```

dove i diversi campi indicano:

ACCT: è un identificativo assegnato al cliente

MT: è un numero che indica il tipo di messaggio, se esso è nuovo oppure una ritrasmissione.

XYZ: è un codice che indica il tipo di evento che è avvenuto

Q: un numero che può essere 1 o 3 ed indica se l'evento trasmesso è rispettivamente iniziato o finito.

GG: è il numero che identifica la partizione nella quale è stato generato l'allarme

CCC: è un numero che identifica il sensore o zona che ha generato l'allarme.

S: valore di checksum per il controllo degli errori

Il `cp220_3` utilizza i campi ACCT, XYZ, Q, GG, CCC insieme al timestamp nel quale arriva il messagio e li inserisce in una tabella del database dal quale poi saranno prelevati ed inviati all'operatore.
Oltre a questa funzione il modulo all'arrivo di ogni messaggio aggiorna un campo in una tabella chiamata *Ricevitori* per controllare periodicamente lo stato in vita dei ricevitori e la loro connessione con il modulo in questione.
Questo modulo è il più interessante per noi in quanto è quello che permette la ricezione degli allarmi e quindi sarà oggetto di una più approfondita analisi.

3.1.2 cp220_4

Questo modulo si occupa della logica della gestione degli allarmi per capire meglio il funzionamento di questo modulo facciamo un esempio e consideriamo un locale commerciale con prefissati orari di apertura e di chiusura. Il sistema di allarme viene disinserito poco prima dell'apertura, in questo caso alla centrale arriva l'evento di disinserimento dell'impianto ma il cp220_4 controlla l'orario di arrivo di tale evento e calcola che questa segnalazione è conforme all'orario di apertura e quindi lo registra ma non lo inoltra agli operatori di centrale. Nel caso in cui, invece, tale evento di disinserimento si verifica durante le ore notturne, e quindi fuori dal normale orario di apertura allora il software verifica l'anomalia e invia la segnalazione all'operatore che provvederà a gestirla.
Il `cp220_4` si occupa di capire quali segnalazioni inviare all'operatore. Oltre al controllo orario visto in precedenza, si occupa di filtrare le segnalazioni multiple provenienti ad esempio da ritrasmissioni, di filtrare gli impianti in test o disattivati che comunque inviano segnalazioni alla centrale.

3.1.3 MTSfe

Lo `MTSfe` è un software che deriva da *Cobra Italia* e si occupa principalmente della gestione delle periferiche di backup di derivazione automotive ovvero delle periferiche *PowerSat*. Queste periferiche erano state pensate per il controllo di autoveicoli e sono state adattate all'utilizzo negli impianti fissi come periferiche di backup in quanto sono dotate di una decina di ingressi programmabili e di alcune contatti di uscita.
Questo modulo pur essendo rimasto parte integrante del software di LIS è

ancora di proprietà di Cobra Italia è perciò stato impossibile per noi modificarlo, tuttavia uno dei nostri obiettivi a lungo termine era quello di sostituire le vecchie periferiche di backup PowerSat con altre più preformanti e aperte così da poter essere gestite direttamente dal nuovo software.

3.1.4 E-Pro

E-Pro è il software centrale che gestisce l'interazione tra operatore e sistema. Mentre i moduli in C si occupano di ricevere e selezionare gli allarmi il software E-Pro si preoccupa di prelevarli dal database e mostrarli all'operatore per poi aiutarlo nella gestione e controllo della segnalazione.
Questo software è composto da una serie di moduli JAVA EE che vengono eseguiti in un ambiente JBoss. Questi moduli hanno compiti diversi e svolgono le seguenti funzionalità:

- Chiedere in lis quando vai

3.2 Obiettivi della tesi

Gli obiettivi di questa tesi sono diversi e intervengono su diversi aspetti del software preesistente ma tutti questi obiettivi si prefiggono lo scopo principale di strutturare il software in maniera adeguata per permettere l'estensione delle funzionalità in modo rapido e strutturato permettendo così in futuro di non dover ripensare e riscrivere il software per integrare nuovi protocolli o aggiungere nuove funzionalità al software.

3.2.1 Integrazione di nuovi protocolli in minor tempo

Il primo degli obiettivi che vogliamo analizzare è quello dell'integrazione dei nuovi protocolli. Per prima cosa dobbiamo fare una piccola distinzione in due casi il primo caso si ha quando le segnalazioni di allarme arrivano da un ricevitore esterno come avveniva in precedenza con il System III in questo caso il protocollo da integrare è quello del ricevitore che si interpone tra la centrale di allarme ed il software di ricezione. Il secondo caso si ha quando la centrale d'allarme comunica direttamente con il software di ricezione. I due casi se pur distinti sono simili in quanto si può trattare il ricevitore esterno come una centrale d'allarme che comunica gli eventi con identificativi diversi.
Per fare ciò si è pensato di sostituire o comunque affiancare al cp200_3 un nuovo modulo che memorizza gli allarmi sulla base di dati nello stesso modo del cp200_3 per mantenere la retrocompatibilità del software. Questa soluzione è stata una scelta obbligata per non dover riscrivere interamente il software tuttavia, come vedremo nella sezione successiva, non è stata una scelta ottimale.

3.2.2 Strutturazione del software

Il secondo obiettivo che ci siamo prefissati è stato quello di dare al software una struttura più solida e modulare in modo da non dover riprogettare il software in futuro con la richiesta di nuove funzionalità come è stato necessario fare per l'integrazione che abbiamo dovuto fare noi. Per fare ciò si è deciso di strutturare anche la parte C in un software ad oggetti con conseguente passaggio obbligato al linguaggio C++. La scelta del linguaggio C++ rispetto al Java è stata una scelta puramente pratica in quanto le nostre conoscenze erano più sbilanciate verso questo linguaggio inoltre, la gestione delle periferiche seriali è più semplice utilizzando tale linguaggio.

3.2.3 Telegestione

Una funzione completamente nuova richiesta dalla centrale operativa era quella di poter telegestire le diverse centrali direttamente dal software E-Pro. Per fare ciò è stato necessario innanzitutto capire quali erano le funzioni necessarie per una corretta telegestione da parte dell'operatore. In secondo luogo è stato necessario capire quali centrali fossero in grado di permettere tali funzionalità e su quale vettore di comunicazione erano disponibili. Infine a livello pratico è stato necessario capire in quale modo implementare tali funzioni.
Obiettivi secondari alla telegestione sono stati la minimizzazione dei tempi di reazione del software e lo studio di una nuova interfaccia grafica per esprimere in modo immediato le nuove informazioni messe a disposizione dell'operatore.

3.2.4 Utilizzo di nuovi vettori di comunicazione

Gli obiettivi di rinnovamento del software non potevano limitarsi solamente ad un nuovo software ma, soprattutto, erano legati in modo indissolubile dall'utilizzo di nuovi vettori di comunicazione in particolare TCP/IP, GPRS ed SMS per minimizzare i costi di comunicazione e diminuire i tempi di dialogo tra la centrale di allarme e la centrale operativa.
L'utilizzo di questi vettori ha comportato lo studio di protocolli specifici come il Contact-ID o il SIA over IP e l'utilizzo e quindi l'interfacciamento del software con nuovo hardware come i modem GPRS.

3.3 Problematiche legate al software preesistente

Con il nostro arrivo sono state introdotte numerose modifiche al software preesistente tuttavia per mantenere l'operatività e l'usabilità durante tutto lo sviluppo è stato necessario effettuare alcune scelte che permettessero la retrocompatibilità e la normale esecuzione del software preesistente. In parti-

colare è stato necessario mantenere il meccanismo nel quale il cp220_3 memorizzava gli allarmi nel database per diverse ragioni. Questo memorizzazione consisteva nell'inserimento in tabella di un nuovo record così composto:

Ora ricezione:

Ora allarme:

Codice centrale:

Codice allarme:

Numero partizione:

Numero zona:

Gestito:

Il primo problema che si presenta anche se di facile soluzione si ha quando la segnalazione di allarme non porta con se l'ora della segnalazione, questo problema si risolve impostando l'ora della ricezione come ora in cui è avvenuta la segnalazione, tuttavia questo tipo di informazione è superflua in quanto non viene utilizzata in nessuna altra parte del software.
Il secondo problema più complesso consiste nel codice di allarme, esso è simile al Contact ID tuttavia mentre il Contact ID ha una struttura `QXYZ` dove Q è uno tra i numeri 1, 3 o 5 che indicano rispettivamente il nuovo evento, il termine di un evento e la continuazione di una segnalazione mentre XYZ è un codice identificativo del tipo di evento. I problemi che si presentano sono di tre tipi il primo puramente di forma consiste nel fatto che il codice di allarme veniva memorizzato nella forma `XYZQ` e questo comporta delle elaborazioni aggiuntive prima di memorizzare il dato. Inoltre il codice Contact ID non è univoco e quindi per centrali differenti avremmo significati differenti questo, in precedenza era stato risolto con una tabella nel database che associava ad un determinato tipo di centrale le corrispondenti etichette con il significato del codice. Questo meccanismo è rimasto invariato tuttavia questo comporta che ad ogni integrazione è necessario aggiungere centinaia di record a questa tabella per poter permettere la conversione. Un altro problema riscontrato è stato il fatto che non tutte le tabelle comunicano tramite protocollo Contact Id e questo ha comportato l'introduzione di una tabella di traduzione per convertire i codici provenienti da altri protocolli in codici Contact Id.
Un problema che abbiamo riscontrato sempre riguardante i codici Contact Id riguardava il valore del campo `Q` in quanto questo campo è utilizzato dal cp220_4 per effettuare il controllo orario di un impianto i codici 1401 e 3401 indicano rispettivamente l'inserimento ed il disinserimento da parte dell'utente dell'impianto, il cp220_4 sfrutta questi due codici per verificare

che tali eventi avvengano nelle fascie orarie prestabilite. Questo meccanismo funzionava correttamente per le centrali già integrate in quanto esse rispettavano questi codici per indicare gli inserimenti e i disinserimenti, tuttavia, per alcune centrali integrate durante il nostro percorso ci è capitato di trovare centrali che invertivano i due codici e questo ci ha obbligati ad utilizzare la tabella di traduzione per mantenere un comportamento corretto del software.
Il principale problema riscontrato tuttavia nell'utilizzo del codice precedente è stato proprio la comprensione del suddetto codice sorgente mal commentato, con refusi di vecchie funzioni provenienti da versioni precedenti e soprattutto la mancanza di una struttura logica del programma, basti pensare che il cp220_3 e il cp220_4 sono due programmi che svolgono due funzioni completamente distinte ma che in realtà provengono dallo stesso codice sorgente compilato con parametri differenti. Per ovviare a questo problema abbiamo innanzitutto introdotto il codice in un sistema di controllo versione, eliminato oltre diecimila righe di codice inutilizzato e commentato ogni singola funzione tramite un sistema di generazione della documentazione automatica. Questo ci ha permesso di comprendere le funzionalità del software anche se in alcuni casi non è servito a capirne il reale funzionamento o la logica con la quale è stato programmato; questo non ha causato grosse difficoltà ma potrebbe crearne quando si cercherà di sostituire il cp220_4 con un nuovo modulo meglio strutturato.

Capitolo 4

Ricevitori 2.0

In questo capitolo tratteremo la progettazzione e la realizzazione del nuovo ricevitore per la ricezione degli allarmi tramite vettori TCP/IP sfruttando sia le normali linee ADSL e GPRS.

4.1 Nuovi vettori di comunicazione: dal PSTN al TCP/IP

Con la diffusione della fibra ottica e delle comunicazione VoIP sono sempre meno le tradizionali linee PSTN che permettono la comunicazione di messaggi tramite i toni. Si è deciso perciò di passare alla comunicazione TCP/IP per comunicare gli eventi di allarme. Questo tipo di comunicazione permette di utilizzare sia connessioni ADSL che connessioni GPRS senza dover modificare nulla per quanto riguarda i protocolli di trasmissione.
Per poter utilizzare questa tipo di vettori di comunicazione sono stati adattati due protocolli standard utilizzati normalmente nella comunicazione PSTN per essere trasmetti su canali TCP/IP, questi due protocolli sono:

- Contact-ID over IP
- SIA over IP

Per l'analisi e lo studio del protocollo si è fatto riferimento a due documenti della Security Industry Assocation, questi documenti sono ANSI/SIA DC-09-2007 per la trasmissione di eventi sulla rete internet e AnSI/SIA DC-07-2001 che descrive l'interfaccia di comunicazione.

4.2 I protocolli di comunicazione

I due protocolli di comuncicazione vengo trasmessi nello stesso modo quindi la nostra analisi partirà con la descrizione della struttura del pacchetto per poi descrivere le informazioni trasmette da questo protocollo.

4.2.1 La struttura del pacchetto

Il pacchetto di trasmissione è così formato:

$$\langle LF\rangle\langle CRC\rangle\langle 0LLL\rangle\langle''ID''\rangle\langle Sequence\#\mathbf{!}segment\#|\rangle$$
$$\langle \mathbf{R}reciver\rangle\langle \mathbf{L}line\#\rangle[data]\langle timestamp\rangle\langle CR\rangle$$

Dove i campi indicati sono rispettivamente:

LF: indica il carattere esadecimale `0x0A` e sta ad indicare l'inizio del pacchetto;

CRC: campo utilizzato per il controllo degli errori tramite un meccanismo di Cyclic redundancy Check a 16 bit;

0LLL: campo utilizzato per indicare la lunghezza del pacchetto. Essa è calcolata considerando come primo carattere le virgolette del campo ID e come ultimo il carattere ']';

"ID": il campo ID è una stringa che identifica la tipologia di messaggio contenuta nel campo `data` quelli più importanti per noi sono i tag:

- SIA-DCS,
- ADM-CID.

utilizzati per indicare che il messaggio contenuto nel campo `data` è un messaggio di allarme con la normale codifica SIA oppure Contact-ID;

Sequence#!segment#: questo campo è composto da due sotto-campi il primo, *Sequence* è un numero di quattro cifre obbligatorio e serve ad indicare il numero sequenziale del messaggio inviato, se questo valore è seguito dal carattere "`!`" allora è presente un secondo numero utilizzato soprattutto nel caso in cui il messaggio contenuto nel campo `data` fosse troppo lungo da non poter essere inviato in un solo messaggio;

Rreceiver: questo campo è valore composto da un numero variabile di cifre che precedute dalla lettera `R` che identificano chi sta trasmettendo, in molti casi questo valore conincide con il codice della centrale;

Lline#: campo variabile composto dalla lettera `L` seguita da 1 a 6 cifre ed indica la linea di ricezione;

[...data...]: stringa che contiene le informazioni da trasmettere essa è composta da una parentesi quadrata seguita dal numero identificativo della centrale preceduto dal carattere "#" e seguito dal carattere "`|`", dopo questo carattere è presente la vera informazione del messaggio, il delimitatore di fine stringa è una parentesi quadrata chiusa;

Nome	Id	Descrizione
Tempo di occorrenza	"H"	Timestamp nel quale si è verificato l'evento
MAC Address	"M"	Mac address del dispositivo trasmettitore
Verifica	"V"	Informazioni riguardo ad audio o video associate l'evento
Testo di allarme	"I"	Breve testo che contiene informazioni riguardanti l'allarme o un commento
Nome del sito	"S"	Nome del sito nel quale è avvenuto l'allarme
Nome dell'edificio	"O"	Etichetta che contiene informazioni riguardanti l'edificio che ha generato l'evento.
Luogo	"L"	Indicazione precisa di dove è avvenuto l'evento segnalato
Longitudine	"X"	Longitudine del luogo
Latitudine	"Y"	Latitudine del luogo
Altitudine	"Z"	Altitudine del luogo

Tabella 4.1: Possibili valori iniziali per il campo `xdata`

timestamp: un campo non obbligatorio che indica l'istante in cui il messaggio è stato accodato per l'invio, esso ha la seguente formattazione autoesplicativa

`_HH:MM:SS,MM-DD-YYYY`

CR: è il delimitatore finale del pacchetto e corrisponde al carattere ASCII corrispondente al valore esadecimale `0x0D`

Con lo standard DC09 viene introdotto anche un campo supplementare tra quello `data` ed il `timestamp` questo campo, denominato `xdata` anchesso compreso tra parentesi quadrata estende la potenza di espressione del protocollo. Il campo `xdata` inizia sempre con un carattere ASCII maiuscolo compreso nel range "G" e "Z" il cui significato è mostrato in Tabella4.1

4.2.2 La criptazione del pacchetto

La struttura del pacchetto appena mostrata è utilizzabile così com'è in caso di comunicazione tra una centrale di allarme e un ricevitore in ambiente locale. Tuttavia quando le informazioni devono viaggiare attraverso internet è necessario che le informazioni siano protette in qualche modo. Per fare ciò lo standard DC09 prevede che i pacchetti siano criptati tramite algoritmo di criptazione AES che può utilizzare chiavi a 128, 192 o 256 bits.
Tuttavia non viene criptato l'intero pacchetto ma solamente il campo `data` dello stesso. Per indicare che il pacchetto è criptato si aggiunge il carattere

"*" prima dell'etichetta nel campo ID.
Visto che la criptazione AES richiede che il pacchetto da criptare sia di lunghezza multipla di 16 per rispettare questo vincolo lo standard prevede l'inserimento di un campo `pad` composto da caratteri random tra il carattere "[" e il campo account all'interno del campo `data`.
Secondo lo standard è necessario che il software di ricezione implementi la criptazione tramite una qualsiasi delle tre chiavi, tuttavia nel nostro caso abbiamo implementato solo la criptazione con chiave a 128 bit lasciando ad una futura implementazione le altre due chiavi. Questa supposizione è valida in quanto le centrali di un determinato tipo implementano solamente un tipo di criptazione.

4.2.3 I tipi di pacchetto

Dopo aver visto come sono strutturati i pacchetti di informazione vediamo ora quali informazioni possono essere trasmesse da questi pacchetti. Lo standard prevede una classificazione per le tipologie di pacchetti, in particolare si distinguono tre classi principali:

- Event Messages
- Supervisor Messages
- Acknowledgement Messages

Inoltre lo standard DC07 prevede per uno sviluppo futuro dei messaggi di *data/operation request* pensati per essere inviati dal ricevitore per richiede lo svolgimento di alcune operazioni o lo stato di alcuni componenti.

Event messages

Gli event messages sono quei messaggi inviati dalla ceentrale di sicurezza per comunicare degli eventi al ricevitore. Essi rispettano lo standard appena descritto, il campo `ID` di questo tipo di messaggi può essere uno dei seguenti:

- SIA-DCS
- ADM-CID
- SIA-PUL
- ACR-SF
- ADM-41E
- FBI-SF
- SK-FSK1

tuttavia gli unici tag che noi supporteremo saranno quelli del SIA-DCS e ADM-CID i quali sono anche gli unici obbligatori secondo lo standard.

Supervisor message

Questo tipo di messaggi non sono obbligatori, tuttavia sono molto consigliati, in quanto permettono di monitorare periodicamente lo stato della connessione. Questi messaggi sono inviati periodicamente dalla centrale di allarme al ricevitore, il tempo tra una trasmissione e l'altra può essere impostato secondo lo standard da un minimo di 10 secondi ad un massimo di 1080 ore. Se nessun tipo di messaggio raggiunge il ricevitore in questo intervallo di tempo la comunicazione fallisce e il ricevitore dovrebbe segnalare la mancata comunicazione, inoltre, un evento di mancata comunicazione dovrebbe essere registrato dalla centrale.
Quando il sistema di supervisione è attivo, periodicamente la centrale invia un messaggio strutturato come in precedenza ma con `ID` uguale a *NULL* e campo `data` vuoto. Un esempio di messaggio è il seguente:

$$\langle LF\rangle\langle CRC\rangle\langle 0LLL\rangle\langle''NULL''\rangle\langle 0000\rangle$$
$$\langle \mathbf{R}recv\rangle\langle \mathbf{L}pref\rangle[]\langle timestamp\rangle\langle CR\rangle$$

Acknowledgment message

Quando il ricevitore riceve dalla centrale un evento essp deve rispondere con un messaggio che può essere di quattro tipi:

- ACK
- NAK
- DUH
- RSP

Il messaggio di ACK corrisponde ad una risposta positiva e viene inviato quando il ricevitore riceve correttamente l'evento senza errori, un esempio di messaggio di ACK è il seguente:

$$\langle LF\rangle\langle CRC\rangle\langle 0LLL\rangle\langle''ACK''\rangle\langle seq\rangle$$
$$\langle \mathbf{R}recv\rangle\langle \mathbf{L}pref\rangle[]\langle timestamp\rangle\langle CR\rangle$$

dove i campi `seq`, `recv` e `pref` vengono copiati dal messaggio originale al quale si vuole dare una risposta.
Il messaggio di NAK è simile a quello di ACK tuttavia cambia il campo `ID` e il numero di `seq` che viene impostato a 0000, un esempio è riportato di seguito.

$$\langle LF\rangle\langle CRC\rangle\langle 0LLL\rangle\langle''NAK''\rangle\langle 0000\rangle$$
$$\langle \mathbf{R}recv\rangle\langle \mathbf{L}pref\rangle[]\langle timestamp\rangle\langle CR\rangle$$

Il pacchetto DUH viene inviato nel caso in cui il ricevitore, pur avendo verificato che il pacchetto è formattato correttamente e non contiene errori,

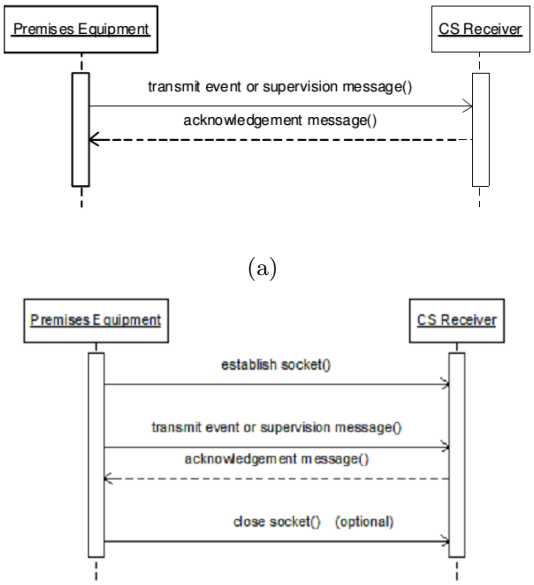

Figura 4.1: Esempio di trasmissione UDP 4.1(a) e TCP 4.1(b)

non è in grado di tradurlo o comunque di interpretare la richiesta. In questo caso i campi `seq`, `recv` e `pref` sono uguali a quelli della richiesta ricevuta. Il pacchetto RSP è stato introdotto come pacchetto di risposta per i messaggi di data/operation request tuttavia come questi pacchetti è pensato per un uso futuro. A differenza dei pacchetti precedenti il campo `data` contiene dei valori. Il numero di sequenza, del ricevitore e della linea sono copiati dal pacchetto di richiesta.

4.2.4 La connessione

Lo standard DC09 prevede che la connessione tra il ricevitore e la centrale possa avvenire sia tramite l'utilizzo dello *User Data Protocol* (UDP) sia tramite l'utilizzo del *Transmission Control Protol* (TCP), il ricevitore da noi implementato permette attualmente solo l'utilizzo della modalità TCP, in quanto la modalità UDP è meno diffusa ed implementata tramite hardware con una scheda di espansione per il ricevitore System III.
Da notare il fatto che per la trasmissione tramite UDP nell'header del messaggio è necessario introdurre la porta della centrale d'allarme sulla quale il ricevitore dovrà inviare la risposta al messaggio. In Figura4.1 vediamo la sequenza di messaggi che avviene durante la trasmissione di un evento.

4.3 La struttura dati

Come abbiamo detto nel Capitolo3 uno dei nostri obiettivi è quello di mantenere la retrocompatibilità con il vecchio software di Lis fino al completo aggiornamento dei moduli. Per fare ciò è stato necessario mantenere la struttura dati precedente per far si che il resto del software potesse prelevare i dati senza nessuna complicazione. In particolare la tabella più importante per la ricezione degli eventi era quella `allarmi_contact_id` i cui campi si ricavano dallo script di creazione del Listato 4.1

```
1  CREATE TABLE allarmi_contact_id
2  (
3          ac_id integer NOT NULL DEFAULT nextval(('"
               allarmi_contact_id_seq"'::text)::regclass),
4          ac_centrale character varying(20),
5          ac_allarme character varying(10),
6          ac_area bigint,
7          ac_zona bigint,
8          ac_giorno smallint,
9          ac_mese smallint,
10         ac_anno smallint,
11         ac_ora smallint,
12         ac_minuto smallint,
13         ac_secondo smallint,
14         ac_data_inserimento timestamp without time zone DEFAULT now()
               ,
15         ac_pending character(1) DEFAULT 's'::character varying,
16         ac_porta_seriale integer,
17         ac_n_ricevitore smallint,
18         ac_n_gruppo smallint,
19         CONSTRAINT allarmi_contact_id_pkey PRIMARY KEY (ac_id)
20 )
```

Listing 4.1: Tabella allarmi_contact_id

Come si nota i campi da compilare sono diversi anche se non tutti necessari. Il campo allarme contiene il codice Contact ID dell'allarme ricevuto, nel paragrafo successivo vedremo come questo meccanismo sia stato adattato per l'utilizzo anche dei codici di allarme SIA. Il campo `pending` serve al cp200_4 per identificare quali allarmi sono già stati processati in quanto questa tabella mantiene anche lo storico giornaliero degli allarmi ricevuti.
Oltre a questa tabella si è deciso anche di aggiornare una serie di tabelle collegate tra loro che hanno la funzione di monitorare lo stato dei ricevitori. Nel vecchio software per verificare la corretta esecuzione del software, ogni qualvolta che una segnalazione giungeva ad uno dei ricevitori veniva aggiornato un campo nella tabella `seriale` il quale è collegato alla tabella `ricevitori`; questo collegamento è mostrato in Figura4.2. Il codice di creazione di queste tabelle è mostrato nel 4.2.

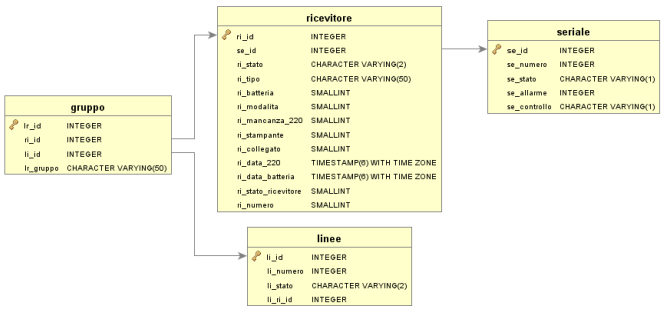

Figura 4.2: Schema relazionale delle tabelle che controllano i ricevitori

```
1  CREATE TABLE seriale
2  (
3          se_id integer NOT NULL DEFAULT   nextval(('"seriale_se_id_seq
               "'::text)::regclass),
4          se_numero integer,
5          se_stato character varying(1) DEFAULT 's'::character varying,
6          se_allarme integer,
7          se_controllo character varying(1),
8          CONSTRAINT pk_seriale PRIMARY KEY (se_id)
9  )
10
11 CREATE TABLE ricevitore
12 (
13         ri_id integer NOT NULL DEFAULT  nextval(('"
               ricevitore_ri_id_seq"'::text)::regclass),
14         se_id integer,
15         ri_stato character varying(2) DEFAULT 'n'::character varying,
16         ri_tipo character varying(50),
17         ri_batteria smallint,
18         ri_modalita smallint,
19         ri_mancanza_220 smallint,
20         ri_stampante smallint,
21         ri_collegato smallint,
22         ri_data_220 timestamp with time zone,
23         ri_data_batteria timestamp with time zone,
24         ri_stato_ricevitore smallint,
25         ri_numero smallint,
26         CONSTRAINT pk_ricevitore PRIMARY KEY (ri_id),
27         CONSTRAINT fk_ricevito_reference_seriale FOREIGN KEY (se_id)
28         REFERENCES seriale (se_id) MATCH SIMPLE
29         ON UPDATE RESTRICT ON DELETE RESTRICT
30 )
```

Listing 4.2: Tabelle ricevitori

Questa meccanismo se pur non necessario per il corretto funzionamento del vecchio software è stato mantenuto, con dei piccoli adattamenti, per monitorare il funzionamento del nuovo software di ricezione. Tuttavia come si nota dalla complessità delle tabelle questo sistema porta con se anche degli elementi caratteristici del passato come l'utilizzo di una tabella `SERIALE` utilizzata dai tempi in cui i ricevitori erano ancora collegati tramite questo tipo di connessione cablata.

4.4 Architettura del sistema

Analizziamo ora come è stato sviluppato il sistema. Si è deciso di passare ad un softwre strutturato per classi. L'idea era quella di avere un controllore che monitorasse periodicamente i diversi ricevitori e nel caso questi non fossero avviati li riavviasse in automatico. I ricevitori dal canto loro dovevano comportarsi tutti pressochè alla stessa maniera ovvero le funzioni principali che dovevano svolgere erano quella di aggiornare il campo `controllo` della tabella seriale e caricare l'allarme sul database rispettando lo standard Contact-ID.

4.5 Implementazione

Inanzitutto si è deciso di sviluppare il software in linguaggio C++ aggiornato allo standard 0x rilasciato nel 2011 per supportare meglio il multi-threading e per fare ciò si è deciso di utilizzare il compilatore gcc-4.8 l'ultimo rilasciato al momento dell'implementazione

Bibliografia

[1] Dallmeier, cur. *PRemote-HD*. 2015. URL: http://www.dallmeier.com/fileadmin/user_upload/upload_dallmeier.com/PDFs/Downloads/Broschures/PRemote-Handout_en.pdf.

[2] LIS s.r.l., cur. *LIS, Chi Siamo*. 2015. URL: http://www.lis-srl.it/chi-siamo.asp.

[3] Wikipedia, cur. *Sicurezza*. 2015. URL: http://it.wikipedia.org/wiki/Sicurezza.

[4] Wikipedia, cur. *Vigilanza Privata*. 2015. URL: http://it.wikipedia.org/wiki/Vigilanza_privata.

Appendice A

Documentazione del progetto logico

Documentazione del progetto logico dove si documenta il progetto logico del sistema e se è il caso si mostra la progettazione in grande del SW e dell'HW. Quest'appendice mostra l'architettura logica implementativa (nella Sezione 4 c'era la descrizione, qui ci vanno gli schemi a blocchi e i diagrammi).