

Network per la comunicazione efficace con la  
popolazione per emergenze di Protezione Civile

Azione 2 - Studio di fattibilità per la realizzazione  
di un sistema di alerting basato sulla tecnologia  
cell broadcasting

*Codice IReR: 2009B057 e 2010B008*

*Project leader: Elvina Degiarde*

**RAPPORTO FINALE**

Milano, giugno 2011

La ricerca è stata affidata ad IReR dalla Direzione Generale Protezione Civile, Polizia Locale e Sicurezza, Regione Lombardia

*Responsabile di progetto:* Elvina Degiarde, Éupolis Lombardia - Istituto Superiore per la ricerca, la statistica e la formazione

*Gruppo di lavoro tecnico:* Alberto Biancardi, Luca Vaghi, responsabili regionali di ricerca, D.G. Protezione Civile - Regione Lombardia; Antonella Belloni, Promozione della cultura di Protezione Civile D.G. Protezione Civile; Domenico De Vita, coordinatore di emergenza e della sala operativa, D.G. Protezione Civile; Paolo Fassi; Chiara Ghidorsi, Francesco Vullo Claudia Zuliani; D.G. Protezione Civile

*Gruppo di ricerca:* Franco Osculati Mox Consulting s.r.l

La l.r. 16/2004 art 1 prevede che la Regione Lombardia concorra alla protezione delle popolazioni e dei territori dagli effetti di pubbliche calamità.

La Direzione Generale Protezione Civile è il centro di competenza regionale che nelle fasi di prevenzione e di emergenza deve garantire un servizio di informazioni per la popolazione.

Nel corso di due anni 2009-2010 è stata svolta un'attività di ricerca per definire soluzioni utili per divulgare attraverso vari canali messaggi diretti alla popolazione, nonché definire le modalità tecnologiche utili al servizio.

La ricerca è stata articolata in tre differenti azioni, ciascuna con una metodologia specifica e cioè:

Azione 1) Network per la comunicazione/informazione: definizione delle procedure per la comunicazione, l'individuazione dei canali più idonei in funzione delle diverse tipologie di media e lo studio dei relativi linguaggi comunicativi per le diverse categorie di utenza, relativamente alla popolazione presente sul territorio lombardo.

Azione 2) Studio di fattibilità per la realizzazione di un sistema di alerting basato sulla tecnologia cell broadcasting: individuare le potenzialità di un sistema di alerting della popolazione mediante telefonia mobile, analizzando in dettaglio la possibilità di impiego della tecnologia Cell Broadcasting (sistemi di telecomunicazione di seconda e terza generazione), confrontando casi di successo a livello internazionale, per inquadrare nel modo migliore il contesto tecnologico e applicativo.

Azione 3) Studio ed analisi della normativa vigente in tema di privacy: valutazione delle possibilità di utilizzo di strumenti di comunicazione diretti alla popolazione presente sul territorio regionale tenendo conto delle norme vigenti in materia di privacy.

In queste pagine si presentano i risultati della seconda Azione della ricerca

# Indice

<i>Introduzione</i>	7
 Capitolo 1	
<i>Caratteristiche ed evoluzione della tecnologia mobile</i>	9
1.1. Gli standard di telefonia mobile	9
1.1.1. Le tecnologie di seconda generazione o 2G	9
1.1.2. Le tecnologie di terza generazione o 3G	10
1.2. L'architettura della rete	10
1.2.1. Il Global System for Mobile Communications (GSM)	10
1.2.2. Base Station System	11
1.2.3. Network Sub System	13
1.2.4. Componente amministrativa	14
1.3. GPRS	15
1.4. L'architettura di base EDGE	16
1.5. L'architettura di base HSCSD	17
1.6. UMTS	18
1.6.1. La rete UMTS R99	19
1.6.2. La rete UMTS R4	21
1.6.3. La rete UMTS R5	22
 Capitolo 2	
<i>Il Cell Broadcast</i>	23
2.1. Architettura Cell Broadcast	24
2.2. Il funzionamento del Cell Broadcast	25
2.3. Caratteristiche specifiche	26
2.3.1. Messaggio di Cell Broadcast	26
2.4. Potenzialità di Cell Broadcast	31
2.5. Analisi della copertura di rete	32
2.5.1. Il concetto di copertura	33
2.5.2. I dati disponibili in rete	34
2.5.3. L'analisi della copertura	35
2.5.4. La copertura TIM	35
2.5.5. La copertura Vodafone	36
2.5.6. La copertura Wind	37
2.5.7. La copertura TRE	38
2.5.8. La dislocazione delle BTS	40
2.6. Il terminale mobile	41
2.6.1. Architettura	41
2.6.2. Requisiti del terminale mobile	42
2.6.3. Indagine diffusione terminale mobile	43

2.6.4. Istruzioni di configurazione del Cell Broadcast	45
Capitolo 3	
Casi di studio: introduzione e analisi delle applicazioni	53
3.1. Le applicazioni	54
3.2. Il Giappone	55
3.2.1. La tecnologia di riferimento	55
3.2.2. La realizzazione della rete di alerting	57
3.3. L'Olanda	58
3.3.1. Raggiungibilità	61
3.3.2. Accettazione	63
3.3.3. Tecnologia	64
3.3.4. I contenuti	66
3.4. Gli Stati Uniti d'America	66
3.4.1. La scelta tecnologica	67
3.5. India	69
3.6. Il progetto CHORIST	71
3.6.1. Gli obiettivi di progetto	72
3.6.2. Le attività di progetto	73
Capitolo 4	
Requisiti procedurali della sala operativa	81
4.1. Il funzionamento della sala operativa	81
4.1.1. Lo scenario attuale	82
4.1.2. Situazioni a tendere	87
4.2. La sicurezza	95
4.2.1. La sicurezza informatica	97
4.2.2. La sicurezza operativa	102
Capitolo 5	
Studio interfaccia di comunicazione con Cell Broadcast Centre	105
5.1. Specifiche progetto pilota	106
5.1.1. Comunicazione sala operativa verso CBC operatore: primo scenario ipotizzato	106
5.1.2. Considerazioni sul primo scenario ipotizzato	109
5.2. Specifiche sistema evolutivo	109
5.2.1. Gestione protocollo	110
5.3. Amministrazione del DB	111
5.3.1. Interfaccia PC - CBC	111
5.3.2. Interfaccia CBC - PC	113
5.3.3. Parametri caratterizzanti del messaggio	114
5.4. Realizzazione del progetto pilota: linee guida	114
5.4.1. Formalizzazione messaggi interfaccia PC – CBC	114

5.4.2. Comando di Insert	117
5.4.3. Comando di Cancel	118
5.4.4. Comando di Query	119
5.4.5. Caratteristiche valide per sistema di trial	121
5.4.6. Altri aspetti implementativi e organizzativi	121
Allegato	
<i>Acronimi, glossario e riferimenti</i>	125
<i>Riferimenti e Link utili</i>	129



## *Introduzione*

Negli ultimi decenni la telefonia mobile e la trasmissione di informazioni (multimediali e via Internet) hanno subito uno sviluppo ed una diffusione notevole, diventando i due canali di comunicazione più diffusi tra la popolazione.

I sistemi radiomobili infatti hanno raggiunto livelli di utenza paragonabili, e talvolta superiori, a quelli della telefonia fissa. Internet invece è diventato uno dei mezzi più importanti per raccogliere e distribuire informazioni in tutto il mondo, offrendo servizi sempre più complessi.

Da parecchi anni si sta quindi lavorando allo sviluppo di nuovi sistemi, denominati di “terza generazione” (3G), in grado di conciliare la mobilità dell’utente con la crescente esigenza di comunicazione multimediale. In altri termini si vuole far confluire in un’unica realtà la telefonia mobile e i servizi multimediali.

Le origini della tecnologia di terza generazione risalgono alla metà degli anni Ottanta, quando l’ITU (*International Telecommunication Union*) propose il progetto di un nuovo ed unico sistema radiomobile, chiamato in un primo momento FPLMTS (*Future Public Land Mobile Telecommunication Systems*) e poi rinominato IMT-2000 (*International Mobile Telecommunications - 2000*). Inizialmente ITU definì i requisiti minimi che un generico sistema doveva soddisfare per diventare un candidato per IMT-2000. Sulla base di questi requisiti, i vari enti di standardizzazione proposero diverse soluzioni. In Europa l’ETSI (*European Telecommunications Standard Institute*) progettò il sistema UMTS (*Universal Mobile Telecommunications System*) con l’obiettivo di superare le limitazioni imposte dai sistemi di seconda generazione. Al fine di giungere ad uno standard accettato a livello mondiale, iniziò una stretta interazione tra ETSI ed altri enti di normativa quali ARIB (*Association of Radio Industries and Business*) in Giappone, TTA (*Telecommunications Technology Association*) in Corea e ANSI (*American National Standards Institute*) negli Stati Uniti.

Queste collaborazioni, note con il termine di *Partnership Projects* (PPs), di cui fanno parte esperti di diversi enti di standardizzazione, hanno il compito di garantire la compatibilità dei sistemi. Tra queste si ricorda l’organismo 3GPP (*3rd Generation Partnership Project*) costituito da ETSI, ARIB, CWTS (*China Wireless Telecommunication Standard Group*), TTA e TTC (*Telecommunications Technology Committee*) che ha definito lo standard UMTS.

Attualmente gli standard GSM e UMTS rappresentano le tecnologie più

diffuse per i terminali mobili e lo standard di terza generazione (3GPP) è il riferimento attuale per gli operatori di telefonia mobile. Entrambe le reti GSM e UMTS mettono a disposizione la possibilità di diffondere informazioni, tramite messaggi in modalità uno a molti (broadcast), che possono essere ricevuti da dispositivi mobili opportunamente configurati presenti nella zona in cui il messaggio viene diffuso.

Queste caratteristiche rendono particolarmente interessante la tecnologia mobile per gli scopi di alerting in caso di eventi calamitosi, sfruttando la modalità di funzionamento Cell Broadcast in grado di raggiungere la popolazione in aree oggetto di eventi potenzialmente pericolosi.

La comprensione della tecnologia di seconda e di terza generazione consente di capire quali siano i meccanismi di funzionamento del Cell Broadcast e di meglio definire i requisiti che devono possedere i processi di funzionamento della Centrale Operativa della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza.



## Capitolo 1

### *Caratteristiche ed evoluzione della tecnologia mobile*

Il capitolo analizza sinteticamente gli aspetti tecnologici della telefonia mobile focalizzando l'attenzione sugli argomenti che riguardano il Cell Broadcast dal punto di vista dell'utilizzo necessario alla Direzione Generale Protezione Civile, Polizia Locale e Sicurezza.

#### 1.1. Gli standard di telefonia mobile

Ai fini dello studio per l'applicazione del Cell Broadcast per la Direzione Generale Protezione Civile, Polizia Locale e Sicurezza è importante analizzare sia pur brevemente gli standard tecnologici che realizzano la diffusione di messaggi uno a molti (broadcast) e in particolare gli standard di seconda generazione (2G) che a loro volta costituiscono la base su cui si sono stati sviluppati gli standard e i sistemi di terza generazione (3G).

Gli standard di riferimento e le informazioni di dettaglio sono consultabili sul sito del consorzio 3GPP (<http://www.3gpp.org>).

##### *1.1.1. Le tecnologie di seconda generazione o 2G*

La telefonia cellulare di seconda generazione (2G) è stata introdotta dallo standard GSM in Finlandia nel 1991. Le novità introdotte dalla nuova tecnologia rispetto al precedente standard (TACS) riguarda soprattutto l'introduzione della componente digitale e la possibilità di trasmettere e ricevere pacchetti di dati, in quanto sia il canale di identificazione sia il canale di conversazione sono digitali. Infatti i terminali mobili di seconda generazione consentono di criptare digitalmente la conversazione e di scambiarsi messaggi di testo tra utenti (uno-a-uno) e tra gestore e utenti (uno-a-molti). Caratteristica importante della tecnologia GSM è che per la prima volta è introdotto un sistema di comunicazione uno a molti (broadcast) basato sulla tecnologia Cell Broadcast.

Le tecnologie 2G hanno inoltre permesso agli utenti di accedere ad altri servizi

a costi contenuti sia pure con limitazioni significative quali l'accesso a servizi disponibili via internet.

### *1.1.2. Le tecnologie di terza generazione o 3G*

Gli standard di terza generazione (3G) nascono con l'obiettivo di superare i limiti della telefonia di seconda generazione rendendo disponibile l'accesso a qualsiasi servizio, da qualsiasi luogo da un unico punto cercando di superare i confini tra comunicazione telefonica, informazione e multimedialità.

I servizi abilitati dalle tecnologie 3G aumentano la possibilità di trasferimento di dati non-voce quali download da Internet, navigazione su Internet, mailing e la videochiamata, oltre a rendere disponibili i servizi già presenti con la tecnologia 2G.

La tecnologia di terza generazione più diffusa è l'UMTS compatibile con lo standard 3GPP ed è la tecnologia di trasferimento dati voce e dati non-voce più diffuso in Europa e in Italia.

## 1.2. L'architettura della rete

Gli standard GSM e UMTS utilizzano un'architettura di rete che consente al terminale mobile di comunicare e trasferire informazioni con altre unità mobili o più in generale con altri sistemi.

L'evoluzione degli standard e la disponibilità di nuovi servizi ha comportato l'adattamento continuo della rete e della sua architettura alle nuove esigenze che si è evoluta partendo dall'architettura GSM per poi arricchirsi dei sistemi necessari per la realizzazione dello standard UMTS. Nei paragrafi successivi si analizza l'evoluzione dell'architettura di rete partendo dalla struttura base GSM fino alle più moderne realizzazioni che implementano lo standard UMTS.

Per ogni architettura saranno presi in considerazione i singoli componenti illustrandone la funzione e le modalità operative.

### *1.2.1. Il Global System for Mobile Communications (GSM)*

Lo standard GSM (Global System for Mobile Communications) è lo standard di telefonia mobile più diffuso del mondo. Caratteristica fondamentale del GSM è, come anticipato, che la tecnologia su cui si basa è di tipo "digitale" sia per il canale di identificazione che per il canale voce. Lo standard GSM si basa sulle raccomandazioni CEPT (Conferenza Europea delle amministrazioni delle Poste e delle Telecomunicazioni) che ha costituito l'ETSI (European Telecommunications Standards Institute) che di fatto ha sviluppato lo standard GSM.

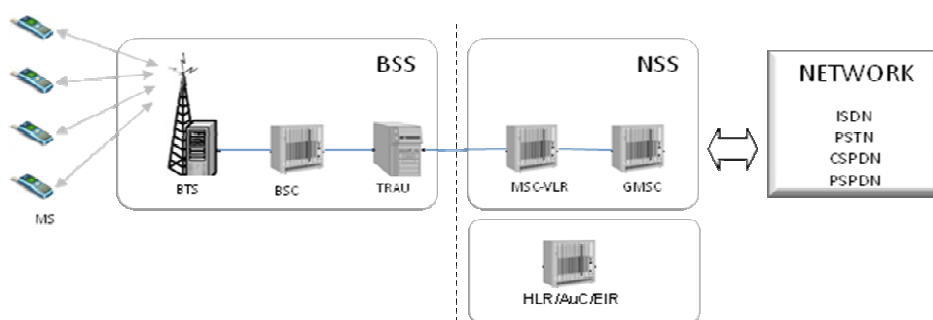
L'ETSI fa parte del consorzio 3GPP (Third Generation Partnership Project) nato

nel dicembre 1988, consorzio tra enti con l'obiettivo di standardizzare sistemi di telecomunicazione in diverse parti del mondo.

Caratteristica peculiare dello standard GSM è la messa a disposizione di una serie di servizi per l'utente a basso costo: tra questi servizi sono da annoverare il servizio SMS oltre lo scambio dati con tecnologia a pacchetto.

La tecnologia su cui si basa il GSM è ad accesso multiplo a ripartizione nel tempo, o TDMA (Time Division Multiple Access) che è una tecnica di multiplexazione numerica dove la condivisione del canale è realizzata mediante ripartizione del tempo di accesso allo stesso. In Figura 1.1 è riportata l'architettura base di un sistema GSM

**Figura 1.1 - Architettura GSM di base**



Ogni componente della rete svolge un compito predefinito nel garantire la connessione tra l'utente e altri sistemi siano essi altri utenti o servizi di altro genere (es. accesso a Internet).

L'architettura è composta sostanzialmente da due macro sistemi:

- BSS (Base station Subsystem) che comprende BTS, BSC e TRAU;
- NSS (Network Subsystem) che comprende MSC-VLR, GMSC e HLR/AuC/EIR

Nei successivi paragrafi è illustrato il funzionamento di ogni singolo sottocomponente.

### *1.2.2. Base Station System*

È la parte di network che si occupa della comunicazione e della gestione del segnale tra il terminale mobile e il network switching subsystem (NSS) e comprende le unità che consentono di fornire la copertura radio di un'area costituita da una o più celle (BTS).

Su questo principio si basa il principio di localizzazione geografica del messaggio di alerting. Infatti la diffusione del messaggio stesso avviene nell'area coperta dalla BTS di ogni microcella cui è stato inviato l'alert. Aree di dimensioni più grandi sono definite combinando l'attivazione contemporanea di più BTS che garantiscono la copertura dell'area interessata alla diffusione del messaggio di

alert.

Ogni Base Station system è composto da tre elementi: il Base Station Controller (BSC), il Base Transceiver Station (BTS) e il Transcoding and Rate Adaptation Unit (TRAU).

Compito principale del BSS è gestire la trascodifica del canale voce, l'allocazione dei canali radio verso il terminale mobile (MS), il paging, la qualità della trasmissione e ricezione sull'air interface

La stazione base di controllo (BSC) governa il funzionamento di uno o più BTS e fornisce la connessione tra un terminale mobile e il centro di commutazione (MSC). In funzione della densità delle BTS sul territorio è possibile che esistano più BTS gestite da un singolo BSC: un caso tipico è rappresentato da una grande area urbana in cui ci sono un gran numero di BTS controllate da una o poche BSC.

I compiti fondamentali del BSC sono quelli di gestire la configurazione e il settaggio dei canali radio (instaurazione e rilascio delle connessioni), il frequency-hopping, gli handover, i parametri di configurazione della rete e i relativi allarmi, fungere da interfaccia tra il BTS e il TRAU, implementare il protocollo di livello 3 del GSM tra cui la gestione della chiamata, gestire e allocare le risorse aeree e terrestri, raccogliere le misure di performance della rete.

La connessione BTS-BSC, che generalmente non sono co-locati, è assicurata da una linea dedicata pulse-code modulation (PCM) a 2,048 Mbit/s che mette a disposizione 32 canali a 64 kbps. Dato che la codifica vocale utilizzata dal GSM è diversa da quella PCM occorre un particolare dispositivo, detto TRAU (Transcoder Rate Adapter Unit), che realizzi un adattamento o trascodifica dalla codifica GSM (13 kbps netti; 16 kbps compresa la ridondanza per la codifica di linea) alla codifica PCM (64 kbps).

La trascodifica può avvenire nel BSC (TRAU installato nel BSC) in modo da far convivere quattro canali di traffico GSM in un canale PCM e quindi sfruttare in modo migliore la connessione BTS-BSC (trascodifica remota); oppure direttamente nella BTS (TRAU installato nella BTS), conveniente solo nel caso di co-locazione BTS-BSC (trascodifica locale).

Il termine BTS identifica l'insieme dei ricetrasmittitori e dei componenti necessari per garantire la copertura territoriale di una cella. Sono deputati alla gestione delle comunicazioni con il terminale mobile e gestiscono le seguenti funzioni:

- Frequency Hopping: tecnica di trasmissione radio usata per aumentare la larghezza di banda di un segnale; consiste nel variare la frequenza di trasmissione a intervalli regolari in modo pseudocasuale attraverso un codice prestabilito.
- Discontinuous transmission (DTX): tecnica utilizzata per spegnere temporaneamente un cellulare quando non si riscontra transito di dati (no voice). Questo sistema ottimizza l'efficienza della comunicazione e preserva la carica della batteria riducendo inoltre casi di interferenza.
- Dynamic Power Control (DPC): sistema che regola la potenza di trasmissione del terminale mobile da parte della stazione radio base, che invia un segnale affinché funzioni con la potenza minima necessaria.

- Antenna Diversity. Per migliorare la qualità del segnale ricevuto spesso si utilizzano due antenne riceventi, poste ad una distanza pari ad un multiplo dispari di un quarto di lunghezza d'onda (a 900 MHz la lunghezza d'onda è di 30 cm). Questa tecnica, nota come Antenna diversity o diversità nello spazio, consente di risolvere i problemi connessi al fading. Le antenne possono essere spaziate verticalmente o orizzontalmente; nel primo caso si ha una maggiore facilità di installazione, mentre nel secondo caso si hanno prestazioni superiori.
- Gestione degli algoritmi di cifratura.
- Encryption - è il processo di creazione delle variabili di autenticazione e di cifratura utilizzando chiavi specifiche e un algoritmo di crittografia.
- Cifratura - processo di conversione da formato testo a dati criptati tramite l'utilizzo di chiavi speciali e un algoritmo di cifratura. La trasmissione tra il terminale mobile e la BTS è criptata.
- Monitoraggio della connessione radio mediante misurazioni sulla qualità dei canali di segnalazione e traffico ed inoltro di queste al BSC affinché le elabori e prenda le necessarie decisioni.

I requisiti fondamentali richiesti ad una BTS sono la regolarità di funzionamento, l'affidabilità, la compatibilità e il minimo costo dato il grande numero di BTS disperse sul territorio, specialmente nelle aree urbane più estese.

Il BTS è l'elemento che copre fisicamente l'area geografica denominata "cella" (o microcella) e rappresenta l'elemento atomico indirizzabile dal punto di vista territoriale come precedentemente descritto. Un messaggio di Cell broadcast viene pertanto diffuso nell'area geografica fisicamente coperta dalla BTS.

Il TRAU è un elemento della componente BSS e ha compito fondamentale di trasformare il segnale codificato GSM in un formato compatibile con la rete fissa quali ISDN, PSTN, ecc.

### *1.2.3. Network Sub System*

Il Network Sub System contiene le componenti necessarie per il controllo della gestione delle comunicazioni tra il BSS e la rete fissa. Il Network Sub System è composta da tre elementi: il Mobile Service Switching Centre (MSC), il Visitor Location Register (VLR) e il Gateway MSC (GMSC).

La MSC è la componente che effettua funzioni analoghe a quelle di un nodo in una rete telefonica pubblica o in una ISDN. Inoltre assolve a tutte le funzionalità di registrazione, autenticazione, handover e il routing di un cliente che ha richiesto un servizio di roaming. La componente MSC agisce anche come un gateway tra reti di telefonia pubblica PSTN o reti ISDN e funge da interfaccia verso il centro messaggi e ha in carico una certa area del territorio, ovvero controlla tutte le BSC dislocate nelle vicinanze e deve servire tutte le terminali mobili presenti nell'area.

La MSC inoltre funge da nodo di una rete telefonica pubblica o in una ISDN e assolve ai compiti necessari ad un utente, registrazione, autenticazione, aggiornamento della localizzazione, handover e il routing di un cliente che ha

richiesto un servizio di roaming. La componente MSC agisce anche come un gateway tra reti di telefonia pubblica PSTN o reti ISDN e funge da interfaccia verso il centro messaggi SMSC, ovvero MSC controlla le BSC in una determinata area geografica servendo le MS che transitano nell'area controllata.

Le funzioni di roaming e la capacità di routing delle chiamate in una rete GSM, sono in carico a due componenti Home Location Register (HLR) e Visitor Location Register (VLR) unitamente alla componente MSC.

HLR è un database che raccoglie le informazioni di tipo amministrativo e la localizzazione corrente del terminale mobile, relative agli utenti della rete GSM. La componente VLR è posta assieme alla componente MSC per ridurre i tempi di accesso alle informazioni richieste durante una chiamata. Il contenuto della VLR è un sottoinsieme di informazioni prelevate dal HLR.

La componente MSC deve scambiare continuamente informazioni con un database, detto Visitor Location Register (VLR), che memorizza, temporaneamente, le informazioni relative ai terminali mobili che si trovano in quell'area (identità dell'utente IMEI, numero telefonico MSISDN, parametri di autenticazione, ecc.). I terminali mobili in questione sono semplicemente "in visita" nell'area servita dal VLR. Esse, infatti, si possono spostare in qualsiasi momento entro l'area servita da un altro VLR.

Il VLR è la componente che insieme all'MSC consente di gestire la mobilità degli utenti. Infatti il VLR memorizza, temporaneamente, le informazioni relative alle terminali mobili che si trovano in quell'area controllata dal MSC (identità dell'utente IMEI, numero telefonico MSISDN, parametri di autenticazione, ecc.).

Il GMSC rappresenta l'interfaccia con la rete pubblica fungendo da trascodifica tra i protocolli utilizzati dalla rete pubblica e dalla rete GSM.

#### *1.2.4. Componente amministrativa*

Questa componente realizza la parte amministrativa della rete ed è composta da tre elementi che sono coesistenti in un unico sottocomponente. I tre elementi sono costituiti dall'Home Location Register (registro di localizzazione abbonati) o HLR, Authentication Center (centro di autenticazione che verifica l'autenticità della carta SIM) o AuC e Equipment Identity Register (registro di identificazione dei telefoni) o EIR.

La HLR è costituita da un database che contiene le informazioni relative ad ogni utente della rete e alla localizzazione del terminale mobile. Per ogni utente sono memorizzate i dati relativi al contratto e i dati sulla localizzazione del terminale mobile, necessari per la contabilizzazione e dell'instradamento delle chiamate verso altri MSC nella cui area si trova il terminale mobile.

L'HLR si occupa principalmente della sicurezza/autenticazione (dialogo con AuC), della gestione della localizzazione, delle informazioni sull'instradamento, della gestione dati utente e costi chiamate, della gestione (attivazione/disattivazione) dei servizi supplementari.

L'EIR contiene una lista dei codici IMEI dei terminali mobili, per gestire l'utilizzo di apparati mobili rubati, difettosi o non omologati. I codici IMEI sono

memorizzati in tre liste differenti: White List (IMEI autorizzati), Grey List (IMEI di apparecchi non omologati), Black List (IMEI bloccati). Un EIR deve contenere almeno una White List.

AuC è costituito da un database in cui sono memorizzate le chiavi primarie utilizzate dalla procedura di identificazione e autenticazione del terminale mobile e di cifratura dei flussi di informazioni radio. Tali chiavi primarie sono usate per generare i parametri temporanei impiegati nelle procedure di sicurezza d'accesso alla SIM.

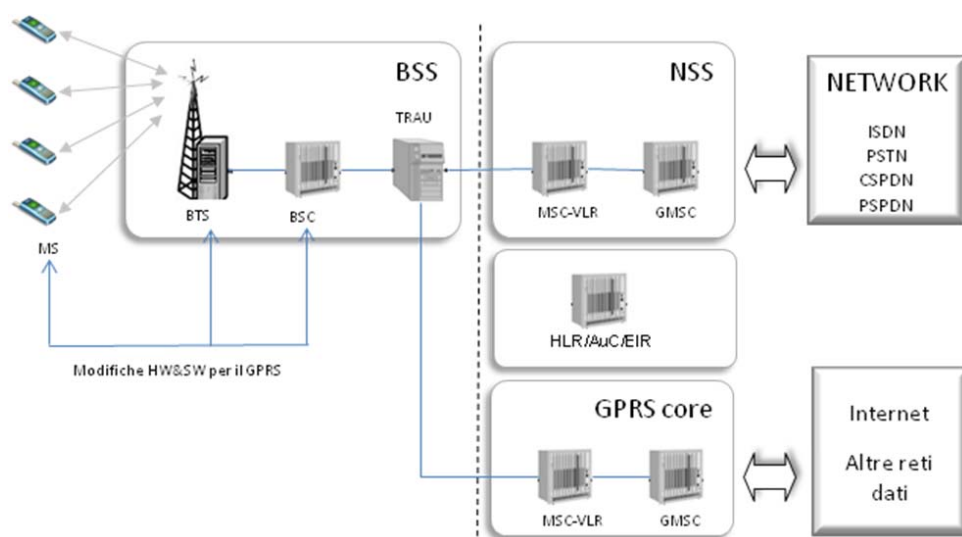
### 1.3. GPRS

Il GPRS (General Packet Radio Service) è una tecnologia di telefonia mobile nata per il trasferimento di dati a media velocità, usando i canali TDMA dello standard GSM. Il funzionamento della tecnologia GPRS è strettamente integrato a quelle del GSM e la definizione delle specifiche è affidata al Comitato 3GPP.

Il GPRS espande le funzionalità dei servizi di scambio dati basati su GSM, fornendo:

- MMS: Multimedia Messaging Service ovvero messaggistica multimediale;
- PTP: Point-to-Point ovvero interconnessione fra reti internet e reti basate su X.25;
- PTM: Point-to-multipoint ovvero chiamate di gruppo (conversazione bidirezionale contemporanea tra più persone) e chiamate multicast (conversazione monodirezionale da uno a molti);
- servizi in modalità anonima: accesso anonimo a determinati servizi.

**Figura 1.2 - Architettura GPRS**



Il Serving GPRS Support Node (SGSN) è responsabile per il delivery dei pacchetti di dati da e per il terminale mobile oltre che provvedere al routing e trasferimento di pacchetti dati, la gestione della mobilità del terminale e l'autenticazione del terminale. Le funzioni più importanti del SGSN sono le seguenti:

- esegue il detunnel dei pacchetti dati GTP (GPRS Tunnelling Protocol) dal GGSN (downlink);
- esegue il Tunnel dei pacchetti IP verso il GGSN (uplink);
- effettua la gestione della mobilità;
- effettua il billing del traffico utente.

Il Gateway GPRS Support Node (GGSN) ha il compito di interfacciare la componente GPRS della stazione con le reti esterne a pacchetto (packet switched networks) quali Internet e reti X.25.

Dal punto di vista di una rete esterna il GGSN si comporta come un router in quanto “nasconde” la struttura GPRS verso la rete esterna.

Il GGSN converte i pacchetti GPRS nell'opportuno formato di protocollo Packet Data Protocol (PDP) (es. protocollo IP o X.25) e viceversa converte il pacchetto dati proveniente dalla rete verso l'indirizzo GSM dell'utente.

## 1.4. L'architettura di base EDGE

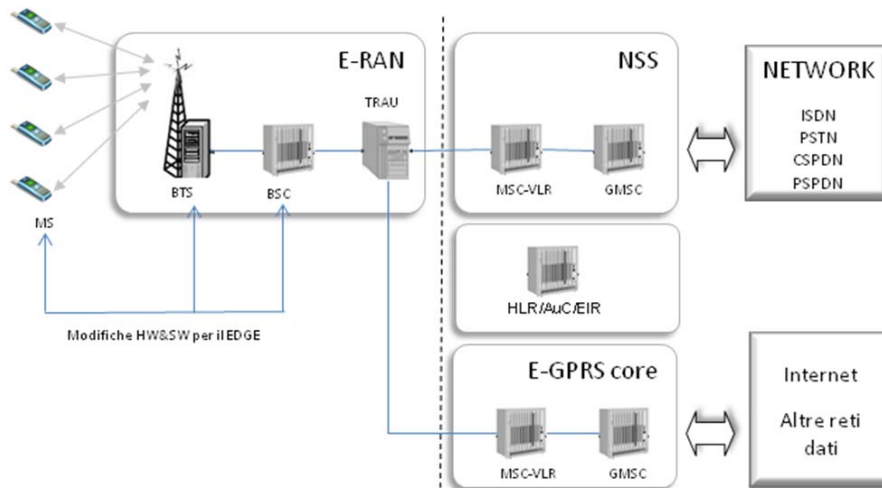
L'EDGE (Enhanced Data rates for GSM Evolution) o EGPRS (*Enhanced GPRS*) (Figura 1.3) costituisce un'evoluzione del GPRS concepita per il trasferimento dati sulla rete GSM con l'obiettivo di aumentare la velocità di trasferimento dei dati. L'EDGE consente di trasferire dati a 200 Kb/sec contro i 40 Kb/sec del GPRS.

È possibile utilizzare la connessione EDGE solamente se il terminale mobile sia compatibile con lo standard. I servizi usufruibili sono rappresentati dalla connessione internet, l'utilizzo del protocollo FTP, la connessione Peer to peer e tramite il protocollo DTM (Dual Transfer Mode) effettuare le videochiamate anche su rete GSM.



## EDGE

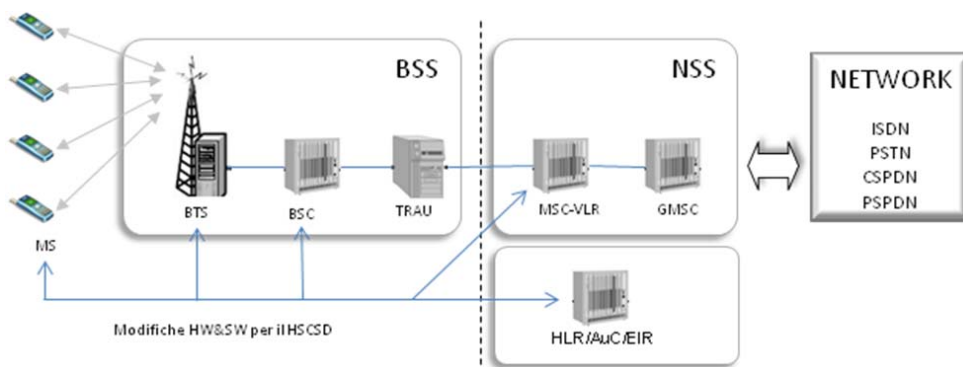
**Figura 1.3 – Architettura**



### 1.5. L'architettura di base HSCSD

HSCSD (High-Speed Circuit-Switched Data) è un'evoluzione del meccanismo originale di trasporto dati reso disponibile dalla tecnologia GSM che aumenta la velocità di trasmissione dei dati consentendo l'introduzione di metodi di correzione degli errori.

**Figura 1.4- Architettura HSCSD**



La tecnologia HSCSD richiede che le partizioni di tempo (slot) siano riservati ad un singolo utente per la trasmissione dei dati: questo comporta che la chiamata vocale (che è configurata sulla rete per avere maggior priorità), può interrompere la trasmissione dati generando ritardi nelle procedure di trasferimento dati.

Inoltre gli slot riservati aumentano il costo del servizio che rende la tecnologia HSCSD meno economica delle tecnologie basate su GPRS.

## 1.6. UMTS

L'UMTS (Universal Mobile Telecommunications System) è la tecnologia di telefonia mobile di terza generazione (3G), che costituisce l'evoluzione della tecnologia GSM di seconda generazione definito dall'ITU (International Telecommunications Union) all'interno dell'IMT2000 e attualmente in corso di standardizzazione da parte dell'ETSI (European Telecommunications Standards Institute).

L'esigenza che si prefigge di soddisfare l'UMTS è quella di aumentare la velocità di trasferimento dati per consentire l'accesso più veloce ai servizi messi a disposizione da Internet. Infatti il sistema UMTS supporta un transfer rate massimo di circa 2 Mb/s (1920 kb/s) oltre i servizi già garantiti dalla rete GSM.

Dal punto di vista architetturale l'UMTS utilizza la tecnologia W-CDMA (Wideband Code Division Multiple Access), sistema di terza generazione evoluzione delle reti 2G (GSM).

Il W-CDMA è un'interfaccia a banda larga e spettro espanso (spread spectrum) basata sulla tecnologia di accesso multiplo a divisione di codice CDMA (direct sequence Code Division Multiple Access); il W-CDMA raggiunge velocità superiori al CDMA e consente di gestire un maggior numero di utenti rispetto alla tecnica di accesso a divisione di tempo TDMA (Time Division Multiple Access) utilizzata dalle reti 2G GSM.

Lo standard ha subito parecchie evoluzioni ed è costituito da differenti versioni (Release, vedi Tabella 1.1): ai fini del presente documento saranno prese in considerazione solamente le Release 99, Release 4 e Release 5.

**Tabella 1.1 - Standardizzazione delle tecnologie di terza generazione**

Versione	Rilascio	Informazioni
<b>Release 98</b>	1998	Queste e le release precedenti specificano le reti pre-3G GSM
<b>Release 99</b>	2000 Q1	Specifica la prima rete UMTS 3G, include interfaccia per CDMA
<b>Release 4</b>	2001 Q2	Originariamente ' <b>Release 2000</b> ' – Introduce diverse novità, incluso interfacciamento verso mondo IP
<b>Release 5</b>	2002 Q1	Introduce IMS e HSDPA
<b>Release 6</b>	2004 Q4	Integra operatività con reti W-LAN, e introduce l'HSUPA, oltre a migliorie all'IMS come il Push to Talk over Cellular (PoC)
<b>Release 7</b>	2007 Q4	Si focalizza su migliorie rispetto alle prestazioni della rete stessa. Include specifiche per HSPA+ (High Speed Packet Access Evolution), migliorie nella gestione delle SIM ed evoluzioni per l'EDGE.
<b>Release 8</b>	In progress, not ready before Mar 2009	Non ancora Pronta: Long Term Evolution. Si occuperà dei sistemi evoluti di quarta Generazione (4G)
<b>Release 9</b>	In progress, expected to be frozen in Dec 2009	Non ancora pronta: Ulteriore evoluzione, che vertirà alla interoperabilità tra sistemi 4G
<b>Release 10</b>	In progress	LTE Advanced

Fonte: <http://en.wikipedia.org/wiki/3GPP>

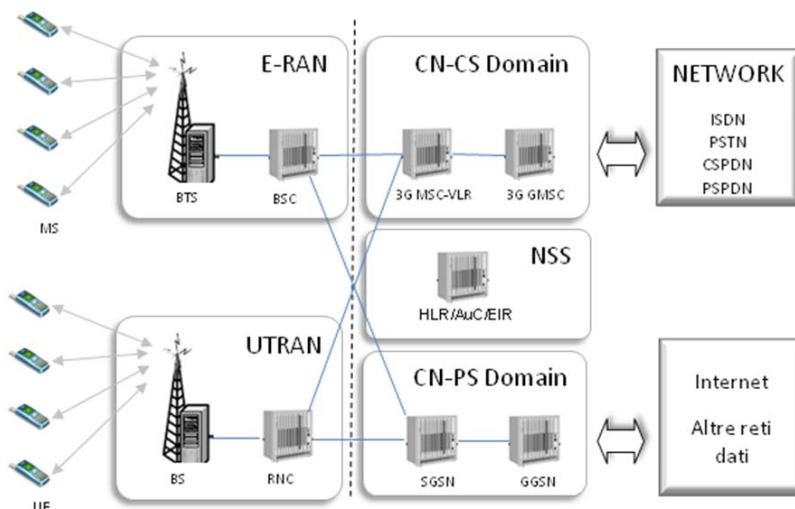
#### 1.6.1. La rete UMTS R99

La rete UMTS è costituita da tre differenti domini che interagiscono tra di loro: UMTS Terrestrial Radio Access Network (UTRAN), Core Network (CN) e User Equipment (UE).

La funzione principale del Core Network (CN) è quello di fornire le funzionalità di switching, routing e transito del traffico utente, ovvero il sistema di accesso alla rete.

Per ottenere la rete UMTS il core network dei sistemi di comunicazione mobile di “seconda generazione” sono state ottimizzate per il trasporto vocale tramite connessione a circuito, mentre UMTS deve essere in grado di fornire anche il trasferimento dati nella modalità a pacchetto. Si sono separati elementi della rete che si occupano della gestione delle risorse radio da quelli che regolano il flusso dati all’interno della rete fissa. In questo modo si è in grado di passare dai vecchi sistemi (gsm, gprs) a quelli nuovi di “terza generazione”, riutilizzando il sistema di rete con diverse tecnologie di accesso (Figura 1.5). In questo senso la componente BSS si è trasformata in E-ran (edge Radio Access Network) modificando il funzionamento per supportare il protocollo wcdma.

**Figura 1.5 - Architettura rete UMTS R99**



Il funzionamento dei sottocomponenti BTS, BSC, MSC-VLR e GMSC rimane sostanzialmente invariato.

L'architettura UMTS ha introdotto la componente UTRAN che è composta da una o più Base station (BS) che svolge verso lo User Equipment (UE) la funzione svolta dalla BTS verso il MS.

#### *1.6.1.1. UTRAN*

Con UMTS Terrestrial Radio Access Network (UTRAN) si intende la parte che implementa l'accesso alla rete core da parte dei terminali UMTS. E' composto dalla Base Station (BS), altrimenti noto come NodeB o Base Station, e il Radio Network Controller (RNC) che ha il compito di gestire una o più BS con le stesse modalità presenti nella rete GSM.

Il componente UTRAN è collocato tra l'interfaccia con il terminale mobile (BTS) e i componenti per la gestione dei dati a pacchetto. Il suo compito principale è quello di svolgere il collegamento tra la parte radio e la parte gestione network sia dal punto di vista del segnale che dal punto di vista dei dati.

La versione R99 dell'UMTS mantiene la parte core network CN-PS identica all'architettura GSM evoluta (GPRS): il che significa che lo standard GSM rimane operativo, sia pur nelle sua versione più evoluta, anche nell'architettura UMTS.

Come nell'architettura GSM il Radio Network Controller (RNC) è l'elemento che governa le BS (Node B) ad esso collegate in termini di gestione delle risorse radio, della loro configurazione, degli aspetti relativi alla mobilità e della sicurezza (criptatura). Si evidenzia che nell'architettura UMTS non è più presente la sottocomponente TRAU.

I compiti principali della RNC sono relativi alla gestione dei canali radio e dei canali terrestri (attraverso la SGSN), tra cui si possono evidenziare:

- Outer Loop Power Control: Gestisce ed ottimizza la qualità del segnale in down link.
- Load control: controllo di carico dei canali.

- Admission Control: Controllo di accesso al canale.
- Packet scheduling: Supervisione della Schedulazione dei dati a pacchetto.
- Handover control: Controllo procedure di spostamento tra celle diverse.
- Security functions: Funzioni di controllo lato sicurezza.
- Mobility Management: Procedure di gestione della mobilità.

La RNC è connessa con la parte di switching della core network in particolare al sottocomponente SGSN che svolge gli stessi compiti dell'architettura GSM.

#### *1.6.1.2. CN CS Domain*

È composta da due elementi, il Mobile Switching Center (MSC) che combinato con il Visitor Location Register (VLR) e il Gateway Mobile Switching Center (GMSC) controlla la gestione delle comunicazioni dell'utente verso la rete fissa, oltre che gestire gli aspetti legati alla sicurezza, gestione della mobilità ecc. Le sue funzionalità sono simili a quelle descritte per l'architettura GSM.

Il GMSC ha in carico le connessioni in ingresso e in uscita verso le altre reti quali PSTN, ISDN, ecc.

#### *1.6.1.3. CN PS Domain*

Il CN PS Domain controlla il trasporto dei dati utenti utilizzando la tecnologia di packet switching: i dati sono organizzati a pacchetti indipendenti ma correlati tra di loro che vengono poi riassemblati.

Il CN PS domain è composto da due sottoelementi base che sono un'evoluzione dalla versione 2.5 del sistema GSM (GPRS) svolgendo lo stesso compito.

La differenza rispetto all'architettura GSM consiste nel fatto che in ambito UMTS su questi elementi sono state implementati sistemi IP multimedia (IM CN) che consentono agli operatori di offrire agli utenti servizi multimediali basati su applicazioni Internet e relativi protocolli.

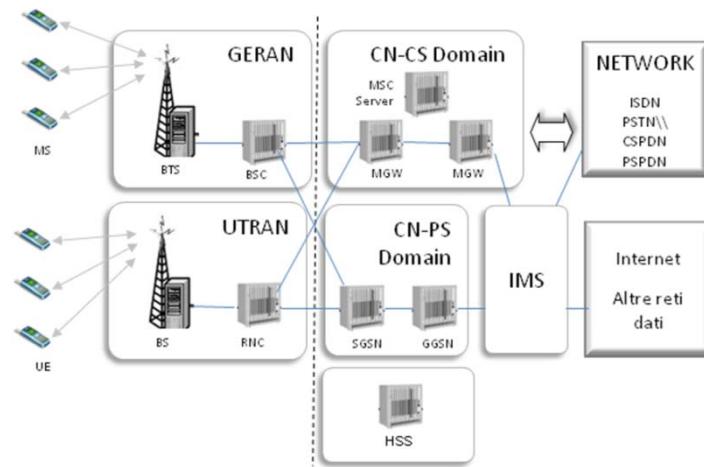
### *1.6.2. La rete UMTS R4*

La maggior innovazione introdotta nella release 4 dell'architettura 3GPP consiste nell'introduzione del protocollo IP all'interno dell'architettura come elemento di comunicazione sia verso network già funzionanti con quel protocollo, sia verso le reti fisse classiche.

La spinta verso il protocollo IP e verso l'utilizzo di sistemi sempre più orientati alla multimedialità e all'accesso a Internet, hanno fatto emergere nuovi elementi dell'architettura tra cui il Multimedia Gateway (MGW).

Nel dominio CN CS i flussi dati utente transitano attraverso i MGW che sono elementi che mantengono la connessione ed effettuano il ruolo di switching quando richiesto. Il funzionamento della rete è garantito dal un elemento separato chiamato MSC Server che deriva direttamente dal MSC/VLR. Un solo MSC Server può gestire più MGW introducendo il concetto di scalabilità del sistema: questo approccio è conosciuto anche come "soft switching".

**Figura 1.4 - Architettura rete UMTS R4**



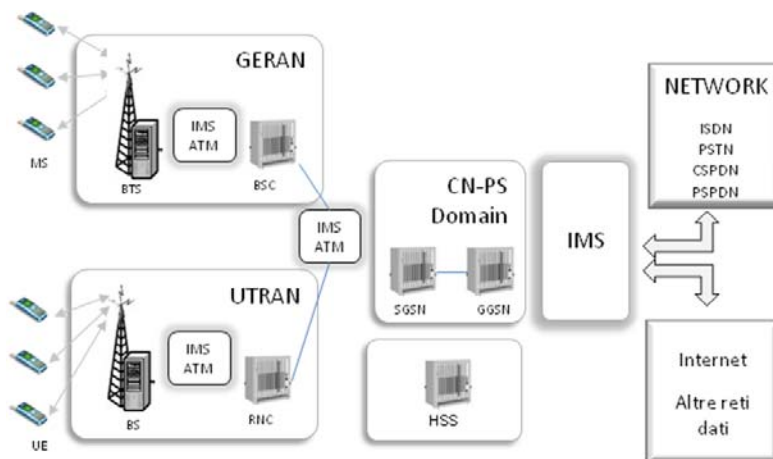
La Release 4 inoltre è caratterizzata da numerose modifiche nelle relazioni nella gestione del traffico dati e voce. Lo standard infatti prevede che il traffico utente sia generalmente gestito con la tecnologia “packed switched” anche per la voce, sfruttando la tecnologia VoIP.

#### 1.6.3. La rete UMTS R5

Nella 3GPP Release 5, come mostrato in Figura 1.7, introduce il protocollo IP anche all’interno dei componenti UTRAN e GERAN. Questa scelta comporta che il CN CS Domain non sia più necessario, perchè sostituito dalle funzionalità messe a disposizione del protocollo IP.

Si noti che, mentre l’interfaccia dell’architettura verso il network è forzosamente IP based, la parte interna può essere basata sia su protocollo IP che sulla tecnologia classica Asynchronous Transfer Mode (ATM) o su di una loro combinazione a discrezione dell’operatore.

**Figura 1.7 - Architettura rete UMTS R5**



## Capitolo 2

### *Il Cell Broadcast*

Il Cell Broadcast è una tipologia di servizio, definita all'interno degli standard GSM e UMTS, che consente ad un "content service provider" anche diverso dell'operatore di telefonia mobile, di diffondere in modalità uno a molti (broadcast) delle informazioni a tutti i terminali mobili fisicamente presenti in una area geografica determinata a priori.

Per "content service provider" si intende un ente o un'azienda che abbia interesse a diffondere un messaggio informativo o pubblicitario verso utenti di telefonia mobile che ne abilitino il canale.

Dal punto di vista della diffusione alla popolazione di messaggi di alerting, il Cell Broadcast offre notevoli potenzialità a strutture pubbliche quali la Direzione Generale Protezione Civile, Polizia Locale e Sicurezza che sarebbe posta nelle condizioni di allertare un gran numero di cittadini in aree specifiche del territorio in particolare quelle soggette all'allarme.

La granularità di diffusione del messaggio può coincidere con la superficie coperta da una singola BTS (per le reti GSM) o Node B (per le reti UMTS), oppure ad un area di più grandi dimensioni ottenibile diffondendo il messaggio a più BTS: questa caratteristica specifica rende il Cell Broadcast una piattaforma ideale per raggiungere un insieme 'anonimo' di utenti GSM/UMTS presenti in un'area predefinita.

Il principale vantaggio del Cell Broadcast, rispetto alle altre modalità di comunicazione, risiede nella capacità di raggiungere in tempi brevissimi un numero molto elevato di utenti che si trovano in un'area geografica determinata, senza generare alcun carico aggiuntivo sulla rete in quanto i messaggi non sono singolarmente indirizzati e vengono trasmessi, almeno in parte, su canali di controllo indipendenti dal traffico. Ciò li rende particolarmente adatti all'uso in caso di emergenza.

I terminali mobili hanno la possibilità di abilitare o disabilitare i messaggi broadcast non desiderati: ogni messaggio infatti è identificato univocamente da un numero di serie e di versione per consentire ai terminali mobili di determinare se si tratta di un nuovo messaggio da presentare all'utente o di un messaggio già ricevuto. Il numero di trasmissioni e la frequenza di ripetizione verso i terminali mobili dei messaggi possono essere concordate tra l'operatore e il fornitore di informazione, in funzione del contenuto informativo e dei rispettivi accordi commerciali. I differenti argomenti contenuti nei messaggi di Cell Broadcast sono

distinti tra di loro da diversi codici che ne identificano la tipologia del contenuto

I titoli degli argomenti sono definiti dallo standard 3GPP, e corrispondono a codici diversi come di seguito riportato :

- 000 - Indice.
- 010 - Notizie lampo
- 020 - Ospedali
- 022 - Dottori
- 024 - Farmacie
- 030 - Viabilità strade a lunga percorrenza
- 032 - Viabilità strade locali
- 034 - Taxi
- 040 - Condizioni meteorologiche
- 050 - Distretto (provincia)
- 052 - Informazioni sulla rete
- 054 - Servizi tramite operatore
- 056 - Elenco abbonati nazionale
- 057 - Elenco abbonati internazionale
- 058 - Servizio clienti nazionale
- 059 - Servizio clienti internazionale

Attualmente l'argomento più frequentemente utilizzato (spesso l'unico utilizzato dagli operatori), è lo 050 che consente di visualizzare l'informazione di "micro cella" sul display del terminale mobile.

## 2.1. Architettura Cell Broadcast

In Figura 2.1 è illustrata l'architettura del sistema di Cell Broadcast in grado di supportare la diffusione verso i terminali mobili di messaggi generati dai content service provider.

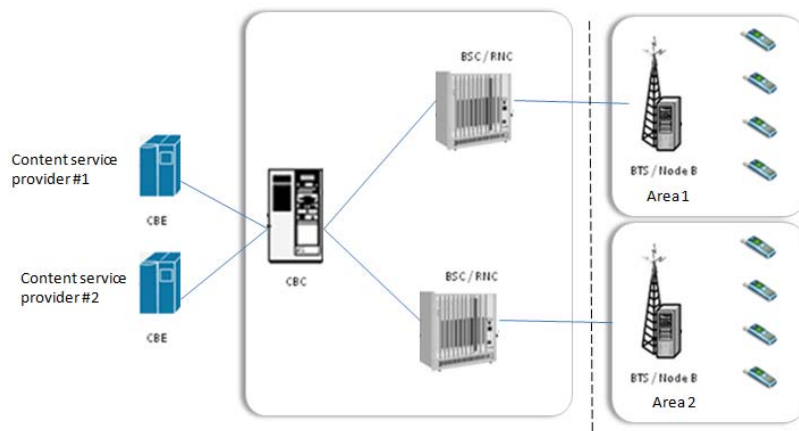
Dal punto di vista architetturale i due componenti che caratterizzano il Cell Broadcast sono il Cell Broadcast Entity (CBE) e il Cell Broadcast Center" (CBC).

Il CBE costituisce l'interfaccia o punto di accesso tra il Content service provider e la rete gestita dall'operatore ed è direttamente connesso con il CBC.

Il CBC ha invece il compito di indirizzare i messaggi dal CBE verso gli elementi BSC/RNC interessati per la corretta diffusione del messaggio verso le BTS che coprono geograficamente l'area interessata.



**Figura 2.1 - Architettura Cell Broadcast**



Un singolo CBC è in grado di servire più CBE e di indirizzare più BSC/RNC. La sottomissione di messaggi di alerting in modalità Cell Broadcast richiede la definizione di un protocollo di comunicazione tra il content service provider e il CBE. Il protocollo non è soggetto a nessuna standardizzazione per cui è necessaria una sua definizione in fase di progettazione del sistema di Cell Broadcast (vedi Capitolo 5).

## 2.2. Il funzionamento del Cell Broadcast

Il Cell Broadcast Entity (CBE) è l'interfaccia utilizzata dai content provider per inviare dei messaggi in modalità Cell Broadcast. Il CBE è costituito normalmente da una piattaforma nella quale è creato il messaggio sia in termini di contenuti sia in termini di attributi quali l'area geografica, la ripetizione, priorità, ecc.: la CBE è inoltre responsabile per la corretta formattazione del messaggio stesso e per la gestione del protocollo di comunicazione con la CBC.

La definizione dell'interfaccia CBE-CBC non è tra gli obiettivi degli standard 2G e 3G ed è lasciata al singolo gestore di telefonia e al content provider le modalità di connessione e comunicazione tra CBE e CBC.

All'interno della rete il CBC è posizionato a monte della BSC per le reti GSM e a monte della RNC per reti UMTS (vedi figure successive).

Dal punto di vista delle interfacce, il CBC è stato specificato nella Release 99 dello standard UMTS sotto il nome di Service Area Broadcast, pertanto garantisce la continuità e la disponibilità dei servizi tra lo standard GSM (2G) e UMTS (3G).

Nello standard UMTS il CBC è parte del Core Service Network ed è stato soggetto a specifiche più di dettaglio rispetto allo standard GSM, soprattutto per quanto riguarda la definizione delle interfacce con la componente RNC.

Una volta identificata l'area e il contenuto del messaggio, l'informazione deve essere comunicata al CBC. In generale è lo stesso CBC a possedere il database che

contiene le informazioni relative alle BTS e la loro area di copertura. Il database mappa l'area di broadcast selezionata identificando quali BTS devono essere attivate. Sulla base di queste informazioni il CBC individua il BSC (RNC) che controlla la BTS (Node B) interessata.

A questo punto il CBC, utilizzando un protocollo standardizzato, invia il messaggio alle BTS (Node B) individuate comunicando tutte le informazioni necessarie (attributi) per la sua diffusione ai terminali mobili.

Il CBC è in grado di specificare il periodo in cui un messaggio deve essere diffuso o può esplicitamente inviare un comando di "stop broadcast" nel momento in cui si intende sospendere la sua diffusione.

## 2.3. Caratteristiche specifiche

La diffusione del messaggio di alert non richiede la conoscenza del numero telefonico del destinatario e il messaggio di alert raggiunge solamente i terminali mobili che, oltre ad essere presenti in una determinata area geografica, hanno esplicitamente abilitato il canale o l'indice dell'argomento di Cell Broadcast riservato alle comunicazioni da parte della Direzione Generale Protezione civile Polizia Locale e Sicurezza.

Attualmente il Cell Broadcast vanta delle potenzialità non ancora sfruttate e la sua combinazione con altre tecnologie è in grado di mettere a disposizione potenzialmente uno strumento di comunicazione multimediale sfruttando la tecnologia 3G in particolare UMTS.

Un'altra caratteristica fondamentale del Cell Broadcast è quella di non essere onerosa per l'utenza finale (cittadino) che riceve la notifica dell'alert allo stesso modo di un SMS. In questo senso non è necessaria la sottoscrizione di alcun contratto e non è richiesto di fornire informazioni personali quali dati sensibili o informazioni private. Al cittadino è richiesta semplicemente l'attivazione del canale di Cell Broadcast riservato alla Direzione Generale Protezione Civile, Polizia Locale e Sicurezza.

Attualmente in Italia è attivo solamente il servizio di Cell broadcast legato alla microcella (canale 50) dove viene diffuso in aria il nome della provincia dove la microcella è ubicata: tutti gli altri canali non trasmettono alcuna informazione.

### 2.3.1. *Messaggio di Cell Broadcast*

Da un punto di vista tecnico le specifiche di riferimento sono contenute nelle specifiche ETSI 23.49 e 23.41. In realtà, a differenza della quasi totalità dei documenti di specifica ETSI, le specifiche relative al Cell Broadcasting, sono decisamente lacunose per quanto riguarda le regole d'implementazione del servizio all'interno della rete degli operatori, ed alcune parti sono lasciate alla libera iniziativa ed implementazione dei singoli costruttori. Nel dettaglio la

specifica 03.41 indica più che altro suggerimenti riguarda la realizzazione tecnica del servizio di Cell Broadcasting, mentre la 23.49 contiene esempi di protocollo per connettere il CBC e il BSC.

Dal punto di vista dell'operatore, che intende utilizzare il servizio di CB per diffondere informazioni, si deve occupare principalmente di definire:

- il testo del messaggio che deve essere visualizzato sul terminale mobile;
- l'area che intende coprire;
- con quale frequenza deve essere inviato il messaggio;
- quanto deve durare il periodo di ripetizione in aria del messaggio stesso;
- la lingua in cui è scritto il singolo messaggio;
- quante pagine compongono il testo del messaggio.

Le caratteristiche citate sono gli elementi di base che caratterizzano il messaggio e che generalmente può e deve inserire lo stesso operatore che si serve del servizio di Broadcasting. Queste informazioni dovranno essere interpretate dal CBC ricevente in modo da codificare concetti come periodo di ripetizione, linguaggio utilizzato e area di broadcasting al fine di essere correttamente interpretati dai vari apparati di rete (fondamentalmente i BSC).

Le informazioni descritte, dovranno essere integrate con altri elementi di più basso livello, per permettere l'identificazione univoca del messaggio all'interno della rete mobile. In questo senso ogni messaggio deve contenere un numero di serie ed un identificativo numerico univoco, elementi che di solito sono inseriti a carico del CBC stesso. Nei paragrafi seguenti analizziamo i singoli elementi che descrivono ogni messaggio di Cell Broadcast nella rete mobile.

#### *2.3.1.1. Parametri*

L'operatore che intende inviare un messaggio, dovrà descrivere un insieme di elementi di base che dovranno essere completati ed integrati da parte del CBC prima di poter essere fisicamente inviati verso i terminali mobili.

In questo paragrafo sarà analizzata la struttura del messaggio che il CBC deve inviare verso la rete di telefonia mobile e che deve giungere ai terminali, componente necessaria per la corretta definizione del protocollo tra il CBC e la Sala Operativa della Direzione Generale Prevenzione, Protezione Civile, Polizia Locale e Sicurezza.

La descrizione della struttura dei singoli messaggi sarà semplificata, focalizzando l'attenzione sugli elementi di maggiore interesse ai fini della ricerca. Per una più dettagliata descrizione del protocollo di comunicazione si rimanda alle specifiche di riferimento (ETSI - 23.41 e 23.49).

Nel momento in cui il CBC riceve la richiesta di invio di un nuovo messaggio, dovrà inviare una richiesta di WRITE\_REQUEST verso la rete mobile specificando i campi descritti in Tabella 2.1.

**Tabella 2.1 - Identificazione campo CBC**

Campo	Descrizione
1	Codice Identificativo del Messaggio
2	Numero di Serie
3	Lista di Celle
4	Periodo di Ripetizione
5	Numero di ripetizioni richieste
6	Numero di pagine del Messaggio
7	Linguaggio Utilizzato
8	Pagine di testo del messaggio

Nel dettaglio:

*Codice Identificativo del Messaggio:*

È costituito da un valore numerico, compreso tra 0 e 65535, che serve per identificare univocamente il messaggio all'interno della rete mobile.

*Numero di Serie:*

È un campo utilizzato per specificare una serie di indicazioni che vengono interpretate direttamente dai mobili. Nello specifico contiene tre gruppi di indicazioni:

- Scope Geografico: fornisce indicazioni sul tipo di area coperta, ma in particolare, fornisce indicazioni ai terminali mobili su come visualizzare il contenuto del messaggio stesso. Tra le altre opzioni, è previsto un 'immediate display', che indica ai mobili di visualizzare il messaggio direttamente sul display del telefonino, senza richiedere particolari azioni da parte dell'utenza finale;
- Numero di Serie: valore che in combinazione col Codice del messaggio è utilizzato dalla rete per identificare univocamente uno specifico messaggio;
- Aggiornamento: valore che viene utilizzato dai mobili per leggere la versione del messaggio stesso.

*Lista di Celle:*

Contiene la lista delle celle alle quali è richiesto di inviare il messaggio verso i mobili. È in pratica la mappatura, in genere a cura del CBC dal concetto di Area di Broadcast, al concetto di copertura delle singole celle dell'operatore.

*Numero di ripetizioni:*

Serve a specificare agli apparati di rete preposti all'invio dei messaggi verso i mobili, quante volte il singolo messaggio dovrà essere inviato in aria dalle celle indicate. Esaurito il numero di ripetizioni richieste, il messaggio viene cancellato dalla rete e non è più inviato ai terminali mobili.

#### *Codifica dei dati:*

È un parametro che serve a specificare l'alfabeto utilizzato nel testo del messaggio e di più genericamente la lingua in cui il testo del messaggio è scritto. Il valore di tale campo può essere utilizzato dai mobili per ricevere solo messaggi scritti nella lingua selezionata dall'utente, che ha così modo di accedere all'informazione in modo più diretto.

#### *Frequenza di Ripetizione:*

Indica l'intervallo di tempo tra una ripetizione del messaggio in aria e quella successiva. La frequenza di ripetizione viene rispettata e garantita per tutto il periodo di ripetizione specificato. Questo meccanismo garantisce la ricezione del messaggio anche agli utenti che entrano nella zona allertata successivamente al primo invio del messaggio di alert fornendo un servizio di informazione più solido e controllabile.

In realtà la struttura e i contenuti dei messaggi di Cell Broadcast sono descritti in modo più complesso ed articolato nelle specifiche di riferimento: la descrizione qui riportata è comunque esaustiva per illustrare le componenti necessarie ai fini della ricerca.

#### *2.3.1.2. Contenuto Informativo*

Il contenuto informativo del messaggio è costituito dal testo che viene inviato al terminale mobile. La sua struttura è organizzata a pagine: ogni pagina è lunga al massimo 93 caratteri. Questi caratteri rappresentano il messaggio che sarà inviato ai terminali mobili in un determinato formato (chiamato 'compattato') che utilizza solamente 82 caratteri.

Lo standard ETSI di riferimento prevede che un singolo messaggio possa essere composto da una o più pagine, fino ad un massimo di 15. In realtà, la scarsa diffusione del servizio fino ad oggi, ha portato ad implementazioni del servizio di Cell Broadcast sugli apparati mobili, spesso incomplete e sicuramente lacunose: ne consegue che la gestione dei messaggi multi pagina non è sempre garantita sugli apparati telefonici. Per questo motivo è consigliabile utilizzare messaggi composti da una singola pagina di testo (93 caratteri), integrando il contenuto informativo con ulteriori nuovi messaggi.

#### *2.3.1.3. Interfaccia CBC - BSC*

Le specifiche che definiscono il CBC prevedono una serie di funzioni base di comunicazione (primitive) tra CBC e rete e tra rete e CBC, che consentono di creare/cancellare messaggi e di interrogare la rete sul funzionamento del servizio Cell Broadcast attivato. Di seguito riportiamo le principali funzioni implementate tra il CBC e la rete mobile:

#### *Write Request*

Primitiva con la quale il CBC, su richiesta del CBE, chiede la creazione di un nuovo messaggio da inviare verso i terminali mobili. Le caratteristiche e la struttura di questo messaggio è descritta nel paragrafo precedente.

#### *Kill Request*

Primitiva a disposizione del CBC, per chiedere l'eliminazione di un messaggio precedentemente inviato. Con questa funzionalità, l'operatore ha la possibilità di chiedere la cessazione della schedulazione di uno specifico messaggio (identificato da Codice e Numero di Serie), prima dello scadere del periodo di diffusione. La funzionalità è particolarmente utile in tutti quei casi in cui il messaggio precedentemente inviato non ha più significato, o comunque in cui il contenuto del messaggio non è più attuale. Inviando la richiesta di Kill, l'operatore, tramite CBC, disattiva l'invio ai terminali mobili del testo del messaggio integrando il comportamento eventualmente con nuovi messaggi di cessato allarme o di nuove indicazioni sullo stato dell'allerta. In questo contesto ci si limita a descrivere la primitiva in termini di funzionalità, per quanto riguarda la struttura di dettaglio della primitiva, ed in generale delle primitive che seguono, rimandiamo sempre alla specifica di riferimento (ETSI 23.41).

#### *Status message*

Primitiva che consente all'operatore via CBC, di interrogare la rete mobile sullo stato di invio di uno specifico messaggio. Tramite questa primitiva, l'operatore ha la possibilità di leggere direttamente dalla rete, lo stato di un messaggio specifico, in termini di numero di ripetizioni eseguite con successo ed eventualmente di mancate ripetizioni per cause imputabili a disservizi della rete stessa.

#### *Reset*

Primitiva con la quale il gestore del servizio, via CBC, ha la possibilità di azzerare il Data Base dei messaggi presenti in rete sui BSC. E' di solito utilizzata in fase di avvio del sistema CBC, per consentire l'allineamento tra il CBC stesso e gli altri componenti della rete cui si interfaccia.

#### *2.3.1.4. Primitive BSC - CBC*

In modo simmetrico rispetto a quanto descritto nel paragrafo precedente, gli elementi della rete (generalmente i BSC) hanno la possibilità di comunicare con il CBC, sia per rispondere a richieste da parte del CBC, sia per inviare indicazioni spontanee sul funzionamento del servizio di Cell Broadcast. Anche in questo caso, la descrizione dell'interfaccia viene riportata in modo semplificato e con un livello di dettaglio adatto a questa trattazione, rimandando per eventuali approfondimenti alle specifiche di dettaglio (ETSI 23.41).

Le primitive di comunicazione tra BSC e CBC sono elencate di seguito:

#### *Report Success*

È la primitiva tramite la quale i BSC riscontrano una generica richiesta di *Write request* o di *Kill request* al CBC. Nella risposta inviata al CBC, il BSC fornisce indicazioni circa il buon esito del comando, il successo di scrittura e invio di nuovi messaggi o di successo nel di cancellazione di un messaggio, come richiesto dal CBC. In particolare, in caso di cancellazione di un vecchio messaggio, il BSC fornisce anche indicazioni sullo stato di consegna alla rete del messaggio stesso, quali il numero di volte che il messaggio è stato inviato o l'elenco delle celle che hanno avuto eventuali disservizi.

#### *Failure Indication*

È una fondamentale primitiva che viene utilizzata dal BSC per indicare il temporaneo disservizio di una o più celle o in generale l'indisponibilità del servizio di Cell Broadcast nella rete. È la primitiva fondamentale per il controllo e la sincronizzazione del CBC con la rete stessa e consente meccanismi automatici di auto recovery in caso di temporanei malfunzionamenti della rete stessa.

#### *Status CBCH Rsp & Status Message Rsp*

Primitive utilizzate dai BSC per rispondere alle richieste di stato inviate dal CBC stesso. Permettono di fornire agli operatori di rete indicazioni sullo stato del servizio in tempo reale e con dati aggiornati direttamente dalla rete stessa.

#### *Restart*

È la primitiva con la quale i BSC informano il CBC che sono stati riavviati, e di conseguenza i messaggi di Cell Broadcast devono essere nuovamente inviati ai BSC stessi, che non tengono generalmente memoria dei messaggi da spedire in caso di riavvio degli apparati.

Il set di messaggi descritto è necessario per definire l'insieme dei potenziali comandi che la Sala Operativa della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza è in grado di inviare verso la rete di telefonia mobile

## 2.4. Potenzialità del Cell Broadcast

La tecnologia Cell Broadcast è in grado di supportare una serie di servizi di comunicazione in modalità broadcast (uno a molti). La tecnologia più semplice costituita dall'invio di un messaggio di testo può essere affiancata dalla tecnologia multimediale resa disponibile dalla tecnologia UMTS. Ad oggi la tecnologia necessaria per supportare la multimedialità (3G) non è ancora diffusa così capillarmente come quella di seconda generazione (GSM), impedendo di fatto la realizzazione di un sistema di alerting più sofisticato. Di seguito sono brevemente illustrate alcune aree di applicazione della tecnologia Cell Broadcast analizzata indipendentemente dalla tecnologia utilizzata (2G o 3G) e dalle finalità del presente documento.

#### *Comunicazione Eventi*

Una possibile applicazione del Cell Broadcast è rappresentata dalla diffusione a livello informativo dell'accadimento di determinati eventi che possono essere di natura culturale, sportivo o di qualsiasi altro genere. Il contenuto della informazione può essere di qualsiasi natura, ovvero pubblicità, avvisi, comunicazione di variazione di programmi, ecc.

### *Pubblicità*

La diffusione di messaggi pubblicitari può trarne vantaggi in quanto può essere indirizzata su aree geografiche specifiche mirando in modo più preciso il target di popolazione che si intende raggiungere. Particolarmente importante per questo tipo di applicazione è la convivenza con la tecnologia multimediale.

### *Informazioni sul traffico*

È molto simile all'alerting e consente di inviare messaggi in determinate zone del territorio in cui la situazione del traffico risulta essere congestionata. Il servizio può essere particolarmente utile per le persone che si muovono per lavoro o per affari, permettendo loro di utilizzare percorsi alternativi se preventivamente avvisati. In prospettiva potrebbe essere integrato con i sistemi di navigazione satellitari per il calcolo di percorsi alternativi.

### *M-Marketing*

Le campagne di Mobile Marketing possono essere un canale di comunicazione utilizzabile dalle aziende per raggiungere un grande numero di persone localizzate in una determinata area del territorio interessate a collaborare in campagne di survey.

### *Informazioni turistiche*

Una possibile applicazione del CB riguarda anche la diffusione di informazioni turistiche diffuse presso le stazioni ferroviarie dove il turista in arrivo può essere informato su banche, farmacie, supermercati, condizioni meteorologiche, agenzie di viaggio, ecc.

### *Informazioni aeroportuali*

Nelle aree aeroportuali possono essere diffusi messaggi circa arrivi, partenze, ritardi, cancellazioni e altre informazioni correlate. In aggiunta possono essere diffuse informazioni riguardo collegamenti ferroviari o altri mezzi di collegamento con la città e altri servizi collegati.

## 2.5. Analisi della copertura di rete

In questo paragrafo è analizzato in breve il livello di copertura fornito dagli operatori di telefonia mobile per la tecnologia Cell Broadcast. L'analisi riguarda solamente gli apparati presenti sul territorio di Regione Lombardia in particolare nella zona Rho Fiera.

Il grado di precisione, l'affidabilità e il livello di dettaglio delle informazioni raccolte è funzione della disponibilità dei dati. Un'analisi esaustiva e precisa per la copertura di rete richiede la collaborazione degli operatori di telefonia mobile che sono in possesso dei dati puntuali sulla copertura di rete e della tecnologia utilizzata.



In mancanza dei dati dagli operatori di telefonia, si è proceduto ad un'analisi di copertura utilizzando le informazioni reperite in rete presenti sui siti ufficiali degli operatori di telefonia mobile.

### *2.5.1. Il concetto di copertura*

Per copertura di rete si intende la capacità della rete di soddisfare il requisito di raggiungibilità degli utenti. La raggiungibilità degli utenti si può riferire a differenti caratteristiche in funzione di ciò che si intende misurare. In particolare è possibile definire i seguenti concetti di copertura:

- copertura geografica;
- copertura tecnologica;
- copertura della popolazione.

Con copertura geografica si intende la superficie territoriale all'interno della quale il terminale mobile è in grado di comunicare con la BTS.

In Figura 2.2 sono colorate in giallo e in ocra le aree coperte geograficamente dalla rete: le zone evidenziate con un cerchio rosso non posseggono copertura di rete, per cui un terminale presente in queste zone non è in grado di funzionare.

Tipicamente le zone senza copertura di rete sono localizzate in territori poco abitati (zone montuose) in cui spesso l'orografia impedisce la corretta propagazione del campo elettromagnetico generato dalla BTS.

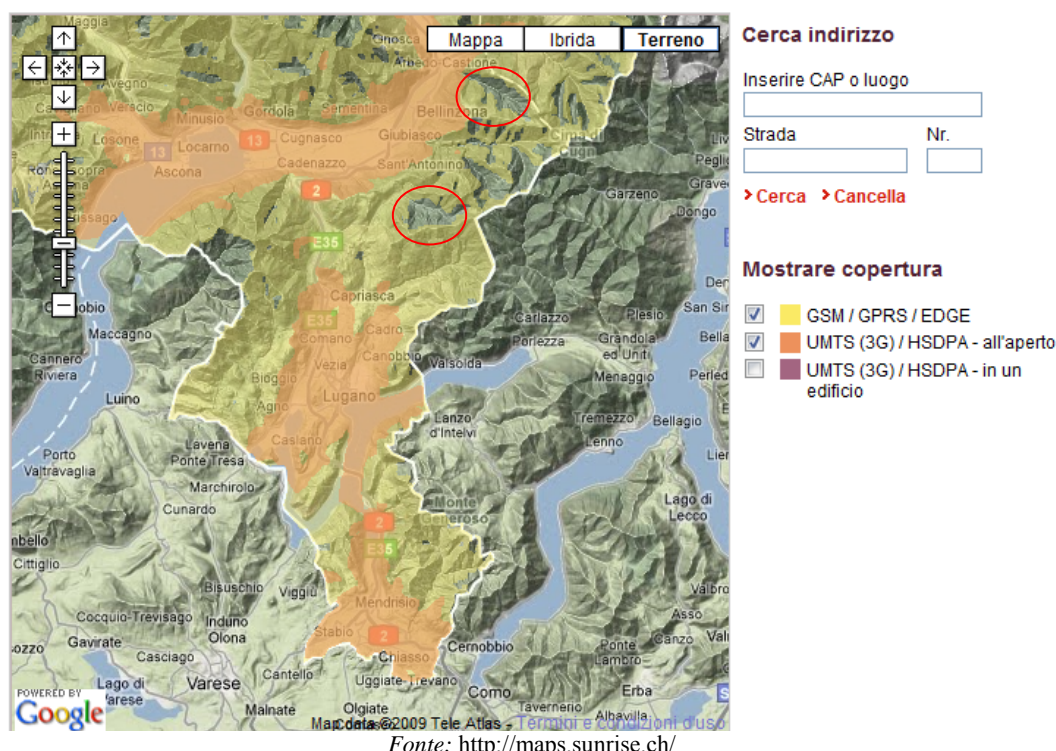
Con copertura tecnologica si intende la disponibilità di una determinata tecnologia in un'area specifica del territorio. Facendo sempre riferimento alla Figura 2.2, si può notare che la superficie territoriale maggiore è coperta dalla tecnologia GSM, GPRS, EDGE, mentre la tecnologia UMTS, HSDPA è diffusa su di un'area territoriale molto più limitata ed è soprattutto concentrata nelle zone più densamente popolate.

Ne segue che i servizi offerti dalla tecnologia UMTS possono essere utilizzati solamente nelle aree "coperte" da tale servizio mentre non sono utilizzabili nelle aree coperte solamente dalla tecnologia GSM.

Ipotizzando che i servizi di alerting utilizzino solamente la tecnologia UMTS, la copertura geografica sarebbe limitata alle aree in cui tale tecnologia è disponibile.

Come diretta conseguenza la popolazione non presente nelle aree coperte dalla tecnologia UMTS o che non posseggono un terminale mobile senza UMTS non sono raggiungibili dal messaggio di alerting.

**Figura 2.2 - Copertura di rete nel Canton Ticino**



Con copertura della popolazione si intende la capacità di raggiungere gli utenti ed è espressa in percentuale rispetto alla totalità della popolazione. La raggiungibilità della popolazione dipende direttamente dalla copertura geografica e dalla localizzazione della popolazione stessa. In un centro urbano altamente popolato, la copertura della popolazione è molto vicino al 100% ovvero tutti i cittadini in possesso di un terminale mobile presenti nell'area sono raggiunti dai servizi. In zone montane o rurali per difficoltà orografiche, di convenienza economica di scarsa diffusione dei terminali mobili, non tutti i cittadini sono raggiungibili dai servizi di telefonia mobile.

Queste misure di copertura sono importanti per valutare il grado di raggiungibilità della popolazione in caso di diffusione di un messaggio di alert.

### *2.5.2. I dati disponibili in rete*

Questi i dati relativi alle coperture UMTS e GSM che è possibile reperire in rete. La doverosa premessa è che queste informazioni non sono facilmente reperibili dai siti degli operatori, quando forse dovrebbe essere una delle informazioni importanti, soprattutto quando si parla della copertura 3G, molto in voga in questo periodo.

#### Copertura TIM:

- copertura GSM: 99,8% della popolazione pari al 98% del territorio;
- copertura UMTS: 85% della popolazione.

#### Copertura Vodafone:

- copertura GSM: 99,4% della popolazione pari all'94% del territorio;
- Ccertura UMTS: 78% della popolazione pari all'80% del territorio;
- 500 centrali e 11.000 stazioni radio base.

#### Copertura Wind:

- copertura GSM: 99,65% della popolazione pari al 94,3% del territorio;
- copertura UMTS: 57,9% della popolazione pari al 16,90% del territorio;
- 11.386 stazioni radio base.

#### Copertura TRE:

- copertura GSM: 99,8% della popolazione pari al 98% del territorio (in Roaming TIM);
- copertura UTMS: 88% della popolazione.

#### *2.5.3. L'analisi della copertura*

Per comprendere la copertura fornita dai quattro gestori di telefonia mobile (TIM, Vodafone, Wind, TRE) nell'area Rho Fiera, si sono stati analizzati i dati pubblicati in rete dagli operatori stessi. Data la disomogeneità e la limitatezza dei dati raccolti non è possibile effettuare un'indagine esaustiva dal punto di vista della raggiungibilità della popolazione: in ottica introduzione di un sistema alerting è pertanto necessario approfondire gli argomenti direttamente con i gestori della telefonia per una corretta analisi della copertura.

Per quanto possibile l'analisi si è limitata al solo comune di Rho e si è svolta consultando i portali degli operatori stessi e raccogliendo i dati. In rete sono disponibili altre informazioni ma è difficile verificarne l'attendibilità e l'affidabilità.

#### *2.5.4. La copertura TIM*

Le informazioni reperibili sul sito di TIM riguardano la copertura geografica e la copertura tecnologica.

**Figura 2.3 - Copertura TIM in Regione Lombardia Comune di Rho**



The screenshot shows a web interface for checking TIM coverage in Italy. On the left is a map of Italy with the Lombardy region highlighted in red. On the right, the text reads: 'Verifica la copertura TIM in ITALIA', 'Verifica se il tuo comune è raggiunto dalla copertura TIM', and a list of technologies: GSM (GPRS e EDGE), UMTS, DVB-H, and UMTS HI Speed. Below this, it says 'Hai scelto la regione: LOMBARDIA', 'Provincia: MI', and 'Per il comune di RHO esiste copertura:'. The coverage status for each technology is listed as 'si' (yes) in red: GSM (GPRS e EDGE): si, UMTS: si, DVB-H: si, and UMTS HI Speed: si. At the bottom are two buttons: 'NUOVA RICERCA' and 'CHIUDI'.

Tecnologia	Copertura
GSM (GPRS e EDGE)	si
UMTS	si
DVB-H	si
UMTS HI Speed	si

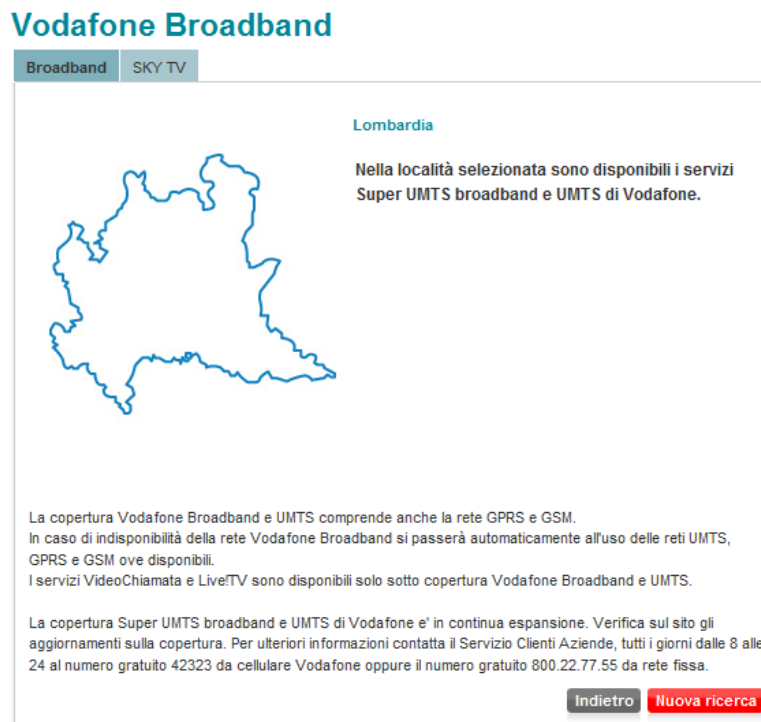
Da Figura 2.3 si evince che il Comune di Rho è coperto per le tecnologie GSM (GPRS ed EDGE), UMTS, UMTS High Speed e DVB - H.

Non sono invece note le informazioni relative alla copertura di popolazione che si assume, essendo un comune ad alta concentrazione abitativa, sia prossima al 100%. Analogamente alla copertura di popolazione si assume che la copertura geografica sia pari al 100% del territorio, essendo in una zona ad alta densità abitativa.

#### *2.5.5. La copertura Vodafone*

Le informazioni reperibili sul sito di Vodafone riguardano la copertura geografica e la copertura tecnologica.

**Figura 2.4 - Copertura Vodafone in Regione Lombardia Comune di Rho**



Da Figura 2.4 si evince che il Comune di Rho è coperto per le tecnologie GSM, GPRS, Super UMTS broadband, UMTS.

Non sono invece note le informazioni relative alla copertura di popolazione che si assume, essendo un comune ad alta densità abitativa, sia prossima al 100%.

Analogamente alla copertura di popolazione si assume che la copertura geografica sia pari al 100% del territorio, essendo in una zona ad alta densità abitativa.

#### *2.5.6. La copertura WIND*

Le informazioni reperibili sul sito di Wind riguardano la copertura geografica e la copertura tecnologica.

**Figura 2.5 - Copertura Wind in Regione Lombardia Comune di Rho**

**Copertura Rete Mobile**  
Per verificare la disponibilità della copertura WIND, seleziona la regione, la provincia e infine il comune di tuo interesse.

Regione


Lombardia

Provincia


Milano

Comune


Rho



Copertura GPRS disponibile



Copertura UMTS disponibile



Copertura HSDPA disponibile

**Wind Ricorda**  
La copertura GSM coincide con quella GPRS.  
La Rete Mobile WIND è in costante evoluzione, verifica periodicamente sul sito gli aggiornamenti relativi alla copertura.  
Per maggiori informazioni sulla copertura chiama il Servizio Clienti dal tuo telefonino WIND.  
  
Ultimo aggiornamento: settembre 2009

Da Figura 2.5 si evince che il comune di Rho è coperto per le tecnologie GSM, GPRS, UMTS e HSDPA.

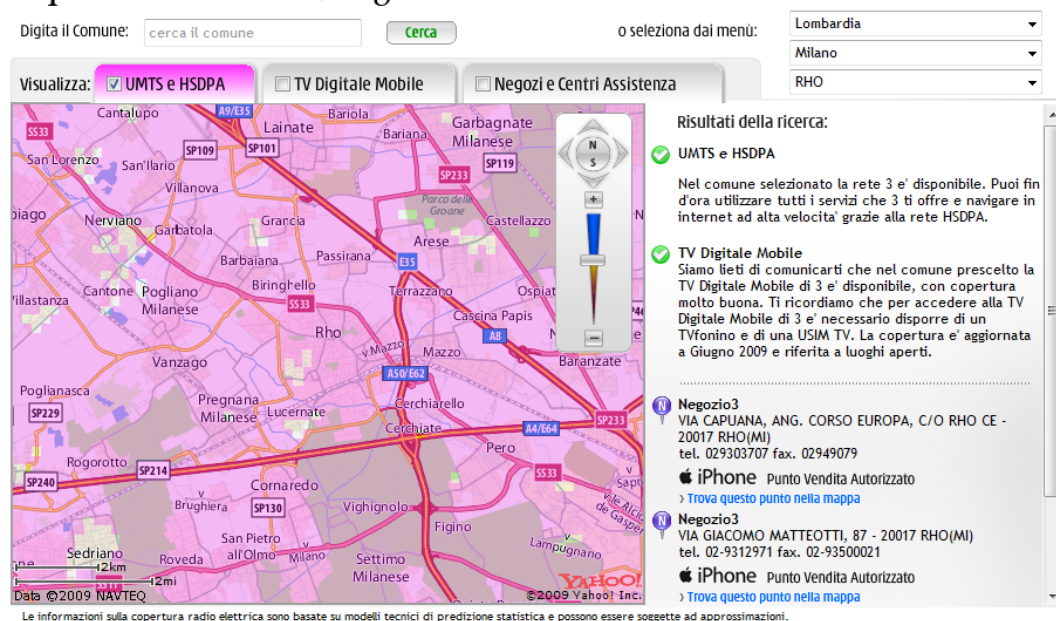
Non sono invece note le informazioni relative alla copertura di popolazione che si assume, essendo un comune ad alta concentrazione abitativa, sia prossima al 100%. Analogamente alla copertura di popolazione si assume che la copertura geografica sia pari al 100% del territorio, essendo in una zona ad alta densità abitativa.

#### *2.5.7. La copertura TRE*

Le informazioni reperibili sul sito di *TRE* riguardano la copertura geografica e la copertura tecnologica.

**Figura 2.6 - Copertura Tre in Regione Lombardia Comune di Rho**

## Copertura Nazionale, Negozi 3 e Centri Assistenza

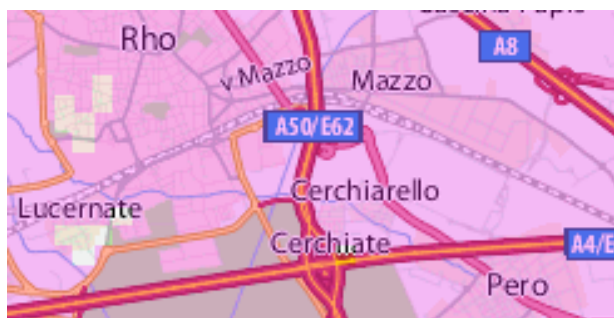


Da Figura 2.6 si evince che il Comune di Rho è coperto per le tecnologie UMTS, HSDPA e Tv Digitale Mobile. Non è chiaro se sia disponibile anche una copertura GSM.

Non sono invece note le informazioni relative alla copertura di popolazione che si assume, essendo un comune ad alta concentrazione abitativa, sia prossima al 100%. A differenza di TIM, Vodafone e Wind, TRE fornisce informazioni anche sulla copertura geografica della zona di Rho: come si può notare da Figura 2.7 esistono delle aree non coperte dalla rete di TRE.

Infatti, come si può notare da Figura , esistono delle aree anche urbane che non sono raggiunte.

**Figura 2.7 - Copertura geografica di Rete di TRE**



In particolare parte del territorio di Lucernate e del centro di Rho non è coperto, mentre la zona Rho Fiera risulta essere completamente coperto geograficamente dalla rete TRE. In questa situazione è possibile dedurre che la copertura della popolazione del comune di Rho non sia coperta al 100%.



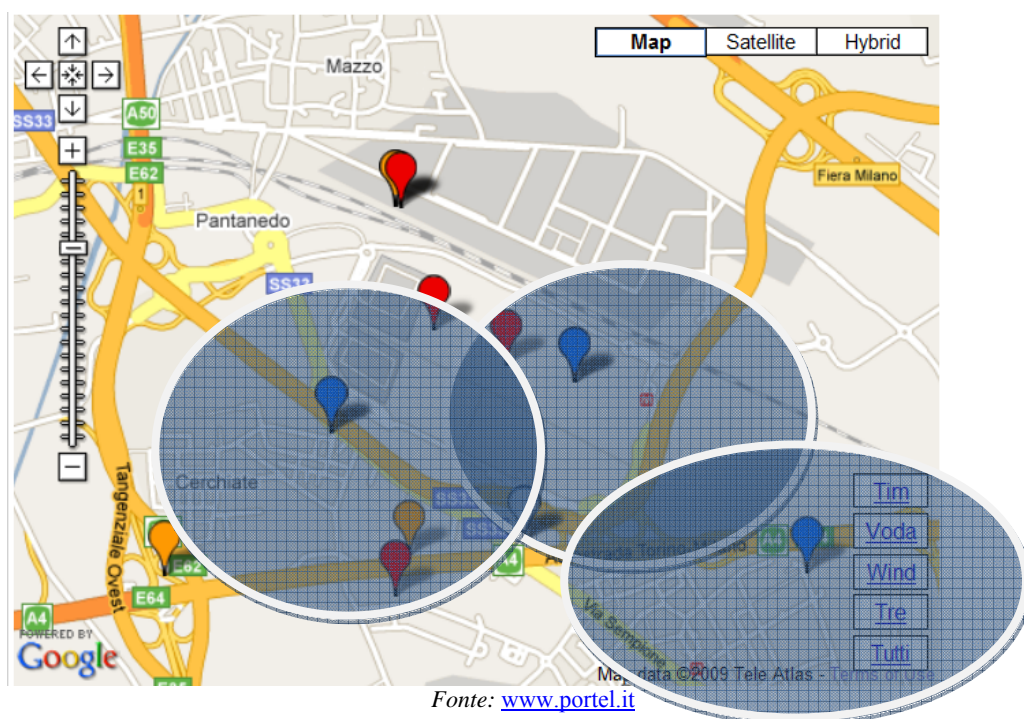
### 2.5.8. La dislocazione delle BTS

Per meglio comprendere il concetto di copertura geografica, si analizza la disposizione delle BTS nell'area Rho Fiera (rif. Figura 2.8) dove si può distinguere la localizzazione delle antenne di TIM (simbolo blu), Vodafone (simbolo rosso), Wind (simbolo beige) e TRE (simbolo bianco).

Non avendo indicazione sulla direzionalità delle antenne e non essendo a conoscenza della potenza di ciascuna antenna, si suppone che ogni BTS copra una superficie ovale e omogenea per ogni antenna.

Per semplicità e chiarezza di rappresentazione, in Figura 2.8 è ipotizzata la copertura delle antenne appartenenti all'operatore TIM.

**Figura 2.8 - Dislocazione BTS area Rho Fiera**



I cittadini che si trovano nell'area coperta dalle BTS di TIM (area evidenziata in turchese nella Figura 2.8) hanno accesso ai servizi forniti dalla rete TIM, ovvero potranno accedere alle tecnologie GSM (GPRS ed EDGE), UMTS, UMTS High Speed e DVB - H.

Estendendo il concetto agli altri operatori, gli utenti di Vodafone, Wind e TRE potranno usufruire dei servizi offerti dai propri operatori nelle aree coperte dalle rispettive BTS.



## 2.6. Il Terminale Mobile

Il terminale mobile, chiamato comunemente cellulare o telefonino, è un apparecchio radio trasmittente e ricevente in grado di comunicare tramite radiofrequenza con la rete telefonica tramite centrali di smistamento, denominate BTS (Base Transceiver Station), molto spesso dotate di tre o più celle, ciascuna capace di diverse connessioni con gli apparecchi mobili.

Il terminale mobile consente di avere sempre disponibile un collegamento telefonico quando si trovi nel raggio di copertura di una cella la cui superficie si estende per un'area variabile in funzione della capacità della BTS. In base alla tecnologia disponibile, il terminale mobile è in grado di accedere ai servizi messi a disposizione dalla rete, in particolare ai servizi di Cell Broadcast.

Tutti i terminali mobili che adottano la tecnologia 2G e 3G posseggono la funzionalità di Cell Broadcast. In funzione del modello e dell'età, si ha la presenza o meno dell'interfaccia di attivazione e a diversi livelli di usabilità.

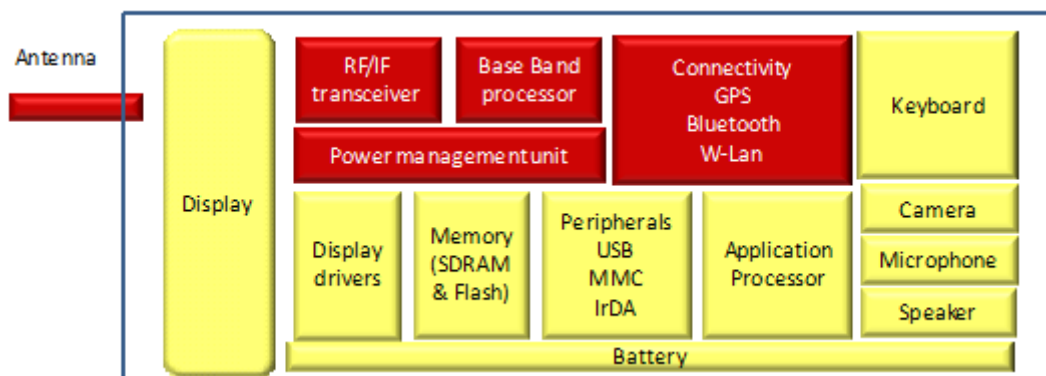
### 2.6.1. Architettura

L'architettura di un terminale mobile è suddivisibile in due parti (o unit) che sovrintendono a funzionalità specifiche. In particolare:

- Communication Unit: gestione della componente radio e implementazione delle tecnologie di comunicazione;
- Application Unit: gestione dei contenuti forniti dalla rete cellulare e dell'interfaccia verso l'utente.

La Figura 2.9 rappresenta lo schema a blocchi di un generico terminale mobile nel quale sono evidenziati i singoli componenti.

**Figura 2.9 - Architettura del terminale mobile**



In particolare si possono distinguere due sottoinsiemi di componenti:

- sottosistema “Communication” composto da Antenna, RF-IF Transceiver, Base-Band processor, Power Management Unit, Connectivity (GPS, Bluetooth, W-Lan);
- sottosistema “Applications” compost da Application processor, Display & drivers, Memory (SDRAM e Flash), Camera module e batterie, Keyboard, Microphone, Speaker, Peripherals (USB, MMC, IRDA), applications & OS.

Il sottosistema Communications possiede delle funzionalità che operano indipendentemente dalle azioni dell'utente (es. controllo della potenza del trasmettitore), mentre altre sono comandate indirettamente dall'utente stesso attraverso delle applicazioni che mettono a disposizione un'interfaccia che ne consente l'utilizzo. Tra queste funzionalità gestite dalle applicazioni è da annoverare l'abilitazione del Cell Broadcast e la conseguente attivazione del canale di message alerting.

#### *2.6.2. Requisiti del terminale mobile*

La corretta ricezione e visualizzazione di un messaggio di alert diffuso con la tecnologia Cell Broadcast presuppone che il terminale mobile possieda alcune caratteristiche legate al sottosistema Applications che consenta da parte dell'utente (cittadino) un facile accesso all'informazione.

La grande quantità di modelli commercializzati e la rapida evoluzione della tecnologia fa sì che la corretta ricezione di un messaggio di alert sia subordinata al soddisfacimento di una serie di requisiti che il terminale mobile deve soddisfare. Infatti solamente la possibilità di modificare alcune configurazioni consente la corretta ricezione di un messaggio di alert.

I requisiti minimi che un terminale mobile deve soddisfare per un facile uso della tecnologia a Cell Broadcast sono i seguenti:

- lo spegnimento del terminale mobile non deve modificare la configurazione del Cell Broadcast, ovvero la sua riaccensione non deve disabilitare la ricezione dei messaggi di alert sui canali attivati;
- l'accesso al menu di configurazione dei servizi di Cell Broadcast deve essere di facile accessibilità e utilizzo. Non dovrebbero essere presenti menu di attivazione specifici quali per esempio l'attivazione del canale 50 presente di default su molti terminali mobili;
- deve essere possibile associare al messaggio di alert un tono specifico che ne identifica la natura e lo distingue dagli altri messaggi comuni (es. SMS). L'utente deve essere inoltre in grado di poter scegliere quale tono associare al messaggio Cell Broadcast di alert;
- la configurazione dei comuni messaggi SMS (point to point messages) non deve interferire con la configurazione dei messaggi di Cell Broadcast;
- il terminale mobile deve essere in grado di visualizzare il messaggio di alert

- non appena ricevuto;
- facilità nel chiamare numeri telefonici o inviare SMS se il messaggio di alert prevede di contattare enti o autorità preposte alla gestione dell'emergenza (funzionalità evoluta);
- il messaggio di alert deve rimanere visualizzato sul display fino a quando non venga rimosso esplicitamente da parte dell'utente. Un messaggio di alert può essere sostituito solamente da un messaggio di alert successivo;
- la sequenza dei messaggi di alert deve essere conservata nella memoria del terminale mobile fino a quando l'utente non ne cancelli esplicitamente il contenuto o si sia raggiunto il numero massimo di messaggi ricevibili da un terminale mobile;
- deve essere disponibile lo scorrimento del testo del messaggio di alert nel caso in cui lo stesso non sia visualizzabile per intero sul display;
- il messaggio di alert deve essere visualizzato nel linguaggio selezionato dalla configurazione del terminale mobile;
- possibilità di raggiungere siti (URL) eventualmente citate nel messaggio di alert (funzionalità evoluta). L'URL deve essere disegnata per essere accessibile sia da terminali mobile di seconda (GPS) che di terza generazione (UMTS).

I requisiti di minima sopra elencati devono essere ulteriormente sviluppati e associati ad una indagine approfondita sulle modalità di funzionamento dei terminali mobili diffusi sul mercato. È necessario anche identificare il grado di copertura dei requisiti da parte dei terminali mobili per valutare il grado di raggiungibilità dei cittadini e l'efficacia nella diffusione di messaggi di alert e dei loro contenuti.

### *2.6.3. Indagine diffusione terminale mobile*

Al fine di analizzare lo scenario riguardo la predisposizione dei terminali mobili alla tecnologia di Cell Broadcast, si è proceduto a una indagine sulle modalità con le quali la parte applicativa è in grado di gestire la configurazione e l'abilitazione dei canali per la ricezione dei messaggi di alert.

L'indagine ha preso in considerazione i 20 modelli più diffusi sul mercato italiano alla data di luglio 2009. L'indagine si è limitata a verificare, attraverso la consultazione dei manuali utente di ogni modello considerato, la facilità di comprensione e di configurazione del Cell Broadcast. In particolare sono stati presi in considerazione i seguenti aspetti:

- esistenza nel manuale utente delle istruzioni per il settaggio del Cell Broadcast;
- modalità di scelta del canale;
- esistenza del settaggio del canale 50 (informazioni microcella);
- facilità nell'accesso all'applicazione di settaggio dei parametri di Cell Broadcast;
- usabilità dell'applicazione.

In considerazione della limitatezza del campione e dell'impossibilità di verificare su tutti i terminali mobili la chiarezza e la facilità e avendo avuto la possibilità di verificare il comportamento solamente su alcuni modelli, i risultati dell'indagine non possono essere considerati esaustivi e sufficientemente rappresentativi. In base alle evidenze emerse è comunque possibile trarre qualche conclusione su come approcciare il problema del settaggio del terminale mobile e di conseguenza la possibilità di raggiungere nella pratica il maggior numero possibile di cittadini.

Si ricorda che la tecnologia Cell Broadcast è disponibile sin dallo standard di seconda generazione (2G) e pertanto si considera presente su tutti i terminali mobili analizzati.

Nella Tabella 2.2 sono riportati i modelli più diffusi alla data dell'indagine con una sintesi delle caratteristiche tecniche relative agli standard che posseggono.

**Tabella 2.2 - Analisi della tecnologia sui modelli più diffusi**

Modello	Caratteristiche
Nokia 5800 XpressMusic	GPRS, EDGE, WCDMA, HSDPA, GSM - Quadri Band, WCDMA (UMTS) / GSM 850/900/1800/1900
Samsung SGH-F480	GPRS, EDGE, UMTS, HSDPA, GSM
LG KP500 Cookie	GPRS, EDGE, GSM -
Samsung SGH-D880 DuoS	GPRS, EDGE, USB, GSM -
Samsung S8300	GSM, UMTS, HSDPA
Nokia N73	WCDMA (UMTS) / GSM 850/900/1800/1900
Samsung SGH E250	GSM 900/1800/1900, GPRS, EDGE
Nokia N70	WCDMA (UMTS) / GSM 900/1800/1900
Samsung SGH-U700	GPRS, EDGE, HSDPA, USB, GSM, WCDMA (UMTS) / GSM 900/1800/1900
Samsung SGH-U600	GPRS, EDGE, USB, GSM
Apple iPhone 8 GB	GPRS, EDGE, GSM
Samsung SGH-E251	GPRS, USB, GSM
Nokia N78	GSM - WCDMA (UMTS) / GSM 850/900/1800/1900 -
Nokia E71	GSM, WCDMA (UMTS) / GSM 850/900/1800/1900
Nokia N96	GSM, WCDMA (UMTS) / GSM 850/900/1800/1900
Nokia E65	WCDMA (UMTS) / GSM 850/900/1800/1900 - 115 g
Nokia 5310 XpressMusic	GSM, GPRS, EDGE, HSCSD
Nokia 7100 Supernova	GPRS, EDGE, GSM
Nokia 3600 Slide	GPRS, EDGE, HSCSD, GSM 850/1900 (Dual Band)
Samsung GT S5230	GSM 850/900/1800/1900, GPRS, EDGE,

L'analisi dei manuali dei terminali mobili ha portato alle seguenti conclusioni:

- i manuali Nokia sono quelli che citano più esplicitamente e diffusamente il Cell Broadcast;
- i manuali Samsung citano raramente il Cell Broadcast anche se si suppone sia presente nel terminale mobile;
- la completezza del manuale è funzione del tipo di modello: più il terminale mobile è di fascia elevata maggiore è la completezza del manuale;
- i cellulari più evoluti (e quindi più costosi) posseggono una facilità e usabilità dell'interfaccia per l'accesso ai parametri di Cell Broadcast.

#### *2.6.4. Istruzioni di configurazione del Cell Broadcast*

Nel paragrafo sono riportati gli estratti dei manuali che riguardano le modalità di configurazione del Cell Broadcast e dalle quali sono ricavate le considerazioni fatte nel paragrafo precedente.

##### *Nokia 5800 Express Music*

Di seguito l'estratto del manuale utente.

#### **BOX 1**

**Selezionare Menu > Messaggi e scegliere Opzioni > Cell broadcast.**

La funzione Cell broadcast (servizio di rete) consente di ricevere dal proprio fornitore di servizi messaggi relativi a vari argomenti, ad esempio il meteo o il traffico. Per gli argomenti disponibili e i relativi numeri, rivolgersi al fornitore di servizi. Il servizio potrebbe non essere disponibile in tutte le regioni.

I messaggi Cell broadcast non possono essere ricevuti su reti UMTS. Le connessioni dati a pacchetto possono impedire la ricezione di messaggi Cell broadcast.

##### *Samsung SGH F480*

Il manuale non cita il Cell Broadcast e non è indicata nessuna istruzione per la sua configurazione. Non sono disponibili neppure indicazioni per la visualizzazione delle informazioni di microcella. Il terminale mobile è dichiarato essere compatibile GPRS, EDGE, UMTS, HSDPA, GSM.

##### *LG KP500 Cookie*

Il manuale non cita il Cell Broadcast e non è indicata nessuna istruzione per la sua configurazione. Non sono disponibili neppure indicazioni per la visualizzazione delle informazioni di microcella.

### *Samsung SGH-D880 DuoS*

Il manuale cita la possibilità di effettuare la configurazione dei Messaggi broadcast. La spiegazione si limita ad una sola frase in cui, tramite la voce “messaggi broadcast” è possibile modificare le impostazioni. Di seguito l’estratto del manuale utente.

#### BOX 2

Menu > Messaggi > Messaggi broadcast

Messaggi broadcast

Modificate le impostazioni per la ricezione dei messaggi broadcast.

### *Samsung S8300*

Il manuale non cita il Cell Broadcast e non è indicata nessuna istruzione per la sua configurazione. Non sono disponibili neppure indicazioni per la visualizzazione delle informazioni di microcella.

### *Nokia N73*

Possiede l’accesso tramite menu al settaggio dei parametri di Cell Broadcast che viene citato esplicitamente. Le istruzioni, anche se sintetiche, sono sufficientemente chiare. Si riporta di seguito il contenuto del manuale.

#### BOX 3

**Cell broadcast** (servizio di rete) consente di ricevere dal fornitore di servizi messaggi su diversi argomenti, ad esempio le condizioni atmosferiche o la situazione del traffico. Per gli argomenti disponibili e i relativi numeri, rivolgersi al fornitore di servizi. Nella vista principale di **Messaggi** selezionare **Opzioni > Cell broadcast**. La vista principale indicherà lo stato di un argomento, il numero e il nome dell'argomento e quell'argomento è stato contrassegnato per il completamento. Non è possibile ricevere messaggi Cell broadcast in reti UMTS. Una connessione GPRS potrebbe impedire la ricezione di messaggi Cell broadcast.

### *Samsung SGH E250*

Il manuale cita la possibilità di effettuare la configurazione dei Messaggi broadcast. La spiegazione si limita ad una sola frase in cui, tramite la voce “messaggi broadcast” è possibile modificare le impostazioni. Di seguito l’estratto del manuale utente.

#### BOX 4

Menu > Messaggi > Messaggi broadcast

Messaggi **broadcast**

Modificate le impostazioni per la ricezione dei messaggi broadcast.

#### *Nokia N70*

Possiede l'accesso tramite menu al settaggio dei parametri di Cell Broadcast che viene citato esplicitamente. Le istruzioni, anche se sintetiche, sono sufficientemente chiare. Si riporta di seguito il contenuto del manuale.

##### **BOX 5**

###### **Cell broadcast**

Verificare con il proprio fornitore di servizi gli argomenti disponibili e i relativi numeri, quindi selezionare

[Messaggi > Opzioni > Impostazioni > Cell broadcast](#)

per modificare le impostazioni.

[Ricezione](#) - Scegliere se ricevere messaggi Cell broadcast.

[Lingua - Tutte](#) consente di ricevere messaggi Cell broadcast in tutte le lingue supportate. Selezionare [consente di scegliere le lingue in cui ricevere i messaggi Cell broadcast](#). Se la lingua desiderata non è presente nell'elenco, selezionare [Altre](#).

[Rileva argomento - Impostando Rileva argomento > Attiva](#), verrà eseguita automaticamente la ricerca di nuovi numeri di argomenti da salvare senza nome nell'elenco degli argomenti. Selezionare [Disattiva](#) per non salvare automaticamente nuovi numeri di argomenti.

#### *Samsung SGH-U700*

Il manuale non cita il Cell Broadcast e non è indicata nessuna istruzione per la sua configurazione. Non sono disponibili neppure indicazioni per la visualizzazione delle informazioni di microcella.

#### *Samsung SGH-U600*

Il manuale non cita il Cell Broadcast e non è indicata nessuna istruzione per la sua configurazione. Non sono disponibili neppure indicazioni per la visualizzazione delle informazioni di microcella.

#### *Apple iPhone 8 GB*

Il manuale non cita il Cell Broadcast e non è indicata nessuna istruzione per la sua configurazione. Non sono disponibili neppure indicazioni per la visualizzazione delle informazioni di microcella.

#### *Samsung SGH-E251*

Il manuale non cita il Cell Broadcast e non è indicata nessuna istruzione per la sua configurazione. Non sono disponibili neppure indicazioni per la visualizzazione delle informazioni di microcella.

#### *Nokia N78*

Possiede l'accesso tramite menu al settaggio dei parametri di Cell Broadcast che viene citato esplicitamente. Le istruzioni, anche se sintetiche, sono più chiare rispetto ad altri manuali. Si riporta di seguito il contenuto del manuale.

## BOX 6

Messaggi contiene le seguenti cartelle:

- **Ricevuti** — I messaggi ricevuti, ad eccezione dei messaggi e-mail e Cell broadcast, vengono memorizzati in questa cartella

Cell broadcast (servizio di rete) consente di ricevere dal fornitore di servizi messaggi su diversi argomenti, ad esempio le condizioni atmosferiche o la situazione del traffico. Per gli argomenti disponibili e i relativi numeri, rivolgersi al fornitore di servizi. Nella vista principale di **Messaggi** selezionare **Opzioni > Cell broadcast**.

Non è possibile ricevere messaggi Cell broadcast in reti UMTS. Una connessione dati a pacchetto potrebbe impedire la ricezione di messaggi Cell broadcast.

Impostazioni Cell Broadcast

Per gli argomenti disponibili e i relativi numeri, rivolgersi al fornitore di servizi.

Premere, quindi selezionare **Messaggi > Opzioni > Impostazioni > Cell broadcast**.

Selezionare tra le seguenti opzioni:

- **Ricezione** — Scegliere se ricevere messaggi Cell broadcast.
- **Lingua** — Selezionare le lingue in cui si desidera ricevere i messaggi: **Tutte**, Selezionate o **Altre**.
- **Rileva argomento** — Scegliere se si desidera che venga eseguita la ricerca automatica di nuovi numeri di argomenti da salvare senza nome nell'elenco degli argomenti.

### *Nokia E71*

Possiede l'accesso tramite menu al settaggio dei parametri di Cell Broadcast che viene citato esplicitamente. Le istruzioni, anche se sintetiche, sono le più chiare tra i manuali analizzati. Si riporta di seguito il contenuto del manuale.



## **BOX 7**

### **Cell broadcast**

Selezionare [Menu > Comunicaz. > Messaggi > Opzioni > Cell broadcast](#).

Con il servizio di rete Cell broadcast, è possibile ricevere dal fornitore di servizi messaggi relativi a diversi argomenti, ad esempio le condizioni atmosferiche o la situazione del traffico in una determinata area geografica. Per gli argomenti disponibili e i relativi numeri, rivolgersi al fornitore di servizi. Non è possibile ricevere i messaggi Cell broadcast quando il dispositivo si trova in modalità SIM remota. Una connessione dati a pacchetto (GPRS) potrebbe impedire la ricezione di messaggi cell broadcast.

Non è possibile ricevere i messaggi cell broadcast sulle reti UMTS (3G).

Per ricevere messaggi Cell broadcast, è necessario attivare la ricezione di tali messaggi. [Selezionare Opzioni > Impostazioni > Ricezione > Attiva](#).

Per visualizzare i messaggi relativi a un argomento, selezionare l'argomento. Per ricevere messaggi relativi a un argomento, selezionare [Opzioni > Sottoscrivi](#).

Suggerimento: È possibile impostare alcuni argomenti come argomenti importanti. Mentre il dispositivo è in modalità standby, l'utente viene informato quando si riceve un messaggio relativo a un argomento importante. Selezionare un argomento, quindi [Opzioni > Seleziona](#).

Per aggiungere, modificare o eliminare argomenti, selezionare [Opzioni > Argomento](#)

### **Impostazioni cell broadcast**

Selezionare [Menu > Comunicaz. > Messaggi > Opzioni > Impostazioni > Cell broadcast](#).

Per ricevere i messaggi cell broadcast, selezionare [Ricezione > Attiva](#).

Per selezionare le lingue in cui si desidera ricevere i messaggi cell broadcast, selezionare [Lingua](#). Per visualizzare nuovi argomenti nell'elenco degli argomenti cell broadcast, selezionare [Rileva argomento > Attiva](#).

## **Nokia N96**

Possiede l'accesso tramite menu al settaggio dei parametri di Cell Broadcast che viene citato esplicitamente. Le istruzioni, anche se sintetiche, sono le più chiare tra i manuali analizzati. Si riporta di seguito il contenuto del manuale.

## **BOX 8**

Messaggi contiene le seguenti cartelle:

- **Ricevuti** — I messaggi ricevuti, ad eccezione dei messaggi e-mail e Cell broadcast, vengono memorizzati in questa cartella.

Cell broadcast (servizio di rete) consente di ricevere dal fornitore di servizi messaggi su diversi argomenti, ad esempio le condizioni atmosferiche o la situazione del traffico.

### **Impostazioni Cell Broadcast**

Per gli argomenti disponibili e i relativi numeri, rivolgersi al fornitore di servizi. Nella vista principale di Messaggi selezionare [Opzioni > Cell broadcast](#). Non è possibile ricevere messaggi Cell broadcast in reti UMTS. Una connessione dati a pacchetto potrebbe impedire la ricezione di messaggi Cell broadcast. Premere [Opzioni](#), quindi selezionare [Messaggi > Opzioni > Impostazioni > Cell broadcast](#).

Selezionare tra le seguenti opzioni:

- **Ricezione** — Scegliere se ricevere messaggi Cell broadcast.
- **Lingua** — Selezionare le lingue in cui si desidera ricevere i messaggi: [Tutte](#), Selezionate o [Altre](#).
- **Rileva argomento** — Scegliere se si desidera che venga eseguita la ricerca automatica di nuovi numeri di argomenti da salvare senza nome nell'elenco degli argomenti.

## **Nokia E65**

Possiede l'accesso tramite menu al settaggio dei parametri di Cell Broadcast che viene citato esplicitamente. Le istruzioni, anche se sintetiche, sono le più chiare e complete tra i manuali analizzati. Si riporta di seguito il contenuto del manuale.

## BOX 9

Con il servizio Cell broadcast, è possibile ricevere dal fornitore di servizi messaggi su diversi argomenti, ad esempio le condizioni atmosferiche o la situazione del traffico in una determinata area geografica. Per gli argomenti disponibili e i relativi numeri, rivolgersi al fornitore di servizi.

Non è possibile ricevere i messaggi cell broadcast sulle reti UMTS o quando il dispositivo si trova in [Modalità SIM remota](#). Una connessione dati a pacchetto (GPRS) potrebbe impedire la ricezione di messaggi cell broadcast. Selezionare [Menu > Messaggi > Opzioni > Cell broadcast](#). Per ricevere messaggi cell broadcast, è necessario attivare la ricezione di tali messaggi. Selezionare [Opzioni > Impostazioni > Ricezione > Attiva](#).

Per visualizzare i messaggi relativi a un argomento, scorrere fino all'argomento e premere il tasto di scorrimento.

Per ricevere messaggi relativi a un argomento, scorrere fino all'argomento, quindi selezionare [Opzioni > Sottoscrivi](#).

**Suggerimento:** È possibile impostare alcuni argomenti come argomenti importanti. Scorrere fino all'argomento e selezionare [Opzioni > Seleziona](#). Mentre il dispositivo è in modalità standby, l'utente viene informato quando si riceve un messaggio relativo a un argomento importante.

Per annullare la ricezione di messaggi cell broadcast, selezionare la lingua dei messaggi ricevuti e scegliere se si desidera rilevare automaticamente nuovi argomenti cell broadcast, quindi selezionare [Opzioni > Impostazioni](#).

Per aggiungere, modificare o eliminare argomenti, selezionare [Opzioni > Argomento](#) e, quindi, selezionare [Aggiungi manualm.](#), [Aggiungi da indice](#), [Modifica](#), [Elimina](#) o [Elimina tutti](#).

Per memorizzare un messaggio cell broadcast nella memoria del dispositivo, selezionare il messaggio e [Opzioni > Salva](#). È possibile memorizzare fino a 50 messaggi nella memoria del dispositivo.

Per trovare numeri e indirizzi che potrebbero essere contenuti nel messaggio cell broadcast, selezionare [Opzioni > Trova](#) e Numero di telefono, Indirizzo e-mail o Indirizzo Web. È possibile quindi effettuare chiamate e inviare messaggi, aprire le pagine del browser o creare preferiti o schede della rubrica.

Per eliminare un messaggio, premere il tasto di cancellazione.

### Impostazioni cell broadcast

Selezionare [Menu > Messaggi > Opzioni > Impostazioni > Cell broadcast](#).

Selezionare una delle seguenti opzioni:

- [Ricezione](#) — Selezionare Attiva per ricevere messaggi cell broadcast.
- [Lingua](#) — Selezionare le lingue in cui si desidera ricevere i messaggi cell broadcast.
- [Rileva argomento](#) — Selezionare Attiva per visualizzare nuovi argomenti nell'elenco degli argomenti cell broadcast.

### *Nokia 5310 XpressMusic*

Il manuale non cita espressamente il Cell Broadcast ma indica comunque la modalità di settaggio dei “Messaggi Info”, traduzione in italiano dell’espressione Cell Broadcast (non verificato sul cellulare).

#### **BOX 10**

È possibile ricevere messaggi su diversi argomenti dal fornitore di servizi (servizio di rete). Per ulteriori informazioni, rivolgersi all'operatore di rete.

Selezionare [Menu](#) > [Messaggi](#) > [Messaggi info](#), quindi una delle opzioni disponibili.

### *Nokia 7100 Supernova*

Il manuale non cita il Cell Broadcast e non è indicata nessuna istruzione per la sua configurazione. Contiene indicazioni per la visualizzazione delle informazioni di microcella.

#### **BOX 11**

[Info microcella](#) — Selezionare Attivo per configurare il dispositivo affinché segnali quando si trova in una rete cellulare basata sulla tecnologia MCN (Micro Cellular Network) e attivi la ricezione delle informazioni sulla microcella.

### *Nokia 3600 Slide*

Il manuale non cita espressamente il Cell Broadcast ma indica comunque la modalità di settaggio dei “Messaggi Info”, traduzione in italiano dell’espressione Cell Broadcast (non verificato sul cellulare).

#### **BOX 12**

È possibile ricevere messaggi su diversi argomenti dal fornitore di servizi (servizio di rete). Per ulteriori informazioni, rivolgersi all'operatore di rete.

Selezionare [Menu](#) > [Messaggi](#) > [Messaggi info](#), quindi una delle opzioni disponibili.

### *Samsung GT S5230*

Il manuale non cita il Cell Broadcast e non è indicata nessuna istruzione per la sua configurazione. Non sono disponibili neppure indicazioni per la visualizzazione delle informazioni di microcella.

## Capitolo 3

### *Casi di studio: introduzione e analisi delle applicazioni*

La necessità di sistemi di alert in grado di raggiungere il maggior numero di cittadini è diventata sempre più stringente a fronte di eventi catastrofici avvenuti negli ultimi anni. In particolare eventi di natura antropica quali l'attacco terroristico contro il WTC del 2001 o di natura calamitosa quali lo tsunami nell'Oceano Indiano nel 2004 hanno destato l'interesse dei governi verso nuove tecnologie per la diffusione di messaggi di allerta.

A fronte di questa esigenza, molte organizzazioni hanno promosso progetti di studio per l'applicazione di tecnologie legate alla telefonia mobile a nelle procedure di alerting alla popolazione: tra questi è possibile citare studi a livello internazionale, quali il progetto Cell@lert promosso dall'associazione non-profit Cellular Emergency Alert System Association (ceasa) e il progetto europeo CHORIST, o sistemi già in fase di realizzazione quali quello olandese (*nome*) o quello indiano o cinese oggetto del presente documento. Questi progetti si pongono come obiettivo lo studio e la realizzazione di sistemi di alerting pubblico basato sulla tecnologia di Cell Broadcast.

In molte realtà nazionali, quali Svizzera e Olanda, è già presente un sistema di alerting basato su tecnologie consolidate quali sirene o messaggi di allerta divulgati via radio o televisione. Questa tecnologia pone molti limiti a livello di diffusione e di interpretazione dei messaggi in quanto legata a regole o convenzioni locali o alla lingua. La tecnologia di Cell broadcasting supera questi limiti e dove presente, l'integrazione con sistemi di alerting già presenti permette di raggiungere la quasi totalità della popolazione interessata dall'evento calamitoso.

Nel maggio 2003 la Cina inizia ad utilizzare tale tecnologia per gestire l'allerta alla popolazione civile in seguito alla crisi originata dalla SARS. Nello stesso anno il Governo Olandese avvia un lungo processo di studio e implementazione del Cell Broadcast per la gestione delle situazioni di Emergenza nazionale, in collaborazione con i principali operatori telefonici presenti sul territorio. Il caso Olandese è probabilmente il primo vero caso di approccio multi operatore per un sistema di gestione delle emergenze a livello mondiale con tecnologia GSM CB, l'ambizioso obiettivo del Governo Olandese è quello riuscire a raggiungere la quasi totalità dei cittadini via telefono cellulare in modo istantaneo in situazioni potenzialmente a rischio per la popolazione.

Infatti nella maggior parte dei casi, l'approccio ad un sistema di alerting basato

su Cell Broadcast è affidato a un singolo operatore, che mette a disposizione la propria tecnologia per la realizzazione del sistema di alerting. Questo tipo di approccio, per quanto interessante, risulta essere molto limitato in quanto non in grado di raggiungere la maggior parte dei cittadini: questo approccio è infatti circoscritto a gruppi ristretti di utenza serviti dall'operatore che rende disponibile la tecnologia e non raggiunge gli utenti degli altri operatori di telefonia mobile presenti sul territorio.

L'approccio è comunque interessante in quanto può essere considerato come preliminare per un successivo studio di fattibilità allargato a tutti gli operatori di telefonia mobile presenti sul territorio.

In generale l'interesse per questa tecnologia cresce esponenzialmente a fronte di eventi catastrofici che coinvolgono parecchie persone difficilmente raggiungibili con i sistemi tradizionali. È il caso di catastrofi naturali come quelle avvenute in India, Giappone, Sri Lanka, Thailandia che hanno compreso l'insufficienza dei tradizionali sistemi di comunicazione alla popolazione a seguito di eventi catastrofici e di portata imprevedibile, ma è anche in caso dei più recenti avvenimenti terroristici o di natura antropica oggetto di studio e di interesse da parte di governi europei e degli USA.

In realtà, nonostante gli annunci e anticipazioni da parte degli organi di informazione sull'utilizzo della tecnologia CB, pochi sono i casi documentati e accessibili riguardo la realizzazione e l'utilizzo pratico di questa tecnologia. Ciò che emerge è che molti governi si stanno interessando o stanno approcciando la tecnologia CB a scopo di alerting. Ciò che appare evidente nei casi analizzati è che la realizzazione pratica di un sistema di comunicazione di questo tipo richiede particolare studio ed attenzione, oltre che il coinvolgimento attivo di tutti gli attori necessari per l'ottenimento del risultato finale quali unità di controllo del territorio, gli operatori di telefonia e la popolazione stessa.

### 3.1. Le applicazioni

Nei paragrafi successivi sono analizzate le caratteristiche peculiari della realizzazione e dell'approccio seguito per implementare sistemi di alerting alla popolazione basati sulla tecnologia Cell Broadcast adottate nei vari paesi che si stanno attrezzando con tale tecnologia.

In particolare sono presi in considerazione le applicazioni sviluppate in India, Giappone, Olanda e il più recente approccio adottato negli USA che si stanno orientando in modo molto deciso alla tecnologia Cell Broadcast.

Oltre gli aspetti puramente tecnologici e architetture, di cui si analizzeranno le caratteristiche principali, saranno evidenziate le differenti modalità di realizzazione e di interpretazione della tecnologia per la gestione efficace della messaggistica di alerting per la gestione delle emergenze.

Un'attenzione particolare è stata posta sul progetto di ricerca Europeo "CHORIST", che ha come obiettivo proprio quello di migliorare l'efficacia e la

tempistica degli interventi in ambito di protezione della popolazione in seguito a disastri naturali, incidenti industriali ed in generale nelle situazioni di emergenza, nell'ottica di migliorare la comunicazione con gli enti che presiedono alla sicurezza pubblica e proporre uno standard nella gestione della messaggistica di alerting.

### 3.2. Il Giappone

A fronte della particolare conformazione geologica a partire dal 2007, il governo Giapponese ha intrapreso un progetto nazionale per la realizzazione di un sistema di alerting rapido alla popolazione a seguito di eventi tellurici denominato *Earthquake Early Detection Warning system* (EEW).

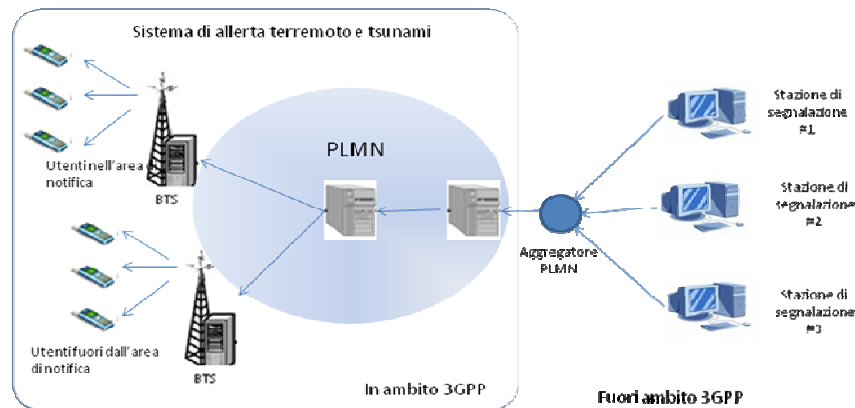
Caratteristica principale ed essenziale del sistema è la sua tempestività e diffusione tra la popolazione nell'invio delle informazioni, per poter gestire al meglio, piani di evacuazione secondo le indicazioni fornite con i messaggi di allerta.

#### 3.2.1. La tecnologia di riferimento

Da un punto di vista tecnico, le linee guida generali seguite dal governo Giapponese, ricalcano l'impostazione delle specifiche standard 3GPP 22.168 “Study for requirements for a Public Warning System”, che definiscono i requisiti sia dal punto di vista dell'utenza finale sia delle strutture di telefonia mobile che devono fornire il servizio di Cell Broadcast.

Nella Figura 3.1 è rappresentata l'architettura generale del sistema di alerting, mettendo in evidenza le caratteristiche e le funzionalità che devono essere fornite dal sistema di rilevamento dell'emergenza, rispetto a quelle che sono in carico al sistema di consegna dei messaggi informativi, delegate quindi alla rete degli operatori di telefonia che vengono descritte e dettagliate in ambito di standardizzazione dagli enti preposti ( 3GPP Group):

**Figura 3.1 - Architettura EEW**



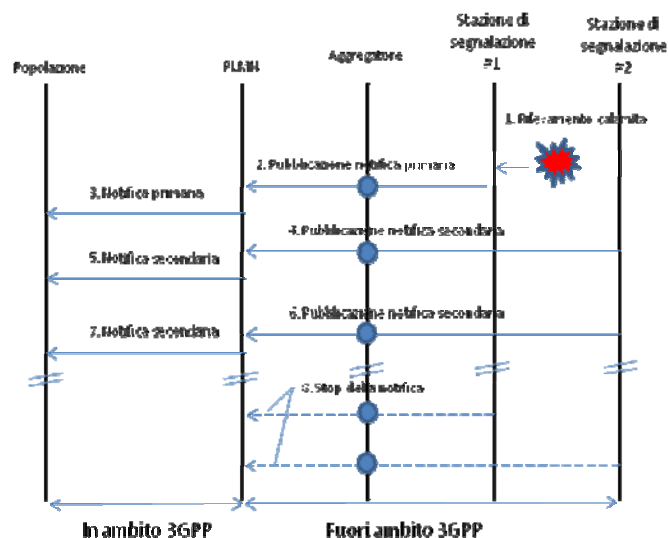
Le specifiche suggeriscono una distinzione della messaggistica di alert in due classi di messaggi, in funzione del contenuto dell'informazione stessa e dell'urgenza richiesta nella comunicazione. In base a questo vengono distinte *notifiche primarie* e *notifiche secondarie*.

Le notifiche primarie sono costituite dai messaggi che contengono informazioni più importanti ed urgenti e devono essere spedite con la massima rapidità dalla rete mobile degli operatori.

Le notifiche secondarie sono costituite dalle comunicazioni complementari alla comunicazione dell'evento calamitoso ed in generale sono fondamentali per coordinare le azioni di gestione dell'emergenza verso i cittadini. In questo senso il contenuto dei messaggi di tipo secondario, indica genericamente *istruzioni* ai cittadini su come comportarsi, dove e come spostarsi mentre l'emergenza precedentemente comunicata è ancora attiva.

Schematizzando possiamo descrivere il flusso dei messaggi in situazioni di emergenza secondo lo schema temporale di Figura 3.2.

**Figura 3.2 - Architettura EEW**





La sequenza delle operazioni è la seguente:

1. rilevamento di un evento che richieda lo stato di emergenza pubblica da parte delle strutture preposte al controllo del territorio;
2. comunicazione dell'emergenza tramite messaggio di tipo Notifica Primaria;
3. rapida diffusione del messaggio verso la popolazione interessata;
4. monitoraggio della situazione ed eventuale invio di Notifiche Secondarie;
5. diffusione di eventuali nuovi messaggi, se necessario con più ripetizioni;
6. sospensione dell'invio dei messaggi in caso di termine della situazione di alert.

### *3.2.2. La realizzazione della rete di alerting*

Sulla base delle specifiche dettate dallo standard citato, è stato realizzato in Giappone a cura di Ntt-DoCoMo (importante operatore di telefonia mobile a livello internazionale), un sistema di alerting basato su tecnologia Cell Broadcast.

Il progetto di ricerca è iniziato nel 2007 ed è stato messo a disposizione all'utenza nell'Aprile del 2009 con il nome di *Early Warning Area Mail*. Questo sistema utilizza la tecnologia Cell Broadcast realizzata sulla rete dell'operatore stesso con lo scopo di inviare informazioni ai cittadini presenti in aree colpite da calamità di origine sia naturale sia antropica.

La rete dell'operatore DOCOMO in Giappone utilizza la tecnologia i-mode (Information Mode) che è un protocollo utilizzato per l'interscambio di dati a pacchetto su piattaforme mobili, quali telefoni cellulari, videofonini e smartphone.

La tecnologia i-mode nasce nel 1999 da un'idea della stessa NTT DoCoMo, che la implementa per la rete giapponese di telefonia mobile.

A differenza del sistema WAP (Wireless Application Protocol) utilizzato in molti paesi (tra i quali anche l'Italia), che impiega il Wireless Markup Language (WML) per visualizzare le informazioni presenti sui siti WAP, i-mode utilizza una versione semplificata dell'HTML, denominata HTML (Compact HTML) e il protocollo HTTP per trasferire le informazioni, in modo rapido, dai content provider al terminale mobile degli utenti. Il servizio permette di visitare i siti realizzati appositamente e di usufruire di servizi come il mobile banking, consultare l'oroscopo, scaricare suonerie, giochi ecc.

In Giappone l'i-mode conta oltre 38 milioni di terminali abilitati e 8 milioni e mezzo di utenti abbonati paganti. I fornitori di contenuti sono oltre 6000 e molto ha pesato il modello remunerativo del revenue sharing con l'operatore mobile, che ha garantito ai content provider un ritorno economico significativo.

Questo contesto, nel quale si inseriscono come business anche aziende interessate più all'advertising (messaggi pubblicitari) che all'alerting, ha portato a un maggior sviluppo e diffusione della tecnologia di Cell Broadcast che è sicuramente più accessibile da parte degli utenti rispetto al contesto italiano.

Su questa tecnologia, Ntt-DoCoMo ha implementato un servizio di Cell Broadcast che non si limita ad inviare brevi messaggi di testo ma riesce a spedire vere e proprie e-mail direttamente agli utenti di telefonia mobile. In questo modo i

contenuti dei messaggi sono costituiti da un testo più ampio rispetto alle possibilità offerte dal servizio Cell Broadcast tradizionale, ed il contenuto informativo può essere meglio dettagliato e contenere informazioni più complete circa la segnalazione dell'emergenza e le azioni consigliate agli utenti finali.

Ntt-DoCoMo ha affidato all'Agenzia Meteorologica Giapponese il compito di intercettare e verificare le emergenze in corso. All'Agenzia fanno capo tutti i presidi di controllo nazionale e regionale e l'invio delle comunicazioni ai cittadini è coordinato in modo centralizzato. Ntt-DoCoMo ha dichiarato che a Marzo 2009, sono più di 18.000.000 gli utenti che utilizzano cellulari con funzionalità in grado di gestire le "area mail".

Ntt-DoCoMo non si è limitata ad organizzare ed implementare il servizio sugli apparati di rete installati in modo fisso sul territorio (esempio BTS). Il progetto ha previsto la realizzazione di una vera e propria flotta di veicoli mobili dotati di Base Station portatili in grado di intervenire quando richiesto, nelle zone colpite da situazioni calamitose e nelle quali non è più garantita la copertura da parte delle postazioni BTS.

Inoltre è stata predisposta una flotta di veicoli dotati di gruppi elettrogeni e di batterie per i terminali mobili, per garantire il servizio di alerting anche in caso di distruzione o di messa fuori uso delle apparecchiature fisse (es. BTS, BSC, MSC, ecc. riferimento alle generalità).

### 3.3. L'Olanda

La scelta di utilizzare il Cell Broadcasting per comunicare con i cittadini nelle situazioni di emergenza, è il frutto di una ricerca preliminare commissionata dallo stesso governo Olandese. Obiettivo della ricerca è quello di identificare nuove tecnologie per prevenire, allertare ed informare la popolazione nelle situazioni di crisi in caso di calamità.

La ricerca deve fornire la miglior tecnologia disponibile su larga scala e, allargando l'indagine alle persone diversamente abili quali persone non udenti o con gravi problemi di udito, verificarne il livello di raggiungibilità. Si precisa che l'Olanda è attualmente dotata di un sistema di alert basato su sirene che vengono attivate in caso di eventi calamitosi.

Le conclusioni della ricerca hanno portato a identificare il sistema di Cell Broadcast come la migliore soluzione per l'ottenimento degli obiettivi definiti.

A partire dal 2004, un consorzio di enti, composto da LogicaCMG, l'olandese BackStream e la fondazione (Olandese) "Platform Mobile Messaging", sono state incaricate dal ministro per gli Affari Economici per lo studio di un primo sistema di alerting basato sulla tecnologia Cell Broadcast, il progetto è stato interamente finanziato dal Governo Olandese. I cinque operatori di telefonia mobile, operanti in Olanda, si sono resi disponibili a partecipare al progetto, attivando il servizio anche nelle zone l'infrastruttura necessaria dove era presente, ma non ancora stata configurata.

Il territorio Olandese è stato suddiviso in 5000 aree, ognuna delle quali rappresenta una Cella e come tale raggiungibile da messaggi di Cell Broadcast. Le celle rappresentano la più piccola area indirizzabile, mentre un'area può essere composta da più celle identificabili come aree coperte da ogni singola BTS.

La caratteristica fondamentale dell'esperienza Olandese, è stata la decisione di iniziare adottando la tecnologia così come è, e di lavorare per approssimazioni successive, affinando le procedure e migliorandole laddove carenti.

A differenza di altri approcci, gli Olandesi non si sono chiesti se o come adattare la tecnologia alle loro esigenze ma hanno fatto il percorso contrario, utilizzando da subito la tecnologia disponibile, lavorando a posteriori di volta in volta sui dati e sui risultati ottenuti per migliorare la qualità del servizio erogato.

A questo proposito sono stati selezionati gruppi di utenti tipo per categoria e si è iniziato da subito a collezionare riscontri sul servizio erogato.

La lettura della documentazione reperibile in rete conferma questo approccio: a più riprese sono stati pubblicati i risultati dei vari livelli di verifica del servizio e si è lavorato progressivamente sulla tecnologia, migliorando il processo di informazione e formazione degli utenti "campione", o chiedendo una maggiore collaborazione e partecipazione degli operatori telefonici nell'ottica di far evolvere il servizio a livello di rete mobile, di aspetti propri della comunicazione, rivedendo la struttura dei singoli messaggi e perfezionando gli aspetti di rilevazione dei risultati ottenuti e studiando dei meccanismi di riscontro da parte degli utenti sempre più evoluti e attendibili.

I cittadini hanno partecipato attivamente all'introduzione della tecnologia: in prima battuta si è concesso ai cittadini di usare il proprio cellulare per l'effettuazione delle prove, delegando agli stessi anche la parte di configurazione del terminale mobile. Questo aspetto ha evidenziato alcune problematiche di configurazione di determinati terminali mobili, ma anche differenze di comportamento dei vari modelli presenti sul mercato.

I primi risultati ottenuti sono stati fondamentali per poter comprendere meglio le caratteristiche e gli aspetti da approfondire rispetto alla tecnologia: in una fase successiva ci si è concentrati sugli aspetti di funzionamento della rete.

A questo scopo sono stati consegnati ai cittadini coinvolti, cellulari prescelti e configurati dalle autorità, apparecchi che sono successivamente stati donati agli utenti campione.

In questo modo, una volta stabilito che era necessario occuparsi anche degli aspetti di configurazione dei terminali mobili, ci si è potuti concentrare sugli aspetti di funzionamento della rete in quanto tale, occupandosi delle modalità di comunicare e sui dati relativi alla percentuale di popolazione raggiungibile.

I risultati raggiunti nelle indagini olandesi, hanno dimostrato che la percentuale di popolazione raggiunta tramite servizio Cell Broadcast è molto alta (compresa tra l'80% e il 94% degli utenti). I problemi tecnici trovati possono essere risolti in breve tempo, la rete degli operatori ha funzionato in base alle aspettative, e anche la configurazione dei mobili per la ricezione dei messaggi Cell Broadcast non si è rivelato essere un ostacolo insormontabile, sebbene in alcuni casi, l'invio di messaggi lunghi ha dato qualche problema su alcuni terminali.

Le conclusioni del Governo Olandese indicano il Cell Broadcast come lo

strumento più adatto ad affiancare i classici sistemi di alert (sirena), nelle situazioni di allerta alla popolazione, oltre a esser uno strumento decisamente apprezzato dai cittadini.

La fase di implementazione vera e propria doveva essere portata comunque avanti in molto attento: il sistema si è rivelato complesso, sia da un punto di vista tecnico, sia per quanto riguarda la messa in funzione della struttura organizzativa necessaria per il suo supporto.

Nel momento in cui i punti critici del sistema sono stati individuati attraverso una sperimentazione concreta e di conseguenza risolti in modo adeguato, il Cell Broadcast risulta essere lo strumento più adatto per gestire le situazioni di alert verso la popolazione.

Il punto di maggior difficoltà da superare per poter riuscire ad introdurre la tecnologia di Cell Broadcast come strumento di comunicazione, è riuscire a coinvolgere i cittadini e portarli ad usare la tecnologia come normale strumento di comunicazione anche al di fuori della specifica emergenza.

Nei paragrafi che seguono sono riportati alcuni contenuti della relazione fatta dalla “Delf University of technology” (NL - maggio 2008), dopo due anni di lavoro condotti sulla tecnologia in esame: la relazione presenta i principali risultati ottenuti nelle varie fasi di verifica sul campo del servizio.

La relazione è incentrata sull’analisi dei risultati ottenuti rispetto ai quattro temi fondamentali che sono stati analizzati dall’esperienza Olandese:

- Raggiungibilità: ovvero quanto la tecnologia è efficace nel raggiungere la popolazione.
- Accettazione: come viene percepito il nuovo servizio offerto da parte dei cittadini ma anche come la nuova tecnologia è accettata da parte degli amministratori che la dovranno gestire.
- Tecnologia: a quale livello di affidabilità si pone la tecnologia e quanto sia disponibile sul campo, dal punto di vista dell’infrastruttura di rete (operatori) e dal punto di vista terminali mobili.
- Contenuti: come deve essere impostato un messaggio Cell Broadcast, quale deve essere la sua struttura e quali i suoi contenuti per poter dare indicazioni precise, non interpretabili ed utili ai cittadini, ottenendo il comportamento desiderato in situazione di emergenza.

Un’ultima nota introduttiva riguarda le modalità di realizzazione delle diverse fasi del progetto. In questo senso è interessante evidenziare come l’approccio seguito nella realizzazione sia stato di tipo incrementale, questo ha portato a sviluppare la ricerca in due diversi passi successivi.

Il primo passo ha utilizzato una logica di “best effort” (BE), vale a dire si è cercato di realizzare un primo prototipo dell’infrastruttura tecnologica essenziale, in tempi brevi e con costi ed investimenti minimi, per verificare la fattibilità generale del progetto per migliorarne successivamente i punti critici, affinando di volta in volta gli aspetti tecnologici di comunicazione.

Il secondo passo, chiamato “increased vigilanc” (IV), ci si è concentrati sugli

aspetti di maggior interesse che hanno dimostrato qualche criticità nel primo passo, ottenendo dati significativi e mirati. Questo ha portato alla realizzazione di un primo scenario tecnologico sicuramente funzionante, ma con dei limiti per quanto riguarda in particolare la capillarità del servizio e la sua affidabilità nel lungo periodo. Nella sua ultima fase (2007), per quanto riguarda l'infrastruttura, si è deciso di concentrarsi su un unico operatore telefonico, in modo da poter meglio verificare gli aspetti di vigilanza sull'attendibilità del servizio stesso.

### *3.3.1. Raggiungibilità*

Per misurare il grado di raggiungibilità della popolazione è stato chiesto al gruppo di cittadini che ha partecipato alla verifica della tecnologia, di configurare il proprio terminale mobile secondo le indicazioni fornite, abilitando opportunamente le funzionalità di Cell Broadcast sullo stesso.

Le modalità del test prevedevano l'invio casuale di messaggi di Cell Broadcast da parte delle autorità che gestivano il servizio in momenti non definiti e ai cittadini stessi è stato chiesto di confermare la ricezione dei messaggi inviando gratuitamente un messaggio di risposta ad un numero prestabilito. Nella risposta i cittadini dovevano inserire alcune informazioni contenute nei messaggi ricevuti.

I dati sulla raggiungibilità sono stati ricavati dai ricercatori registrando il numero di risposte ai messaggi di Cell Broadcast correttamente inviate. Oltre a questo i ricercatori hanno inoltre provveduto a campionare una serie di dati contattando direttamente i cittadini che non avevano risposto direttamente al messaggio Cell Broadcast in modo da ovviare alla 'svogliatezza di alcuni utenti poco sensibili alle finalità del test.

La verifica ha avuto come oggetto i seguenti aspetti:

- corretta spedizione del messaggio da parte della rete;
- corretta ricezione del messaggio da parte del terminale mobile;
- lettura del messaggio da parte del cittadino;
- risposta con contenuto appropriato da parte del cittadino.

Nel caso in cui la risposta a tutti i quesiti fosse stata positiva, il messaggio doveva essere considerato andato a "buon fine".

Il fallimento di uno qualsiasi dei quattro punti è stato considerato come obiettivo non raggiunto e quindi non se ne è tenuto conto in fase di calcolo delle percentuali di successo.

Nella prima fase del test, utilizzando l'approccio di tipo Best Effort (BE), la catena dei quattro punti precedenti è stata interrotta spesso a causa della inaffidabilità iniziale della infrastruttura tecnologica, e questo ha portato a dei risultati di raggiungibilità poco soddisfacenti da un lato, ma anche ad evidenziare, e quindi affrontare e risolvere aspetti fondamentali sull'impostazione della rete.

I dati principali ricavati per quanto concerne la raggiungibilità del servizio sono sintetizzabili come segue.

Con l'approccio BE, e utilizzando i terminali mobili degli utenti sono stati

raggiunti tra lo 0% e il 29% dei cittadini. In particolare, lo 0% dei cittadini è stato raggiunto nelle situazioni in cui il problema dell'infrastruttura ha inibito completamente la spedizione dei messaggi stessi.

Risolvendo i problemi dal punto di vista tecnico legati alla rete degli operatori, e considerando le situazioni in cui gli utenti sono riusciti effettivamente a configurare adeguatamente il proprio terminale, le percentuali di raggiungibilità del servizio (rispetto di tutti e quattro i punti precedenti), si sono collocate tra il 25% e il 51%, sempre considerando il primo approccio Best Effort.

Passando all'approccio più attento ed evoluto di tipo Increased Vigilance per quanto riguarda gli aspetti di infrastruttura, utilizzando un modello unico di terminale, per eludere qualsiasi problema iniziale di configurazione dello stesso ed utilizzando una sola pagina di testo nei messaggi di Cell Broadcast (utilizzando quindi un massimo di 93 caratteri per il contenuto del testo), le percentuali sono salite tra il 72% e l'88% del campione di cittadini coinvolti. Nelle stesse condizioni, ma utilizzando l'invio di più pagine di testo (spedizione di più di 93 caratteri), le percentuali scendono ancora tra il 32% e il 43%.

Questo fenomeno è dovuto in parte alla poca familiarità nella gestione di questi messaggi sui terminali mobili e in parte al comportamento spesso poco esplicito nella visualizzazione degli stessi messaggi da parte del terminale mobile.

Utilizzando gli accorgimenti di Increased Vigilance su tutta la catena di comunicazione, e non solo per quanto riguarda il controllo dell'infrastruttura, le percentuali di raggiungimento dei terminali salgono tra l'86% e il 94%.

Per quanto riguarda il comportamento degli utenti campione, è possibile evidenziare come circa il 37% delle persone contattate ha risposto entro i sette minuti successivi all'invio del messaggio. Entro le due ore dall'invio del messaggio la percentuale delle risposte ricevute sale al 76%. Considerando la situazione con Increased Vigilance, le percentuali diventano il 52% di risposte entro i primi 7 minuti dall'invio del messaggio e l'82% di risposte ricevute entro le due ore dall'invio.

È stato evidenziato anche che le risposte che non sono mai arrivate sono principalmente dovute al fatto che le persone hanno ricevuto il messaggio in momenti poco opportuni e che quindi non hanno potuto rispondere in tempi accettabili. Altri motivi per giustificare la mancata risposta sono stati l'aver cancellato troppo presto il messaggio senza averlo letto, principalmente per distrazione o per poca praticata nel gestire il terminale.

Si è pertanto concluso che la raggiungibilità dei cittadini dipende non solo dal funzionamento dell'infrastruttura e dalla corretta configurazione e funzionamento del terminale ma anche il modo con cui le persone utilizzano il loro terminale.

Anzitutto i messaggi possono essere letti solo nel momento in cui le persone hanno con sé il cellulare. In questo caso la raggiungibilità è risultata diversa nelle diverse ore del giorno, ma anche in giorni diversi, a seconda se lavorativi, fine settimana o vacanze. Il 12% dei partecipanti al test ha dichiarato che spegne sistematicamente il telefonino durante le ore notturne, e il 28% degli stessi ha dichiarato che il telefono non viene portato in camera da letto durante la notte: solo il 44% delle persone ha dichiarato di avere il terminale a portata di mano sempre nelle ore notturne.

Nei test pratici tra i partecipanti che hanno usato il proprio apparecchio, gli ultra 65enni hanno risposto mediamente meno spesso rispetto ai loro colleghi di test più giovani mentre nei casi in cui è stato fornito loro un apparecchio opportunamente configurato, non è stata riscontrata alcuna significativa differenza in termini di numero di risposte se i messaggi Cell Broadcast sono composti da un'unica pagina informativa. Più difficile è stata invece la gestione di questa categoria di persone, per quanto riguarda i messaggi composti da più pagine, in questi casi le risposte sono state più lente rispetto a quelle degli altri colleghi più giovani. Uomini e donne hanno risposto in modo simile, senza particolari differenze in termini di tempistiche e quantità di risposte.

La raggiungibilità delle persone che si trovano presso i confini dell'area di broadcast è stata oggetto di un'analisi specifica. Quanto emerso è riconducibile al fatto che le zone di confine di un'area non garantiscono i risultati che ci si aspetterebbe. In alcuni casi, le persone situate entro l'area di broadcast, in prossimità dei suoi confini non hanno mai ricevuto il messaggio. Viceversa, si sono verificate situazioni in cui persone che stazionavano oltre i confini dell'area prescelta, hanno ricevuto ugualmente il messaggio, anche se non indirizzato a loro in modo specifico. I risultati hanno dimostrato che la scelta e la gestione delle aree deve essere fatta in modo molto più attento, e in generale è preferibile evitare la scelta di aree troppo piccole specie se situate in zone geografiche complesse da un punto di vista territoriale.

### *3.3.2. Accettazione*

Le valutazioni sul grado di accettazione del servizio proposto sono state fatte su due fronti: accettazione da parte dei cittadini da una parte e accettazione da parte degli amministratori dall'altra.

#### *I Cittadini*

Per quanto riguarda l'apprezzamento da parte dei cittadini della nuova tecnologia, si è proceduto facendo interviste ad hoc alle persone coinvolte nella fase di test sia prima sia dopo le prove sul campo. I risultati indicano che il gradimento del servizio è molto alto da parte degli utenti. I cittadini hanno espresso parecchie aspettative dal sistema proposto e paradossalmente questo potrebbe essere un problema nella fase iniziale del servizio nel momento in cui le aspettative non dovessero essere rispettate, specie nella fase di normale tuning del servizio stesso, in cui ci si aspetta qualche disservizio da ricondurre a problemi "di gioventù" della tecnologia.

D'altra parte le aspettative dei cittadini devono essere sfruttate per renderli partecipi ed attivi nell'applicazione corretta della tecnologia. I cellulari devono essere correttamente configurati, e tenuti con se sempre e accesi.

Le prove hanno dimostrato che tra i cittadini con un minimo di esperienza nella gestione della tecnologia in questione, l'80% (BE) e il 94% (IV) dei partecipanti hanno confermato la validità del nuovo servizio in affiancamento al sistema delle sirene. Una percentuale degli intervistati (tra il 9% e il 24%) ha ipotizzato la

possibilità di rimpiazzare completamente il sistema di sirene con il servizio di Cell Broadcast. Nonostante ciò in generale, le aspettative iniziali dei partecipanti sono state in qualche modo ridimensionate, e questo fornisce una misura della difficoltà del percorso da compiere per raggiungere la fruibilità del servizio.

In generale si è constatato che gli aspetti tecnologici del nuovo servizio non sono ancora sufficientemente chiari a tutti gli utenti, che spesso hanno confuso i messaggi Cell Broadcast con semplici SMS, perdendo in qualche modo l'importanza della gestione delle tempistiche nella visualizzazione e nei tempi di risposta richiesti dal test.

#### *Le Amministrazioni*

Per capire il grado di accettazione del nuovo servizio dal punto di vista delle persone coinvolte nell'amministrazione del paese, sono stati coinvolti nelle varie fasi di test alcuni sindaci e rappresentanti pubblici. Le opinioni variano da persona a persona intervistata in funzione della percezione personale circa la scelta di usare il Cell Broadcast.

La definizione delle caratteristiche tecniche del servizio e della sua realizzazione sono ancora da definire al meglio. Questo aspetto porta molti intervistati a non sbilanciarsi e a non prendere posizioni chiare rispetto al grado di accettazione del servizio stesso.

Una preoccupazione fondamentale degli intervistati è quella di inserire le procedure di allerta via Cell Broadcast, non come modalità separata di comunicazione ai cittadini, ma integrandole completamente con le attuali vigenti procedure di gestione delle emergenze. Inoltre l'uso della nuova tecnologia deve essere accompagnato da un'attività precisa di monitoraggio della copertura e mappatura della rete telefonica mobile, in particolare il sistema deve essere monitorato almeno inizialmente nelle situazioni in cui la crisi è in atto, in modo da verificare e garantire la copertura cellulare richiesta in ogni situazione.

#### *3.3.3. Tecnologia*

Come anticipato, l'approccio seguito inizialmente per quanto riguarda l'infrastruttura è stato di tipo Best Effort.

Questa soluzione ha consentito di portare avanti il progetto di ricerca nelle sue fasi iniziali in modo snello e veloce impostando e testando i principi generali della tecnologia, ma si è rivelato limitato nel momento in cui si è iniziato a lavorare sui dati raccolti, in quanto non più idoneo a garantire la prestazione che il sistema richiedeva in fase avanzata di analisi.

Nella seconda fase del progetto di test (2007) si è deciso di scegliere un unico interlocutore tra gli operatori di telefonia e di concentrarsi sulla qualità del servizio erogato lavorando su sistemi di riscontro dell'effettiva, corretta e completa spedizione dei messaggi e per instaurare un'intensa collaborazione tra gli enti preposti dal governo e i referenti dell'operatore di telefonia mobile.

I risultati ottenuti con questa scelta sono stati decisamente interessanti e questo ha consentito di focalizzare l'attenzione sugli altri aspetti della catena di



comunicazione. Nella fase conclusiva della ricerca, i dati relativi alle prestazioni della rete, sebbene limitatamente all'unico operatore partner, sono stati decisamente confortanti e il servizio è stato garantito globalmente nelle sue prestazioni sia in termini di affidabilità che in termini di tempistica nella distribuzione dei messaggi.

Oltre gli aspetti di fruibilità del servizio strettamente legati agli operatori, si è cercato di migliorare durante le fasi di test anche gli aspetti di disponibilità e configurazione del servizio da un punto di vista dei terminali mobili. Inizialmente molti utenti hanno deciso di utilizzare il proprio cellulare.

Questo ha portato ad scontrarsi con una serie di problemi che rischiavano di spostare l'attenzione non tanto al servizio in sé ma ad aspetti collegati. I problemi principali legati all'uso di tanti apparecchi diversi sono stati da una parte la configurazione dei singoli apparati, non sempre chiara nei manuali utente e non sempre facile da realizzare, ma in particolare ha evidenziato talvolta problemi nella ricezione dei messaggi di Cell Broadcast, quasi sempre legati all'invio di testo su più pagine di messaggio (nelle prove effettuate i messaggi di testo non erano sempre limitati alla spedizione di una singola pagina, ovvero 93 caratteri, ma spesso sono state usate più pagine per descrivere le situazioni di alert). Oltre a ciò sono stati riscontrati problemi specifici di perdita delle impostazioni del mobile a seguito di un reinserimento della SIM card su certi apparecchi o difficoltà nell'impostare correttamente il tono di avviso che notifica il ricevimento di un messaggio.

Sebbene meno realistico come scenario, si è deciso di utilizzare nella fase avanzata del progetto, un unico modello di terminale mobile, opportunamente configurato in modo da potersi concentrare sugli aspetti di raccolta dati del servizio da parte degli utenti e sui problemi dell'infrastruttura, elementi fondamentali per gli scopi della ricerca condotta.

Riassumendo i risultati per quanto riguarda gli aspetti di terminale mobile la ricerca olandese ha ricavato i seguenti dati:

- circa l'80% dei partecipanti è riuscito a configurare correttamente il proprio terminale per ricevere i messaggi Cell Broadcast;
- il problema della ricezione di messaggi composti da più di una pagina è abbastanza generalizzato, e si presenta indifferentemente sia su modelli di cellulari recenti che su modelli più vecchi;
- in alcuni casi (circa il 10% degli intervistati) il terminale ha perso almeno in parte le impostazioni di configurazione in seguito a normali operazioni (spegnimento, cambio SIM etc);
- in alcuni casi il ricevimento del messaggio di Cell Broadcast non è adeguatamente segnalato dal terminale, per assenza totale di avviso acustico o per limitata gamma di toni difficilmente identificabili.

### *3.3.4. I contenuti*

La possibilità di comunicare con i cittadini via messaggio di testo è uno strumento innovativo nelle mani degli enti preposti alla gestione delle situazioni di crisi.

L'uso di Cell Broadcast consente di fornire informazioni concrete per quanto riguarda le azioni da compiere e cosa evitare di fare in situazioni critiche. La conseguenza di ciò è che la fornitura di informazioni durante situazioni di crisi è più diretta rispetto al classico utilizzo di sirene.

Proprio per questo motivo nel messaggio spedito, oltre ad essere indicata la zona impattata dall'evento, ci si può e deve concentrare sulle azioni da intraprendere. Il messaggio Cell Broadcast è risultato essere più efficace se il testo contenuto è breve, meglio se viene utilizzato un formato in stile telegramma, con le indicazioni di data e ora dell'invio dell'emergenza. La possibilità di impostare il terminale in modo da poter chiaramente distinguere il tono di ricezione del messaggio di Cell Broadcast è una funzionalità che sarebbe particolarmente utile e che non è ad oggi disponibile su tutti i terminali mobili.

## 3.4. Gli Stati Uniti d'America

La ricerca sulla diffusione dei messaggi di alerting negli Stati Uniti parte dalla firma del il Presidente degli Stati Uniti d'America del cosiddetto Security and Accountability For Every Port (SAFE Port) Act, legge che stabilisce nuove regole e condizioni per la sicurezza negli USA, in data 13 Ottobre 2006.

Nel documento, è contenuta una sezione chiamata "Warning Alert and Response Network" riferito come "WARN Act", con l'obiettivo di identificare e definire un nuovo canale per la comunicazione di messaggi di alert verso la popolazione. Il WARN Act, nasce con l'obiettivo di supportare la trasmissione wireless delle informazioni nei casi di pubblica emergenza tramite le reti degli operatori di telefonia, che veicolano verso gli utenti finali messaggi riguardanti situazioni di attacco terroristico, calamità naturali ed in generale in caso di eventi pericolosi per la popolazione.

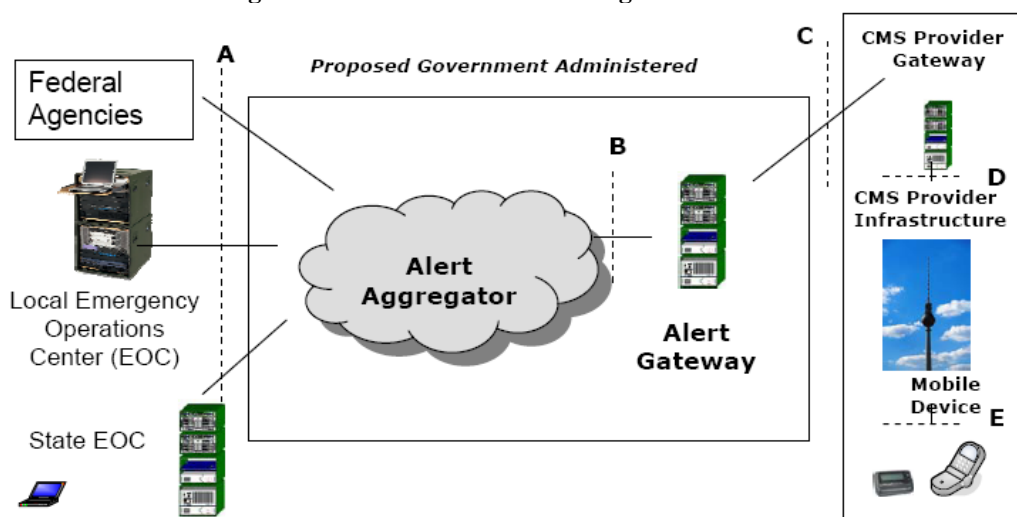
Il progetto nasce con il coinvolgimento diretto e attivo degli operatori telefonici interessati: infatti, per la valutazione del sistema migliore a scopi di alert, viene costituito ad opera della Commissione delle Comunicazioni Federali degli stati uniti (FCC) un comitato apposito denominato Commercial Mobile Service Alerts Advisory Committee (CMSAAC), con lo scopo di studiare e valutare le raccomandazioni tecniche e i sistemi più adatti per il supporto delle comunicazioni wireless nei casi di alert in situazioni di emergenza pubblica. Il comitato CMSAAC identificava nella tecnologia Cell Broadcast l'unica applicabile al contesto di riferimento nei casi di allerta wireless in situazione di emergenza.

In Figura è riportato lo schema architetturale della soluzione impostata dal Governo Americano. Tale schema si evidenzia che il flusso delle informazioni

transita da un insieme di centri di controllo sparsi sul territorio, dedicati alla raccolta degli stati di emergenza di varia natura (principalmente meteo, terrorismo, eventi naturali, chimici e emergenze minori, ecc.), verso un centro che funge da aggregatore e gestore degli alert individuati.

L'informazione passa (interfaccia A) dalle agenzie federali che rilevano l'evento ad un 'Alert Agregator' (centro B), centro che informa direttamente al governo federale degli Stati Uniti. Compito dell'Alert Agregator è quello di filtrare e di validare le informazioni ricevute. Quando l'alert è stato validato, il centro ha la possibilità, tramite un "Alert Gateway", di inviare i messaggi di alert ai vari gateway CMS dei singoli operatori (interfaccia C) che provvedono all'invio dell'informazione verso le celle indicate (elemento D) e quindi ai terminali mobili presenti sul territorio (elemento E).

**Figura 3.3 - Architettura di alerting USA**



Il progetto denominato CMAS, Commercial Mobile Alert System, nasce dunque con l'obiettivo di consentire alla Federal Emergency Management Agency (FEMA), di filtrare e divulgare informazioni originate da fonti sicure e accreditate, quali la Casa Bianca, il servizio meteorologico nazionale e gli uffici della protezione civile locali, rendendo possibile la spedizione dei messaggi verso interfacce sicure degli operatori di telefonia.

Gli operatori che hanno voluto aderire al progetto volontariamente, dovranno iniziare a sviluppare e testare da una parte i sistemi per connettersi al FEMA per ricevere le informazioni da spedire agli utenti e dall'altra la parte di rete per verificare che la trasmissione avviene secondo quanto previsto dallo standard.

#### *3.4.1. La scelta tecnologica*

Da un punto di vista tecnologico, l'approccio americano è decisamente originale sia rispetto ad altre scelte europee che rispetto ad altre implementazioni a livello



Un altro aspetto peculiare dell'approccio Americano è quello di essersi occupato di entrare nel merito dell'implementazione dell'applicazione Cell Broadcast a livello di ogni singolo operatore, indicando e 'suggerendo' alcuni punti fondamentali da soddisfare che non erano definiti univocamente a livello di Standard 3GPP e che lasciavano spazio ad interpretazioni e implementazioni diverse e che non sempre andavano nella direzione desiderata.

In questo senso sono state richieste caratteristiche di implementazione che prevedessero funzionalità specifiche (DRX transmission mode, identificazione flessibile delle celle referenziate dai singoli operatori, connessione con CBC implementata obbligatoriamente via TCP/IP et altro) dettagli che sicuramente esulano dalla trattazione di questa ricerca, ma che rivelano il livello di accuratezza e di dettaglio dell'analisi portata avanti in ottica CMAS e l'interesse che il governo Americano sta dedicando a questo tipo di progetto.

### 3.5. India

Il Cell Broadcast può e deve essere visto anche come servizio di broadcast di informazioni, a prescindere da finalità di alerting in contesti di protezione civile.

Ne è un interessante esempio l'esperienza maturata in India su un'idea dell'inglese Celltick che tramite gli operatori affiliati al gruppo Hutchinson in India, hanno realizzato un sistema di comunicazione agli utenti della rete basato sul Cell Broadcast. I contenuti inviati agli utenti spaziano nei vari campi dell'informazione, ultime notizie, intrattenimento, divertimento, astrologia ed altri.

In pratica vengono mandati agli utenti, via Cell Broadcast, singoli messaggi tematici fungono da "titolo", da richiamo per gli utenti che se lo desiderano, possono approfondire l'argomento o la notizia, accedendo ad un menu personalizzato, che gli permette una vera e propria navigazione nei contenuti vari via cellulare mobile.

Questo servizio è stato realizzando sviluppando opportuni applicativi, che vengono inseriti direttamente nelle SIM-Card rilasciate dagli stessi operatori. Ci si riferisce ad un contesto molto particolare, e decisamente diverso rispetto agli esempi visti in precedenza, ma che ci consente di vedere i servizi e la tecnologia Cell Broadcast da un altro punto di vista, molto meno 'standard' nei suoi impieghi, ma interessante da un punto di vista di appeal dei servizi che si posso realizzare e degli sviluppi tecnologici che ci posso essere intorno alle funzionalità di base.

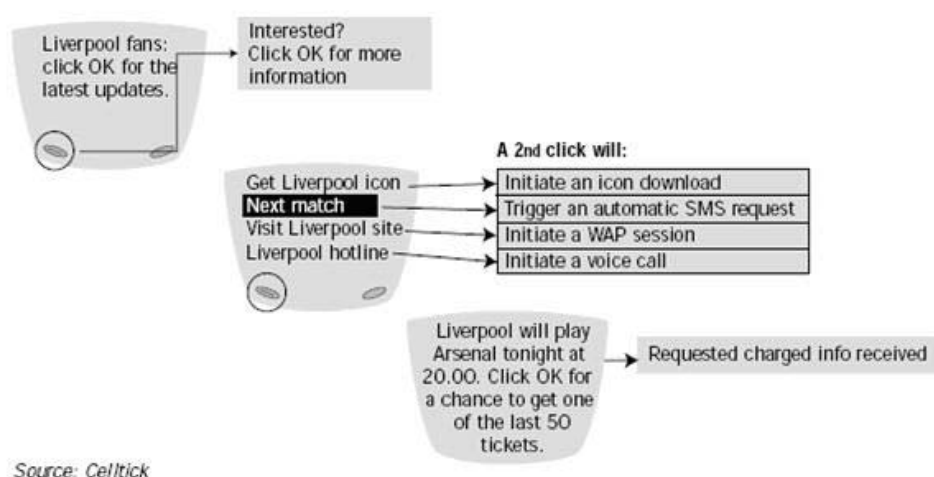
Gli utenti ricevono via Cell Broadcast i contenuti generici inviati dal gestore della rete in modo gratuito. In seguito posso selezionare direttamente da monitor del Terminale mobile il contenuto di interesse, accedendo alle informazioni non più via Cell Broadcast ma tramite meccanismi di trasferimento dati che possono essere via SMS, WAP o voce.

Il sistema è stato realizzato attraverso lo sviluppo di applicativi specifici, che

vengono preinstallati sulle SIM degli operatori e che consentono un altissimo livello di personalizzazione delle funzionalità degli apparecchi mobili. In realtà la soluzione tecnologica realizzata da Celltick, consente alla rete mobile di parlare direttamente con la SIM piuttosto che col terminale mobile. La SIM stessa ha un chip interno evoluto che consente di eseguire gli applicativi personalizzati realizzati ad hoc per l'operatore specifico. In questo modo è possibile la realizzazione non solo di servizi personalizzati, ma anche di interfacce utente molto sofisticate e di facile utilizzo, realizzando menu interattivi molto efficaci.

Lo schema generale di funzionamento del servizio è descritto nella seguente Figura 3.5.

**Figura 3.5 - Schema di funzionamento del servizio Celltick**



Source: Celltick

Fonte: Celltick sa

Le ragioni che hanno portato allo studio di un'architettura così sofisticata ed articolata, sono in realtà molto semplici. Il Cell Broadcast non è mai stato adottato come servizio da parte degli operatori, in quanto non si è riscontrati vantaggi economici. Gli operatori hanno da sempre preferito puntare sui più noti e familiari servizi di SMS. Con gli SMS gli operatori telefonici, danno la sensazione di essere 'vicini' al singolo utente in prima persona ed in modo diretto.

Il messaggio, è percepito come contatto diretto e personale, che gioca un ruolo importante da un punto di vista delle relazioni e dell'immagine l'operatore fornisce, senza trascurare il fatto che implementando servizi interattivi via SMS, l'interazione dell'utente con la rete avviene via SMS e il costo dei servizi è facilmente recuperabile.

Con la soluzione introdotta in India dal gruppo Hutchinson, il problema della tariffazione dei servizi via Cell Broadcast è stato risolto creando un insieme di servizi interattivi ed accattivanti per gli utenti finali. Gli utenti da una parte vengono invogliati ad accedere all'ampio insieme di contenuti via Cell Broadcast, dall'altro ogni volta che intendono accedere ai singoli contenuti, utilizzano servizi come trasmissione dati, servizi voce o SMS a pagamento.

Il servizio funziona con tutti i modelli di terminali mobili con preinstallazione

dell'applicativo specifico dell'operatore, in pratica può funzionare su tutti i mobili che rispettano le specifiche di fase 2+, come dichiarato da Balu Nayar, direttore generale - Servizi a Valore Aggiunto - Hutchinson Mumbai.

Da un punto di vista dei requisiti della rete, la configurazione richiede l'installazione di uno speciale back-end presso gli apparati degli operatori. Oltre a ciò la piattaforma di Cell Broadcast, deve incorporare un server centrale, appositi gateways per connettere gli SMSC e i BSC della rete e uno strumento di amministrazione e controllo delle fonti di informazione.

Lo sforzo implementativo non è stato limitato al set-up del sistema, ma a tutti gli aspetti di gestione e configurazione dei contenuti inviati. La struttura dei contenuti è basata su differenti canali e i contenuti stessi sono selezionabili dagli utenti come può avvenire per i più comuni canali Radio/TV tematici, con aggiornamenti orari delle notizie, informazioni economiche locali, nazionali e internazionali etc.

### 3.6. Il progetto CHORIST

CHORIST (Integrating Communications for enhanced environmental risk management and citizens safety) è un progetto sviluppato a livello europeo nel periodo giugno 2006-luglio 2009 e finanziato dalla Comunità Europea con l'obiettivo di gestire i rischi ambientali sia in relazione ad eventi naturali (meteorologici, sismici, ecc.) sia in relazioni a catastrofi dovute agli insediamenti industriali. Il progetto propone delle soluzioni basate su tecnologie disponibili per aumentare in modo significativo la velocità e l'efficacia di intervento e di comunicazione verso la popolazione delle aree interessate dal potenziale pericolo.

Il progetto, durato 38 mesi, ha coinvolto 16 nazioni:

- Gran Bretagna: Avanti Communications, British Association for Public Safety Communications Officers Limited (BAPCO);
- Belgio: European Emergency Number Association (EENA);
- Francia: EADS Defence and Security Systems, Thales Communications, Institute Eurecom;
- Spagna: Tradia Telecom (parte di Abertis), Vodafone Spagna;
- Finlandia: EADS Secure Network Oy, (Teknillinen Korkeakoulu - TKK), Helsinki University of Technology;
- Olanda: one2many, Stichting Platform Mobile Messages (SPMM), Technische Universiteit Delft (TUD);
- Repubblica Ceca: Komocentra;
- Italia: Elisag Datamat, European Commission Directorate General Joint Research Centre (JRC).

Il costo del progetto è stato di 12.820.000,00 Euro di cui 7.088.928,00 Euro finanziati dalla Comunità Europea.

### 3.6.1. Gli obiettivi di progetto

L'obiettivo del progetto è sviluppare un sistema integrato in grado di rendere più efficiente la gestione degli eventi legati a rischi ambientali e migliorare la comunicazione tra autorità, forze dell'ordine e cittadini rendendola più capillare, efficace e affidabile. Per i partner del progetto CHORIST questo significa creare e implementare sistemi di allerta in grado di avvertire le autorità, nonché impiegare sistemi di comunicazione dedicati agli operatori in grado di raggiungere la popolazione.

Attualmente la popolazione è avvertita principalmente attraverso i mezzi di comunicazione di massa quali radio e televisione. Questo significa che i giornalisti fanno parte della "catena" informativa che lega le autorità alla popolazione. Ciò comporta che l'informazione non è diffusa solamente nell'area interessata dall'evento, ma è ricevuta a livello nazionale. Non sono inoltre sfruttati canali disponibili e largamente diffusi quali la telefonia mobile e la rete Internet.

CHORIST ha integrato i canali disponibili e utilizzati in parallelo con l'obiettivo di avvertire la popolazione su eventi calamitosi.

Tra questi canali ci sono radio, TV e il servizio **Cell broadcast** verso la popolazione, mentre sono utilizzati i canali multimediali per le comunicazioni verso le forze dell'ordine.

In particolare il progetto CHORIST ha sviluppato e integrato tre moduli specifici in grado di coprire la catena di rilevazione, alerting e gestione di un evento calamitoso:

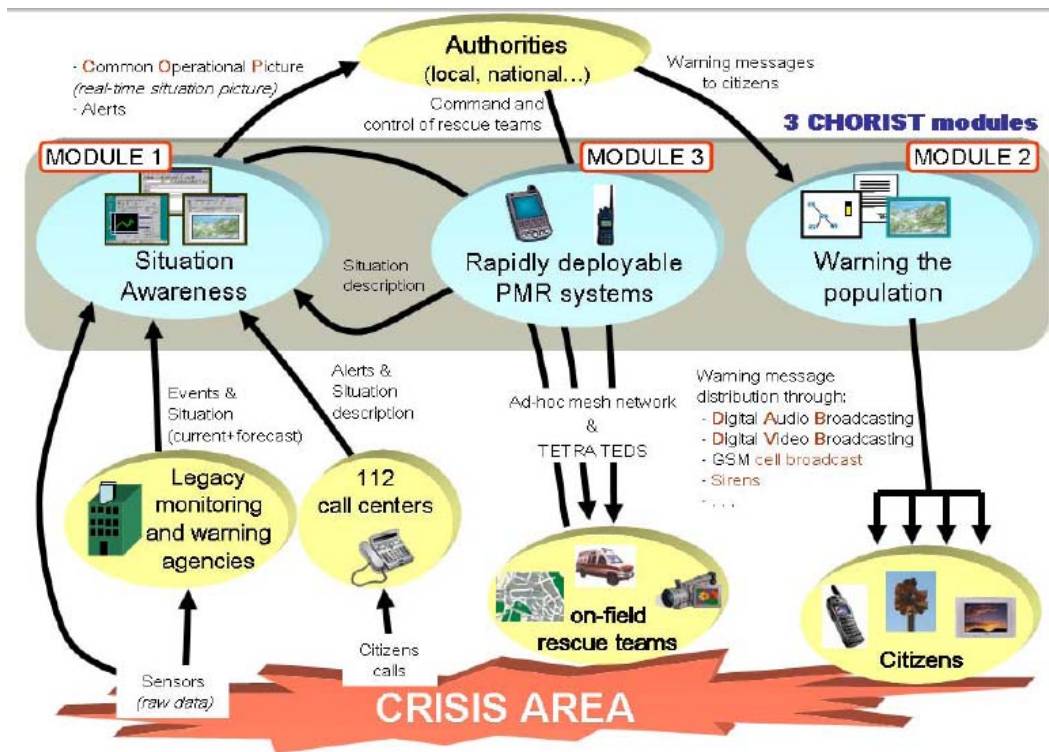
- *Modulo 1*: Sviluppare una catena di alerting interamente integrata, affidabile ed efficace in grado di rilevare eventi calamitosi da una rete eterogenea di sensori, differenti enti e cittadini stessi.
- *Modulo 2*: Integrare mezzi di comunicazione eterogenei (radio, televisione, telefonia, sirene) per inviare messaggi dalle autorità verso il maggior numero possibile di cittadini presenti nell'area colpita con il minimo ritardo possibile.
- *Modulo 3*: Rendere disponibile un sistema di comunicazione voce e trasmissione dati ad alta velocità (compresa una rete dedicata) sicuro, rapido, disponibile e interoperabile.

La logica adottata per lo sviluppo delle soluzioni tecniche necessarie per supportare il problema di fornire informazioni alle autorità e alla popolazione è quella della catena "watch-decide-act", ovvero osservare, stabilire e capire cosa sta accadendo, decidere cosa fare e agire.

La Figura 3.6 (fonte "Project CHORIST Solution for early warning" - A compendium of project findings) illustra graficamente il modello CHORIST che si colloca tra l'area di crisi e le autorità, mettendo loro a disposizione gli strumenti necessari per la gestione dell'emergenza.



**Figura 3.6 - Modello CHORIST**



### 3.6.2. Le attività di progetto

La struttura del progetto di ricerca CHORIST, è costituita di un sottoinsieme di numerosi Sotto Progetti (SP):

- Sistemi di Allerta (SP2); questi sistemi comprendono meccanismi di comunicazione DAI cittadini;
- Sistemi di comunicazione VERSO I cittadini (SP3);
- Sistemi di comunicazione CON le aree di crisi(SP4).

I tre Sotto Progetti indicati, sono completati con altri sotto progetti più trasversali:

- supporto ingegneristico allo sviluppo di applicativi(SP1);
- supporto in ottica integrazione e validazione(SP5);
- specifico SP dedicato agli aspetti di Project Management, Standardizzazione, divulgazione ed impatto dei risultati raccolti(SP0).

In totale sono stati impostati sei Sotto Progetti.

## *I Moduli di CHORIST*

Come già accennato CHORIST è composto da tre moduli:

- MODULO 1: Situation Awareness;
- MODULO 2: Warning the population;
- MODULO 3: Rapidly Deployable Systems.

Nei paragrafi successivi sono brevemente analizzati i singoli moduli in termini di funzionalità messe a disposizione e di architettura tecnologica.

### *Modulo 1*

Il Modulo 1 raccoglie le informazioni dalle agenzie nazionali o internazionali che monitorano o prevedono rischi legati a fenomeni naturali (es. tempo meteorologico, eruzioni vulcaniche, terremoti) oppure legati a rischi in zone altamente industrializzate.

Le informazioni provenienti da una rete di sensori dedicati (quali per esempio misuratori di livello di laghi o fiumi, telecamere, ecc.) vengono integrate con le comunicazioni provenienti dalle popolazioni e veicolate attraverso i call centre.

Queste informazioni sono processate e attraverso modelli matematici, simulazioni o informazioni già disponibili nei database è possibile determinare l'impatto immediato e futuro sulla popolazione dell'evento calamitoso per poter essere poi correttamente gestito.

Il risultato della rilevazione è comunicato alle autorità attraverso il COP (Common Operational Picture) che fornisce in tempo reale lo scenario relativo all'area di crisi: lo scenario è integrato con le informazioni relative al livello di alert stabilito. Il valore aggiunto consiste nel fornire un'informazione chiara, concisa e consolidata alle autorità comunicando l'evento calamitoso e le possibili conseguenze.

Per raccogliere i dati dalla popolazione CHORIST utilizza il numero 112 (European Emergency Number Association - EENA) cui risponderanno, secondo le direttive della Comunità Europea, le centrali operative uniche. La chiamata sarà gratuita, sia da telefonia fissa che mobile e il servizio sarà del tipo 24x7.

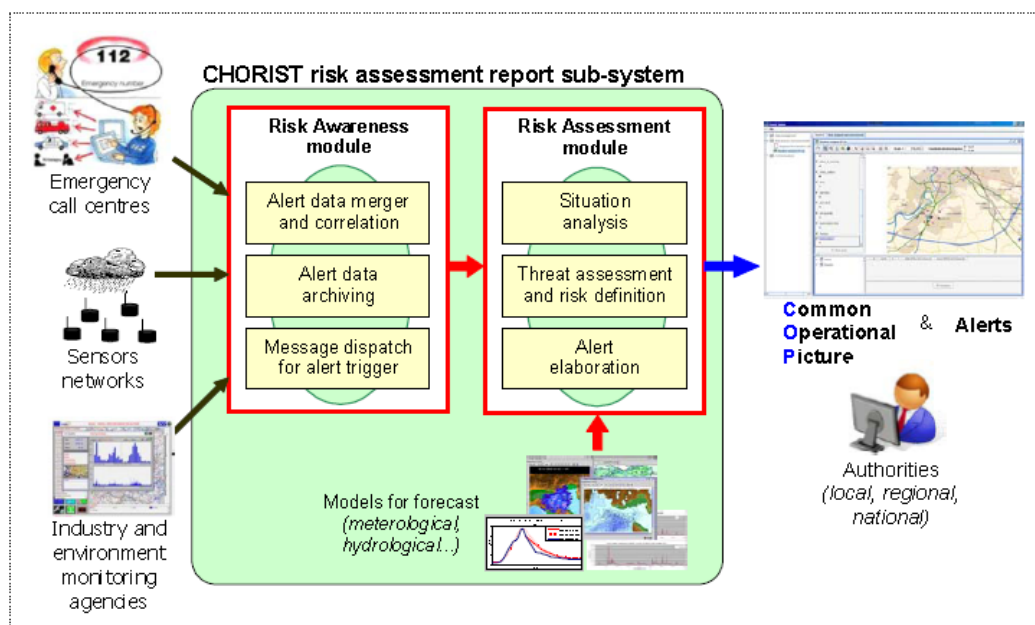
Il modulo 1 di CHORIST prevede inoltre un sottosistema di rappresentazione geografica (GIS - Geographic Information System) che riporta in modo grafico informazioni quali la densità della popolazione e infrastrutture critiche (ponti, edifici, oleodotti, linee alta tensione, ferrovie, industrie, ecc.) che consentono un'analisi della situazione e permettono alle autorità di prendere la corretta decisione per la gestione dell'evento calamitoso.

Il core del modulo 1 è rappresentato da due sottomoduli che permettono l'analisi e la valutazione del rischio:

- Risk Assessment sub-module;
- Risk Awareness sub-module

La Figura 3.7 rappresenta sinteticamente l'architettura del modulo 1 mettendo in evidenza le interfacce tra i sottomoduli, il flusso delle informazioni e il ruolo svolto dagli attori coinvolti.

**Figura 3.7 - Architettura del modulo 1**



Fonte: "Project CHORIST Solution for early warning" - A compendium of project findings

Lo sviluppo del modulo 1 è stato seguito da Avanti communication, Elsat Datamat e EC Joint research Centre. Entrambi i moduli sono integrati in una GUI (graphic user interface). Il sottomodulo Risk Awareness raccoglie i dati dal campo classificandone rischio e gravità e associando una scala di colore in funzione della gravità.

La parte di Risk Assessment utilizza i dati provenienti dal database geo-politico dell'European Commission's Join Research Centre che consente la definizione di una mappa di vulnerabilità geograficamente localizzata che informa sul rischio attuale e previsto all'interno dell'area in oggetto.

Il modulo è inoltre dotato di una serie di simulatori che hanno l'obiettivo di formare gli operatori e gli utenti di CHORIST a interpretare correttamente le informazioni e gestire nel modo corretto la situazione di catastrofe simulata.

La Figura 3.8 è un esempio di simulazione di esondazione di un corso d'acqua a fronte di fenomeni atmosferici non comuni.

**Figura 3.8 - Esempio di simulazione di esondazione**



*Fonte: "Project CHORIST Solution for early warning" - A compendium of project findings)*

La simulazione permette di valutare visivamente quali siano le aree geografiche a rischio e quali siano le aree impattate dall'evento calamitoso. Questo permette alle autorità competenti di predisporre in anticipo l'intervento delle forze di protezione civile, vigili del fuoco, ecc. e di diffondere alla popolazione messaggi di alert per poter gestire al meglio la situazione.

#### *Modulo 2*

È il modulo che consente alle autorità di diffondere il messaggio di alert verso la popolazione interessata dall'evento calamitoso. Un'interfaccia grafica consente alle autorità di confezionare velocemente il messaggio di alert e di diffonderlo in pochi minuti verso la popolazione.

Il messaggio fornisce informazioni circa la natura dell'evento e indica le azioni che la popolazione deve intraprendere (es. chiudere le finestre, stare all'interno o uscire dalle abitazioni, ecc.). Il messaggio può anche dirottare su altri canali di comunicazione quali radio, televisione o web per ottenere ulteriori informazioni.

Nell'ambito del progetto sono stati condotti test di simulazione con sirene, radio e televisione, cell broadcast. Si è dimostrato che la tecnologia, in particolare il cell broadcast è in grado di raggiungere in brevissimo tempo un numero elevato di cittadini.

Attualmente, a livello europeo, i sistemi più utilizzati per diffondere un messaggio di allarme in aree geografiche identificate sono le sirene acustiche, in grado di codificare un numero molto limitato di messaggi basato sul numero di impulsi inviati, la loro lunghezza, la tonalità della sirena.

Questa tipologia di diffusione degli alert presenta limiti notevoli per i seguenti motivi:

- interpretabilità: la codifica può essere intesa dalla popolazione in modi errati o in ogni caso interpretabili;
- limitatezza della codifica: solo pochi messaggi possono essere diffusi per cui sono indirizzabili pochi eventi;
- non conoscenza della codifica: la popolazione non residente (es. turisti) non è in grado di interpretare il suono delle sirene e comportarsi di conseguenza.

In Italia le sirene non sono in uso, per cui la diffusione di messaggi è basata su televisione e radio che non sono in grado di raggiungere tutta la popolazione: infatti sono raggiungibili solamente le persone in casa o in auto con l'apparecchio acceso e sintonizzato su di un canale specifico o con la funzione TP attiva.

La tecnologia attualmente mette a disposizione un numero di canali di comunicazione in grado di raggiungere un gran numero di cittadini in un'area geografica definibile e modificabile istantaneamente con una drastica diminuzione dell'interpretabilità del messaggio.

In particolare CHORIST identifica i seguenti canali di diffusione dei messaggi di alert (in ordine di vetustà):

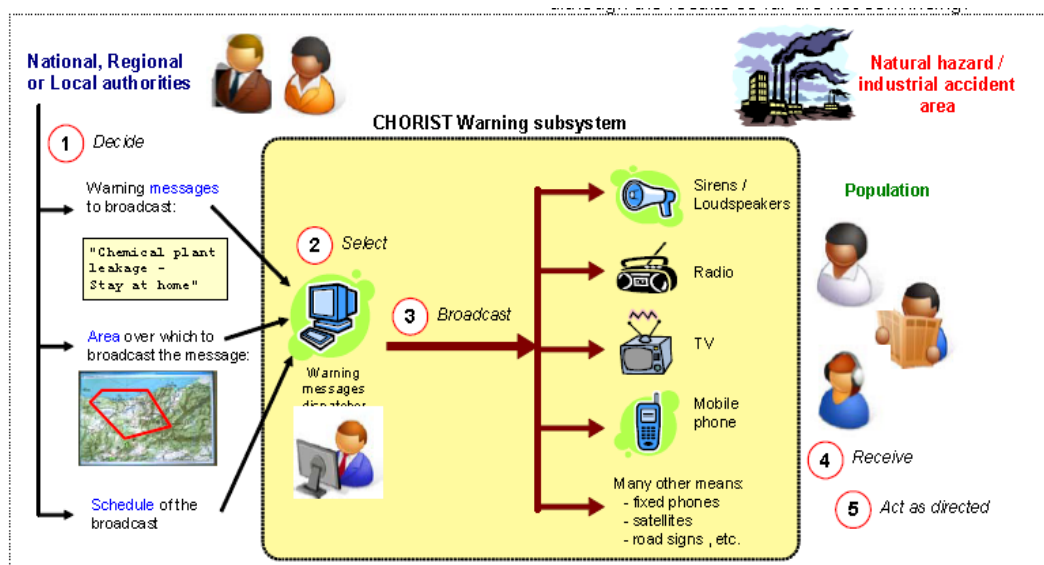
- sirene: con le limitazioni sopra indicate;
- altoparlanti interni alle abitazioni: limitati per definizione del fatto di essere installati internamente alle abitazioni, ma che possono fornire, contrariamente alle sirene, messaggi di qualsiasi tipo;
- linea telefonica fissa: possono inviare messaggi preregistrati di qualsiasi tipo. Hanno la limitazione della raggiungibilità dei cittadini, del fatto che siano interni e che la comunicazione è del tipo punto-punto (non broadcast), hanno dei vincoli di privacy ovvero deve essere noto il numero di telefono;
- telefonia cellulare: lo standard Cell Broadcast è l'unica via percorribile per raggiungere con la telefonia mobile un gran numero di persone senza la limitazione di dover conoscere il numero di cellulare, gli inconvenienti del canale SMS e le limitazioni dovute alla privacy;
- canali radio: la copertura geografica è massima sia a livello locale sia a livello nazionale. Gli alert possono essere inviati sia in modalità testo (tecnologia RDS) che in modalità voce. Il limite è nella raggiungibilità della popolazione;
- canali televisivi: analogamente ai canali radio: reti convenzionali, satellitari o via cavo possono essere utilizzate per trasmettere messaggi di alert. Le limitazioni sono simili a quelle indicate per i canali radio;
- cartelli stradali;
- internet: i feed RSS o l'Instant Messaging protocol possono essere utilizzati come canali di diffusione dei messaggi di alert. Attualmente la limitazione è dovuta alla disponibilità di GPRS o UMTS sui terminali mobili. Le email e i siti web possono essere utilizzati per diffondere notizie più estese. In

questo caso la limitazione è ancora maggiore richiedendo blackberry o UMTS.

CHORIST pone particolare attenzione sulla tecnologia Cell Broadcast essendo il canale che fornisce maggior capillarità senza le limitazioni sopra elencate e dando la possibilità di indirizzare aree geografiche ben identificate. La limitazione maggiore è dovuta alla disponibilità sui terminali mobili dell'interfaccia necessaria per l'abilitazione del Cell Broadcast.

In Figura 3.9 è illustrata l'architettura del modulo 2 (CHORIST warning subsystem) che provvede a diffondere il messaggio di warning.

**Figura 3.9 - Esempio di simulazione di esondazione**



Fonte: "Project CHORIST Solution for early warning" - A compendium of project findings

Il sottomodulo Message Creator & Dispatcher consente alle autorità di generare e diffondere il messaggio di alert attraverso una o più combinazioni dei canali disponibili.

Il Message Creator & Dispatcher è organizzato su di una catena autorizzativa di tre livelli:

- Livello 1: qualifica l'informazione ricevuta circa la situazione calamitosa;
- Livello 2: decide quale messaggio inviare, in quale area e tramite quali canali;
- Livello 3: effettua l'invio del messaggio secondo le specifiche definite.

Dal punto di vista tecnologico il Message Creator & Dispatcher è costituito da un web server accessibile simultaneamente via internet o intranet tramite Firefox. Il messaggio ha la seguente struttura:

- livello di allarme ("alarm", "warning", o "information");
- localizzazione (poligono su una mappa);

- contenuto informativo;
- azione;
- informazioni aggiuntive;
- originatore del messaggio;
- data e ora.

Per ogni messaggio può essere inoltre definito per quanto tempo e per quante volte debba essere diffuso sui canali previsti. La composizione e la diffusione del messaggio avviene attraverso interfacce grafiche che utilizzano sistemi geografici di localizzazione e si basano su protocollo TCP/IP.

### *Modulo 3*

Attualmente la maggior parte delle organizzazioni di pubblica sicurezza utilizzano per comunicare reti di telecomunicazione digitale o analogiche, note anche con la sigla PMR (Professional Mobile Radio). Questi sistemi attualmente supportano le comunicazioni vocali del tipo uno a molti, dove una singola persona trasmette un messaggio vocale e gli altri rimangono in ascolto: in generale non è supportata una modalità di scambio informazioni testuali o multimediali se non attraverso la tecnologia SMS e un limitato accesso ai dati.

Gli standards in uso nel PMR digitale sono rappresentati dal TETRA, TETRAPOL e P25 che hanno evidenti limiti legati alla tecnologia ormai datata.

Le tecnologie moderne (interfacce radio e protocolli di rete) mettono a disposizione delle infrastrutture notevolmente differenti rispetto ai vecchi standard attualmente ancora in uso. Infatti le moderne tecnologie mettono a disposizione servizi che vanno oltre la voce e gli SMS. In particolare sono disponibili tecnologie che posseggono una larghezza di banda sufficiente per supportare i seguenti servizi:

- servizi di video streaming on line e off line che possono diffondere filmati realizzati in zone differenti dell'area calamitosa;
- trasferimento file (FTP) che sono in grado di trasferire:
  - mappe (topografie, città, edifici, ecc.)
  - fotografie ad alta definizione per analisi di scenari, identificazione di persone, ecc.
  - foto aeree o satellitari
- accesso ai database:
  - accesso a db con impronte digitali
  - foto segnaletiche
  - accesso ai registri automobilistici
  - database legati agli aspetti sanitari
  - materiali pericolosi
  - dati geografici
  - accesso da remoto ad apparecchiature automatiche quali cartelli stradali dinamici, telecamere, ecc
  - accesso al servizio di e-mail
  - accesso ad internet.





## Capitolo 4

### Requisiti procedurali della Sala Operativa

L'introduzione della tecnologia Cell Broadcast per la diffusione di messaggi di alert verso la popolazione, mette a disposizione della Sala Operativa della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza un nuovo canale di comunicazione per la diffusione diretta di informazioni e avvisi verso la popolazione. Questa nuova modalità di diffondere note informative in modo diretto implica che l'attuale *modus operandi* della Sala Operativa si adegui ai vincoli e ai requisiti richiesti dalla tecnologia Cell Broadcast.

L'analisi e la definizione delle procedure necessarie per la gestione dei messaggi di alert è stata effettuata partendo dallo studio del funzionamento attuale della Sala Operativa, che adotta la normativa CFRM 2009 pubblicata nel BURL n. 8/8753 del 22 gennaio 2009.

Il capitolo definisce i requisiti e i flussi procedurali da introdurre presso la Sala Operativa della Direzione Generale, Protezione Civile, Polizia Locale e Sicurezza, stabilendo ruoli e responsabilità e introducendo le regole necessarie per la corretta gestione della comunicazione verso la popolazione utilizzando la tecnologia Cell Broadcast.

#### 4.1. Il funzionamento della sala operativa

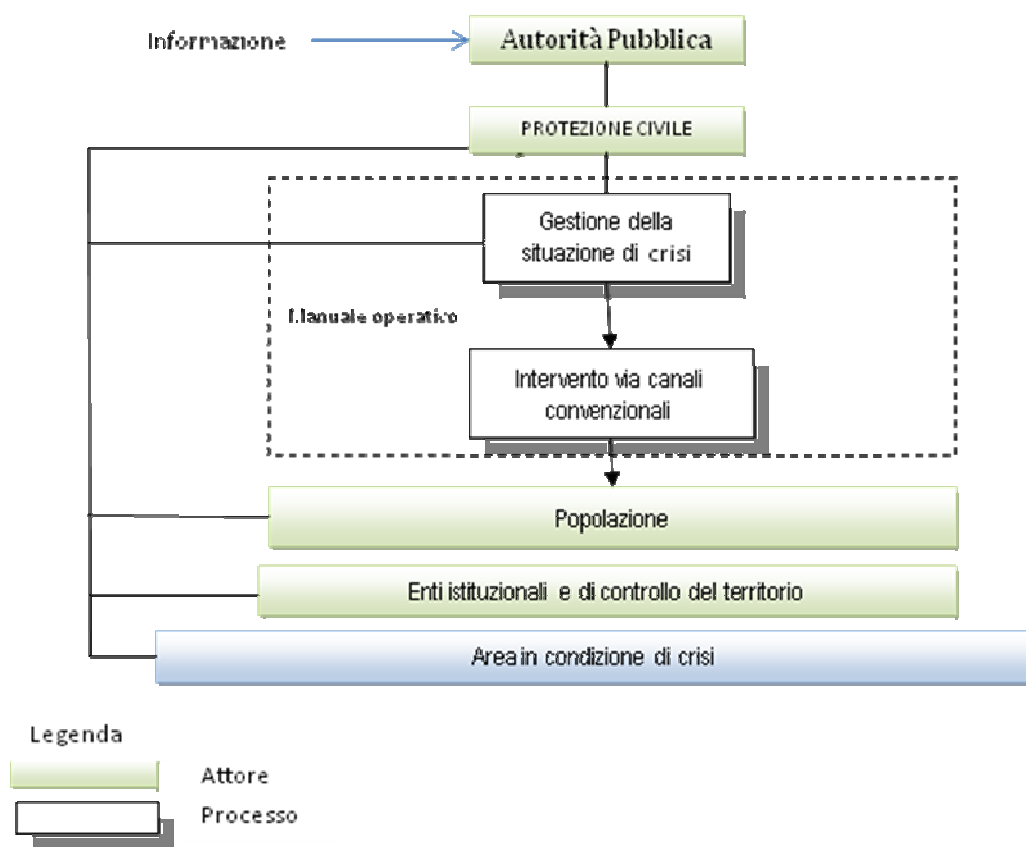
Il paragrafo propone un modello di funzionamento della Sala Operativa della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza che soddisfi i vincoli e i requisiti dettati dalla tecnologia Cell Broadcast e dalla normativa vigente. Lo scopo è quello di definire delle procedure operative che permettano la diffusione di messaggi di alert verso la popolazione a fronte del verificarsi di situazioni calamitose di origine naturale e antropico.

#### 4.1.1. Lo scenario attuale

Sulla base delle informazioni contenute nel “Manuale di Sala Operativa” e del contenuto della normativa vigente si è provveduto a disegnare il modello attuale di funzionamento della Sala Operativa e alla mappatura dei livelli di allerta e di rischio su un modello che preveda la gestione della messaggistica di alert e la definizione della struttura del messaggio.

In Figura 4.1 è riportato l’attuale flusso procedurale di funzionamento della Sala Operativa.

**Figura 4.1 - Scenario di crisi**



La normativa in vigore prevede che le comunicazioni delle tra la Sala Operativa o l’Unità di Crisi (nei casi più gravi) della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza avvenga attraverso canali istituzionali individuati dalla normativa stessa. In particolare sono definiti i seguenti canali convenzionali:

- ARPA Lombardia;
- Presidi territoriali:
  1. Pubbliche amministrazioni;

2. Agenzie e strutture operative della pubblica amministrazione;
3. Enti di regolazione dei grandi laghi alpini;
4. Società private e soggetti privati.

- Agenzia Interregionale del fiume PO;
- Sedi Territoriali provinciali;
- Comuni.

Il flusso di informazioni tra Sala Operativa o l'Unità di Crisi e gli enti preposti è di tipo bidirezionale: la normativa non prevede nessun tipo di comunicazione diretta tra la Sala Operativa o l'Unità di Crisi e la popolazione. Infatti la diffusione dei comunicati verso la popolazione viene gestita con l'utilizzo dei canali convenzionali: televisione, radio, internet, bollettini.

La segnalazione di uno stato di allerta o di evento calamitoso sono rilevati attraverso differenti canali, quali sensori presenti sul territorio (es. videosorveglianza o altri tipi di sensori, stazioni meteorologiche, ecc.), modelli matematici previsivi, informative diramate da enti preposti quali la pubblica sicurezza, la popolazione o enti istituzionali quali pompieri o carabinieri.

Attraverso questi canali l'informazione giunge alla Sala Operativa della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza che provvede ad attivare le opportune procedure di gestione in conformità a quanto stabilito nel manuale operativo.

La direttiva generale CFRM 2009 prevede la gestione delle situazioni di allerta attraverso due fasi distinte:

- fase previsionale;
- fase di monitoraggio e sorveglianza.

Sia la fase previsionale che la fase di monitoraggio e sorveglianza possono richiedere la diffusione di comunicazioni verso gli enti preposti alla gestione della situazione di alert sia messaggi verso la popolazione.

La normativa vigente identifica le seguenti tipologie di rischio classificandole secondo il seguente schema:

- rischio idrogeologico;
- rischio idraulico;
- rischio temporali forti;
- rischio neve;
- rischio valanghe;
- rischio vento forte;
- rischio ondate di calore;
- rischio incendio boschivo.

La normativa inoltre identifica le Zone omogenee di allerta, Scenari di rischio, Soglie e Livelli di allerta localizzando sul territorio delle aree geografiche e definendo dei codici di allerta correlati al livello di criticità dell'evento calamitoso

in atto (si faccia riferimento alla direttiva per ulteriori dettagli).

La direttiva regionale è integrata dal “Manuale di Sala Operativa” che definisce il flusso informativo e le modalità di gestione dell’informazione e responsabilità / ruoli. Il Manuale di sala operativa identifica e classifica esplicitamente sei livelli di criticità, descrivendone puntualmente la procedura operativa.

Il manuale fa riferimento ai codici definiti nella direttiva regionale identificando quattro fasi in funzione delle quali si adottano le opportune modalità d’intervento.

Le fasi identificate e descritte sono le seguenti:

**A - FASE DI NORMALITÀ O CRITICITÀ ORDINARIA - CODICE 1**

**B - FASE DI PREALLARME - CRITICITÀ MODERATA - CODICE 2**

**C - FASE DI ALLARME - CRITICITÀ ELEVATA - CODICE 3**

**D - FASE DI EMERGENZA - CODICE 4**

Come estensione ai codici definiti dalla direttiva regionale sono stati introdotti i seguenti scenari:

**E - FASE DI MASSIMA PERICOLOSITÀ PER GLI INCENDI BOSCHIVI**

**F - EVENTO ISTANTANEO (O IMPREVISTO)**

Ogni fase può potenzialmente generare la necessità di diffondere messaggi di alert verso la popolazione con l’utilizzo della tecnologia Cell Broadcast.

Le procedure operative per le altre tipologie di evento calamitoso sono trattate nella fase F che, a causa della loro natura intrinseca di imprevedibilità, non richiedono la diffusione di messaggi di alert ma solamente la segnalazione di eventi e di eventuali azioni da intraprendere. In questo caso non è presente in modo esplicito una classificazione della natura dell’evento, ma sono citate a titolo di esempio alcuni eventi significativi.

L’elenco completo degli eventi riconosciuti e gestiti dalla Sala Operativa della Protezione Civile è riportato in Tabella 4.1, dove sono indicati, per ogni evento, un identificativo, una descrizione, un ambito evento, un identificativo di rischio.

**Tabella 4.1 - Tipologia di eventi**

ID tipo Evento	Descrizione Evento	ID Ambito Evento	ID Tipo Rischio
27	Vento forte	1	
28	Fulmini	1	
29	Rilascio nube tossica	2	
30	Rilascio nube non tossica	2	
31	Rilascio nube non identificata	2	
32	Incidente aereo	2	
33	Incidente ferroviario	2	
34	Incidente metropolitana	2	
35	Incidente automobilistico	2	
36	Incendio in ambito residenziale/commerciale	2	

*segue*

Continua Tabella 4.1

ID tipo Evento	Descrizione Evento	ID Ambito Evento	ID Tipo Rischio
37	Manifestazione di contestazione (corteo)	2	
38	Grandi eventi	2	
39	Fiera	2	
40	Fuga di gas	2	
41	Attacco terroristico	2	
42	Black-out	2	
43	Blocco infrastrutture	2	
44	Collasso strutture	2	
45	Trasporto merci pericolose	2	
46	Esercitazione	4	
47	Interventi extra regionali	3	
999	Altro	999	
1	Caduta massi	1	1
2	Carenza idrica	1	1
3	Colata di detrito	1	1
4	Dispersione di liquidi tossici o nocivi	2	6
5	Emissione (radioattive, tossiche e nocive)	2	5
6	Erosione spondale sul reticolo idrografico	1	1
7	Esondazione corsi d'acqua minori	1	1
8	Esondazione fiumi maggiori (Fasce PAI)	1	1
9	Esondazione laghi	1	1
10	Frana di crollo	1	1
11	Frana superficiale	1	1
12	Grandinata	1	1
13	Incendio boschivo con coinvolgimento di aree urbanizzate	1	3
14	Incendio boschivo con coinvolgimento di infrastrutture	1	3
15	Incendio boschivo con coinvolgimento di sole aree boscate o pascolo	1	3
16	Incendio impianto produttivo	2	5
17	Incidente a mezzo di trasporto di sostanze pericolose	2	6
18	Scoppio - esplosione impianto produttivo	2	5
19	Sisma	1	2
20	Tromba d'aria	1	1
21	Valanga/slavina	1	1
22	Frana	1	4
23	Rigurgito fognature	1	6
24	Ondata di calore	1	6
25	Nevicata	1	6
26	Temporale	1	2
48	Recupero animali	2	
49	Persona dispersa	2	

La codifica così come descritta in Tabella 4.1 può essere utilizzata per determinare il contenuto dei messaggi di alert verso la popolazione, utilizzando come attributo del messaggio l'ID tipo evento: questo identificativo ha il vantaggio di essere univoco.

#### *4.1.1.1. Le attività e i processi*

Sulla base del flusso operativo descritto nel Manuale di Sala Operativa e sulla base dell'analisi della tecnologia Cell Broadcast contenuta nel presente documento, è possibile disegnare un flusso procedurale che consenta la gestione del sistema di alerting basato sulla tecnologia Cell Broadcasting.

La determinazione del contenuto del singolo messaggio di alert, così come la definizione degli attributi del messaggio quali criticità, priorità, frequenza di ripetizione in aria, ecc. sono determinati dall'attività di "Atomizzazione" della segnalazione che ha scomposto l'informazione aggregata in informazioni "atomiche" o segnalazioni elementari.

A valle dell'attività di atomizzazione, ogni segnalazione può essere classificata, in base alla sua natura, come allerta o come evento e di conseguenza associare ad essa degli attributi che ne definiscono la modalità di diffusione: si faccia riferimento al Manuale di Sala Operativa per i dettagli.

La classificazione della segnalazione stabilisce la natura e il contenuto del messaggio di alert e oltre che sulla sua gestione. Infatti se la segnalazione è classificata come allerta (ovvero non si è ancora in presenza di un accadimento) l'obiettivo del messaggio di alert è quello di avvisare la popolazione indicando dei comportamenti da tenere o delle azioni preventive da effettuare, mentre se la segnalazione è classificata come evento (ovvero si è in presenza di un fatto successo) il contenuto e gli attributi del messaggio hanno l'obiettivo di informare la popolazione sull'accaduto gestendone il comportamento o le azioni da compiere.

In fase di progettazione della struttura dei messaggi è necessario individuare una corretta classificazione con la relativa associazione degli attributi di diffusione dei messaggi stessi.

#### *4.1.1.2. Ruoli e responsabilità*

Il Manuale della sala Operativa identifica i ruoli responsabili per la gestione di un evento calamitoso. In particolare:

- Dirigente U.O. (o sostituto);
- Responsabile Sala situazioni (o sostituto);
- Responsabile Funzionale Monitoraggio Rischi - CFMR (o sostituto);
- Responsabile del Centro Operativo Antincendi Boschivi - AIB (o suo sostituto);
- Funzionari Reperibili di turno della D.G. Protezione Civile, Polizia Locale e Sicurezza;
- Membri titolari (e/o supplenti) delle altre D.G.;
- Coordinatore H24;
- Operatore Tecnico H24;
- Rappresentante altre D.G.;
- Tecnico di supporto;
- Volontari supporto segreteria e call center della Sala Situazioni;
- Funzionario di turno reperibili - Team Emergenza;
- Funzionario di turno reperibile in sala operativa;

- Volontario addetto alle comunicazioni di emergenza.

Questi ruoli sono identificati e istituzionalizzati per poter gestire correttamente la situazione di alert previste dalla normativa in vigore. L'adozione della tecnologia Cell Broadcast per la diffusione di messaggi verso la popolazione introduce una serie di attività e di responsabilità che attualmente non sono previste dal Manuale di Sala Operativa e potenzialmente la ridefinizione, sia pur parziale, di ruoli e responsabilità. Potrebbe inoltre rivelarsi necessaria, in fase di progettazione dei flussi procedurali, l'introduzione di nuovi ruoli e la modifica dei flussi procedurali per la gestione della situazione di alert.

Questi adeguamenti si rendono necessari per il corretto funzionamento della Sala Operativa della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza che si prevede l'utilizzo della tecnologia di Cell Broadcast per la comunicazione verso la popolazione.

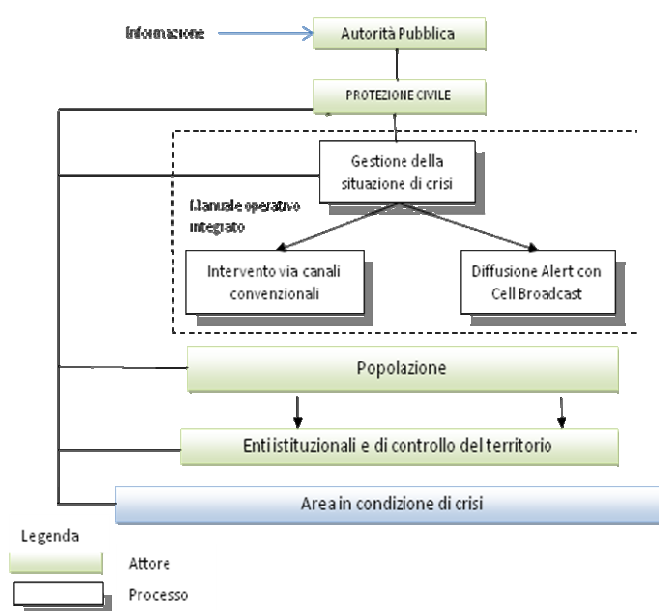
#### 4.1.2. Situazione a tendere

La Figura 4.2 ipotizza lo scenario operativo della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza nel caso di gestione di una situazione di crisi in cui l'informazione verso la popolazione civile sia diffusa tramite l'utilizzo della tecnologia di Cell Broadcast.

Rispetto allo scenario attuale viene introdotta l'attività di "Diffusione alert con Cell Broadcast" che consente la composizione, l'approvazione, l'autorizzazione e la diffusione del messaggio di alert.

Il processo è disegnato per garantire la massima sicurezza nel controllo del contenuto e nella sua diffusione per evitare che vengano diffuse informazioni errate e potenzialmente pericolose verso la popolazione.

**Figura 4.2 - Procedura di Sala Operativa con Cell Broadcast in caso di scenario di crisi**



Dal punto di vista operativo le attività di “Diffusione Alert con Cell Broadcast” è responsabilità di uno o più operatori di Sala Operativa che hanno l’obiettivo di predisporre e diffondere il corretto messaggio di alert verso la popolazione in funzione dello scenario che si è verificato o che si presume si verifichi.

Analogamente allo scenario attuale si ipotizza che le informazioni giungano alla sala operativa attraverso i canali convenzionali: sulla base delle informazioni ricevute la Direzione Generale Protezione Civile, Polizia Locale e Sicurezza applica le procedure di gestione contenute nel Manuale di Sala Operativa e può decidere se inviare comunicazioni alla popolazione utilizzando la tecnologia di Cell Broadcast.

Si precisa che l’utilizzo della tecnologia Cell Broadcast richiede che siano classificate anche le situazioni non esplicitamente definite nel Manuale di Sala Operativa al fine di consentire la predisposizione di note informative predefinite e permettere all’operatore di gestire con la massima efficienza e sicurezza la diffusione dell’alert.

#### *4.1.2.1. Il messaggio di Alert*

Il messaggio di alert deve avere una struttura logica che consenta di mappare i livelli di criticità previsti dalla normativa e dal manuale della Sala Operativa in modo congruente con rischi indicati e che costituiscono una delle possibili classificazioni del messaggio di alert.

Analizzando quanto descritto dal Manuale di sala Operativa e dalla normativa vigente, si ipotizza la seguente struttura logica del messaggio di alert:

**Tabella 4.2 - Struttura del messaggi di alert.**

Campo	Obbl.	Descrizione
Identificativo messaggio	S	Identificativo unico del messaggio di alert
Codice allarme	S	Contiene il codice che identifica la gravità dell’alert (rif. 0)
Tipo di scenario	S	Indica la causa dell’allerta o l’evento che ha generato l’intervento della PC
Luogo dell’evento	S	Localizzazione geografica dell’evento
Informazioni aggiuntive	N	Altre note riguardanti l’evento o il rischio
Azioni richieste	N	Azioni suggerite o richieste alla popolazione (es. non uscire di casa, evacuare la zona, ecc.)
Ulteriori informazioni	N	Indicazione su dove ottenere informazioni di dettaglio sull’evento (es. numero verde, internet TV, radio, ecc.)
Identificativo operatore	S	Identificativo dell’operatore che ha diffuso il messaggio di alert
Timestamp	S	Data e ora di creazione e diffusione del messaggio



Oltre quelli già classificati nel Manuale Operativo è possibile individuare altre tipologie di scenario quali attacco terroristico, incidente stradale, epidemia, pericoli dovuti al collasso di edifici, disordini, disastro nucleare, emergenza industriale e di conseguenza identificare opportunamente codici, descrizione e gli altri attributi necessari per la corretta diffusione del messaggio stesso.

In particolare l'informazione "Tipo di scenario" deve indicare la causa dell'allerta o l'evento verificatosi: mentre per la parte legata a scenari naturali è identificabile una classificazione precisa, per la parte antropica non è definita una classificazione altrettanto puntuale.

Considerando l'imprevedibilità dell'evento la procedura di gestione dell'alert deve prevedere la possibilità di gestire messaggi non classificati a priori.

#### *4.1.2.2. I requisiti di operatività con il Cell Broadcast*

La procedura operativa di gestione del Cell Broadcast richiede una serie di attività che garantiscano la diffusione dell'informazione corretta sul territorio individuato escludendo il rischio di divulgare informazioni errate sul territorio.

La diffusione del messaggio di alert è classificabile come una serie di azioni che garantiscono la corretta generazione e diffusione del messaggio stesso. Le azioni che compongono la procedura sono le seguenti:

- presa in carico;
- analisi informazione;
- approvazione;
- notifica;
- creazione messaggio;
- diffusione e gestione.

Si suppone in prima approssimazione che i ruoli coinvolti nella gestione dei messaggi di alerting della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza siano quelli definiti nel manuale della Sala Operativa. Come già evidenziato ciò non esclude che sia necessario in fase di analisi di dettaglio definire nuovi ruoli e/o nuove responsabilità.

Si ipotizza inoltre che la Sala Operativa abbia a disposizione una piattaforma informatica che metta a forniscia delle funzionalità a supporto del processo definito e che permetta di gestire l'invio dei messaggi di alert con l'operatore di telefonia mobile.

Si suppone che i ruoli necessari per la diffusione di un messaggio di alert verso la popolazione siano i seguenti:

- *Ruolo 1* - Volontari supporto segreteria e call center della Sala Situazioni;
- *Ruolo 2* - Funzionario di turno reperibile in sala operativa;
- *Ruolo 3* - Operatore Specializzato;
- *Ruolo 4* - Funzionari Reperibili di turno della DG Protezione Civile, Polizia Locale e Sicurezza.

I ruoli indicati hanno il compito di garantire la corretta composizione e diffusione del messaggio di alert in funzione dell'evento calamitoso in corso.

Il processo per la creazione e la diffusione di un messaggio può essere scomposto in una serie di passi che hanno lo scopo di individuare, selezionare/definire e distribuire l>alert. Il processo è schematizzato in Figura 4.3.

**Figura 4.3 - Processo di gestione del messaggio di alerting.**



#### Presain carico:

Il *Ruolo 1* riceve comunicazione della situazione di alert e ne prende in carico la gestione per provvedere alla sua diffusione.

Il formato con cui arriva a *Ruolo 1* la comunicazione può essere:

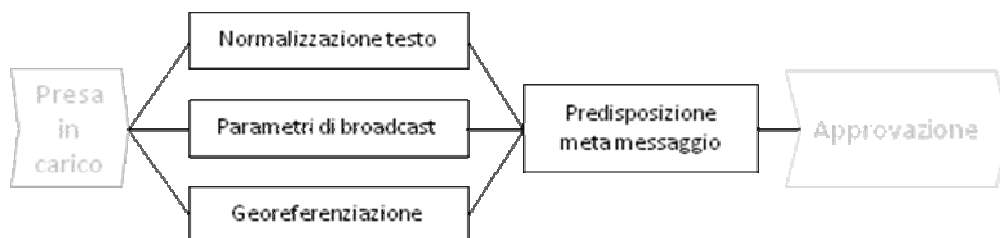
- cartaceo;
- telefonico;
- mail;
- fax.

Si suppone che il messaggio arrivi già scomposto nelle sue componenti prima della fase di presa in carico, ovvero abbia già subito il processo di “atomizzazione”. In questo modo è possibile associare a una singola segnalazione un singolo messaggio di alert.

#### Analisi informazione

Il *Ruolo 1* analizza il contenuto della comunicazione e verifica che siano disponibili tutte le informazioni necessarie per poter procedere alla predisposizione e diffusione del messaggio di alert. Le attività di analisi dell'informazione sono riassunte in Figura 4.4.

**Figura 4.4 - Processo di analisi dell'informazione**



Le attività di predisposizione del contenuto e degli attributi del messaggio di alert sono le seguenti:

- normalizzazione testo: il testo ricevuto viene normalizzato per renderlo comprensibile alla popolazione e consentire la ricerca di messaggi simili tra quelli predefiniti e reperibili all'interno del "centro gestione alert CB";
- parametri di broadcast: sono valorizzati i parametri di broadcast quali priorità, ripetizione, ecc. questi parametri sono assegnati in funzione della segnalazione e rappresentano caratteristiche quali la ripetizione, la priorità, la frequenza, ecc.;
- georeferenziazione: definizione dell'area geografica interessata all'evento e all'interno della quale il messaggio di alert verrà diffuso;
- predisposizione meta messaggio: è una versione intermedia del messaggio con il contenuto informativo e gli attributi di alto livello.

Nel caso in cui le informazioni ricevute siano incomplete o non corrette *Ruolo 1* richiede le informazioni mancanti o notifica la non correttezza al Operatore specializzato che ha sottomesso la richiesta.

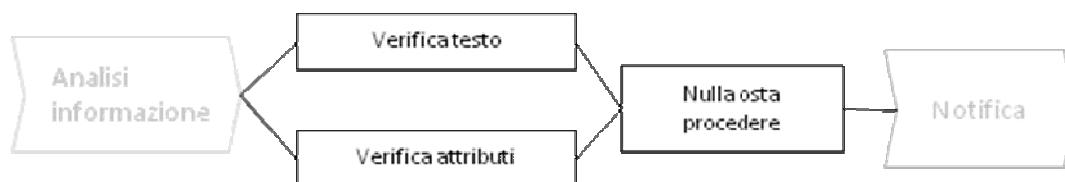
Nel caso in cui il contenuto informativo del messaggio sia già disponibile in archivio, il *Ruolo 1* provvede a selezionare il messaggio da diffondere predisponendo in ogni caso sia i parametri di Cell Broadcast sia le informazioni di georeferenziazione. Nel caso in cui il contenuto informativo del messaggio non sia disponibile, *Ruolo 1* provvede alla stesura del testo del nuovo messaggio.

Quando il nuovo messaggio è approvato e inviato agli operatori di telefonia mobile, sarà archiviato e reso disponibile per eventuali futuri utilizzi.

#### Approvazione

Il *Ruolo 2* prende in carico il messaggio da diffondere predisposto da *Ruolo 1*, con l'obiettivo di verificarne il contenuto e autorizzarne la diffusione. Questa parte del processo viene eseguita sia nel caso in cui il contenuto informativo del messaggio di alert è già presente come predefinito sia nel caso in cui il messaggio di alert non è presente all'interno della piattaforma informatica di gestione degli alert. Nel caso di nuovo messaggio, *Ruolo 2* ha il compito di apportare eventuali modifiche o correzioni sia nella forma che nel contenuto informativo.

**Figura 4.5 - Processo di Approvazione**



Le attività di verifica del contenuto e degli attributi del messaggio di alert sono le seguenti:

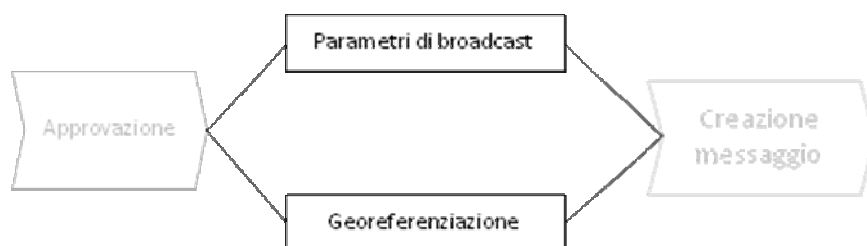
1. verifica testo: il contenuto informativo del messaggio è controllato sia nel caso di alert predefinito sia nel caso di alert nuovo;
2. verifica attributi: analogamente al contenuto informativo, sono verificati gli attributi del messaggio garantendone la congruenza con le caratteristiche della situazione di crisi che si è verificata;
3. nulla osta procedere: autorizzazione alla diffusione del messaggio.

Nel caso in cui il messaggio non venga approvato viene riattivata la fase di Analisi informazione congiuntamente alla comunicazione delle modifiche richieste.

#### Notifica

Il messaggio viene comunicato al *Ruolo 3*, specializzato per la parte di comunicazione verso gli operatori di telefonia mobile, che provvede alla verifica “sintattica” del messaggio di alert con lo scopo di prevenire errori nella sottomissione del messaggio stesso al CBC degli operatori telefonici.

**Figura 4.6 - Processo di Notifica**



Le attività di notifica del messaggio presuppongono la verifica della correttezza sintattica dei parametri, in particolare sono le seguenti:

- verifica dei parametri di broadcast: sono controllati dal punto di vista sintattico la correttezza dei parametri che caratterizzano il messaggio, al fine di garantire la linearità della creazione del messaggio, evitando ricicli ed errori nel confezionamento del messaggio di alert;
- verifica della georeferenziazione: controllo che la definizione dell'area di diffusione sia corretta dal punto di vista sintattico.

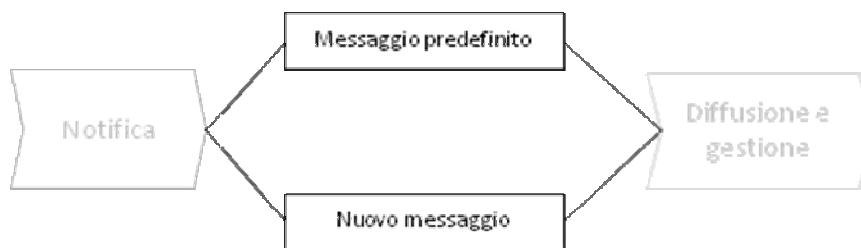
Nel caso in cui il messaggio non superi la fase di notifica, viene riattivata la fase di Analisi dell'informazione, comunicando le correzioni richieste.

Completata la verifica sintattica dei parametri e del contenuto del messaggio *Ruolo 3* chiede il nulla osta a procedere a *Ruolo 4* per la creazione e la diffusione del messaggio di alert verso la popolazione.

### Creazione messaggio

Il *Ruolo 3* provvede alla creazione del messaggio fisico da inviare al CBC dell'operatore di telefonia mobile sulla base delle indicazioni contenute nel messaggio. La predisposizione è supportata da strumenti informatici che permettano automaticamente o manualmente la diffusione del messaggio di alert.

**Figura 4.7 - Processo di Creazione messaggio**



Le attività di creazione messaggio sono le seguenti:

- messaggio predefinito: nel caso in cui il contenuto informativo sia predefinito, l'attività di creazione consiste solamente nella selezione dell'opportuno messaggio di alert;
- nuovo messaggio: in questo caso la *Ruolo 3* dovrà introdurre il testo del messaggio da diffondere e catalogare opportunamente il nuovo messaggio, memorizzandolo all'interno del "Centro gestione alert Cell Broadcast".

Sia nel caso di messaggio predefinito che di messaggio nuovo è possibile che sia necessario definire di volta in volta gli attributi. Infatti un messaggio di alert con lo stesso contenuto informativo può essere diffuso in zone diverse del territorio o con una frequenza di ripetizione differente.

### Diffusione e gestione

Il *Ruolo 3*, verificate tutte le condizioni di correttezza del contenuto informativo e degli attributi del messaggio, provvede alla diffusione del messaggio di alert attraverso il "Centro gestione alert CB" e alla sua gestione post diffusione.

Il *Ruolo 4* ha comunque la possibilità di interrompere in qualsiasi momento il processo di preparazione e diffusione del messaggio di alert e di modificarne i parametri (es. ripetizione in aria o priorità) anche quando il messaggio è già stato diffuso in aria.

Questa possibilità consente di modificare le comunicazioni verso la popolazione in funzione del modificarsi delle condizioni dello scenario calamitoso.

Operativamente spetta a *Ruolo 3* eseguire materialmente le operazioni necessarie per ottemperare alle richieste espresse da *Ruolo 4*.

**Figura 4.8 - Processo di diffusione e gestione messaggio**



Le attività di diffusione e gestione messaggio sono le seguenti:

- diffusione: è l'attività che permette centro gestione alert Cell Broadcast di comunicare con i sistemi dell'operatore di telefonia mobile e fornire al CBC tutti i parametri e informazioni necessarie per una operare in modo corretto la diffusione del messaggio di alerting;
- cancellazione messaggio: è l'attività che permette di rimuovere un messaggio di alert inviato al CBC dell'operatore di telefonia mobile. L'attività è a carico di *Ruolo 3* che, sulla base delle indicazioni contenute nel meta messaggio o su indicazioni dirette da parte di *Ruolo 4* provvede alla rimozione del messaggio di alert indicato;
- richiesta stato messaggio: è l'attività di monitoraggio della diffusione del messaggio di alert e consente la verifica della corretta diffusione dello stesso. Sono ipotizzabili due modalità di corretta diffusione del messaggio di alert:
  1. attraverso l'interfaccia con l'operatore di telefonia mobile
  2. attraverso personale della PC presente fisicamente nella zona del territorio in cui è avvenuta la diffusione del messaggio di alert.

È compito di *Ruolo 3* monitorare il corretto funzionamento della diffusione del messaggio di alert informando *Ruolo 4* in caso di malfunzionamenti o problemi relativi al funzionamento degli apparati.

- Gestione feedback: la comunicazione con l'operatore di telefonia mobile implica uno scambio di comandi e risposte con piattaforma informatica di Cell Broadcast. L'esito dei comandi deve essere monitorato e opportunamente gestito.

Non è prevista la modifica e ridiffusione di un messaggio già diffuso: questa eventualità è gestita come un nuovo messaggio di alert.

#### **4.1.2.3. Matrice RACI**

La matrice RACI (Responsible, Accountable, Consulted, Informed) è uno strumento per la rappresentazione delle responsabilità assegnate alle singole risorse.

Di fatto la matrice RACI pone in relazione le risorse con le attività delle quali sono responsabili, o con loro aggregazioni. Tipicamente, pone in relazione le

risorse umane di un'organigramma con i principali processi di diffusione dei messaggi di alert cui sono responsabili.

In altre parole la matrice RACI specifica il tipo di relazione fra la risorsa e l'attività: con tale strumento viene indicato “chi fa che cosa”, all'interno di una organizzazione.

Una modellazione di questo tipo non tiene conto della tecnologia, in termini di informazioni scambiate fra gli attori e delle applicazioni eventualmente utilizzate.

**Tabella 4.3 - Matrice RACI (esempio)**

	Presa in carico	Analisi informazioni	Approvazione	Notifica	Creazione messaggio	Diffusione e gestione
Ruolo 1	R	I,C	C	I,C	R	A, I, C
Ruolo 2	A, I	A	R	I	C	R
Ruolo 3	I	R	I	R	A	C
Ruolo 4	I	I			I,C	A

R - Il ruolo corrispondente è Responsabile del processo (unica persona)

A - Il ruolo corrispondente l'Accountable del processo

C - Il ruolo deve essere Consulted sul rilascio del deliverable

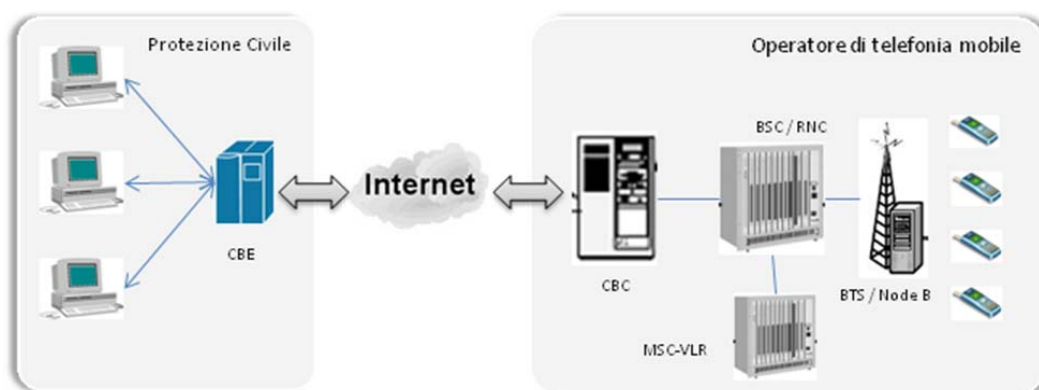
I - Il ruolo viene Informed del deliverable

Un approccio di questo tipo aiuta a fare chiarezza rispetto a chi fa cosa, nel processo che va dalla presa in carico alla diffusione e gestione del messaggio di Cell Broadcast.

## 4.2. La sicurezza

L'architettura su cui si basa la gestione dei messaggi di alert tramite tecnologia Cell Broadcast è quella illustrata in Figura 4.9. Gli apparati di Protezione Civile (CBE) colloquiano con il CBC dell'operatore di telefonia mobile attraverso la connettività resa disponibile da Internet.

**Figura 4.9 - Architettura Cell Broadcast per Sala Operativa Protezione Civile**



Questa condizione rende vulnerabili i sistemi esposti sul WEB con possibilità di attacchi da parte di hacker. È importante individuare i requisiti di sicurezza cui devono sottostare entrambi i sistemi. In particolare si fa riferimento alla Sicurezza Informatica, suddivisa in sicurezza logica e sicurezza fisica, e alla sicurezza operativa che garantisce la corretta diffusione del messaggio di alert.

Si definisce “incidente” qualsiasi evento che è in grado di compromettere il corretto funzionamento dei sistemi e delle apparecchiature della Sala Operativa o di pregiudicare la riservatezza delle informazioni presenti o in transito. È possibile classificare gli incidenti in due categorie:

- incidente puro;
- tentativo di attacco.

Per Incidente puro si intende un evento che causa un degrado o un fermo nell'erogazione dei servizi e richiede un intervento da parte dei tecnici per la rimozione della causa e il ripristino del corretto funzionamento.

Per tentativo di attacco una serie di eventi provenienti dall'esterno che producono un degrado delle prestazioni dei servizi, un'interruzione nell'erogazione dei servizi o l'accesso non autorizzato a informazioni o dati riservati.

Ad ogni incidente o tentativo di attacco è possibile associare un livello di criticità che ne fornisce una misura qualitativa della gravità dello stesso in termini di:

- gravità del danno prodotto o potenziale;
- entità del disservizio causato;
- quantità dei sistemi coinvolti;
- impatto su sistemi giudicati critici dall'utente finale.

In base a queste valutazioni è possibile classificare la criticità dell'incidente secondo una griglia predefinita. In fase progettuale dovranno essere definita questa griglia sulla base dell'analisi tecniche e infrastrutturale degli apparati utilizzati dalla Sala Operativa.



La sicurezza informatica ha l'obiettivo di impedire il verificarsi di incidenti o tentativi di attacco e limitarne le conseguenze nel caso si dovessero verificare.

#### *4.2.1. La sicurezza informatica*

Si intende per Sicurezza informatica quella disciplina che si occupa della salvaguardia dei sistemi informatici da potenziali rischi e/o violazioni dei dati e dell'infrastruttura. I principali aspetti di protezione del dato sono la confidenzialità, l'integrità dei dati e la disponibilità. La sicurezza informatica si suddivide in sicurezza logica che garantisce l'accesso ai dati, alle applicazioni, l'integrità dei dati, ecc., mentre la sicurezza fisica si occupa di garantire l'integrità dell'infrastruttura informatica regolando opportunamente gli accessi ai locali che ospitano l'infrastruttura e garantendo i parametri di operatività degli stessi (temperatura, umidità, incendio, ecc).

Nello scenario ipotizzato in Figura 4.9 è possibile suddividere le problematiche legate alla sicurezza sulla base degli attori coinvolti. Per quanto riguarda la protezione civile i sistemi sono situati presso Lombardia Informatica che ne cura la gestione sia infrastrutturale che applicativa, garantendo tutti gli aspetti di sicurezza informatica connessi. Le policy di sicurezza adottate da Lombardia Informatica dovranno garantire la sicurezza contro attacchi nei confronti degli apparati che costituiranno il CBE.

Per quanto riguarda l'operatore di telefonia mobile si dovranno predisporre le misure di sicurezza adeguate per garantire la protezione degli apparati di CBC da possibili attacchi.

##### *4.2.1.1. La sicurezza Logica*

La *sicurezza logica* ha come obiettivo la protezione delle risorse informatiche e dei dati da danni accidentali o dolosi che possono compromettere la corretta erogazione di un servizio. La sicurezza logica si occupa anche della protezione di informazioni preservandola da accessi non autorizzati o da azioni volte a ottenere impropriamente informazioni cui non possono accedere.

La sicurezza logica si ottiene attraverso la definizione e l'implementazione di misure di carattere tecnico preventivo, supportate da adeguate procedure di configurazione e gestione. Ne consegue che la salvaguardia di risorse informatiche e dati si ottiene non solo attraverso delle soluzioni tecnico-informatiche, ma anche attraverso la definizione di un insieme di regole che garantiscono la protezione dei dati e delle risorse.

Le linee guida che servono per poter realizzare in modo corretto un sistema di sicurezza logica delle risorse informatiche e dei dati possono essere sintetizzate come segue :

- garantire la disponibilità delle risorse, compresi i dati, agli utenti dei servizi del sistema informatico autorizzati;
- impedire attacchi rivolti a violare la riservatezza dei dati e delle informazioni, consentendone la fruizione soltanto a persone o sistemi

- informatici autorizzati;
- assicurare l'integrità dei dati e delle informazioni e più in generale delle risorse, non consentendo modifiche non autorizzate.

Le linee guida si declinano in una serie di regole e di misure preventive che hanno l'obiettivo di assicurare la congruità e la sicurezza dell'informazione. La prima regola base è quella di definire una procedura per l'accesso in azienda o di uscita dalla medesima di un dipendente utente o collaboratore, oppure l'assegnazione o dismissione di password e caselle di posta elettronica collegate alla presenza di personale in azienda, l'individuazione di limiti e responsabilità di utilizzo delle risorse informatiche e dei dati.

Nell'ottica della sicurezza logica è inoltre fondamentale garantire la gestione delle gerarchie e le modalità di distribuzione delle password e dei privilegi di amministrazione, con relative responsabilità e limiti di utilizzo, nei diversi settori del sistema aziendale. Questo aspetto risulta particolarmente critico per la parte autorizzativa per la diffusione dei messaggi di alert: la certezza del contenuto e la correttezza degli attributi del messaggio di alert possono essere garantiti da un corretto iter autorizzativo e dalla linea gerarchico-organizzativa.

La sicurezza logica richiede anche la definizione di policy interne che prevedano la l'identificazione di ruoli specifici e l'assunzione di responsabilità di singoli o gruppi rispetto alle operazioni che si devono effettuare e all'accesso a risorse informatiche e dati importanti.

La sicurezza logica ha anche il compito di prevenire eventuali attacchi che provengono dall'esterno (ovvero dal Web): l'accesso non autorizzato a risorse informatiche o a dati e il causare un degrado di erogazione del servizio rappresentano potenziali minacce da cui ci si può difendere attuando misure di sicurezza logica.

Nel seguito del capitolo verranno presi in considerazione solamente quegli attacchi che possono recare danno alla Sala Operativa della Direzione Generale Protezione Civile, Prevenzione e Polizia Locale.

Si deve infatti considerare che la parte esposta su web non è costituita da un portale informativo o da servizi interrogabili dall'utenza, ma di un canale di comunicazione tra le apparecchiature di Sala Operativa e le apparecchiature degli Operatori di Telefonia Mobile.

Ciò implica che alcune tipologie di attacchi non possono essere portati in quanto si è in presenza di un'applicazione atipica e non convenzionale: possono invece essere realizzati attacchi che portano degrado al servizio, con le conseguenze immaginabili in caso di alert, o che possono generare diffusione di messaggi non autorizzati verso la popolazione.

I possibili attacchi verso le apparecchiature informatiche che sovrintendono all'operatività della Sala Operativa per la messaggistica di alerting e l'operatore telefonico sono classificabili nelle seguenti categorie:

- degrado di servizio;
- spionaggio elettronico (sniffing);
- dirottamento di sessione (hijacking).

Le apparecchiature di CBE devono garantire la difesa da tutte le categorie di attacchi sopra citate.

#### *Degrado di servizio*

Il degrado di servizio si riferisce principalmente al rallentamento delle prestazioni delle applicazioni di supporto al Cell Broadcast dovuto ad un attacco da parte di hacker. Questa forma di attacco è conosciuta anche come “denial-of-service attack” (DoS attack) o “distributed denial-of-service attack” (DDoS attack) e ha l’obiettivo di sottrarre risorse di calcolo agli utenti autorizzati.

Bersagli tipici di un DoS attack sono i siti Internet che vengono massivamente utilizzati per saturare le prestazioni dei server e di conseguenza degradare permanentemente o temporaneamente i tempi di risposta.

Un metodo comune è quello di saturare di richieste la macchina target con frequenti richieste per rallentare a tal punto il servizio da essere reso inutilizzabile.

Questo fenomeno risulta essere pericoloso in quanto il CBC si affaccia sul Internet e come tale soggetto a potenziali attacchi di tipo DoS.

I sintomi di attacchi DoS possono essere i seguenti:

- rallentamento inusuale delle risorse di rete quali per esempio l’accesso a risorse esposte su Internet;
- indisponibilità di risorse in assenza di malfunzionamenti;
- impossibilità di accedere a siti web o più in generale a risorse di rete.

Un ulteriore sintomo di un attacco DoS è il rallentamento dell’accesso a Internet per via della riduzione di banda causata dall’attacco stesso. In questo caso non sono compromesse le prestazioni del server, ma le prestazioni della connettività tra server e la rete. Se l’attacco è condotto su larga scala, possono essere compromesse intere aree geografiche.

Gli attacchi DoS possono essere diretti ad apparati di rete, ad apparecchiature di routing e a server DNS. Il manifestarsi di questi attacchi consiste nei seguenti fenomeni:

- consumo anomalo di risorse quali banda, spazio disco, CPU;
- compromissione di informazioni di configurazione quali quelle di routing;
- reset forzato di sessioni TCP;
- compromissione di sessione tra componenti che comunicano tra di loro aumentando artificialmente il traffico di rete.

Da considerare come attacchi DoS sono i cosiddetti malware che si installano su server e Personal computer senza l’esplicito consenso dell’utente. Gli effetti di attacchi malware sono i seguenti:

- saturazione della potenza di calcolo della CPU;
- generazione di errori nel microcodice della macchina;
- blocco della macchina;
- messa fuori uso del sistema operativo.

Le soluzioni attualmente più diffuse per proteggersi da attacchi DoS sono costituite dalle liste di controllo degli accessi (Access Control Lists - ACL) e server proxy.

Le ACL hanno l'obiettivo di bloccare indirizzi IP non autorizzati o più in generale non noti, mentre i server Proxy hanno il compito di disaccoppiare i server che insistono sulla rete interna da Internet, operando da filtri e impedendo di effettuare alcuni tipi di operazione: di fatto il Proxy rappresenta il canale di uscita verso Internet.

#### *Spionaggio elettronico (sniffing)*

Lo spionaggio elettronico consiste nello sfruttare elementi presenti su qualsiasi e personal computer o server quali la cache utilizzata per velocizzare la navigazione Internet o i cookies, che mantiene in locale elementi di pagine web per velocizzare la navigazione.

Gli scopi dello spionaggio è quello di ricavare informazioni sul comportamento dell'utente per poterne tracciare un profilo che poi possa essere utilizzato per secondi fini per esempio commerciali.

In considerazione della delicatezza delle informazioni che vengono scambiate tra la Sala Operativa e gli operatori di telefonia mobile, è necessario garantire che l'infrastruttura informatica su cui vengono generati e inviati i messaggi di alert non sia soggetta ad attacchi di spionaggio elettronico.

Una possibile soluzione, che dovrà comunque essere analizzata e verificata in fase di progettazione e realizzazione, è l'adozione di protocolli sicuri quali il protocollo HTTPS o una Virtual Private Network o VPN.

La VPN è una rete privata instaurata tra soggetti che utilizzano un sistema di trasmissione pubblico e condiviso quale Internet. Lo scopo delle reti VPN è di dare ai singoli soggetti le stesse possibilità delle linee private in affitto ad un costo inferiore sfruttando le reti condivise pubbliche, garantendo l'impossibilità di accesso alla rete stessa da parte di soggetti terzi.

#### *Dirottamento di sessione (hijacking)*

Session hijacking (dirottamento di sessione) è una tecnica di attacco basata sull'intercettazione di una sessione valida al fine di accedere a risorse informatiche senza essere in possesso dei permessi necessari. Un utilizzo classico del session hijacking è l'intercettazione di una sessione utente al fine di accedere senza averne diritto ad un'area web ad accesso riservato.

Il dirottamento di sessione costituisce una delle più gravi minacce per i computer esposti su Internet. L'obiettivo è quello di ottenere l'accesso ad un computer facendoli credere di essere connessi ad un indirizzo fidato, l'attacco si concretizza quando l'hacker sostituisce parte dell'indirizzo IP dei pacchetti con quelli del proprio indirizzo alterando i numeri di sequenza.

La tecnica più utilizzata è quella denominata "man-in-the-middle attack", dove l'hacker si frappone nello scambio di dati tra due computer intercettandone le informazioni.

La tipologia di attacco hijacking è particolarmente pericoloso in quanto potenzialmente permette l'intercettazione dei messaggi tra la Sala Operativa e gli

Operatori di Telefonia con la possibilità di intervento sul contenuto del messaggio stesso.

#### *4.2.1.2. La Sicurezza Fisica*

La “Sicurezza Fisica”, riguarda la protezione fisica delle risorse e la definizione di misure atte a mantenere un ambiente di lavoro protetto che impedisca perdite di informazione e di patrimonio intellettuale di proprietà dell’ente.

Obiettivo della sicurezza fisica è quello di prevenire e ridurre il rischio di accessi fisici o virtuali non autorizzati e danni o interruzione di servizi (posta elettronica, accesso a sistemi informativi etc).

Un aspetto importante è il controllo dell'accesso ai locali che ospitano i sistemi che deve essere permesso ai soli addetti ai lavori che deve essere adeguato, ma anche la definizione di policy di disaster recovery.

Per la Sicurezza Fisica del luogo è necessario provvedere alle seguenti misure:

- *Accesso limitato e controllato alla sala macchina*  
Limitare e controllare tutti gli accessi ai vari locali e avvalendosi di sistemi di sicurezza elettronici come controllo con l’uso di badge o scanner biometrici.
- *Adeguare l'ambiente all'uso*  
Adottare sistemi di: Climatizzazione per mantenere l'ambiente ad una temperatura adeguata. Anti-incendio a gas, appropriati per i locali contenenti apparati elettronici ed elettrici. Gruppi elettrogeni per l'erogazione continua di elettricità anche in caso di down della linea principale.
- *Disaster recovery*  
Definire policy e installare sistemi per il disaster recovery, effettuare il backup e spostarli dal luogo dei sistemi in produzione.
- *Password sul BIOS*  
I comuni BIOS mettono a disposizione vari livelli di protezione basati sull'autenticazione utente tramite password. È possibile usufruire di questa protezione sia in caso di reboot della macchina o per il solo cambiamento delle impostazioni del BIOS, la soluzione consigliata è la seconda perché in caso di reboot volontario non verrà richiesto l'inserimento della password che dovrà essere inserita da locale.
- *Boot Loader*  
Ulteriore possibilità di protezione al boot è la password del proprio boot loader. In caso di un server è bene che al boot non venga richiesta nessuna password a meno che non venga modificata la procedura standard di boot, come ad esempio l'aggiunta di parametri all'avvio del kernel, questo per evitare la presenza fisica di un operatore ad ogni reboot. Analogamente va richiesta una password nel caso si cerchi di passare opzioni di boot diverse da quelle di default.  
Tenere presente che queste password sono facilmente superabili nel caso in cui il sistema venga riavviato effettuando un boot da cd-rom o da floppy.

- *Disattivare il reboot via tastiera*

In questo modo si evita la possibilità accidentale o dolosa di riavvio dell'apparecchiatura. La misura è particolarmente importante per servizi che devono garantire la disponibilità 7x24.

#### 4.2.2. *La sicurezza operativa*

La sicurezza operativa ha come obiettivo quello di limitare errori operativi o accessi non autorizzati alle informazioni. In questo contesto ci si riferisce in modo particolare al controllo della sicurezza per le applicazioni e l'infrastruttura interna alla Sala Operativa, applicazioni che permettono di diffondere verso la popolazione messaggi di alert.

Considerando il rischio di diffondere messaggi errati con la possibilità di generare allarmi non reali verso la popolazione, risulta particolarmente importante la definizione dei requisiti di sicurezza operativa. In particolare:

1. controllo degli accessi;
2. sicurezza della postazione di lavoro.

##### *Controllo degli accessi*

L'accesso alle applicazioni deve essere limitato al personale autorizzato: ciò richiede un meccanismo che riconosca la risorsa che si appresta all'utilizzo dell'applicazione.

Il dimensionamento di questo meccanismo dipende dall'importanza delle applicazioni e dagli effetti che esse producono: nel caso in esame l'effetto potenziale è quello di diffondere informazioni scorrette verso la popolazione.

Due requisiti fondamentali per la sicurezza operativa sono rappresentati dall'identificazione e autenticazione dell'utente.

*Identificazione:* è la procedura che permette all'applicazione di identificare l'utente che intende accedere a un determinato servizio. L'identificazione è costituito nel caso più semplice dal nome utente e nei casi più complessi da tessere provviste di microchip.

*Autenticazione:* è la procedura che verifica che la persona che si identifica sia effettivamente chi dichiara di essere. Il caso più comune è costituito dalla password, mentre casi più complessi possono essere lettura dell'impronta digitale o lettura dell'iride.

La fase di identificazione o di autenticazione hanno livelli di sicurezza crescenti in funzione delle policy e di conseguenza della tecnologia adottata per garantire la sicurezza logica. In particolare possono essere identificati:

1. credenziali (something you know);
2. smart card o badge (something you have);

### 3. riconoscimento biometrico (something you are).

È possibile aumentare la sicurezza logica per l'accesso ai servizi informatici combinando le forme di identificazione e autenticazione sopra citate: questo tipo di tecnica è conosciuta come autenticazione a due fattori (two factor authentication).

Normalmente la tecnica più utilizzata è quella delle credenziali anche se sempre più spesso anche su PC ad uso domestico sono comparsi sistemi di riconoscimento delle impronte digitali. Il riconoscimento tramite credenziali è soggetto a policy quali per esempio una lunghezza minima o massima, la presenza di caratteri alfanumerici (numeri e lettere), la presenza di lettere maiuscole o di caratteri speciali.

Limite delle credenziali risiede nella possibilità di essere in qualche modo spiate o captate al legittimo proprietario ed essere utilizzate per accedere dolosamente a servizi informatici cui non si è autorizzati ad accedere. E' evidente che sistemi più complessi sono meno soggetti ad abusi e di conseguenza garantiscono una maggior sicurezza per l'accesso ad applicazioni o risorse informatiche riservate.

Dopo l'autenticazione il passo successivo è quello della profilazione, ovvero vengono assegnati alla persona autenticata una serie di accessi a risorse informatiche di differente significato e importanza.

Nello scenario di una situazione di alert è importante che siano profilate correttamente le risorse che gestiscono le fasi necessarie per la diffusione di messaggi di alert è necessario che le autorizzazioni in punti chiave del processo definito siano date da responsabili della Sala Operativa piuttosto che da semplici operatori. L'autorizzazione all'accesso a informazioni o alla piattaforma che permette la diffusione di alert verso la popolazione deve essere normata da policy che definiscono le figure abilitate all'accesso di determinati servizi e sotto quali condizioni. Queste policy devono essere implementate tramite la configurazione o parametrizzazione di applicazioni che forzano il rispetto delle regole.

#### *4.2.2.1. I livelli autorizzativi*

L'accesso alle applicazioni e la profilazione degli utenti che dovranno provvedere alla diffusione di messaggi di alert dovranno essere stabiliti sulla base di livelli autorizzativi correlati ai ruoli prima definiti.

Sulla base dei ruoli definiti si dovranno associare dei livelli autorizzativi che consentono la corretta esecuzione del processo.

I livelli autorizzativi sono collegati al Ruolo 2 e al Ruolo 4 che consentono rispettivamente l'approvazione e la diffusione del messaggio.

**Tabella 4.4 - Matrice dei livelli autorizzativi**

	Presa in carico	Approvazio ne	Notifica	Autorizzazio ne
Ruolo 1				
Ruolo 2		X		
Ruolo 3				
Ruolo 4				X

Il Ruolo 1 e il Ruolo 3 non hanno associato dei livelli autorizzativi in quanto hanno il compito della presa in carico e definizione del contenuto informativo del messaggio (Ruolo 1) e della definizione e valorizzazione degli attributi del messaggio in termini di parametri di diffusione (Ruolo 3).

Le applicazioni informatiche che realizzeranno la procedura di gestione della diffusione del messaggio di alert dovranno implementare correttamente i ruoli definiti al fine di garantire la corretta diffusione del messaggio.

La non conformità del contenuto del messaggio o la non conformità degli attributi dello stesso rispetto i requisiti di diffusione comportano un riciclo del processo di composizione e diffusione del messaggio stesso.

In caso di urgenza e di necessità immediata di diffusione del messaggio di alert il Ruolo 4 può a sua discrezione decidere di abbreviare la procedura assumendo tutti i livelli autorizzativi per la composizione e diffusione del messaggio stesso.



## Capitolo 5

### *Studio interfaccia di comunicazione con Cell Broadcast Centre*

Il capitolo si propone di definire l'interfaccia di comunicazione tra la sala operativa della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza e il sistema di gestione del servizio Cell Broadcast della rete telefonica mobile. Già nella prima fase della ricerca, è stato identificato in Telecom Italia, l'operatore candidato ad essere partner di questo progetto di studio, sia per quanto riguarda l'approccio generale alla tecnologia che per quanto riguarda l'affiancamento nell'eventuale fase di realizzazione di un primo prototipo di sistema di allerting funzionante su un area predefinita, da realizzarsi in una fase successiva al completamento della ricerca stessa.

Il fatto di essere riusciti nella prima fase della ricerca ad identificare un unico operatore come partner della ricerca, ha delle implicazioni importanti sui risultati ottenuti.

Da una parte infatti, il fatto di interfacciarsi con un'unico interlocutore ha consentito di semplificare l'analisi consentendo di focalizzarsi al meglio sugli aspetti tecnici, evitando articolate e delicate azioni di normalizzazione delle procedure rispetto ad interlocutori con esigenze potenzialmente distanti su alcuni aspetti pratici, sia da un punto di vista dell'approccio che per quanto riguarda i contenuti.

Da un altro punto di vista, l'approccio può risultare carente per certi aspetti, e calibrato su una specifica implementazione tecnologica, risultando incompleto se condiviso con le procedure e la tecnologia di altri operatori. È altresì vero che la soluzione finale individuata con l'operatore partner, è stata appositamente studiata in modo da risultare facilmente replicabile con pochi adattamenti su tecnologie diverse, modificando e adattando il solo modulo di interfacciamento con il CBC del nuovo operatore stesso.

Telecom Italia ha da subito manifestato la sua disponibilità ed interesse ad approfondire i temi della ricerca. Con i referenti di Telecom Italia si è iniziato a ragionare su come impostare l'interfaccia di comunicazione che deve essere sviluppata tra la Sala Operativa della Protezione Civile e gli apparati di rete di telefonia mobile che implementano le funzionalità di Cell Broadcasting.

Inizialmente, su iniziativa di MOX Consulting che segue la parte tecnica della ricerca stessa, si è proposto all'operatore di impostare lo studio dell'interfaccia di connessione tra la Sala Operativa Protezione Civile e elementi di rete mobile, su

due fronti:

- stesura di un protocollo di comunicazione semplificato, nell'ottica di definire un primo sistema funzionante a tutti gli effetti ma con delle semplificazioni significative per quanto riguarda sia gli aspetti di completezza e solidità dell'interfaccia di comunicazione tra la sede della Direzione Generale Protezione Civile e il CBC dell'operatore di telefonia e sia la definizione dell'area di applicazione dei messaggi da inviare ai mobili (Progetto Pilota);
- impostazione, studio e specifica di dettaglio delle caratteristiche di una versione più evoluta e completa rispetto al prototipo nell'ottica di applicare il sistema di allerting sull'intera area del territorio regionale, con la possibilità di caratterizzare ed indirizzare al meglio il messaggio stesso (Sistema Evoluto).

In questa direzione MOX Consulting ha redatto un primo documento col quale si suggerivano due possibili diversi scenari, uno specifico per la realizzazione del trial, il progetto pilota da realizzarsi con modalità ridotta e semplificata e un secondo nell'ottica di realizzare un'interfaccia più completa per un sistema funzionante a tutti gli effetti a livello regionale.

## 5.1. Specifiche Progetto Pilota

Il seguente paragrafo descrive le fasi seguite per definire i requisiti di comunicazione tra la Direzione Generale Protezione Civile e il CBC dell'operatore di telefonia, nell'ottica di implementare rapidamente un primo trial del sistema di comunicazione ai cittadini.

Le intenzioni fissate fin dall'inizio della ricerca, erano quelle di strutturare un sistema semplificato ma con funzionalità comunque compatibili, per quanto possibile con lo spirito dell'approccio generale della ricerca in termini di qualità del servizio che si intende proporre all'utente finale.

### *5.1.1. Comunicazione Sala Operativa verso CBC operatore: Primo scenario ipotizzato*

Il primo passo verso la formalizzazione di un protocollo semplificato di comunicazione tra Sala Operativa e CBC dell'operatore, è stato suggerito inizialmente da MOX a Telecom Italia.

In questo paragrafo descriviamo brevemente i principi che stanno alla base della proposta di funzionamento concludendo con una serie di considerazioni e commenti derivati dalla discussione dei temi con l'operatore stesso.

Le principali caratteristiche e vincoli che sono stati inizialmente suggeriti

all'operatore partner per il sistema prototipale sono elencabili come segue:

- comunicazione PC - CBC via mail, simulando contenuti e modalità del protocollo reale;
- template di definizione del messaggio da inviare fissato a priori
- possibilità di definire:
  - testo del messaggio a cura della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza;
  - frequenza di ripetizione in aria (intervallo tra una ripetizione e la successiva);
  - numero di ripetizioni totali richieste;
  - testo del messaggio in due lingue (ITA, ENG);
  - numero di pagine per messaggio fissa a uno;
- area di Broadcasting fissa per tutti i messaggi, corrispondente alla zona Rho Fiera, zona "EXPO 2015" (o altra area identificata come area campione dal gruppo di ricerca);
- possibilità di attivare la schedulazione di un solo messaggio alla volta sulla rete telefonica dell'operatore;
- Message Identifier e Serial Number fissi per tutti i messaggi inviati dalla PC. Alla ricezione di una nuova richiesta, l'eventuale messaggio più "vecchio" in fase di schedulazione, viene cancellato e rimpiazzato da quello contenuto nella nuova richiesta;
- capacità del sistema CBC o di un suo componente esterno, di inviare mail di conferma di esecuzione del comando richiesto.

La scelta si basa sull'impostazione di un protocollo molto semplice di comunicazione basato sull'invio di mail dalla Sala Operativa verso il CBC dell'operatore di telefonia. Il contenuto della mail riporta direttamente, secondo uno schema predefinito e condiviso tra la Sala Operativa e il gestore dell'apparato CBC, i dettagli del messaggio da inviare:

- Testo del messaggio in Italiano
- Testo del messaggio in versione Inglese
- Frequenza di ripetizione
- Numero di ripetizioni totali richieste

L'area di distribuzione del messaggio è nelle intenzioni fissata a priori e coincide con l'area scelta per il trial, mentre i valori del Message Identifier e del Serial Number sono fissi e impostati a priori.

Le primitive definite a livello di protocollo per la gestione dei messaggi prevedono la possibilità di

- creare un nuovo messaggio;
- cancellare un messaggio schedulato;
- interrogare il CBC sullo stato di trasmissione del messaggio inviato.

Sulla base di quanto detto, la richiesta di *invio per un nuovo messaggio* deve essere specificata via mail con la seguente struttura contenuto informativo:

Oggetto mail:

creazione messaggio

Contenuto mail:

message type: create

message text ITA: Messaggio di prova: Prova di Cell Broadcasting su area Expo 2015

message text ENG: Test Message: Cell Broadcasting Trial over Expo 2015 Area

message frequency: 1 minuto

message repetition: 120

Analogamente la richiesta di eliminazione del messaggio precedente viene essere fatta come:

Oggetto mail:

Eliminazione messaggio

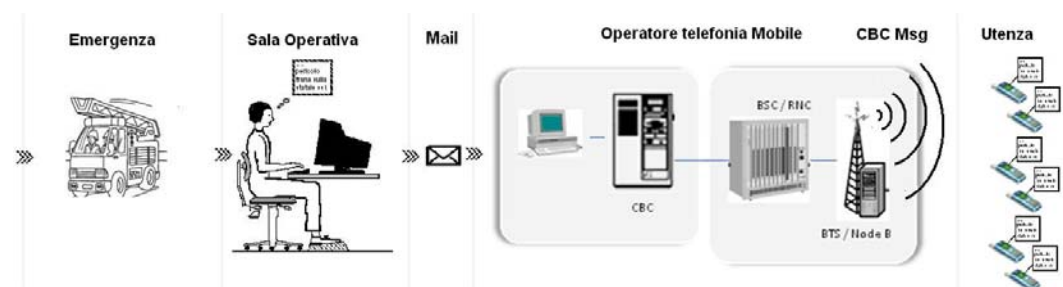
Contenuto mail:

message type: Cancel

Nella fase di prototipo è prevista la possibilità' di attivare un unico messaggio sul CBC, quindi per la sua cancellazione non è richiesto di specificare per quale messaggio si richiede la cessazione della schedulazione verso l'utenza.

Il sistema dell'operatore di telefonia, scompone il messaggio ricevuto nelle sue componenti in modo automatico da un software realizzato ad hoc e i contenuti vengono indirizzati al CBC dell'operatore secondo le specifiche proprie della macchina stessa.

In questo modo i messaggi di prova compilati in Sala Operativa possono essere facilmente e velocemente inviati al CBC, con un meccanismo molto semplice ed efficace schematizzabile come segue:



## Proposta iniziale di interfaccia di comunicazione Sala Operativa - CBC

### *5.1.2. Considerazioni sul primo scenario ipotizzato*

La proposta di interfaccia presentata e proposta è stata oggetto di analisi da parte dei referenti tecnici dell'operatore di telefonia partner.

Sulla base degli elementi presenti nella proposta e ragionando rispetto alle caratteristiche di funzionamento del CBC utilizzato dall'operatore, sono state fatte alcune considerazioni che hanno portato alla definizione di una proposta differente rispetto a quanto ipotizzato e che hanno portato a semplificare il sistema per il prototipo e ad ipotizzare una soluzione che come vedremo più' avanti si avvicina molto a quella che potrebbe essere la soluzione del Sistema evoluto di comunicazione tra Sala Operativa e CBC dell'operatore.

L'analisi congiunta con l'operatore ha evidenziato che il sistema proposto, oltre ad essere poco evoluto, richiedeva anche uno sforzo maggiore di implementazione rispetto alla soluzione finale "a regime", che è risultata essere di più semplice implementazione grazie ad alcune funzionalità software già presenti sul CBC che l'operatore intende utilizzare per il sistema di allerting.

La realizzazione del sistema di generazione automatica delle mail verso il CBC, e dall'altra di un sistema automatico ed intelligente di elaborazione delle mail ricevute e della relativa codifica in formato "CBC", risulta poco conveniente, specie considerando il fatto che nell'ottica di voler realizzare un sistema definitivo ed evoluto, il prototipo sviluppato non è riutilizzabile e il lavoro sarebbe stato solo un esercizio finalizzato alla prima prototipizzazione del sistema stesso.

Si è dunque concordata l'implementazione di un sistema di comunicazione in fase di trial, già impostato nella direzione del funzionamento su larga scala, scalabile e flessibile e al tempo stesso minimamente oneroso in termini di realizzazioni di specifici applicativi software, per l'operatore di telefonia. La definizione quindi del sistema di interfacciamento della Sala Operativa con il CBC dell'operatore partner, segue le indicazioni riportate nel paragrafo seguente, che descrive la proposta per l'interfacciamento del sistema evoluto.

## 5.2. Specifiche Sistema Evoluto

In questo paragrafo sono dettagliati gli aspetti di comunicazione tra la Direzione Generale Protezione Civile, Polizia Locale e Sicurezza e il CBC dell'operatore di telefonia, nell'ottica di realizzare come anticipato nel paragrafo precedente, sia un sistema di comunicazione per il progetto prototipo, sia un sistema di alerting evoluto e capillare a livello regionale per la comunicazione ai cittadini.

Per definire le caratteristiche e il contenuto informativo dei messaggi inviati dalla centrale della sala operativa della protezione civile in direzione del CBC dell'operatore di telefonia scelto, si è preso in esame l'interfaccia tra lo stesso CBC

e i BSC della rete, cercando di identificare gli elementi caratterizzanti i Cell Broadcast messages stessi e come questi possono essere utilizzati per meglio identificare e distinguere le varie tipologie di messaggi che devono essere indirizzati agli utenti finali da parte della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza da un lato e per interagire in modo efficace con l'elemento di rete CBC dell'operatore Mobile dall'altro.

In questo contesto si sono prese come riferimento le specifiche di interfaccia descritte nello standard 3GPP 23.041, per perfezionare in seguito il dettaglio dell'interfaccia in funzione delle caratteristiche specifiche implementate dall'operatore specifico.

In quest'ottica è possibile identificare tre funzionalità tipiche che dovranno essere realizzate:

- funzionalità di Gestione protocollo;
- funzionalità di Amministrazione del DB dei messaggi sul CBC (e di conseguenza sui BSC della rete);
- funzionalità relative ai Parametri caratterizzanti il messaggio.

Le funzionalità, oltre che soddisfare i requisiti procedurali sopra esposti, costituiranno l'interfaccia tra Direzione Generale Protezione Civile, Polizia Locale e Sicurezza e CBC dell'operatore, permettendo di implementare i comandi e le funzioni di base utili al corretto funzionamento di un sistema di alert completo e sicuro. Le funzionalità relative alla gestione del protocollo di comunicazione tra Direzione Generale Protezione Civile, Polizia Locale e Sicurezza e CBC dell'operatore sono indirizzate all'implementazione di tutti gli aspetti di apertura e gestione di una sessione di collegamento tra gli apparati della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza e il CBC, le funzionalità di amministrazione del DB identificano le primitive che permettono la corretta gestione della messaggistica di alerting da parte della struttura della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza, mentre le funzionalità relative ai parametri dei messaggi, riferiscono alle caratteristiche specifiche di invio dei messaggi verso la popolazione.

Nei seguenti paragrafi le singole funzionalità vengono meglio descritte e dettagliate.

#### *5.2.1. Gestione Protocollo*

In questa sessione ci occuperemo dei messaggi che hanno lo scopo di implementare la gestione del protocollo tra Direzione Generale Protezione Civile, Polizia Locale e Sicurezza e CBC dell'operatore e possono essere dedicati all'apertura di una sessione, la sua chiusura e alla gestione degli aspetti di sicurezza quali la gestione degli accessi e l'impostazione delle credenziali dell'utenza di Direzione Generale Protezione Civile, Polizia Locale e Sicurezza.

Le principali primitive che rientrano in questo contesto sono le seguenti:

- Connect: Apertura di una connessione tra Direzione Generale Protezione Civile, Polizia Locale e Sicurezza e CBC;
- Disconnect: Chiusura di una sessione;
- PasswordMng: Gestione password operatore.

Le specifiche di dettaglio di questa funzionalità dovranno essere impostate e condivise con i referenti tecnici dell'operatore di telefonia.

### 5.3. Amministrazione del DB

In questa arte sono definite le caratteristiche di interfacciamento tra Direzione Generale Protezione Civile, Polizia Locale e Sicurezza e CBC, per quanto riguarda le primitive e i flussi di messaggi utili al controllo del data base dei messaggi che la Direzione Generale Protezione Civile, Polizia Locale e Sicurezza vuole gestire sul CBC dell'operatore.

Distinguiamo il flusso delle informazioni nelle due direzioni, ovvero in uscita ed in entrata dalla Direzione Generale Protezione Civile, Polizia Locale e Sicurezza.

#### 5.3.1. Interfaccia PC - CBC

Per quanto concerne l'interfaccia in direzione Direzione Generale Protezione Civile, Polizia Locale e Sicurezza - CBC, le primitive che permettono il controllo della spedizione dei messaggi di Cell Broadcast da parte della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza sono le seguenti:

- Insert: Consente di registrare ed attivare un nuovo messaggio;
- Cancel: Consente di cancellare un messaggio precedentemente registrato;
- Query: Consente di richiedere informazioni circa lo stato di un messaggio.

La sintassi e i formalismi da rispettare nell'implementazione delle primitive descritte, viene riportata in seguito. In questi paragrafi è definito il contenuto informativo dei singoli comandi e descriviamo alcuni aspetti tecnici dei comandi stessi.

##### 5.3.1.1. Insert

Il comando di Insert inviato dalla sede della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza verso l'operatore di telefonia Mobile, ha lo scopo di registrare un nuovo messaggio di Cell Broadcast sul CBC e di definirne le caratteristiche di Broadcasting. Il codice identificativo di questa primitiva dovrà essere definito in modo univoco tra la Direzione Generale Protezione Civile, Polizia Locale e Sicurezza e l'operatore di telefonia.

Per i dettagli che riguardano campi che caratterizzano il Broadcast vero e proprio si rimanda al paragrafo seguente. In questo contesto ci limitiamo a definire i parametri che serviranno a definire nome e cognome del messaggio stesso: Message ID e Serial Number.

*Message Identifier*: Il codice identificativo dei messaggi originati dalla protezione Civile, dovrà essere definito di comune accordo tra Direzione Generale Protezione Civile, Polizia Locale e Sicurezza e Operatore. Si ipotizza un Message Identifier UNICO per tutti i messaggi che hanno come originatore la sala operativa della Protezione Civile, in modo da facilitare il processo di fidelizzazione degli utenti finali almeno per quanto concerne le impostazioni degli apparati mobili. A titolo puramente indicativo, si suggerisce il codice 920, già utilizzato in precedenti contesti simili internazionali.

*Serial Number*: Il numero seriale dei messaggi inviati dalla Direzione Generale Protezione Civile, Polizia Locale e Sicurezza, è impostato su due BYTE e versa costruito secondo le seguenti regole, salvo diverse indicazioni fornite dall'operatore di telefonia Mobile.

I due ottetti del SR vengono suddivisi in gruppi di bit. In particolare la suddivisione viene fatta in tre gruppi, che identificano i campi Geographical Scope, Message Code e Update Number, come riportato nel seguente schema:

Octet 1								Octet 2							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
G.Scope		Message Code								Upd Number					

*Gscope*: Il valore attribuito al GeographicalScope, è utilizzato principalmente dal terminale mobile, e ai fini dell'applicazione che si vuole implementare, porta con sé l'indicazione del Display Mode, ovvero di come il messaggio dovrà essere gestito in termini di visualizzazione sul display del terminale mobile. Il valore indicato nei messaggi dalla Direzione Generale Protezione Civile, Polizia Locale e Sicurezza, è fissato al valore binario '00', col quale si indica al mobile immediate display, ovvero visualizzazione immediata ed automatica sul display del terminale mobile senza alcun intervento da parte dell'utente.

*Message Code*: Il message code viene utilizzato per differenziare i messaggi originati dalla Direzione Generale Protezione Civile, Polizia Locale e Sicurezza, che come indicato precedentemente hanno in comune il campo Message Identifier.

*Update Number*: Il campo Update Number, avrà sempre valore uguale a zero. La gestione di diverse versioni di un messaggio verrà fatta direttamente dalla sala operativa della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza, eliminando, se necessario, messaggi vecchi o superati nel loro contenuto informativo, e inserendone altri completamente nuovi.



In sintesi il campo Serial Number avrà come parte variabile sempre e solo il campo Message Code, che sarà elemento fondamentale per distinguere i diversi messaggi con originatore la Direzione Generale Protezione Civile, Polizia Locale e Sicurezza.

#### *5.3.1.2. Cancel*

Il comando di Cancel, ha lo scopo di gestire l'eliminazione di un messaggio precedentemente inviato e non ancora scaduto come periodo di ripetizione dalle BTS verso i mobili

Il messaggio da rimuovere dal database del CBC sarà identificato dalla coppia Message Id e Serial Number indicati nella richiesta proveniente dalla Direzione Generale Protezione Civile, Polizia Locale e Sicurezza. I due campi MSG Id e Serial Number identificano in modo univoco il messaggio da eliminare. In caso di necessità da parte della Direzione Generale Protezione Civile, Polizia Locale e Sicurezza, di rimpiazzare un messaggio precedentemente inviato con uno con testo aggiornato e più consoni a gestire la situazione, sarà cura della stessa PC procedere con l'eliminazione del vecchio messaggio (con comando di Cancel) ed invio del nuovo messaggio con testo modificato (con comando di Insert).

#### *5.3.1.3. Query*

Il comando di Query, ha lo scopo di fornire informazioni statistiche circa lo stato di spedizione di un messaggio precedentemente inviato e non ancora scaduto come periodo di ripetizione dalle BTS verso i mobili.

Il messaggio per il quale si richiedono informazioni di spedizione, sarà identificato dalla coppia Message Id e Serial Number indicati nella richiesta proveniente dalla PC. Anche in questo caso, i due campi MSG Id e Serial Number identificano in modo univoco il messaggio di interesse.

### *5.3.2. Interfaccia CBC - PC*

Per quanto concerne l'interfaccia in direzione CBC - PC, si ipotizza di implementare le seguenti primitive:

- *Insert:*  
primitiva che consente l'inserimento di un nuovo messaggio nel sistema
- *Cancel:*  
primitiva che consente la cancellazione di un messaggio inserito
- *Query:*  
primitiva che consente al gestore del servizio di interrogare il sistema per avere indicazioni sullo stato di funzionamento

### *5.3.3. Parametri caratterizzanti del Messaggio*

I parametri caratterizzanti ogni singolo messaggio dovranno essere i seguenti:

- Messagi ID: implementato ed utilizzato come sopra descritto;
- Serial Number: implementato ed utilizzato come sopra descritto;
- Area di broadcasting: le regole di definizione devono essere meglio definite tra PC e operatore Mobile durante la fase di implementazione del sistema. Si suggerisce in questo contesto un dettaglio a livello di quadranti di provincia, identificando provincia e quadrante interessato: NordOvest, NordEst, SudOvest e SudEst;
- Periodo di Ripetizione: Durata della ripetizione del singolo messaggio da parte delle BTS interessate;
- Frequenza di ripetizione: Identifica l'intervallo di tempo di ripetizione del singolo messaggio in aria da parte delle BTS interessate;
- Codifica del linguaggio: Identifica la lingua in cui il messaggio è scritto;
- Testo del Messaggio: identifica il testo vero e proprio del messaggio inviato da inviarsi agli utenti. Si ipotizza di fissare il numero dei caratteri significativi di testo a 93, e di limitare il numero di pagine del singolo messaggio stesso ad UNO.

## **5.4. Realizzazione del progetto pilota: linee guida**

### *5.4.1. Formalizzazione messaggi interfaccia PC - CBC*

L'accesso al servizio Cell Broadcast attraverso un opportuna interfaccia, consente agli operatori della sala operativa della protezione civile regionale, di effettuare le operazioni di Cancel, Insert e Query relativamente ai messaggi di Cell Broadcast, previa mutua autenticazione.

L'interfaccia di comunicazione è stata analizzata in collaborazione con il partner di telefonia mobile. La soluzione finale proposta è impostata su un'interfaccia web con architettura client server. Nello specifico la parte di client richiedente deve essere realizzata presso la sala operativa della regione, mentre la parte server viene implementata su apposita Smart Platform direttamente sugli apparati di telefonia dell'operatore, che provvederà anche all'abilitazione degli indirizzi IP del richiedente.

Le richieste provenienti dalla sala operativa e le relative risposte, devono transitare su connessioni sicure usando il protocollo HTTPS con mutua autenticazione. Tali richieste andranno indirizzate alla Smart Platform tramite URL concordata con il seguente formato.

`https://<IP address>[:<port>]/CBC/FrontEnd`

La piattaforma messa a disposizione dall'operatore, si attende una transazione di tipo **POST**, un contenuto di tipo **application/x-www-form-urlencoded** ed una variabile di nome **xmlRequest** che contiene un documento in formato XML.

Nel seguito un esempio che riporta in modo schematico il flusso di una richiesta da parte del sistema in sala operativa e la relativa risposta da parte dell'applicativo installato presso l'operatore di telefonia mobile:

*Richiesta:*

```
POST /MAP3/FrontEnd http/1.1
Host: www.myhost.foo
Content-Type: application/x-www-form-urlencoded
Content-Length: xx
```

```
xmlRequest=<Request>...</Request>
```

*Risposta:*

```
200 OK
Content-Type: text/xml
Content-Length: yy
```

```
<?xml version=1.0" encoding="utf-8"?><Response>...</Response>
```

Nel prossimo paragrafo viene illustrato il formalismo XML che deve essere utilizzato per gestire le richieste dalla sala operativa verso gli apparati di rete dell'operatore e la struttura delle rispettive risposte.

#### *5.4.1.1. Richieste*

Il documento XML associato alla variabile `xmlRequest` è composto da varie sotto strutture contenute nella sezione `Request`:

```
<Request>
  <Header>...</Header>
  <Parameters>...</Parameters>
</Request>
```

La sezione *Header* del documento contiene informazioni presenti per qualsiasi tipologia di richiesta. Tale sezione viene riportata con le medesime informazioni anche nel messaggio di risposta.

La sezione *Parameters* contiene invece i parametri relativi alla specifica tipologia di servizio richiesto.

#### 5.4.1.2. Risposte

Il documento XML di risposta è composto da varie sotto strutture contenute nella sezione Response:

```
<Response>
  <Header>...</Header>
  <Parameters>...</Parameters>
</Response>
```

#### 5.4.1.3. Esito delle richieste

Oltre ai codici di errore standard gestiti al livello del protocollo HTTP, vengono predefiniti i seguenti codici per il tag <ResultCode> presente nelle varie tipologie di risposte:

- **1xx** - Si riferisce ad errori relativi alla validazione di una richiesta
  - 101 - Metodo non valido*
  - 102 - Content type non valido*
  - 103 - Parametro xmlRequest assente*
  - 104 - Errore di parsing XML*
  - 105 - Elemento o contenuto richiesto assente*
  - 106 - Servizio non valido*
  - 107 - Operazione non valida*
  - 108 - Contenuto non valido*
- **200** - Richiesta evasa con successo
- **3xx** – Sono gli errori di comunicazione con la componente CBC
  - 301 - Timeout*
- **5xx** - Sono gli errori interni al servizio CBC che dipendono dalla funzionalità richiesta
  - To be defined*

#### **Cancel**

*To be defined*

#### **Insert**

*To be defined*

#### **Query**

*To be defined*

Altri valori specifici (1xx, 3xx o 5xx) potranno essere definiti ulteriormente.

Nel seguente paragrafo vengono analizzati i flussi informativi relativamente alle diverse primitive messe a disposizione dall'operatore per il corretto e completo controllo dei messaggi di Cell Broadcast.

### 5.4.2. Comando di Insert

#### 5.4.2.1. Richiesta (Sala Operativa -> Operatore)

##### **Header**

Di seguito una descrizione dei parametri contenuti sotto il tag <Header>:

Tag	Descrizione	Valore
Service	Tipologia di servizio	<b>CBC</b>
OperationType	Tipologia di operazione richiesta.	<b>Insert</b>
OperationKey	Identificativo univoco della richiesta per il sistema richiedente	È riportato "as-is" nel messaggio di risposta ad uso esclusivo del richiedente.
ClientId	Sistema richiedente	Il valore va concordato e fornito nella richiesta, es. "Trial-Expo2015"
Priority	Priorità	Per uso futuro

##### **Parameters**

Di seguito una descrizione dei parametri contenuti sotto il tag <Parameters>:

Node	Descrizione	Valore
Messages	Definizione dei messaggi	TBD
<b>Subnodes</b>	<b>Descrizione</b>	<b>Valore</b>
Message	Informazioni relative al singolo messaggio	TBD
	Attributo <i>duration</i> valorizzato con la durata di ripetizione.	
	Attributo <i>frequency</i> valorizzato con la frequenza di ripetizione.	
	Attributo <i>start</i> valorizzato con la data di attivazione.	
	Attributo <i>text</i> valorizzato con il contenuto del messaggio.	

#### 5.4.2.2. Risposta (Operatore -> Sala Operativa)

Il documento XML di risposta è composto da varie sotto strutture contenute nella sezione Response:

```
<Response>  
  <Header>...</Header>  
  <Parameters>...</Parameters>  
</Response>
```

### *Header*

Vedere paragrafo precedente.

### *Parameters*

I parametri presenti nella risposta sono i seguenti:

Tag	Descrizione	Valore
ResultCode	Codice esito della richiesta	Può assumere uno dei valori definiti al paragrafo § <b>Errore. L'origine riferimento non è stata trovata.</b>
ResultMessage	Messaggio che descrive l'esito della richiesta	In caso di esito negativo contiene la descrizione dell'errore

Node	Descrizione	Valore
Messages	Informazioni sui messaggi	TBD
<b>Subnodes</b> Message	<b>Descrizione</b> Informazioni relative al singolo messaggio  Attributo <i>id</i> valorizzato con l'id associato al messaggio.  Attributo <i>duration</i> valorizzato con la durata di ripetizione.  Attributo <i>frequency</i> valorizzato con la frequenza di ripetizione.  Attributo <i>start</i> valorizzato con la data di attivazione.  Attributo <i>text</i> valorizzato con il contenuto del messaggio.	<b>Valore</b>  TBD

### *5.4.3. Comando di Cancel*

#### *5.4.3.1. Richiesta (Sala Operativa -> Operatore)*

### *Header*

Di seguito una descrizione dei parametri contenuti sotto il tag <Header>:

Tag	Descrizione	Valore
Service	Tipologia di servizio	<b>CBC</b>
OperationType	Tipologia di operazione richiesta.	<b>Cancel</b>
OperationKey	Identificativo univoco della richiesta per il sistema richiedente	È riportato "as-is" nel messaggio di risposta ad uso esclusivo del richiedente.
ClientId	Sistema richiedente	Il valore va concordato e fornito nella richiesta, es. "Trial-Expo2015"
Priority	Priorità	Per uso futuro

### Parameters

Di seguito una descrizione dei parametri contenuti sotto il tag <Parameters>:

Tag	Descrizione	Valore
Message	Attributo <i>id</i> valorizzato con l'id associato al messaggio da cancellare.	TBD

#### 5.4.3.2. Risposta (Operatore -> Sala Operativa)

Il documento XML di risposta è composto da varie sotto strutture contenute nella sezione Response:

```
<Response>
  <Header>...</Header>
  <Parameters>...</Parameters>
</Response>
```

### Header

Vedere paragrafo §0.

### Parameters

I parametri presenti nella risposta sono i seguenti:

Tag	Descrizione	Valore
ResultCode	Codice esito della richiesta	Può assumere uno dei valori definiti al paragrafo § <b>Errore. L'origine riferimento non è stata trovata.</b>
ResultMessage	Messaggio che descrive l'esito della richiesta	In caso di esito negativo contiene la descrizione dell'errore

#### 5.4.4. Comando di Query

##### 5.4.4.1. Richiesta (Sala Operativa -> Operatore)

### Header

Di seguito una descrizione dei parametri contenuti sotto il tag <Header>:

Tag	Descrizione	Valore
Service	Tipologia di servizio	<b>CBC</b>
OperationType	Tipologia di operazione richiesta.	<b>Query</b>
OperationKey	Identificativo univoco della richiesta per il sistema richiedente	È riportato "as-is" nel messaggio di risposta ad uso esclusivo del richiedente.
ClientId	Sistema richiedente	Il valore va concordato e fornito nella richiesta, es. "Trial-Expo2015"
Priority	Priorità	Per uso futuro

#### 5.4.4.2. Risposta (Operatore -> Sala Operativa)

Il documento XML di risposta è composto da varie sotto strutture contenute nella sezione Response:

```
<Response>
  <Header>...</Header>
  <Parameters>...</Parameters>
</Response>
```

##### Header

Vedere paragrafo precedente0.

##### Parameters

I parametri presenti nella risposta sono i seguenti:

Tag	Descrizione	Valore
ResultCode	Codice esito della richiesta	Può assumere uno dei valori definiti al paragrafo §Errore. L'origine riferimento non è stata trovata.
ResultMessage	Messaggio che descrive l'esito della richiesta	In caso di esito negativo contiene la descrizione dell'errore

Node	Descrizione	Valore
Messages	Informazioni sui messaggi	TBD
Subnodes		
Message	Informazioni relative al singolo messaggio	TBD
	Attributo <i>id</i> valorizzato con l'id associato al messaggio.	
	Attributo <i>channel</i> valorizzato con il canale in uso.	
	Attributo <i>duration</i> valorizzato con la durata di ripetizione.	
	Attributo <i>frequency</i> valorizzato con la frequenza di ripetizione.	
	Attributo <i>operation</i> valorizzato con il tipo di operazione richiesta.	
	Attributo <i>start</i> valorizzato con la data di attivazione.	
	Attributo <i>status</i> valorizzato con lo stato della richiesta.	
	Attributo <i>text</i> valorizzato con il contenuto del messaggio.	



#### *5.4.5. Caratteristiche valide per sistema di Trial*

Il sistema utilizzato per il trial sarà progettato ed implementato introducendo volutamente alcune limitazioni nel servizio erogato in modo da realizzare da una parte un prototipo semplificato e di più' rapida implementazione, e dall'altra un sistema più' facilmente monitorabile, per focalizzare l'attenzione sugli aspetti che riguardano l'efficacia e i contenuti della comunicazione piuttosto che aspetti strettamente legati alla tecnologia stessa in uso.

Una prima limitazione che si intende realizzare è legata all'area di broadcast individuata per la realizzazione del trial.

Come visto in precedenza, una delle caratteristiche fondamentali del sistema di Cell Broadcast, è sicuramente quella di poter indirizzare superfici geografiche piccole o grandi a piacere.

Nella realizzazione del trial si è deciso di limitare l'area di azione del sistema alla zona nord est di Milano, indicata come Area Expo2015.

La scelta di limitare il campo di azione del sistema ad un'area molto ben circoscritta e fissata a priori, è dovuta al fatto che il trial non è indirizzato a testare la tecnologia di Cell Broadcast in quanto tale, ma a testare e validare le potenzialità e l'efficacia.

In questo senso fissando in modo rigido e a priori l'area di impatto del trial, è possibile instaurare un contatto diretto con la popolazione e monitorare adeguatamente il territorio indirizzato, ricavandone indicatori precisi, e in modo rapido, sulla qualità del servizio stesso che ne permettano la migliore messa a punto.

Sempre nell'ottica di semplificare ed ottimizzare le operazioni di monitoring del servizio, si è scelto di limitare il numero dei messaggi di Broadcast contemporanei ad un singolo messaggio. Questo vuol dire che nelle fasi di set up e messa a punto del sistema, la sala operativa avrà la possibilità di inviare un solo messaggio per volta sull'area prescelta, ed eventuali nuovi messaggi andranno sempre a sostituire ed eliminare il precedente.

Anche questo vincolo è stato concepito nell'ottica di non complicare la fase di acquisizione di familiarità verso il nuovo tipo di servizio da parte dell'utenza, in modo da poter concentrare le attenzioni verso aspetti di base e più' centrali del nuovo sistema di comunicazione verso la popolazione.

#### *5.4.6. Altri aspetti implementativi & organizzativi*

##### *5.4.6.1. Coinvolgimento della popolazione*

Obiettivo principale del prototipo è quello di verificare l'efficacia nella diffusione dei messaggi verso la popolazione. In questo senso diventa importante definire cosa si intende misurare, individuare ed applicare un metodo che consenta di comprendere come il campione di utenti si comporta a fronte del ricevimento di un messaggio 'reale'.

Questa assunzione implica la necessità di stabilire dei criteri e degli indicatori che consentano di verificare e misurare sul campo l'efficacia della nuova

tecnologia.

I punti sui essenziali da analizzare e sviluppare riguardano la definizione dei seguenti aspetti:

- identificazione e coinvolgimento della popolazione;
- predisposizione delle modalità di esecuzione del pilota;
- abilitazione dei terminali mobili.

Il raggiungimento dell'obiettivo implica la predisposizione degli strumenti necessari per il coinvolgimento attivo del campione della popolazione dal punto di vista metodologico e dal punto di vista tecnologico. In questa direzione dovranno essere predisposti degli strumenti per la raccolta di informazioni che permettano di comprendere ed elaborare il comportamento della popolazione a seguito del trial.

L'approccio suggerito dovrà prendere spunto dai risultati dell'analisi dei case study oggetto della ricerca: in particolare il caso olandese considerato tra i più avanzati a livello europeo, l'esperienza CHORIST, nonché gli studi effettuati da Giappone e India.

Gli obiettivi dell'analisi, i criteri e le misurazioni dovranno essere discussi e condivisi con la Direzione Generale Protezione Civile, Polizia Locale e Sicurezza.

#### *5.4.6.2. Gestione dei terminali mobili*

Una parte fondamentale nel progetto di trial, ha la definizione delle procedure da attuarsi per l'abilitazione dei terminali mobili alla ricezione dei messaggi di Cell Broadcast. Come visto in precedenza, l'abilitazione dei diversi terminali alla ricezione dei messaggi di Cell Broadcast, non è sempre agevole e in molti casi neppure facile.

Per la configurazione dei terminali dell'utenza campione all'interno del progetto di trial, si ipotizza di orientarsi verso due tipi di soluzione. Una modalità automatica e una manuale per avere la possibilità di configurare il maggior numero possibile di terminali mobili:

- 1 abilitazione manuale diretta, sotto la supervisione di un esperto, utilizzando le indicazioni fornite dal produttore dei terminali mobili;
- 2 abilitazione del servizio Cell Broadcast tramite un'applicazione software realizzata ad hoc. Tale applicazione potrà essere caricabile su un set predefinito di modelli, che abilita la ricezione del Cell Broadcast. Questa funzionalità potrà essere utilizzata sui terminali mobili con supporto nativo di Java.

Queste premesse non garantiscono a priori la copertura della configurazione di qualsiasi tipo di terminale mobile. Eventuali campioni di utenza per i quali non sarà possibile garantire la corretta configurazione dei terminali mobili, dovranno essere necessariamente esclusi a priori dal campione di riferimento per la prima fase di testing delle funzionalità del servizio.

Allo stato attuale della ricerca, l'unico operatore che ha partecipato in modo

attivo allo studio della soluzione di comunicazione via Cell Broadcast, è stato Telecom Italia, che ha anticipato anche un forte interesse a partecipare alla fase di trial. In base a ciò risulta vincolante il fatto che l'utenza selezionata dovrà essere dotata di connessione mobile con SIM card di Telecom Italia.

#### *5.4.6.3. Elaborazione feedback e presentazione*

Un'efficace raccolta ed elaborazione dei dati relativi all'analisi delle informazioni raccolte dalla popolazione richiede la predisposizione di un'applicazione che metta a disposizione un Database e una serie di algoritmi che rendano disponibili gli indicatori richiesti.

I requisiti richiesti dovranno essere definiti a valle della scelta delle misure da effettuare e della definizione dei relativi criteri. L'applicazione dovrà essere costituita da un layer di data entry, un layer di storage dati (DB), un layer di calcolo, e un layer di reporting.



## Allegato

### *Acronimi, glossario e riferimenti*

#### *Lista degli acronimi e glossario:*

- 3GPP 3rd Generation Partnership Project
- ANSI American National Standards Institute
- ARIB Association of Radio Industries and Business (Giappone)
- ATIS Alliance for Telecommunications Industry Solutions WTSC Wireless Technologies and Systems Comitee
- BLUETOOTH specifica industriale per reti personali senza fili (WPAN: Wireless Personal Area Network)
- BSC Base Station Controller - elemento che fa da ponte tra la Mobile Switching Center e la BTS
- BSS Base station Subsystem
- BTS Base Transceiver Station - Stazione radio base, ripetitore di segnali radio
- CBC Cell Broadcast Center
- CBE Cell Broadcast Entity
- CEASA Cellular Emergency Alert System Association (CEASA)
- CEPT Conferenza Europea delle amministrazioni delle Poste e delle Telecomunicazioni
- CMAS Commercial Mobile Alert System
- CMSAAC Commercial Mobile Service Alerts Advisory Committee
- CN Core network
- COP Common Operational Picture
- CS Circuit switch
- CWTS China Wireless Telecommunication Standard Group
- DTM Dual Transfer Mode
- DVB-H Digital Video Broadcasting - Handheld: standard del consorzio europeo DVB per una modalità di radiodiffusione terrestre studiata per trasmettere programmi TV, radio e contenuti multimediali ai dispositivi mobili, come i più comuni smartphone, i palmari e i telefoni cellulari evoluti
- EDGE Enhanced Data rates for GSM Evolution
- EENA European Emergency Number Association
- EEWS Earthquake Early Detection Warning system
- EGPRS Enhanced GPRS

- EIR Equipment Identity Register
- ETSI European Telecommunications Standard Institute
- FCC Commissione delle Comunicazioni Federali degli stati uniti
- FTP File Transfer Protocol
- Frequency hopping tecnica di trasmissione radio usata per aumentare la larghezza di banda di un segnale
- GERAN GSM EDGE Radio Access Network
- GGSN nodo con funzionalità di gateway tra una rete wireless GPRS e una rete Internet o altre reti private (per esempio Lan o X25)
- GIS Geographic Information System
- GMSC Gateway Mobile Switching Centre
- GPRS General Packet Radio Service
- GPS Sistema di Posizionamento globale
- GSM Global System for Mobile Communications
- GTP GPRS Tunnelling Protocol
- HLR Home Location Register
- Handover Procedura che consente ad un utente di proseguire una conversazione anche quando, spostandosi, passa da una cella ad un'altra.
- HSCSD High-Speed Circuit-Switched Data
- HSDPA High Speed Downlink Packet Access, protocollo introdotto nello standard [UMTS](#) per migliorarne le prestazioni, aumentando la capacità delle reti, ed ampliando la larghezza di banda che, in download, può raggiungere la velocità massima teorica di 14,4 Mb/s
- HSUPA High-Speed Uplink Packet Access: protocollo di accesso dati per le reti di telefonia mobile con velocità di Upload fino a 5,76 Mbit/s
- HTML HyperText Markup Language
- IMEI International Mobile Equipment Identity
- IMS Architettura di rete per la convergenza di tutti i dispositivi di telecomunicazioni (fissi e mobili) in un'unica rete IP, per offrire servizi voce e multimediali
- IRDA Integrated Services Digital Network
- ISDN Integrated Services Digital Network
- ITU International Telecommunication Union
- JRC Joint Research Centre
- MGW Multimedia Gateway
- MMS Multimedia Messaging Service
- MSC Mobile Switching Center
- MS Mobile Station
- MSISDN numero univocamente associato ad un contratto telefonico di telefonia mobile (GSM o UMTS)
- NSS network switching subsystem
- OS Sistema Operativo
- Paging Procedura per la localizzazione di mobile chiamato
- PDP Packed Data Protocol (es. protocollo IP o X.25)
- Pps Partnership Projects
- PS Packet switch

- PSTN Rete Telefonica Generale
- PTM Point-to-multipoint
- PTPPoint-to-Point
- PWS Public Warning System
- RDS Radio Data System - standard della European Broadcasting Union per inviare informazioni digitali su trasmissioni in modulazione di frequenza
- RNC Radio Network Controller
- SAFE act Security and Accountability For Every Port
- SDRAM Synchronous Dynamic Random Access Memory
- SGSN Serving GPRS Support Node
- SIM Subscriber Identity Module
- SMS Short Message Service
- TACS Total Access Communications System: standard di rete per i telefonini di prima generazione
- TDMA Time Division Multiple Access: accesso multiplo a ripartizione nel tempo
- TETRA Terrestrial Trunked Radio: standard di comunicazione a onde radio per uso professionale
- TRAU Transcoding & rate adapter unit
- TTA Telecommunications Technology Association (Corea)
- UMTS Universal Mobile Telecommunications System
- URL Uniform Resource Locator: sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa in Internet
- USB Universal Serial Bus
- UTRAN UMTS Terrestrial Radio Access Network
- VLR Visitor Location Register.
- W-CDMA Wideband Code Division Multiple Access
- WAP Wireless Application Protocol
- WARN Warning Alert and Response Network
- WLAN wireless local area network
- WML Wireless Markup Language
- Routing instradamento dei pacchetti di dati
- Roaming, possibilità, offerta dal GSM, che permette ad un utente di essere sempre rintracciabile anche in nazioni diverse dalla propria (purché esista un operatore GSM locale con il quale il proprio operatore abbia raggiunto accordi di *roaming internazionale*) oppure, nella propria nazione, ma in zone non coperte dal proprio operatore (*roaming nazionale*)
- Gateway sistema per l'inoltro dei pacchetti di dati verso l'esterno.





*Riferimenti e Link utili:*

<http://www.logica.com/>  
<http://www.cellbroadcastforum.org/>  
<http://en.wikipedia.org/wiki/3GPP>  
<http://www.3gpp.org>  
<http://maps.sunrise.ch/>  
<http://www.portel.it>  
<http://www.celltick.com>  
<http://www.logicacmg.com>  
<http://www.chorist.org>  
<http://www.3gtech.info/3gpp-earthquake-and-tsunami-warning-service-etws.html>  
<http://www.arib.or.jp>  
<https://service.projectplace.com/pub/english.cgi/0/283748154>  
<http://www.unisdr.org/ppew/ppew-index.htm>  
<http://www.omanmobile.om/en/OmanMobileWebLib/Business/CellBroadcast.aspx?LinkID=2&MenuId=26>  
<http://cell-broadcast.blogs.sapo.pt>  
<http://ict4d-in-srilanka.blogspot>