Emergency Services: The Way Forward

Golara Khayltash and Hu Hanrahan
Centre for Telecommunications Access and Services
School of Electrical and Information Engineering
University of the Witwatersrand,
Johannesburg
Email: g.khayltash@ee.wits.ac.za, h.hanrahan@ee.wits.ac.za
Tel: +27 11 717-7250; Fax: +27 11 403-1929

***Abstract*— Emergency services are vital for the minimization of damage, injury and loss of life. These services are, by definition, a combination of telecommunications and information services, and are by nature, distributed. However, most current emergency services do not take advantage of emerging technology, and hence, are restricted in the functionality they offer. This paper proposes the design of an emergency service, which can be offered as a service or application on any core network, using OSA/Parlay Application Programming Interfaces (APIs) for the application to access underlying telecommunication network functionality.**

Keywords - Emergency Services, Distributed Systems, Reference Model for Open Distributed Processing.

I. Introduction

You are driving down the highway, and a car in front of you swerves into a tree. What is the first thing you do, after thanking your lucky stars it wasn't you? Pull out your cell phone and dial 112, or the plethora of emergency numbers available in South Africa. Of course, the tow trucks get to the scene before the ambulance, but it is a reasonable assumption that the police and ambulance services will also arrive soon.

Accidents and emergencies of various forms unfortunately happen with increasing frequency, especially in the larger cities. Without an efficient and reliable emergency service available and accessible to all, the toll on human life, as well as debilitating injuries and damage to property, would be unthinkable.

The main issues facing South African emergency services are:

- not having one global number that can be used for all emergencies, although specified in the Telecommunications Act of 2001 [1] [1].
- difficulties in pinpointing emergency locations in rural areas and informal settlements
- long delay in deployment of ambulances

In addition, some of the technical issues facing emergency services internationally center on the difficulties emergency call centres face in obtaining location information from mobile phones, with impending legislation deadlines compounding the issue by adding the need for obtaining the location of a VoIP caller. At the moment, especially in the United States, many emergency call centres or public safety answering points (PSAPs) are unable to process location information from mobile networks, and as a result, will need to upgrade their facilities. Furthermore, mainly in some European countries, despite legislation, Emergency Authorities, as the PSAPs are called there, are unable to request the address details of a fixed call, despite decrees stating that network operators must facilitate access by the 112 emergency call service to the relevant databases, to obtain caller location information and other subscriber information [5].

Linked to this issue of call centers being unable to request location information from an external database is the lack of smooth interworking between various systems, caused mainly by non-compatible interfaces and formats, which ultimately result in critical information not being available when needed.

All these issues result in the delay of getting vital assistance to people in emergencies, putting their survival at even more risk. Time is of the essence in the successful handling of emergencies, time that should not be wasted in obtaining and confirming location and other information that can be accessed from databases and through other means.

This paper proposes a design of an emergency service which will work seamlessly with other related services, and that can be implemented on any core network or call centre infrastructure throughout the country.

II. Requirements for an Emergency Service

In most countries, there is specific legislation covering the use and implementation of these emergency numbers. For instance, the current model for 911 services in the United States specifies that:

- the numbers should be touch-tone generated
- incoming calls will be forwarded from the local or end switch to a PSAP (public safety answering point) responsible for the caller's location area
- the caller's location should be transmitted automatically to the PSAP using available resources, usually in a packet switched manner.
- calls need to be connected to the PSAP within 1.2 seconds of the last digit being dialed

One addition made for all European countries states that

- "calling 112 is free for the end user, be it a fixed or mobile call." [5]

Further legislation for wireless and mobile communication, as well as more sophisticated information transfer, caused by

[1] There is no single emergency number that can be used throughout the country. There are separate nation-wide numbers for police (10111) and ambulance (10177) [2], a single "all emergency number", 107m introduced for the greater Cape Town municipality [3], and 112 introduced as an emergency number for mobile callers [4]

the advent of mobile communications, and, more recently, voice over IP, is in the process of being considered and implemented [6]. Enhanced 911 (E911) is an example of legislation that has been approved, and is in the process of being implemented. E911 refers to "an emergency telephone system which includes network switching, database and Customer Premise Equipment (CPE) elements capable of providing selective routing, selective transfer, fixed transfer, ANI (automatic number identification) and ALI (automatic location identification) [7]."

III. Background

Emergency services have, until now, been executed using the Public Switched Telephone Network (PSTN), with an Intelligent Network overlay allowing related services to be implemented, such as call forwarding and reverse charge billing. However, due to the nature of the PSTN, this and other services could only be developed and offered by the telco, keeping in mind the structure and architecture of the network. In addition, any change made to the service would take a long time to be implemented.

With the emergence of mobility and next generation networks, the communication network is no longer based on a rigid and highly formalized infrastructure. It has become desirable for third parties to be able to rapidly create many innovative applications, and to implement them without the long waiting processes for formal standardization. Recently, therefore, there has been a great deal of effort made towards "opening" up the network, especially for application development. Networks are moving towards an open service architecture, which appears to the users of the system as a single, integrated computing facility.

With the advent of open distributed services, networks have opened up in terms of topology, platforms and evolutions. Applications and network control have been separated, making it possible for different parties to provide different services. This open architecture enables third party providers to provide services that will be able to access core network functionality through Application Programming Interfaces (APIs), and will be applicable irrespective of the core technologies being implemented on a specific network. This means that applications can run on and migrate to any core network implementation. Based on this, services and applications can be created and deployed rapidly. No longer is service provision the sole domain of the network operator.

In the previous models of emergency services, since the functionality of the service resided in the network as an IN overlay, the features offered by the service were limited by the functionality of the network. However, in the new model of open service architecture, the different components of the service lie in the Service Capability Servers, which are separate from the network, and can be accessed by users of any network. This enables the service to offer far more functionality to the user, despite any technical limitations of the network being used.

A service as crucial as an emergency service needs to be as up to date as possible, and use all available technology to improve its functionality. Creating an emergency service on open service architecture will streamline the service, making it more efficient, faster, and most importantly, able to save more lives.

In light of the new ways services can be offered through open distributed systems, and the necessity of having efficient and reliable emergency services, this paper examines the design of an emergency number service which can be implemented on any underlying network, and addresses some of the concerns that present day emergency services face.

IV. Open Distributed Systems - A Brief Overview

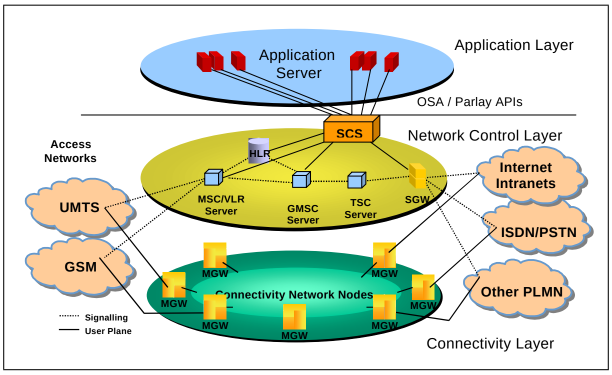

Fig. 1. Open Service Architecture [8]

In an open distributed architecture, which is illustrated above in **Figure 1**, the applications are logically found in the upper layer, which is called the Application Layer [8]. The layers below the Application Layer form the Service Control Layer, in which the Service Capability Servers reside. These Service Capability Servers each contain one aspect of the necessary functionality to handle calls, for example call control or charging. Below that is the Network Resource layer or the core layer, which controls the routing and distribution of calls. The application layer is based on open distributed technology, so applications can access core network functionality through open and standardized APIs.

Taking a closer look in **Figure 2** below, applications, - for instance, an emergency service - that reside on application servers are implemented by Service Capability Servers (SCS), which are nodes found on the border between the Application and the core network. These SCSs implement Service Capability Features (SCFs) which in turn contain the functionality for controlling calls, and potentially interact with the core network. The APIs, which form the service capability servers, should be network independent, so that applications do not have to rely on network details. It also enables easy migration and portability of applications to other networks, including legacy networks.

In addition to implementing the APIs, the SCFs provide an interface to GIS information. Network related data, for instance, the location of telephones, or information stored in a mobile database - if the caller is calling from a mobile phone - will reside on databases. The SCF will provide a link between these databases and the service, by accessing the necessary information in a transparent manner.

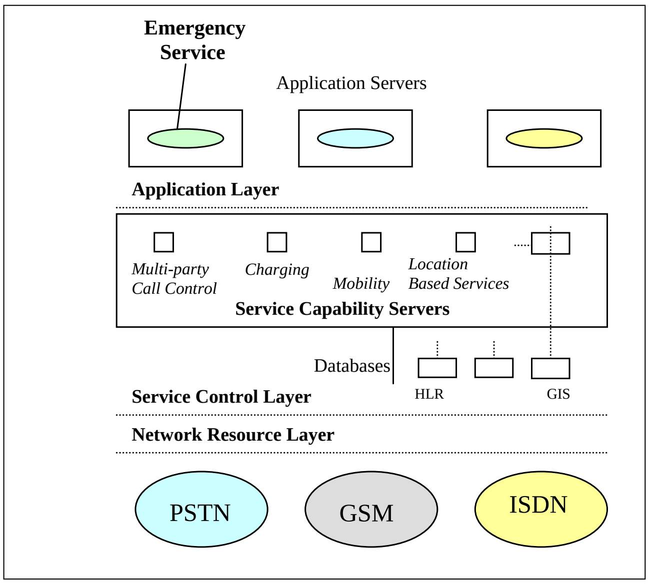

Fig. 2. Detailed Overview of Open Service Architecture

In an emergency service, the associated APIs address user interaction - playing announcements to and obtaining information from the caller, user location - obtaining the location and caller identification of the caller, and charging the service instead of the caller, to mention a few.

V. Design Considerations

An emergency service is potentially complex and needs to be specified from a top-down perspective. An object-oriented approach is well suited to this approach, in which the most fundamental objects are first defined, and other objects inherit from them to add more detail. Object orientation (OO) also enables boundaries between systems to be clearly identified. Interworking can then be encouraged, monitored or prevented at system boundaries [9]. This is very much the approach of the Reference Model for Open Distributed Processing (RM-ODP) [10], which is a tool for design of services using open distributed architectures, which integrates the two aspects of telecommunications and information services into one distributed framework, and through its Object Oriented approach, decreases the overall complexity of creating the service.

Modelling using UML (unified modelling language) [11] finds its place in the RM-ODP and continues the OO paradigm in helping to identify the various players and domains involved in an emergency service, how they interact with each other, and how information will be handled by the system. Because of these reasons, the RM-ODP has been chosen as an approach to designing an emergency service, since it integrates the two aspects of telecommunications and information services into one distributed framework, and through its object oriented approach, decreases the overall complexity of creating the service.

In addition, the open standards approach of the RM-ODP can be especially beneficial in a case such as emergency services, where different companies may have been contracted to provide emergency service centres in different states or provinces. Although the type of structure and technology used in the emergency centres may differ, using an open standards approach will enable interoperability between the different systems, and create a national system that will function and appear unified.

The RM-ODP uses five viewpoints to describe ODP systems. To simplify the vast amount of information associated with each system, these viewpoints each look at a certain aspect of a system, at a different level of complexity. The enterprise viewpoint defines the purpose, scope and policies of a system at a very high and technology independent level. The information viewpoint examines the semantics of information and information processing between the objects; the computational viewpoint defines the execution of the process as a model of distributed processing, and describes the functional decomposition of objects, attributes and interaction of objects. The engineering viewpoint describes the infrastructure required to support distribution, and the technology viewpoint examines choices of technology for the implementation of the system.

There is a range of standards in place to allow applications to access network functionality, the best known and most currently used of which are the OSA/Parlay standards. Instead of devising a new set of standards, we propose to use the OSA/Parlay standards in this project to enable the emergency service to be able to use the core network of whichever telecommunication network it will be implemented on.

Parlay is based on open service access (OSA) architecture, which was briefly explained above, and illustrated in **Figure 3**. Parlay gateways are found between third party service applications and the telephone network infrastructure. Through the Parlay APIs, which are the units that allow access to the functionality of the network, these third party services can be run securely on any telecom operators network, with full access to the networks functionality, independent of the implementation and protocols used in the underlying network. This eliminates the need to tailor make services and applications for each specific network and environment that it might be run on, and creates a single generic application that is able to run on any underlying technology, greatly simplifying the service creation process, and opening up applications to a much wider user base.

VI. The Enterprise Viewpoint

The first step in the design of the emergency service consists of a high-level, technology independent description of what the service does. All the various participants, or role players, in the service are listed, as well as what each of them can and can not do. In addition, it puts role players into natural groupings, called communities and federations, based on common purposes between the role players [10].

The nature of an emergency service is different from most other applications in several respects. Because of its urgent character, the service needs to be extremely robust, and cannot afford any down time. In addition, it needs to be absolutely secure, since it accesses, uses and produces very sensitive information, like medical records and personal information. Finally, the design methodology used in creating an emer-

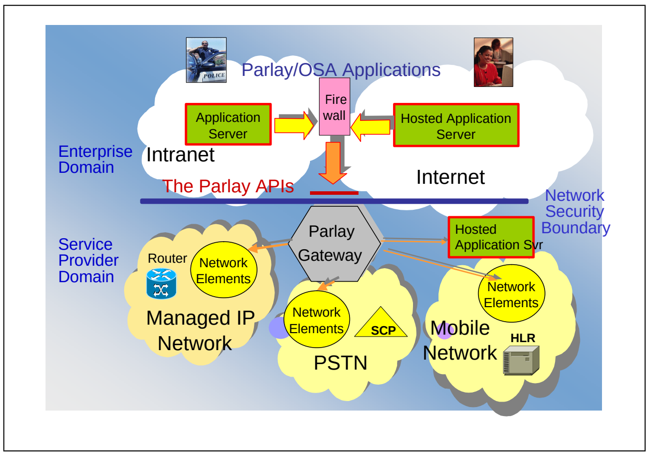

Fig. 3. Parlay in the network [12]

gency service needs to cope with both the telecommunication world as well as the software engineering world, since the functionality of the service is through telecommunications, but the software and databases that it needs to function are in the information technology world. Lastly, records of emergencies and related information need to be saved in a manner that can be accessed by the necessary organizations at a later time, for example, the police.

The infrastructure of the emergency service consists of local emergency centres located in every municipality. The staff at these centres are separate from emergency response personnel, and are responsible for call taking and dispatch of the appropriate emergency staff to the scene of the emergency. These emergency services are obligated to provide continuous and reliable service. Incoming calls will be routed to the emergency centre closest to the caller, and must be answered by an dispatcher within a specified number of rings, without busy tones or voice messages being played. After the location and information about the emergency is obtained, both from the caller and relevant databases, the dispatchers will dispatch relevant emergency personnel to the site, and send related information, such as the location and perhaps the medical records of people involved, through a data connection to the emergency personnel who are attending the call. When the emergency has been dealt with, a record of the call and emergency will be saved. These emergency calls are free for the caller, and will be billed to the government agent.

In the case of people calling about routine or maintenance issues, like an electricity blackout or burst pipe, as soon as the operator has ascertained that the situation is not an emergency, the caller will be routed to an automated voice response system, which will give the numbers for the relevant municipality offices, and will free the lines for real emergency calls.

A. Role Players in the Emergency Service

In the enterprise viewpoint of the emergency system, the role players are the:

1) **Caller** - any person dialling the emergency service number from any telephone or network to report an emergency.
2) **Telco** - telecommunication agent responsible for providing authorization and connectivity from caller to emergency service.
3) **Government agent** - organization responsible for commercially managing the services offered to the caller according to a contractual agreement.
4) **Service provider** - organization that offers the emergency service to the government agent.
5) **Emergency service** - technical infrastructure that enables callers to be answered by the operator, information to be gathered, verified, stored, and dispatched to relevant emergency response staff.
6) **Emergency service dispatcher** - emergency service staff, who receives emergency calls, collects information, and dispatches it to appropriate emergency response staff.
7) **Emergency response staff** - any person who receives emergency information from the emergency service dispatcher, and is tasked with responding to the emergency, for example, police, paramedic, fire and rescue services.

There can be many different business models for an emergency service; for instance, the telco could act as a service provider and government agent. This paper examines the design of a possible emergency service without imposing any of the various models on it.

The policies that define the service are grouped into three areas by the RM-ODP: obligations, which are actions which the role players must fulful, permissions, which are the different options available to the role players, and prohibitions between the role players, the actions which they are not allowed to perform. In the next section, the obligations, permissions and prohibitions of the emergency service operator will be examined as an example.

B. The Emergency Service Operator

The *obligations* of the emergency service operator consist of:

1) Response provided by emergency service operator within specified time period, i.e., five rings.
2) Prompt gathering and verification of caller information, location information and relevant history by emergency service operator through caller, and assisted by caller line identification (CLI), caller location identification, and associated databases.
3) Prompt dispatch of emergency information and location to closest appropriate emergency personnel by emergency service operator, i.e.; through transmitting a map of emergency location and relevant support information, like fire hydrant locations in the case of a fire.
4) Accurate logging of all relevant information and details by emergency service operator.

The *permissions* of the emergency service operator consist of:

1) Rerouting a caller to an automated voice response system after ascertaining the caller does not have a valid emergency.

2) Access to relevant databases not in the domain of the emergency service, like medical records and the Home Location Register (HLR) for mobile callers, by the emergency service.
3) Initiating multi-party calls between the caller, emergency service operator and emergency response staff.
4) Reporting a caller to the police if the information received from them has been deliberately false or misleading.

The *prohibitions* of the emergency service operator consist of:

1) Dissemination of gathered information to any third parties apart from emergency response staff and legal services.

In addition, assistance communities, support federations, security issues and quality of service are examined in the enterprise viewpoint. Following a detailed description of the roles and actions the role players can perform, use cases are created, which analyze the system and break it down into all the requirements and tasks that need to be performed by it. These actions are grouped into use cases that identify the interactions between the end user and the system. **Figure 4** illustrates the various use cases involved in the emergency service.

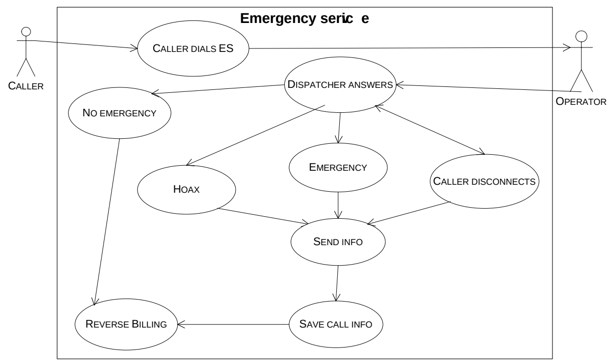

Fig. 4. Use Case Model of Emergency Service

Each use case then fully describes that area of the service. For instance, the first use case is:

Use Case: Caller dials emergency service

- Caller dials emergency number from any telephone capable of making outgoing calls
- Call is routed to closest emergency centre

A comprehensive description of the entire enterprise viewpont can be found in [13].

VII. The Information Viewpoint

After the role players in the service have been defined, and their permissions and prohibitions have been clarified, the information viewpoint is examined, in which the information that is passed between the role players is identified.

The first step in the information viewpoint is to take the use case diagrams that were listed in the enterprise viewpoint, and create robustness diagrams [14] from them. Robustness diagrams essentially make sure that the use cases are robust enough to represent the requirements of the system that is being built, acting as a bridge from the high level descriptions of the use cases to detailed design shown in the next steps of the design process.

A robustness diagram provides a graphical view that illustrates the description found in a use case. Drawing the robustness diagram for a use case gives a visual completeness check that shows the entire use case has been accounted for. As an example, the robustness diagram for the first use case is illustrated below in **Figure 5**.

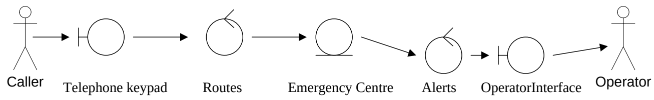

Fig. 5. Robustness Diagram: Caller dials emergency service

The robustness diagrams are then illustrated by message sequence charts, which visually illustrate at a high level the flows of information between the various classes that comprise the emergency service.

VIII. The Computational Viewpoint

The computational viewpoint of the RM-ODP is, at its simplest level, a snapshot of all the ways the components in the service interact with each other. It is a model of the system and its environment in terms of the individual, logical components which are sources and sinks of information. The viewpoint enables distribution through functional decomposition of the system into objects which interact at interfaces [10].

The relation between the objects in the gateway has already been defined in the OSA/Parlay standards, so the only thing left to define is the relationship between the databases, the database manager, and the application. For completeness, **Figure 6**, which is the component diagram, shows a complete overview of all the components within the service and how they communicate with each other.

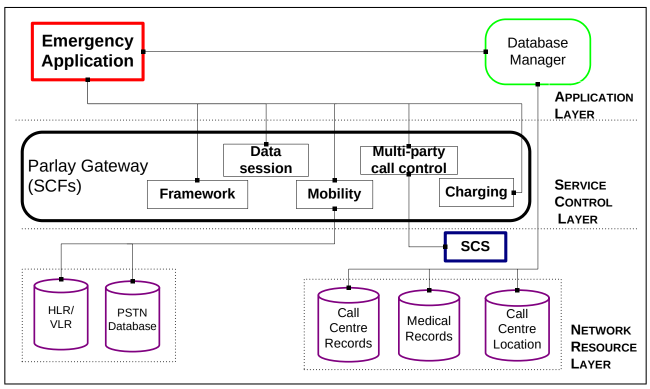

Fig. 6. Computational Diagram of the Emergency Service

Figure 6 visually illustrates how the SCFs that are used in this service make up the OSA/Parlay gateway, as well as illustrating the open distributed architecture of the emergency application, with the emergency application logically falling in the application layer, the OSA/Parlay gateway and the functionality it contains belonging to the service control layer, and below that, the network resource layer.

The computational viewpoint concludes with message sequence charts that decompose the emergency application into the OSA/Parlay SCF interfaces and illustrate how the interfaces communicate with each other, an example of which is illustrated in **Figure 7**.

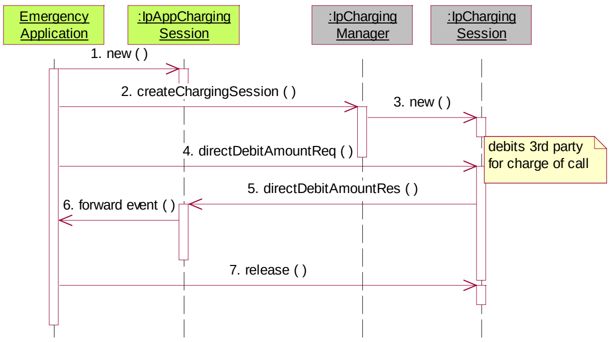

Fig. 7. Sequence Diagram: Reverse Billing

IX. Conclusion

The design methodology provided by the RM-ODP has proved very suitable in this work for rapid service creation in refining the design of a program to the level that coding can begin, once the standards had been deciphered. The viewpoints initially help to fully clarify the requirements of the system, and then continue refining the design until it can be implemented in a programming language. The design is also implementation independent.

Further, the use of OSA/Parlay APIs in accessing the network functionality have also proved beneficial and straightforward to implement and comprehensive in their scope. But perhaps their greatest advantage is that they allow the application to run on any platform, irrespective of the level of functionality it already provides. This is crucial for an emergency service such as this one, for it relies on advanced technology to improve its implementation. Using the OSA/Parlay APIs allows the improved functionality of this service to be offered anywhere, even in areas that have only a very basic telecommunications network.

Some of the benefits that this design can offer over conventional emergency services are:

- allowing the caller, emergency centre dispatcher and emergency response personnel full access to all the functionality of the service, despite any limitations on their telecommunications network
- finding the location of the caller, unless the call has been made from a VoIP phone
- ease and speed of obtaining relevant information, be it the home address of the caller, or previous records of emergency calls made from the same number
- the range of backup information available to the dispatcher and emergency personnel, such as medical records and details of present medical conditions or allergies to medication
- ease and speed of sending relevant information to emergency response personnel, such as map of emergency or history of violence at a particular residence
- offering the service as a third party service provider enables a municipality or even country to offer an emergency service to its population, without having to wait for the government to provide this service

These benefits not only address the issues facing emergency services in South Africa, but also streamline the implementation of the service, making it more efficient and faster than most current emergency services, and most importantly, able to save more lives.

References

[1] The Federal Communications Commission ((FCC)), *Federal Communications Commission: 911 Services*, `http://www.fcc.gov/911.html`

[2] US Department of State, *Consular Information Sheet - South Africa* `http://travel.state.gov/travel/cis_pa_tw/cis/cis_1008.html`

[3] Cape Town Emergency Services, `http://www.go-cape.co.za/emergency.htm`

[4] Emergency Telephone Number, `http://en.wikipedia.org/wiki/Emergency_telephone_number#Africa`

[5] Helios Technology Ltd, *Caller Location in Telecommunication Networks in view of enhancing 112 Emergency Services.* `http://europa.eu.int/information_society/topics/telecoms/regulatory/studies/documents/helios_final_report.pdf.`

[6] *National Emergency Number Association.* `http://www.nena9-1-1.org/9-1-1TechStandards/TechInfoDocs/FMSG-TID%20Feb2002.pdf.`

[7] *National Emergency Number Association.* `http://www.nena9-1-1.org/technical/Standards-PDF/nenamg.pdf.`

[8] A.-J. Moerdijk and L. Klostermenn, *Open Service Architecture: Concepts and Standards.* `http://www.ericsson.com/mobilityworld/developerszonedown/downloads/docs/parlay/OSA_concepts_standards.pdf.`

[9] J. Crowcroft, *Open Distributed Systems*, `http://www.cs.ucl.ac.uk/staff/J.Crowcroft/ods/node3.html.`

[10] ISO/IEC JTC1/SC21/WG7, *ITU-T X.901 ISO/IEC 10746-1 ODP Reference Model Part 1. Overview.* 0.5em minus 0.4emDraft International Standard (DIS) output from the Editing meeting in Helsinki, (Finland), 15-18 May 1995.

[11] The Object Management Group, *Unified Modelling Language*, `http://www.uml.org/`

[12] Z. Lozinski, Senior Technical Staff Member, IBM and President, The Parlay Group, *Parlay/OSA - a new way to create wireless services.* `http://www.parlay.org/imwp/idms/popups/pop_download.asp?contentID=6915.`

[13] G. Khayltash and H. Hanrahan,*Design of Emergency Services: An Enterprise Viewpoint.* South African Telecommunication, Network and Access Conference 2002, George, South Africa, September 2002.

[14] Agile Modelling, *Robustness Diagrams.* `http://www.agilemodeling.com/artifacts/robustnessDiagram.htm.`

X. Biography

Golara Khayltash holds a BSc(Eng.) degree in Electrical Engineering from the University of Cape Town. She is presently pursuing her MSc(Eng.) degree at the University of the Witwatersrand's CeTAS Laboratory.

Hu Hanrahan is Professor of Communications Engineering at Wits University. He leads the Centre for Telecommunications Access and Services (CeTAS), a research and advanced teaching centre devoted to improving knowledge and practice in the evolving telecomms access networks and telecomms services.