1. DIMETRA SYSTEM FUNCTIONS

The system functions are herein described; in order to offer a better understanding they have been divided into the following sections:

- Basic Extended Area Trunking Services
- TETRA Tele-Services
- Supplementary Radiomobile-type Services
- Data Service
- Telephone Interconnection
- Supplementary Telephone-type Services
- Security Services
- Direct Mode
- Features in Terminal Devices
- Advanced DIMETRA Functions

1.1 Basic Extended Area Trunking Services.

The DIMETRA system is a radio trunking system and as such allows high utilisation of radio channel resources; a trunking system can offer a service to more radios than a conventional system with the same number of channels. This is achieved by dynamic assignment of traffic channels using a digital control channel, and because all the available traffic channels are shared among all the users.

The use of a control channel permits not only the assignment of channels but also the establishment of more sophisticated management methods that are not possible in conventional systems, such as the creation of priorities between users etc.

Furthermore, the DIMETRA system is a TDMA (Time Division Multiple Access) system, which permits a more advanced and efficient trunking operation.

Operation as a control channel isn’t uniquely reserved to a single frequency; any traffic channel can take on this operating mode if so required. This allows a more efficient use of channel resources, be they traffic channels or control channels.

1.1.1 Group Organisation

Radio users will typically be organised in operation groups, according to the operational requirements of the client; for example a maintenance group, an installations group, an observation group, etc. When a user makes a call, the other users in that group can listen to the call, while users outside the group cannot, unless programmed for this.

This organisation in groups allows an efficient use of resources and means that users only have to worry about speaking and listening to other users in the same group; a user in a conventional system must listen to all communications and decide in which of those they should intervene.

1.1.2 Register and Roaming

All users and their situations are registered by the system. The register includes the group that the user has selected, as well as the user’s individual identity, which is unique for each user in the system.

All system users are registered in their pre-selected group or individual terminal (ID), when one of the following actions occurs:

- Device Start-up: The user is validated before being authorised for network access.
- Change of Group: When a user changes operation group, the system is informed.
- Change of Location: When a radio moves from one location to another, the system is automatically informed.
- Device Shutdown: The system will not assign more calls to a device that has been turned off.

1.1.3 Trunking Call

The advantages of telephone trunking systems are also applicable to radio systems; when a radio user initiates a call, the radio uses a control channel to indicate to the system that it requires a traffic channel, as illustrated in the adjoining figure.

The system validates the call request, temporarily assigns a traffic channel, and indicates the concession of the channel to all members of the group. The members of group B respond via the temporary traffic channel.

When the call ends, all members of group B return to the control channel, leaving the traffic channel available for other users.

1.2 TETRA Tele-Services

The system supports the following basic tele-services:

- Group Call
- Multigroup or Diffusion Call (Broadcast)
- Private Call

Voice calls can be semi-duplex or full-duplex. Group calls, emergency calls, individual calls and multigroup calls are always semi-duplex, while telephone calls are full-duplex.

Consoles have basically the same call facilities as radios, in addition to the capacity to make multiple group calls or individual calls. They also have other facilities such as Priority Console, which allows the dispatcher to interrupt communication from a radio.

1.2.1 Group Call

This is the usual type of call in the system. Each radio user, on pushing PTT, communicates with their conversation group in the same way as a user of a conventional system need only push to speak. A user can belong to more than one group. A group consists of one or more users that can include a control console. Group call is a semi-duplex service where only one of the users can transmit at a given moment.

The different conversation groups are programmed into the radio channel switch in the same way as channels are programmed in a conventional system, so that if a user wants to change conversation group they only have to rotate the switch.

1.2.2 Semi-Duplex Individual Call

The individual call allows selective calls to be made between two users. The user must set their radio to individual call mode; select the radio they want to call to, from a list or by using the keypad; and push PTT to initiate the call. The calling user will be able to make the individual call so long as the user being called is not busy. The calling unit will receive a recognition sign if the individual call takes place correctly. If the user being called has a terminal with a screen, then the identifier (ID) of the calling user will be displayed.

The call will come to an end when one of the users leaves individual call mode, or automatically, when the time set by a timer runs out.

In the DIMETRA system individual calls are given the name, private calls.

In the DIMETRA system the network manager will be able to enable or disable this service for each terminal in the network, as well as being able to adjust important parameters for this type of call.

The individual call can be:

- MS to MS
- MS to Console
- Console to MS

The Console can interrupt the MS in conversation.

The MS can store the ID of the calling MS/Console, in order to redial in the case of there being no response to an incoming individual call.

The individual call allows the selection and re-selection of cells defined in the TETRA standard.

For every user it is possible to specify the locations that they can use for individual calls.

1.2.3 Multigroup Call - "Broadcast"

The multigroup call is used to make a call to various conversation groups simultaneously. Multigroup calls are calls in a single direction; that is to say, from whoever initiates the call to all groups and their members.
This type of call operates in such a way that users already engaged in a call are not interrupted.

1.3 Supplementary Radiomobile-type Services

1.3.1 Emergency Call

The emergency call has the highest level of priority in the system. When a user makes an emergency call, the priority level of their group rises to the maximum level.
The emergency call process is initiated by pushing the emergency button for a given time. This causes the transmission of an emergency alarm in the control channel; because of this it isn’t necessary for there to be a free traffic channel in the instant of pushing the emergency button. The emergency alarm presents itself to the operator both audibly and visually, furthermore indicating the identity of the radio that has transmitted the alarm.
Transmission of the emergency alarm is maintained during some time (normally 30 seconds) with the aim of assuring the availability of a channel for the call. The console can cancel the waiting time.
For a terminal that has entered emergency mode, the mode is deactivated by pressing the emergency button for a fixed time. However the call itself continues until cancelled by the Console.
To initiate voice communication it is necessary to push the PTT button. The DIMETRA system can be configured to act in two distinct manners in the event that all traffic channels are occupied when it comes to assigning a traffic channel for the emergency call:

- Interruption of call already taking place: The system identifies the user with the least priority in the location, indicates to him or her that they must abandon the channel, and then assigns the traffic channel to the emergency call. This is all done in a transparent way, and within a span of time less than three seconds.
- First in queue: The emergency call becomes the first call in the queue waiting for a traffic channel. When the next traffic channel becomes available it will be assigned to the emergency call.

The DIMETRA system supports the following possibilities:

- MS to Group/Console
- Console to Group

A console doesn’t have emergency mode, nor sends an emergency alarm, but it can however initiate an emergency call to a group; in such a case a TETRA traffic channel will be dedicated to that group until the Console controller deactivates the emergency call.
An MS that is not in emergency mode will not enter into such a mode when it receives a group emergency call.

1.3.2 Late Entry

The DIMETRA system provides this service for all group calls and for all emergency calls. The signals corresponding to a call are sent periodically, throughout the duration of the call, via the control channel. This signalling can be directed to any radio on the traffic channel at any moment after the call has been initiated.
This will allow users to join a call at any point during that call, even though they were not available in the moment the call was established (out of cover area, terminal turned off, etc.).
Late entry signals are sent only in those locations where group members are registered, with the aim of minimising over-the-air signalling.

1.3.3 Identification of the Calling Terminal

Whenever a radio transmits, it sends its identifier to the system and to the other devices that participate in the conversation. This allows the receiver of

the call to identify the origin of the call; the identifier number (ID), or the corresponding alias text, are displayed on the screen of the receiver.
Moreover, the visual presentation of unit identifiers allows the operator to observe the identifiers sent across the control channel. Unit identifiers can be constituted of fleet numbers in order to facilitate their identification by the operator. These identifiers can be displayed at the console or in the management system

1.3.4 Call Priorities

Some users or user groups might need calls or messages more urgently than other users. The system provides a process of priorities that assures that urgent calls and messages are treated in an efficient way. The system has 10 levels of priority.
When the system is occupied, calls are stored in a queue according to the priority associated with the call, instead of following FIFO philosophy (First In First Out). In the moment that traffic channels are available the system will process calls in accordance with the position of the call in the call queue.

· Priority for the most recent user

This is a specific system property that assures continuity, in a natural way, of calls that are already taking place. When two users have the same level of priority, the user that used the system most recently will be served first.

· Emergency priority

The highest level of priority in the system is the emergency call. What is more, emergency calls can have a higher grade of priority still; one that guarantees direct access to the system, even though this might necessitate the cutting of lower priority communications that are already under way.

· Console Priority

In those cases where it is necessary, the system will allow a console operator to interrupt a call already taking place.

1.3.5 Ambience Listening

A console operator can activate the ambience listening feature of a mobile user. The radio being monitored does not present any external indication that it has been activated. This feature allows an operator in the office to listen discreetly to the radio user and to his or her surroundings; a feature especially useful during kidnappings or emergency situations.
If the radio being listened to is turned off, the terminal must continue transmitting without giving any indication of the fact that it is operating; likewise when the terminal is turned on again. Furthermore, it must be possible to operate the MS like a normal MS during ambience listening (the MS must be able to receive and make calls). The ambience listening feature can only be deactivated by the Elite operator.

1.3.6 Call Forwarding on No Reply (CFNRy)

Telephone or individual calls are automatically forwarded to another user or extension if the user being called does not reply.
This type of call forwarding can be initialised from a radio terminal and/or from a console.

1.3.7 Call Forwarding on Not Reachable (CFNRc)

Telephone or individual calls are automatically forwarded to another user or extension if the user being called cannot be located. This situation occurs when the radio is off, occupied or outside the cover area.
This type of call forwarding can be initialised from a radio terminal and/or from a console.

1.3.8 Data service

The system supports a great variety of data transmission services, described as follows.

1.3.8.1 Status Call

The system allows the use of status messages. The user sends the operator a numeric code, upon receipt of which the operator will see the following details on their screen: the terminal identifier, the group identifier, the time the message was sent (hours and minutes), the numeric status code, and a small descriptive sentence associated with the received code. Status messages are transmitted using the control channel.
Each terminal can have a set of programmed status messages. Each set contains up to 16 different codes, and the system supports up to 50 different sets.

1.3.8.2 Short Data Transport Service (SDTS)

The Short Data Transport Service (SDTS) provides a carrier service that allows applications to transfer data by means of the TETRA Short Data Service (SDS). Data is transported between two ends; each end having an Individual Short Subscriber Identity (ISSI) and a software application. Multiple end point identities can be used in order to allow the final user to simultaneously operate various applications.
The connection between the radio system infrastructure and the user's data network is established through a router (SDR) using TCP/IP.
The radio infrastructure automatically maintains a register of the location where the radio is subscribed. This assures that messages are sent to the correct user.
The Short Data Transport Service (SDTS) uses the control channel to provide an efficient mode for the transport of user-specific data with a maximum length of 140 characters. This service is more than adequate for non-vocal communications like status messages, text messages, access to databases, automatic localisation of vehicles, telemetry, etc.

1.3.8.3 Text Message Service (Console to mobile device)

This service will allow the control operator to send up to 128 characters of free text to any terminal equipped for SDS; to receive confirmation that the message has been received; and to receive a second confirmation when the user reads the message.
If the mobile terminal isn't available, the system will keep the message during a predetermined time and will send it to the terminal as soon as it reappears in the system. Each device will have a specified capacity for storing text messages until read by the user.
The text message service also provides a Windows API for the adaptation of third-party applications. An example might be an answer machine that sends predefined text messages to a radio, according to a user selection made by means of DTMF signalling; in this way simulating a system of predefined radio-messages.

1.3.8.4 Peripheral Equipment Interface (PEI) for SDST

The Short Data Transport Service (SDTS) provides a carrier service that allows applications to transfer data by means of the TETRA Short Data Service (SDS). An application can be one incorporated in the radio unit itself or can be an external application, available through the Peripheral Equipment Interface (PEI). This interface, defined according to the TETRA standard, uses Hayes AT commands from the external device to control the TETRA terminal device. DIMETRA's choice of PEI is an RS232 series connection, using a specific "expander" for TETRA.

1.3.8.5 Voice and Short Data Simultaneously

The TETRA standard allows the transport of short data messages during voice communications. This can be done in order to display additional information during a call.

1.3.8.6 Data Transmission by Packet Switching

Transmission of data by packet switching consists of slicing the message to be transmitted into sequential packets, including in each packet the destination address and the packet position inside the complete message. The packets can follow different routes and arrive at the destination point at different times, or even in a different order. At the destination point the packets are temporarily stored and grouped into the correct order, in such a way that the original message is reconstructed.

The Packet Data Gateway (PDG) offers a link to external systems, using TCP/IP with Ethernet standard 10Mbps, as the physical interface. In this way IP connectivity with mobile units or portable computers, is provided.

Mobile devices and Data Terminal Equipment (DTE) are assigned an IP address, compatible with users' existing IP networks.

There exists a mobile data network simulator to facilitate the development and testing of data applications.

1.3.8.7 Multi-Slot Data Packets

The system supports Packet Data Channel Handling (PDCH) in single individual slots, and in multiple individual slots. Each PDCH slot (interval of the TETRA frame) works at 7.2 kbit/s in the air interface. This provides the user with a rate of approximately 3 kbit/s, after eliminating the TETRA control call and the error reduction mechanisms. The data capacity in each PDCH slot can be shared among all subscribers who access at the same time, in order to obtain the maximum rate of 12 kbit/s, after error protection.

By assigning multiple slots to a specific call it will be possible to operate at a maximum of 28.8 kbit/s in the air interface, giving the user a rate of 12 kbit/s, after error protection.

1.3.9 Telephone Interconnection.

1.3.9.1 General

Telephone interconnection allows a user to make duplex calls from their radio to the RTC, RDSI or PABX, just as calls can be made from the RTC, ISDN or PABX to a radio user.

The DIMETRA system provides a large series of interfaces, both analogue and digital, to support this type of call.

In addition to the basic call services, the mobile radio terminal is capable of activating the following supplementary services:

- Always forward calls coming from a fixed network telephone subscriber to another number.
- Direct dial for basic RDSI call, and for basic E&M call.
- Shared Service Algorithm.

1.3.9.2 Call from Radio User to Telephone Network

A DIMETRA radio can make this type of call if its configuration and definition of privileges in the system so authorise it. Furthermore, any radio can transmit DTMF signals if required by the telephone system.

The call is initiated by dialling the telephone number, or selecting it from the list of numbers held by the radio, before going over-the-air (before pushing PTT). PTT is then pushed and the call process begins--the dialled telephone number is located and the mobile user is informed of the process by means of audible tones.

When the fixed subscriber picks up the telephone, an audio connection is finally made, and the conversation commences (full-duplex). The call ends when the fixed subscriber hangs up the telephone or when the MS disconnects, both parties being informed that the call has ended. The SwMI, just as much as the MS, can cut off the call if the time authorised for this type of call expires.

Once a traffic channel is assigned to the mobile terminal radio in order to make a telephone interconnection call, the call will remain with that channel until the call ends, even if neither of the parties is speaking; that is to say, trunking is not performed during a telephone interconnection call.

If there are no available channels to establish the call in the cell where the calling MS can be found, the SwMI puts the call in a queue until there are channels available. During this time, the user can cancel the call petition.

On finishing the call the MS returns directly to the network in TMO.

1.3.9.3 Call from the Telephone Network to a Radio User

Any telephone line is able to gain access to radio users if the DIMETRA system is configured to allow this type of conversation.

The fixed subscriber can basically make the call in two ways:

1. Dialling in two steps: whereby the telephone subscriber dials the number of the DIMETRA System Telephone Interconnection Gateway, from where they will receive a new dialling tone inviting them to dial the identity number of the TETRA subscriber (individual mobile).
2. Dialling in a single step: Whereby the DIMETRA network and the Telephone network are integrated in such a way that any accessible mobile user has a unique telephone number assigned. The terrestrial subscriber contacts directly with the Gateway when they call the mobile station; they dial the telephone number directly associated with the mobile.

The mobile user is alerted to the receipt of a call by means of audible tones; they can then “pick-up” the call, and in so-doing produce the full-duplex audio connection.

When the MS responds to the call, the SwMI assigns a permanent traffic channel until the call ends, even if neither of the parties is speaking; that is to say, trunking is not performed during a telephone interconnection call.

If there are no available channels to establish the call in the cell where the calling MS can be found, the SwMI puts the call in a queue until there are channels available. During this time, the user can cancel the call petition.

The call ends when the fixed subscriber hangs up the telephone or when the MS disconnects, both parties being informed that the call has ended. The SwMI, just as much as the MS, can cut off the call if the time authorised for this type of call expires.

On finishing the call the MS returns directly to the network in TMO.

1.3.9.4 Roaming

When a mobile user moves through the network they are “roaming” from cell to cell. The DIMETRA system maintains a mobility database with the roaming information of all users.

If a mobile station is in the process of making or receiving a call, while it is leaving the cover area of its actual cell, attention to the call will be interrupted. If the call had already been established, the connection will be interrupted in the old cell and the mobile station registered in the new cell. The call can then be re-established in the new cell by means of an automatic petition from the mobile station. A change of cell will therefore mean a small interruption in communication, perceptible at the most by a slight crackle.

1.3.9.5 Telephone Interconnection Through CentraCom

This interface provides the possibility for an Office Console to make calls via a CEB connected to the telephone system, typically a local PABX. When the call is established, it can be connected to a TETRA group using the Console.

1.3.10 Supplementary Telephone-type Services

1.3.10.1 Direct Dialling

This facility allows a telephone subscriber in the fixed network to directly dial, in the Telephone Interconnection Gateway, the number of the mobile user to which they are calling, without the necessity to follow the two-step procedure described previously.

This direct dialling service supports up to 4,000 mobile user numbers. The digits that identify the mobile terminal (DDI), in the number dialled from the fixed telephone terminal, can vary from 2 to 7.

1.3.10.2 Unconditional Call Forward

When a mobile user activates this service, any call entering from the telephone network will be redirected towards the number set by the mobile terminal during activation of this function.

The network manager can configure this characteristic for each one of the mobile stations, as required.

1.3.10.3 Shared Service Algorithm

This function manages the interactions of normal group calls and private calls, with the telephone interconnection. The Network Manager programmes and controls the number and duration of interconnection calls, according to the hour of the day. The maximum number of simultaneous interconnection calls permitted, and the maximum duration of these calls, can be adjusted within each one-hour period throughout the day. Both parameters can be established for each one of the covered locations individually.

1.3.11 Security Services

1.3.11.1 ETSI Standard Over-Air Encryption

The air interface encryption mechanism is a requirement of many public security organisations, because it can be used to provide relatively cheap, secure communications. It is able to do this since the algorithms are stored in the radio terminal itself, without additional hardware.

The air interface encryption mechanism makes use of a Static Cipher Key (SCK), which has to be programmed in the base stations. The entire system uses the same static SCK key.

1.3.11.2 ETSI Standard Over-Air Encryption with Dynamic Key

The ETSI over-air encryption TETRA standard is performed according to the TEA2 algorithm. All the signalling and traffic sent in the air interface is encrypted, including the identification of the users.

1.3.12 Direct Mode

1.3.12.1 General

Direct Mode Operation (DMO) of the system allows users to communicate among themselves, both inside and outside the trunking system cover area.

The Direct Mode does not form part of the trunking operation, and therefore, when operating in this mode a terminal is beyond the reach of the trunking system. When a user selects Direct Mode, the terminal un-registers from the trunking system, before entering in DMO.

In comparison with trunking mode operation, Direct Mode only uses a single frequency, so communication is simplex.

The DMO services available for a DIMETRA terminal are:

- Group Calls
- Intrinsic Services: Caller Identification and Late Entry

1.3.12.2 Group Calls

The group call is a bidirectional point-multipoint communication between the calling terminal and one or various terminals belonging to the same group. Communication is established between all those terminals that have selected the same group, and which in effect find themselves on the same Direct Mode carrier frequency.

The system supports more than one group on the same Direct Mode carrier frequency, although only one group will be capable of communicating at this frequency at any particular instant.

1.3.12.3 Gateway Direct Mode

Gateway Direct Mode is used as a link between the radio user operating in Direct Mode, and the TETRA network. It is normally used to provide communications to a user outside the cover area.

The available services are:

- Group Calls
- Emergency Calls

To make use of gateway operation, users must first go to the gateway. When the call is established, the gateway must make sure that the user who is transmitting is inside the “timing” dictated by the traffic channel assignation system.

The man-machine radio user interface will indicate if a repeater or a gateway has been selected.

A mechanism exists in order to avoid that during an emergency operation a user abandons their vehicle, forgetting to select the gateway operation mode: the Nokia mobile devices control unit continuously monitors the DMO channel, in search of signals sent by portable units that operate in DMO, and that are directed in an appropriate manner to the gateway. Once the correct signal and routing information is decoded, Gateway mode operation is provided in an automatic and instantaneous manner.

In Gateway mode, automatic operation mode can be deactivated using the device control panel, by simply selecting Direct Mode operation. This characteristic is useful if users want to operate in DMO mode independently of the principal TETRA network.

1.3.12.4 Direct Mode Repeater

In Direct Mode Operation (DMO) the Repeater is used to provide a service to users independently of the principal TETRA network. This service is similar to the conventional service, with a repeater in TMO mode, except that it only uses a single RF channel. The time division operation uses transmission time intervals that are distinct from those of other mobile devices. Reception of the signal is generated before the retransmission, according to TETRA standard specifications.

The DMO repeater can also be used when a DMO Gateway doesn’t provide sufficient RF cover.

Selecting operation as a repeater is a decision taken deliberately (normal operation is in Gateway mode), because of which it is not considered necessary that such an operation is activated in an automatic way. To select operation as a repeater, the user vehicle will need to select the Repeater option using the appropriate control panel button.

It is essential that there is only one repeater activated in a DMO cover area, serving the same user group.

1.3.12.5 DMO Dual Watch

A terminal equipped with Dual Watch operates just as much in Direct Mode (DMO) as in TMO mode. When DMO is activated, the MS monitors, in Trunking Mode (TMO), any activity originated by the group that it belongs to, in the cell where it finds itself. If the MS is active in TMO, it will be monitored in predetermined DMO groups.

The change between TMO and DMO as a primary operation, is selected manually in the MS.

On the screen of the MS, icons will indicate the mode in which it finds itself: DMO, TMO and Dual Watch.

When a user changes mode, just as much from TMO to DMO as vice versa (with or without Dual Watch) they must notify the office manager. The office manager can remotely activate/deactivate an MS in DMO via Dual Watch, if the radio is already in DMO, or they can do so via TMO directly.

1.3.13 Terminal Device Features

1.3.13.1 Group Scanner

A mobile user can listen out for a series of groups, in addition to those they have selected at any moment. They will preferably monitor their own group when it is active. The group scanner function is independent of the TETRA network (the network won’t automatically “illuminate” additional channels in order to support the group scanner). Excessive load on the network is minimised by illuminating only those cells that contain subscribers.

1.3.13.2 Monitoring of the Priority Group

Monitoring of the priority group is a feature used by the group scanner; it gives monitoring priority to one of the scanned groups. The group scanner function is independent of the TETRA network (the network won’t automatically “illuminate” additional channels in order to support the group scanner).

Excessive load on the network is minimised by illuminating only those cells that contain subscribers.

1.4 Cryptographical Security and Access

1.4.1 Introduction

Security measures are essential in any modern system of mobile telecommunications. Since their origins, mobile communication systems have been the object of external attacks, such as eavesdropping and third-party intrusions. During the last decade ETSI has developed and standardised a series of digital systems for mobile and cordless communications, all of which have included a range of characteristics to guarantee security. In this sense DIMETRA represents right now the most advanced technology that exists in security mechanisms.

- TETRA is, after GSM and DECT, the third consecutive system of mobile telecommunications standardised by ETSI, making full use of the accumulated experience.
- TETRA is directed, as its fundamental market, towards Public Security users; in the development of TETRA all the characteristics defined by this type of user have been borne in mind.
- TETRA has been developed with the direct collaboration of Public Security user groups.

Set against this background, the result is a system that provides a great number of security measures, scaled in an adequate manner so as to permit different grades of security to cater for the various types of user and their operations.

1.4.2 Philosophy Behind the Development of TETRA Security Characteristics

The design and specification of TETRA security characteristics can be qualified as “structured and open”.

Structured, to allow maximum flexibility in the final application of different features. With this objective ETSI formed the security group that developed the specification; the security requirements being defined by different representative groups of Public Security users. The result is the ETR 086-3 specification, in which are defined all the security characteristics that the TETRA system provides.

Open; from the start it was clear that an open design should be used, in order to preserve the very benefits of having a standard, and to guarantee that the security of TETRA was based on the robustness of the designed mechanisms, and not on the fact that the security specifications were secret--a vulnerability that can be found in the majority of private systems.

1.4.3 Security Functions in DIMETRA

Until the appearance of TETRA, digital systems for existing PMRs limited their security characteristics to end-to-end encryption methods, and to certain techniques that concerned entering onto a network. As mentioned already, as far as digital security systems are concerned TETRA goes much further than any other, and covers the following functions inside the system:

- Security Mechanisms: these are different functions, independent among themselves, that provide solutions for specific network security problems.
- Security Management Mechanisms: these are functions that guarantee the management and operation of the security mechanisms.

1.4.3.1 Security Mechanisms

1.4.3.1.1 Authentication

The TETRA standard supports Mutual Authentication between a Mobile Station (MS) and the Switching and Management Infrastructure (SwMI). This makes it possible to control access to and from terminals in a TETRA system in order to determine if the terminals are included in the system database. Mutual authentication can be used furthermore, in order to establish and exchange additional security parameters.

In Direct Mode Operation (DMO) there is no explicit authentication mechanism available; in this case Static cipher Keys are used, by means of which an implicit authentication mode is established.

Although not an authentication mode in itself, air encryption does fulfil a similar function (security of authorisation to communicate).

In the DIMETRA system implicit terminal authentication is already available--terminals are registered and checked in the system database, and only if the validation is correct can the terminals operate within the system.

In the second quarter of the year 2000 explicit authentication will be available, as described below:

Each Nokia radio terminal will be programmed with a secret key used for authentication. Each key will be loaded, together with other details, when the radio is programmed. Once loaded, it will not be possible to read the key. The same key will be loaded for authentication in the central database where the terminal is included. The authentication mechanism used by the system consists of sending a random code to the terminal; the terminal calculates a mathematical reply to the code, and returns that reply to the system. The system compares it with the reply that has calculated itself, and if the match is correct it will allow the terminal to operate in the system. Authentication is normally conducted on initially joining a system; it could be applied more frequently, but unless the terminal remains in the system more than a predetermined time, or shows unusual mobility (such as rapidly jumping to a distant cell), it will not be necessary to re-authenticate the terminal.

Since the process functions using a calculation based on a secret key, the key itself is never exchanged, and must not be changed during the entire life of the terminal. If the radio is stolen and recovered, the radio and the authentication centre can be programmed with a new key by means of a simple manual programming procedure. Therefore, during the life of the terminal, any action regarding the administration of keys should be an exception and only for very concrete reasons. No mechanism exists for exchanging keys over the air, since this is not usually necessary during the life of a terminal; furthermore this must not be done if it is suspected that a terminal’s key has been compromised.

1.4.3.1.2 Encryption of the Air Interface

Encryption of the air interface is applied between the terminal and the base station, and covers all the different types of communication: voice, data and direct mode. This mechanism uses static and dynamic keys to guarantee the security and privacy of communications.

The process of dynamic keys uses an individual Derived Cipher Key, generated by the authentication mechanism, together with programmed secret keys, group identities, and a generated and distributed Common Cipher Key (used as a key modifier).

If so required, the dynamic mechanism necessitates that the group keys are loaded during initial programming of the groups; if this isn’t done then the key administration process can be automatic. The use of the dynamic Derived Cipher Key, and the mechanism that governs the modification of the group key by the Common Cipher Key, implies that the lifetime of the group key should be as long as the lifetime of the terminal. So, once the initial keys are loaded into the terminal, it shouldn’t ever be necessary to take any future action regarding the administration of keys.

An alternative procedure can be used for initial loading of a ciphered key into a radio, or into the system. It could be less secure, since it uses a single key for the whole system, during its entire lifetime, but nevertheless it could provide an adequate level of protection.

In 1999 the DIMETRA OmniLink provides static cipher keys; in the second quarter of the year 2000 it will provide the dynamic mechanism.

1.4.3.1.3 End-to-End Encryption

This type of encryption necessitates that all terminals, including the consoles, exchange information between themselves in such a way that this information cannot be listened to in any point of the transmission. This is achieved by encrypting the information at each end.

The TETRA standard permits the application of any end-to-end encryption system that each group of final users might decide to use. ETSI has not yet become involved in the definition of an end-to-end encryption standard, since user interest in this type of encryption would be very limited. Standardisation of this type of encryption would go against the final objective of the ETSI—that of guaranteeing very exclusive functional characteristics to reduced groups of users.

Nokia has many years of experience applying real end-to-end encryption systems for a large number of very accomplished users in the field of Public Security. The DIMETRA system will have an end-to-end encryption module available for its terminals. This module will be available in the year 2000 for mobile terminals and portable computers, and in the year 2001 for consoles. At present all DIMETRA terminals are furnished with an adequate fixture for connection (without cables) of the encryption module.

This module is based on the UCM (Universal Crypto Module) circuit, which permits the utilisation of different existing encryption algorithms, like DVI-XL, DVP-XL and DES-OFB. Likewise, for those users that might not trust the standard algorithms, the UCM supports the use of custom algorithms that can be developed by authorised organisms. For a custom algorithm to be included (for example one provided by the Police force), it will be necessary for the appropriate organism to define the algorithm in conjunction with the Nokia Cryptography Design Centre, in order to assure that it can be loaded onto the UCM without any problem.

Furthermore, this module is obviously subject to the usual export restrictions that apply to such items. End-to-end encryption algorithms work with keys, and so the adequate administration of these keys is fundamental to the protection of information confidentiality. This concept is normally known as "Key Administration". The procedures can be manual and/or automatic. Owing to the character of the operations in which this type of encryption is applied, this management method for the manual control of keys is the most widespread.

The alternative--that of automatic management--is carried out using a tool called the Key Management Facility. This alternative includes the dispatch of keys over the air, and is called Over-The-Air-Replacement (OTAR). At present Nokia uses this mechanism in all Public Security systems; it can be adapted and extended to the DIMETRA system in a later phase of the project.

1.4.3.1.4 Activation and Deactivation of Terminals

TETRA supports six different options for the activation or deactivation of terminals. These mechanisms are applicable just as much for voice, as for data and direct mode. In the Nokia DIMETRA system, the activation and deactivation of terminals is managed by means of the user database; besides other things this provides the following functions:

· Terminal Blocking: this function is carried out directly in the user database, and results in the rejection by the system, of any type of communication to or from the terminal in question. The blocked terminal will not be able to perform any kind of operation in the system, nor join or receive calls, nor make any type of voice or data communication.

· Terminal Check: this characteristic enables determination a terminal's location, by forcing it to join the network, following the complete standard procedure for joining.

· Terminal Tracking: permits the active tracking of a terminal, first in order to detect its presence in the system, and then to observe its behaviour, the area in which it can be found, the groups in which it works, the type of communications it makes, etc.

1.4.3.2 Security Management Mechanisms

1.4.3.2.1 Security in the Network Manager System

The global system administrator has the capacity to create the necessary structure of identities, with their corresponding keys, in order to completely control access to the different elements of the system. Although this structure might seem rigid, it is totally adaptable to the operative organisation of the users--assigning for example, different managers for user groups, locations etc., and allowing control to be maintained over all the fundamental elements of system security.

1.4.3.2.2 Authentication Key

The authentication key is designated K. The TETRA standard establishes three ways to define K:

· A User Authentication Key (UAK): 128 bit word stored in the terminal or on an electronic card.

· An authentication code introduced by the user.

· A combination of the UAK and a PIN introduced by the user.

1.4.3.2.3 Encryption Keys

There are various types of encryption key; these are derived or transferred during the authentication process. Among these keys, the management of which is fundamentally automatic, are some of long duration. In order to increase system protection, the TETRA standard defines a series of special, long duration key-protection mechanisms. The keys are as follows:

· Derived Cipher Key (DCK): Key derived during the authentication process; this key therefore provides an implicit form of authentication during any communication. It is used, for example, to encrypt communications from the terminal to the infrastructure.

· Common Cipher Key (CCK): Key generated by the Switching and Management Infrastructure (SwMI), and distributed to the terminals in encrypted form, along with the DCK. It is used to encrypt communications from the infrastructure to the terminals.

· Group Cipher Key (GCK): Key associated with a specific user group.

· Static Cipher Keys (SCK): Predetermined keys that can be used without previous authentication. They are called “static” because they aren’t derived from a dynamic process like authentication. They can be distributed like GCK keys, and can have diverse applications, such as for example, their use in direct mode.

1.4.3.2.4 Transfer of Authentication Information Between Different TETRA Networks

If a mobile TETRA station moves to another TETRA network, the TETRA network “visited” will need to obtain authentication information from the network of the “visiting” mobile station. It needs this information in order to be able to perform mutual authentication, and to generate and distribute the encryption keys. The transfer of authentication information between networks can be carried out in three ways:

· The most direct method consists of simply transferring the authentication key to the visited network. For reasons of security this method isn’t always advisable.

· A second option consists of transferring certain information that can be used by the visited network in order to initiate a simple authentication process. This is basically the process used by GSM networks, and can be implemented in a very secure manner. Nevertheless, in TETRA systems transferring such information in a regular way can cause overloading of the system.

· The third option consists of permitting the terminal’s own TETRA network to transfer, just once per session, the authentication key for an MS; this can be used in repeated authentications by the visited network, without revealing the original authentication key belonging to the MS in question. This last option combines security and efficiency.

1.4.4 Intrinsic TETRA security

In addition to all the functions explained in the previous sections, TETRA provides, because of its own functionality and technology, a very high level of security. This communication security is based on the following fundamentals:

· TETRA is a digital system, which increases the complexity needed in devices used for eavesdropping.
· TETRA uses Time Division Multiple Access (TDMA) as access method. In comparison with FDMA systems, this increases the complexity needed in devices used for eavesdropping.
· In order to increase the robustness of the information transmitted via radio, against the typical disturbances faced by such transmissions (fading, multipath, etc.), TETRA uses interleaving. Interleaving consists of slicing the information and disordering it within the data frames; this reduces to a minimum the effects caused by a possible loss of information, and also adds one more difficulty for those who might wish to obtain unauthorised access to the system.

· TETRA is a trunking system that assigns new channels for each communication. DIMETRA too is a transmission trunking system that assigns new channels for each communication; a fact that makes unauthorised monitoring of a conversation very difficult.(Being a TDMA system the channels are actually time slots).
· Closed Group Working: each terminal is programmed to work in a series of conversation groups. Besides individual and telephone call groups, the terminal isn’t able to participate or listen to any type of conversation.
In order to modify the programming of a radio it is necessary to have the software programme for the device, the system key, and a detailed knowledge of the group arrangement, for those groups to which the radio will need access.

1.4.5 Levels of System Security

As we have explained in the previous sections TETRA provides a series of security services much more advanced, and covering a much wider range, than any other existing system. These services can be classified in the following way:

1. Intrinsic Security of the Technology
2. Joining
3. Authentication
4. TETRA air encryption
5. End-to-end encryption

Services 1 to 4 can guarantee total communications security while avoiding the operational disadvantages and the cost involved in equipping the whole network with end-to-end encryption. There are many advantages of designing a network based on a security system that reaches level four (air encryption), without the need to recur to the use of air-to-air encryption for all devices on the network. These advantages can be summarised in the following fundamental points:
· Cost of the terminals is reduced.
· Maintenance costs for the encryption module are eliminated.
· Maintenance costs of the terminals is reduced, as manipulation of the device to install the encryption module is not necessary.
· Greater ease of key management
· Permits the use of terminals from all the different TETRA manufacturers.
· The lack of encryption modules means that terminals can be more compact.
· Reduction in energy consumption by the terminals, thus increasing their autonomy (or allowing their weight to be reduced by using smaller batteries).
· Increase in the security of key control (key injectors, etc.) for end-to-end encryption, which will only be available for reduced groups.
For the reasons given it is clear that, TETRA in general, and DIMETRA in particular, bring levels of security to a system that are wholly adequate for planning a network that relies principally on the use of air encryption; reserving end-to-end encryption for the reduced groups of users that, for their special way of operating, need a different level of security.

1.5 Advanced DIMETRA functions.

The following section covers the features that the DIMETRA system provides and that make DIMETRA the most advanced TETRA system currently available in the market.

1.5.1 “Open Channel” Group Call in Extended Area PMR Systems

This type of conversation is very usual in PMR mobile radio systems. It doesn’t however form part of the basic design of other systems, like for example, mobile telephone systems.

This type of call is basic because it is necessary for many group members to act at the same time, and rapidly. The members of conversation groups can be in different cover areas and must of course maintain conversation when passing from one zone of cover to another.

TETRA provides the protocol adequate for this type of feature and DIMETRA provides the appropriate switching capacity to assure rapid reconfiguration when a user passes from one zone of cover to another, and from one control zone to another.

This one-to-many functionality saves channel space as all group members work on the same traffic channel. This is contrary to telephone or cellular systems, where this type of call is known as a conference call, each member of the group needs their own traffic channel, and digitally coded voice needs to be decoded, before incorporating it into the switching matrix and freshly recoding it afterwards.

1.5.2 Rapid Call Set-up

The access time is defined as the delay between initiation of a call (PTT), and the point at which the communication is really established with another radio unit (suppression of receptor silence). The Nokia DIMETRA system has an access time inferior to 500 milliseconds.

When a conversation ends, the radios return to the control channel and leave the traffic channel free for other users to use.

1.5.3 Busy System

If any user requests access to the system when all the voice channels are in use, they will receive an audible engaged tone and be placed in the waiting queue until a channel is assigned to them in accordance with their pre-assigned level of priority. When a channel becomes available, the system notifies they first radio unit in the queue using “re-dial”. This consists of a short series of beeps, heard through the operator’s radiotelephone. This characteristic makes it unnecessary for the radio operator to lose valuable time in manipulating his or her radiotelephone in an attempt to achieve access to the channel.

1.5.4 Dynamic Location Assignation

In the DIMETRA system the traffic channels are only assigned to those locations in which they are needed. For example when a user makes a group call, the system assigns a traffic channel only in those locations where there is a member of that group. The traffic channels in other locations are left free to attend other calls.

The feature, Dynamic Location Assignation, enables the DIMETRA system to have more capacity for traffic management than a system with the same number of communication resources, but without this feature.

1.5.5 Busy Override

In order to make a group call one would theoretically have to wait until there was a traffic channel available in all locations where there was a user. Under normal conditions, if one or more of the required locations was occupied, the system would not process the call. However, the user who initiates the call can decide to wait for all locations to be available, or go ahead with the call; in this case any users who are in busy locations will be incorporated into the call as soon as a traffic channel becomes free in their location.

An exception to this mode of working occurs when critical users or critical locations are involved in the call. In this case the call cannot leave out such users or locations and will have to wait until traffic channels are liberated in the required locations.

1.5.6 Critical Locations and Users

In order to assure cover in certain pre-programmed areas, the system can be configured so that a call is not carried out until a traffic channel is available in locations defined as critical, or in locations where users defined as critical find themselves, even when the calling user initiates a “busy override”.

· Critical Locations. The system manager determines which (critical) locations must always receive transmissions, for each call group. When a call group has a series of critical locations defined, the user can start the call only when all these locations have a channel available. Non-critical locations will only be activated if there is a traffic channel free; if a group member is in a non-critical location that does not have available channels, they will not receive the call until a channel becomes free.

· Critical Users. When a user initiates a group call for a group that has a series of critical users defined, the locations in which these critical users find themselves at the time of the call behave like critical locations. A group can have up to 16 critical users.

1.5.7 Automatic Selection of Location

The location in which a user is registered, transmits information about its neighbouring locations, such as the identity and the main carrier frequency (the carrier that contains the control channel). In this way any radio always has a dynamic list of its nearest locations.

When a user moves, the level of field intensity received by the radio will indicate when it has to change location. The radio compares the intensity of the signal received on the present control channel with that received from adjacent locations. The list of adjacent locations is put into order according to the intensity of the signal received. When the device detects that the signal received from another location is significantly greater than that from its current location, it will register itself in the new location.

1.5.8 Preferred Location. Home Site.

In order to assure better performance a DIMETRA device can be programmed to select some locations with preference to others. This flexibility permits the system designer to create a more efficient manner of working, whereby the population of radio users is distributed across locations, assuring quicker system access.

This feature is very useful for users who normally work in areas where there is an overlap in the cover provided by two locations. In such a situation it could happen that the radios were registering themselves first in one location and then in the other, too frequently. Not only would this be without benefit for the user concerned, but it would also make far-from-optimised use of the network, because there would be users occupying channels in both locations when the service could be covered with just one.

1.5.9 Location Access

The DIMETRA Location Access functionality is similar to the Area Selection service in the TETRA standard. It allows a network operator to define a number of locations where specific types of call are available (group call, private call or telephone call), and also to define the locations that should always be included when calls are established.