Communications Monitoring

(October 2007)

- About Elaman
- Strategic Monitoring Center
- Lawful Interception Marking Terminals
- Passive Telecommunications Monitoring System
- Internet Monitoring (Strategic & Tactical)
- GSM On Air Active, Passive & Semi-Active / GSM Locating
- Satellite Monitoring Systems
- Radio Frequency Spectrum Monitoring
- Computer Monitoring / IT-Intrusion
- PABX Monitoring
- Room Monitoring
- Analytical Software / Forensic / Speech Technology
- Training and Consultancy

Index

Company **Profile**

ELAMAN GmbH, established in 2004, provides advanced integration systems, international consultancy and strategic technologies in communication systems, national security and defence. Our highly experienced international managers focus on providing solutions enabling our customers to be more adequately equipped to counter the threat of today and tomorrow.

ELAMAN is a german based company with its headquarters in Munich/Germany.
Our aim is to provide comprehensive security products and solutions, technical consultancy and services as well as professional training for governments and security agencies.

ELAMAN is a leader in International marketing and trading specialized in defence technology, communications and security.

Through strategic partnerships with many leading international companies, we provide law enforcement agencies alike with unique technology solutions all from one source.

Part of our philosophy is the conviction that training and the understanding of products and technology are critical factors and major strengths in assuring successful security solutions.
Major projects have been carried out for National Intelligence Agencies, Internal Security Agencies, Military Intelligence, VIP Security (Royal Guard) and Special Forces.

ELAMAN works closely with clients to develop a total system solution to their needs and to ensure that they are equipped, trained and manned to meet the formidable challenges in the field of communication.

Elaman GmbH
German Security Solutions

Seitzstr. 23
80538 Munich
Germany

Tel.: +49 - (0)89 - 24 20 91 80
Fax.: +49 - (0)89 - 24 20 91 81

info@elaman.de
www.elaman.de

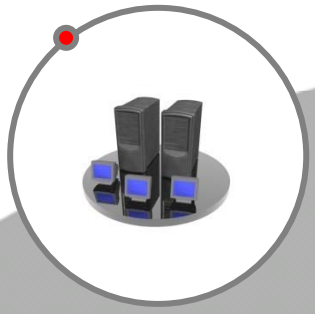
Communications
Monitoring Concept

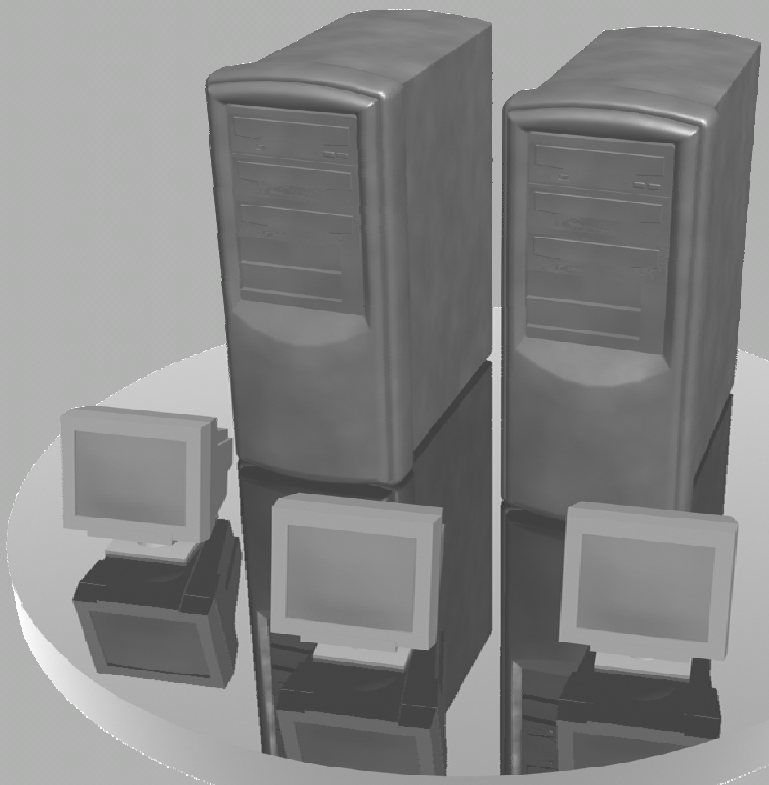
Elaman provides its clients with the perfect communications monitoring solution.
Our complete portfolio is equipped with the most sophisticated equipment, tried-and-tested techniques, and well-experienced managers making us your one-stop company that enables you to construct an entire communication monitoring system.
We give our clients the possibility to be best equipped in all communication monitoring areas which include Passive Monitoring, Computer Monitoring, GSM/UMTS Monitoring and Location Finding, Satellite Monitoring, IP Monitoring, Radio Frequency Monitoring and Room Monitoring.

Nowadays the threats our clients are exposed to are highly sophisticated and advance, thus the only way to be well-protected from these threats is to match – and surpass – their technological level.

We have designed all our communications monitoring systems to fit perfectly together and complement each other in all operational tasks and fields.

Strategic Monitoring Center &
Lawful Interception Marking
Terminals





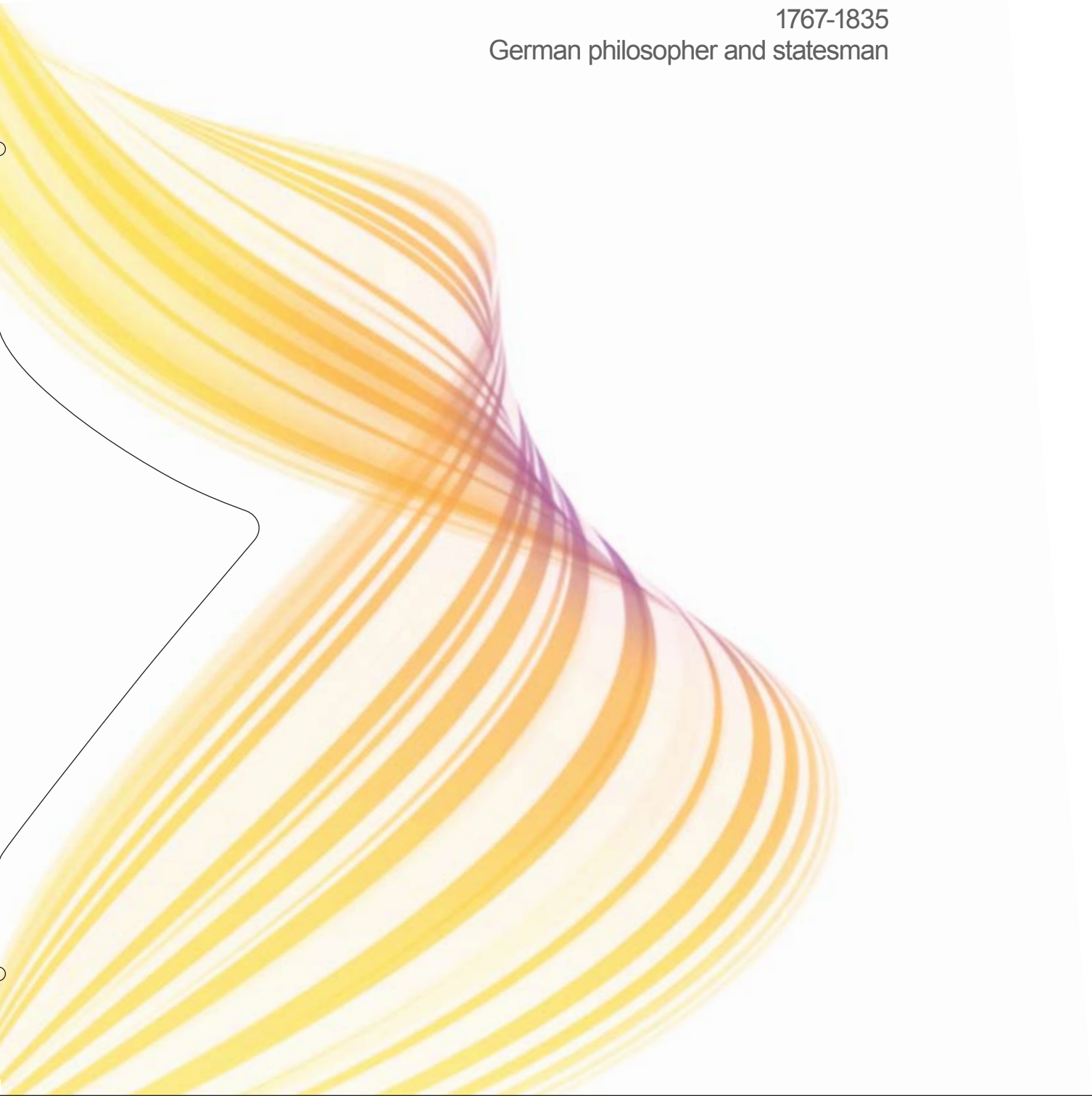
Index

Making the world safer
with trend-setting intelligence solutions

Nokia Siemens Networks

“Without Security
there is no Freedom.”

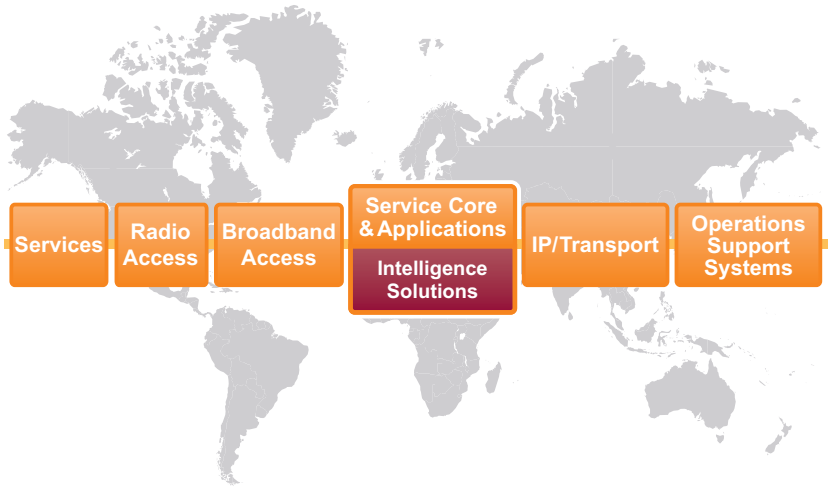
Wilhelm Freiherr von Humboldt
1767-1835
German philosopher and statesman



Intelligence Solutions for a dynamic world.

The world of communications is changing constantly. New technologies and ways of communication are being invented daily. Evolving from novelty to ubiquity, they become available to friend or foe alike.

For authorized groups worldwide it is not enough merely to keep pace with technological progress. To be ahead of innovation is the key to securing peace and prosperity worldwide.



In this context, Nokia Siemens Networks Intelligence Solutions is a well-founded choice and a safe investment in a secure future. It represents the clear decision for a financially strong and stable vendor with operations in more than 150 countries around the world. The global service network and distribution system includes customized services and after-sales support in line with our customers' individual needs and operational demands.

Our product lines Monitoring Center and Intelligence Platform offer tailored solutions for lawful interception, monitoring and intelligence analysis to law enforcement agencies, government agencies and authorized groups worldwide. They enable them to master the challenges of a changing world.

Customers in more than 60 countries around the world trust Nokia Siemens Networks Intelligence Solutions. To date, more than 90 solutions have been sold and we are proud to state that we have never lost a customer.

Intelligence Solutions
Monitoring Center
Keep your eyes open

"Keep your eyes open" is not only the imperative duty of law enforcement agencies worldwide – it is everyday reality in the Monitoring Center.

What can better represent the very essence of our intelligence solutions than the peerless black panther? Constantly alert, his vigilant eye misses nothing. That is why we have chosen the panther's eye as the symbol for our Monitoring Center.

One solution for all networks, vendors and technologies.

The Monitoring Center has been specifically developed to service the complex monitoring needs of law enforcement agencies worldwide. It is a remarkably versatile combination of interoperating software and hardware modules and is designed to perform all tasks related to lawful interception in an absolutely secure, auditable, reliable and verifiable manner in accordance with ETSI LI standards. Its unique modular Front-End and Back-End architecture allows the monitoring and interception of all types of voice and data communication in all networks, i.e. fixed, mobile, Next Generation Network (NGN) and the internet.

Despite its complexity, the Monitoring Center's modular design is extremely flexible – allowing for customized solutions, scalable in size and capacity. It has been designed to address all networks and monitoring requirements. Our customers can choose from a wide range of add-on applications to access already available information and provide additional intelligence.

The Monitoring Center's unified view-concept greatly facilitates investigative work and opens completely new and efficient ways to pursue leads.

Intelligence Solutions
Intelligence Platform
Trace the track…to stay ahead

The black panther is characterized by its remarkable elegance of movement and outstanding intelligence. Its position at the top of the food chain is undisputed. Its nose is so sensitive that it can trace even the faintest track. That is why we have chosen the panther's nose as the symbol for our Intelligence Platform.

Today, the greatest challenge which law enforcement agencies have to face worldwide is not data collection, but data analysis. It is not a matter of obtaining and accessing authentic data, but of putting information in context and transforming it into intelligence.

Intelligence is the synergetic product of connecting the dots and providing meaningful and trustworthy information to decision-makers about the changing nature of threats.

Our Intelligence Platform is a comprehensive and flexible intelligence analysis solution. It dissects huge amounts of data and finds hidden clues in seemingly meaningless snippets of information. It creates new intelligence by using sophisticated intelligence applications and extensive automation to process mass data.

The basic principle of the Intelligence Platform is very simple: It offers one platform and one desktop for all functions. However, the modular, scalable design allows for a high degree of customization by which all features can be configured to meet customer requirements. Optional intelligence modules can be added separately on request.

The Intelligence Platform provides intelligence which results from the collection, processing, integration, analysis, evaluation and correlation of available data, thereby supporting the entire intelligence cycle.

It is the smart analytical tool for intelligence personnel and analysts, enabling them to trace the track and helping decision-makers to fulfill their mandates: To identify and predict trends, patterns or problem areas that require action. Its outstanding features enable them to react on a level totally unmatched in today's and tomorrow's world of preemptive security.

The Nokia Siemens Networks Intelligence Platform sets new standards in intelligence. It offers innovative tailored solutions which are characterized by operational agility independent of time and place. It has been designed to meet all law-enforcement and governmental requirements and standards – to trace the track and stay ahead.

Our Vision
With insight and ingenuity we will continue to break new ground and lead the way for innovative intelligence solutions. We are convinced that our expertise will enhance peace and thereby contribute to the quality of peoples' lives.

Our Commitment
We deliver evolutionary security solutions by combining best-of-class products, state-of-the-art technologies, services and creativity, thus generating sustainable customer benefits.

Our Core Values
We are guided by customer-centered principles. These are based on mutual trust, reliability and stability.

Our Credo
It is idle merely to philosophize about warnings like "Without security, there is no freedom". Good governance acts upon them and takes appropriate measures to make the world a safer place for individuals, families and nations.

We believe that this is where true freedom begins.

Our Mission
We are making the world safer with trendsetting intelligence solutions.

We are pioneers, constantly pushing boundaries to break new ground for innovative solutions.
We are passionate, employing all our talent and energy to help our customers fulfill their mandates.
We are pragmatic, determined to make sure that our solutions always meet our customers' needs.

Nokia Siemens Networks GmbH & Co. KG
Intelligence Solutions
DE-81359 Munich
Germany

Visiting address:
Hofmannstr. 51, Munich, Germany
Switchboard +49 89 722 00

Order No. C40100030B2007091EN

IS-sales.nsn@nsn.com
www.nokiasiemensnetworks.com

Intelligence Solutions
Lawful Interception and Monitoring

Nokia Siemens Networks

Using telecommunications to target terrorism and crime

State-of-the-art systems for communication monitoring

Contents

Never before has information been exchanged so rapidly and in so many ways. Needless to say, criminals and terrorist organizations have also been quick to realize the vast opportunities presented by modern telecommunications.

When it comes to fighting crime and thwarting terrorist attacks, law enforcement and government security agencies need the right communication tools to get results.

This is why state-of-the-art systems are an absolute 'must' in monitoring the communications of specific groups or individuals, for example in preventing criminal activities or collecting hard and fast evidence.

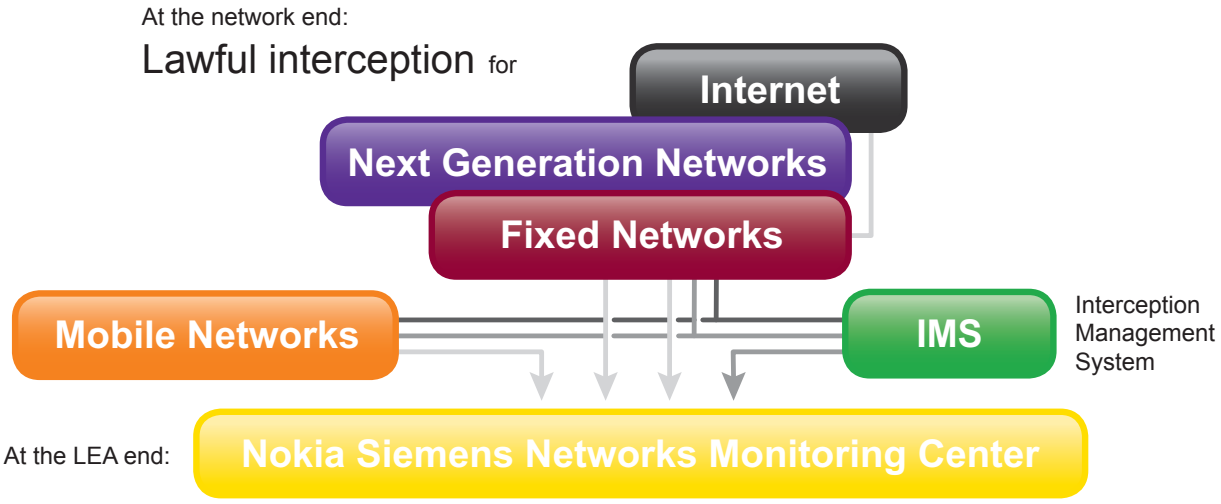
Network operators around the world are also increasingly involved in issues through the changes in legislation and standardization that require their equipment to be able to monitor or record all forms of telecommunications whenever necessary.

Based on ETSI compliant components, Nokia Siemens Networks Intelligence Solutions has the perfect and comprehensive solution for your needs, whether you are a network operator, a service provider, law enforcement or governmental agency. Our offer is scalable in size and capacity and with extendable interfaces, and even on a turnkey basis, if you like.

Nokia Siemens Networks Intelligence Solutions is worldwide the only vendor who can offer a complete end-to-end lawful interception solution.

We also offer you a wide range of services with worldwide support. Prior to and after project implementation – with 150 years of expertise in telecommunications and an internationally experienced team of security-cleared experts.

Our ‘Lawful Interception and Monitoring concept’ – the solution for the needs of all networks, LEAs, and government agencies.



Equipping network operators for all eventualities ...

Is it sufficient to install special equipment as the need arises?

There are many benefits with Nokia Siemens Networks LI solutions integrated in standard network equipment. The beauty of these is that they

- come from a single source
- do not require any additional space or camouflage
- are ready for operation at all times
- fulfill the most stringent of legal requirements
- do not interfere with regular network operations in any way
- function reliably, securely and discreetly on the basis of globally proven network technology
- permit centralized operation and system maintenance/ troubleshooting

Do you need high-security areas and specially trained staff for all switches?

This is no longer necessary if you use our efficient Interception Management System (IMS). With low space and cost requirements, IMS offers location as well as organization-independent and thus highly flexible administration of lawful interception. Even in its smallest configuration, it can handle

- central administration of more than 1,000 lawful interceptions at any one time in different networks
- integration of system users located far from the central IMS server or external users working with LI applications from other vendors

As a telecom carrier you probably already know that you are obliged to perform lawful interception in all your networks and for all the telecommunications services you offer. This means you need to have the equipment required by law and be prepared to act rapidly, if need be. After all, your operating license depends on it.

Understandably, however, you also want to minimize the resources deployed in lawful interception and prevent this from interfering with your core business. So, how can you make sure you are always prepared – in terms of both staff and technology – while remaining within your budget?

What about the need to invest in new solutions each time the requirements have changed?

Choose a system that can evolve over time and thus meet all your future needs. The network-end LI solutions from Nokia Siemens Networks can be

- scaled in size
- configured separately in terms of capacity
- adapted to comply with different legal requirements
- expanded if necessary to accommodate new standards and interfaces

Are there any additional precautions to protect the system and network from unauthorized access?

Security is already an integral component. LI solutions from Nokia Siemens Networks

- are based on standard network equipment, and thus not even detectable by experts
- function completely independently of regular network operations
- are operated centrally via a management system with a security-oriented user concept and sophisticated access protection
- additionally protect the network elements against unauthorized access through a special authentication process

Or perhaps would you rather avoid all the hassle?

Then let us do the work.

With a service mandate you can delegate the entire area of lawful interception to our security-cleared LI experts. These are well versed in all the relevant technical and legal issues on an international level.

Please have a look at page 23 for more on our comprehensive service offer.

Answering the transformation of the telecom landscape ...

Is a complete data inflow from all networks guaranteed?

You can be sure of this, if the network uses LI solutions by Nokia Siemens Networks. Collecting data from fixed and mobile public networks, Next Generation Networks and the internet provides you with

- Intercept Related Information (IRI), i.e. details on any successful or unsuccessful target activity
  - for example every telephone call that is diverted, any changes made on the subscriber line (such as feature activation and deactivation) or, in case of mobile networks, the subscriber's current location
- call content, i.e. the complete content of all voice, fax and data transmissions from or to the target
- notification of all LI-relevant incidents (e.g. setting up or activation/deactivation of lawful interception in the network)

* See page 12 for a list of targets that can be monitored using Nokia Siemens Network end-to-end solutions.

Can you decide which target-data needs to be intercepted?

You should only receive the data you really need. With this in mind the Nokia Siemens Networks LI solutions offer the following data delivery options

- separate delivery of call content and IRI
- joint delivery of call content and IRI (always the case for internet data transfers, otherwise optional)
- delivery of IRI only (converted on request into e.g. ETSI or text format)
- delivery to up to five LEAs (defining for each recipient either IRI only or both, IRI and call content)

Recent changes in legislation will place an even greater burden on you in the future. Meanwhile, new technologies and the ever-expanding range of network-independent services are transforming the telecommunications landscape into a virtual jungle, with a labyrinth of intertwining paths which makes it increasingly difficult for you to follow leads. Your job is getting more and more complex.

What you really need to do now – perhaps together with the responsible network operators – is to cast a critical eye over both the end-to-end systems used for collecting and transfering information and your own equipment which receives and analyzes the data.

Is it possible to monitor all types and sizes of data transfer?

Definitely, if you use the Nokia Siemens Networks Monitoring Center at your agency. This versatile system

- 'understands' all forms of voice, fax and data communication from all fixed and mobile networks based on components from leading vendors as well as Next Generation Networks (NGN) and the internet
- is designed as standard to process call content and IRI sent separately
- can also handle huge volumes of information (e.g. from the internet) – with no loss of quality or data – thanks to its highly efficient recording systems (e.g. with full duplex/high-speed mode, voice compression)

Is data interpretation sufficiently quick?

Our Monitoring Center helps to speed up your investigative work as it

- automatically saves the data received from the networks in case-specific folders, ruling out any confusion
- permits authorized individuals to quickly access the specific information needed
- facilitates and accelerates the monitoring/surveillance process and data analysis with a range of user-friendly, practical features
- offers new and efficient ways of pursuing leads (e.g. geographic information system)

Can the system easily be adapted?

No matter which new technical or organizational requirements come into effect, the modular Nokia Siemens Networks Monitoring Center keeps you flexible and up-to-date at all times, as it

- is continually enhanced, in parallel with the evolution of network technologies
- can be extended or modified at any time on the basis of existing hardware/software components
- grows in terms of size and capacity in accordance with your needs
- can be configured in line with current requirements and adapted to comply with different legislation

IMS – the secure manager for all networks

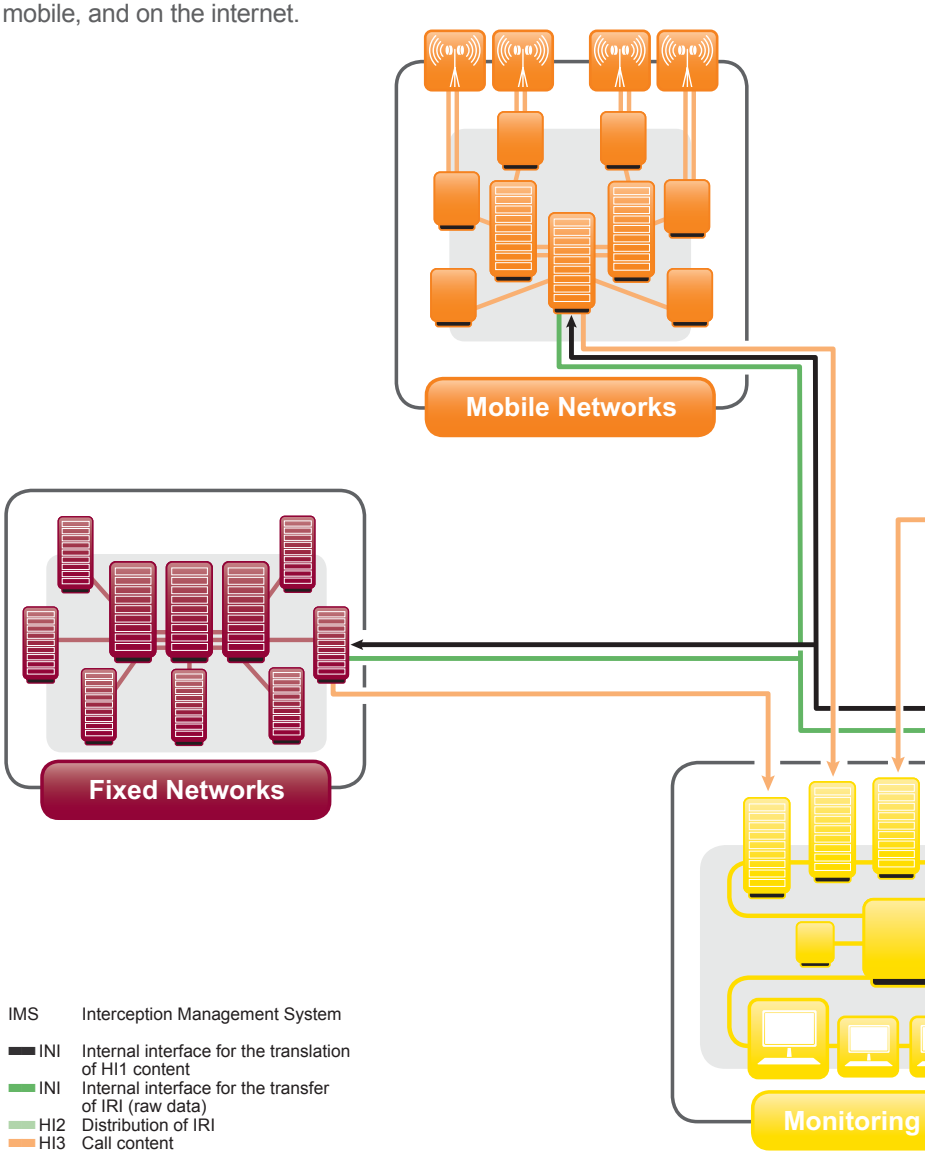
Universal

IMS is an interception management system for secure, reliable and verifiable central control of all LI-related tasks required at the network end: From setting up, starting, modifying and ending the LI instance in the network element to the administration of user-rights and auditing as well as alarm-handling and system maintenance/ troubleshooting. It is also used for mediation and distribution of IRI (Intercept Related Information, please see page 14) and for setting different filters in the data collectors used for internet surveillance.

As part of the Nokia Siemens Networks 'Lawful Interception and Monitoring concept', the IMS combined with the LI components and the Monitoring Center produces a comprehensive solution for all network and LEA requirements.

However, it can be used for vendor-independent central administration of lawful interception in all ETSI-compliant public networks: Fixed, mobile, and on the internet.

It can be used alone, in conjunction with other LI management systems, or even as an umbrella system.



An interception order has been issued. The instructions are clear. Now they need to be translated into machine language and communicated to the network.

How can this be done in a fast, economical and accurate manner? How to prevent any inadvertent or willful manipulation of the network element during the input procedure? Who checks that everything has been done properly? And what about discretion and data protection? – The answer is the Interception Management System (IMS).

Flexible

With IMS, tailor-made solutions can easily be created for a wide variety of circumstances

- with its client/server architecture, the system can be scaled to match any network size without compromising performance
- the range of offered functions also grows with the need and with special, optional feature-packages on the customer's request
- a special IMS function is available to assist in upgrading Nokia Siemens Networks network elements

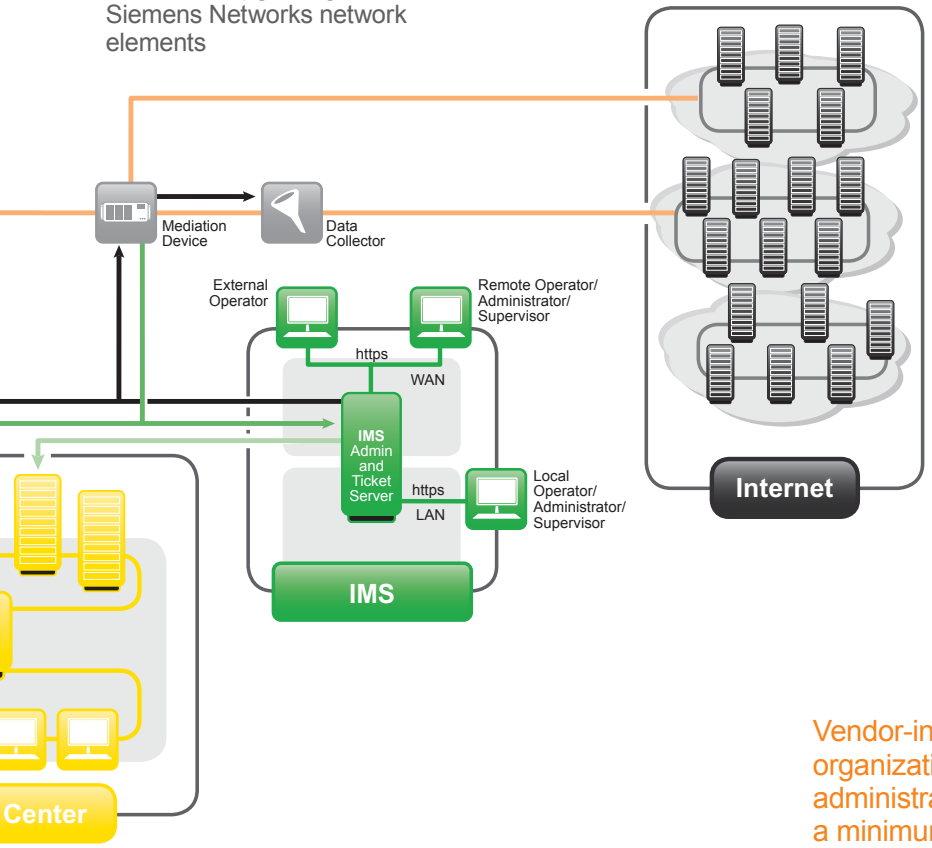
Depending on whether it is for stand-alone operation or in conjunction with other LI-operating systems, the individually configurable IMS can be used either for all LI tasks (full mode), for LI administration only (admin-mode) or for routing the IRI only (ticket-mode). This ensures a broad range of application variants for the system.

Region-independent

Now being operated in some 40 different countries around the world, IMS is globally deployed. Its security-oriented user-concept, which divides the tasks as standard into the functions of operator, administrator and supervisor, each of which with clearly defined rights, can easily be adapted to comply with different legislations.

IMS can be operated from user stations. These can be either centrally or remotely located. Remote access can be secured using VPNs. The IMS is further supported by the external operator interface. This also ensures IMS access to system-users operators, administrators, supervisors) working with an LI application by another vendor.

Other external interfaces, which may be extended as necessary, provide for the smooth integration of IMS into heterogeneous network infrastructures.



Vendor-independent. Regardless of the location and organization: IMS is all the network operator needs for administration of lawful interception in all networks with a minimum of financial and human resources.

IMS – the secure manager for all technologies and networks

Secure

Protected in a high-security area or by a firewall, IMS is operated completely separately from regular network management. The functions performed by IMS (e.g. setting up, modifying and ending lawful interception in the network or converting and distributing IRI) cannot be performed by a conventional network management system. Likewise, the IMS interception manager does not perform any standard network management functions.

IMS provides complete system and data protection by means of a hierarchically structured user concept. The GUI, strictly adapted to each specific task area, prevents users from exceeding their authority. No user of the system can access the content of the IRI transported via IMS to its authorized destination. An optional variety of system access blocks all unauthorized individuals (e.g. login with a chip card, sophisticated password system).

In addition, the LI-fixed network solutions include a special authentication procedure for additional security. This automatically comes into play in each dialog between IMS and the network element, optimally protecting the latter from sabotage.

Alert

As a LEA you can also protect yourself from sabotage or third-party monitoring by organizing yourself as a CUG (Closed User Group) in IMS. All activity in or via IMS, whether successful or not, to/from the network or to/from your Monitoring Center, is automatically logged and stored, allowing it to be checked at any time. Only the supervisor has access to this database.

Any attempt at external manipulation is immediately detected by a special IMS function. In all cases of unexpected or irregular incidents (such as network element or transmission failures), a sophisticated alarm system ensures that the relevant person is immediately notified (by a pop-up window, email, or SMS).

Our comprehensive security concept, which, as a rule, also incorporates https-based communication between IMS clients and the IMS server, redundant servers and interfaces as a rule, as well as an uninterruptible power supply, guarantees the best possible protection against unauthorized access and loss of data. This is also true when the system is operated from remote or external user stations.

High-performance browsers, for example, help the IMS Supervisor fulfill his control function. One of these is the log browser which makes it easier for him to keep an overview of the various procedures processed via IMS...

IMS prevents users from exceeding their authorization through user-specific menus, strictly tailored for the specific authorizations of operators, administrators and supervisors. A range of efficient and practical features simplify and speed up the execution of all the LI-related tasks to be performed on the network side.

Important for law enforcement agencies...

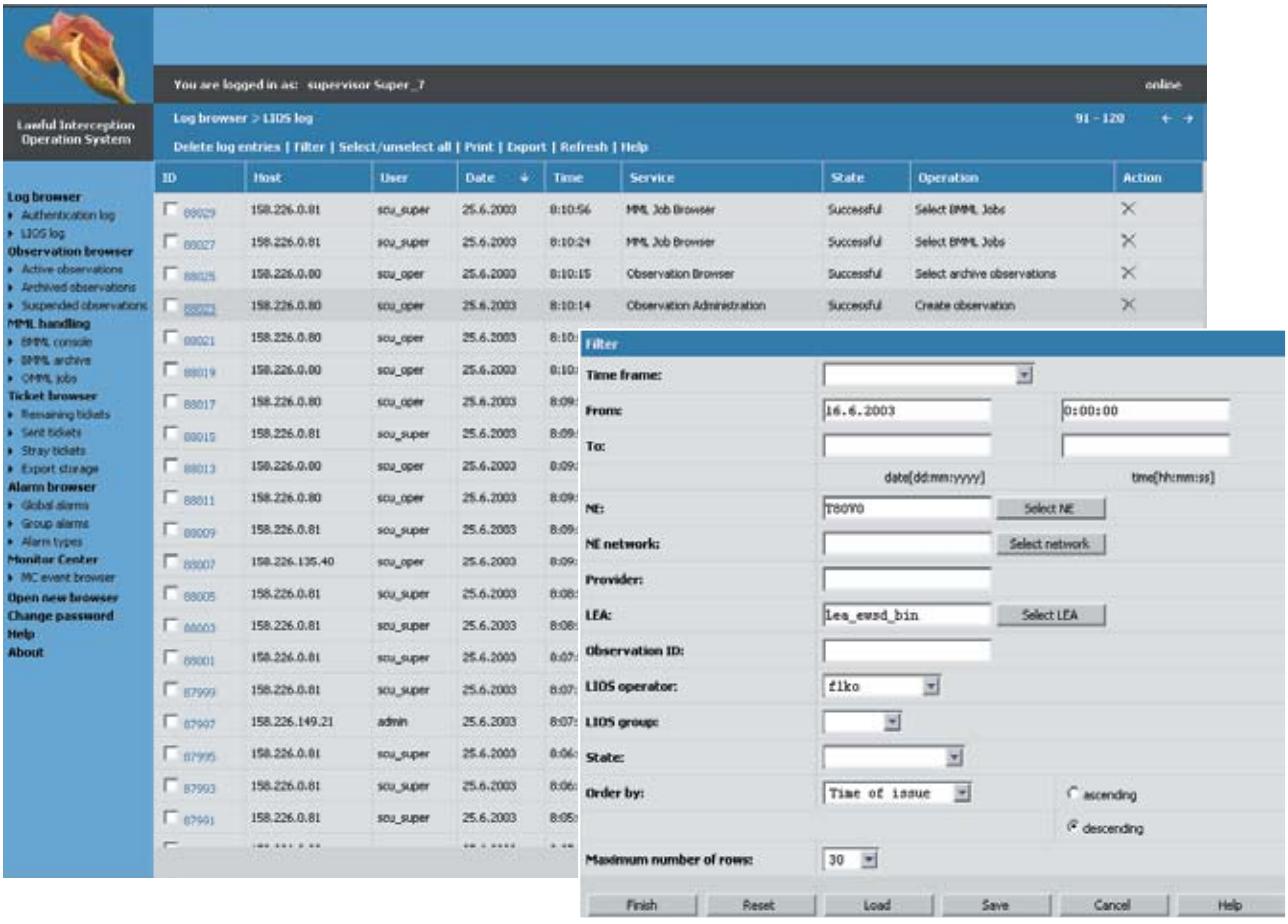
Intercept Related Information (IRI) which cannot be forwarded to you straight away is never lost. It can subsequently be retrieved via IMS only and, on your request, also be manually made available for you as a file on a removable storage medium.

Economical

The centralized interception provided by IMS, independent of both location and organization, results in substantial savings for you, the network operator, in terms of both space and staff.

A single IMS is enough to manage several thousand lawful interceptions running concurrently in various networks. Its Windows-based, user-friendly interface (see example below) and a maximum of automatic procedures minimize IMS input-errors, and simplify and speed up all steps involved.

... here the supervisor can define which processes he would like to see listed in the log browser



Lawful Interception and how it works ...

The Nokia Siemens Networks end-to-end LI solutions can be used to monitor the following targets

in fixed networks and Next Generation Networks

- all types of subscriber access
  - analog subscriber access
  - ISDN-BA and ISDN-PA
  - coin- or card-operated payphones
  - directory-number-based calls in IP networks
  - PBX directory numbers (if included in the signaling)
  - individual MSNs (multiple subscriber numbers) of an ISDN basic access
- switch-internal subscriber numbers
- FDNs (foreign directory numbers, i.e. switch-external directory numbers, such as in case of calls from or to extensions or directory numbers in transit traffic)
- nailed-up connections (dedicated lines)
- calls with call diversion
- conference calls (a special LI function combines the call content in this case)

in mobile networks

In addition to the targets of fixed networks and Next Generation Networks

- all types of mobile phones
- circuit-switched traffic in GPRS and 3G networks
- packet-switched traffic in GPRS and 3G networks

on the internet

- internet traffic at access points in the following areas
  - local loop / access provider
  - service provider
  - backbone

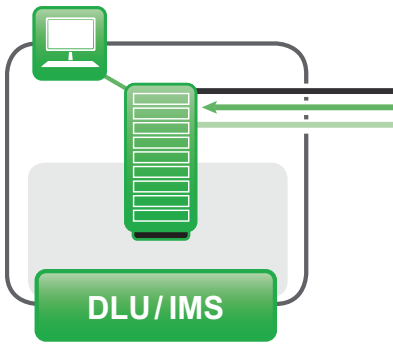
What are your main expectations of an end-to-end lawful interception solution?

As a network operator you want to be able to comply with the legal requirements at minimum cost and prevent any adverse effects on your core business.

As a law enforcement agency you want to be able to monitor a complete spectrum of targets, receiving only the relevant data from the network – as required by your organization.

The LI solutions as a part of our 'Lawful Interception and Monitoring concept', designed for deployment in various different networks, address the needs of both sides.

No need for camouflage. No extra space required. No interference with regular network operation: For the network operator, LI solutions integrated into standard network equipment are the most discreet, secure and cost-effective means of performing lawful interception in fixed and mobile networks from Nokia Siemens Networks. For you, the law enforcement agency, these solutions guarantee a complete, needs-oriented and confidential data inflow from all networks.



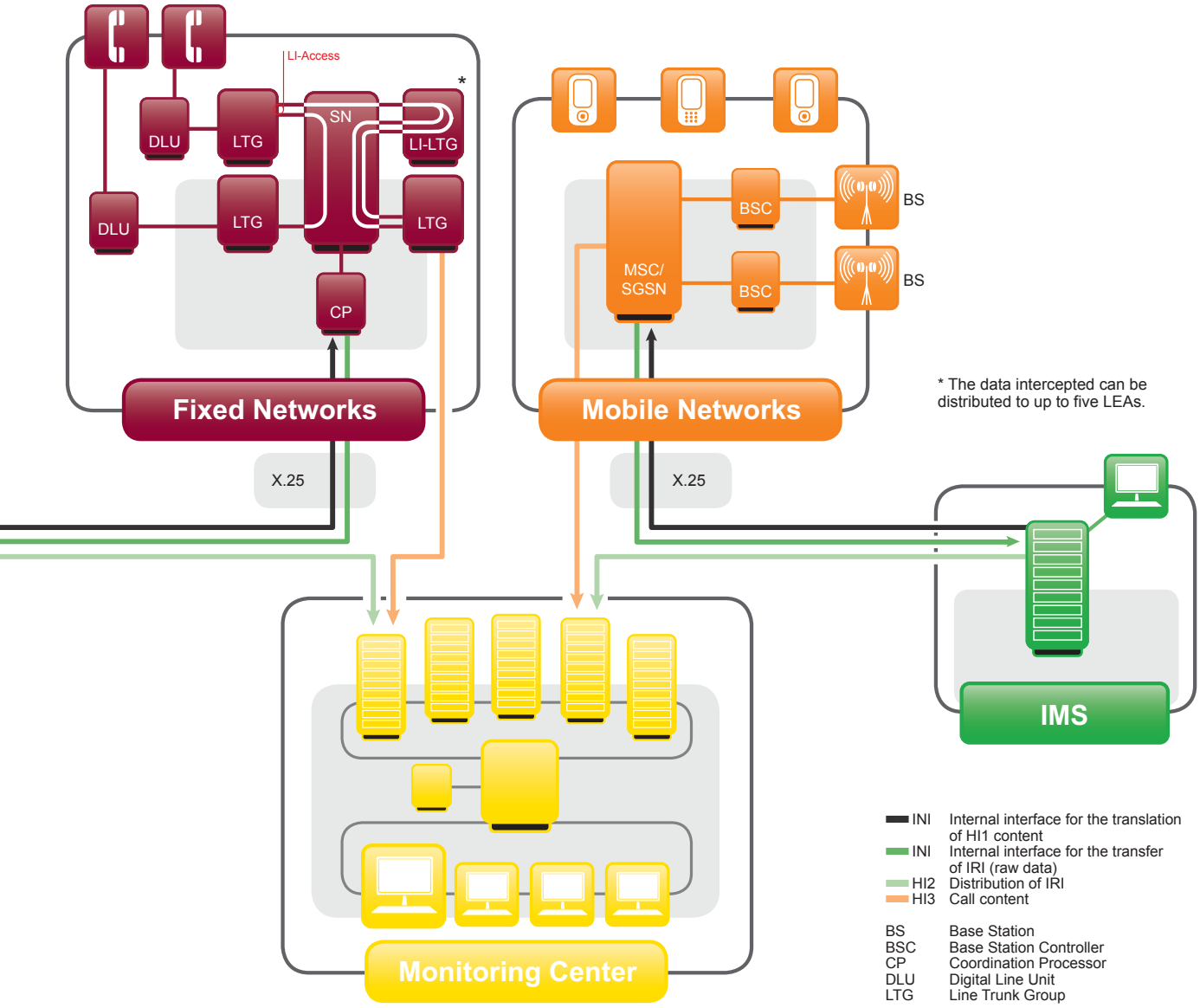
... in fixed and mobile networks ...

The lawful interception has been set up using IMS. Its starting and ending times have been defined. The subscriber line in question has already been marked for interception. At the defined time, IMS activates the interception in the network element. Once this has been done, LI begins to operate for the entire monitoring period.

Verifiable

Whenever a call becomes active on the line under surveillance, the call content (i.e. the entire content of incoming and outgoing phone calls, fax or data transmissions) is automatically intercepted and copied to a monitoring connection, which is established to the authorized LEA only for the duration of the current interception procedure.

Should any interruption or irregularity occur during this automatic procedure, the IMS operator in charge is immediately notified by email, SMS or a pop-up window. Using the messages on the IMS screen, the operator can check at any time whether data collection is running smoothly in the network.



... in fixed and mobile networks ...

Discreet

The establishment of a monitoring connection, the interception and recording of the data on the basis of standard network equipment is invisible to the target-subscriber. The process does not interfere with regular network operation in any way.

As the subscriber is not aware of the interception process, even if it starts after a call has become active, there is no risk that he may hear suspicious tapping noises and therefore perhaps cut short the call. Its recorded content is sent to the LEA's equipment directly from the switch. This is the reason why it cannot be intercepted or accessed at the IMS or manipulated in any way.

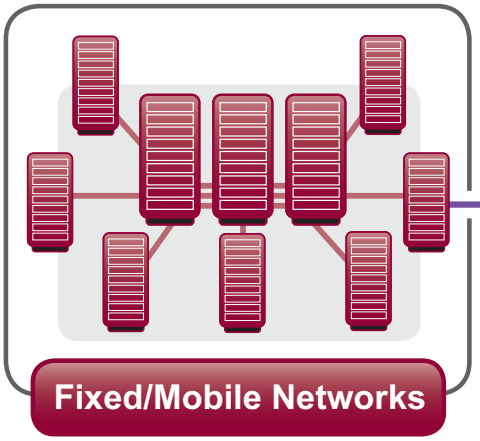
Comprehensive

Moreover, apart from the complete and discreet recording of call content, the Nokia Siemens Networks LI solutions also perform another important function: As soon as there is an activity (whether successful or not) on the monitored access, they also generate intercept related information (IRI). This may include information on the date and time of the call, the directory number of the other party, the call direction (incoming or outgoing), any call diversion procedures invoked, and (optional in mobile networks) the current location of the target subscriber. They also provide information on any technical or administrative changes made on the marked access (e.g. feature activation or deactivation).

Regardless of the call content, an IRI is first sent to IMS. From here it is forwarded via a data network (public X.25, ISDN or IP network) to the monitoring equipment of the LEA. Based on the unambiguously assigned ID criteria, the IRI is automatically correlated with the corresponding call content at the LEA. The transmission of this data on two completely separate paths is of benefit to the LEA for two reasons:

LEA-friendly

- you can decide in each case whether you need only the IRI (which often includes sufficient information in itself) or also the call content, thereby minimizing the data inflow, and thus also the time you need to evaluate it
- you can be assured that even if you do not receive any call content (for technical or other reasons), you will nevertheless have the IRI which – as already explained on page 11 – cannot get lost, even in the case of delivery problems



All the advantages of a tried-and-tested standard network solution have been incorporated into this network of the future. For you, the network operator, the LI solution for number-based traffic in Next Generation Networks is one more argument to move into the world of IP. For the LEA, this is an important addition to the range of targets it can monitor.

... in Next Generation Networks ...

Nokia Siemens Networks facilitates the migration process through a variety of solutions designed to incorporate existing TDM networks into an IP core network. Of course, this also includes an IP-based solution for LI, for secure and discreet interception of number-based traffic (i.e. voice and fax connection as well as ISDN data transmissions) in Next Generation Networks.

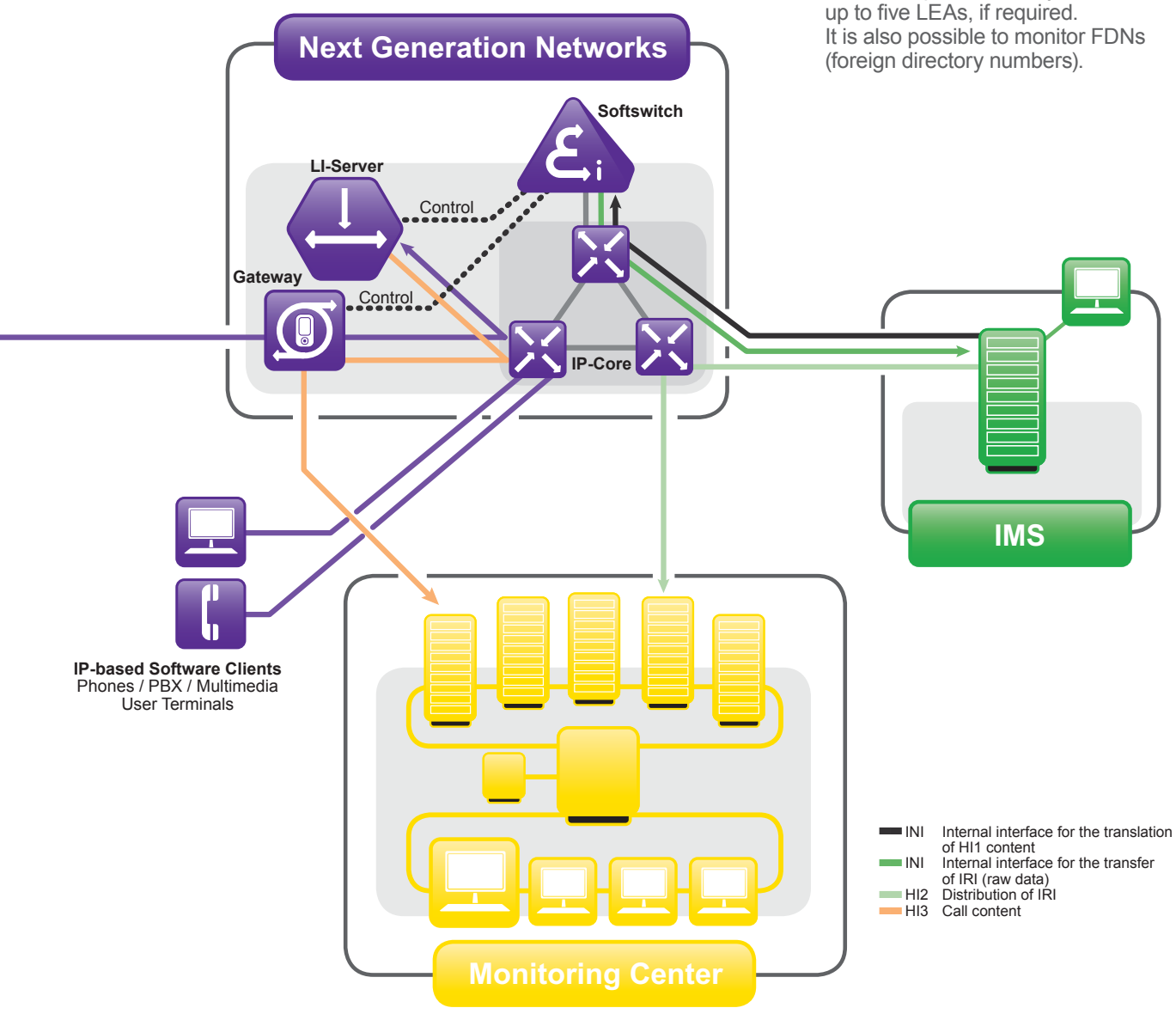
Future-oriented

As in TDM networks, the interception is set up, started and ended in a dialog between the IMS LI management system and the network element which controls the traffic to or from the monitored number. In this solution it is a standard softswitch.

Once the LI instance has been activated, this network element – in a dialog with various gateways – arranges for all the traffic concerning the target number to be routed via an LI server. Thanks to the appropriate precautions, the subscriber does not notice anything.

The packages duplicated in this server and readdressed in accordance with the instructions from the softswitch are then forwarded in the IP network to a gateway, from where they are sent to the LEA's monitoring equipment. The IRI generated in the softswitch reaches the LEA via IMS, independent of the call content.

Even in this purely IP-based solution, the intercepted data may be sent to up to five LEAs, if required. It is also possible to monitor FDNs (foreign directory numbers).



... and on the internet

The internet has become an increasingly complex formation of public and private computer networks that now also includes wireless transmission media. Every day masses of data pass through this global network used by more and more people who exchange information and keep in contact in many different ways.

The ETSI specifications on the monitoring of internet users are in place and are already met by the Monitoring Center. The Nokia Siemens Networks concept offers LEAs a comprehensive solution to help them fight crime on and via the internet. The end-to-end components of this solution are

Customized

By means of integrated LI functionality in the components of the IP network as well as by separate high-performance data collectors data can be intercepted and filtered based on predefined criteria.

According to the requirements, interception can be deployed at different access points: At the internet access provider, the internet service provider, or the internet backbone itself.

A mediation device used for adapting interfaces and also re-filtering, if necessary, distributes the required data to the LEAs.

Several types of data collectors with different interfaces and throughputs are available. Combined with individual mediation devices which also directly interface to LI-enabled IP network components, they produce perfectly tailored solutions.

As part of the Siemens 'Lawful Interception and Monitoring concept', these data collectors team up with the LI components and IMS or the Monitoring Center to produce a comprehensive solution that meets all the needs of both network operators and LEAs.

They can also be used on a vendor-independent basis for secure, reliable and verifiable collection of voice and data communication on the internet.

The integrated LI functionality and the data collectors outlined here record all types of IP-based telecommunication, including web sessions, email and chats, from

- internet service/acess providers
- internet backbone connections
- internet core computers and all other IP sources.

For the network operator the LI solution is a secure and yet flexible basis to easily record huge volumes of intercepted data in this telecommunications area. For the LEA it is an efficient means to pursue leads in the global network. And for the internet it is powerful, reliable and for lease, according to your preference.

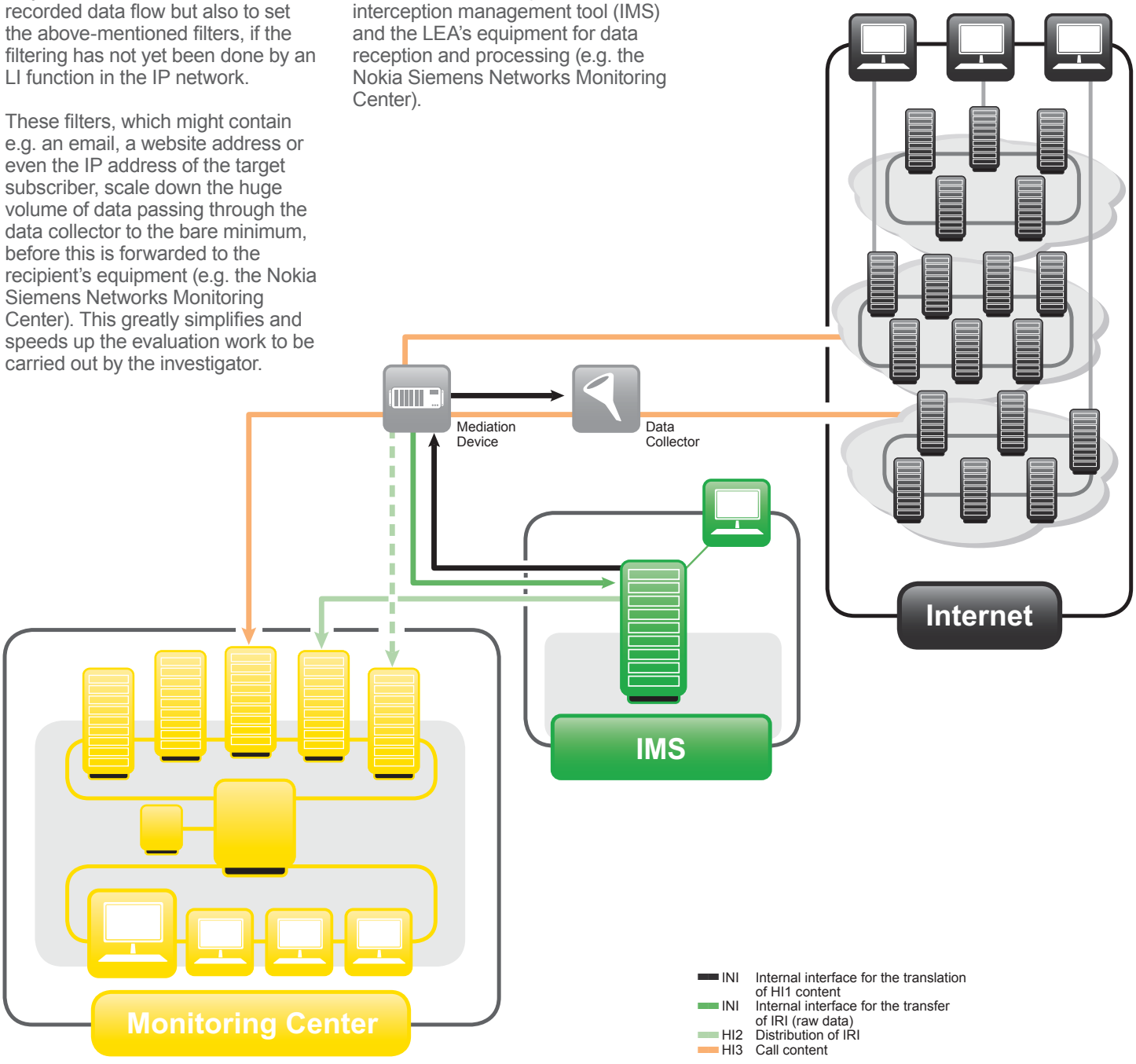
Efficient

Lawful interception is set up and managed in the data collectors by means of an appropriate and powerful interception management system such as IMS. This will be used by the the LI operator not only to define the destination of the recorded data flow but also to set the above-mentioned filters, if the filtering has not yet been done by an LI function in the IP network.

These filters, which might contain e.g. an email, a website address or even the IP address of the target subscriber, scale down the huge volume of data passing through the data collector to the bare minimum, before this is forwarded to the recipient's equipment (e.g. the Nokia Siemens Networks Monitoring Center). This greatly simplifies and speeds up the evaluation work to be carried out by the investigator.

Secure

Any system connected to the internet is at great risk of coming under attack. This risk has been minimized in the solution described. Virtual private networks, anti-virus and anti-hacker tools and special firewalls are used to protect both the interception management tool (IMS) and the LEA's equipment for data reception and processing (e.g. the Nokia Siemens Networks Monitoring Center).



Our Monitoring Center
a perfect match

The interception has been activated. The process is running. Information from various sources is flowing along different paths into your equipment.

What now?

The incoming data has to be decoded and allocated to its specific case. Any misunderstandings or confusion arising here could have serious consequences. During evaluation, even the tiniest of details may need to undergo more in-depth analysis.

How can you protect this valuable data from manipulation or theft? And what happens in the case of a power outage?

To meet this challenging task, law enforcement agencies in more than 60 countries around the world place their trust in the Nokia Siemens Networks Monitoring Center.

Versatile

Our Monitoring Center is an extremely versatile construction of software and hardware modules. Its various components work together in perfect harmony, enabling it to perform all the LI-related tasks of a law enforcement agency in a secure, reliable and verifiable manner; from decoding, converting, correlating and analyzing the information received, to its storage and interpretation, and even a wide range of administrative tasks. As part of the Nokia Siemens Networks 'Lawful Interception and Monitoring concept', the Monitoring Center teams up with the network components and the IMS to form a comprehensive solution that meets all the needs of both, network operators and LEAs.

By virtue of its ETSI compliance and modular architecture, it can also be incorporated into all monitoring solutions based on the telecom systems of other leading vendors.

The Nokia Siemens Monitoring Center monitors all types of voice, fax and data communication in fixed and mobile networks as well as in Next Generation Networks (NGN) and on the internet:

- telephone conversations
- fax and modem traffic
- SMS and MMS
- emails, web sessions, chats etc.

It also supports the reception, processing, correlation and evaluation of the IRI described on page 14. If preferred, it can be configured for countrywide monitoring of all fixed networks, mobile networks, NGN and the internet.

Flexible

Changes to requirements? Heterogeneous network infrastructures? New technologies to be addressed, higher data volumes to be handled, or more types of communication to be monitored?

This is all very easy with the Nokia Siemens Networks Monitoring Center. Its modular design, which comprises Front-End and Back-End components (see illustration), makes it extremely flexible. The individual Front-Ends which support the interfaces from the different telecommunications networks can be adapted to match a wide variety of communications systems and replaced or expanded as necessary.

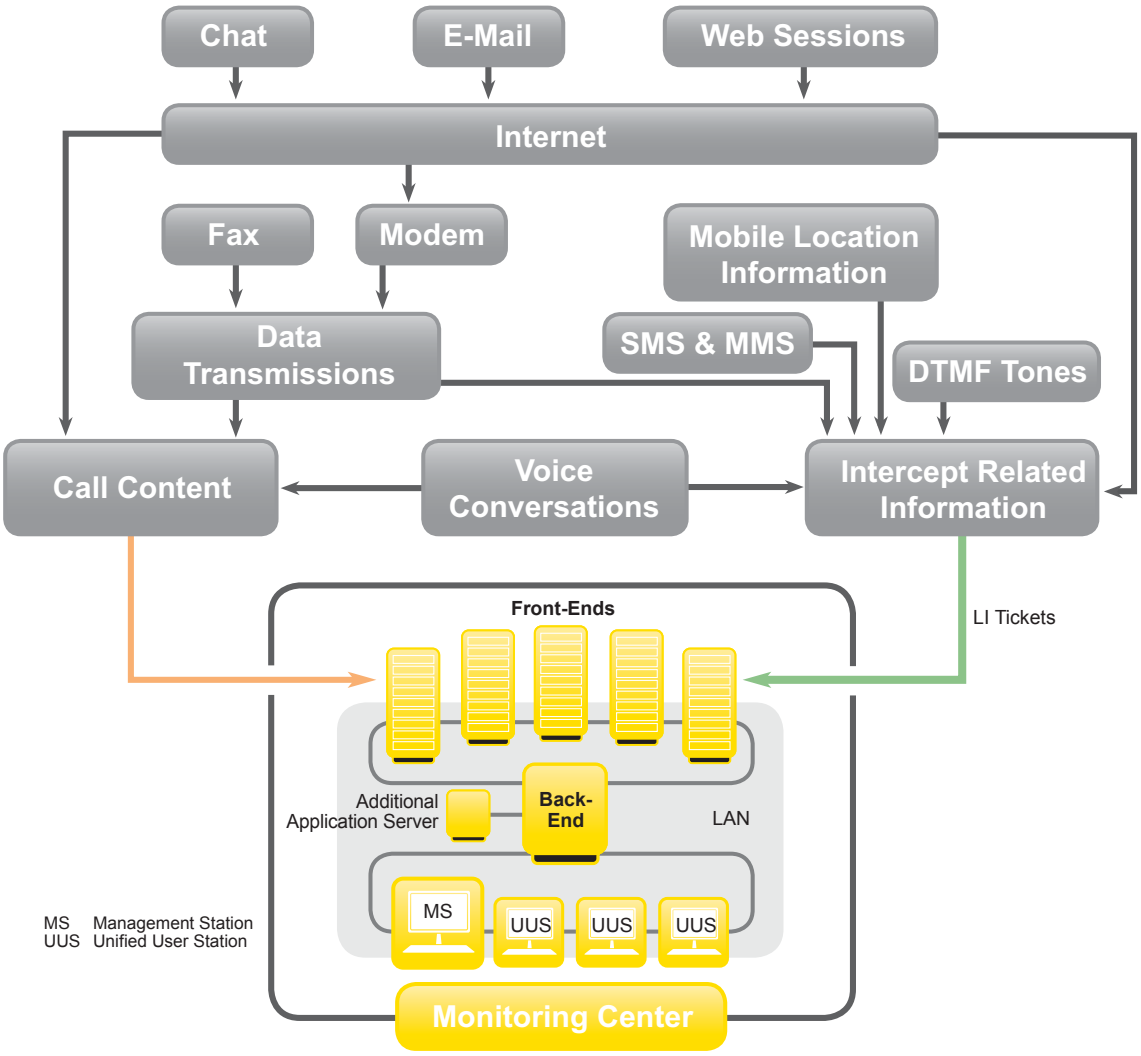
Thus, the system can be modified or expanded at all times on the basis of the existing hardware and/or software. For you, the LEA, this means you only need to invest in the elements you actually need, resulting in a customized solution that satisfies all your requirements at all times.

Deployed throughout the world, our Monitoring Center is everything a law enforcement agency needs for efficient monitoring and prompt evaluation of all types of telecommunication, today and tomorrow.

A perfect match, meeting all requirements.

The **Nokia Siemens Networks Monitoring Center** – assists LEAs in their investigative work by

- monitoring of all types of voice, fax and data communication in fixed and mobile public networks, the NGN and on the internet
- problem-free interaction with lawful interception solutions in heterogeneous network infrastructures
- extensive process automation (decoding, processing, assignment and storage of intercepted data)
- various recording modes (mono, stereo, full duplex, high speed) and voice compression
- automatic recognition of fax and modem data during call recording
- optimized on-screen presentation of data
- user-friendly features for timely data analysis
- add-ons (e.g. geographic information system, link analysis) for efficient ways to pursue leads



The Nokia Siemens Networks Monitoring Center

Process-optimized

As a primary function, the wide range of automated processes supports and facilitates the investigator's work. This begins with the incoming information. The various Front-Ends first decode the data received from the networks – widely varying in terms of both type and volume – and convert it into a uniform system-internal format. Subsequently, the processed data is forwarded to the Back-End.

The Back-End, where the incoming content and IRI are combined and automatically assigned to the corresponding interception case and stored in folders, offers a Windows-based user interface which is made up of two components.

The benefit is an immediate access to call content – even if IRIs are delayed. And this happens quite often.

The Management Station (MS) enables the system administrator to adapt the configuration of our Monitoring Center to the LEA's changing requirements at all times.

The Unified User Station (UUS) is a versatile part that assists the LEA in performing day-to-day monitoring tasks. It provides the LEAs with all recordings and other information from the network in an optimized form with the click of the mouse-button. The LEA can quickly and easily retrieve the LI information sent from the network from the folder in which it is stored. Thanks to system-internal fax and data demodulation/ decoding, the recorded signals are displayed as readable documents on the screen (e.g. as a fax page or a web page).

User-friendly

Regardless of whether the LEA is monitoring phone calls, reading the content of a fax or SMS, or for instance evaluating an internet chat session, it always controls the individual processes on the user interface in the same intuitive manner, irrespectively of any system expansions.

Our Monitoring Center offers different operating modes for receiving and recording data intercepted in the network; some of these are automatically controlled, some manually configured, according to requirements.

This greatly simplifies the investigator's work and allows a more efficient deployment of system resources.

The system automatically detects if a fax or data transmission begins during the recording of a telephone conversation. It then accordingly switches to the 'high quality' or 'high speed' recording mode. This subsequently guarantees a successful demodulation of the digital signals during transmissions which use the entire bandwidth.

Various levels of compression available to economize on storage space when recording voice calls two modes available when setting up monitoring in IMS

- stereo (advantage: both conversation directions can subsequently be interpreted separately or together)
- mono (saves online capacity)

Bringing the LEA closer to its target…

The UUS (Unified User Station) of our Monitoring Center supports the LEA with a Windows-based user-friendly interface for data evaluation, for example in wiretapping.

Innovative

A significant number of add-ons are available to complete the scope of the Nokia Siemens Networks Monitoring Center.

Offering efficient means of pursuing leads, these are all most valuable to investigative work.

One example is location tracking by means of the Geographic Information System (GIS):

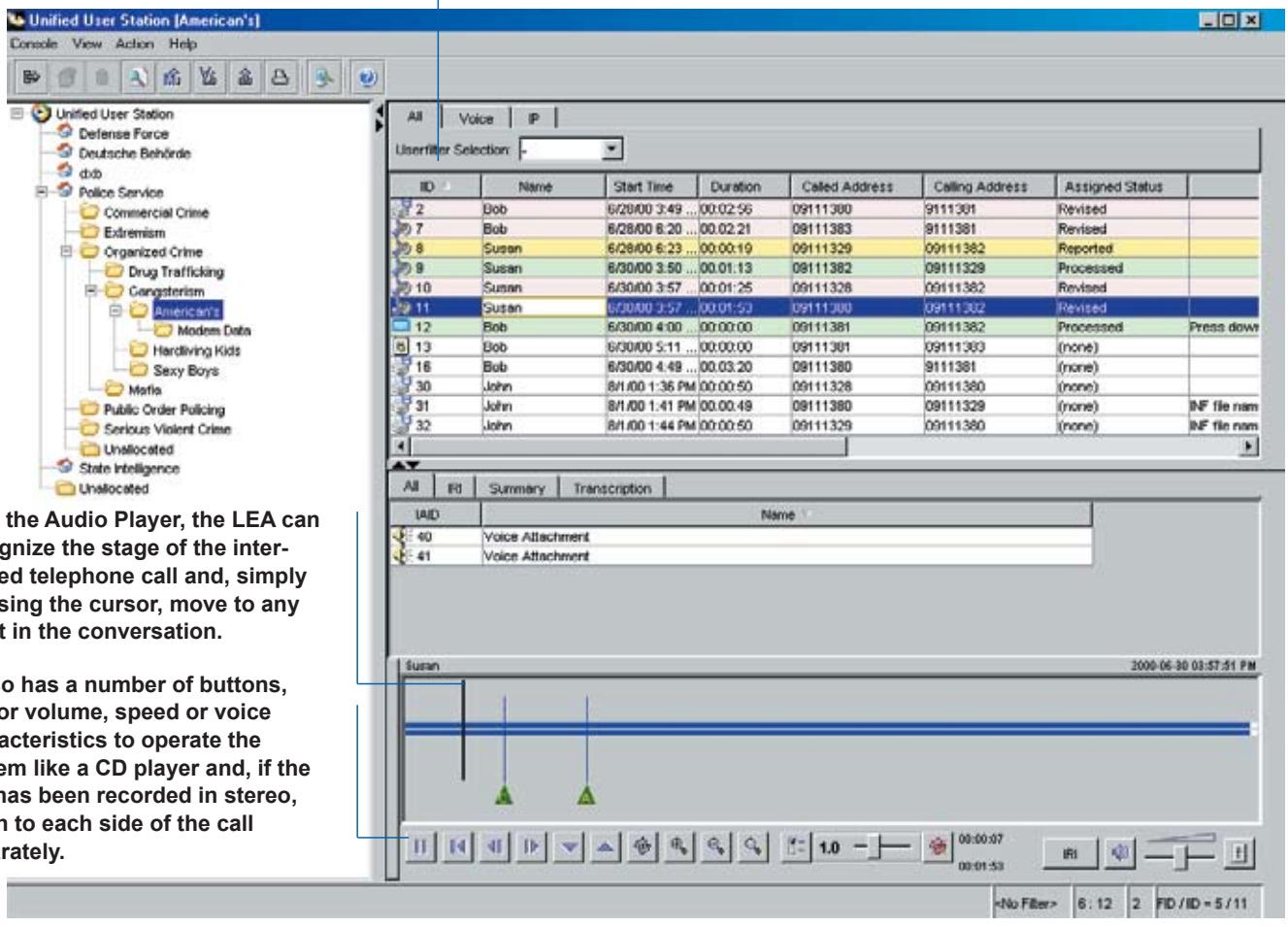
Within mobile telephone networks, this feature determines the current location of the marked mobile device (with variable accuracy within and between networks).

The obtained information is transmitted to the Nokia Siemens Networks Monitoring Center (in the form of IRI).

There it is visualized on a map on which the user's (or at least the phone's) current movements and route can be tracked live – as long as the corresponding data continues to flow.

System users have a number of different map views and layers to select from.

Powerful filters help the LEA to quickly identify the important conversation.



With the Audio Player, the LEA can recognize the stage of the intercepted telephone call and, simply by using the cursor, move to any point in the conversation.

It also has a number of buttons, e.g.for volume, speed or voice characteristics to operate the system like a CD player and, if the call has been recorded in stereo, listen to each side of the call separately.

Nokia Siemens Networks Monitoring Center

Reliable

When it comes to data and system protection, the Nokia Siemens Networks Monitoring Center is again an excellent choice, and one that also meets the customer's special needs.

Through its modular, multilevel security and control concept for authorities, administrators, groups of LEAs and individual LEAs, it can be adapted to meet the requirements of individual organizational structures and different legal requirements.

Unauthorized system access is prevented by means of a series of protective mechanisms involving individual passwords coupled with user-specific rights.

Special precautions have been taken to ensure that the case-specific folders, which store all the data intercepted in the course of monitoring, cannot be confused or mixed up under any circumstances.

An entire range of special system-internal measures protect the recorded data from manipulation, theft or destruction. If necessary, all of these mechanisms may be reinforced (e.g. against hacking or other internet threats) by firewalls, VPNs or virus/intrusion protection tools.

System components can also be duplicated to guarantee system availability and prevent the loss of any saved data. And in order to prevent data getting lost in the case of a power outage during monitoring, the Nokia Siemens Networks Monitoring Center can also be equipped with its own uninterruptible power supply system.

Our Services
rounding off the product

Worldwide

Service components prior to and during project implementation

- recommendations for optimizing system capacities
- project management
- system and network integration
- training for system users
- technical workshops
- tailored financing solutions and leasing arrangements

Service components after project implementation

- system support
- system maintenance
- hardware and software upgrades
- advice and system optimization

Individual

And then there are special services ...

... for the network operator

- comprehensive advice in meeting the legal requirements when planning LI solutions for new NGN and IP networks
- assumption of all the tasks involved in the case of judicially authorized interception (i.e. outsourcing the LI operator, administrator and supervisor functions to suitably qualified Nokia Siemens Networks experts)

... and for the law enforcement agency

- in-depth analysis of the monitoring possibilities (including traffic analyses)
- basic training in the field of lawful interception in IP networks

Nokia Siemens Networks offers a wide range of monitoring services for supporting both network operators and law enforcement agencies.

As part of the Nokia Siemens Networks ‘Lawful Interception and Monitoring concept’, these services team up with the LI-, IMS- or MC-features and produce a comprehensive solution that meets all needs of network operators and LEAs.

The components of LI and Monitoring at a glance

At the network end ...

IMS
An ETSI-compliant management system implemented in a client/server architecture as a vendor-independent solution, also used for the mediation and distribution of IRI. It provides centralized control and administration of lawful interception in public fixed and mobile networks, as well as in NGN and the internet

LI 1 – for monitoring all forms of telecommunication in public fixed networks
A solution based on standard network elements used to automatically duplicate/generate all data (call content and IRI) from any activity on a target and forward this to up to five LEAs.

LI 2 – for monitoring all forms of telecommunication in mobile networks
A solution based on standard network elements used to automatically duplicate/generate all data (call content and IRI) from any activity on a target and forward this to up to five LEAs.

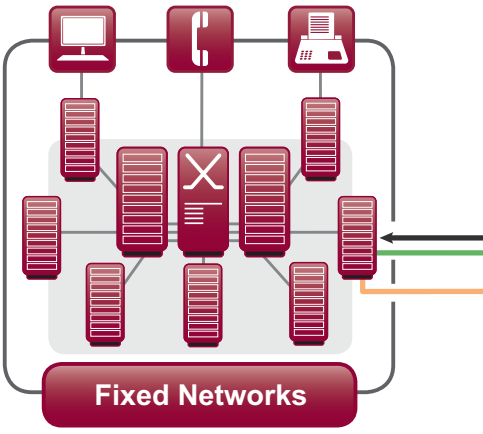
LI 3 – for monitoring number-based traffic in Next Generation Networks (NGN)
A solution based on standard network elements (softswitch and LI server), used in an NGN (IP core network with integrated TDM networks) to automatically duplicate/generate all data (call content and IRI) from any activity on a target and forward this to up to five LEAs.

LI 4 – for internet surveillance
A solution based on integrated LI functionality in IP components or on special equipment (powerful data collectors) used to duplicate and filter the flow of data to access points around the access provider, the service provider or the backbone. There are a number of different data collectors and, upon request, these are also available in combination with individually configured mediation devices (for interface adaptation and data distribution).

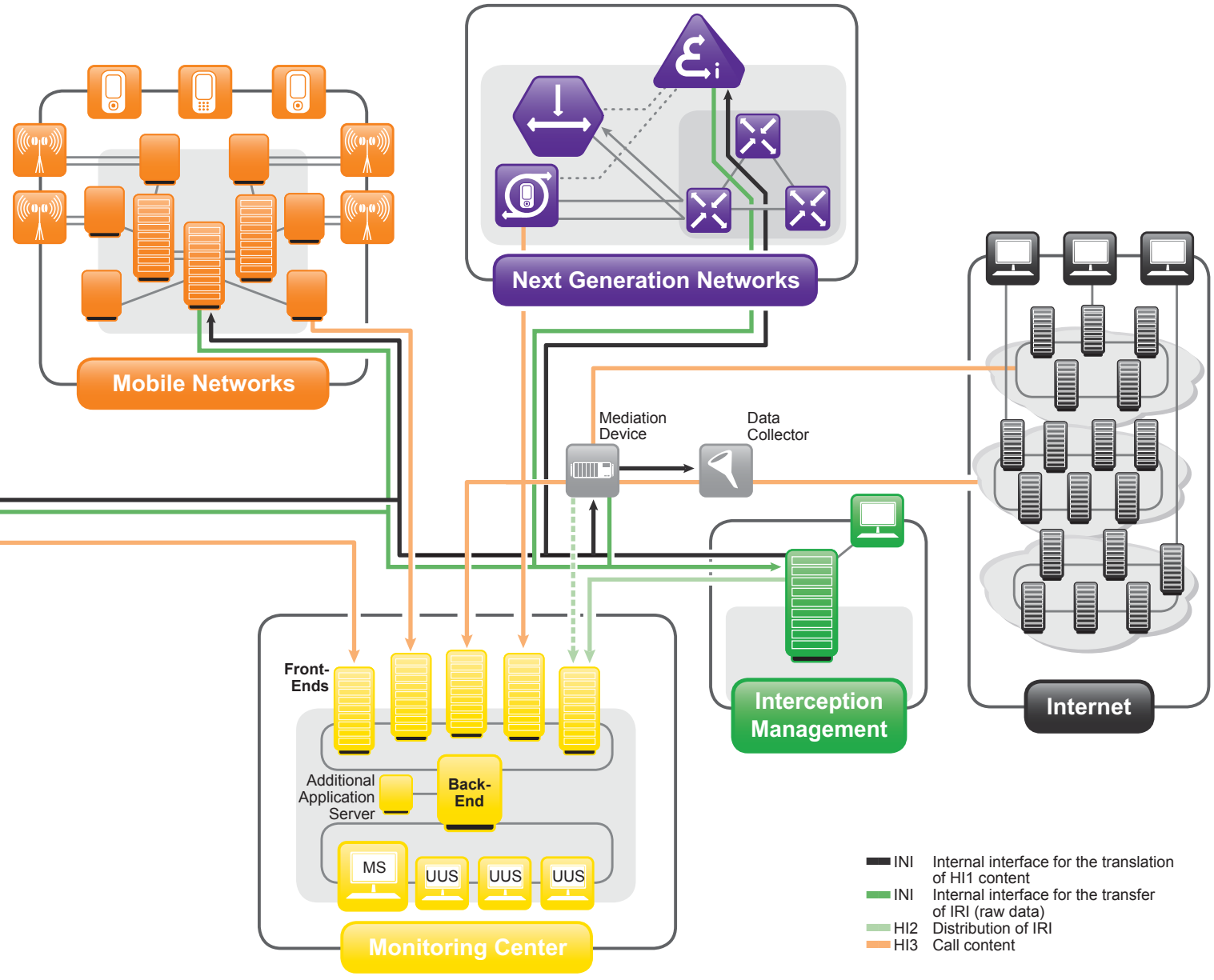
On the LEA side…

For receiving, processing and evaluating all types of voice, fax and data traffic from all fixed and mobile public networks, from Next Generation Networks and the internet.

Our Monitoring Center is a modular, vendor-independent and ETSI-compliant system, configured as standard to receive the call-content and intercept related information (IRI) separately.



The ‘Lawful Interception and Monitoring UUS concept’ offer solutions that meet the needs of both network operators and LEAs.



Our customers' benefits – at a glance

- individual, ETSI-compliant solutions, scalable in size and capacity for all network and LEA requirements
- secure, discreet, verifiable, cost- and space-saving performance of LI in all networks
- complete spectrum of possible targets
- immediate access to call content – even if IRIs are delayed
- nationwide monitoring
- fully automatic recording/generation and processing of all data from all activities of the target
- high level of system and data security
- great flexibility in the administration of LI instances (independent of location and organization)
- simple and fast data processing/evaluation through a maximum of process automation and user-friendly, practical functionality
- efficient ways to pursue leads

Our strengths – our customers' gain

Nokia Siemens Networks is a leading global enabler of communications services. The company provides a complete, well-balanced product portfolio of mobile and fixed network infrastructure solutions and addresses the growing demand for services. It is one of the world's largest telecommunications infrastructure companies and has operations in some 150 countries. Its headquarter is in Espoo, Finland. The merger has combined Nokia's former Networks Business Group and the former carrier related businesses of Siemens Communications.

The excellent quality of our end-to-end solutions is founded on our particular strengths:

IP convergence
Our convergence solutions open up an enitirely new world of IP services and solutions to our customers – with the same proven level of security and reliability as our voice communication. Futureproof migration strategies guarantee the best possible protection of your investments.

Broadband access
What is the use of the fastest network without high-speed access? Our broadband access products facilitate every kind of high-speed access to the widest range of services.

Optical networking
Offering almost unlimited bandwidth and continually breaking records in transmission speed, Nokia Siemens Networks optical networks lay the foundations for the data superhighways of the future.

Partners for profitable networks
Our customers' profitability is always our highest priority. Our products and services open up new business opportunities for them and help them optimize processes. We integrate their existing systems to protect their investments. Our solutions make communication more cost-effective and contribute to a faster return on investment.

Abbreviations

3G	3rd Generation Mobile Networks
CUG	Closed User Group
DTMF	Dual Tone Multi Frequency
ETSI	European Telecommunication Standards Institute
FDN	Foreign Directory Number
GSM	Global System for Mobile Communication
GPRS	General Packet Radio Service
GUI	Graphical User Interface
HI	Handover Interface according to ETSI
HI1	HI for manual or electronic transfer of lawful interception orders
HI2	HI Intercept Related Information (LI tickets)
HI3	HI Content of Communcation (Call content)
https	Hypertext Transfer Protocol, Secure
IMS	Interception Management System
INI	Internal Interface according to ETSI
IP	Internet Protocol
IPsec	Internet Protocol Security
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISDN-BA	ISDN Basic Access
ISDN-PA	ISDN Primary Rate Access
LAN	Local Area Network
LEA	Law Enforcement Agency
LI	Lawful Interception
LTG	Line Trunk Group
MMS	Multimedia Messaging Service
MS	Management Station
MSC	Mobile Switch Controller
MSN	Multiple Subscriber Number
NGN	Next Generation Networks
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
SMS	Short Message Service
TDM	Time Division Multiplex
UUS	Unified User Station
VPN	Virtual Private Network
WAN	Wide Area Network
WWW	World Wide Web
X.25	Data network protocol

Nokia Siemens Networks GmbH & Co. KG
Intelligence Solutions
DE-81359 Munich
Germany

Visiting address:
Hofmannstr. 51, Munich, Germany
Switchboard +49 89 722 00

Order No. C40100033B2007091EN

IS-sales.nsn@nsn.com
www.nokiasiemensnetworks.com

Intelligence Solutions
Monitoring Center

Nokia Siemens Networks

Keep your eyes open

Intelligence Solutions
Monitoring Center

The Third Millennium began with a world of open borders and easy trafficking, a global village where any major destination can be reached within 24 hours.

Never before could information be exchanged so rapidly and in so many ways.

Needless to say that criminal groups and terrorist organizations also have been quick to realize the vast opportunities presented by modern communications.

When it comes to fighting crime and thwarting terrorist attacks, law enforcement and government security agencies need the right tools to get results and fulfill their mandate. Therefore, state-of-the-art monitoring center solutions are an absolute 'must' for lawful interception (LI). By monitoring the communications of specific groups or individuals, law enforcement agencies (LEAs) can discover hidden patterns and criminal structures, anticipate and prevent crimes, and collect hard and fast evidence for prosecution.

The Nokia Siemens Networks Monitoring Center (MC) has been specifically developed to service the complex needs of law enforcement agencies worldwide. It is completely user-friendly in that it offers a unified view of all intercepted data, regardless of their source. No matter what kind of data or from whichever sort of network, the Monitoring Center presents them in a standardized way because its unique architecture can concurrently handle all technologies and vendors. It is both, flexible and scalable and performs the tasks of monitoring in an auditable, secure, reliable and verifiable manner, according to ETSI LI standards.

The Nokia Siemens Networks Monitoring Center is deployed all over the world. So far more than 90 Monitoring Center solutions have been installed in over 60 countries.

The Monitoring Center is the perfect match for LEAs' needs for efficient monitoring and prompt evaluation of all types of communication – today, tomorrow and after tomorrow.

Intelligence Solutions
Keep your eyes open

The Nokia Siemens Networks Monitoring Center can be used for intercepting communications in public fixed and mobile circuit-switched networks, Next Generation Networks (NGN) and the internet.

It has been designed for integration within every telecommunications network – with any type of modern standardized switch following the ETSI recommendation (e.g. Nokia Siemens Networks, Ericsson, Alcatel, Nortel, Lucent, Motorola, Huawei). Customers vastly benefit from this multi-vendor capability as it allows easy interaction with lawful interception solutions in heterogeneous network infrastructures.

The Monitoring Center monitors two general types of intercept: Voice and data.

However, within those two types it manages the following more specific types

- internet sessions (e.g. web sessions, e-mail, chat, VoIP)
- voice conversations
- fax transmissions
- location-based information for mobile networks (location-tracking, GIS)
- SMS and MMS messages
- modem transmissions including local loop internet
- call related information
- DTMF in-band transmissions

The Monitoring Center supports interceptions from the following sources

- fixed networks PSTN
- mobile networks GSM, CDMA, GPRS, UMTS
- Next Generation Networks (NGN)
- IP Networks: Local loop, ISP, and the internet
- trunk monitoring (passive interception)
- satellite monitoring (passive interception)
- surveillance equipment

The Monitoring Center is an extremely versatile construction of interoperating software and hardware modules. It performs all LI-related tasks on the intercepted information – storage and interpretation as well as a wide range of administrative tasks – in a secure, auditable, reliable and verifiable manner. Because of its LI-conceived modular architecture, it is flexible enough to be configured as an IP interception and delivery solution to other law enforcement monitoring facilities (LEMFs).

Intelligence Solutions
Lawful Interception

The Nokia Siemens Networks Monitoring Center offers different operating modes to receive and record the intercepted data, some of which are automatically controlled and some manually configured, according to the customer's requirements and operational needs.

The operating modes greatly simplify the investigative work of LEAs and allow them to deploy more efficiently Monitoring Center system resources

- to discover hidden patterns and unlawful activities
- to anticipate and prevent crimes
- to take action and provide evidence for prosecution – and –
- to secure peace and prosperity among law-abiding citizens

Service and target monitoring are two different types of lawful interception. They may differ in scale and intent, but they both use granular triggering and filtering to fulfill their ultimate purpose.

Service monitoring

- is pro-active, even in the worldwide web
- controls the entire communications spectrum of possible targets (e.g. suspected pedophile chat rooms and websites)
- checks either each single segment of intercept or those clearly defined
- trawls in both clear and dirty water, looks for potentially unlawful activities
- generates suspects who eventually become the object of target monitoring
- defines and refines new strategic or tactical approaches
- typically requires huge data storage but smaller archiving space
- is usually used by secret services

In contrast, target monitoring may be a result of service monitoring, but it is also an independent investigative method to be used by authorized groups.

Target monitoring

- is re-active
- checks on a particular person or defined groups
- collects specific data
- controls all activities of a defined target
- will possibly be used in a judicial process
- needs typically lesser data storage but larger archiving space
- is usually used by LEAs and police forces for collecting evidence on specific persons or groups

The Nokia Siemens Networks Monitoring Center has been designed to perform both service and target monitoring, according to the customer's needs and requirements with characteristic intercept features like

- detailed trigger mechanisms allowing the interception of the "needle in the haystack"
- fine filters permitting investigators to discern the important data
- hot monitoring warning investigators on the targets' activities, allowing near real-time listening, viewing and/or reading of the communication
- live monitoring for forwarding intercepted calls to agents in the field
- single unified view of all interception types presented to the user

The Monitoring Center's unified view for all intercepts greatly facilitates the tasks of LEAs. If need be, different national and international agencies may grant each other access rights and easily exchange crucial information. Consequently, the concept of agencies cooperating across institutional or national boundaries becomes reality.

The Monitoring Center – one solution for all networks, vendors and technologies meets the monitoring requirements of LEAs worldwide.

Highlights

- monitoring of all types of voice, fax and data communication in fixed as well as mobile public networks and the internet
- smooth interaction with lawful interception solutions in heterogeneous network infrastructures
- extensive process automation (decoding, processing, assignment and storage of intercepted data)
- various recording modes (mono, stereo, full duplex, high speed) and voice compression
- automatic recognition of fax and modem data during call recording
- optimized on-screen presentation of data
- user-friendly features for timely data analysis
- multi-language interfaces
- add-ons for completely new and efficient ways to pursue leads

Benefits

The Architecture
The Nokia Siemens Networks Monitoring Center architecture of Front-End and Back-End parts results from the necessity to interface with a wide range of networks and technologies. This design is the core essence of its success.

Front-Ends
The Front-End components are specific for the target network such as mobile networks or the internet. Multiple Front-Ends are used to connect to different switch manufacturers' interfaces and to appropriately scale to the size of the networks. The data vary widely in terms of type and volume and need to be converted into a uniform system-internal format. Consequently, all voice and other data received from networks are transformed into a single internal format and passed on to the Back-End.

Back-End
The Back-End receives the processed data from the Front-End components, correlates content and Intercept Related Information (IRI) and automatically assigns it to the corresponding folders as configured in the system. The Back-End offers a Windows-based user interface made up of two components:

The Management Station (MS)
The MS enables the system administrator to adapt the configuration of the Monitoring Center to the LEAs' changing requirements at anytime, and to perform routine administrative tasks such as adding new users or folders to the system.

The Unified User Station (UUS)
The UUS provides the LEA-user with all recordings and other information from the network in an optimized form. Thus, the user can easily and quickly retrieve the relevant LI information from the respective folders. System-internal fax and data demodulation and decoding allow the recorded signals to be displayed as readable documents on the screen (e.g. fax, SMS, web pages). Powerful filters help the LEA to quickly locate, listen to and replay relevant phone conversations.

The Nokia Siemens Networks Monitoring Center can never be outdated.

On-demand upgrades
The world of communications is ever-changing: New technologies and ways of communication are constantly invented, Next Generation Networks infrastructures established, higher data volumes need to be handled and multiple types of communications monitored.

Requirements may change – our Monitoring Center will remain the perfect match. Despite the complexity, its modular design of Front-End and Back-End components guarantee extreme flexibility. The individual Front-Ends, which supply the interfaces to the different networks, can easily be adapted to match new requirements. But either can be modified, expanded or replaced as necessary, at any time. Yet the management and presentation essentially remain the same. This has many benefits for the user: The system does not need to be expanded more than necessary. This means that there are no 'fork-lift' upgrades – no total software or hardware replacements. Customers only have to invest in those modules they actually need. The result is a tailored solution that satisfies their requirements at all times.

Scalable
Depending on the applications, the system installations can vary in size - from a few computers to an extensive system of many recorders, data collectors, system servers and clients. The complexity ranges from passive connection to a single trunk line that is responsible for monitoring an entire nation's fixed, mobile, NGN and internet networks.

Distributable
The Nokia Siemens Networks MC performs its monitoring and management tasks from a scalable, distributable and reliable platform (LAN, WAN, MAN) with facilities which ensure the safety of system and intercepted data.

Reliable
Intercepted data is valuable. Customers need to be able to rely on the Monitoring Center solution, which must protect the system sufficiently so that neither manipulation nor theft or even power outage can corrupt the data (e.g. server protection, UPS concepts, RAID strategy, etc.). In addition, the Monitoring Center offers mass storage and archiving solutions (e.g. NAS, SAN). Various levels of compression are available to economize on storage space, if needed.

The Nokia Siemens Networks Monitoring Center is extremely flexible

- it can be integrated into any existing infrastructure and is applicable to a vast range of monitoring tasks, whether fixed, mobile or internet
- it can be configured as an IP interception and delivery solution for other LEMFs
- it is – on-demand and without compromises – scalable and adaptable to the size of the organization

The Monitoring Center's secure environment comprises

- network security
- physical security
- logical security
- link security
- data and capability access security

The Monitoring Center has a modular, multilevel security and control-concept for authorities, administrators and LEAs. This can be adapted to meet the requirements of individual organizational structures and different legal requirements.

Special precautions have been taken to ensure that, under any circumstances, the intercepted data cannot be, confused or mixed up.

A range of special system internal and external measures (firewalls, VPNs, virus/intrusion protection tools, etc.) safeguard the recorded data against manipulation, theft or destruction. System components can also be duplicated to guarantee system availability and prevent the loss of stored data. Using an appropriately specified uninterruptible power supply (UPS) concept, the Monitoring Center has been designed to survive power outages.

The Nokia Siemens Monitoring Center is extremely secure and reliable because of its

- multiple, granular levels
- holistic security-concept
- flexible configuration
- sophisticated user-rights and access control mechanisms

Database
Its database allows for add-on applications. These can either be provided by Nokia Siemens Networks or the customer himself integrates the data in the infrastructure by means of defined interfaces.

Nokia Siemens Networks constantly seeks to augment the service-scope of the Monitoring Center, not only by addressing emerging communications trends but also by making further use of information which is already at hand and by providing additional intelligence. Hence a wide range of add-on applications is available, such as:

Mobile Location Tracking (MLT)
Based on a Geographical Information System (GIS), the MLT is an ideal solution to track, record, extrapolate, and anticipate the movements of mobile devices. Within mobile networks, the current location of marked mobile devices can be determined. The intercept related information (IRI) is transmitted to the Monitoring Center. There, the so-called footprints of the mobile device are visualized on a map on which the user's (or rather the device's) current movements and route can be tracked.

Link analysis
Link analysis may be used to find and graphically display correlating data of intercepted targets. This kind of information, which cannot be achieved manually, reveals previously unknown relationships between targets.

Plaese have a look at our application notes.

Ahead through innovation

The features of our Monitoring Center – at a glance

- universal monitoring center concept for all monitoring requirements within all telecommunication networks:
  - fixed networks PSTN (local and international exchanges)
  - mobile networks GSM, CDMA, GPRS, 3G (UMTS/W-CDMA)
  - Next Generation Networks (NGN)
  - IP Networks (local loop, access network, ISP and internet backbone)
- automatic correlation of communication content to IRI
- mono and stereo voice recording, optionally compressed
- full duplex/no compression recording for data demodulation (fax, internet, e-mails, etc.)
- customized add-on applications
- centralized or decentralized Monitoring Center
- transportable Monitoring Center (‘MC to go’)
- scalable and adaptable to customer requirements
- joint roadmap for upcoming telecommunications technology and Monitoring Center

By forming strategic alliances with other companies in highly specialized technological areas (e.g. data demodulation, speaker recognition, language identification, etc.), Nokia Siemens Networks follows a best-in-class principle and involves specialized partners to maintain its Monitoring Center solutions at the leading edge.

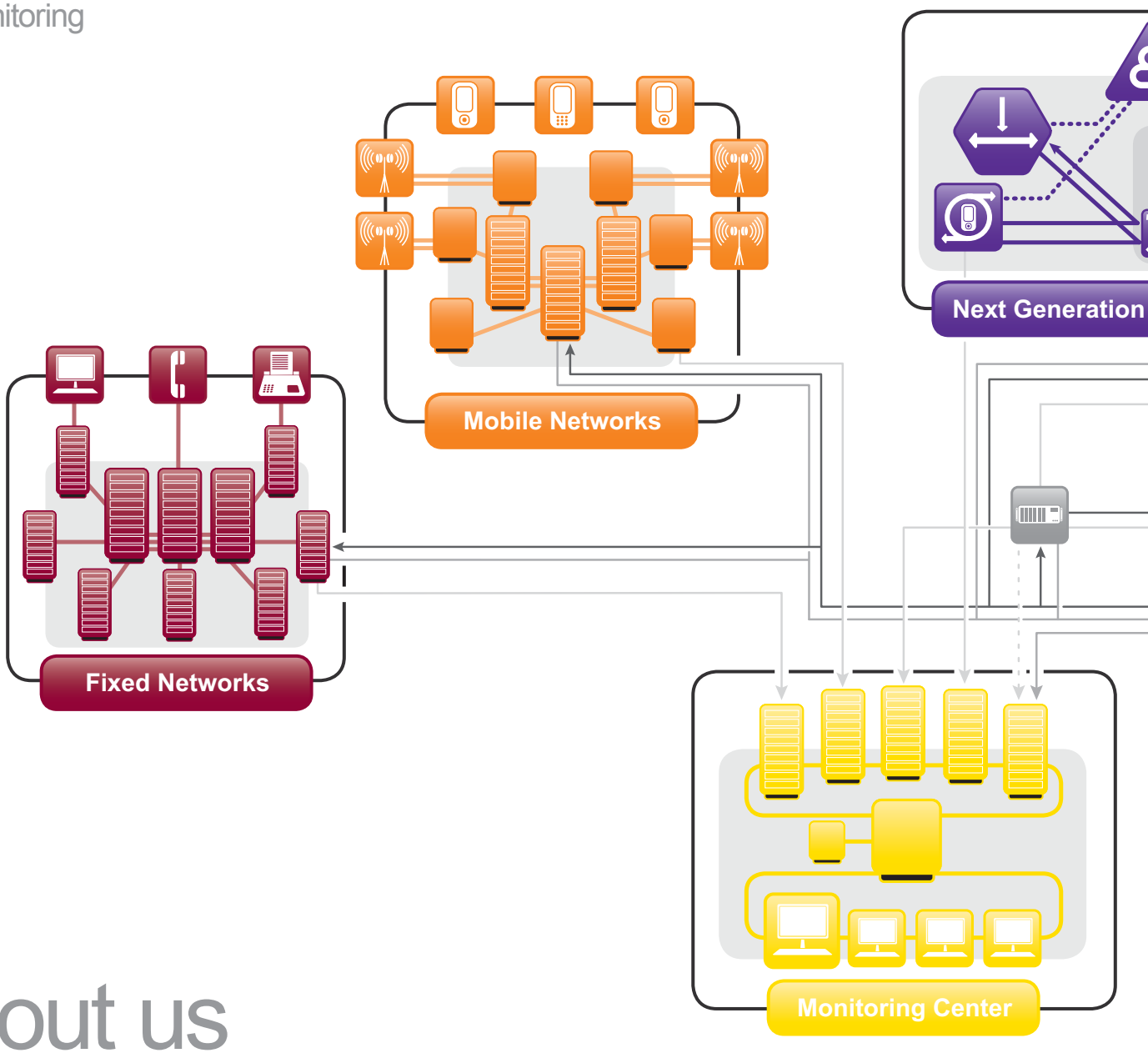
Nokia Siemens Networks has set standards around the world and across all technologies. In the context of this creative climate new ideas can grow, which allow us to remain at the forefront of developing innovative solutions like

- pre-ETSI LI IP
- country and vendor-specific ETSI standard adaptations
- IPIS (internet protocol interception system)
- LI-solutions for IP core routers
- generic systems designed for tailoring
- the transportable Monitoring Center – ‘MC to go’

Highlights

- tailored, ETSI compliant solutions, scalable in size and capacity, designed to address all network and LEA requirements
- optional configurable for other legal arrangements or country specific variations on ETSI
- secure, discreet, verifiable, cost- and space-saving performance of LI in all networks
- complete spectrum of interceptable network infrastructures
- nationwide monitoring possible
- fully automatic recording and processing of all data concerning all activities of the target
- high level of system and data security
- great flexibility: independent of location and organization
- simple, fast data processing and evaluation because of a maximum of process automation and user-friendly, practical functionality

Lawful Interception and Monitoring



About us

The Nokia Siemens Networks Monitoring Center is a well-founded choice and safe investment in a secure future. It represents the clear decision for a strong and stable company combining innovative power and strength to the advantage of all our customers. i.e. network operators, LEAs and government agencies.

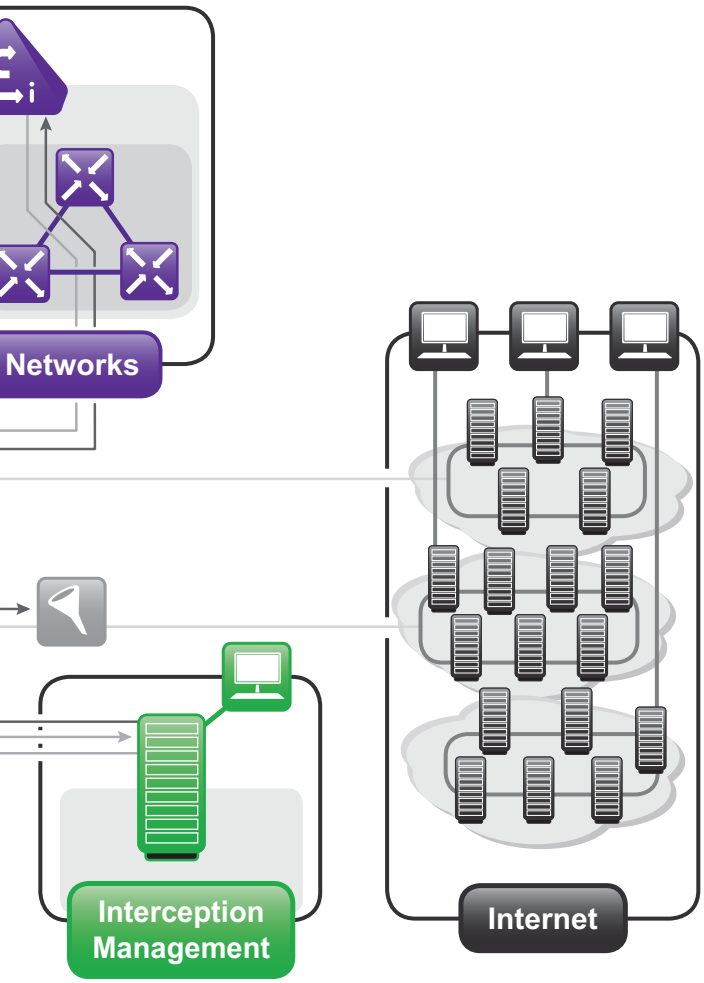
These benefit from a global service network and distribution system which include customized monitoring services and after-sales-support depending on their operational needs and demands.

Examples are

- consultation, network questionnaires and technical workshops
- all-round assistance in meeting legal requirements when planning LI solutions for new IP networks
- tailored financing solutions and leasing arrangements
- project management
- system and network integration
- training of system users
- system support
- system and capacity optimization
- system maintenance, hard- and software upgrades

The Nokia Siemens Networks business unit 'Intelligence Solutions' (IS) has a unique best-in-class experience with lawful interception and government agency requirements based on experience from numerous projects within its Monitoring Center product line. Deep understanding of security issues – inside military organizations, MOI, and other security services – as well as a broad security awareness contribute to IS' excellent relationships, which are based on trust, reliability and stability – result in long term, thoroughly satisfied customers.

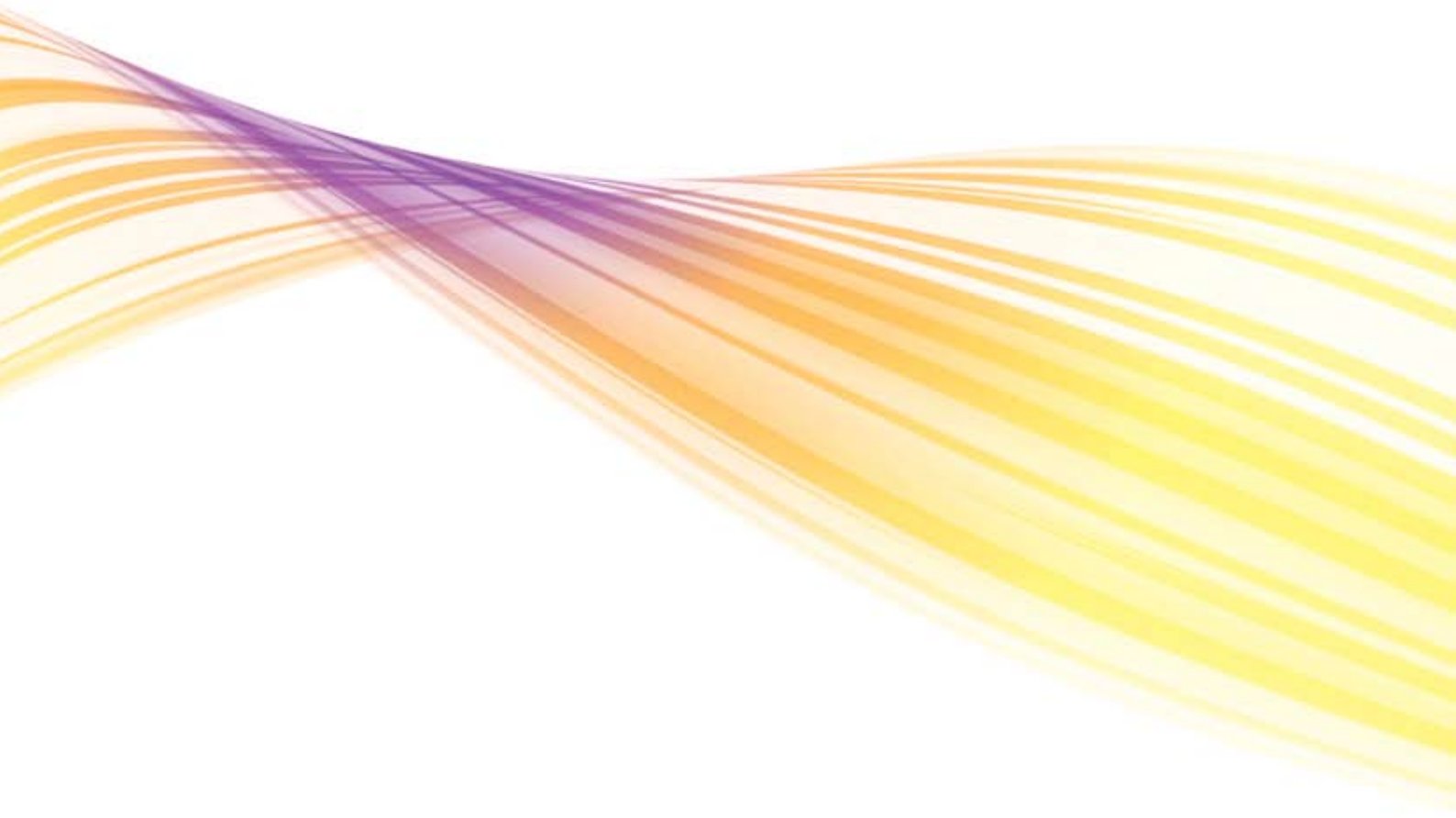
Making the world safer with trend-setting intelligence solutions



Nokia Siemens Networks is one of the world's largest network communications companies – with 60,000 employees and a leading position in all key markets across the world. And, it is one of the three largest telecom suppliers in the world, with a growing customer base in over 160 countries across five continents. With 2006 pro forma revenues of €17 billion, the Nokia Siemens Networks business base is strong enough to lead the way successfully into the future.

List of Abbreviations

3G	3rd generation mobile networks
CDMA	Mobile network: Code Division Multiple Access
DTMF	Dual Tone Multi Frequency
ETSI	European Telecommunication Standards Institute
GIS	Geographical Information System
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
IP	Internet Protocol
IPIS	Internet Protocol Interception System
IRI	Intercept Related Information
IS	Business Unit Intelligence Solutions within Nokia Siemens Networks
ISP	Internet Service Provider
LAN	Local Area Network
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
MAN	Metropolitan Area Network
MC	Monitoring Center
MLT	Mobile Location Tracking
MMS	Multimedia Messaging Service
MOI	Ministry of the Interior
MS	Management Station
NAS	Network Attached Storage
NGN	Next Generation Network
PSTN	Public Switched Telecommunications Network
RAID	Redundant Array of Inexpensive Disks
SAN	Storage Attached Network
SMS	Short Message Service
UMTS	Universal Mobile Telecommunications System
UPS	Uninterruptible Power Supply
UUS	Unified User Station
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
W-CDMA	Wideband CDMA



Nokia Siemens Networks GmbH & Co. KG
Intelligence Solutions
DE-81359 Munich
Germany

Visiting address:
Hofmannstr. 51, Munich, Germany
Switchboard +49 89 722 00

Order No. C40100031B2007091EN

IS-sales.nsn@nsn.com
www.nokiasiemensnetworks.com

Lawful Interception of Telecommunication Services

Throughout the world telecommunication services providers are required to support law enforcement agencies in their fight against crime and terrorism. Network operators and telecommunication service providers must provide interception capabilities in their network for people under surveillance. The legal framework of lawful interception (LI) is defined by national laws and regulations and is complemented by various international technical standards.
LIMS (Lawful Interception Management System) is a proven solution for network operators and service providers for the management of all LI related activities. The system is based on a central management platform for the surveillance of communication services and represents the interface to all authorized law enforcement agencies and their monitoring centers.
LIMS offers the broadest range of supported network elements, which enables lawful interception in virtually any fixed, mobile and Internet service provider's environment without any negative impact on the performance and reliability of the network. Communication services supported include voice, fax, SMS, MMS, e-mail, voicemail, VoIP, Push-to-Talk, as well as various other Internet services. While the system is designed for large-scale networks with millions of subscribers, the LIMS suite can easily be adapted to provide an economically feasible solution for networks with only a few thousand users. The modular architecture of LIMS facilitates cost-effective extension and adaptation to new technologies and regulatory requirements.
The design concept of LIMS complies with international LI standards of ETSI, 3GPP, ANSI, and PacketCable and satisfies the highest security requirements to protect the privacy of all associated data.
We support providers and carriers seeking lawful interception solutions by offering consulting and technical support services and also provide managed service models, together with qualified solution partners.

Benefits

Compliance
- Surveillance of all common telecommunication services incl. voice, data, fax, SMS, MMS, Push-to-Talk, e-mail, VoIP in fixed, mobile networks
- Complies with regulatory requirements in numerous countries worldwide
- Conforms to international lawful interception standards developed by ETSI, 3GPP, ANSI, PacketCable and others

Cost Efficiency
- Central management of all interception decisions in the network
- Modular architecture that enables cost-efficient solutions for small and very large communication networks
- Simple integration into available networks
- Almost free of maintenance

Reliability

- Complies with highest security demands, tamper-proof
- No negative impact on performance or reliability of the network and services
- Continuous extension by latest technologies and standards
- Close cooperation with regulatory authorities and standardization bodies
- More than 12 years of experience in lawful interception

Key features and Functionality Lawful Interception Standards

- ETSI TS 101 331, ES 201 158, TS 101 671, ES 201 671, TR 102 053, TR 101 943, TR 101 944, TS 102 232, TS 102 233, TS 102 234
- CALEA, ANSI J-STD-025-B, ATIS T1.678
- 3GPP TS 33.106, TS 33.107, TS 33.108
- PacketCable 1.5

Services

- VoIP (SIP, H.323, RTP)
- GSM, GPRS, UMTS
- CDMA, CDMA2000
- SMS, MMS, Voicemail
- Push-to-Talk over Cellular (PoC)
- PSTN (Fixed Telephony)
- Internet Access (IP)
- E-mail (POP3, SMTP, IMAP)
- other IP-based services

Performance

- Maximum number of subscribers: virtually unlimited, scalable configurations from 1,000 to several million subscribers
- Maximum number of interception targets: scalable up to thousands of parallel interception targets
- Filter performance: up to 200 Mbps per interception access point (E-Mail, VoIP)

Vendor Interfaces

- Acme Packet, Alcatel, Cisco, Comverse, Ericsson, Huawei, Iptel.org, Juniper, Lucent, Motorola, Nokia, Nortel, Unisys, Siemens, Sun, WaterCove, and others

Network Interfaces

- 10/100Base-T, 1000Base-T/F, X.25, ISDN, E1/T1, SS7 interfaces

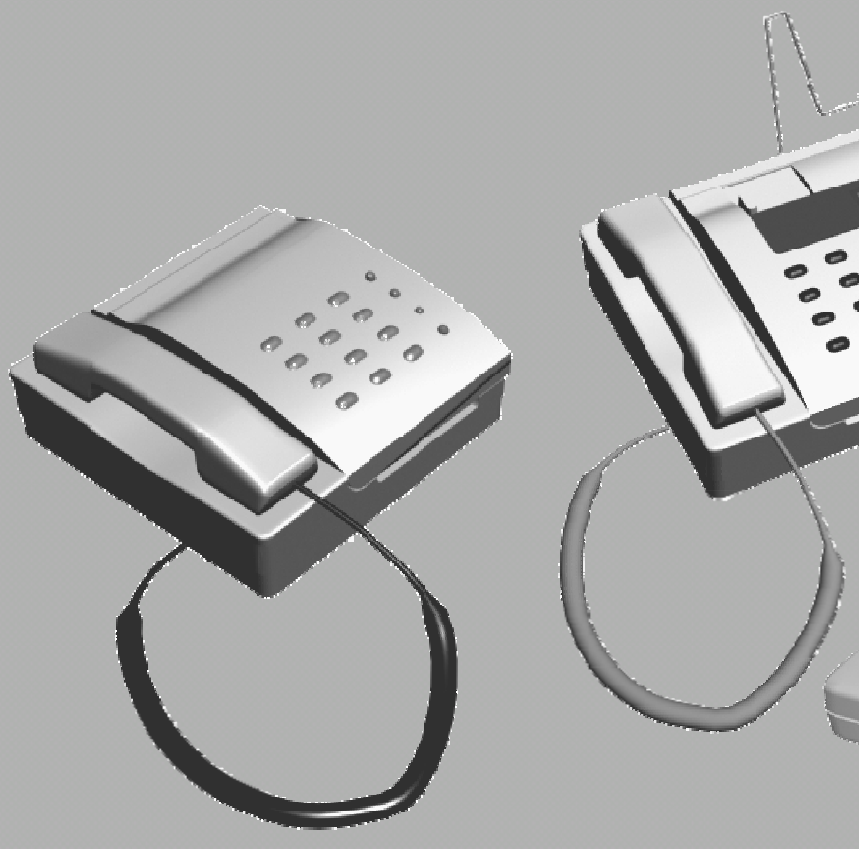
Security

- Role-based Access Control (RBAC)
- Transparent separation of multiple authorities
- Detailed accounting of all system events and user actions
- IPsec/SSL/TLS encryption
- Encrypted storage, backup
- Mirrored hard disks
- System monitor and alarms
- High-availability module (hot-standby)
- Secure remote access

Others

- Integrated billing capabilities
- Easy to use graphical user interface
- Network segregation to enable outsourced business models
- Remote administration of other LI systems
- Various language kits

Passive Telecommunications
Monitoring System



Index

Zebra Optical Gateway

The Zebra optical gateway is designed to connect the Zebra monitoring centre system to SDH/SONET and E3/DS3 telephony networks. It provides a highly dense connectivity solution: 2 bi-directional STM1/OC3 carriers can be intercepted in a single 1U 19" rack module. The unit supports 1 STM4/OC12 input. An expansion module (currently under development) provides connectivity for 12 E3/DS3 inputs. Used in conjunction with the Zebra monitoring centre system, the Zebra gateway provides a very powerful telecommunications monitoring solution.

Unlike general purpose media gateways and protocol converters, the Zebra gateway is designed to support the requirements of communication monitoring. This allows the Zebra monitoring centre system to support features that were not possible with the previous generation of monitoring equipment, for example:

The Zebra gateway and Zebra monitoring centre system can process primary rate carriers containing only SS7 signaling timeslots (e.g.: 31 signaling timeslots on an E-1)

- The Zebra gateway supports any combination of hyper channels (consecutive timeslots used together to provide one bigger n x 64 kbps channel) together with E0/D0 (64 kbps) channels on the same carrier
- The Zebra gateway supports channelized E1/T1, E3/DS3 and STM1/OC3 (unframed streams used as bit streams)
- E1/T1, E0/DS0 channels, hyper channels and channelized carriers can be mixed on the same gateway
- The Zebra optical gateway can be used in conjunction with other Zebra gateways (for example: the Zebra E1/T1 gateway) in the same Zebra monitoring centre system
- The Zebra monitoring centre system reads data from the Zebra gateway over Ethernet, allowing the processing of monitored streams to be farmed out to as many servers on the network as required for the connected capacity. This allows a Zebra system to be scaled up to an unprecedented capacity of over 150 000 monitored channels in a single system

Specifications

Dimensions and weight	The Zebra optical gateway is a 1U 19" rack module 8kg
Capacity	8 SDH inputs provide a capacity of 4 monitored SDH bearers, each with a protection switching input. The system supports automatic switchover to the backup bearer when protection switching is used. All the traffic offered on every connected STM-1 bearer, or one STM-4 bearer can be processed.
Carrier type configuration	4 × STM1/OC3 or 1 × STM4/OC12 On expansion module: 12 × E3/DS3
Channel configuration	Any combination of signaling channels, bearer channels, hyper channels and channelized primary rate, E3/DS3 or STM1/OC3 may be configured.
Input signal strength	0 to – 40dB
Termination and connectivity	SFP connectors offer: Optical connectivity short and long-haul. Electrical connectivity for STM1/OC3. Coaxial 1.6/5.6 connectors support electrical connection of E3/DS3.
LAN	3 × 1 Gbps Ethernet Copper or fibre
AC power input	110V to 240V AC Automatic switching
Redundant power input	110V to 240 VAC Automatic switching
Power consumption	100W
Multiplexing	All standard types of multiplexing are supported, including, E13, M13 and G.747.
VoIP	The Zebra gateway supports the interception of VoIP streams in hyper channels or channelized primary rate or higher multiplexed streams. Protocol processing is on open platforms.
ATM	Interception of ATM carried over E1/T1 is supported. Protocol processing happens on open platforms.

Telephone Line Monitoring Zebra System

The Zebra system is a powerful telecommunications monitoring solution. It combines support for ETSI Lawful Interception with very dense passive monitoring in one hybrid solution. The Zebra system is suitable for law enforcement as well as intelligence gathering and is scalable from 16 E1 carriers (or equivalent channels) to more than 5,000 E1 carriers (or equivalent) in one integrated system.

Glossary

Bearer	Transmission bearer, typically of SDH/SONET optical transmissions. E.g.: STM-1, STM-4, etc bearer. Analogous to carrier (below).
Carrier	Transmission carrier, typically of PDH transmissions. E.g.: E1, DS3, etc carrier. Analogous to bearer (above).
ETSI LI	Lawful interception method standardized by the ETSI. See [1].
FTP	File transfer protocol (TCP/IP). See [1]
Hi-Z	High impedance buffering used to insulate passively monitored carriers from potential noise and signal reflections originating from the monitoring equipment.
ISDN PRI	Primary rate (E1/T1) ISDN. See [1]
LED	Light emitting diode
LI	Common abbreviation of ETSI LI (above).
LIID	Lawful intercept identifier. See [1]
MC	Monitor centre
PBX	Private branch exchange
PLMN	Public land mobile network – GSM, 3G.
Primary rate	2.048 Mbps (E1) or 1.544 Mbps (T1). See ITU-T Recommendation G.703
PSTN	Public switched telephone network – fixed line networks.
WAN	Wide area network

References

[1] ETSI TS 101 671 V2.13.1 (2006-01), Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic.

[2] Telephone Line Monitoring Zebra E1-T1

[3] Telephone Line Monitoring Zebra E1-T1 Gateways

System overview

Figure 1 shows how the Zebra system couples to the carriers of telephony networks. Active FTP and ISDN PRI protocol stacks support the ETSI LI handover interfaces 2 and 3 for circuit and packet switched interceptions. Passive SS7, R2MFC and SS5 protocol stacks support passive monitoring between switches in a carrier network, as well as between the gateway switches. The same passive protocol stacks support interception of satellite streams. A passive ISDN stack supports trunk-side interception of PBX traffic.
The support for these interfaces and protocols allow the Zebra system to be applied to any type of monitoring in the carrier network, including PSTN and PLMN networks.

The Zebra system can capture intercepts in the following modes:
Passively – the system connects passively to carriers or bearers between switches. Hi-Z buffers hide the Zebra system from the monitored network. No additional load is placed on the monitored network. Sessions on the monitored carriers/bearers are detected by protocol analysis or VOX activity. The system can be configured to record all traffic on the monitored carriers/bearers.

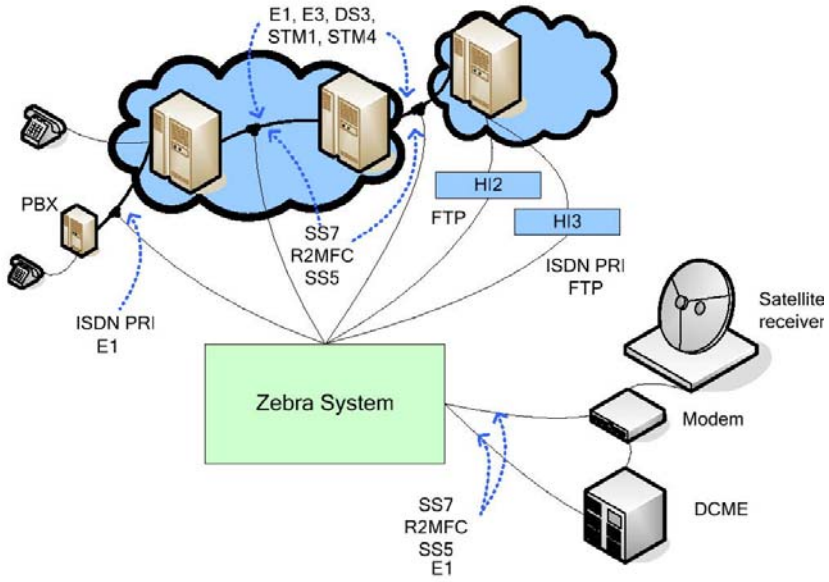


Figure 1. System overview

Actively/LI – The system connects actively to the ETSI Lawful Interception handover interfaces 2 and 3 of one or more switches. A marking terminal is used to mark targets in the monitored network.
The switches of the monitored network select monitored sessions based on the marked targets.

The switches make calls to the Zebra system over ETSI LI HI3 containing the content of the circuit switched monitored sessions and push files containing the content of packet switched monitored sessions to a file server of the Zebra system.
Intercept related information is sent to the Zebra system by switches of the monitored network over ETSI LI HI2.
Passive monitoring is typically used for large scale intelligence gathering while active monitoring/LI is mainly used for law enforcement.
A Zebra system can be configured to support both actively and passively monitored interfaces in one system.

Passive monitoring

The Zebra system is a very powerful passive monitoring system. Figure 2 shows the configuration of a passive Zebra system (coupling to monitored carriers not shown) with the following capabilities:

1. Connect to 384 bi-directional E1 carriers.
2. Record every session on every channel.
3. Store all intercepts for 7 days.
4. Demodulate all fax and internet sessions.

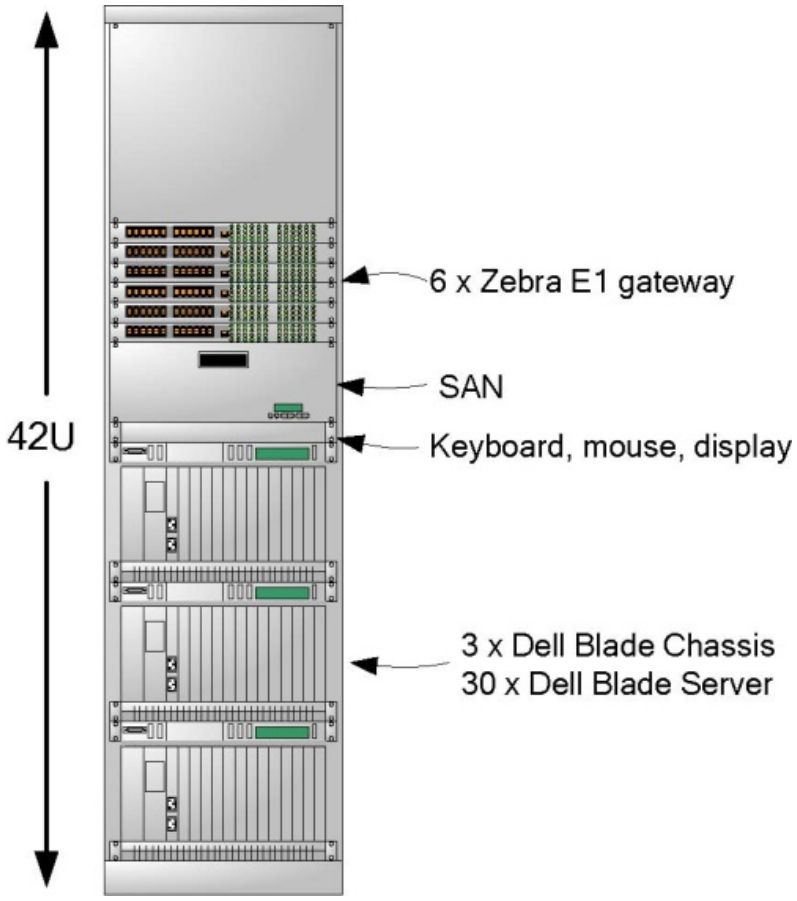


Figure 2. 384 x E1 passive monitoring system

Such a system is capable of monitoring any configuration of protocols on its input carriers, including: SS7 ISUP and TUP, SS5, R2MFC. When no signaling is available recordings can be triggered on VOX. Future versions of the system will support H.323, SIP and other packet protocols.

These protocols are normally transmitted on n × 64 kbps hyper channels, as well as unstructured PDH and SDH/SONET carriers. A system can support a mixture of PDH and SDH/SONET interfaces, e.g.: E1 and STM4.

The philosophy of the Zebra passive monitoring system can be summarized as: store everything, filter for known targets, and search the past for new targets.

Active monitoring

The Zebra system supports ETSI LI handover interfaces 1 and 2 as specified in ETSI TS 101 671 V2.13.1 (2006-01).

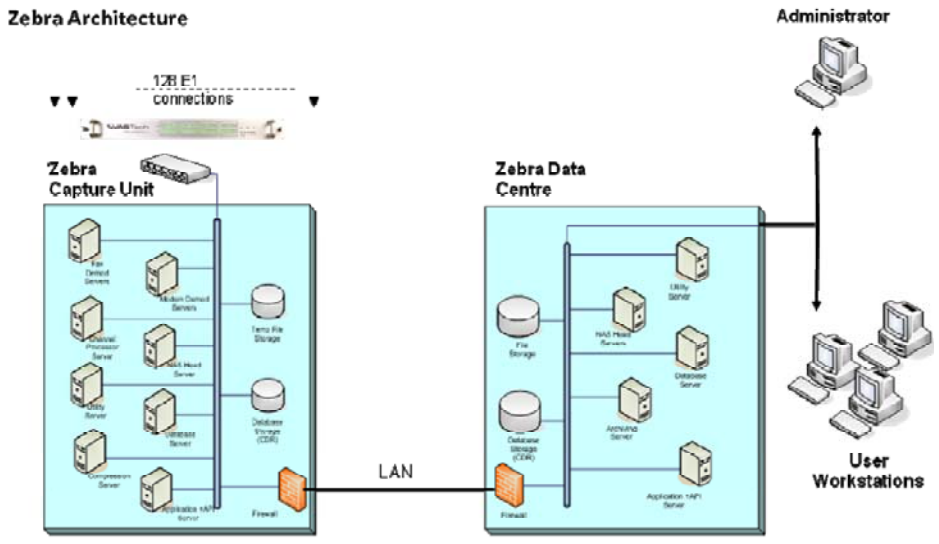
Figure 3. Zebra 128 E1/T1 gateway

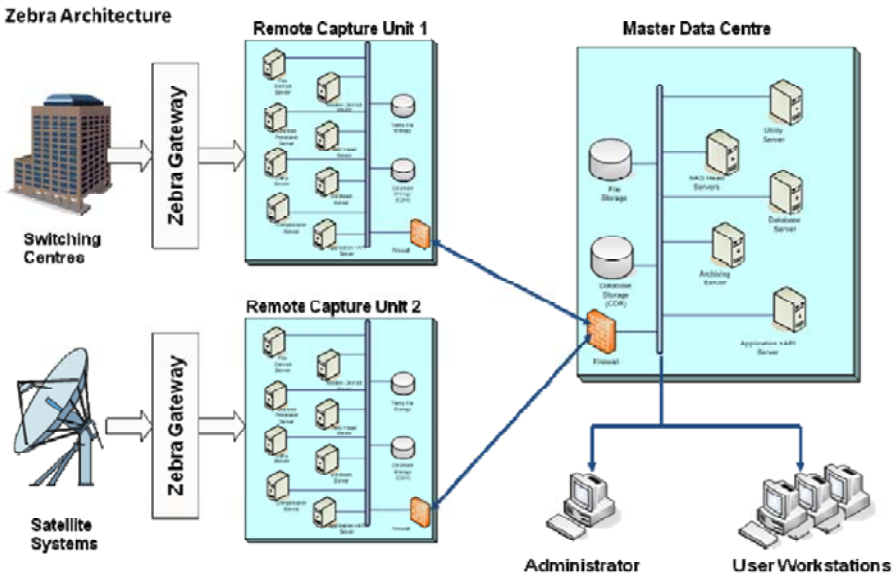
The Zebra enhanced user station will support user access to all LI meta data by 2007Q1.
The Zebra system connects to monitored networks by means of the Zebra gateway. The Zebra gateway is used to extract monitored TDM traffic and send it to processing servers of a switched local area network. This approach has a number of advantages:

- Supports all types of channels – the Zebra system can process any combination of individual E0 (64 kbps) TDM channels, n×64 kbps hyper channels and unstructured primary rate (1.544/2 Mbps) streams.
- Unlimited scalability – the Zebra gateway sends the contents of each monitored stream to the server requesting it. This allows the monitored traffic to be fanned out to as many servers as required for the load.
- Density – the Zebra E1 gateway couples 128 E1 inputs in each 1U 19" rack module. This helps to reduce the footprint of a monitoring system significantly. For example, Figure 2 shows a system capable of storing and processing 100% of the traffic on 384 bi-directional E1 streams in a single 19" cabinet.

The Zebra E1/T1 gateway supports long haul and short haul termination (down to -45 dB) at 120Ω, 100Ω and 75Ω.
The Zebra 128 × E1/T1 gateway is currently available. A gateway for SDH STM-1 and STM-4 as well as E3/DS3 will be available in 2007Q1. Both E1/T1 and SDH/E3/DS3 gateways can be used in the same system.

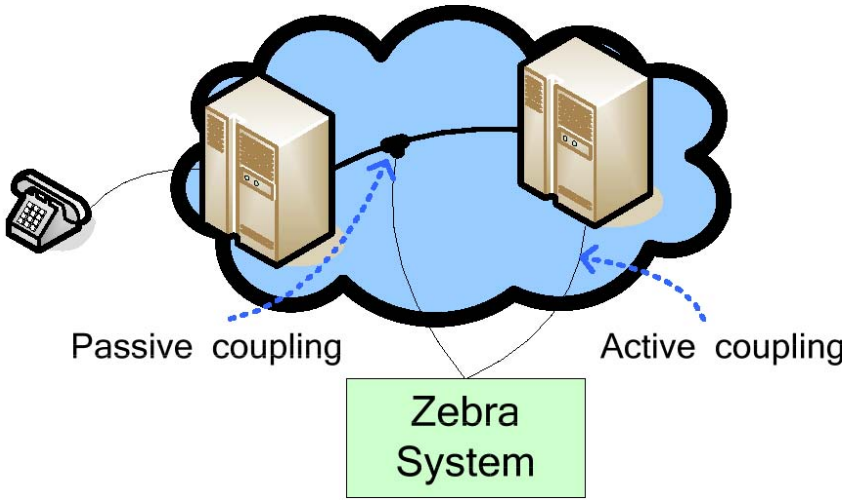
See reference [2] for more details.





Coupling

The Zebra system can couple actively or passively to monitored networks.



Passive coupling is used for passive trunk monitoring applications and is invisible to the monitored network. No network resources are consumed by the passive monitoring of carriers.
Active coupling is typically used for ETSI LI monitoring. The network actively couples with the monitoring equipment and makes monitoring calls to the monitoring equipment. Monitored network resources are required for making the observed calls to the monitor centre.
The management of large amounts of carrier cable can be a challenge, especially in large passive monitoring systems. We offer a modular coupling system that supports the connectivity management of large numbers of monitored carriers in conjunction with optional high impedance buffering (Hi-Z) and LED indication of the status of passively monitored carriers. One coupling frame is required for each Zebra E1 gateway to connect to 128 E1 inputs (64 bi-directional).

Figure 5 shows a Zebra coupling frame for 128 twisted pairs. This coupling frame occupies 9U rack space.

See reference [3] for more detail.

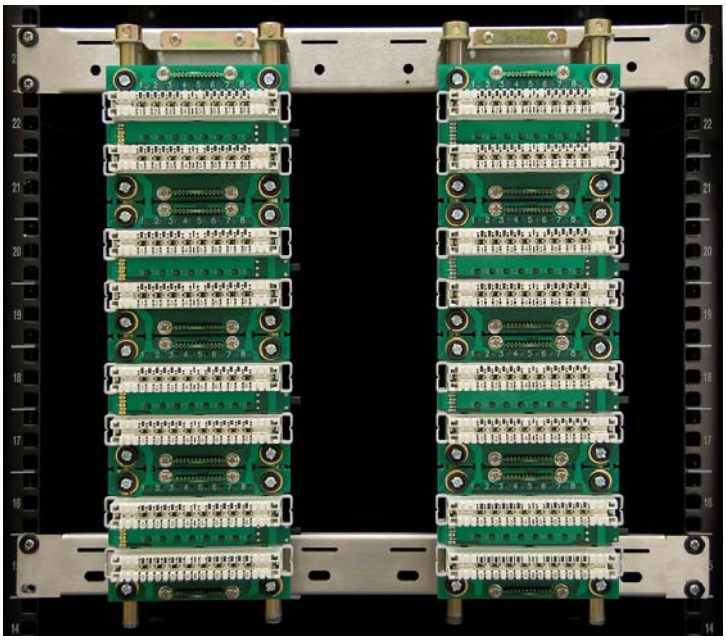
Hi-Z buffering

We offer an optional hi-z buffer with the Zebra coupling frame (Figure 5). The Hi-Z buffer module consists of a single printed circuit board that mounts behind the coupling board. It has a smaller profile than the coupling board and, therefore, consumes no additional rack space.

The Zebra Hi-Z buffer ensures that any signal flowing back to the monitored network is at least 20 dB attenuated and, therefore, prevents interference with the monitored carriers. Hi-Z buffering is used in passive monitoring applications where the Zebra system T's off live monitored carriers between switches (Figure 4, passive coupling).

Another application of the Hi-Z buffer is to split an E1 input off to multiple devices, for example, redundant gateways, protocol analyzers, etc. See reference [3] for more detail.

Figure 5. Carrier coupling frame for twisted pair



Access control

The configuration and intercepts stored in the Zebra system are only accessible to authorized users of the Zebra system.

User workstation

We currently offers a basic user station for filtering and browsing stored intercepts, playing audio and viewing fax/modem intercepts.

The Zebra enhanced user station that will offer sophisticated filtering and searching, playback and visualization of content, as well as the viewing of fax/Internet sessions, will become available by 2007Q1.

The Zebra enhanced user station is also designed with integrated link/network analysis to assist investigators in the visualization of associations between targets.

Administration workstation

The Zebra admin workstation supports the following functions:

- User management – the administrator can create and manage the users of the system
- Interception management – the configuration of intercepted carriers, including machine assisted SS7 CIC mapping and the automatic classification of SS5, SS7 signaling and SS7 audio channels
- Signal and signaling analysis – allows the administrator to view signaling messages, listen in real-time to channels, manually record channels and visualize the content of recordings
- Health monitoring

Migration between Zebra deployment units

Modern interception systems are often geographically distributed. The Zebra system supports the migration of intercepts between geographically distributed Zebra deployment units. A set of filters can be configured to determine which intercepts are migrated.

Migration filters select intercepts based on telephone numbers and content type (for example, voice, fax and data).

It is possible to configure remote deployment units to pre-process intercepts before migration, for example, compression of voice recordings or demodulation and decoding of fax and internet intercepts. By configuring migration filters to migrate processed intercepts more information can be migrated over a WAN link.

Compression

Intercepts are stored at the original compression rate (e.g.: G.711 A-law or μ-law). Many processes, like fax/modem demodulation and speaker identification, require audio in the original format. Voice intercepts can be compressed:

1. when migrated between Zebra deployment units, or
2. when stored for a configurable period of time.

Any codec available for the Linux system can be integrated with the Zebra system. The following codecs are available by default and free of licensing constraints:

1. G.711 A-law and μ-law.
2. Speex 5 kbps – 15 kbps.

The following table lists the available code rates for Speex that are supported by the Zebra system. Field tests indicate that 8 kbps provide acceptable quality for most intelligence applications.

Speex codec quality vs bit rate		
Bit-rate (bps)	*mflops*	*Quality/Description*
2,150	6	Vocoder (mostly for comfort noise)
5,950	9	Very noticeable artifacts/noise, good intelligibility
8,000	10	Artifacts/noise sometimes noticeable
11,000	14	Artifacts usually noticeable only with headphones
15,000	11	Need good headphones to tell the difference
18,200	17.5	Hard to tell the difference even with good headphones
24,600	14.5	Completely transparent for voice, good quality music
3,950	10.5	Very noticeable artifacts/noise, good intelligibility

Fax/Internet processing

The VASTech Zebra system offers integrated fax/modem processing. Protocols supported by integrated demodulator are:

- Full V.90 modem decoding
- All lower modem speeds and protocols
- Group 3 and Group 4 Fax
- All fax speeds and protocols up to and including high-speed V.34
- ISDN BRI – 64 Kbps
- Other Capabilities:
- V.42 error correction
- V.42bis compression
- V.14 async-to-sync conversion
- STAC Electronic LZS
- Van Jacobson
- Microsoft PPC
- Email and internet sessions
- Decodes PPP, TCP, UDP, HTTP, POP3, SMTP, IMAP, NNTP, IRC, TELNET, FTP, VoIP H.323, ICQ, AOL IM, Yahoo IM, MSN Messenger and many other internet protocols and services

Integration with 3rd party tools

We can offer integration with a number of 3rd party tools, for example,
Document – offers powerful indexing and searching facilities on documents
Visual link – offers advanced link analysis capabilities

An integration API is available for integrating other applications with the Zebra system.

Scalability

The system can be seamlessly scaled up as follows:

- 128 E1 inputs (64 bi-directional) per E1 gateway
- Up to 400 bi-directional E1s in each deployment unit
- Multiple deployment units combine into one or more data centers, each with the capacity to store, process and make available to user intercepts from more than 5000 E1s
- Network storage systems – commercial SAN storage is used. This allows the system to be scaled up as required. We currently use the following storage units
- 1U 19" rack module – over 10 million compressed call minutes capacity
- 4U 19" rack module – over 50 million compressed call minutes capacity
- Any combination of these units can be configured in a Zebra system

Redundancy

Figure 6 shows a Zebra system capable of processing and storing 64 bi-directional E1s. It shows the basic hardware building blocks:

- Zebra gateway – redundant power supply: 240V AC and -48V DC
- Nexsan SAN storage unit – supports redundant power, cooling, fiber channel connections, storage processors (in the case of the 4U 40 TB model). Hard disk drives are hot swappable and configured in RAID 10 arrays for Zebra systems.
- The Dell blade server chassis can be configured with redundant power supplies, fan modules, Ethernet switch modules and fiber channel switch modules. Power supply and fan units are hot swappable.
- Dell blade servers can be configured with two Ethernet ports and two fiber channel ports

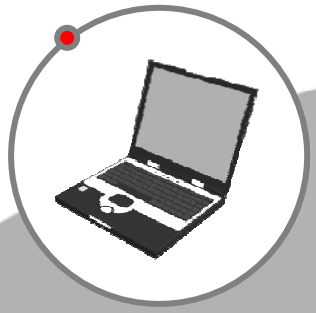
Figure 6. Zebra hardware

Roadmap

Our development laboratory is constantly adding new functionality to the Zebra system. The following major features are planned for 2007Q1:

- Zebra enhanced user station – will provide sophisticated filtering, support of the metadata of new protocols and ETSI LI, as well as integrated link analysis
- Comprehensive support of ETSI LI HI2 and HI3 compliant with ETSI TS ETSI TS 101 671 V2.13.1 (2006-01)
- STM1/STM4 gateway – the STM1/STM4 gateway will support 4 STM1 or 1 STM4 interfaces. It will also support up to 4 E3 or DS3 inputs. Any combination of multiplexed channels will be supported on the SDH streams, including: M13, E3 and ITU-T G.747. In addition unstructured streams will be supported at primary rate, 32Mbps (E3) and 42Mbps (DS3)
- VoIP – H.323 and SIP will be supported
- Speaker identification – support for text independent speaker identification is planned

Internet Monitoring
(Strategic & Tactical)



Index

Portable Modem Interception

The unit is a true portable modem intercept solution to be used in operations where direct access to the target lines is required.

This unit can be deployed in the field close to the target or installed on a permanent basis, for example, in a monitoring center. Due to the unique design of the physical line interface the system is completely undetectable by the target and is transparent to all parties on the line, making it ideal for all covert operations.

System Summary

The system is delivered as a complete turnkey solution, including all cables and accessories. It consists of a high quality and specially designed PSTN line interface and a lunchbox computer for recording and decoding. It is very easy to operate and it only needs a few hours of training to use it at its fullest potential.

The system intercepts all dialup modem traffic on a two wire analog PSTN line, and has no influence on normal voice or fax traffic on the intercepted target line.

V.90 and V.92 is supported but will be trained down to 33.600 from the interface box towards the target.

The target line is connected in sequence to the line interface box that in turn connects to the lunchbox computer; power it up and you are ready to go.

You can listen to any Voice over IP traffic. The audio player contains an automatic gain control filter to enhance the audio.

With these advanced tools you are able to follow whatever the target is doing on the internet and easily pinpoint any illegal activity.

Information can be copied to the built-in CD or DVD writer for presentation in court or other purposes.

The intercepted traffic is decoded into readable information for access to a broad range of tools for dealing with the intercepted data.

- Web pages
- E-mails
- Attachments
- Chat Sessions
- Web Mail
- Voice Over IP
- File Transfers
- Messenger Services

Applications	Features
- Field deployment and other temporary set-up scenarios - Permanent set-up in monitoring centers and offices - Operations where direct access to target lines are required - Internal investigations - Covert operations	- Easy set-up - Easy to operate - Automatic modem detection - Supports V.90 and V.92 - Web page decoder and viewer - E-mail decoder and viewer - Password acquisition for non-encrypted protocols

Technical specifications

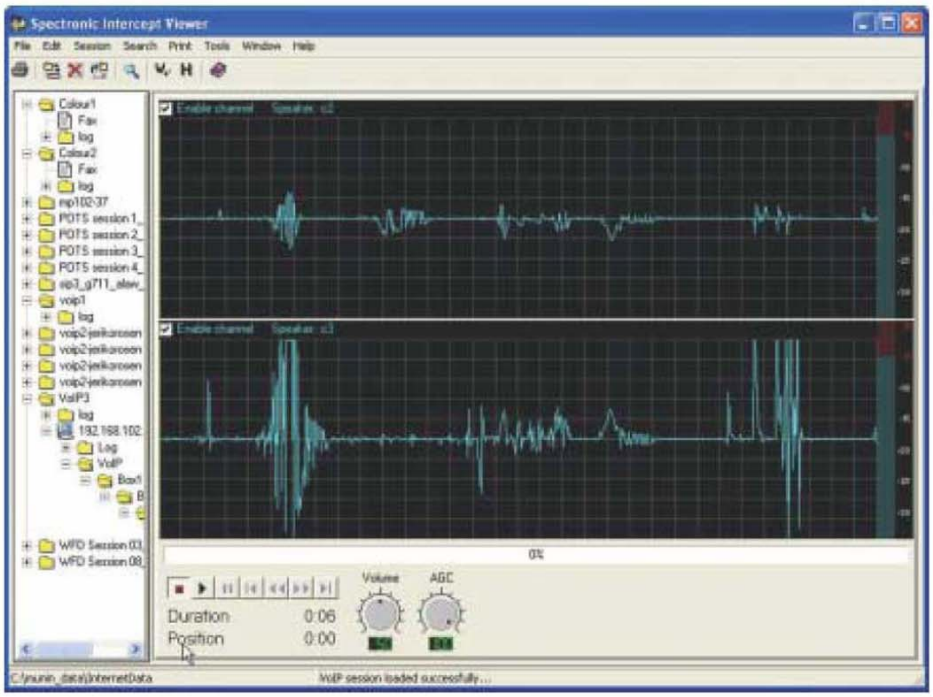
Internal Modems	
Protocols	V.21 Bell, V.22 Bell, V.22bis, V.23, V.32,
Internet protocols	HTTP, POP3, SMTP, IMAP, NNTP, IRC,
PSTN Line Interface	
Connector	Modular plug (RJ11) in parallel with Banana Jack
Power Input	
Connector	IEC Plug, 115 / 230 V Selections
Power Supply	
AC input	250 W / 100-120 V / 50-420 Hz,
	200-250 V / 50-60 Hz auto select
	EN60950 EMI EN55022 Class B
Dimensions (HxWxB)	41x31x25 cm / 16.1x12.2x9.8 inches
Weight	9.75 kg / 21.5 lbs.

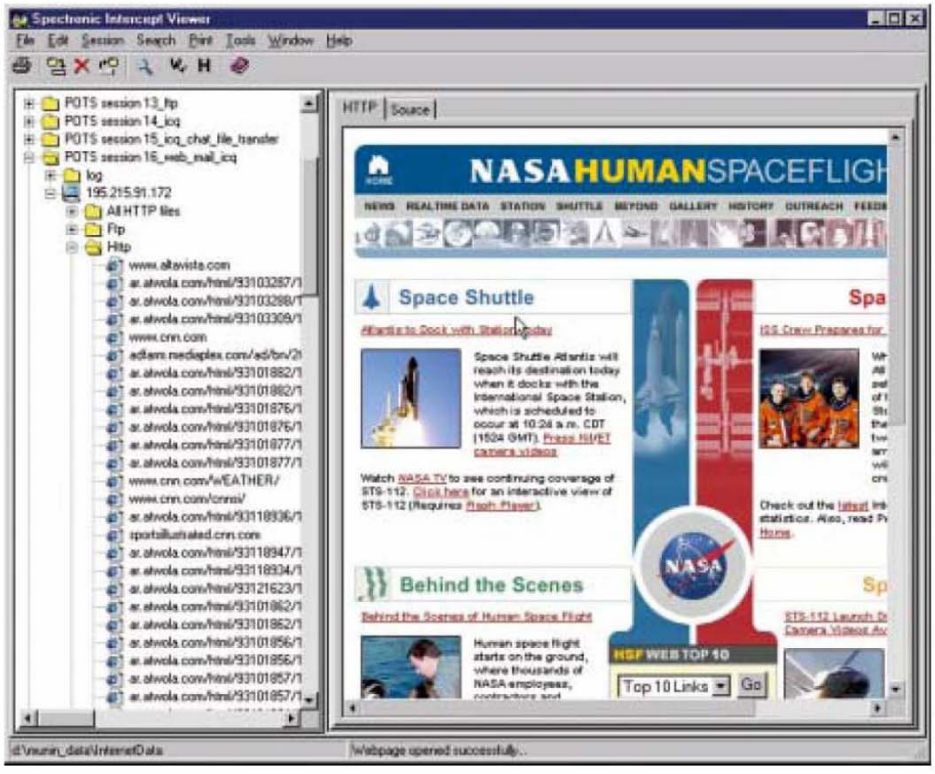
Environmental specifications

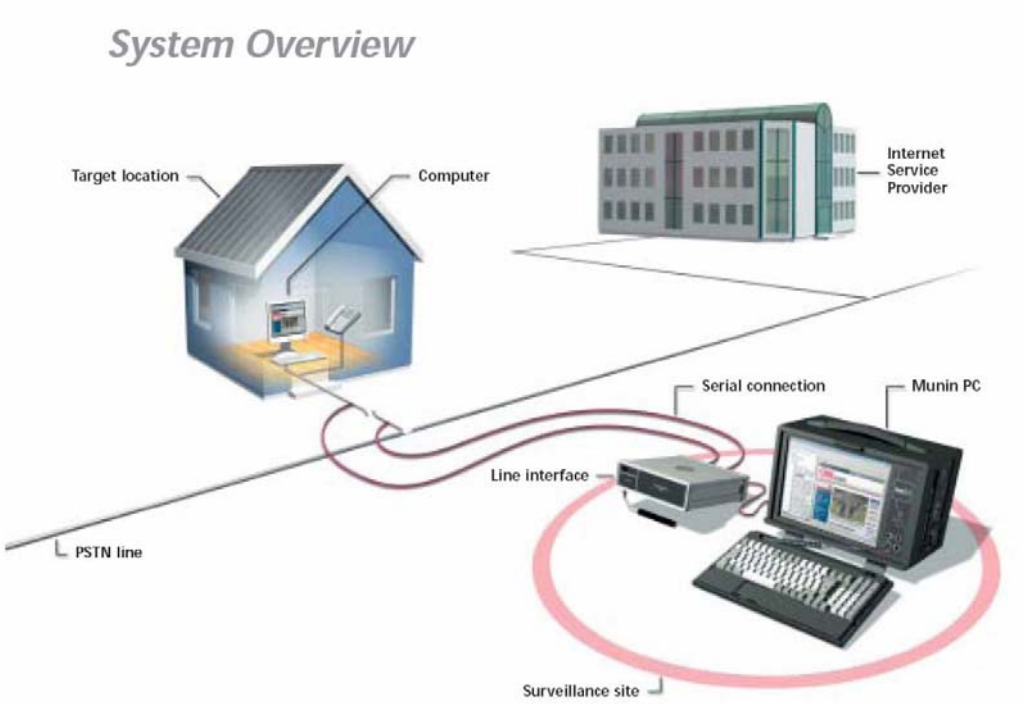
Temperature	
Operating temp. Range	0° C to +50° C / 32 F to 122 F
Storage temp. Range	-40° C to +70° C / -40 F to 158 F
Humidity	
Range	Max. 90%

Options

Hard Carrying Case
Dial-in Access
Model 4001 is also available with a stationary PC


Spectronic Intercept Viewer
File Edit Session Search Print Tools Window Help
Duration 0:06
Position 0:00
Volume
AGC

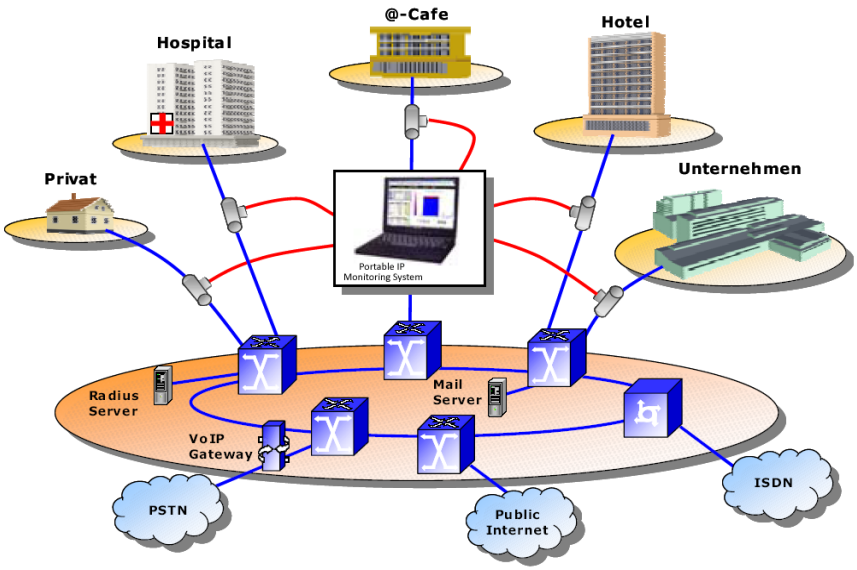

Spectronic Intercept Viewer
File Edit Session Search Print Tools Window Help
HTTP Source
NASA HUMANSPACEFLIGH
Space Shuttle
Behind the Scenes
Top 10 Links
Go


System Overview
Target location
Computer
Internet
Service
Provider
Serial connection
Munin PC
Line interface
PSTN line
Surveillance site

Portable IP Monitoring System

The ever increasing mobility of communication in our society with laptops, mobile phones, WLAN and PDAs has its drawbacks. The mobile criminal offender takes advantage of gaps in the criminal prosecution, like monitoring of WLAN-spots, internet-cafes, hotel rooms and airports. With our Portable IP Monitoring System we want to help close these gaps.

The Unit is a portable system for recording, reconstruction and evaluation of IP-data and their applications, e.g. email, web-sessions, and chat.



The System supports surveillance teams and S.W.A.T. to receive relevant information on location immediately and guarantees the access.

The System reads the data, filters them according to predefined filter criteria (depending on the specific usage and the legal regulations), adds a timestamp to the data and saves it in raw format in a database. Using the Analyzer User Interface the data can be reconstructed und evaluated – online or offline, residential or on location. For archiving purposes the saved raw data can be exported automatically or manually via FTP to already existing archiving media. Re-importing of archived raw data is also possible.

It consists of three functional parts. The recording of the raw data, picked up from different kinds of communication lines, the database management for internal organizational purposes of these data and the reconstruction function to analyze and evaluate the recorded IP-based data.

The Internet has produced a veritable flood of communication options, which are also being used by criminal offenders.

Our Company is an innovative provider of technology and services for monitoring, recording and reconstructing of telecommunications data for carriers and law enforcement agencies.

The service concept of the company enables carriers and Internet Service Providers (ISPs) to meet their statutory obligations in the most cost-effective way. With the Monitoring Center offered by the company and with the IP Monitoring product line state-of-the-art solutions are available for the law enforcement agencies to reconstruct, analyze and archive all kinds of communication data (voice, facsimile, modem and IP-data). The Company solutions are based strictly on the statutory specifications of the country concerned. In Germany, for instance, these are embodied in the Telecommunications Monitoring Ordinance (known under its German acronym 'TKUEV')

IP Data Monitoring

This unit is for the recording, reconstruction and evaluation of IP-data, which is passively recorded from different communication lines.

The unit reads the IP-data, filters it according to predefined filter criteria, adds a timestamp to the IP-data (NTP-Server) and stores it in raw format in its own database.

With the Graphical User Interface (GUI) the recorded IP-data can – even online – be reconstructed and evaluated. For archiving purposes the stored raw data can automatically or manually be exported via FTP to already existing archiving media. Re-importing of archived raw data is also possible.

Additional Entry

The unit's database combined with its powerful search functions enables the user to search for detailed activities and applications, recorded during weeks or even months. Within seconds he gets the list of communication data and content generated during a defined period of time, for example, by a specific host together with its IP-address.

The unit consists of three functional groups:
- Recording of raw IP-data, tapped from different communication links
- Database Management
- Reconstruction of IP-data

IP-data can be received by the unit via a wide range of Network Interface Cards (NICs) because it has the ability to record directly from the communication lines. The connection is realized with either network tap(s), SPAN-Port(s) or Mirror Port(s).

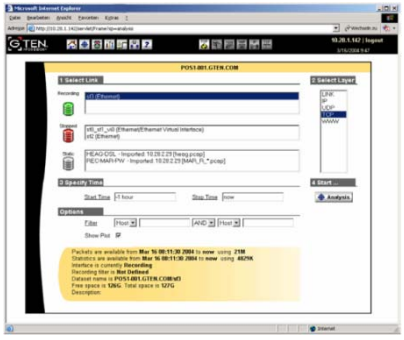
Important: All of the available NICs are passive, which means they are only able to receive data and cannot transmit any data. For that reason the unit is totally „invisible" in a communication network and cannot be identified.

For reconstruction of the stored IP-data a standard web-browser (e.g. MS Internet Explorer) is used, which has access to the unit via the integrated Ethernet Management Interface. The Internet Explorer is connected to the implemented Web-Server, which provides the GUI for reconstructing the data. By using simple mouse clicks user requests are transmitted to the database.

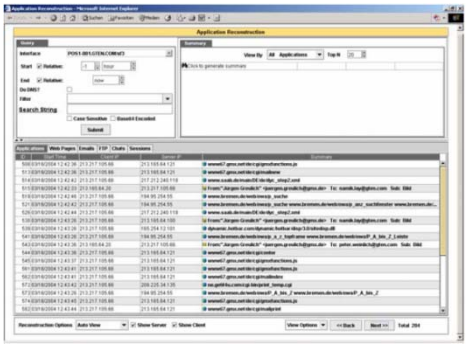
A GUI is available for the user. It is used, depending on the user rights granted, to configure the unit, to set-up monitoring tasks, for user administration, alarm management, data export/import and finally for reconstructing the IP-data.

Included is a sophisticated string search function enabling the user to search for characters or character combinations within the complete TCP-communication. The results are presented as a list showing all the communication by application (e.g. email, HTTP, FTP, TELNET etc.). With a simple mouse click the listed applications can be reconstructed and displayed.

Start page for IP-data analysis



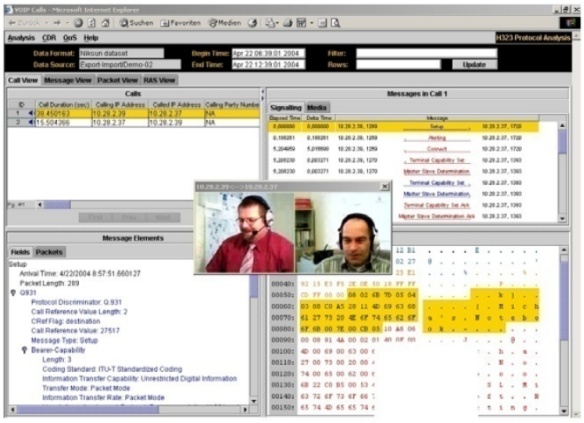
List of recorded IP-data (by applications)



Specification

Available NICs:

- 10/100 Mbit/s Ethernet mit 1, 2 or 4 ports
- 10/100/1000 Mbit/s Ethernet (Copper)
- Gigabit Ethernet 1000 Mbit/s (Fiber)
- T1, E1
- FDDI (UTP or Multi-Mode-Fiber)
- V.35
- X.21
- HSSI
- T3, E3
- OC-3 (SMF or MMF) for ATM or POS
- OC-12 (SMF or MMF) for ATM or POS



Reconstruction of VoIP (Audio and Video)

Supported Network Protocols accord. OSI-Reference-Model

Layer 2 = Link-Layer
Frame Relay
HDLC
CISCO HDLC
PPP
Bay PPP
MLPPP
802.3/VLAN

Layer 3 = Network-Layer
IP
ATM und IP
POS und IP
WCP Compression
STAC Compression

Reconstruction

PPP (displayed as ASCII or HEX)
- PAP
- IPCP
- LCP

Ethernet (displayed as ASCII or HEX)
- IP
- ICMP
- UDP
- TCP

TCP (displayed like application or ASCII)
- SMTP
- POP3
- HTTP
- IMAP4
- Telnet
- Chat
- IRC
- FTP
- VoIP (optional)

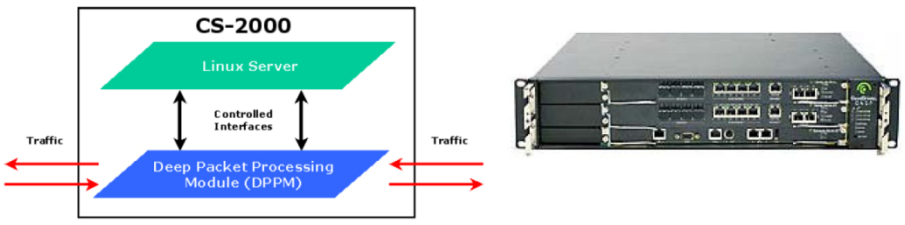
Hardware

Form Factor: 19" rack mountable, 1U, 2U or 5U
Dual Intel XEON Processors
2 GB RAM
CD-ROM
10/100 Mbit/s Ethernet Management Port different SCSI-Hard-Disk combinations from 144 GB to more than 1 TB Depending on the configuration
- with/without RAID-0, RAID -5
- redundant power supplies
- optional Gigabit Management Port

Manipulation and Blocking: Cloudshield CS2000

In their efforts to generate value for their organizations, networking engineers are constrained by available applications' platforms. Open conventional servers are unable to perform at the speeds of the network, and high-speed appliances are closed, inaccessible, and often fixed function systems. **In-Network Computing** combines the best of these computing architectures resulting in a multi-purpose, high-speed programmable packet processing platform. The CS-2000 removes the barriers to innovation and service development.

The major innovation in the CS-2000 is the programmable Deep Packet Processing Module, or DPPM. The DPPM provides a complete set of computing resources and instruction sets designed for, and dedicated to, packet processing in the data plane. The DPPM delivers ASIC-based appliance performance in a general platform.



Faster, more CPUs is Not the Answer

CPUs, RAM, bus and disk drive technologies all benefit from continued performance improvements. However, the one area where CPU-based computing platforms fall short is network performance. The problem is not CPU speed, but its design.

The CS 2000 has created a new network applications' platform - a general purpose deep packet processing platform combined with an open Linux server blade. It is designed for applications focused on **real-time** network traffic processing.

CS-2000 provides the application developer high-speed processing, high-speed RAM, a high-speed database, and a structured programming language for data plane-resident packet operations.

This results in:
- No more CPU interrupt latency
- No more PCI bus bandwidth constraints
- The power to operate on every packet – every bit of every packet – on the wire in real-time

The CS-2000 also provides conventional Linux server resources for off-line analysis and non real-time application functions.

What is requested by Carriers, ISPs, Enterprise Networks...?

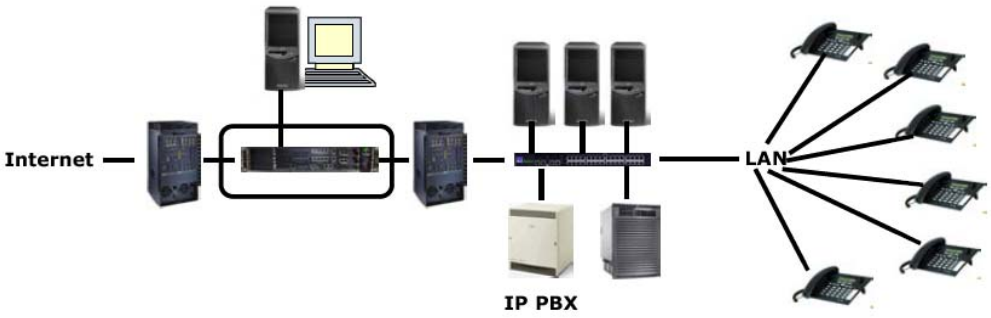
Network Management
- Per Call SLA Measurement
- Usage Based Billing
- Traffic Statistics

Session Management (Ensure Services) Protocols
- H.323, SIP
- MGCP
- RTSP

Security (Protect Infrastructure) Content Support
- SIP Proxy/Gateway
- Stateful Firewall
- Denial of Service Protection

CONTENT Support
- Lawful Interception
- RTSP Multicasting
- Compression via Aggregation

Quality of Service (Manage Convergence)
- Content Based Routing
- Traffic Prioritization



Configuration

A proper **CS-2000** configuration includes:
- a single **DPPM** (see specifications) and
- a single Linux-based **ASM** (Application Server Module)

The ASM is a dual 1GHz Pentium server with 1 Gigabyte of RAM and a 60 Gigabyte hard disk. The ASM, today, supports Redhat Enterprise Linux and hosts the web-based system management server software and database, an SNMP Agent, and DPPM control APIs. Under normal load, these components utilize less than 20% of the available ASM resources. That leaves more than 80% of the Linux server resources for running non real-time application functions.

The CS-2000 is really two computers to create one robust In-Network Computing platform. There is a high-performance packet processing computer for all real-time packet operations, and a standard Pentium-based server for less time-critical operations.

Features

Deep Packet Processing:
- up to 5 Gbps Layer 2-7 analysis
- recognition and processing up to 1 Mio simultaneous data streams
- secure, transparent network installation
- Ipv4 and Ipv6 support

Management:
- Web based management system
- integrated script based CLI (Command Line Interface)
- SNMP v1, v2c, v3 GET/TRAP support

User access:
- Telnet (CLI), SSH (CLI) and http/http-S (web)
- Ethernet (all), COM port (CLI), KVM (CLI)

Specification

- 19" Rack mountable 2U
- Dimensions: 8.74 x 48.26 x 60 [cm]
- Weight:11 kg

Power requirements:
- DC: -40.5 bis –72 VDC
- 300 Watt
- 6,25 A bei –48 VDC
-
- AC: 110 bis 240 VAC
- 50 bis 60 Hz
- 300 Watt
- 2.5 A bei 120 VAC

DPPM
DPPM-500 Gigabit Ethernet
- 3 Mio packets/s
- 2 Gbps data throughput
- Gigabit Ethernet: 4x unidirectional
- 2x bidirectional

Copper:
- 10/100/1000 Base-T Ethernet, RJ45
- Fiber: SX: 850nm multi-mode

19" Rack mountable 2U
Dimensions:8.74 x 48.26 x 60 [cm]
Weight: 11 kg

Power requirements

DC: -40.5 bis –72 VDC
300 Watt
6,25 A bei –48 VDC

AC: 110 bis 240 VAC
50 bis 60 Hz
300 Watt
2.5 A bei 120 VAC

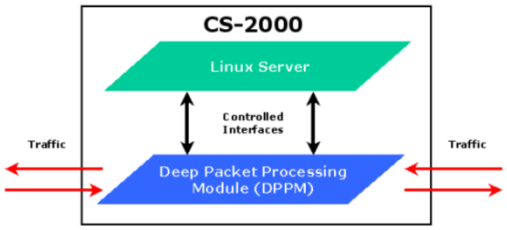
DPPM

DPPM-500 Gigabit Ethernet
3 Mio packets/s
2 Gbps data throughput
Gigabit Ethernet: 4x unidirectional
2x bidirectional
Copper:
10/100/1000 Base-T Ethernet, RJ45
Fiber: SX: 850nm multi-mode

Manipulation and Blocking: CS-2000 High End
High Performance Network Platform

Networking engineers are constrained by available applications platforms. Open conventional servers are unable to perform at the speeds of the network, and high-speed appliances are closed, inaccessible, and often fixed-function systems.

CS-2000 combines the best of these computing architectures resulting in a multi-purpose, high-speed programmable packet processing platform. With the CS-2000, GTEN removes the barriers to innovation and service development.



The major innovation in the CS-2000 is the programmable Deep Packet processing Module, or DPPM. The DPPM provides a complete set of computing resources and instruction sets designed for, and dedicated to, packet processing in the data plane. The DPPM provides ASIC-based appliance performance in a general platform.

Faster, More CPUs is Not the Answer

CPUs, RAM, bus and disk drive technologies all benefit from continued performance improvements. However, the one area CPU-based computing platforms fall short is network performance. When heavy packet processing is required, CPU-based computing platforms cannot keep pace. The problem is not CPU speed, but its design.

GTEN has a new network applications platform – a general purpose deep packet processing platform combined with an open Linux server blade. Designed for applications focused on real-time network traffic processing, the CS-2000 provides the application developer high-speed processing, high-speed RAM, a high-speed database, and a structured programming language for data plane-resident packet operations. No more CPU interrupt latency, no more PCI bus bandwidth constraints, but the power to operate on every packet – every bit of every packet – on the wire in real-time. The CS-2000 also provides conventional Linux server resources for off-line analysis and non real-time application functions.

The CS-2000 enables network operators and network applications developers to implement their ideas, build differentiating service features, deliver benefits to customers, and bring value to their companies.

Modular System Delivers the Capacity You Need

DPPM–500 Deep Packet Processing Module for high-performance packet processing applications on Gigabit Ethernet networks. Providing 2 gigabits per second (Gbps) packet processing performance, the DPPM-500, has 4 Gigabit Ethernet ports (Copper or Fiber) plus one 1000Base-T Gigabit Ethernet capture port on the front panel.

DPPM–600 provides DPPM 500 features at full line rate for OC-48 / STM-16 SONET/SDH links. The DPPM-600 supports two OC-48c/STM-16 PoS (Packet over SONET/SDH) interfaces and up to 2.5 Gbps of packet processing performance. Network interfaces are OC-3.12 / STM 1.4 capable. RAVE applications can be executed on either DPPM model without modification.

A proper **CS-2000** configuration today includes a single DPPM and a single Linux-based **Application Server Module** (ASM). The ASM is a dual Pentium server with 1 GB of RAM and a 60 GB hard disk. The ASM, supports Linux and hosts the web-based system management server software and database, an SNMP Agent, and DPPM control APIs. Under normal load, these components utilize less than 20% of the available ASM resources. That leaves more than 80% of the Linux server resources for running non real-time application functions.

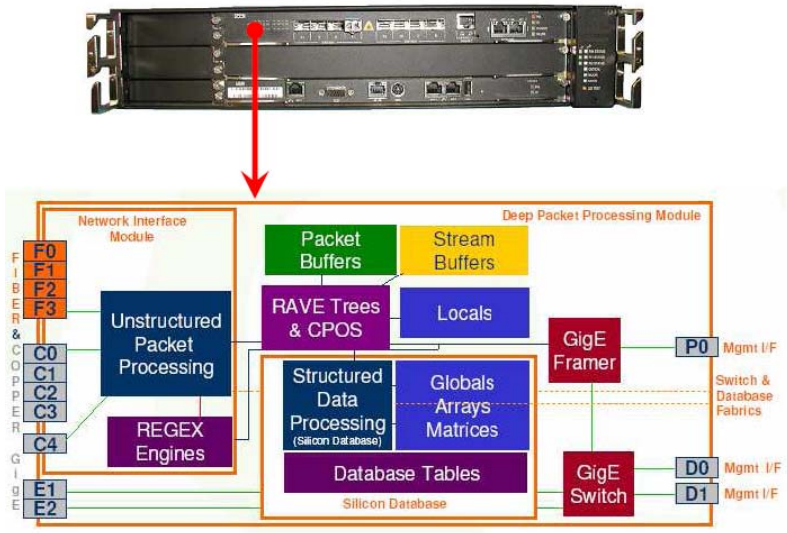
The **CS-2000** is really two computers to create one robust network computing platform. There is a high-performance packet processing computer for all real-time packet operations, and a standard Pentium-based server for less time-critical operations. No longer is fixed functionality a requirement for achieving high performance.

CS-2000 Features

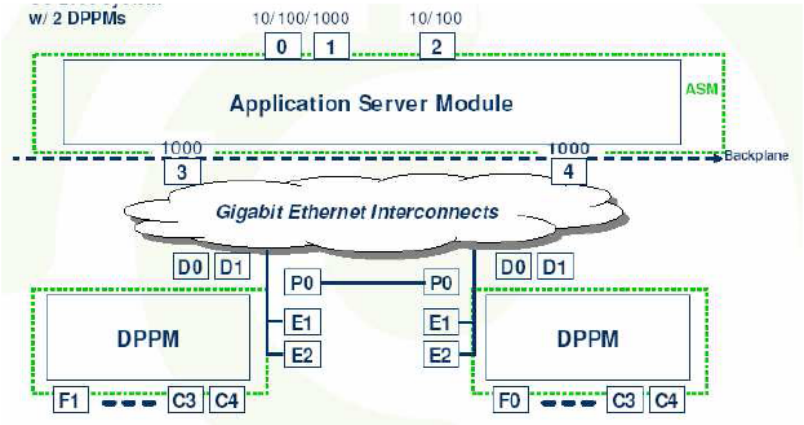
Deep Packet Processing
- Up to 5 gigabits per second L2-7 inspection and analysis
- Detect and track Up to 1 million simultaneous flows
- Secure transparent network installation
- Native IPv4 and IPv6 support, can be taught others **Management**
- Web-based element management system
- Integrated scriptable command line interface (CLI)
- SNMP v1, v2c, v3 GET/TRAP support
- User access:
- Telnet (CLI), SSH (CLI), and HTTP / HTTP-S (web)
- Ethernet (all), COM port (CLI), KVM (CLI)

Hardware Overview

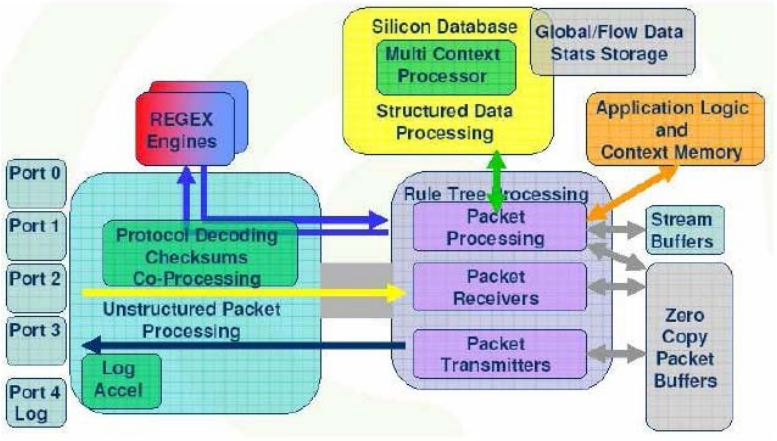
Hardware Overview: GE PPM



Hardware Overview: System Level Port Distribution plus Out of Band Management Architecture (CS-2000 system with 2x DPPMs)



Hardware Overview: Network Processing Pathways



Specifications

DPPM-600 – Packet over SONET
4 million frames / second; 2.5 Gbps data throughput
SONET / SDH Interfaces
- 2x OC-48c / STM-16 POS OC-12c / STM-4 & OC-3c / STM-1 ready optics and SFPs
- SR-1: 1310 nm single mode
- IR-1: 1310 nm single mode
- LR-2: 1550 nm single mode

Dedicated 1000 Base-T for packet capture/logging

DPPM-500 – Gigabit Ethernet
3 million packets / second; 2 Gbps data throughput
Gigabit Ethernet Interfaces:
- 4x unidirectional, 2x bi-directional
  Copper - 10/100/1000 Base-T Ethernet, RJ-45
  Optics and SFPs
- SX: 850 nm multi-mode
- LX: 1310 nm single-mode

Dedicated 1000 Base-T for packet capture/logging
ASM – Application Server ModulesDual
Pentium, 1 GB RAM, 60 GB HD
2x 10/100/1000 Base-T Ethernet RJ-45
1x 10/100 Base-T Ethernet RJ-45
1x RS-232 console port
1x USB port

Chassis
- 19" rack-mount 2 HU
- Dimensions (HxWxD) 87 x 482 x 600 mm
- Weight: 11 kg

Power Requirements

DC power, AC power
- DC input power 300 watts
- AC input power 300 watts
- DC input voltage - 40.5 to - 72 VDC
- 90 – 240 VAC
- 6.25 Ampere at - 48 VDC

Manipulation and Blocking: Cloudshield Packet Works DE
Developers' Toolkit for CS-2000 In-Network Computing Platform

IDE Puts Needed Tools Within Reach

CloudShield's Packet Works IDE is a comprehensive Suite for developers of applications on CloudShield CS 2000 *In*-Network Computing platforms. The IDE supports development, compilation, emulation, and debugging of high speed network applications for CloudShield's CS 2000 platform. Leveraging the extensible Eclipse IDE framework, users can access a wide range of additional, open source plug-ins to customize the IDE to meet their needs.

Key Functions

- Traditional text-based RAVE programming
- Flow chart style RAVE programming
- Step-thru debugger & traffic simulator
- CVS client components
- Extensible open source IDE framework offers additional languages and developer's tools

RAVE Revolutionizes Network Application Development

RAVE is CloudShield's high-level data plane programming language which makes it easy to develop deep packet processing applications. It is a comprehensive developers' tool with over 400 packet processing function calls. RAVE users have experienced prototype development times in days, instead of months and have built deployable applications in under four weeks.

RAVE provides users easy access to a variety of options to process, manipulate and analyze packets, including the following features:

- Packet decode
- String search and data compare
- Drop, forward or capture data
- Packet modification

RAVE applications run in conjunction with CPOS which handles execution of the RAVE function calls, ensuring the best available resource executes the command. No need to apply steep learning curves of device-centric programming: CloudShield's RAVE and CPOS eliminate the lower level programming functions by providing a higher level language for you to port, develop, and manage applications.

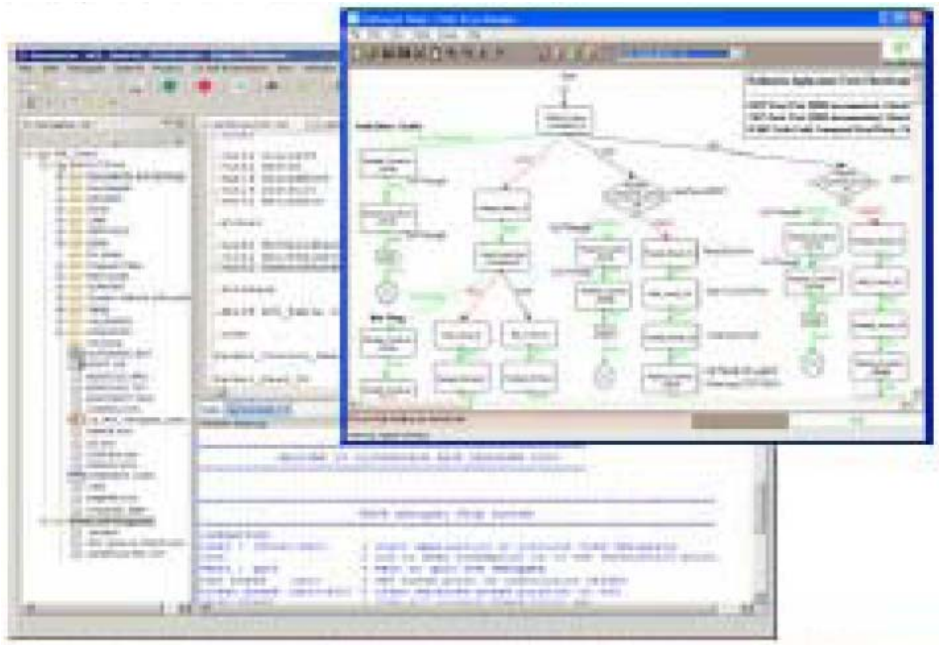
The PacketWorks IDE provides the developer two RAVE editors for building CS 2000 data plane packet programs: a text based RAVE plug-in editor for the Eclipse workbench; and graphical packet operations flow chart style editor called Visual RAVE.

The RAVE plug-in editor presents a traditional programming interface used for project oriented programming. Visual RAVE's graphical interface enables developers to easily design packet processing flow and logic. Rules and actions to be performed on packets are represented as a visual decision tree. Variable definition and application coding is accomplished through dialog boxes and drag and stop functions.

Available RAVE functions includes:

- Packet functions: packet field read/write/expand/collapse/redirect/forward/drop
- Math function: variable add/subtract, Boolean logic
- Database functions: Insert/update/Read/Select/Search

PacketWorks IDE & Visual RAVE (Insert)



CloudShield Provides Path to the Next level

CloudShield's *In*-network Computing Platforms offer new levels of performance, flexibility, and deep packet processing that speed the development of high-speed network applications. CloudShield platforms position application computing capabilities in the network enabling network security and traffic management applications with full layer 2-7 packet inspection on multi-gigabit links. The combination of CloudShield's revolutionary Deep Packet Processing Modules, Linux server, and RAVE *In*-network computing programming language can take existing or new applications to new markets and high-speed network locations in record time.

CloudShield's *In*-network Computing Platforms have revolutionized high-speed network application development by combining a broadly accessible development environment and high-capacity, programmable packet processing platform. Network application developers now have the packet processing capacity today's networks demand, and a simple programming environment that enables fast application development. CloudShield lowers market entry costs, and reduces development time to open up new growth opportunities.

The CloudShield PacketWorks IDE utilizes the open IDE framework from Eclipse.org for packet processing application development tool integration. Formed in 2001 by 8 industry leading software companies, Eclipse.org is an open source software framework for creating, integrating, and deploying application development tools. By leveraging Eclipse, PacketWorks IDE programmers are assured access to a growing list of programming languages and tools to support application development beyond data plane packet processing operations—data presentation, UI and application heuristics development, to name a few. Available Eclipse framework plug-ins includes, PHP, PERL, C/C++, and Java programming languages and compilers. Programmers can build on the PacketWorks IDE to meet all their network application programming needs.

The chart below highlights the components included in the PacketWorks IDE distribution image.

PacketWorks IDE Summary of Benefits:

Improved Deep Packet Processing Application Development
Program, compile and debug CS-2000 applications on a PC
Comprehensive RAVE program debugger supports:
- Application break point step through
- LIBPCAP traffic simulation (before and after)
- Variable tracing
- Memory use and allocation
- More traditional text-based RAVE language speeds development and supports multi-programmer projects
- Visual RAVE offers fast GUI-based programming
- Functional reference utilities available for modification/incorporation into applications

Fast Path to High-Speed Network Applications
- Easy access to CloudShield's high-performance high capacity applications-ready platforms
- Flexible porting options easily extend performance range of existing applications to support multi-gigabit deployments
- Developers ramp up in hours-to-days, not weeks-to-months

A Complete Developer's Environment
- Based on widely-deployed Eclipse open framework
- Available C++, Java and ether language IDE plug-ins
- Supports team-based CS-2000 applications development
- Projects/Developers can work with CVS-protected files

CloudShield PacketWorks IDE 1.0 Facilities*	
IDE Framework	• Eclipse
Languages & Editors	• RAVE (plug-in) • Visual RAVE • RAVE Debugger (Win)
IDE Extensions	• Java SDK • CVS client plug-in
Supporting Tools	• MySOL for Windows • WinPCAP • Ethereal
*See Packet Works IDE Installation guide for component revision matrix	

Minimum System Requirements	
Processor	1GHz Pentium III-class processor (or equivalent) recommended
Operating System	PacketWorks IDE can be installed onto one of the following systems: • Windows 2000 Professional (SP3) • Windows XP Professional (recommended)
Memory	256 MB of RAM minimum 512 MB of RAM (recommended)
Hard Disk	I Gig of hard disk space
Installation Drive	CD-ROM or DVD-ROM (Note; PacketWorks IDE is also FTP Downloadable)
Display	Super VGA (1024 x 768) or higher resolution with 256 colors

Manipulation and Blocking: P2P Traffic Filter

This Unit is a filter for peer-to-peer (P2P) traffic. Detection of P2P traffic is based on protocol signatures, which are updated on a regular basis. Compared to legacy port-based methods, the number of mismatches is drastically reduced and thus the filtering does not interfere with normal network usage. In addition to filtering P2P traffic additional communication methods like Instant Messenger and VoIP can be filtered.

P2P traffic can be handled in several ways:

- **Block**: Blocking prevents any P2P communication taking place
- **Shape**: Shaping throttles P2P traffic to an acceptable rate. The throttling is invisible to users of the network as file sharing applications continue to work as normal
- **Bridge**: All traffic is bridged transparently
- **Statistics**: Statistics of P2P usage are generated. This might be useful to get actual usage data to specify the traffic shaping rules

These modes can be activated manually as well as on a configurable time schedule.

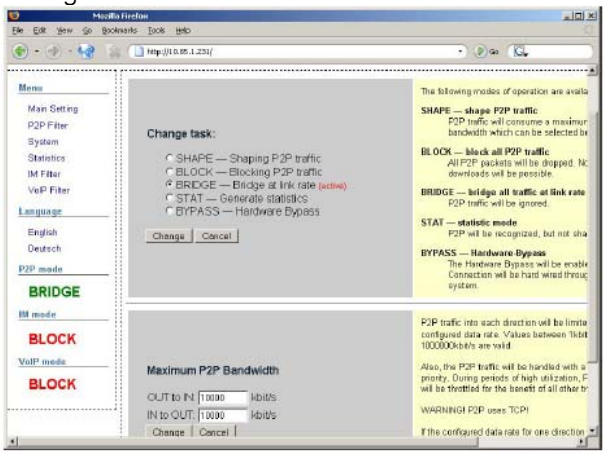
As the unit operates as a transparent bridge it appears completely invisible to normal network users. Administration personnel can manage the system via a separate network interface.

An integrated hardware bypass is automatically enabled if the system loses its power connection. Therefore, the deployment of the unit poses no negative impact on the reliability of the network. The bypass can also be manually activated by the administrator.

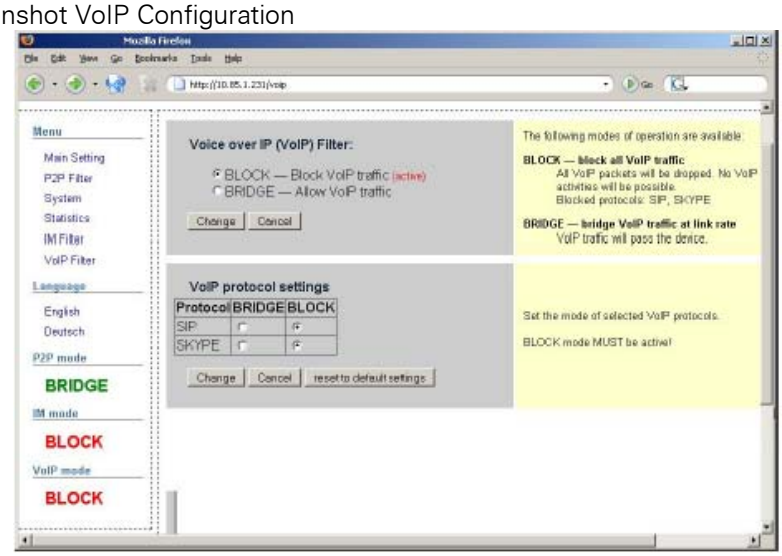
Administration is done via an intuitive web interface. Besides configuration, it features detailed graphical statistics on network utilization and P2P usage.

P2P protocols used by file sharing networks are subject to frequent changes with new protocols appearing every few months. Only regular protocol signature updates can ensure the filter's effectiveness.
The maximum throughput is 1.6 Gbits/s. An entry level version with 350MBit/s throughput is available as well.

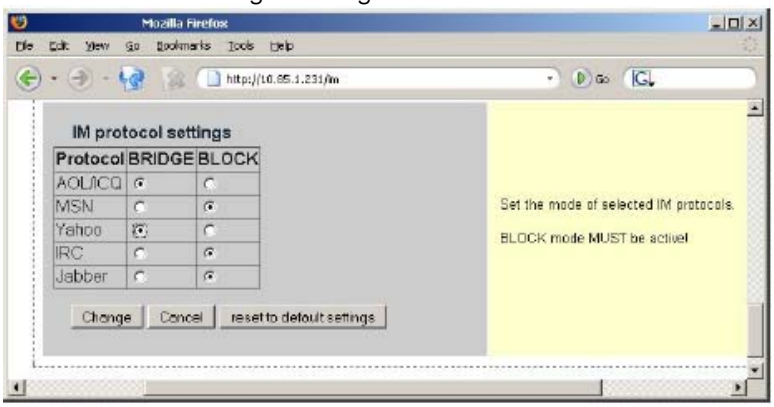
Screenshot Filtering Modes



Screenshot VoIP Configuration



Screenshot Instant Messenger Configuration



Specifications

Performance:

Max. throughput:	1,600 Mbit/s (optional: 350 Mbit/s)
Max. packet rate:	240,000 packets/s
Network connections:	
Bridge:	2x 10/100/1000Base-T with hardware bypass
Management:	1x 10/100/1000Base-T
Chaining:	1x 10/100/1000Base-T for joint management of multiple units

Supported protocols:

P2P: Ares, Gnutella, AppleJuice, Fasttrack (Kazaa, Grokster, BitTorrent, iMesh, Morpheus), DirectConnect, Soulseek, Edonkey, WinMX

VoIP: SIP, Skype,

Instant Messenger: AIM (AOL), ICQ, MSN Messenger, Yahoo Messenger, IRC, Jabber

Hardware:

Form factor:	19" rack mountable, 1U
Width/height/depth:	426 x 43.5 x 431.8 mm
Power supply:	ATX 250W
Weight:	12 kg
Console:	serial DB-9 connector
Network:	4 x 10/100/1000Base-T (2 x bridge, 1 x management, 1 x chaining)
Certifications:	CE / FCC Class A

Countrywide IP Monitoring
(See the following Brochure)

Monitoring Center

Application Note

IP Interception System - IPIS

The IP Interception System offers flexible and scalable solutions to mark and intercept at multiple and varied points in the Internet and to deliver this data to one or more authorised Law Enforcement Agencies.

Where integrated in Internet components, IPIS supports the embedded LI functions. With no embedded LI, IPIS offers a range of Data Collectors to capture and filter the data.

SIEMENS

Global network of innovation

Overview

The IP Interception System (IPIS) performs Lawful Interception (LI) based on captured data from the Internet, mediation of various network devices and delivery of the intercepted data to Law Enforcement Agencies (LEA).

It can operate with the Siemens Monitoring Center or other Law Enforcement Monitoring Facilities (LEMF) chosen by the LEA. It supports the integrated LI functions of market leading switch and router vendors, and where none is available, offers a range of Data Collectors to filter and capture the desired data.

The Data Collectors directly offer Ethernet and ATM interfaces and bandwidths ranging from small ISPs to peering points in the Internet. Other interfaces are supported using adapters. IPIS can also manage ETSI LI sources.

A well conceived security architecture ensures access to targets and data only by authorized persons. Security of both data and management transmissions is always offered with IPIS but customer specific solutions can be easily implemented.

IPIS Applications

The IPIS is capable of intercepting data in the Internet, in other IP based networks and VoIP in Next Generation Networks (NGN). It can be configured to intercept and deliver a range of data using very granular triggers to select the types of data or the targets to be intercepted.

The IPIS is used in several application scenarios including the following:

- Email only interception and delivery
- VoIP interception in NGN
- General Internet interception

All IP data received into the IPIS can be distributed to LEAs according to ETSI standards. The LEA can extract IP data based on triggers set in the IPIS. The following trigger types can be set in the IPIS:

- Email, such as SMTP, POP3, IMAP4 & Webmail
- Web/HTTP, FTP or IRC
- VoIP
- Keyword/String Search
- IP Address
- Instant Messaging

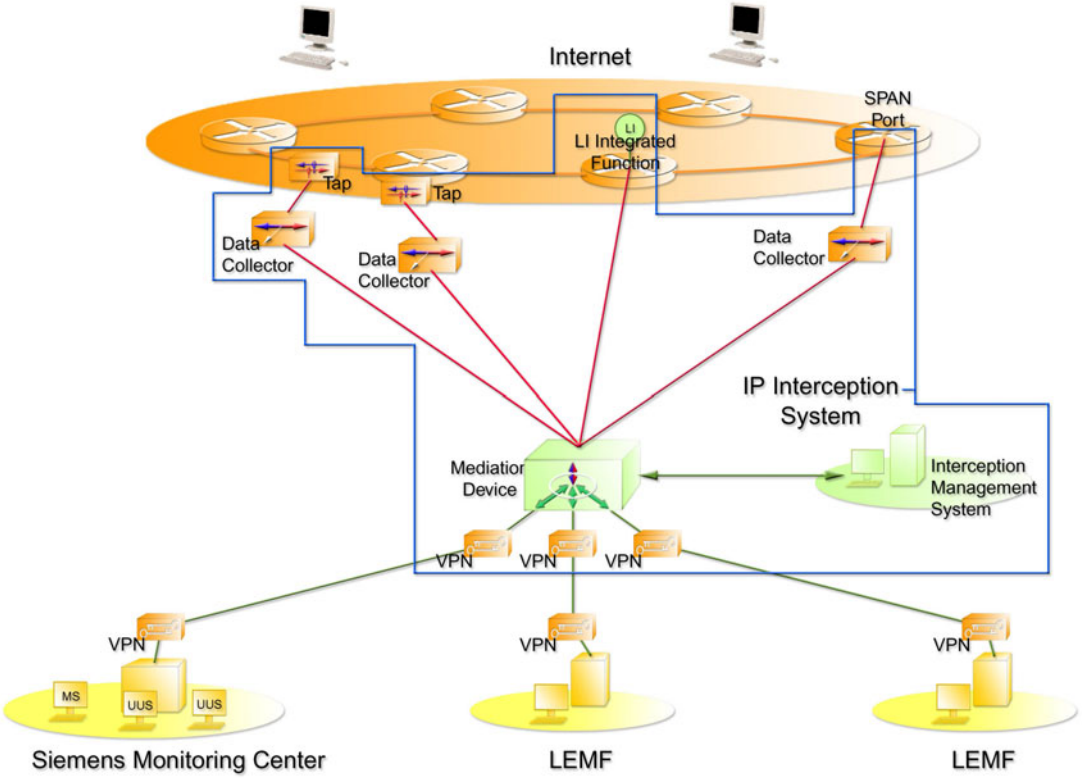


Figure 1. LI Network, Mediation and LEMF environment

Background to IP Interception

Most modern Circuit Switched networks have an integrated Lawful Interception (LI) function. The Lawful Interception function intercepts the targeted calls and forwards them to Law Enforcement Agencies (LEA), as directed by an Interception Management System (IMS). Meta-data about the call (Intercept Related Information) is sent to the IMS which forwards it to the appropriate LEA.

In contrast to this mature standards environment, the Internet is still in the process of LI standardisation. Most IP interception is performed by Data Collectors that are located near or inside the Internet nodes and essentially filter it for desired data.

There are a few IP Switch and Router vendors that have started to implement LI functions and these will become more common in networks over time.

The varied mixture of Switch or Router integrated LI function and Data Collectors from different vendors needs a Mediation and Delivery application to mediate between the Internet and the LEA.

Siemens IP Interception System

Siemens offers the IP Interception System to address the needs of Lawful Interception in the Internet. There are several components in the solutions as well as flexible configurations to suit the needs of the customer. This application note looks more closely at these solutions from Siemens.

The Networks

There is an ever-increasing array of networks that use IP as their data transmission protocol. The Internet is the first that comes to mind, but it also includes GPRS, UMTS, VoIP networks – Next Generation Networks (NGN) and many Wireless Networks. Where there is a mandate to perform Lawful Interception in any or all of these networks, the first questions are how and where to access the data.

IPIS offers a wide variety of possibilities to gain access to and manage the flow of the intercepted data from the networks.

These include:

- Taps
- SPAN Ports
- Devices with integrated LI functions
- Data Collectors
- Load balancing techniques, including IP Application and Aggregation switching
- Interface/Protocol Mediation

Taps

Network Taps are used to connect to different physical signals in an unobtrusive manner.
They are available for electrical and optical lines for different transmission speeds.

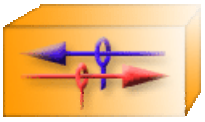


Figure 2. IP Tap

SPAN Ports

In most network switches, a SPAN or mirroring Port can be configured to copy the traffic of a single or of multiple switch ports. Also complete VLANs can be mirrored. However, over-subscription of SPAN Ports can lead to a loss of data.

Figure 3. SPAN Port

Integrated LI Function

Due to the evolving requirements of Lawful Interception in IP networks, leading Internet Switch and Router manufacturers have started development to integrate an LI Function directly into their devices.

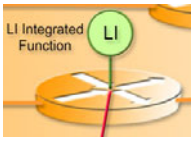


Figure 4. Integrated LI function

Advantages:

- More security as only the targeted data leaves the network
- No additional components within the network

Data Collectors

A Data Collector is a device used to intercept data from IP based networks, most notably the Internet.

They come in many forms but generally operate by passively tapping the traffic on a communications link and filtering an unobtrusive copy of the data for desired content. Only the filtered data is forwarded to the LEA.

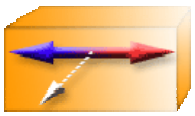


Figure 5. Data Collector

Advantages:

- Independence from other network components
- High data output rates

Load Balancing Techniques

Load Balancers can aggregate Ethernet based signals and distribute them to multiple Data Collectors based on load balancing and/or traffic filtering schemes. The Load Balancer ensures that data, which belongs to a unique session, is forwarded to the same connected Data Collector. In addition to aggregation and load balancing, pre-filtering of traffic can be performed based on an IP protocol and port qualifier (e.g. protocol TCP with port 25).

Interface/Protocol Mediation

With special components like Routers, transport protocols (e.g. Frame Relay, HDLC, ATM) can be removed. In addition, the IP traffic can be mediated from various electrical or optical transmission media (e.g. E3/T3, STM-1/OC-3, STM-4/OC-12) to Ethernet connections.

Mediation Device

The Mediation Device sits between the Data Collectors and/or the integrated LI functions on the network side and the LEMFs or Monitoring Centers on the Law Enforcement Agencies' side.

Figure 6. Mediation Device

Its purpose is to mediate requests for intercepted content by authorised entities and convert them into commands that are understood by the various Data Collector implementations and integrated LI functions in the networks. It must also understand the delivery protocols and mechanisms of the Data Collectors and the integrated LI functions and convert the intercepted data into a form suitable for delivery to one or more Law Enforcement Agencies.

Marking Terminals

Marking Terminals connect to the Mediation Device and are used by Operators to mark parts of the Internet traffic for interception by setting or defining targets/triggers.

Figure 7. IMS – Marking Terminal

The marking process specifies identifying aspects of Internet Traffic such as an IP address, an email address, etc. The targets/triggers are placed by the Mediation Device into the Data Collectors or integrated LI functions of the networks.

Law Enforcement Monitoring Facility (LEMF)

LEMF is the term used by ETSI to denote the application used by the Law Enforcement Agency to receive, analyse and archive intercepted data. The Monitoring Center (MC) from Siemens is such a LEMF and it is a typical representative of a system that receives intercepted data from the Mediation Device of the IPIS.

Figure 8. Law Enforcement Monitoring Facility

The MC is designed with a flexible architecture and can also be used to play the role of the Marking Terminal where this is allowed under a country's LI laws. It can receive and process

intercepted data from the Internet as well as from PSTN, Mobile, 3G and NGN networks.

GPRS and UMTS networks

In GPRS and UMTS networks, subscribers can be marked for monitoring of IP traffic by IMS systems. The Intercept Related Information (HI2) is transmitted via the IMS system to the LEMF while the Call Content (HI3) is transmitted directly from the appropriate network element to the LEMF. These transmissions are IP connections which can be based on various transport networks (e.g. Ethernet, ISDN, X.25).

For marked GPRS and UMTS subscribers, the whole IP traffic is intercepted and forwarded to the LEMF, regardless of the IP application used (Web, Mail, Chat, etc.). This traffic does not need to pass through the Mediation Device.

The Challenge of Rapid Evolution

No network has evolved as far and as fast as the Internet. Its constant change presents continuous challenges to the LI technology developers to keep pace with the communications applications being used in the Internet. As an example, the use of VoIP is spreading rapidly and presented its own challenges to LI technology. VoIP interception is now supported in the IPIS and MC.

Another evolution of the Internet is towards broadband and the consequent increase in amounts of data that the LEA must manage.

The Siemens VDR group is proactive and anticipatory in its analysis and development of technologies and architectures to address the constant change in Internet applications and mass data management. This is reflected in the range of protocols supported and the various load-balancing and data segregation techniques employed in the Siemens solutions.

Feature	Highlights
Direct Access capabilities	- 100 Mbps and 1 Gbps Ethernet electromagnetic taps - 1, 2.5, 10 Gbps Ethernet optical taps - E3 electromagnetic taps - STM-1/OC-3 and STM-4/OC-12 optical taps
Interface/protocol mediation	- E3 with HDLC to Ethernet - E3 with Frame Relay to Ethernet - E3 with PPP to Ethernet - STM-1/OC-3 Packet-over-SONET with HDLC to Ethernet - STM-1/OC-3 Packet-over-SONET with Frame Relay to Ethernet - STM-1/OC-3 Packet-over-SONET with PPP to Ethernet - STM-1/OC-3 ATM with AAL5 to Ethernet - STM-4/OC-12 Packet-over-SONET with HDLC to Ethernet - STM-4/OC-12 Packet-over-SONET with Frame Relay to Ethernet - STM-4/OC-12 Packet-over-SONET with PPP to Ethernet - STM-4/OC-12 ATM with AAL5 to Ethernet
Data Collectors	- Filtering of IP-based traffic according to various trigger criteria - High throughput rates
Interfaces to Integrated LI Functions	- Various, dependent on the vendor
Triggers	- E- mail (SMTP, POP3, IMAP4, Webmail) - Web/HTTP, FTP, IRC - VoIP - Keyword/String Search - IP Address - Instant Messaging
Mediation Device	- Supports numerous Data Collectors - Load Balancing - Supports multiple LEMF for delivery - Marking terminal - Access and marking security
Marking Terminal	- Remote locations - GUI for Trigger creations
VPN Devices (Optional)	- Secures the connection between Data Collector and Mediation Device when they are deployed in different locations as well as the connection between the Mediation Device and the LEMF. - Appropriate models can be supplied by Siemens but also dedicated customer equipment can be integrated on request if required by national legislation.

Abbreviation	Description
3G	Third Generation
AAL5	ATM Application Layer 5
AOL	America OnLine
ATM	Asynchronous Transfer Mode
E3	34.368Mbps ITU standard - Europe
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
H.323	ITU H series standard
HIx	Handover Interface
HDLC	High level Data Link Control
LI	Lawful Interception
ICQ	Chat protocol (Pronounced "I seek you")
IMAP4	Internet Message Access Protocol version 4
IMS	Interception Management System
IP	Internet Protocol
IRC	Internet Relay Chat
ISDN	Integrated Services Digital Network
ITU	International Telecommunications Union
LEA	Law Enforcement Agency

Abbreviation	Description
LEMF	Law Enforcement Monitoring Facility
MC	Monitoring Center
MS	Management Station
MSN	Microsoft Network
NGN	Next Generation Network
NNTP	Network News Transfer Protocol
OC-x	Optical Carrier - x
POP3	Post Office Protocol version 3
PPP	Point To Point Protocol
PSTN	Public Switched Telecommunications Network
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SONET	Synchronous Optical Network
SPAN	Switched Port Analyser
STM-x	Synchronous Transport Module - x
T3	44.736Mbps ITU standard - US
TCP	Transmission Control Protocol
UMTS	Universal Mobile Telecommunications System
UUS	Unified User Station
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
X.25	ITU-T standardisation for wide area communications

Contact:
Siemens Voice and Data Recording (VDR)
Sales Office Fax: +49 89 722 49801
VDR-sales.com@siemens.com

Voice & Data Recording
Hofmannstr. 51
D – 81379 Munich
Germany

Document number S41045-N691-B018-03-7629

GSM On Air,
Active, Passive & Semi Active
GSM Locating

Index

Active On Air GSM: GSM-XPZ – Overview

Designed as a tactical tool for law enforcement, Government agencies and the Military, the GSM-XP family of GSM active interception solutions have proven to be a global hit with proven success in the field.
MMI is proud now to provide preliminary specifications for its next generation solution. Based on commercial base-station technology this offers a quantum leap in mobile acquisition rate, higher transmit power, operational ranges and for the first time simultaneous operation on multiple networks and simultaneous servicing of multiple targets.

A range of products will be available targeted to provide an optimal solution for different mission scenarios. Key features include:

- Up to 50 Watts output power on 2 simultaneous channels
- Up to 4 simultaneous channels, allowing emulation of
- 4 broadcast channels on one network
- 4 broadcast channels on four different networks
- Dual band solutions covering 900/1800 or 850/1900 MHz and for the first time
- a world box providing 850/900/1800/1900MHz capability
- Real time monitoring and intercept of up to 4 simultaneous calls
- Integrated antenna switch on the vehicle models
- Capability to service multiple targets – up to 7 targets per carrier
- Ruggedised carry-case
- Multiple form factors to cover different operational scenarios

Model Variants

Three variants will be available:

- GSM-XPZ-PV (Vehicle model)
- GSM-XPZ-HP (Highly Portable model)

GSM-XPZ-PV: The vehicle model is designed for customers with an 'in-country' requirement, i.e. operation within their own borders. The system may require a vehicle installation which will be performed in-country by qualified MMI representatives.

The nature of the installation allows the system to transmit up to 50 Watts which when added to the improved receive sensitivity and channel equalisation dramatically extends the range. In addition the system will support multiple channels simultaneously to a maximum of 4 channels within the unit. The PV system is supplied with a bench top power supply to allow normal use when not installed into a vehicle.

GSM-XPZ-HP: A new model variant this is designed for customers who wish to operate discretely close to the target. Packaged into a small case, such as a briefcase, the system can be easily used in public places without alerting targets.
In addition the system will support multiple channels simultaneously to a maximum of 2 channels within the unit. The highly portable variant will be able to transmit up to 250mW in 2 channels configured either as 900/1800 or 850/1900 variants. The antennas will be integrated with there an option to add an external Power Pack to increase transmitted RF power.

Features

Generic Features for GSM-XPZ-PV systems

- Ability to adjust BTS power to a maximum 50W
- Ability to transmit 4 GSM broadcast channels simultaneously
- Enhanced IMSI acquisition rate (theoretically to 60 registrations per BTS per second)
- Intercept of 4 outgoing target calls simultaneously.
- Perform a Blind Call per GSM timeslot = 7 blind calls simultaneously per channel
- Up to 28 Simultaneous Blind Calls whilst IMSI Grabbing
- Advanced manipulation of BCH data to ensure better phone retention (once locked)
- Ability to survey spectrum using custom phone modules
- Display of SERVER & 6 neighbouring cell information to enable simple cell emulation

- Ability to adjust target mobile power once in a call to maximum 2W transmission
- Visual indication of RX power lev (mobile reporting BTS received signal strength)
- Advanced configuration of BTS for emulation of any network type
- Off-line mode for mission file viewing
- Powerful database search facility for quick target identification
- Multiple antenna management using In-built antenna switching circuitry
- Remote system operation via wireless link

Control Options

To provide users with maximum flexibility a range of control options is available; direct Ethernet connection to the controlling laptop; wireless connection using a suitably enabled device e.g. PDA, Laptop etc. In this mode multiple users will be able to connect and view the following information over a secure connection:

- Target Identification – included as standard
- Voice Intercept (only available on PV variant)
- SMS Intercept
- Direction Finding support
- Service Denial
- Bubble mode

The operator will be able to adapt the Graphical User Interface (GUI) to display the key information. The GUI will build on the familiarity of the existing GSM-XP to allow both novice and experienced users the control to easily simultaneously operate 4 basestations.
To enhance security, mission data is stored on an external memory device. This can be easily switched between multiple systems, or used to examine mission data offline on a separate PC or on the GSM-XPZ itself. This also allows for protection of mission data, should the system have to be loaned to other organisations or returned to MMI. All events as per current GSM-XP operation will be time stamped and logged in a mission file along with intercepted Voice/SMS data. To maintain the integrity of the data the mission files cannot be edited or recorded voice replayed without using MMI software.

Operational Modes

Research & Release	Allows phones from up to 4 networks to simultaneously attach to the GSM-XPZ enabling their IMSI / IMEI to be logged. Once logged, they are released back to the real network - the most covert operational mode.
Research & Lock	Locks selected target phones to the GSM-XP BTS Ping Mode Clones the selected BTS exactly including LAC. A much quicker and more efficient way of capturing mobiles as it removes the overheads associated with a location update – the least covert operational mode.
Bubble Mode	Unless otherwise specified all phones registering to the system will be locked to the system thus creating a bubble of phones restricted from accessing the real networks.
Service Denial to all Hostiles	Sends a service denial message to all phones, potential hostiles, that prevents them from rejoining a real network.
Exclusive Network	Allows friendly phones to use the XPZ as a means to covertly contact other operatives. Calls made in this way do not use the real network and are therefore secure.

Target Mobile Actions

Overt Call	Allows operator to call a target phone and optionally converse.
Blind Call	Covert (silent) call to a target phone. Used in conjunction with directional finding equipment.
Send SMS	Allows operator to send SMS to a target phone.
SIM Swap Indication	Shows indication of SIM swap.
Make Target	Allows operator to make a phone a target.
Invalidate Target	Allows operator to deny service to a selected target.
Make Reject	Allows operator to reject selected phones from the GSM-XP to prevent any interference by the system.
Show Target	History Shows all recorded activity by the target phone.

Technical Specifications

The specification will vary depending upon the model purchased however the key specifications are presented below:

Radio Interface

Transmit/Receive Frequencies:	Euro Variant: E-GSM, GSM, DCS US Variant: 850 , PCS Quad Variant: 850, E-GSM, GSM, DCS, PCS
Channel Frequency:	200 KHz
Output Power:	PV up to 50W per band HP up to 250mW per band
Receive Sensitivity:	>-95dBm (RAKE receiver).

GSM/GPRS Functionality

Channel Capability:	
TS0	FCCH, SCH, BCCH, CCCH, SDCCH/4, SACCH/C4 TCH/F+FCCH/F+SACCH/TF
TS1-7	SDCCH/8, SACCH/C8 TCH/F+FCCH/F+SACCH/TF
	Call Control Capabilities: BS Originated Call (Covert or Alerting), MS Originated Call (BS Terminated or BS Extended onto real Network), MS Camp on, MS Camp off, BS Call Disconnect, MS Call Disconnect
Hopping:	No
Electrical MMI:	Ethernet
Speech Encoding/Decoding:	Full Rate speech (FR) GSM06.10
MS Power Level Control:	GSM900; 5 to 19, GSM1800; 0 to 13.
SACCH MEAS Results:	RXLEV, Timing Advance.
SMS Point-to-Point:	Mobile Originated, BTS Originated

General Specifications

Size:

PV -	200mm (H) x 500mm (W) x 580mm (D)
HP -	70mm (H) x 280mm (W) x 290mm (D)
Weight:	PV < 28 Kg (55lbs) HP < 4.5 Kg (10bs)
Operating Temperature:	-5° C to +45°C (23°F to 113°F)
Storage Temperature:	-10° C to +70° C (14°F to 158°F)

Power Consumption

GSM-XPZ-PV	600W
GSM-XPZ –HP	40W

Power Supply

GSM-XPZ-PV	24 Vdc
GSM-XPZ -HP	2 x Li-Ion Batteries (300Wh approx 8 hrs) or 12 Vdc input

Interface Connectors

GSM-XPZ-PV	Antennas via N-Type connectors: 2 x 900MHz, 2 x 1800MHz, 2 x combined 900/1800MHz connectors for Omni-directional antennas. Data/Audio Interface via Ethernet Secure Wireless WPA (Optional)
GSM-XPZ-HP	In-built 900/1800MHz Omni-directional antennas. Data Interface via Ethernet Secure Wireless WPA

Active On Air GSM: GSM Mobile Tracer & Locator
(GSM-MTL3)

Description

The GSM-MTL3 enables reception of IMSI and IMEI from mobile phones within its reception area. The device is applicable to all GSM networks of the world. Additionally, in connection with the Mobile Finder GSM-MF, the GSM-MTL3 version provides pinpoint localization of mobile phones. Interferences with public networks are generally avoided through complete implementation of the GSM protocol and a specific processing. A preceding automatic network analysis sets up ideal adjustment of the system and, thus, ensures uncomplicated operation of the GSM-MTL3.
By means of an optional Portable Analyzer GSM-PA (PDA with Bluetooth measuring mobile phone), the concealed remote analysis is also possible in the near of target mobile phone. Thus, the time-consuming manual analysis and adjustment of the network structure will not be necessary.

According to special demands, a more extensive network analysis and manual processing of GSM parameters may be conducted as well.

Operation of GSM-MTL3 occurs through a wireless control and administration unit via HF transmission path (also with optional battery pack.)

Operating modes are as follows:

- IMEI / IMSI are read out; telephone is released into real network; another log-on to the GSM-MTL3 will only be possible, if LAC is changed
- IMEI / IMSI are read out; telephone is released into real network, but cannot be back posted into real network, i.e. mobile phone can be locked by GSM-MTL3
- GSM-MTL3 holds onto a certain mobile phone; communication is prevented on purpose; this operation remains unperceivable for mobile phone
- GSM-MTL3 holds onto a certain mobile phone; after establishing silent call, localization can be carried out by means of the GSM-MF

Collected data will be stored in a SQL data base within the control and administration unit. The data can be analyzed offline and exported to other applications.

Technical Data

Frequency range:	Downlink:	GSM900	925 MHz – 980 MHz
		GSM1800	1805 MHz – 1880 MHz
			optional GSM 850 / 1900 MHz
	Uplink:	GSM900	880 MHz – 915 MHz
		GSM1800	1710 MHz – 1785 MHz
			optional GSM 850 / 1900 MHz
Output power:		10 mW – 3 W (other power ranges on request)	
Input sensitivity:		ca. –90 dBm	
Mobile – power control:		GSM900/850 GSM1800/1900	3 mW – 2 W 1 mW – 1 W
Measurement reading:		RXLEV, RXQUAL (mobile phone) RX level (GSM-MT(L)3)	
Power supply:		12 V DC (230 V AC with external adapter)	
Connections:		4x SMA socket, 1x 12VDC socket	
Remote control:		HF transmission path 433MHz / 150 mW	

Scope of Delivery:
- Pilot suitcase with GSM-MTL3 and 2x dual band patch antennae
- Control and administration unit
- HF radio module with USB connection
- 230 V AC/12 V DC adapter
- GSM-MF Mobile Finder
- Software
- User's manual

Options:
- GSM-PA Portable Analyzer (Model No. 580 200 0009)
- GSM-MF Mobile Finder (Model No. 580 200 0008)
- GSM-PNF (Model No. 580 200 0010)
- GSM-NA (Model No. 580 200 0011)
- Battery pack (rechargeable)
- External antennae (see catalogue, product line 160)

Active On Air UMTS: 3G-FD Overview

The introduction of the next or 3rd Generation mobile means the criminal/terrorist is now able to communicate securely, safe in the knowledge he is highly unlikely to be intercepted. The accelerated global take-up of this service now presents a major security threat. The 3G-FD, a complementary product to the GSM-XPZ, significantly extends the capabilities of MMI's portfolio of 3G products. Using the 3G-FD, it will be possible for the first time to acquire the identity of a UMTS (3G) mobile phone, natively in 3G.
Building on the impressive capabilities of MMI's current product range, the 3G-FD will support working in tandem with the GSM-XPZ, where a single GUI will allow control of both systems. This will allow a user to simultaneously acquire identities of both GSM and 3G phones and to display this and other information in a real-time converged database.
When working in tandem with a GSM-XPZ it is possible to acquire a phone in 3G and then force the target mobile to move onto the GSM-XPZ cell and simultaneously setup a Blind Call. Once this has been done, all the features available on the XPZ can be used on the phone. The MMI technology uses standard 3GPP techniques to achieve this function and therefore has full control over the target mobile phone during handover from 3G to 2G.

MMI's native 3G technology is unique in the marketplace. The technology enables control of target mobile phones and normal rejection of non-target mobile phones all on 3G. Unlike a jamming solution, non-target 3G mobile phones are caught on 3G and then allowed to continue to use their normal 3G network.

A range of products will be available targeted to provide an optimal solution for different mission scenarios.

Key features include:

- Based on industry standard components compliant to 3GPP standards (R99)
- Up to 20 Watts output power
- Single channel, allowing emulation of a single UMTS cell
- Covers UMTS Band I
- Operation in tandem with GSM-XPZ PV
- Over 30 man years development

3G-FD Features

Generic Features
- Ability to adjust NodeB power from 1mW to a maximum of 20W
- Ability to transmit a 3GPP configured UMTS cell
- Covert 3G native IMSI acquisition
- Fast UMTS cell configuration using optional MMI 3G Spectrum Scanner
- Advanced configuration of Node B for emulation of any network type
- Unified database for display of 2G and 3G mobile phones
- Identification whether mobile phone is caught on 2G or 3G
- Off-line mode for mission file viewing
- Powerful database search facility for quick target identification
- Remote system operation via wireless link
- Mobile phone "3G icon" remains on 3G

Operation modes
- Native 3G Research and release
- Native 3G Push specific target mobile to GSM-XPZ and instantly Blind Call
- Network Survey using optional MMI 3G Spectrum Scanner

Technical Specifications

The specification will vary depending upon the model purchased however the key specifications are presented below:

NodeB Module
Output Power: From 1mW to 20W
Frequency Range: UMTS Band I
Downlink 2110 to 2170 MHz
Uplink 1920 to 1980 MHz

General Specifications

Dimensions 200mm (H) x 500mm (W) x 580mm (D)
Weight: FD <36 Kg
Operating Temperature: 0 degrees C to +45 degrees C
Storage Temperature: 0 degrees C to +70 degrees C
Power Consumption 600 W maximum
Power Supply 24 V

GSM-Vehicle Direction Finding (GSM-VDF)

General Overview

The VDF is a lightweight, portable and state of the art digital direction finder for tracking and geo-locating GSM cell phones. The VDF features the latest Super Resolution DF processing algorithms.

The VDF is a standalone system designed to work with any GSM manipulation system on the market today.
Map integration is made easy thanks to an ESRI compliant GIS Mapping engine.

Main Features

- DF on ARFCN and Timeslot in 'Slotted' mode for increased accuracy when using GSM-XPZ
- DF on ARFCN in 'Non-Slotted' mode
- DF simultaneously in Azimuth and Elevation

- Robust, low profile lightweight antenna unit
- 8 element spatially diverse omni-directional antenna array for highly accurate target resolution
- Antenna unit designed for covert internal or external mounting
- User friendly Graphical User Interface (GUI)
- ESRI GIS Mapping engine capable of supporting multiple map formats
- Bearing Direction given in relation to North and vehicle heading
- Integrated GPS and Electronic compass for non moving Line of Bearing (LOB) resolution
- Recording & Playback of LOBs and mission Data
- Geo-locate targets to within a few meters
- A dual band digital receiver featuring 8 self calibrating phase synchronous digital receiver branches
- Highly stable Rubidium reference for long term tracking of time slotted GSM signals.

Key Specifications

Function	Provides RF signal strength indication on a selectable RF channel
Channel Range	GSM 900/1800 ARFCN 975-1023, 0-124. 512-885
Direction Finding Axis	Simultaneous in Azimuth and Elevation
Resolution	Better than 5°
Accuracy	Better than 5°
Sensitivity	Typically -120dßm
DF Algorithms	Super Resolution DF with self calibration
VDF Receiver	W 448mm x H 135mm x D 348mm 7.2kg
VDF Antenna	W 270mm x H 60mm 1.3kg
GPS Datum	WGS-84
Magnetic Compass	2 Axis tilt compensated digital compass
Power Supply	12Vdc, 7.5A, 90W (Rubidium reference cold) 12Vdc, 4.5A, 54W (Rubidium reference warm)
Antenna (in-vehicle)	Azimuth 360°, Elevation (as per vehicle aperture)
Antenna (rooftop)	Azimuth 360°, Elevation 80°
Mapping Formats	MxD Files supported

Further information available on request.

Direction Finding: GSM-XP-HHDF Overview

The GSM-XP-HHDF, a complementary product to the GSM-XP-DBDF, significantly enhances GSM-XP operational effectiveness when locating targets.

A highly unique design the GSM-XP-HHDF dramatically enhances the ability of the user to operate in new scenarios with a level of covertness previously considered not possible. The benefits to the user are:

- operate within buildings
- direction find targets to within a few metres
- small in size can be worn within a shirt pocket
- audio and visual target indication
- ability to change RF channel in the field
- minimise operational time within the danger zone
- requires only standard AA batteries

GSM-XP-HHDF Features

The GSM-XP-HHDF is designed to work in conjunction with both the GSM-XP-V and GSM-XP-R systems. Available in 2 options, supporting either the GSM-XP 918V/R or GSM-XP 819V/R, location finding of a radiating target mobile can be performed in conditions where vehicle deployment is not possible.

The key features of the GSM-XP-HHDF are:

- small in size
- simple yet flexible user interface.
- LED indication to show received signal strength
- audio indication
- squelch control to allow sensitivity adjustment
- volume control
- vibration alert
- dual band operation
- RF selectability in the field
- RF channel indication
- range of external holders for covert mounting
- capability for wireless loop attachment to enable highly covert operation

GSM-XP-HHDF Specifications

The specification of the GSM-XP-HHDF unit will vary depending upon the model purchased. Two options are available:

- GSM-XP-HHDF-918 is a 900/1800 MHz variant
- GSM-XP-HHDF-819 is a 850/1900 MHz variant

Function

Function: Provides RF signal strength indication on a selectable RF Channel

Operational Modes:	LED signal strength indication only Audio signal strength indication only LED and audio signal selection
Channel Range:	GSM-XP-HHDF-918: ARFCN 975-1023 , 0-124 , 512-885 GSM-XP-HHDF-819: ARFCN 128-251, 512-810
Channel Selection:	ARFCN selectable from GUI across channel range pplicable to the Option
Interfaces:	On/Off Volume control Mode/Channel Selection Antenna connector (SMA) RF sensitivity adjustment (squelch) USB (for future function)
Power Supply:	2xAA Batteries
Antennas (supplied):	Dual band monopole Dual band rectangular patch

Radio Performance

RF

Receive Sensitivity: >-typically -97dBm

Frequency Range (GSM-XP-HHDF-918):
880MHz to 915MHz (GSM900 Uplink)
1710MHz to 1785MHz (GSM1800 Uplink)

Frequency Range (GSM-XP-HHDF-819):
824MHz to 849MHz (850 Uplink)
1850MHz to 1910MHz (1900 Uplink)

General Specifications

Size:	90mm (H) x 65mm (W) x 28mm (D)
Weight:	140g
Operating Temperature:	0 degrees C to +50 degrees C
Storage Temperature:	-20 degrees C to +75 degrees C
Power:	2xAA cells
Battery Life:	typically better than 10 hours (dependent on usage)

Direction Finding: GSM Mobile Finder (GSM-MF)

User's Manual

General Description

In connection with the GSM mobile tracer & locator (GSM-MTL3), the GSM mobile finder (GSM-MF) enables pinpoint localization of mobile phones.

The device provides 50 reception channels for selection of an unassigned frequency. The wide range of its reception dynamics (-100 dBm to +7 dBm) ensures localization of both adjacent and distant mobile phones. An especially designed aerial enables systematic direction detection and, thus, a rapid approach to the sought mobile phone.

The compact design of the device ensures concealed operation.

Absolute reception field strength of the respective channel is shown on a display (1 dB steps).
Relative field strength is signaled through changing tone pitch or intermitted sound.

Getting started

Settings

Default settings of the GSM-MF are realized via the menu system (*see0*

MENU).

Use the following keys:

[M]	Retrieve menu and submenus
[▲]	Select menu functions or menu values
[▼]	
[S]	Save and close menu

Direction finding

Select a free traffic channel and put the mobile device into transmission mode (e.g. silent call). This can be realized by means of the GSM Mobile Tracer & Locator GSM-MTL 3 or any other suitable device.
Adjust the selected traffic channel on the GSM-MF and localize the target through directing the aerial to the maximum signal level. Thereby the absolute reception field strength will be shown on the display. Relative field strength is signaled through changing tone pitch or intermitted sound (according to audio settings).

MODE MENU

Manual mode (hand)
In manual mode, a reception level, which has to be within the preset range of the measuring window, corresponds to the respective audio signal or intermitted sound. Thus, increase and decrease in reception field strength can be discerned.

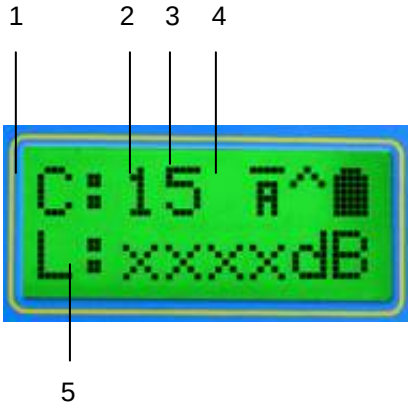
Automatic mode (auto)
In automatic mode, the strongest audio signal or intermitted sound is constantly synchronized on the highest reception level measured. Audio signals or intermitted sound will decrease at lower reception levels. Therefore, optimum position of the aerial has to be controlled constantly.

SET menu
Change of audio signal or intermitted sound is realized for one adjustable measuring window each. If the reception level is above or below the sensitivity level set for the measuring window, further changes of the signal will not occur. To continue direction finding, adjust settings for the measuring window accordingly.

Manual adjustment of measuring window (hand)
Press the "S" key [12] to select either the medium audio signal (manual mode) or the maximum value (automatic mode). Instead of the "S" key [12], the remote control, which is included in the scope of delivery, may be equally used.

Automatic adjustment of measuring window (auto)
In SET menu's automatic mode, the medium audio signal (manual mode) or the maximum value (automatic mode) is selected automatically, when the lower or upper limit set for the measuring window is reached.

DISPLAY



1	traffic channel
2	operating mode
3	set limit for measuring window
4	battery status
5	absolute reception field strength

Technical data

Frequency range:	GSM-Channel 1: 890.2 MHz … GSM-Channel 50: 900.0 MHz	(Steps of 200kHz)
Sensitivity:	approx. –100 dBm	
Power supply:	9 V battery block	

Scope of delivery: GSM-MF, LogPer-antenna HyperLOG 7025, GSM Body worn DF antenna, headphones, remote control unit, 9 V battery block, user's manual

Appendix

TOOLS

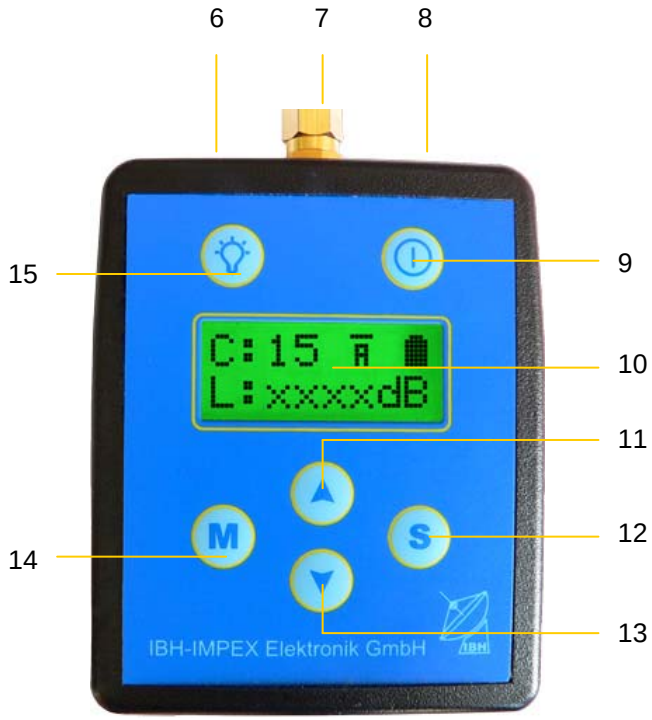


fig. 1: tools

6	remote control connection
7	aerial connection
8	headphones connection
9	ON/OFF switch
10	display
11	volume control / menu select
12	SET / close menu
13	volume control / menu select
14	open menu
15	display lighting ON/OFF

MENU

	menu	submenu	function
1	**TCH**		select traffic channel
2	**Audio**	***Sound***	signal field strength through audio signals
		Pulse	signal field strength through intermitted sound
3	**Mode**	***Hand***	reception level corresponds to respective signal
		Auto	set measuring window to maximum value automatically
4	**Range**	***Short***	set measuring window to approx. 15 dB
		Large	set measuring window to approx. 30 dB
5	**Speed**	***Slow***	change response speed of direction finding signal
		Fast	
6	**Set**	***Hand***	select medium audio signal (hand mode) or maximum value (auto mode) manually
		Auto	select medium audio signal (hand mode) or maximum value (auto mode) automatically, when reaching lower or upper limit set for the measuring window
7	**Contrast**		display settings
8	**Calibration**		reserved for default settings

Passive GSM Monitoring System: Falcon D+

1. General Definition of Purpose

The System is designed for surveillance tasks and monitoring of telephone conversations within the GSM 900/1800 networks. The system provides the option of both stationary and mobile operation.

2. Technical data

The system ensures monitoring of audio and data traffic within standard GSM 900/1800 networks:

- Without application of encryption algorithms
- Application of encryption algorithm A5/2 [real-time] (decoding time: 0.01 sec.)
- Application of encryption algorithm A5/1 [real-time] when Ki is known
- Default configuration of the system - 8 reception channels
- The system ensures registration of radio-electronic circumstances within the radio cells to be monitored (frequency and characteristics of BCCH-channels)
- Channels to be monitored are, according to task, manually selected by the user
- The system contains a database (up to 100,000 calling partners), operating in real-time, which can be accessed corresponding to the selected search criteria and parameters
- Calling partners are identified according to the IMEISV, IMSI, TMSI, ISDN number (local and international number)
- Assessment of presence of calling partners to be monitored and identification of specific parameters (TMSI) occurs automatically by means of a mobile phone with special software. The special software is contained in the scope of delivery
- Registration and storage of telephone conversations occurs on system's hard disk

- The system ensures registration and storage as audio codec - types FR, EFR, HR
- Playback of recordings may be carried out by the system itself (CoolEdit-Software)
- Identification of SMS and DTMF data

System's coverage:

- Down-Link - up to 10-km
- Up-Link - up to 500-m in city
- Assessment of coverage between calling partner and base station; accuracy of up to 550-m
- Delivery format: in a special PC casing and Notebook
- Operation System software: Windows XP

3. Scope of delivery

The System main components:

- PC Pentium 4-1.7 GHz or higher, 2 GB RAM, 80 GB HDD
- Circuit board with main generator and power supply module for receiver
- Circuit board with 8 duplex-channel receivers
- Circuit board with main processor ADP6201PCI for digital signal processing
- Data input module ADM214x10MX
- Antenna system with integrated amplifier
- Notebook with LAN interface and cable
- Special software for analysis and evaluation
- User's manual
- **Optional**: Mobile telephone with special function for assessment of calling partner's presence within the monitored GSM-cell (Ping-Handy)
- **Optional**: Mobile telephone with Net monitor

4. Technical operating conditions

Technical data and operating conditions

In order to avoid destruction of the system, pay attention to the following:

- Power source (type and voltage) must correspond to PC power supply!
- Ambient temperature and humidity must comply with the operating standards of the respective device!
- The system must not be operated and/or stored in rooms that contain dust, acid, alkali and corrosion gas!
- No operation under conditions which might lead to unfavorable mechanical, chemical, or atmospheric influences!
- Do not expose the device to heavy vibrations!
- When the device has been exposed to low temperatures, do not turn it on immediately! Minimum temperature must be reached first; perspiration water must evaporate
- When the device has been exposed to extreme conditions (storage, transport), it must "acclimatize" under optimum conditions for at least 2 hours

5. Description and function of the System

Preparing the system for use
Make sure the device is not damaged. If, however, there is anything of concern, please contact the manufacturer.

Security advice
Make sure the power source complies with the specifications of the PC's power supply before connecting the device to the mains supply.
Do not shut the louvers of the device!
The device must be turned off before any alterations in configuration are carried out.
Alterations on the system require approval of the manufacturer!
Do not use the antenna close to power transmission lines!
Do not use the antenna close to transmission antennas!

Installation for the System
Note: For installation of software direct on The System Controller, you need an external monitor, mouse and keyboard. If LAN connection is working you can setup by Notebook client (remote controlled).

Installing the driver for ADP6202PCI module
Install the driver by means of the standard tools of the system software. The driver Adp6201a.sys is found in the installation file THE SYSTEM Adp6201 Driver.
Restart your The System Controller after successful installation!

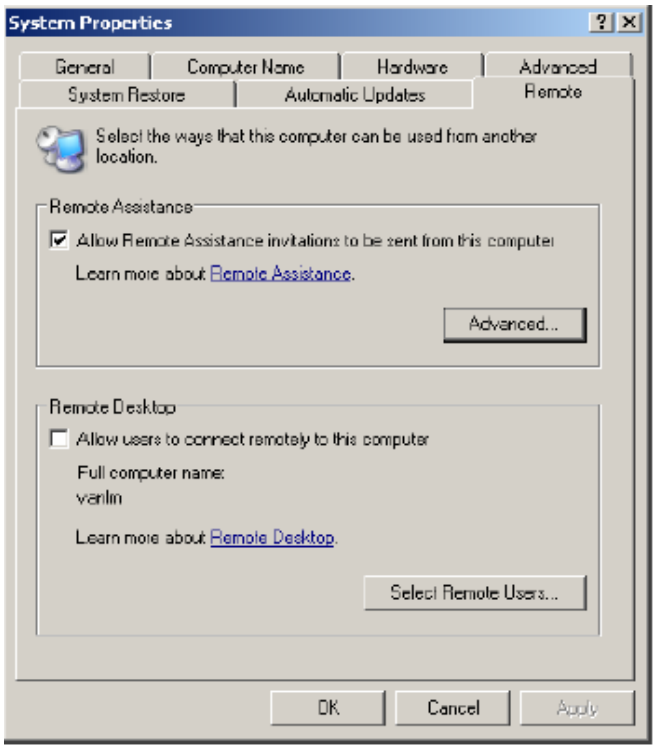
Installing the System
In order to install the software, activate setup.exe from the installation file The System. The installation assistant guides you through the selection of files and software configuration. You may install the full version by choosing the installation option Typical. On successive "starts", the setup.exe program allows complete or partial reinstallation of the software. On system installation a single user (root) will be created, who has no password or administrator's rights. The system will be assigned the IP-address 127.0.0.1 and a database GSM39 will be created. Restart the system after successful software installation!

To Install USB Cable driver for connection of the PING-mobile phone (If in delivery scope), connect the PING-mobile phone to the system using the USB cable and install the driver using the enclosed CD.

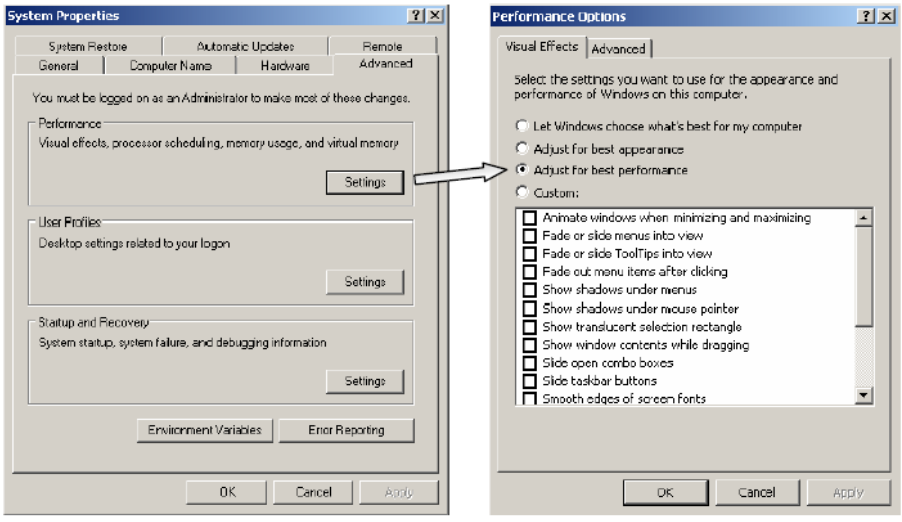
Installing the software on Notebook client

Before installation, please check some parameters in your Notebook client PC as follows:

- Right mouse click in My Computer on desktop PC and select properties. Select Remote window and set parameters as below:

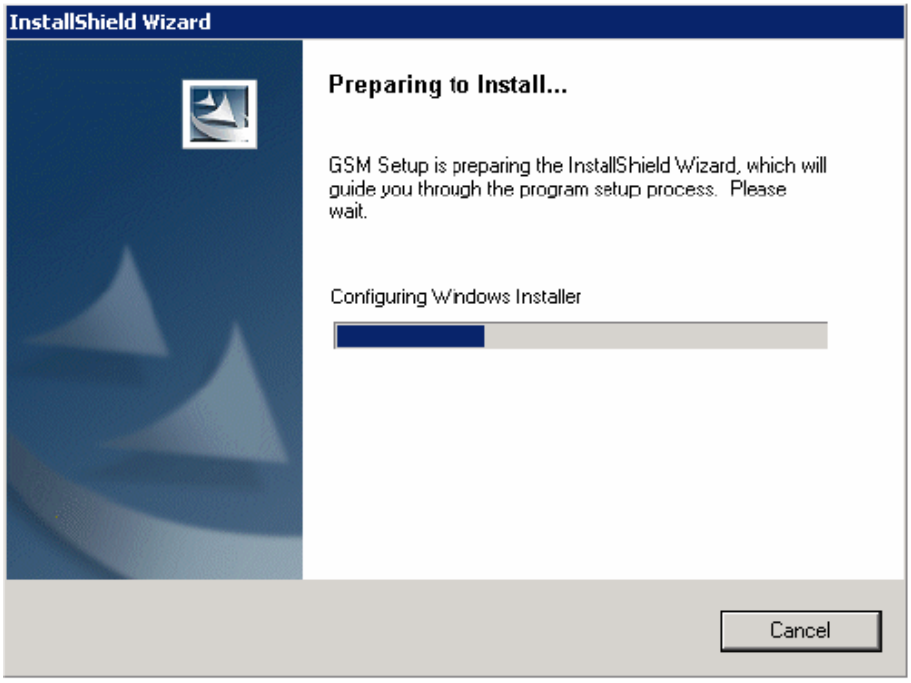


Select Advance window. In "Performance" press Settings button to set parameters as below:

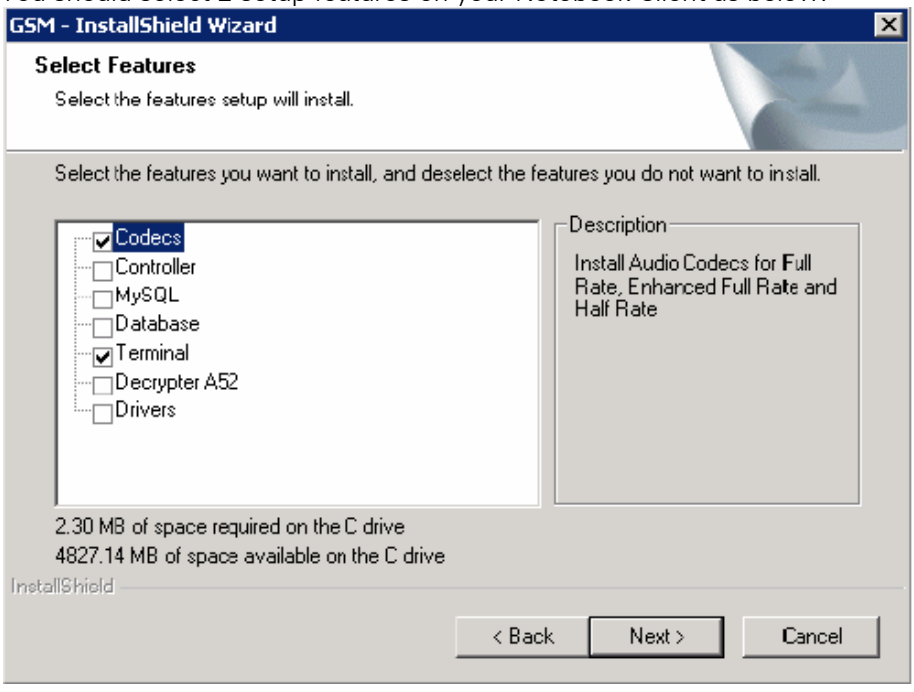


Now you can install software The System on your Notebook client.

In order to install the software, activate setup.exe from the installation file The System. The installation assistant guides you through the selection of files and software configuration.



You should select 2 setup features on your Notebook Client as below:



On successive "starts" the setup.exe program allows complete or partial reinstallation of the software. On system installation a single user (root) will be created, who has no password or administrator's rights. Database GSM39 will be created.

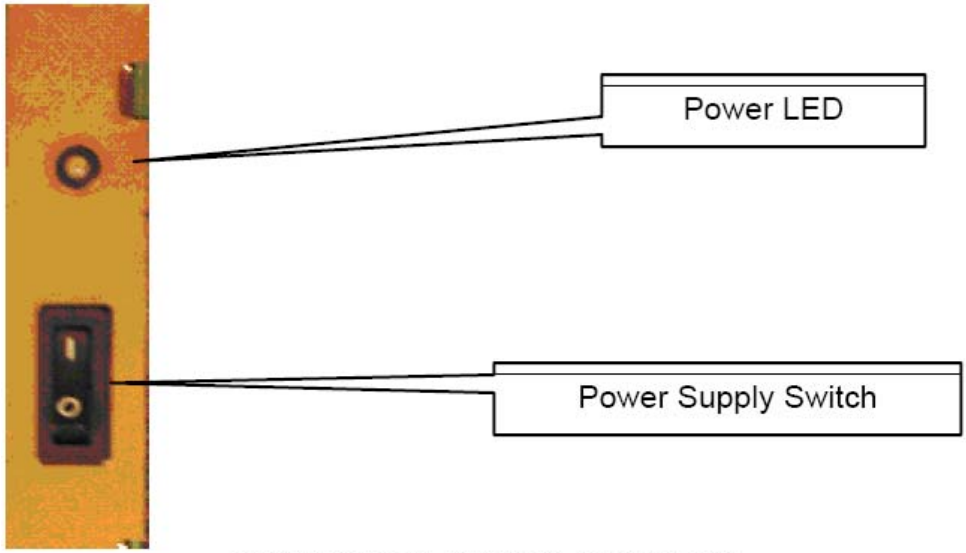
Restart the Notebook client after successful software installation!

Preparing the system for use
Connect network cable (LAN cable) from Notebook client to The System Controller.

Note: Cross over cable can be connected from The System Controller direct to Notebook client. Normal cable connection can be used for connection from The System Controller to Notebook client by means of Hub or Switch.

Connect the antenna cable to the BNC socket on the rear side of the THE SYSTEM Controller.

If you have ordered the optional Ping-Mobile phone, then connect the Ping-mobile phone to the COM or USB socket of the THE SYSTEM Controller. An extension cable (USB) can be used so that mobile phone and antenna are suitably apart from each other
Connect the power supply cable to the mains supply; then, turn on the THE SYSTEM Controller. Green LED: hardware is ready for use. Red LED: Turn off hardware's power supply; wait for about 10 seconds and turn it on again. If LED is red again, turn off power supply and contact the manufacturer
Hardware of the THE SYSTEM Controller is ready for use after approximately 10 minutes of warming



Power Supply Switch & Power LED

The figure below shows operation of the THE SYSTEM Controller in Decoder and Controller mode. The 2 positions of the decoder mode (Loader A52) are as follows:

- **Green**: calculation data are loaded in main memory
- **Red**: loading process is running

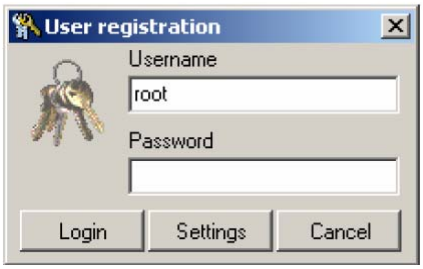
- Turn on Notebook client after startup completed, double click on "Terminal" Icon on Desktop

Note: The first time running "Terminal", please select correct server's name and Database (GSM39) as below:

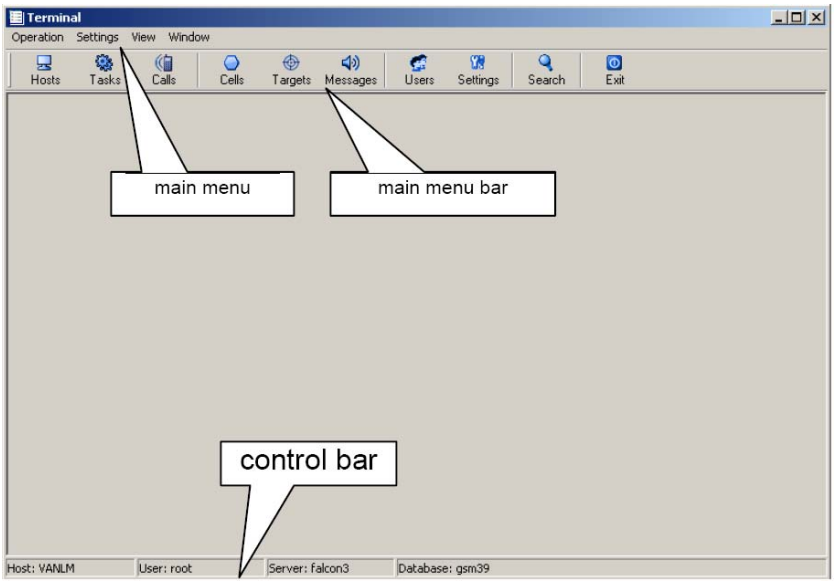
Starting the System
Be sure that **The System Controller** and **Notebook client** are completed at startup.

Double click on the Icon "Terminal" (on desktop Notebook client) to start the system. Enter a name and password into the dialogue box (as figure below).

Select a database in the **Settings** file.



On first starting, you can interrupt the starting process by pressing **Esc** button.
After the loading process the menu window **Control center** will appear on the screen.

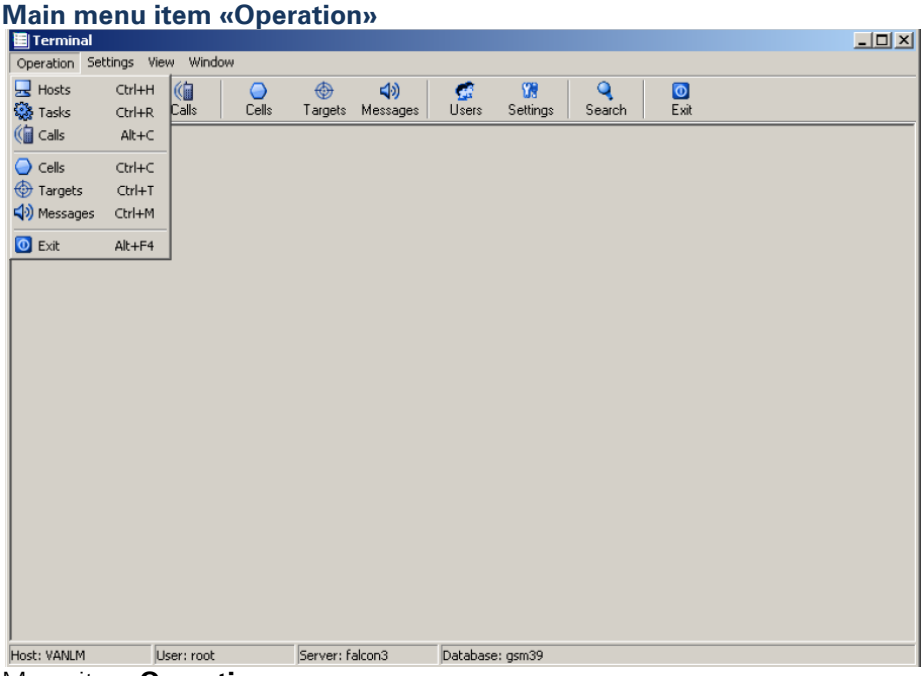


Main menu operation.

Operating the «THE SYSTEM» system

Main menu items

Main menu item «Operation»

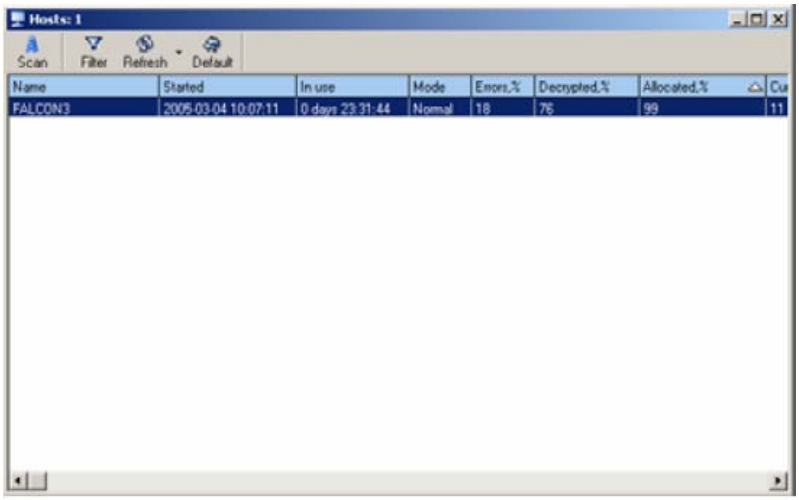


Menu item **Operation**

Menu item <Hosts>

The menu item **Hosts** will show you one or more Hosts in the system you have. THE SYSTEM system can have one or more Hosts receivers. In this menu there is more information relative to GSM network and THE SYSTEM receiver. Open the menu window **Hosts** from the main menu **Operation > Hosts** or click the icon 

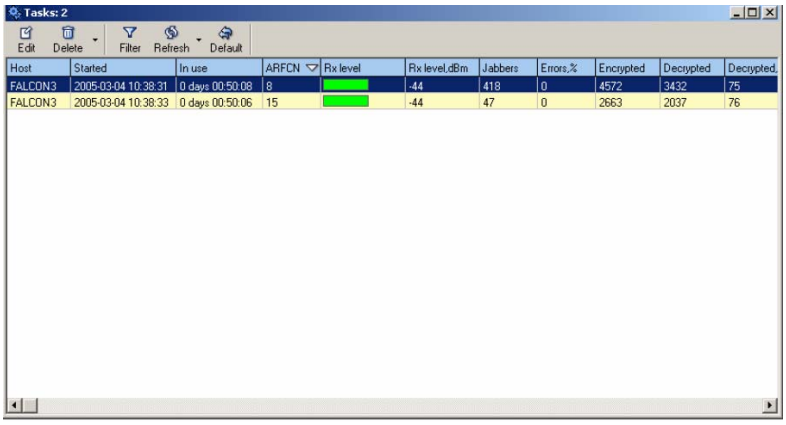
on the main menu bar.



Menu item <Tasks>

In this menu, you can see the **tasks** of the receiver, the Channel monitored, the Rx level, and the percentage of decrypted.
Open the menu window **Tasks** from the main menu **Operation > Tasks** or click the icon 

on main menu bar.

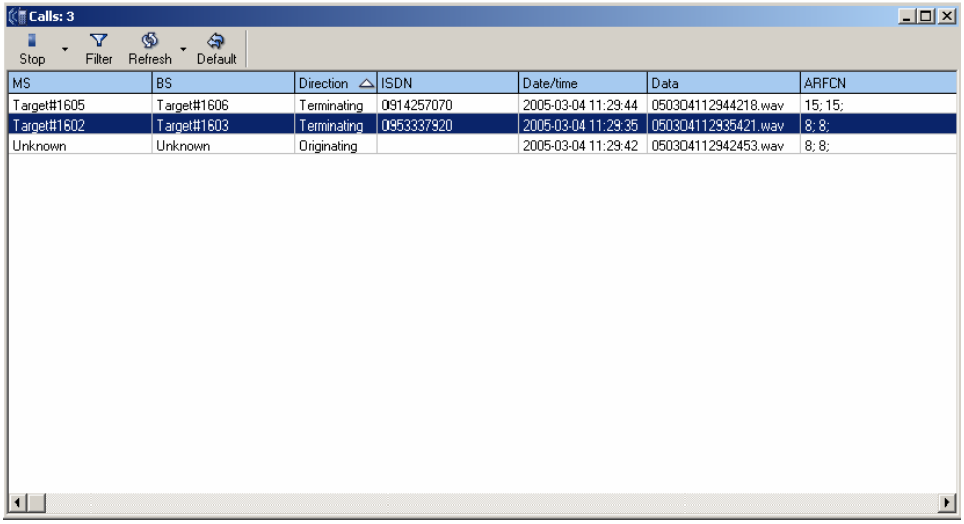


Menu item **Task**

Menu item <Calls>

Menu item **Calls** serves for live listening in higher priority.
Open the menu window **Calls** from the main menu **Operation > Calls** or click the icon 

on main menu bar.

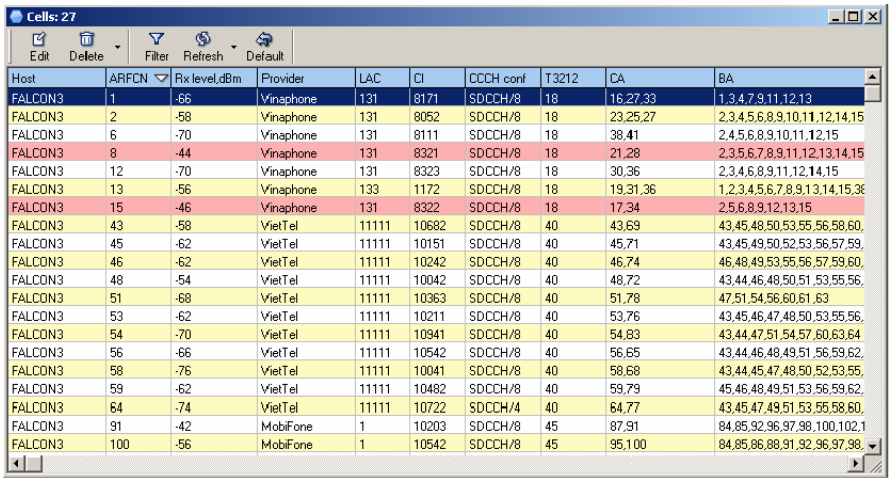


Menu item **Calls**

Menu item <Cells>

The menu item **Cells** serves for network provider, base station, channel number...
Open the menu window **Cells** from the main menu **Operation > Cells** or click the icon 

on main menu bar.



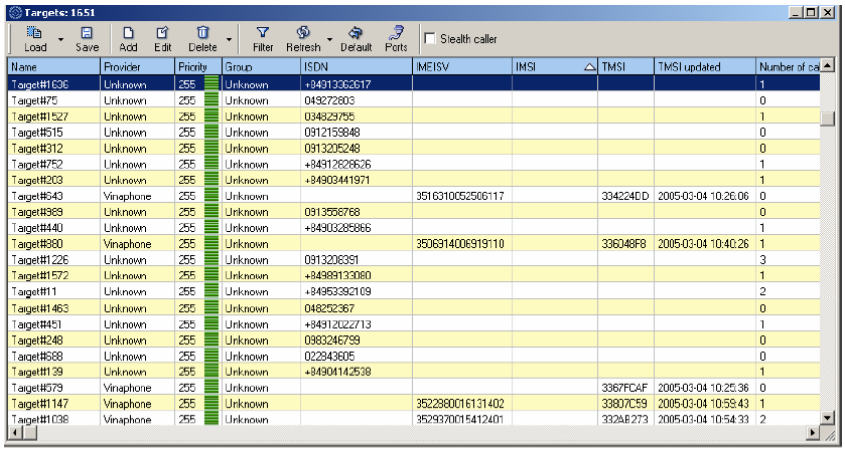
Menu item **Cells**.

Menu item «Targets»

The menu item **Targets** retrieves a list of the target files to be monitored and edited that have been stored in the database. Furthermore, in this menu there is an automatic search for targets within the radio cell to be monitored.

In order to retrieve the **Targets** window, either select **Operation > Targets** from the main menu, or click the icon 

on main menu bar.



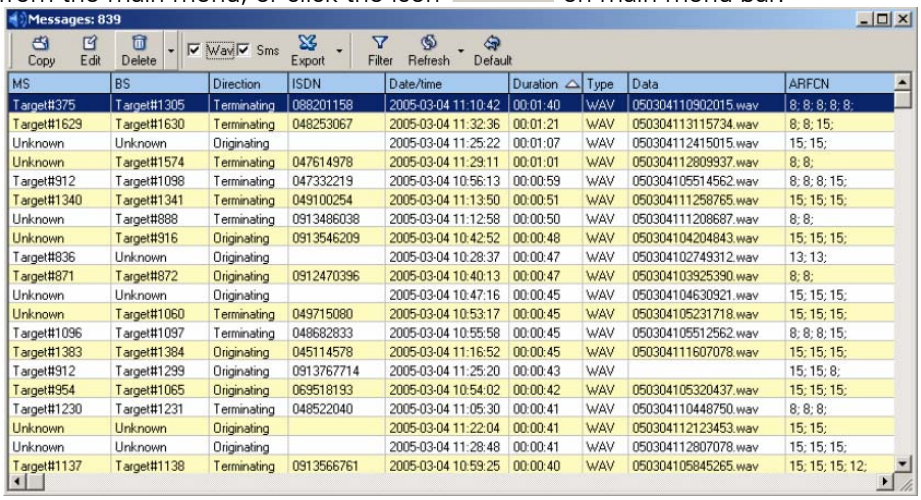
Menu item **Targets**

Menu item «Messages»

The menu item **Messages** retrieves the search window wherein audio recordings can be played back, as well as messages displayed.

In order to retrieve the **Messages** window, either select **Operation > Messages** from the main menu, or click the icon 

on main menu bar.



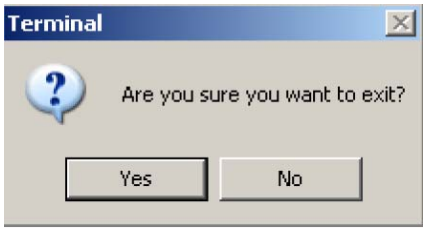
Menu item **Messages**

Menu item «Exit»

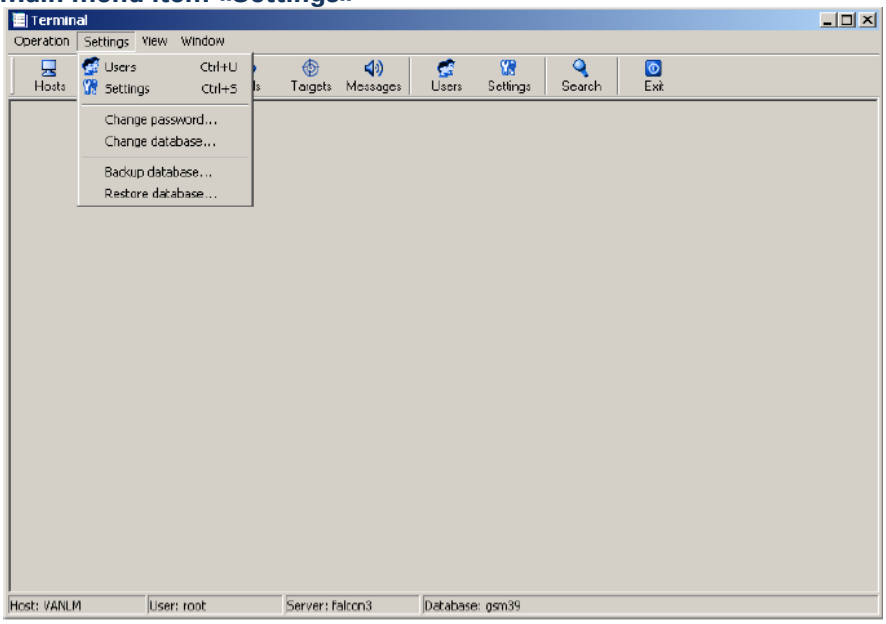
The sub-menu item **Exit** terminates the operation.

Click the icon 

on main menu bar, and the pop up window will ask you if you wish to exit. Select either **Yes/No** depending on what you wish to do.



Main menu item «Settings»



Main menu item **Settings**

Menu item «Users»

The submenu **Users** retrieves the authentication window wherein user rights can be defined.
In order to retrieve the **Users** window, either select **Operation > Users** from the main menu, or click the icon 

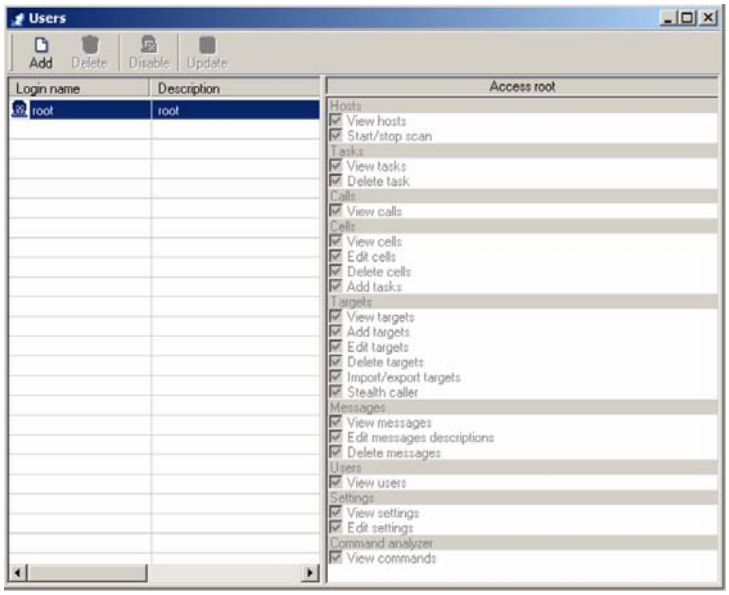
on main menu bar.

There are various functions that define the rights of the respective user:

dd		**new user**
elete		**delete user**
isable		**disable user**
pdate		**storage of alterations in Access**

The **Users** window displays name (**Login name**) and description of the user (**Description**) in the form of a table. User rights are defined within the **Check Box** by ticking the respective options within the **Access** pad.

Only the **root** user may administer users and assign them their rights.



Submenu **User**

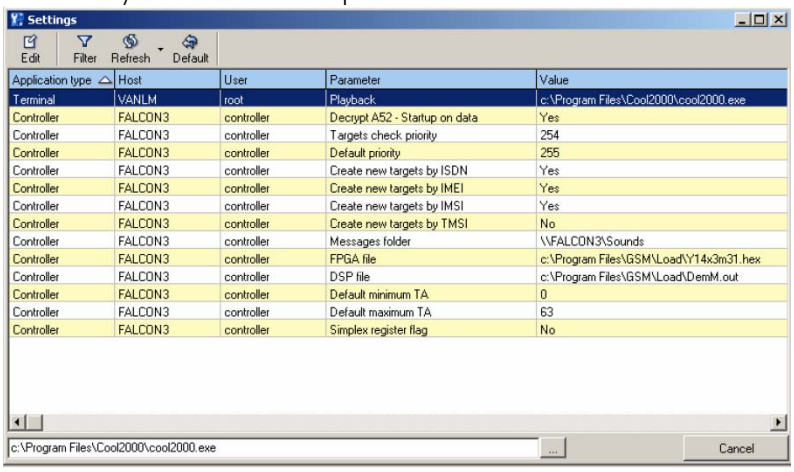
Menu item «Settings»

The menu item **Settings** sets the parameters of **The System Controller.** In order to retrieve the **Setting** window, either select **Settings > Settings** from the main menu, or click the icon 

on main menu bar.

The menu item serves for retrieval of the playback window, selection of loaded protocol data, selection of the path for connection to the Audio file and retrieval of the folder containing decoder data.

Types of loaded data:
«*.out» - file for loading ADP6201PCI
«*.hex» - loading file FPGA;
«...\cool2000.exe» - playback with CoolEdit software
«...\\The System3\Sounds» - path for connection to the Audio file



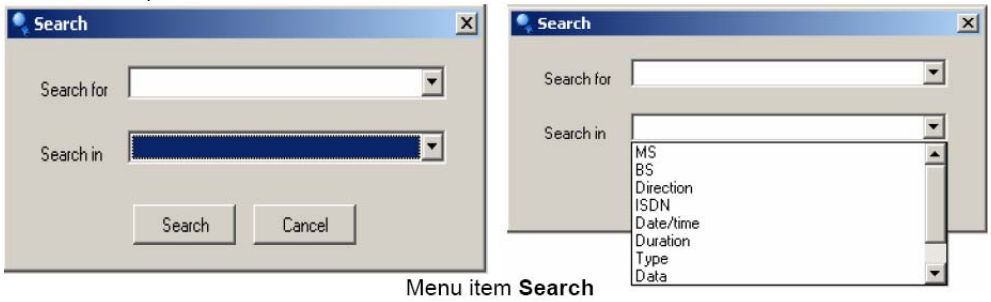
Menu item **Settings**

Submenu «Search»

The menu item **Search** finds essential parameters. This menu is only activated when another menu is already open.

In order to open **Search** menu, click the icon 

on main menu bar.

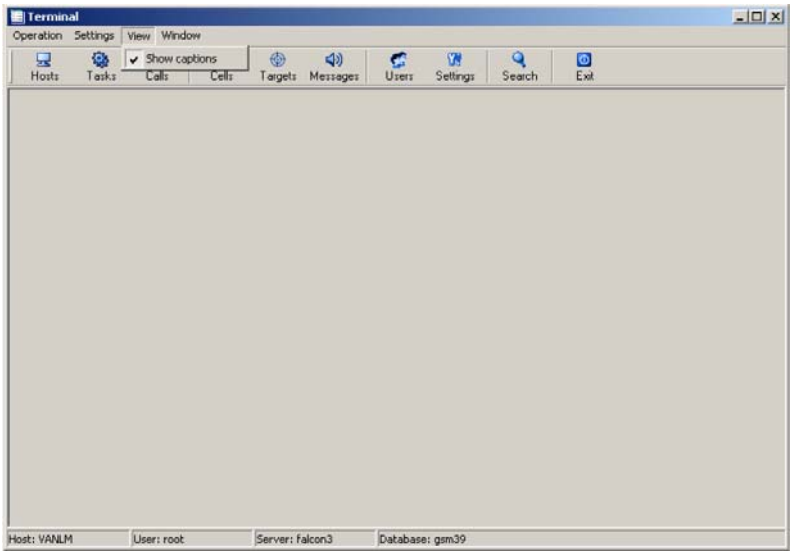


Menu item **Search**

Menu item «Change password»

The menu item **Change password** retrieves the password window of the current user of the THE SYSTEM system.

Main menu item «View»



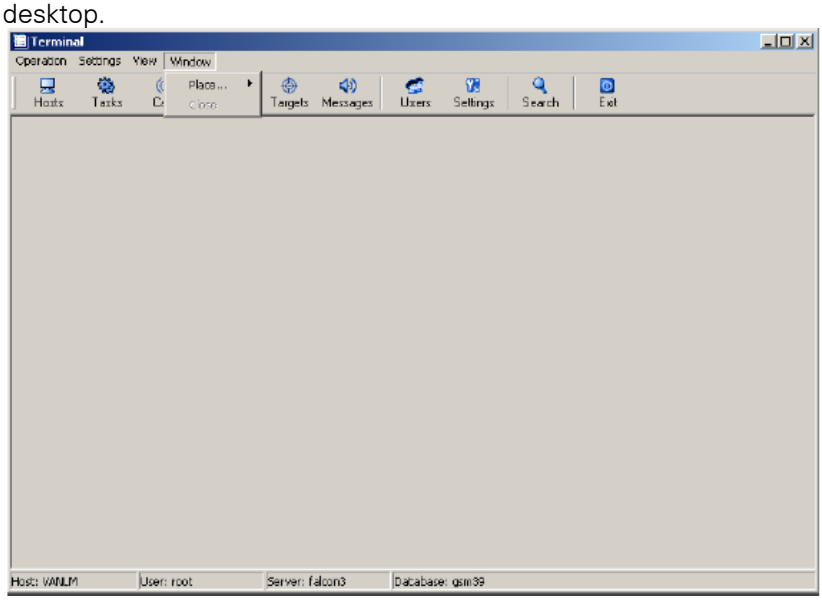
Main menu item **View**

Menu item «Show captions»

The menu item **Show captions** serves for pasting/deleting captions for keys of the main menu bars and sub-menu bars.

Main menu item «Window»

The main menu item **Window** serves for placing and aligning dialog boxes on the desktop.



Main menu item Window

6. Radio monitoring GSM 900/1800

Installation and use of antenna

The antenna is an essential part of the system. Effectivity of the THE SYSTEM system depends on thorough installation and use of the antenna.

Connecting the antenna to the system

Connect the antenna to the system using the cable. The amplifier's PSU has an integrated resetting fuse in order to avoid damage to the system from a short circuit within the antenna or antenna cable. Resetting of fuse lasts approx. 1 hour.

Short circuit within PSU of the amplifier might cause reduced reception signals.

In such case you should:

- turn off the system's power supply
- fix antenna or antenna cable (remedy the cause for short circuit)
- Turn on the system again after approx. 1 hour
- perform system start
- If the problem cannot be solved, please contact the manufacturer
- Other causes for reduced reception signals could be a tear-off or damaged contact within the antenna cable.
- In such case you should:
- turn off the system's power supply
- make sure the antenna cable is not torn
- turn on the system's power supply again
- perform system start

If the problem cannot be solved, please contact the manufacturer.

Operating conditions
The antenna is not designed for operation under conditions of precipitation. If the antenna is operated on any roof, you should equip it with additional weatherproof casing.

Do not fold or compress the antenna cable! Do not damage its slipcover or its plug! Do not use any antennas which are not supplied by scope of delivery! Screw the antenna tightly onto the antenna casing and **The System Controller**!

Recommendations for installation of antenna
By selecting the place of installation, pay attention to the following:
do not operate antenna nearby power transmission lines
do not operate antenna nearby transmission antennas
do not shield antenna with any metal construction
secure maximum distance between reception antenna and Ping-mobile phone (If in the delivery scope)

The location where the antennas are to be installed should comply with the criteria required by the base stations to be monitored (BCCH channels). Thus, the location should ensure minimal numbers of errors and maximum reception level for all channels.
Concerning this, the menu window **Tasks** provides all necessary information.

7. User's steps to operate the system

Net-monitoring – mobile phone (Optional)
The NET-monitoring mobile phone serves for quick definition of main parameters of GSM networks, as well as definition of control channels of the base stations. In order to activate the NET-Monitoring mobile phone, select the menu item "**Net monitor**" and the corresponding pages from the opened window.

Important pages are:
Page 1 – Information about BCCH-channel's number of current base station and distance between base station and MS in relative measuring units (1 relative measuring unit = 550m)
Pages 3-5 – Information about BCCH channel numbers of neighboring base stations
Page 10 – Information about TMSI and the channel number of current base station
Page 11 – BCCH channel system information of current base station
Page 12 – Information about activation of encoding and encoding type (CIPHER: A5x) and activation of HOPPING. These parameters are only displayed by Net-Monitor mobile phone during active phone call

The «Netmonitor.pdf» document provides detailed descriptions of all pages of the "**Netmonitor".**
Note: Use a SIM-card for your NET-Monitoring mobile phone, which is supplied by the respective GSM provider to be monitored. Conduct all measurements, nearby objects, (targets) to be monitored.

Analysis of radio-electronic circumstances
Open the window **Hosts** to analyze the radio-electronic circumstances. Select the main menu window **Operation > Hosts** or click the icon Hosts on main menu bar. Click Scan to start scanning process. To interrupt scanning process, click Stop .

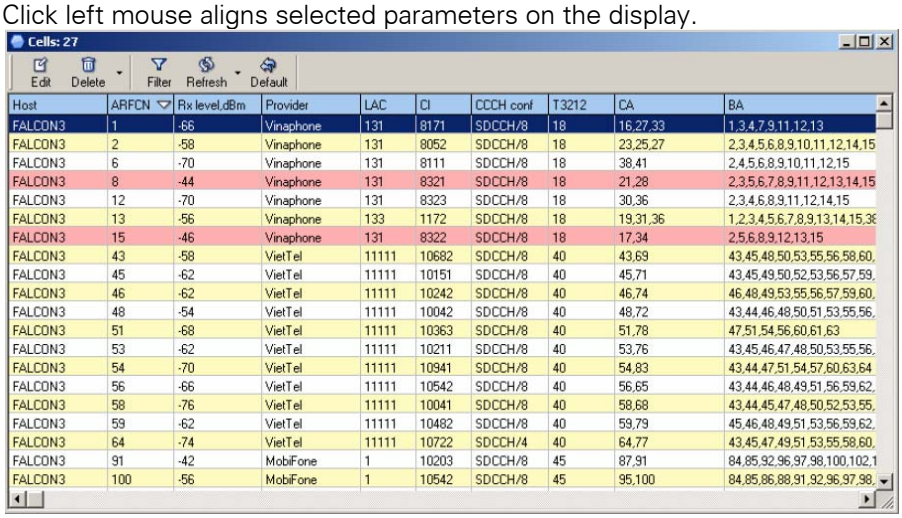
After that, the following parameters appear in table form within **Cells** window:

ID	ID Number
Hosts	Hosts name
ARFCN	Radio channel number of base station (ARFCN) BS
Rx-level	Signal strength of BS dBm
NCC	Color code of network
BCC	Color code of BS
MCC	Radio code of country
Country	Name of country
MNC	Radio code of network
Provider	Name of provider
LAC	Code of zone
CI	Network identify
CCCHconf	Configuration of CCCH
T3212	Timer 3212
CA	Number of channels used by BS
BA	Number of channels of neighboring BS
Errors, %	Number of processed data packets, number of erroneous data packets
Date/time	Date and time of recording
Comment	operator's comments on recordings

The line **ARFCN BS** displays current results of analysis (**Last:** 74)

Right mouse click displays desired parameters in this window.

Click left mouse aligns selected parameters on the display.



Host	ARFCN	Rx level,dBm	Provider	LAC	CI	CCCH conf	T3212	CA	BA
FALCON3	1	-66	Vinaphone	131	8171	SDCCH/8	18	16,27,33	1,3,4,7,9,11,12,13
FALCON3	2	-58	Vinaphone	131	8052	SDCCH/8	18	23,25,27	2,3,4,5,6,8,9,10,11,12,14,15
FALCON3	6	-70	Vinaphone	131	8111	SDCCH/8	18	38,41	2,4,5,6,8,9,10,11,12,15
FALCON3	8	-44	Vinaphone	131	8321	SDCCH/8	18	21,28	2,3,5,6,7,8,9,11,12,13,14,15
FALCON3	12	-70	Vinaphone	131	8323	SDCCH/8	18	30,36	2,3,4,6,8,9,11,12,14,15
FALCON3	13	-56	Vinaphone	133	1172	SDCCH/8	18	19,31,36	1,2,3,4,5,6,7,8,9,13,14,15,3
FALCON3	15	-46	Vinaphone	131	8322	SDCCH/8	18	17,34	2,5,6,8,9,12,13,15
FALCON3	43	-58	VietTel	11111	10682	SDCCH/8	40	43,69	43,45,48,50,53,55,56,58,60,
FALCON3	45	-62	VietTel	11111	10151	SDCCH/8	40	45,71	43,45,49,50,52,53,56,57,59,
FALCON3	46	-62	VietTel	11111	10242	SDCCH/8	40	46,74	46,48,49,53,55,56,57,59,60,
FALCON3	48	-54	VietTel	11111	10042	SDCCH/8	40	48,72	43,44,46,48,50,51,53,55,56,
FALCON3	51	-68	VietTel	11111	10363	SDCCH/8	40	51,78	47,51,54,56,60,61,63
FALCON3	53	-62	VietTel	11111	10211	SDCCH/8	40	53,76	43,45,46,47,48,50,53,55,56,
FALCON3	54	-70	VietTel	11111	10941	SDCCH/8	40	54,83	43,44,47,51,54,57,60,63,64
FALCON3	56	-66	VietTel	11111	10542	SDCCH/8	40	56,65	43,44,46,48,49,51,56,59,62,
FALCON3	58	-76	VietTel	11111	10041	SDCCH/8	40	58,68	43,44,45,47,48,50,52,53,55,
FALCON3	59	-62	VietTel	11111	10482	SDCCH/8	40	59,79	45,46,48,49,51,53,56,59,62,
FALCON3	64	-74	VietTel	11111	10722	SDCCH/4	40	64,77	43,45,47,49,51,53,55,58,60,
FALCON3	91	-42	MobiFone	1	10203	SDCCH/8	45	87,91	84,85,92,96,97,98,100,102,1
FALCON3	100	-56	MobiFone	1	10542	SDCCH/8	45	95,100	84,85,86,88,91,92,96,97,98,

To define base stations for monitoring, select **Cells** window from the main menu **Operation > Cells** or click the icon 

. ARFCN channels of the monitored base stations can be entered by double clicking on the line of **Cells** window.

Notice: System has 8 receivers, but you should switch on a maximum of up to 5 receivers. Remaining receivers are used for free resources (hopping and handover).

The database provides several functions, which can be accessed by clicking the icons from the toolbar:

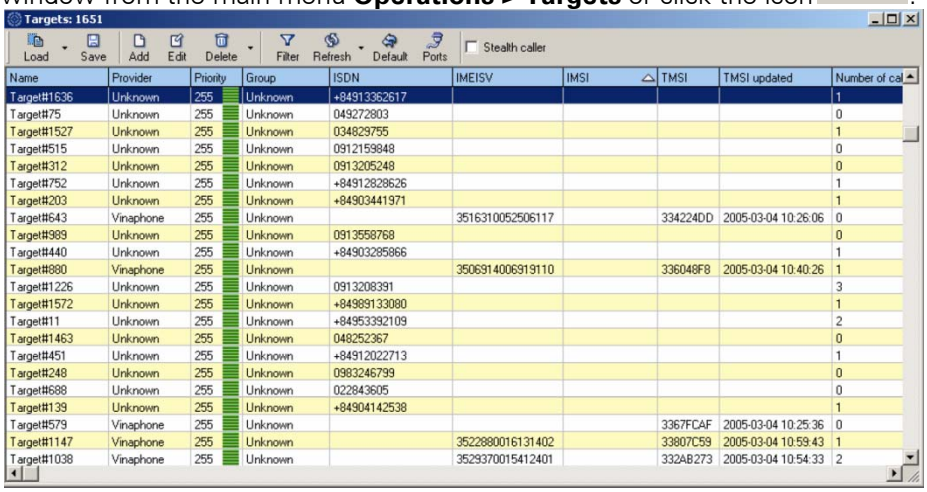
Edit <F4>		**Editing comments on selected BS**
Delete <Del>		**Deleting BS**
Filter <Ctrl+F>		**Cells filter**
Refresh <F5>		**Renewal of list of BS**
Default		**Restore default**

Database

Database «Targets»

In order to work with the **Targets** database, open the data base display and editor window from the main menu **Operations > Targets** or click the icon 

.



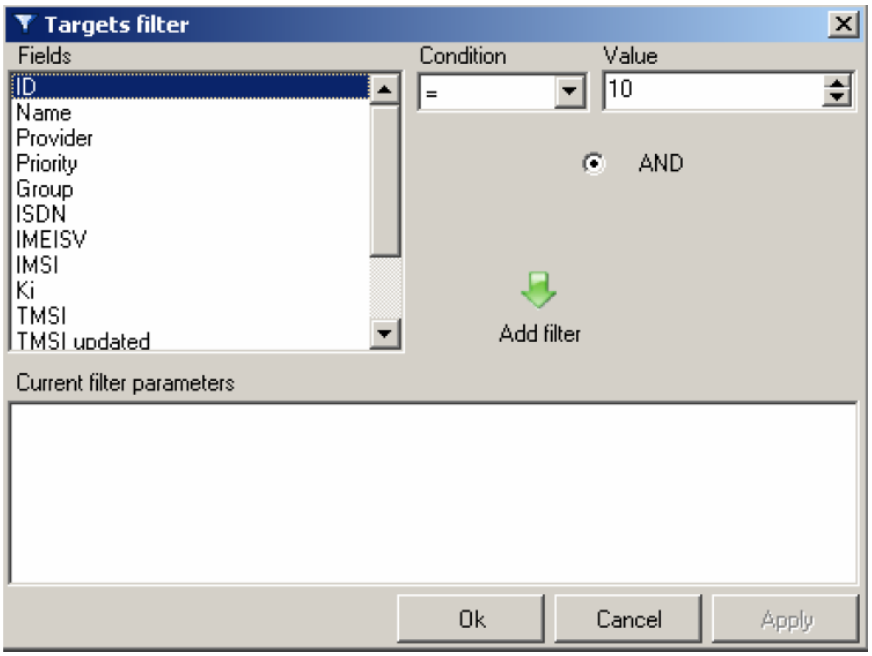
Name	Provider	Priority	Group	ISDN	IMEISV	IMSI	TMSI	TMSI updated	Number of ca
Target#1636	Unknown	255	Unknown	+84913362617					1
Target#75	Unknown	255	Unknown	049272803					0
Target#1527	Unknown	255	Unknown	034829755					1
Target#515	Unknown	255	Unknown	0912159848					0
Target#312	Unknown	255	Unknown	0913205248					0
Target#752	Unknown	255	Unknown	+84912828626					1
Target#203	Unknown	255	Unknown	+84903441971					1
Target#643	Vinaphone	255	Unknown		3516310052506117		334224DD	2005-03-04 10:26:06	0
Target#989	Unknown	255	Unknown	0913558768					0
Target#440	Unknown	255	Unknown	+84903285866					1
Target#880	Vinaphone	255	Unknown		3506914006919110		336048F8	2005-03-04 10:40:26	1
Target#1226	Unknown	255	Unknown	0913208391					3
Target#1572	Unknown	255	Unknown	+84989133080					1
Target#11	Unknown	255	Unknown	+84953392109					2
Target#1463	Unknown	255	Unknown	048252367					0
Target#451	Unknown	255	Unknown	+84912022713					1
Target#248	Unknown	255	Unknown	0983246799					0
Target#688	Unknown	255	Unknown	022843605					0
Target#139	Unknown	255	Unknown	+84904142538					1
Target#579	Vinaphone	255	Unknown				3367FCAF	2005-03-04 10:25:36	0
Target#1147	Vinaphone	255	Unknown		3522880016131402		33807C59	2005-03-04 10:59:43	1
Target#1038	Vinaphone	255	Unknown		3529370015412401		332AB273	2005-03-04 10:54:33	2

Menu item **Targets**.

The window displays the following object data in table form:
ID – Own identifier
Name – Object name
Provider – Name of provider
Priority – Assigned object priority
Group – Name of object group
ISDN – ISDN-number of object
IMEISV – IMEISV of object
IMSI – IMSI of object
Ki – Ki of object
TMSI – Current TMSI of object
TMSI updated – Renewal time for TMSI of object
Comment – Comments on recording
Number of calls – Number of received messages from object
Host – Host name

Right click mouse in this window to change number of data to be displayed within corresponding window.
Within the database those objects are processed whose priority is higher than it is defined in the **Check priority window**.
Messages from low priority objects are only registered on availability of sufficient resources. Registered low priority objects will be saved in the database as new objects with a priority of 255.
All object data is entered into the data base. Messages from objects, whose priority is not less than the assigned one, are processed first and resources of the system are made available. All object data is stored on HDD.
The database provides several functions, which can be accessed by clicking the icons from the tool bar:

Load		loads Targets database from file
Replace… <Alt+R>		exchange of current object list for object list from file
Append… <Alt+A>		extending the object list with objects from file
Save		Storage of current object list in file
Add target <F2>		adding new object
View detail/edit target <F4>		editing of selected object
Delete target <Del>		deletion of selected object
Delete the list		deletion of all objects or selected groups
Delete all Targets		deletion of all targets
Filter <Ctrl+F>		window for system settings and display of objects



Target Filter.

Activate **CheckBox** to show objects and enter the required parameter.

Refresh <F5> 

renewal of object list

The toolbar contains the **Find on** pad, wherein you can search for objects. The upper part of the window displays number of object, e.g.: **Targets #**.

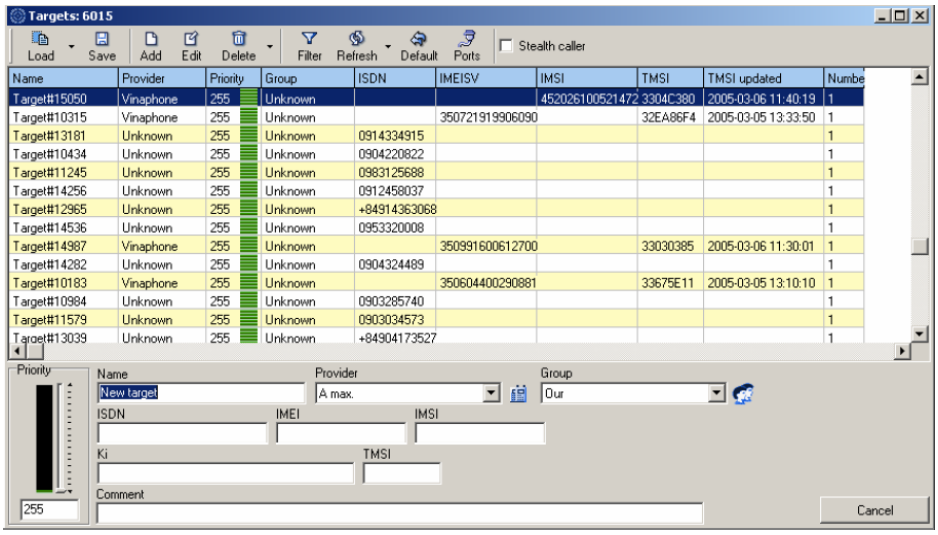
For each message the data of two objects (calling and answering) will be updated simultaneously within the database.
If involved objects are not contained in the database, they must be added to the database.

Double click on objects with left mouse to view messages from the selected objects.

On adding a new object (**Add target** <**F2**> 

) or editing a newly selected object (**View detail/Edit target**<**F4**> 

), an extra window with identification criteria will be opened.



Menu item **Targets**

The following object data is displayed in the editing window:
Priority – priority of object
Name – object name
Provider – name of provider
Group – name of object group
ISDN – ISDN-number of object
IMEI – IMEI of object
IMSI – IMSI of object
Ki – Ki of object
TMSI – current TMSI of object
Comment – comment on recording

On entering new data or editing existing data, the changes must be made within the corresponding line.

Name of provider and name of object group can be taken from the database.

Editing displayed parameters occurs in dialog boxes by clicking the icons  and  . The changes are stored in the database via **Save**  .

Click **Edit**  if you do not want to save the changes made in the editing mode.

Real-time listening-in occurs via:
Open window **Calls** then live listen telephone conversation

You should switch off the operating mode **Calls**, when either no listening-in or listening into messages of only a small number of objects is necessary.

Searching an object within monitored zone (with optional Ping-Mobile phone)
Searching for an object within the monitored zone can occur easily by means of the **Ping-mobile phone** (if in delivery scope). The **Ping-mobile phone** makes a "silent" call to get access to current parameters of the object.

Note. You must use a SIM-card of the monitored provider for your Ping-mobile phone

There are two options for searching for an object:

1. manual search
2. automatic search

Manual search

Select call diversion for **Ping-mobile phone**
Go to system's control panel «Ping-mobile phone»; tick **Stealth caller** in CheckBox of the **Targets** window
Turn off **Automat** in CheckBox
Open field **Caller ISDN:** enter ISDN-number of **Ping-mobile phone**
Select object with phone number from **Targets** window
Dial object's phone number with your **Ping-mobile** phone and press Call
When the message "diversion of all phone calls" appears on your display, abort phone call immediately. Repeat this procedure at intervals (5-10 times at intervals of 5-10 seconds)
Thereafter, press stop key on your **Ping-mobile** phone

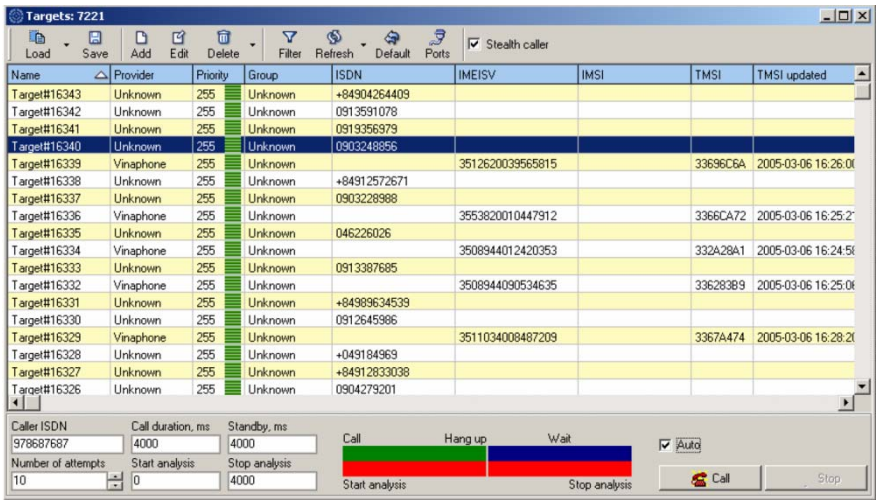
If the wanted object is within the monitored zone, identification criteria of the object, such as telephone number, IMSI, IMEISV and current TMSI, will appear on the display of the THE SYSTEM system.

Automatic search

Connect **Ping-mobile phone** to the THE SYSTEM system by means of the interface cable; COM- or USB port. The window **Settings** > **Devices** > **Phone connection** shows the port to use. Secure maximum distance between THE SYSTEM system and Ping-mobile phone
Activate Ping-mobile phone from the tool bar of the **Targets** window; **Stealth caller** in CheckBox
Click **Automat** in CheckBox
Settings for Ping-mobile phone:

field **Caller ISDN:** ISDN-number of Ping-mobile phone
field **Call duration, ms:** duration of impulse in msec
field **Standby, ms:** - duration of break between calls in msec
field **Number of attempts:** - number of calls
field **Start analysis, ms:** - start time of analysis of received message in msec
field **Stop analysis, ms:** - end time of analysis of received message between calls in msec

Select object with ISDN-number from **Targets** window
Press **Call** and **Stop** to start and finish search



windows **Targets**

Operator's tasks:

1. Define optimum pulse length of **Call duration** (green indication) on Ping-mobile phone panel, as well as length of **Standby** between calls (blue indication) in order to avoid the call being put through to BS. Optimum settings can be identified by means of the NET Monitoring mobile phone (serves as virtual target).
2. Define optimum intervals for analysis of received messages (red indication), with measuring time of call until reception of message and time of **Start analysis** until **Stop analysis.**

Any test telephone with known IMEI, IMSI or TMSI can be used for this procedure.
The NET-Monitoring mobile phone (optional) can also be used for easier identification of call parameters for the Ping-mobile phone.

If the object is found within the monitored zone, search will be stopped and identification criteria of the object such as IMSI, IMEISV and current TMSI will appear on the display.

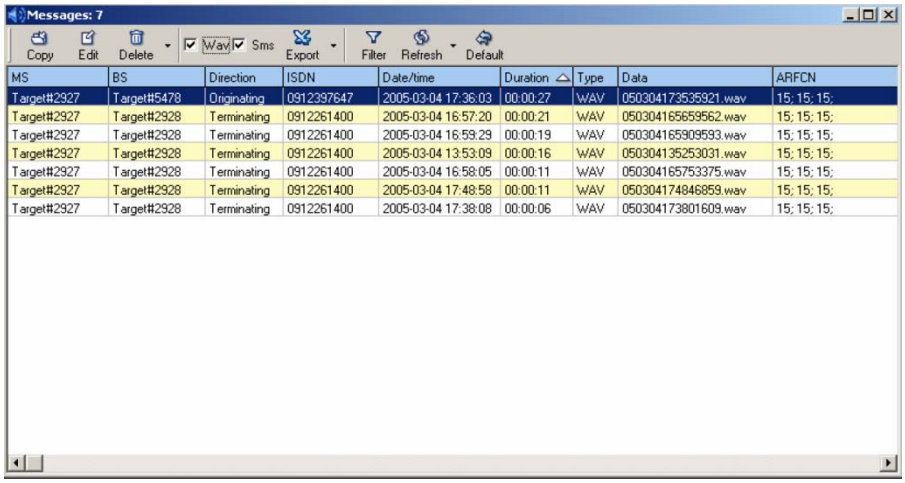
Note 1. The recommended search algorithm for an object does not guarantee absolute information. It serves only as an auxiliary means for the operator of the system.

Note 2. Erroneous handling of the Ping-mobile phone might lead to complete exposure of the operation of the system!

Database < Messages >
In order to work with the **Messages** database, open the display and edit the database window from the main menu **Operation > Messages** or click the icon 

.

Double click in the window database **Targets** with left mouse button to view only the selected object in the windows **Messages**.



window **Messages**

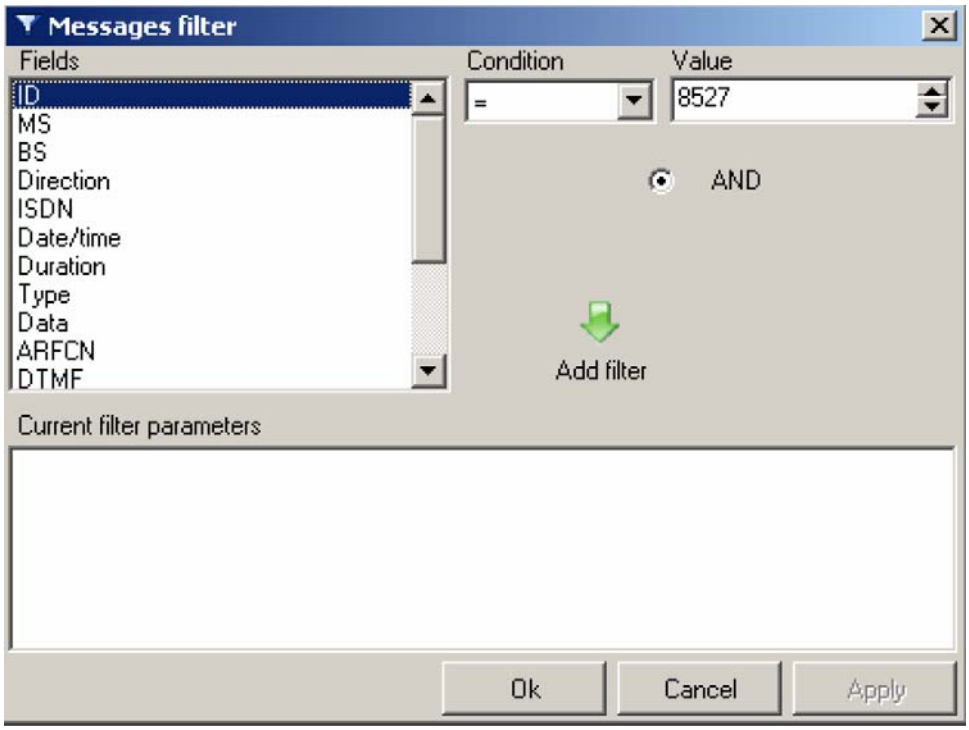
The window displays the following data in table form:
ID – internal identifier
MS – object name of MS for current connection
BS – object name of BS for current connection
Direction – direction of connection for MS object
ISDN – ISDN-number of object via BS
Date/time – date and time of message
Duration – duration of message
Type – type of message
Data – Content of text message or file name containing audio recording
ARFCN – channel number of BS, wherein message from object occurred
DTMF – content of DTMF message
Comment – comments on recording
Status – state of processing of messages
User – name of user working with data base
Checked – date and time of editing of file containing recording of message
Host – host name

Right mouse click tdetermines number of displays on screen.

Click on headline with left mouse button to define position of the selected parameters on the display.

The database provides several functions that can be activated by clicking the icons from the tool bar:

Copy file <F2>		Copying the file containing recording of selected message
Edit message <F4>		Editing comments on selected message
Delete message <Del>		Deletion of message
Delete file <Shift+Del>		Deletion of file and recording of selected message
Delete the list		Deletion of all messages from data base
Filter <Ctrl+F>		Retrieval of system settings window



Window Message **Filter**

Within the Message **Filter** window you may create user-defined filters on the basis of varying criteria and parameters. Creation of filters containing symbols occurs in the Value window, e.g. % ....% symbols: parameter DTMF-Filter: % 34%

Refresh list of messages <F5> 

- updates message list.
The Find on.pad serves for searching messages within the database. The upper part of the window displays the overall number of messages, e.g.:Messages: 4.

Playback of selected messages occurs via double clicking with left mouse button or pressing <Enter>.
The following entry windows will be opened for editing of messages (Edit <F4> 

):
Check Box Processed - operator ticks <<play back message>>
Comment - operator's comments on recording.

All changes will be stored in the database by clicking apply.

8. Technical Data

	GSM 900	GSM 1800
Reception channels	8	
Target numbers	up to 1000	
Identification through	IMSI, TMSI, IMEI, Class mark, Telephone number, Distance	
Frequency range of Downlink (BTS_MS)	935 ... 960 MHz	1805 ... 1880 MHz
Frequency range of Uplink (MS_BTS)	890 ... 915 MHz	1710 ... 1785 MHz
Channel spacing	200 kHz	
Number of channel	124	375
Frequency deviation	45 MHz	95 MHz
Frequency stability	0,03 ppm	
Receiver type	wide range receiver	
Receiver sensitivity	-105 dbm	
Antenna impedance	50	
Time of frequency change in Hopping mode	< 500 µs	
Dynamics range	> 75 dB	
Volume range	25 dB	
Demodulator	GMSK, asynchrony	
Decoder	for Protocol A5-2	
Speech codex	RPE/LTP: FR, EFR	
Channel structure	TDMA/FDMA	
System software	Windows XP	
Audio format	standard Wave-format	
Power supply	220 VAC, 50 Hz; 110 VAC, 60 Hz or external battery 12 V DC	
Operating temperature range	+ 5 °C ... 40 °C	

9. Scope of delivery

Main unit *THE SYSTEM*

- Control unit (Notebook)
- Network-connecting cable
- Power supply cable 230VAC
- Dual-band antenna (magnetic mount)
- User manual
- Transport case

GSM-Monitoring System Semi Active: Falcon E+

Description

The FALCON E+ system is designed and developed as a Semi Active OFF-THE-AIR GSM-Monitoring system. The system provides the option of both stationary and mobile operation

The FALCON E+ system deciphers A5.1 and A5.2 ciphering algorithms online. The system does not require the service providers SIM for operation because uses cloning of the targets phone in real time. Therefore, all the calls made by the target are billed into its account.

Main Features

- The system ensures monitoring of audio and data traffic within standard GSM 900/1800 networks (800/1900 on request) and deciphers A5.1 and A5.2 algorithms online
- Default configuration of the system - 8 reception channels (4 duplex channels, monitoring of both forward and reverse conversation channels)
- The system ensures registration of radio-electronic conditions within the radio cells to be monitored (frequency and characteristics of BCCH-channels)

- The operator can select the required targets based on their IMSI or IMEI. Upon selecting the targets the system acts as a virtual base station (BTS) for these targets.

- When one of the targets initiates a call, the FALCON E+ system automatically calculates the ciphering key and authentications parameters. These parameters are then cloned onto another mobile phone attached to the system (up to 4). The targets calls are now routed through the cloned mobile phones, maintaining the same encryption and target identity.

- The system contains a database (up to 100,000 calling partners), operating in real-time, which can be accessed corresponding to the selected search criteria and parameters.

- Calling partners are identified according to the IMEISV, IMSI, TMSI, ISDN number (local and international number)

- Retrieving of target IMEI/IMSI for using targets mobile number and silent call

- Registration and storage of telephone conversations, call related information, network information and Short Message Service (SMS) to the system's hard disk.

- The system ensures registration and storage as audio codec - types FR, EFR, HR.
- Playback of recordings may be carried out by the system itself

- Identification of SMS and DTMF data.

Scope of Delivery:

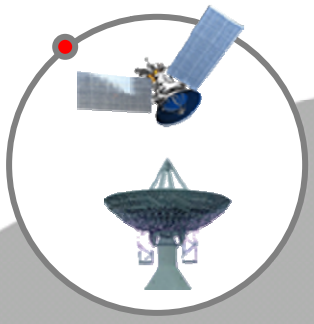
- Main unit *FALCON E+*
- Control unit (Notebook)
- Virtual base station (mono band) with power supply unit
- GSM antenna (omni-directional)
- network-connecting cable
- Power supply cable 230VAC
- Power supply cable12 VDC
- User manual
- Transport case (2 pcs.)

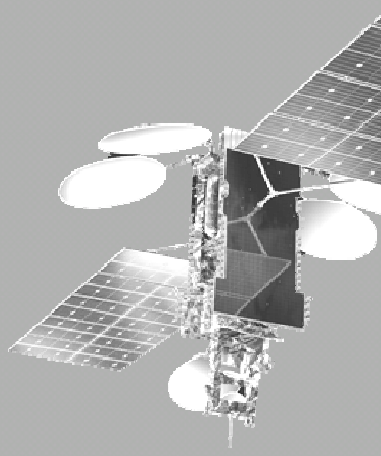
Technical data

	GSM900		GSM1800
Reception Channels		(4 Duplex channels)	
Target Numbers		Up to 1000	
Data entries		Up to 100'000	
Identification	Through IMSI, TIMSI, IMEI, Class mark, Telephone Number, Distance		
Monitoring	Voice (A5.0, A5.1, A5.2), SMS, DTMF		
Recording	Audio codec type FR, EFR, HR		
Playback		CoolEdit Software	
Frequency Range of Down Link BTS -> MS	935…..960 MHz		1805…..1880 MHz
Frequency Range of Up-Link MS -> BTS	890….915 MHz		1710….1785 MHz
Channel Spacing		200 kHz	
Number of Channels	124		375
Frequency Deviation	45 MHz		95 MHz
Frequency Stability		± 0.03 ppm	
Receiver Type		Wide Range Receiver	
Receiver Sensitivity		- 105 dBm	
Output Power	10 mW – 3 W, (other power ranges on request)		
Mobile Power Control	3 mW – 2W		1 mW – 1 W
Operating Range	Down Link up to 10 km Up Link up to 500 m in city		
Assessment of coverage accuracy		Up to 550 m	
Antenna Impedance		50Ω	
Time of frequency Change in Hopping Mode		< 500 µs	
Dynamics Range		> 75 dB	
Volume Range		25 dB	
Demodulator		GMSK, asynchrony	
Decoder		For Protocol A5.2	
Speech Codex		RPE/LTP:FR, EFR	
Channel Structure		TDMA/FDMA	
System Software		Windows XP	
Audio Format		Standard Wave-Form	
Interface		TCP/IP	
Remote Control		via LAN, ADSL,	
Power Supply		220 VAC, 50 Hz 110 VAC, 60 Hz	
Operating Temperature		+ 5° C …. 40°C	

elaman
GERMAN SECURITY SOLUTIONS

Satellite Monitoring Systems





Index

Thuraya Monitoring System

1- The Thuraya Personal Satellite Communications System

The Thuraya network has been in operation since early 2001, and is currently based on the Thuraya-2 geostationary satellite in an inclined orbit at a longitude of approximately 44° East. The Thuraya system provides telecommunications coverage to Europe, North, Central and some parts of Southern Africa, the Middle East, West and Central Asia, and the Asian Subcontinent, including more than 110 countries. Using a reduced capacity Thuraya-1 satellite at 98° East, provides some areas of the Far-East. In January 2007 the Thuraya-3 satellite was launched into the current location of the Thuraya-1 satellite, this new satellite has extended the coverage area of the Thuraya network to areas of Central and Eastern Russia and the Far East, including the eastern and south-eastern areas of mainland Asia, Japan, Taiwan, Malaysia, Indonesia, Brunei, the Philippines and Papua New Guinea.

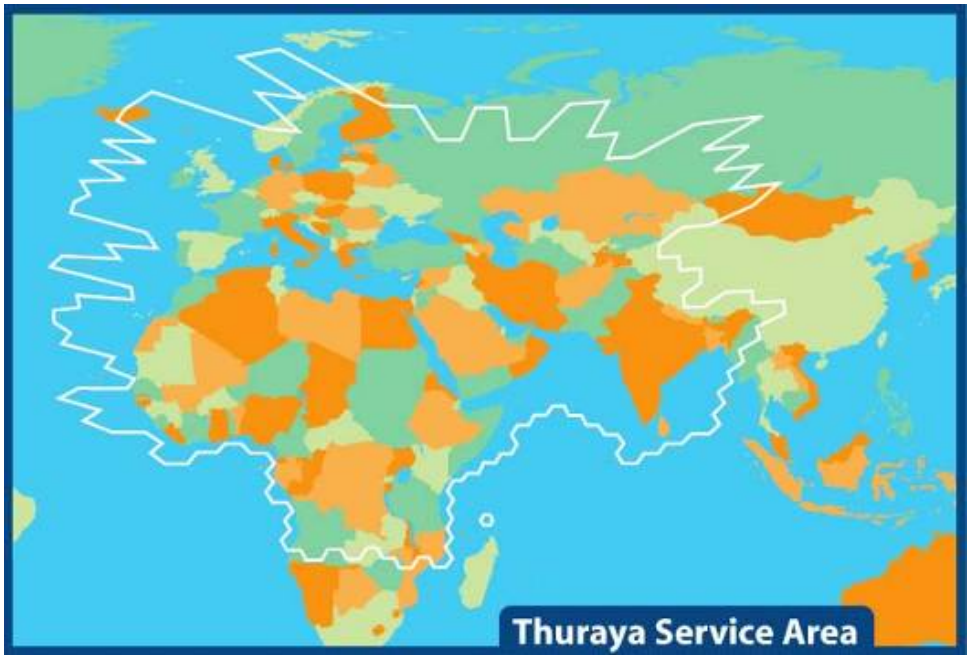


Figure 1 – Map Showing Current Commercial Coverage from the Thuraya-2 Satellite

Since its introduction, the Thuraya system has proven to be extremely popular and exceeded the 150,000 subscriber barrier by the mid-2003, and it is estimated to currently have in the region of 340,000 subscribers Thuraya forecast that they will ultimately achieve 1.75 million subscribers. One of its main appeals is to people living or traveling in the remote areas of Africa, the Middle East and Asia, where terrestrial infrastructure is not in place. The Thuraya network is designed to support 13,750 simultaneous telephone calls, and in some countries typical call levels are known to exceed 2,000 calls per hour.

2- The Strategic Thuraya Monitoring System

2.1- Principles of the Strategic Thuraya Monitoring System Operation

The strategic Thuraya Monitoring System (TMS) offered by TRL is designed to passively intercept downlinks from the Thuraya satellite at C-Band and L-Band.

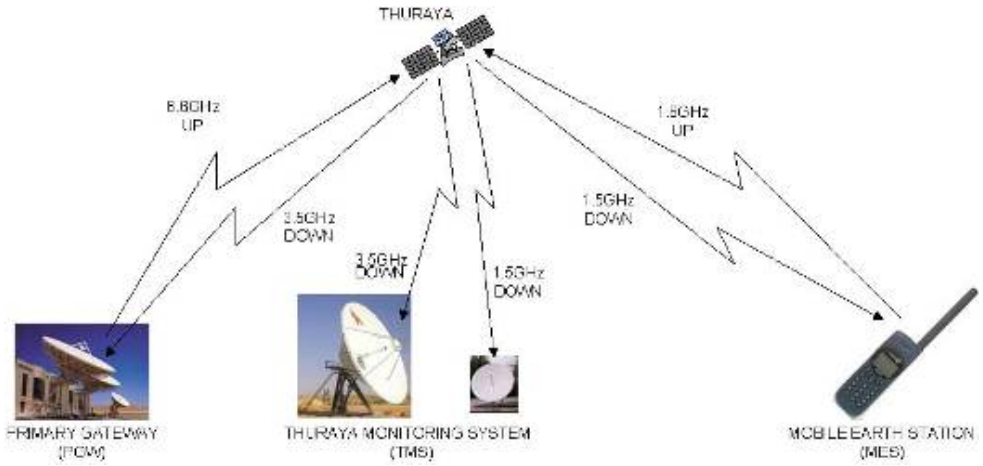


Figure 2 – Principle of TMS Operation

An L-Band antenna receives transmissions from the network to the Thuraya handset (MES), and a C-band antenna receives transmissions from the Thuraya handset to the network via the satellite.

The new system is designed to provide full duplex call interception and recording for all calls passing through a cluster of seven spotbeams centered on the geographical location of the installed system. It may be possible to perform duplex call intercept on other nearby spotbeams, but this cannot be guaranteed due to frequency reuse implemented on the Thuraya network at L-Band.

Additionally, with the inclusion of the optional Transportable Remote L-Band Monitoring System, all calls passing through an additional cluster of seven spotbeams centered on the geographical position of the remote system, may be intercepted and recorded.

In addition to the call intercept, the strategic TMS has the capability to monitor call activity for all spotbeams transmitted by the Thuraya satellite, by receiving the C-band signaling information. The proposed system has the capacity to monitor 25 such spotbeams.

Where the system is able to perform C- and L-Band monitoring of a given spotbeam, the following data is recorded by the system for every call:

- Date and time of the call
- A 4 or 5 digit subset of the IMSI of the MES
- The GPS position of the MES
- The telephone number dialled by the MES (in Mobile Originated calls only)
- The TMSI of the MES
- The Ciphering Key Sequence Number
- The RAND
- The SRES
- The Encryption Algorithm implement on the call
- The system also produces a computer file of the call that was recorded; this file is available for offline analysis

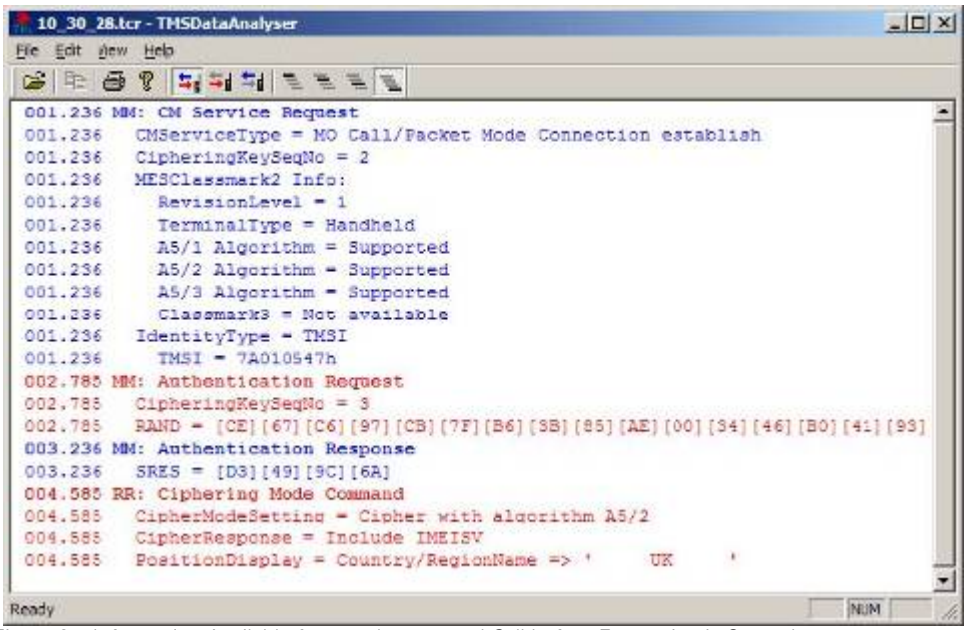


Figure 3 – Information Available from an Intercepted Call before Encryption is Started

Where the system is only able to perform C-band monitoring of a given spotbeam, the following data is recorded by the system for every call:

- Date and time of call
- A 4 or 5 digit subset of the IMSI of the MES
- The GPS position of the MES
- The telephone number dialled by the MES (in Mobile Originated calls only)

For C-Band only monitoring, the call cannot be intercepted, and therefore no recording file is generated.

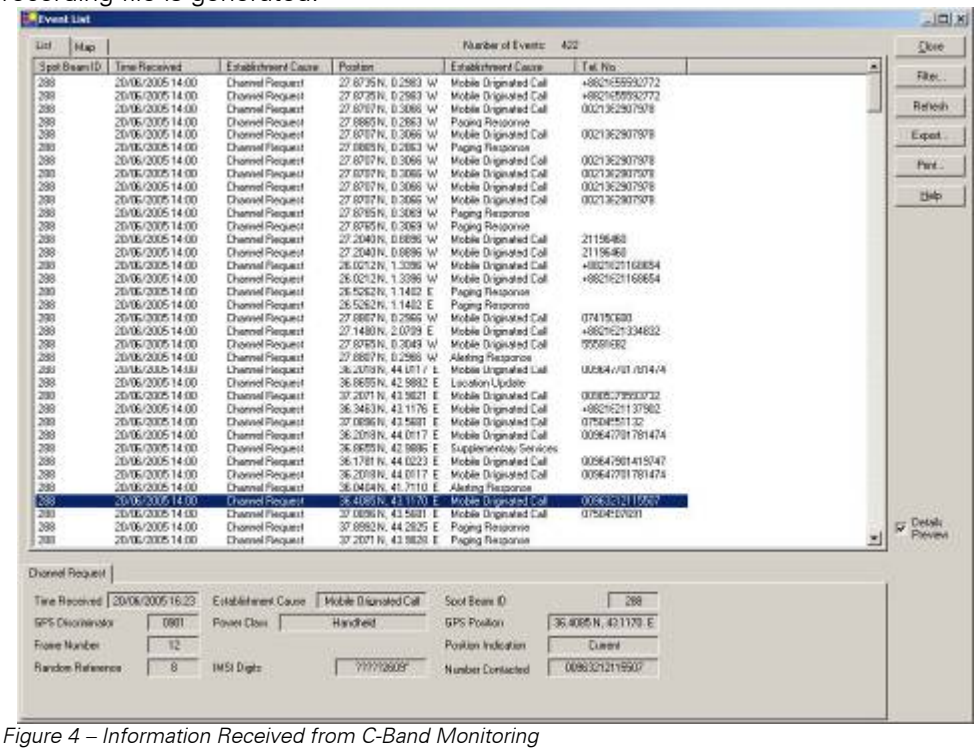


Figure 4 – Information Received from C-Band Monitoring

2.2- Decryption

TRL has now identified, tested and verified the functionality of a Thuraya Cryptanalysis and Decryption device provided by a third-party company. This company is a proven supplier of passive GSM monitoring systems including A5/2 cryptanalysis and decryption. The Thuraya cryptanalysis and decryption unit is their complete solution, developed as a result of determining the Thuraya encryption algorithm and developing their existing GSM cryptanalysis product to process the Thuraya traffic.

This solution when connected to the Strategic Thuraya Monitoring System provides the capability for the play-back of audio voice calls and the display of the SMS, fax and data sessions.

2.2.1- Additional Functionality Available with a Cryptanalysis Solution

With the Thuraya cryptanalysis and decryption solution integrated with the strategic TMS, the following additional information becomes available from calls intercepted in a full duplex C and L-band monitoring system:

- **Human Comprehensible Call Content**. This would include live and archived stereo audio playback of voice calls, and presentation of decoded SMS and fax. Additionally, a range of commercial data protocols would also be supported for decoding data transmitted over the Thuraya network.
- **MES IMEI**. The IMEI of the MES would be recorded, significantly enhancing the ability to identify and track particular Thuraya terminals.
- **Calling Line Identity Presentation** (CLIP). The telephone number of call originator would be available on some calls. In particular, the telephone number of the land-line in fixed originated calls, and the telephone number of both parties in a Thuraya terminal to terminal call would become available.

Cryptographic and Cryptanalysis technology is subject to export control by the governments of many Western countries, including the United Kingdom. Upon development of a GMR-1 cryptanalysis solution, any European or North American developer would be obliged to apply to their respective governments for permission to export the solution.

2.3- A Typical Strategic Thuraya Monitoring System

A typical TMS system would include:

- Full duplex interception of Thuraya calls for terminals located within the same spotbeam as the monitoring system, and up to 6 spotbeams immediately adjacent to that central spotbeam
- Antenna system, including a 9.3m C-Band antenna and demodulator subsystem for monitoring of up to 1088 simultaneous calls in the area covered by the main installation – including GPS co-ordinates of mobile terminals
- Analysis subsystem, complete with 6 server computers and 8 analysis workstations complete with TMS analysis software
- Full Operator, Administrator and Maintainer training programs, held both at TRL and at the customer's site if required
- Comprehensive operation and support documentation
- Full warranty for the first year
- The option of a Remote L-Band Unit, to extend the interception coverage of the monitoring system, to another group of up to 7 spotbeams anywhere within the Thuraya coverage

- C-band Only monitoring of Terminal activity in any Thuraya spotbeam on the satellite. Up to 35 spotbeams can be monitored in the default configuratio This monitoring provides the GPS position and the dialed telephone numbers for all Thuraya phones operating in the spotbeams of interest

The proposed strategic Thuraya Monitoring System comprises 3 subsystems, each are described below:

2.3.1- RF/IF Subsystem

The RF/IF subsystem receives the downlink signals from the Thuraya satellite that are intended for the MES and the PGW. It includes the following components:

Outdoor Equipment

- 9.3m Diameter C-Band Earth Station Antenna
- Flat Plate L-Band Antenna

Low Noise Amplifiers are included with all antennas, as well as Inter-Facility Cabling between the Antennas and the Customer Supplied Equipment Room. The 9.3m C-Band Antenna is fully motorized.

Figure 5 – Typical C-Band Antenna

- Satellite Tracking Antenna Controller
- Satellite Beacon Tracking Receiver
- 4 C-Band Synthesized Tuneable Downconverters
- 1 L-Band Synthesis Tuneable Downconverter
- RF/IF Signal Distribution
- 10 MHz GPS Corrected Station Frequency Reference
- Uninterruptible Power Supply

The above indoor equipment is supplied installed in a 19" rack cabinet.

2.3.2- Demodulator Subsystem

The demodulator subsystem receives the satellite signals from the RF/IF subsystem at IF, and demodulates them. It includes the following:

- Demodulator Cards. A sufficient number of demodulator cards will be supplied in order to perform dual C- and L-band monitoring and call intercept of all traffic on up to seven spotbeams surrounding the monitoring station, as well as C-band only monitoring for at least 10 other spotbeams. If the optional Remote L-Band Monitoring System is also ordered, then the strategic system will be fitted with additional demodulator cards to provide C-band monitoring and call intercept for the spotbeams monitored by the remote system. The demodulator cards are fitted in to card racks, each housing 12 cards.
- Ethernet Switch
- Uninterruptible Power Supply

All components of the Demodulator Subsystem are supplied installed in a 19" rack cabinet.

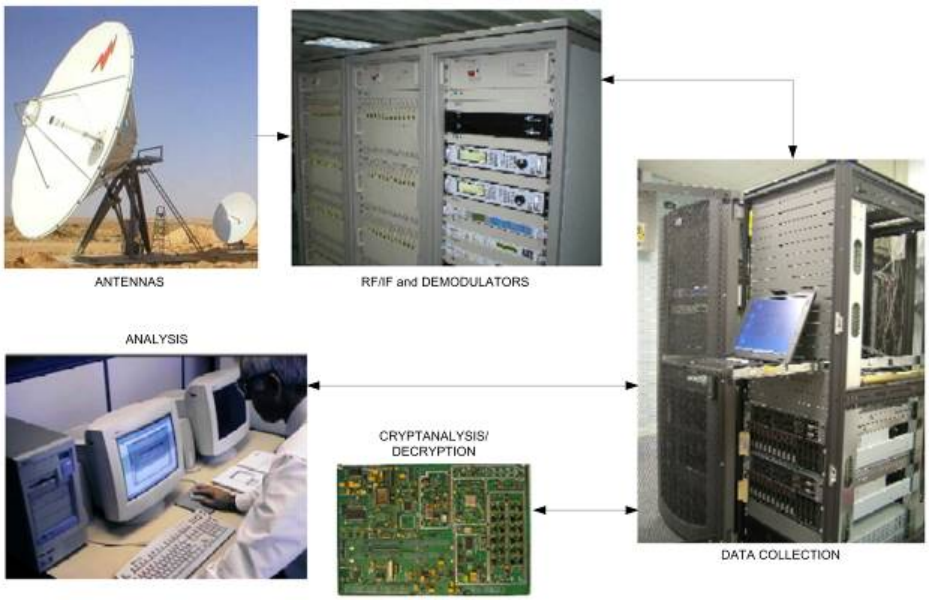


Figure 6 – Typical TMS Equipment

2.3.3- Analysis Subsystem

The analysis subsystem configures the demodulator subsystem according to the User's operational requirements. It receives the satellite signals from the Demodulator subsystem via an Ethernet network, and stores them in the server computers. The analysis software performs decoding and de-multiplexing of the received signals and interprets them providing the User with information about the traffic on the Thuraya network as described in Section X2.1X. The software includes a geographical mapping interface based on the ESRI standard ArcGIS software, and displays the positions of the MESs making calls on the Thuraya network, as well as information related to the available spotbeams on a map.

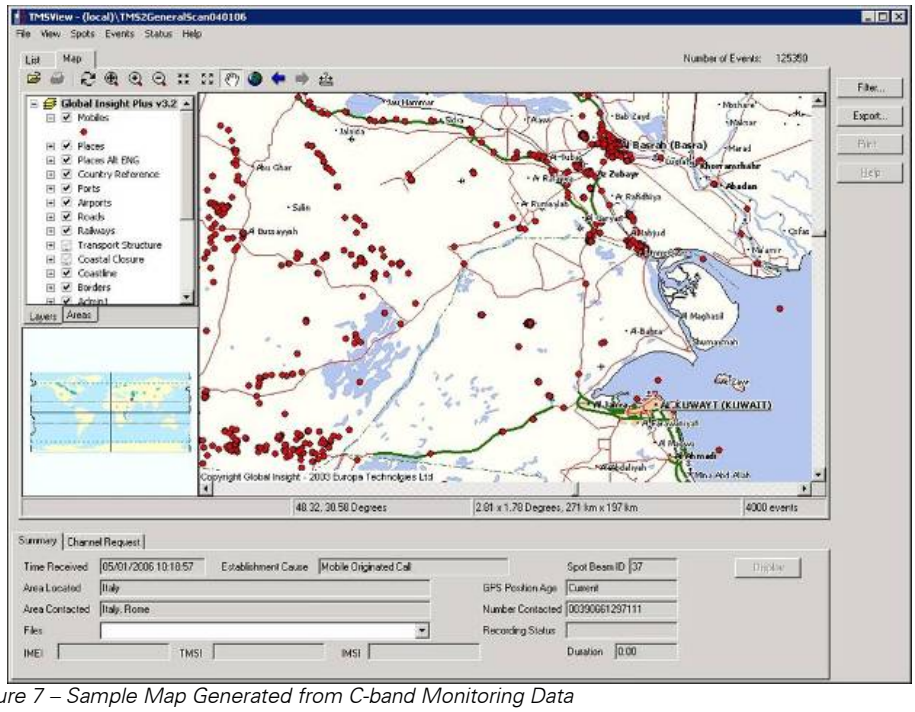


Figure 7 – Sample Map Generated from C-band Monitoring Data

The Analysis Subsystem includes the following components:

19" Rack Mounted

- Server Computers
- Keyboard, Video, Mouse (KVM) Drawer
- KVM Switch
- Ethernet Switch
- Uninterruptible Power Supply

Free Standing

- Workstation Computers with 19" LCD TFT Flat Screen Monitors
- Uninterruptible Power Supply Units

It is assumed that suitable buildings, civil works and electrical power is to be provided by the customer, and therefore is not included within the scope of this proposal.

Training is provided in the administration, operation and maintenance of the system both at TRL facilities, and at the customer site upon completion of the system installation.

The strategic TMS is supplied with a full spares pack to reduce potential system downtime in the event of a component failure.

The TMS has a modular design allowing all aspects to be scaled to meet customer requirements.

Remote L-Band Thuraya Monitoring Expansion
A Remote L-Band Thuraya Monitoring System (TMS) expands upon the amount of spotbeams that a strategic TMS can provide full duplex call intercept for.

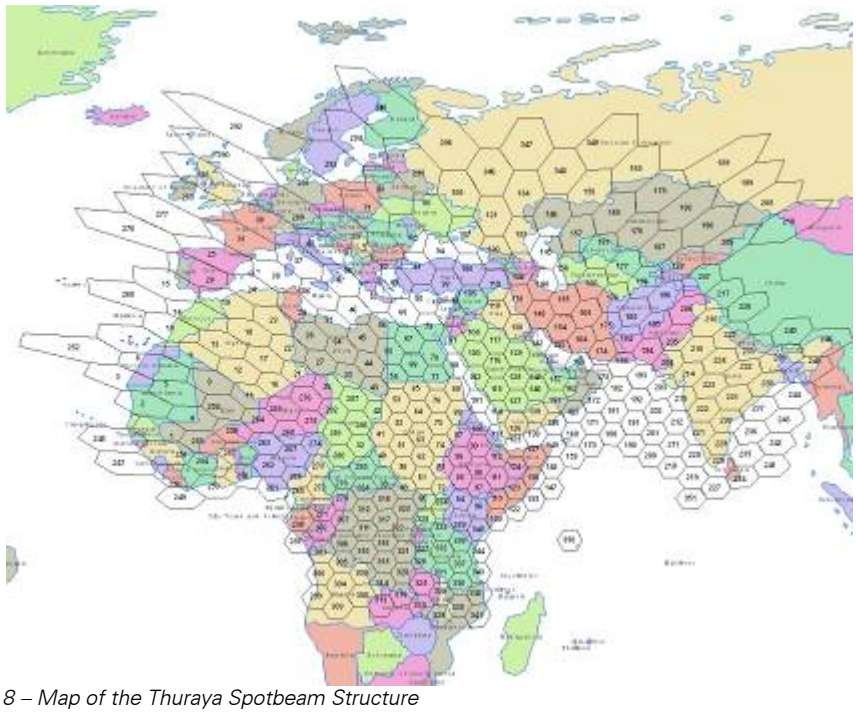


Figure 8 – Map of the Thuraya Spotbeam Structure

The strategic TMS can provide full duplex monitoring for a cluster of up to seven spotbeams centered on its geographical location. The addition of a Remote L-Band TMS can extend this coverage to another cluster of up to seven spotbeams anywhere within the coverage area of the Thuraya satellite.

The Remote L-band TMS should be connected to the strategic TMS via an 'always on' connection, such as a Leased Line, WAN, or satellite link (e.g. VSAT). In this way the Remote L-band TMS acts in a similar way to the L-band part of the strategic TMS. Information is passed across the remote link to ensure that the interceptions of two monitoring systems are synchronized. TRL recommend the use of a VSAT link for remote areas, and can offer this as part of a 'turnkey' solution if required.

The Remote L-band TMS comprises the following components:

Outdoor Equipment

- Flat Plate L-Band Antenna and Associated RF Cables

Rack Mount Indoor Equipment

- L-band Downconverter
- 12 Demodulator Cards are supplied as standard, in most cases this will enable L-band monitoring and call intercept of all traffic on the seven spotbeams surrounding the remote monitoring station. The demodulator cards are fitted into card racks, each housing 12 cards
- Server computer
- Uninterruptible Power Supply
- Ethernet Switch
- A full spares pack is also included

3- The Semi-Strategic Thuraya Monitoring System

The Semi-Strategic TMS operates in the same way as the Strategic Thuraya monitoring system, except that it is designed to work with a trailer-mounted 4.6m C-band antenna. Because of the reduced size of the antenna, it is not capable of intercepting the call content, instead it is used to monitor Thuraya activity in any spotbeam, providing the operator with the GPS positions of Thuraya terminals active within the spotbeams of interest, and the telephone numbers being dialed by these terminals.

The Semi-Strategic TMS comprises the following components:

- 4.6m Trailer Mounted C-Band Antenna
- Satellite Tracking Antenna Controller
- Satellite Beacon Tracking Receiver
- 4 C-Band Synthesised Tuneable Downconverters
- RF/IF Signal Distribution
- 10 MHz GPS Corrected Station Frequency Reference
- Demodulator Cards. A sufficient number of demodulator cards will be supplied in order to perform C-band only monitoring for up to 12 spotbeams
- Ethernet Switch
- Server Computer loaded with TMS Server software
- Keyboard, Video, Mouse (KVM) Drawer
- Uninterruptible Power Supply
- Laptop computer loaded with TMS Client software

Figure 9 – Typical Semi-Strategic TMS Antenna

4- The Tactical Thuraya Monitoring System

The tactical Thuraya Monitoring System operates in the same way as the strategic system, except that it only receives L-Band signals. In order for it to be able to intercept both side of a duplex call, as well as receiving the L-Band satellite downlink to the Thuraya terminal, it also receives the L-band uplink from the target terminal via radio line-of-sight.

The tactical system will intercept all of the same information available from a strategic system, but only for terminals with its radio line-of-sight. The range of the system can vary from up to 10 km in clear terrain and from an advantageous monitoring point, to as little as a few hundred meters in dense urban areas or inside buildings.

The tactical TMS comprises the following components:

- Flat Plate L-Band Satellite Downlink Antenna
- Flat Plate L-Band Target Downlink Antenna
- RF Cables
- Tactical TMS Chassis fitted with 6 Demodulator Cards, Ethernet Switch Card, IF/FRU Card, and a Dual Downconverter card
- Laptop Computer

A full spares pack is also included.

Figure 10 – Tactical Thuraya Monitoring System

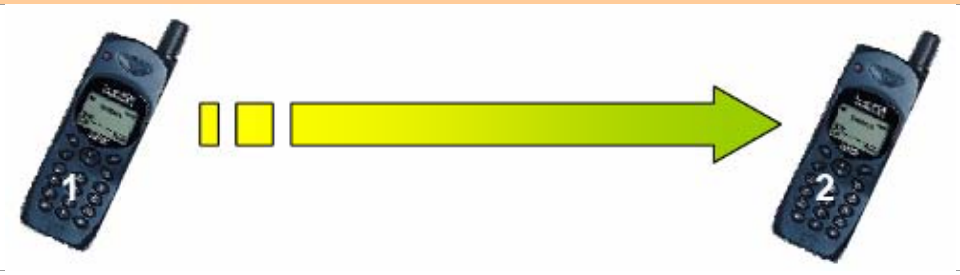
Thuraya Monitoring System Identities and information captured

In the following scenarios, the Thuraya terminal marked "1" is always assumed to be in the coverage area of the Thuraya Monitoring System (L&C Band):

Thuraya Makes Call to Landline	
Thuraya MES1 information captured: Date and time call made GPS Location TMSI IMEI	Landline Phone Information captured: Number
Call content captured: Duplex - Voice, SMS, Data*	

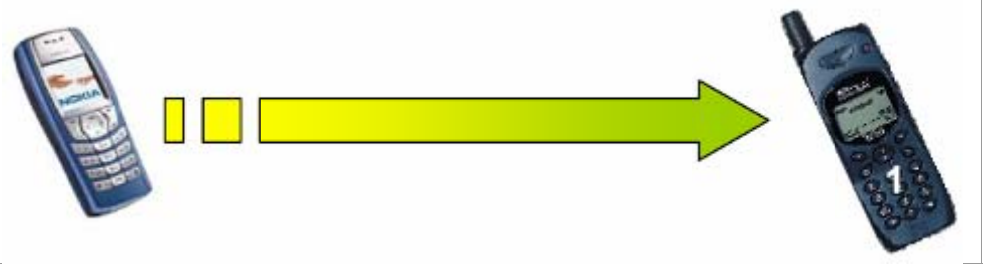
Thuraya Makes Call to GSM Phone	
Thuraya MES1 information captured: Date and time call made GPS Location TMSI IMEI	GSM Phone Information captured: Number
Call content captured: Duplex - Voice, SMS, Data*	

Thuraya 1 Makes Call to Thuraya 2 in Area covered by TMS (L&C Band)	
Thuraya MES1 information captured: Date and time call made GPS Location Number (ISDN) – if not blocked TMSI IMEI	Thuraya MES2 Information captured: Date and time call received GPS Location Number (ISDN) TMSI IMEI
Call content captured: Duplex - Voice, SMS, Data*	



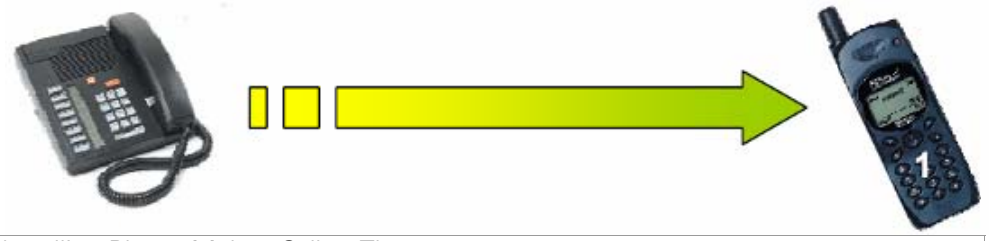
Thuraya 1 Makes Call to Thuraya 2 in Area not covered by TMS

Thuraya MES 1 information captured: Date and time call made GPS Location TMSI IMEI	Thuraya MES 2 Information captured: Date And Time (if C Band coverage) GPS Location (if C Band coverage) But it is not possible to 'pair' this event with the call made from MES1
Call content captured: Duplex - Voice, SMS, Data*	



GSM Phone Makes Call to Thuraya

GSM Phone information captured: Number (if not blocked)	Thuraya MES1 Information captured: Date and time call received GPS Location TMSI IMEI
Call content captured: Duplex - Voice, SMS, Data*	



Landline Phone Makes Call to Thuraya

Landline Phone information captured: Number (if not blocked)	Thuraya MES1 Information captured: Date and time call received GPS Location TMSI IMEI
Call content captured: Duplex - Voice, SMS, Data*	

Thuraya Switches on

Thuraya MES1 Information captured:
Date and time call received
GPS Location
TMSI
IMEI

Thuraya Switches Off

Thuraya MES1 Information captured:
Date and time
GPS Location
TMSI
IMEI

5- Recoverable File Types

Typical file types which will be recovered and viewable from e-mail attachments or file transfers (FTP) are as follows:-

Text files	Text, Rich text, Postscript, PDF
Web Pages	Text, HTML
Sound Files	Basic audio, x-aiff, wav
Pictures	Image files, gif, jpeg, pjppeg, tiff, x-png, x-bitmap bmp, x-jg, x-emf, x-wmf
Video clips	Avi, mpeg
Programs/applications	Base64, x-msdownload, octet-stream
Compressed files	x-compressed, x-zip-compressed, x-gzip-compressed
Application files, for Example	Microsoft Word documents Microsoft Excel spreadsheets Microsoft PowerPoint presentations Word perfect documents Lotus Notes documents

6- Protocols Supported

Underlying Protocols

The following Data Layer protocols are supported:

- SLIP
- PPP
- Synchronous
- PPP (Bit Stuffed Flag Frames)
- X Modem, Y MODEM

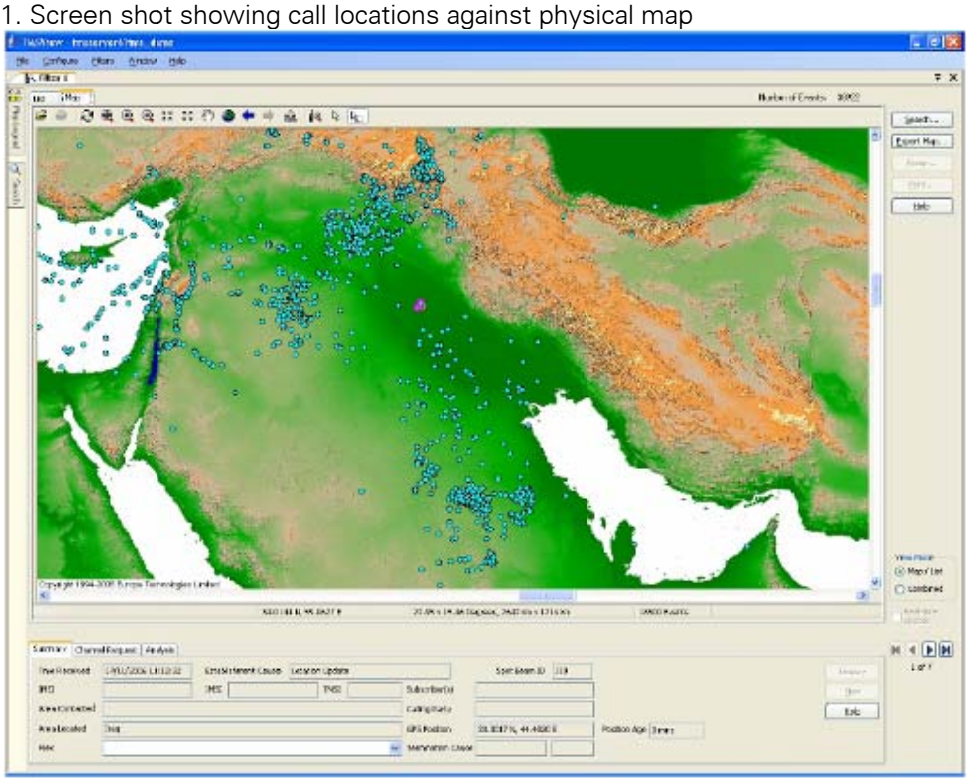
TCP/IP Protocols

- HTTP (WWW)
- FTP (File Transfer)
- POP3 (e-mail)
- SMTP (e-mail)

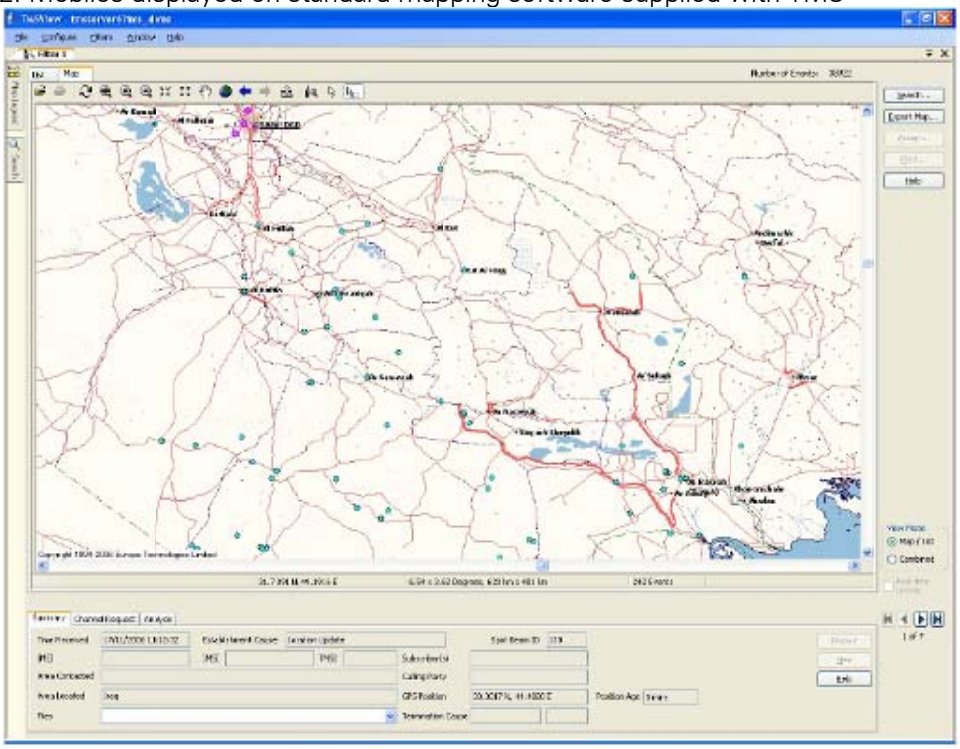
Modem Protocols (File Transfer)

- XMODEM,
- XMODEM-1K
- XMODEM-CRC
- YMODEM
- YMODEM-1K
- YMODEM-CRC

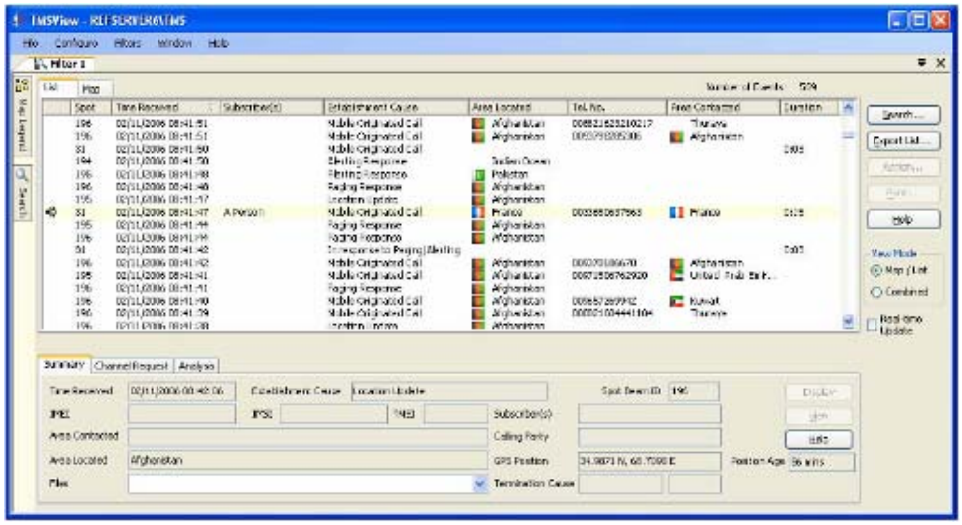
1. Screen shot showing call locations against physical map



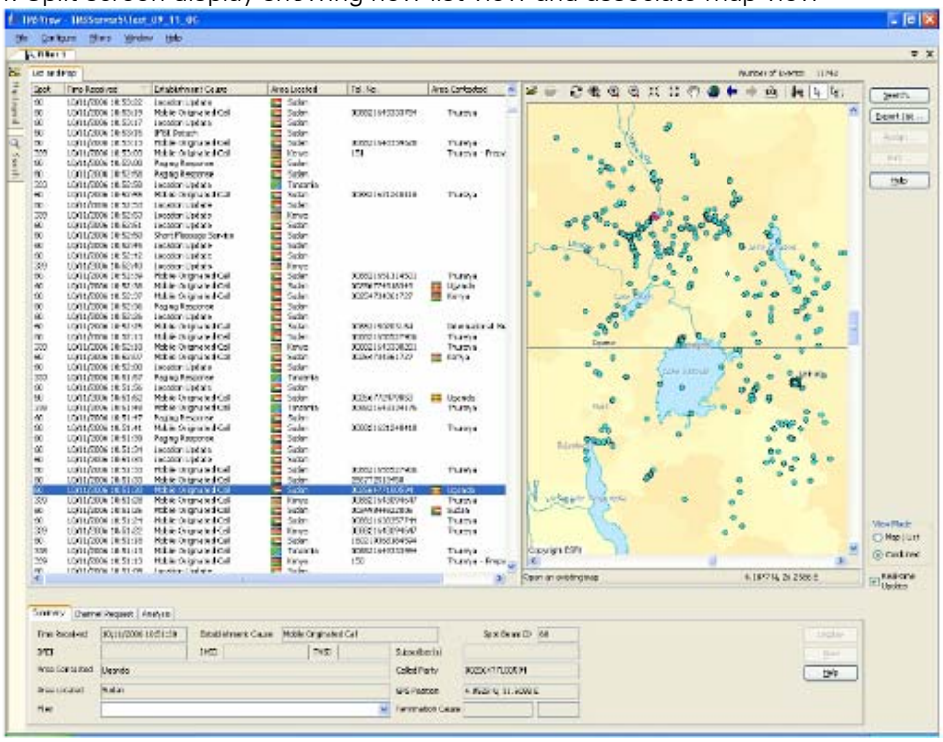
2. Mobiles displayed on standard mapping software supplied with TMS



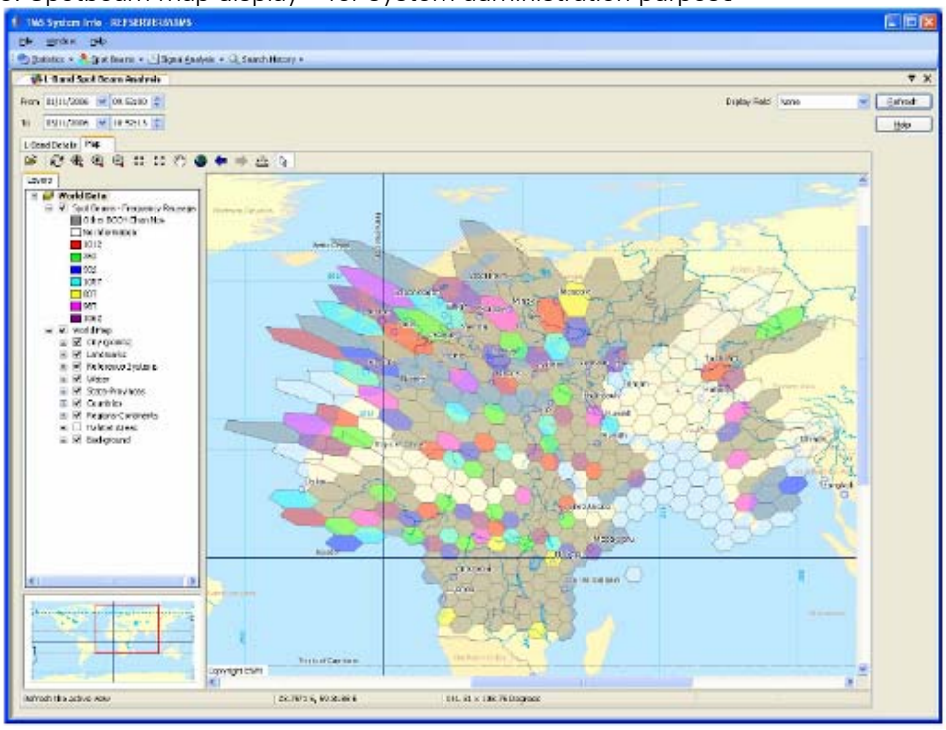
3. List View



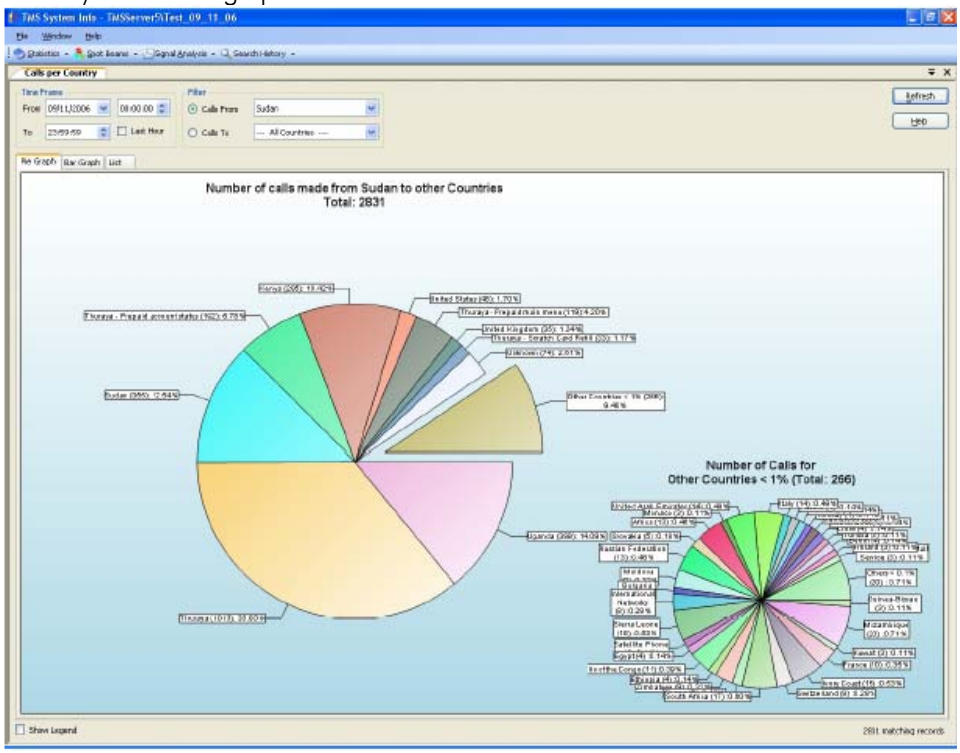
4. Split screen display showing new list view and associate map view



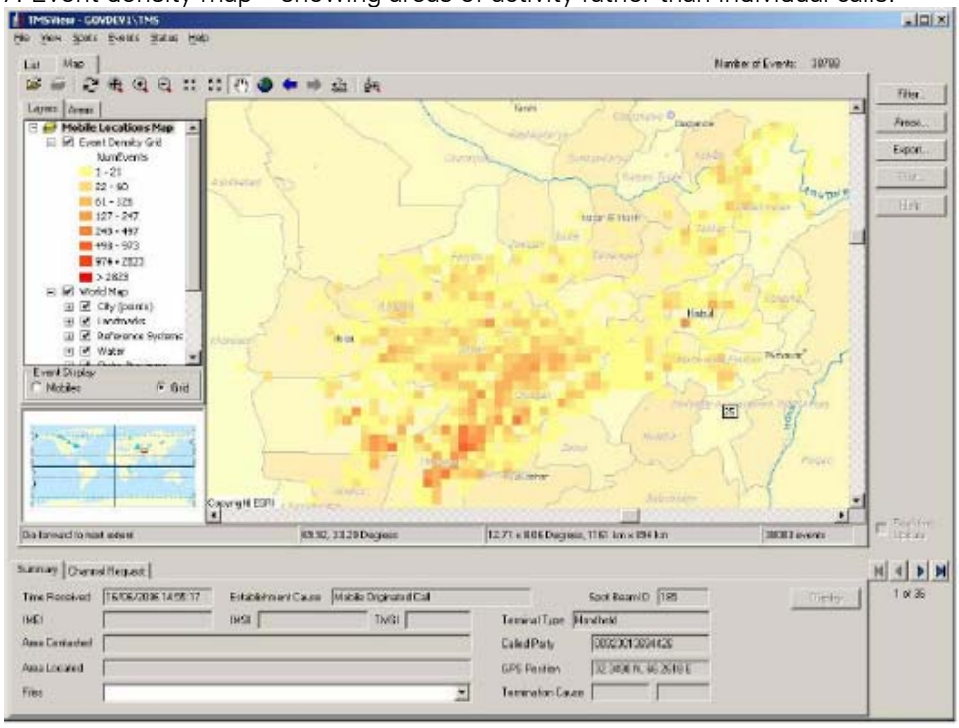
5. Spotbeam map display – for system administration purpose



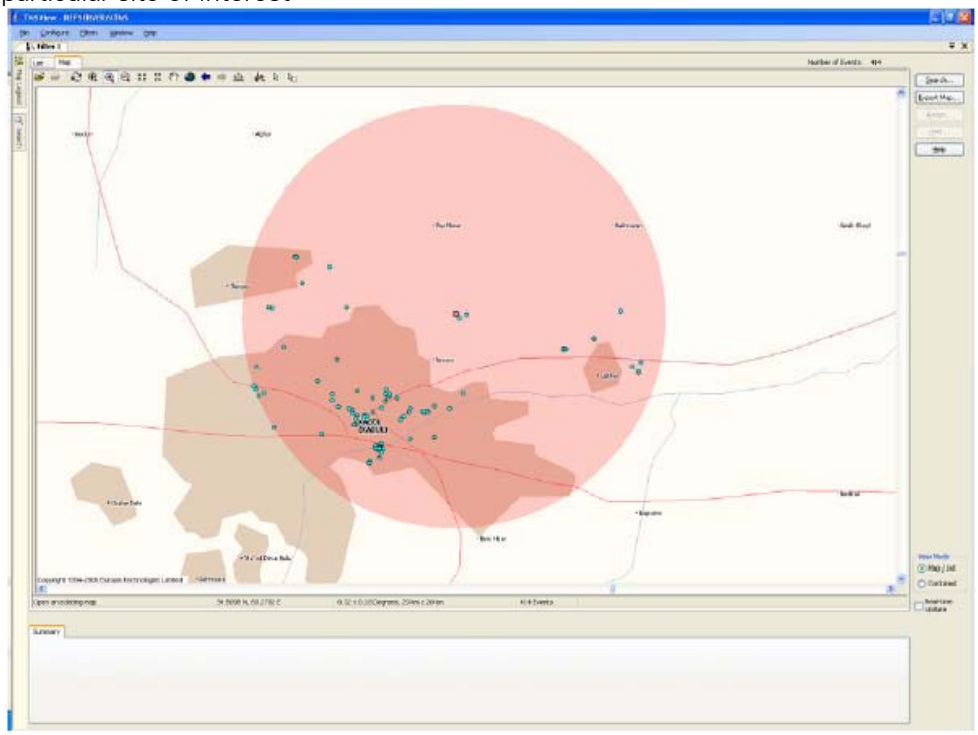
6. Analysis of calls graph - user definable



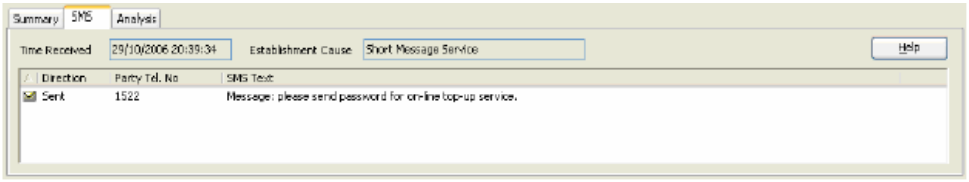
7. Event density map – showing areas of activity rather than individual calls.



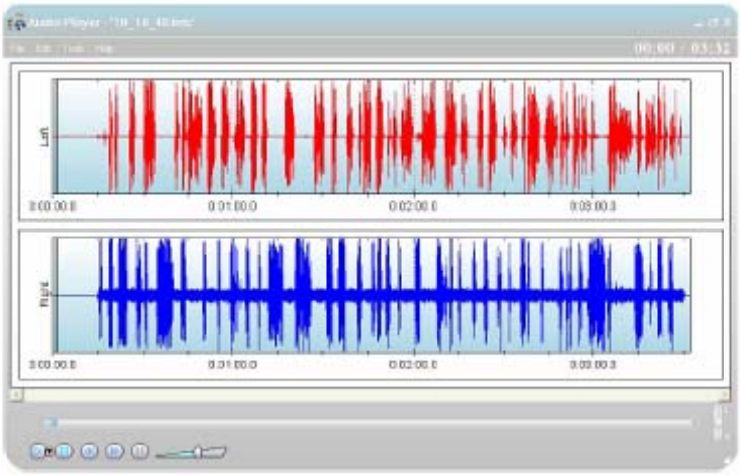
8. Geo-location map screen – to set up geo-fence area to filter calls from a particular site of Interest



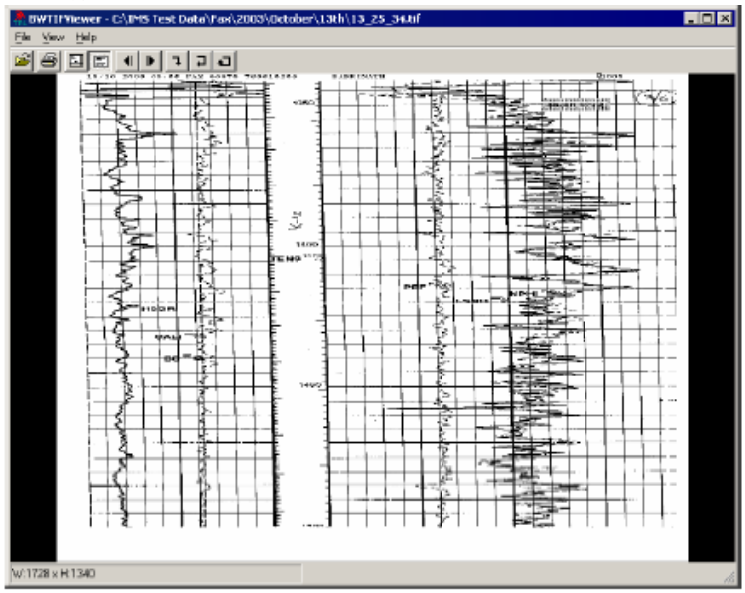
9. SMS View



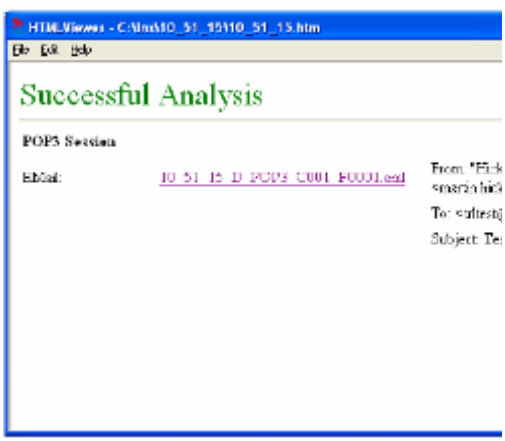
10. Audio Player

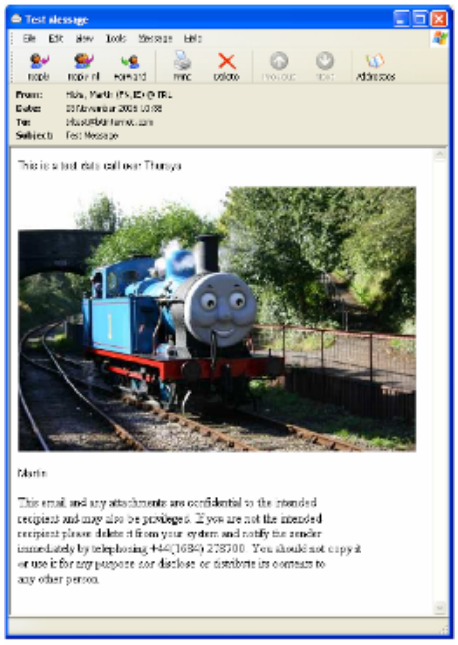


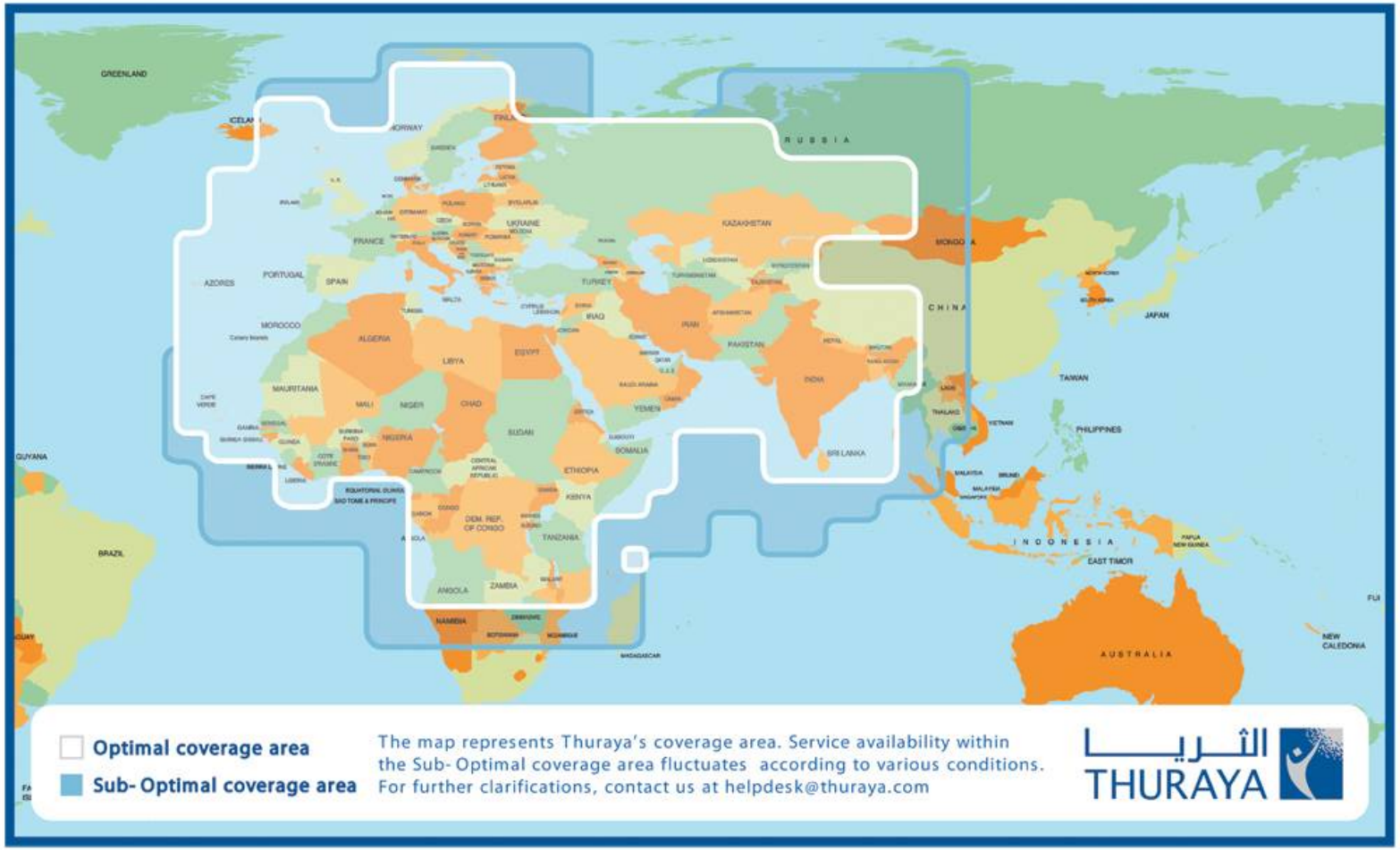
11. Fax View



12. Data View (POP3 example)







Marlin Portable Monitoring Unit

Overview

Marlin is a rapidly deployable system for the monitoring of calls made across the Inmarsat and Thuraya satellite systems. The call intercept is invisible to both the user and the satellite network.

Marlin enables traffic between the mobile terminal and the satellite to be monitored in a line of sight operation, within radio range of the target.

Control of the system is via an intuitive windows based GUI. Incoming calls are displayed in real-time, and voice is played via a laptop computer, with each side of the call played back on either channel of the stereo output. Software to decode and display a number of fax and data protocols is included with the GUI.

Information relating to the identification of called and calling parties is recorded, along with the geographical location (depending on service type and network).

Physical Description

The Marlin Portable Monitoring System comprises:

- Laptop
- Satellite and Target Antennae
- Marlin Portable Monitoring Unit
- Power Supply

These are supplied in travel cases for easy transport.

The monitoring unit itself is housed in a small desktop case (a rack mountable version is also available).
It contains the following removable cards:

- 2 x Multi-channel Demodulator Cards
- 1 x Dual L-band Down Converter

Each card sits horizontally and plugs into the unit from the front, allowing easy replacement of individual cards. A backplane provides power and signal distribution within the unit, along with accommodating an Ethernet Switch and Frequency Reference.

Key Features

Platform

- Satellite to ground monitoring in line of sight
- Intercept of up to 7 calls simultaneously
- Small, portable form factor
- Lightweight
- L-band 'Target' and 'Satellite' inputs
- Built in high stability reference
- 10/100BaseT Ethernet Control & Data Interface

Inmarsat

- B (including HSD)
- M
- Mini-M
- Gan (including HSD)

Thuraya

- Voice, Fax and Data
- Up to 3 spot-beams simultaneously monitored
- Up to TBC simultaneous calls

Technical Description

The Demodulator Card includes the following:

- Wideband High Speed ADC
- Digital Down-Converter
- Digital Signal Processor
- Ethernet Interface

The Demodulator Card accepts an instantaneous bandwidth of 34MHz, centered around 72MHz. The signal is filtered for image rejection, and then digitized by a high-speed analog-to-digital converter. Frequency-tuning is performed by a digital down converter (DDC). The resultant base-band signals are filtered by a programmable digital filter and DMA'd directly to the DSP for demodulation. The demodulated data is output via the Ethernet Interface.

The Dual Down Converter Card takes L-band input from the Satellite and Target antennas, and down-converts to the 72MHz required by the demodulator cards. Power is supplied to the antenna LNAs via the same connection, allowing rapid deployment. It features variable attenuation to accommodate the wide range of signal conditions experienced in the tactical environment.

The backplane provides a 10 MHz reference and IF input signal to each of the Demodulator Cards. The 10MHz frequency reference is derived from a temperature compensated crystal oscillator with a stability of 1ppm.

The Ethernet Switch provides 4 10/100BaseT auto-negotiating Ethernet ports. Two of the ports connect internally to the Demodulator Cards. The remaining two ports are connected to RJ-45 connectors on the front of the unit. One allows connection to the laptop required for control of the Marlin. The other is an expansion port. This allows a second unit to be 'daisy chained', so that both units may be controlled from a single laptop, or for the connection of compatible accessories.

Specifications

Ref Input	
Target Connector	BNC Female
Satellite Connector	TNC Female
Input Impedance	50 Ω
Target Attenuation	0 – 60 dB in 30dB steps
Satellite Attenuation	0 – 24 dB in 6dB steps
Target Frequency Range	1626.5 – 1660.5 MHz
Satellite Frequency Range	1525.0 – 1559.0 MHz
Internal Frequency Reference	
Reference Frequency	10 MHz
Reference Type	Temperature Compensated Crystal Oscillator (TCXO)
Reference stability	1ppm
Ethernet Control & Data Interface	
Connector	Female RJ-45
Number of Connectors	2
Interface Type	10/100BaseT auto-negotiating
Description	Command input/data and status output, daisy chain to subsequent unit
Physical	
Unit Dimension	135mm (h) x 315mm (w) x225mm (d) (excludes 19" rack mounting hardware)
Weight	5.2 kg unit standalone, 6 kg rack mounted
Unit contents	2 x Demodulator Cards 1 x Dual Down Converter
Card Size	233 (h) x 220 (d)
Color	RAL 9006 Light Grey
Operating Temperature	0°C to +40°C
Storage Temperature	0°C to +60°C
Relative Humidity	10% to 90% non-condensing
Cooling	Internal forced air cooling provided
CE Approval	
Safety	EN60950 LVD
EMC	EN55022 Emissions EN55024 Immunity
External Power Supply	
Voltage	115-230V AC
Frequency	60-50 Hz
Voltage selection	Auto-ranging
Power Consumption	250W
Dimensions	65mm (h) x 188mm (w) x 95 (d)
Weight	0.8 kg

Inmarsat Monitoring System

1- Introduction

1.1- General

This Proposal describes a basic Inmarsat monitoring system that provides automated interception and recording of selected Inmarsat calls within a single Ocean Region. The system is designed to be expanded very easily, or tailored to specific customer requirements as desired.

The Proposal should be read in conjunction with any attached TRL Technology Ltd (TRL) Commercial Letter.

1.2 Principles of IMS Operation

The Inmarsat series of satellites provide world-wide communications capability through a number of geostationary satellites, strategically located to provide overlapping coverage of the earth's surface to latitudes in excess of 80° North and South of the equator.

Communication between the satellite and Mobile Earth Stations (MES) is effected using frequencies around 1.6 GHz and 1.5 GHz for the uplink and downlink frequencies respectively. The fixed Land Earth Stations (LES) that provide connections to the terrestrial communications network communicate with the satellite using frequencies around 6.4 GHz and 3.6 GHz for the uplink and downlink frequencies. Additional channels are used for command and control/monitoring purposes.

Satellites currently providing the service are of the Inmarsat 3 generation. The older Inmarsat 2 series satellites used single, shaped beam antennas to optimise coverage over their designated areas. The current Inmarsat 3 satellites use a number of spot beams for communication with the MES which can be combined and reconfigured from the ground for optimum performance against changing operational needs. The IMS has been optimised to cater for spot beam operations, whilst retaining the flexibility required to revert to Inmarsat 2 standards if necessary.

Provided that the monitoring system is located within the coverage region of the satellite, the downlink to any MES can be monitored in the 1.5 GHz band. However, it is extremely unlikely that the corresponding uplink channel can be monitored directly, unless the MES is physically close to the monitoring system. MES uplink channels are therefore monitored by using the corresponding LES downlink channel around 3.6 GHz. This downlink channel may be Right or Left hand circularly polarised according to Inmarsat operational requirements.

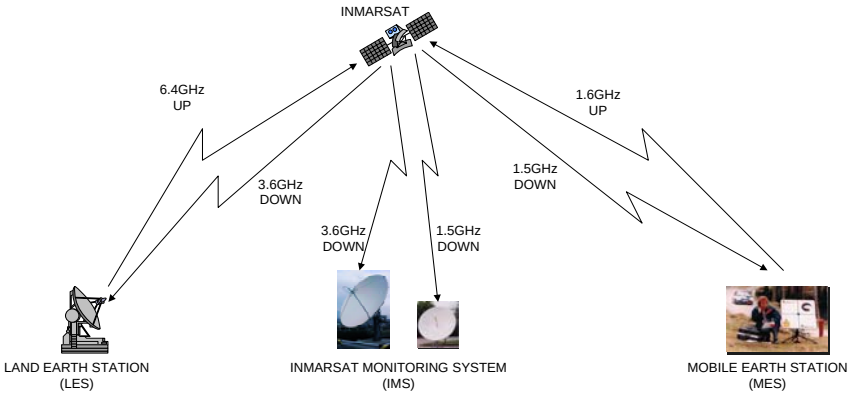


Figure 0-1 Principle of IMS operation

The Inmarsat system provides world-wide communications via a number of LES, several of which access the same satellite concurrently. A Network Control Station (NCS) co-ordinates the various LES to ensure that communications channels are allocated between the LES without conflict. The control channels between the NCS and LES also pass through the satellite, and are utilised by the IMS.

1.3- Call Intercept System Overview

The TRL Inmarsat Monitoring System (IMS) is designed to intercept and record voice, facsimile and data calls to and from selected terminals using the Inmarsat communications system. The IMS can be extensively configured to select terminals whose full identity is not known, or to log and/or record particular types of call, or to record calls made to particular parts of the world or to specific telephone numbers.

Voice calls may be monitored in real-time, or recovered and played back from the system database. Facsimile and data calls may generally be displayed with the simple viewer incorporated in the system, or exported for analysis or manipulation by other systems or with user-specific software.

The generic system is capable of monitoring and recording Inmarsat A, B, C, D, M and mini-M signals, including High Speed Data (HSD) signals used by B and M4 (GAN) terminals.

2- Technical Requirements

The flexibility of the IMS is such that it can be difficult for a Customer to decide on the system configuration that best satisfies his operational needs, until he has operated the system in his own environment. The IMS is designed to be expanded and modified by the addition of extra hardware and software as a Customer's requirements change and new services become available.

This technical proposal describes a basic, balanced Inmarsat monitoring system that can form the basis for more complex systems tailored to a Customer's specific requirements.

2.1- Intercept functionality

The baseline system is capable of receiving Inmarsat B, C, M, and mini-M transmissions from a single satellite, and for a single Ocean Region. This includes high speed data traffic from Inmarsat B and M4 terminals. Inmarsat A reception is also possible with this system, although decoding of A facsimiles requires an additional, and optional, software add-on.

The basic system is to capture and record up to ten simultaneous duplex communications with Inmarsat terminals against criteria selected by the users (IMS).

The basic system provides three workstations for signal analysis of recorded traffic, and for monitoring voice traffic "live".

2.2- Location of equipment

It is assumed that all the equipment will be located together at a single site.

A set of RF equipment, comprising antennas and other necessary hardware, must be located such that the length of cable between the antennas and the system rack does not exceed 80 metres, and the Ethernet cabling between the racks and computers does not exceed 100 metres.

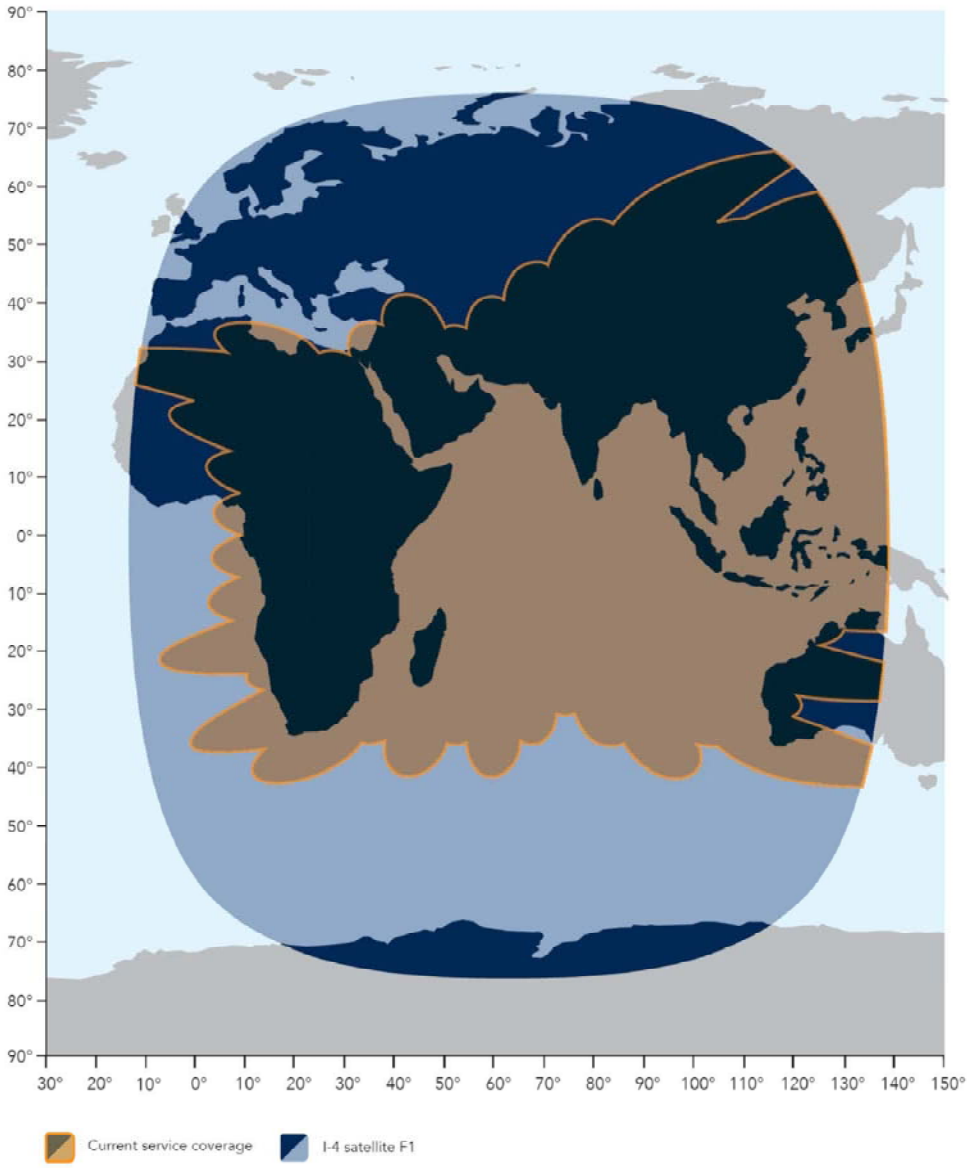
2.3- Implementation

The offer is for the provision of a turnkey baseline system to be installed by TRL personnel at the Customer's nominated site, complete with all necessary training, handbooks and support to enable the end users to operate and maintain the equipment. TRL will provide all the electronic equipment and antenna facilities required for the system.

The Customer must provide a suitable site with accommodation and furniture for the equipment, and suitable power supplies to operate the equipment and antennas.

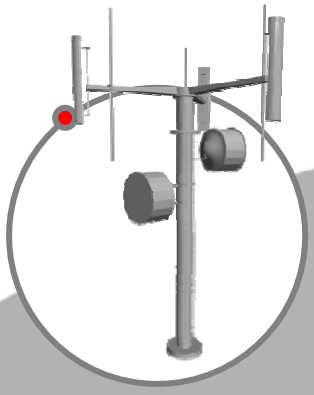
It is assumed that access to Customer's sites is restricted. TRL will co-operate with the Customer to utilise cleared/approved sub-contractors to perform the antenna civil works. The antennas and equipment rack will be installed by TRL technicians and subcontractors. All necessary security passes and clearances shall be provided by the Customer.

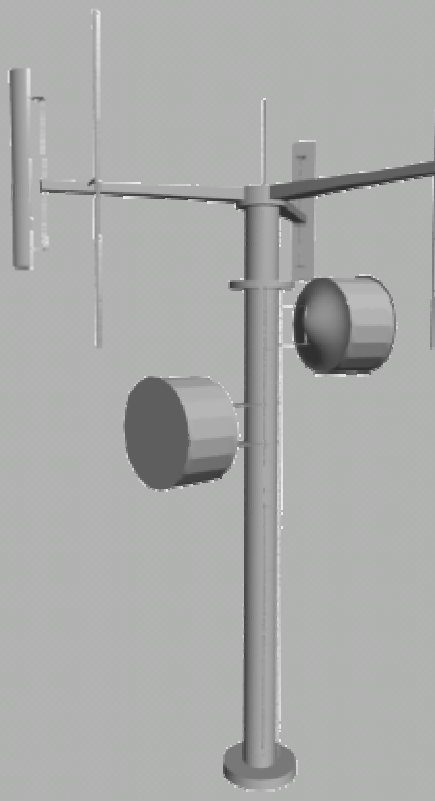
Service coverage for IsatPhone, LandPhone and FleetPhone



The map depicts Inmarsat's expectations of coverage, but does not represent a guarantee of service. The availability of service fluctuates depending on various conditions. Voice services coverage May 2007

Radio Frequency Monitoring





Index

RMS – Radio Monitoring & Direction Finding

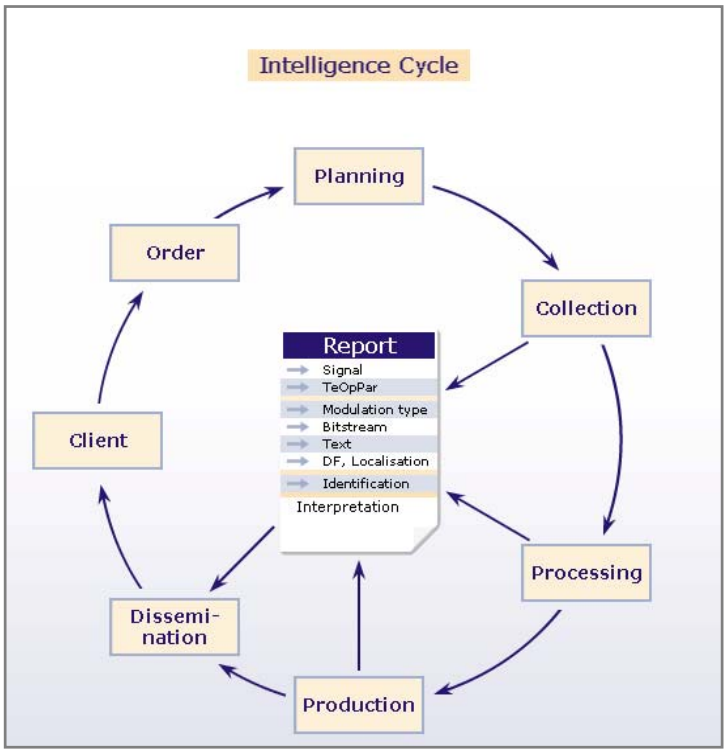
RMS – Radio Monitoring and Surveillance Solutions

Specialized in the application of the digital signal processing and pattern recognition to communication intelligence, we have the capability to design, produce and deliver complete RMS solutions. We offer comprehensive products for signal analysis, automatic detection & classification, demodulation & decoding, as well as for wideband signal acquisition & processing. We can supply the whole range, from a single stand-alone product to a complete RMS solution, from a single source.
And as an associate partner, we will also support and advise you in large high-tech projects,

COMINT System Design

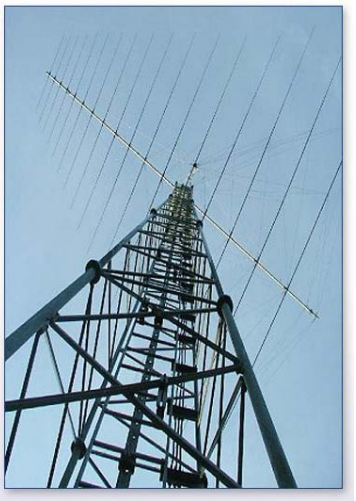
In close cooperation with our clients and partners, we have developed innovative ideas and concepts for tailor-made, integrated complete solutions.

You can trust our expertise to provide precisely the technology you require for all phases of the intelligence circle: from planning and direction, through collection and processing, to analysis, production and dissemination. We have developed system solutions for optimum collection of the information and data you have gathered, for discussing it in a team, and for its evaluation and distribution thus living you the best possible support throughout the entire *intelligence cycle.*



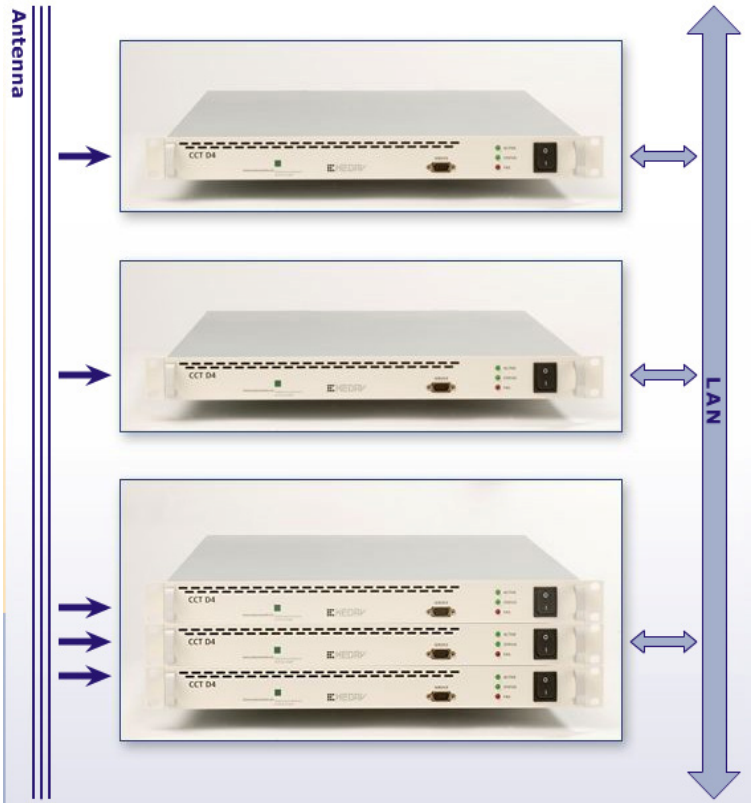
Antennas

By forging partnerships and joint ventures with other highly-specialized companies we can offer you a wide range of antennas for almost any task or application.



Tuners

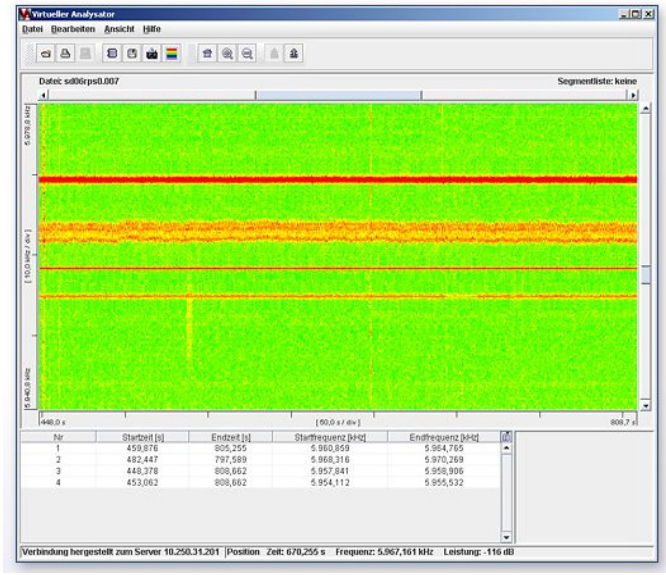
Innovation means: CCT - Because the ComCat CCT tuner can be seamlessly integrated into modern IT structures and concepts. Our tuners directly communicate with PCs and acquisition servers in the system. While just as powerful as conventional, highly-specialized receivers, they are much more flexible in the uses they can be put to. From synchronized multiple-channel reception, through various broadband analysis and evaluation options, to customized design, everything is possible. In IT networks, too, our tuners communicate smoothly with other servers and clients.

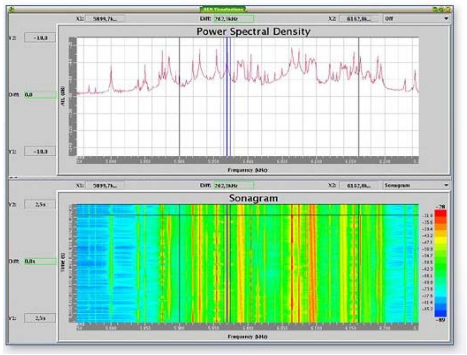


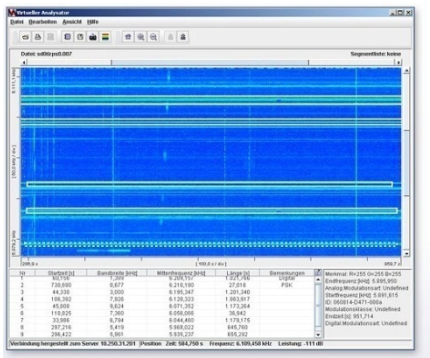
Broadband Technology

We are establishing new standards in broadband technology. This is the ideal method for reliably detecting all types of signals, including bursts or frequency hoppers. And significantly reduces the signal search, detection, and processing effort while improving performance. Excellent results are the outcome.

What about the costs? With broadband tuner technology you can now save on expensive signal processing hardware. Because this sophisticated processing software runs on standard PCs which means more flexibility and a system that is always up to date.







Broadband Search and Direction Finding Systems

Our CCT broadband tuners were also developed for use in direction finding or DF systems.
They include functions for:

- Synchronization and
- Calibration

The following DF algorithms are available:

- Watson Watt (HF)
- Amplitude correlation (VHF/UHF)
- Interferometer

We supply direction finding antennas for an abundance of different applications. Together with our partners we can supply a wide range in this area, too.

Signal Analysis

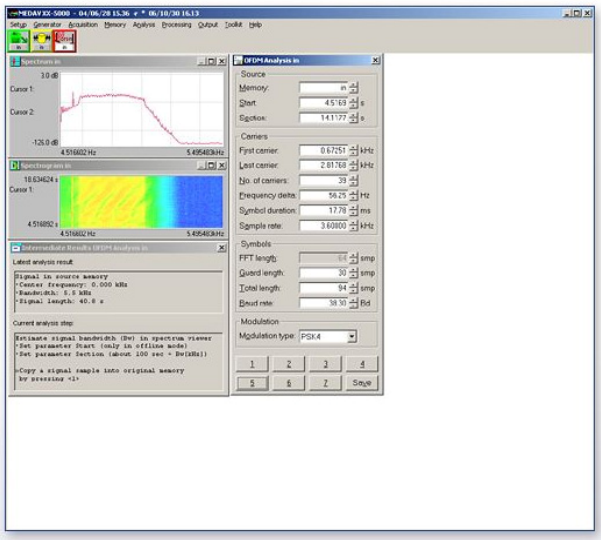
Elaman supplies innovative products and solutions for interactive signal analysis and signal processing:

For example:

- Time-signal analysis
- Spectrum analysis
- DF analysis

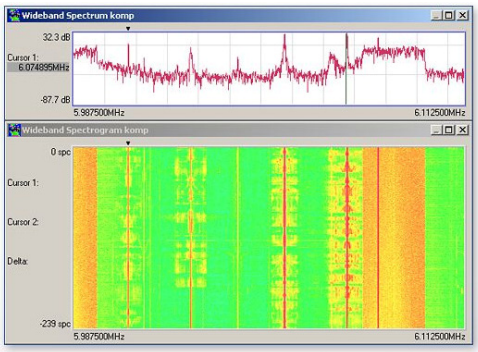
Or:

- Demodulation
- Decoding
- Classification

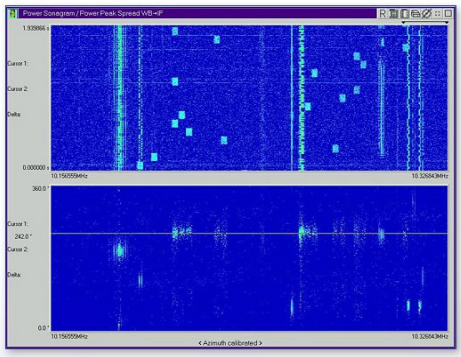


Time Signal Analysis

Using these sophisticated analysis algorithms and advanced COMINT signal processing, experts can also derive meaningful results for difficult signal scenarios providing a basis for swift and reliable decision-making.



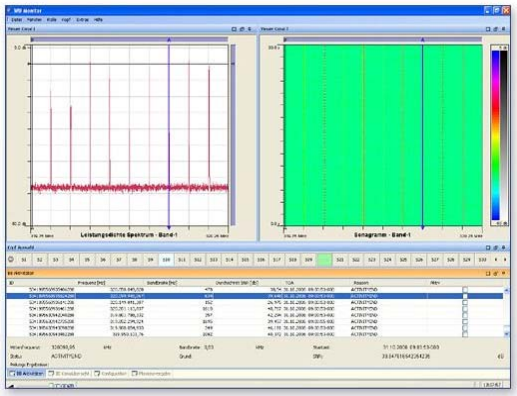
Spectrum Analysis

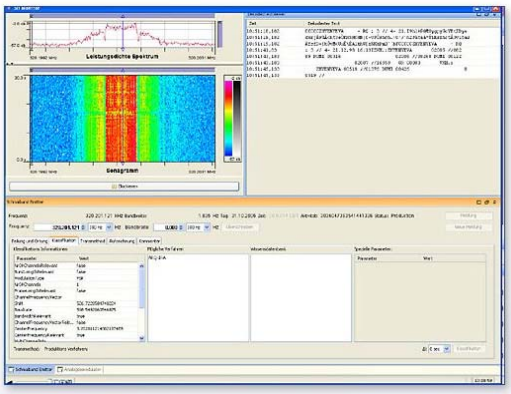


DF Analysis

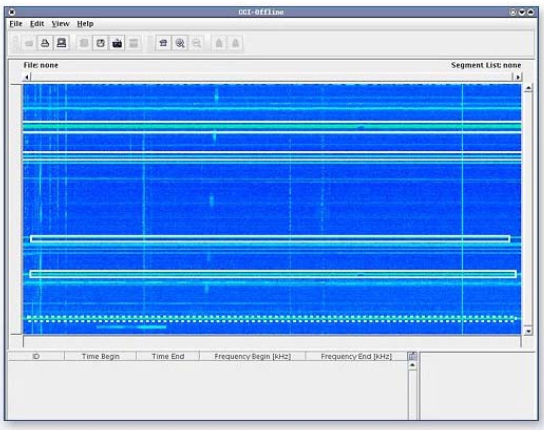
Signal Detection and Classification

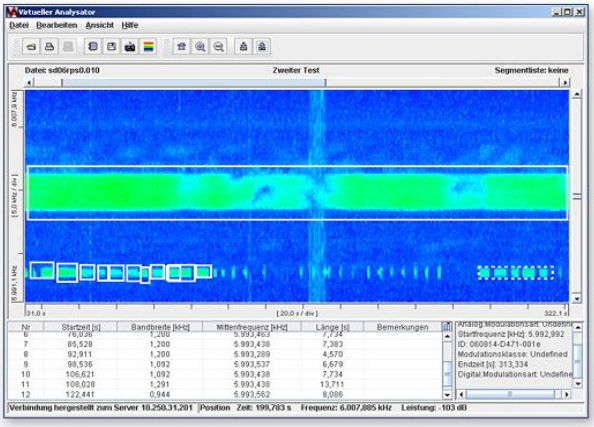
Our software allows signal detection and classification to be performed largely automatically. First, the program generates a symbolic representation of the broadband signal. Individual emitters are detected by the system and described as segments in the time-frequency domain. The meta data, too, are automatically added to the segments. The result is a list of emitters with all the important technical parameters, such as signals, spectrums, and modulation types, and other meta data.





Needless to say these data are decisive to further processing. If adequately conditioned, they provide an invaluable source of information. And secure the necessary knowledge advantage.





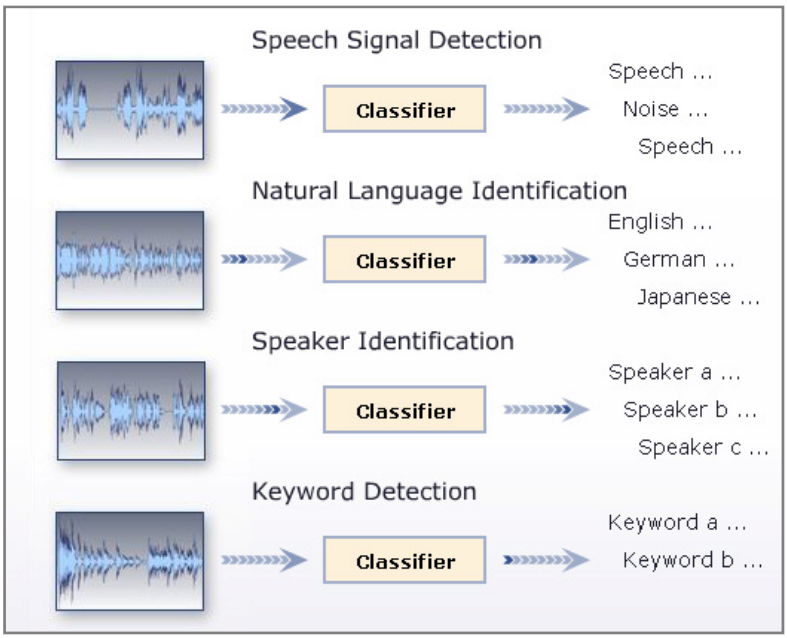
Speech Technology

We also develop programs and software for natural language technology and speech recognition. The human voice and language are very complex, so we work with the latest speech pattern recognition technology.

We can provide speech recognition software to solve the following tasks:

- Speech signal detection
- Natural language identification
- Keyword detection

We also supply training and configuration systems. So you can configure and train our language recognition software according to your needs simply and ergonomically.



Virtual Devices and PC-Based Architecture

Traditionally, conventional technical equipment for signal processing has comprised individual devices or dedicated hardware modules based on VXI technology, for example. This technology was tried, tested, and reliable, but also bulky, inflexible, and costly – by no means ideal.
So we have consciously sought new directions in the development of our equipment. Today, the virtual devices are software modules which boast the functions of hardware devices but run on commercially available PCs without any specialized hardware.

The advantages to you:

- More flexibility
- Improved integration into server-based IT systems
- Considerable cost savings

By separating the processor and software lifecycles no huge investment is ever needed to keep you equipment state of the art. Putting you in control of your future.

Production of finished Intelligence

Are you looking for an innovative but low-cost comprehensive RMS solution that works? Do you want to optimize the working processes in your operations to allow you to make the right decisions quickly and reliably? With us you have found what you were looking for.

With our system solutions we can help you to collate all the latest messages, reports and information, compare them with your own level of knowledge and evaluate them. The systems will support you with fast processing and reliable archiving of data and will enhance your internal communication. All the resources of your department, your experience, knowledge, and know-how, are exploited to the fullest. And we will provide the interfaces you need to ensure that cooperation with other departments and areas also runs smoothly.

We can even supply complete workstations including equipment, software, and technical support, if that is what you need. This makes use of synergies, optimizes work routines, and prepares and supports decision-making processes perfectly.

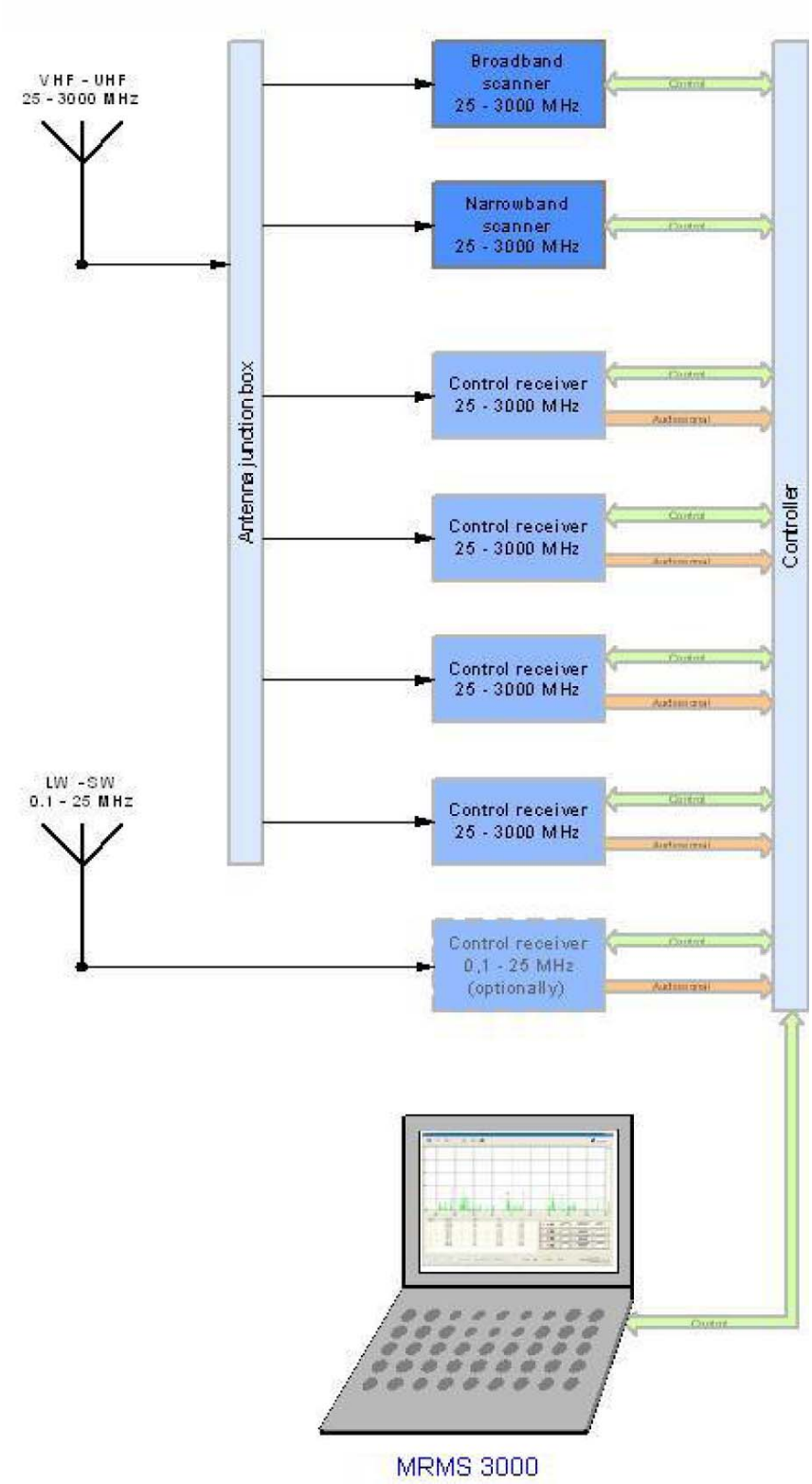
Tactical Portable Spectrum Monitoring System: MRMS 3000

The radio monitoring & analysis system MRMS 3000 has been developed for operational services. It has got a modular set-up and is used for swift radio monitoring within a frequency range from 25 MHz to 3 GHz.
Rapid FFT analysis allows of high-speed search run of ca. 20 MHz/s. Downstream monitoring receivers enable listening-in and recording of up to four signals simultaneously. Minimum response time between start of search run and activation of monitoring receiver is ca. one second.
By adding another search receiver, the frequency band can be extended to the 100 kHz to 25 MHZ range. Within this range, the search run speed is only 45 steps/s (i.e. step size of 12.5 kHz at 562.5 search run speed).

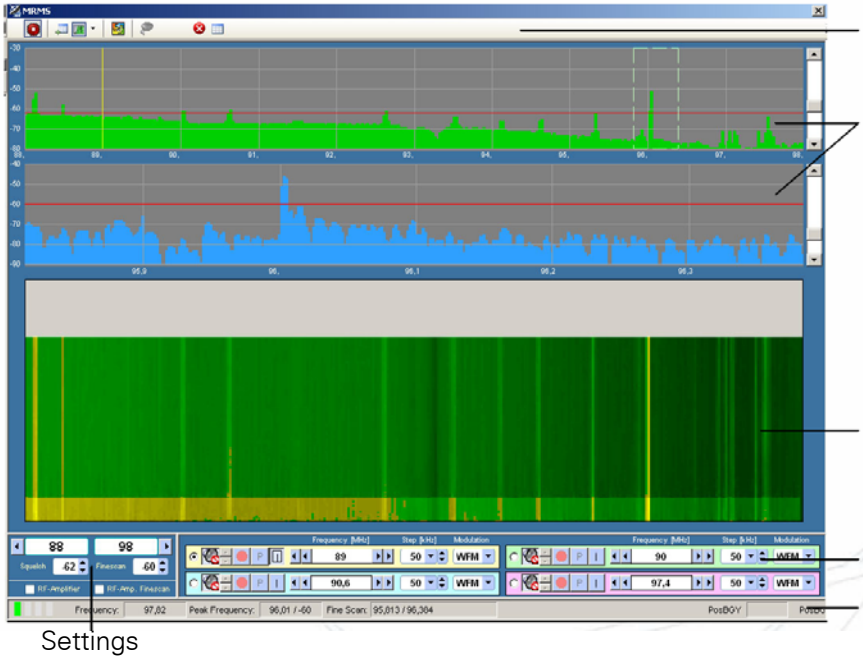
An easily operated software controls the system and assures the following functions:
- frequency band monitoring in search mode (search mode)
- analysis of radio signals
- demodulation and decoding of more than 100 standardised protocols

The system consists of:
- one broadband and narrow band receiver each
- up to 4 monitoring receivers
- a software-based demodulator, decoder and analyser
- a control processor
- aerial units (corresponding to respective frequency range)

System Overview



Programm Window



Operating modes

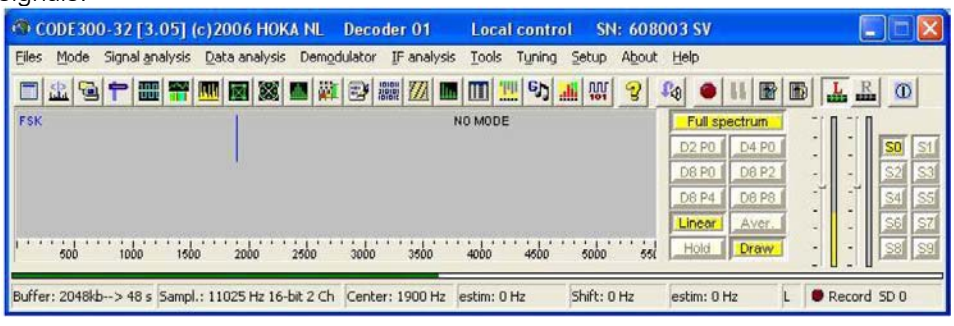
1. Search mode

Frequency search run with two adjustable cut-off frequencies. Parameters are modifiable (step size, reception level). Found reception signals will be stored in a frequency table.

From	To	Frequency	Command	Level	Squelch	RFamp
11.07.07 09:17:20	11.07.07 09:18:36	90,6	Radio Brocken	-56	-57	
11.07.07 09:17:19	11.07.07 09:19:12	92,6		-56	-57	
11.07.07 09:17:18	11.07.07 09:19:12	98,4		-53	-57	
11.07.07 09:17:18	11.07.07 09:19:12	96,05	Mr. X	-50	-57	
10.07.07 15:32:21	10.07.07 15:32:22	90,05		-57	-60	
10.07.07 15:32:19	10.07.07 15:32:26	96,05		-50	-60	
10.07.07 15:32:18	10.07.07 15:32:26	95,3		-60	-60	
10.07.07 15:32:18	10.07.07 15:32:26	92,6		-54	-60	
10.07.07 15:32:18	10.07.07 15:32:26	90,6		-56	-60	
10.07.07 15:32:18	10.07.07 15:32:26	90		-56	-60	
10.07.07 15:32:18	10.07.07 15:32:26	88,45		-52	-60	
10.07.07 15:32:18	10.07.07 15:32:26	88,1		-48	-60	
10.07.07 15:30:13	10.07.07 15:30:30	96,05		-49	-60	
	<=10.07.2007	>88				

2. Analysis of radio signals

A special software decoder takes on the analysis and demodulation of radio signals.



3. Demodulation and decoding

Demodulation and decoding are carried out by means of a special software. Supported codecs are the following:

Codecs & Protocols

Common Modes		**MFSK Modes**			
ASCII	☑	COQUELET 13	☑	STANAG 4285	☑
AUTOSPEC	☑	COQUELET 8	☑	STANAG 4529	☑
BAUDOT	☑	COQUELET 8 Auto	☑		
BAUDOT SYNCHR	☑	COQUELET 8 Auto Start	☑	**Audio Recording**	
BF6 BAUDOT	☑	COQUELET 8 FEC	☑	Radio Quality	☑
CW	☑	CROWD 36	☑	Telephone Quality	☑
CW II	☑	FIRE	◈		
FAX AM (SAT)	☑	PICCOLO 12	☑	**Signal Analysis**	
FAX FM (HF)	☑	PICCOLO 6	☑	AFP Oscilloscope	☑
HELLSCREIBER	☑			Analogue Oscilloscope	☑
PACKET AX 25	☑	**CIS Modes**		Auto Classification	☑
PACTOR I	☑	405 391	◈	Eye Pattern	☑
PACTOR II	☑	81-29	◈	FFT Special with zoom	☑
PSK 31	☑	81-81	◈	FSK Oscilloscope	☑
SITOR A/B Auto	☑	BAUDOT F7B	☑	Phase Oscilloscope	☑
SSTV	☑	BEE 36-50	◈	Phase Plane	☑
		CIS 11 TORG 10/11	☑	Phase Spectrum	☑
Special Modes		CIS 12 FIRE	◈	Shift & Speed Measurement	☑
AUM 13	◈	CIS 14 TORG 14	☑	Straddle	☑
EPIRB	☑	R 37	◈	Waterfall	☑
GMDSS HF	☑			Waterfall and sonogram	☑
HF Datalink	☑	**Selcall**			
IRA ARQ	☑	ARINC ANNEX 10	☑	**Data Analysis**	
MEROD	☑	CODAN 8500 Selcall	☑	Bit Analysis	☑
NUM 13	◈	CCIR1	☑	Character Analysis Duplex	☑
SKYFAX	◈	CCIR2	☑	Character Analysis Simplex	☑
TWINPLEX	☑	CCITT	☑	Character Count	☑
VISEL	☑	CTCSS	☑	Correlation Bit	☑
GW DATAPLEX	☑	DCSS	☑	Correlation Mode	☑
		DTMF	☑	Correlation VHF	☑
ARQ Modes		EEA	☑	ITA 2 Analysis	☑
ARQ 2 TDM 242	☑	EIA	☑	Speed Bit Analysis	☑
ARQ 4 TDM 342	☑	EURO	☑		
ARQ 6 70	☑	NATEL	☑		
ARQ 6 90/98	☑	TT Classification	⇨	**IF Analysis**	
ARQ 625 SITOR A	☑	VEDW	☑	Spectrum	☑
ARQ DUPLEX	☑	ZVEI 1	☑		
ARQ E	☑	ZVEI 2	☑	**Tools**	
ARQ E3	☑	ZVEI ITA xtone	☑	Audio Inverter	☐
ARQ POL	☑			Data and Text editor	☑
ARQ S ARQ I00S	☑	**VHF / UHF Modes**		DCF 77	☑
ARO SWED	☑	ACARS SITA	☑	RS232 Output	+
HC ARQ	☑	ATIS GMDSS	☑	Generator	☑
RS ARQ	☑	CITYRUF	☑	LMS Filter	☐
RS ARQ MERLIN	☑	ERMES	☑	Modulation Classifier	☑
TOR DIRTY	☑	FLEX	☑	Alphabet Mapping	☑
		FMS BOS	☑	TEXT Scanning	☑
FEC Modes		GOLAY	☐	Editing all code tables	+
FEC 100	☑	MDT	☑	Two channel audio input by lan	+
FEC I00 dirty	☑	MPT 1327	☑	Bit stream out from MIL modes	+
FEC I00 Interleaved	☑	POCSAG	☑	RAW ASCII text save	☑
FEC I00 Raw	☑	INMARSAT-C	☑		
FEC A	☑	INMARSAT-C TDMA	☑		
FEC B SITOR B	☑			Analogue Classifications	⇨
FEC S	☑			Digital Classifications	⇨
HNG FEC	☑				
ROU FEC	☑	**MIL STD 188 Series**			
		MILSTD 188 110 Serial	☑		
		MILSTD 188 110 39 tone	☑		
		MILSTD 188 141 ALE	☑		
Available	☑	In preparation	☐	No information available	◈
Optional	+	Available but not tested	⇨		

Technical Data

Search receiver	2
Receiver type	threefold frequency conversion with rapid FFT analysis
Sensitivity	AM: 25- 225 MHz 0.6 µV (10 dB S/N) 225-1700 MHz 0.8 µV NFM: 25-1700 MHz 0.35 µV (12 dB SiNAD) 1700-2700 MHz 0.6 µV 2700-3000 MHz 1.5 µV WFM: 25-1700 MHz 2.0 µV (12 dB SiNAD)
Search speed	20 MHz/s

Monitoring receiver	max. 4
Receiver type	PLL-controlled with threefold frequency conversion
Sensitivity	AM: 30- 470 MHz 0.32 µV (10 dB S/N) NFM: 30- 470 MHz 0.23 µV (12 dB SiNAD) 470-1000 MHz 0.45 µV 1000-1300 MHz 2.5 µV 1300-2040 MHz 1.7 µV 2040-3000 MHz 15 µV WFM: 30- 470 MHz 1.5 µV (12 dB SiNAD)
Modulation modes	WFM, NFM, SFM, WAM, AM, NAM, USB, LSB, CW
Selectivity (@6dB):	
SSB/NAM	3 kHz
AM/SFM	6 kHz
WAM/NFM	12 kHz
WFM	150 kHz (@3dB)

Power supply	12 VDC 4.0 A AC/DC adaptor 115 ... 230 V AC/50 ... 60 Hz, 300 W (included in scope of delivery)
Dimensions	430 x 340 x 235 mm
Weight	approx. 15 kg

Scope of delivery:	MRMS 3000 Telescope aerial, user's manual, PSU, transport box
Optional:	Frequency band enhancement from 100 kHz, additional aerials

elaman
GERMAN SECURITY SOLUTIONS

Computer Monitoring & IT Intrusion

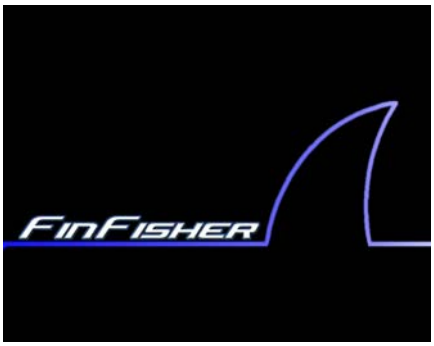
Index

1. FinFisher Introduction

The philosophy behind the FinFisher IT intrusion package is to provide the government end-user with today's advanced hacking tools and techniques to enable Intelligence Agencies to use such hacking components to obtain Intelligence information that cannot be obtained any other way. The Intrusion tools can be used by Government Departments for internal introduction/training to the hacking threats being faced today.

Features

- Information Gathering
- Sniffing
- Exploitation



FinFisher Products

FinFisher IT Intrusion Programe consists of the following FinFisher Products:

FinFisher HQ	Graphical user interface HQ software for FinFisher 1 and 2
FinFisher 1	Extract locally stored user accounts, system and network information from the target PC.
FinFisher 2	Make a copy of all locally stored e-mails and get a copy of all local files with given file-extensions.
FinFisher 3	2 bootable CD-ROMs to: a) Clear the Windows Administrator account password and b) Wipe all local hard-disks.
FinSpy	A trojan-horse-like software for remote surveillance of one or multiple target systems.
FinFly	A transparent HTTP proxy that can modify executables while they are being downloaded.

FinFisher Hacking PC	Robust notebook including FinTrack and Windows system which both are loaded with all up-to-date hacking tools including scripts for easier usage and automatism. This package also includes special hardware like a high-power Wireless LAN adapter, a modified Bluetooth dongle and 2 wireless antennas.

Finfisher Training

Basic Hacking Course	1 or 2 week basic hacking course covering up-to-date hacking tools and techniques (using the FinFisher Hacking PC). *Topics include:* Profiling, Attacking and many more.
Exploiting Software	1 week course covering techniques to discover and exploit bugs in software. *Topics include:* Software bugs, Shellcode, Exploit archives / frameworks, writing custom exploits, etc.
Root kits	1 week course covering root kit / trojan horse techniques. *Topics include:* Analysis, usage and development of professional root kits.
Hacking VoIP	1 week course covering various techniques to eavesdrop Voice-over-IP communication, get access to accounts and more. *Topics include:* RTP sniffing, RTP injection, SIP account brute-forcing, SIP password cracking, etc.
Wireless Hacking	1 week course covering different Wireless hacking techniques including Wireless LANs, Bluetooth and wireless keyboards. *Topics include:* WEP / WPA cracking, Bluetooth Sniffing and Link-Key cracking, etc.
Covert Communication	1 week course covering covert communication techniques and programs. *Topics include:* Steganography, cryptography, network protocols, etc.

FinFisher Services

FinAudit	Professional 1 or 2 week penetration testing of local network to discover possible attack vectors and ensure the security of the network.
Optional	Alternatively, ask to join our restricted to government only one-day intrusion seminar. For further information on the above products please contact our IT department.

The FinFisher Project – Function and Purpose

In essence, it is an aggressive IT hacking component. It utilizes and incorporates Black Hat Hacking tactics to enable Intelligence Agencies to be able to gather information from target systems that would otherwise be extremely difficult to obtain legally.

The FinFisher Project operates on the understanding that there is a need for "authorized" Agencies to obtain information, using such methods, as they need to be pro-active against the strategies and tactics employed by their Targets. They can then alert the appropriate Law Enforcement or Military units and organizations within their country to intercept and prevent an incident, as opposed to reacting after.

The System has also been developed with operational simplicity in mind, so that Intelligence operators require the minimum of technical ability and skill when using the tactical components within the FinFisher Project.

The FinFisher Project is scalable, thus becoming more complex in capability and operation as the objectives of the user become more complex, and their knowledge and understanding of the Systems they are attacking become more advanced.

Appropriate Note

The FinFisher System has been developed to assist Intelligence Agencies obtain information from civilian individuals and groups. It is not intended, or has it been tested, to see if it has the capability to break into advanced complex government or military security systems with secret, or above security, classification.

Also, while every effort has been made to ensure the FinFisher Project can get past known Anti-Virus and Anti-Spyware Products and local Firewalls and Security, no guarantees are given in this area as these products are continuously being developed on a daily basis.

Also no guarantees can be given as to the effect these products have on the target's PC. They are designed to remove information as discreetly and covertly as possible. But each system can react differently depending on settings, applications and configurations, so the result is unknown.

Recommended Finfisher Kits

FinFisher Starter Kit – This kit includes *FinFisher 1, 2, 3, HQ* and the *FinFisher Hacking PC* kit.

FinFisher Software Kit – This kit includes only *FinFisher 1, 2, 3* and *HQ*.

2. FinFisher Products

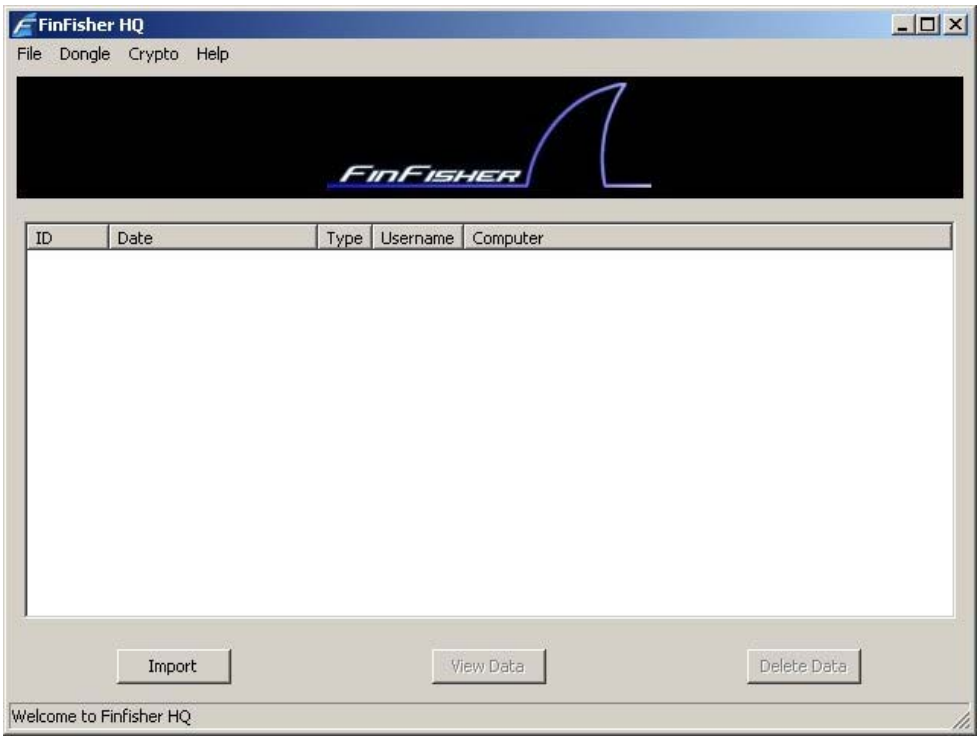
FinFisher HQ

The FinFisher HQ software is the main software for FinFisher 1 and 2. It is used to configure the operational options of those 2 devices and to import / decipher the gathered data and generate reports according to the FinFisher type.

It can also be used to update and repair FinFisher 1 and 2 device systems.

The FinFisher HQ Software shows all gathered and imported data in a sorted list.

Screenshot



FinFisher HQ supports Windows systems equal to and newer than Windows 2000. It is pre-installed on the FinFisher Hacking PC.

FinFisher 1

FinFisher 1 is an U3-enabled USB device that is activated when inserted into the targets system with no or little user intervention.
The functionality is configured using the FinFisher HQ software. Also the gathered data is deciphered, imported and analysed by the FinFisher HQ software.

The data collected by the device is stored in encrypted form and can only be decrypted and accessed at the head-quarter where the HQ software is running. It uses a private- / public-key cryptography mechanism by utilizing various known algorithms.

This prevents data from being disclosed or the device being misused if it gets lost or stolen. Also the operational agent cannot be forced to decipher the data as he needs the private key which remains on the HQ system.

The device indicates when the data gathering process is done so the agent knows when to remove it from the system.
If removed prematurely, due to operational necessity, the device will not be damaged or compromise the security of the gathered data or the software contained on the device.
The device contains a component that deactivates and then reactivates all known installed Anti-Virus / Anti-Spyware software.
The device contains the following data gathering capability (subject to the information being available on the target's PC and accessible by the FinFisher device):

- Display Windows user accounts and password hashes
- Display details of passwords and other email accounts information on the following email applications: Outlook Express, Microsoft Outlook 2000 (POP3/SMTP Accounts only), Microsoft Outlook 2002, IncrediMail, Eudora, Netscape Mail, Mozilla Thunderbird, Group Mail Free, and Web-based email accounts.
- Display username and password details of MSN Messenger, Windows Messenger (Windows XP), Yahoo Messenger (Version 5.x/6.x), ICQ Lite 4.x/2003, AOL Instant Messenger, AOL Instant Messenger/Netscape 7, Trillian, Miranda, and Gaim / Pidgin
- Display stored passwords for network shares
- Display details of all Dial-Up accounts, including the user name, password, and the domain
- Display the details of the lost password of Outlook .PST (Personal Folders) file
- Display stored remote desktop passwords
- Display passwords stored by the Internet Explorer
- Display the list of all LSA secrets stored in the registry. The LSA secrets may contain RAS / VPN, Auto-logon and other system passwords / keys.
- Display the content of the protected storage which might contain various passwords
- Display the list of all installed Windows updates (Service Packs and Hotfixes)
- Display the product ID and the CD-Key of MS-Office, Windows, and SQL Server
- Display the list of DLLs that are automatically injected into every new process

- Display the list of all processes currently running. For each process, it lists all modules (DLL files) that the process loads into memory. For all processes and modules, additional useful information displayed is: product name, version, company name, description of the file, and the size of the file

- Display the list of all applications that are loaded automatically when Windows boots. For each application, additional information is also displayed (product name, file version, description, and company name)

- Display the list of all currently opened TCP and UDP ports. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, and so on), the time that the process was created, and the user that created it

- Display information about the target network adapters: IP addresses, hardware address, WINS servers, DNS servers, MTU value, number of bytes received and sent, the current transfer speed, and more. In addition display general TCP/UDP/ICMP statistics for the target computer.

- Display all information from the history file on the target computer, and display the list of all URLs that the target has visited with the Internet Explorer browser in the last few days.

- Display the details of all wireless network keys (WEP / WPA) stored by the 'Wireless Zero Configuration' service of Windows XP

- Display all auto-complete e-mail addresses stored by Microsoft Outlook

- Display all cookies stored by Mozilla Firefox

FinFisher 1 supports Windows systems equal to and newer than Windows 2000.

FinFisher 2

FinFisher 2 is an U3-enabled USB device that is activated when inserted into the targets system with no or little user intervention.

The functionality is configured using the FinFisher HQ software. Also the gathered data is deciphered, imported and analysed by the FinFisher HQ software.

The data collected by the device is stored in encrypted form and can only be decrypted and accessed at the head-quarter where the HQ software is running. It uses a private- / public-key cryptography mechanism by utilizing various known algorithms.
This prevents data from being disclosed or the device being misused if it gets lost or stolen. Also the operational agent cannot be forced to decipher the data as he needs the private key which remains on the HQ system.
The device indicates when the data gathering process is done so the agent knows when to remove it from the system.

If removed prematurely, due to operational necessity, the device will not be damaged or compromise the security of the gathered data or the software contained on the device.
The device contains a component that deactivates and then reactivates all known installed Anti-Virus / Anti-Spyware software.
The device contains the following data gathering capability (subject to the information being available on the target's PC and accessible by the FinFisher device):

- Make a copy of any locally stored emails (Microsoft Outlook / Outlook Express, Mozilla Thunderbird, Opera Mail).

- Make a copy of files with a specific file extension after making a search through all local drives

FinFisher 2 supports Windows systems equal to and newer than Windows 2000.

FinFisher 3

FinFisher 3 are 2 bootable CD-ROMs.

The devices have to be inserted and the target system has to be rebooted. Little user-interaction is required during the whole process.
If removed prematurely due to operational necessity, the device will not be damaged.

The devices contain the following functionality:

- Clear the Windows Administrator password
- Securely wipe the local hard-disks

FinSpy

FinSpy is a professional trojan horse for Windows systems.

It can be used to monitor one or multiple targets PC's including their online activities, logging every keystroke, getting access to their accounts and so on.

FinSpy contains 3 components:

- Client
- Proxy
- Trojan

The client software is used by the agents to generate the trojan executable and communicate with the proxy server to access individual infected systems.
The trojan executable, on infection, connects back to the proxy server to publish its online status.
All network data is encrypted using a private- / public-key cryptography mechanism by utilizing various known algorithms.

FinSpy supports Windows systems equal to and newer than Windows 98.

FinFly

FinFly is a transparent HTTP proxy that can modify content while it is being downloaded.

It can be used infect executables that are downloaded from a webserver with FinSpy or custom trojan horses.

Using the configuration file, IP addresses can be selected which means that only a certain range or a single address is going to be infected or a certain range should be ignored by the proxy.

FinFly comes with a special loader that merges the trojan horse with the original executable. On execution, the trojan gets installed, is removed from the original and then the original executable gets executed. Using this technique, most common malware detection mechanism of common Anti-Virus / Anti-Spyware utilities can be bypassed.

Optional the proxy can be extended to modify any other file types and also totally replace files while they are being downloaded.

FinFly supports Linux systems equal to and newer than 2.6. Windows and BSD support can be added on request.

FinFisher Hacking PC

The FinFisher Hacking PC consists of a robust notebook plus various hacking equipment.

It can be used to locally (Wireless LAN, Bluetooth) or remotely attack single systems or networks. The kit is equipped with all generic components that are used by professional hackers.

The equipment includes:

Notebook
1 Steatite M230 Ruggedized Notebook

Wireless
1 PCMCIA Wireless Adapter
1 Bluetooth Adapter (modified to support antennas)
1 Directional antenna
1 Omni-directional antenna

Ethernet
1 USB-to-Ethernet adapter
1 Cross-over Ethernet cable
1 Ethernet cable

Storage
1 500Gb hard disk (including rainbow tables, default password lists, etc.)

Case
1 Case

Misc
1 Power Surge Adapter
1 CD-Holder
Windows Driver CD's

The software includes:

FinTrack – An operating system based on BackTrack / Linux that includes patched wireless drivers, all common and up-to-date hacker tools and lots of additional scripts for easier and faster usage.

Windows XP – Including the FinFisher HQ software and all common up-to-date hacker tools that are available for the Windows platform.

FinAudit

FinAudit is a 1 or 2 week professional penetration testing for a given network to discover all possible vulnerabilities in systems and software and help securing the IT environment.
The audit can be done remotely and locally. A local audit should always be considered to detect all attack vectors for local, physical and especially insider attacks.
FinAudit includes a complete IT based penetration test against the available and public / used infrastructure and all public and internal systems.
A complete audit and fixing of discovered vulnerabilities helps to prevent attacks and information disclosure. Single software can also be checked for vulnerabilities including a full source-code analysis.

At the end of the penetration testing, a detailed report including all possible attack vectors and vulnerabilities including a presentation and consulting are delivered.

On request, a service to help securing the network, system and communication can also be provided.

3. FinFisher Training

Basic Information

Duration:
1 or 2 Week Course

Qualifications:
On the successful completion of the course, all students will receive a certificate including an individual assessment.

Student Group:
The course has been designed for Government Security Agencies responsible for managing and carrying out Intelligence Hacking Operations. The technical level of the course is tailored to each individual group. Specific threats concerning the students can be incorporated into the course. The training is designed for 2 to 4 people.

Aim:
To update on IT Intell Hacking facilities linked to the FinFisher product deliveries with an introduction to the FinFisher/FinSpy IT technical espionage; the art of carrying out all forms of Intell Hacking ,in friendly and unfriendly environments while remaining undetected and covert.

Language:
The course is conducted in English.

Objectives:
At the end of the course students will be able to demonstrate and perform takes relating to:

- IT Intell Hacking Profiling-Footprinting
- IT Intell hacking Profiling-Scanning
- IT Intell Hacking Attacks Password/ Webecurity/ Exploits
- IT Intell Hacking Attacks Networks / Wireless LAN / Bluetooth
- Exploiting Software
- VoIP Hacking
- Covert Communications

Location:
United Kingdom or Germany (students should fly to London or Munich)

Basic Training Package includes:

- All teaching, practical and course work in Germany
- Course notes in hard copy and CD-ROM
- Individual student assessment
- Recommendations for future development of skills and equipment
- Designed for 2-4 persons
- Uses during the training period of all Hardware and Software

Rates
Including-Hotel accommodation - includes three daily meals, laundry, daily rate for 2-4 persons-Incl Local Transport-Communications.

FinTraining Course List

FinTraining Course Overview				
Course No.	*Course name*	*Duration*	*Location*	*Number of students*
8601-1	**FinTraining Intensive/basic** Aim: Practical knowledge of it hacking of networks and exploiting the weakness.	1 week	Uk or Germany	2 TO 4 students
8601-2	**FinTraining Extended** Aim: Indepth knowledge of it hacking of network and exploiting their weaknesses.	2 weeks	UK OR Germany	2 TO 4 students
8602	**FinTraining Advanced Exploiting Software** Aim: How to exploit bugs in software for intell manipulation	1 week	UK OR Germany	2 TO 4 students
8603	**FinTraining Advanced Root Kits** Aim: how to use root kits-detect and enhance root kits	1 week	UK OR Germany	2 TO 4 students
8604	**FinTraining Advanced VoIP Hacking** Aim: How to manipulate servers/VoIP as well as voice monitoring	1 weeks	UK OR Germany	2 TO 4 students
8605	**FinTraining Wireless Hacking** Aim: How to get access to wireless LAN networks/Bluetooth/wireless keyboard	1 week	UK OR Germany	2 To 4 students
8606	**FinTraining Covert Comms** Aim: How to hide specific information in protocols/ media/ cryptography.	1 week	UK OR Germany	2 to 4 students
8607	**FinAudit 1 or 2 week in country penetration testing of Endusers Local Network.** Aim: The auditors will perform Hacking attacks on the enduser networks to show the liabilities and weaknesses.	1 or 2 Weeks	In country	2 to 4 Students

FinTraining Hacking Courses

Course 8601 Intensive:

Fintraining 8601-01 : Basic Hacking Course (1 week) Intensive					
	Monday	*Tuesday*	*Wednesday*	*Thurs day*	*Friday*
Week 1	**FinFisher** • FinFisher HQ • FinFisher 1 • FinFisher 2 • FinFisher 3 **Toolset** • FinFisher Hacking PC • Equipment • FinTrack **Profiling** Footprinting • Search Engines • Archives • Target Websites • "Who is" Records • DNS Analysis • First Contact	**Profiling** Scanning • Mapping • Port scanning • Service Fingerprinting • OS Fingerprinting • Analysis Enumeration • CGI • NetBIOS • SNMP • RPC • NFS • Other	**Attacking** Passwords • Bypass • Default • Brute force • Cracking • Trusted Web security • Code Exposure • Input Validation • CGI • XSS • SQL Injection • Other	**Attacking** Exploits • Overflows • Format Strings • Race Conditions • Archives • Exploiting • Frameworks • Fuzzer Root-kits • Backdoors • Hiding Log-cleaner Network • Sniffing • Rerouting • War-dialing	**Attacking** Wireless LAN • Discovery • Encryption • Advanced • Hardware Bluetooth • Discovery • Attacks • Hardware Advanced • Custom Exploits

Course 8601 Intensive/Basic/Extended:

FinTraining 8601-02: Basic Hacking Course For Beginner (2 weeks) indepth					
	Monday	*Tuesday*	*Wednesday*	*Thursday*	*Friday*
Week 1	**FinFisher** • FinFisher HQ • FinFisher 1 • FinFisher 2 • FinFisher 3 **Toolset** • FinFisher Hacking PC • Equipment • FinTrack	**Profiling** Foot printing • Search Engines • Archives • Target Web-sites • "Who is" Records • DNS Analysis • First Contact Scanning • Mapping • Port scanning • Service Finger-printing • OS Fingerprint-ing • Analysis	**Profiling** Enumeration • CGI • NetBIOS • SNMP • RPC • NFS • Other	**Attacking** Passwords • Bypass • Default • Brute force • Cracking • Trusted	**Attacking** Web security • Code Ex-posure • Input Vali-dation • CGI • XSS • SQL Injec-tion • Other
Week 2	**Attacking** Exploits • Overflows • Format Strings • Race Condi-tions • Archives • Exploiting • Frameworks • Fuzzer	**Attacking** Root-kits • Backdoors • Hiding • Log-cleaner	**Attacking** Network • Sniffing • Rerouting • War-dialing	**Attacking** Wireless LAN • Discovery • Encryp-tion • Advanced • Hardware	**Attacking** Bluetooth • Discovery • Attacks • Hardware Advanced • Custom Exploits

Course 8602:

FinTraining: Exploiting Software					
	Monday	*Tuesday*	*Wednesday*	*Thursday*	*Friday*
Week 1	**Introduction** • Famous Examples **Vulnerabilities** • Code Exposure • Authentication Bypass • Unexpected Input • SQL Injection • XSS • Race Conditions • Overflows • Format Strings	**Exploits** • Online Archives • Modification and / Customization • Frameworks	**Finding Bugs** • Source-Code Analysis • Fuzzing • Debugging	**Writing Exploits** • Unexpected Input • Overflow • Format-String	**Examples** • Web-Applications • Server • Clients • Embedded

4. FinFisher Project Overview

The Finfisher project will be realized in 3 phases:

Phase I (ready in October 2007)

1. FinFisher Kit
2. Training

1. FinFisher Kit

The following sections describe the FinFisher kit and software as it is in Phase I.

Hardware Components:

Notebook
1 Steatite M230 Ruggedized Notebook

Wireless
1 PCMCIA Wireless Adapter
1 Bluetooth Adapter (modified to support antennas)
1 directional antenna
1 Omni-directional antenna

Ethernet
1 USB-to-Ethernet adapter
1 cross-over Ethernet cable
1 Ethernet cable

Storage
1 500Gb USB 2.0 hard disk

FinFisher Devices
2 Sandisk Cruzer 4 GB U3-USB
2 CD-ROMs

Case
1 Peli-Case Medium 1500

Misc
1 Power Surge Adapter
1 CD-Holder
Windows Driver CD's

Software Components

FinFisher HQ	Graphical user interface HQ software for FinFisher 1 and 2
FinFisher 1	Extract locally stored user accounts, system and network information from the target PC.
FinFisher 2	Make a copy of all locally stored e-mails and get a copy of all local files with given file-extensions.
FinFisher 3	2 bootable CD-ROMs to: a) Clear the Windows Administrator account password and b) Wipe all local hard-disks.

2. Training

The following section describes the FinFisher training as it is in Phase I.

Basic Hacking Course
Basic 1 week Hacking Course that covers:

- Usage of all FinFisher components
- Basic IT security knowledge
- Basic hacking techniques

Consulting
1 week of generic IT security consulting regarding the FinFisher package.

Phase II (ready in December 2007)

1. Generic FinFisher Feature Requests
2. FinFisher 2 Feature Requests
3. FinTrack
4. Training

1. Generic FinFisher Feature Requests

The following points describe generic additionally requested features concerning the FinFisher package.

Support individual FinFisher 1 and 2 USB device creation
Offer functionality within the graphical user interface to create a FinFisher 1 or 2 system onto an attached USB storage device.

The amount of possible FinFisher creations will be restricted to a certain limit by a licensing system.

Create an USB Dongle to recover deleted files
We are at the present time not able to build the requested device in a way that it could compete with existing and established forensic software.

A market research can be done to generate a list of available products.

Add Windows 98 support to FinFisher 1 and 2
As the FinFisher devices 1 and 2 only support Windows systems newer than / equal to Windows 2000 some major rework and functionality testing has to be performed.
It is currently not certain if the whole feature-set of FinFisher 1 and 2 will be available to older systems.

2. FinFisher 2 Feature Requests

The following points describe the additionally requested features within the FinFisher 2 system.

PGP / PGPi / GnuPG support
Local software installations of the default PGP software (PGP, PGPi, GnuPG) should be recognized. If the above software is present the private and public key databases should be retrieved onto the FinFisher device.

Graphical selection for file-types
The GUI configuration interface for FinFisher 2 devices should offer the possibility to select groups of file-extensions by global file types.

The following file-types should be selectable:

- Images (JPEG, GIF, BMP, PNG …)
- Documents (DOC, DOCX, TXT, XLS …)
- Compressed Files (ZIP, RAR, LZM, TAR, GZIP…)
- PGP Encrypted Files (PGP, GPG, ASC)

Find and retrieve all password-protected files
A functionality will be added to check the following file-types for password protection and retrieve them to a separate folder if they are protected:

- Office Documents
- ZIP Archives
- RAR Archives

Find and retrieve all files with wrong file extensions
The FinFisher 2 system will check every file in the given search location against a known file-type MIME database and verify that the file extension is correct. On incorrect or spoofed file extension, the file is retrieved to a separate folder.

This feature will be restricted to a list of known or user-specified file-types.

Create a list of files within the given search path
A list of all files in the given search path is created and stored in ASCII format onto the FinFisher device.

3. FinTrack

The following sections describe the FinFisher specific modifications to the BackTrack system.

Scripts
Additional scripts for common attack techniques including:
- Man-in-the-middle
- Router mode
- Etc.

Configurations
Customized configurations for easier usage of common attack tools

4. Training

The following section describes the FinFisher training as it is in Phase II.

Hacking Course
1 week Hacking Course that covers:

- New FinFisher functionality
- Advanced hacking techniques

Phase III (ready in approx. March 2008)

1. Trojan Horse
2. Training

1. Trojan Horse

The following points describe the additionally requested features for the FinFisher 3 system.

Server Executable has to be enciphered
Various methods have to be provided to encipher the trojan horse executable. These include:

- PXE
- UPX

Custom Configuration
All options of the system should be fully configurable, this includes the configuration of:

- Network Ports
- Communication Protocols
- Executable / Process name
- Feature Set
- Encryption Algorithm and Passphrase

Alarm
On connect of certain infected clients an alarm has to be triggered.

This alarm will be generated either by an e-mail to a given mail address or by executing a locally available software.

Central Server
A central server software will manage all connections from and to infected clients. Agents use a client software to connect this central server and get access to the clients.

Traceroute
An option is provided to display the current location by country of infected clients.
This will either be done by custom code or by calling the external program Neotrace.

Reverse Connect
A reverse-connect option has to be part of the trojan to enable bypassing common firewalls and NAT restrictions. A certain event will trigger the infected system to connect back to the central server and allows it using this connection as a command channel.

Live Configure
The trojan should be configurable on connection via the command channel.

Worm Feature to spread through Outlook on Request
At some point, the trojan should offer a functionality to send itself to contacts of the Microsoft Outlook address-book using the local mail server configuration.

Source Code should be provided
The full-disclosure of the source code will be bound to a special pricing and a custom license which restricts re-usage within other projects and reselling.

2. Training

The following section describes the FinFisher 3 training.

Trojan Horse Usage
1 week course that consists of:

- FinFisher 3 functionality
- Example Usages
- Advanced Configuration / Modification

Source-Code Introduction
1 week course that gives an insight on the source-code, possible modification and more.

The courses can be combined into a 1 week training.

Recommended Additional Components

FinFisher 6 – Finfly Download Proxy
The FinFisher FinFly Download Proxy is a HTTP proxy that is able to modify executable files while they are being downloaded by 1 or multiple clients.

The proxy offers 2 options:

- Replace executable files
- Modify executable files

In the modification progress, the original executable is downloaded, merged with a local executable file and sent to the client.

On execution of the modified executable on the client side, the appended executable gets executed first before the original executable is restored and executed so it will pass all internal checksums verifications.

Optional, additional modules can be provided that replace other types for files, for example all images.

Usage: The FinFly Download Proxy can be used for trojan horse infection. This can be single or multiple clients (by IP addresses) or all participants of the network that are routed through the HTTP proxy.

Required Operating System: Linux / BSD (Windows Version on request)

FinFly Download Proxy will be ready in March 2008.

5. FinFisher Delivery Schedule

M1: Received order

		DUR	M 1	M 2	M 3	M 4	M 5	M 6	M 7	M 8	M 9	M 10	M 11
Implementation Schedule													
1	Project Award	1 day											
2	Phase I	2 month											
3	Phase II	2 month											
4	Phase III / Trojan	4 month											
5	FinFly Proxy	2 month											
6	FinTraining Basic	1 week											
7	FinTraining Trojan	1 week											
8	FinTrai-ning:Exploitin g	1 week											
9	FinTraining FinFly	1 week											

Training	
Deliveries	

PABX Monitoring

Index

PABX Monitoring for Small Business

MARATHON EVO*lite* is an easy-to-use communications recording solution purposely designed to meet the requirements of small to medium sized organizations in a cost-effective package. MARATHON EVO*lite* can be configured to record, live monitor and archive communications at one location. It also provides the flexibility to connect multiple recording platforms, departments and/or locations, with data automatically transferred to the central INTERACTION server or a defined MARATHON EVO*lite* recorder platform.

Open architecture

MARATHON EVO*lite* lays its engineering foundation on being the WORLD´S FIRST Linux-based communications recorder, providing power, reliability and open source flexibility in a cost effective package. With its scaleable channel array, MARATHON EVO*lite* captures and records all customer interactions from 4 up to 60 channels simultaneously with a minimum on-line storage of 50,000 recording hours.

Capture what matters

With MARATHON EVO*lite* you can design a tailored communications recording solution to fit the unique requirements of your business by combining selective, rules based, total and record-on-demand recording.

Fast and efficient search and replay

ASC´s advanced user interface applications allow easy access to calls and data over local networks (LAN/WAN), Intranet and Internet. Multi-language support is built into the system to easily provide for localization and support.
All ASC applications are easy to use and deploy, require minimal training and administration, yet they produce amazing results.
Other ASC communications recording applications include:

- POWERplay, a feature rich application that allows playback over LAN/WAN connections
- WEBplay, a powerful truly browser based search and replay interface that requires no proprietary software to be installed on user's PC
- INSTANT WEBplay, a browser based interface for quick access to recent calls recorded on multiple channels
- Threat Call Recording, a facility required by organizations that need to protect their company and employees' welfare while maintaining call privacy

- Last Call Repeat (LCR), a facility to provide the most recent calls from any telephone in the world
- INSPIRATIONpro, a quality monitoring software for contact centers, improves the quality of customer interaction hereby reducing agent turnover, increasing productivity and profits

Optimum storage technology

MARATHON EVO*lite* comes standard with an expanded hard drive that guarantees a minimum on-line storage of 50,000 recording hours, with the option to upgrade to larger drive sizes. The system can also be equipped with AIT or a DVD drive for archiving. A second DVD drive can be added to extend archive capacity. This also allows for playback of previously recorded media. Additionally calls can be saved as .wave files and sent via e-mail.

Stay connected with MARATHON EVOlite:

- Trunk side recording of ISDN, E1, T1 and analog lines
- PCM 30 integration with leading turrets and dealer boards
- Digital extension taps for "industry leading" PBXs
- Service observe and single step conference
- Online Monitoring
- VoIP Recording with EVOip

Seamless integration

- Call Tagger provides free seating capability without CTI
- Additional call details captured through CTI
- Powerful APIs for easy to implement applications
- Application Data Integration (ADI) – captures data from existing applications and tags it to the call database

Additionally, the application can control when the recorder starts and stops to allow you to record only pertinent details.

Secure and protected access

MARATHON EVO*lite*'s multi-level access system requires user authorization for access to specific functions and channels. Supervisors can allocate individual security levels and specific user profiles for each user. This greatly reduces the risk of valuable information falling into the wrong hands.

Technical data

Channels and recording devices	
Analog inputs	4 ... 48 channels
Digital inputs	4 ... 48 channels MVTC
	or 15 ... 60 channels PRI / PCM 30
	or mixed configuration of analog/digital
Hard disk (built-in)	up to 175,000 standard hours (with 4.8 kbps)
Signal input (analog)	symmetrically, 1 ... 200 mV or 10 ... 2000 mV;
	impedance 600 ohms or > 22 kOhms
Protocols (digital)	PCM 30; PRI: E1 – ISDN / T1 – ISDN / T1 – RBS;
	BRI ISDN EDSS1, proprietary
Voice over IP (VoIP)	H.323, SIP, RTP
Audio input (analog)	
Frequency range	300 ... 3400 Hz, +/- 3 dB
Signal-to-noise ratio	> 42 dB (A)
Distortion factor	< 3%
Cross talk attenuation	> 60 dB / 1 kHz
AGC amplifier	response time 20 ms / 20 dB
	recovery time 200 ms … 4.7 sec. / 20 dB adjustable
Operation modes	
Data compression	4.8, 16, 24, 32, 40 or 64 kBit/sec
	selectable for each channel
Start delay	0 ms
Stop time	1 … 120 sec. adjustable
Time synchronization	optional: NTP, input for minute pulse, DCF 77,
	GPS, IRIG B, IRIG E, Hopf
	output: minute pulse (option)
Alarm contact	relay outputs for optical and audible alarm (option)
Environment	
Power supply	90 ... 250 V AC
Temperature range	+41 ... +95 °F (+5 … +35 °C)
Dimensions (WxHxD)	7.9 x 11.9 x 18.3“ (200 x 300 x 463 mm)
Weight	approx. 30 lbs (15 kg)
Conformity	
Security standards	EN 60950, UL 60950 / CSA C22.2
EMC / ESD	EN 55022, FCC Part 15 class A,
	EN 55024, EN 61000-3-2, EN 61000-3-3
PTT	FCC Part 68, TBR 3, TBR 4, TBR 21, PTC212/05/004

PABX Monitoring

Fits All Needs - Current and Future

MARATHON EVOLUTION is a universal communications recording solution that satisfies the demanding requirements of busy financial trading floors, high volume contact centers, mission critical air traffic control centers and life-saving public safety control rooms.
MARATHON EVOLUTION perfectly fits your current needs and is designed to evolve as your business grows.

Engineered To Evolve, Built To Endure

MARATHON EVOLUTION, the world's first Linux-based communications recorder, designed for all applications provides power, reliability and open source flexibility in a cost effective package. Based on recognized industry standards with built-in scalability, MARATHON EVOLUTION secures your investment in a critical area of your business.

A-La-Carte Feature Selection

MARATHON EVOLUTION is the only communications recording platform that enables you to select exactly what you need for your current requirements and empowers you to add more functionality when your business demands it. MARATHON EVOLUTION, with its scaleable channel array, captures and records all interactions from 4 up to thousands of channels simultaneously.
The system can be configured to record, live monitor and archive communications at one location and to provide search and replay facilities locally or via LAN / WAN, Intranet or Internet.

Distributed Recording Mode

This configuration provides the flexibility to connect multiple recording platforms, departments and/or locations and automatically transfer the data to the central interaction platform for on-line access and archiving providing unique disaster recovery capabilities.

Fast and Efficient Search and Replay

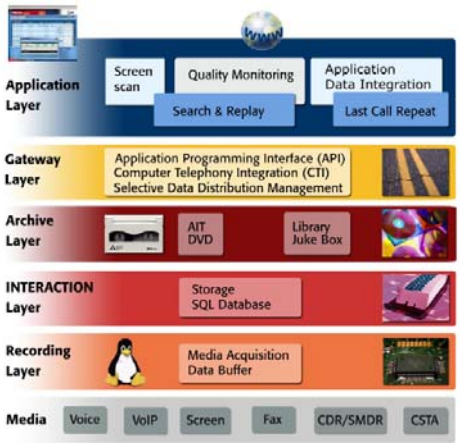
ASC´S advanced user interface applications allow easy access to calls and data over local networks (LAN/WAN), Intranet and Internet. Multi-language support is built into the system to easily provide for localization and support.
All ASC applications are easy to use and deploy, require minimal training and administration, yet they produce amazing results.

ASC communications recording applications include:

- Powerplay, a feature rich application that allows playback over LAN/WAN connections
- Webplay, a powerful truly browser based search and replay interface that requires no proprietary software to be installed on user's PC
- Instant Webplay, a browser based interface for quick access to recent calls recorded on multiple channels
- Threat Call Recording, a facility required by organizations who need to protect their company and employees' welfare while maintaining call privacy
- Last Call Repeat (LCR), a facility to provide the most recent calls from any telephone in the world
- Inspirationpro, a quality monitoring software for contact centers, improves the quality of customer interaction hereby reducing agent turnover, increasing productivity and profits

Seamless Integration

- Call Tagger provides free seating capability without CTI
- Additional call details captured through CTI – CTI integrations into the most likely PBXs
- Powerful APIS for easy to implement applications
- Application Data Integration (ADI) – Captures data from existing applications and tags it to the call. additionally the application can control when the recorder starts and stops to allow you to record only pertinent details



Highlights

- Enhanced reliability, security and performance through Linux operating system
- Scaleable channel array allows for virtually unlimited recording channels
- A-la-carte features – you only purchase what you need
- Powerful, browser-based user interfaces make it easy to use, install and manage
- Multiple recording configurations for single site/department or your entire enterprise
- Open, flexible APIs enable integration with existing customer applications
- Selective and rules based recording and archiving
- Reduced service and maintenance costs through install wizard, recovery tools and remote maintenance

Technical Data

Channels and recording devices	
Analog inputs	4 ... 192 channels
Digital inputs	4 ... 120 channels MVTC, 15 ... 360 channels PRI,
	15 ... 480 channels PCM 30 / PCM 32
	or mixed configuration of analog / digital / VoIP
VoIP	4 ... 32 channels (active) 4 ... 120 channels (passive)
Hard disk (built-in)	up to 175,000 channel hours (with 4.8 kbps)
External storage	Disk Array Storage (DAS), Network Attached Storage (NAS)
Signal input (analog)	symmetrically, 1 ... 200 mV or 10 ... 2000 mV;
Impedance	600 ohms or > 22 kOhms
Protocols (digital)	PCM 30; PCM 32; PRI: E1 – ISDN / T1 – ISDN / T1 – RBS;
	BRI ISDN EDSS1, proprietary
Voice over IP (VoIP)	H.323, SIP, RTP
Audio input (analog)	
Frequency range	300 ... 3400 Hz, +/- 3 dB
Signal-to-noise ratio	> 42 dB (A)
Distortion factor	< 3%
Cross talk attenuation	> 60 dB / 1 kHz
AGC amplifier	response time 20 ms / 20 dB
	recovery time 200 ms … 4.7 sec. / 20 dB adjustable
Operation modes	
Data compression	4.8, 16, 24, 32, 40 or 64 kBit/sec
	selectable for each channel
Start delay	0 ms
Stop time	1 … 120 sec. adjustable
Time synchronization	optional: NTP, input for minute pulse, DCF 77,
	GPS, IRIG B, IRIG E, Hopf
	output: minute pulse (option)
Alarm contact	relay outputs for optical and audible alarm (option)
Environment	
Power supply	90 ... 250 V AC
Temperature range	+41 ... +95 °F (+5 … +35 °C)
Dimensions (WxHxD)	19 x 7 x 19,8“ (483 x 177 x 503 mm)
Weight	approx. 50 lbs (25 kg)
Conformity	
Security standards	EN 60950, UL 60950 / CSA C22.2
EMC / ESD	EN 55022, FCC Part 15 class A,
	EN 55024, EN 61000-3-2, EN 61000-3-3
PTT	FCC Part 68, TBR 3, TBR 4, TBR 21, PTC212/05/003

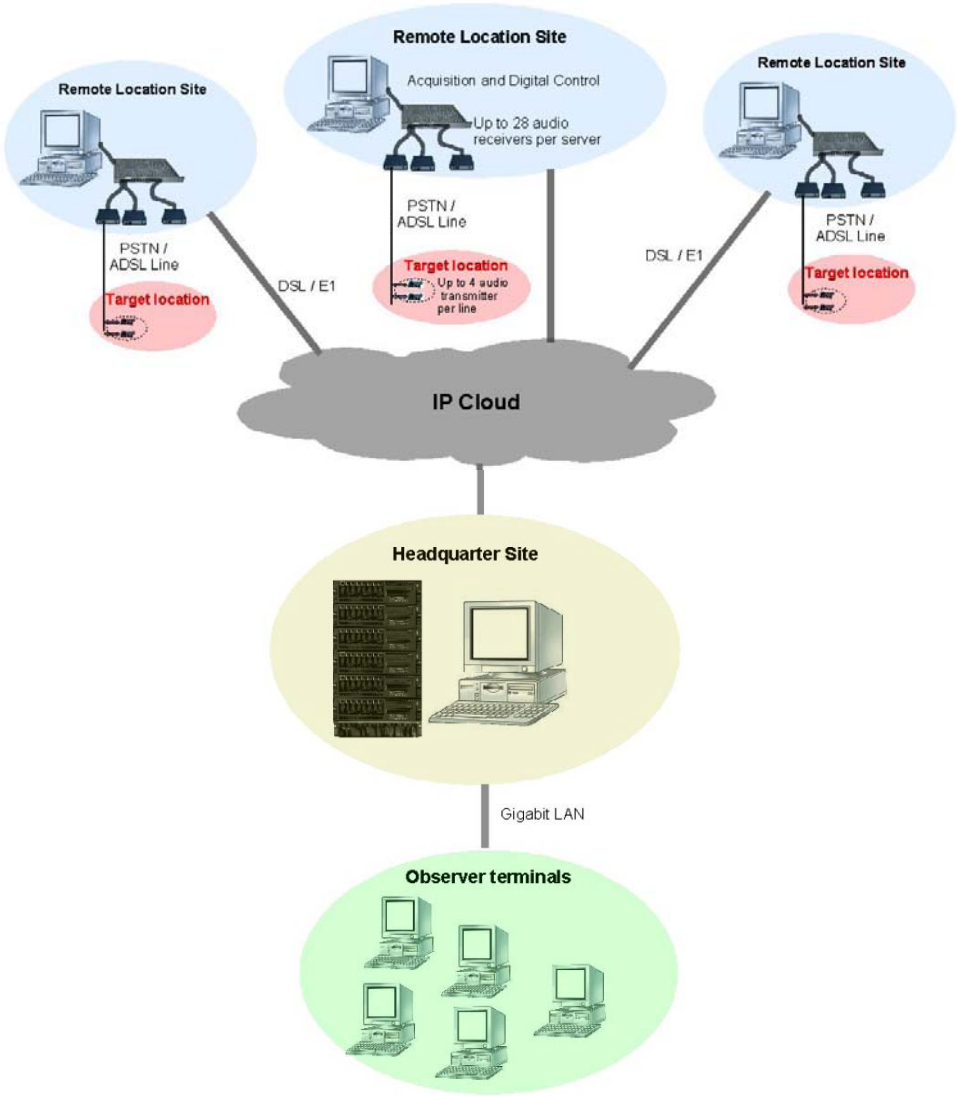
Room Monitoring

Index

Audio Surveillance Network

1 Product Description

Audio Surveillance Network (ASN) is a complete solution for law enforcement agencies to collect, transmit, store and analyze audio coming from distant targets at a centralized location. ASN consists of both hardware and software elements suitable for building a countrywide audio surveillance system, or to conduct standalone tactical operations. A typical ASN layout consists of various target locations, remote location sites, a central headquarters and a set of observer terminals.



Audio is captured form a target location by audio transmitters containing tiny microphones, and transferred to the remote location site over a telephone line. Usually, a remote location site exists near a location exchange. It contains a large bank of receivers to collect audio from various target locations. The received audio channels are digitized and stored in a remote location server.

The audio data is sent to the headquarters using a DSL or E1 link. The headquarters stores digital audio coming from a number of remote locations in a huge database. Observer terminals access the headquarters database using custom written audio surveillance software. An ActiveX based audio player offers audio analysis capability and on-line comment tag submission to the observers. ASN is the only system of its kind that offers real-time audio surveillance from a number of distant targets from beginning to end.

2 System Elements

The Following system elements have been developed to build an ASN.

Target Location
- Xad Audio Transmitter (XTL-ATx)

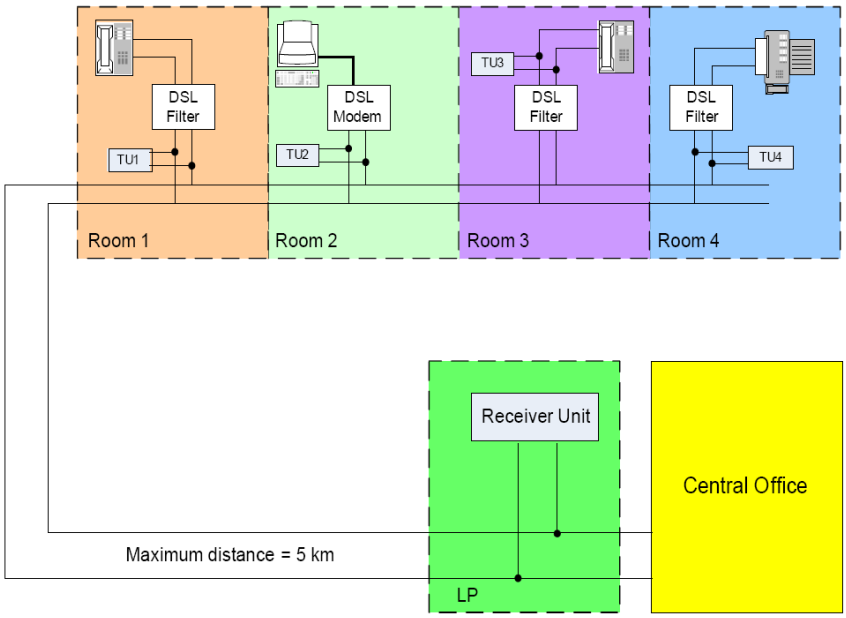
Remote Location Site
- Xad Audio Receiver (XKL-ARx)
- Xad Audio Acquisition Platform (XRL-ACQ)
- Xad Remote Location Server (XRL-SER)
- Xad Remote Location Software (XRL-SW)

Headquarters
- Xad Headquarter server (XHQ-SER)
- Xad Headquarter Software (XHQ-SW)

Audio Transmitters (XRL-ATx)
Audio is collected from the target location using Audio Transmitters (XTL-ATx). Each transmitter contains a high gain, sensitive microphone, which is installed on the target line irrespective of the location and polarity. The installation does not interfere with the normal operation of telephone equipment. XTL-ATx comes in two versions – XRL-ATP works with standard POTS, while XRL-ATA is designed for ADSL enabled telephone lines. For major operations, up to four XRL-ATx units can be deployed per target. A user can remotely activate the desired XRL-ATx leaving the others in standby mode.

Each XRL-ATx has built-in intelligence to sense the line status and start-stop its operation independent of the user intervention. Salient features of an XRL-ATx are listed below:

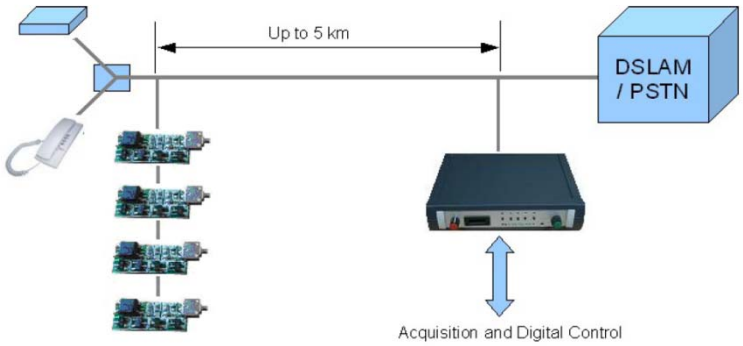
- Small size 16 x 9 mm
- Low current consumption (active 4mA, standby 4µA
- High gain microphone 48 dB
- Polarity free installation
- Seamless operations on PSTN and ADSL enabled lines
- Automatic start-stop and mute functions
- Choice of 4 transmitters per line



Audio Receiver (XRLS-ARx)
Audio Receiver (XRLS-ARx) is a very low noise state-of-the-art receiver to extract clear audio signals from noisy telephone lines at a distance of 5 Km from the target location. XRLS-ARx outputs receive audio to the headquarters and phono sockets. There are manual control buttons on the XRLS-ARx to switch between multi-transmitter installations or mute all, if required. XRLS-ARx also provides a digital interface which is used to control XRLS-ARx from the headquarters' software. Main features of XRLS-ARx are listed below:

- Transparent operations on PSTN and ADSL enabled lines
- Standalone and network operation
- Automatic voltage control
- Manual button control for standalone operations
- Digital control interface
- Logic circuitry to control up to 4 audio transmitters
- Built-in digital voltmeter
- Audio Vu-meter
- Automatic volume control
- Phono socket
- Headphone socket

-



Audio Acquisition Platform (XRLS-ACQ)
The Audio Acquisition Platform (XRLS-ACQ) is a 1U height 19 inch rack mount unit. It consists of a custom built PCB to acquire, digitize and transfer 28 audio channels to a Remote Location Server (XRLS-SER).

ACQ uses four 8-bit analog to digital converters to digitize the audio channels. The digital audio samples are buffered before sending them to XRLS-SER using a USB 2.0 interface. Main features of the XRLS-ACQ platform are listed below:

- 19 inch rack mountable casing
- Parallel A/D conversion of 28 analog audio channels
- 64KB buffer memory to ensure data continuity
- High speed data transfer using USB2 interface
- Integrated interface for audio and transmitter control using RJ45 ports
- Acquisition status display

Xad Remote Location Server (XRLS-SER)
The Remote Location Server (XRLS-SER) is a powerful machine built with 64 bit AMD 2.0GHz dual core processor and Linux operating system. The industrial PC casing with front and rear fan support provides ruggedness to operate in extreme temperatures expected at a remote location site. The remote location server is lockable at the front providing extra security to the system.

Remote Location Server Software (XRLS-SW)
The remote location server software (XRLS-SW) runs on XRLS-SER and controls the main functionality of a remote location site. It is written in C++ under a Linux operating system. For security reasons, a user interface has not been built in the remote location software. The remote location operator uses a console window to execute commands for each task. Main features of XRLS-SW are listed below:

- Command line interface for added security and reliability
- Security database installation without user interaction
- Built under Linux for easy integration, faster speed and stability
- Database storage for systematic archiving of audio streams
- Automatic audio acquisition and uploading according to the headquarters' schedule
- Thread based real-time audio encoding and uploading
- Local audio offload option for emergency
- Segmentation of audio streams into packets for quick transmission
- Synchronized time stamping of audio data cross the ASN
- Lossless compression of audio data for integrity and completeness
- Remote control of attached audio devices from the HQ software
- Password protection, activity logging and secure reporting to HQ software
- Memory management and automatic deletion of contents
- Separate audio device set-up and local testing utility

Transmission Hardware
The requirement for transmission hardware (E1 routers, DSL and related components) may differ in each case. Depending upon the requirement, we can specify the transmission hardware to be used in an ASN.

Headquarter Servers (XHQ-SER)
The HQ is the main control center of the ASN. It is connected to remote location sites in a star network topology. The XHQ-SER comprises two database servers, a storage server, and an application server. The database servers are similar in specification to XRLS servers. The storage configuration is tailored according to the requirements. To build redundancy, the database servers are connected to the storage server in cluster configuration. The application server is an apache based server, which hosts web-based HQ server software. It allows the observer terminal to access the huge audio database.

Headquarter Server Software (XHQ-SW)
The headquarter server software (XHQ-SW) provides the main control of the ASN. XHQ-SW software is accessed by the Microsoft Internet Explorer through a Web-based environment. The complex system information remains hidden behind a user friendly graphical user interface (GUI).

All the software pages are interconnected. A user can navigate across them using a dynamic menu bar. The menu items vary according to the user access privileges.

The main features of the XHQ-SF are listed below:

- Secure login feature with individual access rights
- Personalized home page portal for each user
- Easy and dynamic remote location site creation
- Site and target location based user access
- Hierarchical user and group management structure
- Entity based access rights and on the fly user creation
- Automatic information update across the network
- Time, tag and target based audio content search
- ActiveX based audio player with audio range control
- Custom audio play list with forward/backward audio search options
- Real-time audio access and analyze feature
- Observer comment tagging and retrieval
- Audio save option for privileged users
- Automatic e-mail feature within the groups
- Audio transmitter control for each remote location site
- Network site status reporting
- Advanced audio download scheduler for target locations
- Activity log and reporting

Observer Terminals (OT)
Observer Terminals are standard PCs connected to the HQ server in an intra net configuration. They access XHQ-SW to access and listen to audio records stored in the HQ database. ASN setup does not require an installation of the client software. Updates are automatically reflected to the observer terminals when XHQ-SW is updated on the headquarter application server.

Audio Transmission via Power Lines (ACC)

Features

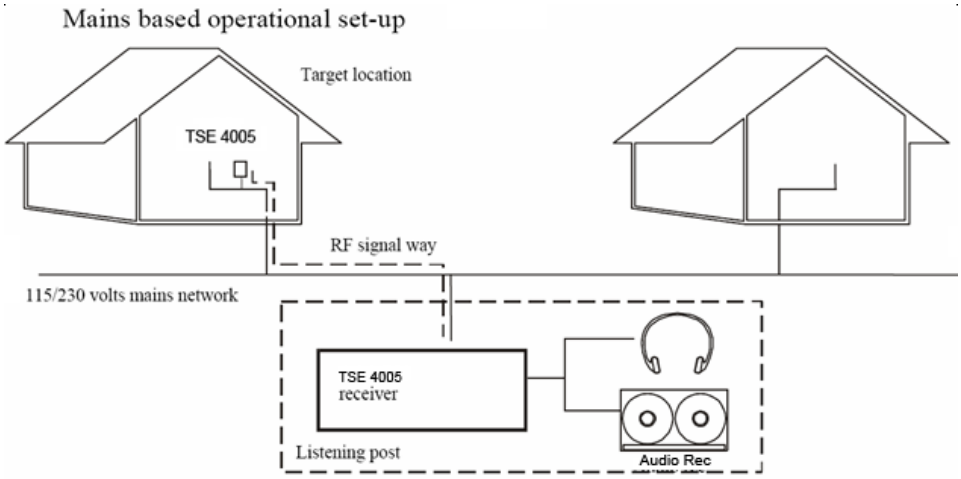
- Micro-size FM transmitter
- FM/PLL signal transmission
- Parametric equalizer
- Scrambled model available
- Long range
- Proven technology
- Smart VOX with noise cancellation

Options

STANDARD TRANSMITTER MODEL -TXS
Model -TXS is the standard micro transmitter module with onboard audio circuits.

EXTENDED MICROPHONE MODEL -TXR
Model -TXR is a module where the miniature microphone element is separated from the transmitter board and mounted on 2 meters of wire, making counter-measure detection extremely difficult.

SCRAMBLED MODULE MODEL -TXS-S AND -TXR-S
In order to maintain a low probability of detection and to counter casual interception, we have designed a micro-sized circuit for scrambling intelligence audio with minor degrading of the audio quality.



Technical Specifications

RECEIVER -RX	
Carrier frequency to be specified by customer or standard	140 kHz +/- 500 Hz
Sensitivity (fmod. = 1 kHz, deviation +/- 3 kHz)	- 82 dBm at 20 dB S/N
Sensitivity (fmod. = 1 kHz, deviation +/- 3 kHz)	- 48 dBm at 50 dB S/N
Selectivity - 30 dB	+/- 20.65 kHz
Common mode rejection	70 dB
AM rejection (Vin = - 20 dBm, AMmod = 30 %)	40 dB
Distortion (Vin = - 20 dBm, deviation = +/- 3 kHz)	0.55 %, 1 kHz
Input impedance	275 ohm
Audio frequency response - 3 dB (line out)	300 Hz to 5 kHz
Output voltage line out (deviation = +/- 3 kHz)	700 mV (no load)
Output voltage tel. out (deviation = +/- 3 kHz)	230 mV (600 ohm load)
Output impedance tel. out	600 ohm
Output impedance line out	1 kohm
Output impedance headphones out	47 ohm
Parametric equalizer frequency adjustment range	100 Hz to 10 kHz
Parametric equalizer Q adjustment range	0.4 to 4 kHz
Parametric equalizer gain adjustment range	+/- 15 dB
Meter range RF level	- 80 to -20 dBm
Power supply	115 / 230 VAC (50 - 60 Hz)
Dimensions	265 x 255 x 82 mm
Weight	2.8 Kg. / 6.17 lbs
TRANSMITTER -TXS	
Carrier frequency	140 kHz +/- 500 Hz
Output impedance	10 ohm
Output voltage (140 kHz sine)	500 mV RMS into 10 ohm
Max. modulation	+/- 5 kHz
Frequency response	150 Hz to 3.5 kHz - 3 dB
Current consumption	3 mA DC
Audio amplifier AGC range	< 66 dB
Microphone vibration sensitivity	< 66 dB
Dimensions Model 4005-TXS	42 x 22 x 12 mm
Dimensions Model 4005-TXR	14 x 9 x 7 mm / 42 x 22 x 12 mm
Dimensions Model 4005-TXS-S	14 x 9 x 7 mm / 42 x 22 x 12 mm / 35 x 12 x 4 mm
Dimensions Model 4005-TXR-S	14 x 9 x 7 mm / 42 x 22 x 12 mm / 35 x 12 x 4 mm

Multi Room Monitoring via Telephone Lines (Heimdal)
(TSE 4004)

The TSE 4004 Wired Room Monitoring System is a highly professional system designed for remote monitoring where full transmitter control via standard PSTN lines is needed. TSE 4004 is designed to allow the user to install up to 8 transmitters, using a combination of active phone lines or spare wires and mains lines. The individual transmitters can be switched on and off remotely. The modular TSE 4004 system consists of transmitter(s), one receiver module, PSTN modules and of control software for PC.

Transmitters

The TSE 4004 transmitters incorporate the following advanced features: scrambler, AGC and remote control receiver.
The remote controlled functions of the transmitters are power on/off and scrambler on/off.
Two different types of transmitters have been developed for the TSE 4004 system. The TSE 4004 Wired Monitoring transmitter (HWM) is to be used on active phone lines or spare wires. The TSE 4004 Carrier Current transmitter (HCC) is to be used on active mains lines.

Receiver System

The RX module is a small, flat and compact cabinet, which is only 44 mm high. One RX module handles 2 transmitters simultaneously.
The RX module has the following features:

- Target line interface for both PSTN and spare wires (HWM) and mains wires (HCC)
- Dual tuner - each with 4 channels
- High impedant input for LF audio. Enables monitoring of PSTN line without transmitter
- Audio descrambler
- Remote control of transmitters
- Noise masking for HWM transmitters
- Line output for recording
- Output for headphones

It is possible to have both HWM and HCC transmitters operating at the same time, enabling the operator to monitor, for example, one HWM transmitter and one HCC transmitter simultaneously.
The RX module is powered from an external low voltage source. The RX module is delivered with a mains adapter, but can also be powered from a car battery.

PSTN Module – Remote set-up

The PSTN module provides a link from the listening post to the monitoring site. One PSTN module is needed at the monitoring site and one at the listening post. The PSTN module can handle 2 lines simultaneously and transfers both the audio from the transmitter and the remote control commands.
The PSTN module at the monitoring site can also be dialed up from standard telephone equipment, including mobile phones. Access to the system is done by means of the telephone keypad. This feature enables the operator to make a quick control of the TX / RX / PSTN set-up.
The PSTN module is very easy to install – it is connected to the receiver via one single cable, containing all the required signals and power.

Control Software

All facilities in the TSE 4004 system can be software controlled via a PC. The control set-up can be provided by connecting the control PC directly to the receiver module or to the local PSTN module at the listening post.

Applications

- TSE 4004 is ideal for operations requiring:
- Single room monitoring
- Multi-location room monitoring
- Phone lines, spare wires and mains lines
- Local set-up
- Remote set-up
- Undercover “black-box” set-up

Features

- 4 active transmitter channels
- High audio quality
- Small size transmitters
- Audio scrambling
- Remote control of transmitters
- PSTN module for link of intercepted audio to remote listening post
- Current re-injection on phone lines for system security
- Small “black-box” receiver unit
- Control of software via PC
- Easy to install
- Easy to use

Technical Specifications

RX module	Number of channels	4
	Frequency range	110-240 kHz
	Sensitivity	10 dBuV / 20 dB SINAD
	Number of built-in tuners	2
	Modulation	FM
	Remote control transmitter	28 kHz, OOK
	Serial interface to PC / PSTN module	RS-232
	Power source	7-11 VAC or 10-15 VDC
	Dimension (HxWxD)	44x130x164 mm / 1.7x5.1x6.5 inches
Transmitters General data	Number of channels	4
	Frequency range	110-240 kHz
	Type of modulation	FM
	Audio scrambling	Frequency inversion
	Remote controllable	Yes
	Packing	Shrink tube, black
HWM specific data	Transmitted power	50 mVRMS into 100 ☐
	Line voltage range	6-80 VDC
	Dimensions (HxWxD)	Approx. 7.5x32x20 mm / 0.3x1.3x0.8 inches
HCC specific data	Transmitted power	500 mVRMS into 2 ☐
	Mains voltage range	85-265 VAC
	Dimensions (HxWxD)	Approx. 15x35x23 mm / 0.6x1.4x0.9 inches
PSTN module – Remote set-up	PSTN interface	Global compliant, SW controlled
	Number of PSTN lines	2
	Data mode	FSK / DTMF
	Tape control	VOX controlled, adjustable from PC SW
	Serial interface to PC / RX module	RS-232
	Dimension (HxWxD)	44x130x84 mm / 1.7x5.1x3.3 inches

Wired Audio Monitoring via PSTN Lines (RFM)
(TSE 4006)

System Introduction

The room and telephone monitoring system TSE 4006 is developed by GAMMA to allow the audio monitoring of room and telephone conversation via standard PSTN telephone lines. The TSE 4006 is designed to operate without interfering with the normal functions of the telephone system and to provide the very high speech quality requirements of surveillance operatives. Transmitters use current when operating and this normally creates a voltage drop in the PSTN line being used. The TSE 4006 receiver is equipped with a special circuit which replaces the current used so that there is no voltage drop in the telephone line. This makes the TSE 4006 difficult to detect by automatic central exchange loop current detector systems.

Description

The TSE 4006 is specifically designed for covert audio surveillance operations. The TSE 4006 has the ability to monitor a room and its telephone line by utilizing the existing telephone system. All room and telephone conversations can be monitored and recorded from a remote location. TSE 4006 utilizes techniques which have not been previously used in PSTN line monitoring and consists of two units: a front end transmitter module TSE 4006-TX and an FM receiver combined with a line intercept amplifier TSE 4006RX.

Transmitter

The TSE 4006 transmitter module incorporates a highly sensitive microphone coupled to a pre-amplifier with a wide dynamic range, fast acting AGC (Automatic Gain Control), and FM-modulator. It is protected against high voltage spikes and calling signals on the line. The TSE 4006 is available in a variety of forms including a scrambled version TSE 4006-TXS-S or TSE 4006-TXR-S.

Receiver

The TSE 4006-RX receiver is built into a strong aluminum housing containing the FM receiver, Mixer circuitry and a line intercept amplifier with a high impedance differential input and very high common mode rejection. This assures that the highest possible signal to noise ratio is achieved. The built-in mixer circuitry allows the operative to listen to either the room conversation or the telephone conversation - or both at the same time. The receiver TSE 4006-RX is equipped with a de-scrambler module, which is capable of de-scrambling the signals from TSE 4006-TXS-S and TSE 4006TXR-S. Outputs are provided for Headphones, Tape/aux., VOX switch and a 600 ohm balanced output for re-transmission on a standard PSTN dial up line or CCITT M1020 line (leased line).

Applications

A hard wired audio surveillance system is more difficult to detect than a conventional radio transmission system and is capable of giving better speech quality. There is no "drop out" of signal, a common problem with radio transmission systems. The TSE 4006 system incorporates some unique features, and is specifically designed for covert operations. The transmitter is to be installed via parallel connection with the target line and can be concealed inside the telephone, behind the wall socket or anywhere with direct access to the telephone line.

The TSE 4006 system is designed to work with PSTN slave lines without amplifiers and filters.

Typical methods of deployment:

- During new construction work
- Exchanging the telephone
- Hard wiring into the telephone line during covert entry
- Simulated repair of the PSTN communication network

Audio Level/Line Voltage Meter

The TSE 4006-RX is fitted with an analog meter, which enables the line DC voltage or the audio dBm level to be measured by switching between the two modes.

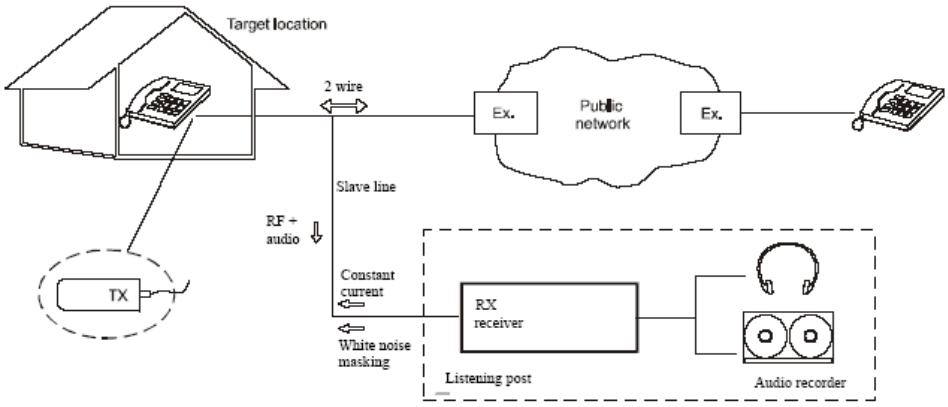
Smart Vox with Noise Cancellation

VOX sensitivity can be set on the front panel. The newly developed intelligent VOX circuitry is equipped with two LEDs for easy setting, and has the capability to distinguish a voice from ambient background noise, increasing the VOX reliability in noisy environments.

Dual Output

The TSE 4006-RX is fitted with 2 audio outputs; an RCA jack socket with line level output for tape recorder and a standard 600 ohm balanced telephone line output for re-transmission of the monitored audio via the PSTN network.

Telephone based operational set up



Technical Features

Fitted with CRS System

All transmitters use current when operating. A major problem for most PSTN line parasitic transmitters is the current drawn from the PSTN line that enables the transmitter to function.

If the transmitter draws more than approx. 6 mA, the line status changes from on-hook to off-hook. This change in current consumption, even when less than 6 mA, is easily detectable by counter surveillance methods and indicates an abnormality in the line. Gamma has developed a Current Re-injection System (CRS) to overcome these problems. The CRS system re-inserts the current used by the TSE 4006-TX unit which avoids a voltage drop across the target telephone line. This ensures that the targeted PSTN line is unaffected by the presence of the TSE 4006-TX unit and makes the system difficult to detect by conventional counter surveillance methods.

Operational Features

Adjustable Off-Hook Threshold Level
The TSE 4006-RX unit is equipped with on-hook/off-hook threshold level adjustment at the rear of the receiver, which can be set between 10 and 40 Volts.

Parametric Equalizer
In order to optimize the audio quality, the monitored signal is passed through a parametric equalizer with variable boost or cut in the 100 Hz to 10 kHz frequency range and variable Q.

Activity Indicator
For ease of operation the receiver unit TSE 4006-RX is fully equipped with LED status indicators.

Options

Standard Transmitter Module
The TSE 4006-TXS is our standard miniature transmitter with built-in microphone.

Extended Microphone Version
On the TSE 4006-TXR transmitter the microphone is mounted on 2 metres of cable, separate from the transmitter board. This allows the microphone to be placed in the target room and the electronics package to be in an adjacent room - a technique that makes it very difficult to locate the transmitter by conventional counter surveillance methods.

British Telecom Outlet Versions
Integrated wall outlet TSE 4006-TXBT-I and External wall outlet TSE 4006-TXBT-W.

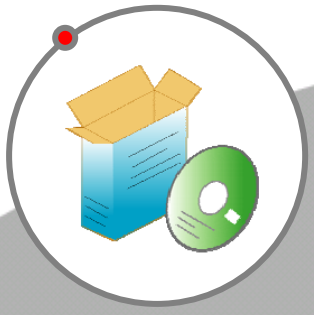
Scrambled Versions TSE 4006-TXS-S and TSE 4006-TXR-R
The TSE 4006-TXS-S transmitter uses a Gamma developed, analogue-speech protection system, which ensures the highest possible quality of retrieved speech. A descrambler module in the TSE 4006-RX receiver is able to decode the signals from the TSE 4006-TXS-S or TSE 4006-TXR-R.

Capacitor Housing Version TSE 4006-TXC
The TSE 4006-TXC transmitter is built into a capacitor housing. which allows the unit to be deployed inside existing electronic equipment.

Technical Specifications

RECEIVER/INTERCEPT AMPLIFIER TSE 4006-RX	
Carrier to be specified by customer or standard	140 kHz +/- 500 Hz
Sensitivity (fmod. = 1kHz, deviation + - 3kHz)	- 82 dBm at 20 dB S/N
Sensitivity (fmod. = 1 kHz, deviation + - 3kHz)	- 48 dBm at 50 dB S/N
Selectivity - 30 dB	+/- 20.65 kHz
Common mode rejection	70 dB
AM rejection (Vin = - 20 dBm, AMmod = 30 %)	40 dB
Distortion (Vin = - 20 dBm, deviation = + - 3 kHz)	0.55 %, 1kHz
Input impedance (140 kHz)	> 1kOhm
Audio frequency response - 3dB (line out)	300 Hz to 5 kHz
Over voltage spikes and ring protection circuit	> 180 V
AUDIO SECTION	
Differential input impedance AC	> 25 kOhm
Differential input impedance DC	> 3 mOhm
Gain (input to line out)	0 dB (1kHz)
Frequency response (input to line out)	290 Hz - 8.3 kHz - 3dB
Common mode rejection (0 dBm input)	> 70 dB
Signal to noise ratio (0 dBm input)	> 60 dB
Harmonic distortion (0 dBm output, 1kHz)	< 0.2 %
Off hook level adjustment range	10 to 40 VDC
MIXER AUDIO SECTION	
Output voltage line out (deviation = +/- 3 kHz)	700 mV (no load)
Output voltage telephone out (deviation = +/- 3kHz)	230 mV (600 ohm load)
Output impedance telephone out	600 ohm
Output impedance line out	1 kOhm
Output impedance headphones out	47 ohm
Parametric equalizer frequency adjustment range	100 Hz to 10 kHz
Parametric equalizer Q adjustment range	0.4 to 4
Parametric equalizer gain adjustment range	+/- 15 dB
Meter range RF level	- 80 to -20 dBm
Meter range DC level	0 to 60 VDC
Output line current for transmitter	3 mA DC
Max. output voltage for transmitter	72 VDC
Max. noise masking voltage for transmitter	0.3 V RMS
Power supply	115/230 VAC (50 - 60 Hz)
Dimensions	265x260x82 mm
	10.4x10.2x3.2 inches
Weight	2.8 kg / 6.17 lbs
TRANSMITTER TSE 4006-TX	
Carrier frequency	140 kHz +/- 500 Hz
Output impedance	47 ohm
Output voltage (140 kHz square wave)	500 mV RMS
Max. modulation	+/- 5kHz
Frequency response	150 Hz to 3.5 kHz - 3 dB
Current consumption	3 mA DC
Over voltage spikes and ring protection circuit	> 180 V
Audio amplifier AGC range	50 dB
Microphone vibration sensitivity	< 66 dB
Dimensions TSE 4006-TXS	38x10x10 mm
	1.5x0.4x0.4 inches
Dimensions TSE 4006-TXR	38x10x10 & 10x7x5 mm
	1.5x0.4x0.4 & 0.4x0.3x0.2 inches
Dimensions TSE 4006-TXC	30x10x21 mm
	1.2x0.4x0.8 inches
Dimensions TSE 4006-TXS-S	38x10x14 mm
	1.5x0.4x0.6 inches

Analytical Software, Forensic
& Speech Technology



Index

Analytical Software

iBase for Arabic speaking Organizations

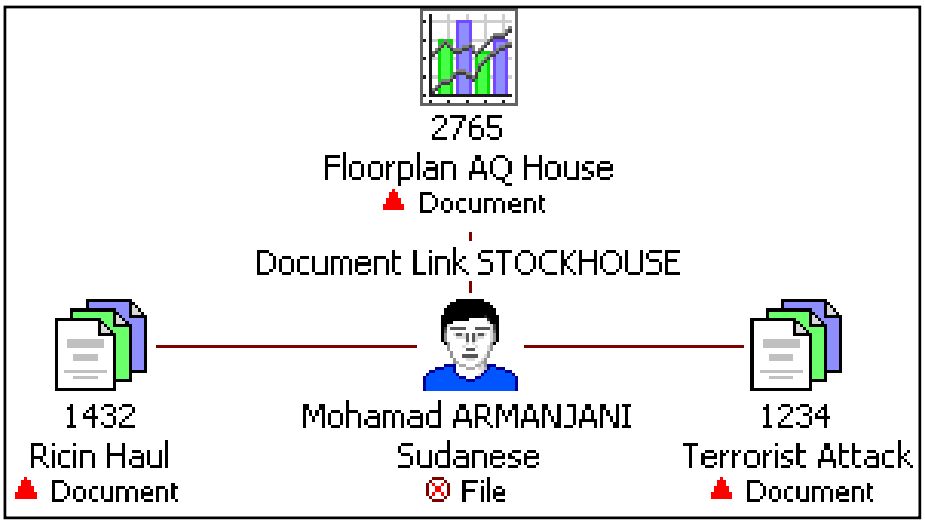
To process and analyze large quantities of data (eg. to retain and be able to query mobile and landline billing data over longer periods of time), or to permanently store data, the i2 database component iBase should be considered. The database consists of two parts: iBase User and iBase Designer. The iBase User component is required to access and manipulate information in the database and display it in the Analytical Notebook. The iBase Designer component allows the user to design or change the way the database is set up and how it operates. Each organization needs only one of these 'Designer' components. The iBase Designer part of the course covers the design and maintenance of the database. There will need to be at least one person in each organization who has the technical ability to configure and permanently maintain the database.

The advanced querying facility in iBase allows for more effective data mining and significantly increases the analytical power of the software. There is the added advantage of providing the organization with a database to store and access their information easily.

i2's iBase 4 does not currently operate using Arabic characters. In spite of the work around solutions laid out below, it will still be necessary to assign an English speaking IT expert to be the key operator or 'super user' for the system.

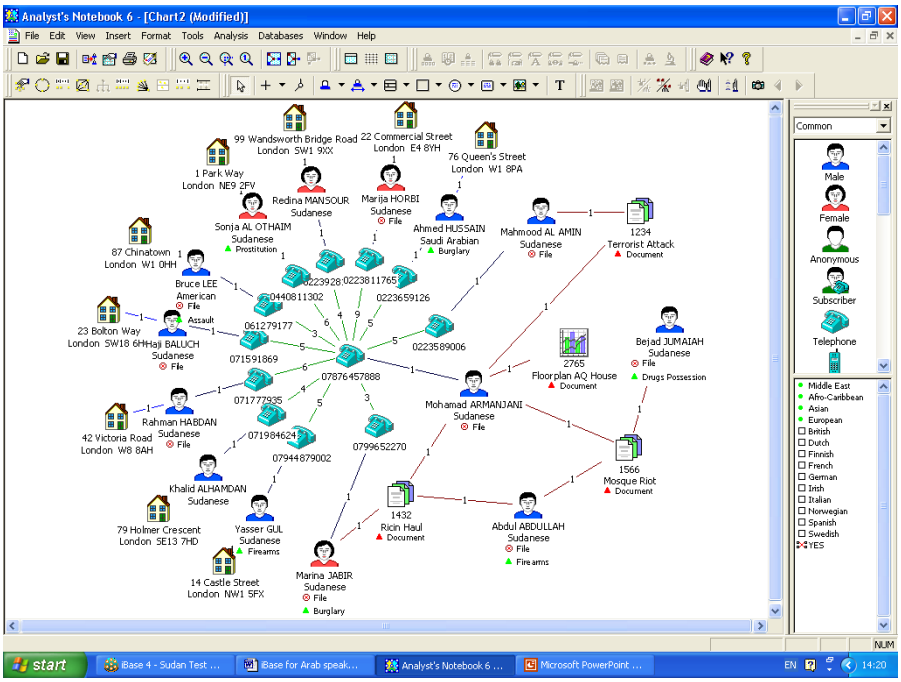
Options for creating an English/Arabic iBase Database:

- Hyperlinks can be embedded into the individual database entries, which when activated open original Arabic documents, such as operational files, charts of police floor plans, Excel spreadsheets, PDFs, html documents, scanned documents, etc. (Photographs can be embedded into the database proper).
- A series of symbols attached to entities indicate to non-English speaking users that there are Arabic language documents (such as bio-data, agent reports, files, etc.), which relate to the entity. (see below)

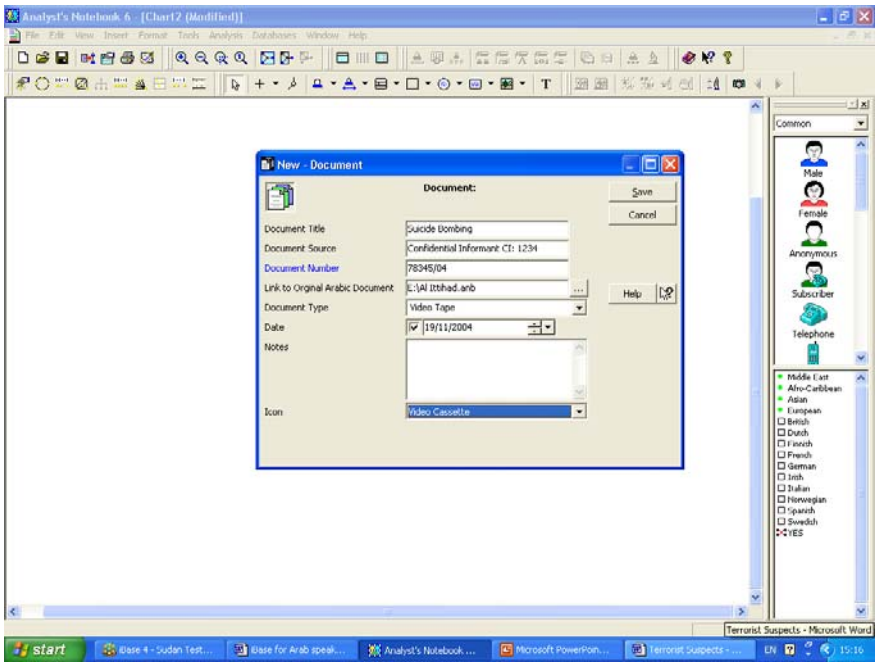


iBase Screen Shots

iBase 4 screen shot showing a 'Find Entry' screen and (below) a typical entry of a person's details. The designer of the database has included a field where a hyperlink to an Arabic file ('Associated Files') can be accessed from this screen.



ANB can also be used as a data entry point. The analyst needs only to draw a visual interpretation of the relationships between people and other entities to be displayed, and the information will automatically be stored in iBase.



MELANIE - Intelligence Environment

Why Speech Classification?

The increasing quantity of speech signals needs an effective and high quality means for the analysis of audio data.
Obtaining support from an automated software tool is highly appreciated by operators working with the analysis of speech files.

MELANIE can help support the operator with:
- Automated analysis of incoming speech signals
- A means for analysis of incoming speech signals using the results of the MELANIE classifiers.

What Can Be Analysed?

MELANIE provides a software library for the classification of incoming speech signals referring to

- Speech Detection:
The parts of audio signals containing speech are marked. For storing the incoming signals, only those parts containing speech may be stored.

- Language Identification:
All incoming audio signals are classified according to the speech prevailing in the audio files. All languages of the world can be identified as soon as training material is available.

• Speaker Identification:

Speakers in incoming audio signals can be identified. The algorithm is independent of the spoken language, thus a speaker can be found also when communicating in another language.

Training material for the speaker to be analysed is necessary, a rejection of unknown speakers is made.

Product Description

For these classifiers, training, testing, and automatic production can be performed. For each application, libraries of software functions are available, together with a standardized and open interface (CORBA).

• Training environment: Classifiers can be trained optimally for the domain of the user. In a simple script-based training, the user can build the classifiers according to his domain and data material.

• ELAMAN offers trained models for some applications, the user does not have to train the classifier's parameters.

• Production environment: This environment automatically classifies all incoming audio signals using the available classifiers. A simple standardized interface is given for the automatic production 24/24h. The production environment is available as PC license or as site license.

The classifiers can be used via the CORBA interface. They can be integrated into PC-based OEM applications.

Classifiers are available for the following applications:

SQ Speech	Detection and Language Identification
MP Language	Identification
GMM Speaker	Identification

Technical Data

Input format — Real signal comprising

- Sample Rate: 8, 16 kHz
- Data Type: PCM, A-law, µ-law

Also available as options, routines for processing other data formats.

Output	The classification result can be accessed from the output interface. The output is provided as: • Classification results in equidistant configurable time segments, e.g. for generating a label track (maximum score, individual score for all classes) • Classification results for the entire signal up to the signal end (maximum score, individual score for all classes)
Interfaces	Standard interface CORBA enables the access to all results of MELANIE.
Performance	The classifiers show reliable classification accuracy combined with a high processing speed. Realtime factor: Depending on the type of classifier and the amount of classes (such as languages, speakers), ranging from 1/7 to 1/20 with e.g.: • Hardware: P4; 3 GHz; 1GB RAM • Different Classes: 10

Company Principles and Policy

Technology
… in development and company management is state-of-the-art, and represents only the best.

Quality
… in all areas of our company is regarded as the almost requirement for risk-free and successful cooperation with our customers, and business partners.

Market Position
… we are the specialists in the field of signal and data processing as well as pattern recognition, and we are glad to face competition.

Colleagues
… form the roots of our company, and give the performance required for maintaining and building the technical base, and close personal cooperation we have with our clientele.

Growth
… we strive toward a healthy, stable foundation at home and abroad.

Services
… are comprehensive and complete. As a full-system company we offer standard equipment, systems, and services.

Trust
… in the relationships to our business partners, and within our own company forms the basis of our business.

MELANIE – Language Identification, MP

Functionality

Speech signals can be analysed according to the language prevailing in the speech. For each speech signal, an overall score and probability is estimated. In addition, these values can also be estimated for any time interval.

Training of Models

Goal Training is performed in order to optimise the models on the languages and channel of the application.

Training Data The training data must be labeled according to the language in the speech signal. The data must be representative and as similar as possible to the data of the application. A minimum of one hour of data is required for each language.

Trained Models In case of insufficient data, trained models for a set of languages can be provided to use the system from scratch.

Technical Data

OperatingSystem Available on Windows XP and Linux

Processing Time
- On a P4; 3GHz, 1GB RAM computer
- Classifying 10 different languages
- 1/7 of real time; i.e. a signal of 7 minutes length is processed in one minute

Recognition Rate The recognition rate depends on the number of languages, on the similarities and charactistics of the languages, and on the speech quality. For example, when distinguishing 5 languages in radio quality, an accuracy of 80 % can be obtained.

Products

Mel-Pr-MP-site Production environment for MELANIE MP (site license)
Mel-Pr-MP-PC Production environment for MELANIE MP (PC license)
Mel-Tr-MP Training environment for MELANIE MP
Mel-LM-MP Trained language models for classification with MP

MELANIE – Speaker Identification, GMM

Functionality

Speaker identification determines the probability of a set of speakers in speech signals.

The algorithm is especially useful when searching for a certain speaker in mass audio data.

Training of Models

Goal	Training is performed in order to optimise the models on the respective speaker.
Training Data	The training data must be labeled according to the prevailing speaker. If possible, the speaker data should be obtained from different channels and languages. A minimum of two minutes speech is required for each speaker.

Technical Data

OperatingSystem	Available on Windows XP and Linux
Processing Time	• On a P4; 3GHz, 1GB RAM computer • 1/8 of real time; i.e. a signal of 8 minutes length is processed in one minute
Recognition Rate	The recognition rate depends on the number of speakers, on the similarities of the speakers among each other and on the speech quality.

Products

Mel-Pr-GMM-site	Production environment for MELANIE GMM (site license)
Mel-Pr-GMM-PC	Production environment for MELANIE GMM (PC license)
Mel-Tr-GMM	Training environment for MELANIE GMM

MELANIE Speech Detection & Language Identification, SQ

Functionality

Speech signals are often recorded with pauses and noise within the speech signal. This algorithm is able to detect those parts of a speech signal that contain speech on larger segments of audio signals. The results are very useful to reduce the amount of data that have to be stored and anaylsed.
Speech signals can be analysed according to the language prevailing in the speech.

For each speech signal, an overall score and probability is estimated. In addition, these values can also be estimated for any time interval.

Training of Models

Goal	Training is performed in order to optimise the models on the languages and channel of the application. Training
Data	The training data must be labeled according to either speech/nonspeech or with the prevailing language. The data must be representative and as similar as possible to the data of the application. A minimum of one hour of data is required for each language.
Trained Models	In case of insufficient data, trained models for a set of languages can be provided to use the system from scratch.

Technical Data

OperatingSystem	Available on Windows XP and Linux
Processing Time	• On a P4; 3GHz, 1GB RAM computer • Classifying 10 different languages • 1/15 of real time; i.e. a signal of 15 minutes length is processed in one minute
Recognition Rate	The recognition rate depends on the number of languages, on the similarities and charactistics of the languages, and on the speech quality.

Products

Mel-Pr-SQ-site	Production environment for MELANIE SQ (site license)
Mel-Pr-SQ-PC	Production environment for MELANIE SQ (PC license)
Mel-Tr-SQ	Training environment for MELANIE SQ
Mel-LM-SQ	Trained language models for classification with SQ

MELANIE - Topic Spotting, TOP

Production Module for fast and reliable spotting of the topic/category prevailing in speech signals. Training module for topic spotting parameters.

Functionality

Speech signals can be analysed according to the topic/category prevailing in the speech. For each speech signal, an overall score and probability is estimated. In addition, these values can also be estimated for any time interval.

Training of Models

Goal	Training is performed in order to optimise the models on the topic and channel of the application.
Training Data	The training data must be labeled according to the topic in the speech signal. The data must be representative and as similar as possible to the data of the application. A minimum of one hour of data is required for each language.

Technical Data

OperatingSystem	Available on Windows XP and Linux
Processing Time	• On a P4; 3GHz, 1GB RAM computer • Classifying 3 different classes/ topics • 1/14 of real time; i.e. a signal of 14 minutes length is processed in one minute
Recognition Rate	The recognition rate depends on the number of topics, on the similarities and the overlap among topics, and on the speech quality. For example, when distinguishing 2 topics in radio quality, an accuracy of 87 % can be obtained.

Products

Mel-Pr-TOP-site	Production environment for MELANIE TOP (site license)
Mel-Pr-TOP-PC	Production environment for MELANIE TOP (PC license)
Mel-Tr-TOP	Training environment for MELANIE TOP

MELANIE – Trained Models for Language Identification

Functionality

Using the models, MELANIE classifiers can be used from scratch without an additional training step.
These trained language models can be recommended if not sufficient training material is available for the languages to be classified. The performance is the better, the more close the data of the application correspond to the used language model. For these trained models, the type of signal quality is given in the following table.

Available models

Short Cut1	Language	Dialect	Quality
CAF-ARA-EG-TEL	Arabic	Egyptian	Telephone
MED-ARA-RTV	Arabic	Microfon	Radio / TV
CAF-CHI-TEL	Chinese, Mandarin	Mainland	Telephone
CAF-CHI-TW-TEL	Chinese, Mandarin	Taiwan	Telephone
MED-CHI-RTV	Chinese		Radio / TV
MED-SCR-RTV	Croatian		Radio / TV
MED-CZE-RTV	Czech		Radio / TV
MED-DUT-RTV	Dutch; Netherlands		Radio / TV
CAF-ENG-US-TEL	English	American , non-Southern	Telephone
CAF-ENG-US-S-TEL	English	American , Southern	Telephone
MED-ENG-RTV	English		Radio / TV
CAF-FAS-TEL	Farsi		Telephone
MED-FIN-RTV	Finnish		Radio / TV
CAF-FRE-CA-TEL	French Canadian		Telephone
MED-FRE-RTV	French		Radio / TV

Short Cut2	Language	Dialect	Quality
CAF-GER-TEL	German		Telephone
MED-GRE-RTV	Greek		Radio / TV
CAF-HIN-TEL	Hindi		Telephone
MED-HUN-RTV	Hungarian		Radio / TV
MED-IND-RTV	Indonesian		Radio / TV
MED-ITA-RTV	Italian		Radio / TV
CAF-JPN-TEL	Japanese		Telephone
MED-JPN-RTV	Japanese		Radio / TV
CAF-KOR-TEL	Korean		Telephone
MED-NOR-RTV	Norwegian		Radio / TV
MED-POL-RTV	Polish		Radio / TV
MED-POR-RTV	Portuguese		Radio / TV
MED-RUM-RTV	Romanian		Radio / TV
MED-RUS-RTV	Russian		Radio / TV
MED-SCC-RTV	Serbian		Radio / TV
MED-SLV-RTV	Slovenian		Radio / TV
CAF-SPA-TEL	Spanish	Non-Caribbean	Telephone
CAF-SPA-C-TEL	Spanish	Caribbean	Telephone
MED-SPA-RTV	Spanish		Radio / TV
MED-SWE-RTV	Swedish		Radio / TV
CAF-TAM-TEL	Tamil		Telephone
MED-THA-RTV	Thai		Radio / TV
MED-TUR-RTV	Turkish		Radio / TV
CAF-VIE-TEL	Vietnamese		Telephone

MELANIE – VIDA, Visual Documents Analysis

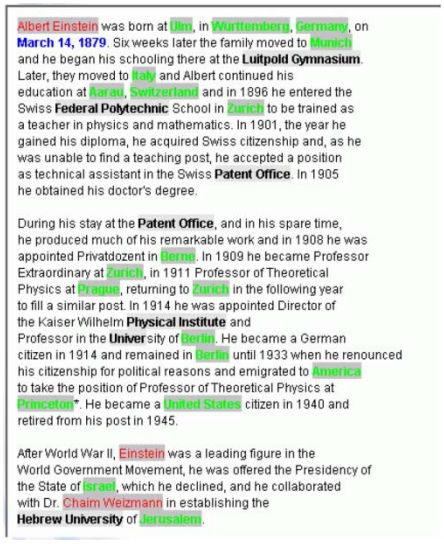
(Analysis and Visualisation of Texts)

VIDA – Visual Document Analysis

- Interactive user interface for visual representation of documents and analysis results
- Analysis of documents against defined criteria e. g.
  - number of words in the text
  - entities such as places, names, organizations
- Statistical analysis of texts
  - keywords
  - n-grams
  - word associations
- Automatic national language identification for texts in
  - German
  - English
  - French
  - Italian
- Text abstraction for speed reading and faster scanning of information
- Analysis results displayed in tables and graphs
  - word frequencies
  - associations
- Text tagging, where texts are highlighted according to relevant criteria
- Relations between keywords
- Finding similar texts

Finding important text entities

Words in the various meaning categories are found automatically. Different highlighting is used in the text for each of the meaning categories.


Albert Einstein was born at Ulm, in Württemberg, Germany, on March 14, 1879. Six weeks later the family moved to Munich and he began his schooling there at the Luitpold Gymnasium. Later, they moved to Italy and Albert continued his education at Aarau, Switzerland and in 1896 he entered the Swiss Federal Polytechnic School in Zurich to be trained as a teacher in physics and mathematics. In 1901, the year he gained his diploma, he acquired Swiss citizenship and, as he was unable to find a teaching post, he accepted a position as technical assistant in the Swiss Patent Office. In 1905 he obtained his doctor's degree.

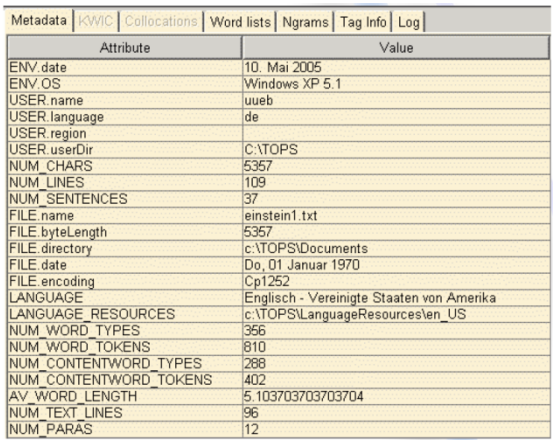
During his stay at the Patent Office, and in his spare time, he produced much of his remarkable work and in 1908 he was appointed Privatdozent in Berne. In 1909 he became Professor Extraordinary at Zurich, in 1911 Professor of Theoretical Physics at Prague, returning to Zurich in the following year to fill a similar post. In 1914 he was appointed Director of the Kaiser Wilhelm Physical Institute and Professor in the University of Berlin. He became a German citizen in 1914 and remained in Berlin until 1933 when he renounced his citizenship for political reasons and emigrated to America to take the position of Professor of Theoretical Physics at Princeton". He became a United States citizen in 1940 and retired from his post in 1945.

After World War II, Einstein was a leading figure in the World Government Movement, he was offered the Presidency of the State of Israel, which he declined, and he collaborated with Dr. Chaim Weizmann in establishing the Hebrew University of Jerusalem.

Metadata

General information on the analysed document is compiled as metadata. This metadata includes the following information, for example:

- Document name
- Source directory
- Creation date
- Number of words, lines and characters
- National language

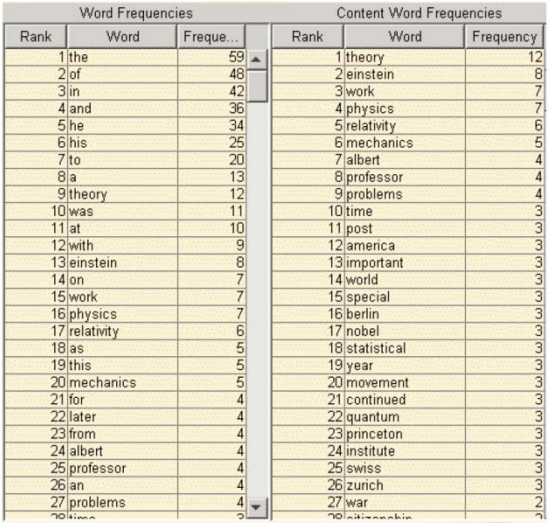


Metadata | KWIC | Collocations | Word lists | Ngrams | Tag Info | Log

Attribute	Value
ENV.date	10. Mai 2005
ENV.OS	Windows XP 5.1
USER.name	uueb
USER.language	de
USER.region	
USER.userDir	C:\TOPS
NUM_CHARS	5357
NUM_LINES	109
NUM_SENTENCES	37
FILE.name	einstein1.txt
FILE.byteLength	5357
FILE.directory	c:\TOPS\Documents
FILE.date	Do, 01 Januar 1970
FILE.encoding	Cp1252
LANGUAGE	Englisch - Vereinigte Staaten von Amerika
LANGUAGE_RESOURCES	c:\TOPS\LanguageResources\en_US
NUM_WORD_TYPES	356
NUM_WORD_TOKENS	810
NUM_CONTENTWORD_TYPES	288
NUM_CONTENTWORD_TOKENS	402
AV_WORD_LENGTH	5.103703703703704
NUM_TEXT_LINES	96
NUM_PARAS	12

Word statistics

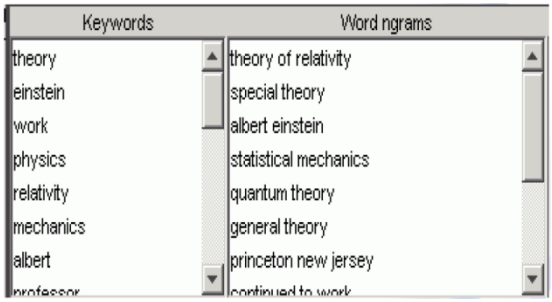
A set of word statistics provides information on the most frequently used words
and the most frequently used words relevant to the content i.e. keywords.



Word Frequencies			Content Word Frequencies		
Rank	Word	Freque...	Rank	Word	Frequency
1	the	59	1	theory	12
2	of	48	2	einstein	8
3	in	42	3	work	7
4	and	36	4	physics	7
5	he	34	5	relativity	6
6	his	25	6	mechanics	5
7	to	20	7	albert	4
8	a	13	8	professor	4
9	theory	12	9	problems	4
10	was	11	10	time	3
11	at	10	11	post	3
12	with	9	12	america	3
13	einstein	8	13	important	3
14	on	7	14	world	3
15	work	7	15	special	3
16	physics	7	16	berlin	3
17	relativity	6	17	nobel	3
18	as	5	18	statistical	3
19	this	5	19	year	3
20	mechanics	5	20	movement	3
21	for	4	21	continued	3
22	later	4	22	quantum	3
23	from	4	23	princeton	3
24	albert	4	24	institute	3
25	professor	4	25	swiss	3
26	an	4	26	zurich	3
27	problems	4	27	war	2

Keywords – Word n-grams

Statistical determination and listing of all keywords and word n-grams (common sequences of words).



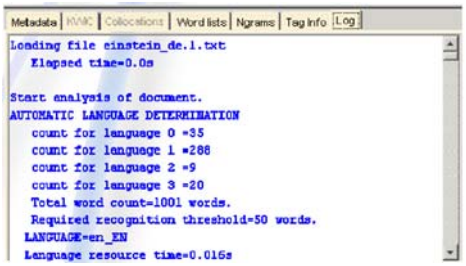
Keywords	Word ngrams
theory	theory of relativity
einstein	special theory
work	albert einstein
physics	statistical mechanics
relativity	quantum theory
mechanics	general theory
albert	princeton new jersey
professor	continued to work

National language identification

Automatic determination of the language of a text. National language identification is currently implemented for the following languages:

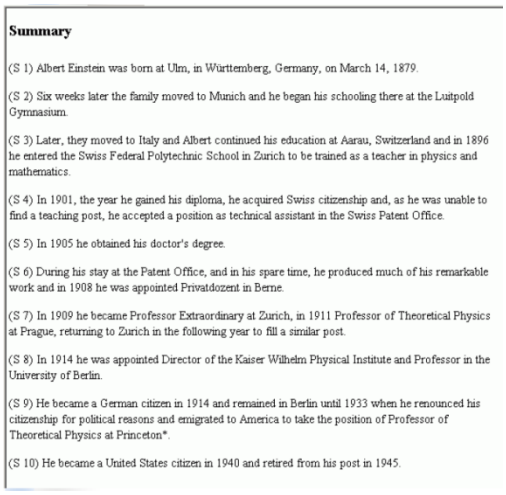
- German
- English
- French
- Italian

Other languages can be implemented on request.



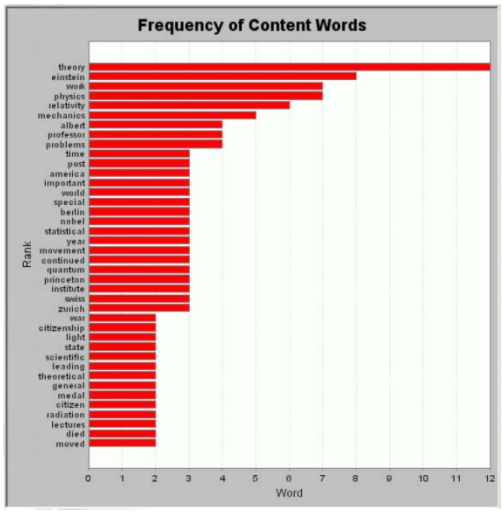
Abstraction

A summary can be generated automatically to enable speed-reading of the text.



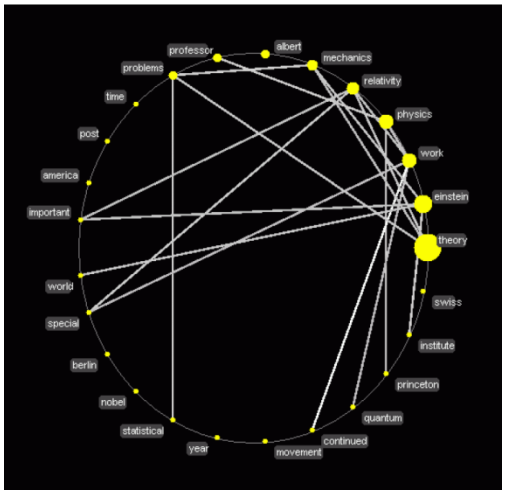
Visualisation – Frequency

Visual representation of the frequency of specified keywords in the text.



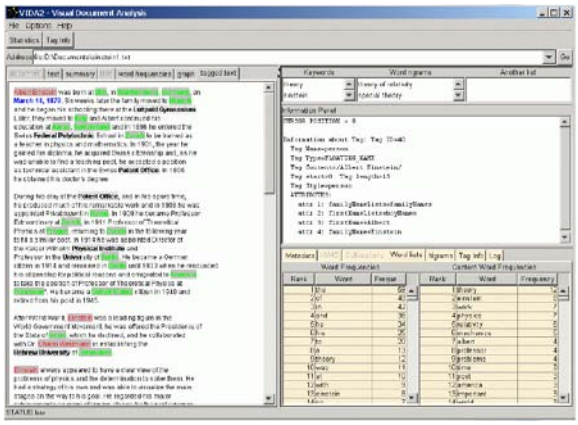
Visualisation – Associations

VIDA includes the visualisation option of an association graph for delivering faster identification of the text content.



Visualisation – Entities

VIDA provides coloured highlighting of entities and also lists entities and keywords in a table.



Finding similar texts

VIDA provides a function that assesses the similarity of texts, for text location. This function automatically lists in a table all the texts analysed, in order of decreasing
similarity. In addition, the most important matches are output in keywords.

Ähnlichkeit	Text	Übereinstimmung
1.0	einstein_de.1	einstein einsteins zeit physik relativitätstheorie theorie albert später
0.75	einstein_de.3	einstein einsteins zeit physik relativitätstheorie albert
0.5	einstein_de.2	einstein zeit relativitätstheorie albert
0.25	einstein_en.2	einstein albert
0.125	einstein_en.1	einstein
0.125	einstein_en.3	einstein
0.125	einstein_en.4	einstein
0.125	einstein_de.4	einstein
0	en_alqaida	
0	en_bush	

VIDA – Specification

Operating systems	Windows, Linux
Automatic national language identification	• German • English • French • Italian • Other languages on request
Text analysis	• English • German • Other languages on request
Statistical analysis of texts	Based on word lists and rules

No linguistic knowledge necessary

Functions

- Word statistics
- Automatic determination of keywords and n-grams
- Word associations
- Histogram for word frequencies
- Marking (tagging) of entities: proper names, places, date, etc.
- Visualisation of associations and entities

Ordering information

VIDA-Inter Vida tool, to be used interactively, incl. graphical user interface

VIDA-Prod Vida program to be embedded in software environment

VIDA-Conf Vida configuration software, used for adaptation to new domain

MELANIE - Word Spotting, WS

Functionality

Speech signals are often recorded with pauses and noise within the speech signal. This algorithm is able to detect those parts of a speech signal that contain speech on larger segments of audio signals. The results are very useful to reduce the amount of data that have to be stored and anaylsed.
Speech signals can be analysed according to the language prevailing in the speech.

For each speech signal, an overall score and probability is estimated. In addition, these values can also be estimated for any time interval.

Training of Models

Goal	Training is performed in order to optimise the models on the languages and channel of the application. Training
Data	The training data must be labeled according to either speech/nonspeech or with the prevailing language. The data must be representative and as similar as possible to the data of the application. A minimum of one hour of data is required for each language.
Trained Models	In case of insufficient data, trained models for a set of languages can be provided to use the system from scratch.

Technical Data

OperatingSystem	Available on Windows XP and Linux
Processing Time	• On a P4; 3GHz, 1GB RAM computer • Classifying 10 different languages • 1/15 of real time; i.e. a signal of 15 minutes length is processed in one minute
Recognition Rate	The recognition rate depends on the number of languages, on the similarities and charactistics of the languages, and on the speech quality.

Products

Mel-Pr-SQ-site	Production environment for MELANIE SQ (site license)
Mel-Pr-SQ-PC	Production environment for MELANIE SQ (PC license)
Mel-Tr-SQ	Training environment for MELANIE SQ
Mel-LM-SQ	Trained language models for classification with SQ

SCOOTY – Speech Classification Online and Offline Technology

SCOOTY Overview

What can SCOOTY be used for?

SCOOTY is a speech analysis system. In a process from signal detection, recording, processing and filtering to evaluation, SCOOTY is part of the evaluation by analysing audio files for the following features:

- speech/non-speech detection
- language identification

The core parts of SCOOTY executing this analysis are called "classifiers". Based on a client / server architecture, SCOOTY provides a software environment for:

- training
- configuration
- classification
- production

How is SCOOTY used?

The process is the following: After classifier training and configuration, SCOOTY produces classification results without further user intervention. Training and Test result data as well as configuration data are stored in the data resource (a kind of an archive) and are recalled for production.

Production results are also saved in the archive and concurrently shown on screen to allow monitoring of progress and results.

Who uses SCOOTY?

Everybody working on speech and language is a possible user of SCOOTY software. Typical users of the software are people working on huge amounts of speech data coming in. This can be a university working on the structure of speech and languages, such as dialects, accents, and language history. A benefit from the use of SCOOTY can also be drawn by research institutes in medicine treating with diseases in the production and perception of speech.

What is the benefit when using SCOOTY?

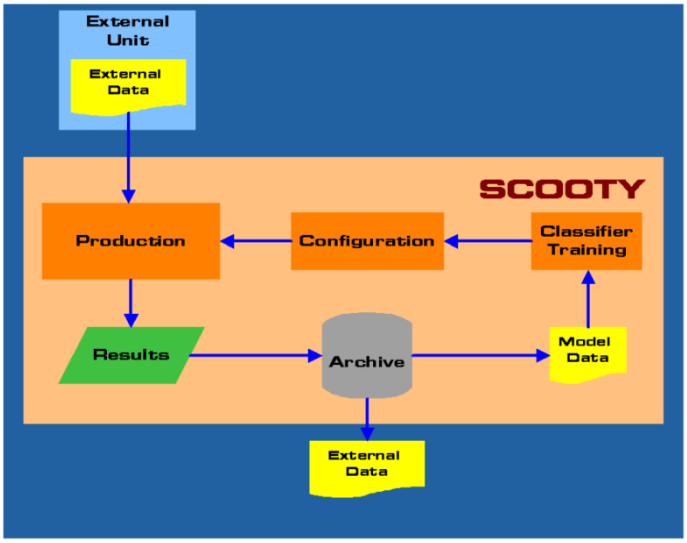
Using SCOOTY, large amounts of speech signals can automatically be processed and sorted according to their characteristics.

The performance of the system depends on the training data that are fed to the system. Speech files can be sorted according to the characteristics, giving an indication on the spoken speech. Eventually, an indication can be given also on the dialect, depending on the training data.
The accuracy for the classification of a language depends on the involved languages and especially on the training material that is used for the estimation of the classifier. Out of 1000 files for classification, usually 600 files can be classified correctly, according to the spoken language.

Does the structure of SCOOTY fit into my environment?

The SCOOTY software is based on a client/server architecture consisting of the following parts:

- SCOOTY client(s) – graphical user interface
- processing server – signal parameterisation and classification
- archive server – data management

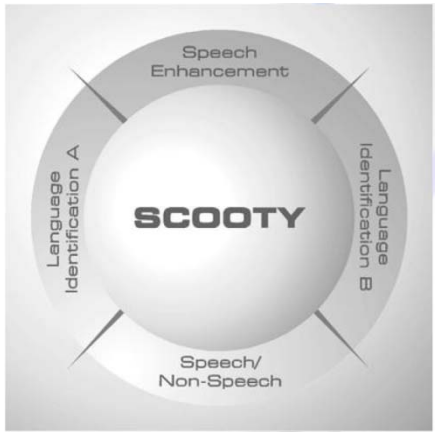


Each of these software parts is available as single user version or network version, and each of them is available for different operating systems. They can be combined freely and platformindependently via TCP/IP, so they are highly adaptable to system and application requirements.

Classifiers

How does SCOOTY use the classifiers?

SCOOTY performs the classification with the following classifiers:
- a speech/non-speech classifier
- two language classifiers using different algorithms estimating the probability for the involved languages.



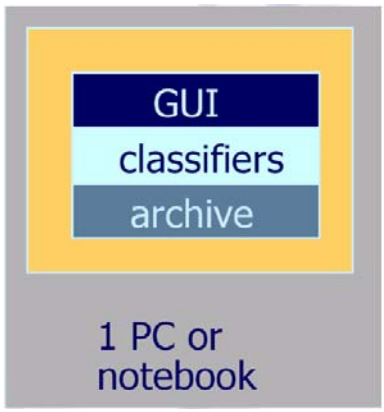
Furthermore, SCOOTY **enhances** the **speech** quality of the input signal to improve the reliability of the classification results.

SCOOTY applies cascaded classifiers and the signal enhancement to the input signal containing WAVE files. The classifiers are equipped with an extensive parameter set. The parameters are adjusted during classifier training to gain optimum quality of classification results.

System Configuration Examples

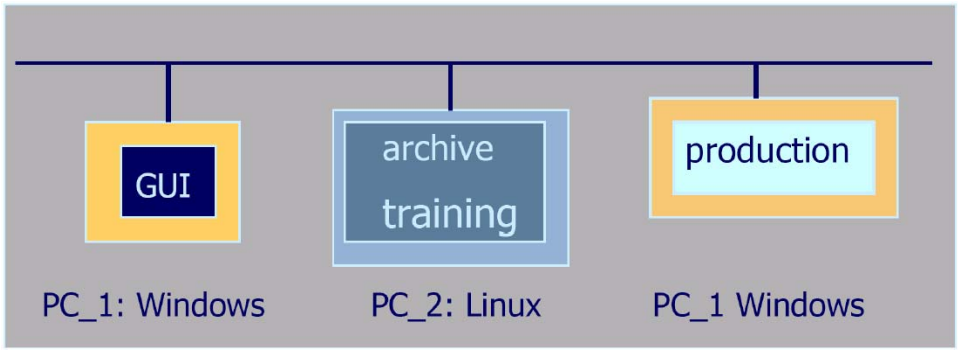
Example 1:

SCOOTY runs on 1 PC or notebook and is used by 1 user.

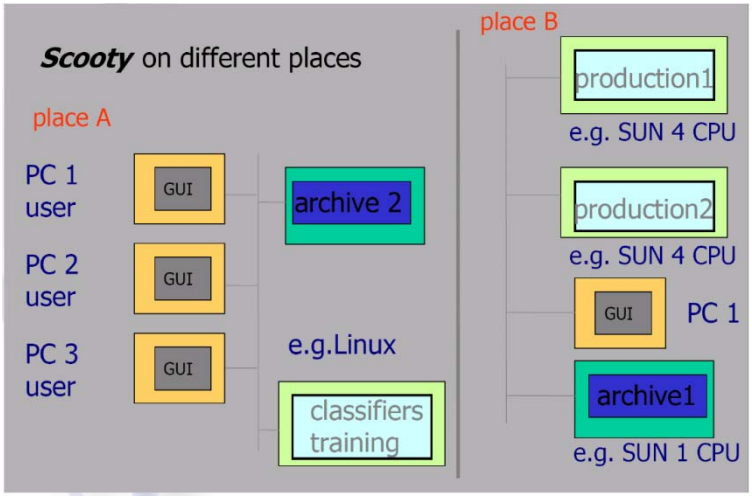


Example 2:

SCOOTY is distributed over 3 workstations connected via a network. Still it is used by 1 user but the workstations perform different tasks, such as classifier training and production.



Example 3:
SCOOTY is used by multiple users working on different tasks at different places. Operators at place A work on classifier training and designing different SCOOTY configurations, while other users work directly on the production results. A network connection between places A and B is not necessary.



Classifier Parameterization and Training

How can SCOOTY find "my" languages?

The SCOOTY classifiers are trainable to allow them to be adapted to individual customer requirements. The results of the training process are special model data, which are later used during classification. Best classification results are achieved with customer training and test data.

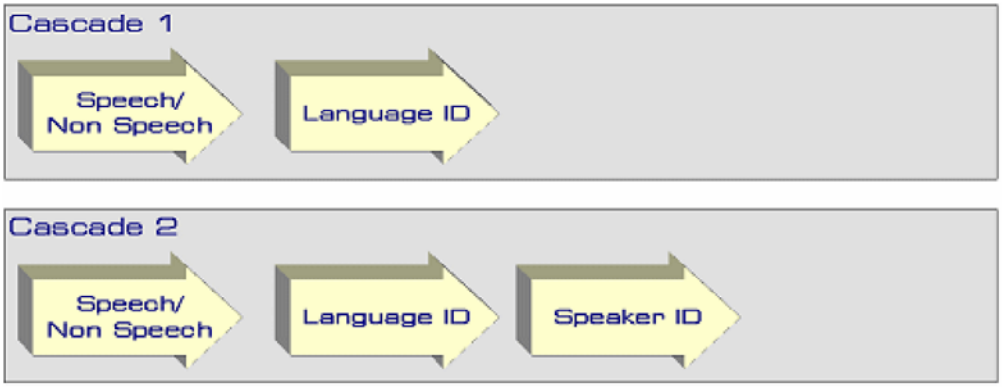
SCOOTY is equipped with a complete training and test environment for the classifiers. This covers a transcription tool to generate label files (they contain information about whether an audio file contains speech, and if so, about the language) and a graphical user interface for easy classifier training and testing.

Classification Process Configuration

Is SCOOTY flexible to meet my requirements?

SCOOTY allows the use of the available classifiers in different combinations:
- cascading of classifiers and signal enhancement
- exclusion of unnecessary classifiers
- use of differently parameterized classifiers

Different combinations and cascades of classifiers can be summarized to signal flows. The following figure shows 2 valid cascades, each specially adapted to a certain scenario:



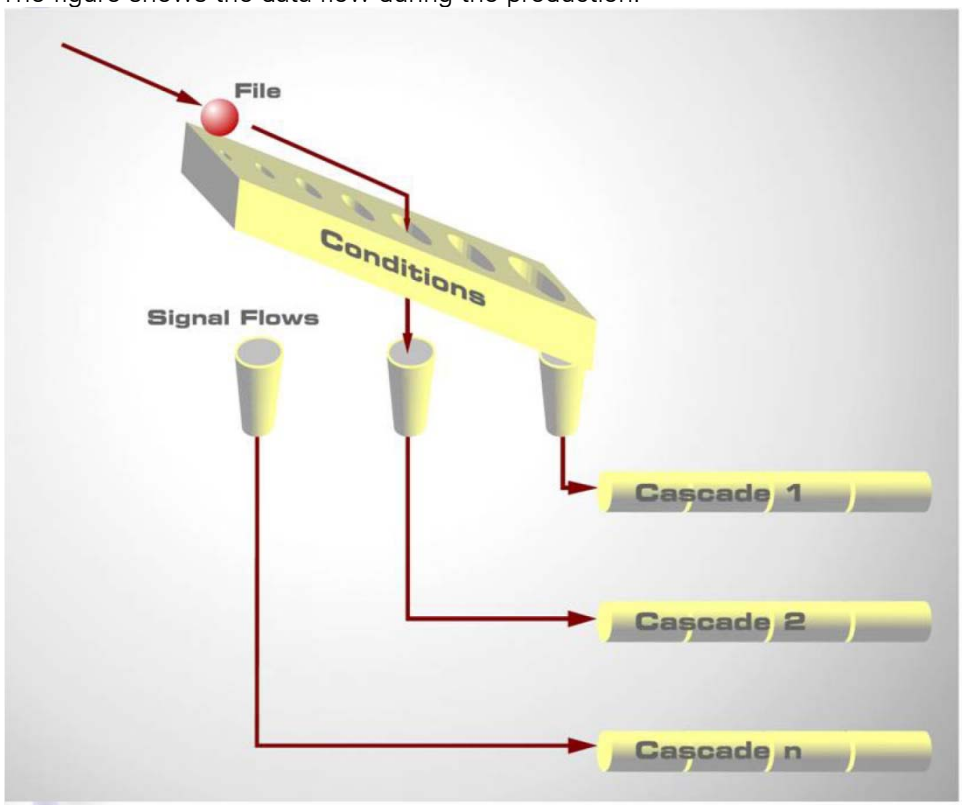
Production

How does SCOOTY work?

After starting the production, SCOOTY reads its input directory and processes the input files in a hierarchical order. Each input file represents a task for SCOOTY. SCOOTY processes them in the order of priorities. For each task, SCOOTY produces result files and additionally displays the results on the screen. No further user intervention is required, but the user can observe the production progress and status.

During production, SCOOTY selects one of the configured signal flows (cascades) for each task. The selection depends on information provided by an external control unit. The file then runs through a cascade of classifiers assigned to the selected signal flow. In the cascade, the file is finally analyzed. This concept allows SCOOTY to analyze signal files from different sources.

The figure shows the data flow during the production:



A processing server coordinates the classification process. It encapsulates classification functions in a way that they are externally available as services.

Result Retrieval and Display

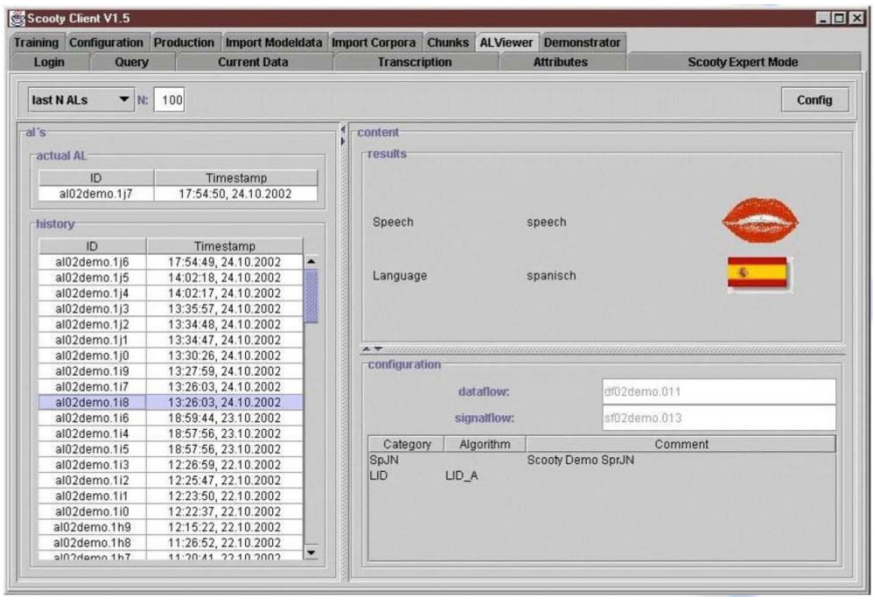
How can I view and further process SCOOTY's results?

Classification results are:
- Detected speech
- Identified languages

SCOOTY stores the results, the protocol of all activities and processed files in an archive:
- A work log of each classification (text format)
- Label and score files of each classification (linked information in text and XML format)
- Training and test results, model data, test results (text and XML format)
- Signal files (WAVE format)

The LogViewer is an extensive retrieval tool to recall the results from the archive. Other result files are additionally stored in an output directory from which they can be taken by other processes. SCOOTY provides all results for extensive statistical computing. The archive allows the user to search for all types of data.

Additionally, during production temporary results are displayed on screen:



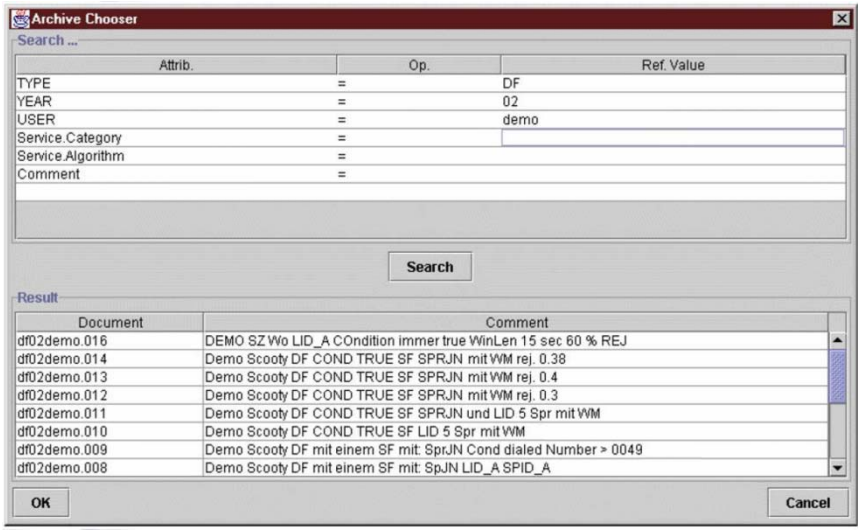
Data Management

Isn't it difficult for me to handle all these complex data?

All information is provided with attributes, after which it can easily be searched and sorted. SCOOTY provides a user-friendly graphical user interface for comfortable and fast data retrieval and viewing.

A central data handling resource (the archive) is the pool for any type of information. All relevant data appearing in the SCOOTY workflow are stored on the archive server. The SCOOTY archive assures traceability of processes, data consistency and cross-reference consistency. It stores:

- training, test results and model data
- configuration data
- production results



Further Developments

I need different information from the audio signal. Will there be more classifiers?

Currently, the following classifiers are under development:

- word spotter
- topic spotter based on sound files
- text visualisation and classification
- speaker identification

Furthermore, there will be the opportunity of text analysis of audio files.

Feature Summary

The following list summarizes the features of SCOOTY:

- System for automatic signal classification
- Server client architecture
- Use of standard hardware
- Scalable
- Extensible with new classifiers
- Trainable with customer data
- All algorithms for training available
- Improvement of the quality of classification
- Full support preparing data for training
- Powerful archive for offline job analysis
- Support of statistical computation based on classified data

Do not hesitate to contact us if you need more detailed information.

Further Features and Services

Scalability SCOOTY can be run on systems ranging from a single user – single computer (all components installed on one computer) up to client server networks (components distributed over several computers).

Extensibility The software is based on a modular concept. All modules are available separately and for different operating systems. For details see the SCOOTY pricing schedule.

User Training User training is available for training and configuration of classifiers, setting up production configuration, and evaluation of results according to customer specific requirements. The training level depends on customer requirements. The training can be held at customer's site or ours, using example data or data from customer environment. Contact ELAMAN for details.

Consulting Service ELAMAN helps and consults on classifier training and testing, or, if required, performs the classifier training and test for customers.

Software Support The software licenses include free software support inclusive of all updates for 1 year.

Customer Documentation The system is equipped with a user manual an installation instructions. The software provides context sensitive online help. All documentation is available in English and German.

System Requirements

Platforms (all program components)

- Windows 2000, Windows XP
- Linux (S.u.S.E. 7.x and higher)
- SUN Solaris 8.x

Archive Server:

- Disk space: > 100 Gbyte, depends on usage
- RAM: > 256 MByte
- CPU: one processor machine

Server for Classifiers

- Disk space: ca. 40 GByte for training
- RAM: > 512 MByte
- CPU: two or more processor machine

Client (Graphical User Interface)

- Normal PC or notebook
- Disk space: 30 GByte
- RAM: 256 MByte
- CPU: ca. 600 MHz Pentium

Interfaces

- Input: file based (Text-/WAV files), header file with information must be specified
- Output: file based (Text, XML)

Performance Data

Hardware dependent, e. g.: Pentium PC 1-2 GHz
- a single LID classifier faster than realtime

Training & Consultancy

Product Training

Training is a fundamental and integral factor in the successful implementation and running of a security or surveillance operation. One of the main reasons for this is the high level of sophistication involved in the equipment required.

Recognising this ELAMAN always provides full training and technical backup for all products supplied to our clients.

- Maintenance Training
- Operator Training
- Admin- and Supervisor Training

All Trainings will be carried out by experienced Trainers and will be conducted in Europe and/or at customer's premises in order to reach the highest level of skills for the students.

Communication
Monitoring Consultancy

As part of a total service to governments and law enforcement agencies, ELAMAN provides one of the most vital and key elements in an overall security and intelligence programtechnical consultancy.

- Entire technical consultancy for interception applications for existing systems and upcoming new implementations and requirements (communications monitoring, spectrum monitoring and locating, etc.).
- Collecting new interception requirements and transforming these into technical specifications in order to define tender specifications and to approach and select suppliers.
- Recommending technical and performance improvements and support for technical evaluation of offers and suppliers.
- Providing recommendations and technical concepts for new interception solutions (e.g. monitoring of Thuraya, passive monitoring systems, satellite monitoring solutions, internet monitoring etc.).
- Providing information out of the market of suppliers for monitoring surveillance systems.

GOVERNMENTAL SECURITY SOLUTIONS




If you would like further Information about ELAMAN,
or would like to discuss a specific requirement or project, please contact us at:

Elaman GmbH
German Security Solutions
Seitzstr. 23
80538 Munich
Germany

Tel: +49-89-24 20 91 80
Fax: +49-89-24 20 91 81
info@elaman.de
www.elaman.de