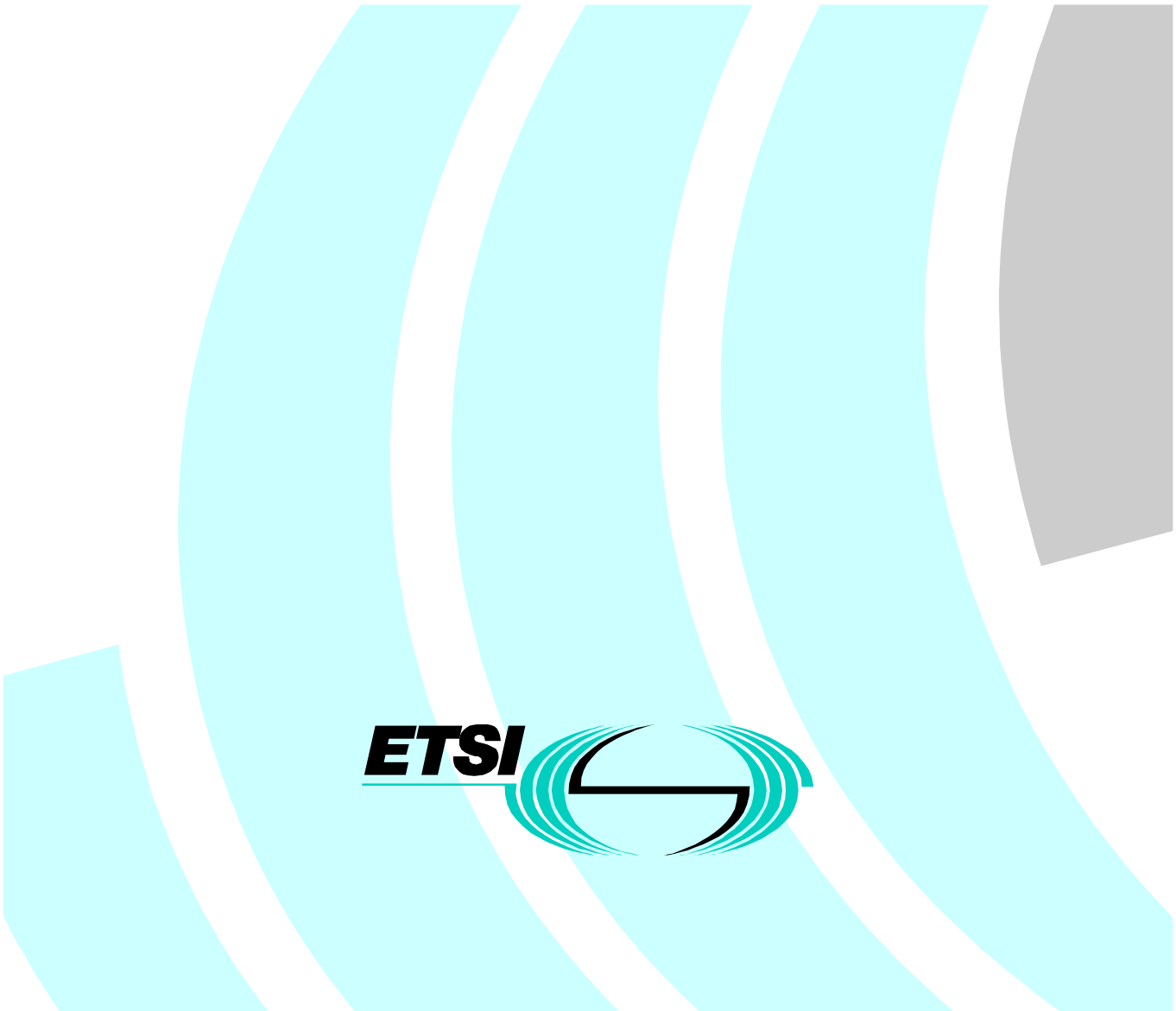
Draft EN 301 040 V2.0.0 (1998-07)

European Standard (Telecommunications series)

Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface



Reference
DEN/TETRA-06027-1 (9mo01000.PDF)

Keywords
TETRA, security, voice, data

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet
secretariat@etsi.fr
http://www.etsi.fr
http://www.etsi.org

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.fr/ipr or http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (EN) has been produced by ETSI Project Terrestrial Trunked Radio (TETRA), and is now submitted for the Public Enquiry phase of the ETSI standards Two-step Approval Procedure.

Due to incorporation of considerate new technical content the present document is submitted for a second Public Enquiry.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

1 Scope

The present document describes the implementation of a Lawful Interception interface in a TETRA system. It provides the requirements and specification of the interface within a TETRA system for the purpose of providing data to Law Enforcement Agencies (LEAs) in the area of Lawful Interception (LI) of communications.

The provision of a Lawful Interception interface for TETRA is a national option, however where it is provided it shall be provided as described in the present document.

The structure of lawful interception in telecommunications is in two parts: The internal interface of a network that is built using a particular technology; and, the external interface (known as the Handover Interface) that links the LEA to the network. Between these two parts may lie a mediation function to cater for national variances and delivery of the result of interception.

The Handover Interface may be the subject of national regulation and therefore the mediation function may be a matter of national regulation.

The subject of the present document is the internal LI interface that lies between the TETRA infrastructure and the mediation function.

The present document describes the data content of information flows from the TETRA system to the mediation function. It does not describe a communications protocol stack but assumes the use of one with entry made at layer 7 (application layer). The EN has been written with ROSE as a target layer 7 protocol and with the ASN.1 Basic Encoding Rules (BER) as the target layer 6 (presentation) protocol. To facilitate this the data definitions are made with ASN.1. This method allows configuration of either local or remote mediation functions. The EN does not specify how ROSE and BER are used.

The present document is structured as follows:

- clause 4 outlines the essential requirements for the TETRA LI interface;
- clause 5 presents the structural and behavioural models of the LI interface;
- clause 6 presents the data model and allocation behaviour in the LI interface.

The present document applies to TETRA services where access to the communication of TETRA Subscriber Identities (TSIs) is available in a network (Switching and Management Infrastructure (SwMI) or Radio Packet Data Infrastructure (RPDI)). Whilst this does not prohibit lawful interception of TETRA Direct Mode Operation (DMO) it removes the liability of network operators and service providers to provide a result of interception when communication does not make use of their networks.

The present document describes the normal and exceptional operation in each of the three operational phases of T-LI:

1 Setup

   The actions taken within the TETRA network to establish the monitoring of a target and the communications paths to the mediation function.

2 Monitoring

   The monitoring of target activity and its delivery to the mediation function.

3 Cleardown

   The removal of a monitor facility against a target and the cleardown of the communications paths to the mediation function.

The present document does not describe the means of transporting data from the TETRA network to the LEA, but describes only the means of capturing and encoding the activities of a target within the TETRA network and delivering this data to the mediation function.

The present document does not define the operations or technical requirements of the Handover Interface that takes data from the mediation function to the LEMF.

The present document does not define the operations or technical requirements of the Law Enforcement Monitoring Facility (LEMF).

NOTE 1: The present document presupposes some familiarity with the operation of TETRA systems and of lawful interception.

NOTE 2: The present document suggests a barrier to external manipulation of the TETRA infrastructure by means of a mediation function.

NOTE 3: No testpoint is provided in the present document to ensure conformance. This is addressed national standards pending the completion of a common handover interface being developed by ETSI TC SEC-LI under work item DES/SEC-003003 and to which the present document is provided as input.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, subsequent revisions do apply.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] Official Journal of the European Communities, 99/C329/01: "Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications".

[2] ETR 331: "Security Techniques Advisory Group (STAG); Definition of user requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies".

[3] ETS 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".

[4] ETS 300 392-2: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following definitions apply:

call: Any connection (fixed or temporary) capable of transferring information between two or more users of a telecommunication system where at least one of the parties to the call(for the purposes of the present document) is a user of a TETRA system.

content of communication: The information exchanged between two or more users of a telecommunications service where at least one of the users is accessing the service in a TETRA network whilst a call is established, excluding intercept related information. This includes information which may, as part of some TETRA service, be stored by one user for subsequent retrieval by another.

NOTE 1: The user in the above definition may be any addressable entity in the TETRA domain using either a TSI [3] or some other valid network address (undefined).

Coordinated Universal Time (UTC): The time scale maintained by the Bureau Internationale de l'Heure (International Time Bureau) that forms the basis of a coordinated dissemination of standard frequencies and time signals.

NOTE 2: The source of this definition is Recommendation 460-2 of the Consultative Committee on International Radio (CCIR). CCIR has also defined the acronym for Coordinated Universal Time as UTC.

co-target: The correspondent of the target (i.e. the individual or group address with whom the target is communicating).

identity: A technical label which may represent the origin or destination of any TETRA traffic, as a rule clearly identified by a physical communication identity number (such as a telephone number) or the logical or virtual communication identity number (such as a personal number) which the subscriber can assign to a physical access on a case-by-case basis.

intercept related information: A collection of information or data associated with TETRA services involving the target, specifically call associated information or data, service associated information or data (e.g. service profile management by subscriber) and location information.

Interception (OR Lawful Interception): The action (based on the law), performed by a network operator/service provider, of making available certain information and providing that information to an LEMF.

NOTE 3: In the present document the term interception is not used to describe the action of observing communications by an LEA.

interception interface: The physical and logical locations within the network operator's/service provider's TETRA facilities where access to the content of communication and intercept related information is provided. The interception interface is not necessarily a single, fixed point.

interception measure: A technical measure which facilitates the interception of TETRA traffic pursuant to the relevant national laws and regulations.

interception subject: A person or persons, specified in a lawful authorization, whose communications are to be intercepted.

Law Enforcement Agency (LEA): A organization authorized by a lawful authorization based on a national law to receive the results of communication interceptions.

Law Enforcement Monitoring Facility (LEMF): A law enforcement facility designated as the transmission destination for the results of interception relating to a particular interception subject.

lawful authorization: Permission granted to an LEA under certain conditions to intercept specified communication and requiring co-operation from a network operator/service provider. Typically this refers to a warrant or order issued by a lawfully authorized body.

LI interface: A physical and logical interface across which the results of interception are delivered from a network operator/service provider to a LEMF.

NOTE 4: In ETR 331 [2] this interface is termed the handover interface. The term handover is used in TETRA systems to describe the maintenance of a call when the mobile party moves between cells.

location information: Information relating to the geographic, physical or logical location of an identity relating to an interception subject.

mediation function: The function that lies between the LEA and the TETRA SwMI that translates data from the SwMI for use by the collection function of the LEA. The mediation function may be resident in the TETRA SwMI and is specified by the protocols and data on the interface to the TETRA SwMI (as defined in the present document) and to the collection function (as defined by the LEA).

multi-user gateway: A reserved address given to a gateway port that is used only for intermediate call support, e.g. ISDN gateway.

Private Mobile Radio (PMR): A radio system designed for a closed user group.

Public Access Mobile Radio (PAMR): A radio system available to members of the general public generally by subscription. The owner and operator are unlikely to be the same as the user.

Public Network Operator (PNO): The operator of a public infrastructure which permits the conveyance of signals between defined network termination points by wire, by microwave, by optical means or by other electromagnetic means.

Quality of Service (QoS): The quality specification of a TETRA channel, system, virtual channel, computer-TETRA session, etc. Quality of service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate or call blocking probability.

reliability: The probability that a system or service will perform in a satisfactory manner for a given period of time when used under specific operating conditions.

result of interception: Information relating to a target service, including the content of communication and intercept related information, which is passed by a network operator or service provider to an LEA. Intercept related information may be provided whether or not call activity is taking place.

served user: The user receiving the intercepted traffic.

service provider: The natural or legal person providing one or more public communication services whose provision consists wholly or partly in the transmission and routing of signals on a network. A service provider need not necessarily run his own network.

NOTE 5: To avoid confusion the term TETRA service provider may be used to distinguish the operator of a TETRA system from the service provider in traditional public networks.

target: The identity associated with a target service (see below) used by the interception subject.

Target Group TETRA Subscriber Identity (GTSI): The identity associated with a target service (see below) used by the interception subject where the interception subject is a group.

target service: A communication service associated with an interception subject and usually specified in a lawful author**iza**tion for interception.

NOTE 6: There may be more than one target service associated with a single interception subject.

Target Terminal Equipment Identity (TEI): The identity associated with a target service (see above) used by the interception subject where the interception target is an equipment.

telecommunication: Any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ASSI	Assigned Short Subscriber Identity
BS	Base Station
CCIR	Consultative Committee on International Radio
CGI	Cell Global Identification
CONS	Connection Oriented Network Service
DMO	Direct Mode Operation
EN	European Norm
GTSI	Group TETRA Subscriber Identity
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISI	Inter-System Interface
ITSI	Individual TETRA Subscriber Identity
LA	Location Area
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LII	Lawful Interception Interface
MNI	Mobile Network Identity

MS	Mobile Station
PAMR	Public Access Mobile Radio
PISN	Public Integrated Services Network
PMR	Private Mobile Radio
PNO	Public Network Operator
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RPDI	Radio Packet Data Infrastructure
SCLNS	Specific ConnectionLess Network Service
SDL	Service and Description Language
SS	Supplementary Service
SSI	Short Subscriber Identity
SwMI	Switching and Management Infrastructure
TEI	TETRA Equipment Identity
TS	Technical Specification
TSI	TETRA Subscriber Identity
TETRA	Terrestrial Trunked Radio
UTC	Coordinated Universal Time
VC	Virtual Circuit

4 User (LEA) requirements - the administrative interface

This clause presents the user requirements derived from [1] and specifically related to the lawful interception of TETRA with the LEA being the user.

The network operator/service provider shall use best endeavours at all times to comply with the requirements of the LEA. The specific information to be made available shall be made clear by the LEA.

The present document describes the internal LI interface of a TETRA network, and does not specify the means by which data is delivered to the LEA or to its designated Law Enforcement Monitoring Facility (LEMF). However the internal LI interface is defined in such a way that data may be carried transparently on most networks.

NOTE: In this context "internal" means within the boundary of the TETRA infrastructure. The boundary may extend in such a manner that the TETRA LI function is remote from other components of the SwMI, or it may be co-located with other SwMI components.

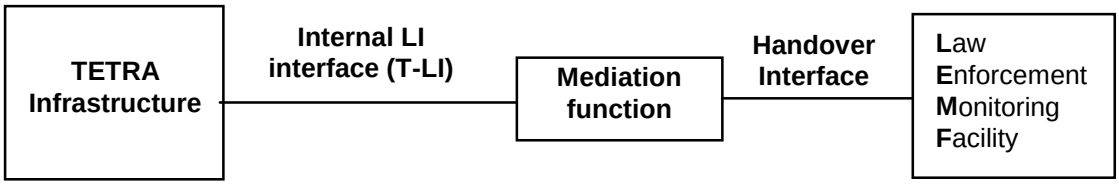


Figure 1: General reference model of lawful interception from user perspective

The general reference model of figure 1 shows that the overall LI interface lies between the LEMF and the TETRA infrastructure. The subject of the present document is the internal LI interface that lies between the TETRA infrastructure and the mediation function.

4.1 Non-disclosure

The network operator/service provider and the LEA should jointly agree confidentiality on the manner in which interception measures are implemented in a given TETRA installation with the manufacturers of the technical installations for the implementation of interception measures.

Information relating to target identities and target services to which interception is being applied at any time in the life of the TETRA installation and as defined thereafter by the LEA should not be made available to unauthorized persons.

4.2 Identification of the identity to be intercepted

The target may be any valid TETRA Subscriber Address (TSI). If the TSI is used for group communication it shall be referred to as a Group TSI (GTSI), if used for an individual it shall be referred to as an Individual TSI (ITSI). The address space of TETRA is "flat" so there is no reserved address space for either GTSIs or ITSIs. A multi-user gateway should not be allowed to be a target.

If the target is an individual (ITSI) it is possible that the target may belong to one or more groups. Groups of which the target is a member shall be identified as those groups to which the target's ITSI has made a group attachment. The attachment that identifies these groups may be requested by the MS with the target's ITSI, enforced by the SwMI or a permanent attachment; and provision shall be made for interception of communications within groups to which the target's ITSI is attached by any of these means. The group communications should cease being intercepted after such time that the SwMI deems the MS to no longer be attached to the group, e.g. by specific detachment, de-registration etc.

In some instances network addresses (TSIs) may be provided in blocks to user groups (e.g. to fleet operators). The network operator/service provider shall make every effort to identify an unique target identity based upon data present in the original warrant. If the network operator/service provider is unable to map an unique address to the characteristics of the target defined in the interception warrant the LI interface shall not be invoked.

In some instances the target may be a particular equipment identified by its Terminal Equipment Identity (TEI). The network operator/service provider shall use best endeavours to identify a target TSI. This may require the network operator/service provider to invoke the Mobility Management (MM) service and to use the TEI PROVIDE protocol exchange to identify the ITSI using the target equipment. The present document does not impose a mandate for the support in TETRA systems of this protocol. The use of such a service should not break the rules of service transparency given in subclause 4.6.

4.3 Result of interception

4.3.1 Network validity of result of interception

A network operator/service provider shall only provide a result of interception for targets operating in their network irrespective of the target belonging to that network. If an interception target migrates to a second TETRA network there shall be no requirement for the home network operator/service provider to provide a result of interception from the visited network.

4.3.2 Identification of result of interception

The result of interception provided at the LEMF side of the LI interface shall be given a unique identification that shall allow identification of the LEA, the target, network operator/service provider and the warrant reference.

The internal interface shall in addition provide a unique identification to correlate the data to be submitted to the LEMF with the internal interception provision.

4.3.3 Format of result of interception

The network operator/service provider shall, prior to delivery of the result of interception:

1) remove any air interface encryption, scrambling and channel coding;

2) provide the LEA with decrypted material for applications where relevant keys and algorithms are available.

The content of real time communication shall be provided as a verbatim bit stream. In particular no speech transcoding shall be applied (in the TETRA SwMI), and where appropriate TETRA encoded speech shall be provided to the MF.

4.3.4 Content of result of interception

The result of interception shall contain:

- the content of all calls originated by the target;

- the content of all calls addressed to the target;
- the content of multi-party calls in which to the best knowledge of the network operator/service provider the target is participating;
- the content of broadcast calls to a user population of which to the best knowledge of the network operator/service provider the target is a member.

In addition the result of interception shall contain:

1) the identities that have attempted communication with the target, successful or not;
2) the identities that the target has attempted communication with, successful or not;
3) identities used by or associated with the target;
4) details of services used and their associated parameters;
5) those signals emitted by the target invoking additional or modified services;
6) time-stamps for identifying the beginning, end and duration of the connection;
7) actual destination and intermediate directory numbers if call has been diverted;
8) location information;
9) advice of charge for provision of result of interception.

The result of interception shall apply to all call types if, and as long as, to the best knowledge of the network operator/service provider, the target is a participant.

For group calls, the GTSI shall be identified as being used by the ITSI where to the best knowledge of the network operator/service provider the target is a participant in the group. This may be achieved by recording the ATTACH/DETACH GROUP IDENTITY messages that dynamically associate an ITSI to a GTSI, or by defining an ITSI as always attached to a group. If a group requires dynamic attachment and the target has not explicitly attached then there is no association of ITSI to GTSI for that group.

NOTE: For further explanation of this topic see ETS 300 392-2 [4], subclauses 14.5.2 and 16.8.

4.3.5 Auditing of result of interception

In order to prevent, and to trace, misuse of the technical functions integrated in the TETRA installation enabling interception, any activation or application of these functions in relation to a given identity shall be fully recorded, including any activation or application caused by faulty or unauthorized input. The records should cover some or all of the following items:

1) the identity of target;
2) the target service(s) concerned;
3) the LEMF to which the result of interception is routed;
4) an authenticator suitable to identify the operating personnel (including date and time of input);
5) a reference to the lawful authorization.

The network operator/service provider should ensure that the records are tamper-proof and only accessible by authorized individuals in accordance with local laws relating to data privacy.

4.4 Location information

A network operator shall provide to the best of their knowledge any location information that may be requested by the LEA and addressed within the initiating warrant. Such data should be within the normal operating parameters of the TETRA network and may take one or more of the following forms:

1) the current location area (or base station if available) at which the target is registered;

2) the current line identity associated with a registered target;

3) the line or service identity to which the target is currently registered and to which calls are redirected.

The location information should be delivered at one or more of the following times:

1) with registration;

2) with result of interception;

3) as specified by the LEMF.

4.5 Time constraints

The result of interception shall be made available during the period specified by the interception warrant, at the LEMF side of the LI interface.

A network operator shall provide data for new calls from the time commencing no earlier than the time at which the interception request is received.

The instance of the LI interface and communication shall be established to the LEMF as quickly as possible after issue of an interception warrant. Thereafter the result of interception shall be delivered to the LI interface on a real-time or near real-time basis.

4.6 Service transparency

The LI interface shall be implemented and operated with due consideration for the following:

1) unauthorized persons should not be able to detect any change from the un-intercepted state;

2) communicating parties should not be able to detect any change from the un-intercepted state;

3) the perceived operating facilities of any network service should not be altered as a result of any interception measure;

4) the perceived quality of service of any network service should not be altered as a result of any interception measure.

4.7 LI interface instances

Each instance of the LI interface shall support the transmission of result of interception related to a single target. If an LEA requires a TETRA network to provide multiple result of interceptions to one or more LEMFs these shall be delivered from separate instances of the LI interface. The preceding may be achieved by using separate physical communication channels for each product or by multiplexing many result of interceptions onto a single physical communication channel. The correlation between the content of communication and intercept related information shall be unique.

4.8 LI interface events

The LEMF shall be informed by the TETRA network through the LI interface of the following events:

1) the activation of an intercept measure;

2) the deactivation of the intercept measure;

3) any change of the intercept measure;

4) the temporary unavailability of the intercept measure.

The LI interface shall be active for the period of the warrant. At the expiry of the warrant the LI interface shall remain active until all result of interception relating to the target has been delivered. Such data may include an advice of charge from the network operator/service provider indicating the sum of resources used in providing the result of interception.

5 Description of internal TETRA LI interface

The TETRA LI interface does not describe a communications protocol or interface, rather it defines a means of interpreting data and actions within a TETRA SwMI/RPDI for supply to the mediation function.

The functional and behavioural model is described using SDL and is shown in this clause. The detail data definitions and assignments are given in clause 6.

5.1 Functional model

The functional model is developed from the reference model provided in clause 4 of the present document.

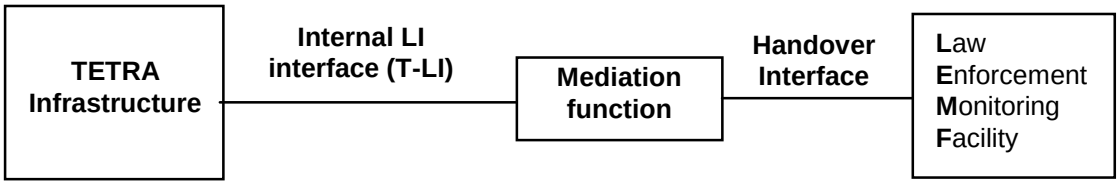


Figure 2: Reference model of interception

The present document only considers the roles of the TETRA Infrastructure and the TETRA side of the mediation function.

In order to better describe the behaviour of the internal LI function subclause 5.2 describes the sequence of information flows across the internal LI interface.

5.2 Information flow sequences

5.2.1 LEA control interactions and information flows

Figure 3 shows the stimuli from the LEA and the responses from the SwMI that are translated by the mediation function.

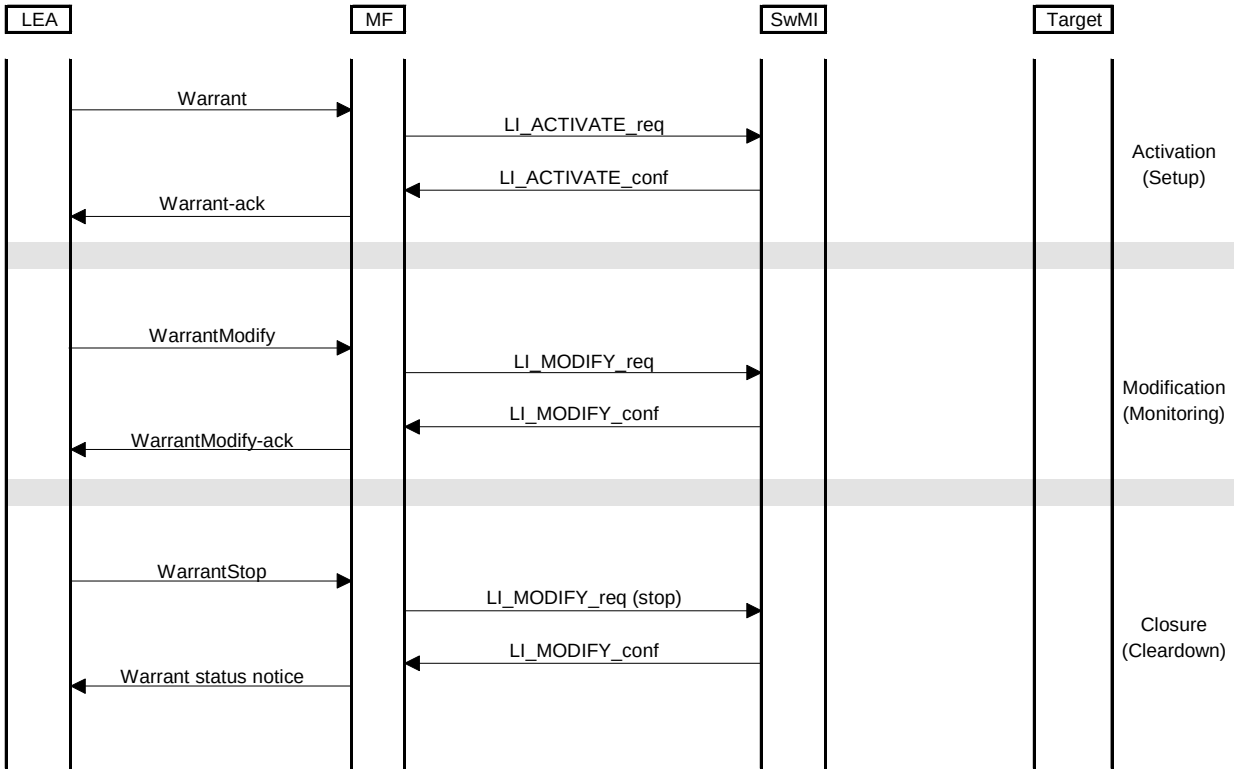


Figure 3: External stimuli and information flow sequences for TETRA LI

The LI_ACTIVATE_req information flow shall contain sufficient data to allow the SwMI to validate the request and to make the required target activity data available to the MF. The returned information flow (LI_ACTIVATE_conf) shall contain an unique identifier for the interception applied within the network. Any subsequent information flows (LI_MODIFY_req/conf) shall refer to this unique identifier. No protocol timers are defined in the present document for the req/conf exchanges but the requirements stated in subclause 4.5 shall apply.

The information flows that initiate or modify the interception are described as ASN.1 data structures as shown in subclauses 5.2.1.1 through to 5.2.1.5. The ASN.1 definitions given below are collated in annex E.

NOTE: The information flows assume the use of a signalling protocol for an automatic T1 interface. The related external interface (HI1 from DES/SEC-003003) may be manual.

5.2.1.1 LI_ACTIVATE_req

This information flow is sent from the MF to the SwMI to request redirection of traffic (in T_TRAFFIC_ind and CT_TRAFFIC_ind information flows) and signalling (in TARGET_ACTIVITY_MONITOR_ind and TARGET_COMMS_MONITOR_ind information flows).

```
LI_ACTIVATE_req ::= SEQUENCE
{
    TimeStamp              UTCTime,
    InvokeId               INTEGER,
    Target_Address         AddressType,
    ExpiryDateTime         UTCTime,
    Target_name            VisibleString      OPTIONAL,
    Additional_target_data VisibleString      OPTIONAL,
    Monitor_Service_List   SEQUENCE of ActivityType DEFAULT {AllServices}
};
```

Protocol constraints:

Response to = None

Response expected = LI_ACTIVATE_conf

5.2.1.2 LI_ACTIVATE_conf

If the request is successful the Result element of the information flow shall be set to TRUE and the TLIInstanceid set. The TLIInstanceid shall thereafter be used as the TETRA specific pointer to the interception. If the request is unsuccessful the Result element shall be set to FALSE and the TLIInstanceid shall not be returned. (I.e. the presence of the TLIInstanceid is conditional on the value of Result).

```
LI_ACTIVATE_conf ::= SEQUENCE
{
    TimeStamp           UTCTime,
    InvokeId            INTEGER,
    Result              BOOLEAN,
    TLIInstanceid       TLIIdType       OPTIONAL   -- Conditional on value of Result --
};
```

Protocol constraints:

Response to = LI_ACTIVATE_req

Response expected = None

5.2.1.3 LI_MODIFY_req

An interception may be modified many times in its life. Each modification is addressed using the reference identity (TLIInstanceid) and a sequential ModificationNumber. The modification may be one of a selection as shown below.

```
LI_MODIFY_req ::= SEQUENCE
{
    TLIInstanceid           TLIIdType,
    Timestamp               UTCTime,
    ModificationNumber      Integer,
    ModificationType        CHOICE
    {
        Halt                    BOOLEAN,
        Reset                   BOOLEAN,
        ExpiryDateTime          UTCTime,
        Target_name             VisibleString,
        Additional_target_data  VisibleString,
        Monitor_Service_List    SEQUENCE of ActivityType
    }
};
```

Protocol constraints:

Response to = None

Response expected = LI_MODIFY_conf

5.2.1.4 LI_MODIFY_conf

If the modification request is successful then Result shall be set to TRUE, else it shall be set to FALSE.

```
LI_MODIFY_conf ::= SEQUENCE
{
    TLIInstanceid           TLIIdType,
    Timestamp               UTCTime,
    ModificationNumber      Integer,
    Result                  BOOLEAN
};
```

Protocol constraints:

Response to = LI_MODIFY_req

Response expected = None

5.2.1.5 LI_STATUS_ind

This information flow from the SwMI to the MF reports changes in the status of the SwMI. This may indicate for example problems in the ability to provide interception.

```
LI_STATUS_ind ::= SEQUENCE
{
   TLIInstanceid          TLIIdType,
   Timestamp              UTCTime,
   TETRA_Sys_Status       StatusType
};
```

Protocol constraints:

Response to = None

Response expected = None

5.2.2 Target traffic interactions and information flows

Figure 4 shows an example of the transmission of traffic from the target using a TETRA Air Interface (AI) connection to the SwMI and undertaking a call. The principle captured applies to all target activity such as registration.

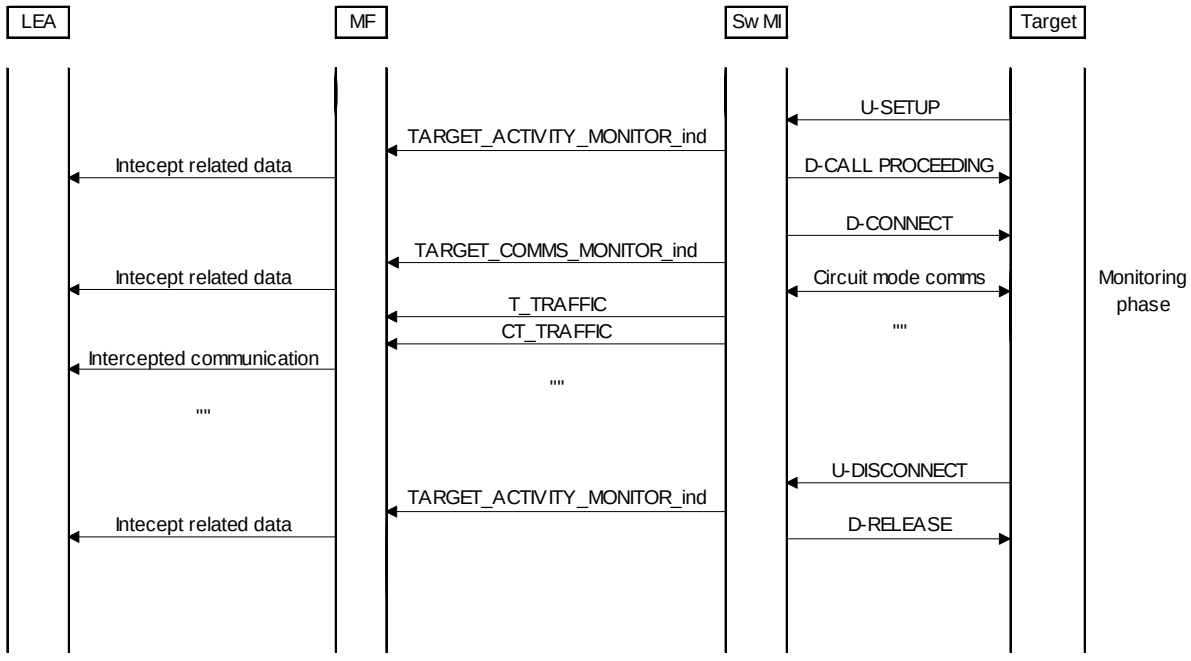


Figure 4: Example information flow sequence for TETRA LI when target makes and clears a call

The information flows that indicate the activity of the target (signalling or traffic) are described as ASN.1 data structures as shown in subclauses 5.2.2.1 through to 5.2.2.5.

5.2.2.1 TARGET_ACTIVITY_MONITOR_ind

This information flow shall provide in summary form the activity of the target on the SwMI to the MF. It shall have a header section indicating who, when and where, with a body section indicating the what of the target activity.

```
TARGET_ACTIVITY_MONITOR_ind ::= SEQUENCE
{
   TLIInstanceid                TLIIdType,                  -- header, who –
   Timestamp                    UTCTime,                    -- header, when –
   Target_Location              LocationType,               -- header, where –
   TargetAction                 ActivityType,
   Supplementary_Target_address AddressType                 OPTIONAL,
   Co_target_address            SEQUENCE of AddressType     OPTIONAL,
   Co_target_location           SEQUENCE of LocationType    OPTIONAL
};
```

Protocol constraints:

Response to = None

Response expected = None

5.2.2.2 TARGET_COMMS_MONITOR_ind

This information flow is used to indicate the change of target activity from signalling or packet mode data towards circuit mode activity. It identifies the logical location of the T_TRAFFIC_ind and CT_TRAFFIC_ind information flows.

```
TARGET_COMMS_MONITOR_ind ::= SEQUENCE
{
   TLIInstanceid                TLIIdType,
   Timestamp                    UTCTime,
   Target_location              LocationType,
   Supplementary_Target_address AddressType OPTIONAL,
   Target_comms_id              CircuitIdType,
   Co_target_address            SEQUENCE of AddressType OPTIONAL,
   Co_target_comms_id           SEQUENCE of CircuitIdType OPTIONAL
};
```

Protocol constraints:

Response to = None

Response expected = None

5.2.2.3 T_TRAFFIC_ind

This information flow carries a TETRA AI traffic packet of the target to the MF. This applies to circuit mode traffic only.

```
T_TRAFFIC_ind ::= SEQUENCE
{
    TLIInstanceid       TLIIdType,
    TrafficPacket       BitString
}
```

Protocol constraints:

Response to = None

Response expected = None

5.2.2.4 CT_TRAFFIC_ind

This information flow carries a TETRA AI traffic packet of the co-target to the MF. This applies to circuit mode traffic only.

```
CT_TRAFFIC_ind ::= SEQUENCE
{
    TLIInstanceid          TLIIdType,
    TrafficPacket          BitString
}
```

Protocol constraints:

Response to = None

Response expected = None

5.3 Structural model

5.3.1 Block interaction model

Figure 5 shows the structure of TETRA LI. This is modelled as one block representing the internal LI function that communicates to the external world. The external world provides inputs to the system and receives outputs from the system. The sources and sinks may be either the SwMI or the MF.

The model introduces three logical interfaces to the MF:

T1.in/out This is the control element channel. It is used to carry information related to the establishment and modification of the interception measure. It is also used to carry knowledge of the TETRA SwMI status to the MF.

T2 This channel is used to carry intercept related information as contained in the TARGET_ACTIVITY_MONITOR_ind and TARGET_COMMS_MONITOR_ind information flows. Such data includes the carriage of packet mode data.

T3.t/ct This channel pair is used to carry the result of interception for circuit mode traffic. The signal format is used to maintain the packet structure of the TETRA speech or data.

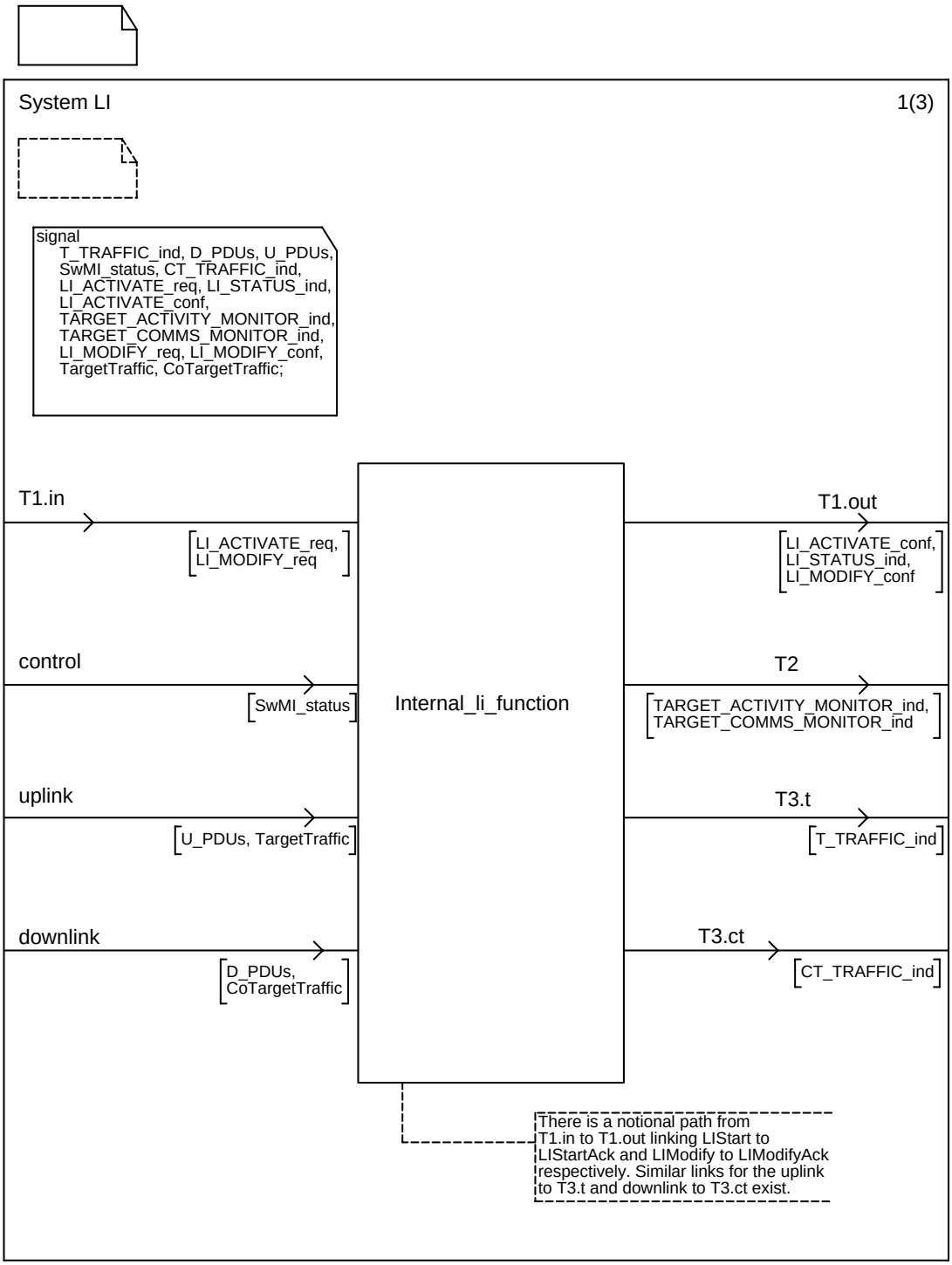


Figure 5: SDL block interaction diagram for T-LI

5.3.2 Process interaction model

The block interaction model described in 5.3.1 is broken down to consider in more detail the structure within the block. Figure 6 shows the block internal_LI_function broken down into 4 discrete processes:

Control:

Receives LI_ACTIVATE_req. Determines if target is valid. Returns unique identifier in LI_ACTIVATE_conf for valid targets and set a timer for the session. Distributes unique identifier to other processes in the block in the signal Instance in order to initiate these processes. Receives LI_MODIFY_req to allow modification of the original request and confirms the implementation of these requests in the LI_MODIFY_conf. Reports statsu to the MF using the LI_STATUS_ind flow which is generated in response to data received from the SwMI_Monitor process.

Target_Monitor:

Receives notification of U_PDUs (from target) and D_PDUs (to target) and system level data from SwMI. Packages and these in TARGET_ACTIVITY_MONITOR_ind flows (data structures). On creation of speech or other circuit mode calls this process uses the signal Switch to start the Comms_provision process and informs the MF using the TARGET_COMMS_MONITOR_ind flow.

Comms_provision:

This process controls the establishment of the T3 links to the mediation function on the receipt of command "Switch" from the Target_Monitor process. Provides the traffic to the MF using the C/CT_TRAFFIC_ind flows.

SwMI_Monitor:

Monitors SwMI and reports SwMI condition for the current intercept to the Control process.

There may be one or many instance of each process depending upon implementation. For single instances of each process where there are many intercepts the internal management of each process should be able to manage each target independently.

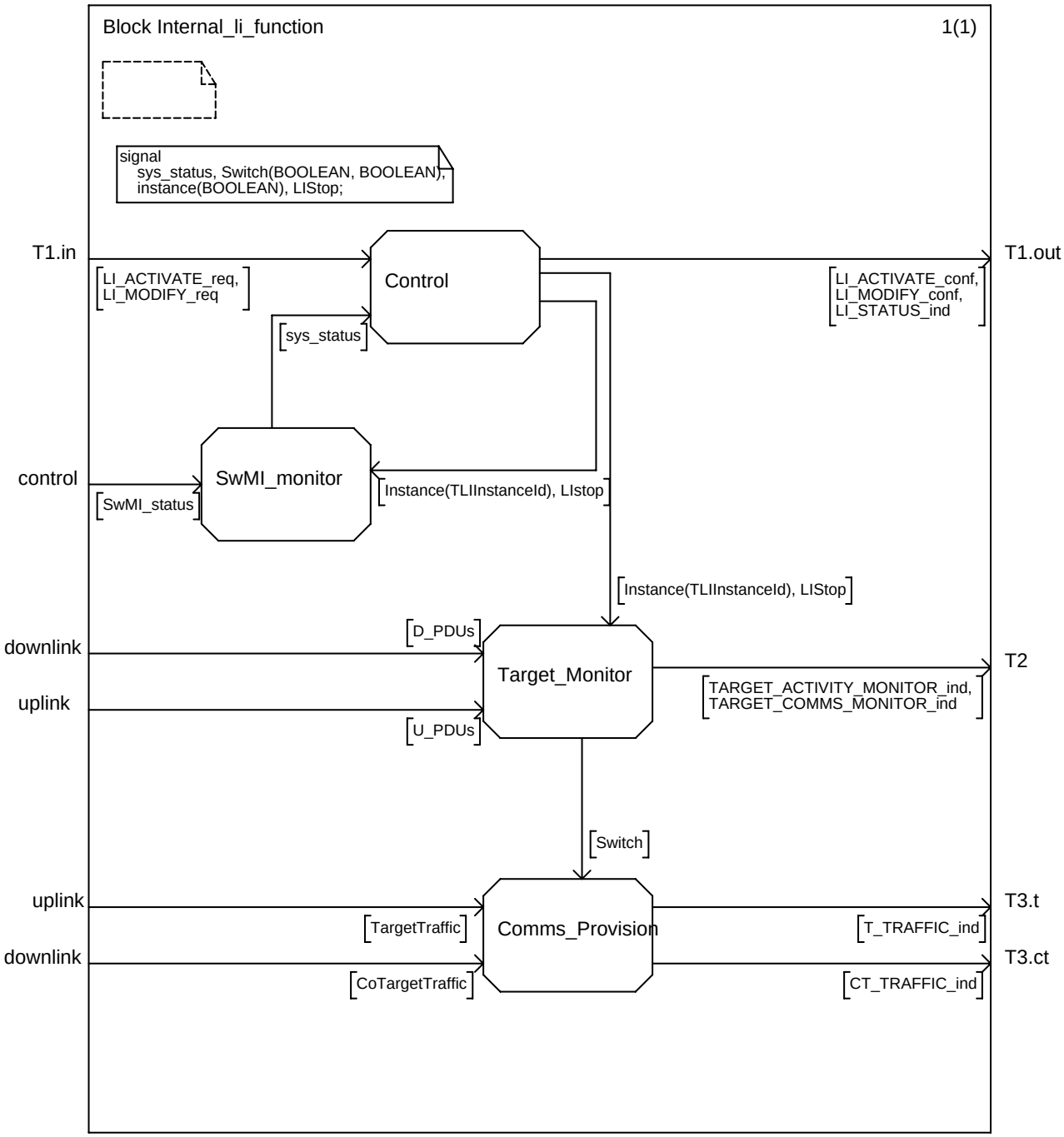


Figure 6: SDL breakdown of Internal LI function block

6 Data provision and encoding

In addition to the data identified in the following subclauses the SwMI may need to provide additional audit data (see subclause 4.3.5). The detail definition and provision of such data is outside the scope of the present document.

6.1 Identification of result of interception

The result of interception provided at the LEMF side of the LI interface shall be given a unique tag that shall allow identification of the LEA, the target, network operator/service provider and the warrant reference. This tag shall be first returned in the LI_ACTIVATE_conf information flow and form part of the subsequent header data in TARGET_ACTIVITY_MONITOR_ind and TARGET_COMMS_MONITOR_ind information flows, as well as being used in the LI_MODIFY and LI_STOP information flows.

TLIIdType ::= INTEGER(0 .. 65535) -- 16 bits –

6.2 Provision of identities

All identities used by the target or co-target in communication, successful or unsuccessful, shall be identified using the AddressType data element defined below.

```
AddressType ::= SEQUENCE
{
    TSI     TSIType,
    SEQUENCE of SupplementaryAddress     CHOICE
    {
        TETRAaddress    TSIType,
        PISNaddress     PISNType,
        IP4address      INTEGER (0 .. 2^32-1),    -- 32 bits –
        IP6address      INTEGER (0 .. 2^64-1),    -- 64 bits –
        E164address     BitString,
        X121address     BitString,
        TEI             TEIType
    } OPTIONAL
}
```

The (co) target may use many identities for communication. All addresses used shall be bound to the (co) target TSI that forms the principal monitoring key.

Examples of supplementary identities to the (I)TSI include:

- Alias Short Subscriber Identity (ASSI) (assigned by the hosting network);
- Group TSI (each ITSI may be associated with several groups);
- IP address (used for IP service);
- PISN address (used for calls to PTSN/ISDN gateways);
- TETRA Equipment Identity (TEI).

If the (co) target is to be identified by means of the TEI the SwMI shall support the TEI_PROVIDE exchange described in ETS 300 392-7 clause 4.

6.2.1 Target

The address used by the SwMI in communicating with the target shall be provided in the Supplementary_Target_address element of the TARGET_ACTIVITY_MONITOR_ind information flow.

When an ITSI attaches to the group using the ATTACH DETACH GROUP IDENTITY request primitive this group identity shall be indicated in the Supplementary_Target_address element of the TARGET_ACTIVITY_MONITOR_ind information flow.

6.2.2 Co-target

The identity of co-targets shall be given in the Co_target_address information element of the TARGET_ACTIVITY_MONITOR_ind information flow. In instances where several co-targets can be identified the element shall be repeated within an array.

6.3 Provision of details of services used and their associated parameters

The activity of the target shall be given in the TargetAction element of the TARGET_ACTIVITY_MONITOR_ind.. The TargetAction element shall be of type ActivityType defined below.

```
ActivityType::= SEQUENCE
{
    Activity          ActivityClassType,
    CallRelation      ENUMERATED
                      {
                          Begin,
                          End,
                          Continue,
                          Report
                      },
    Direction         ENUMERATED
                      {
                          ToTarget,
                          FromTarget
                      } OPTIONAL,
    Scope             ENUMERATED
                      {
                          Point2Point,
                          Point2MultiPoint,
                          Broadcast
                      } OPTIONAL,
    C_PlaneData       BitString  OPTIONAL,
    SS_type           SSType     OPTIONAL
}
```

6.3.1 Circuit mode services (U-plane)

For circuit mode services the TARGET_ACTIVITY_MONITOR_ind information flow shall indicate the direction of the call (to- or from- target). It shall also indicate whether the call is initiated as point-to-point or as point-to-multipoint.

The ActivityType!Activity element shall be set to one of:

TETRASpeech

SingleSlotData24

SingleSlotData48

SingleSlotData72

MultiSlotData2_24

MultiSlotData2_48

MultiSlotData2_72

MultiSlotData3_24

MultiSlotData3_48

MultiSlotData3_72

MultiSlotData4_24

MultiSlotData4_48

MultiSlotData4_72

The sub-elements Direction and Scope shall be provided.

6.3.2 Data services (C-plane)

6.3.2.1 Short data (unacknowledged)

The short data services comes in a number of variants. In the encoded variants the translation of message identity to textual message may not be known to the SwMI.

The ActivityType!Activity element shall be set to one of:

SDSType1

SDSType2

SDSType3

SDSType4

Status

The ActivityType!Scope and ActivityType!Directon elements shall be set accordingly. Finally the ActivtyType!Data element shall contain the user defined data.

NOTE: The SDS message may be sent to the MF both on entry to the store and on retrieval from the store.

6.3.2.2 Short data (acknowledged)

NOTE: The acknowledged SDS service is described in ETS 300 392-2.

The short data services comes in a number of variants. In the encoded variants the translation of message identity to textual message may not be known to the SwMI.

The ActivityType!Activity element shall be set to one of:

SDS_ACK_Type1

SDS_ACK_Type2

SDS_ACK_Type3

SDS_ACK_Type4

Status_ack

SDS_Acknowledgement_success

SDS_Acknowledgement_fail

The ActivityType!Scope and ActivityType!Directon elements shall be set accordingly. The ActivtyType!Data element shall contain the user defined data.

NOTE 1: The SwMI may store and forward SDS messages so there may be a significant delay between transmission of an SDS_ACK_ event and the receipt of the paired SDS_Acknowledgement_ event.

NOTE 2: The SDS message may be sent to the MF both on entry to the store and on retrieval from the store.

6.3.2.3 Specific Connectionless Network Service (SCLNS)

The SwMI in general will not be able to identify the source and destination applications for packet mode data services. The connectionless packet mode data service shall be indicated as below.

The ActivityType!Activity element shall be set to:

SCLNS_PacketData

The ActivityType!Scope and ActivityType!Direction elements shall be set accordingly. The ActivityType!Data element shall contain the user defined data.

6.3.2.4 Connection Oriented Network Service (CONS)

The CONS service defined in TETRA is a delta to ISO 8348 and ISO 8878. The ActivityType!Activity element shall be set to:

CONS_PacketData

The ActivityType!Scope and ActivityType!Direction elements shall be set accordingly.

The ActivityType!Data element shall contain the user defined data and may be further decoded within the MF to identify Virtual Circuit (VC) establishment activities.

6.3.2.5 Internet Protocol

The IP address used by the target shall be provided in the TargetAddress!SupplementaryAddress element of the TARGET_ACTIVITY_MONITOR_ind data structure. Similarly the IP address of the correspondent shall be provided in the co-target address element.

The ActivityType!Activity element shall be set to:

InternetProtocol

The ActivityType!Scope and ActivityType!Directon elements shall be set accordingly. Finally the ActivityType!Data element shall contain the full IP Packet (IP header plus data).

6.4 Provision of those signals emitted by the target invoking additional or modified services

Signals that modify or invoke non-call related services shall be given in the same form as for services described in subclause 6.3 using the TargetAction element of the TARGET_ACTIVITY_MONITOR_ind data structure.

6.4.1 Authentication

Authentication may be invoked at registration or periodically by either the MS or by the SwMI.

NOTE: Mutual authentication is considered as two separate authentications.

The ActivityType!Activity element shall be set to one of:

SwMI_authentication_success

SwMI_authentication_fail

ITSI_authentication_success

ITSI_authentication_fail

6.4.2 OTAR

Cipher keys of type GCK (Group Cipher Key), CCK (Common Cipher Key), and SCK (Static Cipher Key) may be renewed (refreshed) by the SwMI.

The ActivityType!Activity element shall be set to one of:

OTAR_SCK_success

OTAR_SCK_fail

OTAR_GCK_success

OTAR_GCK_fail

OTAR_CCK_success

OTAR_CCK_fail

6.4.3 Enable/Disable

The SwMI may elect to disable a subscription or an equipment during a session. Such an action by the SwMI shall be indicated by setting TargetAction element of the TARGET_ACTIVITY_MONITOR_ind to one of the following:

TARGET_SUSCRIPTION_DISABLED_T

TARGET_EQUIPMENT_DISABLED_T

TARGET_SUSCRIPTION_DISABLED_P

TARGET_EQUIPEMENT_DISABLED_P

TARGET_SUBSCRIPTION_ENABLED

TARGET_EQUIPMENT_ENABLED

NOTE: The _T or _P suffix indicates temporary or permanent disable.

6.4.4 Registration

For a session based system such as TETRA registration is the means by which a target indicates to the system the ability to make and receive calls. Indication of registration is given by setting TargetAction element of the TARGET_ACTIVITY_MONITOR_ind to one of:

Session_registration

Session_deregistration

6.4.5 Migration

This is the act of moving from one SwMI to another. This uses a variant of the registration procedure.

Indication of migration is given by setting TargetAction element of the TARGET_ACTIVITY_MONITOR_ind to MIGRATION. The new location is given in the header field. As a result of a successful migration the target is de-registered from the previous system and its registration moved to the new system. This may result in several related information flows.

6.4.6 Roaming

This is the act of moving within a SwMI from one Location Area (or serving cell) to another. This uses a variant of the registration procedure.

Indication of roaming is given by setting TargetAction element of the TARGET_ACTIVITY_MONITOR_ind to ROAMING. The new location is given in the header field.

6.4.7 Supplementary services

The TETRA system supports a number of supplementary services. The following encoding of the TargetAction element of the TARGET_ACTIVITY_MONITOR_ind information flow shall be applied.

Activity = SupplementaryService

Direction shall be set as appropriate

Scope shall not be set

Data shall not be set

SS_type shall be set as appropriate

6.5 Provision of time-stamps for identifying the beginning, end and duration of the connection

The header of TARGET_ACTIVITY_MONITOR_ind information flow shall contain a mandatory timestamp information element. This element shall be of the type defined below:

UTCTime.

NOTE 1: UTCTime is derived from the Coordinated Universal Time system (see subclause 3.1).

NOTE 2: In ETS 300 392-2 [4], table 254, it is stated that the network time element is zeroed at 00:00 hours on the first of January every year.

NOTE 3: In ETS 300 392-2 [4], table 254, it is stated that the network time element is incremented every 2 seconds.

6.6 Provision of actual destination and intermediate directory numbers if call has been diverted

The address used by the SwMI in communicating with the target shall be provided in the target-address element of the TARGET_ACTIVITY_MONITOR_ind information flow. This shall be differentiated from the target which is to be found by the correlation given in the TLIInstanceId element of this information flow.

6.7 Provision of the U-plane content of the communication from and to the target

The communication from the target shall be provided in its native TETRA format to the mediation function. The communication shall be provided on separate links to the mediation function (one each for target and co-target communications).

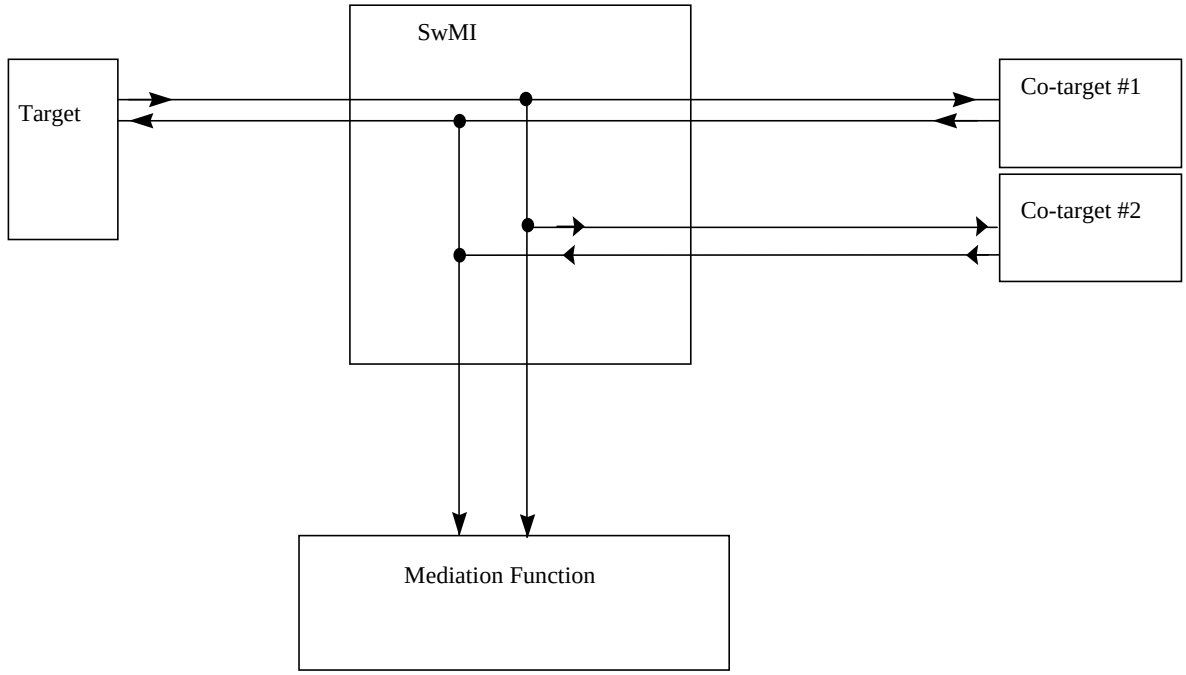


Figure 7: Separate delivery for the interception of target and co-target content

6.8 Provision of location information;

Location information relating to the target should be provided in the header of every TARGET_ACTIVITY_MONITOR_ind information flow. The header element shall specify whether the data provided relates to a mobile TETRA user (MS), or a fixed TETRA user (LS).

The location data shall be provided using the following data construct:

```
LocationType ::= CHOICE
{
    MS_Loc      TETRA_CGIType,
    LS_Loc      TETRA_LS_AddressType
}
```

6.8.1 Mobile users of TETRA

The SwMI shall indicate the location of mobile TETRA users using the TETRA Cell Global Identification (CGI) defined below.

```
TETRA_CGIType ::= SEQUENCE
{
    mcc    MCC_Type,
    mnc    MNC_Type,
    lai    LocationAreaType,
    CI     CellIdType    OPTIONAL
}
```

Where:

```
CellIdType ::=          INTEGER (0 .. 65535)  -- 16 bits –
LocationAreaType ::=    INTEGER (0..16383)    -- 14 bits, as defined in ETS 300 392-2 –
MCC_Type ::=            INTEGER (0..1023)     -- 10 bits, as defined in ETS 300 392-1 –
MNC_Type ::=            INTEGER (0..16383)    -- 14 bits, as defined in ETS 300 392-1 –
```

On initialization of the interception facility part of this structure can be populated with system default values (for mnc and mcc particularly).

The SwMI network management should, in addition, provide an up to date translation of TETRA_CGI to national map co-ordinates. The method of provision is outside the scope of the present document.

6.8.2 Fixed line users of TETRA

Fixed line users shall be identified by the PISN (Private Integrated Services Network) number allocated to their access port to the SwMI.

NOTE: In normal TETRA operation a TETRA LS is addressed by its TSI (normally ITSI), which may in some implementations be mapped to an ISDN or PSTN line connection. If the latter is true then the this address is given in the target-address element of the TARGET_ACTIVITY_MONITOR_ind information flow.

6.9 System status data

Changes in system status shall be made available to the mediation function in the TETRA_Sys_Status element of the LI_STATUS_ind information flow.

```
StatusType ::= ENUMERATED
{
    NetworkFullyAvailable,
    NetworkErrorsAffectingIntercept,
    ReconfigurationInProgress,
    SessionExpired,
    GatewayServicesUnavailable
}
```

Annex A (informative): Explanatory diagrams

These diagrams are intended to be illustrative of the abstractions employed, and are not intended to limit the scope of the present document.

A.1 General network arrangements

The general arrangement for a network which is capable of providing interception facilities is as shown below:

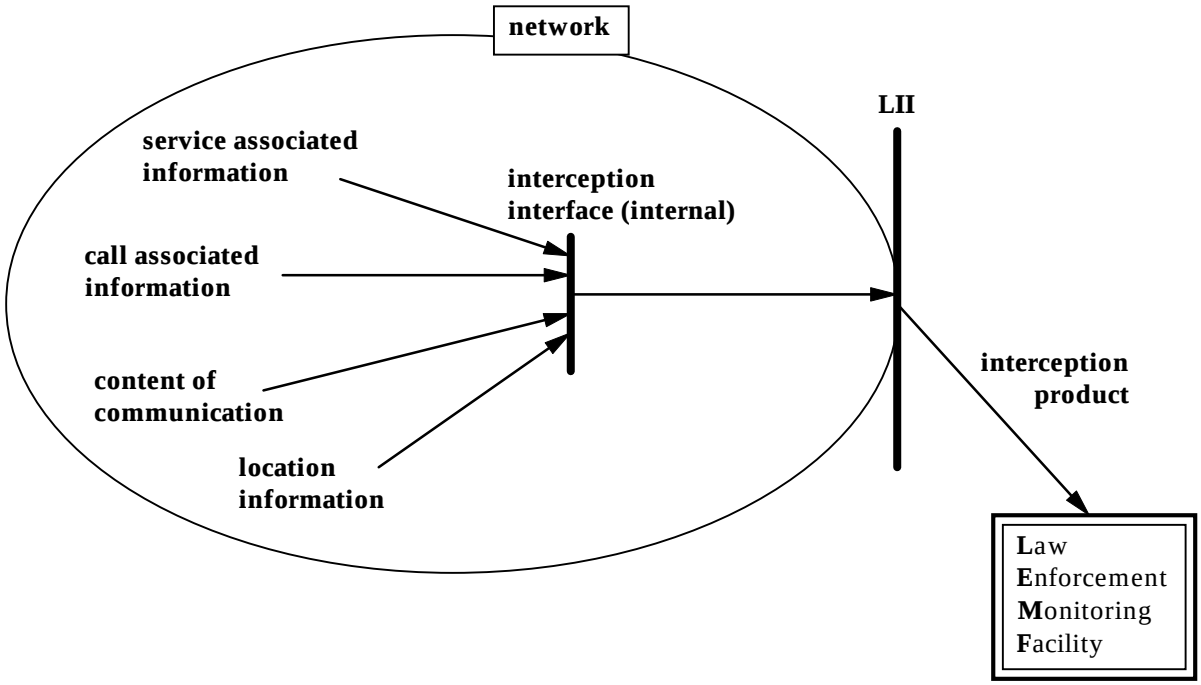


Figure A.1: General network arrangements for interception

Information relating to some target service is collected within the network at an interception interface. This information is then passed to an optional buffer, depending on specific circumstances, and then to a LI interface. From the LI interface information is then passed to the LEMF.

The information collected includes some or all of:

- the content of communication;
- call associated data;
- service associated data;
- location information.

A.2 Service providers

A service provider is an entity which takes advantage of the connectivity offered by a network provider to offer some service which the network's connectivity on its own is otherwise incapable of providing. Depending on circumstance, a service provider may be part of the same organization which operates a network or the service provider may belong to a different organization. The service provider relies on the co-operation of the network operator to deliver their service to their customer. The service provider may also provide some services with the assistance of other service providers.

The services which a service provider may offer are essentially unlimited. Possibilities include:

- voice storage services;
- personal numbers;
- card calling services;
- short data message services;
- data applications;
- dispatching services.

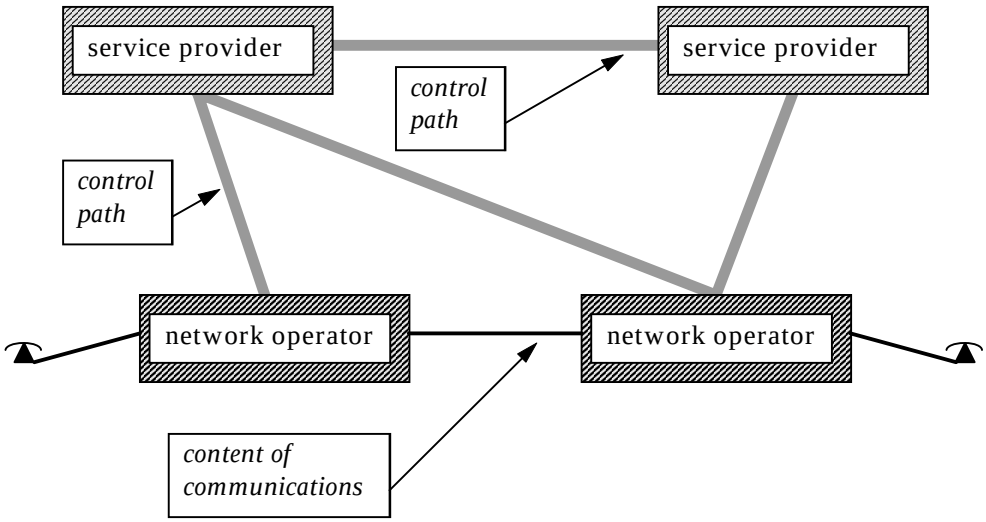


Figure A.2: Service provider relationship to a network operator

Figure A.2 shows that, in general, a service provider has no direct access to the content of communications.

A.3 Service across multiple SwMIs

The following diagram illustrates interception of communication with a Mobile Station (MS) which is registered on its' home SwMI:

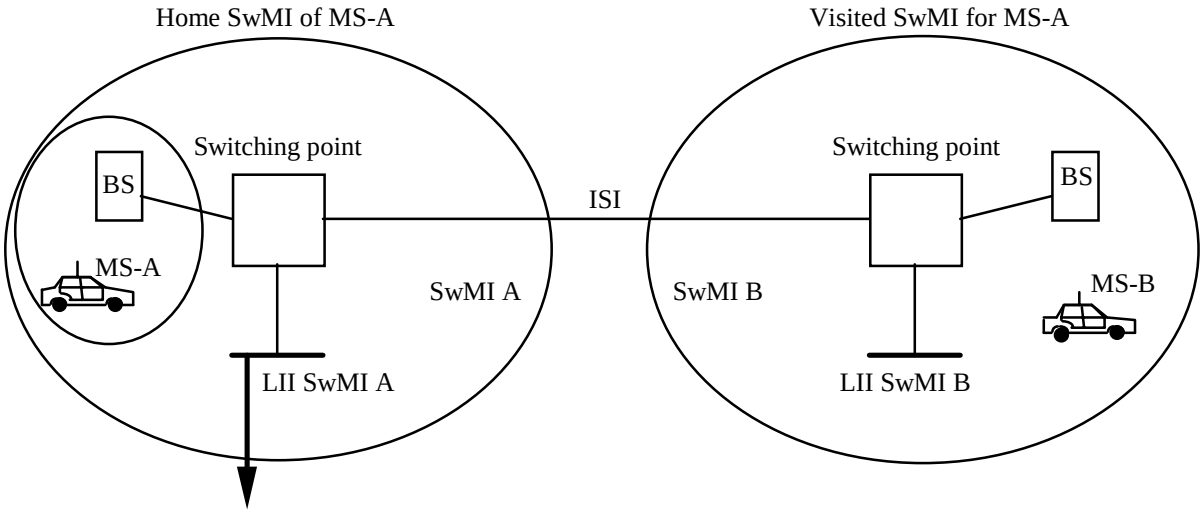


Figure A.3: Service interception with call between 2 SwMIs, target in home SwMI

If the interception target is MS A, the handover interface of SwMI A can provide information on Location Area (LA) A; and that communication is with MS B located in SwMI B; but does not know the LA for MS B. Handover interface of SwMI B is not able to provide interception information as interception target MS A is not registered on SwMI B.

The following diagram illustrates the alternative case, when an MS is registered on a SwMI that is not his home SwMI:

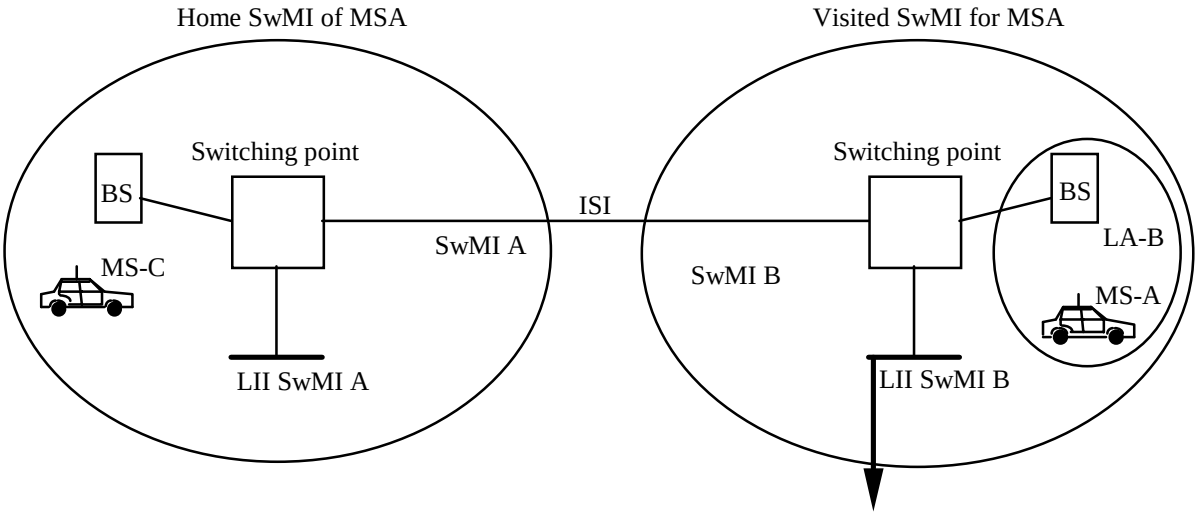


Figure A.4: Service interception with call between 2 SwMIs, target in vSwMI

If the interception target is MS A, now roamed to visited SwMI B, the handover interface of SwMI A can no longer provide information as the MS is out of his home SwMI. The handover interface of SwMI B can provide information on MS A, including the LA B details. If the MS is in communication with MS C, located on MS A's home SwMI, only the interface of SwMI B can provide information concerning MS C, as information can only be associated with the target for interception, MS A.

A.4 Service across international borders

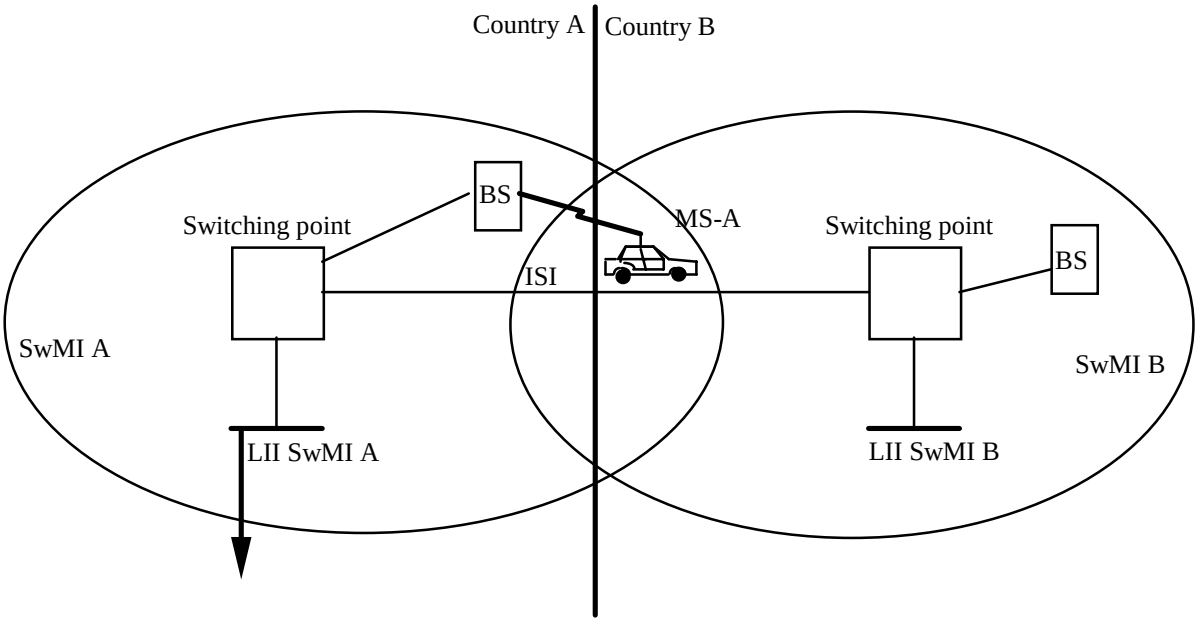


Figure A.5: Service interception in a single SwMI with target on foreign territory

If the interception target MS A is operating from within the borders of country B, but is registered on SwMI A and making use of cross-border coverage, all interception information shall be present at the handover interface of SwMI A, not that of SwMI B.

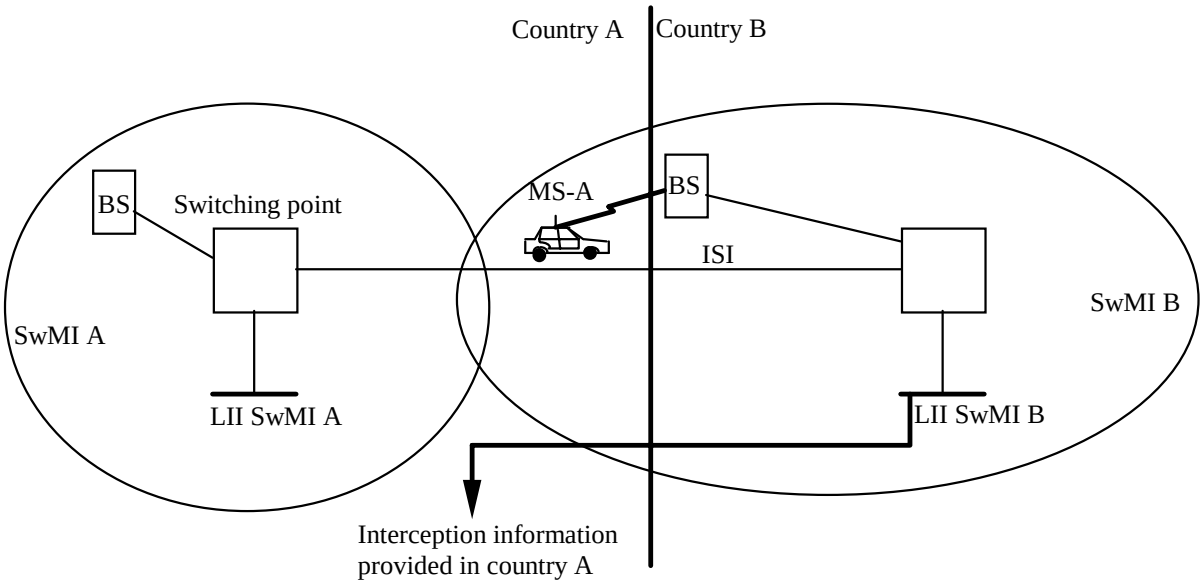


Figure A.6: Service interception in a single SwMI with target and LEMF on foreign territory

If a service provider uses a SwMI based in a foreign country, country B, to provide service across a border into the home country, country A, for geographical coverage or other reasons, he may be required to provide lawful interception information within country A. This shall be achieved by extending the handover interface of the foreign SwMI, SwMI B, into country A.

Annex B (informative): Process behavioural model

This annex provides, by means of SDL diagramming of state transitions, a set of examples of how the protocols described in clause 5 may be further understood.

The behavioural model describes how, within each process, input signals are handled and output signals returned. It also shows the state transition behaviour.

The control process should on successful validation of a request (LI_ACTIVATE_req) initiate the Target_monitor and SwMI_monitor processes.

The Comms_provision process should be initiated by the Target_monitor process on the receipt of any message indicating a switch from C-plane to U-plane.

B.1 Control process

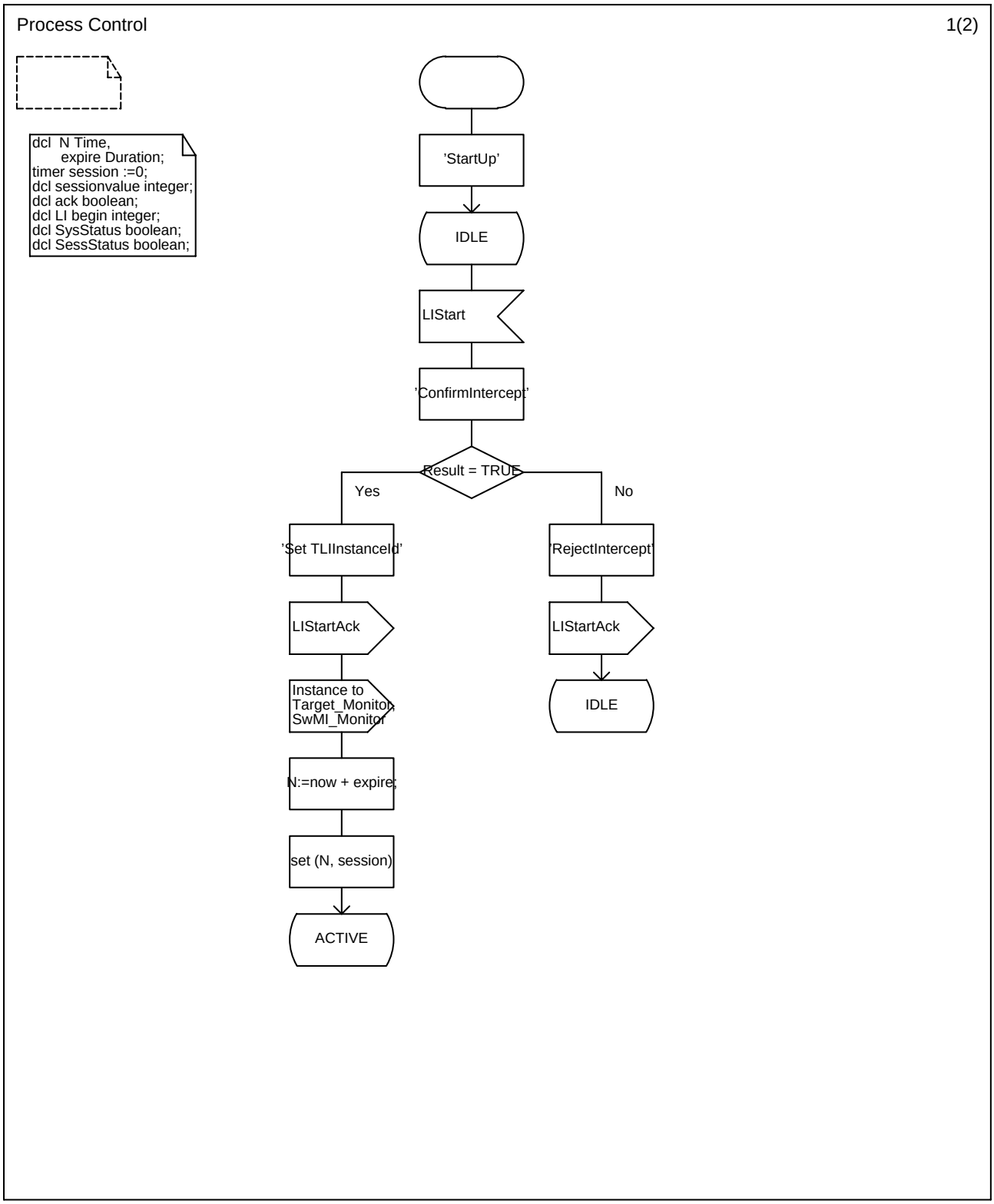


Figure B.1: Behaviour of Control process (page 1 of 2)

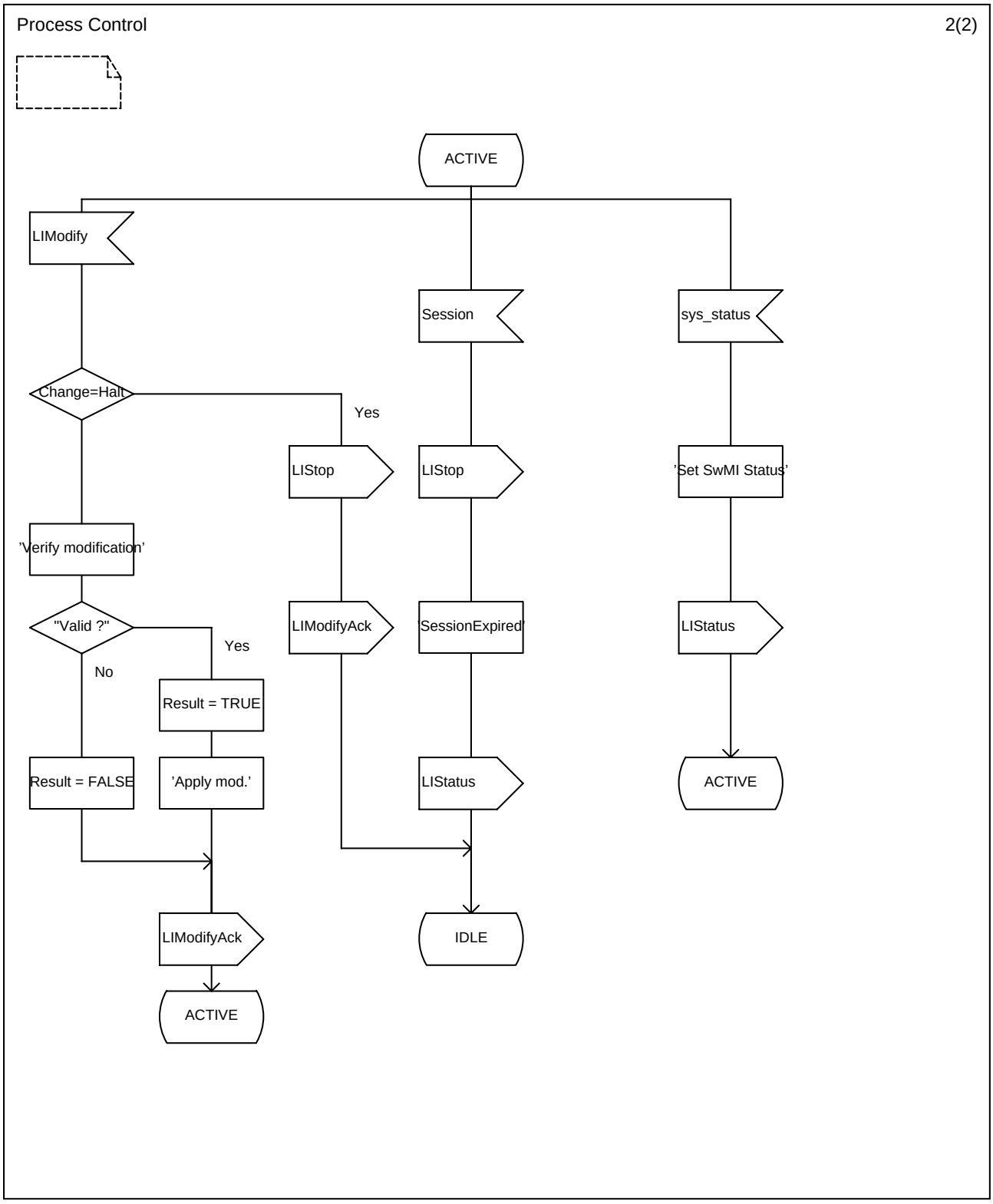


Figure B.2: Behaviour of Control process (page 2 of 2)

The block "ConfirmIntercept" performs the following checks:

For valid target, warrant, service and LEA the TLIInstanceId field in the LI_ACTIVATE_conf data structure is set. If any of the test fails the field is not set. The succeeding check then returns LI_ACTIVATE_conf with a null TLIInstanceid field and T_LI_Status of "Bad" (or invalid warrant) for the failure condition.

B.2 Target_monitor process

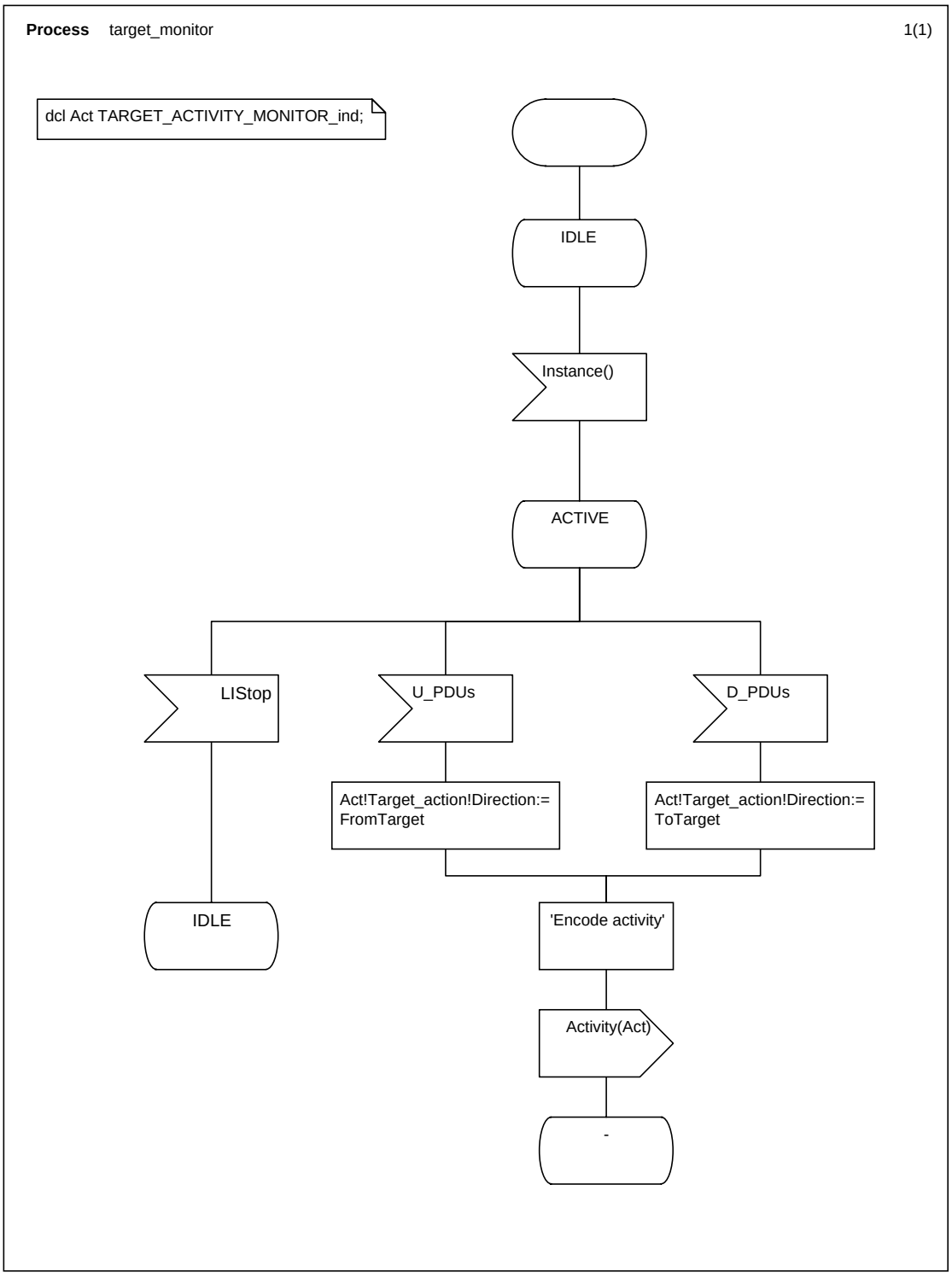


Figure B.3: Behaviour of Target_monitor process

B.3 Comms_provision process

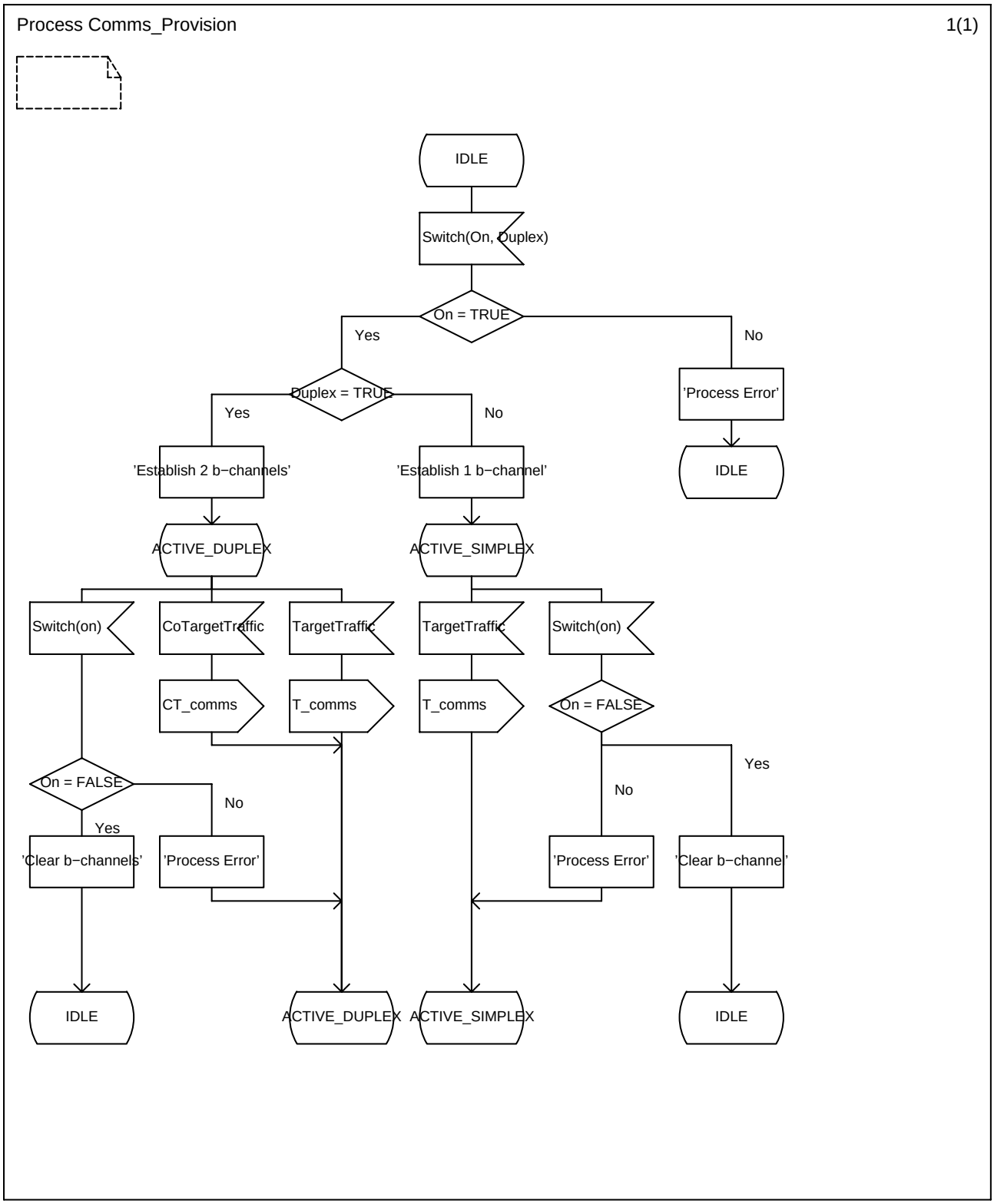


Figure B.4: Behaviour of Comms_provision process

B.4 SwMI_monitor process

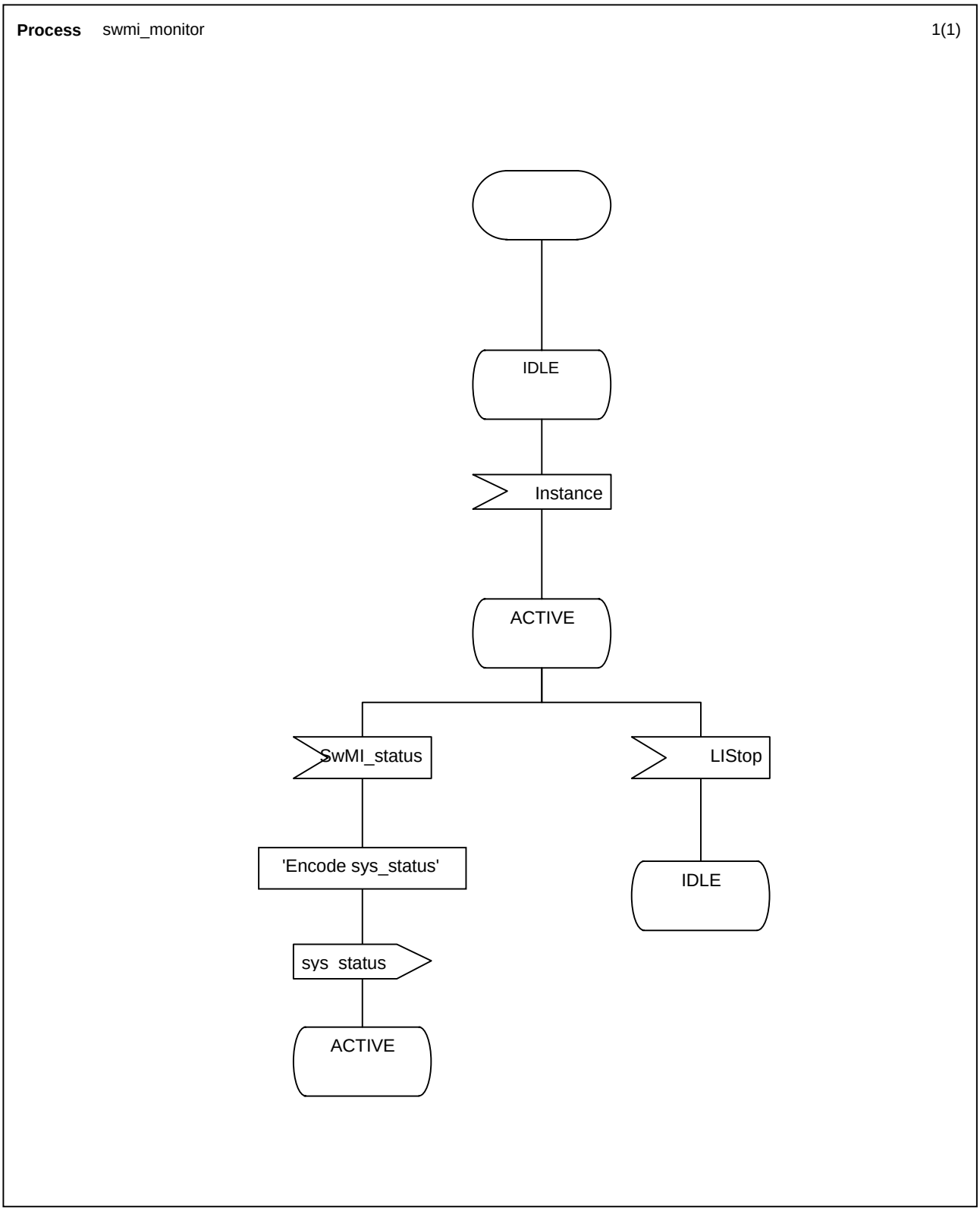


Figure B.5: Behaviour of SwMI_monitor process

B.5 Inter-Process Communication (IPC)

There are a number of signals described in the process model that do not appear on the external interfaces. These signals carry inter-process data and in the main act to start or stop, or to initiate state changes in, other processes.

Annex C (informative): Example encoding of target behaviour

This annex gives examples of how typical target behaviour is encoded by the LI mechanisms described in the main text.

C.1 Call setup from target to TETRA co-target

For a TETRA user (target) making a call attempt to another TETRA user the call setup message (U-SETUP) may take the following form:

U-SETUP ::=
PDU-Type = U-SETUP
Area selection = All areas this system
Hook method selection = No hook signalling
Simplex/Duplex selection = Duplex
Basic Service Information = Speech + Clear mode + Point-to-point + One slot
Request to transmit/send data = Not valid (for duplex operation)
Call priority = Priority not defined
Called party type identifier = TSI
Called party SSI = SSI of co-target
Called party extension = MNI of co-target
External subscriber number = Not provided
Facility = Not provided
Proprietary = Not provided

This shall be described using the TARGET_ACTIVITY_MONITOR_ind as follows:

ActivityType =
{
TETRASpeech,
FromTarget,
Point2Point
}
Co-targetAddress =
{
TETRAaddress!MNI = MNI of co-target,
TETRAaddressSSI = SSI of co-target
}

C.2 Target registration

For a TETRA user (target) registering to the TETRA SwMI the message (U_LOCATION_UPDATE_demand) may take the following form:

U-LOCATION UPDATE DEMAND::=
PDU type = U-LOCATION UPDATE DEMAND
Location update type = ITSI attach
Request to append LA = False
Cipher control = Ciphering on
Ciphering parameters = TEA1, DCK, null
Class of MS = 'bit map as appropriate'
Energy saving mode = Not provided
LA information = Not provided
SSI = Target SSI
Address extension = Target MNI
Group identity location demand ack = Not provided
Group identity location demand = Not provided
Proprietary = Not provided

This shall be described using the TARGET_ACTIVITY_MONITOR_ind as follows:

ActivityType =
{
Session_registration,
FromTarget
}
TargetAddress =
{
TETRAaddress!MNI = MNI of target,
TETRAaddress!SSI = SSI of target
}

The encryption parameters will be used by the SwMI to start an authentication exchange which will be notified to the intercept function in a later message.

Annex D (informative): Interim testing regime

In order to facilitate basic testing of the implementation whilst awaiting a formal definition of the handover interface the following scheme is suggested. Adherence to the test specification in this annex is voluntary.

D.1 Overview

The test point shall be at the output point of a "dummy" mediation function. The mediation function will be a BER (Basic Encoding Rules) machine that encodes the information flows (LI_ACTIVATE etc.) from the interception machine as defined for TETRA in the main body of the present document.

The carrier may be any protocol capable of carrying BER encoded data and may include FACILITY messages of DSS1/PSS1.

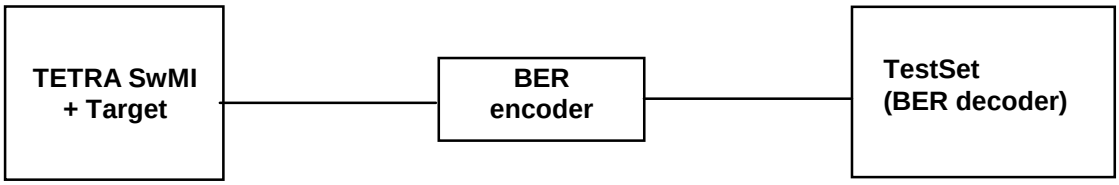


Figure C.1: Test configuration

D.2 Test Purposes

Provide test purposes for each of call setup, registration, de-registration, connectionless transfers (e.g. SDS), authentication, call in progress, etc.

Annex E (normative): ASN.1 Data definitions

This annex brings together the data definitions given in the SDL model and described in clauses 5 and 6.

E.1 Information flows

```
LI_ACTIVATE_req ::= SEQUENCE
{
        TimeStamp                   UTCTime,
    InvokeId                    INTEGER,
    Target_Address          AddressType,
        ExpiryDateTime          UTCTime,
        Target_name             VisibleString       OPTIONAL,
        Additional_target_data  VisibleString       OPTIONAL,
        Monitor_Service_List    SEQUENCE OF ActivityType DEFAULT {AllServices}
};

LI_ACTIVATE_conf ::= SEQUENCE
{
        TimeStamp                   UTCTime,
    InvokeId                    INTEGER,
    Result                      BOOLEAN,
        TLIInstanceid               TLIIdType           OPTIONAL    -- Conditional on value of
Result --
};

LI_MODIFY_req ::= SEQUENCE
{
        TLIInstanceid               TLIIdType,
        Timestamp                   UTCTime,
        ModificationNumber      Integer,
    ModificationType        CHOICE
    {
        Halt                        BOOLEAN,
        Reset                       BOOLEAN,
            ExpiryDateTime          UTCTime,
            Target_name             VisibleString,
            Additional_target_data   VisibleString,
            Monitor_Service_List    SEQUENCE OF ActivityType
    }
};

LI_MODIFY_conf ::= SEQUENCE
{
        TLIInstanceid               TLIIdType,
        Timestamp               UTCTime,
        ModificationNumber      Integer,
        Result                      BOOLEAN
};

LI_STATUS_ind ::= SEQUENCE
{
    TLIInstanceid                   TLIIdType,
    Timestamp                       UTCTime,
    TETRA_Sys_Status        StatusType
};

TARGET_ACTIVITY_MONITOR_ind ::= SEQUENCE
{
    TLIInstanceid                       TLIIdType,                          -- header, who –
    Timestamp                           UTCTime,                        -- header, when –
    Target_Location                 LocationType,                       -- header, where –
    TargetAction                    ActivityType,
    Supplementary_Target_address    AddressType                     OPTIONAL,
    Co_target_address               SEQUENCE of AddressType     OPTIONAL,
    Co_target_location                  SEQUENCE of LocationType    OPTIONAL
};
```

```
TARGET_COMMS_MONITOR_ind ::= SEQUENCE
{
    TLIInstanceid                       TLIIdType,
    Timestamp                           UTCTime,
    Target_location                     LocationType,
    Supplementary_Target_address    AddressType OPTIONAL,
    Target_comms_id                 CircuitIdType,
    Co_target_address                   SEQUENCE  of  AddressType   OPTIONAL,
    Co_target_comms_id              SEQUENCE of  CircuitIdType  OPTIONAL
};

T_TRAFFIC_ind ::= SEQUENCE
{
        TLIInstanceid               TLIIdType,
    TrafficPacket               BitString
}

CT_TRAFFIC_ind ::= SEQUENCE
{
        TLIInstanceid               TLIIdType,
    TrafficPacket               BitString
}
```

E.2 Information element definitions

```
ActivityClassType ::= ENUMERATED
{
    AllServices,
TETRASpeech,
SingleSlotData24,
SingleSlotData48,
SingleSlotData72,
MultiSlotData2_24,
MultiSlotData2_48,
MultiSlotData2_72,
MultiSlotData3_24,
MultiSlotData3_48,
MultiSlotData3_72,
MultiSlotData4_24,
MultiSlotData4_48,
MultiSlotData4_72,
SDSType1,
SDSType2,
SDSType3,
SDSType4,
Status,
SDS_ACK_Type1,
SDS_ACK_Type2,
SDS_ACK_Type3,
SDS_ACK_Type4,
Status_ack,
SDS_Acknowledgement_success,
SDS_Acknowledgement_fail,
SCLNS_PacketData,
CONS_PacketData,
InternetProtocol,
SwMI_authentication_success,
SwMI_authentication_fail ,
ITSI_authentication_success,
ITSI_authentication_fail,
OTAR_SCK_success,
OTAR_SCK_fail,
OTAR_GCK_success,
OTAR_GCK_fail,
OTAR_CCK_success,
OTAR_CCK_fail,
TARGET_SUSCRIPTION_DISABLED_T,
TARGET_EQUIPMENT_DISABLED_T,
TARGET_SUSCRIPTION_DISABLED_P,
TARGET_EQUIPEMENT_DISABLED_P,
TARGET_SUBSCRIPTION_ENABLED,
TARGET_EQUIPMENT_ENABLED,
Session_registration,
Session_deregistration,
MIGRATION,
ROAMING,
SupplementaryService
};
```

```
ActivityType::= SEQUENCE
{
        Activity            ActivityClassType,
        CallRelation        ENUMERATED
        {
            Begin,
            End,
            Continue,
            Report
        },
        Direction           ENUMERATED
{
ToTarget,
FromTarget
        } OPTIONAL,
        Scope               ENUMERATED
{
Point2Point,
Point2MultiPoint,
Broadcast
} OPTIONAL,
        C_PlaneData     BitString   OPTIONAL,
        SS_type         SSType  OPTIONAL
}

AddressType ::= SEQUENCE
    {
        TSI TSIType,
SEQUENCE of SupplementaryAddress    CHOICE
        {
            TETRAaddress    TSIType,
            PISNaddress     PISNType,
            IP4address      INTEGER (0 .. 2^32-1),    -- 32 bits –
            IP6address      INTEGER (0 .. 2^64-1),    -- 64 bits –
            E164address     BitString,
            X121address     BitString,
            TEI             TEIType
        } OPTIONAL
    }

CellIdType ::= INTEGER (0 .. 65535)     -- 16 bits –

LocationAreaType ::= INTEGER (0..16383)     -- 14 bits, as defined in ETS 300 392-2 –

LocationType ::= CHOICE
{
        MS_Loc      TETRA_CGIType,
        LS_Loc      TETRA_LS_AddressType
}


MCC_Type ::=            INTEGER (0..1023)   -- 10 bits, as defined in ETS 300 392-1 –

MNC_Type ::=            INTEGER (0..16383)  -- 14 bits, as defined in ETS 300 392-1 –
```

```
SSType ::= ENUMERATED
{
            AmbienceListening,
            AdviceofCharge,
            AccessPriority,
            AreaSelection,
            BarringofIncomingCalls,
            BarringofOutgoingCalls,
            CallAuthorizedbyDispatcher,
            CallCompletiontoBusySubscriber,
            CallCompletiononNoReply,
            CallForwardingonBusy,
            CallForwardingonNoReply,
            CallForwardingonNotReachable,
            CallForwardingUnconditional,
            CallingLineIdentificationPresentation,
            CallingConnectedLineIdentificationRestriction,
            ConnectedLineIdentificationPresentation,
            CallReport,
            CallRetention,
            CallWaiting,
            DynamicGroupNumberAssignment,
            DiscreetListening,
            CallHold,
            IncludeCall,
            LateEntry,
            ListSearchCall,
            PriorityCall,
            PreemptivePriorityCall,
            ShortNumberAddressing,
            TransferofControl,
            TalkingPartyIdentification
};

StatusType ::= ENUMERATED
{
        NetworkFullyAvailable,
        NetworkErrorsAffectingIntercept,
        ReconfigurationInProgress,
        SessionExpired,
        GatewayServicesUnavailable
}

TETRA_CGIType ::= SEQUENCE
{
        mcc MCC_Type,
        mnc MNC_Type,
        lai     LocationAreaType,
        CI      CellIdType  OPTIONAL
}

TLIIdType ::= INTEGER(0 .. 65535)   -- 16 bits –

TSI_Type ::= SEQUENCE
{
            mcc       MCC_Type,
            mnc       MNC_Type,
            ssi         SSI_Type
};
```

Bibliography

- GSM 01.33: "Digital cellular telecommunications system; Lawful Interception requirements for GSM (GSM 01.33)".
- ETS 300 393-1: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Packet Data Optimized (PDO); Part 1: General network design".
- ETS 300 393-2: "Terrestrial Trunked Radio (TETRA); Packet Data Optimized (PDO); Part 2: Air Interface (AI)".
- ETR 086-3: "Trans European Trunked Radio (TETRA) systems; Technical requirements specification; Part 3: Security aspects".
- ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic reference model - Part 2: Security Architecture".
- ETS 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
- ETS 300 393-7: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Packet Data Optimized (PDO); Part 7: Security".
- ETS 300 396-1: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 1: General network design".
- ETS 300 396-2: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 2: Radio aspects".
- ETS 300 396-3: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 3: Mobile Station to Mobile Station (MS-MS) Air Interface (AI) protocol".
- ETS 300 396-6: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".
- ETR 330: "Security Techniques Advisory Group (STAG); A guide to legislative and regulatory environment".
- CM(95)101: "Council of Europe Recommendation on Problems of Criminal Procedural Law connected with Information Technology" (Strasbourg, 31 July 1995,(adopted 7-8 September 1995)).
- Draft TR-45 TIA/EIA SP-3580A: "Lawfully Authorized Electronic Surveillance".
- ITU-T Recommendation X.219: "Remote operations: model, notation and service definition".
- ITU-T Recommendation X.229: "Remote operations: protocol specification".
- ETS 300 402-1: "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Data link layer; Part 1: General aspects [ITU-T Recommendation Q.920 (1993), modified]".
- ETS 300 402-2: "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Data link layer; Part 2: General protocol specification [ITU-T Recommendation Q.921 (1993), modified]".
- ES 201 158 (V1.1): "Telecommunications Security; Lawful Interception (LI); Requirements for network functions".
- "Technical Directive setting forth Requirements as provided for by §13 of the Telecommunications Traffic Interception Ordinance (TR FÜV)", Bundesamt für Post and Telekommunikation, Version 2.0, April 1997.
- GHIS 2.0: "Government Handover Interface Specification" (UK).
- "Support and evaluation of prototype TETRA (Trans-European Trunked Radio) equipment for demonstration and development programmes."; Shakeshaft, N.E., 1995, K2a. M.Eng., Bath - 45-8233.

- DES/SEC-003003: "Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic; Description of a handover interface for 64 kbit/s speech and data services".

- ISO/IEC 11572 (1996): "Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Circuit mode bearer services - Inter-exchange signalling procedures and protocol".

- ISO/IEC 11582 (1995): "Information technology - Telecommunications and information exchange between systems - Private Integrated Services Network - Generic functional protocol for the support of supplementary services - Inter-exchange signalling procedures and protocol".

- ITU-T Recommendation. X.209: "Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1)".

History

Document history				
V1.1.1	June 1997	Public Enquiry	PE 9744:	1997-06-06 to 1997-10-31
V2.0.0	July 1998	Second Public Enquiry	PE 9846:	1998-07-17 to 1998-11-13