EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 425

September 1995

Source: ETSI TC-ECMA

Reference: DE/ECMA-00010

ICS: 33.040.10, 33.040.30

Key words: PTN, supplementary service

Private Telecommunication Network (PTN); Specification, functional model and information flows Call intrusion supplementary service

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

Contents

Blank page

Foreword

This European Telecommunication Standard (ETS) has been produced by the European Computer Manufacturers Association (ECMA) on behalf of its members and those of the European Telecommunications Standards Institute (ETSI).

This ETS is one of a series of standards defining services and signalling protocols applicable to Private Telecommunication Networks (PTNs). The series uses the ISDN concepts as developed by the ITU-T (formerly CCITT) and is also within the framework of standards for open systems interconnection as defined by ISO.

This ETS specifies the Call Intrusion supplementary service.

The ETS is based upon the practical experience of ECMA member companies and the results of their active and continuous participation in the work of ISO, ITU-T, ETSI and other international and national standardization bodies. It represents a pragmatic and widely based consensus.

This ETS was produced by ECMA using the ECMA guidelines for the production of standards and using the ECMA stylesheet. In order to avoid undue delays in the approval process for this ETS it has been agreed that this ETS will not be converted to the ETSI stylesheet.

Blank page

1 Scope

This European Telecommunication Standard (ETS) specifies the Call Intrusion supplementary service (SS-CI), which is applicable to basic services supported by Private Telecommunication Networks (PTNs). Basic services are specified in ETS 300 171.

Call Intrusion (SS-CI) is a supplementary service which, on request from the served user, enables the served user to establish communication with a busy called user (user B) by breaking into an established call between user B and a third user (user C).

Service specifications are produced in three stages, according to the method described in ETS 300 387. This ETS contains the stage 1 and stage 2 specifications of SS-CI. The stage 1 specification (clause 6) specifies the supplementary service as seen by users of PTNs. The stage 2 specification (clause 7) identifies the Functional Entities involved in the supplementary service and the information flows between them.

The purpose of the stage 1 and stage 2 specifications is to guide and constrain the work on signalling protocols at stage 3. Stage 3, the definition of the network and access layer 3 signalling protocols to support the supplementary service, is defined in separate standards.

NOTE 1

For this ETS, stage 2 does not consider the split of functionality between a functional TE at user B and the local PTNX. TE functions and local PTNX functions at user B are included in the same Functional Entity.

2 Conformance

In order to conform to this ETS, a stage 3 standard shall specify signalling protocols and equipment behaviour that are capable of being used in a PTN which supports the supplementary service specified in this ETS. This means that, to claim conformance, a stage 3 standard is required to be adequate for the support of those aspects of clause 6 (stage 1) and clause 7 (stage 2) which are relevant to the interface or equipment to which the stage 3 standard applies.

3 References

ETS 300 171	Private Telecommunication Network (PTN); Specification, functional models and information flows; Control aspects of circuit mode basic services (1992)
ETS 300 173	Private Telecommunication Network (PTN); Specification, functional models and information flows; Identification supplementary services (ISSD) (1992)
ETS 300 189	Private Telecommunication Network (PTN); Addressing (1992)
ETS 300 237	Private Telecommunication Network (PTN); Specification, functional models and information flows; Name identification supplementary services (1993)
ETS 300 256	Private Telecommunication Network (PTN); Specification, functional models and information flows; Diversion supplementary services (1993)
ETS 300 258	Private Telecommunication Network (PTN); Specification, functional models and information flows; Path replacement additional network feature (1993)
ETS 300 260	Private Telecommunication Network (PTN); Specification, functional models and information flows; Call transfer supplementary service (1993)

ETS 300 361	Private Telecommunication Network (PTN); Specification, functional model and information flows; Call offer supplementary service (1994)
ETS 300 363	Private Telecommunication Network (PTN); Specification, functional model and information flows; Do not disturb and do not disturb override supplementary services (1994)
ETS 300 365	Private Telecommunication Network (PTN); Specification, functional model and information flows; Call completion supplementary services (1994)
ETS 300 387	Private Telecommunications Network (PTN); Method for the specification of basic and supplementary services (1994)
ETS 300 415	Private Telecommunication Network (PTN); Terms and definitions (1995)
CCITT Recommendation I.112	Vocabulary of terms for ISDNs (1988)
CCITT Recommendation I.210	Principles of telecommunication services supported by an ISDN and the means to describe them (1988)
CCITT Recommendation I.221	Common specific characteristics of services (1988)
CCITT Recommendation Z.100	Specification and Description Language (SDL) (1988)

4 Definitions

For the purpose of this ETS the following definitions apply:

4.1 External definitions

This ETS uses the following terms defined in other documents:

– Basic Service	(CCITT Rec. I.210)
– Calling Party Name	ETS 300 237
– Connection	(CCITT Rec. I.112)
– Integrated Services Digital Network	(CCITT Rec. I.112)
– Name	ETS 300 237
– Network Determined User Busy	(CCITT Rec. I.221)
– Number	ETS 300 189
– Private Telecommunication Network Exchange (PTNX)	(ETS 300 415)
– Public	(ETS 300 415)
– Service	(CCITT Rec. I.112)
– Signalling	(CCITT Rec. I.112)
– Subaddress	ETS 300 189
– Supplementary Service	(CCITT Rec. I.210)
– Private Telecommunication Network	(ETS 300 415)
– Terminal Equipment	(ETS 300 415)
– User	(ETS 300 171)
– User Determined User Busy	(CCITT Rec. I.221)

This ETS refers to the following basic call Functional Entities (FEs) defined in ETS 300 171:

- Call Control (CC)
- Call Control Agent (CCA)

This ETS refers to the following basic call inter-FE relationships defined in ETS 300 171:

- r1
- r2
- r3

This ETS refers to the following basic call information flows defined in ETS 300 171:

- DISCONNECT request/indication
- RELEASE request/indication
- RELEASE response/confirmation
- SETUP request/indication
- SETUP response/confirmation

This ETS refers to the following basic call information flow elements defined in ETS 300 171:

- Destination number
- Connection type

This ETS refers to the following information flow elements defined in ETS 300 173:

- Originating number
- Originating subaddress

4.2 Busy

A property of a user for whom either a Network Determined User Busy or User Determined User Busy condition exists.

4.3 Conference type connection

A connection between the served user, user B and user C, where all users have user information connection with each other.

4.4 Consultation

Invocation of SS-CI after the calling user has been informed that a call has failed because of busy at the destination.

4.5 Consultation timer

A timer governing the time in which the calling user is allowed to request invocation of SS-CI after being informed that a call has failed because of busy at the destination. The duration of the timer is an implementation option.

4.6 Established call

The active call that is selected for intruding on.

4.7 Forced release

The release of the established call on request from the served user during the intrusion state.

4.8 Immediate invocation

Invocation of SS-CI as part of the initial call set up.

4.9 Impending intrusion state

The condition of an established call and an intruding call after provision of an impending intrusion warning notification and before establishment of communication between the served user and user B.

4.10 Impending intrusion warning notification

A notification provided before communication is established between the served user and user B.

4.11 Implementation option

An option for the implementor of the service to include or not to include in the service providing system.

4.12 Intruding call

A call in which the served user requests SS-CI.

4.13 Intrusion state

The condition of an established call after establishment of communication between the served user and user B and prior to termination of SS-CI or invocation of Wait On Busy (WOB).

4.14 Intruding call connected notification

A notification provided on establishment of communication between the served user and user B.

4.15 Isolation

The breaking of the user information connection to and from user C during the intrusion state.

4.16 Path retention

The retaining of the network connection between the originating CC and the destination CC so that a supplementary service (such as SS-CI) can be invoked without establishing a new connection.

4.17 Served user

The user who requests SS-CI.

4.18 Time to intrusion

The duration of the impending intrusion state.

4.19 User B

The wanted user that is subject to the call intrusion.

4.20 User C

The other user in the established call.

4.21 WOB state

A state that can be entered from the intrusion state and in which the intruding call is disconnected from user B and is waiting for user B to answer the call.

5 List of acronyms

ANF	Additional Network Feature
CC	Call Control (Functional Entity)
CCA	Call Control Agent (Functional Entity)
CCBS	Call Completion to Busy Subscriber
CCNR	Call Completion No Reply
CFB	Call Forwarding Busy
CFNR	Call Forwarding No Reply
CFU	Call Forwarding Unconditional
CI	Call Intrusion
CICL	Call Intrusion Capability Level
CIPL	Call Intrusion Protection Level
CLIP	Calling Line Identification Presentation
CLIR	Calling/Connected Line Identification Restriction
CNIP	Calling Name Identification Presentation
CNIR	Calling/Connected Name Identification Restriction
CO	Call Offer
COLP	Connected Line Identification Presentation
CONP	Connected Name Identification Presentation
CT	Call Transfer
DND	Do Not Disturb
DNDO	Do Not Disturb Override
FE	Functional Entity
ISDN	Integrated Services Digital Network
NDUB	Network Determined User Busy
PTN	Private Telecommunication Network
PTNX	Private Telecommunication Network Exchange
SDL	Specification and Description Language
SS	Supplementary Service
TE	Terminal Equipment
UDUB	User Determined User Busy
WOB	Wait On Busy

6 SS-CI stage 1 specification

6.1 Description

6.1.1 General description

Call Intrusion (SS-CI) is a supplementary service which, on request from the served user, enables the served user to establish communication with a busy called user (user B) by breaking into an established call between user B and a third user (user C). On successful intrusion, user C is either connected in a conference type connection with the served user and user B or disconnected from user B (isolated).

An intrusion request is only accepted if the served user has a higher Call Intrusion Capability Level (CICL) than the Call Intrusion Protection Level (CIPL) of both user B and user C.

There are three implementation options that provide the served user with additional capabilities following successful intrusion:

- Forced release, allowing the served user to release the established call;
- Isolation, allowing the served user, if a conference type connection has been established, to isolate user C;
- WOB, allowing the served user to cause a transition from the intrusion state to the WOB state.

6.1.2 Qualifications on applicability to telecommunication services

SS-CI is applicable to all circuit mode basic telecommunication services defined in ETS 300 171 where considered meaningful.

6.2 Procedures

6.2.1 Provision and withdrawal

SS-CI shall be provided or withdrawn after pre-arrangement with the service provider.

SS-CI shall be provided on a per PTN number basis. For each PTN number, the supplementary service may be provided for those basic services for which it is considered meaningful (see 6.1.2) provided at that PTN number or for only some of these basic services provided at that PTN number.

A Call Intrusion Capability Level (CICL) shall be allocated to the served user. Call Intrusion Protection Levels (CIPLs) shall be allocated to potential individual users B and C within the PTN and to gateways to other networks (for use on behalf of users outside the PTN). The procedure by which CICL and CIPL are allocated is outside the scope of this ETS.

CICL shall have a value in the range 1 (lowest capability) to 3 (highest capability). At least one of the CICL values shall be offered.

CIPL shall have a value in the range 0 (no protection) to 3 (total protection). CIPL values 0 and 3 shall be offered, and values 1 and 2 may, as an implementation option, be offered.

NOTE 2

It is not precluded that CIPL values can be variable, e.g. a user may have the possibility to change the CIPL value with a user procedure. CIPL values assigned to gateways may also be variable, e.g. depending on whether the gateway is used for an incoming or outgoing call to the PTN. The details of such capabilities are outside the scope of this ETS.

At least one of the methods of invoking SS-CI (see 6.2.2.2.1) shall be supported. If both methods given in 6.2.2.2.1 are supported, then a user may be provided with one or both methods.

A number of implementation options concern features available to the served user during call intrusion. The served user may, at time of provision of SS-CI, be given the choice of being provided with some, all or none of these or the options may be generally available. These implementation options are: forced release, isolation, and WOB.

When these options are selectable on a per served user basis, they may be selectable separately for each basic service for which SS-CI is provided, or selectable only for all basic services for which SS-CI is provided.

6.2.2 Normal procedures

6.2.2.1 Activation, deactivation, interrogation and registration

SS-CI shall be activated by the service provider upon provision, and deactivated upon withdrawal.

Registration and interrogation shall not apply.

6.2.2.2 Invocation and operation

6.2.2.2.1 Methods of invoking SS-CI

There are two different ways to invoke SS-CI. A PTN shall offer one or both of these ways. These ways are:

a) Consultation: the served user, on being informed that a call has failed because of busy at the destination, shall be able, within a defined period (consultation timer), to request SS-CI.

b) Immediate invocation: the served user shall be able to request SS-CI as part of the initial call set up.

6.2.2.2.2 Verification and selection of compatible call

If the consultation method is provided to the served user, the following procedure shall apply. If a call fails due to busy at the called user B and the PTN is not aware that intrusion is not allowed (e.g. because of insufficient CICL), the PTN shall notify the served user that the call has failed because of busy at the called user B and that intrusion may be possible. The served user may then request SS-CI.

If the immediate invocation method is provided to the served user, the served user may request SS-CI with the initial call set up.

For both invocation alternatives the following shall apply. Upon receiving an intrusion invocation request from the served user, the PTN shall check that the user B's number used by the served user, when requesting the service, is also a number involved in a compatible call in the active state. A called user's subaddress supplied by the served user shall not be taken into account when selecting a call to intrude on. Further, the PTN checks that the CIPL values of the users in the active call are lower than the CICL value of the served user. If user B's CIPL value is lower than the CICL value and user B has several compatible calls in the active state, the CIPL values of the other users in the calls shall be checked, in any order, until a CIPL value lower than the CICL value is found. A call that passes these checks shall be selected as the established call.

When the established call has been selected, the users in the established call may as an option be provided an Impending intrusion warning notification and short delay before the connection between the served user and user B is formed. If this

notification is provided, it shall be sent to both users in the established call and optionally to the served user and the impending intrusion state shall be entered.

NOTE 3

The Impending intrusion warning notification can be accompanied by an in-band tone or announcement to user B and user C. An in-band tone or announcement can be given to the served user.

If no Impending intrusion warning notification is provided, the procedures of 6.2.2.2.4 for setting up the connection between the served user and user B shall apply immediately.

6.2.2.2.3 Actions during impending intrusion state

6.2.2.2.3.1 Impending intrusion state ends

A time period, time to intrusion (1-10 seconds, implementation option), after the Impending intrusion warning notification has been provided the impending intrusion state shall be terminated and the procedures of 6.2.2.2.4 for setting up the connection between the served user and user B shall apply.

6.2.2.2.3.2 Release of intruding call

If the served user releases the intruding call during the impending intrusion state, user B and user C shall each be notified that intrusion has terminated. SS-CI shall be terminated.

6.2.2.2.3.3 Release of established call

If user B or user C releases the established call, the served user shall be notified that intrusion is no longer applicable. SS-CI shall be terminated and the network shall attempt to present the call from the served user to user B and continue in accordance with basic call procedure.

6.2.2.2.4 Setting up the connection between served user, user B and user C

There are two different ways (implementation options) for the served user to be connected to user B. Either the network shall form a conference type connection between user B, user C and the served user, or the network shall isolate user C and connect the served user only to user B. In either case, when the connection has been established, the intrusion state shall be entered.

If the first option is implemented, the users in the established call shall be provided with an Intruding call connected notification when the served user is connected. The served user shall receive confirmation that the intrusion request has been accepted and that a conference type connection has been formed.

NOTE 4

The three users can also receive a superimposed in-band indication (e.g. a repeated tone) while the conference type connection exists.

If the latter option is implemented, user C shall be given a notification that isolation has occurred and user B shall be informed that user C has been isolated and that an intrusion has occurred. The served user shall receive confirmation that the intrusion request has been accepted and that isolation has occurred. The served user and user B shall be connected and no conference type connection shall be formed. The established call shall remain in progress but with the user information connection to user C broken.

NOTE 5

User C can also receive an in-band tone or announcement while isolated.

6.2.2.2.5 Actions during intrusion state

6.2.2.2.5.1 Release of intruding call

If the served user releases the intruding call, the established call shall revert to the state that existed before the intrusion state, and the intrusion state shall be terminated. User B and user C shall be notified that the intrusion state has been terminated.

If user B releases the intruding call, the established call shall revert to the state that existed before the intrusion state, and the intrusion state shall be terminated. User C shall be notified that the intrusion state has terminated.

6.2.2.2.5.2 Release of the established call

If user B or user C releases the established call, the served user shall be notified that call intrusion has terminated. If user C releases the established call, user B shall be notified that intrusion has terminated. The intruding call shall become an ordinary call between user B and the served user.

6.2.2.2.5.3 Forced release

As an implementation option the served user may, during the intrusion state, request a forced release of user C. User C may be isolated or in a conference type connection when the request is made. A successful forced release shall be notified to the served user, to user B and to user C. The intruding call shall continue as an ordinary call between the served user and user B, the established call shall be released, and the intrusion state shall be terminated.

6.2.2.2.5.4 Isolation on request from served user

If a conference type connection is used, user C may (implementation option) be isolated from the conference type connection on request from the served user. If the request is accepted the served user shall receive confirmation and the established call shall be disconnected from user B, but not released. The served user shall be connected only to user B. The intrusion state shall continue and the ensuing situation shall be identical to the situation where isolation occurred when the intrusion state was entered. User C and user B shall be notified that user C has been isolated.

6.2.2.2.5.5 Transition from intrusion state to WOB state

As an implementation option it may be possible for the served user to request transition from the intrusion state to the WOB state. On acceptance of such a request, the served user shall receive a confirmation, the established call shall revert back to the state that existed before intrusion, user B shall be reconnected to user C if isolated, the intruding call shall be disconnected from user B and the intrusion state shall be terminated. The intruding call shall not be released but shall enter the WOB state. User B shall be notified that the intrusion has terminated and WOB has been invoked. User C shall be notified that the intrusion has terminated.

6.2.2.2.6 Actions during WOB state

6.2.2.2.6.1 Served user releases

If the served user releases during the WOB state, user B shall be notified and SS-CI terminated.

6.2.2.2.6.2 User B answers the waiting call

If user B answers the waiting call, SS-CI shall be terminated, and the served user shall be notified and connected to user B. The call shall become an ordinary call between user B and the served user.

6.2.2.2.6.3 Re-intrusion request

When the network receives a request for re-intrusion, the network shall verify the request and select an established call in accordance with 6.2.2.2.2 and set up the connection in accordance with 6.2.2.2.3 (if applicable) and 6.2.2.2.4.

6.2.2.2.6.4 User B becomes not busy

If the PTN detects that the necessary resources have become available, it shall transfer an incoming call indication to user B. If user B starts alerting, the served user shall receive an appropriate indication.

6.2.3 Exceptional procedures

6.2.3.1 Activation, deactivation, registration and interrogation

Not applicable.

6.2.3.2 Invocation and operation

If the served user requests invocation of SS-CI as part of the initial call request, and immediate invocation is not provided to the served user, then the request shall be ignored and the call shall proceed as if the request had not been made.

If a SS-CI or re-intrusion request is rejected, the served user shall be informed, and may be given an indication of the reason for the rejection. Possible reasons to reject a SS-CI or re-intrusion request are e.g.:

- served user has a lower or equal CICL compared with user B's and/or user C's CIPL value;
- user B is busy but not involved in a compatible call in the active state;
- temporary lack of resources;
- the established call is already being intruded upon;
- the established call is intruding on another call.

If SS-CI is requested and user B is found to be not busy, the call shall be treated as a normal incoming call to user B.

If a forced release, isolate or WOB request from the served user is denied by the PTN, the served user shall be notified and may be given an indication for the reason of the denial. The intrusion state shall remain.

If an intrusion request from the WOB state is rejected, the WOB state shall remain.

If consultation applies to the call, the call shall be released either if the served user does not request invocation within the defined time period (consultation timer) or if the served user requests invocation within the defined time period (consultation timer) and this request is rejected.

Consultation shall not apply if the called user is busy and the PTN is aware that intrusion is not allowed. Basic call procedures shall apply.

6.3 Interactions with other supplementary services and ANFs

Interactions with other supplementary services and ANFs for which PTN standards were available at the time of the publication of this ETS are specified below.

6.3.1 Call Completion to Busy Subscriber (CCBS)

SS-CCBS requested by the served user while in the intrusion state shall be rejected.

While in the WOB state, the served user may be able to invoke SS-CCBS.

While in the WOB state the intruding call shall have priority over any SS-CCBS request against that same user B, when resources at that user B become available.

NOTE 6

If a call fails because of busy at the destination, either SS-CI or SS-CCBS or both can be applied.

6.3.2 Call Completion No Reply (CCNR)

No interaction.

6.3.3 Do Not Disturb (DND)

If a call for which SS-CI has been invoked as part of the initial call set up (immediate invocation) fails because of SS-DND active, then the invocation of SS-CI shall be rejected.

6.3.4 Do Not Disturb Override (DNDO)

If a called user has SS-DND active, and SS-DNDO is successfully invoked, then:

- if SS-CI immediate invocation is applicable to the call, then the invocation of SS-CI shall apply to the call after SS-DND has been overridden;
- if SS-CI consultation is applicable to the call, it shall apply after SS-DND has been overridden.

6.3.5 Calling Line Identification Presentation (CLIP)

User B shall, as part of the intruding call, receive the Calling Line Identification of the served user, unless Calling Line Identification Restriction (CLIR) applies and user B has no override capability.

No indication of the served user's identity shall be provided to user C.

6.3.6 Calling/Connected Line Identification Restriction (CLIR)

When CLIR is invoked at the served user, Calling Line Identification shall not be presented to user B, unless user B has an override capability.

When CLIR is invoked at user B, Connected Line Identification shall not be presented to the served user, unless the served user has an override capability.

6.3.7 Connected Line Identification Presentation (COLP)

The served user shall receive the Connected Line Identification of user B when the intrusion state is entered, unless CLIR applies.

The served user shall not receive the Connected Line Identification of user C.

6.3.8 Calling Name Identification Presentation (CNIP)

User B shall, as part of the intruding call, receive the Calling Name Identification of the served user, unless Calling Name Identification Restriction applies and user B has no override capability.

No indication of the served user's name shall be provided to user C.

6.3.9 Connected Name Identification Presentation (CONP)

The served user shall receive the Connected Name Identification of user B when the intrusion state is entered, unless CNIR applies.

The served user shall not receive the Connected Name Identification of user C.

6.3.10 Calling/Connected Name Identification Restriction (CNIR)

When CNIR is invoked at user B, Connected Name Identification shall not be presented to the served user, unless the served user has an override capability.

When CNIR is invoked at the served user, Calling Name Identification shall not be presented to user B, unless user B has an override capability.

6.3.11 Call Forwarding Unconditional (CFU)

SS-CI, if invoked, shall be applied to a busy user that has been forwarded to as a result of one or more invocations of SS-CFU.

6.3.12 Call Forwarding No Reply (CFNR)

SS-CI, if invoked, shall not be applied to a busy user arrived at as a result of one or more forwardings, at least one of which is SS-CFNR. The procedures of SS-CFNR shall apply.

A WOB call that is alerting user B shall not be subject to SS-CFNR.

6.3.13 Call Forwarding Busy (CFB)

If SS-CI is requested as part of the initial call set up, and if the called user is busy and has SS-CFB active, the call shall be forwarded. If the call is forwarded to a user who is also busy, SS-CI shall be applied to the forwarded to user. If the call undergoes more than one forwarding, at least one of which is SS-CFB, but excluding SS-CFNR, then SS-CI shall be applied to the final forwarded to user if that user is busy.

If the calling user is informed that a call has failed because of busy at the destination, and if SS-CI is subsequently invoked, SS-CI shall be applied to the SS-CFB forwarding user or to the SS-CFB forwarded to user. If the call has undergone more than one forwarding, at least one of which is SS-CFB, but excluding SS-CFNR, then SS-CI shall be applied either to the first SS-CFB forwarding user or to the final forwarded to user. Choice between the two is an implementation option. An implementation may permit the calling user to make the choice.

6.3.14 Call Transfer (CT)

The served user shall not be able to invoke SS-CT during the impending intrusion state or the intrusion state. It shall be possible for a served user, during the WOB state, to invoke call transfer for transferring a third user to user B provided that the call between the served user and the third user is in the active state. However, it shall not be possible to transfer two calls both of which are in the WOB state. Transfer during the WOB state shall operate in a similar manner to call transfer during the alerting state, except that the WOB state shall continue. The third user may be notified that the call is waiting for a busy called user. If user B subsequently enters an alerting phase and a notification that the call is waiting at a busy called user has been given to the third user, the third user shall be notified that user B is alerting. If user B subsequently answers the call and a notification that the call is waiting at a busy called user has been given to the third user, the third user shall be notified that user B has answered.

During the impending intrusion state or the intrusion state, user B shall not be able to transfer an established or intruding call. During the WOB state, user B shall not be able to transfer an intruding call.

A user C may be able to transfer an established call in the intrusion state and the impending intrusion state. If transfer occurs, the user that becomes connected to user B shall become the new user C. If transfer occurs during the impending intrusion state, the new user C shall receive an impending intrusion warning notification. If transfer occurs during intrusion state, the new user C shall receive an intruding call connected notification or a notification that isolation has occurred, as appropriate.

6.3.15 Path Replacement (ANF-PR)

Path replacement may be denied while a call is in intrusion state. This applies both to the established call and the intruding call.

6.3.16 Call Offer (CO)

A SS-CO request made after a SS-CI request has been accepted by the PTN shall be rejected.

NOTE 7

SS-CI service includes a similar service to SS-CO - WOB. This can be used instead of SS-CO.

A SS-CI request made after a SS-CO request has been accepted by the PTN shall be allowed. If the request is rejected due to intrusion not allowed, the SS-CO state shall remain. If SS-CI is accepted by the PTN, the SS-CO request shall be cancelled.

If both SS-CI immediate invocation and SS-CO immediate invocation are requested at call set up, the services shall be rejected, and the call shall proceed as if neither of the services had been requested.

If the served user is provided with SS-CO network invocation (immediate) and the served user requests SS-CI immediate invocation, the network shall not invoke SS-CO.

NOTE 8

If a call fails because of busy at the destination, either SS-CI or SS-CO can be applied.

6.4 Interworking considerations

When interworking with another network which supports an equivalent feature, it may be possible to cooperate with the other network to provide SS-CI.

If a call is made with invocation request of SS-CI to a destination in a network that does not support SS-CI, then the invocation request of SS-CI shall be rejected and the call shall proceed as if there had been no SS-CI invocation request.

6.5 Overall SDL

Figure 1 contains the dynamic description of SS-CI using the Specification and Description Language (SDL) defined in CCITT Rec. Z.100 (1988). The SDL process represents the behaviour of the network in providing SS-CI to a served user.

Input signals from the left and output signals to the left represent primitives from and to the served user.Input signals from the right represent either primitives from user B, or inputs from the basic call process, or inputs from an internal process.

Output signals to the right represent primitives to user B or user C.

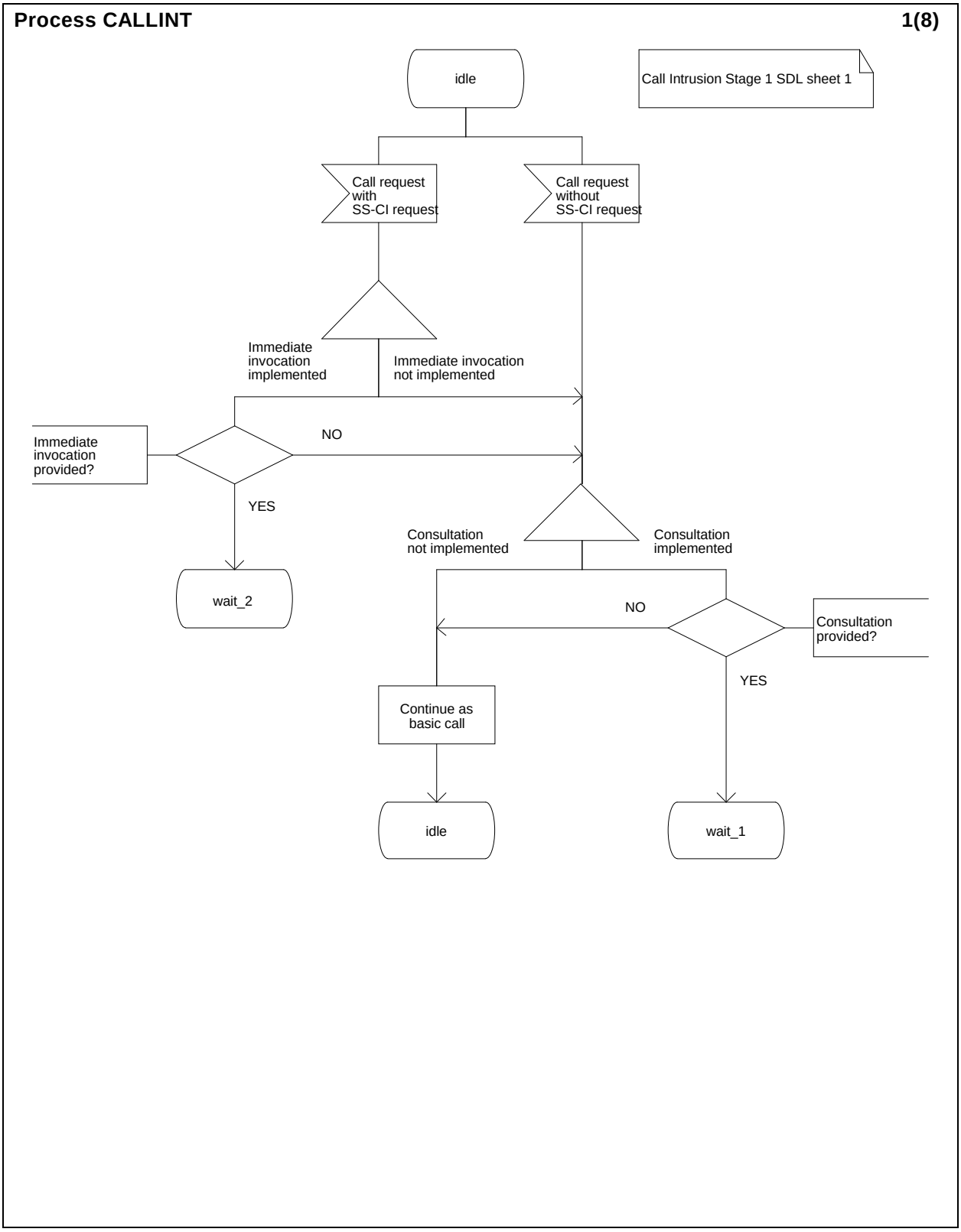

Figure 1 (sheet 1 of 8) - SS-CI overall SDL

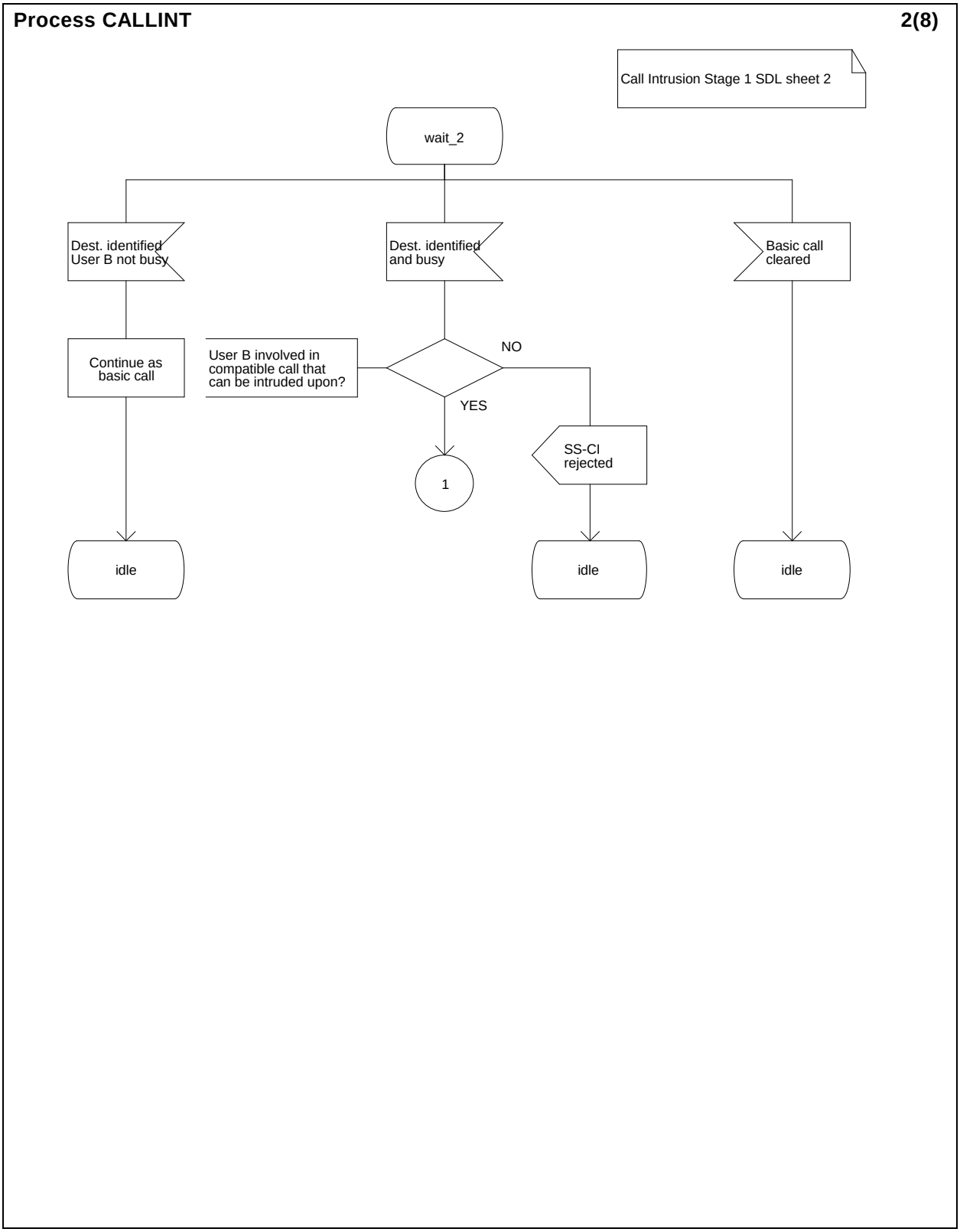

Figure 1 (sheet 2 of 8) - SS-CI overall SDL

Process CALLINT **3(8)**

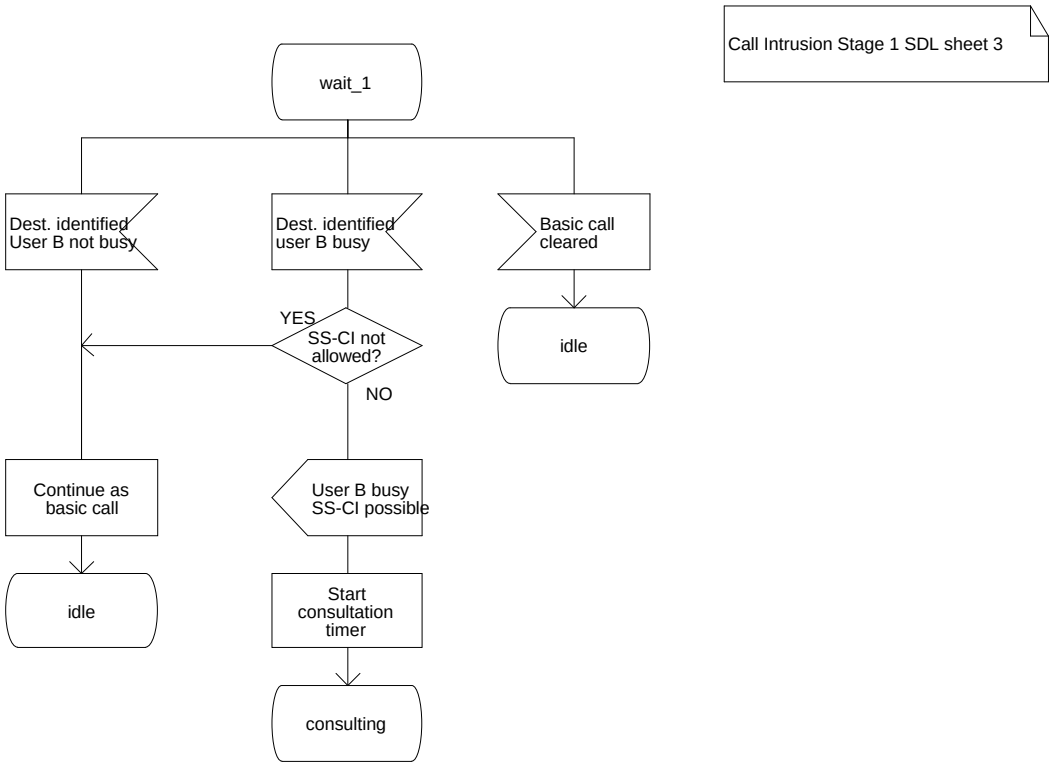

Figure 1 (sheet 3 of 8) - SS-CI overall SDL

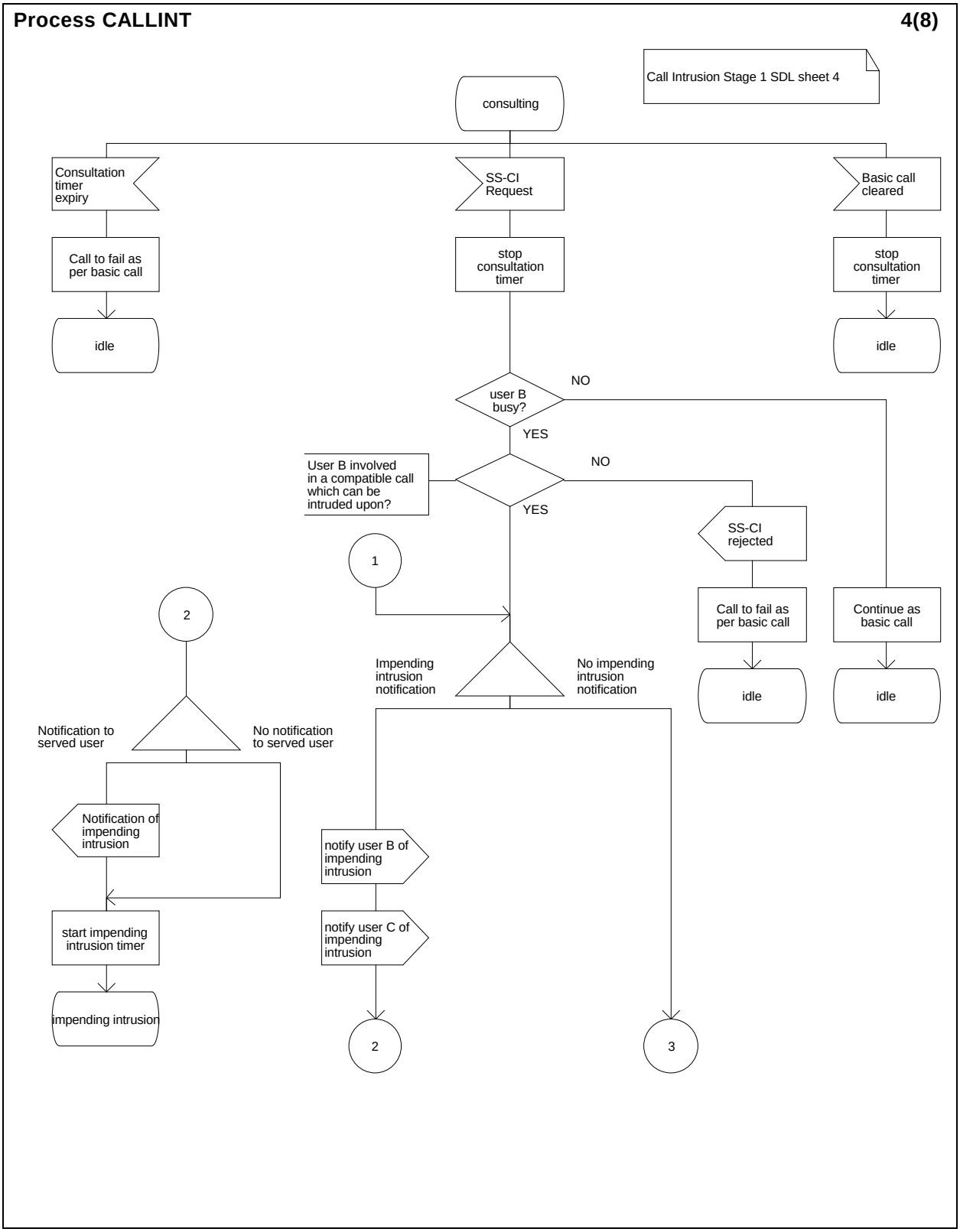

Figure 1 (sheet 4 of 8) - SS-CI overall SDL

Process CALLINT **5(8)**

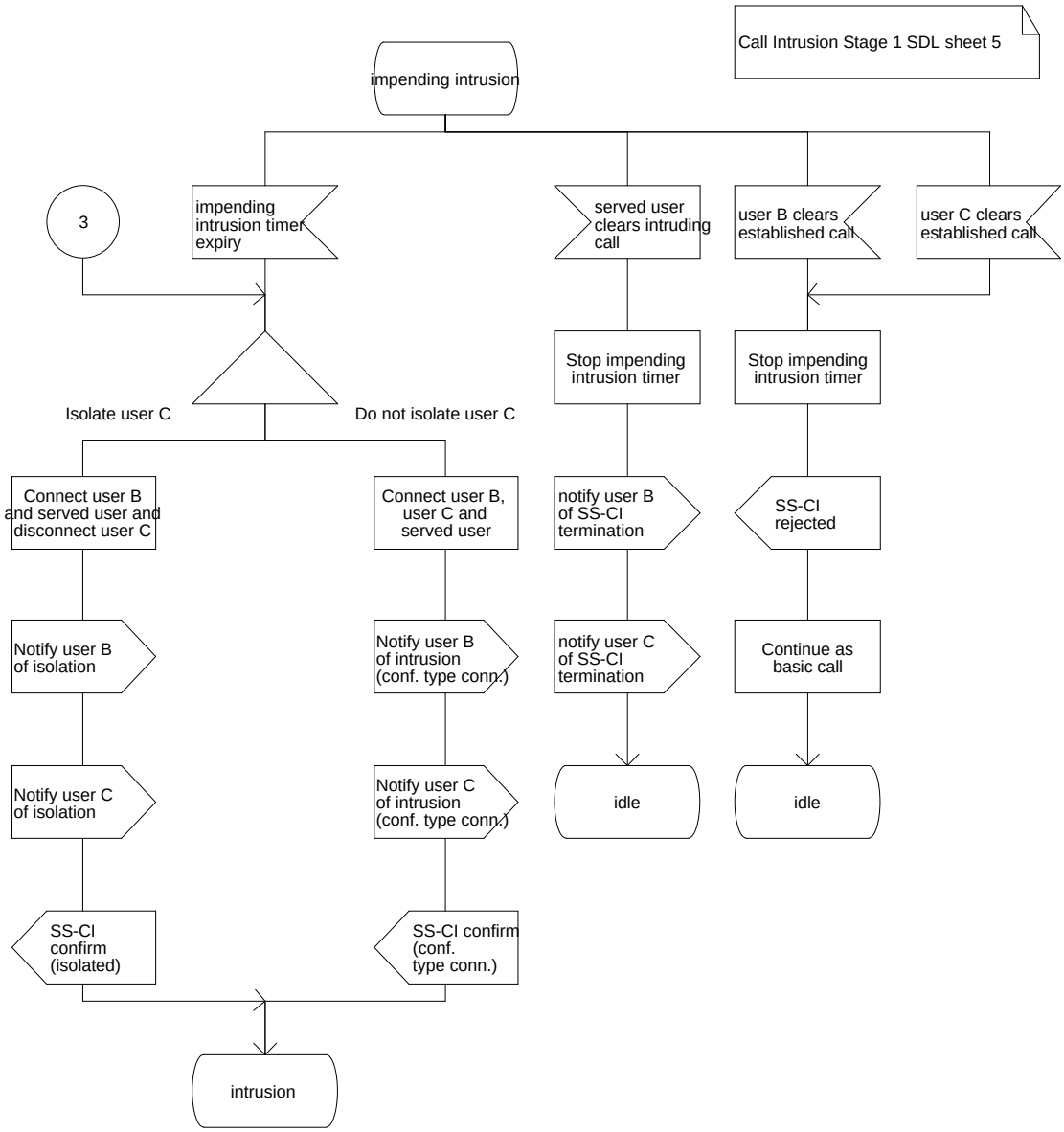

Figure 1 (sheet 5 of 8) - SS-CI overall SDL

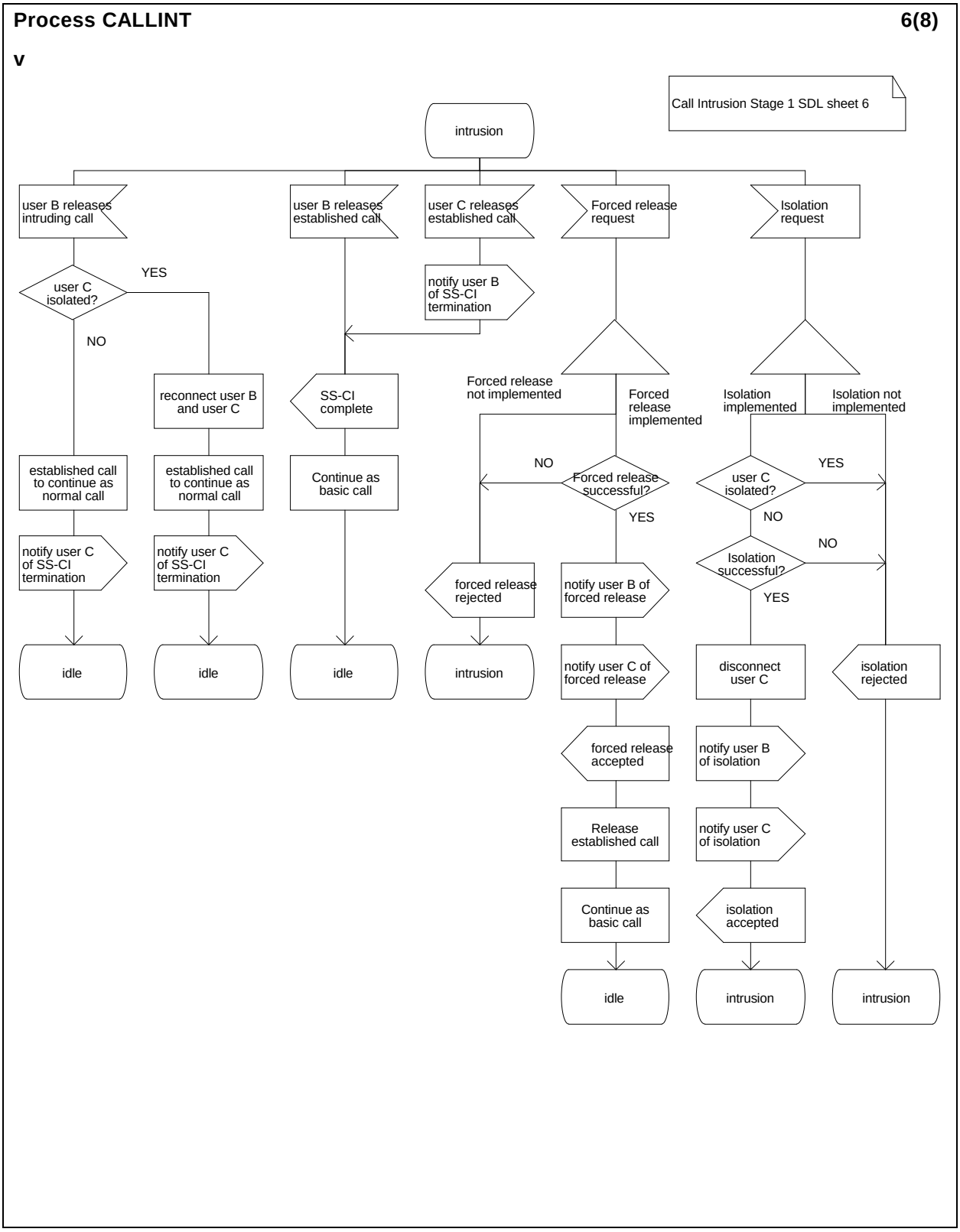

Figure 1 (sheet 6 of 8) - SS-CI overall SDL

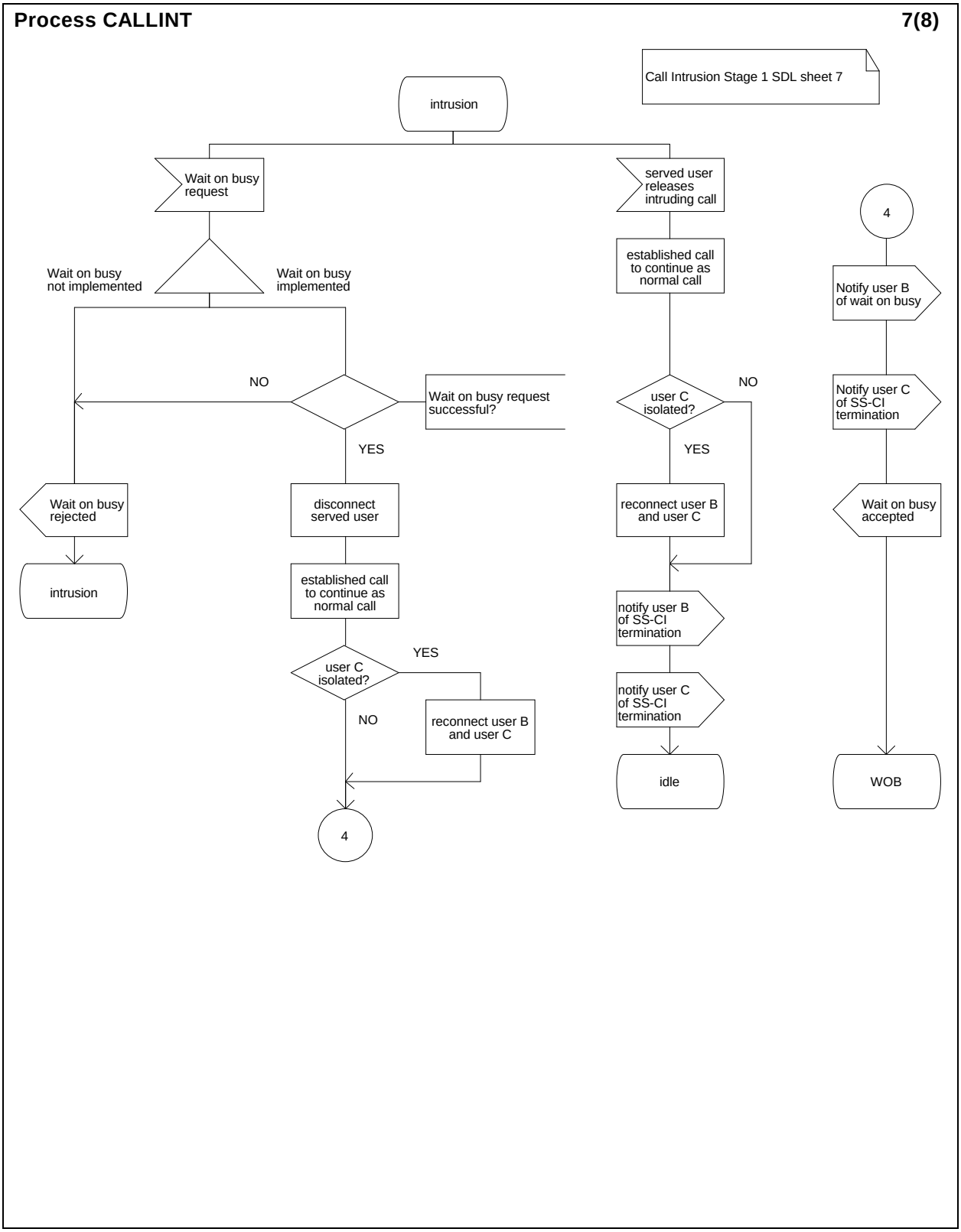

Figure 1 (sheet 7 of 8) - SS-CI overall SDL

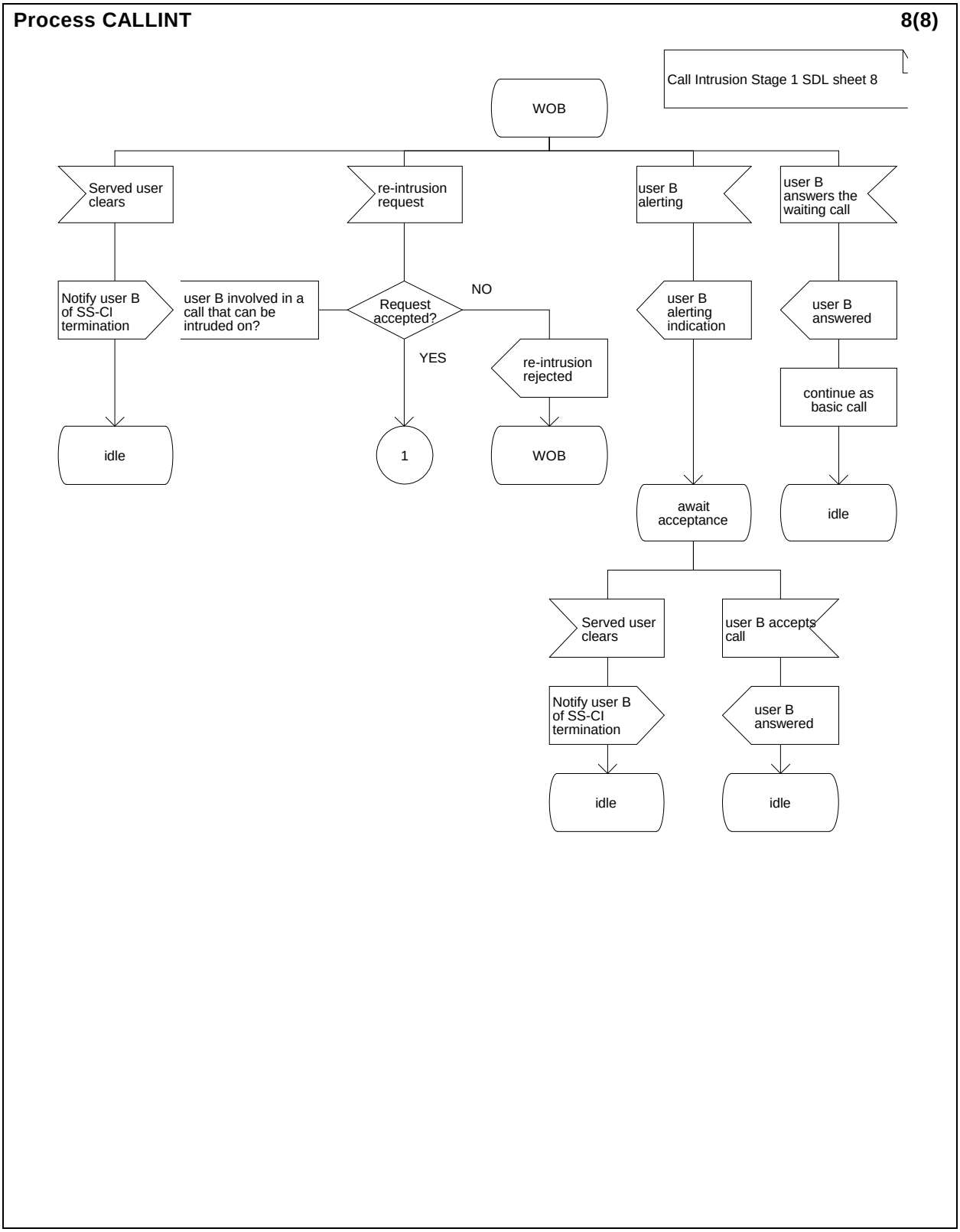

Figure 1 (sheet 8 of 8) - SS-CI overall SDL

7 SS-CI stage 2 specification

The stage 2 specification provides two different methods for operation of SS-CI within the network. With the path retention method, if a busy user is encountered the network connection between the originating CC and the destination CC is not released in accordance with ETS 300 171 but is instead retained awaiting a possible SS-CI request. With the non-retention method, if a busy called user is encountered and the basic call SETUP request/indication was not accompanied by a request for SS-CI, the network connection is released in accordance with ETS 300 171. Therefore, with the non-retention method, if SS-CI is requested after encountering a busy called user a new network connection has to be established.

Either one of the methods can be used to support any one of the two methods of invoking SS-CI:

- Immediate invocation can be supported by the non-retention method by accompanying the SETUP request/indication with a request for SS-CI.
- Immediate invocation can be supported by the path retention method by accompanying the SETUP request/indication with a request for path retention and then, when the path is retained because the called user is busy, requesting SS-CI.
- Consultation can be supported by the non-retention method by not accompanying the SETUP request/indication with a request for SS-CI and then, when the connection is released because the called user is busy, consulting the calling user. SS-CI can then be requested if necessary by repeating the SETUP request/indication, this time accompanied by a request for SS-CI.
- Consultation can be supported by the path retention method by accompanying the SETUP request/indication with a request for path retention and then, when the path is retained because the called user is busy, consulting the calling user. SS-CI can then be requested if necessary using the retained connection. If it is determined that SS-CI is not required, the connection is released.

The stage 3 standard for SS-CI at the Q reference point shall support both options, shall permit a PTNX supporting FE2 functionality to support either path retention or non-retention or both, and shall require a PTNX supporting FE3 functionality to support both path retention and non-retention.

7.1 Functional model

7.1.1 Functional model description

The functional model shall comprise the following Functional Entities (FEs):

FE1 SS-CI requesting entity;
FE2 Served user's service control entity;
FE3 SS-CI control entity, and user B's control entity;
FE4 User C's control entity;
FE5 User C's agent.

The following relationships shall exist between these FEs:

ra between FE1 and FE2;
rb between FE2 and FE3;
rc between FE3 and FE4;
rd between FE4 and FE5.

Figure 2 shows these FEs and relationships.

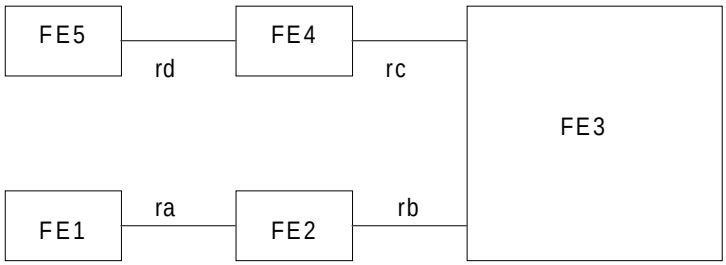

Figure 2 - Functional model for SS-CI

The further division of FE3 into an FE that is collocated with user B's CCA (and therefore allocatable to a functional TE) and an FE that is collocated with user B's CC (and therefore allocatable to a PTNX) is outside the scope of this ETS.

7.1.2 Description of the Functional Entities

7.1.2.1 SS-CI requesting entity, FE1

This functional entity:

- receives requests from the served user and passes these on to FE2;
- receives information from FE2 and passes it on to the served user.

7.1.2.2 Served user's service control entity, FE2

This functional entity:

- at the time of original basic call r1_SETUP_request/indication:
  - receives and validates request from FE1 for immediate invocation of SS-CI;
  - determines if immediate invocation or consultation is applicable for the call;
  - if SS-CI is applicable for the call, determines if the path retention method or the non-retention method is to be used and, as appropriate, sends a path retention request or immediate invocation request to FE3 at the time of the original basic call r2_SETUP-request/indication, or retains the call setup information;
- if consultation applies to the call and all conditions for performing consultation are met:
  - informs FE1 that the original call has encountered busy and that SS-CI may be requested;
  - limits the length of the consultation by clearing the call if the served user has not responded, by clearing the call or requesting SS-CI, within the consultation time;
  - receives request, during consultation, from FE1 for invocation of SS-CI, sends an appropriate SS-CI invocation request (depending on whether path retention or non-retention is used) to FE3, and sends the result of the invocation request to FE1;
- if immediate invocation applies and path retention is used, on receipt of the information from FE3 that the original call has encountered busy and SS-CI is allowed, sends a SS-CI invocation request to FE3;
- receives request from FE1 for isolation, forced release and WOB, and passes these on to FE3 if allowed;
- receives request from FE1 for re-intrusion following WOB, and passes this on to FE3 if allowed;

- receives from FE3 responses to requests and passes them on to FE1;
- receives from FE3 information concerning progress of intrusion (e.g. intrusion impending, intrusion commenced, end of intrusion) and passes them on to FE1.

7.1.2.3 Intrusion service control entity and user B's control entity, FE3

This functional entity:

- on an incoming call with an SS-CI request to a called user who is busy, checks if SS-CI is allowed and accepts or rejects the request accordingly;
- on an incoming call without an SS-CI request but with a path retention request to a called user who is busy, checks if SS-CI would be allowed, taking into account the CICL value and the called user's CIPL value, and if so retains the path from FE2 and offers FE2 the possibility of invoking SS-CI;
- having retained the path and offered FE2 the possibility of invoking SS-CI, and on receipt of an SS-CI request from FE2, checks if SS-CI is allowed and accepts or rejects the request accordingly;
- to check whether intrusion is allowed, the FE checks that the CIPL values of the users in the active call are lower than the CICL value; see also 6.2.2.2.2;
- selects the established call;
- if intrusion is accepted, forms a conference type connection or isolates user C;
- on request from FE2, performs isolation of user C;
- on request from FE2 converts from the intrusion state to the WOB state;
- on request from FE2, initiates forced release of user C;
- sends request for CIPL value of potential user C to FE4 and receives responses;
- handles termination of intrusion through release of intruding or established call;
- sends to FE2 responses to requests and information concerning progress of intrusion;
- provides notifications to user B;
- sends to FE4 information for providing notifications to user C.

7.1.2.4 User C's control entity, FE4

This functional entity:

- provides FE3 with user C's CIPL value;
- receives information flows from FE3 and forwards these to FE5.

7.1.2.5 User C agent, FE5

This functional entity:

- receives information flows from FE4 and informs the user.

7.1.3 Relationship of functional model to basic call functional model

An example of a relationship between the FEs for SS-CI and the FEs for the basic call is shown in figure 3.

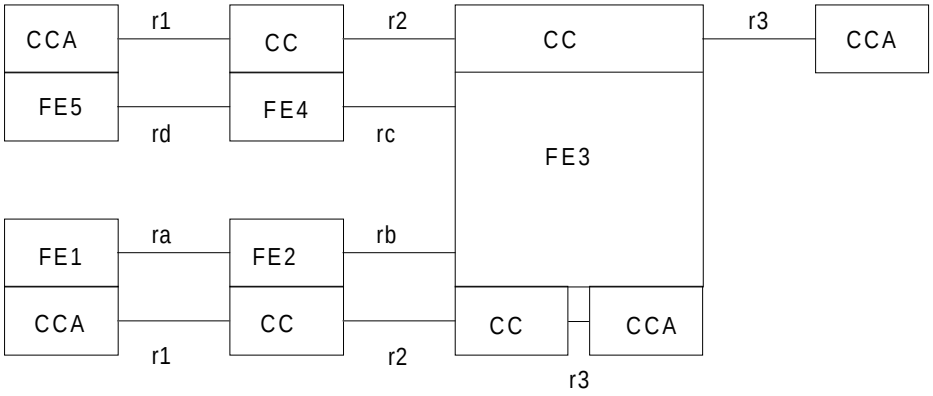

Figure 3 - Example relationship between the model for SS-CI and basic call

7.2 Information flows

7.2.1 Definition of information flows

In the tables listing the elements in information flows, the column headed "Request" indicates which of these elements are mandatory (M) and which are optional (O) in a request/indication information flow, and the column headed "Confirm" indicates which of these elements are mandatory (M) and which are optional (O) in a response/confirmation information flow.

7.2.1.1 Relationship ra

7.2.1.1.1 INFORM

INFORM is an unconfirmed information flow across ra from FE2 to FE1. It is used to inform FE1 that the called user is busy and that SS-CI may be requested. There are no elements within the INFORM information flow.

7.2.1.1.2 CI_INV

CI_INV is a confirmed information flow sent across ra between FE1 and FE2. It is used to invoke intrusion. The response indicates one of the following:

- intrusion performed, user C isolated;
- intrusion performed, user C not isolated;
- intrusion not performed with reason.

Table 1 lists the elements within the CI_INV information flow.

Table 1 - Content of CI_INV

Element	Request	Confirm	note
Result		M	9
User C isolated		O	10

NOTE 9

This element takes one of the values: short term denial, not authorized, not applicable, success, long term denial.

NOTE 10

This element is sent if intrusion is successful and user C has been isolated.

7.2.1.1.3 WARNING

WARNING is an unconfirmed information flow across ra between FE1 to FE2. It is used to notify the served user of the impending intrusion. There are no elements within the WARNING information flow.

7.2.1.1.4 ISOLATE

ISOLATE is a confirmed information flow across ra between FE1 to FE2. It is used to request isolation of user C. The response indicates one of the following:

- user C isolated;
- user C not isolated with reason.

Table 2 lists the elements within the ISOLATE information flow.

Table 2 - Content of ISOLATE information flow

Element	Request	Confirm	note
Result		M	11

NOTE 11

The element takes one of the values: success, not applicable, long term denial.

7.2.1.1.5 FORCE_REL

FORCE_REL is a confirmed information flow across ra between FE1 and FE2. It is used to request the forced release of user C. The response indicates one of the following:

- user C released;
- user C not released with reason.

Table 3 lists the elements within the FORCE_REL information flow.

Table 3 - Content of FORCE_REL information flow

Element	Request	Confirm	note
Result		M	12

NOTE 12

The element takes one of the values: success, not applicable, long term denial.

7.2.1.1.6 EST_TERM

EST_TERM is an unconfirmed information flow across ra between FE1 and FE2. It is used to inform FE1 that the established call has been released. There are no elements within the EST_TERM information flow.

7.2.1.1.7 REQUEST_WOB

REQUEST_WOB is a confirmed information flow sent across ra between FE1 and FE2. It is used to request WOB. The response indicates one of the following:

- WOB request accepted;
- WOB request not accepted with reason.

Table 4 lists the elements within the REQUEST_WOB information flow.

Table 4 - Content of REQUEST_WOB information flow

Element	Request	Confirm	note
Result		M	13

NOTE 13

The element takes one of the values: success, not applicable, long term denial.

7.2.1.1.8 B_ALERTING

B_ALERTING is an unconfirmed information flow sent across ra between FE1 and FE2. It is used to inform FE1 that user B is alerting. There are no elements within the B_ALERTING information flow.

7.2.1.1.9 B_ANSWER

B_ANSWER is an unconfirmed information flow sent across ra between FE1 and FE2. It is used to inform FE1 that user B has answered the waiting call. There are no elements within the B_ANSWER information flow.

7.2.1.2 Relationship rb

7.2.1.2.1 CI_ACT

CI_ACT is an unconfirmed information flow across rb between FE2 and FE3. It is used to indicate to FE3 that path retention is required if intrusion is possible.

Table 5 lists the elements within the CI_ACT information flow.

Table 5 - Content of CI_ACT information flow

Element	Request	Confirm	note
CICL	M		14

NOTE 14

This element takes one of the values: 1, 2, 3.

7.2.1.2.2 ISOLATE

ISOLATE is a confirmed information flow across rb from FE2 to FE3. It is used to request isolation of user C. The response indicates one of the following:

- user C isolated;
- user C not isolated with reason.

Table 6 lists the elements within the ISOLATE information flow.

Table 6 - Content of ISOLATE information flow

Element	Request	Confirm	note
Result		M	15

NOTE 15

The element takes one of the values: success, not applicable, long term denial.

7.2.1.2.3 WARNING

WARNING is an unconfirmed information flow across rb between FE2 and FE3. It is used to notify FE2 of the impending intrusion. There are no elements within the WARNING information flow.

7.2.1.2.4 FORCE_REL

FORCE_REL is a confirmed information flow across rb between FE2 and FE3. It is used to request the forced release of user C. The response indicates one of the following:

- user C released;
- user C not released with reason.

Table 7 lists the elements within the FORCE_REL information flow.

Table 7 - Content of FORCE_REL information flow

Element	Request	Confirm	note
Result		M	16

NOTE 16

The element takes one of the values: success, not applicable, long term denial.

7.2.1.2.5 EST_TERM

EST_TERM is an unconfirmed information flow across rb between FE2 and FE3. It is used to inform FE2 that the established call has been released. There are no elements within the EST_TERM information flow.

7.2.1.2.6 REQUEST_WOB

REQUEST_WOB is a confirmed information flow sent across rb between FE2 and FE3. It is used to request WOB. The response indicates one of the following:

- WOB request accepted;
- WOB request not accepted with reason.

Table 8 lists the elements within the REQUEST_WOB information flow.

Table 8 - Content of REQUEST_WOB information flow

Element	Request	Confirm	note
Result		M	17

NOTE 17

The element takes one of the values: success, not applicable, long term denial.

7.2.1.2.7 CI_AVAIL

CI_AVAIL is an unconfirmed information flow across rb between FE2 and FE3. It is used to inform FE2 that the path has been retained and intrusion may be possible. There are no elements within the CI_AVAIL information flow.

7.2.1.2.8 CI_INV

CI_INV is a confirmed information flow sent across rb between FE2 and FE3. It is used to invoke intrusion. The response indicates one of the following:

- intrusion performed, user C isolated;
- intrusion performed, user C not isolated;
- intrusion not performed with reason.

Table 9 lists the elements within the CI_INV information flow.

Table 9 - Content of CI_INV

Element	Request	Confirm	note
Result		M	18
User C isolated		O	19
CICL	M		20

NOTE 18

This element takes one of the values; short term denial, not authorized, not applicable, success, long term denial.

NOTE 19

This element is sent if intrusion is successful and user C has been isolated.

NOTE 20

This element takes one of the values: 1, 2, 3.

7.2.1.2.9 B_ALERTING

B_ALERTING is an unconfirmed information flow sent across rb between FE2 and FE3. It is used to inform FE2 that user B is alerting. There are no elements within the B_ALERT information flow.

7.2.1.2.10 B_ANSWER

B_ANSWER is an unconfirmed information flow sent across rb between FE2 and FE3. It is used to inform FE2 that user B has answered the waiting call. There are no elements within the B_ANSWER information flow.

7.2.1.3 Relationship rc

7.2.1.3.1 INFO_REQ

INFO_REQ is a confirmed information flow sent across rc between FE3 and FE4. It is used to request user C's CIPL. Table 10 lists the elements within the INFO_REQ information flow.

Table 10 - Content of INFO_REQ information flow

Element	Request	Confirm	note
CIPL		M	21

NOTE 21

This element takes one of the values: 0, 1, 2, 3.

7.2.1.3.2 WARNING

WARNING is an unconfirmed information flow sent across rc between FE3 and FE4. It is used to inform FE4 that intrusion is impending. There are no elements within the WARNING information flow.

7.2.1.3.3 C_INTR

C_INTR is an unconfirmed information flow sent across rc between FE3 and FE4. It is used to inform FE4 that intrusion is in progress and user C is in conference type connection. There are no elements within the C_INTR information flow.

7.2.1.3.4 C_ISOLATED

C_ISOLATED is an unconfirmed information flow sent across rc between FE3 and FE4. It is used to inform FE4 that user C has been isolated. There are no elements within the C_ISOLATED information flow.

7.2.1.3.5 C_FORCED_REL

C_FORCED_REL is an unconfirmed information flow sent across rc between FE3 and FE4. It is used to inform FE4 that user C has been forced released. There are no elements within the C_FORCED_REL information flow.

7.2.1.3.6 INTR_TERM

INTR_TERM is an unconfirmed information flow sent across rc between FE3 to FE4. It is used to inform FE4 that the intrusion state has terminated. There are no elements within the INTR_TERM information flow.

7.2.1.4 Relationship rd

7.2.1.4.1 WARNING

WARNING is an unconfirmed information flow sent across rd between FE4 and FE5. It is used to inform FE5 that intrusion is impending. There are no elements within the WARNING information flow.

7.2.1.4.2 C_INTR

C_INTR is an unconfirmed information flow sent across rd between FE4 and FE5. It is used to inform FE5 that intrusion is in progress and user C is in conference type connection. There are no elements within the C_INTR information flow.

7.2.1.4.3 C_ISOLATED

C_ISOLATED is an unconfirmed information flow sent across rd between FE4 and FE5. It is used to inform FE5 that user C has been isolated. There are no elements within the C_ISOLATED information flow.

7.2.1.4.4 C_FORCED_REL

C_FORCED_REL is an unconfirmed information flow sent across rd between FE4 and FE5. It is used to inform FE5 that user C has been forced released. There are no elements within the C_FORCED_REL information flow.

7.2.1.4.5 INTR_TERM

INTR_TERM is an unconfirmed information flow sent across rd between FE4 to FE5. It is used to inform FE5 that the intrusion state has terminated. There are no elements within the INTR_TERM information flow.

7.2.2 Relationship of information flows to basic call information flows

7.2.2.1 Information flows over ra

INFORM request/indication shall be sent independently of a basic call information flow.

CI_INV request/indication shall be sent:

- together with basic call information flow r1_SETUP request/indication if this is sent at the same time;
- otherwise independently of a basic call information flow.

In the case of re-intrusion, CI_INV response/confirmation shall be sent independently of basic call information flow otherwise it shall be sent:

- if success:
  - together with basic call information flow r1_SETUP response/confirmation;
- if failure:
  - together with basic call information flow r1_REPORT request/indication if this is sent at the same time (e.g. if the called user enters an alerting phase);
  - with basic call information flow r1_SETUP response/confirmation if this is sent at the same time (e.g. if called user is busy but SS-CI not provided);
  - with basic call information flow r1_DISCONNECT request/indication if this is sent at the same time (e.g. if called user is busy but SS-CI not possible at the time of invocation).

ISOLATE request/indication shall be sent independently of a basic call information flow.

ISOLATE response/confirmation shall be sent independently of a basic call information flow.

FORCE_REL request/indication shall be sent independently of a basic call information flow.

FORCE_REL response/confirmation shall be sent independently of a basic call information flow.

EST_TERM request/indication shall be sent independently of a basic call information flow.

REQUEST_WOB request/indication shall be sent independently of a basic call information flow.

REQUEST_WOB response/confirmation shall be sent independently of a basic call information flow.

WARNING request/indication shall be sent independently of basic call information flow.

B_ALERTING request/indication shall be sent independently of a basic call information flow.

B_ANSWER request/indication shall be sent independently of a basic call information flow.

7.2.2.2 Information flows over rb

CI_ACT request/indication shall be sent in conjunction with basic call information flow r2_SETUP.

CI_AVAIL request/indication shall be sent independently of a basic call information flow.

CI_INV request/indication shall be sent:

- together with basic call information flow r2_SETUP request/indication if this is sent at the same time;
- otherwise independently of a basic call information flow.

In the case of re-intrusion, CI_INV response/confirmation shall be sent independently of basic call information flow otherwise it shall be sent:

- if success:
  - together with basic call information flow r2_SETUP response/confirmation;
- if failure:
  - together with basic call information flow r2_REPORT request/indication if this is sent at the same time (e.g. if the called user enters an alerting phase);
  - with basic call information flow r2_SETUP response/confirmation if this is sent at the same time (e.g. if called user is busy but SS-CI not provided);
  - with basic call information flow r2_RELEASE request/indication if this is sent at the same time (e.g. if called user is busy but SS-CI not possible at the time of invocation).

ISOLATE request/indication shall be sent independently of a basic call information flow.

ISOLATE response/confirmation shall be sent independently of a basic call information flow.

FORCE_REL request/indication shall be sent independently of a basic call information flow.

FORCE_REL response/confirmation shall be sent independently of a basic call information flow.

EST_TERM request/indication shall be sent independently of a basic call information flow.

REQUEST_WOB request/indication shall be sent independently of a basic call information flow.

REQUEST_WOB response/confirmation shall be sent independently of a basic call information flow.

WARNING request/indication shall be sent independently of basic call information flow.

B_ALERTING request/indication shall be sent independently of a basic call information flow.

B_ANSWER request/indication shall be sent independently of a basic call information flow.

7.2.2.3 Information flows over rc

INFO_REQ request/indication shall be sent independently of a basic call information flow.

INFO_REQ response/confirmation shall be sent independently of a basic call information flow.

WARNING request/indication shall be sent independently of basic call information flow.

C_INTR request/indication shall be sent independently of basic call information flow.

C_ISOLATED request/indication shall be sent independently of basic call information flow.

C_FORCED_REL request/indication shall be sent together with basic call information flow r2_RELEASE request/indication.

INTR_TERM request/indication shall be sent independently of basic call information flow.

7.2.2.4 Information flows over rd

WARNING request/indication shall be sent independently of basic call information flow.

C_INTR request/indication shall be sent independently of basic call information flow.

C_ISOLATED request/indication shall be sent independently of basic call information flow.

C_FORCED_REL request/indication shall be sent together with basic call information flow r1_/r3_DISCONNECT request/indication.

INTR_TERM request/indication shall be sent independently of basic call information flow.

7.2.2.5 Summary

Table 11 summarizes the relationships of the SS-CI information flows with those of the basic call.

Table 11 - Relationship of the SS-CI information flows with the basic call

Information flow			Independent of basic call flow	With basic flow	Basic call flows
ra	INFORM	request	yes	no	
	CI_INV	request	yes	yes	r1_SETUP req/ind
	CI_INV	confirm	yes	yes	r1_REPORT req/ind r1_SETUP resp/conf r1_DISCONNECT req/ind
	ISOLATE	request	yes	no	
	ISOLATE	confirm	yes	no	
	FORCE_REL	request	yes	no	
	FORCE_REL	confirm	yes	no	
	EST_TERM	request	yes	no	
	REQUEST_WOB	request	yes	no	
	REQUEST_WOB	confirm	yes	no	
	WARNING	request	yes	no	
	B_ALERTING	request	yes	no	
	B_ANSWER	request	yes	no	
rb	CI_AVAIL	request	yes	no	
	CI_ACT	request	no	yes	r2_SETUP req/ind
	CI_INV	request	yes	yes	r2_SETUP req/ind
	CI_INV	confirm	yes	no	r2_REPORT req/ind r2_SETUP resp/conf r2_RELEASE req/ind
	ISOLATE	request	yes	no	
	ISOLATE	confirm	yes	no	
	FORCE_REL	request	yes	no	
	FORCE_REL	confirm	yes	no	
	EST_TERM	request	yes	no	
	REQUEST_WOB	request	yes	no	
	REQUEST_WOB	confirm	yes	no	
	WARNING	request	yes	no	
	B_ALERTING	request	yes	no	
	B_ANSWER	request	yes	no	
rc	INFO_REQ	request	yes	no	
	INFO_REQ	confirm	yes	no	
	WARNING	request	yes	no	
	C_INTR	request	yes	no	
	C_ISOLATE	request	yes	no	
	C_FORCED_REL	request	no	yes	r2_RELEASE req/ind
	INTR_TERM	request	yes	no	
rd	WARNING	request	yes	no	
	C_INTR	request	yes	no	
	C_ISOLATED	request	yes	no	
	C_FORCED_REL	request	no	yes	r1_/r3_DISCONNECT req/ind
	INTR_TERM	request	yes	no	

7.2.3 Information flow sequences

A stage 3 standard for SS-CI shall provide signalling procedures in support of the information flow sequences specified below. In addition, signalling procedures should be provided to cover other sequences arising from error situations, interactions with basic call, interactions with other supplementary services, different topologies etc..

In the figures, SS-CI information flows are represented by solid arrows and basic call information flows are represented by broken arrows. A dashed elipse embracing two information flows indicates that the two information flows occur simultaneously. Within a column representing a SS-CI functional entity, the numbers refer to functional entity actions listed in 7.3.

The timers used through all the figures:

T1 = Consultation timer;

T2 = Time to intrusion.

7.2.3.1 Normal operation, consultation, path retention

Figure 4 shows the information flow sequence for a successful intrusion attempt, using consultation and path retention. In this particular sequence an impending intrusion warning notification is given to user B and user C and after a delay a conference type connection is formed.

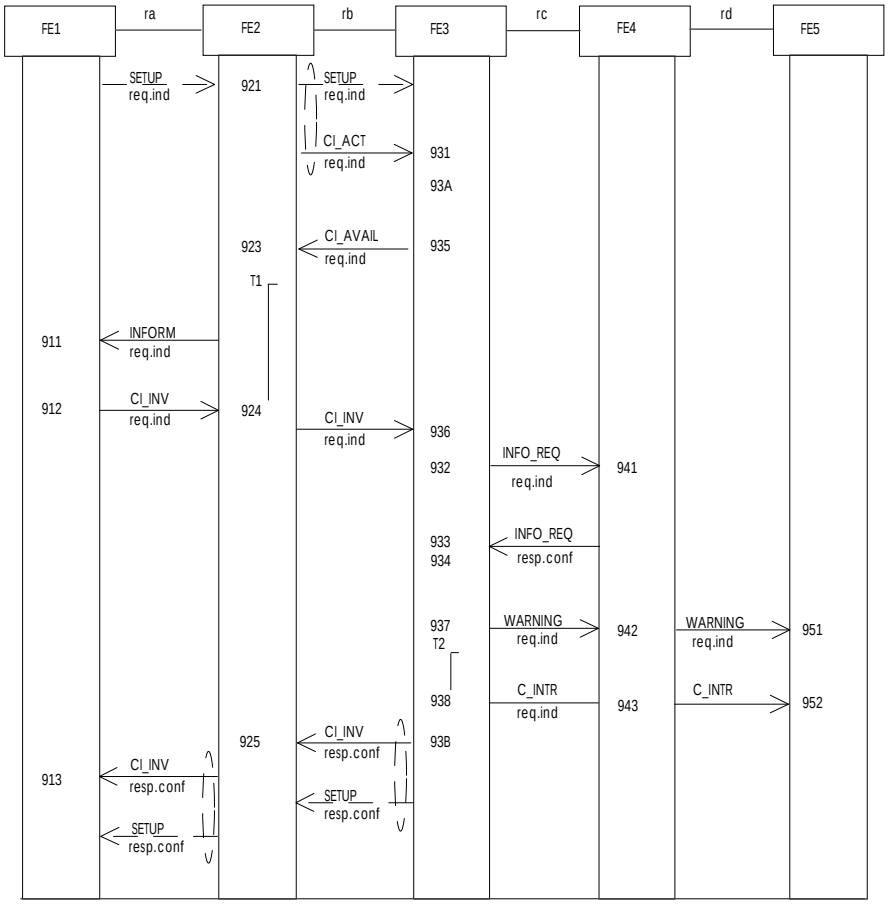

Figure 4 - Information flow sequence for SS-CI, normal operation, consultation, path retention

7.2.3.2 Normal operation, consultation, non-retention

Figure 5 shows the information flow sequence for a successful intrusion attempt using consultation and non-retention. In this particular sequence an impending intrusion warning notification is given to user B and user C and after a delay a conference type connection is formed.

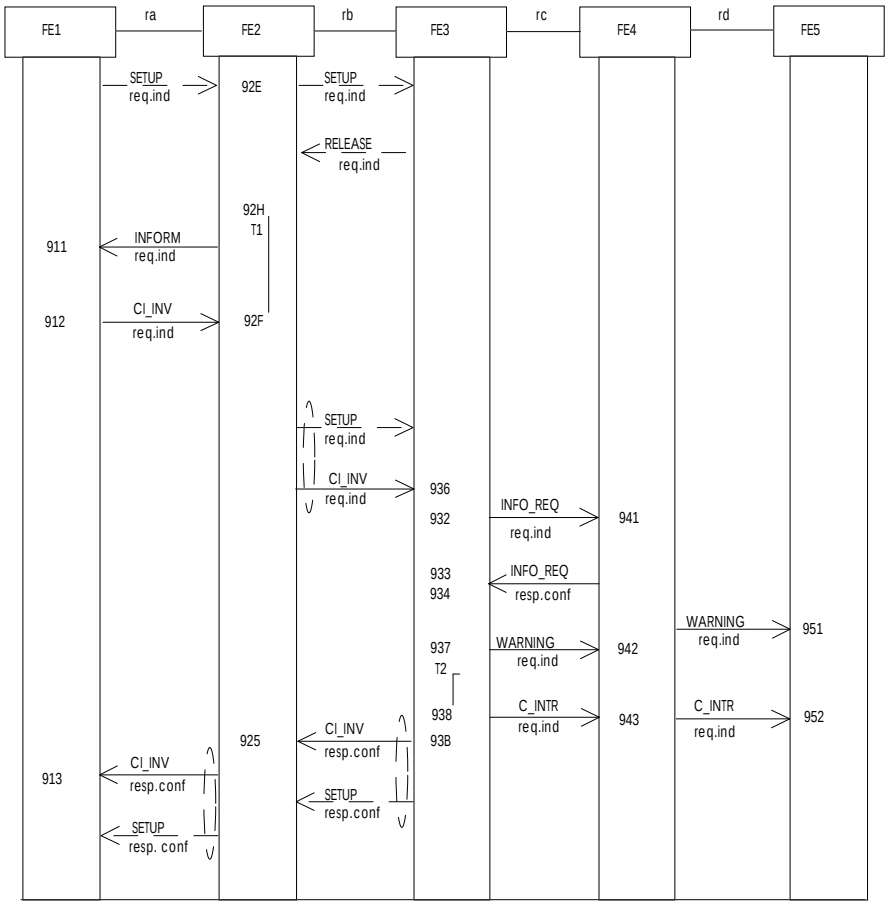

Figure 5 - Information flow sequence for SS-CI, normal operation, consultation, non-retention

7.2.3.3 Normal operation, immediate invocation, non-retention

Figure 6 shows the information flow sequence for a successful intrusion attempt using immediate invocation and non-retention. In this particular sequence an impending intrusion warning notification is given to user B and user C and after a delay a conference type connection is formed.

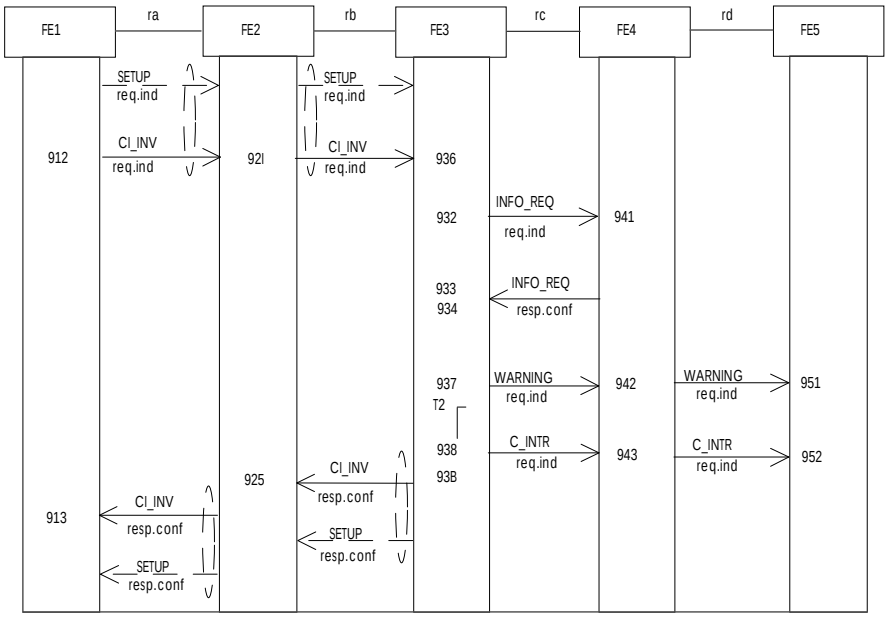

Figure 6 - Information flow sequence for SS-CI, normal operation, immediate invocation, non-retention

7.2.3.4 Normal operation, immediate invocation, path retention

Figure 7 shows the information flow sequence for a successful intrusion attempt, using immediate invocation and path retention. In this particular sequence an impending intrusion warning notification is given to user B and user C and after a delay a conference type connection is formed.

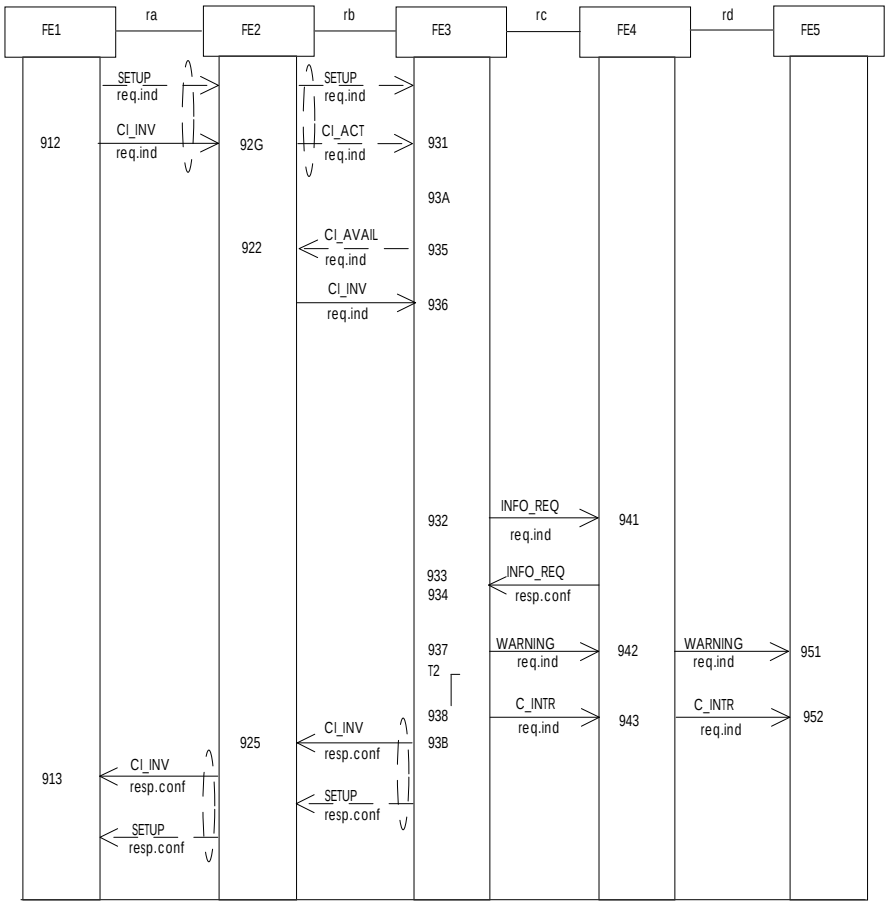

Figure 7 - Information flow sequence for SS-CI, normal operation, immediate invocation, path retention

7.2.3.5 Normal operation, immediate invocation, path retention, user C isolated at intrusion

Figure 8 shows the information flow sequence for a successful intrusion attempt using immediate invocation and path retention. In this particular sequence an impending intrusion warning notification is given to user B and user C and after a delay user C is isolated and served user is connected to user B. During the intrusion state the intruding call is released, the isolation of user C is terminated, user C and user B are reconnected.

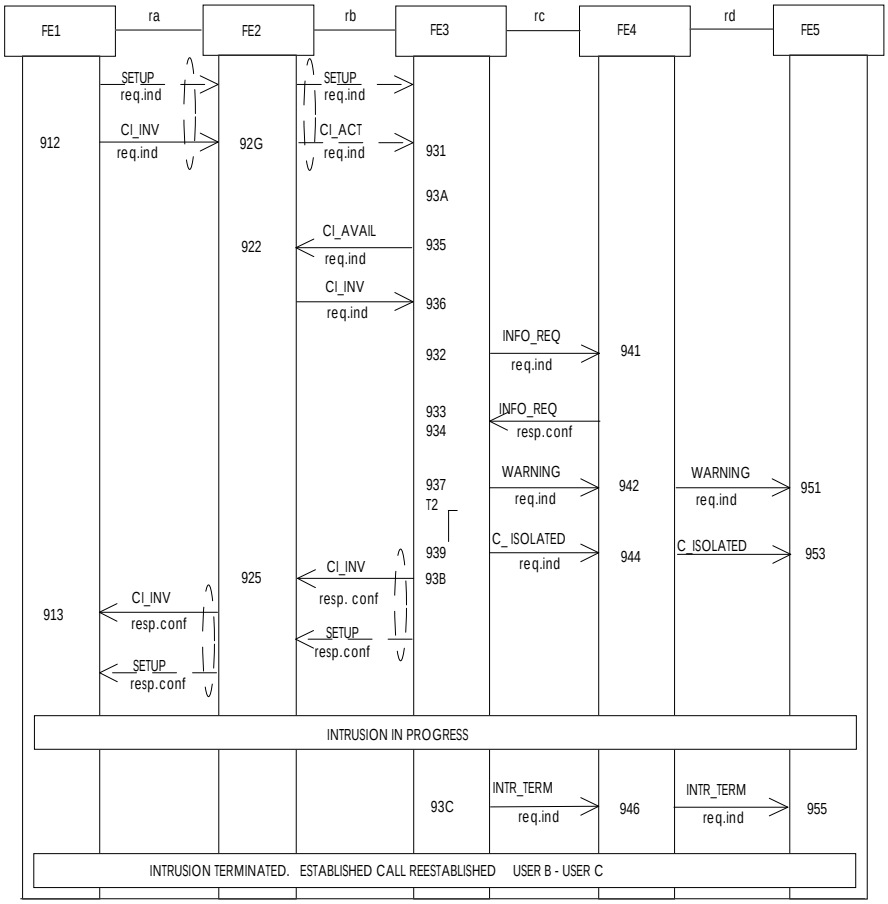

Figure 8 - Information flow sequence for SS-CI, normal operation, immediate invocation, path retention, user C is isolated

7.2.3.6 Normal operation, immediate invocation, immediate intrusion, non-retention

Figure 9 shows the information flow sequence for a successful intrusion attempt using immediate invocation and non-retention. In this particular sequence a conference type connection is formed immediately without an impending intrusion warning notification.

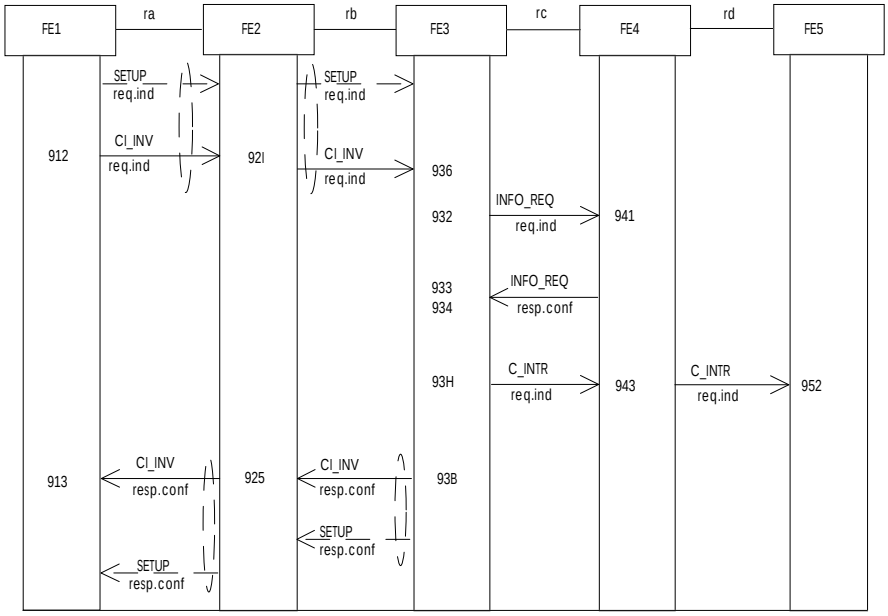

Figure 9 - Information flow sequence for SS-CI, normal operation, immediate invocation, immediate intrusion, non-retention

7.2.3.7 Normal operation, immediate invocation, path retention

Figure 10 shows the information flow sequence for a successful intrusion attempt, using immediate invocation and path retention. In this particular sequence an impending intrusion warning notification is given to served user, user B and user C and after a delay a conference type connection is formed.

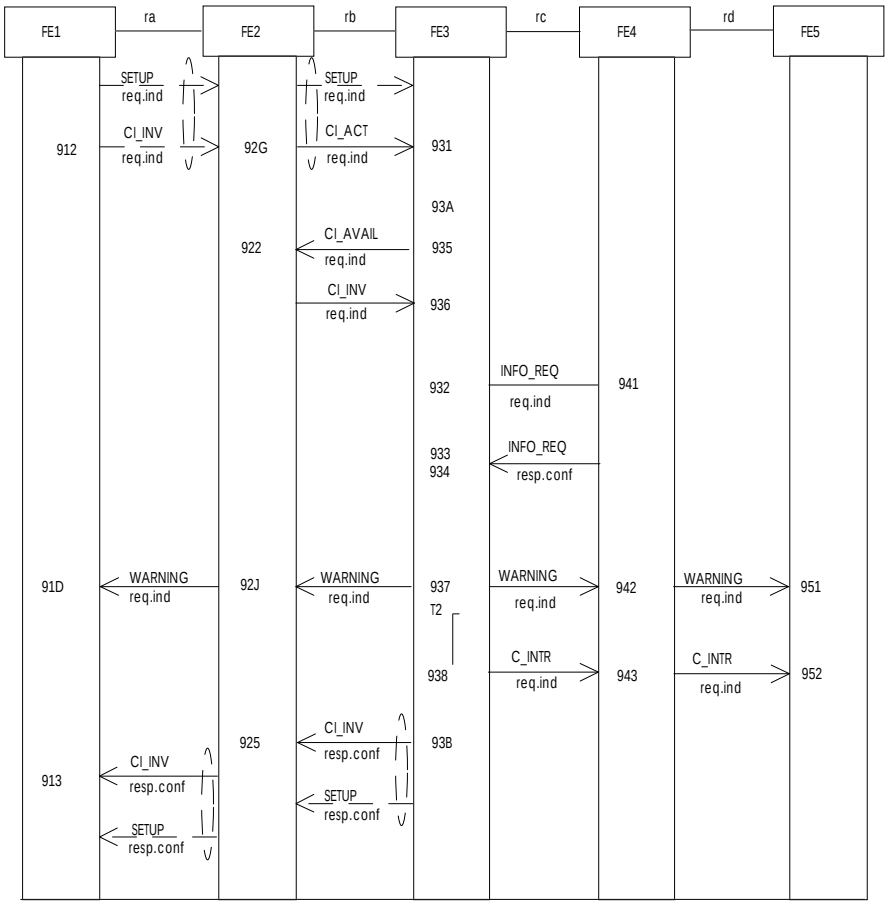

Figure 10 - Information flow sequence for SS-CI, normal operation, immediate invocation, path retention

7.2.3.8 Normal operation, isolation of user C

Figure 11 below shows the information flow sequence for a successful isolation on request from served user, after intrusion has been accepted and a conference type connection has been formed.

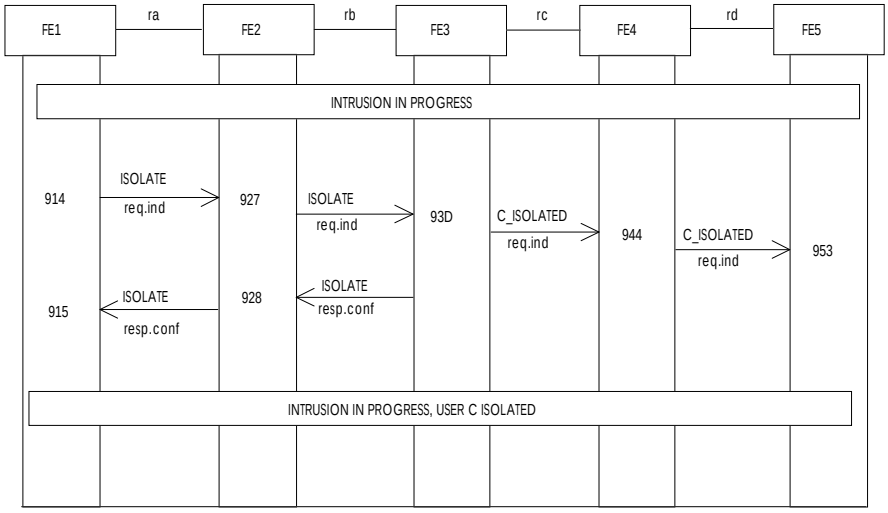

Figure 11 - Information flow sequence for SS-CI, normal operation, isolation of user C

7.2.3.9 Normal operation, Forced Release of user C

Figure 12 below shows the information flow sequence for a successful forced release of user C.

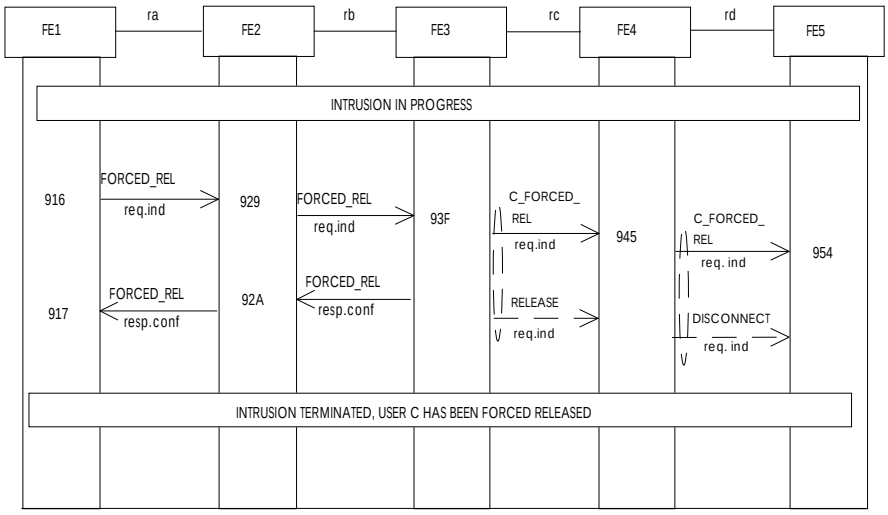

Figure 12 - Information flow sequence for SS-CI, normal operation, forced release of user C

7.2.3.10 Normal operation, user B or user C releases the established call

Figure 13 below shows the information flow sequence when the established call is released by user B or user C during the intrusion state.

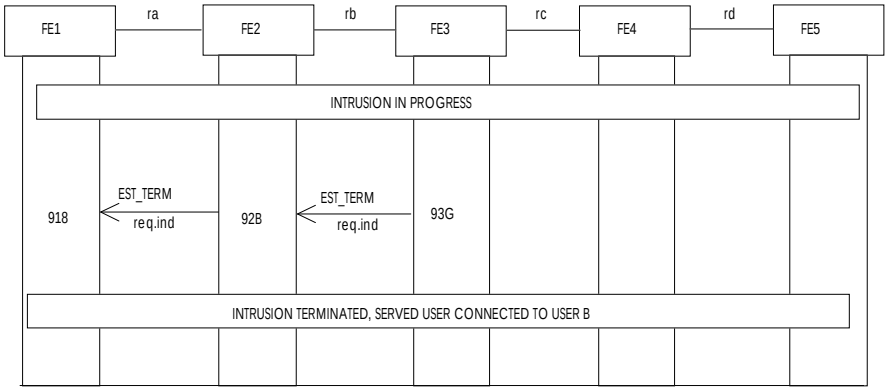

Figure 13 - Information flow sequence for SS-CI, user B or user C releases the established call

7.2.3.11 Normal operation, release of the intruding call

Figure 14 below shows the information flow sequence when the intruding call is released by served user or user B during the intrusion state.

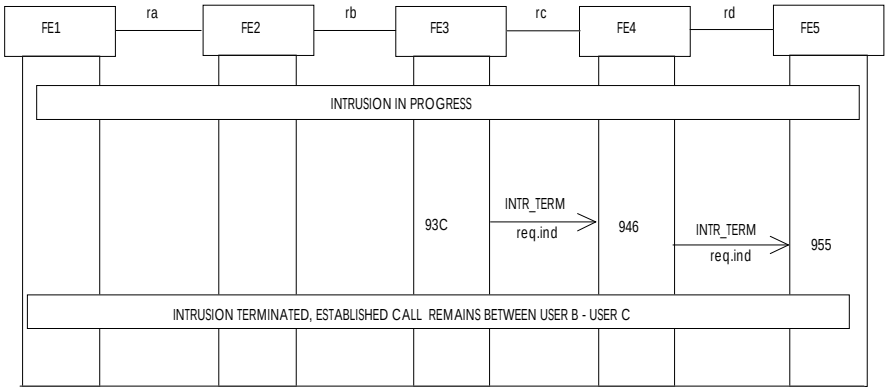

Figure 14 - Information flow sequence for SS-CI, intruding call released during the intrusion state

7.2.3.12 Normal operation, WOB requested

Figure 15 below shows the information flow sequence for a successful WOB request made by the served user. In this particular sequence user B subsequently starts alerting and answers the call.

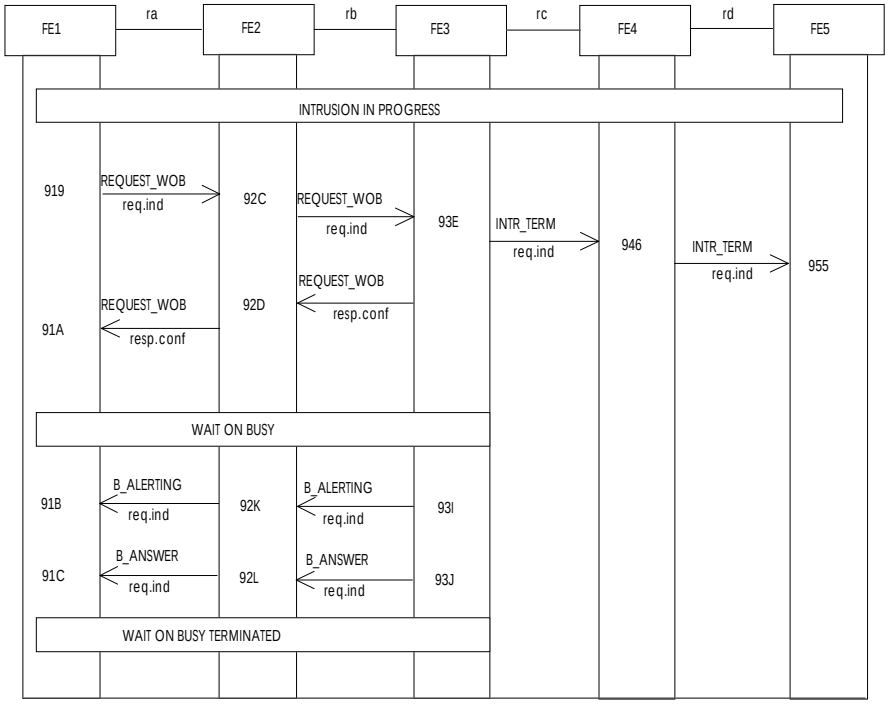

Figure 15 - Information flow sequence for SS-CI, normal operation, WOB requested

7.2.3.13 Normal operation, new intrusion during WOB

Figure 16 below shows the information flow sequence for a successful new intrusion requested during the WOB state. In this particular sequence an impending intrusion warning notification is given to user B and user C and after a delay a conference type connection is formed.

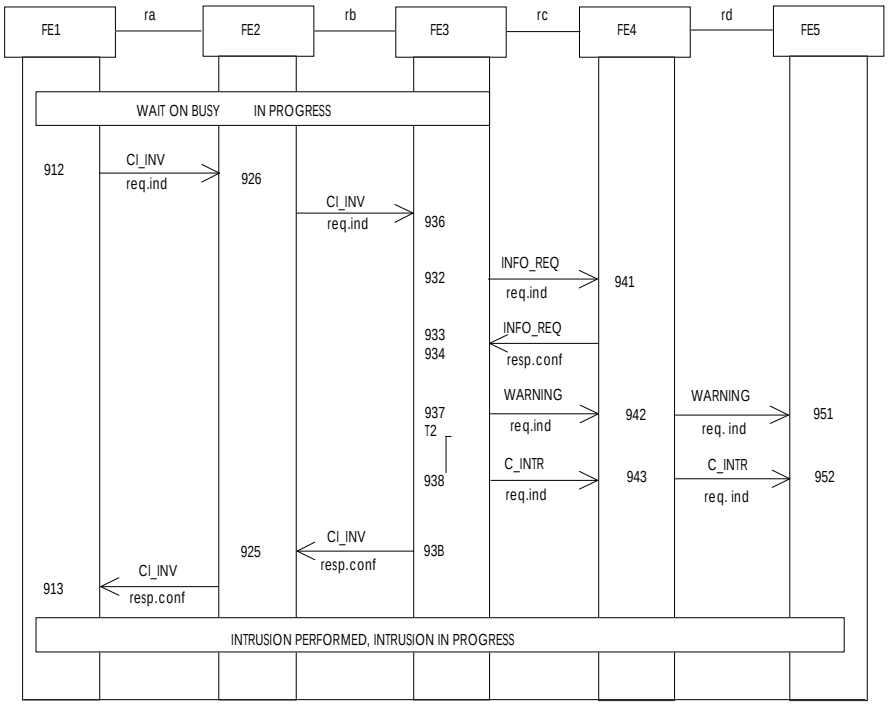

Figure 16 - Information flow sequence for SS-CI, normal operation, new intrusion during the WOB state is requested

7.3 Functional Entity actions (FEAs)

The following FE actions shall occur at the points indicated in the figures of 7.2.3.

7.3.1 Actions of FE1

911: The FE shall receive an INFORM req.ind information flow and inform the served user that the called user is busy and that intrusion may be possible.

912: The FE shall receive the user's request for call intrusion and send the CI_INV req.ind to FE2.

913: The FE shall receive the CI_INV resp.conf information flow from FE2 and inform the served user of the result of the request for intrusion.

914: In response to a request from the served user to isolate user C, the FE shall send the ISOLATE req.ind information flow to FE2.

915: The FE shall receive the ISOLATE resp.conf information flow from FE2 and inform the served user of the result of the request.

916: In response to a forced release request from the served user, the FE shall send the FORCED_REL information flow to FE2.

917: The FE shall receive the FORCED_REL resp.conf information flow from FE2 and indicate the result to the served user.

918: The FE shall receive the EST_TERM req.ind information flow from FE2. The FE shall inform the served user that the established call has been released.

919: In response to a WOB request from the served user, the FE shall send the REQUEST_WOB req.ind information flow to FE2.

91A: The FE shall receive the REQUEST_WOB resp.conf information flow from FE2 and indicate the result to the served user.

91B: The FE shall receive the B_ALERTING req.ind information flow from FE2 and inform the served user.

91C: The FE shall receive the B_ANSWER req.ind information flow from FE2 and inform the served user.

91D: The FE shall receive the WARNING req.ind information flow from FE2 and inform the served user.

7.3.2 Actions of FE2

921: The FE shall check whether the user is provided with SS-CI using the consultation method and, if provided, send a CI_ACT req.ind information flow together with basic call SETUP information flow to FE3.

922: The FE shall receive the CI_AVAIL req.ind information flow from FE3 and send the CI_INV req.ind information flow to FE3.

923: The FE shall receive the CI_AVAIL req.ind information flow from FE3. The FE shall start timer T1 (consultation timer) and store the call information for the duration of T1. The FE shall send an INFORM req.ind information flow to FE1.

924: The FE shall receive the CI_INV req.ind information flow from FE1. The FE shall stop the timer T1 and send CI_INV req.ind information flow to FE3.

925: The FE shall receive the CI_INV resp.conf information flow from FE3 and send the CI_INV resp.conf information flow to FE1.

926: The FE shall receive the CI_INV req.ind information flow from FE1 and send the CI_INV req.ind information flow to FE3.

927: The FE shall receive the ISOLATE req.ind information flow from FE1. The FE shall check whether the user is provided with isolation capability. If provided, the FE shall send the ISOLATE req.ind information flow to FE3.

928: The FE shall receive the ISOLATE resp.conf information flow from FE3 and send the ISOLATE resp.conf information flow to FE1.

929: The FE shall receive the FORCE_REL req.ind information flow from FE1, check whether the user is provided with forced release, and send the FORCE_REL req.ind information flow to FE3.

92A: The FE shall receive the FORCE_REL resp.conf information flow from FE3 and send the FORCE_REL resp.conf information flow to FE1.

92B: The FE shall receive the EST_TERM req.ind information flow from FE3 and send the EST_TERM req.ind information flow to FE1.

92C: The FE shall receive the REQUEST_WOB req.ind information flow from FE1, check whether the user is provided with WOB, and send the REQUEST_WOB req.ind information flow to FE3.

92D: The FE shall receive the REQUEST_WOB resp.conf information flow from FE3 and send the REQUEST_WOB resp.conf information flow to FE1.

92E: All information in the basic call SETUP information flow shall be retained.

92F: The FE shall receive the CI_INV req.ind information flow. The FE shall stop the timer T1 (consultation). The basic call process shall be stimulated to setup a new call with the information retained from the original setup. A CI_INV req.ind information flow shall be sent, together with the basic call information flow SETUP req.ind to FE3.

92G: The FE shall receive the CI_INV req.ind information flow from FE1, check whether the user is provided with SS-CI using immediate invocation method, and send the CI_ACT req.ind information flow to FE3 together with the basic call information flow SETUP req.ind.

92H: The FE shall start a timer T1 (consultation timer) and store the call information for the duration of T1. The FE shall send the INFORM req.ind information flow to FE1 informing FE1 that called user is busy and intrusion may be possible.

92I: The FE shall receive the CI_INV req.ind information flow from FE1 and check whether the user is provided with SS-CI using the immediate invocation method. If provided, the FE shall send the CI_INV req.ind information flow to FE3.

92J: The FE shall receive the WARNING req.ind information flow from FE3 and send the WARNING req.ind information flow to FE1.

92K: The FE shall receive the B_ALERTING req.ind information flow from FE3 and send the B_ALERTING req.ind information flow to FE1.

92L: The FE shall receive the B_ANSWER req.ind information flow from FE3 and send the B_ANSWER req.ind information flow to FE1.

7.3.3 Actions of FE3

931: The FE shall receive the CI_ACT req.ind information flow from FE2.

932: The FE shall send the INFO_REQ req.ind information flow to FE4.

933: The FE shall receive the INFO_REQ resp.conf information flow from FE4.

934: The FE shall compare the CICL with the CIPLs for user B and user C and determine whether intrusion is allowed or not.

935: If intrusion may be possible, the FE shall inform FE2 by sending the CI_AVAIL req.ind information flow. If intrusion is not possible, normal basic call release procedure shall take place.

936: The FE shall receive the information flow CI_INV req.ind from FE2.

937: The FE shall send the WARNING req.ind information flow to FE4. The FE may also send the optional WARNING req.ind information flow to FE2. The FE shall start timer T2. The FE shall inform user B. The FE may also apply an in-band tone or announcement to user B and user C.

938: The FE shall determine that a conference type connection is to be formed. When the timer T2 has elapsed, the FE shall establish the intrusion connection by joining the served user, user B and user C in a conference type connection. The FE shall send the C_INTR req.ind information flow to FE4. The FE shall inform user B that intrusion is in progress. The FE may also apply an in-band indication to connected users during the intrusion state.

939: The FE shall determine that user C is to be automatically isolated. The FE shall isolate user C when timer T2 elapses. The FE shall send the C_ISOLATED req.ind information flow to FE4. The FE shall inform user B

that user C has been isolated. The FE shall set up a connection between served user and user B.

93A: The FE shall compare the CICL value with the CIPL value for user B and determine whether intrusion is allowed or not.

93B: The FE shall send the CI_INV resp.conf information flow to FE2.

93C: If the intruding call is released, the FE shall send an INTR_TERM req.ind information flow to FE4. The FE terminates the intrusion. The established call shall revert back to the state that existed before the intrusion took place. User B shall be informed that intrusion has terminated.

93D: The FE shall receive the ISOLATE req.ind information flow from FE2. The FE shall send the C_ISOLATED req.ind information flow to FE4. The FE shall isolate user C from the conference type connection. The FE shall inform user B regarding the isolation. The FE shall send an ISOLATE resp.conf information flow to FE2, with the result of the requested isolation. The FE shall remove the in-band warning indication, if applicable.

93E: The FE shall receive the REQUEST_WOB req.ind information flow from FE2. The FE shall send the INTR_TERM req.ind information flow to FE4. The FE shall make the established call revert back to the state that existed before the intrusion occurred. User B shall be informed that the intrusion is terminated, and that a WOB state applies. The FE shall send the REQUEST_WOB resp.conf information flow to FE2.

93F: The FE shall receive the FORCE_REL req.ind information flow from FE2. The FE shall initiate a disconnect and release of the established call. The FE shall send the C_FORCED_REL req.ind information flow to FE4. The FE shall inform user B of the forced release of user C. The FE shall send the FORCE_REL resp.conf information flow to FE2. The FE shall remove the in-band warning indication tone, if applicable.

93G: If user B or user C releases the established call during the intrusion state (handled by basic call procedures) the FE shall send a EST_TERM req.ind information flow to FE2. The FE makes the intruding call an ordinary call between served user and user B. The intrusion state is terminated.

93H: The FE shall establish the intrusion connection by joining the served user, user B and user C in a conference type connection. The FE shall send the C_INTR req.ind information flow to FE4. The FE shall inform user B that intrusion is in progress. The FE may also apply an in-band indication to connected users during the intrusion state.

93I: If user B makes available resources and starts alerting, the FE shall send the B_ALERTING req.ind information flow to FE2.

93J: If user B answers the waiting call during the WOB state, the FE shall send the B_ANSWER req.ind information flow to FE2.

7.3.4 Actions of FE4

941: The FE shall receive the INFO_REQ req.ind information flow from FE3 and send the INFO_REQ resp.conf information flow to FE3.

942: The FE shall receive the WARNING req.ind information flow from FE3 and send the WARNING req.ind information flow to FE5.

943: The FE shall receive the C_INTR req.ind information flow from FE3 and send the C_INTR req.ind information flow to FE5.

944: The FE shall receive the C_ISOLATED req.ind information flow from FE3 and send the C_ISOLATED req.ind information to FE5.

945: The FE shall receive the C_FORCED_REL req.ind information flow from FE3 and send the C_FORCED_REL req.ind information flow to FE5.

946: The FE shall receive the INTR_TERM req.ind information flow from FE3 and send the INTR_TERM req.ind information flow to FE5.

7.3.5 Actions of FE5

951: The FE shall receive the WARNING req.ind information flow. The FE shall provide the user with the impending intrusion warning indication.

952: The FE shall receive the C_INTR req.ind information flow from FE4. The FE shall inform the user.

953: The FE shall receive the C_ISOLATED req.ind information flow from FE4. The FE shall inform the user.

954: The FE shall receive the C_FORCED_REL req.ind information flow from FE4. The FE shall inform the user.

955: The FE shall receive the INTR_TERM req.ind information flow from FE4. The FE shall inform the user.

7.4 Functional Entity behaviour

The FE behaviours shown below are intended to illustrate typical FE behaviour in terms of information flows sent and received.

The behaviour of each FE is shown using the Specification and Description Language (SDL) defined in CCITT Rec. Z.100 (1988).

7.4.1 Behaviour of FE1

Figure 17 shows the normal behaviour of FE1. Input signals from the left and output signals to the left represent primitives from and to the served user. Input signals from the right and output signals to the right represent information flows from and to FE2 and input signals from the collocated CCA.

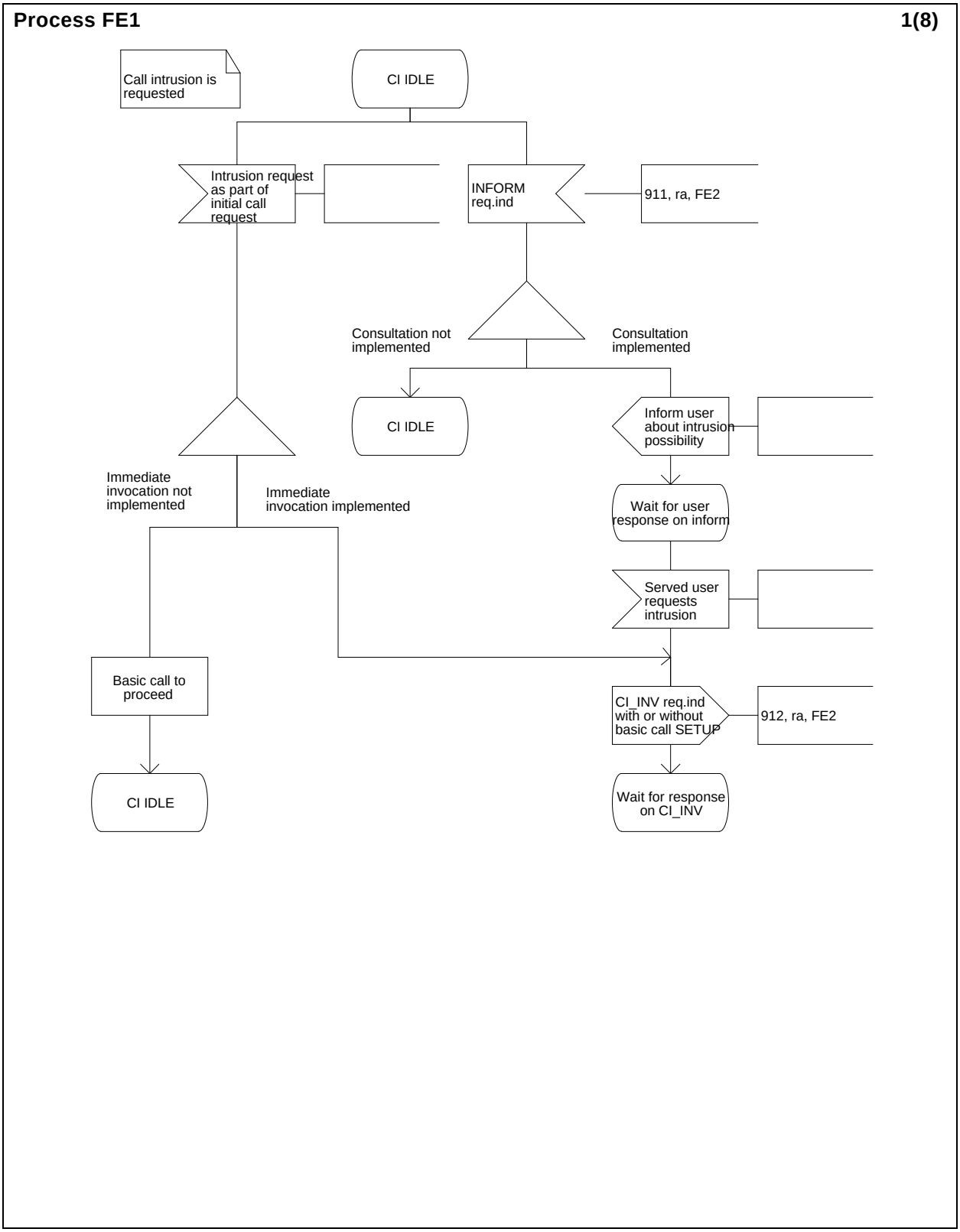

Figure 17 (sheet 1 of 8) - SS-CI, SDL for FE1

Process FE1 **2(8)**

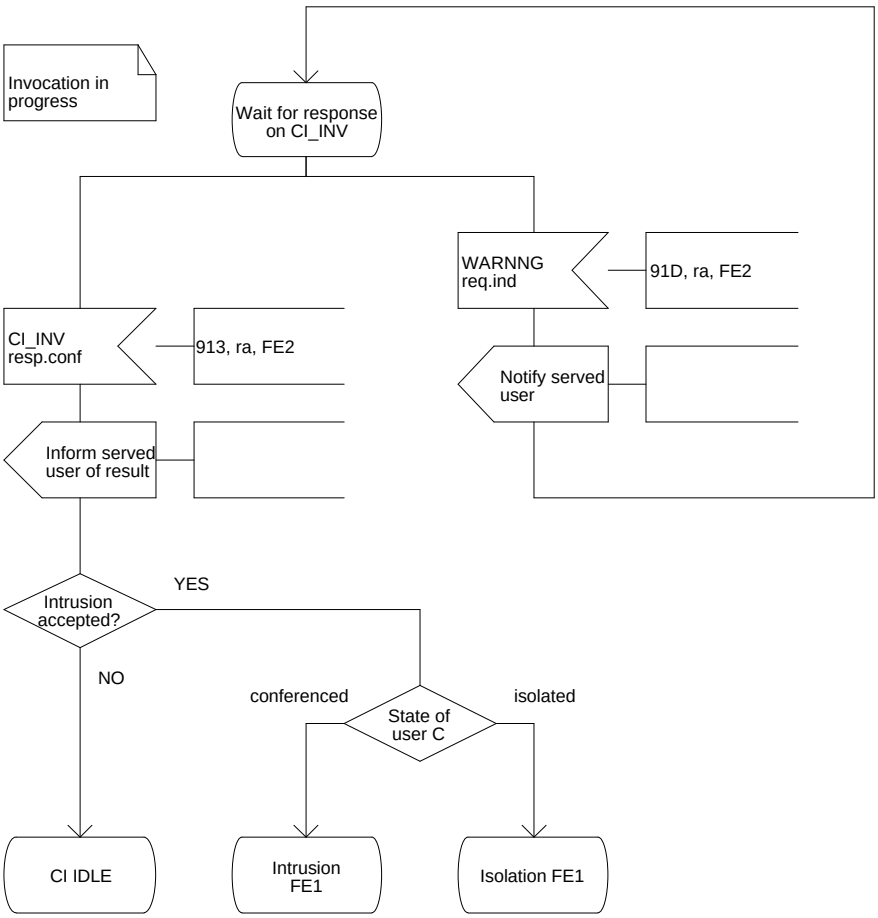

Figure 17 (sheet 2 of 8) - SS-CI, SDL for FE1

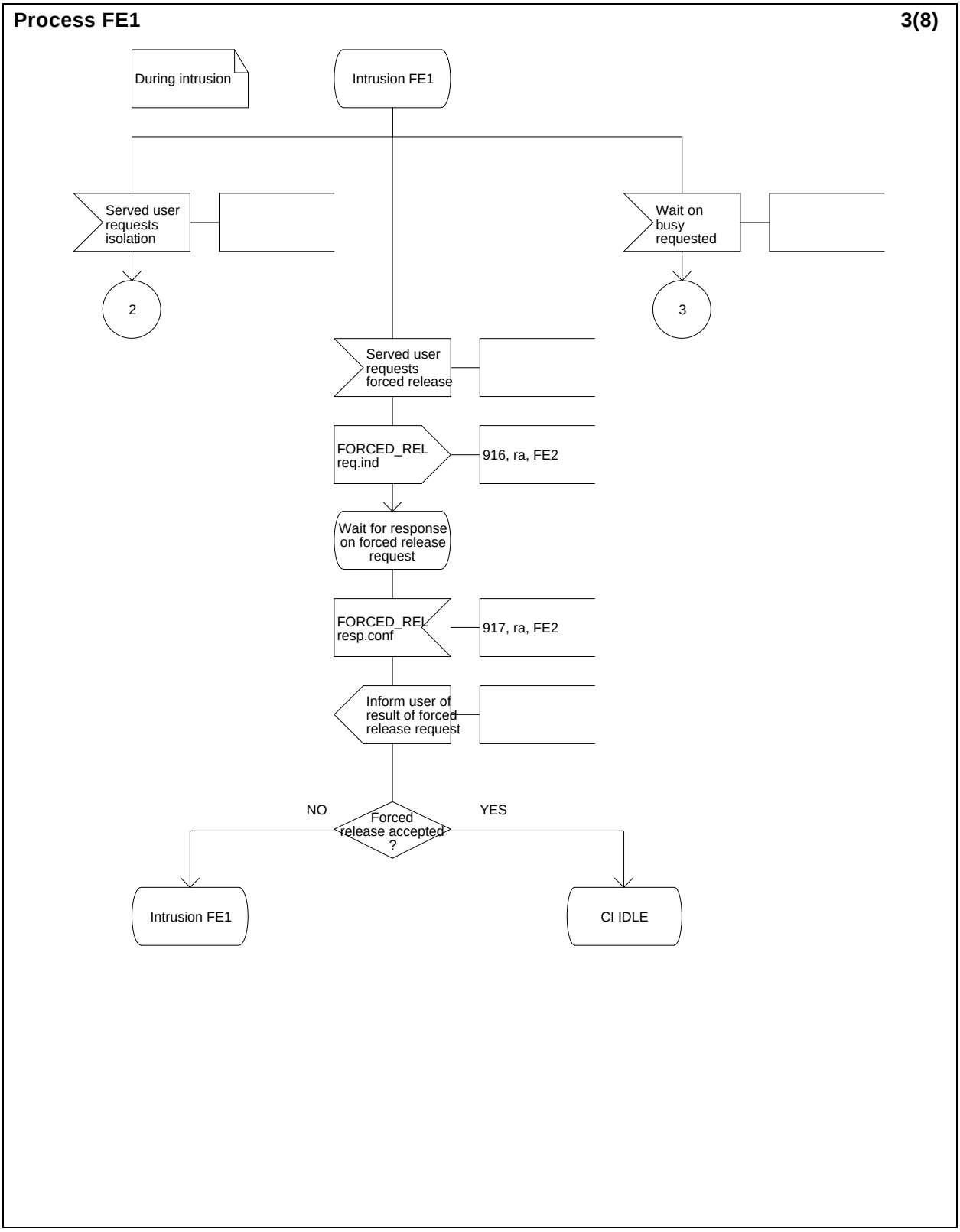

Figure 17 (sheet 3 of 8) - SS-CI, SDL for FE1

Process FE1 **4(8)**

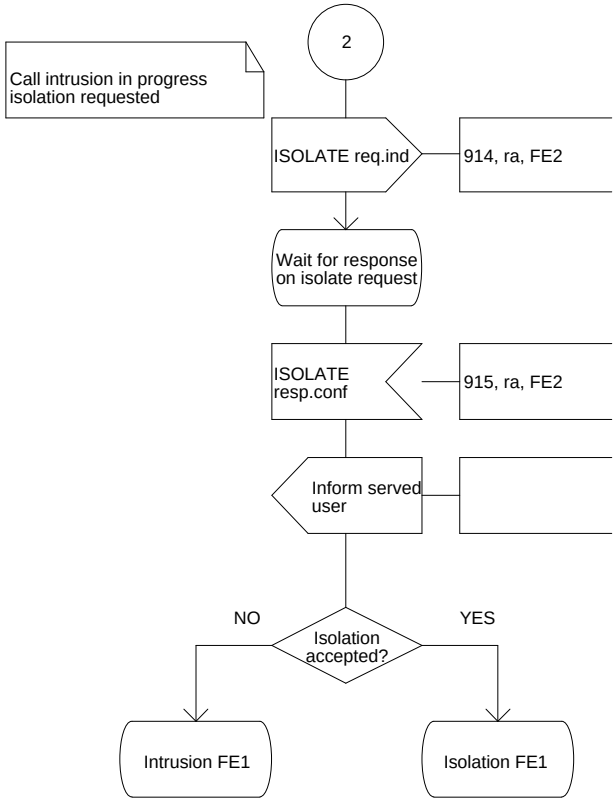

Figure 17 (sheet 4 of 8) - SS-CI, SDL for FE1

Process FE1 **5(8)**

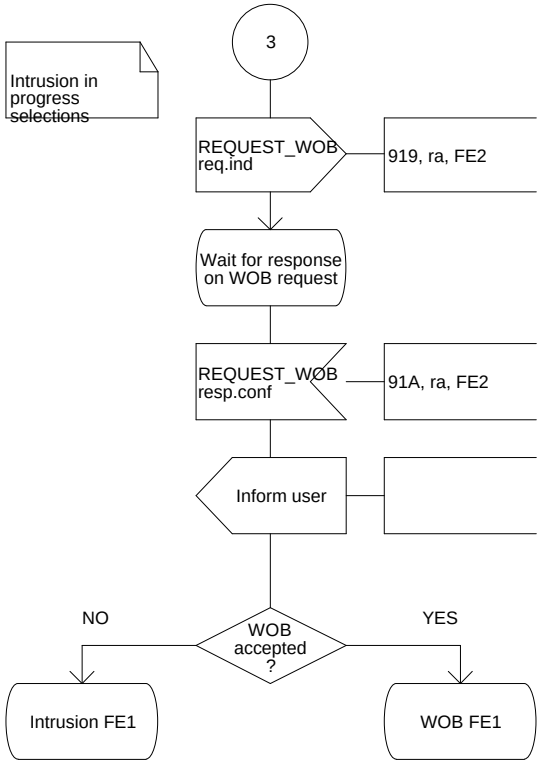

Figure 17 (sheet 5 of 8) - SS-CI, SDL for FE1

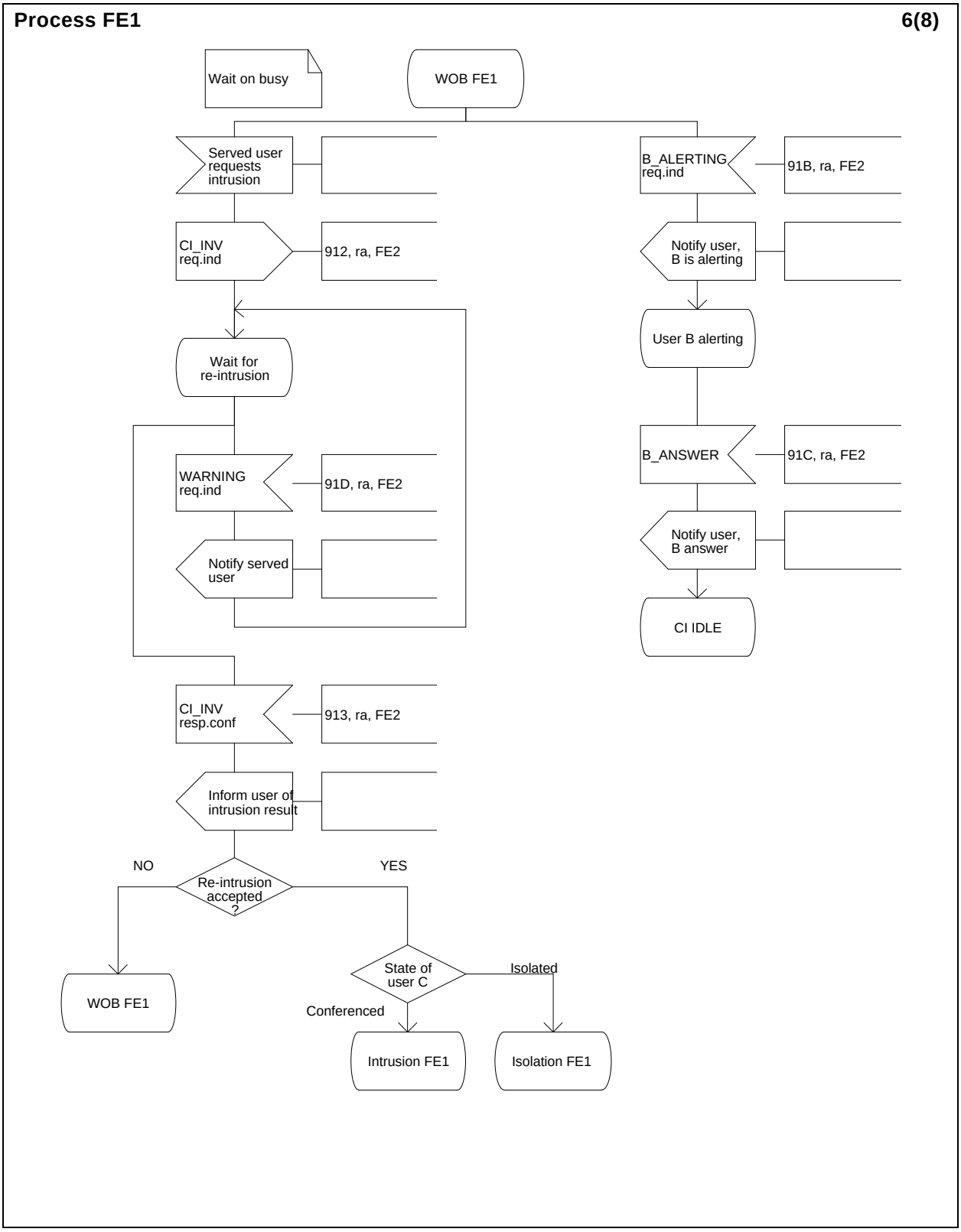

Figure 17 (sheet 6 of 8) - SS-CI, SDL for FE1

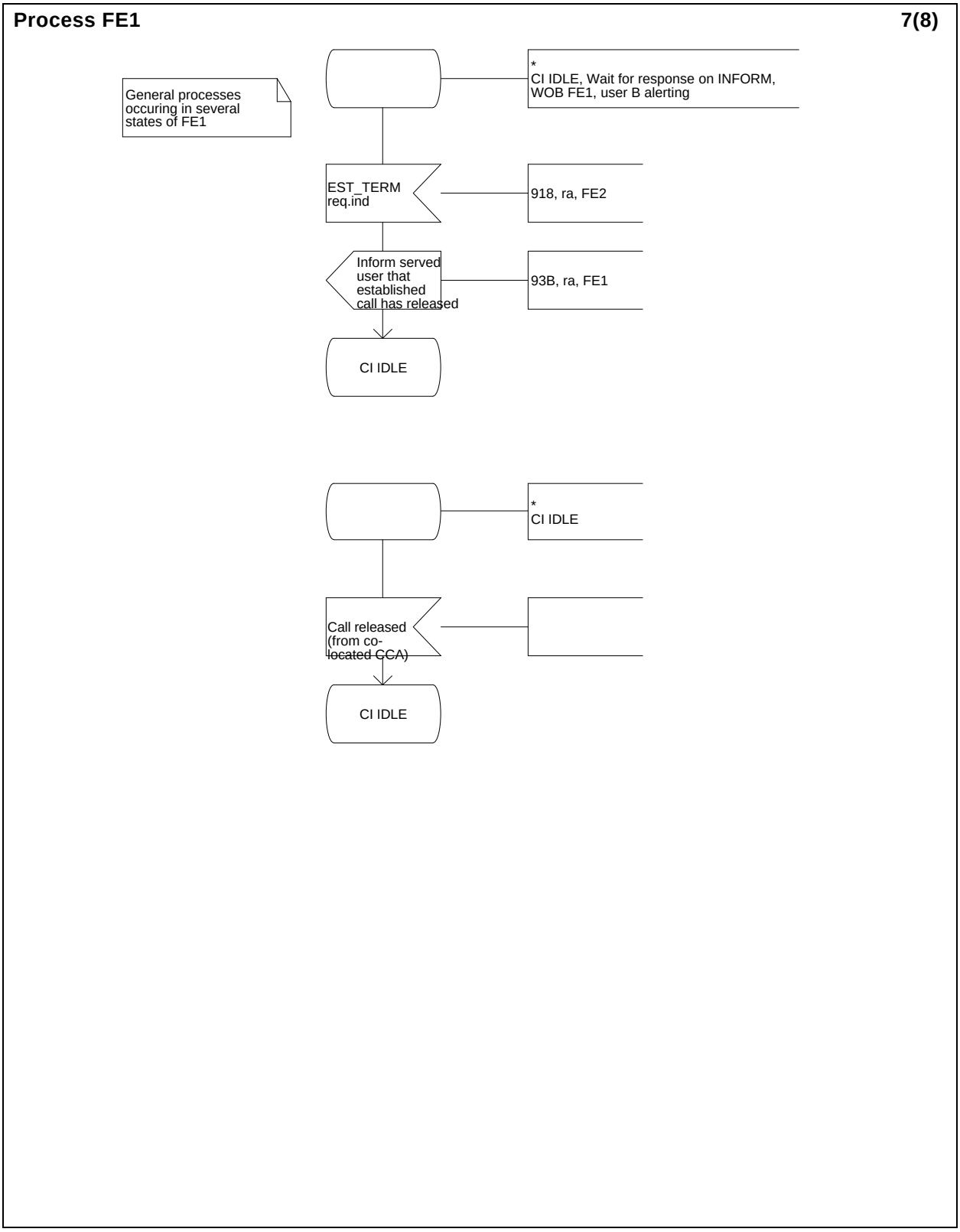

Figure 17 (sheet 7 of 8) - SS-CI, SDL for FE1

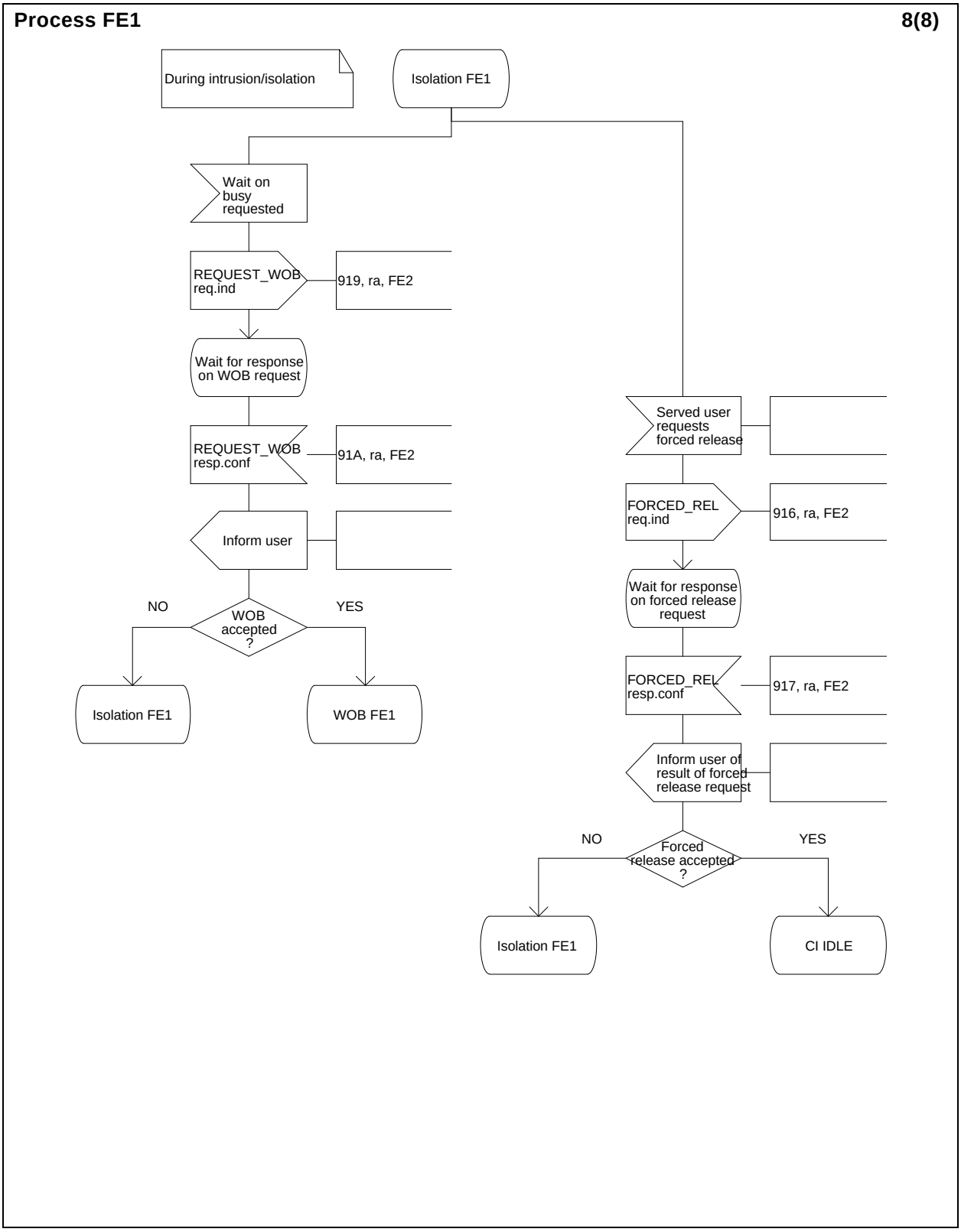

Figure 17 (sheet 8 of 8) - SS-CI, SDL for FE1

7.4.2 Behaviour of FE2

Figure 18 shows the normal behaviour of FE2. Input signals from the left and output signals to the left represent primitives from and to FE1. Input signals from and output signals to the right represent information flows from and to FE3 and input signals from the collocated CC.

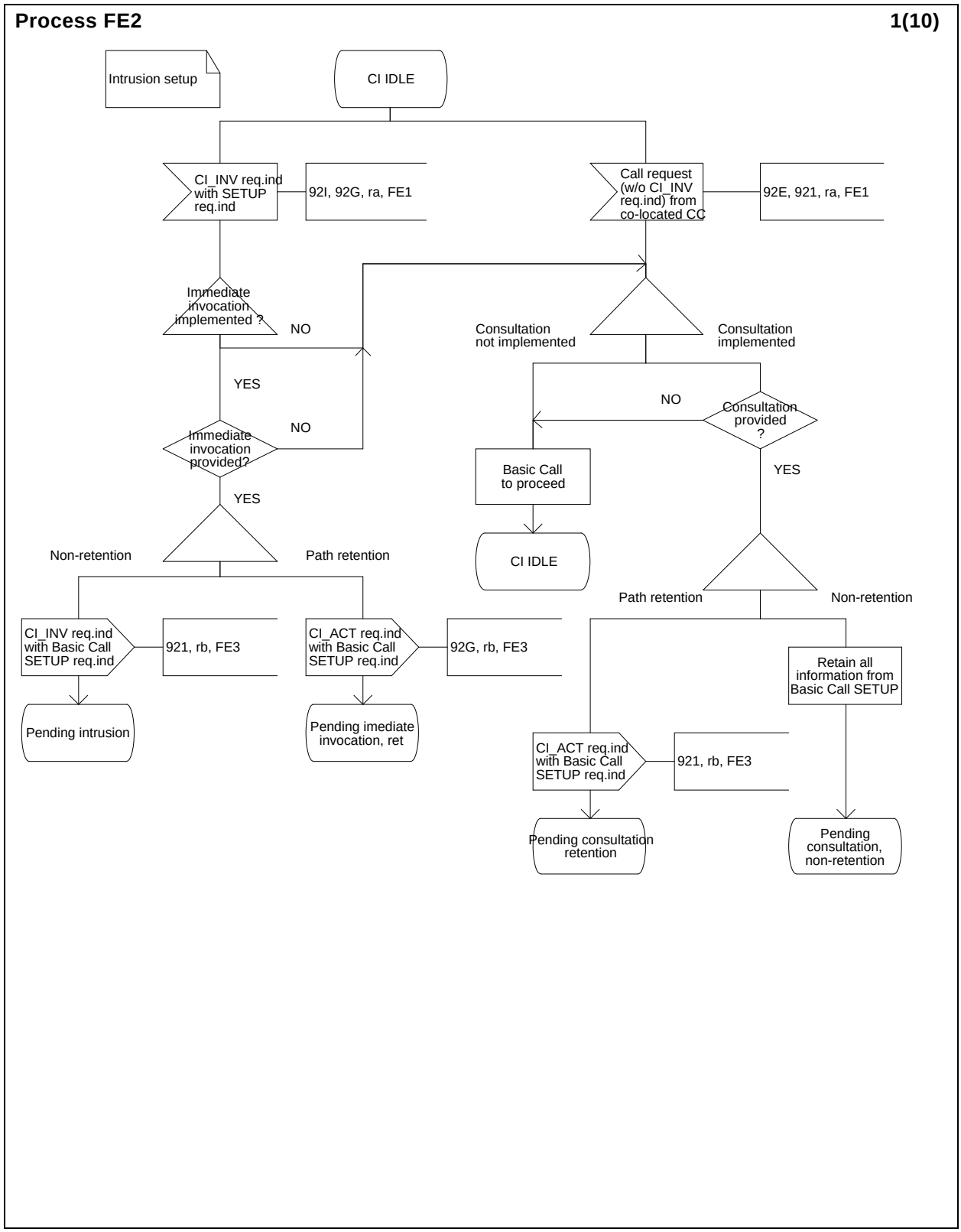

Figure 18 (sheet 1 of 10) - SS-CI, SDL for FE2

Process FE2 **2(10)**

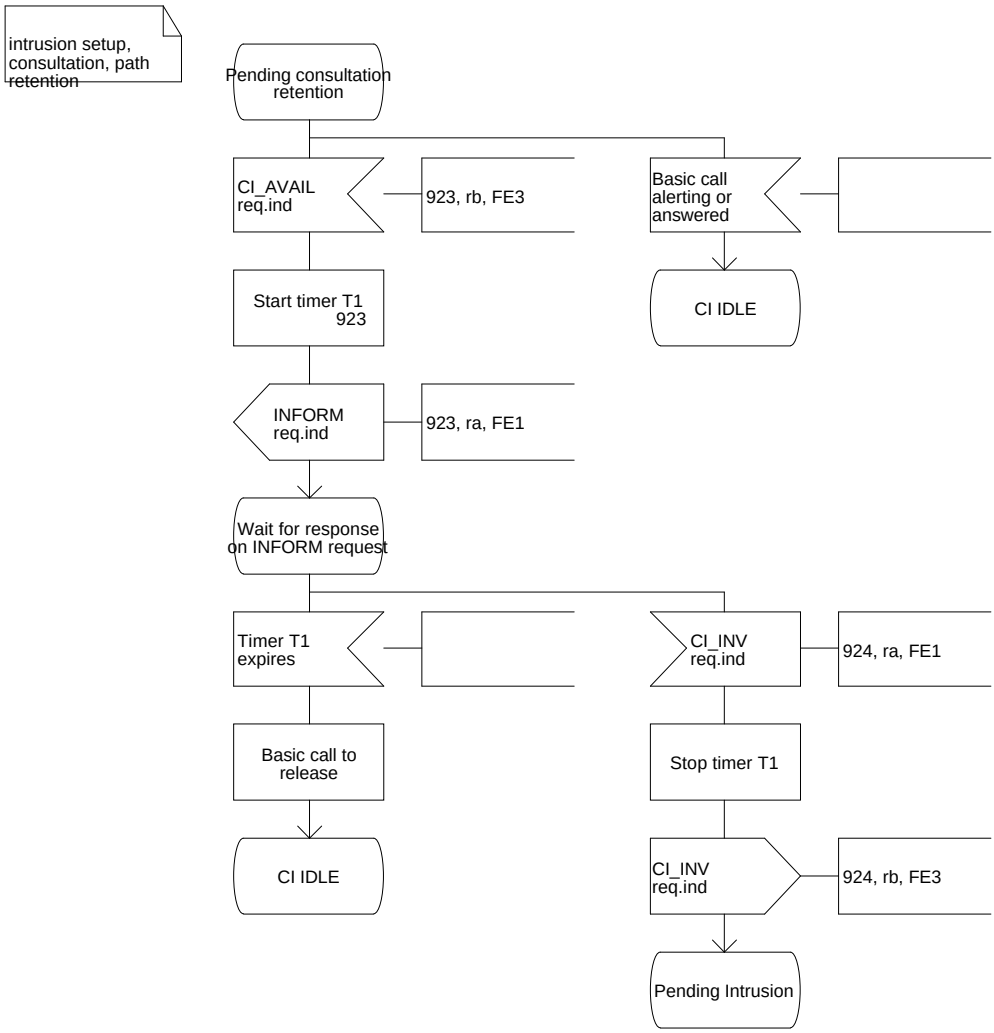

Figure 18 (sheet 2 of 10) - SS-CI, SDL for FE2

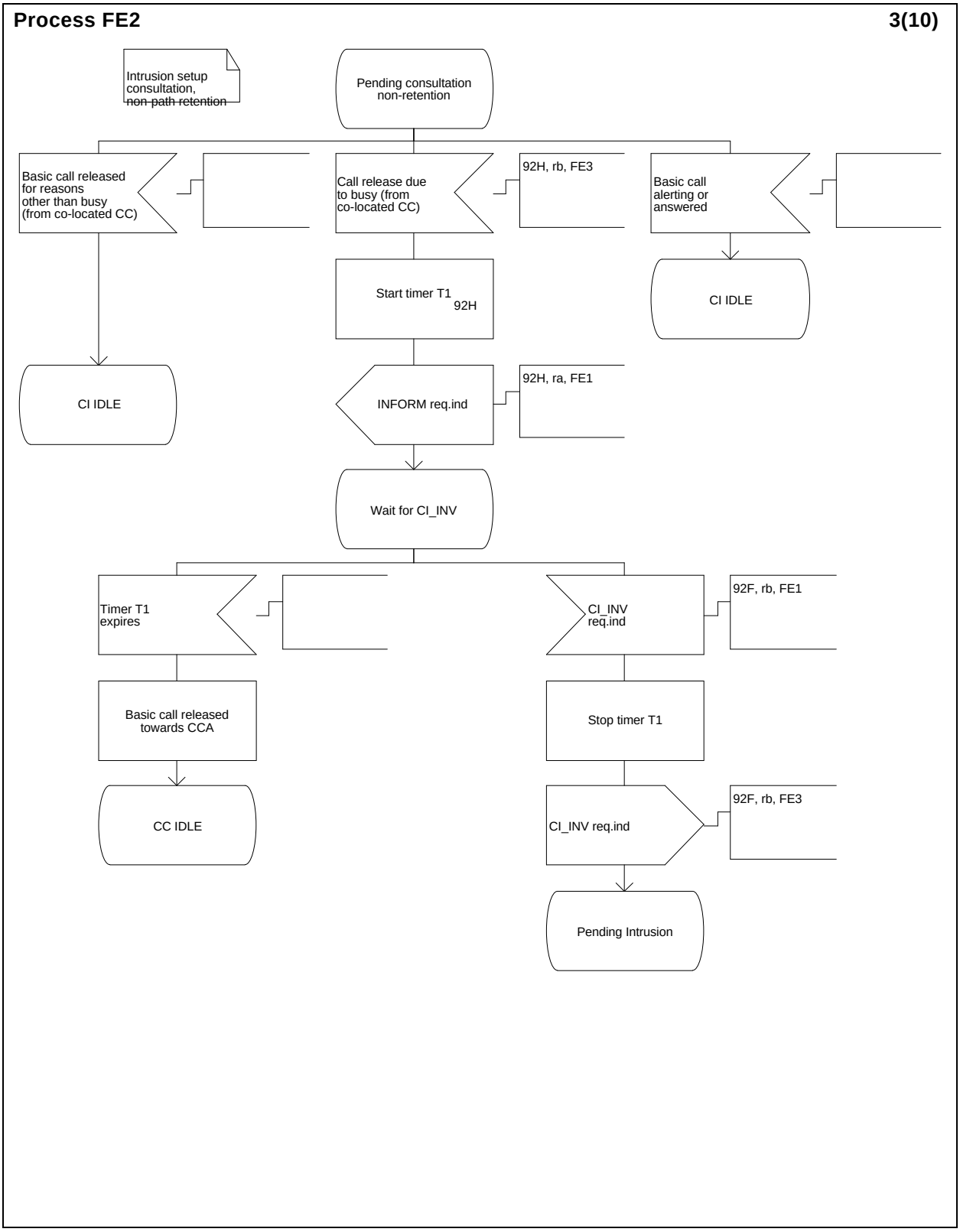

Figure 18 (sheet 3 of 10) - SS-CI, SDL for FE2

Process FE2 **4(10)**

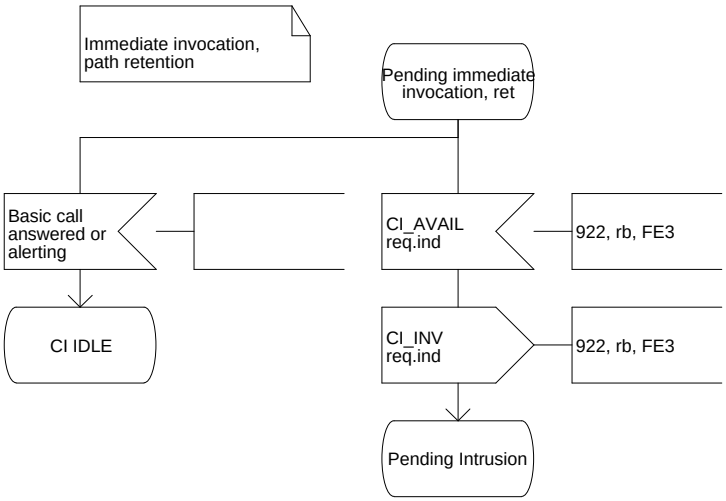

Figure 18 (sheet 4 of 10) - SS-CI, SDL for FE2

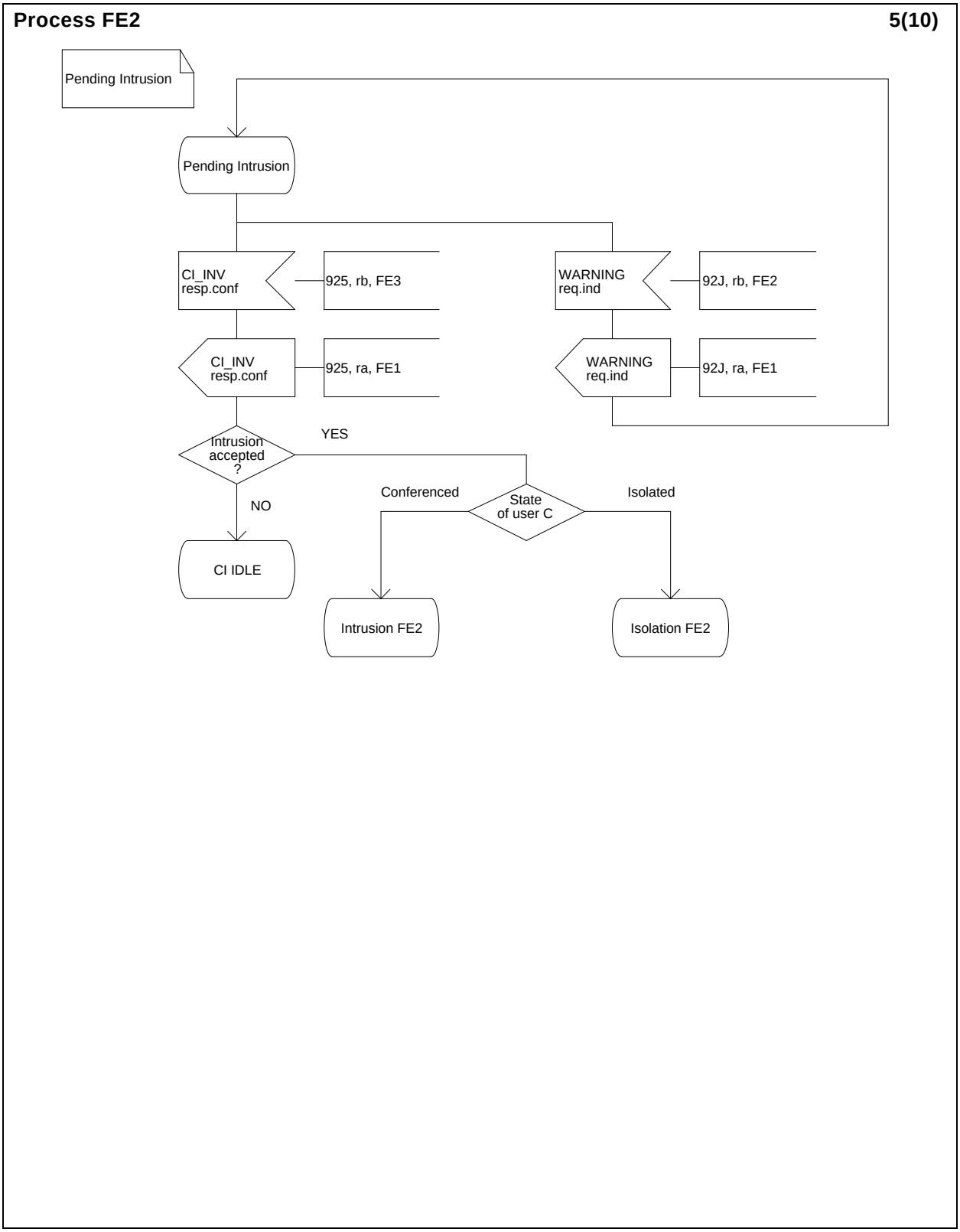

Figure 18 (sheet 5 of 10) - SS-CI, SDL for FE2

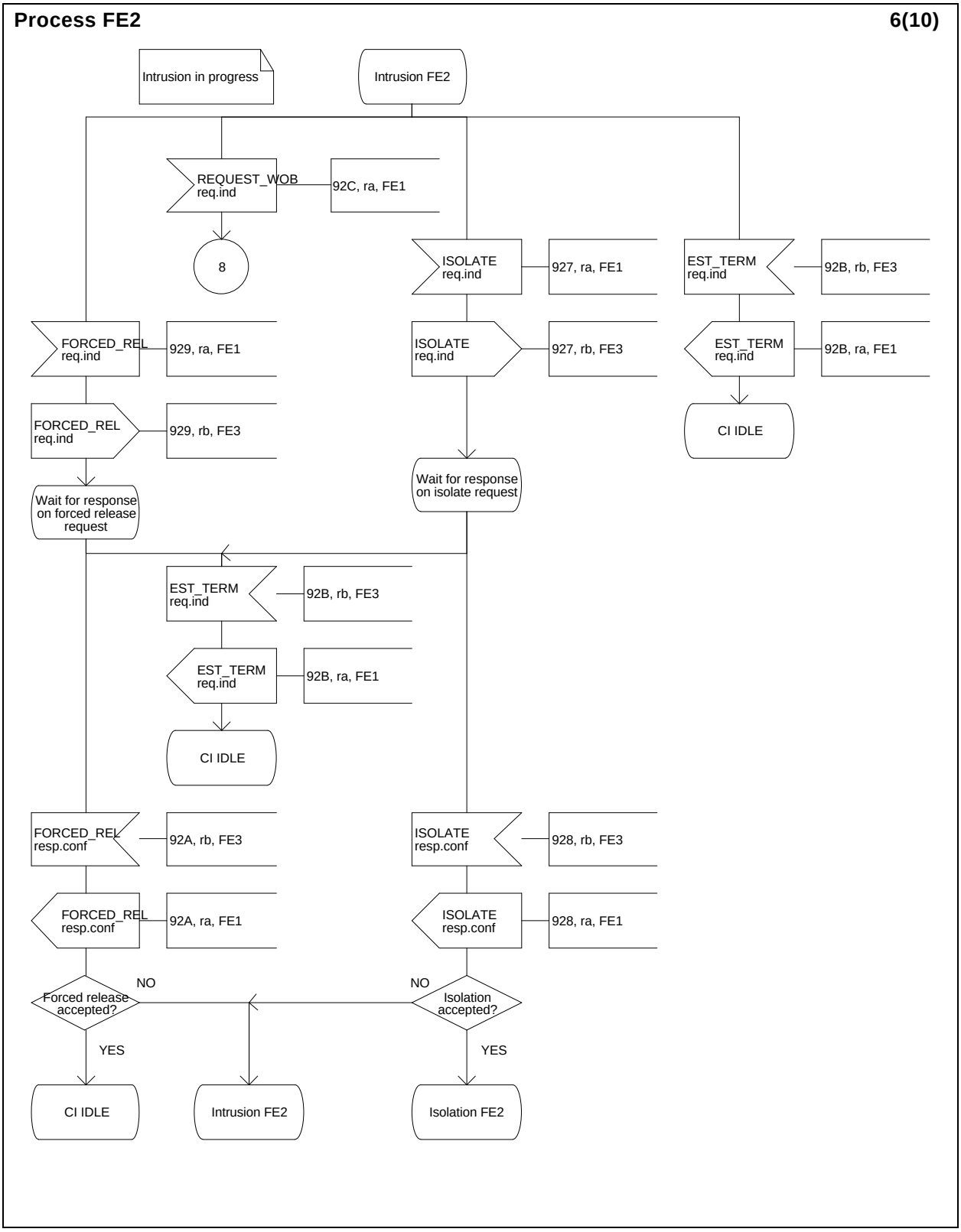

Figure 18 (sheet 6 of 10) - SS-CI, SDL for FE2

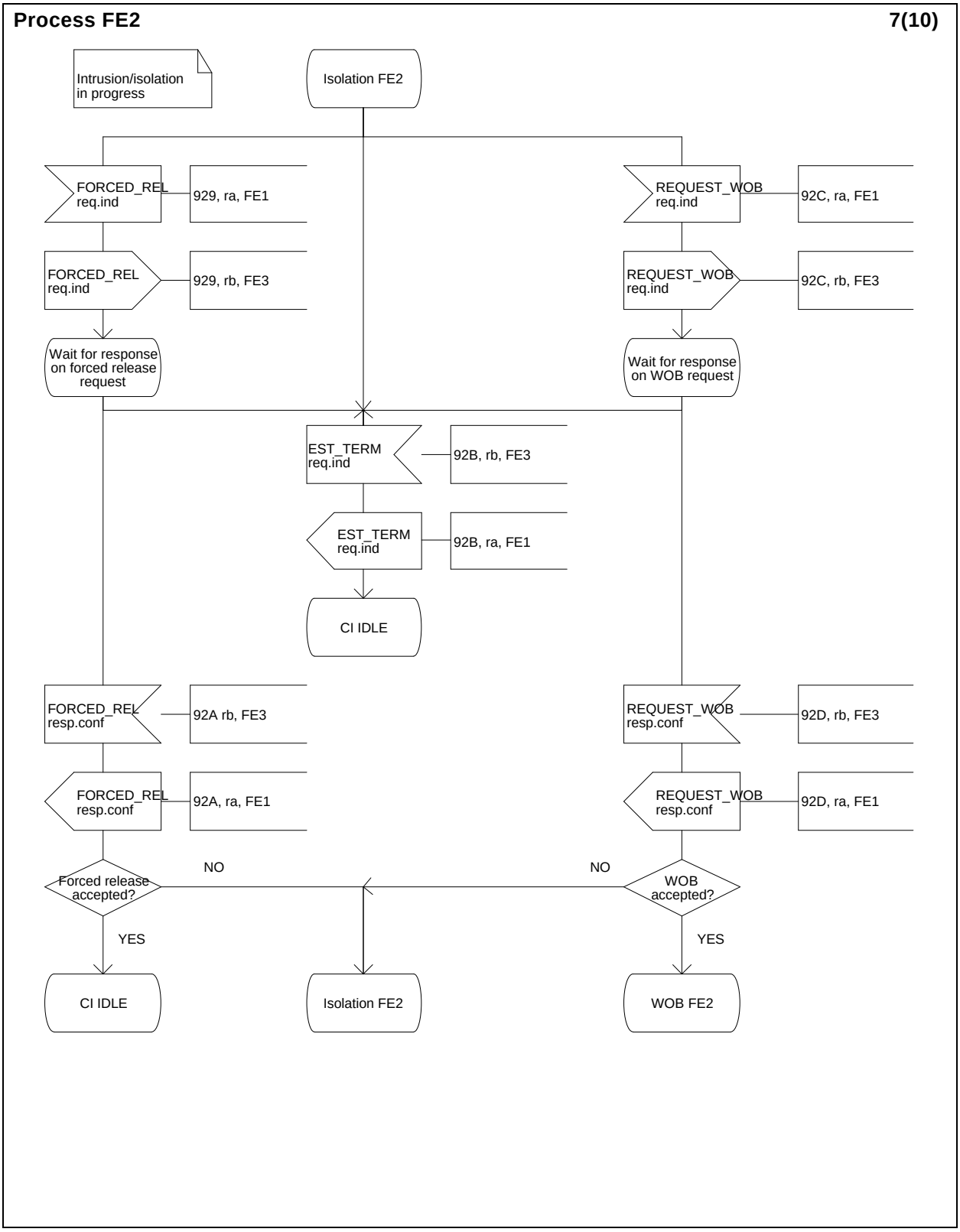

Figure 18 (sheet 7 of 10) - SS-CI, SDL for FE2

Process FE2 **8(10)**

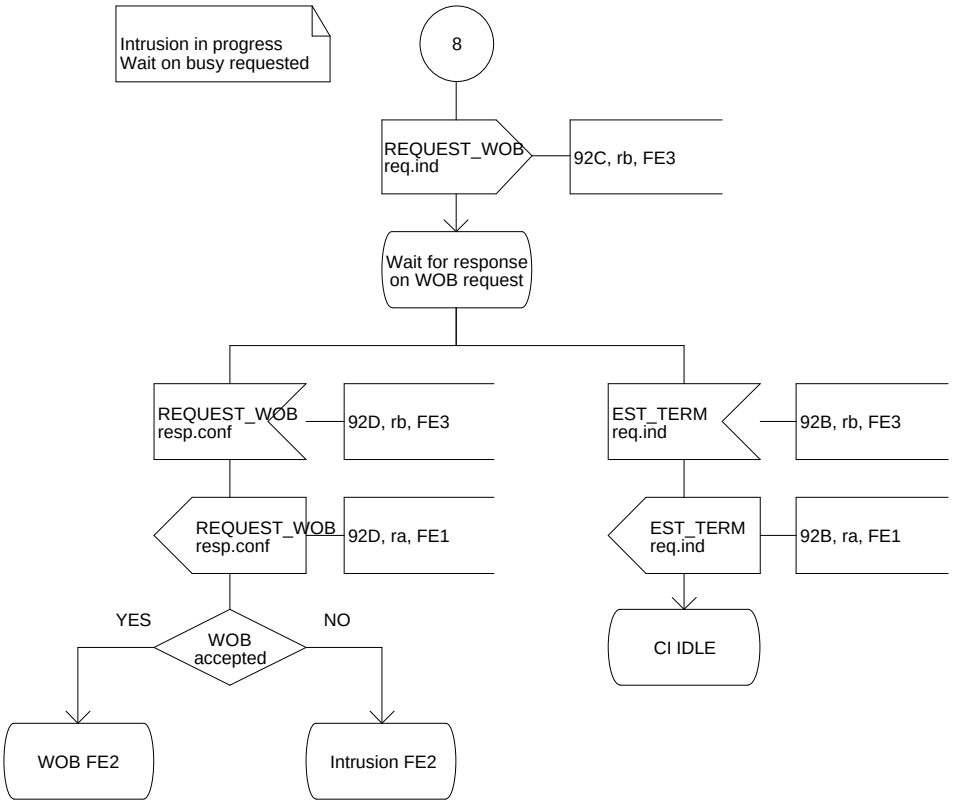

Figure 18 (sheet 8 of 10) - SS-CI, SDL for FE2

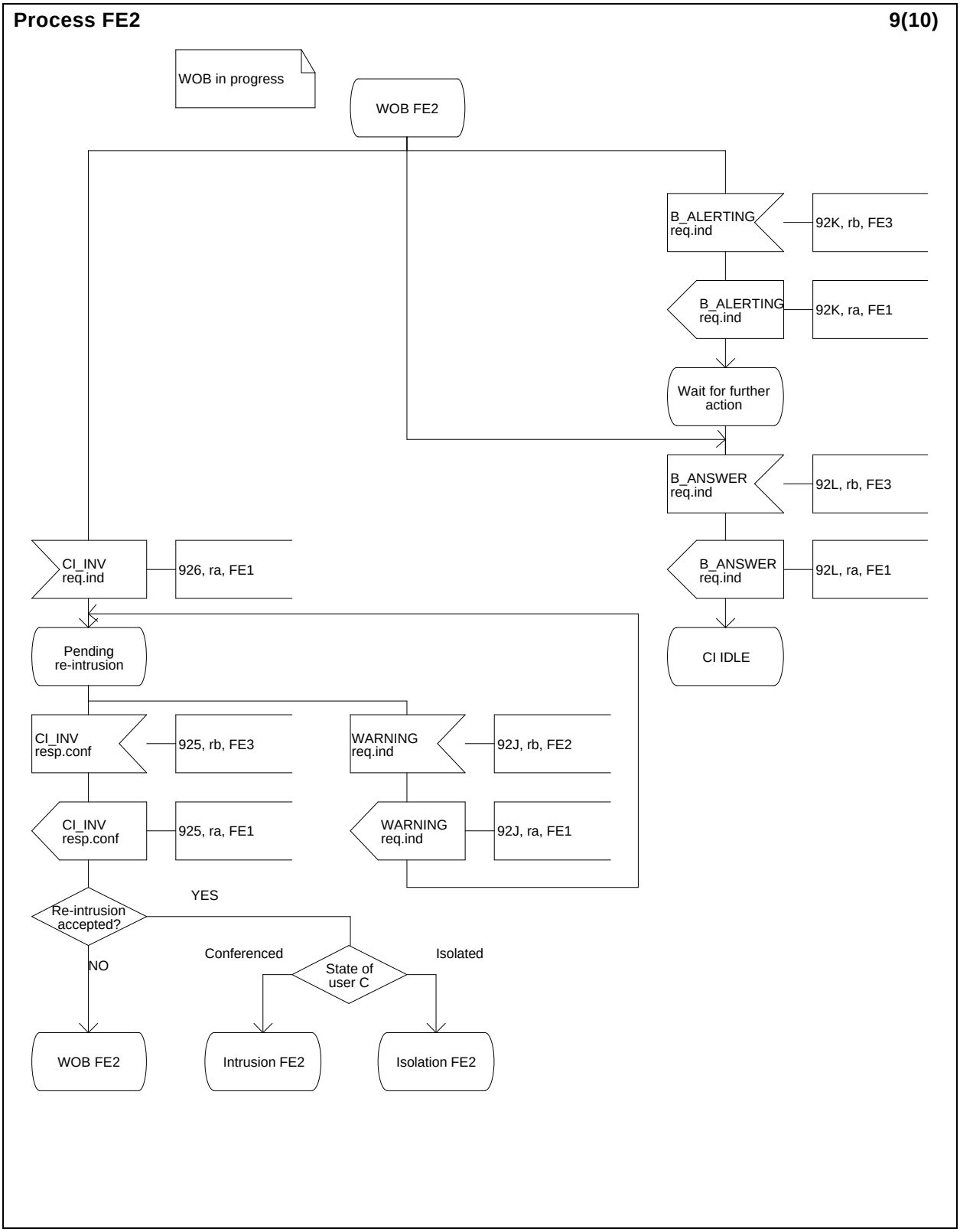

Figure 18 (sheet 9 of 10) - SS-CI, SDL for FE2

Process FE2 **10(10)**

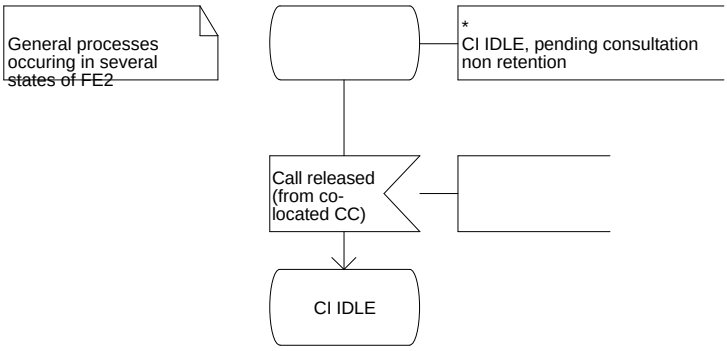

Figure 18 (sheet 10 of 10) - SS-CI, SDL for FE2

7.4.3 Behaviour of FE3

Figure 19 shows the normal behaviour of FE3. Input signals from the left and output signals to the left represent primitives from and to FE2. Input signals from and output signals to the right represent information flows from and to FE4 and input signals from the collocated CCA.

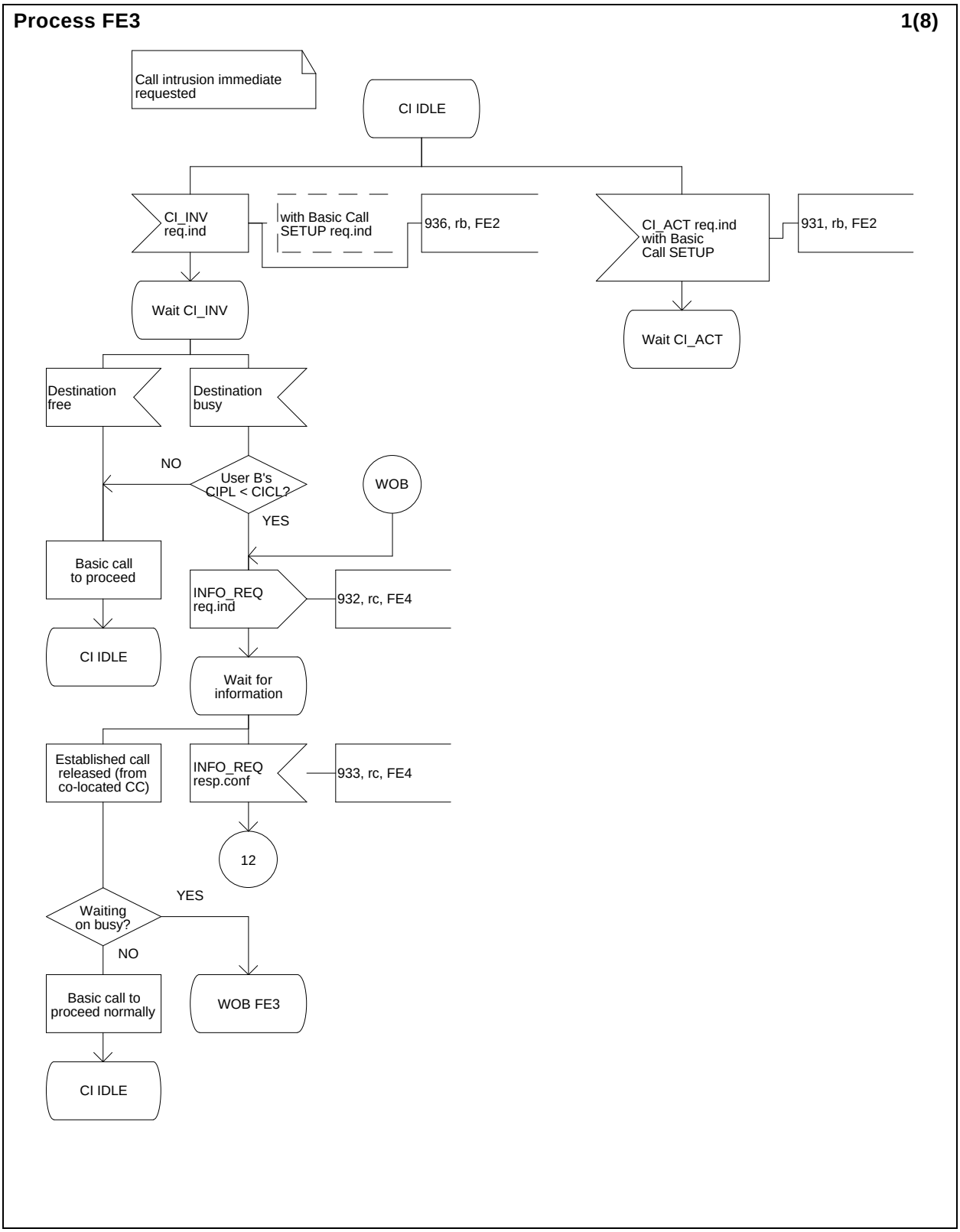

Figure 19 (sheet 1 of 8) - SS-CI, SDL for FE3

Process FE3 **2(8)**

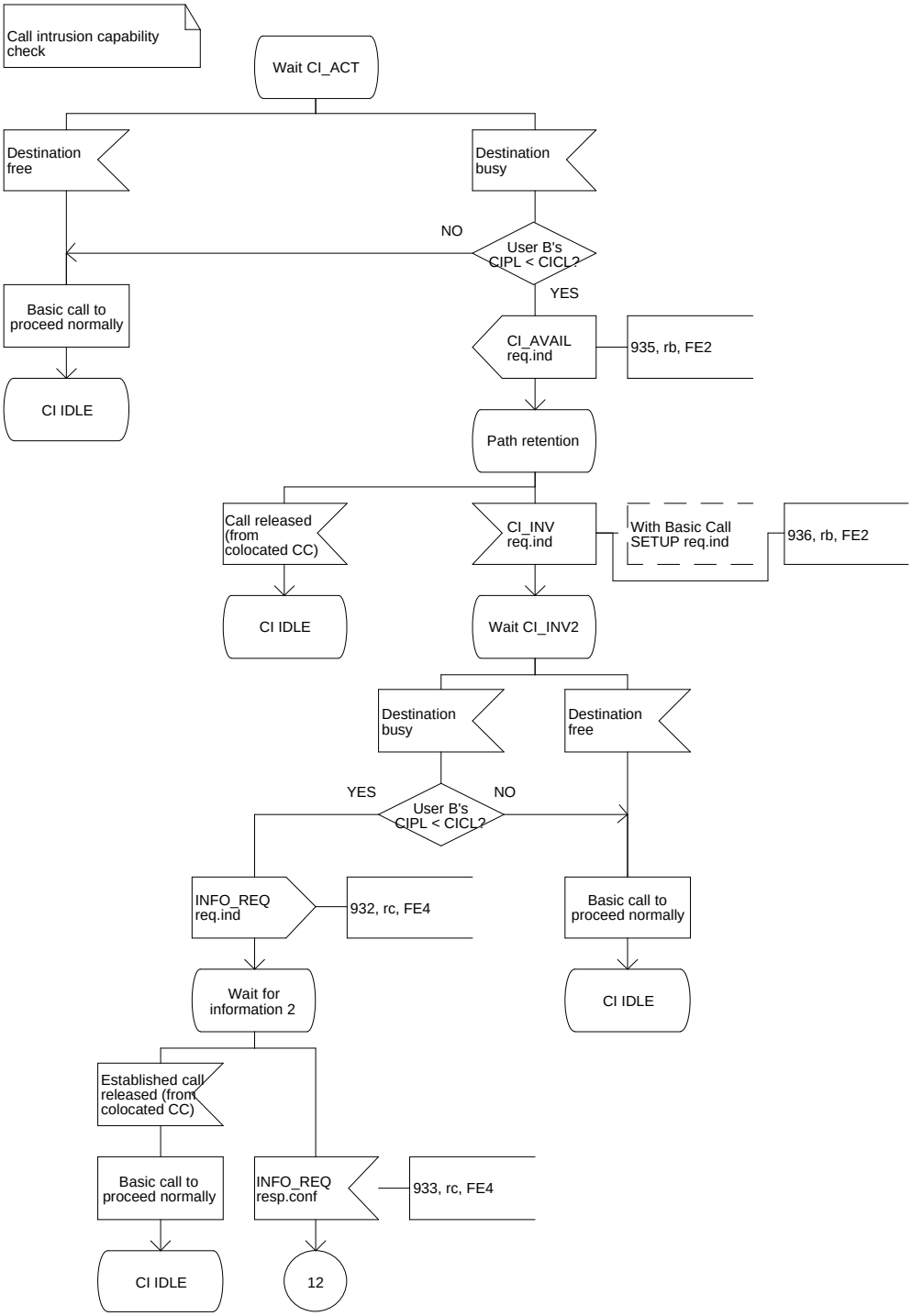

Figure 19 (sheet 2 of 8) - SS-CI, SDL for FE3

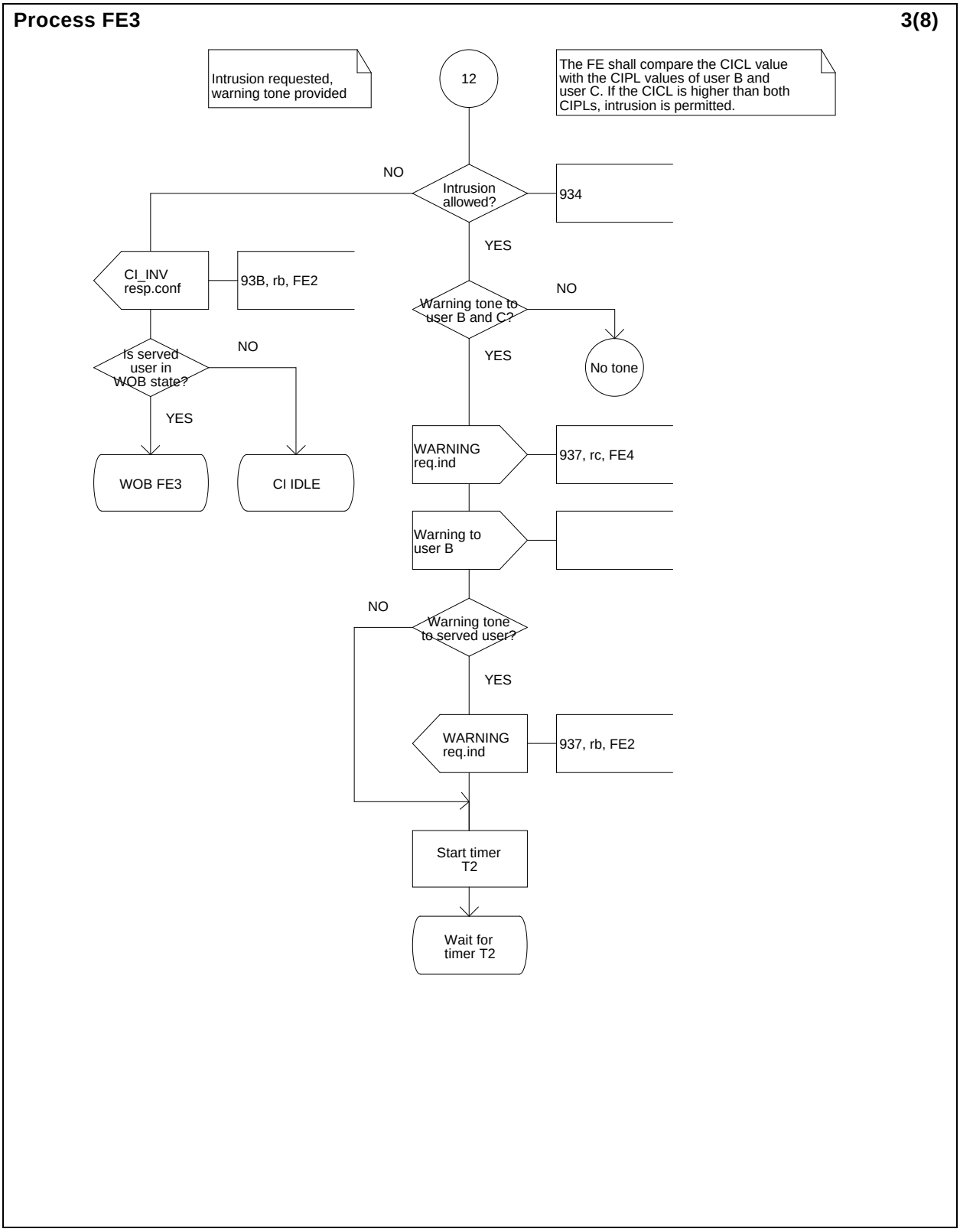

Figure 19 (sheet 3 of 8) - SS-CI, SDL for FE3

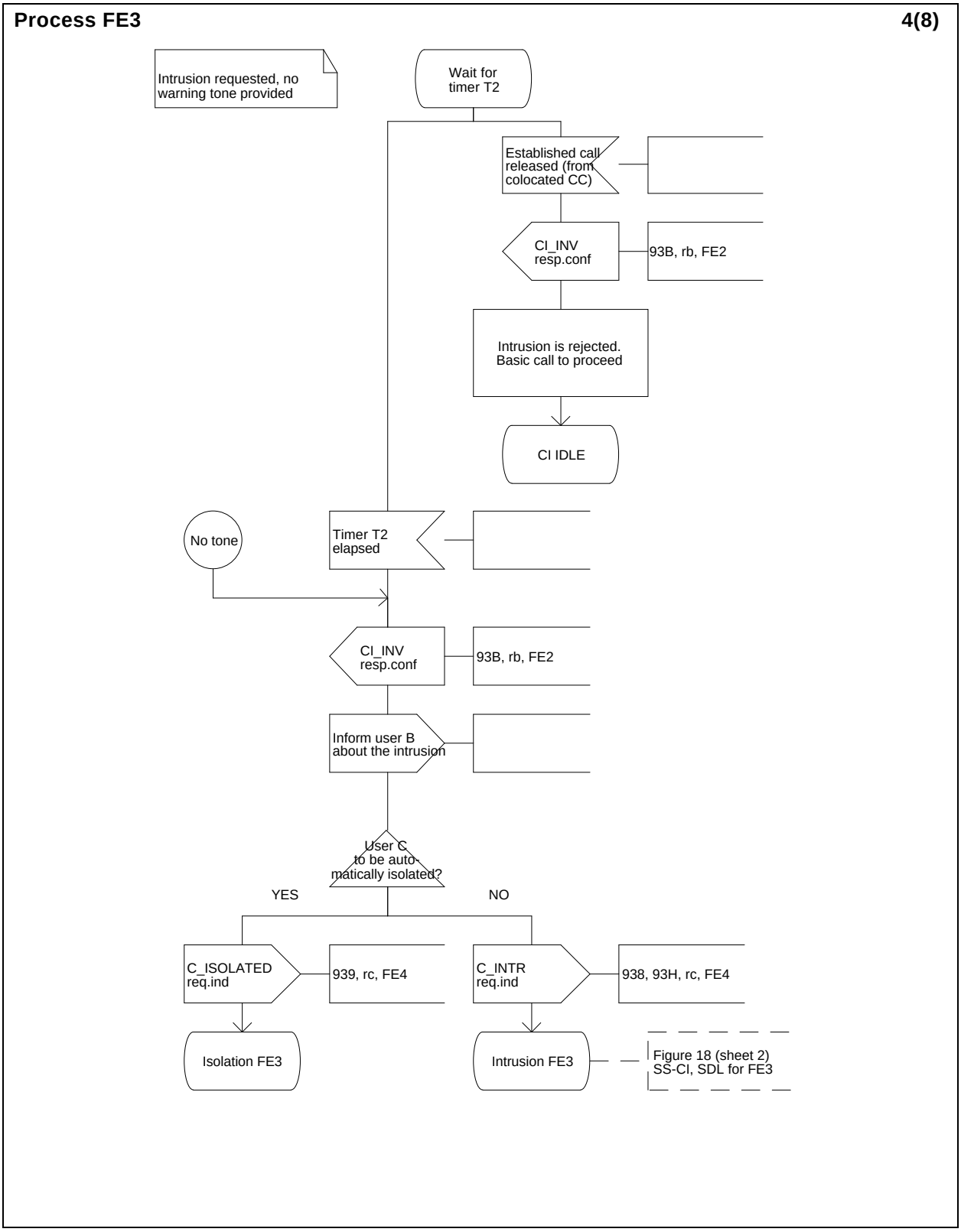

Figure 19 (sheet 4 of 8) - SS-CI, SDL for FE3

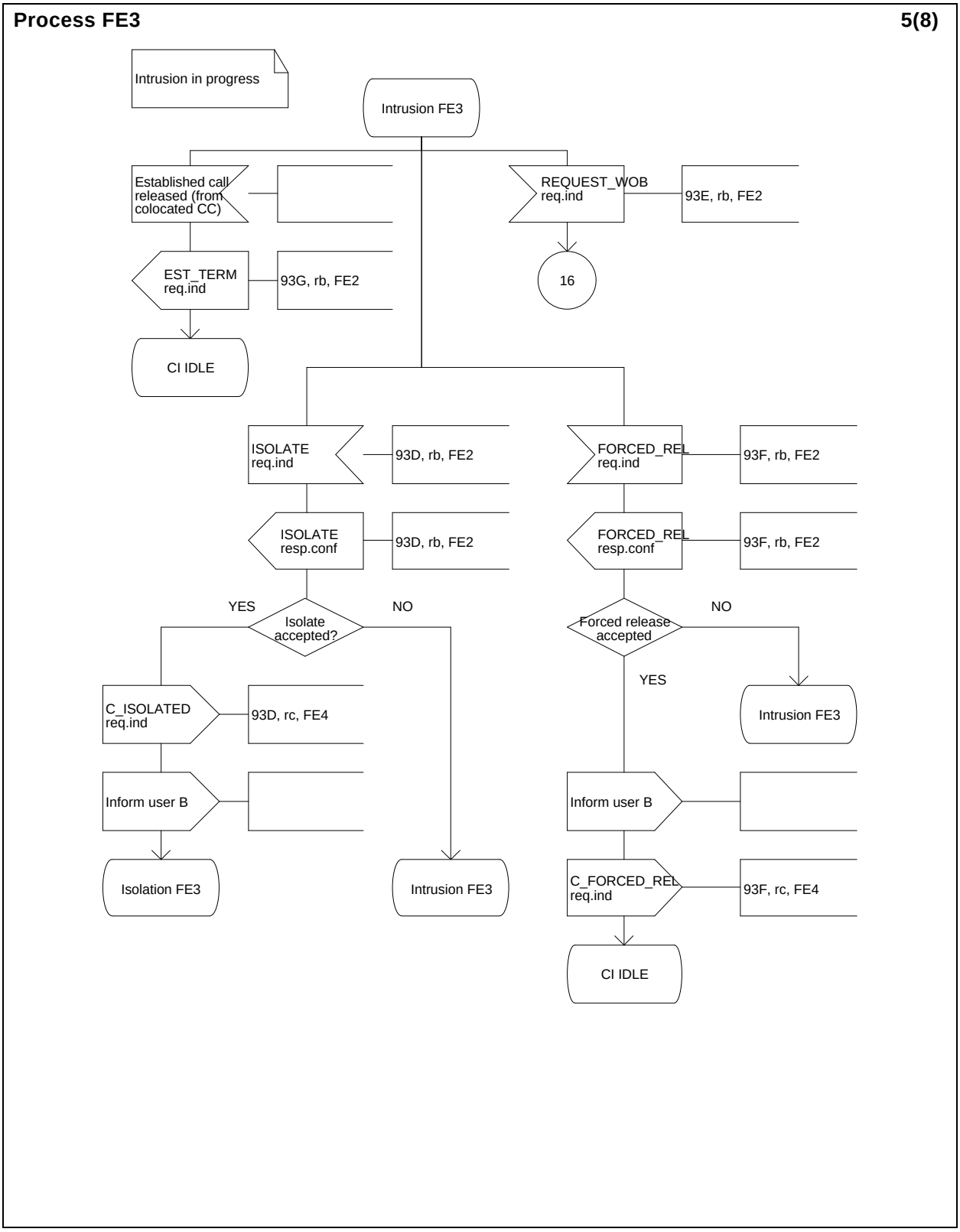

Figure 19 (sheet 5 of 8) - SS-CI, SDL for FE3

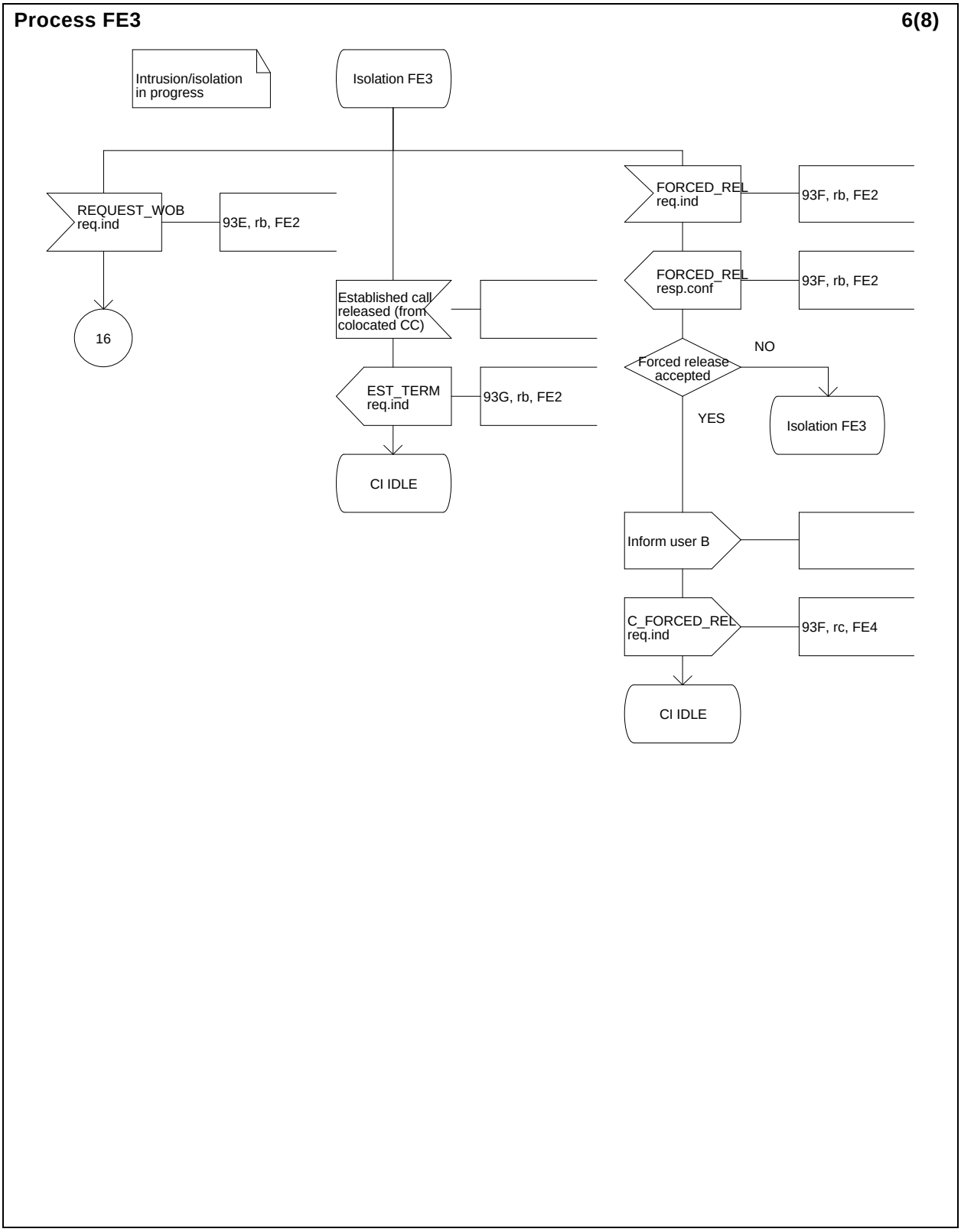

Figure 19 (sheet 6 of 8) - SS-CI, SDL for FE3

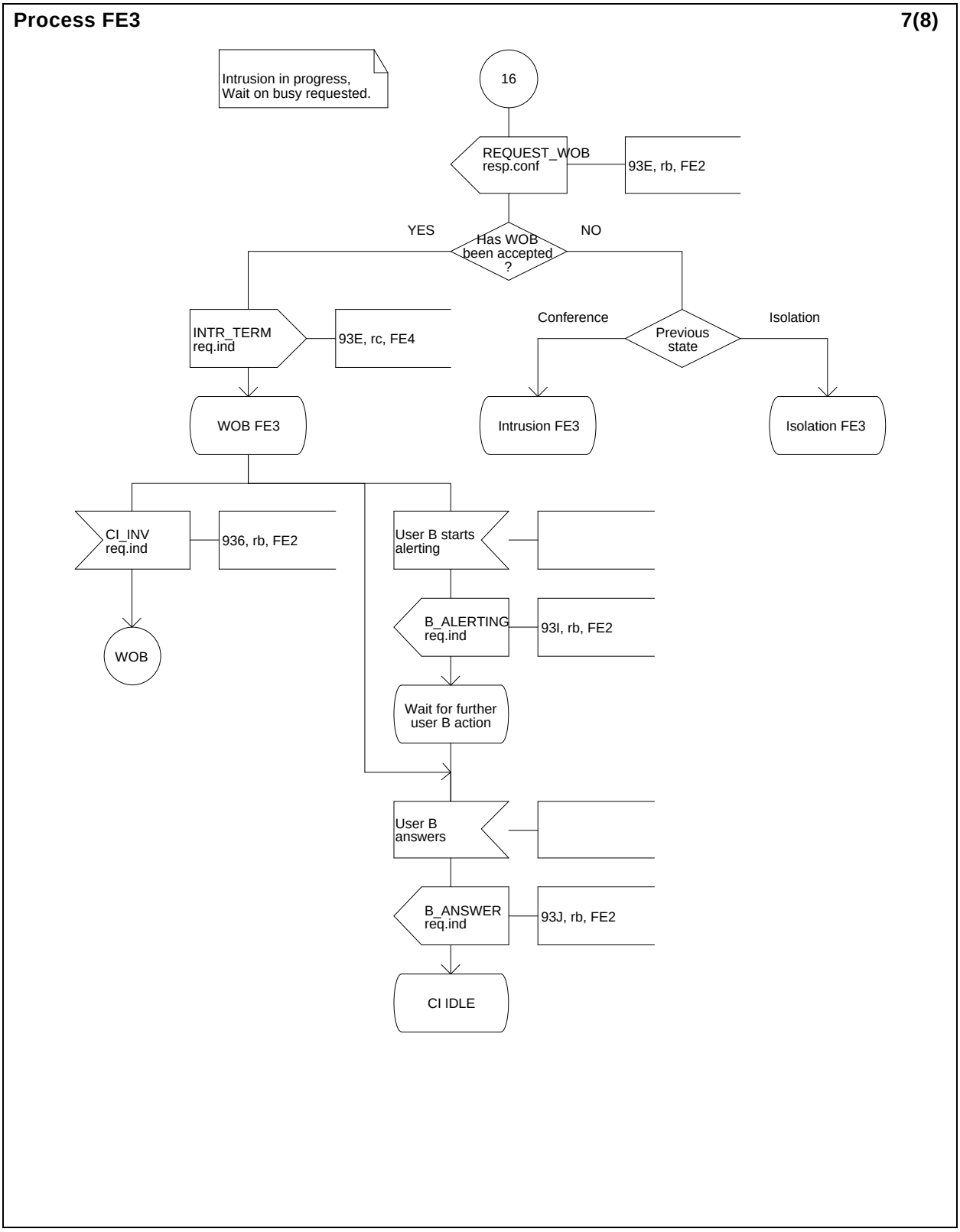

Figure 19 (sheet 7 of 8) - SS-CI, SDL for FE3

Process FE3 **8(8)**

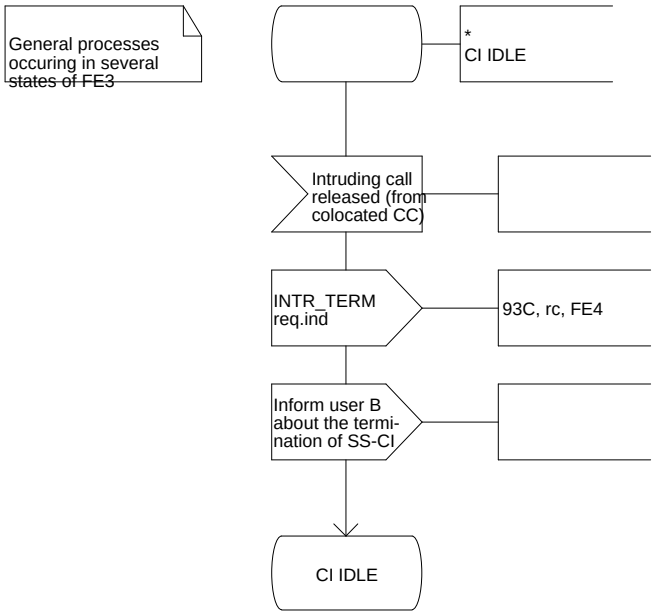

Figure 19 (sheet 8 of 8) - SS-CI, SDL for FE3

7.4.4 Behaviour of FE4

Figure 20 shows the normal behaviour of FE4. Input signals from the left and output signals to the left represent primitives from and to FE3. Input signals from and output signals to the right represent information flows from and to FE5 and input signals from the collocated CC.

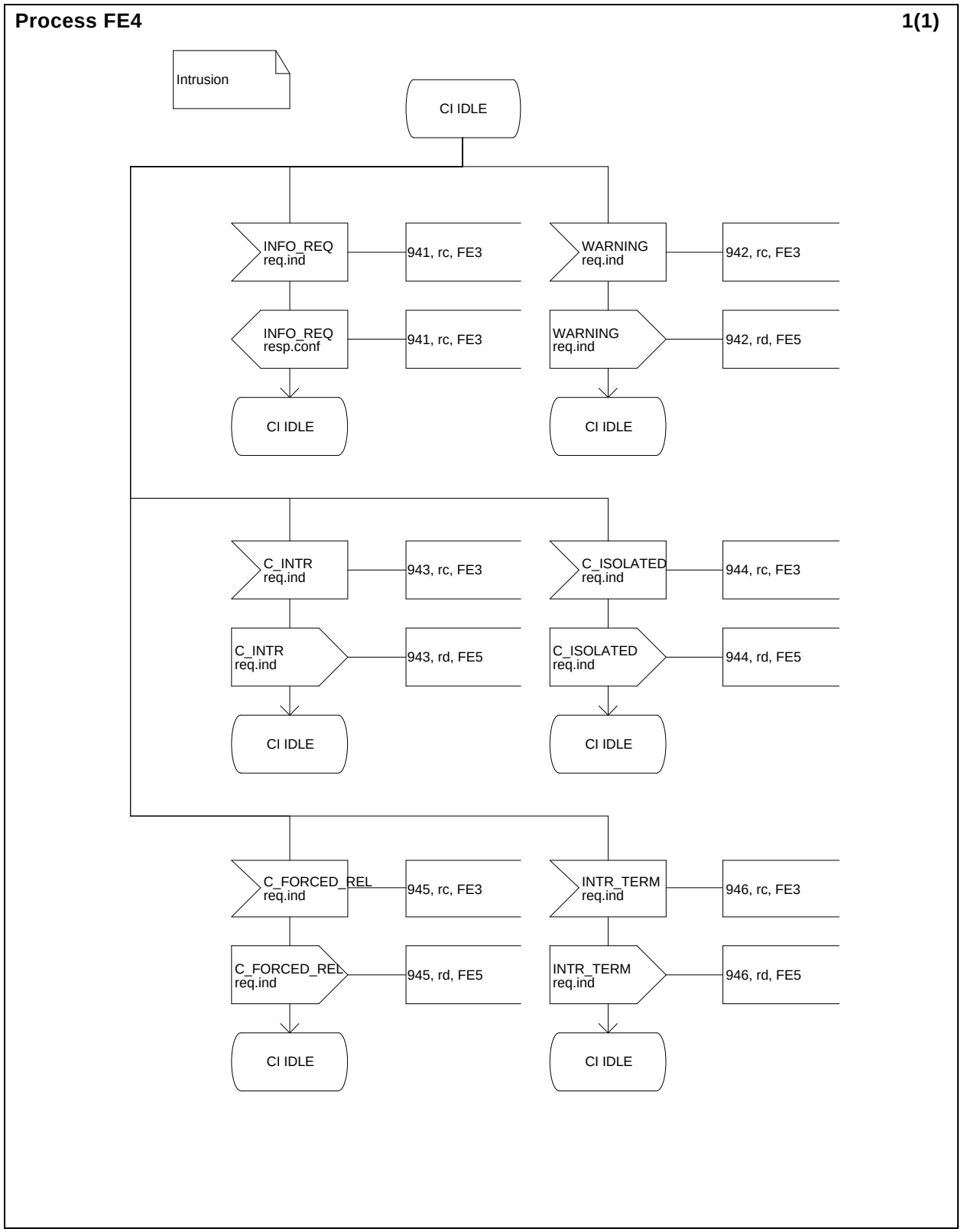

Figure 20 - SS-CI, SDL for FE4

7.4.5 Behaviour of FE5

Figure 21 shows the normal behaviour of FE5. Input signals from the left and output signals to the left represent primitives from and to FE4. Input signals from and output signals to the right represent primitives from and to the user and input signals from the collocated CCA.

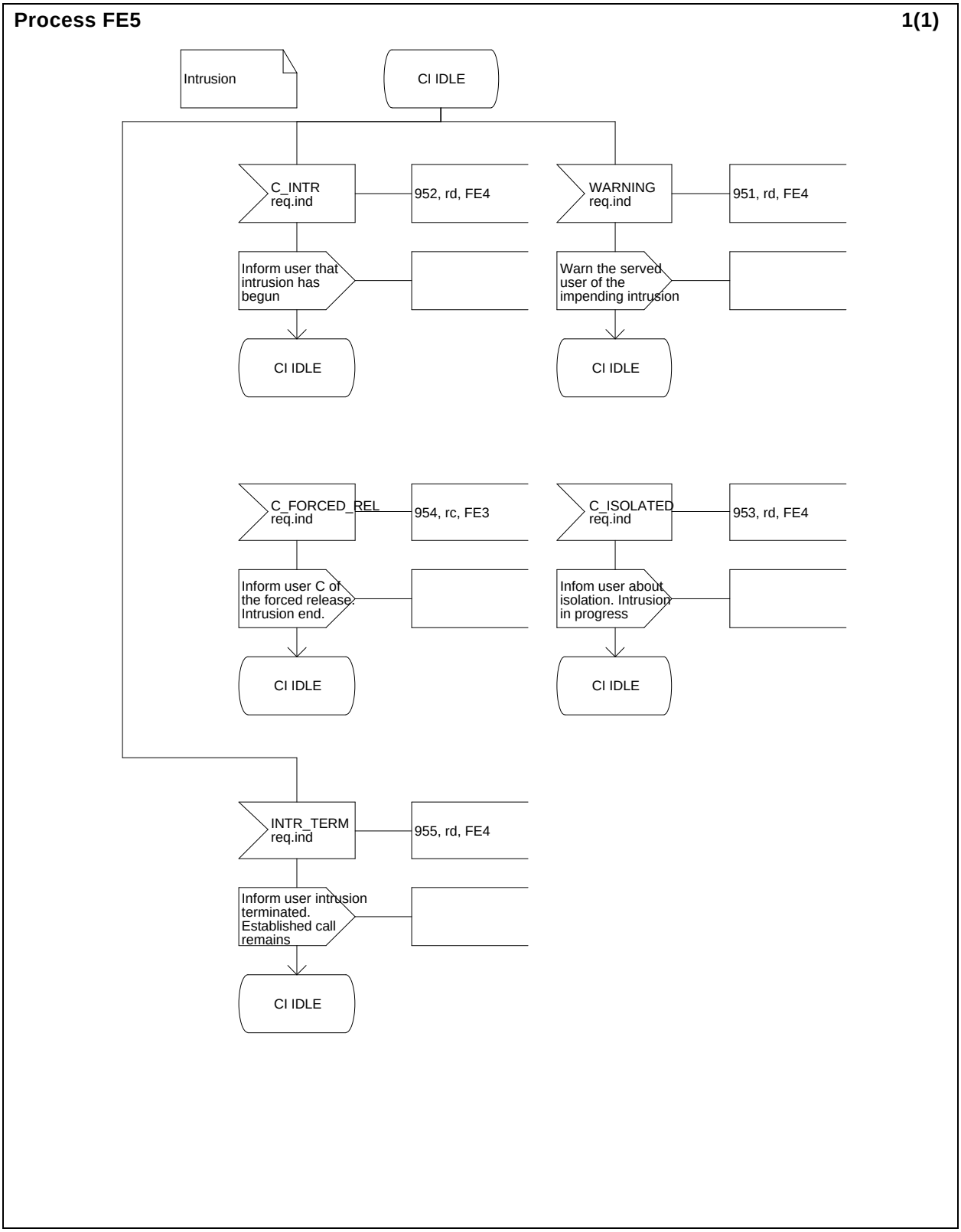

Figure 21 - SS-CI, SDL for FE5

7.5 Allocation of Functional Entities to physical equipment

The allocation of FEs to physical locations as shown in table 12 shall apply. "TE" represents a TE attached to a PTN. Where a TE is stimulus with respect to SS-CI, any FE shown as residing in the TE shall reside instead in the TE's local PTNX.

Table 12 - Scenarios for allocation of FEs to physical equipment

Scenario	FE1	FE2	FE3	FE4	FE5
1	served user TE	served user PTNX	user B PTNX/TE	user C PTNX	user C TE

7.6 Interworking considerations

On an incoming call from another network:

If the other network supports SS-CI, then FE1 and FE2 shall be in the other network (table 13, scenario 2).

On an outgoing call to another network:

a) If the other network fully supports SS-CI, then FE3 shall be in the other network (table 13, scenario 4).

b) If the other network does not support SS-CI, then FE3 shall be in the gateway PTNX (table 13, scenario 7) and:

   1) shall supply a response/confirmation with Result = "long term denial" to a CI_INV request/indication;

   2) shall ignore receipt of a CI_ACT request/indication.

c) If the other network supports SS-CI only without path retention, then FE3 shall be distributed between the gateway PTNX and the other network (table 13, scenario 8). The gateway PTNX:

   1) shall forward any CI_INV request/indication to the other network;

   2) on receipt of CI_ACT request/indication, shall send a request for call establishment without SS-CI to the other network.

      If the call fails due to busy called user, the Gateway PTNX may optionally retain all call set up information and send a CI_AVAIL request/indication to FE2. On receipt of a CI_INV request/indication, the Gateway PTNX shall send a request for call establishment with SS- CI to the other network. Depending on the result of the request for call establishment, FE2 shall send a CI_INV response/confirmation specifying appropriate value for element Result. The actions performed may depend on the requirements of the other network.

If user B is in the PTN, user C is in another network, and the other network is able to supply FE4 functionality, FE4 and FE5 shall be in the other network (table 13, scenario 5).

If user B is in the PTN, user C is in another network, and the other network is unable to provide FE4 functionality, FE4 shall be in the Gateway PTNX and FE5 shall be in the other network (table 13, scenario 3).

If user C is in the PTN and user B is in another network, FE1, FE2 and FE3 shall be in the other network (table 13, scenario 6).

Table 13 - Scenarios for allocation of FEs to physical equipment for normal operation in case of interworking with another network

Scenario	FE1	FE2	FE3	FE4	FE5
2	other N/W	other N/W	user B PTNX/TE	user C PTNX	user C TE
3	served user TE	served user PTNX	user B PTNX/TE	gateway PTNX	other N/W
4	served user TE	served user PTNX	other N/W	other N/W	other N/W
5	served user TE	served user TE	user B PTNX/TE	other N/W	other N/W
6	other N/W	other N/W	other N/W	user C PTNX	user C TE
7	served user TE	served user PTNX	gateway PTNX	other N/W	other N/W
8	served user TE	served user PTNX	gateway PTNX + other N/W	other N/W	other N/W

History

Document history			
June 1994	Public Enquiry	PE 65:	1994-06-13 to 1994-10-14
April 1995	Vote	V 77:	1995-04-03 to 1995-05-26
September 1995	First Edition		
October 1995	Converted into Adobe Acrobat Portable Document Format (PDF)		

ISBN 2-7437-0209-5
Dépôt légal : Septembre 1995