FREQUENTIS

iSAS

Security Target Lite

EWSE23EN90002.10

History Chart

Rev.	Date	Changed Page(s)	Cause of Change	Implemented
1.0	2012-05-15	All sections	Initial Version	Döderlein

No.	Action	Name	Signature	Date
1	Prepared	C. Döderlein		2012-05-15
2	Approved	R. Madarasz		2012-05-15
3	Released	B. Pedersen-Krieger		2012-05-15

FREQUENTIS NACHRICHTENTECHNIK GMBH
Robert-Bosch-Str. 11B, 63225 Langen, Germany, http://www.frequentis.com/
Amtsgericht Offenbach, Reg.Langen HRB 3496 UID Nr. DE 154335662, Steuer-Nr. 035 233 30505.

Contents

Illustrations

Tables

---------- END OF SECTION ----------

1. Security Target Introduction

This section describes the Target of Evaluation (TOE) in a narrative way on three levels of abstraction:

- the Security Target (ST) reference and the TOE reference, which provide identification material for the ST and the TOE that the ST refers to;
- the TOE overview, which briefly describes the TOE;
- the TOE description, which describes the TOE in more detail.

1.1. Security Target Reference

This chapter refers to the complete Security Target, which was the basis for the evaluation. The document in hand is the sanitized public version of the complete Security Target.

ST Name:	Security Target for iSAS
ST Version:	1.7
ST Document Number:	EWSE23EN90001.17
Authors:	Frequentis Nachrichtentechnik GmbH
Keywords:	Secure audio switch, Trusted audio switch, Red/Black separation, Audio interface
ST Evaluation Status:	Formal evaluation by Technical Center for Information Technology and Electronics – WTD 81 is completed.

1.2. TOE Reference

Developer Name:	Frequentis Nachrichtentechnik GmbH
TOE Name:	iSAS
Release	1.0
Evaluation Status:	Formal evaluation by Technical Center for Information Technology and Electronics – WTD 81 is completed.

1.3. TOE Overview

1.3.1. Use and major security features of the TOE

The TOE, hereinafter referred to as a Secure Audio Switch (iSAS), is installed in settings were a user (S.User) needs to operate CLASSIFIED and UNCLASSIFIED voice communication via a common user interface and the same set of audio devices (see Fig. 1-1).

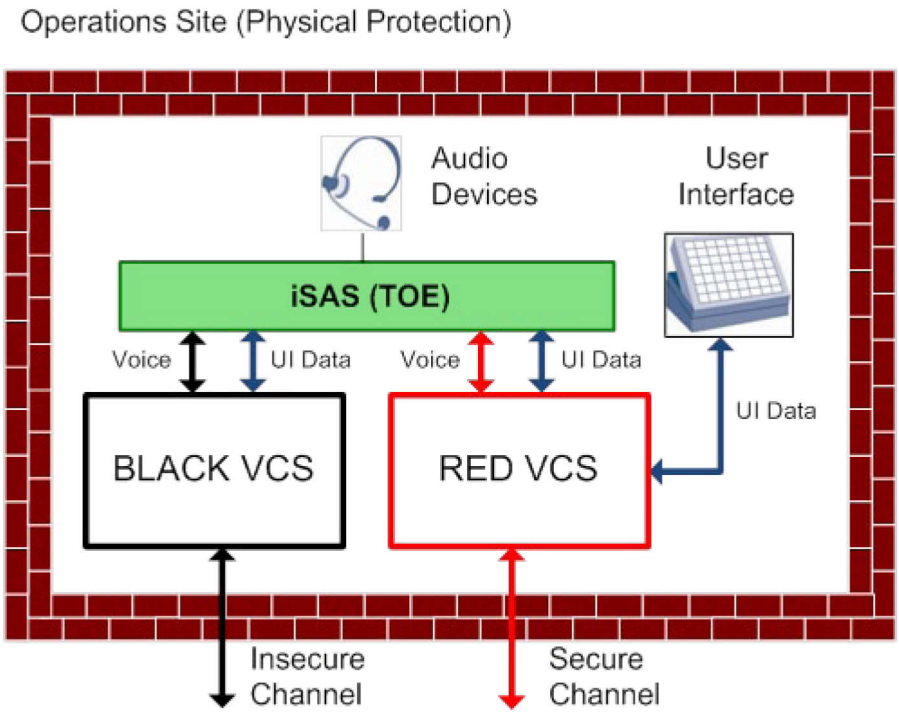

Fig. 1-1: TOE and its Environment

The CLASSIFIED and UNCLASSIFIED voice information is processed by dedicated, physically separated voice communication systems (RED and BLACK VCS) and transmitted via secure or insecure communication channels. The TOE and the VCSs are installed in a physically protected operations site.

In operation, the user (S.User) can control the voice transmission path (Microphone_Inputs) separately from the voice reception path (Earpiece_Outputs).

The TOE connects the Microphone_Inputs to either the RED VCS or the BLACK VCS. To switch between RED and BLACK VCS the user (S.User) must perform some specific action (e.g. push a button, turn a knob, etc.). The TOE then visually indicates whether the Microphone_Inputs are connected to the BLACK or RED VCS.

The TOE connects the Earpiece_Outputs to either the RED VCS or BLACK VCS or to both VCSs (mixed signal). To switch between the RED, BLACK and BOTH mode the user (S.User) must perform some specific action (e.g. push a button, turn a knob, etc.). The TOE then visually indicates whether the Earpiece_Outputs are connected to the BLACK VCS, RED VCS or to both VCSs.

A common user interface (e.g. touch entry device), which is integrated into the RED VCS controls both the RED and the BLACK VCS. The TOE mediates the flow of user interface data (User_Interface_Data) between the RED VCS and the BLACK VCS in order to prevent the User_Interface_Data from being misused to bypass the separation of CLASSIFIED and UNCLASSIFIED voice information.

The TOE does not have, and in fact specifically precludes, any features that permit voice information to be shared or transferred between the BLACK and RED VCS via the TOE.

1.3.2. TOE Type

The TOE is a device that permits a user (S.User) to operate CLASSIFIED and UNCLASSIFIED voice communication via a common user interface and the same set of audio devices. The user can rely on the TOE unique architecture to keep the CLASSIFIED and UNCLASSIFIED voice information completely separate.

1.3.3. Required non-TOE hardware/software/firmware

The TOE is intended for use with Frequentis VCS. The digital format of the audio signal as well as other control signals are not intended for connection with general purpose voice communication systems.

For communication with the RED and BLACK VCS the TOE requires the following non-TOE firmware (see Fig. 1-8):

- Non-TOE Firmware for dedicated Secure Processing
- Non-TOE Firmware for dedicated Insecure Processing

Additionally the TOE requires the following non-TOE hardware:

- Audio device(s)
- RED VCS including the user interface (e.g. touch entry device)
- BLACK VCS

1.4. TOE Description

The TOE description provides general description of the security capabilities of the TOE in more detail including the wider application context into which the TOE will fit.

1.4.1. Application context

This chapter describes the typical usage of the TOE at an operator working position together with a Frequentis VCS. However, the application of the TOE is not limited to those setups.

The operator position equipment is designed either for console mounting (see Fig. 1-2, Fig. 1-3) or as a desktop version (see Fig. 1-4). The user (S.User) operates both VCSs via a touch entry device (TED) that is integrated into the RED operator position electronic.

The TOE is an audio interface device providing flow control between the audio devices and the operator position electronics of the RED and BLACK VCS. The TOE is connected to the RED and BLACK operator position electronics via fibre optics.

In order to cover a wide range of possible installation scenarios the TOE is composed of three separate hardware modules: The actual secure audio switch (MOD iSAS-P) and two remote control devices (MOD iSAS-RC 01 and MOD iSAS-RC 02).

Depending on the space available and whether the operator position is fitted into a console or is placed on desk, the TOE is operated in one of the following ways:

- Operation via Touch Entry Device - Console Version (see Fig. 1-2): The operator switches the audio devices between RED and BLACK VCS via the touch entry device. Additionally the TOE provides assured visual indication at the MOD iSAS-P housing whether the Microphone_Inputs/Earpiece_Outputs are connected to the BLACK or RED VCS. The touch entry device is out of scope of the TOE. Therefore, this setup requires that the MOD iSAS-P is mounted visible and the operator regularly checks the assured indication at the MOD iSAS-P housing.
- Operation via Remote Control Device - Console Version (Fig. 1-3): If the assured indication directly at MOD iSAS-P housing is not visible to the operator, the TOE is operated via a remote control device. The remote control device is implemented as a Key and Lamp Module in a separate housing designed for console mounting. This type of remote control device (MOD iSAS-RC 02) is part of the TOE.
- Operation via Remote Control Device - Desktop Version (see Fig. 1-4): In case of the desktop version the Secure Audio Switcher (MOD iSAS-P) is integrated into the desktop remote control device. The desktop remote control device contains a key and lamp module for operation of the TOE. This type of remote control device (MOD iSAS-RC 01) is part of the TOE.

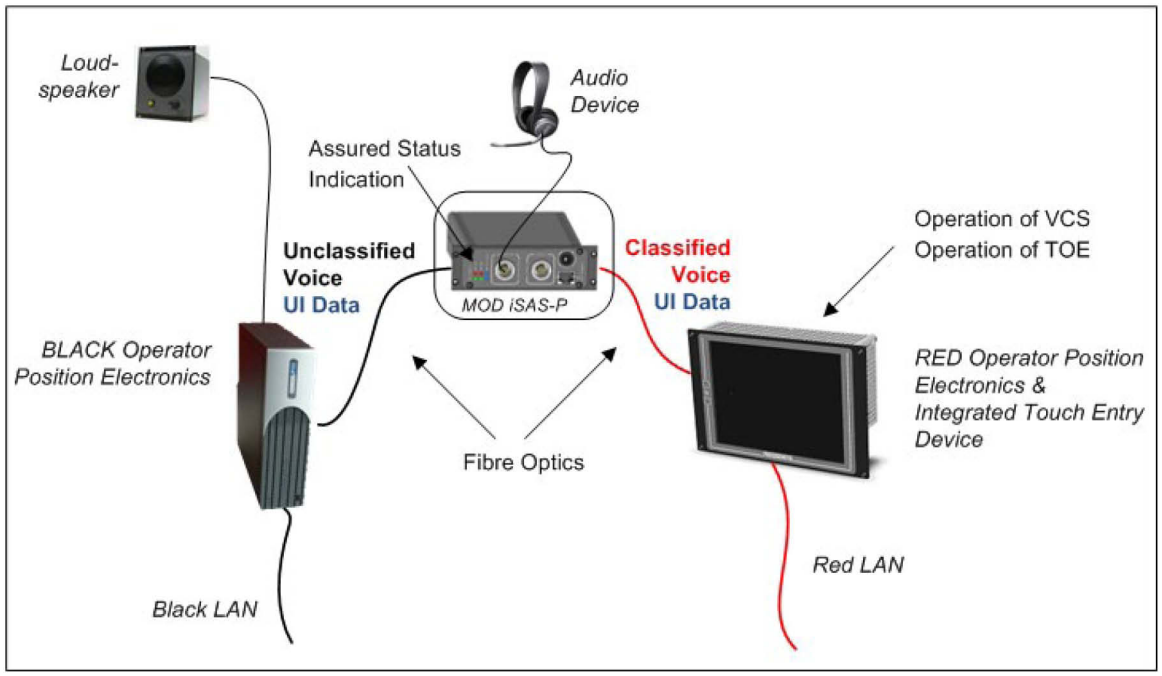

Fig. 1-2: TOE and Operator Position Equipment for Console Mounting – Operation via Touch Entry Device

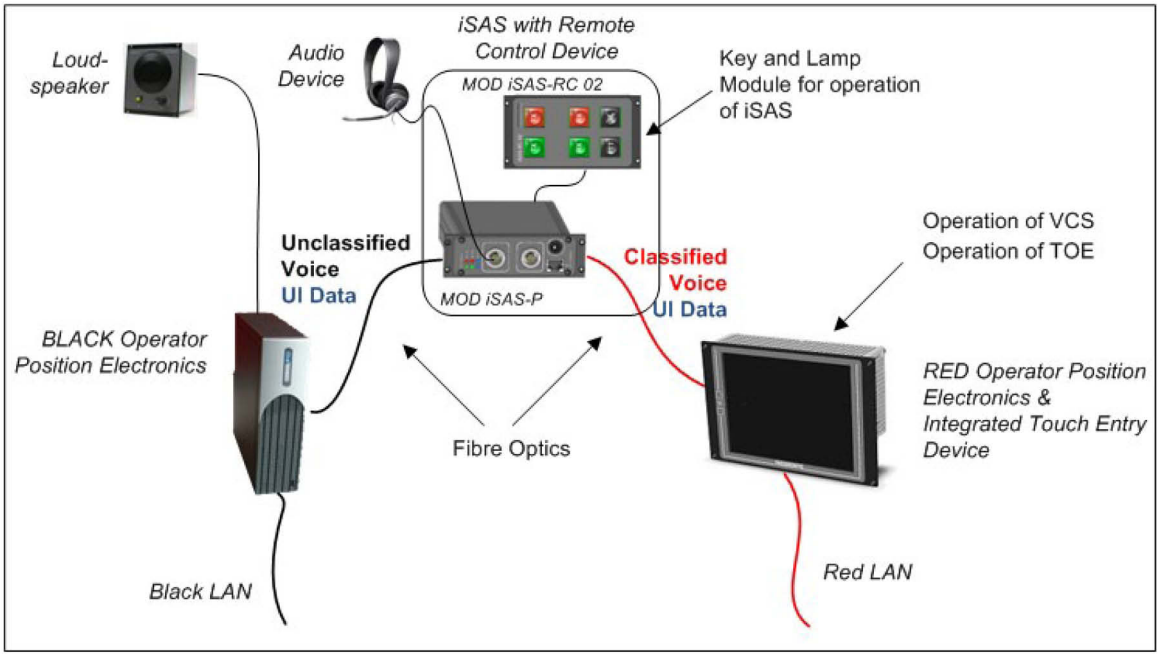

Fig. 1-3: TOE and Operator Position Equipment for Console Mounting – Operation via Remote Control Device

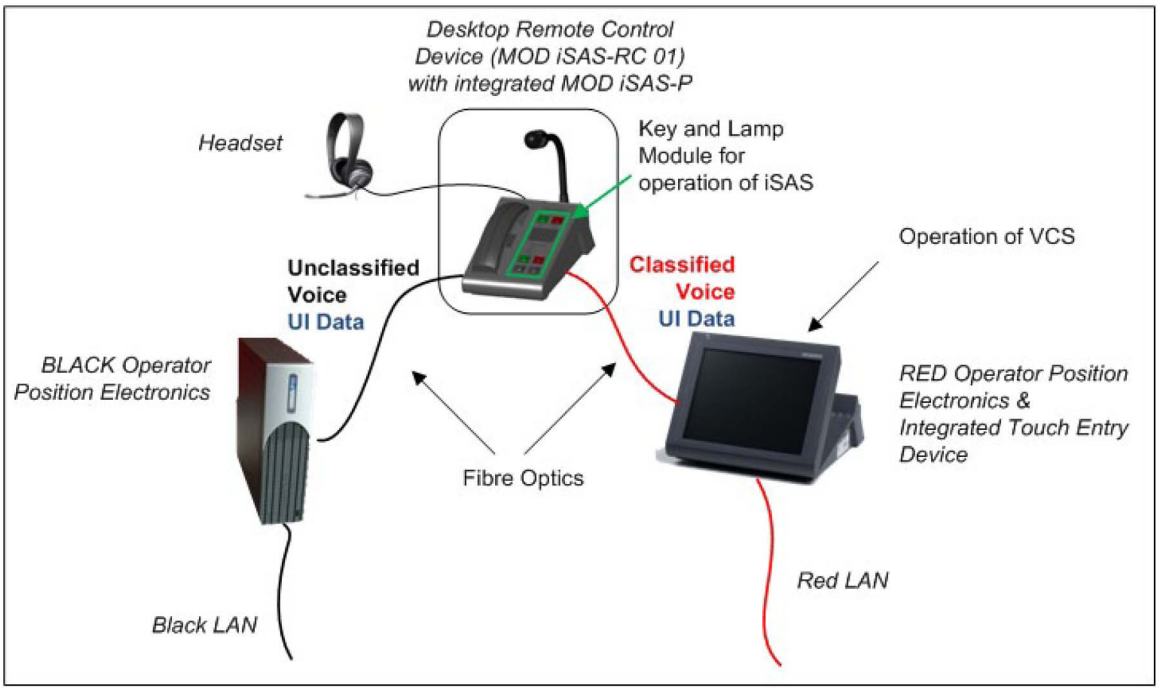

Fig. 1-4: TOE and Operator Position in a Desktop Setup – Operation via Desktop Remote Control Device

During normal operation the TOE is used by a single user/operator (S.User). During training a coach can connect an audio device in parallel to the operator/trainee. In this case the VCS provides the coach with the possibility to override the operator.

The TOE provides audio interfaces for the following set of audio devices:

- Operator audio devices:
  - Binaural/Monaural Headset (OP_Headset)
  - Handset
  - Handheld/Gooseneck Microphone (Gooseneck)
  - Loudspeaker
- Coach audio devices:
  - Binaural/Monaural Headset (CO_Headset)

In order to support this set of audio devices the TOE can handle multiple receive (RX) and transmit (TX) audio streams from both the RED and BLACK VCS.

1.4.2. Security Boundaries

1.4.2.1. Physical Scope

The physical scope of the TOE consists of:

- MOD iSAS-P hardware
- MOD iSAS-RC 01 hardware
- MOD iSAS-RC 02 hardware
- PLD firmware implementing the security functions of the MOD iSAS-P
- Associated guidance documentation.

The MOD iSAS-P hardware consists of the following main components:

- Secure/Insecure Processing Unit (S/I-PU) implements the main security functions of the MOD iSAS-P
- Secure Transfer Unit (SEC-TU) - Programmable Logic Device (PLD) for dedicated secure processing
- Insecure Transfer Unit (INSEC-TU) - Programmable Logic Device (PLD) for dedicated insecure processing
- Mechanics

The front and rear view of the TOE is shown in Fig. 1-5.

Fig. 1-5: MOD iSAS-P Front (Left) and Rear (Right) View

The Remote Control Device is implemented as Key and Lamp module. The Remote Control Device is available in two mechanical designs:

- MOD iSAS-RC 01: Desktop Version (see Fig. 1-6)
- MOD iSAS-RC 02: Console Version (see Fig. 1-7)

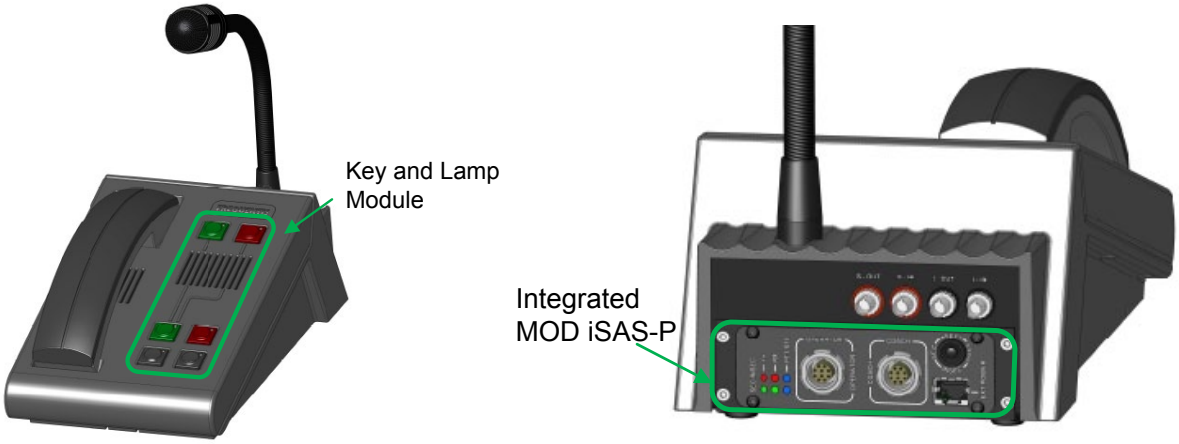

Fig. 1-6: Front and Rear View Remote Control Device - Desktop Version (MOD iSAS-RC 01)

Fig. 1-7: Remote Control Device – Console Version (MOD iSAS-RC 02)

1.4.2.2. Logical Scope

The TOE logical scope and boundary consists of the security functions/features provided/controlled by the TOE.

The TOE provides the following security functions (see also Fig. 1-8):

- Voice Information Flow Control (TSF.VFC)
- User Interface Data Flow Control (TSF.DFC)
- Management Interface (TSF.MNI)
- Protection of TSF (TSF.PRT)

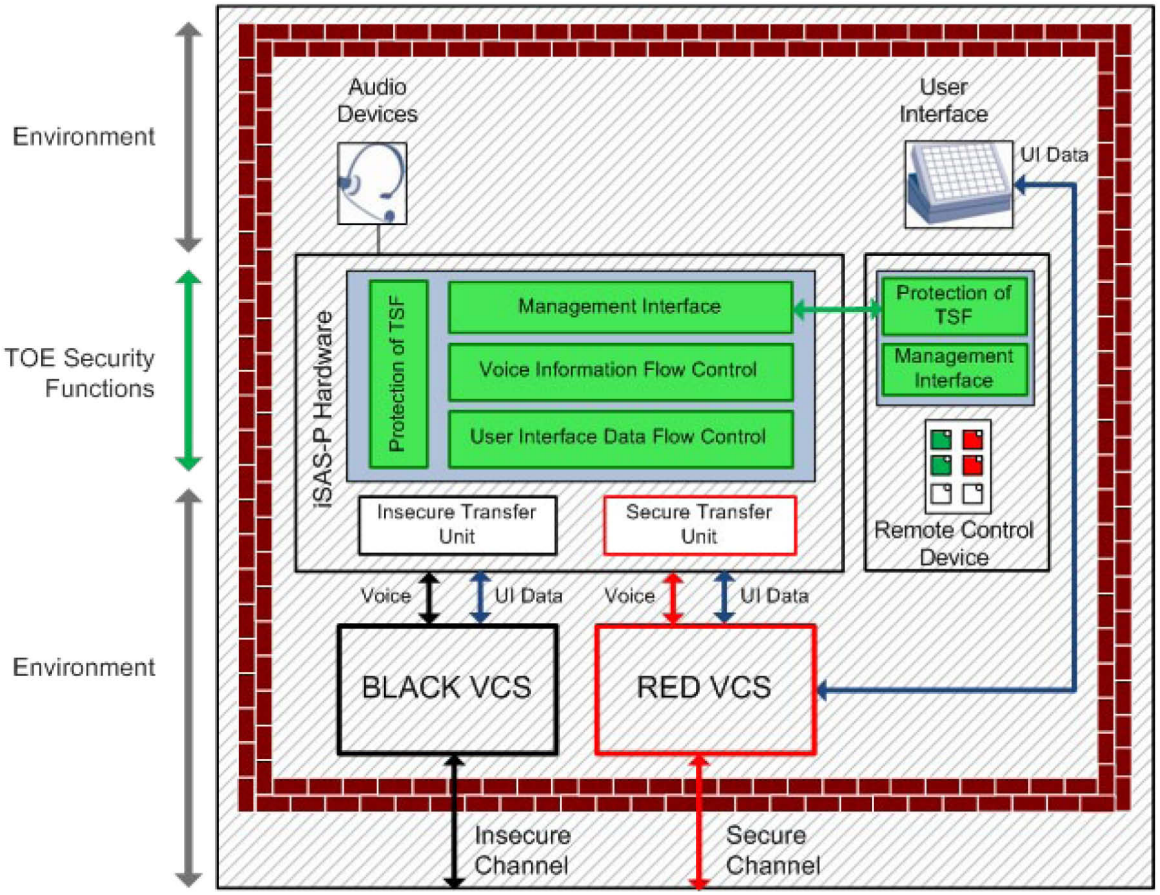

Fig. 1-8: Logical Scope of the TOE

Voice Information Flow Control

Microphone_Inputs are switched either to the RED or BLACK VCS by a common TX selector. The TX selector provides two positions:

- SECURE: Transmission of CLASSIFIED Voice Information
- INSECURE: Transmission of UNCLASSIFIED Voice Information

The TX selector is controlled by the user (S.User).

Each audio device has its dedicated Push To Talk (PTT) input. The user (S.User) needs to press PTT for voice transmission. The TOE disconnects inactive Microphone_Inputs (no PTT).

All voice information received from the RED and BLACK VCS is routed to the Earpiece_Outputs according to a common RX selector. The RX selector provides three positions:

- SECURE: Reception of CLASSIFIED voice information
- INSECURE: Reception of UNCLASSIFIED voice information
- BOTH: Simultaneous reception of CLASSIFIED and UNCLASSIFIED voice information

The RX selector is controlled by the user (S.User).

User Interface Data Flow Control

The operator uses a common user interface (e.g. touch entry device) to control both the RED and the BLACK VCS. The common user interface – that is part of the RED VCS – communicates the User_Interface_Data to the BLACK VCS via the TOE.

The TOE mediates the flow of User_Interface_Data between the RED VCS and the BLACK VCS in order to prevent the user interface connection from being misused to bypass the Voice Information Flow Control.

Management Interface

The TOE provides an assured indication of the RX and TX state via LEDs at the MOD iSAS-P housing.

The TOE includes two alternative key and lamp modules for remote control (MOD iSAS-RC 01 and MOD RC 02).

Additionally the TOE provides a remote control interface for operation via an external user interface that is part of the RED VCS (e.g. touch entry device).

Protection of TSF

The TOE provides a Fail Secure security function.

1.4.2.3. Out of Scope

The following firmware and hardware features are outside the scope of the defined TSF and are therefore not evaluated:

- Non-TOE firmware for Secure Transfer Unit
- Non-TOE firmware for Insecure Transfer Unit
- Audio device(s)
- RED VCS including the user interface (e.g. touch entry device)
- BLACK VCS

---------- END OF SECTION ----------

2. Conformance claims

2.1. CC Conformance Claim

This Security Target and the TOE:

- claims conformance to CC version 3.1 R2
- is CC Part 2 conformant
- is CC Part 3 conformant

2.2. PP Claims, Package Claim

This Security Target:

- does not claim conformance to any Protection Profile (PP)
- is EAL 4 augmented by components:
  - ASE_TSS.2
  - ADV_INT.3
  - AVA_VAN.5

2.3. Conformance Rationale

PP-related conformance claim rationale

This ST does not claim conformance to any PP, so there is no rationale related to this.

Package-related conformance claim rationale

This ST is EAL4 augmented, as ASE_TSS.2, ADV_INT.3 and AVA_VAN.5 were added to the EAL 4 package. The EAL4 package as well as the additional assurance components contain no uncompleted operations.

---------- END OF SECTION ----------

3. Security Problem Definition

This section analyses and defines the security problem that is to be addressed.

3.1. Assets

The only asset identified for the TOE is the CLASSIFIED voice information processed by the TOE for which a loss of confidentiality must be prevented.

3.2. User

The TOE can be simultaneously used by up to two types of users:

- Operator: During normal operation the TOE is used by a single user – the Operator. The Operator communicates with the TOE and VCS via a set of audio devices (OP_Headset, Handset, Gooseneck, Loudspeaker).
- Coach: For training purposes a Coach can connect an audio device (CO_Headset) in parallel to the Operator. In this case the VCS (not the TOE) provides the Coach with the possibility to override the Operator.

All users with physical access to the TOE have the permission to use any of its audio devices and/or operate the TX and RX selector. Therefore, the TOE does not identify the users and assign them to different roles. From the point of the TOE a single role exists – the S.User (see Tab. 3-1).

Subject	Remark
S.User	All users of the TOE (Operator and Coach) that communicate with the TOE via any of its audio devices and/or operate the TX and RX selector. S.User has physical access to the TOE.

Tab. 3-1: TOE Users

3.3. Threat Agents

Following threat agents where identified that can adversely act on the assets.

Threat Agent	Adverse Action
TA.External	A human or a process acting on his behalf being located outside the TOE and outside the operations site. The goal of the TA.External is to pick up CLASSIFIED voice information. TA.External has access to nearly unlimited resources in terms of money and time. Therefore the TA.External has a high attack potential in terms of CC.
TA.User	An end-user of the TOE with no intent to perform unauthorized actions. TA.User may unintentionally perform an unauthorized action and thereby facilitate TA.External access to CLASSIFIED voice information.
TA.Technician	A person responsible to install and maintain the TOE with no intent to perform unauthorized actions. TA.Technician may unintentionally perform an unauthorized action and thereby facilitate TA.External access to CLASSIFIED voice information.

TA.Malfunction	A Malfunction of the TOE might facilitate TA.External access to CLASSIFIED voice information. Malfunctions to be considered are limited to single failures.

Tab. 3-2: Threat Agents

3.4. Assumptions

A.Physical_Protection *Physical Protection*

The TOE and the RED and BLACK VCS are installed in a physically protected area (operations site), at least approved for the highest security level of information handled in the TOE.

A.TEMPEST_Facility *Tempest Facility Zone*

The TOE is operated in a TEMPEST facility zone that allows the use of COTS products for the processing of the highest security level of information handled in the TOE.

A.TEMPEST_Evaluation *Prevention of compromising emanation*

The TOE is subject to a TEMPEST evaluation, which is carried out independent of the Common Criteria certification.

The TEMPEST evaluation of the TOE prevents unacceptable compromising electromagnetic emissions and ensure that the interface to the BLACK VCS does not contain unintentional CLASSIFIED voice information.

A.Training *User Training*

All users are trained in the correct use of the TOE and VCS and follow the operational guidelines.

A.Clearance *User Clearance*

All users have a minimum clearance for the highest security level of information handled in the TOE, and are authorized for all information handled by the TOE.

User activity shall be monitored to the extent that sanctions can be applied when malfeasance occurs.

A.Installation *TOE Installation and Maintenance*

The TOE is installed and maintained according to the installation and maintenance guidelines.

A.Headset *Headsets devices*

Appropriate headsets and associated cables prevent unacceptable acoustic coupling between:

- Earpiece and microphone of the audio device.
- Ambient noise and microphone

Note: This assumption does not hold for the handset and Gooseneck.

A.VCS *Separation of RED and BLACK VCS*

The voice information transmitted by the RED VCS is strictly separated from the voice information transmitted by the BLACK VCS. Vulnerabilities associated with the VCS or its connections to the TOE are a concern of the application scenario and not the TOE.

All communication channels of the RED VCS that leave the operations site are either encrypted with approved crypto devices or implemented as approved circuits (secure channels). Vulnerabilities associated with the RED communication channels are a concern of the application scenario and not the TOE.

A.RED_VCS_Accreditation *Accreditation of RED VCS*

The RED VCS is accredited for the highest security classification processed in the system.

3.5. Threats

This section shows the threats that are to be countered by the TOE, its operational environment, or a combination of the two.

T.Illicit_Information_Flow

CLASSIFIED voice information might be transferred to insecure channels.

Threat Agent:

- TA.External
- TA.Malfunction in combination with TA.External

Endangered Asset:

- Confidentiality of CLASSIFIED voice information

Adverse Action:

- The TOE insufficiently protects CLASSIFIED voice information from being transferred to the BLACK VCS. Persons (TA.External) outside the physically protected area pick up the CLASSIFIED voice information from the insecure channels.

- A malfunction in the TOE causes CLASSIFIED voice information to be transferred to the BLACK VCS. Persons (TA.External) outside the physically protected area pick up the CLASSIFIED voice information from the insecure channels.

T.Tx_Indication_Spoofing

A user may think that he is speaking via a secure channel while he is actually speaking via an insecure channel.

Threat Agent:

- TA.User in combination with TA.External
- TA.Malfunction in combination with TA.User and TA.External

Endangered Asset:

- Confidentiality of CLASSIFIED voice information

Adverse Action:

- The user may think that the Microphone_Inputs are connected to the RED VCS while they are actually connected to the BLACK VCS. The user then speaks CLASSIFIED. The CLASSIFIED voice information is transmitted to the BLACK VCS and is picked up from the insecure channels by persons (TA.External) outside the physically protected area.
- TOE malfunction gives the user an indication that the Microphone_Inputs are not connected to the BLACK VCS, while in reality the Microphone_Inputs are connected to the BLACK VCS. The user then speaks CLASSIFIED. The CLASSIFIED voice information is transmitted to the BLACK VCS and is picked up from the insecure channels by persons (TA.External) outside the physically protected area.

T.Rx_Indication_Spoofing

A user may think that he is hearing UNCLASSIFIED voice information while he is actually hearing CLASSIFIED voice information.

Threat Agent:

- TA.User in combination with TA.External
- TA.Malfunction in combination with TA.User and TA.External

Endangered Asset:

- Confidentiality of CLASSIFIED voice information

Adverse Action:

- The user may think the Earpiece_Outputs are not connected to RED VCS while they are actually connected. The user activates an audio device then speaks UNCLASSIFIED. The CLASSIFIED voice information from the earpiece of the audio device is picked up by the microphone and transmitted

to the BLACK VCS. Persons (TA.External) outside the physically protected area pick up the CLASSIFIED voice information from the insecure channels.

- TOE malfunction gives the user an indication that the Earpiece_Outputs are not connected to the RED VCS, while in reality the Earpiece_Outputs are connected to the RED VCS. The user activates an audio device then speaks UNCLASSIFIED. The CLASSIFIED voice information from the earpiece of the audio device is picked up by the microphone and transmitted to the BLACK VCS. Persons (TA.External) outside the physically protected area pick up the CLASSIFIED voice information from the insecure channels.

T.Acoustic_Coupling

Microphones connected to insecure channels might pick up CLASSIFIED speech.

Threat Agent:

- TA.User in combination with TA.External

Endangered Asset:

- Confidentiality of CLASSIFIED voice information

Adverse Action:

- When the microphone is connected to the BLACK VCS, and the earpiece is connected to the RED VCS the microphone might pick up CLASSIFIED voice information from the earphone. The CLASSIFIED voice information is transmitted to the BLACK VCS and picked up from insecure channels by persons (TA.External) outside the physically protected area.
- When the microphone is connected to the BLACK VCS and another user (TA.User) in the room TA.User speaks CLASSIFIED voice information this CLASSIFIED voice information might be picked up by the microphone. The CLASSIFIED voice information is transmitted to the BLACK VCS and picked from insecure channels by persons (TA.External) outside the physically protected area.

T.Non-Permissible_Data_Inbound

A threat agent with access to the BLACK VCS may send non-permissible data through the TOE that result in gaining access to CLASSIFIED voice information in TOE or the RED VCS.

Threat Agent:

- TA.External

Endangered Asset:

- Confidentiality of CLASSIFIED voice information

Adverse Action:

- TA.External gains access to the BLACK VCS via the external interfaces leaving the operations sites. Subsequently TA.External modifies the BLACK VCS. The modified BLACK VCS sends non-permissible data through the User_Interface_Data connection to the RED VCS. The non-permissible data result in the BLACK VCS gaining access to CLASSIFIED voice information. The BLACK VCS forwards the CLASSIFIED information to persons (TA.External) outside the physically protected area via insecure channels.

T.Non-Permissible_Data_Outbound

A threat agent with access to the RED VCS may send non-permissible data through the TOE that result in CLASSIFIED voice information being transferred to the BLACK VCS. This voice information may be monitored by an attacker and used to his advantage.

Threat Agent:

- TA.External

Endangered Asset:

- Confidentiality of CLASSIFIED voice information

Adverse Action:

- TA.External gains access to the RED as well as the BLACK VCS via the external interfaces leaving the operations sites. Subsequently TA.External modifies the RED VCS and the BLACK VCS. The modified RED VCS misuses the User_Interface_Data connection to the BLACK VCS in order to transfer a continuous CLASSIFIED voice stream. The BLACK VCS forwards this information to Persons (TA.External) outside the physically protected area via insecure channels. This enables TA.External to monitor the CLASSIFIED voice communication and use this information to his advantage.

Note: Due to the assumptions concerning the operational environment no threat of physical tampering exists, if the TOE is installed at the operations site. Protection against physical tampering prior to installation at the operations site is implicitly provided by the assurance packet chosen for the TOE (Family ALC_DEL - Delivery procedures).

Note: Protection against logical tampering (modification of TSF code or data structures) is implicitly provided by the assurance packet chosen for the TOE (ADV.ARC.1).

3.6. Organizational Security Policies

The security target identifies no organization security policies (OSPs) to which the TOE must comply.

---------- END OF SECTION ---------

4. Security Objectives

4.1. Security Objectives for the TOE

OT.Tx_Status *Transmission Status indication*

The user shall unambiguously be made aware whether the Microphone_Inputs are connected to a BLACK VCS.

OT.Rx_Status *Receive Status Indication*

The user shall unambiguously be made aware whether the Earpiece_Outputs are connected to a RED VCS.

OT.Tx_Flow_Control *Transmission Flow Control*

Voice information from the Microphone_Inputs assigned to the RED VCS by the user shall not be transferred to the BLACK VCS.

OT.Rx_Flow_Control *Receive Flow Control*

Classified voice information received from the RED VCS shall not be transferred to the BLACK VCS.

Voice information received from the RED and BLACK VCS shall be routed to the Earpiece_Outputs according to the user selection (SECURE/INSECURE/BOTH).

OT.Acoustic_Coupling *Prevention of Acoustic Coupling*

To prevent unacceptable acoustic coupling via audio devices, the TOE shall ensure the following:

- Inactive Microphone_Inputs (no PTT) shall be disconnected.
- If transmission via the handset or Gooseneck is active (PTT), the TOE shall prevent that CLASSIFIED voice information is received from the RED VCS while the Microphone_Inputs are connected to the BLACK VCS.
- If the handset is not in use (ON-Hook), the TOE shall prevent that voice information is received by the handset.
- The Loudspeaker_Output shall only be connected to the BLACK VCS.

OT.Mediate_Data *Mediation of user interface data*

The TOE shall mediate the flow of User_Interface_Data between the RED VCS and the BLACK VCS in order to prevent the user interface connection from being misused to:

- Access classified voice information from the BLACK VCS.

- Transmit comprehensible voice information continuously from the RED VCS to the BLACK VCS.

OT.Fail_Secure *Fail Secure Behaviour*

The TOE shall prevent that the Microphone_Inputs are erroneously connected to the BLACK VCS in the event of a single failure of the TSF.

4.2. Security Objectives for the Operational Environment

OE.Physical_Protection *Physical Protection of Operations Site*

The operation site shall have physical protection, which is at least approved for the highest level of information handled in the TOE.

OE.TEMPEST_Facility *Tempest Facility Zone*

The TOE shall be operated in a TEMPEST facility zone that allows the use of COTS products for the processing of the highest security level of information handled in the TOE.

OE.TEMPEST_Evalutation *Prevention of compromising emanation*

The TOE shall be subject to a TEMPEST evaluation, which is carried out independent of the Common Criteria certification.

The TEMPEST evaluation of the TOE shall prevent unacceptable compromising electromagnetic emissions and ensure that the interface to the BLACK VCS does not contain unintentional CLASSIFIED voice information.

OE.Physical_Access *Physical Access of TOE*

Only authorized persons shall be given physical access to the TOE.

OE.Clearance *Clearance of TOE Users*

All users shall have a minimum clearance for the maximum-security level of information handled in the TOE. User activity shall be monitored and user shall be accountable for their actions.

OE.Installation *Installation and Maintenance of TOE*

The TOE shall be installed and maintained according to the installation and maintenance guidelines.

The installation shall assure that the RX and TX status of the TOE is visible to the operator.

OE.User_Training *User Training*

The users shall be trained to use the TOE.

If the TOE is controlled via an external user interface, that is not part of the TOE, the operators shall be trained to check the assured RX and TX status indication at the TOE.

OE.Headset *Use of Appropriate Headset*

Appropriate Headsets shall be used in order to prevent unacceptable acoustic coupling between:

- Earpiece and microphone, when receiving CLASSIFIED voice information while transmitting UNCLASSIFIED voice information.
- A neighbouring user and the microphone of the user, when the neighbouring user is talking CLASSIFIED information while the user transmits UNCLASSIFIED voice information.

OE.Neighbour_Acoustic_Coupling *Prevention of Acoustic Coupling from Neighbouring Users*

Each user shall be made aware of the TX state of ongoing transmission of a neighbouring user. Operational procedures, not technical solutions shall regulate concurrent use of CLASSIFIED and UNCLASSIFIED conversations to prevent acoustic coupling of CLASSIFIED conversations to be transmitted on UNCLASSIFIED communication channels.

OE.VCS *Separation of RED and BLACK VCS*

The voice information transmitted by the RED VCS shall be strictly separated (logical or physical) from the voice information transmitted by the BLACK VCS.

All communication channels of the RED VCS that leave the operations site either shall be encrypted with approved crypto devices or implemented as approved circuits (secure channels).

OE.RED_VCS_Accreditation *Accreditation of RED VCS*

The RED VCS shall be accredited for the highest security classification processed in the system.

4.3. Security Objectives Rationale

Assumptions - Threats- Policies / Security Objectives	OT.Tx_Status	OT.Rx_Status	OT.Tx_Flow_Control	OT.Rx_Flow_Control	OT.Acoustic_Coupling	OT.Mediate_Data	OT.Fail_Secure	OE.Physical_Protection	OE.TEPMEST_Facility	OE.TEMPEST_Evaluation	OE.Physical_Access	OE.Clearance	OE.Installation	OE.User_Training	OE.Headset	OE.Neighbour_Acoustic_Coupling	OE.VCS	OE.RED_VCS_Accreditation
A.Physical_Protection								x			x		x					
A.TEMPEST_Facility									x									
A.TEMPEST_Evaluation										x								
A.Training														x				
A.Clearance												x						
A.Installation													x					
A.Headset															x			
A.VCS																	x	
A.RED_VCS_Accreditation																		x
T.Illicit_Information_Flow			x	x			x											
T.Tx_Indication_Spoofing	x						x						x					
T.Rx_Indication_Spoofing		x			x								x		x			
T.Acoustic_Coupling					x										x	x		
T.Non-Permissible_Data_Inbound						x												
T.Non-Permissible_Data_Outbound						x												x

Tab. 4-1: Mapping of Objectives to Assumptions, Threats and Policies

---------- END OF SECTION ----------

5. Extended Component Definition

This ST does not contain extended SFRs or extended SARs.

---------- END OF SECTION ----------

6. Security Requirements

6.1. Security Functional Requirements (SFRs)

This section contains the functional requirements that are provided by the TOE. These requirements consist exclusively of functional components from Part 2 of the Common Criteria (CC).

Words which appear in *italics* are tailorings of requirement definitions via an assignment operation.

Words which appear in **bold** are tailorings of requirement definitions via a selection operations.

Words which appear in ***bold italics*** are tailorings of requirement definitions via a selection operations followed by an assignment operation.

Iterations are identified by appending an identification ("_RX", "_TX", "_UI") to the short name of iterated components and elements.

The Tab. 6-1 list the functional components included in this ST.

Component	Name
FAU_ARP.1	Security alarms
FAU_SAA.1	Potential violation analysis
FDP_ETC.1	Export of user data without security attributes
FDP_IFC.1	Subset Information flow control policy
FDP_IFF.1	Simple security attributes
FDP_IFF.5	No illicit information flows
FDP_ITC.1	Import of user data without security attributes
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_SMF.1	Specification of Management Functions
FPT_FLS.1	Failure with preservation of secure state

Tab. 6-1: TOE Security Functional Requirements

6.1.1. Terms and definition for information flow control SFPs

This section contains terms and definitions used in the subsequent SFRs to define the information flow control SFPs. The terms and definitions are listed here by category. In addition, the glossary (see chapter 9) also contains these terms and definitions in alphabetical order.

6.1.1.1. Information flow control SFPs

The following table lists the information flow control SFPs defined in the subsequent SFRs.

SFP	Description
TX_SFP	Information flow control SFP for transmission of voice information (Voice_TX_Information).
RX_SFP	Information flow control SFP for reception of voice information (Voice_RX_Information).
Data_SFP	Information flow control SFP for communication of user interface data (User_Interface_Data).

Tab. 6-2: Information flow control SFPs

6.1.1.2. Information

The following table lists the information under control of the information flow control SFPs.

Information	Description	SFP
Voice_TX_Information	Voice information from the user indented for transmission to the VCS.	TX_SFP
Voice_RX_Information	Voice information from the VCS indented for reception by the user.	RX_SFP
User_Interface_Data	The user controls both the RED and the BLACK VCS via a common user interface. User_Interface_Data is information that is communicated via the TOE for this purpose.	Data_SFP

Tab. 6-3: Information

6.1.1.3. Subjects

The following table lists the subjects under control of the information flow control SFPs.

Note: For the definition of the SFPs this ST makes use of the term "subject" as defined in Common Criteria, Version 3.1, Release 2, Part 2, Annex F.5 [1]. This ST describes subjects of the SPF in the generic sense of input/output channels and interfaces of the TOE.

Subject	Description	SFP
Analogue Audio Inputs		
Microphone_Inputs	Microphone inputs of the TOE to all audio devices: Mic_Input_OP_Headset and Mic_Input_CO_Headset and Mic_Input_Handset and Mic_Input_Gooseneck	TX_SFP
Mic_Input_OP_Headset	Microphone input of the TOE to the binaural/monaural headset for use by the operator.	
Mic_Input_CO_Headset	Microphone input of the TOE to the binaural/monaural headset for use by the coach.	

Mic_Input_Handset	Microphone input of the TOE to the handset.	
Mic_Input_Gooseneck	Microphone input of the TOE to the handheld/gooseneck microphone.	
Analogue Audio Outputs		
Earpiece_Outputs	Earpiece outputs of the TOE to the headsets and speaker of the handset: Ear_Output_OP_Headset and Ear_Output_CO_Headset and Ear_Output_Handset	RX_SFP
Ear_Output_OP_Headset	Earpiece output of the TOE to the binaural/monaural headset for use by the operator.	
Ear_Output_CO_Headset	Earpiece output of the TOE to the binaural/monaural headset for use by the coach.	
Ear_Output_Handset	Speaker output of the TOE to the handset.	
Loudspeaker_Output	Audio output of the TOE to the loudspeaker.	
Interfaces to VCSs		
RED_VCS_Interface	Interface of the TOE to the BLACK VCS.	TX_SFP, RX_SFP, Data_SFP
BLACK_VCS_Interface	Interface of the TOE to the RED VCS.	

Tab. 6-4: Subjects

6.1.1.4. Security Attributes

The following table lists the **information security attributes**.

Information	Security Attribute	Description
Voice_TX_Information, Voice_RX_Information	CLASSIFIED	CLASSIFIED information is information regarded as sensitive by the security authorities for the owners of the TOE (e.g. Information up to the German Classification Level VS-GEHEIM or equivalent NATO/national classification levels).
	UNCLASSIFIED	UNCLASSIFIED information is information regarded as not sensitive to disclosure by the security authorities for the owners of the TOE. (e.g. Information up to the German Classification Level VS-NfD or equivalent NATO/national classification levels).
User_Interface_Data	Transport_Data_Frame	The data frames of the transport level protocol used to communicate User_Interface_Data via the TOE.

	Checksum of the Transport_Data_Frame	The transport data frame includes a checksum in order to detect transmission errors.
	Application_Protocol	The application level protocol used to communicate User_Interface_Data via the TOE.
	Application_Message_Type	The application message type defines the semantic of an Application_Protocol message. E.g.: The application message type “OBJ STATE CHANGED”: means that a state of an object at the common user interface has changed (e.g. a button was pressed).
	Payload_Data_Rate	Number of Payload bits that are communicated via the TOE per unit of time. Payload is all content of User_Interface_Data that is not inspected for semantic correctness by the TOE (e.g. the numeric value identifying the object at the common user interface).

Tab. 6-5: Information Security Attributes

The following table lists the **subject security attributes**.

Subject	Security Attribute	Description
Earpiece_Outputs	SECURE	Security attribute of a subject that is allowed to receive CLASSIFIED Voice_RX_Information.
	INSECURE	Security attribute of a subject that is allowed to receive UNCLASSIFIED Voice_RX_Information
	BOTH	Security attribute of a subject that is allowed to receive CLASSIFIED as well as UNCLASSIFIED Voice_RX_Information

Tab. 6-6: Subject Security Attributes

6.1.2. Security audit (Class FAU)

This section specifies the security audit requirements.

6.1.2.1. FAU_ARP.1 Security alarms

FAU_ARP.1.1

The TSF shall take [

The following actions:

- *visually indicate a failure to warn the S.User,*
- *immediately stop transmission of User_Interface_Data and*
- *stop operation after a defined time (giving the S.User the possibility to react accordingly)*]

upon detection of a potential security violation.

6.1.2.2. FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*none*] known to indicate a potential security violation;

b) [*Violations of at least one of the following Data_SFP rules even though the User_Interface_Data message has been transmitted error-free (Transport_Data_Frame is syntactically correct and the Checksum of the Transport_Data_Frame is correct):*

- *The Application_Protocol is syntactically correct*
- *The Application_Message_Type is permissible*
- *The Payload_Data_Rate from RED_VCS_Interface to BLACK_VCS_Interface (Outbound) does not exceed the data rate required for comprehensive continuous voice transmission].*

6.1.3. User data protection (Class FDP)

This section specifies the information flow control requirements.

6.1.3.1. FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1.1

The TSF shall enforce the [*information flow control TX_SFP and RX_SFP*] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2

The TSF shall export the user data without the user data's associated security attributes.

6.1.3.2. FDP_IFC.1_TX Subset information flow control – Voice TX

FDP_IFC.1.1_TX

The TSF shall enforce the [*information flow control TX_SFP*] on [

the following subjects:

- *Microphone_Inputs*
  - *Mic_Input_OP_Headset*
  - *Mic_Input_CO_Headset*
  - *Mic_Input_Handset*
  - *Mic_Input_Gooseneck*
- *RED_VCS_Interface*
- *BLACK_VCS_Interface*

For the following information:

- *Voice_TX_Information*].

6.1.3.3. FDP_IFC.1_RX Subset information flow control – Voice RX

FDP_IFC.1.1_RX

The TSF shall enforce the [*information flow control RX_SFP*] on [

the following subjects:

- *Earpiece_Outputs*
  - *Ear_Output_OP_Headset*
  - *Ear_Output_CO_Headset*
  - *Ear_Output_Handset*
- *Loudspeaker_Output*
- *RED_VCS_Interface*
- *BLACK_VCS_Interface*

for the following information:

- *Voice_RX_Information*].

6.1.3.4. FDP_IFC.1_UI Subset information flow control – UI Data

FDP_IFC.1.1_UI

The TSF shall enforce the [*information flow control Data_SFP*] on [

the following subjects:

- *RED_VCS_Interface*
- *BLACK_VCS_Interface*

For the following information:

- *User_Interface_Data*].

6.1.3.5. FDP_IFF.1_TX Simple security attributes – Voice TX

FDP_IFF.1.1_TX

The TSF shall enforce the [*information flow control TX_SFP*] based on the following types of subject and information security attributes: [

- *Voice_TX_Information security attributes (as determined by the TX selector)*
  - *CLASSIFIED*
  - *UNCLASSIFIED*].

FDP_IFF.1.2_TX

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

Active Voice Transmission (PTT active):

- *CLASSIFIED Voice_TX_Information shall be transmitted to the RED_VCS_Interface*
- *UNCLASSIFIED Voice_TX_Information shall be transmitted to the BLACK_VCS_Interface*].

FDP_IFF.1.3_TX

The TSF shall enforce the [*no additional information flow control SFP rules*].

FDP_IFF.1.4_TX

The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5_TX

The TSF shall explicitly deny an information flow based on the following rules: [*none*].

6.1.3.6. FDP_IFF.1_RX Simple security attributes – Voice RX

FDP_IFF.1.1_RX

The TSF shall enforce the [*information flow control RX_SFP*] based on the following types of subject and information security attributes: [

- *Voice_RX_Information security attributes is determined by the source*
  - *CLASSIFIED*
  - *UNCLASSIFIED*
- *Earpiece_Outputs security attributes are determined by the RX selector:*
  - *SECURE, if RX selector = SECURE*
  - *INSECURE; if RX selector = INSECURE*
  - *BOTH, if RX selector = BOTH*].

FDP_IFF.1.2_RX

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

Voice Reception:

- *CLASSIFIED Voice_RX_Information shall be received by the Earpiece_Outputs, if its security attribute (determined by the RX selector) is SECURE*
- *UNCLASSIFIED Voice_RX_Information shall be received by the Earpiece_Outputs, if its security attribute (determined by the RX selector) is INSECURE*
- *CLASSIFIED Voice_RX_Information as well as the UNCLASSIFIED Voice_RX_Information shall be received by the Earpiece_Outputs, if its security attribute (determined by the RX selector) is BOTH*
- *UNCLASSIFIED Voice_RX_Information shall be received by the Loudspeaker_Output*].

FDP_IFF.1.3_RX

The TSF shall enforce the [*no additional information flow control SFP rules*].

FDP_IFF.1.4_RX

The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5_RX

The TSF shall explicitly deny an information flow based on the following rules: [

Voice Reception:

- *CLASSIFIED Voice_RX_Information shall not be received if UNCLASSIFIED Voice_TX_Information is transmitted via the Mic_Input_Handset or Mic_Input_Gooseneck (PTT active)*
- *The CLASSIFIED Voice_RX_Information shall not be received by the Ear_Output_Handset, if the handset is inactive (ON-Hook)*].

6.1.3.7. FDP_IFF.1_UI Simple security attributes – UI data

FDP_IFF.1.1_UI

The TSF shall enforce the [*information flow control Data_SFP*] based on the following types of subject and information security attributes: [

- *Transport_Data_Frame*
- *Checksum of the Transport_Data_Frame*
- *Application_Protocol*
- *Application_Message_Type*
- *Payload_Data_Rate*].

FDP_IFF.1.2_UI

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

User Interface (UI) Data Transmission between RED_VCS_Interface and BLACK_VCS_Interface (both directions):

- *The Transport_Data_Frame is syntactically correct*
- *The Checksum of the Transport_Data_Frame is correct*
- *The Application_Protocol is syntactically correct*
- *The Application_Message_Type is permissible*].

FDP_IFF.1.3_UI

The TSF shall enforce the [*no additional information flow control SFP rules*].

FDP_IFF.1.4_UI

The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5_UI

The TSF shall explicitly deny an information flow based on the following rules: [

User Interface (UI) Data Transmission:

- *The Payload_Data_Rate from RED_VCS_Interface to BLACK_VCS_Interface (Outbound) exceeds the data rate required for comprehensive continuous voice transmission*].

6.1.3.8. FDP_IFF.5_TX No illicit information flows – Voice TX

FDP_IFF.5.1 _TX

The TSF shall ensure that no illicit information flows exist to circumvent [*TX_SFP*].

6.1.3.9. FDP_IFF.5_RX No illicit information flows – Voice RX

FDP_IFF.5.1_RX

The TSF shall ensure that no illicit information flows exist to circumvent [*RX_SFP*].

6.1.3.10. FDP_IFF.5_UI No illicit information flows – UI Data

FDP_IFF.5.1_UI

The TSF shall ensure that no illicit information flows exist to circumvent [*Data_SFP*].

6.1.3.11. FDP_ITC.1_TX Import of user data without security attributes – Voice TX

FDP_ITC.1.1_TX

The TSF shall enforce the [*information flow control TX_SFP*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2_TX

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3_TX

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [

- *Voice_TX_Information is imported from the Microphone_Inputs, if the corresponding PTT is active*
- *Voice_TX_Information security attributes are determined by the TX selector:*
  - *CLASSIFIED, if TX selector = SECURE*
  - *UNCLASSIFIED; if TX selector = INSECURE*].

6.1.3.12. FDP_ITC.1_RX Import of user data without security attributes – Voice RX

FDP_ITC.1.1_RX

The TSF shall enforce the [*information flow control RX_SFP*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2_RX

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3_RX

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [

- *Voice_RX_Information security attributes are determined by the VCS interface:*
  - *CLASSIFIED, if reception via RED_VCS_Interface*
  - *UNCLASSIFIED, if reception via BLACK_VCS_Interface*].

6.1.4. Security management (Class FMT)

This section specifies the management of several aspects of the TSF.

6.1.4.1. FMT_MSA.1_TX Management of security attributes – Voice TX

FMT_MSA.1.1_TX

The TSF shall enforce the [*information flow control TX_SFP*] to restrict the ability to [***set, indicate***] the security attributes [*CLASSIFIED / UNCLASSIFIED of Voice_TX_Information*] to [*S.User*].

6.1.4.2. FMT_MSA.1_RX Management of security attributes – Voice RX

FMT_MSA.1.1_RX

The TSF shall enforce the [*information flow control RX_SFP*] to restrict the ability to [***set, indicate***] the security attributes [*SECURE / INSECURE / BOTH of the Earpiece_Outputs*] to [*S.User*].

6.1.4.3. FMT_MSA.3_TX Static attribute initialization – Voice TX

FMT_MSA.3.1_TX

The TSF shall enforce the [*information flow control TX_SFP*] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2_TX

The TSF shall allow the [*none*] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.4. FMT_MSA.3_RX Static attribute initialization – Voice RX

FMT_MSA.3.1_RX

The TSF shall enforce the [*information flow control RX_SFP*] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2_RX

The TSF shall allow the [*none*] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.5. FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [

- *Set the state of the TX selector*
- *Set the state of the RX selector*
- *Set the PTT state*
- *Assured indication of the TX selector state to the S.User*
- *Assured indication of the RX selector state to the S.User*
- *Assured indication of the PTT state to the S.User*

during normal TOE operation].

6.1.5. Protection of the TSF (Class FPT)

This section relate to the integrity of the mechanisms that constitute the TSF.

6.1.5.1. FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [*Single failure of the TSF implementing the information flow control TX_SFP*].

6.2. Security Assurance Requirements (SARs)

Assurance requirement components are those of Evaluation Assurance Level 4 (EAL 4; Methodically designed, tested and reviewed) augmented by ASE_TSS.2, ADV_INT.3 and AVA_VAN.5.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_INT.3 Minimally complex internals
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.2 TOE summary specification with

	architectural design summary
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.2 Testing: security enforcing modules
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Tab. 6-7: Security Assurance Requirements

6.3. Security Requirements Rationale

6.3.1. SFRs rationale

6.3.1.1. Tracing between SFRs and security objectives

Security Objectives / Security Functional Requirements	FAU_ARP.1	FAU_SAA.1	FDP_ETC.1	FDP_IFC.1_TX	FDP_IFC.1_RX	FDP_IFC.1_UI	FDP_IFF.1_TX	FDP_IFF.1_RX	FDP_IFF.1_UI	FDP_IFF.5_TX	FDP_IFF.5_RX	FDP_IFF.5_UI	FDP_ITC.1_TX	FDP_ITC.1_RX	FMT_MSA.1_TX	FMT_MSA.1_RX	FMT_MSA.3_TX	FMT_MSA.3_RX	FMT_SMF.1	FPT_FLS.1
OT.Tx_Status																			x	
OT.Rx_Status																			x	
OT.Tx_Flow_Control			x	x			x			x			x		x		x		x	
OT.Rx_Flow_Control			x		x			x			x			x		x		x	x	
OT.Acoustic_Coupling								x					x							
OT.Mediate_Data	x	x				x			x			x								
OT.Fail_Secure																				x

Tab. 6-8: Tracing of SFRs to the Security Objectives

6.3.1.2. Fulfilment of TOE SFR dependencies

Component	Dependencies	Dependency fulfilled?
FAU_ARP.1	FAU_SAA.1	Yes
FAU_SAA.1	FAU_GEN.1	No
FDP_ETC.1	FDP_IFC.1	Yes
FDP_IFC.1_TX	FDP_IFF.1_TX	Yes
FDP_IFC.1_RX	FDP_IFF.1_RX	Yes
FDP_IFC.1_UI	FDP_IFF.1_UI	Yes
FDP_IFF.1_TX	FDP_IFC.1_TX	Yes
	FMT_MSA.3_TX	Yes
FDP_IFF.1_RX	FDP_IFC.1_RX	Yes
	FMT_MSA.3_RX	Yes
FDP_IFF.1_UI	FDP_IFC.1_UI	Yes

	FMT_MSA.3	No
FDP_IFF.5_TX	FDP_IFC.1_TX	Yes
FDP_IFF.5_RX	FDP_IFC.1_RX	Yes
FDP_IFF.5_UI	FDP_IFC.1_UI	Yes
FDP_ITC.1_TX	FDP_IFC.1_TX	Yes
	FMT_MSA.3_TX	Yes
FDP_ITC.1_RX	FDP_IFC.1_RX	Yes
	FMT_MSA.3_RX	Yes
FMT_MSA.1_TX	FDP_IFC.1_TX	Yes
	FMT_SMR.1	No
	FMT_SMF.1	Yes
FMT_MSA.1_RX	FDP_IFC.1_RX	Yes
	FMT_SMR.1	No
	FMT_SMF.1	Yes
FMT_MSA.3_TX	FMT_MSA.1_TX	Yes
	FMT_SMR.1	No
FMT_MSA.3_RX	FMT_MSA.1_RX	Yes
	FMT_SMR.1	No
FMT_SMF.1	-	-
FPT_FLS.1	-	-

Tab. 6-9: Security Requirements Dependencies

FAU_GEN.1 (Audit Data Generation) is not included, as the TOE does not perform the potential violation analysis based on audited events. Instead the TOE detects a potential misuse of User_Interface_Data to bypass the separation of CLASSIFIED and UNCLASSIFIED voice information by detecting a violation of certain Data_SFP rules. If the TOE detects such a violation, the TOE will react accordingly.

FMT_SMR (Security Management Roles) is not included because:

- Only authorized persons have physical access to the TOE (see OE.Physical_Access, OE.Physical_Protection, OE.Clearance)
- All users with physical access to the TOE (S.User) have the permission to manage the security attributes (operate the TX and RX selector) (see FMT_MSA.1).

No security management requirements for the User Interface Data Flow Control (Data_SFP) are included, as Data_SFP does not contain any security attributes that require initialisation or management.

6.3.1.3. Mutual support and internal consistency of security requirements

From the details given in this rationale it becomes evident that the functional requirements form an integrated whole and, taken together, are suited to meet all security objectives.

The core TOE functionality is represented by the requirements for information flow control (FDP_ETC.1, FDP_IFC.1, FDP_IFF.1, FDP_IFF.5 and FDP_ITC).

Furthermore a set of requirements is used to describe the way the flow control functions should be managed (FMT_MSA.1, FMT_MSA.3 and FMT_SMF.1).

A further set of requirements (FAU_SAA.1 and FAU_ARP.1) defines the rules to detect a potential security violation (user interface connection is being misused to bypass the Voice Information Flow Control) and the automatic response.

In the end this ST contains a set of SFRs which deals with malfunction of the TOE (FPT_FLS).

Therefore it becomes clear that the SFRs in this ST mutually support each other and form a consistent whole.

6.3.2. SAR rationale

EAL4 is the lowest assurance package, which includes source-code analysis. The source code analysis is necessary to assess the implementation quality and ensure that the TOE contains no malicious code. ZDv 54/100 stipulates that the security gateways protecting classified data have to be evaluated according to EAL4 ([2], Anlage 21 IT-Sicherheitsanforderungen, Lfd. Nr. 5.1.4). EAL4 is specified by NATO as the minimum EAL level for high robustness environments. Higher EAL levels (5, 6 or 7) would require a lot more effort for vendors and evaluators, because semi-formal or formal modelling has to be used ([1], part 2, chapter 8.7-8.9).

EAL4 is augmented by ASE_TSS.2 so that the TOE developer is required to describe at an early stage how the TOE protects itself against logical tampering and bypass.

EAL4 is augmented by ADV_INT.3 in order to make sure that the entire TSF is well structured, not overly complex and has been implemented using sound engineering principles.

EAL4 is augmented by AVA_VAN.5 because we assume attackers who possess high attack potential (high expertise, resources and motivation). AVA_VAN.5 ensures that penetration testing is carried out by the evaluator to determine that the TOE is resistant to attacks performed by those attackers.

6.3.3. Conclusion

Based on the SFR and SAR rationale it is obvious, that all security objectives are achieved.

---------- END OF SECTION ----------

7. TOE Security Summary Specification

7.1. TOE Security Functions

This section summarizes the security functions (TSF) provided by the TOE to meet the security functional requirements specified for the TOE. A detailed specification of the SFRs is provided by the development documentation of the TOE.

7.1.1. Voice Information Flow Control (TSF.VFC)

7.1.1.1. PTT Handling

TSF.VFC.1

Each audio device has its dedicated PTT input. The TOE disconnects inactive Microphone_Inputs (no PTT).

TSF.VFC.2

The state of PTT is indicated via the Management Interface (TSF.MNI).

7.1.1.2. TX Selector

TSF.VFC.3

One common TX selector switches the Microphone_Inputs either to the RED_VCS_Interface or to the BLACK_VCS_Interface. The TX selector provides two positions:

- SECURE: Microphone_Inputs are disconnected from the BLACK_VCS_Interface. Microphone_Inputs are connected to the RED_VCS_Interface, if the associated PTT is activated.
- INSECURE: Microphone_Inputs are disconnected from the RED_VCS_Interface. Microphone_Inputs are connected to the BLACK_VCS_Interface, if the associated PTT is activated.

TSF.VFC.4

The Initial/Default-State of the TX selector is INSECURE.

TSF.VFC.5

The status of the TX selector is set and indicated via the Management Interface (TSF.MNI).

7.1.1.3. RX Selector

TSF.VFC.6

All Voice_RX_Information received from the RED and BLACK VCS is routed to the Earpiece_Outputs according to one common RX selector. The RX selector provides three positions:

- SECURE: The Voice_RX_Information from the RED_VCS_Interface (CLASSIFIED) is connected to the Earpiece_Outputs. Voice_RX_Information from the BLACK_VCS_Interface is disconnected.
- INSECURE: The Voice_RX_Information from the BLACK_VCS_Interface (UNCLASSIFIED) is connected to the Earpiece_Outputs. Voice_RX_Information from the RED_VCS_Interface is disconnected.
- BOTH: The Voice_RX_Information from the RED_VCS_Interface (CLASSIFIED) as well as from the BLACK_VCS_Interface (UNCLASSIFIED) is connected to the Earpiece_Outputs.

The RX selector inhibits Voice_RX_Information flow between RED_VCS_Interface and BLACK_VCS_Interface.

TSF.VFC.7

The Initial/Default-State of the RX selector is INSECURE.

TSF.VFC.8

The status of the RX selector is set and indicated via the Management Interface (TSF.MNI)

TSF.VFC.9

The Loudspeaker_Output is always connected to the BLACK_VCS_Interface only.

TSF.VFC.10

The speaker of the handset (Ear_Output_Handset) is deactivated as long as it is ON-Hook.

TSF.VFC.11

If the handset (Mic_Input_Handset) or Gooseneck (Mic_Input_Gooseneck) is used (PTT active), the RX selector automatically switches to INSECURE, if the TX selector is in the INSECURE state.

7.1.2. Management Interface (TSF.MNI)

7.1.2.1. Trusted Status Interface

TSF.MNI.1

The Trusted Status Interface indicates the state of the TOE in a way that provides assured information on the state of the Voice Information Flow Control to the S.User.

TSF.MNI.2

The state of the TOE is indicated via the following LEDs at the front plate of the MOD iSAS-P housing:

- 2 LEDs (SEC-TX-LED and INSEC-TX-LED) indicating the TX selector state
- 2 LEDs (SEC-RX-LED and INSEC-RX-LED) indicating the RX selector state
- PTT_LED indicating the PTT state

TSF.MNI.3

For test and maintenance purposes, the Trusted Status Interface additionally provides a push-button to trigger a switch of the RX and TX selector state. The push button is located at the MOD iSAS-P housing and is secured against unintended operation.

7.1.2.2. Remote Control Device

TSF.MNI.4

The TOE includes two alternative key and lamp modules for remote control (MOD iSAS-RC 01 and MOD iSAS-RC 02). The remote control modules provide buttons to set the states of TX selector, RX selector and PTT as well as LEDs to indicate the states to the S.User.

7.1.2.3. Remote Control Interface to RED VCS

TSF.MNI.5

The TOE provides a remote control interface for operation (set/indicate the state of TX selector, RX selector and PTT) via touch entry device (TED) of the RED VCS.

The states can be set and indicated via the RED_VCS_Interface, while via the BLACK_VCS_Interface the states can only be indicated.

The control/status information is transmitted via the same physical interface as voice information.

7.1.3. User Interface Data Flow Control (TSF.DFC)

TSF.DFC.1

The TOE implements a firewall mediating the flow of all User_Interface_Data between the RED_VCS_Interface and the BLACK_VCS_Interface in order to prevent the user interface connection from being misused to bypass the Voice Information Flow Control.

TSF.DFC.2

In the direction from the BLACK_VCS_Interface to the RED_VCS_Interface (Inbound) the firewall performs the following checks:

- The Transport_Data_Frame is syntactically correct.
- The checksum of the Transport_Data_Frame is correct.
- The Application_Protocol is syntactically correct.
- The Application_Message_Type is permissible.

TSF.DFC.3

In the direction from the RED_VCS_Interface to the BLACK_VCS_Interface (Outbound) the firewall performs the following checks:

- The Transport_Data_Frame is syntactically correct.
- The checksum of the Transport_Data_Frame is correct.
- The Application_Protocol is syntactically correct.
- The Application_Message_Type is permissible.
- The Payload_Data_Rate does not exceed a predefined limit of 800bit/s.

TSF.DFC.4

The maximum permissible Payload_Data_Rate is fixed (not manageable). The limit of 800bit/s prevents any comprehensive continuous voice transmission via the firewall.

TSF.DFC.5

If a message does not pass the checks as defined by TSF.DFC.2, TSF.DFC.3 and TSF.DFC.4, the firewall discards the message.

Additionally the TOE will:

- visually indicate a failure to warn the S.User,
- immediately stop transmission of User_Interface_Data and
- stop all communication via RED_VCS_Interface and BLACK_VCS_Interface after 30 seconds (giving the S.User the possibility to react accordingly)

if the message does not pass the following subset of checks defined by TSF.DFC.2, TSF.DFC.3 and TSF.DFC.4 even thought the message has been transmitted error-free (Transport_Data_Frame is syntactically correct and the Checksum of the Transport_Data_Frame is correct):

- The Application_Protocol is syntactically correct.
- The Application_Message_Type is permissible.
- The Payload_Data_Rate in the direction from the RED_VCS_Interface to the BLACK_VCS_Interface (Outbound) does not exceed a predefined limit of 800bit/s.

7.1.4. Protection of TSF (TSF.PRT)

7.1.4.1. Fail Secure

TSF.PRT.2

In case of a power failure, all audio devices are disconnected and no voice information is routed.

TSF.PRT.3

The security function TSF.VFC.3 and TSF.VFC.6 is implemented redundantly ensuring that a single failure will not result in an insecure state.

On the one hand, these security functions are implemented by firmware. On the other hand, discreet hardware logic elements (Redundant Secure and Insecure Redundant Gate) connect or disconnect the signal lines for voice information to RED_VCS_Interface / BLACK_VCS_Interface according to the status indicated by the 2-color LEDs of the Trusted Status Interface.

The functionality of the Redundant Gate prevents that a single failure (either of the firmware or of the discrete hardware logic) will result in an insecure state. E.g. if the firmware indicates that the TX selector is set to SECURE, but in reality (due to a failure) the firmware routes Voice_TX_Information to the BLACK_VCS_Interface, the Insecure Redundant Gate will disconnect the signal lines to the BLACK_VCS_Interface.

TSF.PRT.4

The indication at the Trusted Status Interface and the two Remote Control Devices is implemented via 2-color LEDs. Thus the S.User recognises a LED failure by the LED being dark and no misleading operational status is indicated to the S.User.

7.1.5. Mapping of SFR to TSF

The specified TSFs work together to satisfy the TOE SFRs. The following table provides a mapping of SFRs to the TSFs to show that each SFR is captured within a security function.

SFR	Name	TSF	Name
FAU_ARP.1	Security alarms	TSF.DFC	User Interface Data Flow Control
FAU_SAA.1	Potential violation analysis	TSF.DFC	User Interface Data Flow Control
FDP_ETC.1	Export of user data without security attributes	TSF.VFC	Voice Information Flow Control
FDP_IFC.1_TX FDP_IFC.1_RX	Subset information flow control - Voice TX Subset information flow control - Voice RX	TSF.VFC	Voice Information Flow Control
FDP_IFC.1_UI	Subset information flow control - UI Data	TSF.DFC	User Interface Data Flow Control
FDP_IFF.1_TX FDP_IFF.1_RX	Simple security attributes - Voice TX Simple security attributes - Voice RX	TSF.VFC	Voice Information Flow Control
FDP_IFF.1_UI	Simple security attributes - UI Data	TSF.DFC	User Interface Data Flow Control
FDP_IFF.5_TX FDP_IFF.5_RX	No illicit information flows - Voice TX No illicit information flows - Voice RX	TSF.VFC	Voice Information Flow Control
FDP_IFF.5_UI	No illicit information flows - UI Data	TSF.DFC	User Interface Data Flow Control
FDP_ITC.1_TX FDP_ITC.1 _RX	Import of user data without security attributes	TSF.VFC	Voice Information Flow Control
FMT_MSA.1_TX FMT_MSA.1_RX	Management of security attributes - Voice TX Management of security attributes - Voice RX	TSF.VFC	Voice Information Flow Control
FMT_MSA.3_TX FMT_MSA.3_RX	Static attribute initialisation - Voice TX Static attribute initialisation - Voice RX	TSF.VFC	Voice Information Flow Control
FMT_SMF.1	Specification of management functions	TSF.MNI	Management Interface
FPT_FLS.1	Failure with preservation of secure state	TSF.PRT	Protection of TSF

Tab. 7-1: Mapping of SFR to the TSF

7.2. Assurance Measure

The TOE satisfies the CC EAL 4+ assurance requirements,

Per the conformance statement provided in Section 2 of this ST, the evidence requirements will be met with respect to presentation and content as specified in Part 3 of the Common Criteria (CC) for each of the assurance requirements claimed.

---------- END OF SECTION ----------

8. References

[1] Common Criteria for Information Technology Security Evaluation

Part 1, Version 3.1 Release 1, September 2006.

Part 2 and 3, Version 3.1 Release 2, September 2007.

[2] ZDv 54/100, IT-Sicherheit in der Bundeswehr, Mai 2007, Änderung 2 Oktober 2008.

---------- END OF SECTION ----------

9. Glossary

Acoustic Coupling	The vulnerability whereby RED acoustic signals are inadvertently transmitted to a microphone in BLACK equipment. The RED acoustic signals may be acoustic output from RED processors (intentional or incidental) or CLASSIFIED conversations taking place in the area.
Active Voice Transmission	The user activates voice transmission by pressing Push to Talk.
Application_Message_Type	The application message type defines the semantic of an Application_Protocol element. E.g.: The application message type “OBJ STATE CHANGED”: means that a state of an object at the common user interface has changed (e.g. a button was pressed).
Application_Protocol	The application level protocol used to communicate User_Interface_Data via the TOE.
BLACK VCS	Voice communication system, which handles only UNCLASSIFIED or encrypted signals.
BLACK_VCS_Interface	Interface of the TOE to the BLACK VCS.
BOTH	BOTH can have the following meanings: 1. Position of RX selector 2. Security attribute of a subject that is allowed to receive CLASSIFIED as well as UNCLASSIFIED Voice_RX_Information.
Checksum of the Transport_Data_Frame	The transport data frame includes a checksum in order to detect transmission errors.
CLASSIFIED information	CLASSIFIED information is information regarded as sensitive by the security authorities for the owners of the TOE (e.g. Information up to the German Classification Level VS-GEHEIM or equivalent NATO/national classification levels).
Coach	For training purposes a Coach can connect an audio device (CO_Headset) in parallel to the Operator. In this case the VCS (not the TOE) provides the Coach with the possibility to override the Operator.

COMSEC Approved Circuit	A circuit which has been afforded special physical and visual protective measures and which has been authorized, under the terms of this document, for the regular transmission of CLASSIFIED information without cryptographic protection.
Control/status information	Any information communicated between VCS and TOE for the purpose to control the TOE (e.g. set the TX selector or RX selector) or query the status (e.g. query the status of the TX selector or RX selector).
Data_SFP	Information flow control SFP for communication of user interface data (User_Interface_Data).
Ear_Output_CO_Headset	Earpiece output of the TOE to the binaural/monaural headset for use by the operator.
Ear_Output_Handset	Speaker output of the TOE to the handset.
Ear_Output_OP_Headset	Earpiece output of the TOE to the binaural/monaural headset for use by the operator.
Earpiece_Outputs	Earpiece outputs of the TOE to the headsets and speaker of the handset: Ear_Output_OP_Headset and Ear_Output_CO_Headset and Ear_Output_Handset
INSEC-RX-LED	LED indicating the RX selector state. The LED is active, if the RX selector is in the position INSECURE or BOTH.
INSEC-TX-LED	LED indicating the TX selector state. The LED is active, if the TX selector is in the position INSECURE.
INSECURE	INESCURE can have the following meanings: 1. Position of TX selector 2. Position of RX selector 3. Security Attribute of a subject that is allowed to receive UNCLASSIFIED Voice_RX_Information.
Insecure Channel	Communication channel of the BLACK VCS leaving the operations site.
Loudspeaker_Output	Audio output of the loudspeaker.
Management Interface	TSF which implements interfaces to set and

	indicate the state of the TOE.
Mic_Input_CO_Headset	Microphone input of the TOE to the binaural/monaural headset for use by the coach.
Mic_Input_Gooseneck	Microphone input of the TOE to the handheld/gooseneck microphone.
Mic_Input_Handset	Microphone input of the TOE to the handset.
Mic_Input_OP_Headset	Microphone input of the TOE to the binaural/monaural headset for use by the operator.
Microphone_Inputs	Microphone inputs of the TOE to all audio devices: Mic_Input_OP_Headset and Mic_Input_CO_Headset and Mic_Input_Handset and Mic_Input_Gooseneck.
MOD iSAS-P	Hardware module comprising the actual secure audio switch (TOE exclusive remote control devices).
MOD iSAS-RC 01	Hardware module comprising the desktop version of the remote control device for iSAS.
MOD iSAS-RC 02	Hardware module comprising the console version of the remote control device for iSAS.
OFF-Hook	The handset is OFF-Hook, if the user lifts it off the cradle.
ON-Hook	The handset is ON-Hook, if the user puts it on the cradle.
Operations site	A physical protected area where the TOE and the RED and BLACK VCS are located, minimum approved for the highest security level of information handled in the TOE.
Operator	During normal operation the TOE is used by a single user – the Operator. The Operator communicates with the TOE and VCS via a set of audio devices (OP_Headset, Handset, Gooseneck, Loudspeaker).
Payload	Payload is all content of User_Interface_Data that is not check for semantic correctness by the TOE (e.g. the numeric value identifying the object at the common user interface).

Payload_Data_Rate	Average data rate of Payload.
Protection of TSF	TSF that provides protection to the TSFs.
Push To Talk (PTT)	Switch that is activated by the user when he needs to transmit.
RED VCS	Voice communication system which handles only CLASSIFIED signals.
RED_VCS_Interface	Interface of the TOE to the RED VCS.
RX selector	TOE internal function which routes Voice_RX_Information received from the RED and/or BLACK VCS to the Earpiece_Outputs.
RX_SFP	Information flow control SFP for reception of voice information (Voice_RX_Information).
S.User	All users of the TOE (Operator and Coach) that communicate with the TOE via any of its audio devices and/or operate the TX and RX selector. S.User has physical access to the TOE.
SEC-RX-LED	LED indicating the RX selector state. The LED is active, if the RX selector is in the position SECURE or BOTH.
SEC-TX-LED	LED indicating the TX selector state. The LED is active, if the TX selector is in the position SECURE.
SECURE	SECURE can have the following meanings: 1. Position of TX selector 2. Position of RX selector 3. Security attribute of a subject that is allowed to receive CLASSIFIED Voice_RX_Information.
Secure Channel:	Communication channel of the RED VCS leaving the operations site that is either encrypted with approved crypto devices or implemented as COMSEC approved circuit.
TEMPEST	A short name referring to investigation and studies of compromising emanations.
Transport_Data_Frame	The data frames of the transport level protocol used to communicate User_Interface_Data via the TOE.
TX selector	TOE internal function which routes the Voice_TX_Information from the Microphone_Inputs either to the

	RED_VCS_Interface or BLACK_VCS_Interface.
TX_SFP	Information flow control SFP for transmission of voice information (Voice_TX_Information).
UNCLASSIFIED information	UNCLASSIFIED information is information regarded as not sensitive to disclosure by the security authorities for the owners of the TOE. (e.g. Information up to the German Classification Level VS-NfD or equivalent NATO/national classification levels).
User Interface Data Flow Control	TSF which implements the information flow control for User_Interface_Data.
User_Interface_Data	The user controls both the RED and the BLACK VCS via a common user interface. User_Interface_Data is information that is communicated via the TOE for this purpose.
Voice Information Flow Control	TSF which implements the information flow control for Voice_TX_Information and Voice_RX_Information.
Voice_RX_Information	Voice information from the VCS indented for reception by the user.
Voice_TX_Information	Voice information from the user indented for transmission by the VCS.

---------- END OF SECTION ----------

10. Abbreviations

AD	Analogue to Digital
CO_Headset	Binaural/Monaural Headset for use by the Coach
COMSEC	Communication Security
COTS	Commercial Off the Shelf
DA	Digital to Analogue
Gooseneck	Handheld/Gooseneck Microphone
INSEC-TU	Insecure Transfer Unit
iSAS	Secure Audio Switch
LED	Light Emitting Diode
MOD	Module
NfD	Nur für den Dienstgebrauch
OP_Headset	Binaural/Monaural Headset for use by the Operator
PLD	Programmable Logic Device
PTT	Push To Talk
PU	Processing Unit
RX	Receive
SEC-TU	Secure Transfer Unit
S/I-PU	Secure/Insecure Processing Unit
TED	Touch Entry Device
TU	Transfer Unit
TX	Transmit
UI	User Interface
VCS	Voice Communication System
VS	Verschlusssache

---------- END OF DOCUMENT ----------