ROHDE & SCHWARZ

Security Target

R&S

Trusted Audio Switch

Customer: **Ministry of Defense Belgium**

Project: 16CSN05

Main contractor: Rohde & Schwarz Benelux

Contractor's Supplier: Rohde & Schwarz Topex

ROHDE & SCHWARZ

Table of Content

List of Figures

List of Tables

1. Document brief

Document identification	RST-ST-2003. 1012.02
Prepared by:	R&S Topex
Reviewed by:	SRC – CC Expert
Approved by:	Daniel Micu – Project Management

2. Identification

2.1 History of edition

Edition	Revision	Released date	Title or brief description	Prepared by / Changed by
1	1	28.07.2017	*First issue (Draft version)*	R&S Topex/ SRC
1.1	1	10.08.2017	*QS*	R&S Topex/ SRC
1.1	2	10.08.2017	*First final draft*	R&S Topex/ SRC
1.2	1	27.09.2017	*Adjustments after R+S Review*	R&S Topex/ SRC
1.3	1	06.10.2017	*Final draft for Application*	R&S Topex/ SRC
1.4	1	20.02.2018	*Changes to the architecture*	R&S Topex
1.5	1	08.05.2018	*Added - external Red Lamp indicator*	R&S Topex
1.55	2	25.05.2018	*Draft for Evaluation*	R&S Topex/ SRC
1.5	3	26.06.2018	*Added Information after Evaluation*	R&S Topex/ SRC
1.6	1	06.07.2018	*Added some SFP, according with latest development status*	R&S Topex
1.6	2	17.07.2018	*Last changes due to Evaluator comments*	R&S Topex/ SRC
1.6	3	20.07.2018	*Rephrase section 4.3.1 in according to title paragraph*	R&S Topex
1.6	4	24.07.2018	*Small changes according to Evaluations comments*	R&S Topex/ SRC
1.6	5	02.08.2018	*Updated SFR with latest development status*	Nicolae Zaharia
1.6	6	28.09.2018	*Updated SFR with latest development status*	Nicolae Zaharia
1.7	1	05.12.2018	*Update document with Recording Voice Channel and MIC ACTIVE LED*	Nicolae Zaharia
1.7	2	11.01.2019	*Updated with due to Evaluator comments*	Nicolae Zaharia
1.7	3	25.01.2019	*Updated with due to Evaluator comments*	Nicolae Zaharia
1.7	4	15.02.2019	*Updated with due to Evaluator comments*	Nicolae Zaharia
1.7	5	20.02.2019	*Updated with due to Evaluator comments*	Nicolae Zaharia
1.7	6	14.03.2019	*Updated with due to Certification Body comments*	Nicolae Zaharia

Edition: 1.7   Security Target Trusted Audio Switch   Page 7 of 61
Revision: 19
Date: 09.07.2020   RST-ST-2003. 1012.02

1.7	7	10.04.2019	*Updated with due to Evaluator comments*	Nicolae Zaharia
1.7	8	06.05.2019	*Updated with due to Evaluator comments*	Nicolae Zaharia
1.7	9	07.05.2019	*Updated with due to Evaluator comments*	Nicolae Zaharia
1.7	10	23.05.2019	*Updated with due to Evaluator comments*	Nicolae Zaharia
1.7	11	28.06.2019	*Corrected Version on 4.1*	Nicolae Zaharia
1.7	12	23.07.2019	*Updated with BSI comments*	Nicolae Zaharia
1.7	13	24.09.2019	*Clarified the limit of 800bit/s between PUs*	Nicolae Zaharia
1.7	14	07.02.2020	*Modifications for TAS-FO V2*	Nicolae Zaharia
1.7	15	26.03.2019	*Updated with due to Evaluator comments*	Nicolae Zaharia
1.7	16	04.05.2020	*Updated according to BSI comments*	Nicolae Zaharia
1.7	17	29.05.2020	*Corrected Product code to V2*	Nicolae Zaharia
1.7	18	08.07.2020	*Added some Red Lamp Indicator clarifications on 4.3.2.3 State Control (SS.State)*	Nicolae Zaharia
1.7	19	09.07.2020	*Clarification for Red Lamp Indicator*	Nicolae Zaharia

2.2   Referenced documents

Reference	Document Title	Edition	Revision	Date	Author
[1]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components	Version 3.1	5	03.04.2017	CCMB
[2]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Functional Components	Version 3.1	5	03.04.2017	CCMB

3. Abbreviations

Abbreviation	Description
-B	Black equipment
-R	Red equipment
AC	Alternating Current
BoM	Bill of Materials
BIT	Built-in Test
CWP	Controller Working Position
DC	Direct Current
DVI	Digital Visual Interface
E&M	Earth & Mouth
FXO	Foreign Exchange Office
FXS	Foreign Exchange Subscriber / Station
HU	Rack Unit
IAP	Installation Acceptance Plan
IPD	Installation Plan Definition
IDC	Insulation Displacement Connector
IDF	Intermediate Distribution Frame
LAN	Local Area Network
LS	Loudspeaker
LSA-PLUS	Krone LSA-PLUS connector
MW	Management Workstation
NTP	Network Time Protocol
PS	Power Source
PTT	Push To Talk
PU	Processing Unit
PU_RED	Processing Unit Red
PU_BLACK	Processing Unit Black
R&S	Rohde & Schwarz
R/B	Red / Black
RGW	Radio Gateway
RS	Radio Server
Rx	Receive signal

Abbreviation	Description
SDD	System Design Document
SFP	Security Functional Policies
SIP	Session Initiation Protocol
SoS	Scope of Supply
SPK	Speaker
TAS	Trusted Audio Switch
TED	Touch Entry Device
TFT	Thin Film Transistor (Liquid Crystal Display, LCD technology)
TGW	Telephony Gateway
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functionality Interface
TSS	Traffic Statistic Server
TSP	TOE Security Policies
Tx	Transmit signal
USB	Universal Serial Bus
VCMS	Voice Communication Management System
VCS	Voice Communication System
VoIP	Voice over IP
VRS	Voice Recording Server
VTS	VoIP Telephony Server
WAN	Wide Area Network

4. Security Target Introduction

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

- The Security Target (ST) reference and the TOE reference provide identification information for the ST and the TOE that ST is referring to;

- a briefly description in the TOE overview;

- a more detailed description of the TOE in the TOE description.

4.1 Security Target Reference and TOE Reference

Title:	**Security Target R&S** **Trusted Audio Switch**
Editor(s):	Rohde & Schwarz
Document version:	1.7 Revision 19
Document date:	2020-07-09
CC version:	3.1, Revision 5
Assurance level:	EAL4
Certification ID:	BSI-DSZ-CC-1081
Keywords:	Trusted Audio Switch, RED/BLACK separation, Audio/GUI interface
TOE name:	Trusted Audio Switch with fiber optic (TAS-FO) product code: CP2045.16.3.1
TOE version:	TAS-FO V2

4.2 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

4.2.1 Usage and Main Features of the TOE

The TOE is a Trusted Audio Switch (TAS) as the key element in securing RED (CLASSIFIED) communications by keeping the RED and the BLACK (UNCLASSIFIED) networks completely separated, while at the same time allowing the CWP (Controller Working Position) to work in a secure way with both RED and BLACK signals and media which is visualized in the Figure 1: TOE Overview. It provides the following security capabilities:

- Secure switches between RED and BLACK operational modes, based on specific selection area on common user interface (e.g. Touch Entry Device) or mechanical selector switch;

- Prevents red voice signals leak to the unsecure circuits;

- Clearly informs the operator on the current operational mode using several ways:

    o graphical user interface on Touch Entry Device;

    o external Red Lamp indicator;

    o LEDs placed at the front panel of the TOE;

    o Acoustic signal on the headset.

- Clearly informs the operator about the Microphones status by using a Blue LED at the front panel of the TOE;

- Provides the audio interfaces to the controller (up to two stereo headsets, handsets or microphone);

- Provides the interface for connecting one external loudspeaker;

- Provides the interface for connecting one PTT (push to talk) footswitch;

- Provides the interface for External Red Lamp indicator, intended to inform the neighboring operators about CLASSIFIED/UNCLASSIFIED voice information handling by TOE;

- Provides the interface for external mechanical RED/BLACK selector switch;

- Provides the interface for connecting a Touch Entry Device (Touch Screen);

- Assures RED/BLACK separation for simultaneous video data flow from RED and BLACK Processing Units. The simultaneous video data flows are displayed on the same screen (e.g. Touch Entry Device) through HDMI;

- Provides Trusted Filter mechanism for automatically authentication in both domains and also for call control;

- Provides Trusted Recording Channel to the RED Processing Unit for all Voice Information handled by the operator;

- Provides easy audio levels adjustment by using digital knobs on the front panel.
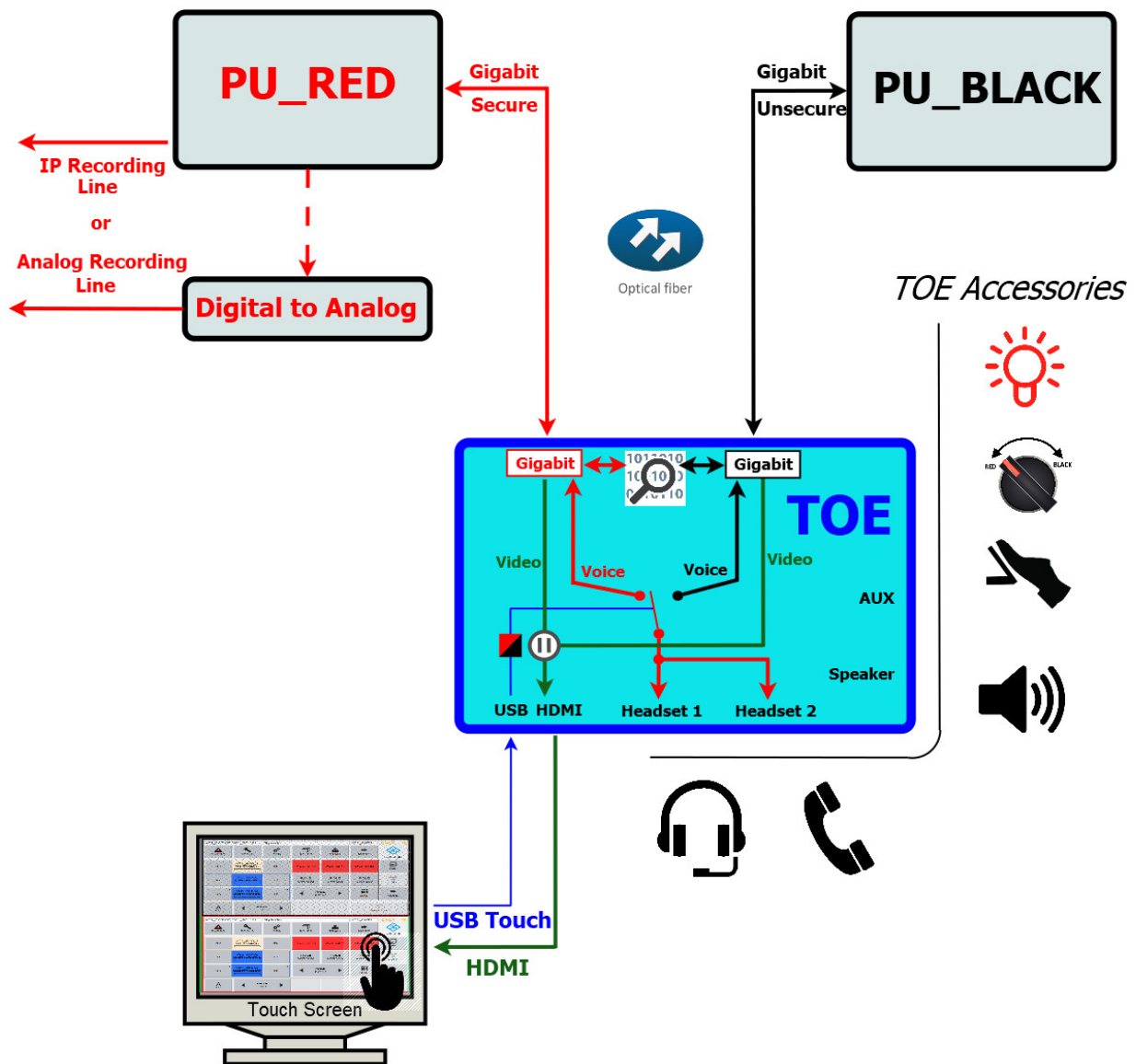
Figure 1: TOE Overview

4.2.2 Required Non-TOE Hardware/Software/Firmware

The TOE will be used with dedicated Processing Units. The format of the digital audio signal and control signals are not part of the main security functionality of the TOE.

The following Firmware is not part of the TOE:

- Non-TOE part of the microcontroller firmware libraries: USB stack, NXP specific libraries for LPC1837.

- Non-TOE part of FPGA IP (Intellectual Property) blocks: Xilinx AXI 1G/2.5G Ethernet Subsystem, Xilinx AXI Interconnect, Xilinx DDR3 Controller, Xilinx VDMA (Video Direct Memory Access), Xilinx AXI Quad SPI.

The following hardware is required but not part of the TOE:

- PU_RED;

- PU_BLACK;

- Accessories

    o Headsets

    o Handsets

    o RED/BLACK selector switch

    o Red Lamp indicator

    o Loud Speaker

    o PTT Foot Switch

- Touch Entry Device (TED).

4.3   TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

4.3.1   Physical Scope of the TOE

Due to physical installation on boundary between RED and BLACK domains, TOE offers several interfaces to interconnect RED/BLACK domains together with Operator's senses like vision, hearing and tactile sense, depicted in Figure 1.

All physical interfaces could be assigned to four functional blocks which can be seen in Figure 5:

1. The audio path (digital plus analogical signals), with RED/BLACK separation assigned to Fiber Optics, HS1 Controller, HS2 Instructor and SPK connectors ;

2. The video path, with RED/BLACK separation assigned to Fiber Optics and HDMI connectors;

3. The decision block which is managing the switching action between RED domain and BLACK domain assigned to USB Touch and AUX connectors;

4. The trusted filter block which is performing deep inspection on the specific Ethernet packets assigned to Fiber Optics connectors.

The input voltage of the power supply is +12 VDC and it is provided by an external AC/DC converter.

Associated User Guidance documentation is delivered with the TOE:

- AGD_OPE.1 Operational user guidance R&S Trusted Audio Switch TAS-FO

- AGD_PRE.1 Preparative procedures R&S Trusted Audio Switch TAS-FO

The operational principle of the TOE can be described as follows:

- For transmission:

o If the external mechanical RED/BLACK selector switch is not present, then TOE identifies the area where the operator touches the screen and opens a RED or BLACK communication chain, according to the pressed area.

o If the external mechanical RED/BLACK selector switch is detected by TOE, then the touch screen presses will not be able to switch between RED/BLACK domains. In this case only external mechanical RED/BLACK selector will switch between RED and BLACK domains.

- For reception - both RED and BLACK audio signals are switched in the TOE and are sent to the operator headset according to the active area on TED; being on the RED domain then TOE can sum the channels from RED and BLACK voice path according to configuration; being on the BLACK domain then TOE can sum the channels from RED and BLACK voice path according to configuration, but only if there are no microphone active;

The TOE allows routing the BLACK path voice to the loudspeaker (according to configuration). The loudspeaker voice path is allowed only from BLACK side, the RED voice path for loudspeaker is automatically dropped by TOE.

The TOE shows the status of Microphones, if any microphone becomes active then TOE lights up the Blue LED, which means the microphone signal is sent to RED or BLACK Processing Unit.

The TOE communicates with RED and BLACK Processing Units over optical fiber connection, one working on the RED topology of the communications network the SECURE one, while the other is working over the black topology of the communications network the UNSECURE one:

- Multiplexed (summed) mode - the data packets processing from the RED and BLACK Processing Units to the TOE is performed exclusively hardware, based upon the type of packet and connector input;

- De-multiplexed mode - the processing of the data packets to the RED or BLACK Processing Units is performed by the TOE, exclusive hardware, based upon the type of signal source and unit status RED/BLACK;

- Bridging function – the data packets filter from RED to BLACK and from BLACK to RED is performed by TOE exclusive hardware, based on deep packet inspection filter.

The TOE is integrated into a standard 1 HU housing. Up to two headset/handsets, one loudspeaker, one PTT footswitch, one external Red Lamp indicator, one mechanical RED/BLACK selector switch, one touchscreen and one video monitor can be connected to the device. The TOE is equipped with two fiber-optic transceivers for two Processing Units communication.

The device can be provided with mechanical adaptation for mounting on or under the desk or for 19" frame, as seen in Figure 2.
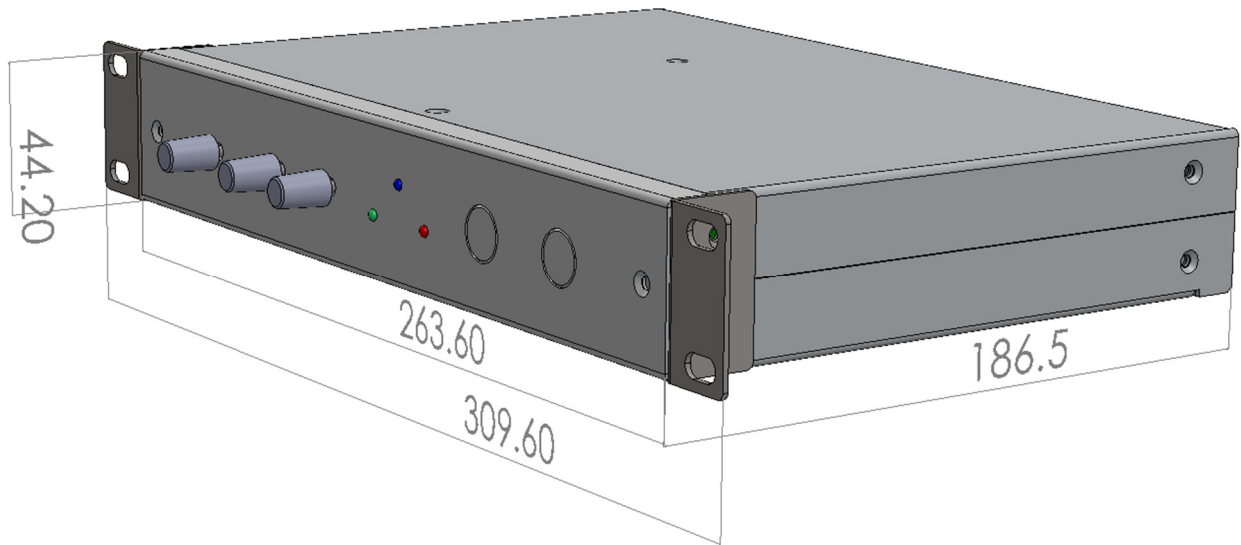
Figure 2: TOE Housing

The front panel is structured as follows:

Figure 3: TOE Front Panel

Table 1 describes the View of Figure 3:

#	Item	Label	Description
1	Green LED	Power	ON – power OK OFF – device not connected to the power supply
2	Green LED	SECURE	ON – CLASIFED communication ongoing OFF – no CLASIFED communication
3	Red LED	UNSECURE	ON – UNCLASIFED communication ongoing OFF – no UNCLASIFED communication
4	Blue LED	MIC ACTIVE	ON – at least one Microphone is active and TOE transmit Voice Information to the RED or BLACK Processing Unit according to the current status OFF – no Microphone is active
4	Rotary switch	SPK	Volume control for External Speaker
5	Rotary switch	HS1	Volume control for channel 1 (Controller audio devices)
6	Rotary switch	HS2	Volume control for channel 2 (Instructor audio devices)
7	Push-pull 10- pin connector	HS1 Controller	Audio port - connects the headphones (stereo) or microphone and PTT switch
8	Push-pull 10- pin connector	HS2 Instructor	Audio port - connects the headphones (stereo) or microphone and PTT switch

Table 1 Description of the Front Panel View

The rear panel is structured as follows:

Figure 4: TOE Rear Panel

Table 2 describes the View of Figure 4:

#	Item	Label	Description
1	Connector 43-01197	SPK	External loudspeaker connector for a passive loudspeaker
2	Connector 43-01207	AUX	External connector for - PTT footswitch - external Red Lamp indicator - external mechanical RED/BLACK selector switch
3	Fiber Optic Data Transceiver	UNSECURE FO	LC-Duplex optical interface connector; nominal wavelength of 850 nm; link lengths up to 300 m; data rate: 1Gb/s
4	Fiber Optic Data Transceiver	SECURE FO	LC-Duplex optical interface connector; nominal wavelength of 850 nm; link lengths up to 300 m; data rate: 1Gb/s
5	USB	USB Touch	USB 2.0 Type A connector, touchscreen detection
6	HDMI connector	HDMI	HDMI connector, Video output
7	DC Socket	DC IN	DC IN D-SUB 2W2, +12 VDC, Imax 1.5 A, Connecting to DC power supply
8	Grounding screw	⏚	Bolt M5 (4023.3882.00RS)

Table 2: Description of the Rear Panel View

4.3.2 Logical Scope of the TOE

The logical scope of the TOE consists of the following security services (Figure 5):

1. Voice Data Flow Control (SS.Voice)

2. Video Data Flow Control (SS.Video)

3. State Control (SS.State)

4. Data Filter Flow Control (SS.Data)
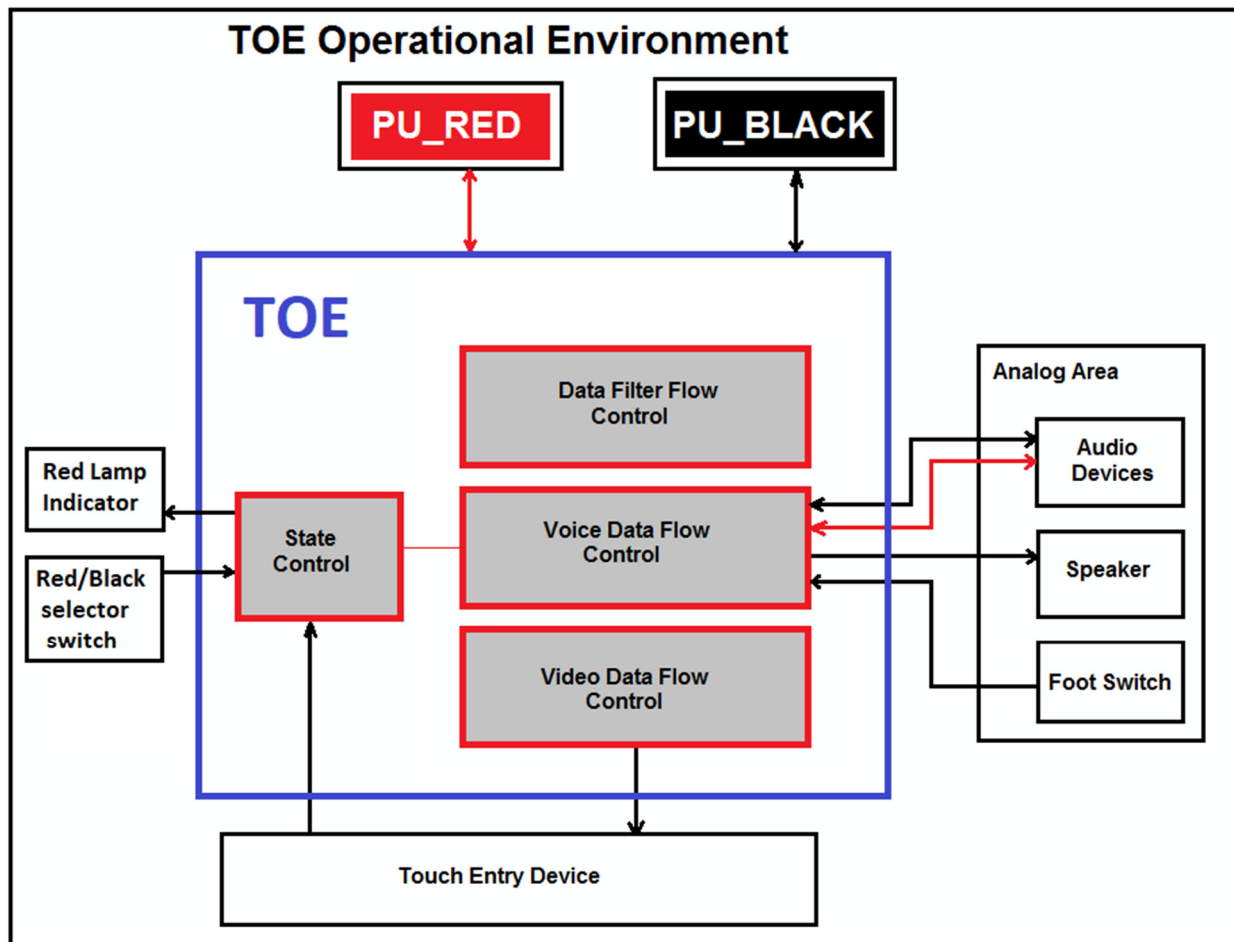
Figure 5: TOE Logical scope

4.3.2.1 Voice Data Flow Control (SS.Voice)

Audio Device input is routed to the PU_RED or PU_BLACK using a Tx voice router. This router provides two operation modes:

- SECURE, which represents transmission of CLASSIFIED voice information,

- UNSECURE, which represents transmission of UNCLASSIFIED voice information.

The operator (S.Operator defined in chapter 6.2) is controlling the router. Each Audio device has its PTT switch (at the headset/handset or foot switch). Each operator (S.Operator) needs to use the PTT for voice communication with VCS. If the PTT is not active the TOE disconnects the microphone.

Voice information that is received from the Processing Units then is routed to the Audio devices output by the Rx router. The Rx switcher, which is controlled by the operator (S.Operator) provides three operation modes:

- SECURE, which represents reception of CLASSIFIED voice information

- UNSECURE, which represents reception of UNCLASSIFIED voice information

- MIXED, which represent reception of CLASSIFIED summed with UNCLASSIFIED voice information.

The TOE is managing the RED and BLACK voice data flow of the Processing Units to prevent bypass of Voice information from RED to BLACK domain.

The TOE provides a Trusted Recording Channel to the RED Processing Unit for all Voice Information received by TOE from different sources: RED or BLACK Processing Units and Microphones. This feature cannot be disabled by anyone who manipulate the TOE.

4.3.2.2   Video Data Flow Control (SS.Video)

The TOE is managing the RED and BLACK video data flow from the Processing Units, in a one way direction, to prevent bypass of information from RED video stream to BLACK video stream and vice versa.

The Video Data Stream comes from Processing Units, it's managed by TOE and it's displayed to Touch Entry Device (TED) using HDMI video signal link.

The TOE reliably decide on the origin of the video stream source (RED or BLACK), and pass through the unaltered video stream.

The alarms, warnings or active area are added on the concatenated video streams by TOE, based on inputs and Built-in Test (BIT) mechanism.

Video signal does not contain confidential information, but the information is displayed on TED that informs the Operator about available voice resources, incoming Radio / Telephony calls and alarms for the corresponding domain, hence video signal shall be displayed correctly on the appropriate part of TED and shall not be by passable from RED video stream to BLACK video stream and vice versa.

4.3.2.3   State Control (SS.State)

The TOE is managing the RED and BLACK domain switching based on external mechanical RED/BLACK selector switch or touch input events. If TOE detects the external mechanical selector switch connected to AUX port, then selecting SECURE/UNSECURE domain is no more available by touches action from the TED.

The touches action come from the Touch Entry Device (TED) using USB data link, they are managed by TOE to select SECURE/UNSECURE domain communication, then they are send to the Processing Units according to selected area.

The indication of the domain status is assured by visual indicators:

- LEDs at the front Panel of the device (Figure 3);
- Active area on graphical interface of the TED;

An audio indication regarding switching from UNSECURE to SECURE communication is played into headset by TOE.

TOE lights the External Red Lamp which indicates the CLASSIFIED/UNCLASSIFIED voice information is handling for the neighboring operator. When TOE is in SECURE state, the HDMI Display and Touch device are detected and Operator is successful login, then the External Red Lamp is active, otherwise the External Red Lamp is inactive, this mean that the Operator cannot handling CLASSIFIED information.

4.3.2.4   Data Filter Flow Control (SS.Data)

TOE assures unique domain authentication using a bridging function between SECURE/UNSECURE domains, also TOE assures call control messages bridging between SECURE/UNSECURE domains.

Performing Data Filter Flow Control the TOE is managing a deep packet inspection for a specific type of packets other unknown packets will be dropped and also a message rate control limit.

The authentication and call control messages do not contain confidential payload.

4.3.3   Out of TOE scope

The following software is not part of the TOE:

- Non-TOE part of the microcontroller firmware libraries: USB stack, NXP specific libraries for LPC1837.

- Non-TOE part of FPGA IP (Intellectual Property) blocks: Xilinx AXI 1G/2.5G Ethernet Subsystem, Xilinx AXI Interconnect, Xilinx DDR3 Controller, Xilinx VDMA (Video Direct Memory Access), Xilinx AXI Quad SPI.

5. Conformance Claims

5.1   CC Conformance Claim

This Security Target and the TOE claim conformance to Part 2 [1] (conformant) and Part 3 [2] (conformant) of the Common Criteria   version 3.1, Revision 5 for Information Technology Security Evaluation.

5.2   PP and Security Requirement Package Claim

This Security Target does neither claim conformance to a Protection Profile nor to a security requirement package.

5.3   CC conformance Claim Rationale

As this Security Target does neither claim conformance to a Protection Profile nor to a security requirement package, a conformance claim rationale is not necessary.

5.4   Package Claim

This Security Target claims conformance to the assurance package EAL4.

6. Security Problem Definition

This chapter introduces the security problem definition of the TOE, which comprises the assets, subjects, assumptions, threats and organizational security policies the TOE has to comply to.

6.1 Assets

The following assets need to be protected by the TOE and its environment.

Asset	Description
Classified voice information	Classified voice information is confidential and must be protected by the TOE.

Table 3: TOE Assets

6.2 Subjects

The TOE can be used by the following subjects outlined in Table 4. There can be two operators using the TOE at the same time. All operators who have access to the TOE can use any audio devices connected to the TOE to communicate with the TOE and VCS.

Subject	Description
S.Operator	S.Operator represents an end-user of the TOE with physical access to the TOE. Operators of the TOE communicate with the TOE via any of its audio devices and operate Tx and Rx voice information.

Table 4: TOE Subjects

6.3 Threat Agents

The following describes threat agents that can adversely act on the assets.

Threat Agent	Description
TA.Ext	A person or process acting on his behalf being located outside the TOE and operational environment. TA.Ext picks up CLASSIFIED voice information. TA.Ext has access to limited resources in terms of money and time and has an enhanced basic attack potential according to CC definition.
TA.Operator	An operator of the TOE may unintentionally perform an unauthorized action and thereby facilitate TA.Ext access to CLASSIFIED voice information.
TA.Tech	A person who is responsible to maintain and install the TOE may unintentionally perform an unauthorized action and thereby facilitate TA.Ext access to CLASSIFIED voice information.
TA.Malfunction	A malfunction of the TOE might facilitate TA.Ext access to CLASSIFIED voice information. TOE responds to a malfunction after the first failure .

Table 5: TOE Threat agents

6.4   Assumptions

The following assumptions need to be made about the operational environment of the TOE to allow the SECURE operation of the TOE.

Assumption	Description
A.Physical_Protection	The TOE and the RED/BLACK Processing Unit are installed in a physically protected area (operational environment) during operation which is approved for the highest security level of information handled by the TOE.
A.TEMPEST_Zone	The TOE is operated in a TEMPEST zone that allows the use of commercial of the shelf products for the processing of the highest security levels of information handled by the TOE.
A.TEMPEST_Evaluation	The TOE is evaluated against TEMPEST attacks, which are out of scope of the CC evaluation.
	The TEMPEST evaluation shall prevent unacceptable compromising electromagnetic emissions (Electromagnetic interference (EMI), Conducted (powerline) and Radiated) and ensure that the interface to the PU_BLACK does not contain unintentional CLASSIFIED voice information.
A.Training	All operators are trained in the correct use to the TOE and Processing Units and follow the operational guidelines.
A.Authorization	All operators are authorized for all information handled by the TOE through the minimum level of clearance for the highest security level of information handled by the TOE.
	To prevent malfeasance operator's activity shall be monitored so that extent sanctions can be applied.
A.Installation	The TOE is installed and maintained according to the installation and maintenance guidelines.
A.Audio_Devices	Appropriate audio devices and associated cables prevent unacceptable acoustic coupling between: - Earpiece and microphone - Ambient noise and microphone This does not hold up for the handset.
A.PU	Voice Information from the PU_RED is separated from the PU_BLACK. Vulnerabilities of the Processing Units or its Connections are not part of the TOE and its evaluation.
	PU_RED communication channels that leave the operational environment are either encrypted with approved crypto devices or implemented as approved circuits (SECURE channels). Vulnerabilities of this out of bounds RED communication channels are not part of the TOE and its evaluation.
A.RED_PU	The PU_RED is accredited for the highest security classification processed in the system.
A.Video	The TED displays the RED/BLACK video streams provided by the TOE separated in such a way that it is visible that the TOE is operating in the intended transfer mode SECURE/UNSECURE.

Table 6: TOE Assumptions

6.5   Threats

The following threats have to be countered by the TOE. Hereby attackers with an enhanced basic attack potential are assumed.

Threat	Description
T.compromise_Information_Flow_Protection	The CLASSIFIED voice information might have transferred to UNSECURE channels:
	Threat Agents are **TA.Ext** and **TA.Malfunction** in combination with **TA.Ext** which endanger the confidentiality of the asset **CLASSIFIED voice information.** Different cases exist:
	• The TOE insufficiently protects CLASSIFIED voice information from being transferred to the PU_BLACK. TA.Ext pick up the CLASSIFIED voice information from the UNSECURE channels.
	• A malfunction in the TOE causes CLASSIFIED voice information to be transferred to the PU_BLACK. TA.Ext pick up the CLASSIFIED voice information from the UNSECURE channels.
T.Tx_Indication_Spoofing	An operator may think that he is speaking via a SECURE channel while he is speaking via an UNSECURE channel.
	Threat Agents are **TA.Operator** in combination with **TA.Ext** and **TA.Malfunction** in combination with **TA.Ext** which endanger the confidentiality of the asset **CLASSIFIED voice information.** Different cases exist:
	• The operator may think that the Microphone_Inputs are connected to the PU_RED while they are actually connected to the PU_BLACK. The operator then speaks CLASSIFIED. The CLASSIFIED voice information is transmitted to the PU_BLACK and is picked up from the UNSECURE channels by TA.Ext outside the operational environment.
	• TOE malfunction gives the operator an indication that the Microphone_Inputs are not connected to the PU_BLACK , while in reality the Microphone_Inputs are connected to the PU_BLACK. The operator then speaks CLASSIFIED. The CLASSIFIED voice information is transmitted to the PU_BLACK and is picked up from the UNSECURE channels by TA.Ext outside the operational environment.
	• TOE malfunction: the graphical user interface shows the operator that he is speaking to the PU_RED while the CLASSIFIED voice information is routed to the PU_BLACK and is picked up from the UNSECURE channels by TA.Ext outside the operational environment.

T.Rx_Indication_Spoofing	An operator may think that he is hearing UNCLASSIFIED while he is hearing CLASSIFIED voice information. Threat Agents are **TA.Operator** in combination with **TA.Ext** and **TA.Malfunction** in combination with **TA.Ext** which endanger the confidentiality of the asset **CLASSIFIED voice information.** Different cases exist: • The operator may think that the Earpiece_Outputs are not connected to the PU_RED while they are actually connected to it. The operator 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 PU_BLACK and is picked up from the UNSECURE channels by TA.Ext outside the operational environment. • TOE malfunction gives the operator an indication that the Earpiece_Outputs are not connected to the PU_RED while they are actually connected to it. The operator 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 PU_BLACK and is picked up from the UNSECURE channels by TA.Ext outside the operational environment. • TOE malfunction: The graphical user interface shows the operator that he is hearing UNCLASSIFIED voice information from the PU_BLACK while the information is CLASSIFIED voice information. The CLASSIFIED voice information from the earpiece of the audio device is picked up by the microphone and transmitted to the PU_BLACK and is picked up from the UNSECURE channels by TA.Ext outside the operational environment.
T.Acoustic_Coupling	Microphones connected to UNSECURE channels might pick up CLASSIFIED voice information. Threat Agents are **TA.Operator** in combination with **TA.Ext** which endanger the confidentiality of the asset **CLASSIFIED voice information.** Different cases exist: • The microphone is routed to the PU_BLACK, and the earpiece is routed from the PU_RED and the microphone might pick up CLASSIFIED voice information from the earphone. The CLASSIFIED voice information is transmitted to the PU_BLACK and is picked up from the UNSECURE channels by TA.Ext outside the operational environment. • The microphone is routed to the PU_BLACK and another operator is in the room TA.operator speaks CLASSIFIED voice information and this CLASSIFIED voice information might be picked up by the microphone.

	The CLASSIFIED voice information is transmitted to the PU_BLACK and is picked up from the UNSECURE channels by TA.Ext outside the operational environment.
T.Non-Permissible_Data_Inbound	A threat agent with access to the PU_BLACK may send non-permissible data through the TOE that result in gaining access to CLASSIFIED voice information in the TOE or the PU_RED. Threat Agent is **TA.Ext** which endangers the confidentiality of the asset **CLASSIFIED voice information.** • TA.Ext gains access to the PU_BLACK via the external interfaces leaving the operations sites. Subsequently TA.Ext modifies the PU_BLACK which sends non-permissible data through the User_Interface_Data connection to the PU_RED. The non-permissible data access from the PU_BLACK leads to gaining access to CLASSIFIED voice information. The PU_BLACK forwards the CLASSIFIED information to TA.Ext, outside the operational environment via UNSECURE channels.
T.Non-Permissible_Data_Outbound	A threat agent with access to the PU_RED may send non-permissible data through the TOE that result in CLASSIFIED voice information being transferred to the PU_BLACK. This voice information may be monitored by a Threat Agent. Threat Agent is **TA.Ext** which endangers the confidentiality of the asset **CLASSIFIED voice information.** • TA.Ext gains access to the PU_RED as well as the PU_BLACK via the external interfaces leaving the operations sites. Subsequently TA.Ext modifies the PU_RED and the PU_BLACK. The modified PU_RED misuses the Data_packets connection to the PU_BLACK in order to transfer CLASSIFIED voice stream. The PU_BLACK forwards the CLASSIFIED information to TA.Ext, outside the operational environment via UNSECURE channels. This enables TA.Ext to monitor the CLASSIFIED voice communication and use this information to his advantage.

Table 7: TOE Threats

Application 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: Additional to physical tampering TOE has implemented protection against logical tampering (firmware, data memory or registers modification by a threat agent) provided by Built-in-Test mechanism (ADV.ARC.1).

6.6 Organizational Security Policies

The TOE does not enforce organizational security policies.

7. Security Objectives

This chapter describes the security objectives for the TOE (in chapter 7.1), the security objectives for the operational environment of the TOE (in chapter 7.2) and contains the security objectives rationale (in chapter 7.3).

7.1 Security Objectives for the TOE

The following security objectives have to be met by the TOE

Security Objective	Description
O.Tx_Status	The operator shall unambiguously be made aware whether the Microphone_Inputs are connected to a PU_BLACK (Black Domain selected) or to a PU_RED (Red Domain selected).
O.Rx_Status	The operator shall unambiguously be made aware whether the Earpiece_Outputs are connected to a PU_BLACK (Black Domain selected) or to a PU_RED (Red Domain Selected).
O.Tx_Flow	Voice information from the Microphone_Inputs assigned to the PU_RED by the operator shall not be routed to the PU_BLACK. If the Domain status is SECURE then Voice information from the Microphone_Inputs are connected/sent to PU_RED. If the Domain status is UNSECURE then Voice information from the Microphone_Inputs are connected/sent to PU_BLACK, but are also connected/sent to PU_RED for recording.
O.Rx_Flow	CLASSIFIED voice information received from the PU_RED shall not be routed to the PU_BLACK. Voice information received from the PU_RED and PU_BLACK shall be routed to the Earpiece_Outputs according to the operator selection (SECURE/UNSECURE). MIXED mode: If the Domain status is SECURE then CLASSIFIED voice information received from the PU_RED and UNCLASSIFIED voice information received from the PU_BLACK can be routed to the Earpiece_Outputs. If the Domain status is UNSECURE and all PTT signals are inactive (all Microphone_Inputs are disconnected) then CLASSIFIED voice information received from the PU_RED and UNCLASSIFIED voice information received from the PU_BLACK can be routed to the Earpiece_Outputs. When any PTT signal is active (at least one Microphone_Input is connected) then only UNCLASSIFIED voice information received from the PU_BLACK shall be routed to the Earpiece_Outputs.
O.Acoustic_Coupling	To prevent unacceptable acoustic coupling via audio devices, the TOE shall ensure the following: - Inactive Microphone_Inputs (no active PTT) shall be disconnected. - If transmission via the handset / headset is active (PTT), the TOE shall prevent that CLASSIFIED voice information is received from the PU_RED while the Microphone_Inputs are routed to the PU_BLACK. - If no audio accessory is detected on an audio interface, TOE shall prevent Voice_Tx information from that audio interface to be sent outside of TOE and shall discard Voice_Rx information for that audio interface. - The Loudspeaker_Output shall only be connected to the PU_BLACK.
O.Mediate_Data	The TOE shall mediate the flow of Data_packets between the PU_RED and the PU_BLACK in order to prevent from being misused to: - Access classified voice information from the PU_BLACK - Transmit comprehensible voice information from the PU_RED to the PU_BLACK.
O.Fail_SAFE	The TOE shall prevent that the Microphone_Inputs are erroneously routed to the PU_BLACK in the event of TSF failure.
O.Video	The TOE must ensure that the routing of Video Data Stream is transferred SAFEly to the Touch Entry Device (TED) to ensure that CLASSIFIED voice information is routed as intended. The TOE shall unambiguously informs the S.Operator regarding RED/BLACK domain selected and also warnings or alarms occurred during operation.

Edition: 1.7
Revision: 19
Date: 09.07.2020

Security Target Trusted Audio Switch

RST-ST-2003. 1012.02

Page 29 of 61

Security Objective	Description
O.Rec	All Voice Information handled by TOE shall be transmitted to PU_RED as Voice Recording Information. The TOE shall ensure that Voice Recording Information is not routed to PU_BLACK or Loudspeaker_Output. The TOE shall ensure that Voice Recording Information is not stopped or manipulated by the Operator or other person.

Table 8: Security Objectives of the TOE

7.2   Security Objectives for the Operational Environment

The following security objectives have to be met by the operational environment of the TOE.

Security Objective	Description
OE.Physical_Protection	The operation site shall have physical protection, which is at least approved for the highest level of information handled in the TOE.
OE.TEMPEST_Zone	The TOE shall be operated in a TEMPEST facility zone that allows the use of COTS products for the processing of highest security level of information handled in the TOE.
OE.TEMPEST_Evalutation	The TOE shall be a subject to a TEMPEST evaluation, which is carried out independent of Common Criteria certification.
OE.Physical_Access	Only authorized persons shall be given physical access to the TOE, PU_RED and Recording Storage device.
OE.Training	The operators 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 status domain indication at the TOE.
OE.Authorization	All operators shall have a minimum clearance for the maximum-security level of information handled in the TOE. Operator activity shall be monitored and operator shall be accountable for their actions and follow the work instructions and operational guidance of the TOE.
OE.Installation	The TOE shall be installed and maintained according to the installation and maintenance guidelines. The installation shall assure that the status domain of the TOE is visible to the operator and also the Red Lamp Indicator is visible to the neighboring operators.
OE.Audio Devices	Appropriate Audio devices, Headsets or Handset, shall be used in order to prevent unacceptable acoustic coupling between: - Headset, when receiving CLASSIFIED voice information while transmitting UNCLASSIFIED voice information. - A neighboring operator and the microphone of the operator, when the neighboring operator is talking CLASSIFIED information while the operator transmits UNCLASSIFIED voice information. To prevent neighboring acoustic coupling, the operator shall ensure that the PTT is inactive if the TOE is in Unsecure state and External Red Lamp Indicator is On at the neighbor Operator.
OE.Neighbour_Acoustic_Coupling	Each operator is made unambiguously aware of the CLASSIFIED/UNCLASSIFIED voice information status of a neighboring operator by watching the External Red Lamp Indicator. 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.PU	The voice information transmitted by the PU_RED shall be strictly separated (logical or physical) from the voice information transmitted by the PU_BLACK. All communication channels of the PU_RED that leave the operational environment either shall be encrypted with approved crypto devices or implemented as approved circuits (SECURE channels).
OE.RED_PU	The PU_RED shall be accredited for the highest security classification processed in the system.
OE.Video	The Touch Entry Displays that are used to connect to the TOE and provide separated touch areas are only operated in the SECURE physical operational environment to assure only accountable personnel is using the TED and the displays are not manipulated.
OE.Cabling	The Fiber Optic connection between Processing Units and TOE shall use the appropriate connectors: - PU_RED shall be connected to "SECURE FO" Fiber Optic connector; - PU_BLACK shall be connected to "UNSECURE FO" Fiber Optic connector.
OE.Rec	The Recording Storage device connected to the PU_RED shall be accredited for the highest security classification processed in the system. The Recording Storage device connected to the PU_RED shall have physical protection, which is at least approved for the highest level of information handled in the TOE. The logical access to the Recording Storage device connected to the PU_RED shall be protected but also the confidentiality during different life cycles of stored data (i.e. audio play, secure deletion).

Table 9: Security Objectives for the Operational Environment

7.3 Security Objectives Rationale

Security Objectives - Security Objectives of the environment/ Assumptions-Threats	A.Physical Protection	A.TEMPEST_Zone	A.TEMPEST_Evaluation	A.Training	A.Authorization	A.Installation	A.Audio Devices	A.PU	A.RED_PU	A.Video	T.compromise_Information_Flow_Protection	T.Tx_Indication_Spoofing	T.Rx_Indication_Spoofing	T.Acoustic_Coupling	T.Non-Permissible_Data_Inbound	T.Non-Permissible_Data_Outbound
O.Tx_Status												X				
O.Rx_Status													X			
O.Tx_Flow											X					
O.Rx_Flow											X			X		
O.Acoustic_Coupling													X	X		
O.Mediate_Data											X				X	X
O.Fail_SAFE											X	X				
O.Video												X	X			
O.Rec											X				X	X
OE.Physical_Protection	X														X	X
OE.TEMPEST_Zone		X													X	X
OE.TEMPEST_Evalutation			X													
OE.Physical_Access	X															
OE.Training				X												
OE.Authorization				X	X											
OE.Installation	X					X						X	X			X
OE.Audio Devices							X						X	X		
OE.Neighbour_Acoustic_Coupling														X		
OE.PU								X								X
OE.RED_PU									X							X
OE.Video										X						
OE.Cabling						X						X				X
OE.Rec	X			X	X				X						X	X

Table 10: Security Objectives Rationale

7.3.1 Countering the threats

The Threat **T.compromise_Information_Flow_Protection** which describes that an attacker may gain CLASSIFIED voice information being transferred falsely to the PU_BLACK is countered by a combination of the objectives *O.Tx_Flow, O.Rx_Flow, O.Rec and O.Fail_SAFE*. The objectives *O.Tx_Flow, O.Rx_Flow and O.Rec* ensure that transferred CLASSIFIED voice information is either not falsely routed or falsely separated by the operator. *O.Fail_SAFE* prevents a wrong connection in case of a single failure of the TOE and protects CLASSIFIED voice information from being captured through an UNSECURE channel. The objective *O.Mediate_Data* ensures that transferred CLASSIFIED voice information is either not falsely routed or falsely separated by the TOE to an UNSECURE channel.

The Threat **T.Tx_Indication_Spoofing** which describes that an operator may think that he is speaking via a SECURE channel while he is actually speaking via an UNSECURE channel. This result to CLASSIFIED voice information being transferred falsely to the PU_BLACK and is countered by a combination of the objectives *O.Tx_Status and O.Fail_SAFE*. The environmental objective *OE.Installation* and *OE.Cabling* ensures that the TOE is correctly installed in the physically SECURE environment and that a malfunction of the TOE is prevented by using the TOE guidance to bring the TOE in a SECURE certified operational state. The objective *O.Tx_Status* prevents missuse and wrong operation of the TOE by the operator by making the operator aware of that the microphone is routed in designated domain. *O.Video* prevents that the GUI shows the operator a SECURE channel while the TOE is connected to the UNSECURE channel.

The Threat **T.Rx_Indication_Spoofing** which describes that an operator may think that he is hearing via an UNSECURE channel while he is actually hearing via a SECURE channel. This result to CLASSIFIED voice information being transferred falsely to the operator and is countered by a combination of the objectives *O.Rx_Status*, *O.Acoustic_Coupling* and *O.Video*. The environmental objectives *OE.Installation* and *OE.Audio Devices* ensure that the TOE is correctly installed in the physically SECURE environment and that only correct working audio devices are used by installing the TOE according the guidance to bring the TOE in a SECURE certified operational state and only use appropriate headsets. The objectives *O.Rx_Status* prevents misuse and wrong operation of the TOE by the operator by making the operator aware that the Ear piece is in a SECURE/UNSECURE state. *O.Acoustic_Coupling* prevents leakage of CLASSIFIED voice information by automatically switch of the communication when not in use and Loudspeaker information are not transmitted. *O.Video* prevents that the GUI shows the operator an UNSECURE channel while there is CLASSIFIED voice information received.

T.Acoustic_Coupling describes that a microphone may transfer CLASSIFIED voice information via an UNSECURE channel. This result to CLASSIFIED voice information being transferred falsely to the PU_BLACK and is countered by a combination of the objective *O.Acoustic_Coupling* and the environmental objectives *OE.Audio Devices, OE.Neighbour_Acoustic_Coupling,* and *O.Rx_Flow*. *O.Acoustic_Coupling* prevents leakage of CLASSIFIED voice information by automatically switch off the communication when not in use and Loudspeaker information are not transmitted. *OE.Audio Devices* ensures that only correct working audio devices are used by using only appropriate headsets. *OE.Neighbour_Acoustic_Coupling* prevents misconfiguration and false separation by showing the operator that another operator is handling CLASSIFIED voice information right now. *O.Rx_Flow* ensures that no CLASSIFIED voice information is sent to the PU_BLACK by acoustic coupling between Earpiece_Outputs and Microphone_Inputs when the system domain status is UNSECURE.

The Threat **T.Non-Permissible_Data_Inbound** which describes that an external attacker may gain CLASSIFIED voice information being transferred falsely to the PU_BLACK by manipulating an external interface is countered by the objective *O.Mediate_Data*. The objective *O.Mediate_Data and O.Rec* ensure that transferred CLASSIFIED voice information is either not falsely routed or falsely separated by the TOE to an UNSECURE channel. *OE.Physical _Protection, OE.TEMPEST_Zone, OE.Rec* and *OE:Installation* ensure that the TOE is installed in a safe and secured environment with access restriction for the personnel correct and safe installation and protection.

The Threat **T.Non-Permissible_Data_Outbound** which describes that an external attacker may gain CLASSIFIED voice information being transferred falsely to the PU_BLACK by manipulating an external interface is countered by the objective *O.Mediate_Data*. The objective *O.Mediate_Data and O.Rec* ensure that transferred CLASSIFIED voice information is either not falsely routed or falsely separated by the TOE to an UNSECURE channel. The environmental objectives *OE.PU, OE.RED_PU, OE.Rec* and *OE.Cabling* ensures that only accredited Procesing Units and Recording Storage device are able to receive Data and therefore protect the TOE implicitly. *OE.Physical _Protection, OE.TEMPEST_Zone* and *OE.Installation* ensure that the TOE is installed in a safe and secured environment with access restriction for the personnel correct and safe installation and protection.

7.3.2   Covering the OSPs

The TOE does not enforce organizational security policies.

7.3.3   Covering the assumptions

The assumption *A.Physical_Protection* is covered by *OE.Physical_Protection, OE.Physical_Access, OE.Installation and OE.REC* as directly follows.

The assumption *A.TEMPEST_Zone* is covered by *OE.TEMPEST_Zone* as directly follows.

The assumption *A.TEMPEST_Evaluation* is covered by *OE.TEMPEST_Evaluation* as directly follows.

The assumption *A.Training* is covered by *OE.Training* and *OE.Authorization* as directly follows.

The assumption *A.Authorization* is covered by *OE.Authorization and OE.REC* as directly follows.

The assumption *A.Installation* is covered by *OE.Installation*, *OE.Cabling* and *OE.REC* as directly follows.

The assumption *A.Audio_Devices* is covered by *OE.Audio_Devices* as directly follows.

The assumption *A.PU* is covered by *OE.PU* as directly follows.

The assumption *A.RED_PU* is covered by *OE.RED_PU* and *OE.REC* as directly follows.

The assumption *A.Video* is covered by *OE.Video* as directly follows.

8. Security Requirements

This chapter defines the security functional requirements (see chapter 9.1) and the security assurance requirements for the TOE (see chapter 9.3). No extended components are defined in this Security Target (see chapter 9.2).

8.1 Security functional requirements for the TOE

The TOE satisfies the SFRs delineated in the following table. The rest of this chapter contains a description of each component and any related dependencies.

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

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

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

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

Component	Name
Security audit (FAU)	
FAU_ARP.1	Security alarms
FAU_SAA.1	Potential violation analysis
User data protection (FDP)	
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 compromised information flows
FDP_ITC.1	Import of user data without security attributes
Security Management (FMT)	
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of Management Functions
Protection of the TSF (FPT)	
FPT_FLS.1_SAFE	Failure with preservation of SECURE state
FPT_FLS.1_Current	Failure with preservation of Current state

Table 11: Security Functional Requirements for the TOE

8.1.1 Terms and definitions for information flow control SFPs

This section contains terms and definitions used in the subsequent SFRs to define the information flow control Security Functional Policies (SFPs). The terms and definitions are listed here by category.

8.1.1.1   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).
Rec_SFP	Information flow control SFP for voice information (Rx and Tx Voice Information)
Data_SFP	Information flow control SFP for data communication.

Table 12: Information flow control SFPs

8.1.1.2   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 operator intended for transmission to the Processing Units.	Tx_SFP
Voice_Rx_Information	Voice information from the Processing Units intended for reception by the operator.	Rx_SFP
Voice_Rec_Information	Voice information from TOE to the PU_RED intended for recording all Voice Information handled by Operator.	Rec_SFP
User_Interface_Data	The operator controls both the RED and the BLACK Processing Units via a Touch Entry Device. User_Interface_Data is information that is communicated via the TOE for this purpose.	Data_SFP

Table 13: SFP Information controlled by the TOE

8.1.1.3   Data Subjects

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

Entity	Description	SFP
Analogue Audio Inputs		
Microphone_Inputs	Microphone inputs of the TOE to all audio Tx_SFP devices: - Mic_Input_OP1_Headset and - Mic_Input_OP2_Headset and - Mic_Input_Handset	Tx_SFP Rec_SFP
Mic_Input_OP1_Headset	Microphone input of the TOE to the binaural/monaural headset for use by the first operator.	
Mic_Input_OP2_Headset	Microphone input of the TOE to the binaural/monaural headset for use by the second operator.	
Mic_Input_Handset	Microphone input of the TOE to the handset.	
Analogue Audio Outputs		
Earpiece_Outputs	Earpiece outputs of the TOE to the Rx_SFP headsets and speaker of the handset: - Ear_Output_OP1_Headset and - Ear_Output_OP2_Headset and - Ear Output Handset - Loudspeaker_Output	Rx_SFP Rec_SFP
Ear_Output_OP1_Headset	Earpiece output of the TOE to the binaural/monaural headset for use by the first operator.	
Ear_Output_OP2_Headset	Earpiece output of the TOE to the binaural/monaural headset for use by the second operator.	
Ear Output Handset	Speaker output of the TOE to the handset.	
Loudspeaker_Output	Audio output of the TOE to the external loudspeaker.	
Interfaces to Processing Units		
RED_PU_Interface	Interface of the TOE to the PU_RED.	Tx_SFP Rx_SFP Data_SFP Rec_SFP
BLACK_PU_Interface	Interface of the TOE to the PU_BLACK.	Tx_SFP Rx_SFP Data_SFP

Table 14: SFP Entities

8.1.1.4 Security Attributes

The following Table 15 lists the SFP information security attributes.

Information	Security Attribute	Description
Voice_Tx_Information Voice_Rx_Information Voice_Rec_Information	CLASSIFIED	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 level).
	UNCLASSIFIED	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 frame of the transport level protocol used to communicate User_Interface_Data via TOE.
	Checksum of the Transport_Data	The transport data between TOE and PU includes a checksum in order to detect transmission errors.
	Application_Protocol	The application level protocol used to communicate VCS via TOE.
	Application_Message_Type	The application message type defines the semantic of an Application_Protocol message. E.g.: The application message type "LOG IN": means that a User is attempt to Log-in. The application messages type "PRESS / UNPRESS" generated by touch screen controller interface for press coordinates. The application messages type "VIDEO" generated by PU to be displayed by TED via TOE.
	Message_Data_Rate	Limited number of allowed messages on specific interface via TOE per unit of time. Each message is inspected according to allowed formats and has a limited rate of frequency, to avoid TOE packet data flooding. Message is all content of User_Interface_Data that is inspected by semantic correctness by TOE (e.g. Control, Acknowledge or Version Check).

	Payload_Data_Rate	Number of Payload bits that are communicated via TOE per unit of time. Payload is all content of User_Interface_Data that is not inspected by semantic correctness by TOE (e.g. the numeric value identifying the user ID).

Table 15: SFP Information Security Attributes

The following table lists the SFP entity security attributes.

Entity	Security Attribute	Description
Earpiece_Outputs	SECURE	Security attribute of an entity that is allowed to receive CLASSIFIED Voice_Rx_Information.
	UNSECURE	Security attribute of an entity that is allowed to receive UNCLASSIFIED Voice_Rx_Information.
	Mixed	Security attribute of an entity that is allowed to receive CLASSIFIED as well as UNCLASSIFIED Voice_Rx_Information.

Table 16: SFP entity security attributes

8.1.2 Security audit (FAU)

8.1.2.1 FAU_ARP.1 Security Alarms
FAU_ARP.1.1

The TSF shall take [*The following list of actions:*

- *Visually indicate a failure to warn the S.Operator,*

- *any failure switches the TOE on the SECURE domain*]

upon detection of a potential security violation.

Note: A visual indication is either a message displayed by TOE on the appropriate TED or a message signalized using the two LEDs: RED (UNSECURE LED) and GREEN (SECURE LED), depending on the failure.

8.1.2.2 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 and also Voice_Rx_Information message has been transmitted error-free (Transport_Data_Frame and the Checksum of the Transport_Data_Frame is correct).*

- *The Application_Message_Type is permissible,*

- *The Application_Protocol is syntactically correct,*

- *The Payload_Data_Rate from Red_PU_Interface to Black_PU_Interface does not exceed the data rate required for comprehensive continuous voice transmission.*

- *The Message_Data_Rate from Red_PU_Interface or Black_PU_Interface does not exceed the maximum data rate]*

Note: If Transport_Data_Frame is incorrect or Checksum of Transport_Data_Frame is incorrect, then the message is discarded.

8.1.3 User data protection (Class FDP)

This section specifies the information flow control requirements.

8.1.3.1 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.

8.1.3.2 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 data subjects:*

- *Microphone_Inputs*
    - *Mic_Input_OP1_Headset*
    - *Mic_Input_OP2_Headset*
    - *Mic_InputHandset*
- *RED_PU_Interface*
- *BLACK_PU_Interface*

For the following information:

- *Voice_Tx_Information*].

8.1.3.3 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_OP1_Headset*
    - *Ear_Output_OP2_Headset*
    - *Ear Output Handset*
- *Loudspeaker_Output*
- *RED_PU_Interface*
- *BLACK_PU_Interface*

From the following information:

- *Voice_Rx_Information*].

8.1.3.4 FDP_IFC.1_Rec Subset information flow control- Voice Rec FDP_IFC.1.1_Rec

The TSF shall enforce the [*information flow control Rec_SFP*] on [*the following data subjects:*

- *Microphone_Inputs*
    - *Mic_Input_OP1_Headset*
    - *Mic_Input_OP2_Headset*
    - *Mic_InputHandset*
- *Earpiece_Outputs*
    - *Ear_Output_OP1_Headset*
    - *Ear_Output_OP2_Headset*
    - *Ear Output Handset*
- *Loudspeaker_Output*
- *RED_PU_Interface*

For the following information:

- *Voice_Rec_Information*].

8.1.3.5 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 data subjects:*

- *RED_PU_Interface*
- *BLACK_PU_Interface*

For the following information:

- *User_Interface_Data*].

8.1.3.6 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 voice router)*
    - *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_PU_Interface*
- *UNCLASSIFIED Voice_Tx_Information shall be transmitted to the BLACK_PU_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].

8.1.3.7 FDP_IFF.1_Rec Simple security attributes - Voice Rec
FDP_IFF.1.1_Rec

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

- *Voice_Rec_information security attributes (as determined by the Tx voice router and Rx Voice router)*
    - *CLASSIFIED*
    - *UNCLASSIFIED*].

FDP_IFF.1.2_Rec

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_PU_Interface and Tx Voice router = SECURE.*

- *UNCLASSIFIED Voice_Tx_Information shall be transmitted to the RED_PU_Interface and Tx Voice router = UNSECURE.*

- *Voice_Rx_Information security attributes is determined by the source*

  - *CLASSIFIED transmitted to the RED_PU_Interface and Rx Voice router = SECURE*

  - *UNCLASSIFIED transmitted to the RED_PU_Interface and Rx Voice router = UNSECURE]*

FDP_IFF.1.3_Rec

The TSF shall enforce the [*information flow control rules Rec_SFP while applying the security attribute:*

- *TRANSMITTED as determined by the Tx voice router or*

- *RECEIVED as determined by the Rx Voice router*

  ].

FDP_IFF.1.4_Rec

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

FDP_IFF.1.5_Rec

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

[none].

8.1.3.8   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 voice router:*

  - *SECURE, if Rx voice router = SECURE*

  - *UNSECURE; if Rx voice router = UNSECURE*

  - *MIXED, (if Rx voice router = UNSECURE and Microphone_Inputs = disconnected) or (if Rx voice router = SECURE)].*

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 voice router) is SECURE*

    - *UNCLASSIFIED Voice_Rx_Information shall be received by the Earpiece_Outputs, if its security attribute (determined by the Rx voice router) is UNSECURE*

    - *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 voice router) is SECURE*

    - *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 voice router) is UNSECURE and Microphone_Inputs are disconnected*

    - *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_InputHandset (PTT active)*].

8.1.3.9 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_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_PU_Interface and BLACK_PU_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,*
- *The Payload_Data_Rate not exceed the rules*].

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 Tranmission:

- *The Payload_Data_Rate from RED_PU_Interface to BLACK_PU_Interface exceeds the data rate required for comprehensive continuous voice transmission*
- *The Application_Protocol is syntactically incorrect*
- *The Application_Message_Type is not permitted*
- *The Checksum of the Transport_Data_Frame is not correct*
- *The Transport_Data_Frame is not syntactically correct*].

8.1.3.10 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*].

8.1.3.11 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*].

8.1.3.12 FDP_IFF.5_Rec No illicit information flows - Voice Rec
FDP_IFF.5.1_Rec

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

8.1.3.13 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*].

8.1.3.14 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 voice router:*

  - *CLASSIFIED, if Tx voice router = SECURE*

  - *UNCLASSIFIED; if Tx voice router = UNSECURE*].

8.1.3.15 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 Processing Units interface:*

  - *CLASSIFIED, if reception via RED_PU_Interface*

  - *UNCLASSIFIED, if reception via BLACK_PU_Interface*].

8.1.3.16 FDP_ITC.1_Rec Import of user data without security attributes - Voice Rec
FDP_ITC.1.1_Rec

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

FDP_ITC.1.2_Rec

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

FDP_ITC.1.3_Rec

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

- *Voice_Rec_Information is imported from:*

    - *Microphone_Inputs, if the corresponding PTT is active;*

    - *RED_PU_Interface and BLACK_PU_Interface while Tx voice router = SECURE;*

    - *BLACK_PU_Interface while Tx voice router = UNSECURE;*

- *Voice_Rec_Information security attributes are determined by the Tx voice router:*

    - *CLASSIFIED, if Tx voice router = SECURE*

    - *UNCLASSIFIED; if Tx voice router = UNSECURE*].

8.1.4 Security management (FMT)

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

8.1.4.1 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.Operator*].

8.1.4.2 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 / UNSECURE of the Earpiece_Outputs*] to [*S.Operator*].

8.1.4.3 FMT_MSA.1_Rec Management of security attributes - Voice Rec FMT_MSA.1.1_Rec

The TSF shall enforce the [*information flow control Rec_SFP*] to restrict the ability to [**set, indicate**] the security attributes [*CLASSIFIED / UNCLASSIFIED of Voice_ Rec_Information*] to [RED_PU_Interface].

8.1.4.4 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.

8.1.4.5 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.

8.1.4.6 FMT_MSA.3_Rec Static attribute initialization - Voice Rec
FMT_MSA.3.1_Rec

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

FMT_MSA.3.2_Rec

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

8.1.4.7 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 voice router*

- *Set the state of the Rx voice router*

- *Set the PTT state*

- *Set the state of the external Red Lamp indicator*

- *Assured indication of the Tx voice router state to the S.Operator*

- *Assured indication of the Rx voice router state to the S.Operator*

- *Assured indication of the PTT state to the S.Operator*

during normal TOE operation].

8.1.5 Protection of the TSF (FPT)

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

8.1.5.1 FPT_FLS.1_SAFE Failure with preservation of SECURE state
FPT_FLS.1.1_SAFE

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*

- *Missing HID / Wrong device (USB touch controller is not attached)*
- *Missing / Wrong Display attached to HDMI port*
- *Communication with any PU is lost*
- *Power-Up initialization Fail*
- *Built in Test failed*
- *TAS-FO does not detect GUI activity on PUs*
- *TAS-FO does not detect X-Server activity on PUs*
- *TAS-FO detects unexpected PUs video resolution*
- *No Operator is authenticated on the PUs to the VCS*
- *Payload_Data_Rate exceeds the data rate predefined limits*].

8.1.5.2 FPT_FLS.1_Current Failure with preservation of Current state FPT_FLS.1.1_Current

The TSF shall preserve a Current state when the following types of failures occur:

[*Single failure of the TSF implementing the information flow control Tx_SFP*

- *Unmatched Redundant Gate[1]*].

8.2 Extended Components definition

No extended components are defined in this Security Target.

8.3 Security assurance requirements for the TOE

The following table lists the chosen evaluation assurance components for the TOE.

---

[1] *The switching implementation, between CLASSIFIED and UNCLASSFIED domains, is based on dual redundancy check; if switching decision does not match on both check levels then TOE will preserve the current state.*

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_TDS.3 Basic modular design
AGD Guidance Documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC Lifecycle	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.1 TOE summary specification
ATE Tests	ATE COV.2 Analysis of coverage
	ATE_DPT.1 Testing : basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Table 17: Security assurance requirements for the TOE

These assurance components represent EAL 4. The complete text for these requirements can be found in [2].

8.4 Security Requirements Rationale

8.4.1 SFRs rationale

8.4.1.1 Tracing between SFRs and security objectives

Security Functional Requirements/ Security Objectives	O.Tx_Status	O.Rx_Status	O.Tx_Flow	O.Rx_Flow	O.Acoustic_Coupling	O.Mediate_Data	O.Fail_SAFE	O.Video	O.Rec
FAU_ARP.1						X			
FAU_SAA.1						X			
FDP_ETC.1			X	X					
FDP_IFC.1_Tx			X						
FDP_IFC.1_Rx				X					
FDP_IFC.1_Rec			X	X					X
FDP_IFC.1_UI						X			
FDP_IFF.1_Tx			X						
FDP_IFF.1_Rx				X	X				
FDP_IFF.1_Rec			X	X					X
FDP_IFF.1_UI						X			
FDP_IFF.5_Tx			X						
FDP_IFF.5_Rx				X					
FDP_IFF.5_Rec			X	X					X
FDP_IFF.5_UI						X			
FDP_ITC.1_Tx			X		X				
FDP_ITC.1_Rx				X					
FDP_ITC.1_Rec			X	X					X
FMT_MSA.1_Tx			X					X	
FMT_MSA.1_Rx				X				X	
FMT_MSA.1_Rec			X	X					X
FMT_MSA.3_Tx			X					X	
FMT_MSA.3_Rx				X				X	
FMT_MSA.3_Rec			X	X					X
FMT_SMF.1	X	X	X	X				X	
FPT_FLS.1_SAFE							X		
FPT_FLS.1_Current	X	X							

Table 18:Tracing between SFRs and security objectives

The security objective **O.Tx_Status** and **O.Rx_Status** are met by *FMT_SMF.1* which describes specific management functions to ensure the correct routing status of the TOE for the operator for transmission and receiving.

The security objective **O.Tx_Flow** is met by a combination of the user data protection SFRs *FDP_ETC.1, FDP_IFC.1_Tx, FDP_IFF.1_Tx, FDP_IFF.5_Tx, FDP_ITC.1_Tx* and the management SFRs *FMT_MSA.1_Tx, FMT_MSA.3_Tx, FMT_SMF.1.*
FDP_ETC.1, FDP_IFC.1_Tx, FDP_IFC.1_Rec, FDP_IFF.1_Tx, FDP_IFF.1_Rec, FDP_IFF.5_Tx, FDP_IFF.5_Rec, FDP_ITC.1_Tx and FDP_ITC.1_Rec describe the protection of user data by setting export rules and security attributes for transmission of classified and unclassified information flow through Secure,

Unsecure and Mixed operation modes. *FMT_MSA.1_Tx, FMT_MSA.1_Rec, FMT_MSA.3_Tx, FMT_MSA.3_Rec, FMT_SMF.1* describe management functionalities to set and indicate the correct status and operational mode of the TOE during transmission information.

The security objective **O.Rx_Flow** is met by a combination of the user data protection SFRs *FDP_ETC.1, FDP_IFC.1_Rx, FDP_IFC.1_Rec, FDP_IFF.1_Rx, FDP_IFF.1_Rec, FDP_IFF.5_Rx, FDP_IFF.5_Rec, FDP_ITC.1_Rx, FDP_ITC.1_Rx, FDP_ITC.1_Rec* and the management SFRs *FMT_MSA.1_Rx, FMT_MSA.1_Rec, FMT_MSA.3_Rx, FMT_MSA.3_Rec and FMT_SMF.1.*
FDP_ETC.1, FDP_IFC.1_Rx, FDP_IFF.1_Rx, FDP_IFF.5_Rx and *FDP_ITC.1_Rx* describe the protection of user data by setting export rules and security attributes for receiving of classified and unclassified information flow through Secure, Unsecure and Mixed operation modes. *FMT_MSA.1_Rx, FMT_MSA.3_Rx and FMT_SMF.1* describe management functionalities to set and indicate the correct status and operational mode of the TOE during receiving information.

The security objective **O.Acoustic_Coupling** is met by a combination of *FDP_IFF.1_Rx* and *FDP_ITC.1_Tx* which describe the import rules of user date when classified and unclassified information is handled by the TOE.

The security objective **O.Mediate_Data** is met by combination of the audit SFRs *FAU_ARP.1, FAU_SAA.1* and the user data protection SFRs *FDP_IFC.1_UI, FDP_IFF.1_UI* and *FDP_IFF.5_UI.*
FAU_ARP.1 and *FAU_SAA.1* describe the alarms to indicate failure and non conformities according to the correct functionality of the security functionalty and logging/ monitoring of security relevant events. FDP_IFC.1_UI, FDP_IFF.1_UI and FDP_IFF.5_UI describe the information flow control rules to ensure all information is handled correctly, safely and secure by the TOE and its monitoring and state rules according to the user interface functionality.

The security objective **O.Fail_SAFE** is met by *FPT_FLS.1_SAFE* which describes the safe mode of the TOE that is triggered by five specific errors.

The security objective **O.Video** is met by a combination of *FMT_MSA.1_Tx, FMT_MSA.1_Rx, FMT_MSA.3_Tx, FMT_MSA.3_Rx and FMT_SMF.1* which describe management functionalities to set and indicate the correct status and operational mode of the TOE during receiving and transmission of information.

8.4.1.2   Fulfillment of TOE SFR dependencies

Component	Dependency	Fulfilled
FAU_ARP.1	FAU_SAA1	X
FAU_SAA.1	FAU_GEN.1	
FDP_ETC.1	FDP_IFC.1	X
FDP_IFC.1_Tx	FDP_IFF.1_Tx	X
FDP_IFC.1_Rx	FDP_IFF.1_Rx	X
FDP_IFC.1_Rec	FDP_IFF.1_Rec	X
FDP_IFC.1_UI	FDP_IFF.1_UI	X
FDP_IFF.1_Tx	FDP_IFC.1_Tx	X
	FMT_MSA.3_Tx	X
FDP_IFF.1_Rx	FDP_IFC.1_Rx	X
	FMT_MSA.3_Rx	X
FDP_IFF.1_Rec	FDP_IFC.1_Rec	X

	FMT_MSA.3_Rec	X
FDP_IFF.1_UI	FDP_IFC.1_UI	X
	FMT_MSA.3	X
FDP_IFF.5_Tx	FDP_IFC.1_Tx	X
FDP_IFF.5_Rx	FDP_IFC.1_Rx	X
FDP_IFF.5_Rec	FDP_IFC.1_Rec	X
FDP_IFF.5_UI	FDP_IFC.1_UI	X
FDP_ITC.1_Tx	FDP_IFC.1_Tx	X
	FMT_MSA.3_Tx	X
FDP_ITC.1_Rx	FDP_IFC.1_Rx	X
	FMT_MSA.3_Rx	X
FDP_ITC.1_Rec	FDP_IFC.1_Rec	X
	FMT_MSA.3_Rec	X
FMT_MSA.1_Tx	FDP_IFC.1_Tx	X
	FMT_SMR.1	
	FMT_SMF.1	X
FMT_MSA.1_Rx	FDP_IFC.1_Rx	X
	FMT_SMR.1	
	FMT_SMF.1	X
FMT_MSA.1_Rec	FDP_IFC.1_Rec	X
	FMT_SMR.1	
	FMT_SMF.1	X
FMT_MSA.3_Tx	FMT_MSA.1_Tx	X
	FMT_SMR.1	
FMT_MSA.3_Rx	FMT_MSA.1_Rx	X
	FMT_SMR.1	
FMT_MSA.3_Rec	FMT_MSA.1_Rec	X
	FMT_SMR.1	
FMT_SMF.1	-	-
FPT_FLS.1_SAFE	-	-
FPT_FLS.1_Current	-	-

Table 19: Fulfillment of TOE SFR 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.1 (Security Management Roles) is not included because:

-   Only authorized persons have physical access to the TOE (see OE.Physical_Access, OE.Physical_Protection, OE.Authorization).

-   All users with physical access to the TOE (S.Operator) have the permission to manage the security attributes (operate the Tx and Rx voice switcher) (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 initialization or management.

8.4.1.3   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.1).

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

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

8.4.2   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. 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 ([2], chapter 8.7-8.9).

Because ASE_TSS.1 belongs to EAL4, the TOE developer is required to describe at an early stage how the TOE protects itself against tampering bypass.

Because AVA_VAN.3 belongs to EAL4, we assume attackers who possess Enhanced-Basic attack potential. AVA_VAN.3 ensures that penetration testing is carried out by the evaluator to determine that the TOE is resistant to attacks performed by those attackers.

8.4.3   Conclusion

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

9. TOE Security Summary Specification

9.1 TOE security functionality

This section summarizes the TOE 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.

9.1.1 Voice Information Flow Control (TSF.VFC)

The TOE Security Functional Requirements satisfied within the following subchapters are *FDP_ETC.1, FDP_IFC.1_Tx, FDP_IFC.1_Rx, FDP_IFC.1_Rec, FDP_IFF.1_Tx, FDP_IFF.1_Rx, FDP_IFF.1_Rec, FDP_IFF.5_Tx, FDP_IFF.5_Rx, FDP_IFF.5_Rec, FDP_ITC.1_Tx, FDP_ITC.1_Rx, FDP_ITC.1_Rec, FMT_MSA.1_Tx, FMT_MSA.1_Rx, FMT_MSA.1_Rec, FMT_MSA.3_Tx, FMT_MSA.3_Rec* and *FMT_MSA.3_Rx*.

9.1.1.1 PTT Operation
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 Blue LED (MIC ACTIVE) on the TOE front panel and also on the Management Interface (TSF.MNI).

9.1.1.2 Tx Voice router
TSF.VFC.3

One common Tx voice router is routing the Microphone_Inputs either to the RED_ PU_Interface or to the BLACK_PU_Interface according to domain status (RED/BLACK). The Tx voice router provides two modes:

- SECURE: Microphone_Inputs are disconnected from the BLACK_PU_Interface. Microphone_Inputs are connected to the RED_ PU_Interface, if the associated PTT is activated and audio device is present (e.g. Headset).

- UNSECURE: Microphone_Inputs are disconnected from the RED_ PU_Interface. Microphone_Inputs are connected to the BLACK_PU_Interface, if the associated PTT is activated and audio device is present (e.g. Headset).

TSF.VFC.4

The Initial/Default-State of the Tx voice router is SECURE.

TSF.VFC.5

The status of the Tx voice router is set and indicated via the Management Interface (TSF.MNI)

9.1.1.3   Rx Voice router
TSF.VFC.6

All Voice_Rx_Information received from the RED and BLACK Processing Units is routed to the Earpiece_Outputs according to one common Rx voice router. The RX separator provides three modes:

- SECURE: The Voice_Rx_Information from the RED_PU_Interface (CLASSIFIED) is connected to the Earpiece_Outputs. Voice_Rx_Information from the BLACK_PU_Interface is disconnected.

- UNSECURE: The Voice_Rx_Information from the BLACK_PU_Interface (UNCLASSIFIED) is connected to the Earpiece_Outputs. Voice_Rx_Information from the RED_ PU_Interface is disconnected.
- MIXED: The Voice_Rx_Information from the RED_PU_Interface (CLASSIFIED) as well as from the BLACK_PU_Interface (UNCLASSIFIED) is connected to the Earpiece_Outputs.

The Rx voice router inhibits Voice_Rx_Information flow between RED_PU_Interface and BLACK_ PU_Interface.

TSF.VFC.7

The Initial/Default-State of the Rx voice router is SECURE.

TSF.VFC.8

The status of the Rx voice router is set and indicated via the Management Interface (TSF.MNI).

TSF.VFC.9

The Loudspeaker_Output is always connected to the BLACK_PU_Interface only.

TSF.VFC.10

Not applicable

TSF.VFC.11

If the handset (Mic_Input_Handset) is used (PTT active), the Rx voice is always on the same domain SECURE/ UNSECURE as Tx voice.

If the headset (Mic_Input_OP1_Headset) is used (PTT active), the Rx voice is always on the same domain SECURE/ UNSECURE as Tx voice.

If the headset (Mic_Input_OP2_Headset) is used (PTT active), the Rx voice is always on the same domain SECURE/ UNSECURE as Tx voice.

TSF.VFC.12

The output level of Analogue Audio Outputs shall be independently adjusted by Operator.

TSF.VFC.13

The output level of Analogue Audio Outputs shall not adjust bellow audible threshold.

9.1.1.4 Rec Voice router
TSF.VFC.14

All Voice_Rx_Information received from the RED and BLACK Processing Units are routed, by using the Voice_Rec_Information channel, only to the RED Processing Unit.

All Voice_Tx_Information received from Microphone_Inputs during PTT active are routed, by using the Voice_Rec_Information channel, only to the RED Processing Unit.

TSF.VFC.15

The Initial/Default-State of the Rec voice router is SECURE.

TSF.VFC.16

The security attribute (CLASSIFIED / UNCLASSIFIED) for Voice_Rec_Information received from Voice_Rx_Information is set by Rx voice router.

The security attribute (CLASSIFIED / UNCLASSIFIED) for Voice_Rec_Information received from Voice_Tx_Information is set by Tx Voice router.

TSF.VFC.17

The direction Rx attribute (RECEIVED) for Voice_Rec_Information received from Voice_Rx_Information is set by Rx voice router.

The direction Tx attribute (TRANSMITTED) for Voice_Rec_Information received from Voice_Tx_Information is set by Tx voice router.

9.1.2 Management Interface (TSF.MNI)

The TOE Security Functional Requirement satisfied within the following subchapters is *FMT_SMF.1*.

9.1.2.1 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.Operator.

The state of the TOE is indicated via the following LEDs:

- One Green LED at the front panel of the housing indicating the voice router SECURE state,

- One Red LED at the front panel of the housing indicating the voice router UNSECURE state,

- One Blue LED at the front panel of the housing indicating at least of one the Microphone_Inputs is active and transmit Voice_Tx_Information according to Tx voice router status,

- One External Red lamp indicating when CLASSIFIED Voice_Information can be handled by the Operator.

9.1.2.2 GUI Device (TED)
TSF.MNI.2

The TOE includes an interface for Touch Entry Device for visual presentation of the voice router control. The interface provides modes to set the states of voice router and PTT as well like Visual indication of the communication states to S.Operator[2].

TSF.MNI.3

The state of the TOE is indicated via TED as follow:
- A Green horizontal line on the middle of GUI and blur colors of the lower half of GUI indicating the voice router is in the SECURE (RED) state;
- A Red horizontal line on the middle of GUI and blur colors of the upper half of GUI indicating the voice router is in the UNSECURE (BLACK) state;

9.1.2.3 GUI Interface
TSF.MNI.4

The PUs provide a GUI interface for each domain at a time, based on press action on the certain area.

9.1.2.4 Audio Interface
TSF.MNI.5

The TOE generate a Message Tone on audio device (Headset or Handset) output interface during domain switching from UNSECURE (BLACK) state to SECURE (RED) state. This Message Tone is summed with current voice signal.

9.1.3 User Interface Data Flow Control (TSF.DFC)

The TOE Security Functional Requirements satisfied within the following subchapters are *FAU_ARP.1, FAU_SAA.1, FDP_IFC.1_UI, FDP_IFF.1_UI* and *FDP_IFF.5_UI*.

TSF.DFC.1

The TOE implements a filter for the User_Interface_Data in order to prevent the user interface connection from being misused to bypass the Voice Information.

TSF.DFC.2

In the direction from the BLACK_PU_Interface and RED_PU_Interface to the TOE (Inbound) the filter performs the following checks:

- The checksum of the Transport_Data is correct.

- The Transport_Data is syntactically correct.

- The Application_Message_Type is permissible.

- Payload_Data_Rate not exceeds the data rate predefined limits.

---

[2] *The visual presentation on the GUI of the PTT active and device present is a VCS function.*

TSF.DFC.3

In the direction from TOE to the RED_PU_Interface and BLACK_PU_Interface (Outbound) the filter performs the following checks:

- The checksum of the Transport_Data is correct.

- The Transport_Data is syntactically correct.

- The Application_Message_Type is permissible.

- Payload_Data_Rate not exceeds the data rate predefined limits.

TSF.DFC.4

The maximum permissible Payload_Data_Rate is fixed (not manageable).

The limit of 800bit/s prevents any comprehensive continuous understandable voice transmission in realtime voice transmission via the trusted filter from RED_PU_Interface to BLACK_PU_Interface as well as from BLACK_PU_Interface to RED_PU_Interface

The limit of Rx voice packets data rate from RED_PU_Interface and BLACK_PU_Interface is limited to the generated data rate for Tx voice packets from TOE.

The TOE configuration packets are permitted one time per Log-in session.

TSF.DFC.5

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

Else if the message pass following subset of checks defined by TSF.DFC.2 and TSF.DFC.3 and exceed the Payload Data Rate defined by TSF.DFC.4 then the TOE will:

- visually indicate a failure to warn the S.Operator,

- immediately switch to RED domain.

Note: A visual indication is either a message displayed by TOE on the appropriate TED or a message signalized using the two LEDs: RED (UNSECURE LED) and GREEN (SECURE LED), depending on the failure.

9.1.4 Protection of the TSF (TSF.PRT)

The TOE Security Functional Requirement satisfied within the following subchapters are: *FPT_FLS.1_SAFE* and *FPT_FLS.1_Current*.

9.1.4.1 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, in case of setting the domain status using TED, is implemented redundantly ensuring that a single failure will not result in an UNSECURE state.

On the one hand, these security functions are implemented by firmware. On the other hand, a hardware implementation (SECURE and UNSECURE Redundant Gate) check the firmware decision and connect or disconnect the signal lines for voice information to RED_PU_Interface /BLACK_PU_Interface if there is a match between the selected area on the TED and the state indicated by the firmware, if there is a mismatch between firmware and hardware then TOE will preserve the state. In this type of failure TOE will indicate on the inactive area of the TED an failure message.

The functionality of the Redundant Gate prevents that a single failure (either of the firmware or of hardware) will result in an wrong state. E.g. if the TED indicates that RED domain is selected, but in reality (due to a failure) the Voice_Tx_Information is routed to the BLACK_PU_Interface, the Redundant Gate will disconnect the signal lines from the BLACK_ PU_Interface.

TSF.PRT.4

TOE indicates the next type of failures to the TED using visual messages thus the S.Operator recognizes any malfunction of the TOE:

- Missing HID / Wrong device (USB touch controller is not attached)

- Communication with any PU is lost

- Built in Test failed

- TAS-FO does not detect GUI activity on PUs

- TAS-FO does not detect X-Server activity on PUs

- TAS-FO detects unexpected PUs video resolution

- No Operator is authenticated on the PUs to the VCS

- Payload_Data_Rate exceeds the data rate predefined limits

- Power-Up initialization Fail

In those cases TOE will preserve the SECURE state.

TSF.PRT.5

TOE indicates the next type of failures using the front panel LEDs messages indication, thus the S.Operator recognizes any malfunction of the TOE:

- Missing / Wrong Display attached to HDMI port

- Built in Test failed

9.1.5 Mapping of SFRs to TSFs

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	TSF	Name
FDP_ETC.1	TSF.VFC	Voice Information Flow Control
FDP_IFC.1_Tx		
FDP_IFC.1_Rx		
FDP_IFC.1_Rec		
FDP_IFF.1_Tx		
FDP_IFF.1_Rx		
FDP_IFF.1_Rec		
FDP_IFF.5_Tx		
FDP_IFF.5_Rx		
FDP_IFF.5_Rec		
FDP_ITC.1_Tx		
FDP_ITC.1_Rx		
FDP_ITC.1_Rec		
FMT_MSA.1_Tx		
FMT_MSA.1_Rx		
FMT_MSA.1_Rec		
FMT_MSA.3_Tx		
FMT_MSA.3_Rx		
FMT_MSA.3_Rec		
FAU_ARP.1	TSF.DFC	User Interface Data Flow Control
FAU_SAA.1		
FDP_IFC.1_UI		
FDP_IFF.1_UI		
FDP_IFF.5_UI		
FMT_SMF.1	TSF.MNI	Management Interface
FPT_FLS.1_SAFE	TSF.PRT	Protection of TSF
FPT_FLS.1_Current	TSF.PRT	Protection of TSF

Table 20: Mapping of SFRs to TSFs

9.2   Assurance Measure

The TOE satisfies the CC EAL 4 security assurance requirements with the conformance statement provided in Section 5 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.